what	question	
1	ad	Active Directory is an implementation of LDAP directory services by Microsoft for use in middleMicrosoft Windows. Active Directory allows administrators to set policies, install programs on many computers, or apply critical updates throughout the organizational structure. Active Directory stores its information and settings in a central organized database. Active Directory contains both logical and physical structures of network components. a) Logical 1.Organization units 2.Domains 3.Tree trees 4.Forest domains b) Physical 1.Network s 2.Networks
2	agpm	Microsoft® Advanced Group Policy Management helps ensure ongoing configuration requiredh Set security on computers through enhanced Group Policy Object Management (GPO) control and management. Computer control makes it easier to control changes to GPOs and to edit them offline. The result is lower risks and reduced end-user outages caused by conflicting or incorrectly configured objects group policy.
3	application pool	Thanksy app pool runs applications independently, one does not shoot other processes. Plus, it's running separately from inetinfo. Recycling-automatic restart (-after time, -after a certain number of requests, -at time, -according to memoirs) divides applications so that they cannot affect other applications on the server. They achieve thatusing the so-called worker process isolation mode. In addition, IIS 7 distinguishes how to handle a request that includes managed resources - using either Integrated mode or Classic mode.
4	HPC architecture	Firsth The 10 most powerful supercomputers in the TOP500 rankings have the same basic architecture. Each is a cluster of Multiple Instruction Stream (Multiple Data Stream) multiprocessor arrays, with each processor having a Single Instruction / Multiple Data architecture (SIMD). executable instructions on a single SIMD processor.

5	archiving and backup	Backed upform an "insurance" against the accident, we back up so that we are able to quickly restorest fully functional state of the system. Backups should be as up-to-date as possible so that we lose as little data as possible if we need to restore Backup types: -Normal (full) - all selected files are backed up regardless of whether they have changed since the last backup -Copy - as usual copying -Incremental - Only what has changed since the last backup is backed up. The attribute changesarchive - Differential - Only what has changed since the last backup is backed up. It does not changearchive attribute - Daily copy - everything that has changed during the day is backed up. Archiving is used to store data in a safe place, they are intended for later use. SundayIt is taken as often as backups. Mostly on external media, eg optical medium
6	What is Auditing? Wherecan we find information about audits and what is all we need to do to ensure that audits are conducted?	Automatic event tracking, audit information is in the Event viewer in Security. Adjustthrough the local security policy or then in the Group Policy Auditing a network's activities is a very important process from a security perspective. It is differenttopic impossibleFor example, find that a user has failed to log in for the second time in the last two minutes, that a user account has been locked, or that an unauthorized user has tried to access files in a shared folder to which he or she has not been granted the necessary permissions. It is always possible to audit successful attempts and unsuccessful attempts. While successful attempts to monitor objects may not be of interest to administrators (they do not provide any information because an expected event occurred), they can be useful in logging audits. When you configure the audit, it is theto consider what to audit.
7	What is DHCP?	Dynamic Host Configuration Protocol (DHCP) is a family name protocol in computer science TCP / IP or the designation of the corresponding DHCP server or client. Used forautomaticallyfor configuring computers connected to a computer network. The DHCP server assigns computers the IP address, netmask, default gateway and DNS server address using the DHCP protocol. The validity of the assigned data is limited, so it is running on the computer DHCP client that extends their validity.
8	what DNS is and how the name translates	DNS (Domain Name System) is a hierarchical system of domain names that is implemented DNS servers and the protocol of the same name through which they exchange information. Its main task and cause is the mutual transfer of domain names and IP addresses of network nodes. However, he later acquired other functions (eg for e-mail or IP telephony) and today serves de facto as a distributed database of network information. The DNS system is a globally distributed database that records which IP address belongs to which domain name, while the IP address can have domain names even more. The database is taken care of by programs called name servers, which provide data from the database to clients, the so-called resolvers.

9	What is a domain, a domain tree, a forest, a connection option (instead of a "connection" was probably another word)	Domainand is a logical group of computers sharing a common central directory database (AD). Domainsý tree is a hierarchical connection of domains created by the parent-child relationship, all domains within the tree share the same namespace, the schema is the same within the domain tree. The forest is the security and administrative boundaries of all the objects that are in it they find. Type of trust relationship, parent-child
10	What is virtualization?	Virtualization allows more than one server to run on a single physical server (hardware) separate servers with their own operating system. A physical server for eachvirtualat the server emulates virtual hardware (processor, memory, disk, network card, drives, peripherals and more). However, the customer does not know at first glance that the server is virtualized. It has its own server with processors, memory and other components, some operating system of its choice runs on it, it has full access to it and works with it as if this operating system ran on its own hardware
11	What is virtualizationWhat is the understanding of a system's state of backup?	Currentcomputer configuration, this includes in particular: Registry RegistrationCOM + class database Startup files including system files Database Certification Services DirectoriesActive Directory SYSVOL Cluster service information Addressi with IIS metadata System files that are protected by Windows In Backup, these system components are referred to as System Status data. The exact system components that make up the System State data depend on the computer's operating system and configuration.
12	DFS	Systemm DFS is practically a signpost that simplifies the orientation and access of users to to different shared folders, which can be "scattered" across different servers in the net. Distributed File System (DFS) allows administrators to group network shares into a single DFS malways the so-called root - this is the shared folder, which contains links (something like shortcuts) to local and remote shared folders. Users now only have to remember one path to the shared folder to take full advantage of DFS, as they will then have access to all componentsfor which they need.

13	Disk array (RAID x etc)	(lecturesand No.4 - data security; slide 3 - 6) RAID (Redundant Array of Independent Disks) RAID 0 (stripping) - not redundant, eg, Disk1 (A1, A3, A5, A7), Disk2 (A2, A4, A6, A8). If one of the disks crashes, we will lose all data. Another advantage is the acceleration of writing RAID 1 (mirroring) - the disks contain the same data (mirroring), so in the event of a crash of one of the disks, we do not lose data. But again, it requires more resources (it needs more space) RAID 5 - stripping with distributed parity, requires min. 3 discs, more can be used (up to 32).Nensuitable for high I / O load. No data is lost in the event of an accident. RAID6 - the same principle as RAID5, but uses double parity; suitable for large fieldsdisks
14	DNS cache	Topic eachý DNS server also works as a DNS cache. For repeated queries then there is no recursive tree search, but the answer is obtained locally. This is because DNS records also store information on how long the record can be used (TTL) and how can it be find out if the record has changed. When it expires, the record is deleted from the DNS cache.
15	domain, structure, tree, relationships between them	1. Domainand is an essential element of the logical structure of AD. Objects are stored directly in the domain (mane millions) that belong to the domain. 2. The domain structure is the security and administrative boundaries of all buildings, which are found in it. 3. A tree is a grouping or hierarchical organization of one or more domains. 4. RelationshipTrust issues are authentication channels that provide users in one domain with access to resources in another domain.
16	dynamic DNS update	Dynamic update allows client computers to register and register dynamically updatedt resource records on the DNS server whenever a change occurs. This reduces the need for manual administration of zone records, specifically for those clients who frequently they change location and use DHCP to obtain an IP address.
17	event viewer	Console for monitoring all system events, each event has its own Source, ID, date, time, computer, type of event (information, warning, error, audit success, audit failure). Events are divided into: 1. Basic system (apps, system, security) 2. Application (for some services) (DNS, ad, DFS replication) 3. Other logs (detailed logs of individual activities) We can filter logs. Logs are stored in * .evtx files
18	GP	a tool for bulk management of permissions and settings applied to both the entire computer and nand the logged in user. Used for: - appliedcompany standards (hiding control panels, network printers, running scripts) - security application (change of permissions on certain folders, password complexity, groupswith the option to log in locally) - bulk installation of applications (Office, Adobe Reader, etc.)

19	GPO management - principles	
20	FSMO role	-Main schema server (Schema Master): One master role holder in onedomain structure. The schema master FSMO role holder is the domain controller responsible for directory schema updates. - Domain Naming Master: One role holder mainabout a server in a single forest. The domain name master FSMO role holder is the domain controller responsible for making changes to the domain-based directory namespace throughout the forest. - Infrastructure Master: One master role holder in one domain. The infrastructure FSMO role holder is the domain controller responsible for updating the SID and distinguished name in the cross-domain object reference. - Relative ID master server (RID Master): One master role holder in one domain. The relative ID (RID) master server FSMO holder is one domain controller responsible for processing RID pool requests from all domain controllers in a given domain. - Emulater Primary Domain Controller (PDC Emulator): One master role holder in one domain. The PDC emulator FSMO role holder is a Windows domain controller that advertises itself to workstations, member servers, and domain controllers that use earlier versions of Windows as the primary domain controller. It is also the main domain crawler that it also handles password mismatches.
21	IIS	Internet Information Services (IIS) is a Web server application and settings module function, created by Microsoft for use with Microsoft Windows. This is the most used web server after Apache HTTP Server. IIS 7.5 supports HTTP, HTTPS, FTP, FTPS, SMTP and NNTP. It is an integral part of the Windows Server product line, as well as some editions of Windows XP, Windows Vista and Windows 7. IIS is not by default settings on.

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). Identity servicesand certificates allow administrators to manage user accounts, and digital certificates allow them to access specific services and systems. Federationn management services, in turn, pave the way for the management of shared resources between authenticated partners and customers, with the possibility that, for example, an IT consultant can use company credentials to connect to the client's network. Active Directory Metadirectory Services. ROLE: Stand alone, Member server - Application server, Domain Controller. File server, Domain Controller, Print server, DHCP server, DNS server, Mail server, Database server, SMS server, IIS server (web) installation types: - core - a command line suitable for servers is installed - full - including gui

23	IIS write what services it provides	1. Common HTTP Features - basic webserver - Static Content, Default Document, Directory Browsing, HTTP Errors, HTTP Redirection 2. Application Development Features - .NET application server - ASP.NET, .NET Extensibility, ASP, CGI, ISAPI Extensions, ISAPI Filters, Server-Side Includes 3. Health and Diagnostics Features -services for server logging and diagnostics - HTTP Logging, Logging Tools, Request Monitor, Tracing, Custom Logging, ODBC Logging 4. Security Features -security services -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 -Improving server performance -Static Content Compression, Dynamic Content Compression 6. Management Tools -services for server management, scripts and consoles -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 -according to OS version (WS2008 unlimited)
24	how to access the domain via the command line	User account management, group management - dsadd reset user password, enable and disable user account - dsmod find group - dsget search within AD - dsquery

25	how to delete an object in AD and how to restore it?	- when an object is deleted, it is not deleted from the database, the object is marked for after deletion laterremoval, this flag is replicated to other controllers, only later is the garbage collection process physically removed from the database, these objects are called tombstones, garbage collection also deletes unnecessary logs, then the process starts the defragmentation thread Recovery: In addition to authoritative recovery from a backup, there is a tool from Microsoft ADDRESSORE. EXE. It is a line utility that allows you to restore an object using adrestore -r after installation

26	what groups are in the security dependency domain, describe the individual groups and how to set them up	Group types: Local Security Distribution Range of groups: 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	Active Directory integrated zone: this is the primary zone that has no records in text file, but stores them directly in the AD database

	and the zone in the text file	

28	What is the difference between iterative translation and forwarding	IterativeIf the query goes to a DNS server, answers can come from other servers. Forwarding uses a recursive query.
29	How can we protect users' mail from viruses, spam, and attacks?	Antispam, firewall settings, creating a new mail account, antivirus program, mail filtering
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. --- Something in the road: IIS 7 has a global configuration file, which contains the default settings of the web server and the applications running on it. Each application then has its own configuration file, which essentially "overwrites" the default settings of the IIS 7 web server.
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 These tools are associated with 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 Microsoft Management Console (MMC) snap-in 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	ANDD Users and Computers - creation of domain accounts, division into categories, assignment of rights, Group Policy Management - setting of policies for PCs, PC groups Remote Desktops - remote connection to 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 - I would say that disk manager for creating partitions, volumes, etc. (I'm not sure) 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 - Protocol standard for user and system authentication. It is primaryauthentication mechanism for Windows 2000 and higher NT LAN Manager (NTLM) - Primary authentication protocol for systems Windows NT. Secure Socket Layer / Transport Layer Security (SSL / TLS) - Primaryprovides an authentication mechanism for access to secure web servers. DACL - sheet 1 or more ACLs over the object also: (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. And apparently it's a cluster of ACEs ACE - Allow / Deny for individual activities over the object for the user or group AD
37	ITIL elements	createdin the domain - dcpromo

38	Registry	theoretically - a hierarchical database containing settings for Windows OS and applications, practically - a place where we find system and application settings that are not otherwise available, object types: registry key e folder equivalent, registry value contains data (custom settings), HKEY_LOCAL_MACHINE (HKLM), HKEY_USERS (HKU)), HKEY_CURRENT_USER (HKCU), registers have a binary structure, each value has a defined data type, the most commonly used - REG_SZ (UTF-16 string), REG_MULTI_SZ (UTF-16 string array), REG_DWORD (numeric value 32bit), REG_QWORD (numeric value 64bit), REG_BINARY (arbitrary data)

39	the distribution of groups according to scope and security, strategy of use and their description	by range: -domain local - permissions for one domain, user members. And a pc from the wall domain -global - permissions for objects in any domain within the forest, members of only groups from the same domain -universal - permissions in different forest domains Group strategies: A - Accounts, G - groups, U - universal groups, DL - domain local groups, P-permissions, L-local groups; Strategy: AGP, AG DL P, AGU DL P, A GG DL P, A GL P
40	splitting bills and shortly about them	Computer accounts Why computers have accounts - They identify computers in the domain -Play itverification and audit of network access and network resources -Play itSet rights for computers (eg when installing software) User accounts
41	groups	Get togetherobjects of the same type (eg users), which we can then set different approachesrights and privileges. Ex. the "librarians" group will certainly have different rights than the "administrators" group

42	services (print spool, etc)	AD, DNS, IIS, DHCP, Windows Update, Themes, Windows Defender, System Time, Each the server application should be installed as a service, http://buchtic.bloguje.cz/251263-systemove-sluzby-windows.php
43	System file management	
44	System Event Notifier, Terminal Services, Windows Time, Workstation	System event notification service Far awaynetwork connection and access to PC resources Time synchronization in the domain API redirector, which gives the computer network access
45	WS 2008 license types and when to use	foundation - the basis for small businesses standard - common standard enterprise - clustering, price approx. 65 thousand data centers - price approx. 150k Web server HPC - for super servers Win.Small Bussiness server 2008 Standard / Premium installation types: - core - a command line suitable for servers is installed - full - including gui

46	DNS record types and description	Common record types: ◦ A - IPv4 host; AAAA - IPv6 host ◦ CNAME - alias ◦ MX - mail exchanger ◦ SRV - service locator ◦ PTR - pointer (reverse translation) ◦ SOA - start of authority; defines some zone parameters ◦ NS - name server
47	Levels of MS 2008 server installation, dependency on compatibility with other OSs, description of levels (Forest and Domain level)	foundation - the basis for small businesses standard - common standard enterprise - clustering, price approx. 65 thousand data centers - price approx. 150k Web server HPC - for super servers Win.Small Bussiness server 2008 Standard / Premium installation types: - core - a command line suitable for servers is installed - full - including gui
48	UAC levels	There are 4 levels in Windows 7 and 2008 R2: ◦ "Always notify" (also in Vista and 2008 R1) Requires confirmation for all use of Administrator rights ◦ "Default" - Request permissions for programs Does not require notification for system configuration ◦ "Default without secure desktop" - Request permissions for programs without a secure desktop ◦ "Never notify" (also in Vista and 2008 R1) Disable the UAC function
49	Network attacks, protection	backdoor, port scanning, social methods, ethernet eavesdropping, stack overflow, attacks against www, IP spoofing Barriers: network user authentication, station security, traffic security, security HIND
50	Advantages and disadvantages of CMD	- oproteven Linux consoles confusing and weak system completion of commands and addresses tab - greater demands on the programmer - speedt work depends on experience and knowledge of commands + there is no risk of a click + speed of work + there is no need to search for something in deep menus or confusing GUIs + admin is not restricted by GUI + possibility of remote administration via 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 Incidentt Management - a process ensuring the fastest possible resumption of service delivery and minimizing the consequences of service outages on business activities Releasese Management - a process ensuring successful distribution and deployment of change in the ICT infrastructure Problem Management - the process of finding out the original causes of incidents
52	name the DNS zones	Zones are divided into: ◦ Ordinary (data in text file) ◦ AD Integrated (data in AD database) -Availableonly on AD domain controllers ◦ Primary -Writable copy DNS zones, each zone has exactly one primary copy ◦ Secondary -Exists read-only, updates with so-called "zone transfers" from the primary zone -Use for redundancy and load distribution -The case can be promoted to primary ◦ Stub
53	Explain what these services are: Alterer (? Not sure), Automatic Update, DHCP Client, Computer Browser	Alerter service: Microsoft service, used to send administrative notifications, alerts users to security, access, and relational issues Automatic Update: allows you to download and install Windows Update. If this service is turned off, Positive is not able to update automatically or the Windows Update Web site. DHCP Client: Manages network configuration by registering and updating IP addresses and DNS names Computer Browser: maintains an updated list of computers on the network and supplies this list computers designated as browsers
54	certificate life cycle, and its attributes	Beginningby creating a request. Then a certificate is issued and it is checked and we can use it. This is followed by either the expiration of the certificate, or during that time we can use this onecertificatest recall (for example, someone attacks our server, etc.). ATof overd expiration can renew the certificate and again it is true that we can then revoke or expire. Thusstill around.

55	methods of authentication in IIS	1. Anonymous (default)) - public access for anyone without verification 2. Basic - uses windows accounts, HTML 1.0 component, allows authentication through proxies, is not secure if we do not use SSL / TLS, allows integration with Kerberos, requires creation of individual windows accounts 3. Digest - removes the main weakness Basic, ie sending passwords as plain text, does not require SSL / TLS to protect passwords, also works with proxies and firewalls, but requires IE5 +, cannot delegate permissions, requires saved passwords in plain text due to reverse translation, requires AD accounts , without the use of SSL / TLS is usually the target of replay attacks 4. Integrated Windows (default) - also known as NTLM, uses NTLM or Kerberos, the best choice for intranets, cannot log in through the firewall, does not allow delegation to other servers when NTLM is selected 5. Client certificates - high security, provides two-way authentication serverua client, allows access to network resources, does not work with all browsers, requires SSL / TLS, can not delegate permissions, more complex settings
55	methods of authentication in IIS	1. Anonymous (default)) - public access for anyone without verification 2. Basic - uses windows accounts, HTML 1.0 component, allows authentication through proxies, is not secure if we do not use SSL / TLS, allows integration with Kerberos, requires creation of individual windows accounts 3. Digest - removes the main weakness Basic, ie sending passwords as plain text, does not require SSL / TLS to protect passwords, also works with proxies and firewalls, but requires IE5 +, cannot delegate permissions, requires saved passwords in plain text due to reverse translation, requires AD accounts , without the use of SSL / TLS is usually the target of replay attacks 4. Integrated Windows (default) - also known as NTLM, uses NTLM or Kerberos, the best choice for intranets, cannot log in through the firewall, does not allow delegation to other servers when NTLM is selected 5. Client certificates - high security, provides two-way authentication serverua client, allows access to network resources, does not work with all browsers, requires SSL / TLS, can not delegate permissions, more complex settings
57	sharing	we set share permissions hidden sharing - last character $, does not affect permissions, the item is not displayed to the client, usefor example, to share scripts

58	politics what it is and what it serves	They are set in the Group Policy Management Editor. Here we can set up to 2000 different setfrom the length of the password to the icon on the desktop. The policy created and set up in this way is then "linked" in Group Policy Management (gpmc.msc) to various domain objects, ie groups or organizational units. Polity, resp. GPO lines have several attributes. Enforced - politics takes precedence over others, "pushing". Pak Link enabled / disabled; Deleted - the link can be deleted, but the GPO remains; a multiple links - a case where multiple GPOs are linked to a container. Important is establishedorder of politicians!
59	what is WINS and its use	WINS - is an MS implementation NetBIOS Name Server (NBNS) for Windows, serving howo name server for computer names in a NetBIOS network environment. Provides a distributed database that maps NetBIOS names to IP addresses. This service was created to address name resolution issues for interfaceNetBIOS in routed environments.
60	Netbios	NetBIOS - is a software interface (API) for access to network communication at the relational level (session) layers. The specific transport protocol, as well as the physical addresses of the stations, are hidden from the programmer. NetBIOS is primarily a set of standard functions, these are independent of the lower layers (and therefore the packet format). E.g. in Microsoft networks, is used for transport protocolat NetBEUI (within LLC?), or TCP / IP and sometimes 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?	Rights - Actions in the system (time change, system settings, ...) Permissions - Object Operations (Read / Write / ...)