Domain and Trust Management in AD DS

Eli Chang

MSSA Cohort #2

Lab Summary 3

3/2/2020

Domain and Trust Management in AD DS

The company has a single AD DS domain with all the domain controllers in the datacenter. There are branch offices with a large number of users so that the current AD DS environment does not meet the company requirements. The amount of network traffic increases as other external users from different partner companies try to access to the internal network. The security department wants to have security for external users. The new AD DS domain and forest deployment should provide optimal services for internal and external users.

DNS Considerations

In the single-forest AD DS environment in the company, there are some considerations to resolve the name resolution and user sign-ins. There are two models: centralized or decentralized. The centralized model is for forest-wide replication so that it makes other local domains in the forest. However, the decentralized model is to configure for domain-wide replication, which means that it is available in the domain. The administrators in the lab are trying to establish a centralized model because they are attempting to configure the domains into the forest. Also, there are three zones: primary, secondary, and stub. The first two zones are already used before, but this is the first-time using stub zone. With the stub zone, it can be created the shortcut to prevent the need for recursive queries to the domain forest root or tree.

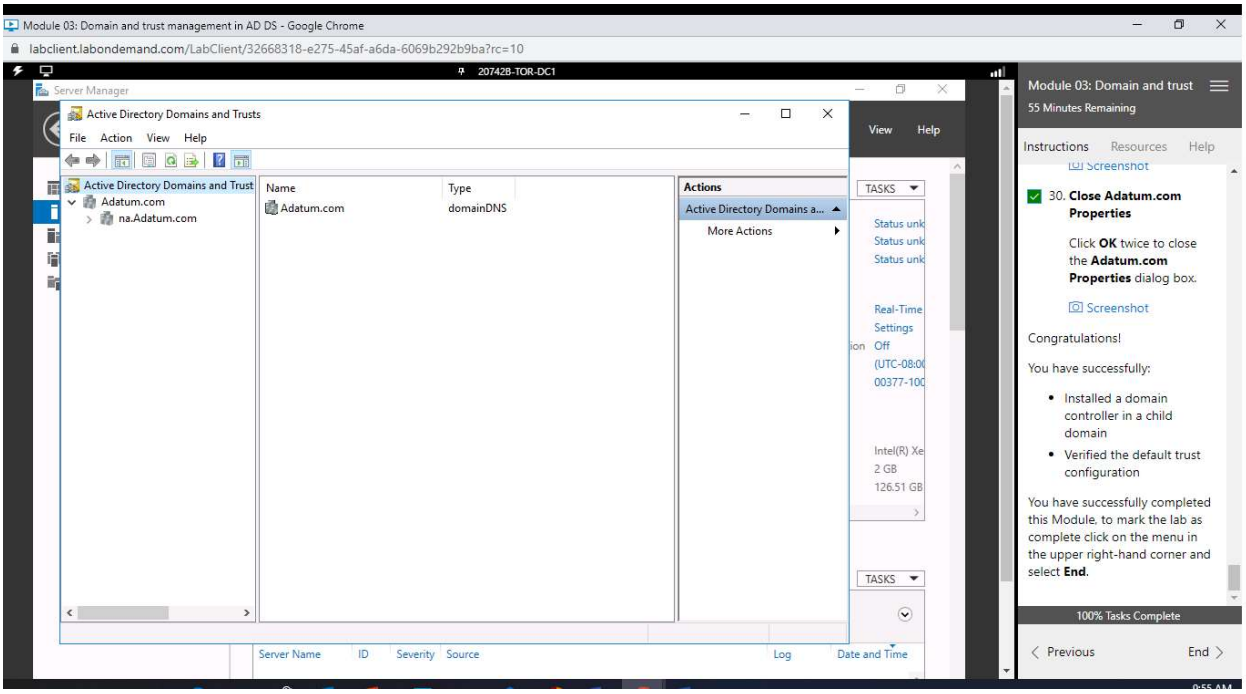
Configuring Selective Authentication

There are three different types of security considerations: SID filtering, selective authentication, and name suffix routing. In selective authentication mode selection, there are two ways to authenticate for the external or forest users in whether they choose domain-wide authentication or Selective authentication. For the first option, any resource with permission is accessible for the authenticated users immediately. The selective authentication allows all users

in the trusted domain are trusted identities, but also, they authenticate only for services on computers. The users are not going to become the authenticated users but grant the allows for authentication permission on the computers.

Configuring a child domain

Child domains have shared common namespace with the parent domain. There are three different domains: forest root, child, and tree domains. The forest root is the base of the AD DS infrastructure. The tree domain is commonly used in merger and acquisition scenarios. Mainly, the child domain aligns with the specific departments within the organization. This domain can also have the child domain to become the parent of it.


Module 03: Domain and trust management in AD DS - Google Chrome
labclient.labondemand.com/LabClient/32668318-e275-45af-a6da-6069b292b9ba?rc=10
20742B-TOR-DC1
Server Manager
Active Directory Domains and Trusts
File Action View Help
Active Directory Domains and Trust
Adatum.com
na.Adatum.com
Name
Type
Adatum.com
domainDNS
Actions
Active Directory Domains a...
More Actions
TASKS
Server Name
ID
Severity
Source
Log
Date and Time
Module 03: Domain and trust
55 Minutes Remaining
Instructions
Resources
Help
Screenshot
30. Close Adatum.com Properties
Click OK twice to close the Adatum.com Properties dialog box.
Screenshot
Congratulations!
You have successfully:
Installed a domain controller in a child domain
Verified the default trust configuration
You have successfully completed this Module, to mark the lab as complete click on the menu in the upper right-hand corner and select End.
100% Tasks Complete
Previous
End