Microsoft® Official Course

Module 5
Implementing Active Directory Domain Services Sites and Replication
Module Overview

• AD DS Replication Overview
• Configuring AD DS Sites
• Configuring and Monitoring AD DS Replication
Lesson 1: AD DS Replication Overview

- What Are AD DS Partitions?
- Characteristics of AD DS Replication
- How AD DS Replication Works Within a Site
- Resolving Replication Conflicts
- How Replication Topology Is Generated
- How RODC Replication Works
- How SYSVOL Replication Works
What Are AD DS Partitions?

Active Directory Database

- **Configuration**: Forest-wide information about the Active Directory structure
- **Schema**: Forest-wide definitions and rules for creating and manipulating objects and attributes
- **<Domain>**: Information about domain-specific objects
- **<Application>**: Information about applications
Characteristics of AD DS Replication

- Multi-master replication ensures:
  - Accuracy (integrity)
  - Consistency (convergence)
  - Performance (keeping replication traffic to a reasonable level)
- Key characteristics of Active Directory replication include:
  - Multi-master replication
  - Pull replication
  - Store-and-forward
  - Partitions
  - Automatic generation of an efficient, robust replication topology
  - Attribute-level and multivalue replication
  - Distinct control of intrasite and intersite replication
  - Collision detection and remediation
How AD DS Replication Works Within a Site

• Intrasite replication uses:
  • Connection objects for inbound replication to a domain controller
  • KCC to automatically create topology
    • Efficient (maximum three-hop) and robust (two-way) topology
  • Notifications in which the domain controller tells its downstream partners that a change is available
  • Polling, in which the domain controller checks with its upstream partners for changes
    • Downstream domain controller directory replication agent replicates changes
    • Changes to all partitions held by both domain controllers are replicated
Resolving Replication Conflicts

• In multi-master replication models, replication conflicts arise when:
  • The same attribute is changed on two domain controllers simultaneously
  • An object is moved or added to a deleted container on another domain controller
  • Two objects with the same relative distinguished name are added to the same container on two different domain controllers

• To resolve replication conflicts, AD DS uses:
  • Version number
  • Time stamp
  • Server GUID
How the Replication Topology Is Generated

- Domain A topology
- Domain B topology
- Schema and configuration topology
- Global catalog replication
How RODC Replication Works

• When an RODC is implemented:
  • The KCC detects that it is an RODC and creates one-way-only connection objects (black) from one or more source domain controllers
  • Write referrals are sent to the source domain controllers from the RODC (gray)

• An RODC performs Replicate Single Object inbound replication during:
  • Password changes
  • DNS updates to a writable DNS server
  • Updates to various client attributes
How SYSVOL Replication Works

• SYSVOL contains logon scripts, Group Policy templates, and GPOs with their content
• SYSVOL replication can take place using:
  • FRS, which is primarily used in Windows Server 2003 and older domain structures
  • DFS Replication, which is used in Windows Server 2008 and newer domains
• To migrate SYSVOL replication from the FRS to DFS Replication:
  • The domain functional level must be at least Windows Server 2008
  • Use the Dfsrmig.exe tool to perform the migration
Lesson 2: Configuring AD DS Sites

- What Are AD DS Sites?
- Why Implement Additional Sites?
- Demonstration: Configuring AD DS Sites
- How Replication Works Between Sites
- What Is the Intersite Topology Generator?
- Optimizing Domain Controller Coverage in Multiple Site Scenarios
- How Client Computers Locate Domain Controllers Within Sites
What Are AD DS Sites?

- Sites identify network locations with fast, reliable network connections
- Sites are associated with subnet objects
- Sites are used to manage:
  - Replication when domain controllers separated by slow, expensive links
  - Service localization:
    - Domain controller authentication (LDAP and Kerberos)
    - Active Directory-aware (site-aware) services or applications
Why Implement Additional Sites?

Create additional sites when:

• A part of the network is separated by a slow link
• A part of the network has enough users to warrant hosting domain controllers or other services in that location
• You want to control service localization
• You want to control replication between domain controllers
Demonstration: Configuring AD DS Sites

In this demonstration, you will see how to configure AD DS sites
How Replication Works Between Sites

Replication within sites:
• Assumes fast, inexpensive, and highly reliable network links
• Does not compress traffic
• Uses a change notification mechanism

Replication between sites:
• Assumes higher cost, limited bandwidth, and unreliable network links
• Has the ability to compress replication
• Occurs on a configured schedule
• Can be configured for immediate and urgent replications
What Is the Intersite Topology Generator?

ISTG defines the replication between AD DS sites on a network.
• Domain controllers register SRV records as follows:
  • _tcp.adatum.com: All domain controllers in the domain
  • _tcp.sitename._sites.adatum.com: All services in a specific site
• Clients query DNS to locate services in specific sites
The process for locating a domain controller occurs as follows:
1. New client queries for all domain controllers in the domain
2. Client attempts LDAP ping to find all domain controllers
3. First domain controller responds
4. Client queries for all domain controllers in the site
5. Client attempts LDAP ping to find all domain controllers in the site
6. Client stores domain controller and site name for further use
7. Domain controller is used for the full logon process, including authentication, building the token, and building the list of GPOs to apply
   • Domain controller offline? Client queries for domain controllers in registry stored site
   • Client moved to another site? Domain controller refers client to another site
Lesson 3: Configuring and Monitoring AD DS Replication

- What Are AD DS Site Links?
- What Is Site-Link Bridging?
- What Is Universal Group Membership Caching?
- Managing Intersite Replication
- Demonstration: Configuring AD DS Intersite Replication
- Best Practices When Deploying RODCs to Support Remote Sites
- Demonstration: Configuring Password Replication Policies
- Tools for Monitoring and Managing Replication
What Are AD DS Site Links?

- Site-links contain sites:
  - Within a Site-link, a connection object can be created between any two domain controllers
  - The default Site-link, DEFAULTIPSITELINK, is not always appropriate given your network topology
What Is Site-Link Bridging?

• By default, automatic site-link bridging:
  - Enables ISTG to create connection objects between site-links
  - Allows disabling of transitivity in the properties of the IP transport

• Site-link bridges:
  - Enable you to create transitive site-links manually
  - Are useful only when transitivity is disabled
What Is Universal Group Membership Caching?

Universal group membership caching enables domain controllers in a site with no global catalog servers to cache universal group membership.
Managing Intersite Replication

• Site-link costs:
  • Replication uses the connections with the lowest cost

• Replication:
  • Polling: Downstream bridgehead polls upstream partners
    • Default is 3 hours
    • Minimum is 15 minutes
    • Recommended is 15 minutes

• Replication schedules:
  • 24 hours a day
  • Can be scheduled
In this demonstration, you will see how to configure AD DS intersite replication
Password replication policies are:

- Used to determine which users’ credentials should be cached on the RODC
- Determined by the Allowed List and the Denied List
Demonstration: Configuring Password Replication Policies

In this demonstration, you will see how to configure password replication policies
Tools for Monitoring and Managing Replication

- **Repadmin.exe examples:**
  - repadmin /showrepl Lon-dc1.adatum.com
  - repadmin /showconn Lon-dc1 adatum.com
  - repadmin /showobjmeta Lon-dc1 "cn=Linda Miller,ou=..."
  - repadmin /kcc

- **Dcdiag.exe /test:**
  - FrsEvent or DFSREvent
  - Intersite
  - KccEvent
  - Replications
  - Topology

- Monitor replication with Operations Manager
- Windows PowerShell
Lab: Implementing AD DS Sites and Replication

- Exercise 1: Modifying the Default Site
- Exercise 2: Creating Additional Sites and Subnets
- Exercise 3: Configuring AD DS Replication
- Exercise 4: Monitoring and Troubleshooting AD DS Replication

Logon Information

Virtual machines: 20412D-LON-DC1 20412D-TOR-DC1

User Name: Adatum\Administrator
Password: Pa$$w0rd

Estimated Time: 45 minutes
A. Datum Corporation has deployed a single AD DS domain, with all the domain controllers located in the London data center. As the company has grown and added branch offices with large numbers of users, it has become apparent that the current AD DS environment does not meet the company requirements. Users in some branch offices report that it can take a long time for them to sign in on their computers. Access to network resources such as the company’s Microsoft Exchange® 2013 servers and the Microsoft SharePoint® servers can be slow, and they fail sporadically. As one of the senior network administrators, you are responsible for planning and implementing an AD DS infrastructure that will help address the business requirements for the organization. You are responsible for configuring AD DS sites and replication to optimize the user experience and network utilization within the organization.
Lab Review

• You decide to add a new domain controller to the LondonHQ site named LON-DC2. How can you ensure that LON-DC2 is used to pass all replication traffic to the Toronto site?
• You have added the new domain controller named LON-DC2 to the LondonHQ site. Which AD DS partitions will be modified as a result?
• In the lab, you created a separate site-link for the Toronto and TestSite sites. What might you also have to do to ensure that LondonHQ does not create a connection object directly with the TestSite site automatically?
Module Review and Takeaways

• Review Questions
• Tools
• Best Practice
• Common Issues and Troubleshooting Tips