**70-412 Chapter:2 Active Directory sites and replication**

Q-1. What are sites?

Ans. Sites enable you to map physical locations, such as branch offices, into Active Directory.  
Sites make it possible for Active Directory clients to locate the closest instance of a particular resource, for example ensuring that a user signing on to a computer in the Sydney office isn’t authenticated by a domain controller in the New York office.

Or, Sites enable you to connect one or more subnets to represent a location where all the  
hosts on those subnets share a high-speed network.

Q-2. What are subnets?

Ans. Subnets enable you to associate IP addresses in either IPv4 or IPv6 format with network locations.

Q-3. What is the name of the first Active Directory site created when you promote the first domain controller in a new forest?  
**Ans.** The name of the first Active Directory site created when you promote the first domain controller in a new forest is Default-First-Site-Name.

**Creating site links**

Site link works:

Site links enable you to connect sites. Site links enable to specify how different Active Directory sites are connected to each other. Sites that are connected to the same site link are considered to be able to replicate with each other directly.

From where:

We can create a new IP site link using the Active Directory Sites and Services console.

Default properties of Site link:  
We can configure site link properties. The default Cost is 100, and site links that have lower costs are preferred for replication over site links that have a higher cost. Replication occurs every 180 minutes by default, 24 hours a day.

PowerShell command: 67p

We can create a site link in windows PowerShell using the New-ADReplicationSiteLink cmdlet.

New-ADReplicationSiteLink “ADL-CBR” –SitesIncluded ADL-SITE, CBR-SITE.

**Site link bridge**

Site Link Bridge works:

Site link bridges enable you to connect site links. You should only do this if you want to  
override the replication topology automatically generated by Active Directory.

OR,

Site link bridges create transitive links between site links. Site link bridges are only necessary  
to do this with complex network topologies as site link bridges are automatically created based on the topology created when you configure site links.

From where:

You can create a site link bridge using the Active Directory Sites and Services console by specifying the two sites links that will be in the bridge.

A site link bridge must contain at least two site links.

PowerShell command: 68p

You can create a new site link bridge in using the Windows PowerShell   
New-ADReplicationSiteLinkBridge cmdlet.  
New-ADReplicationSiteLinkBridge “MEL-ADL-CBR” –SiteLinksIncluded “MEL-ADL”,”MEL-CBR”

**Q. What is SRV record?**

**Ans.** Domain controllers use special Domain Name System (DNS) resource records, known as SRV  
records. SRV records make it possible for clients to use DNS to locate servers that provide services, such as LDAP and Kerberos, to the network.

**Moving Domain Controllers**

1. The domain controller does not automatically reassign itself to a new site if you create the subnet and site objects in the Active Directory Sites and Services console if it has already been added to the Default-First-Site-Name site

2. The domain controller is instead assigned to the first Active Directory site, which is Default-First-Site-Name unless you have changed it.

3. You can move the domain controller using the Active Directory Sites and Services console

4. We can move a domain controller to a different site using the **Move-ADDirectoryServer** powershell cmdlet.

5. You might need to move domain controllers to different sites if you installed them  
before you configured sites and subnets

**What is Active Directory Replication?**

Ans: Replication makes it possible for changes that are made on one Active Directory domain controller to be replicated to other domain controllers in the domain and in some cases to other domain controllers in the forest.

Active directory partitions

**Q. Write the names of active directory default partition?**

Ans: . Active Directory includes the following default partitions:

1. Configuration partition
2. Schema partition
3. Domain partition
4. Application partitions

MCQ

1. The process of promoting the first domain controller in the forest creates the configuration partition.
2. The configuration partition replicates to all domain controllers in the forest.
3. The schema partition stores definitions of all objects and attributes as well as the rules for creating and manipulating those objects.
4. **The domain partition holds information about domain-specific objects such as organizational units, domain-related settings, user, group, and computer accounts.**
5. A new domain partition is created each time you add a new domain to the forest.
6. All objects in every domain partition are stored in the global catalog.
7. Application partitions store application-specific information for applications that store information in Active Directory.

Multi-master replication

Q. What do you mean multi-master replication?

Ans. Active Directory uses multi-master replication. This means that any writable domain controller is able to make modifications of the Active Directory database and to have those modifications propagate to the other domain controllers in the domain. Domain controllers use pull replication to acquire changes from other domain controllers.

Q. A domain controller notifies its first replication partner that a change has occurred

1. within 15 seconds

Q. Additional replication partners have occurred after the previous notification.

1. every 3 seconds

Q. Domain controllers also periodically poll replication partners to determine whether changes are available so that those changes can be pulled and applied to the local copy of the relevant partition. By default, polling occurred once-

1. Every 60 minutes.

Knowledge Consistency Checker (KCC)

Q. What is Knowledge consistency checker (KCC)?

Ans: The Knowledge Consistency Checker (KCC)runs on each domain controller. The KCC is responsible for creating and optimizing the replication paths between domain controllers located at a specific site.

Or, The Knowledge Consistency Checker (KCC) is responsible for establishing the replication topology and ensuring that all domain controllers are kept up-to-date.

MCQ

Q. How long time the KCC topology organization process occurs by default?

1. **Every 15 minutes**

Q. Which of the following services of Active Directory is responsible for maintaining the replication topology?

1. File Replication Service
2. **Knowledge Consistency Checker**
3. Windows Internet Name Service
4. Domain Name System

RODC replication

Q. What is RODC?

Ans. RODCsare a special type of domain controller that are suitable for branch office locations  
that require a local domain controller for authentication but don’t have a secure location where the server can be stored. The key difference between a RODC and a writable domain controller is that RODCs aren’t able to update the Active Directory database.

Q. What is the function of RODC?

Ans. RODCs perform inbound replication using a replicate-single-object (RSO) operation. These cases include:

■ The password of a user whose account password is stored on the RODC is changed.  
■ A DNS record update occurs where the DNS client performing the update attempts to use the RODC to process the update and is then redirected by the RODC to a writable DC that hosts the appropriate Active Directory Integrated DNS zone.  
  
■ Client attributes including client name, DnsHostName, OsName, OsVersionInfo, supported encryption types, and LasLogonTimeStamp are updated.

Properties of RODC:

The Password Replication Policy is unique to each RODC and determines which account passwords are stored on the RODC.  
When you remove an RODC from the domain, you can configure an automatic password reset for all account passwords stored on the RODC

Configure RODC password replication

1. What is the purpose of RODC?

Ans: It is compressed the pressure of writable domain controller specially the field of password and replicate the other delegated action allowed by writable domain controller.

1. Which groups have a Deny setting in Password Replication Policy by default?
2. Account operators
3. Administrators
4. Backup operators
5. Denied RODC password replication group
6. Server operators
7. What is the purpose of RODC Password replication?

Ans: The Password Replication Policy is unique to each RODC, and it enables you to ensure that the passwords that are replicated to each RODC are unique to that RODC.

1. You delete the computer account of an RODC and choose to reset the passwords of computer accounts. What step do you need to take next to restore the computers to normal functionality?  
   Ans. You need to rejoin the computers to the domain to restore normal functionality.
2. Members of the Allowed RODC Password Replication security group are able to have  
   their passwords replicated to the RODC as long as they aren’t members of a group that has a  
   Deny setting in the Password Replication Policy.
3. The Password Replication Policy tab of an RODC’s computer account properties dialog box displays the configuration of allowed and denied security groups for password replication to that RODC.
4. You can check which passwords have replicated to a specific RODC by clicking the Advanced button on the Password Replication Policy tab of the RODC’s computer account’s Properties
5. Monitor and manage replication:

You can use the Active Directory Sites and Services console to trigger replication. You can  
trigger replication on a specific domain controller by right-clicking the connection object and clicking Replicate.

Repadmin: You can use the repadmin command-line tool to manage and monitor replication. This tool is especially useful at enabling you to diagnose where there are problems in a replication topology. You can view specific inbound replication traffic by using repadmin with the /showrepl switch.

SYSVOL replication:

Q. What is SYSVOL?

SYSVOLis a special folder located on each domain controller in the %SystemRoot%\SYSVOL  
folder. This folder hosts logon scripts, group policy templates, and other Active Directory  
items. SYSVOL is replicated to all domain controllers in a domain.

Or, SYSVOL is simply a folder which resides on each and every [domain controller](http://social.technet.microsoft.com/wiki/contents/articles/16757.active-directory-glossary.aspx#Domain_Controller) within the [domain](http://social.technet.microsoft.com/wiki/contents/articles/16757.active-directory-glossary.aspx#Domain). It contains the domains public files that need to be accessed by clients and kept synchronized between domain controllers.

* Prior to the introduction of Windows Server 2008, SYSVOL used File Replication Service (FRS) to perform replication.
* With the introduction of Windows Server 2008, Distributed File System (DFS), a much more efficient replication technology became available to replicate the contents of SYSVOL.
* If your organization has upgraded from a Windows Server 2003 Active Directory environment, SYSVOL may still be configured to use FRS rather than DFS.
* After you have upgraded all domain controllers so that the minimum domain functional level is Windows Server 2008, you can use the Dfsrmig.exe utility to migrate SYSVOL replication so that it uses DFS rather than FRS.
* If your domain was deployed from the beginning using Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 domain controllers, SYSVOL is already configured to use DFS rather than FRS replication.
* You can verify that SYSVOL is using DFS using the dfsrmig.exe command with the /getglobalstate switch.
* The default location for the SYSVOL is C:\Windows\SYSVOL although it can be moved to another location during the promotion of a domain controller. It’s possible but not recommended to relocate the SYSVOL after [DC](http://social.technet.microsoft.com/wiki/contents/articles/16757.active-directory-glossary.aspx#DC) promotion as there is potential for error.
* The SYSVOL folder can be accessed through its share \\domainname.com\sysvol or the local share name on the server [\\servername\sysvol](file:///\\servername\sysvol).

Abdur Razzak

ID: 1204149