Dizajniranje i implementacija Active Directory fizičke topologije

11. PREDAVANJE

Module Overview

- Designing and Implementing Active Directory Sites
- Designing Active Directory Replication
- Designing the Placement of Domain Controllers
- Virtualization Considerations for Domain Controllers
- Designing Highly Available Domain Controllers

Lesson 1: Designing and Implementing Active Directory Sites

- Benefits of Deploying Active Directory Sites
- Options for Designing AD DS Sites
- Collecting Information for an AD DS Site Design
- How Does Automatic Site Coverage Work?
- Considerations for Designing AD DS Sites
- Demonstration: Creating Site Objects

Benefits of Deploying Active Directory Sites

- AD DS sites are highly connected portions of your enterprise
  - Sites represent network segments connected at LAN speeds
- AD DS sites are objects that support:
  - Replication
    - You can define replication boundaries and manage replication through the use of site links
  - Service localization
    - Client systems can quickly find services that are located locally, or the best connected remote site

Options for Designing AD DS Sites

Single-site model

Consider using if one or more of the following are true:

- All computers are in one physical location
- The physical locations are connected with high-speed links
- All domain controllers are in one location

Multiple-site model

Consider using if one or more of the following are true:

- Your organization has several physical locations
- The links between locations are slow or unreliable
- You have other requirements for segregating Active Directory-related network traffic

Collecting Information for an AD DS Site Design

Collect the following information about the existing network:

- Geographic locations, communication links, and available bandwidth
- IP subnets assigned to each location
- Number of users and computers in each domain, in each location
- Domain controller and global catalog server placement
- Site-aware applications

How Does Automatic Site Coverage Work?

All domain controllers use a common algorithm for determining automatic site coverage. The domain controller:

1. Builds a list of target sites, which are those sites that have no domain controllers for its domain.
2. Builds a list of candidate sites, which are the sites that have domain controllers for this domain.
3. Registers service (SRV) records that are specific to the target site for the domain controllers for this domain in the selected site.

Considerations for Designing AD DS Sites

When designing a site topology:

- Consider placing a domain controller in any location that is defined as a site
- Create a site for any location that has a server that runs a site-aware application
- Ensure that the IP subnets map to the correct site objects
- Follow recommendations for when to configure additional sites for branch offices
- Give sites meaningful names
- Move or deploy domain controllers to the Active Directory sites

Lesson 2: Designing Active Directory Replication

- Active Directory Replication Elements
- What Are the KCC and the Intersite Topology Generator?
- Options for Designing Replication Topologies
- Considerations for Choosing a Replication Protocol
- Planning Global Catalog and RODC Replication
- Planning for SYSVOL Replication
- Considerations for Designing Site Links and Bridgehead Servers
- Considerations for Designing Site Link Bridging
- Demonstration: Configuring Active Directory Replication

Active Directory Replication Elements

To properly design AD DS replication, you must understand the purpose of each replication element:

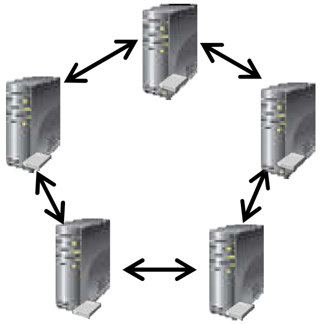
- Connection objects
- Notification
- Polling

What Are the KCC and the Intersite Topology Generator?

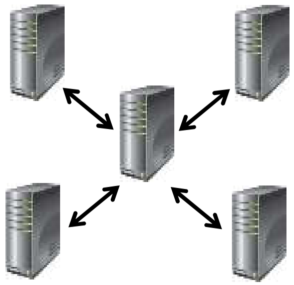
- Knowledge Consistency Checker
  - Generates the replication topology for the Active Directory forest
  - Intrasite and intersite replications have different topologies
- Intersite Topology Generator
  - The instersite topology generator manages the intersite topology for replication
  - One domain controller per site has the role of intersite topology generator
  - You can transfer the intersite topology generator role manually

Options for Designing Replication Topologies

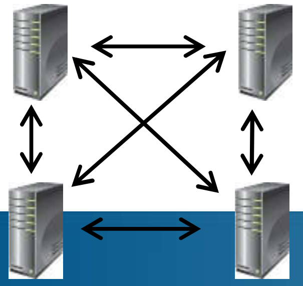
Ring topology



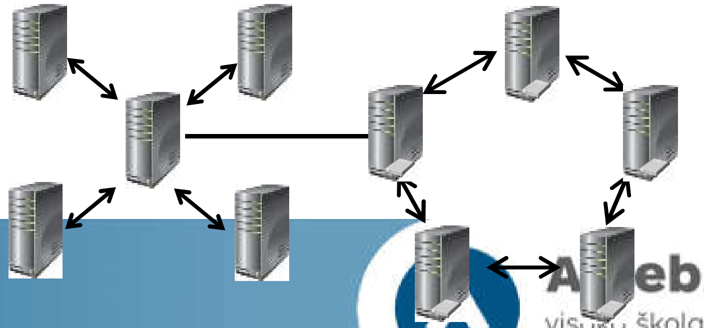
Hub-and-spoke topology



Full-mesh topology



Hybrid topology



Considerations for Choosing a Replication Protocol

The three levels of connectivity for replicating Active Directory information are:

- Uniform, high-speed, synchronous RPC over IP within sites
- Point-to-point, synchronous, low-speed RPC over IP between sites
- Low-speed, asynchronous SMTP between sites

When selecting a replication protocol, consider the following:

- Replication within a site always uses RPC over IP
- Replication between sites can use either RPC over IP or SMTP over IP
- Replication between sites over SMTP is supported only for the schema partition, configuration partition, and global catalog replication

Planning Global Catalog and RODC Replication

In addition to the regular replication process within your Active Directory forest, you should also consider the placement of:

- RODCs
- Global catalog servers

Planning for SYSVOL Replication

- Domain controllers use SYSVOL to replicate logon scripts and GPOs.
- Windows Server 2012 uses DFS Replication, which offers several advantages:
  - Efficient, scalable, and reliable file-replication protocol
  - Differential replication
  - Flexible scheduling and bandwidth throttling
  - Self-healing by using USNs
  - A new MMC snap in UI management tool
  - Built-in health monitoring
  - Improved support for RODCs

Considerations for Designing Site Links and Bridgehead Servers

- The KCC assumes all domain controllers in a site can communicate. Between sites, you represent network paths by creating site link objects. Considerations for site links include:
  - Site link costs
  - Replication frequency
  - Replication schedules
- The bridgehead server is responsible for all replication in and out of the site for a partition:
  - The intersite topology generator selects bridgehead servers automatically
  - Bridgehead servers are selected per partition
- You should not modify the default configuration without a good reason

Considerations for Designing Site Link Bridging

When designing site link bridging, consider the following guidelines:

- If a network is not fully routed, and if you do not have to control Active Directory replication, leave automatic site link bridging enabled
- If a network is not fully routed, configure the site link bridges to map to the physical network connections
- To model the routing behavior of your network, create and configure site link bridge objects
- If all site links within the bridge are required to route transitively, add site links to a site link bridge
- Ensure that each site link in a manual site link bridge has one site in common with another site link in the bridge

Lesson 3: Designing the Placement of Domain Controllers

- Planning Hardware Requirements for Domain Controllers
- Considerations for Deploying Domain Controllers on Server Core
- Considerations for Planning Domain Controller Locations
- Considerations for Planning Global Catalog Server Locations
- Considerations for Planning Operations Master Server Locations
- Guidelines for Monitoring Active Directory Domain Controllers
- Deploying Read-Only Domain Controllers in Branch Offices
- Considerations for Deploying Domain Controllers on Windows Azure Virtual Machines

Planning Hardware Requirements for Domain Controllers

- Free disk space is the most important resource for domain controllers

Drive contains	Provide
Ntds.dit	0.04 GB of storage for each 1,000 users
Active Directory log files	At least 500 MB of available space
SYSVOL shared folder	At least 500 MB of available space
Operating system files with which you run Setup	At least 1.25 - 2 GB of available space

- Allow for more disk space if the domain controller also hosts the global catalog server role

Considerations for Deploying Domain Controllers on Server Core

When deploying a domain controller on a Server Core installation:

- Use Windows PowerShell to install the binaries for the domain controller server role
- Manage AD DS on the Server Core installation remotely
- Apply the same hardware requirements as you would on a full version of Windows Server

Considerations for Planning Domain Controller Locations

When determining whether to deploy a domain controller in a branch office, consider the following:

- Not all locations require a domain controller
- If you deploy a domain controller in a branch, you should create an Active Directory site for that branch
- Deploy RODCs to locations where physical security is a concern
- Always deploy domain controllers to locations that use Active Directory-intensive applications
- Place two domain controllers for each domain in each site

Considerations for Planning Global Catalog Server Locations

When designing global catalog placement:

- Deploy at least one global catalog server in each site
- Deploy two global catalog servers in each site for redundancy
- Deploy multiple global catalog servers if you have sites with a large number of users
- Be aware of applications that require a global catalog presence in the same site

Considerations for Planning Operations Master Server Locations

- Collocate the schema master and domain naming master on a global catalog server
- Collocate the RID master and PDC emulator roles
- Place the infrastructure master on a domain controller that is not a global catalog server, unless:
  - All domain controllers are global catalog servers
  - You have enabled the Active Directory Recycle Bin
- Have a failover plan

Guidelines for Monitoring Active Directory Domain Controllers

- Windows Server 2012 provides several tools that you can use for monitoring:
  - Task Manager
  - Resource Monitor
  - Event Viewer
  - Reliability Monitor
  - Performance Monitor
  - Repadmin
- The Best Practices Analyzer:
  - Compares your Active Directory environment to best practices for prerequisites, configuration, and operation
  - Can be run periodically to monitor for changes

Deploying Read-Only Domain Controllers in Branch Offices

Reasons for deploying an RODC:

- Few, if any IT personnel
- Less secure facilities
- Improved local authentication
- Security issues
- Directory service integrity

Considerations before deploying an RODC:

- Only one RODC allowed per site
- Password replication policy
- Applications that require write access to AD DS

Considerations for Deploying Domain Controllers on Windows Azure Virtual Machines

- Deploy AD DS on a Windows Azure virtual machine for:
  - Redundancy
  - Disaster recovery
  - Reduced latency in remote offices
  - Support Windows Azure-based applications

- Considerations
  - RODC or full writeable domain controller
  - Continuous replication
  - Site placement
  - Replication costs

Lesson 4: Virtualization Considerations for Domain Controllers

- Considerations for Virtualizing Domain Controllers
- Securing Virtualized Domain Controllers
- Considerations for Deploying Virtualized Domain Controllers
- Cloning Domain Controllers

Considerations for Virtualizing Domain Controllers

Advantages:

- Consolidation
- Testing
- Deployment
- Performance

Disadvantages:

- Mishandling vhd or .vhdx image files can result in forest-wide corruption
- Security

Securing Virtualized Domain Controllers

- The host computer on which virtual domain controllers are running must be managed as carefully as writeable domain controllers
- Security guidelines include:
  - Protecting the local administrator account on the host computer
  - Using the Server Core installation as a platform for Hyper-V
  - Protecting .vhd files

Considerations for Deploying Virtualized Domain Controllers

Consider these Virtual domain controller limitations:

- Avoid using differential virtual hard drives for domain controllers
- Do not export virtual machines with domain controllers
- Do not use Hyper-V snapshots
- Disable time synchronization with the host computer

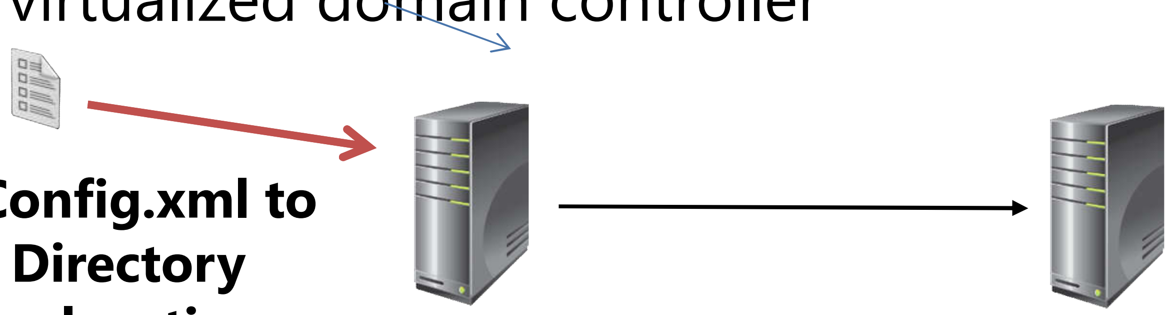
VM-Generation-ID:

- Windows 2012 attribute used to help reduce replication errors due to applied snapshots or rollbacks
- Both virtual host and virtual machine maintain the VM-Generation-ID
- Mismatch at startup indicates a snapshot rollback or restore has occurred
- When an applied snapshot or rollback is detected, the domain controller requests a new RID pool and USN information update

Cloning Domain Controllers

You can safely clone existing virtualized domain controllers by:

- Creating a DcCloneConfig.xml file and storing it in the Active Directory database location
- Taking the virtualized domain controller offline and exporting it
- Creating a new virtual machine by importing the exported virtualized domain controller



DcCloneConfig.xml to Active Directory database location

Export the virtualized domain controller

Import the virtualized domain controller

Lesson 5: Designing Highly Available Domain Controllers

- Planning for High Availability
- Components of an Active Directory High Availability Design
- Considerations for Designing Highly Available Domain Controllers
- Considerations for Designing Highly Available Global Catalog Servers
- Considerations for Designing a Highly Available DNS Infrastructure
- Considerations for Designing a Highly Available Network Infrastructure
- Considerations for Backup and Recovery in AD DS

Planning for High Availability

Consider the following points when planning for high availability:

- Determine acceptable service levels
- Identify risks to your service levels
- Determine how to mitigate risks to these levels
- Plan for capacity
- Determine where hardware vendor cooperation will be necessary

Components of an Active Directory High Availability Design

To make AD DS highly available:

- Deploy multiple domain controllers
- Distribute operations master roles
- Deploy multiple global catalog servers
- Deploy multiple DNS servers
- Provide a redundant network infrastructure

Considerations for Designing Highly Available Domain Controllers

- Install the Active Directory server role on servers with redundant hardware
- Install at least one domain controller per branch site and at least two per hub site
- Enable the TryNextClosestSite Group Policy setting
- Connect domain controllers to highly available network infrastructures
- Ensure that domain controllers have all security updates and antivirus software installed

Considerations for Designing Highly Available Global Catalog Servers

When designing global catalog server placement and high availability:

- In a single-domain forest, configure all domain controllers as global catalog servers
- In a multiple-domain forest, the number of global catalog servers depends on the number of users, links between sites, applications, and other factors

Considerations for Designing a Highly Available DNS Infrastructure

To make DNS highly available, consider the following:

- Implement at least two DNS servers per site
- Integrate DNS zones in AD DS
- Harden security on DNS servers
- Distribute primary and secondary DNS addresses to clients via DHCP

Considerations for Designing a Highly Available Network Infrastructure

When designing a highly available network infrastructure:

- Use redundant network switches that connect to different NICs on domain controllers
- Implement a backup link for branch offices via an alternate operator
- Require an SLA with the telecom operator
- Back up the configuration of network devices, such as switches and routers
- Provide for spare network devices on site

Considerations for Backup and Recovery in AD DS

- Use either Windows Server Backup or Wbadmin.exe
- Backups can be manual or automated
- You must back up all critical volumes for AD DS:
  - System volume
  - Boot volume
  - Volumes hosting SYSVOL, Active Directory database (NTDS.dit), logs

Considerations for Backup and Recovery in AD DS (continued)

- The Active Directory Recycle Bin:
  - Cannot be disabled once it is enabled
  - Now has a user interface to simplify restoration of objects
  - Is enabled and accessed through the Active Directory Administration Center
  - Preserves objects for the lifetime of the tombstone: 180 days by default

Considerations for Backup and Recovery in AD DS (continued)

- Options for restoring AD DS:
  - Nonauthoritative (normal) restore
  - Authoritative restore
  - Full server restore
  - Alternate location restore