Last updated June, 2000. Click here for updates.

Click here to see additional documents related to this study guide.

Contents

Cramsession™ for Designing a Microsoft Windows 2000 Directory Services Infrastructure

Abstract:

This Cramsession will help you to prepare for Microsoft exam 20-219, Designing a Microsoft Windows 2000 Directory Services Infrastructure. Exam topics include Unified Directory Services such as Active Directory and Windows NT Domains, Connectivity of Systems, System Components, and Applications, and Data Replication.

Designing a Microsoft Windows 2000 Directory Services Infrastructure

Analyzing Business Requirements

It is important to identify the business model in place for a number of reasons. Key among them is the fact that similar businesses often have similar needs and requirements. Knowing the geographic scope can help define the infrastructure employed by the IT department. The geographic models and scopes can be summarized as:

Model	Comment
Regional	When implementing technologies that are within companies restricted to regional boundaries, you can often pay less attention to such things as international translations than you would with different models.
National	Of a grander scale than regional, you can still often overlook many factors such as international regulations
International	Importance must be paid to translations, regulations, laws, and representatives from all countries should be involved in IT decision-making processes
Subsidiary	When working with a subsidiary of a larger conglomerate, make certain that approval for the solution generated will be acceptable to the parent company
Branch office	You must go to lengths to verify that solutions implemented here work with technologies employed throughout the rest of the company

During the design phase, it is important to ask such questions as:

- Who is in charge of each department?
- Who manages user accounts (are central polices used)?
- Who manages resource accounts?
- How is administration divided?
- Who must sign-off on purchases and policies?

All processes employed by the company should be documented and diagrammed. Of key importance are company processes related to:

Process	Comment
Information flow	This typically follows the organization chart, but can differ with geographic breaks
Communication flow	It differs from information in that it often lacks formal structure and comes about as a result of communication with others (customers, vendors, etc.).
Service/Product lifecycles	Consider the lifespan of the product: this differs for each product. A computer book may be expected to last 12 months, while a weekly magazine has a lifespan on only 1/52nd of that.
Decision-making	This can follow the organizational chart, or be completely dispersed if the company practices empowerment.

It is important to analyze existing and planned organizational structures when deciding business requirements. These categories can break down into the following key areas:

- Management model - determine if you are dealing with a family-owned, privately held business, or a public company with a CEO and Board of Directors. In the latter, operation and ownership become separate, and can be driven by the need for profit and quick solutions versus long-term planning. Different risk models can be associated with different management models.
- Company organization - some organizations are divided by products (transmissions in one division, four-wheel-drive axles in another, etc.), while other organizations divide operations and responsibilities purely on geographic terms.
- Vendor/partner/customer relationships - know the contact points and whether web presence is offered on an Internet, intranet, and/or extranet basis.
- Acquisition plans - is the company you are designing a solution for actively seeking acquisitions (meaning you must plan for future growth), or are they a likely acquisition target?

Factors that can influence company strategies are many. For the exam, you should know the following five:

1. Company priorities - never assume these are constant. They can change with management teams, market shifts, etc.
2. Projected growth and growth strategy - how is expansion accomplished (acquisition, divestiture, franchises, and so on)
3. Relevant laws and regulations - these are always subject to change, and must be watched carefully. Is the company in a high-profile position (such as house arrest) to be greatly affected by new legislation? Do they work with encryption, spamming, or other areas popular with lawmakers? Are there local laws, or international laws, that can affect the organization?
4. Company's tolerance for risk - how does the company weigh risk against profit: vulnerability against value? Do they employ basic security devices on

sites, such as firewalls, SSL (Secure Sockets Layer), and such? Do they employ physical security at the facility such as card readers, badges, and the like? Do they insist new employees receive training, or are they turned loose for on-the-job training in all instances?

5. Total cots of operations - what is the value of the company's data; of the IT staff's budget; of having server access 24 hours a day versus 8, etc.? Microsoft uses seven categories to group budgeted costs: Hardware and software costs, Management costs, Development costs, Support costs, Communication costs, End-user costs, and Downtime costs.

The structure of IT management should weigh heavily in the analysis of business requirements. Factors that help understand the management structure are shown in the following table:

IT Factors	Comment
Administration type	This can be centralized or decentralized. A classic example of the former would be a segment of government such as HUD or OSHA. All administrators are stationed in Washington, D.C., while branch offices exist throughout the United States. Whenever a branch office needs administration, such as installing new software, it is done remotely (often through SMS). With a decentralized model, an administrator(s) is stationed at each branch office to handle the needs at that office. Hybrid administration has most of the functions performed at a central location, but one or more key contact people are on site for handling lesser responsibilities.
Funding model	Funding can be crucial in implementing technologies. If the IT department is run as a profit center, then departments they administer are charged for services provided: this can be useful in acquiring new software and distributing the cost among many departments who can benefit from it. If the IT department is run as a cost center - a fixed cost that appears as a liability on the business sheets, then it can be more difficult to gain approval to spend additional dollars beyond those already allotted for a set time period.
Outsourcing	Outsourcing is often used because certain needs must be met that cannot be done internally. These can include the need for IT professionals in a tight labor market, the need for occasional service at branch offices, international/temporary needs, and so on. While outsourcing is a good way to solve such issues, it can present problems down the road when you cannot find the group who implemented a solution because they have moved on, and the solution now has problems.
Decision-making process	Does the Chief Technology Officer need to approve all

	expenditures, or can they be signed-off on at a lower level. Does the CTO need to approve all solutions, or does he/she make certain that the solution one department generates is adopted by other departments? Is there autonomy within the divisions, or do they work together to contribute to decisions that affect all?
Change management	Is there a structure in place or not? When changes occur, what is the procedure followed? If there is no procedure, chaos can result. If there is too much of a procedure, no change will ever occur.

Analyzing Technical Requirements

When evaluating the company's technical environment, always factor in the existing as well as the planned environment, and differences between the two. Be sure to look at the following factors:

Technical Factors	Comment
Company size	The geographic scope as well as the owner or organization responsible for the company
User and resource distribution	Where are the users - how are the serviced (DNS, WINS, DHCP, etc.)? How do they reach the resources (servers, printers, and such) they need (hubs, switches, routers, bridges, modems, proxy servers...)
Connectivity between sites	What bandwidth is employed? Are there leased lines, or dial-up connections (with or without multilink see KB# QB235610))? What are the topologies employed (Star versus Mesh)?
Performance requirements	Are users connecting only for authentication, or for the entire session (such as with Terminal Server). Find out the peak utilization, the type of circuits used, requirements of applications, and so on. During this analysis, it is important to identify any bottlenecks and create a baseline from which to judge future modifications.
Access patterns	Are all the resources centralized, or are they disbursed? When users need to access a resource, is it within their LAN 80% of the time, or only 20% (meaning they access the WAN 80% of the time)? Do users go through firewalls, and/or do they use encryption. If they do use encryption, is it for the password, the data or both? Authentication can be accomplished through the use of

	the following, which may be used in conjunction with one another (KB #Q227815): • CHAP - Challenge Handshake Authentication Protocol - one-step above PAP in that it does not use clear-text passwords • EAP- Extensible Authentication Protocol - the client and the server negotiate the protocol that will be used, in much the same way that networking protocols are determined. Possible choices include one-time passwords, username/password combinations, or access tokens. • MS-CHAP - Microsoft Challenge Handshake Authentication Protocol - requires the client to be using a Microsoft operating system (version 2), or a small handful of other compatible OSes (version 1) • PAP - Password Authentication Protocol - uses a plain-text password authentication method and should only be used if the clients you support cannot handle encryption • SPAP - Shiva Password Authentication Protocol - a shade above PAP, it is there for backward-compatibility and is not favored for new installations
Network roles and responsibilities	Roles can be defined as administrative, or associated with a user, a service or other. Administrative roles are those predefined by the operating system with additional responsibilities above a user. Examples include: • Administrator • Backup operator • Server operator User roles simply have the right to logon and use the network resources. Service roles run as services, without user interaction, in the operating system. Other roles include being an application, a group, or owner.
Security Considerations	What are the needs of the organization, and what operating systems does the organization support? Can everything standardize upon TCP/IP (which offers the ability to use numerous security features like IPSec and filters), or must NetBEUI (insecure) be used, along with NWLink (IPX/SPX-compatible transport - (KB# Q203051) and other protocols)? Is it possible to use Kerberos, RADIUS, and EFS (Encrypting File System)? Must all solutions work with third-party tools?

	The most effective means of implementing security with Windows 2000 clients is through the use of Group Policies.

Speeds employed on WANs differ by technologies. The most common technologies, and their associated speeds, are:

- Modems including analog, ISDN, DSL, and cable:

Analog	Traditional modem – requires a single phone line for a connection and is limited in speed to around 57,600bps
ISDN	Integrated Services Digital Network, requires two phone lines, and can reach a speed around 128,000bps
DSL	Digital Subscriber Line, uses existing phone lines (copper), and is available only in certain areas. You must be within a short distance of a switching station, and speeds can reach 9Mbps
Cable	Works with the coaxial from the cable TV company and speeds is reduced with the number of users, but is approximately 2Mbps

- Leased lines:

T1/E1	a T1 is a dedicated line that operates across 24 channels at 1.544Mbps. E1 is the European counterpart: it uses 32 channels and can run at 2.048Mbps
T3/E3	A T3 is a dedicated line of 672 channels (E3 is the European counterpart) able to run at speeds of 43Mbps

When deciding to implement Active Directory of an existing or planned network, it is important to detail the possible impact of so doing. The impact should be calculated in terms of:

- Existing systems and applications - for example, current DNS servers will need to support SRV records
- Existing and planned upgrades and rollouts - identify those that are in the works and calculate any impact AD could have on them
- Technical Support structure - know what is there now (internal versus external), and make certain they will understand any changes that will happened before they happen. Verify that there is a budget for any training

that needs to be done and that all relevant decision-makers are in agreement on the need to support the existing support staff
- Existing and planned network and systems management - this should be viewed in terms of the security policy, any and all network tools used for management, monitoring, and analysis
- Client needs - not only their work needs, but also their support requirements.

Designing a Directory Service Architecture

- Active Directory is a naming scheme that follows the path Forest, Tree(s), Domains (see Active Directory Architecture). A forest can consist of a single domain, or multiple domains (therefore, by definition, a single domain can also be a tree). A tree is a contiguous namespace, meaning the child has the parent as part of its name. Each tree has its own identity within the forest.
- A domain is an administrative as well as security boundary since administrative privileges do not extend past domain boundaries. The simplest network is one with one domain. Reasons for creating additional domains would include:
    - To isolate replication traffic
    - To retain existing NT domain structures
    - To support decentralized administration
    - To support international boundaries
    - To support more than one domain policy
- Domains contain objects, or Organizational Units (OUs). An OU is a container for organizing objects within a domain into logical sub-groupings. Reasons for creating OUs include:
    - To control access to resources
    - To create group policy objects
    - To delegate administration (see Step-by-Step Guide to Using the Delegation of Control Wizard)
    - To group common objects
- Active Directory names are equivalent to DNS names and use the SRV records of DNS to store information about services and thus create "dynamic DNS". The first division of DNS is into domains. The InterNIC (Internet Network Information Center) controls top-level domains, which are summarized in the following table:

Name	Type of Organization
Com	Commercial organizations
Edu	Educational institutions
Org	Non-profit organizations
Net	Networks (the backbone of the Internet)
Gov	Non-military government organizations
Mil	Military government organizations
Num	Phone numbers
Arpa	Reverse DNS
Xx	Two-letter country code, such a "ca" for Canada, "uk" for United Kingdom, etc.

- To refer to a host in a domain, you use a fully qualified domain name (FQDN). The Relative Distinguished Name is the host name of the computer, while the User Principal Name consists of a user logon name and a domain name identifying the domain in which the user account is located.
- Windows 2000 uses a multi-master replication model, and the primary unit of replication is the domain. When domain controllers need to replicate, they examine the values of their Update Sequence Number (USN) for each object, and only replicate the attributes whose objects contain differing USN's. A site (comprised of one or more physical subnets) is a way to create replication boundaries within the Active Directory. Working at the physical layer, a site can consist of multiple domains, and domains can operate in multiple sites.
- The purpose of the Knowledge Consistency Checker (KCC) is to generate a replication topology for both intra-site and inter-site replication. Within a site, replication traffic is done via Remote Procedure Calls over IP, while between sites it is done through either RPC or SMTP (see "How to Optimize Active Directory Replication in a Large Network", KB# Q244368)
- Site link bridges are used to connect sites together and model the routing behavior of a network.
- There is only one schema per Windows 2000 forest, and it is maintained forest-wide by virtue of being stored on every domain controller. Throughout the forest, though, there is only one write-able copy of the schema – held by the Schema Operations Master. Modifying the schema is an irreversible operation, thus schema modification is disabled by default on all domain controllers and only members of the Schema Admins group can make changes.
- The schema container holds all the definitions required to view the objects in the directory, and each is identified by a globally unique number known as

the Object Identifier (OID). You can view Schema contents using the Active Directory Schema MMC snap-in, or the ADSIedit MMC utility.

Designing Service Locations

There are five Operations Master roles:

1. *Domain Naming Master - allows additions and removals of domains in the forest
2. Infrastructure Master - updates group-to-user references when changes occur
3. PDC Emulator - used with older clients
4. RID Master - Relative ID Master - issues IDs to domain controllers as needed
5. *Schema Master - controls all updates to the schema

- Operations Master placement (see KB# Q223346) is crucial to load balancing and fault tolerance. It is also important to convert domain controllers to native mode (non-Windows NT 4.0) enhance Active Directory Performance. The two roles identified by an asterisk are limited to only one controller within the forest, while the other three are per domain roles.
- Global Catalog Servers (see KB# Q232517) should be placed in locations to reduce traffic and help with load balancing and fault tolerance, as well. The first Global Catalog Server is created automatically with the first domain controller within the forest. Active Directory Sites and Services - an MMC snap-in (see Step-by-Step Guide to Active Directory Sites and Services) - allows you to change the role of the GCS to another domain controller. In areas where bandwidth is at a premium, a GCS can be configured to only receive updates after hours. For speed reasons, a GCS should be created at each site.
- Domain controllers should be created for fault tolerance and functionality, as needed. It is recommended that the infrastructure master be placed on a domain controller that is not the global catalog server to even the load and separate the burden of each role.
- DNS servers can be running Windows 2000, or other operating systems, provided they accept SRV records. When you install Active Directory, you must identify a DNS server. If you cannot do so, the Active Directory Installation Wizard will prompt you to convert the existing machine into a DNS server as well.
- Active Directory is created to be scalable and interoperate with other name services (see Active Directory Interoperblity and Metadirectory Overview).

Tools to Know

Active Directory Migration Tool (see Active Directory Migration Tool Overview)	Migrate from Windows NT 4.0 to Windows 2000 with Active Directory
ADSIedit	view the Active Directory Schema
Movetree	move objects within a forest
NTDSUTIL.EXE (see KB# Q255504)	perform many Active Directory administration tasks
REPAdmin (see KB# Q229896)	work with replication between partners
REPLMON (see KB# Q232072)	show the replication topology

Additionally, a complete list of relevant terms can be found in the Active Directory Glossary.

Special Thanks to Emmett Dulaney for contributing material that was used in the writing of this Cramsession