Install and Configure AD Domain Services
Active Directory 101 vs. Exam 70-742

- Implement and manage a certificate authority (CA) hierarchy with AD CS
- Deploy and manage certificates
- Implement and administer Active Directory Federation Services (AD FS)
- Implement and administer Active Directory Rights Management Services (AD RMS)
- Implement synchronization between AD DS and Azure AD
- Monitor, troubleshoot, and establish business continuity for AD DS services
- Secure AD DS and user accounts
- Manage user settings by using GPOs
- Implement and manage Group Policy
- Configure and manage replication
- Implement AD DS sites
- Implement AD DS in complex environments
- Manage objects in AD DS
- Install and configure Domain Controllers
Agenda

• An introduction to Active Directory Domain Services
• Active Directory Domain Controllers
• Deploying a Domain Controller
• Managing Active Directory
• Netwrix Auditor’s reporting functionality
AD Domain Services
Active Directory (Domain Services)

• **Logical components**
  - Partitions
  - Schema
  - Domains
  - Forests
  - Sites
  - Containers
  - Organizational Units

• **Physical components**
  - Domain Controllers
  - Read-only Domain Controllers
  - Databases (ntds.dit)
  - The System Volume (SYSVOL)
  - Global Catalog Servers
How the components relate to each other

• Domain Controllers are grouped
  – In forests to create administrative and schema boundaries
  – In domains and sites to govern replications

• Each DC hosts the AD database and SYSVOL
  – The database and system volume is replicated throughout the domain

• Each DC respects the central schema
  – The schema is set per Active Directory forest

• Objects are created in the database
  – The schema defines the object classes, but objects themselves live in partitions
  – Objects can be grouped in hard-coded containers and Organizational Units
Containers and Organizational Units (OUs)

- Both can hold objects within an AD domain

- Containers are built-in
  - Cannot be created or deleted using the graphical tools or PowerShell
  - Cannot be assigned GPs, offer no delegation options
  - Used for system objects and default locations

- Organizational Units (OUs) are for you
  - One built-in OU: Domain Controllers
  - Can be created and deleted at will
  - Can be assigned Group Policies and offer delegation options
Recent changes in Active Directory

• **Windows Server 2016**
  - Privileged Access Management
  - Azure AD Join
  - Windows Hello for Business

• **Windows Server 2012 R2**
  - Authentication Policies
  - Authentication Policy Silos
  - Protected Users
AD Domain Controllers
Flexible Single Master Operations (FSMO) role holders

1. To support the multi-master model (every Domain Controllers is writable)
2. Two forest-wide roles (Schema Master, Domain Naming Master)
3. Three domain-wide roles (PDC Emulator, RID Master, Infrastructure Master)

Global Catalog Servers (GCs)

2. In multi-domain environments, the Global Catalog caches essential attributes on objects in other domains, thus holds more information
3. This speeds up authentication and makes it more reliable

Read-only Domain Controllers (RODCs)

4. Host a read-only copy of the Active Directory database (and DNS)
5. Can be scoped for authenticating and caching certain objects, only
6. Ideal for branch offices, not so much for perimeter networks
The role of the Global Catalog
Domain Controllers are Access Points

- Host the database
  - Ntds.dit

- Offer authentication Services
  - Kerberos (as Key Distribution Centers)
  - LDAP, NTLM and LM

- Offer file shares (over SMB)
  - The System Volume (SYSVOL) share

- Tips!
  - Make sure you deploy at least two Domain Controllers per domain
  - Deploy Read-only Domain Controllers for insecure branch offices
DNS, Active Directory’s Achilles’ Heel

Everything's connected
- Domain Controllers find other Domain Controllers through DNS
- Domain-joined devices find Domain Controllers through DNS

Domain Controllers register DNS SRV records
- For their authentication services (GC, Kerberos)

When a domain-joined device queries DNS, by default
- All Domain Controllers in its site are returned
- All Domain Controllers in the nearest site are returned (empty site)
- A random list of Domain Controllers is returned (multiple empty sites)
Deploying a Domain Controller
Deployment options for Domain Controllers

Install the Active Directory Domain Services Role

Use Server Manager to install the Role (remotely)

PowerShell:

`Install-WindowsFeature AD-Domain-Services -IncludeManagementTools`
Deployment options for Domain Controllers

1. A Domain Controller for an existing domain
   ➔ Use the Active Directory Domain Services Configuration Wizard (remotely)
   `Dcpromo.exe /unattend
   Install-ADDSDomainController`

2. A Domain Controller for new Domain in an existing Forest
   ➔ Use the Active Directory Domain Services Configuration Wizard (remotely)
   `Dcpromo.exe /unattend
   Install-ADDSDomain`

3. A Domain Controller for a new Forest
   ➔ Use the Active Directory Domain Services Configuration Wizard (remotely)
   `Dcpromo.exe /unattend
   Install-ADDSSForest`
Rapid Deployment options

Install from Media (IfM)

- Ideal for new Domain Controllers in branch offices with limited WAN connectivity
- Export ntds.dit and SYSVOL with ntdsutil.exe and take on disk
- Use the Install from Media section on the Additional Options page when promoting the new branch office Domain Controllers, then only replicate changes

Domain Controller Cloning

- Ideal for virtualized Domain Controllers, Windows Server 2012, and up.
- Depends on the VM-GenerationID feature by the hypervisor
- Governed by Cloneable Domain Controllers group memberships, so fabric admins cannot use it to clone off Domain Controllers
Managing Active Directory
Choose your weapon

- Active Directory Administrative Center
- Windows PowerShell
  - ActiveDirectory module
  - ADDSDeployment module
- Active Directory Users and Computers
- Active Directory Sites and Services
- Active Directory Domains and Trusts
- Active Directory Schema snap-in
- The ds* tools
  - dsadd.exe
  - dsquery.exe
  - dsget.exe, etc.
Active Directory objects

User objects

- Used to log on interactively by colleagues, as a service
- Typical attributes: userPrincipalName, g, sn
- Can use profiles for centralized storage of settings and default folders

Group objects

- Two types: security groups (with sIDs) and distribution groups (no sIDs)
- Four scopes: Local, Domain-local, Universal and Global groups

Computer objects

- Object is used to create the Secure Channel, based on object password
## Default objects and their locations

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>Container</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>User</td>
<td>Users</td>
</tr>
<tr>
<td>Krbtgt</td>
<td>User</td>
<td>Users</td>
</tr>
<tr>
<td>Enterprise Admins</td>
<td>Group</td>
<td>Users</td>
</tr>
<tr>
<td>Schema Admins</td>
<td>Group</td>
<td>Users</td>
</tr>
<tr>
<td>Administrators</td>
<td>Group</td>
<td>Built-in</td>
</tr>
<tr>
<td>Domain Admins</td>
<td>Group</td>
<td>Users</td>
</tr>
<tr>
<td>Server Operators</td>
<td>Group</td>
<td>Built-in</td>
</tr>
<tr>
<td>Account Operators</td>
<td>Group</td>
<td>Built-in</td>
</tr>
<tr>
<td>Backup Operators</td>
<td>Group</td>
<td>Built-in</td>
</tr>
<tr>
<td>Print Operators</td>
<td>Group</td>
<td>Built-in</td>
</tr>
<tr>
<td>Cert Publishers</td>
<td>Group</td>
<td>Built-in</td>
</tr>
<tr>
<td>Everyone</td>
<td>Group</td>
<td>-</td>
</tr>
<tr>
<td>Authenticated Users</td>
<td>Group</td>
<td>-</td>
</tr>
</tbody>
</table>
# Object management with PowerShell

<table>
<thead>
<tr>
<th>PowerShell Cmdlet</th>
<th>Use it to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>New-ADUser</td>
<td>Create a user object in Active Directory</td>
</tr>
<tr>
<td>Set-ADUser</td>
<td>Modify attributes for a user object in Active Directory</td>
</tr>
<tr>
<td>Remove-ADUser</td>
<td>Delete user object from Active Directory</td>
</tr>
<tr>
<td>Set-ADAccountPassword</td>
<td>Reset the password for a user object in Active Directory</td>
</tr>
<tr>
<td>Set-ADAccountExpiration</td>
<td>Modify the expiration date for a user object</td>
</tr>
<tr>
<td>Unlock-ADAccount</td>
<td>Unlock a user object, after it has become locked after too many sign-in attempts</td>
</tr>
<tr>
<td>Enable-ADAccount</td>
<td>Enable a user object</td>
</tr>
<tr>
<td>Disable-ADAccount</td>
<td>Disable a user object</td>
</tr>
<tr>
<td>New-ADGroup</td>
<td>Create a group in Active Directory</td>
</tr>
<tr>
<td>Add-ADGroupMember</td>
<td>Add an object as a member of a group</td>
</tr>
<tr>
<td>Test-ComputerSecureChannel</td>
<td>Verify and repair the trust relationship for a device</td>
</tr>
<tr>
<td>Reset-ComputerMachinePassword</td>
<td>Resets the password for a computer object</td>
</tr>
<tr>
<td>New-ADOrganizationalUnit</td>
<td>Create an OU in Active Directory</td>
</tr>
</tbody>
</table>
Delegation of Control

• Beyond the default delegation settings, based on default objects, permissions on objects can be granted to users or groups

• The Delegation of Control Wizard can be used to assign common administrative tasks, beyond the defaults available like Account Operators, Server Operators, Backup Operators, etc.

• Beyond the Delegation of Control Wizard, the advanced security properties for an OU allow you to grant even more granular permissions
Apply a naming convention to all types of objects and OUs

Disable unused objects, delete stale objects

Apply Global-(Universal)-DomainLocal group nesting

Use Restricted Groups to govern local group memberships

Divide servers and devices into roles per OU, per admin group

Restrict users from creating the default 10 computer objects

Do not use the built-in delegated groups, unless you're 100% confident their scope and permissions are 100% correct
Netwrix Auditor

Know Your Data. Protect What Matters.
About Netwrix Corporation

**Year of foundation:** 2006

**Headquarters location:** Irvine, California

**Global user base:** over 300,000

**Recognition:**
- 7 years among the fastest growing software companies in the US
- More than 140 industry awards
Netwrix Auditor Unified Platform

Data Discovery & Classification

**Infrastructure**
- Netwrix Auditor for Active Directory
- Netwrix Auditor for Network Devices
- Netwrix Auditor for Windows Server
- Netwrix Auditor for VMware

**Unstructured Data**
- Netwrix Auditor for Windows File Servers
- Netwrix Auditor for SharePoint
- Netwrix Auditor for EMC
- Netwrix Auditor for NetApp
- Netwrix Auditor for Exchange

**Structured Data**
- Netwrix Auditor for SQL Server
- Netwrix Auditor for Oracle Database
- Netwrix Auditor for Office 365
- Netwrix Auditor for Azure AD
- Netwrix Auditor for VMware

**Cloud**
- Netwrix Auditor for Office 365
- Netwrix Auditor for Azure AD
- Netwrix Auditor for Amazon Web Services
- Netwrix Auditor for IBM QRadar

**Free Add-ons**
- Add-on for Generic Linux Syslog
- Add-on for Amazon Web Services
- Add-on for ServiceNow ITSM
- Add-on for Splunk
- Add-on for IBM QRadar
Netwrix Auditor

Demonstration
Next Steps

- **Free trial:** Set up Netwrix Auditor in your own test environment [netwrix.com/auditor](http://netwrix.com/auditor)
- **Virtual appliance:** Get Netwrix Auditor up and running in minutes [netwrix.com/go/appliance](http://netwrix.com/go/appliance)
- **In-browser demo:** Run a demo right in your browser with no need to install anything [netwrix.com/go/browser_demo](http://netwrix.com/go/browser_demo)
- **Contact Sales** to obtain more information: [netwrix.com/contactsales](http://netwrix.com/contactsales)

Join us for the next sessions of the course:

- **Manage and Maintain AD Domain Services** ➔ Thursday, 25th April
- **Create and Manage Group Policy** ➔ Tuesday, 30th April
Thank You!

Sander Berkouwer
10-time Microsoft MVP
Active Directory aficionado

Mason Takacs
Solutions Engineer
Netwrix