Lesson 17: Managing Active Directory and SYSVOL Replication

MOAC 70-412: Configuring Advanced Windows Server 2012 Services

Microsoft
Official Academic Course

WILEY

Overview

- Objective 5.4 – Manage Active Directory and SYSVOL replication.
  - Configure replication to Read-Only Domain Controllers (RODCs)
  - Configure Password Replication Policy (PRP) for RODCs
  - Monitor and manage replication
  - Upgrade SYSVOL replication to Distributed File System Replication (DFSR)
  - Understand the requirements and process performed during the migration

Managing Active Directory Replication

Lesson 17: Managing Active Directory and SYSVOL Replication

Active Directory Replication

- Active Directory replication is a critical piece of every Active Directory Domain Services (AD DS) environment.
- By replicating all naming contexts or directory partitions of AD DS, all domain controllers throughout the enterprise keep one another up to date with all changes, ranging from schema updates to modifying items as simple as group membership.
- Having accurate and up-to-date directory partitions allows enterprise operations to run smoothly.

Active Directory Replication

- AD DS replication occurs between two or more domain controllers, a source domain controller, and a replica domain controller.
- The replication process:
  - Replicates new changes/updates
  - Replicates updates of directory objects
  - Ensures all directory updates are transferred to a replica partner
  - Keeps all directory partitions up to date
  - Keeps all domain controllers synchronized
  - Replicates contents of the SYSVOL folder

Intrasite Replication

- Intrasite replication occurs using ***change notification*** between domain controllers located within that site.
- Change notification is a notification in which source domain controllers within a site let their replica domain controllers know there are new changes that can be replicated.
- Intrasite replication is considered Notify-Pull replication, which means that the source domain controller notifies a replica, and then the replica requests the changes.

Intrasite Replication

- Intrasite replication
  - Allows changes to occur as soon as possible because it takes advantage of high-speed local area networks.
  - Utilizes Remote Call Procedure over Internet Protocol (RPC over IP) connectivity, Kerberos authentication, and data encryption allowing efficient and secured data transfer between domain controllers.
  - Does not compress all replication data within a site; unlike intersite replication, where replication data is compressed.
- Intrasite replication topology is generated by the Knowledge Consistency Checker (KCC).

Intrasite Replication

- To further enhance replication within a site, domain controllers use the store-and-forward mechanism to replicate changes to other domain controllers within the site.
- ***Store-and-forward replication*** allows the replica domain controller to store the updates it has received from the source domain controller and issue or forward a change notification to other replica domain controllers.
- This mechanism allows faster replication so the source domain controller does not have to contact every domain controller in the domain to replicate the latest update.

Intrasite Replication

- ***Urgent replication***
  - Allows critical directory information to be delivered to replica domain controllers without waiting the normal, non-urgent, fifteen-second and three-second subsequent intervals.
- ***Non-urgent replication***
  - Is all other replication that does not include account lockouts, account/password policies, and domain controller accounts.
  - Occurs through normal change notification replication operations.

Intrasite Replication

- ***Password change replication*** allows domain controllers to reference one domain controller when a password has been changed on one domain controller and the change has not yet replicated throughout the enterprise.
- ***Replication conflicts*** occur when objects are modified by users in an environment. The same object could be modified by two different users at the same time. In a replication conflict, the latest revision always wins.

Intersite Replication

- Intersite replication
  - Is considered request-pull replication, meaning the replica bridgehead server in one site requests the changes from the source bridgehead server.
  - Occurs between domain controllers residing in separate physical locations within the AD DS topology.
  - Is a cost-based replication, allowing replication to occur across the least expensive link.
- By using scheduling, configured replication intervals, and costs, site links are optimized to provide the fastest and cheapest replication possible between two sites.
- Site topology is created by the KCC and the Intersite Topology Generator, and replication occurs between each site's assigned bridgehead servers.

Intersite Replication

- Intersite replication traffic can occur over RPC over IP or Simple Mail Transfer Protocol (SMTP).
- Change notification is not enabled by default to notify domain controllers in other sites about changes (like it is with intrasite replication). However, it can be enabled.
- Replication between sites depends on replication intervals, costs, and schedules.

Controlling Active Directory Replication

- As an administrator of an enterprise, there will be instances where replication needs to happen at your discretion.
- Through the use of REPADMIN, Windows PowerShell and the Active Directory Sites and Services tool, you can control when replication happens, and whether you need it to happen within a site or across the enterprise.

Read-Only Domain Controllers

- Read-only domain controllers (RODCs)
  - Are used in environments where there is a need for a domain controller in a branch office that does not have a secured physical environment.
  - Are also used when there is a risk of theft, or even rarely, when there is an application requiring installation on a domain controller that users must log in to at the terminal or with terminal services.

Read-Only Domain Controllers

- As the name "read-only domain controller" implies, its involvement with AD DS is truly read-only.
- ***Unidirectional replication*** means replication occurs in only one direction, from a writeable domain controller to the read-only domain controller.
- Implementing ***Filter Attribute Sets*** allows administrators to mark attributes as "Confidential" when being replicated to RODCs.
- Attributes marked as confidential and that are part of the Filtered Attribute Set will not be replicated to an RODC.

Password Replication Policy

- To provide authentication of users and computers at a branch office that utilizes an RODC, the RODC must know and store the password of that user or computer.
- To prevent unwanted users from logging in to or authenticating against an RODC, only users that are members of the Allowed RODC Password Replication Group will be allowed to authenticate to the RODC.
- As an additional option, to prevent users from authenticating against the RODC, add the users or user group to the Denied RODC Password Replication Group.

Password Replication Policy

- By modifying the ***Password Replication Policy (PRP)*** of the RODC within the Active Directory Users and Computers tool, you can *allow* or *deny* passwords to be cached for users.
- When adding users to the Allowed RODC Password Replication Group, do not forget that computers have passwords as well.
- ***Password Prepopulation*** allows user credentials to be pushed to the RODC before those users attempt log on to the RODC.

Password Replication Policy

- Benefits of Password Prepopulation include:
  - Initial logons are faster, since the authentication process won't have to traverse the WAN to the closest, writable, Windows 2008 or later, domain controller.
  - An RODC can be prepared before shipment to the remote site if no WAN link is available when the RODC is brought online.
- Password Prepopulation can only cache passwords when user and computer accounts are configured to have passwords replicated or have been added to the Allowed RODC Password Replication Group.

Monitoring Replication with REPADMIN

- By using REPADMIN.EXE, Windows PowerShell, and/or the Active Directory Replication Status tool (ADREPLSTATUS), you can monitor your environment for failures and take action to put a resolution in place.
- Released by Microsoft in 2012, the Active Directory Replication Status Tool (ADREPLSTATUS) allows for much simpler and straightforward monitoring and troubleshooting, taking the results returned and placing them into an easy-to-use application.

Upgrading SYSVOL Replication

- Many environments started off as an Active Directory environment running Windows Server 2003 or earlier, prior to the addition of Windows Server 2008 and Windows Server 2012.
- The replication process of recently upgraded domain's SYSVOL folders could still be configured to use the File Replication Service (FRS).
- The SYSVOL folder on each domain controller contains a copy of logon scripts and Group Policies, and it is a repository for public access files used by domain controllers.

Upgrading SYSVOL Replication

- To upgrade from File Replication Service (FRS) to Distributed File System Replication (DFSR), the domain functional level must be Windows Server 2008 or higher.
- This means all domain controllers in the domain must be at least Windows Server 2008 or higher.

Upgrading SYSVOL Replication

- Each of the four Global States of an FRS to DFSR upgrade allows all domain controllers to balance and prepare for the next state:
  - **Start (State 0):** Live AD DS SYSVOL replication between domain controllers is performed using FRS.
  - **Prepared (State 1):** Live AD DS SYSVOL replication between domain controllers is performed using FRS.
  - **Redirected (State 2):** Live AD DS SYSVOL replication between domain controllers is performed using DFSR.
  - **Eliminated (State 3):** All Live AD DS SYSVOL replication between domain controllers is performed using DFSR. FRS SYSVOL replication is removed, including the SYSVOL folder and its contents.

Upgrading SYSVOL Replication

- These commands are used to migrate domain controllers to the different states:
  - **`dfsrmig /SetGlobalState 1`**
  - **`dfsrmig /SetGlobalState 2`**
  - **`dfsrmig /SetGlobalState 3`**

Lesson Summary

- Intrasite replication uses change notification when replicating to replica domain controllers within the same site.
- Filtered Attribute Sets can be configured to prevent attributes, considered confidential, from being replicated to Read-Only Domain Controllers (RODCs).
- User and computer passwords can be allowed or prevented from being cached on RODCs.

Lesson Summary

- The REPADMIN.EXE command can be used to troubleshoot and monitor Active Directory replication.
- The Windows PowerShell cmdlet `Get-ADReplication*` can be used to troubleshoot and monitor Active Directory replication.
- The Active Directory Replication Status Tool (ADREPLSTATUS) can be used to troubleshoot and monitor Active Directory replication.
- The SYSVOL folder replication process can be migrated from the File Replication Service (FRS) to Distributed File Service Replication (DFSR).