4/2/2021

Hands On Exercise

Chapter 7

Configuring Advanced Active Directory

(Part1)

El Adel, Taoufik

IT 416 - SPRING 2021 - OLD DOMINION UNIVERSITY

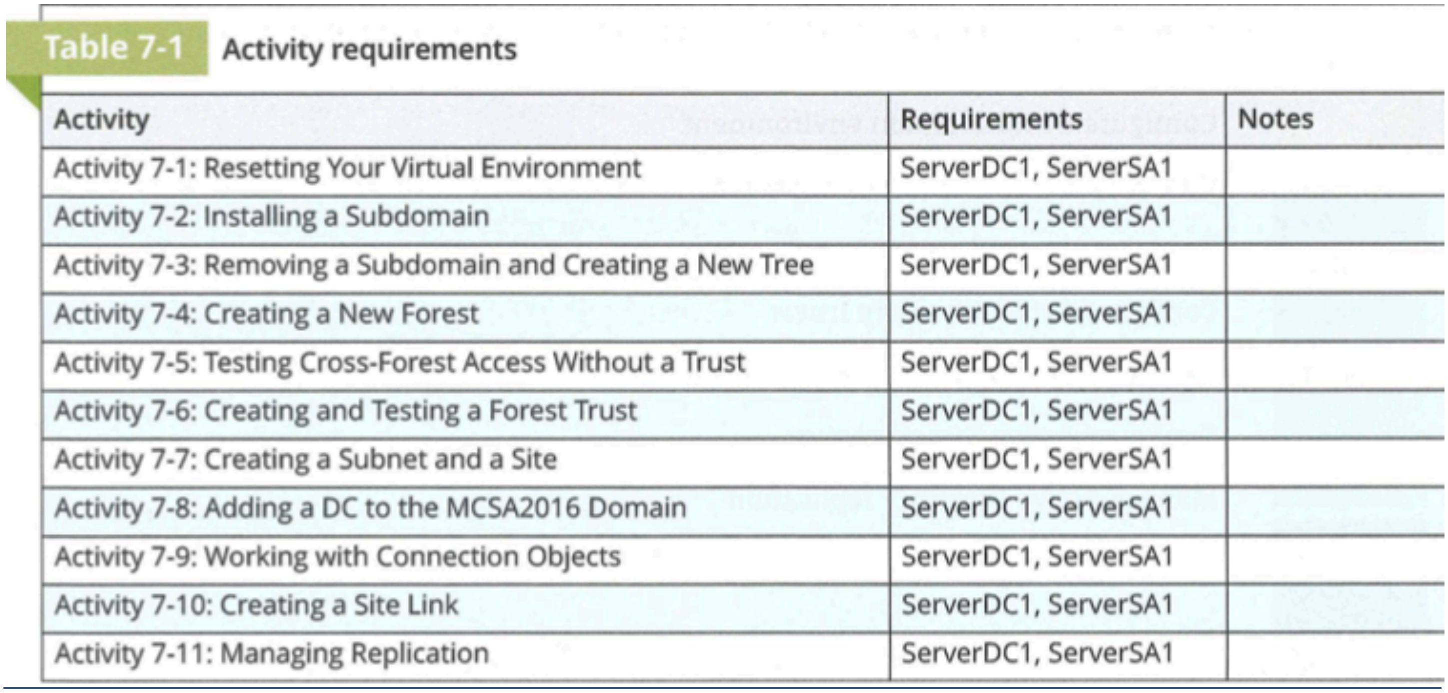
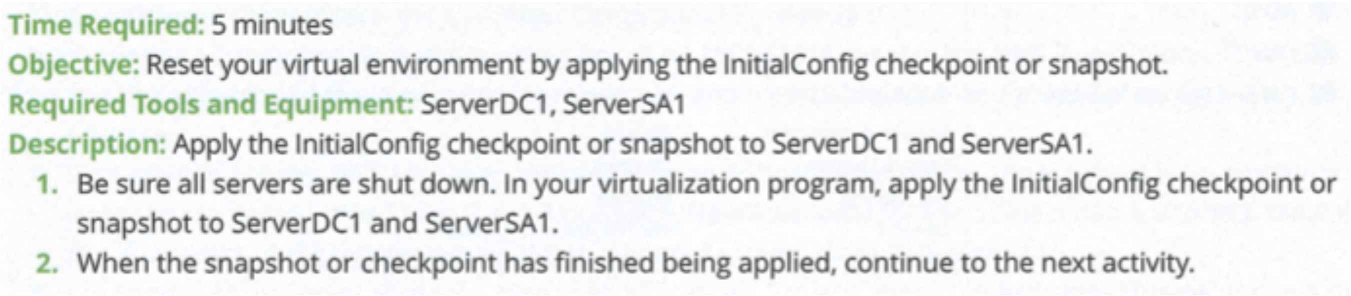


Table 7-1 Activity requirements

Activity	Requirements	Notes
Activity 7-1: Resetting Your Virtual Environment	ServerDC1, ServerSA1	
Activity 7-2: Installing a Subdomain	ServerDC1, ServerSA1	
Activity 7-3: Removing a Subdomain and Creating a New Tree	ServerDC1, ServerSA1	
Activity 7-4: Creating a New Forest	ServerDC1, ServerSA1	
Activity 7-5: Testing Cross-Forest Access Without a Trust	ServerDC1, ServerSA1	
Activity 7-6: Creating and Testing a Forest Trust	ServerDC1, ServerSA1	
Activity 7-7: Creating a Subnet and a Site	ServerDC1, ServerSA1	
Activity 7-8: Adding a DC to the MCSA2016 Domain	ServerDC1, ServerSA1	
Activity 7-9: Working with Connection Objects	ServerDC1, ServerSA1	
Activity 7-10: Creating a Site Link	ServerDC1, ServerSA1	
Activity 7-11: Managing Replication	ServerDC1, ServerSA1	

Activity 7-1: Resetting Your Virtual Environment



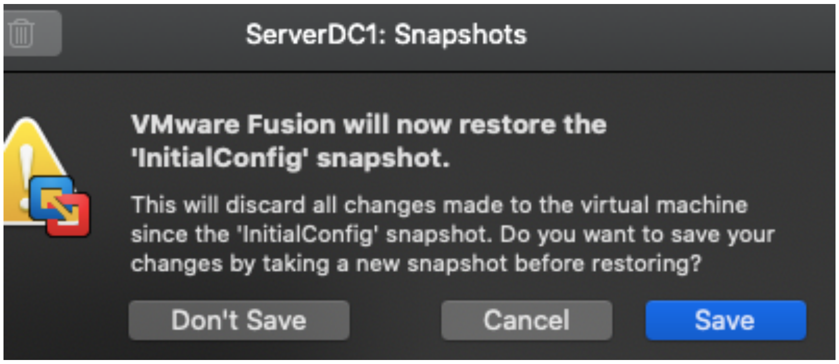
Time Required: 5 minutes

Objective: Reset your virtual environment by applying the InitialConfig checkpoint or snapshot.

Required Tools and Equipment: ServerDC1, ServerSA1

Description: Apply the InitialConfig checkpoint or snapshot to ServerDC1 and ServerSA1.

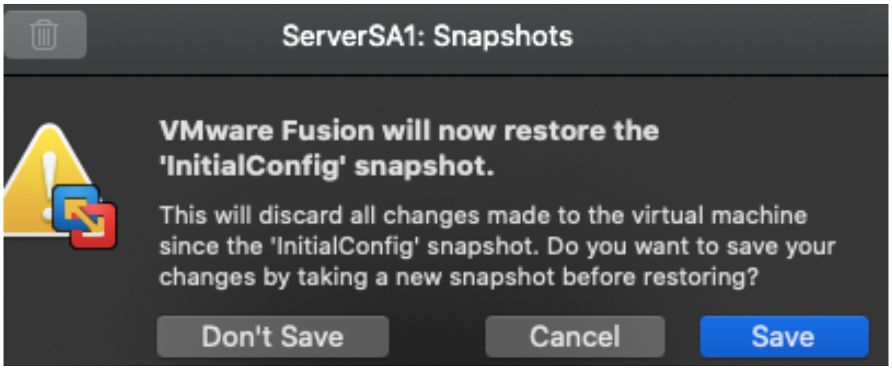
1. Be sure all servers are shut down. In your virtualization program, apply the InitialConfig checkpoint or snapshot to ServerDC1 and ServerSA1.
2. When the snapshot or checkpoint has finished being applied, continue to the next activity.



ServerDC1: Snapshots

VMware Fusion will now restore the 'InitialConfig' snapshot.

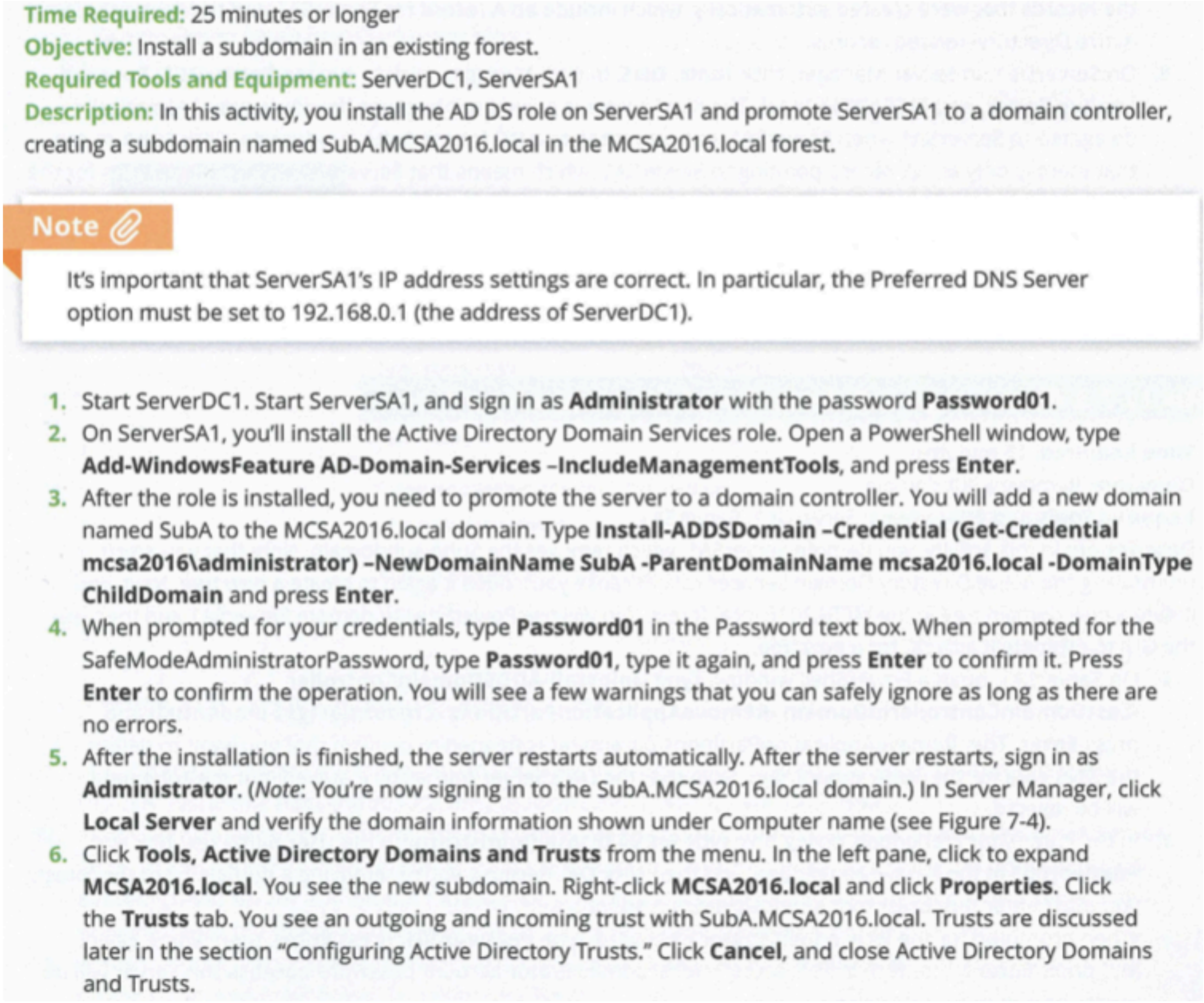
This will discard all changes made to the virtual machine since the 'InitialConfig' snapshot. Do you want to save your changes by taking a new snapshot before restoring?



VMware Fusion will now restore the 'InitialConfig' snapshot.

This will discard all changes made to the virtual machine since the 'InitialConfig' snapshot. Do you want to save your changes by taking a new snapshot before restoring?

Activity 7-2: Installing a Subdomain



Time Required: 25 minutes or longer

Objective: Install a subdomain in an existing forest.

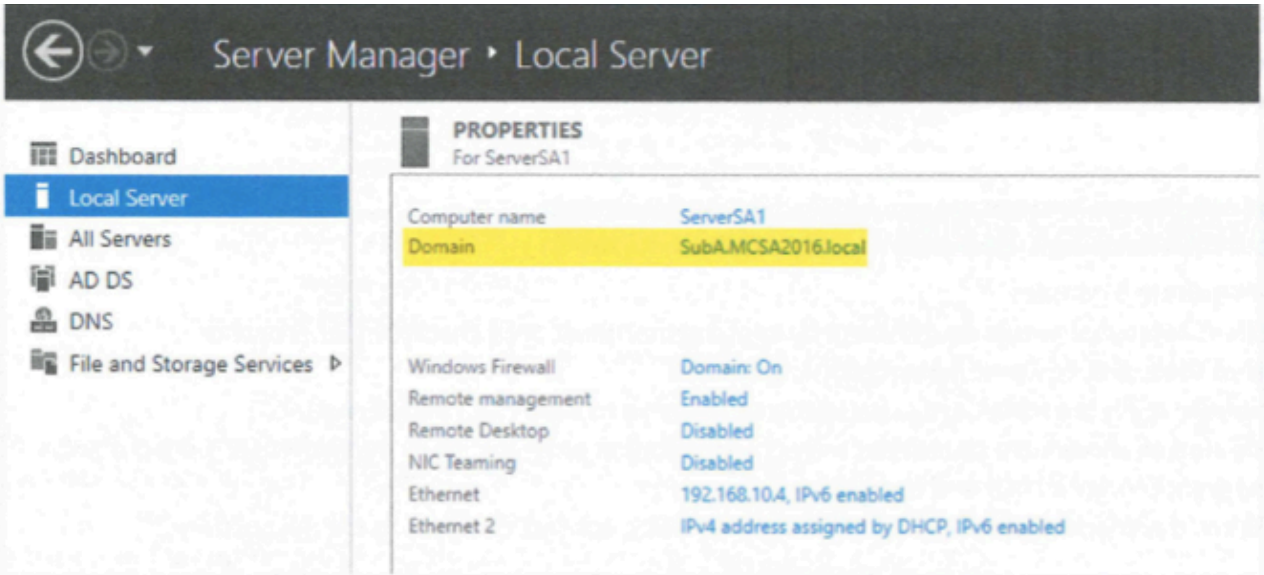
Required Tools and Equipment: ServerDC1, ServerSA1

Description: In this activity, you install the AD DS role on ServerSA1 and promote ServerSA1 to a domain controller, creating a subdomain named SubA.MCSA2016.local in the MCSA2016.local forest.

Note

It's important that ServerSA1's IP address settings are correct. In particular, the Preferred DNS Server option must be set to 192.168.0.1 (the address of ServerDC1).

1. Start ServerDC1. Start ServerSA1, and sign in as **Administrator** with the password **Password01**.
2. On ServerSA1, you'll install the Active Directory Domain Services role. Open a PowerShell window, type **Add-WindowsFeature AD-Domain-Services –IncludeManagementTools**, and press **Enter**.
3. After the role is installed, you need to promote the server to a domain controller. You will add a new domain named SubA to the MCSA2016.local domain. Type **Install-ADDSDomain –Credential (Get-Credential mcsa2016\administrator) –NewDomainName SubA -ParentDomainName mcsa2016.local -DomainType ChildDomain** and press **Enter**.
4. When prompted for your credentials, type **Password01** in the Password text box. When prompted for the SafeModeAdministratorPassword, type **Password01**, type it again, and press **Enter** to confirm it. Press **Enter** to confirm the operation. You will see a few warnings that you can safely ignore as long as there are no errors.
5. After the installation is finished, the server restarts automatically. After the server restarts, sign in as **Administrator**. (*Note*: You're now signing in to the SubA.MCSA2016.local domain.) In Server Manager, click **Local Server** and verify the domain information shown under Computer name (see Figure 7-4).
6. Click **Tools, Active Directory Domains and Trusts** from the menu. In the left pane, click to expand **MCSA2016.local**. You see the new subdomain. Right-click **MCSA2016.local** and click **Properties**. Click the **Trusts** tab. You see an outgoing and incoming trust with SubA.MCSA2016.local. Trusts are discussed later in the section "Configuring Active Directory Trusts." Click **Cancel**, and close Active Directory Domains and Trusts.

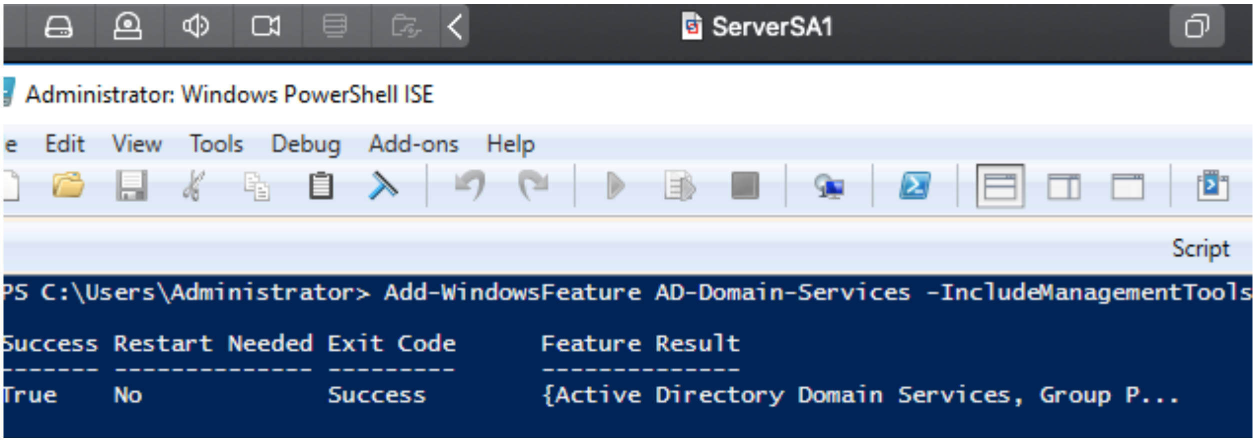


Computer name ServerSA1
Domain SubA.MCSA2016.local

Windows Firewall Domain: On
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled
Ethernet 192.168.10.4, IPv6 enabled
Ethernet 2 IPv4 address assigned by DHCP, IPv6 enabled

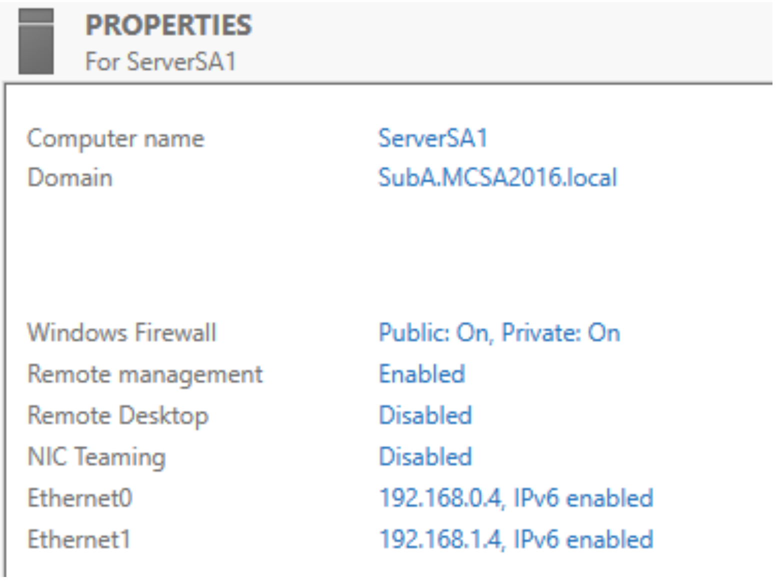
Figure 7-4 ServerSA1 is now in the SubA.MCSA2016.local domain

7. Click **Tools, DNS** to open DNS Manager (DNS was automatically installed when you installed Active Directory on ServerSA1). Click to expand **ServerSA1, Forward Lookup Zones**, and click **SubA.MCSA2016.local** to see the records that were created automatically, which include an A record for ServerSA1 and the folders holding Active Directory–related records.
8. On ServerDC1, in Server Manager, click **Tools, DNS**. In DNS Manager, click to expand **ServerDC1, Forward Lookup Zones**, and **MCSA2016.local**. The SubA folder is grayed out because the zone was automatically delegated to ServerSA1 when ServerSA1 was promoted to a DC for the SubA subdomain. Click **SubA** to see that there is only an NS record pointing to ServerSA1, which means that ServerSA1 will handle queries for the SubA subdomain. Close DNS Manager.
9. Continue to the next activity.


ServerSA1
Administrator: Windows PowerShell ISE
e Edit View Tools Debug Add-ons Help
Script

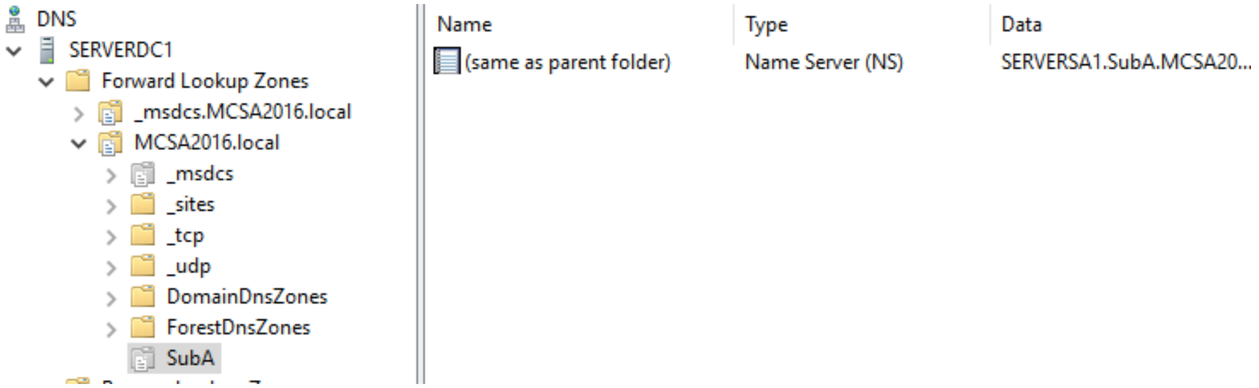
```
PS C:\Users\Administrator> Add-WindowsFeature AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services, Group P...
```



PROPERTIES
For ServerSA1

Computer name	ServerSA1
Domain	SubA.MCSA2016.local
Windows Firewall	Public: On, Private: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet0	192.168.0.4, IPv6 enabled
Ethernet1	192.168.1.4, IPv6 enabled



- DNS
  - SERVERDC1
    - Forward Lookup Zones
      - _msdcs.MCSA2016.local
      - MCSA2016.local
        - _msdcs
        - _sites
        - _tcp
        - _udp
        - DomainDnsZones
        - ForestDnsZones
        - SubA

Name	Type	Data
(same as parent folder)	Name Server (NS)	SERVERSA1.SubA.MCSA20...

Activity 7-3: Removing a Subdomain and Creating a New Tree

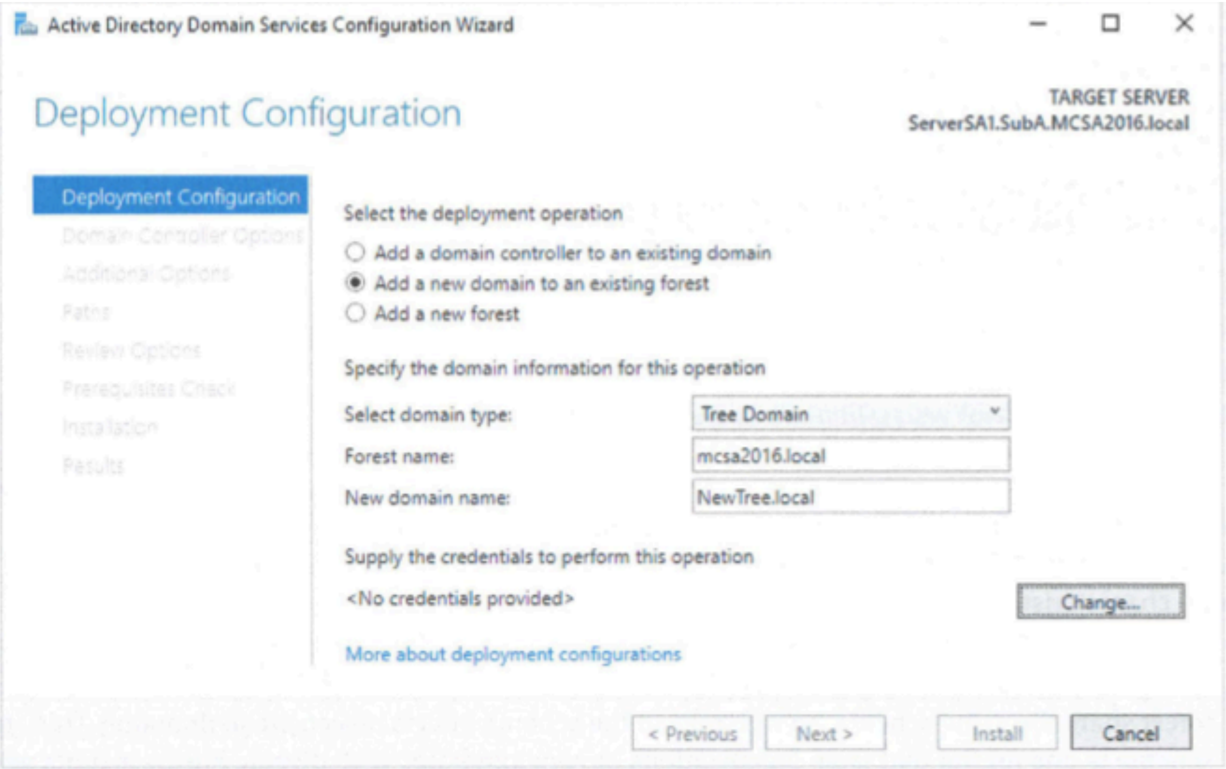
Time Required: 15 minutes

Objective: Remove a subdomain.

Required Tools and Equipment: ServerDC1, ServerSA1

Description: In this activity, you demote ServerSA1, which removes the SubA subdomain. Note that you aren't uninstalling the Active Directory Domain Services role because you'll need it again to create a new tree. Next, you create a new domain tree in the MCSA2016.local forest. You will use PowerShell to demote ServerSA1 and then use the GUI to promote it as a DC for a new tree.

1. On ServerSA1, open a PowerShell window. Type **Uninstall-ADDSDomainController -LastDomainControllerInDomain -RemoveApplicationPartitions -Credential (get-credential)** and press **Enter**. The -RemoveApplicationPartitions parameter is needed to confirm that you want to delete the DNS data for the SubA subdomain. Note that the DNS Server role is still installed, but the zone data will be deleted.
2. In the Enter your credentials dialog box, type **MCSA2016\administrator** in the User name text box and **Password01** in the Password text box, and then click **OK**. Because you're removing a domain from the forest, you must enter the forest root administrator's credentials.
3. When prompted for the local administrator password, type **Password01**, press **Enter**, then type it again, and press **Enter** to confirm it. This sets the local administrator account password because this server will no longer be a domain controller.
4. When you're prompted to continue the operation, press **Enter**. After the operation is complete, the server restarts. At this point, the Active Directory Domain Services role files aren't actually uninstalled, so if you want it to be a DC again, you just need to promote this server.
5. Sign in to ServerSA1 as **Administrator**. Before you can add a new tree to the forest, you need to configure DNS properly on both servers. First, you create a conditional forwarder on ServerSA1 to point to the MCSA2016.local domain.
6. Open DNS Manager. Click to expand **ServerSA1** and then click **Conditional Forwarders**. Right-click **Conditional Forwarders** and click **New Conditional Forwarder.**
7. In the New Conditional Forwarder dialog box, type **MCSA2016.local** in the DNS Domain box. Then click in the **IP addresses of the master servers** text box and type **192.168.0.1** and press **Enter**. Click **OK**. Close DNS Manager.
8. On ServerDC1, open DNS Manager and create a conditional forwarder for the NewTree.local domain you are about to create following Steps 6 and 7 but using **NewTree.local** for the domain name and **192.168.0.4** for the IP address of the master server. When you are finished, close DNS Manager.
9. On ServerSA1, in Server Manager, click the notifications flag and then click **Promote this server to a domain controller**. The Active Directory Domain Services Configuration Wizard starts.
10. In the Deployment Configuration window, click the **Add a new domain to an existing forest** option button. In the Select domain type list box, click **Tree Domain**. Type **MCSA2016.local** in the Forest name text box and **NewTree.local** in the New domain name text box (see Figure 7-5).



Deployment Configuration

Select the deployment operation

○ Add a domain controller to an existing domain
● Add a new domain to an existing forest
○ Add a new forest

Specify the domain information for this operation

Select domain type: Tree Domain

Forest name: mcsa2016.local

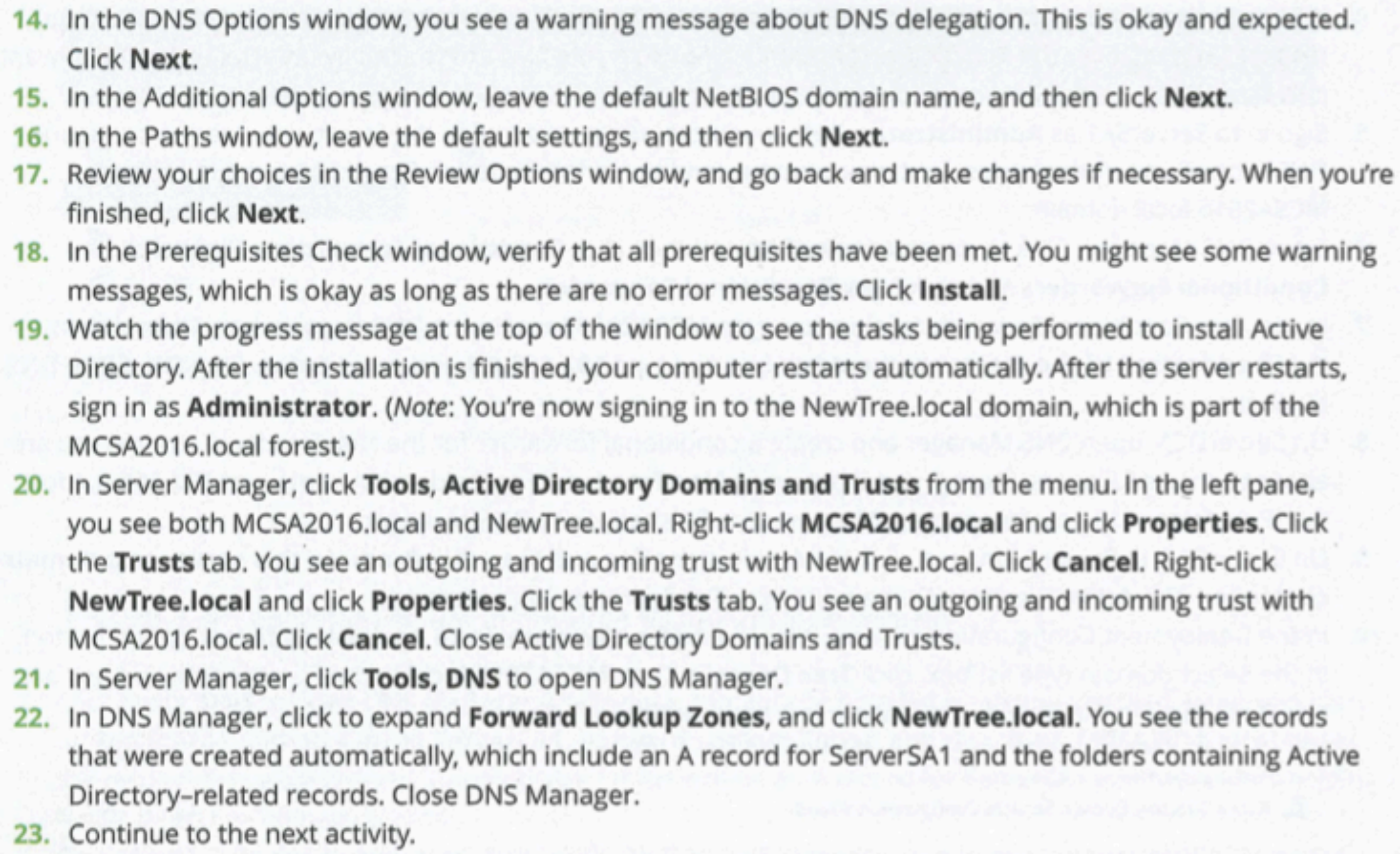
New domain name: NewTree.local

Supply the credentials to perform this operation

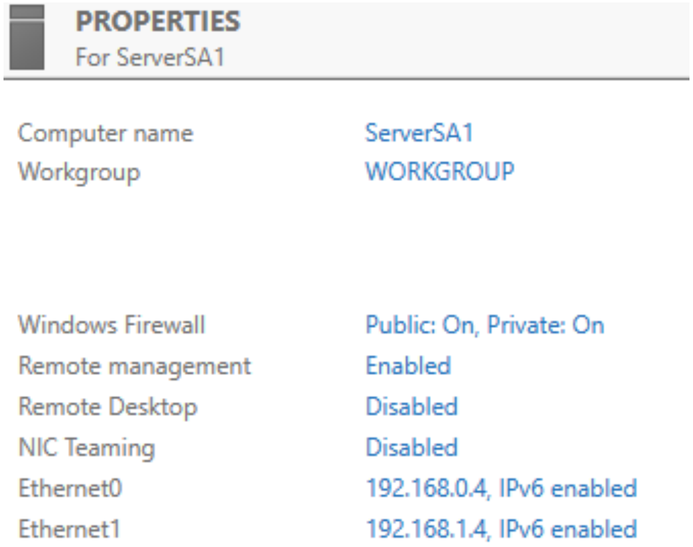
<No credentials provided>

Figure 7-5 Adding a tree to an existing forest

11. Click **Change** to enter credentials. In the Windows Security dialog box, type **MCSA2016\Administrator** for the user name and **Password01** for the password, and then click **OK**. Click **Next**.
12. In the Domain Controller Options window, verify that the domain functional level is set to **Windows Server 2016**. In the Specify domain controller capabilities and site information section, leave the **Domain Name System (DNS) server** and **Global Catalog (GC)** check boxes selected. You should have a DNS server in each domain tree in the forest. Configuring this DC as a global catalog server is optional.
13. In the Directory Services Restore Mode (DSRM) password section, type **Password01** in the Password and Confirm password text boxes, and then click **Next**.

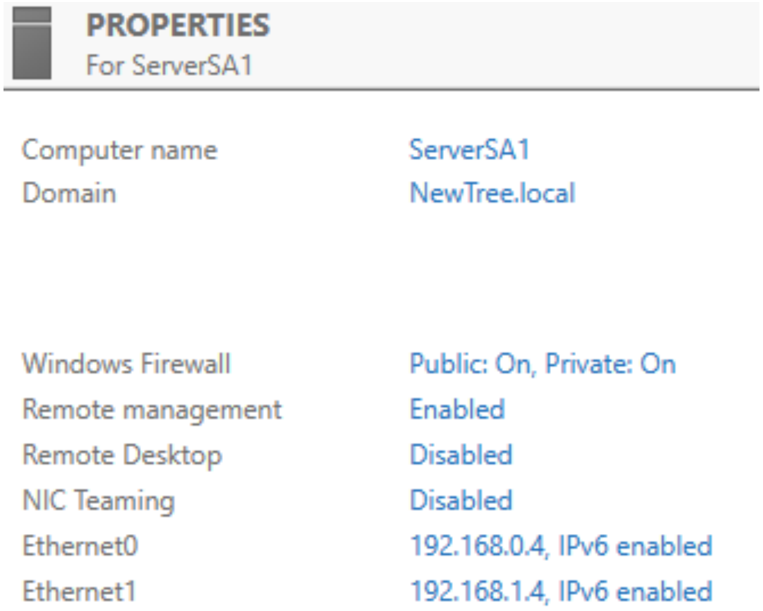


14. In the DNS Options window, you see a warning message about DNS delegation. This is okay and expected. Click **Next**.
15. In the Additional Options window, leave the default NetBIOS domain name, and then click **Next**.
16. In the Paths window, leave the default settings, and then click **Next**.
17. Review your choices in the Review Options window, and go back and make changes if necessary. When you're finished, click **Next**.
18. In the Prerequisites Check window, verify that all prerequisites have been met. You might see some warning messages, which is okay as long as there are no error messages. Click **Install**.
19. Watch the progress message at the top of the window to see the tasks being performed to install Active Directory. After the installation is finished, your computer restarts automatically. After the server restarts, sign in as **Administrator**. (*Note*: You're now signing in to the NewTree.local domain, which is part of the MCSA2016.local forest.)
20. In Server Manager, click **Tools**, **Active Directory Domains and Trusts** from the menu. In the left pane, you see both MCSA2016.local and NewTree.local. Right-click **MCSA2016.local** and click **Properties**. Click the **Trusts** tab. You see an outgoing and incoming trust with NewTree.local. Click **Cancel**. Right-click **NewTree.local** and click **Properties**. Click the **Trusts** tab. You see an outgoing and incoming trust with MCSA2016.local. Click **Cancel**. Close Active Directory Domains and Trusts.
21. In Server Manager, click **Tools, DNS** to open DNS Manager.
22. In DNS Manager, click to expand **Forward Lookup Zones**, and click **NewTree.local**. You see the records that were created automatically, which include an A record for ServerSA1 and the folders containing Active Directory–related records. Close DNS Manager.
23. Continue to the next activity.



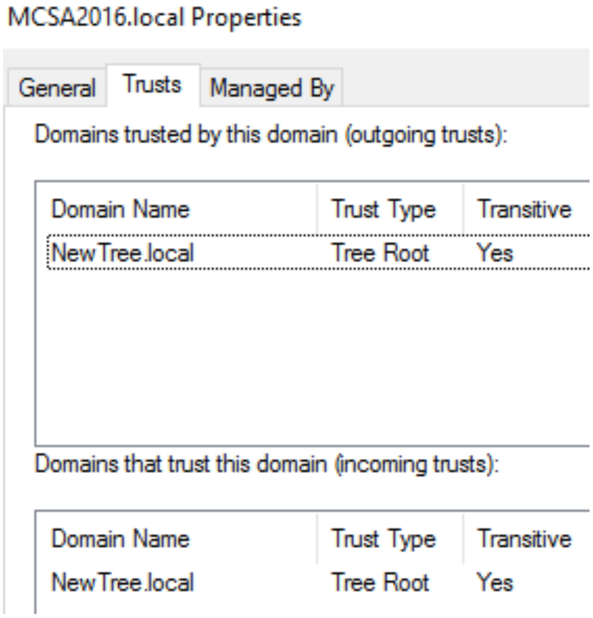
PROPERTIES
For ServerSA1

Computer name	ServerSA1
Workgroup	WORKGROUP
Windows Firewall	Public: On, Private: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet0	192.168.0.4, IPv6 enabled
Ethernet1	192.168.1.4, IPv6 enabled



PROPERTIES
For ServerSA1

Computer name	ServerSA1
Domain	NewTree.local
Windows Firewall	Public: On, Private: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet0	192.168.0.4, IPv6 enabled
Ethernet1	192.168.1.4, IPv6 enabled



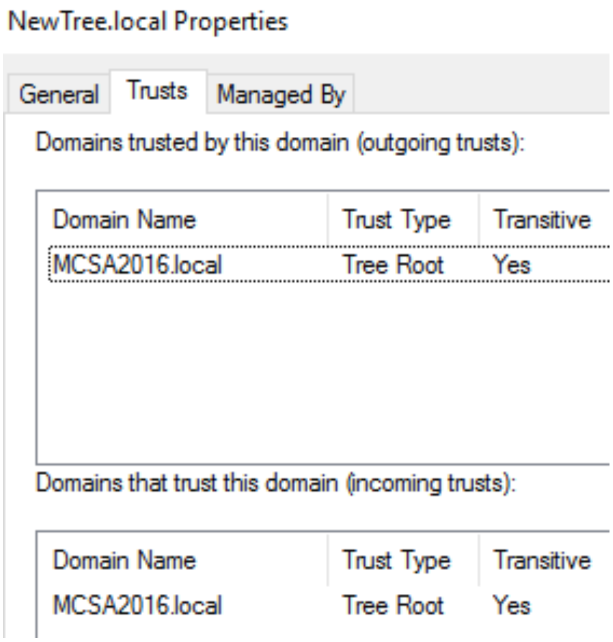
MCSA2016.local Properties

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
NewTree.local	Tree Root	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
NewTree.local	Tree Root	Yes

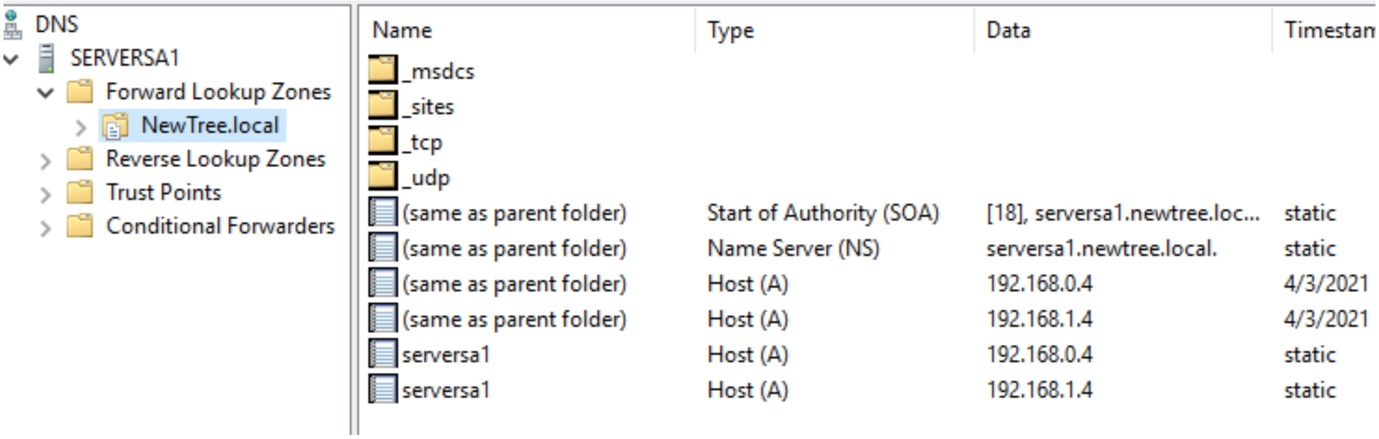

NewTree.local Properties

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
MCSA2016.local	Tree Root	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
MCSA2016.local	Tree Root	Yes



Name	Type	Data	Timestan
_msdcs			
_sites			
_tcp			
_udp			
(same as parent folder)	Start of Authority (SOA)	[18], serversa1.newtree.loc...	static
(same as parent folder)	Name Server (NS)	serversa1.newtree.local.	static
(same as parent folder)	Host (A)	192.168.0.4	4/3/2021
(same as parent folder)	Host (A)	192.168.1.4	4/3/2021
serversa1	Host (A)	192.168.0.4	static
serversa1	Host (A)	192.168.1.4	static

Activity 7-4: Creating a New Forest

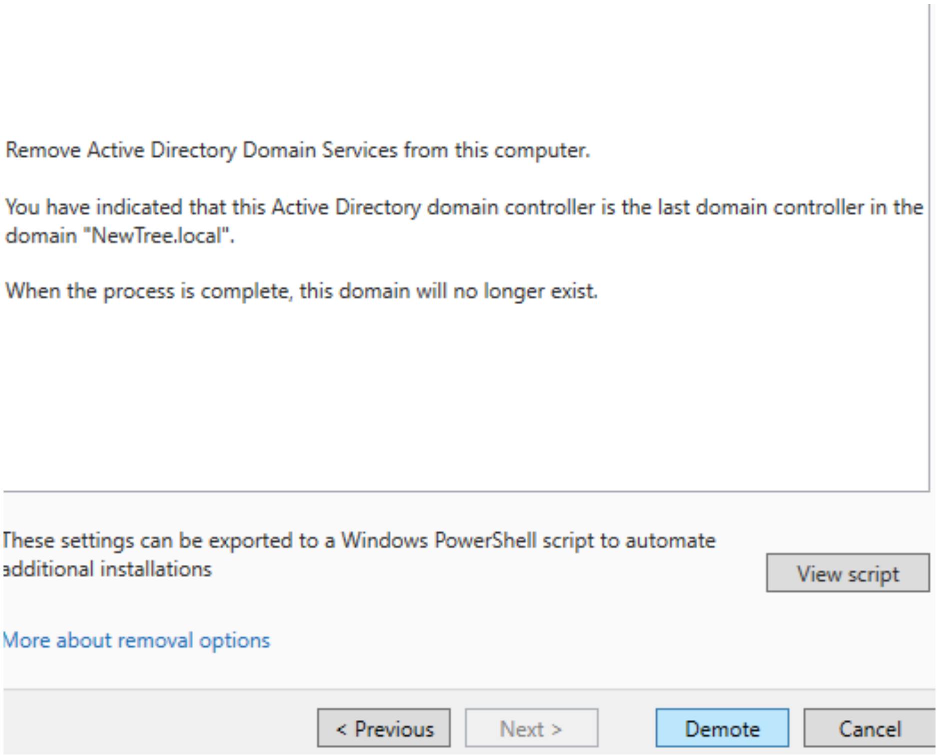
Time Required: 25 minutes or longer

Objective: Create a new forest.

Required Tools and Equipment: ServerDC1, ServerSA1

Description: In this activity, you create a new forest, using ServerSA1 as the DC for the new forest root. First, you demote ServerSA1, and then you promote it, choosing the option to add a new forest. You name the new forest NewForest.local.

1. On ServerSA1 in Server Manager, click **Manage**, **Remove Roles and Features** from the menu to start the Remove Roles and Features Wizard.
2. In the Before You Begin window, click **Next**. In the Server Selection window, click **Next**.
3. In the Server Roles window, click to clear **Active Directory Domain Services**, and then click **Remove Features**. The Validation Results message box states that you must first demote the domain controller. Click **Demote this domain controller**.
4. In the Credentials window, you must enter enterprise administrator credentials. Click **Change**. In the Windows Security dialog box, type **MCSA2016\Administrator** in the User name text box and **Password01** in the Password text box. Click **OK**.
5. Click the **Last domain controller in the domain** check box, and then click **Next**. In the Warnings window, click the **Proceed with removal** check box, and then click **Next**.
6. In the Removal Options window, click the **Remove this DNS zone (this is the last DNS server that hosts the zone)** check box, and then click **Next**.
7. Type **Password01** in the Password and Confirm password text boxes. (It's the password for the local Administrator account when the server is no longer a DC.) Click **Next**.
8. In the Review Options window, click **Demote**. When the demotion is finished, the server restarts.
9. After ServerSA1 restarts, sign in as **Administrator**.
10. You need to ensure that all metadata is cleaned up after the demotion of ServerSA1. On ServerDC1, from Server Manager, open Active Directory Sites and Services. Navigate to **Sites\Default-First-Site-Name\Servers**. If ServerSA1 is listed, right-click it and click **Delete**. Click **Yes** to confirm. Close Active Directory Sites and Services.
11. On ServerSA1, in Server Manager, click the notifications flag, and then click **Promote this server to a domain controller**. The Active Directory Domain Services Configuration Wizard starts.
12. In the Deployment Configuration window, click the **Add a new forest** option button. Type **NewForest.local** in the Root domain name text box, and then click **Next**.
13. In the Domain Controller Options window, type **Password01** in the Password and Confirm password boxes. Click **Next**.
14. In the DNS Options window, click **Next**. In the Additional Options window, click **Next**.
15. In the Paths window, click **Next**. In the Review Options window, click **Next** and then click **Install**. The server will restart.
16. After the server restarts, sign in and verify the installation.
17. Continue to the next activity.

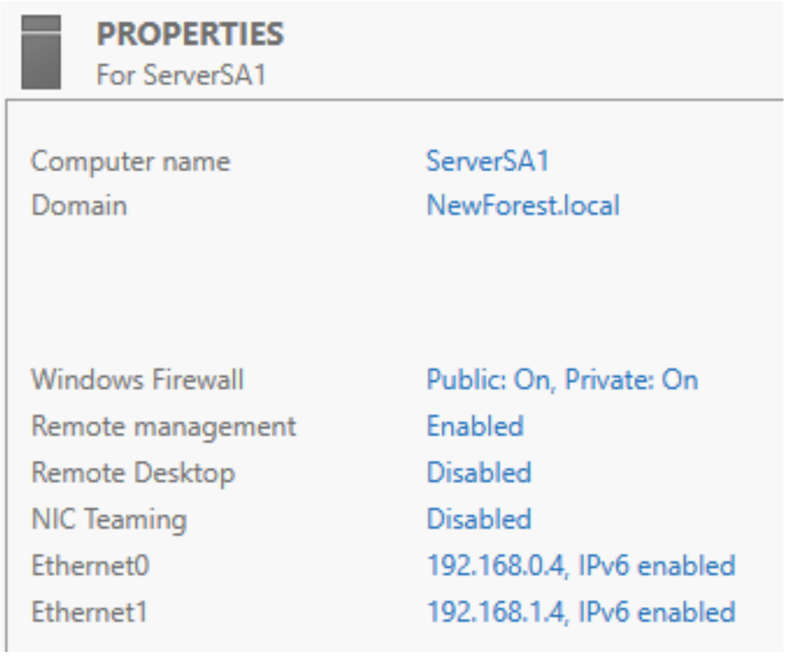


Remove Active Directory Domain Services from this computer.

You have indicated that this Active Directory domain controller is the last domain controller in the domain "NewTree.local".

When the process is complete, this domain will no longer exist.

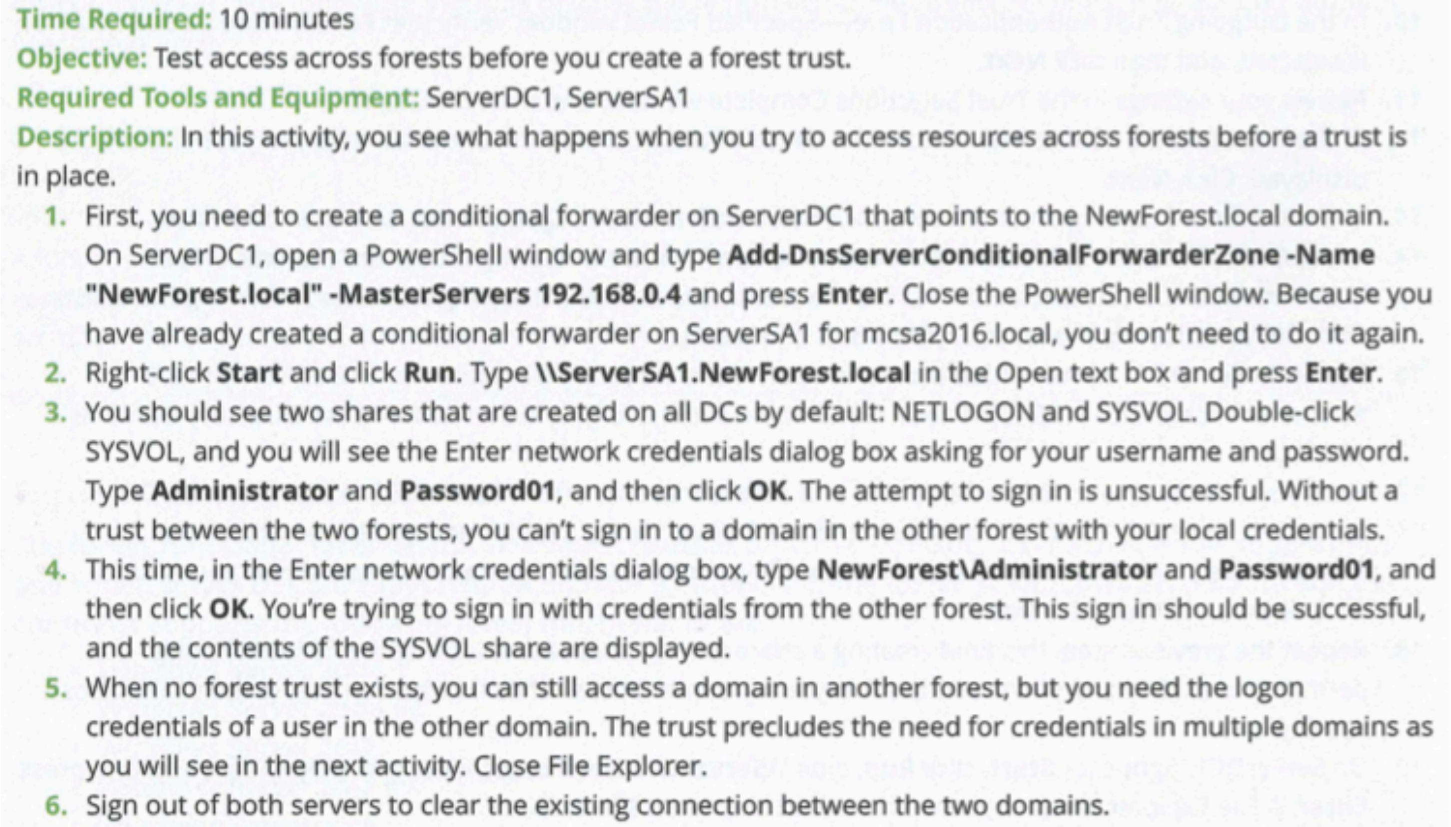
These settings can be exported to a Windows PowerShell script to automate additional installations



PROPERTIES
For ServerSA1

Computer name	ServerSA1
Domain	NewForest.local
Windows Firewall	Public: On, Private: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet0	192.168.0.4, IPv6 enabled
Ethernet1	192.168.1.4, IPv6 enabled

Activity 7-5: Testing Cross-Forest Access Without a Trust



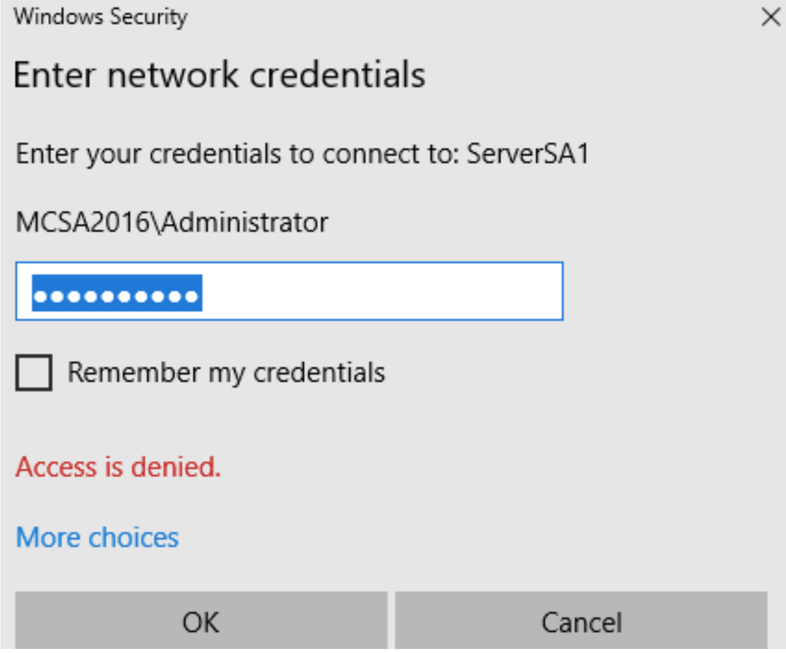
Time Required: 10 minutes

Objective: Test access across forests before you create a forest trust.

Required Tools and Equipment: ServerDC1, ServerSA1

Description: In this activity, you see what happens when you try to access resources across forests before a trust is in place.

1. First, you need to create a conditional forwarder on ServerDC1 that points to the NewForest.local domain. On ServerDC1, open a PowerShell window and type **Add-DnsServerConditionalForwarderZone -Name "NewForest.local" -MasterServers 192.168.0.4** and press **Enter**. Close the PowerShell window. Because you have already created a conditional forwarder on ServerSA1 for mcsa2016.local, you don't need to do it again.
2. Right-click **Start** and click **Run**. Type **\\ServerSA1.NewForest.local** in the Open text box and press **Enter**.
3. You should see two shares that are created on all DCs by default: NETLOGON and SYSVOL. Double-click SYSVOL, and you will see the Enter network credentials dialog box asking for your username and password. Type **Administrator** and **Password01**, and then click **OK**. The attempt to sign in is unsuccessful. Without a trust between the two forests, you can't sign in to a domain in the other forest with your local credentials.
4. This time, in the Enter network credentials dialog box, type **NewForest\Administrator** and **Password01**, and then click **OK**. You're trying to sign in with credentials from the other forest. This sign in should be successful, and the contents of the SYSVOL share are displayed.
5. When no forest trust exists, you can still access a domain in another forest, but you need the logon credentials of a user in the other domain. The trust precludes the need for credentials in multiple domains as you will see in the next activity. Close File Explorer.
6. Sign out of both servers to clear the existing connection between the two domains.



Windows Security

Enter network credentials

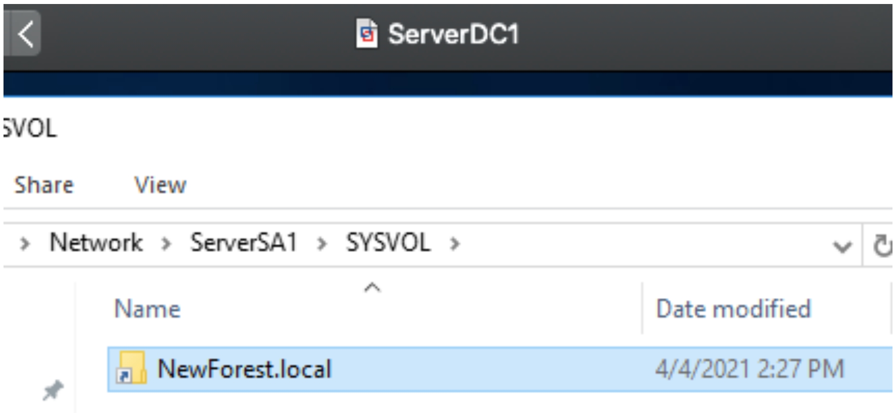
Enter your credentials to connect to: ServerSA1

MCSA2016\Administrator

●●●●●●●●●●●

□ Remember my credentials

Access is denied.



› Network › ServerSA1 › SYSVOL ›

Name	Date modified
NewForest.local	4/4/2021 2:27 PM