**Study guide by ExamNotes.net**

# 70-219

# Designing a Microsoft® Windows® 2000 Directory Services Infrastructure

## Abstract

This ExamNotes Study Guide intends to provide you with information to prepare for the Microsoft W2K 70-219 Exam.

## ExamNotes Study Guide Topics Covered

- Business and Technical Requirement
- Directory Topology
- Naming strategies
- Server, DC, and GC placement
- Company and business models
- Decision making factors
- Roles of operations masters
- Using Organizational Units

## Before you start

This study guide provides you with information on the many different aspects of "W2K Directory Infrastructure Design". You should not use this information as your first step into Active Directory, as this exam is targeted towards candidates with solid background on AD. Backgrounds on Novell NDS or LDAP directory design certainly help, but since AD has many MS proprietary stuff, watch out when studying. There are topics in this exam that overlap with what you can find in exam 215 and 216, such as DNS, RIS, as well as the AD infrastructure. You are encouraged to read those study notes as well.

You should setup two machines as W2K DCs and one W2K client for experimenting with AD on both the server and client end.

By all means read more than one book on the subject and make sure you understand the material well enough so that you could be ready for the scenario questions. There is no quick way to succeed for this topic. The exam has a lot of scenario questions. You must fully understand all the related concepts and be able to think intelligently to decide what is correct and what is not. This study note can only provide you with a certain degree for assistance in preparation. You must work things out and gain experience before even trying to sign up for the exam.

## Directory In Brief

Active Directory is actually a database of network objects. All objects are named in accordance to ANSI X.500 naming structure and are connected to each other via DNS.

Strictly for replication purpose, Active Directory is divided into sites, where each must have a working DNS infrastructure and correct pointers inserted into the DNS database. The replication model is based on multimaster concept, meaning there is no primary domain controllers: all DCs are equal (Microsoft recommends that you have at least two domain controllers within each site for availability purposes). Each site uses a "bridgehead" server to link to other sites.

When designing the Active Directory, you want to make sure that your business requirement is adequately fulfilled.

# Business and Technical Requirements

This part is more about business knowledge. Let's say you are asked to implement a solution for a branch office of a big company. It is natural for you to verify and confirm that solutions implemented here work with technologies employed throughout the company. If this is a subsidiary, you would make certain that, to the parent company, approval for the solution generated will be acceptable.

When implementing technologies for companies restricted to regional boundaries or for a business with a national coverage, the concern for international regulations and translations is minimal. When the business is going global, you will then have to pay attention to issues like languages, regulations and laws. Ideally, representatives from all countries should be involved in decision-making processes related to the technologies implementation.

Keep in mind that not all companies divide themselves based on locations. Some organizations are divided by products, while other organizations divide operations and responsibilities purely on other terms. To a certain extent you want to design your AD to fit their structure, unless the structure is about to be changed.

Before you implement anything, you want to find out about the existing condition of the company. You may ask questions like: Who is in charge? Who manages accounts? Who manages resources? How is administration divided? …etc. You would also want to document and diagram processes take place in the organization. Items include: Information flow, Communication flow, Product lifecycles and Decision-making hierarchy.

When deciding business requirements, you should take into account the organization structure as well. For example, you should find out if you are dealing with a privately held business or a public company with a hired CEO and Board. When operation and ownership are separate, it is often the case that the need for profit and quick solutions is more important than long-term planning. Put it this way, different management models has different attitudes towards risk.

There are many factors that can influence a company's strategies, such as company priorities, projected business growth and growth strategy, relevant laws and regulations, tolerance for risk, and the total costs of operations. All these can have influence towards the IT strategies the company is about to deploy.

One of the factors crucial to technology deployment is the funding model. If the IT department is run as a cost center rather than a profit center, it will for sure be more difficult to gain approval to acquire adequate resources.

Outsourcing your IT functions is always being considered, as certain needs cannot be met internally. While outsourcing is good in many cases, if the team is no longer available, you will have problems supporting and solving problems with the solutions the team implemented.

The decision-making process is another area of concern. Slow decision making process can become a bottleneck for technology deployment. Administration type is also an important factor. This is always about Centralized VS decentralized admin. Of course you may take a hybrid approach so that most of the functions are performed at a central location while one or more key contact people are on site for handling lesser responsibilities.

To summarize the technical requirements, you want to consider the following factors and try to see if it is possible for your plan to match the needs:

- Company size
- User and resource distribution
- Connectivity between sites
- Performance requirements
- Access patterns
- Network roles and responsibilities
- Security Considerations

You want to consider the existing systems and the existing applications. You would also need to know the impact of implementing AD towards the different roles in the organization. It is recommended that a budget be available for training and support. Existing security policy and network management, monitoring, analysis … all these are important factors you must figure out, and compare with the planned new structure.

On this site you can find a list of tutorials on the many different kinds of LAN / WAN technology for use in your infrastructure setup.

## Replication and KCC

Replication efficiency can be maintained with a flexible replication topology that reflects the structure of an existing network. Knowledge Consistency Checker KCC are feed with information on the cost of sending data from one location to another, and which domain controllers are running in the same location. KCC will then build

an inter-site replication topology that is a spanning tree based on low-cost routing decisions between locations, and a more strongly connected intra-site topology. Of course, you may disable KCC and manually create the connection objects required to suit your custom needs.

KCC generates a replication topology more strongly-connected within a site than between sites. It does not compress intra-site replication messages. Also, Intra-site DC replication is change-based while inter-site DC replication is schedule based. Active Directory uses the site information provided by KCC to help users locate the closest machine that offers a needed network or service.

From the above you should be able to tell the reasoning behind the way KCC performs. If message is compressed, there will be lower bandwidth utilization at the expense of CPU utilization, and vice versa. Schedule based replication allow you to conserve bandwidth in peak hours. Faster updates make the information more accurate. You have to assess the trade off.

## Replication Topology

Intra-site replication topology is a bi-directional ring that built with domain controller GUIDs. If a ring contains 7 or more DCs, bi-directional connections are added to keep the path between any pair to less than a hop count of 3. New DCs configured in the site are included in the ring. One bi-directional ring is built for each naming context available in a site. Schema and configuration information have only one bi-directional ring built for them, as they must be replicated to all domain controllers. Keep in mind though, if all DCs are in the same domain, the two rings are the same, meaning the ring that includes all site domain controllers is equivalent to the ring that includes all domain controllers in that domain. You can have more than one distinct ring only when your site has more than one domain.

Inter-site replication has the assumption of slow WAN links. It is designed to minimize traffic rather than CPU cycles. It uses spanning tree, meaning as long as a replication route can be constructed between all sites, the replication topology is functional, without the need to create additional links. Site links are based on the cost of replication and its schedule, which can be configured on a per site-link basis.

W2K uses 2 transports for inter-site replication, namely the Synchronous (scheduled) via RPC over TCP/IP and the Asynchronous via simple mail transfer protocol (SMTP) using the Collaborative Data Objects (CDO v2) interface and the SMTP component in IIS 5. For assessing network load, you may use Performance Monitor, Event Log and Network Monitor. In Performance Monitor, the counters most frequently used to measure replication traffic are the NTDS objects.

## Tools for Replication

Repadmin.exe is a Windows 2000 Resource Kit tool running in the command prompt that is available in the Support Tools folder on the Windows 2000 CD-ROM. It is a replication administration tool that provides a powerful interface into the inner workings of Active Directory replication, and is useful for troubleshooting Active Directory replication problems.

You may use Repadmin.exe to initiate replication by typing the following command:

repadmin /sync directory_partition target_server_name source_server_objectGuid

You may use the following optional switches on the command line:

/force: Overrides the normal schedule.

/async: Starts the replication event.

/full: Forces a full replication of all objects.

Alternatively, you may use the Active Directory Replication Monitor (Replmon.exe) which is included in the Windows 2000 Support Tools Resource Kit. Replmon.exe can initiate replication and report the success or failure of the request.

## Server Roles and Placement

Active Directory defines five FSMO roles: schema master, domain master, RID master, PDC emulator, and infrastructure. The schema master and domain naming master are per-forest roles, while all the others are per-domain roles.

If a domain has more than one DC, you should use Active Directory Sites and Services Manager to select direct replication partners with persistent, "well-connected" links. For faster replication convergence consistency over a large group of computers, the standby server may be in the same site as the primary FSMO server, or in a remote site to provide redundancy in the case of a site-specific disaster at the primary site. Should the standby DC be in a remote site, make sure the connection is configured for continuous replication over a persistent link.

For better performance, you should place the RID and PDC emulator roles on the same primary FSMO DC. If the load on the primary FSMO load justifies a move, place the RID and PDC emulator roles on separate primary DCs that have direct connection

objects to the standby RID and RDC emulator. You should consider to place the infrastructure master on a non-global catalog server that has a direct connection object to some global catalog in the forest, and of course preferably in the same Active Directory site. This is because DCs need a certain degree of fault tolerance. If the infrastructure master is placed on a domain controller that is not the global catalog server, the load and burden of each role can be even out.

If you are planning at the forest level, the schema master and domain naming master roles should be placed on the same domain controller as they are rarely used, and that they should be tightly controlled. It is also recommended that the domain naming master FSMO be placed on a Global Catalog Server.

## Server Roles and Movement

To move the FSMO roles from one computer to another, you can use two different methods: via Transfer or using Ntdsutil.exe tool to seize the roles. MS recommend the first method over the second method.

The transfer of an FSMO role is the preferred way of moving a FSMO role between domain controllers. Transfer can be initiated by the administrator or by demoting a domain controller, but is not initiated automatically by OS. In a transfer, a synchronization of the data that is maintained by the FSMO role owner to the server receiving the FSMO role is performed before transferring the role. This can ensure that any changes can be recorded before the role change.

When you seize an FSMO role from a computer, the "fsmoRoleOwner" attribute is modified on the object that represents the root of the data directly bypassing synchronization of the data and graceful transfer of the role. You should use extreme caution in seizing FSMO roles though.

## Domain VS OU

A simple network usually has one domain. To create additional domains, the typical reasoning includes: to isolate replication traffic, to retain existing NT domain structures, to support decentralized administration, to support international boundaries, or to support more than one domain policy.

In W2K, you can achieve delegated administration with OU. OU is a container for organizing objects within a domain into logical sub-groupings. You can create group

policy objects and associate them with an OU, or you can use the Delegation of Control Wizard for distributed administration.

Keep in mind that the primary reasons for creating an OU are to delegate administrative authority and to apply Group Policy settings. So, when creating OUs, make sure you have a solid justification.

Based on the current administrative requirements for your organization, define and apply GPOs to those OUs containing administrative user accounts and the computer accounts for the domain's servers and clients. The point is, this must align with the company's admin structure.

You are encouraged to group objects by relatively stable characteristics rather than by things of short-term nature. Additionally, the structure should be able to accommodate organizational changes within the domain without requiring changes to the OU structure itself.

Finally, your OU should have a simple structure, as complex structure can cause difficulties in the tracking of permissions and GPOs. You want to spend your time to manage the network via OUs, but not to just manage the OUs themselves.

## Group Membership

When planning our network structure, we always want to maintain centralized administration of computers across the entire domain. But at the same time, we may need local administration of computers in branch offices located remotely. To balance the need for centralized administration of computers against the need for regional control, Group Policy should be deployed to restrict the membership of the local Administrators group on each server and client computer in the domain.

Different types of groups are preferable over the others in different situations. Global groups are for combining users who share a common access profile based on job function or business role. Domain local groups are 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 needed.

As a recommended practice, we usually grant access to a global group by making it a member of a domain local group that is granted access permissions to a set of resources.

## Delegation

The recommended ways of delegation are:

- Create and populate the administrative security groups used to manage Active Directory objects. As administrative authority throughout the domain is distributed among these security groups, you must maintain strict control over their membership.
- Delegate to these groups administrative control over the objects for which they are responsible.
- Provide these groups with the administrative tools they need to exercise their delegated authority.

One method to delegate control over Active Directory objects is to build an access control list that defines the set of permissions granted on that object. You build the access control list on the Properties page of the OU containing the objects over which you want to delegate control.

With the Delegation of Control Wizard, you may delegate complete control of an organizational unit, or you may delegate only certain rights, such as to delegate creation and deletion of users in an organizational unit.

## Migration

Active Directory Migration Tool ADMT provides an easy and fast way to migrate from Windows NT to the W2K Active Directory service, or to restructure your existing Active Directory domains. Most likely you will use this tool to consolidate multiple domains into fewer domains, and possibly a single domain.

The good thing about ADMT is that it has many wizards available. User Migration wizard, Computer Migration wizard, Group Migration wizard, Service Account Migration wizard, Trust Migration wizard, and Reporting wizard are all for simplifying various parts of the migration process.

Before migrating groups, you may want to run the Group Mapping and Merging Wizard to map a group in the source domain to a new or existing group in the target domain. This allows you to ensure that group memberships will reflect the mapping. The “Test the migration settings and migrate later” option allows you to run all these in a trial basis to “test the water” before making actual commitment.