Study guide by ExamNotes.net

Exam 70-217

Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure

Study Guide, written by Yu Chak Tin Michael

Abstract

This ExamNotes Study Guide intends to provide you with information to prepare for the Microsoft W2K 70-217 Exam.

ExamNotes Study Guide Topics Covered

- Active Directory Structure
- Active Directory Object
- DNS integration
- Site Replication
- Group Policy

Before you start

This study guide provides you with information on the many different aspects of "W2K Directory Infrastructure". You should not use this information as your first step into MCSE2000, as this exam is targeted towards candidates with solid background on Windows Networking. Backgrounds on Novell NDS certainly help, too. If you are a beginner, I recommend that you first study the material presented in the NT 4.0 track Networking Essential and TCP/IP, and then complete the 210, 215 and 216 exams before working on this one.

There are topics in this exam that overlap with what you can find in exam 215 and 216, such as DNS and RIS. You are encouraged to read those study notes as well.

Active Directory Structure

A directory service is one of the most important components in a networking environment. Users frequently do not know the exact name of the objects they are interested in. If they know one or more attributes of the objects, they can query the directory to get a list of objects that match the attributes. Put it this way, a directory service allows a user to find any object given one of its attributes.

As a directory service, Active Directory (AD) services provide a single point of network management, allowing you to add, remove, and relocate objects and resources easily. It extends the features of previous Windows-based directory services and adds entirely new features. It is secure, distributed, partitioned, and replicated.

Scope

Active Directory can include every single, every server, and every domain in a single wide area network. It can also include several wide area networks combined. It is scalable.

In general, we prefer to organize the directory in a structure reflecting our real world organization structure or the geographical structure. This is NOT an absolute requirement though.

Namespace

A namespace is any bounded area in which a given name can be resolved, and Name resolution is the process of translating a name into some object or information that the name represents. The Active Directory forms a namespace in which the name of an object in the directory can be resolved to the object itself. In other words, Active Directory has its own naming standard convention.

Distinguished Name (DN) is for uniquely identifying object. It includes the name of the domain that holds the object and also its complete path. It is unique in the directory.

Relative Distingushed Name (RDN) is a part of the name that is an attribute of the object itself, not the complete name. As an example, a user's address is an attribute.

Globally Unique Identifier (GUID) is a unique 128-bit number assigned to objects when they are created. GUID never changes - even if the object is renamed.

User Principal Name (UPN) – a "friendly name"

An example of DN:

/O=Internet/DC=COM/DC=SoftwareHouse/CN=Users/CN=John Junior

DNS has its own name space too. Isn't this confusing? Actually, Active Directory is tightly integrated with DNS. Windows 2000 domain names are DNS domain names. Active Directory fits naturally into Internet and intranet environments, and you can connect Active Directory servers directly to the Internet, as the name wil llaso work on the internet.

Object

An object is a distinct, named set of attributes that represents a resource, such as a user, a printer, a server or an application. Attributes hold data describing the subject identified by the directory object. Examples of attributes are the user's name, location and e-mail address.

Publishing is about creating objects in the directory that either directly contain the information you want to make available or provide a reference to the information you want to make available. When some resources in your network need to be highly accessible, they will have to be published.

Container

A container is a container for a group of objects and other containers. Put it this way, a department is a container that holds a group of staff. The staffs are the objects, and the department is the container.

Organization Unit OU is the most important container in the directory. We use OU to organize objects inside a domain into logical administrative groups such as computers, printers, user accounts, file shares, applications

and even other OUs. N contrast, Classes are logical groupings of objects such as user accounts, computers, domains or organizational units. Domain is a security boundary, as access to objects is controlled by Access Control Lists. Note that all network objects exist within a domain, and that the "domain admin" only has rights to set policies within his/her domain. This is why it is a security boundary.

A simple directory is a container. A computer network or domain is also a container.

Tree and Forest

The Active Directory is a set of one or more trees. Tree describes a hierarchy of objects and containers. Endpoints on the tree are objects, while nodes in the tree are containers. We use a tree to show how objects are connected or the path from one object to another. Remember, a Tree needs a distinct name.

Forest is a set of one or more trees that do not form a contiguous namespace. However, all trees in a forest share a common schema, configuration, and Global Catalog, and that all trees in a forest trust each other via transitive hierarchical Kerberos trust relationships.

A forest does not need a distinct name.

Trust Relationships

Domains in a tree are linked together by trust relationships. Windows 2000 establishes trust relationships between domains based on the Kerberos security protocol. Kerberos trust is transitive and hierarchical—if domain A trusts domain B and domain B trusts domain C, domain A trusts domain C as well. This is different from the trust model in NT4.

This way of trust is Implicit two-way trust. When we say implicit, that means this is effective by default. However, you may go for Explicit one-way nontransitive trush – the NT4 trust. You will need to do this manually though.

Sites and Domain Controller

Site is a location in a network that contains Active Directory servers. We define a site as one or more well-connected TCP/IP subnets. This allows administrators to quickly and easily configure the Active Directory access and replication topology to take advantage of the physical network.

When a user logs on, the Active Directory client finds Active Directory servers in the same site as the user, usually resulting in communication that is reliable, fast, and efficient. This is based on the following assumption: A minimal site consists of a single IP subnet. We assume that all machines located in the same site share a common high-bandwidth network.

Active Directory information is replicated between Domain Controllers DCs and ensures that changes to one DC are reflected in all DCs within a domain. Administrators can specify how often replication occurs, at what times, and how much to be sent, but DCs will immediately replicate important changes, such as if a user account is being disabled.

In NT4, there is a primary to secondary DC relationship. In W2K, we use multimaster replication, meaning that no one DC is the master domain controller - all DCs are peers. For fault tolerant purpose, Active Directory automatically generates a ring topology for replication in the same domain and site.

To migrate a Windows NT 3.51 or 4.0 domain to Windows 2000, you must first upgrade the Primary Domain Controller for the domain to Windows 2000 in order to automatically loads the users and groups from the domain directory into the Active Directory.

A domain with W2K and NT4 as DCs is a mixed domain. The Backup Domain Controllers, member servers, and clients are unchanged and unaware that the PDC is now an Active Directory server. To take full advantage of Active Directory, you should gradually change all NT4 server to W2K, so that the network can run in Native mode.

Keep in mind that W2K Servers are installed as Standalone Member Servers by default. They can access Active Directory information, but do not perform any directory related authentication or storage functions. To promote a machine to a Domain Controller, you run dcpromo.

You may want to equip yourself with the following knowledge:

- Installing the first domain controller in a new forest
- Installing the first domain controller in a new domain tree
- Installing the first domain controller in a new child domain
- Installing an additional domain controller in a domain tree
- Removing Active Directory from domain controller

The Knowledge Base article Q238369 at this site listed the steps in a clear and concise manner.

DCs in the same site replicate using notification, meaning when one DC has changes, it notifies its partners. The partners then request the changes and start the replication process.

The majority of Active Directory replication takes place at predefined intervals. However, some types of changes to objects must take place immediately to allow for proper domain administration. We called this the Urgent Replication Triggers:

- Events that are replicated immediately in native-mode domains include newly locked-out account, changing an LSA secret, and RID manager state changes.

- Events replicated immediately in mixed-mode domains include newly locked-out account, changing an LSA secret, inter-domain trust password changes, RID manager state changes, changes to account lockout policy, changes to domain password policy, and changing the password on a machine account

Please note that a password change by a Directory Service-aware client at a DC is "pushed" by that DC to the PDC FSMO role owner on a best-effort basis. The password change is propagated to other DCs in the domain using normal replication values.

The detail of replication trigger is outlined in the Knowledge based article Q232690 at this site

Regarding replication performance, Directory Replication Agent DRA counters are added to the Performance Console to measure the efficiency of replication traffic.

Schema

Active Directory schema defines the set of all object classes and attributes that can be stored in the directory. Through schema, we define where an object class can be created in a directory tree by specifying the legal parents of the class.

The content of a class is defined by the list of attributes that the class must or may contain. We may extend the schema when there are no existing object classes that meet the need, as new attributes can be added to the schema at any time easily.

Global Catalog

GC is a central repository of information about objects in a tree or forest most often used in Search operations. It can be used to find objects anywhere in the network without replication of all information between DCs. Active Directory automatically creates a global catalog from the domains.

Groups

A Universal group is the simplest form of group that can appear in ACLs anywhere in the forest and contain other Universal groups, Global groups, and users from anywhere in the forest.

A Global group can appear in ACLs anywhere in the forest. It can contain users and other Global groups from its own domain.

A Domain Local group can be used in ACLs only in its own domain. It can contain users and Global groups from any domain in the forest, Universal groups, and other Domain Local groups in its own domain.

Security

All objects in the Active Directory are protected by Access Control Lists ACLs that determine who can see the object and what actions each user can perform on the object. ACL contains a list of Access Control Entries ACEs stored with the object it protects, as binary value called a Security Descriptor.

Delegation allows a higher administrative authority to grant specific administrative rights for containers and subtrees to individuals and groups to eliminate the need for Domain Admin with sweeping authority over large portions of the network. Inheritance lets a given ACE propagate from the container where it was applied to all children of the container. Combining

inheritance with delegation, we can grant administrative rights to a whole subtree of the directory in a single operation.

You perform delegation via the Delegation of Control Wizard. However, it can only assign permissions at the OU or container level.

Options include:

AD Object Type	Scope for tasks being delegated includes: This folder, Existing Objects In This Folder, Creation of Objects In This Folder, or Only The Following Objects In This Folder.
Permissions	General, Property Specific, Creation/Deletion of Specific Child Objects
Tasks to Delegate	Predefined tasks or create custom tasks
Users or Groups	Users or groups you want to delegate control to.

Regarding the Default Security Concerns in Active Directory Delegation, please refer to Knowledge Based article Q235531 at this site

Manipulating Active Directory Objects

Objects can be moved within a domain using the AD Users & Computers console. Note that permissions that have been assigned directly to an object will not change when it is moved. For objects without permissions, they inherit the permissions of the parent container they are moved to. And of course, you can move multiple objects at once.

Moving Active Directory objects between domains is done using the **movetree** command-line utility in the Windows 2000 Support Tools. Their GUID remains unchanged, but the SID does.

An OU can be moved from one domain to another, and the corresponding GPO link is automatically updated without the need for manual modifications.

To move workstations or member servers between domains, you use the **netdom** command-line utility.

To find objects, use LDAP query via Administrative Tools -> AD Users & Computers, right-click a container in the tree and select Find. Users may also query via Search from their Start menu. They can search for computers, shared folders, printers, and users.

FSMO Roles

In a single-master model, only one DC in the entire directory is allowed to process updates. Windows 2000 Active Directory extends the single-master model to include multiple roles and the ability to transfer roles to any DC. Since an Active Directory role is not bound to a single DC, it is referred to as a Flexible Single Master Operation role.

Currently there are five FSMO roles:

- Schema master
- Domain naming master
- RID master
- PDC emulator
- Infrastructure daemon

The schema master FSMO role holder is the DC responsible for performing updates to the directory schema. This is the only DC that can process updates to the directory schema. Once update is complete, it is replicated from the schema master to all other DCs in the directory.

There is only one schema master per directory. Do not confuse schema update with directory database update. All DCs can update the directory database content.

The domain naming master FSMO role holder is the DC responsible for making changes to the forest-wide domain name space of the directory. This is the only DC that can add or remove a domain from the directory.

The RID master FSMO role holder is the single DC responsible for processing RID Pool requests from all DCs within a given domain. When a DC creates a security principal object such as a user or group, it attaches a SID to the object. The SID consists of a domain SID and a relative ID RID unique for each security principal SID created in a domain. Each W2K DC has a pool of RIDs allowed to assign to the security principals it creates. When a DC's allocated RID pool falls below a threshold, that DC issues a request for additional RIDs from the domain's RID master.

The PDC emulator FSMO role holder is a W2K DC that advertises itself as the primary domain controller to down-level workstations, member servers, and domain controllers that are not native W2K.

The infrastructure FSMO role holder is the DC responsible for updating an object's SID and distinguished name in a cross-domain object reference.

GPO

We use Group Policy to define configurations for groups of users and computers via the Group Policy Microsoft Management Console (MMC) snap-in. This snap-in provides built-in features for setting Group Policy, including options for registry-based policies, security settings, software installation, scripts, and folder redirection. Settings created are contained in Group Policy Object associated with selected Active Directory system containers of 4 different levels: sites, domains, and organizational units. Data within GPOs is evaluated by the affected clients using the hierarchical nature of the Active Directory. You can create as many GPOs as you like in theory.

By default, Group Policy affects all computers and users in a selected Active Directory container. However, you can filter the effects of Group Policy. To filter the effects of Group Policy on computers and users, you use membership in security groups and setting discretionary access control list (DACL) permissions. To achieve the highest level of policy settings security, use the Process even if the Group Policy Objects have not changed policy for each of the Group Policy client side extensions that require it. This option ensures that the selected settings are applied at every logon to the Active Directory.

To set Group Policy for a selected Active Directory container, you must have a Windows 2000 domain controller installed, and you must have read and write permission to access the Sysvol folder and modify rights to the currently selected directory container. Note that a system volume folder is automatically created when you install a Windows 2000 domain controller or promote a server to domain controller.

The Administrative Templates node of the Group Policy snap-in uses an administrative template (.adm) file to specify the registry settings that can be modified through the Group Policy snap-in user interface. These settings are written either to the User or Local Machine portion of the registry. Policy settings for user are written to the User portion of the registry database under

HKEY_CURRENT_USER. Computer-specific settings are written to the Local Machine portion of the registry under HKEY_LOCAL_MACHINE.

Windows 2000 includes two .adm files: System.adm and Inetres.adm, which contain all the settings initially displayed in the Administrative Templates node. You may extend the Administrative Templates node of the Group Policy snap-in by using custom .adm files, but not by any MMC snap-in.

Important Tools

Tool	Function
Acldiag.exe	Access Control Lists diagnostic tool
ADSI edit	View and modify objects in the directory
Dfsutil.exe	Distributed File System Utility
Dnscmd.exe	DNS Server Troubleshooting
Dsacls.exe	Manipulate object ACL
Dsastat.exe	DC status check
Ldp.exe	Perform LDAP operations against the directory
Movetree.exe	Move objects between domains in a single forest
Netdom.exe	Manage W2K domains and trust relationships
Nltest.exe	Create a list of PDCs Provide information about trusts and replication.
Repadmin.exe	Replication Administration
Replmon.exe	Replication Monitor
Sdcheck.exe	Security Descriptor Check Utility