2/17/2017

Microsoft Active Directory

Table of Contents

What is Active Directory?

Active Directory is "a collection of services (Server Roles and Features) used to manage identify and access for and to resources on a network."[1] Active Directory has several server roles including Domain Services, Certificate Services, Federation Services, Rights Management Services and a Lightweight Directory Services.[2] Active Directory is what gives networks the ability to have a user login into different computers within the network and have a common experience throughout. It allows Central Management and Authentication of users, workstations and servers.

The 3 Active Directory Partitions

The Active Directory partitions include:

1. **Schema Partition**
   The schema partition "contains definitions of all objects and attributes that you can create in the directory, the rules for creating and manipulating them."[3] There is only one schema partition per forest. As Active Directory is a database, the schema partition defines what is allowed within the database.

2. **Configuration Partition**
   The configuration partition "contains information about forest-wide active directory structure including what domains and sites exist, which domain controllers exist in each forest and which services are available."[4] There is only one configuration partition per forest. The configuration partition keeps track of every resource that is connected to the network and replicates in throughout the domain controllers.

3. **Domain Partition**
   The domain partition contains a "domain controller, which stores users, computers, groups, and other objects…."[5] The domain partition is essentially the data container for the domain. It contains all the data and information about the domain.

[1] Chapman, Christopher. Understanding Active Directory (Video Series). *Microsoft Virtual Academy*. https://mva.microsoft.com/en-US/training-courses/understanding-active-directory-8233?l=aErw3QJy_6904984382
[2] Ibid.
[3] What is active Directory partitions? *Experts* Exchange. https://www.experts-exchange.com/questions/28223350/What-is-active-Directory-partitions.html
[4] Directory Partitions. *Tech-FAQ*. http://www.tech-faq.com/directory-partitions.html
[5] Directory Partitions. *Microsoft TechNet*. https://technet.microsoft.com/en-us/library/cc961591.aspx

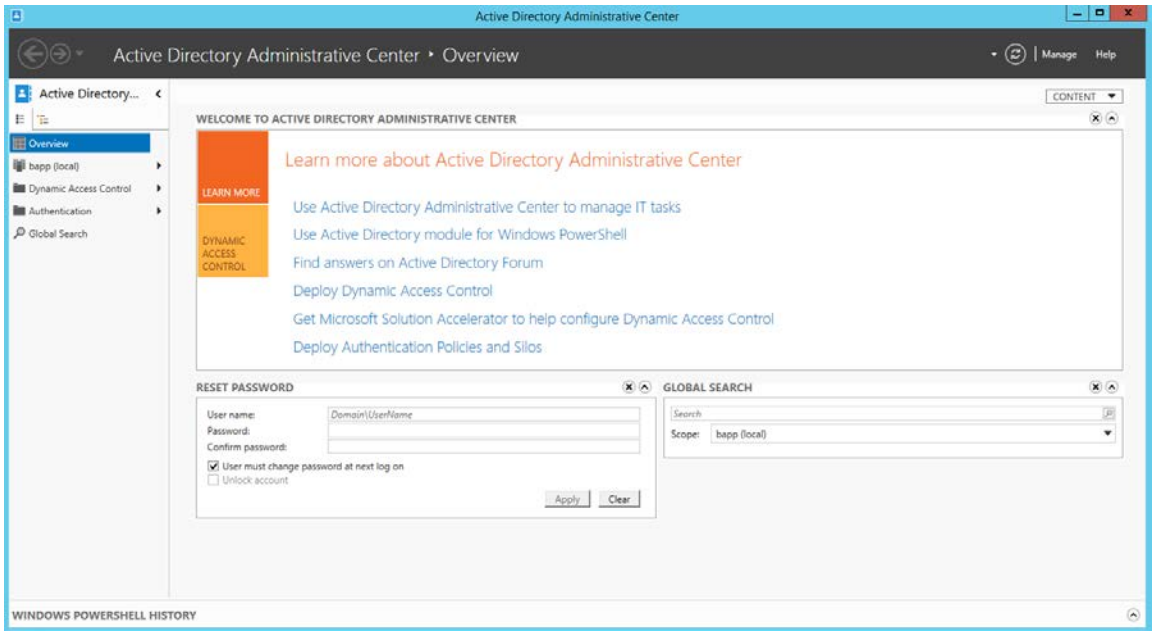
Active Directory Objects Vs Active Directory Organizational Units

An Active Directory Organizational Unit (OU) is a container that holds data in Active Directory. An Active Directory Object (O) is the data that the container (OU) holds. "Objects are located within Active Directory domains according to a hierarchical path, which includes the labels of the Active Directory domain name and each level of container objects. The full path to the object is defined by the distinguished name (also known as a "DN"). The name of the object itself, separate from the path to the object, is defined by the relative distinguished name."[6]

Active Directory Tools Overview

Microsoft has developed several useful and valuable administrative tools for Active Directory. These include:

Active Directory Administrative Center



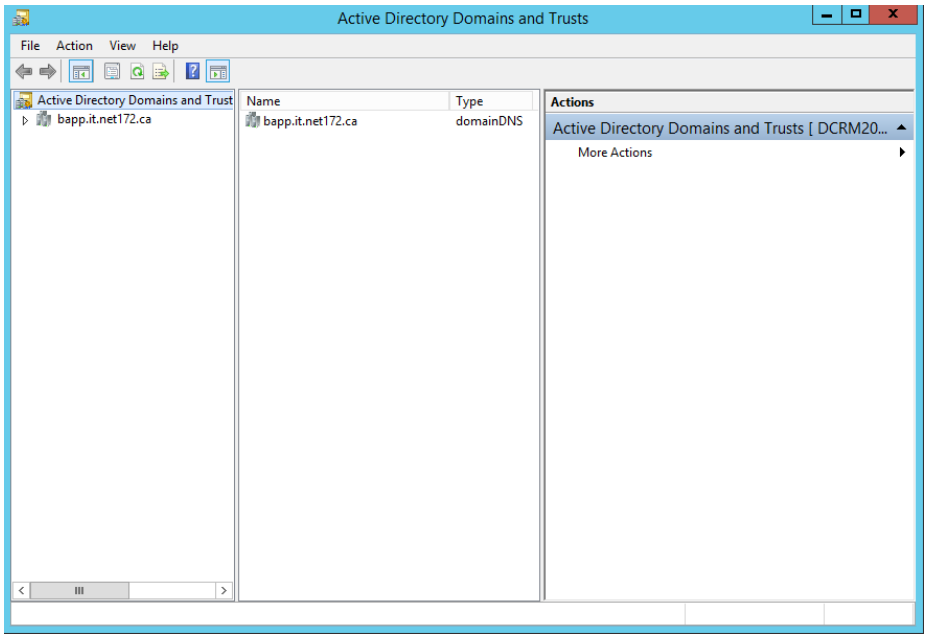
Administrative Center is the overview tool for administering Active Directory. Using Administrative Center, administrators can[7]:

- Create new user accounts or manage existing user accounts
- Create new groups or manage existing groups

[6] Object Naming. *Microsoft Technet*. https://technet.microsoft.com/en-us/library/cc977992.aspx
[7] Active Directory Administrative Center: Getting Started. *Microsoft Technet*. https://technet.microsoft.com/en-us/library/dd560651(v=ws.10).aspx

- Create new computer accounts or manage existing computer accounts
- Create new organizational units (OUs) and containers or manage existing OUs
- Connect to one or several domains or domain controllers in the same instance of Active Directory Administrative Center, and view or manage the directory information for those domains or domain controllers
- Filter Active Directory data by using query-building search

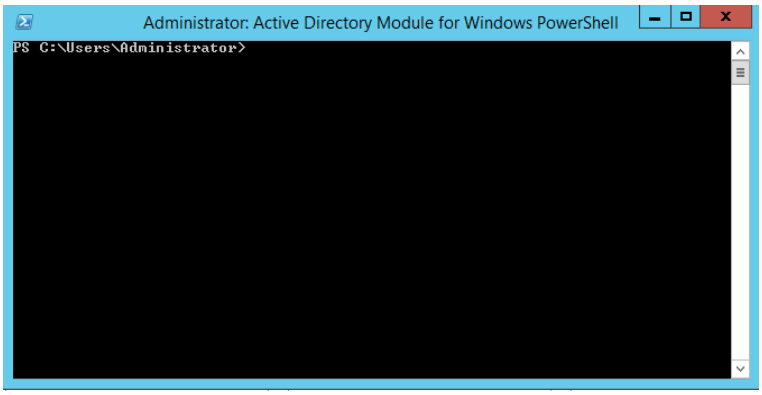
Active Directory Domains and Trusts



Active Directory Domains and Trusts "is the Microsoft Management Console (MMC) snap-in that you can use to administer domain trusts, domain and forest functional levels, and user principal name (UPN) suffixes."[8]

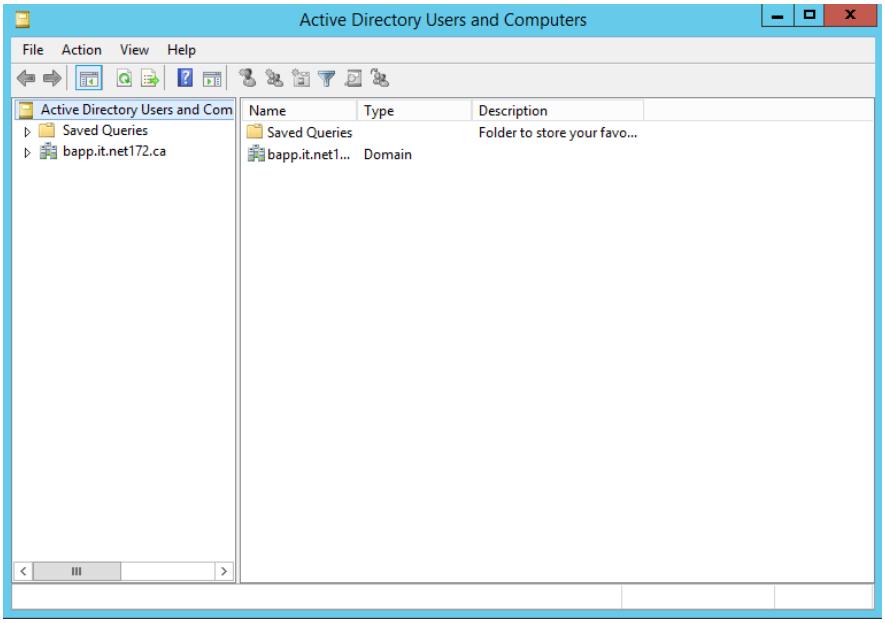
[8] Active Directory Domains and Trusts. *Microsoft Technet*. https://technet.microsoft.com/en-us/library/cc770299(v=ws.11).aspx

Active Directory Module for PowerShell



Active Directory Module for PowerShell " ... consolidates a group of cmdlets. You can use these cmdlets to manage your Active Directory domains, Active Directory Lightweight Directory Services (AD LDS) configuration sets, and Active Directory Database Mounting Tool instances in a single, self-contained package."[9]

Active Directory Users and Computers



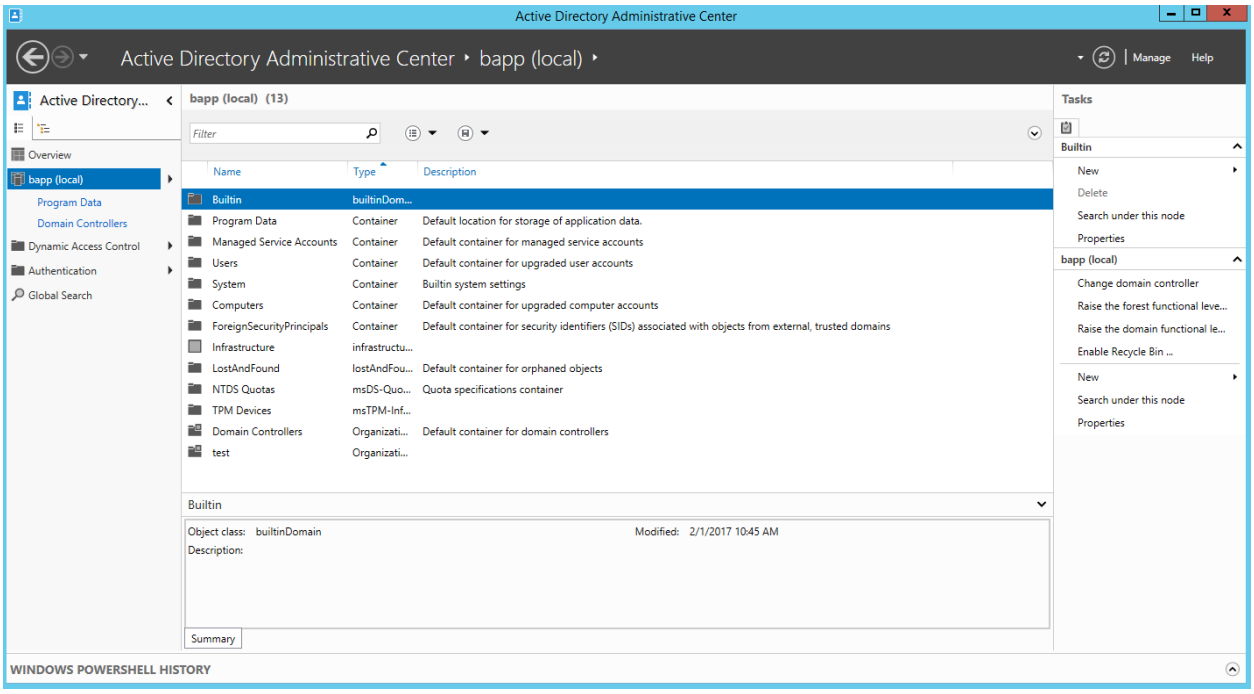
Active Directory Users and Computers "is a Microsoft Management Console (MMC) snap-in that you can use to administer and publish information in the directory."[10]

[9] Active Directory Cmdlets in Windows PowerShell. *Microsoft Technet*. https://technet.microsoft.com/en-us/library/ee617195.aspx

[10] Active Directory Users and Computers. *Microsoft Technet*. https://technet.microsoft.com/en-us/library/cc754217(v=ws.11).aspx

Default Active Directory Organizational Units

By default, Active Directory builds several Organizational Units. A screenshot illustrates this:



The default OUs include:

1. Builtin – "default service administrator accounts and domain local security groups. These groups are pre-assigned permissions needed to perform domain management tasks."[11] Example groups (objects) include Server Operators, Print Operators, Terminal Server License Servers.
2. Program Data – the default location for storage of application data. Contains other OUs for storing applications. This only includes an OU entitled "Microsoft" when first installed.
3. Managed Service Accounts – the default container for managed service accounts. On a fresh install, this OU does not contain any objects.
4. Users – the default container for upgraded user accounts. This OU contains all of the users and groups of users allowed within the domain. Each user and each group represents an object. Example users include the built-in "Administrator" account and the built-in "Guest" account. Example groups include "DnsAdmins" and "Enterprise Admins".
5. System – built-in system settings
6. Computers – the default container for upgraded computer accounts
7. ForeignSecurityPrincipals – the default container for security identifiers (SIDs) associated with objects from external, trusted domains

[11] Default Containers. *PC Care*. https://sites.google.com/a/pccare.vn/it/ent-admin-pages/default-containers

8. Infrastructure
9. LostAndFound – the default container for orphaned objects
10. NTDS Quotas – quota specifications container
11. TPM Devices
12. Domain Controllers – default container for domain controllers

Active Directory Replication

Most organizations will have several servers, and usually at least two domain controllers, a primary and a secondary. Replication is making sure the changes that are made on one domain controller are copied onto the other domain controllers within the organization. "Replication is the process by which the changes that are made on one domain controller are synchronized with all other domain controllers in the domain or forest that store copies of the same information. Data integrity is maintained by tracking changes on each domain controller and updating other domain controllers in a systematic way. Active Directory replication uses a connection topology that is created automatically, which makes optimal use of beneficial network connections and frees the administrators from having to make such decisions."[12]

Duplicate Workstation or Server Names in Active Directory

If two workstations or two servers have the same name in Active Directory, one will not be able to login and authenticate to the domain while the other is already logged in and authenticated. This will result in one of the workstations or one of the servers working. The solution is to change the name of the computer (workstation or server) to something that is unique, as per naming conventions in the domain.[13]

Duplicate Usernames in Active Directory

Similar to workstations or servers, it is critical that usernames not be duplicated in Active Directory. Like workstations or even servers, users are objects within the Active Directory hierarchy. The solution, as above, is to always make sure that you name your objects uniquely, following the naming conventions of the domain.[14] If two usernames are the same, Active Directory will modify one of the usernames automatically, which can lead to extreme complications. Best practice is to ensure no two usersnames are the same.

[12] Active Directory Replication. *Microsoft Technet*. https://technet.microsoft.com/en-us/library/cc961788.aspx
[13] Active Directory: Duplicate Object Name Resolution. *Microsoft Technet*. https://social.technet.microsoft.com/wiki/contents/articles/15435.active-directory-duplicate-object-name-resolution.aspx
[14] Ibid.

Active Directory Protocols: LDAP and SSL

The power of Active Directory is in its ability to tie networked computers together into a domain which shares resources. In order to do this, Active Directory uses:

LDAP

LDAP, Lightweight Directory Access Protocol, is what makes Active Directory so powerful. In essence, LDAP "…is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. "[15] So if a user requires the services of a file server, or a print server, or any other network resource, LDAP is what allows that to happen.

SSL

SSL, Secure Socket Layer, can be used in Microsoft Server 2012 R2 to encrypt communications between client and server. It is used in conjunction with LDAP, and encrypts data communications. "LDAP over SSL/TLS (LDAPS) is automatically enabled when you install an Enterprise Root CA on a domain controller "[16] Using LDAPS allow users to still locate the resources they need in the network (a file server, a print server, etc), but in a secure manner.

[15] LDAP (Lightweight Directory Access Protocol). *SearchMobileComputing*. http://searchmobilecomputing.techtarget.com/definition/LDAP

[16] LDAP over SSL (LDAPS) Certificate. *Microsoft Technet*. https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx