CST223   M09 Assignment – 8.3 Console
Wei Cui   11/09/2017

Lab Objective

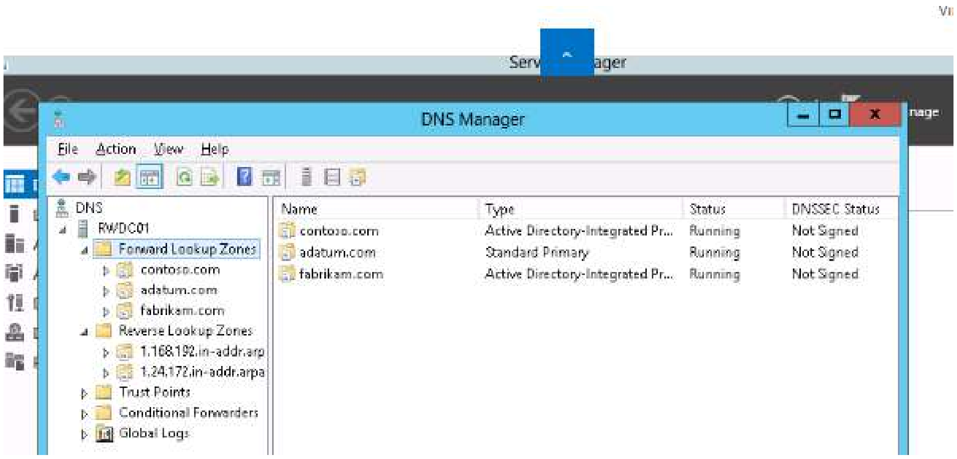
Creating an Active Directory Integrated Zone

Lab Procedures

1. On RWDC01, go to the DNS Manager console.
2. Right-click the Forward Lookup Zones and click New Zone.
3. When the New Zone Wizard starts, click Next.
4. With Primary zone and Store the zone in Active Directory options are already selected, click Next.
5. On the Active Directory Zone Replication Scope dialog box, click Next.
6. On the Zone Name page, type **fabrikam.com** and click Next.
7. On the Dynamic Update page, with the *Allow only secure dynamic updates* selected, click Next.

Question 2	*What is needed to perform secure dynamic updates?* *Active Directory*

8. Click Finish. The fabrikam.com domain is created.



Name	Type	Status	DNSSEC Status
contoso.com	Active Directory-Integrated Pr...	Running	Not Signed
adatum.com	Standard Primary	Running	Not Signed
fabrikam.com	Active Directory-Integrated Pr...	Running	Not Signed

Figure 1 Active Directory integrated zone, fabrikam, was created.

Lab Summary

CST223 M09 Assignment – 8.3 Console
Wei Cui 11/09/2017

During this exercise, I created an Active Directory Integrated zone. According to Microsoft[1], the advantage of Active Directory-integrated zones are the following

- DNS features multimaster data replication and enhanced security based on the capabilities of AD DS.

  In a standard zone storage model, DNS updates are conducted based on a single-master update model. In this model, a single authoritative DNS server for a zone is designated as the primary source for the zone. This server maintains the master copy of the zone in a local file. With this model, the primary server for the zone represents a single fixed point of failure. If this server is not available, update requests from DNS clients are not processed for the zone.

  With directory-integrated storage, dynamic updates to DNS are sent to any AD DS-integrated DNS server and are replicated to all other AD DS-integrated DNS servers by means of AD DS replication. In this model, any AD DS-integrated DNS servercan accept dynamic updates for the zone. Because the master copy of the zone is maintained in the AD DS database, which is fully replicated to all domain controllers, the zone can be updated by the DNS servers operating at any domain controller for the domain. With the multimaster update model of AD DS, any of the primary servers for the directory-integrated zone can process requests from DNS clients to update the zone as long as a domain controller is available and reachable on the network.

  Also, when you use directory-integrated zones, you can use access control list (ACL) editing to secure a dnsZone object container in the directory tree. This feature provides detailed access to either the zone or a specified resource record in the zone. For example, an ACL for a zone resource record can be restricted so that dynamic updates are allowed only for a specified client computer or a secure group, such as a domain administrators group. This security feature is not available with standard primary zones.

- Zones are replicated and synchronized to new domain controllers automatically whenever a new one is added to an AD DS domain.

  Although the DNS Server service can be selectively removed from a domain controller, directory-integrated zones are already stored at each domain controller. Therefore, zone storage and management is not an additional resource. Also, the methods that are used to synchronize directory-stored information offer performance improvement over standard zone update methods, which can potentially require transfer of the entire zone.

- By integrating storage of your DNS zone databases in AD DS, you can streamline database replication planning for your network.

  When your DNS namespace and AD DS domains are stored and replicated separately, you must plan and potentially administer each of these items separately. For example, when you use standard DNS zone storage and AD DS together, you have to design, implement, test, and maintain two different database replication topologies.

For example, one replication topology is needed for replicating directory data between domain controllers, and another topology is needed for replicating zone databases between DNS servers. This can create additional administrative complexity for planning and designing your network and allowing for its eventual growth. By integrating DNS storage, you unify storage management and replication issues for both DNS and AD DS, merging and viewing them together as a single administrative entity.

- Directory-integrated replication is faster and more efficient than standard DNS replication.

  Because AD DS replication processing is performed on a per-property basis, only relevant changes are propagated. Less data is used and submitted in updates for directory-stored zones.

Reference: [1] Understanding Active Directory Domain Services Integration
https://technet.microsoft.com/en-us/library/cc726034(v=ws.11).aspx