IW3 - Active Directory: Introduction, AD structure, FSMO

Ing. Jan Pluskal
UIFS
Brno University of Technology, Czech Republic
ipluskal@fit.vutbr.cz
What is Active Directory?

- Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks and is included in most Windows Server operating systems as a set of processes and services.

- An AD domain controller authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.

- Active Directory makes use of Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.
History

- Roots like everything other in computer networks in RFCs - RFC 1823 (on the LDAP API, August 1995), \[4\] RFC 2307, RFC 3062, and RFC 4533
- Revised and extended functionality and improve administration in Windows Server 2003
- With the release of the last Windows Server 2012 and Windows Server 2012 R2, Microsoft renamed the domain controller role as Active Directory Domain Services (AD DS)
What's New in Active Directory Domain Services

- AD DS improvements in Windows Server 2012 include:
  - **Virtualization that just works**
    - Virtualization-safe technologies and the rapid deployment of virtual domain controllers through cloning.
  - **Simplified deployment and upgrade preparation**
    - The upgrade and preparation processes (dcpromo and adprep) have been replaced with a new streamlined domain controller promotion wizard that is integrated with Server Manager and built on Windows PowerShell.
  - **Simplified management**
    - Active Directory Administrative Center (ADAC) now allows you to perform graphical tasks that automatically generate the equivalent Windows PowerShell commands.
  - **AD DS Platform Changes**
    - Updates to the AD DS platform include improved allocation and scale of RIDs
Logical structure vs Physical structure

- Organizational units
- Domains
- Trees
- Forests

- Active Directory sites (physical subnets)
- Domain controllers

Physical structure

• The physical structure of Active Directory helps to manage the communication between servers with respect to the directory.

• The two physical elements of Active Directory are **domain controllers** and **sites**.
Domain Controllers

- Domain controllers are Windows XXXX Server-based systems that store the Active Directory database.
- Every Windows XXXX domain controller has a writable copy of the directory (except RODC).
- Domain controllers in the same domain contain replicas of the directory that must be synchronized periodically.
Site

- Groups of IP subnets that are connected at high speed.
  - Generally considered to be subnets that are connected at LAN speeds (say 10 Mb) or higher.
- The purpose is to control network traffic relating to replication, as well as to help ensure that users connect to local resources.
- The replication inside the site (intra-site) is almost instantaneous (15 seconds) on the contrary, inter-site replication is scheduled by default in 180 minutes intervals.
  - Inter-site replication can also be scheduled to specific windows to ensure that the replication traffic does not interfere with normal data transfers.
Logical structure

- Active Directory instance consists of a **database** and corresponding **executable code** responsible for servicing requests and maintaining the database.
  - The executable part, known as Directory System Agent, is a collection of **Windows services** and **processes** that run on Windows 2000 and later.

- **Objects** in Active Directory databases can be accessed via LDAP protocol, ADSI (a **component object model** interface), **messaging API** and **Security Accounts Manager** services.
An Active Directory structure is an arrangement of information about objects. The objects fall into two broad categories: resources (e.g., printers) and security principals (user or computer accounts and groups).

Security principals are assigned unique security identifiers (SIDs).

Each object represents a single entity—whether a user, a computer, a printer, or a group—and its attributes.

An object is uniquely identified by its name and has a set of attributes—the characteristics and information that the object represents—defined by a schema, which also determines the kinds of objects that can be stored in Active Directory.

The schema object lets administrators extend or modify the schema when necessary.
• **A logical group** of users and computers that share the characteristics of centralized security and administration.

• **A boundary for security** – this means that an administrator of a domain is an administrator for only that domain, and no others, by default

• **A boundary for replication** – all domain controllers that are part of the same domain must replicate with one another

• Domains in the same forest automatically have *trust relationships configured.*
- A collection of Active Directory domains that share a contiguous namespace
- In this configuration, domains fall into a parent-child relationship, which the child domain taking on the name of the parent.
Forest (a set of trees)

- The largest unit in Active Directory and is a collection of trees that share a common Schema - the definition of objects that can be created.
- All trees are connected by transitive two-way trust relationships, thus allowing users in any tree access to resources in another for which they have been given appropriate permissions and rights.
- **By default** the first domain created in a forest is referred to as the root domain.
AD Forest

• http://static.businessinsider.com/image/51dfec8469bedd5e19000017-1200/image.jpg
Organizational Unit (OU)

• A container object that *helps to organize objects* for the purpose of administration or group policy application.

• An OU exists within a domain and *can only contain objects from that domain*.

• **OU can be nested**, which allows for more flexibility in terms of administration.

• Different methods for designing OU structures exists
  • Geographical
  • For a delegation of administrative authority
  • ...
Global Catalog

- Listings of every object that exists within an Active Directory **forest**
- By default, a domain controller only contains information about objects in that domain
- A **Global Catalog server** is a domain controller that contains information about every object (though not every attribute for each) stored in the entire forest.
- Facilitates and speeds up the search for information in Active Directory.
- By default only the first domain controller created in a forest has a copy of the global catalog.
Active Directory Domain Service Diagram

Administrative tasks easily delegated
John
Full Control
Michael
Can reset users' passwords
Richard
Manage printers
Tom
Modify group membership

Group Policies applied to Users, Groups or Organizational Units

Startup and Shutdown scripts
Desktop Settings
User Configuration

Group Policy 1

Computer Configuration

Auditing and Disk quotas
Start menu
User Configuration

Group Policy 2

Organizational Unit
Workstation
User
Group
Printer
Share
Policy

Legend:

*http://www.conceptdraw.com/How-To-Guide/active-directory-diagram*
• Instalace AD + připojení klienta do domény
  • nastartujte w2012-base a pomocí server manageru nainstalujte AD DS services
  • připojte do domény w8-base
  • vytvořte organizační jednotku, uživatele a skupinu
  • v konzoli AD Users and Computers zobrazte „Advanced Features“, prozkoumejte detailní nastavení uživatele
  • ptejte se lektora na to co, jste zapomněli 😊
Prozkoumání vylepšení v Active Directory Administrative Center

Vytvořte objekt uživatele, skupiny a novou organizační jednotku

- Uživatel Homer (Administrators), Bart
- Skupina Simpsons
- OU Brno

Povolte Active Directory Recycle Bin

Vyzkoušejte smazání a odstranění uživatele a OU
• Management AD objektů v PowerShell
  • Prohlédněte si exitující uživatele a skupiny
    • Get-Command *-AD*
    • Get-ADUser, Get-ADGroup, Get-ADOrganizationalUnit
  • Vytvořte objekt uživatele, skupiny a novou orgaizační jednotku
    • Uživatel Superman (Domain Administrators), Spiderman
    • Skupina Superheroes
    • OU Hollywood
    • New-ADUser, New-ADGroup, New-ADOrganizationalUnit
• Postup obdobný jako ad_introduction_lab.pdf
  Exercise 4, popř. IW2-exercices-03.pdf
• Vzdálená instalace záložního řadiče
  • nastartujte z w2012-base2
    • naaplikujte snapshot na r2 base, tak aby se „zresetoval“ do původního stavu (lektor poradí jak)
    • připojte w2012-base2 do domény vytvoření v Lab1
    • nakonfigurujte base server na použití dns serveru na ad
  • vzdáleně přes w2012-base
    • nainstalujte další řadič domény na base server
    • zkontrolujte zda se w2012-base2 přidal do domény jako DC

Postup obdobný jako ad_introduction_lab.pdf

Exercise 1
Active Directory – lab5

- Vzdálené nasazení Read-Only Domain Controller
- Zapněte virtuální stroj w2012 XXX
- Z w2012-base
  - Použijte PowerShell k instalaci AD DS na daný stroj **Install-WindowsFeature**
  - Povyšte stroj do role RODC obdobně jako ...
    - Delegace lokálního administrátora na uživatele Homer
    - otestujte delegaci lokálního administrátora
    - zkontrolujte přidání nového RODC do AD
    - otestujte možnost nastavení cachování hesel
    - na base serveru (pdc) „odstraňte“ přes users and computers konzoli účet serveru ad (rodc) a sledujte chování (možnost resetu hesla uživatelům co byli cacheování)
Flexible Single Master Operation Roles (FSMO)

- Active Directory has five special roles which are vital for the smooth running of AD as a multimaster system.
- Some functions of AD require there is an authoritative master to which all Domain Controllers can refer to.
- If you de-commission a DC and DCPROMO fails to run correctly or have a catastrophic failure of a DC you will need to know about these roles to recover or transfer them to another DC.
Flexible Single Master Operation Roles (FSMO)

**Forest Wide Roles:**
- Schema Master
- Domain Naming

**Domain Wide Roles:**
- Relative ID (RID) Master
- PDC Emulator
- Infrastructure Master
• Used to introduce manual and programmatic schema updates
• includes those updates that are added by Windows ADPREP /FORESTPREP
  • by Microsoft Exchange
  • by other applications that use Active Directory Domain Services (AD DS)
• **Must be online when schema updates are performed.**
**drink Attribute**

The drink (Favorite Drink) attribute type specifies the favorite drink of an object (or person).

<table>
<thead>
<tr>
<th>CN</th>
<th>drink</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ldap-Display-Name</td>
<td>drink</td>
</tr>
<tr>
<td>Size</td>
<td>-</td>
</tr>
<tr>
<td>Update Privilege</td>
<td>-</td>
</tr>
<tr>
<td>Update Frequency</td>
<td>-</td>
</tr>
<tr>
<td>Attribute-Id</td>
<td>0.9.2342.19200300.100.1</td>
</tr>
<tr>
<td>System-Id-Guid</td>
<td>1a1aa5b5-262e-4df6-aff0</td>
</tr>
<tr>
<td>Syntax</td>
<td>String(Unicode)</td>
</tr>
</tbody>
</table>

- [http://aheil.files.wordpress.com/2005/06/drink.png](http://aheil.files.wordpress.com/2005/06/drink.png)
Domain Naming Master

• Used to add and to remove domains and application partitions to and from the forest.

• *Must be online when domains and application partitions in a forest are added or removed.*
Primary Domain Controller (PDC emulator)

- **Receives password updates** when passwords are changed for the computer and for user accounts that are on replica domain controllers.
- Consulted by replica domain controllers that service authentication requests that have *mismatched passwords*.
- Default target domain controller for Group Policy updates.
- Target domain controller for legacy applications that perform writable operations and for some admin tools.
- Must be online and accessible 24 hours a day, seven days a week.
Relative ID (RID) Master

- Allocates active and standby RID pools to replica domain controllers in the same domain.
- **Must be online for newly promoted domain controllers to obtain a local RID pool that is required to advertise or when existing domain controllers have to update their current or standby RID pool allocation.**
Infrastructure Master

- **Scope:** Domain, Application partition
- Updates cross-domain references and phantoms from the global catalog.
- A *separate infrastructure master* is created for each application partition including the default forest-wide and domain-wide application partitions created by Windows Server 2003 and later domain controllers.
FSMO availability and placement

• The *Active Directory Installation Wizard* performs the initial placement of roles on domain controllers. This placement is frequently correct for directories that have just a few domain controllers.

• It's easier to keep track of FSMO roles if you host them on *fewer computers*.

• If a role has to be moved to a different domain controller, and the current role holder is online and available, you should *transfer (not seize)* the role to the new domain controller.

• *Place the schema master on the PDC of the forest root domain.*

• *Place the domain naming master on the forest root PDC.*
Transfer vs Seize

• **Recommendation** – always transfer if possible
• **Transfer** – both machines has to be online at the same time
• **Seize** – if targeted server has malfunctioned or disappeared, *general rule* - after seizing a role never return the DC back (except PDC, infrastructure)

• **Tools**
  • GUI administrative tools
  • `ntdsutil /roles`
  • `Netdom query fsmo`
Vyzkoušejte přesun jednotlivých FSMO mezi řadiči domény pomocí

- GUI administrativních nástrojů
- Příkazové řádky ntdsutil
- PowerShell Move-ADDirectoryServerOperationMasterRole
Recap

• What is the Active Directory physical and logical structure?
• What are Flexible Single Master Operation Roles (FSMO)?
• What they are used for?
• What is the preferred and safest way transfer/seize?
Sources

- http://support.microsoft.com/kb/223346/en-us
- http://www.ucs.cam.ac.uk/support/windows-support/winsuptech/activedir/fsmoroles
Thank you for attention!
Any questions?!