CNT 4603: System Administration
Spring 2011

Introduction To Active Directory – Part 3

Instructor : Dr. Mark Llewellyn
markl@cs.ucf.edu
HEC 236, 4078-823-2790
http://www.cs.ucf.edu/courses/cnt4603/spr2011

Department of Electrical Engineering and Computer Science
University of Central Florida

More Active Directory Basics

- AD is a directory service that houses information about all network resources such as printers, user accounts, groups of user accounts, security policies, and other information.
- As a directory service, AD (Active Directory Domain Services – or AD DS) is responsible for providing a central listing of resources and ways to quickly find and access specific resources as well as providing a way to manage network resources.
- Writable copies of information in AD are contained in one or more domain controllers (DCs), which are servers that have the AD DS server role installed.
- Servers on a network managed by AD that do not have AD installed are called member servers (and are not domain controllers).

More Active Directory Basics

- Microsoft recommends that are least two DCs should be present in any organization using AD. This is to ensure that if one DC goes down, the other is still available to service user account requests to log on and access resources.
- In AD, a domain is a fundamental component or container that holds information about all network resources that are grouped within it – servers, printers, and other physical resources, users, and user groups.
- A domain is usually a high-level representation of how an organization is structured. Common structures reflect geographic locations or corporate division hierarchies.

More Active Directory Basics

- Every resource is called an object and is associated with some domain.
- When you set up a new user account or a network printer, for example, it becomes an object within a domain.
- In Windows Server 2008, every DC is equal to every other DC in that it contains the full range of information that composes an AD.
- If information on one AD changes, such as the creation of a new user account, it is replicated automatically (see previous section of notes) to all other DCs, in a process known as multimaster replication.

More Active Directory Basics

- In Windows Server 2008 the system administrator can set replication of an AD to occur at a preset interval instead of automatically upon the occurrence of an update in some DC.
- You can also determine how much of AD is replicated each time it is copied from one DC to another.
- AD is designed to make replication efficient so that it transports as little as possible over the network, saving network resources.

More Active Directory Basics

- AD in Windows Server 2008 can:
  - Replicate individual properties instead of entire accounts, which means that a single property can be changed without replicating information for the entire account.
  - Replication can be done based on the speed of the network link, such as replicating more frequently over a LAN than over a WAN.

More Active Directory Basics

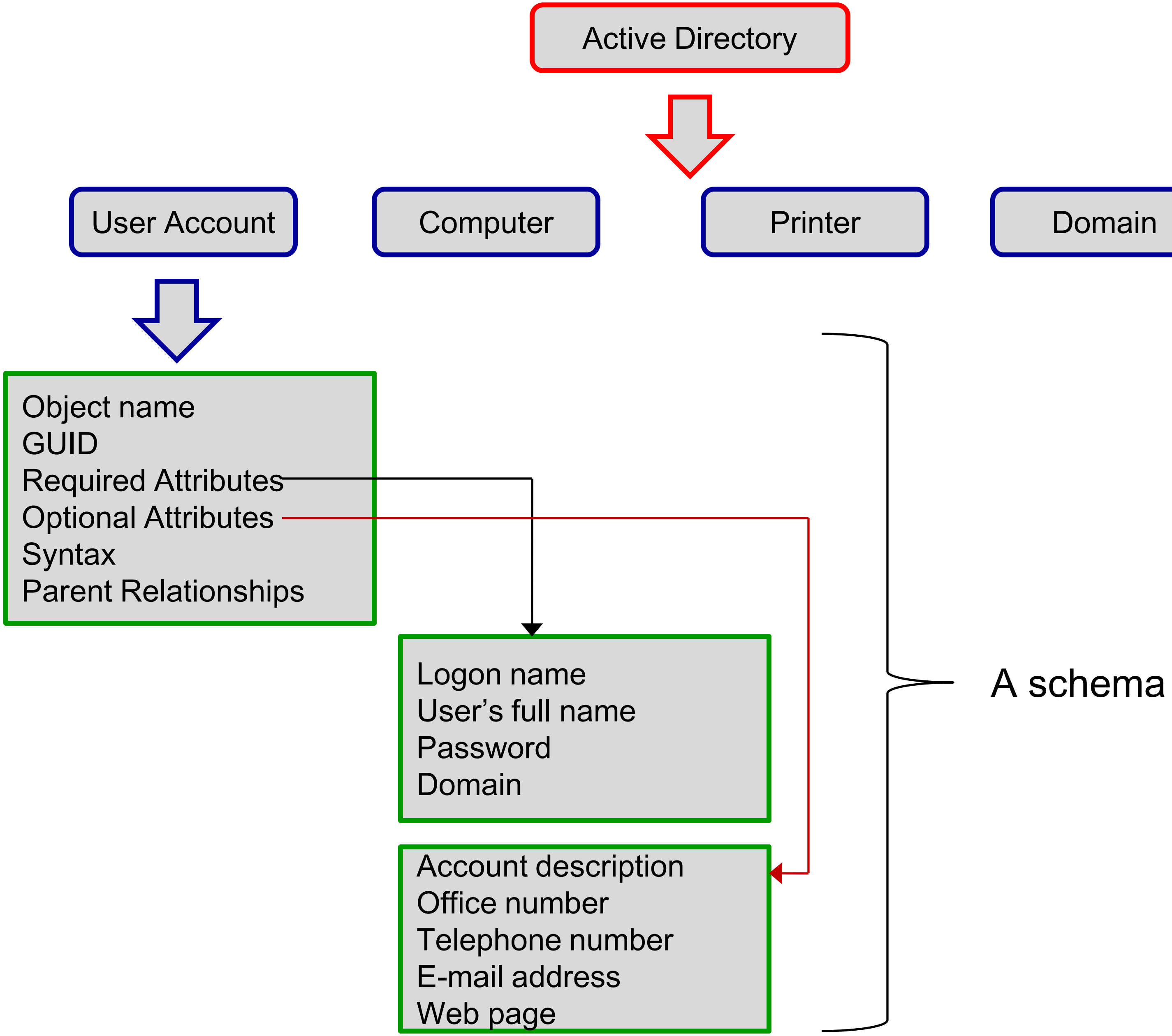
- The AD schema defines the objects and the information pertaining to those objects that can be stored in AD.
- Each kind of object in AD is defined through the schema, which is like a small database of information associated with that object, including the object class and its attributes.
- Schema information for objects in a domain is replicated on every DC.

More Active Directory Basics

- A user account is one class of objects in AD that is defined through schema elements unique to that class.
- The user account class as a whole has the following schema characteristics:
  - A unique object name
  - A globally unique identifier (GUID), which is a unique number associated with the object name.
  - Required attributes – must be defined for each object.
  - Optional attributes – optional definition for any object.
  - A syntax (format) to determine how attributes are defined.
  - Pointers to parent entities, such as to a parent domain.

More Active Directory Basics

- Examples of required user account attributes are:
  - Logon name
  - User’s full name
  - Password
  - Domain
- Examples of optional user account attributes are:
  - Account description
  - Account holder’s office number or address
  - Account holder’s telephone number
  - Account holder’s email address
  - Account holder’s web page
- An example schema for user accounts is shown on the next page.



Active Directory

User Account

Computer

Printer

Domain

Object name
GUID
Required Attributes
Optional Attributes
Syntax
Parent Relationships

Logon name
User’s full name
Password
Domain

Account description
Office number
Telephone number
E-mail address
Web page

A schema

More Active Directory Basics

- To some extent, the optional attributes may be influenced by the security policies that the server administrator sets in AD for a class of objects. We'll see more about security policies in AD later.
- Each attribute is automatically given a version number and date when it is created or changed.
- This information enables AD to know when an attribute value, such as a password, is changed, and update only that value on all DCs.
- When you install Windows Server 2008 for the first time on a network server, designating it as a DC, you also create several object classes automatically.
- The default object classes include domain, user account, group, shared drive, shared folder, computer, and printer.

More Active Directory Basics

- The global catalog stores information about every object within a forest.
- The first DC configured in a forest becomes the global catalog server.
- The global catalog server will store a full replica of every object within its own domain and a partial replica of each object within every domain in the forest.
- The partial replica for each object contains those attributes most commonly used to search for objects.

More Active Directory Basics

- The global catalog serves the following purposes:
  - Authenticating users when the log on.
  - Providing lookup and access to all resources in all domains.
  - Providing replication of key AD elements.
  - Keeping a copy of the most used attributes for each object for quick access.
- The global catalog server enables forest-wide searches of data.
- Because it contains attributes pertaining to every object within a forest, users can query this server to locate an object, as opposed to having to perform an extensive search.

More Active Directory Basics

- The global catalog server also can be used for network logons.
- When a user logs on to the network, the global catalog server is contacted for universal group membership information pertaining to the user's account (universal groups will be covered later in the course).
- In a Windows 2000 domain, if the global catalog was unavailable, the user could only log on to the local computer. In Windows Server 2003 and 2008, if the global catalog is unavailable for group membership information, the user can log on to the network with cached credentials.

More Active Directory Basics

- Cached credentials means that a record is kept in server cache if a user has successfully logged on previously.
- Authentication, when the user logs off and subsequently logs on again, can be performed by checking the cached credentials, instead of the global catalog.
- However, when a user is logging on for the first time and there is no cached credential for that user, if the global catalog is unavailable, access will be provided only to the local computer.

More Active Directory Basics

- By default, the first DC in the forest is automatically designated as the global catalog server. The system administrator has the option of configuring another DC to be a global server as well as designating multiple DCs as global catalog servers.
- There must be at least one global catalog server in a forest.
- In most cases, it also makes sense to place one global catalog server in every site.
- If an organization utilizes email servers, such as for Microsoft Exchange, one global catalog server for every four mailbox servers is recommended . Since global catalog servers can generate heavy network traffic, configuring every DC to be a global catalog server is too much!

Planning Functional Levels and Trusts

- Careful planning about how to set forest and domain functional levels when you implement AD should be performed.
- In the planning, you should remember that it is easier to raise a domain or forest functional level, but lowering a level is very difficult since it cannot be done through the operating system.
- To lower a functional level, you will need to backup the servers and reinstall AD, which is a lengthy and potentially complex task.
- Whether to raise the functional level to take advantage of newer features should be weighed against the versions of servers that must be supported and the anticipated changes within an organization.

Planning Functional Levels and Trusts

- For example, one branch of an organization might have all Windows Server 2008 DCs, but another branch of the organization might have Windows Sever 2003 DCs.

- In this sort of situation, the domains and forests would be kept at the Windows Server 2003 domain and forest functional levels.

- If your organization is currently at the Windows Server 2000 domain and forest functional levels, and there is some likelihood of a merger with another organizations, it would be best to remain at the current functional levels until you are certain about the functional levels already in use at the other organization. In this case, you don't want to raise to the Server 2008 levels and later discover that the other organization has a Server 2003 domain, which would require reinstalling AD.

Planning Functional Levels and Trusts

- On the other hand, if you are in a relatively small organization with no intention of a merger and have upgraded all of your servers to Windows Server 2008, it would be best to raise the forest and domain levels to Windows Server 2008 level.
- This would enable you to take advantage of all the new features, such as better encryption and fine-grained passwords.

Planning Functional Levels and Trusts

- Carefully planning trusts between forests is as important as planning functional level.
- Trusts between forests can be set up to be one- or two- way trusts.
- For example, if Organization A buys Organization B, a one-way trust can be set up to allow employees working on the transition at A to access data in the forest of B, but employees at B would have no access to data in the forest of A.
- Later after the transition is complete, a two-way trust can be established so that employees of each organization can access data in the forest of the other.
- Later still, as the dust from the merger settles, both forests might be merged into a single forest.

Planning Functional Levels and Trusts

- AD also provides other types of trusts.
- An external trust is used to create a trust relationship with a domain that is outside of a forest.
- A realm trust is typically used to enable one- or two- way access between a Windows Server domain within a forest and a realm of Unix/Linux computers. The prerequisite for a realm trust is that the servers in the Windows Server domain and the Unix/Linux realm must all use Kerberos version 5 authentication. Also the Windows domain functional level must be at the 2003 or higher level.

Planning Functional Levels and Trusts

- A shortcut trust is a trust to enable a domain in one forest to quickly access resources in a domain within a different forest.
- The shortcut trust is ideal to enable child domains within multilayered forests to access resources more quickly.
- Consider a situation in which two different forests have child domains that are three levels deep. A client in the lowest level child domain in Forest 1 needs to access a customer database in the lowest level child domain in Forest 2. Each time the client needs to access the database it is necessary to go through multiple levels of domains and two forests, which is time consuming (and CPU intensive). A one- or two-way shortcut trust can be established between the two child domains in different forests to enable faster access.