

# Lab – Mitigating the Loss of Your Forest Root

## Overview

In this lab, you will learn how to mitigate the loss of a failed forest root. You will need to create an additional domain controller for this lab running Server 2016, full Desktop Experience. Name the machine DC3.

It's never a matter of if your forest root will suffer a catastrophic failure, it's just a matter of when. Being proactive and mitigating the risk of not having a forest root requires that we build a replica domain controller and build redundancy into our network design.

## Scenario

In our Active Directory domain there are two domain controller running Windows Server 2016 full Desktop Experience:

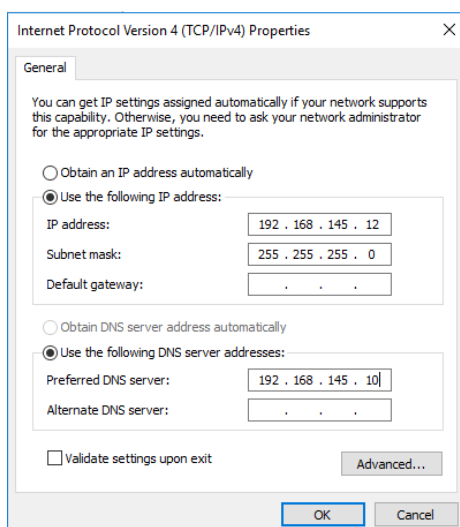
- Forest Root DC1
- Replica DC3

On DC1, perform a snapshot to save your current configuration running Active Directory. We should already have a snapshot for DC1 without Active Directory installed.

DC3 is a replica of the forest root, DC1. We need to have a snapshot saved for DC3 with no Active Directory installed.

Having snapshots taken for our virtual machines to allows us to roll back our servers to a previous configuration thus will not have to reinstall Server 2016 each time we need to install or remove Active Directory.

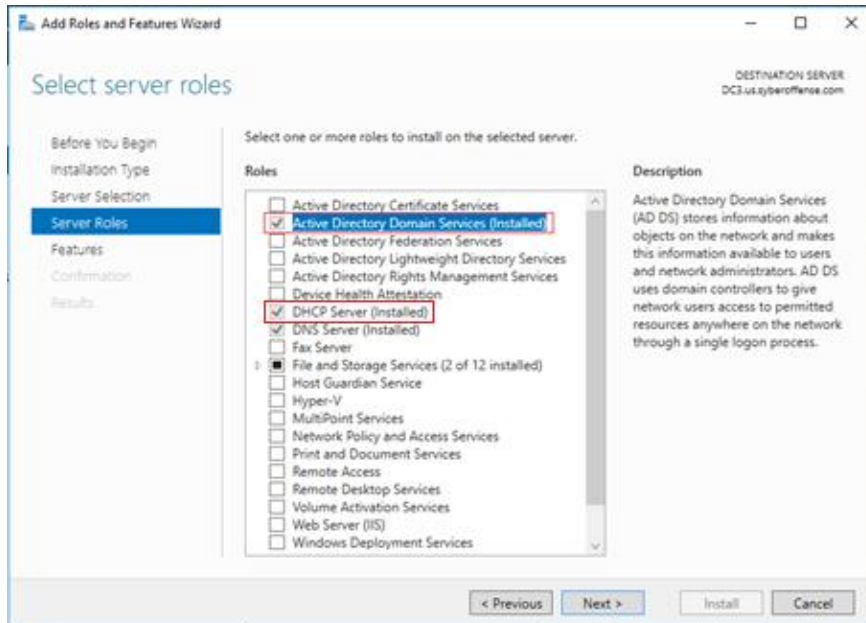
Configure your network adapter for DC3 with the following configuration:



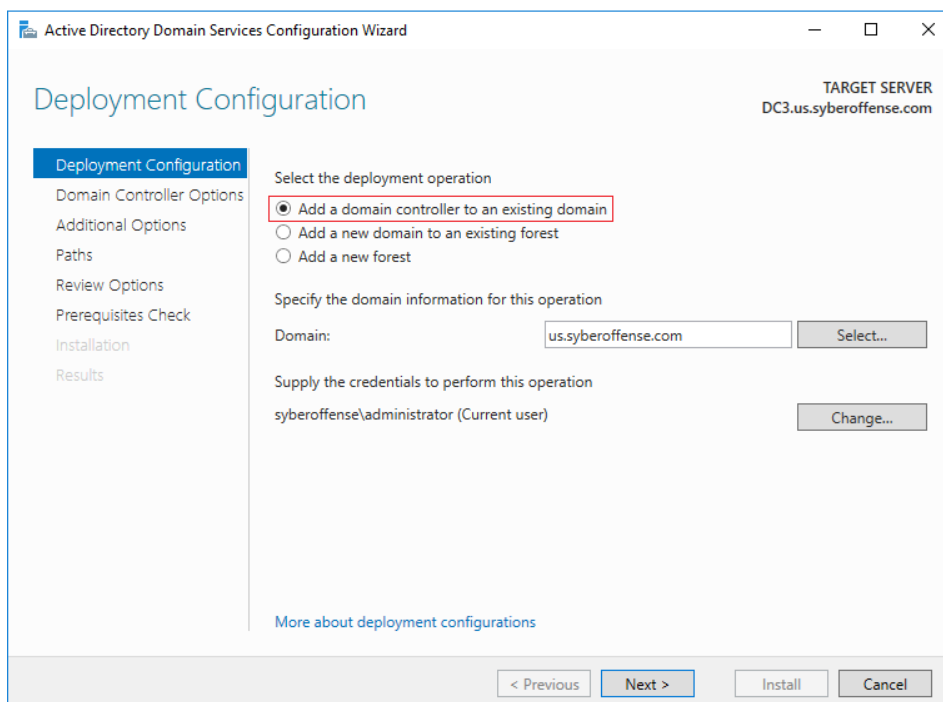
Add the machine to the domain.

## Active Directory Configuration for DC3.

Install the Active Directory Domain Services role along with the DHCP role..



Once the ADDS role has been installed, from Server Manager, click on the informational alert (yellow triangle) and click on the link provided to promote the server to a domain controller.



Note that on the next page DNS and the Global Catalog were not found. The wizard gives you the option to install both.

The screenshot shows the 'Domain Controller Options' screen of the Active Directory Domain Services Configuration Wizard. The left sidebar lists the steps: Deployment Configuration, Domain Controller Options (selected), DNS Options, Additional Options, Paths, Review Options, Prerequisites Check, Installation, and Results. The main area is titled 'Specify domain controller capabilities and site information'. It contains three checkboxes: 'Domain Name System (DNS) server' (checked), 'Global Catalog (GC)' (checked), and 'Read only domain controller (RODC)' (unchecked). Below these is a 'Site name' dropdown menu set to 'Default-First-Site-Name'. Further down, there are two password fields labeled 'Password:' and 'Confirm password:', both containing masked characters. At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link 'More about domain controller options' is also present.

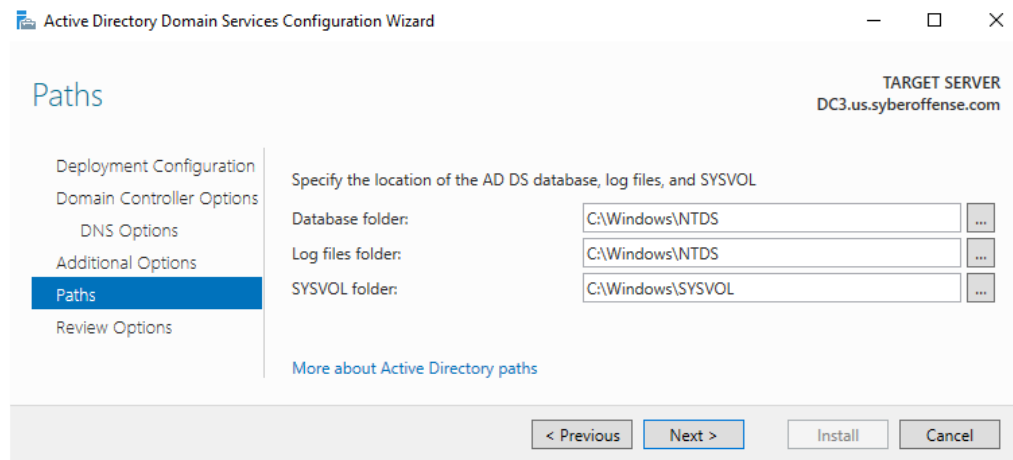
Ignore the warning about no DNS delegation being found. Click Next.

The screenshot shows the 'DNS Options' screen of the Active Directory Domain Services Configuration Wizard. The left sidebar is the same as the previous screen, but 'DNS Options' is now selected. The main area is titled 'Specify DNS delegation options'. It contains a checkbox for 'Update DNS delegation' which is unchecked. Above this checkbox is a yellow warning box with a triangle icon and the text: 'A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found... Show more'. Below the checkbox is a link 'More about DNS delegation'. At the bottom, the same navigation buttons are present: '< Previous', 'Next >', 'Install', and 'Cancel'.

On the next screen, tell DC3 to replicate with DC1.

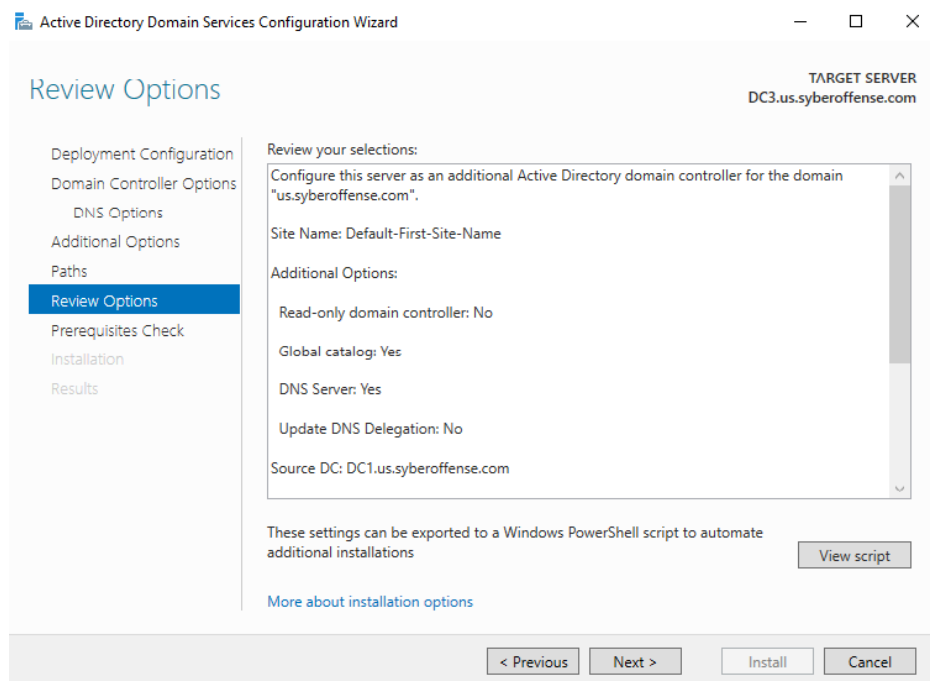
The screenshot shows the 'Additional Options' screen of the Active Directory Domain Services Configuration Wizard. The left sidebar shows 'Additional Options' selected. The main area is titled 'Specify Install From Media (IFM) Options' and 'Specify additional replication options'. Under the first section, there is an unchecked checkbox for 'Install from media'. Under the second section, there is a 'Replicate from:' dropdown menu set to 'DC1.us.syberoffense.com'. Below this is a link 'More about additional options'. At the bottom, the navigation buttons are: '< Previous', 'Next >', 'Install', and 'Cancel'.

Accept the default locations on the next screen and click next.



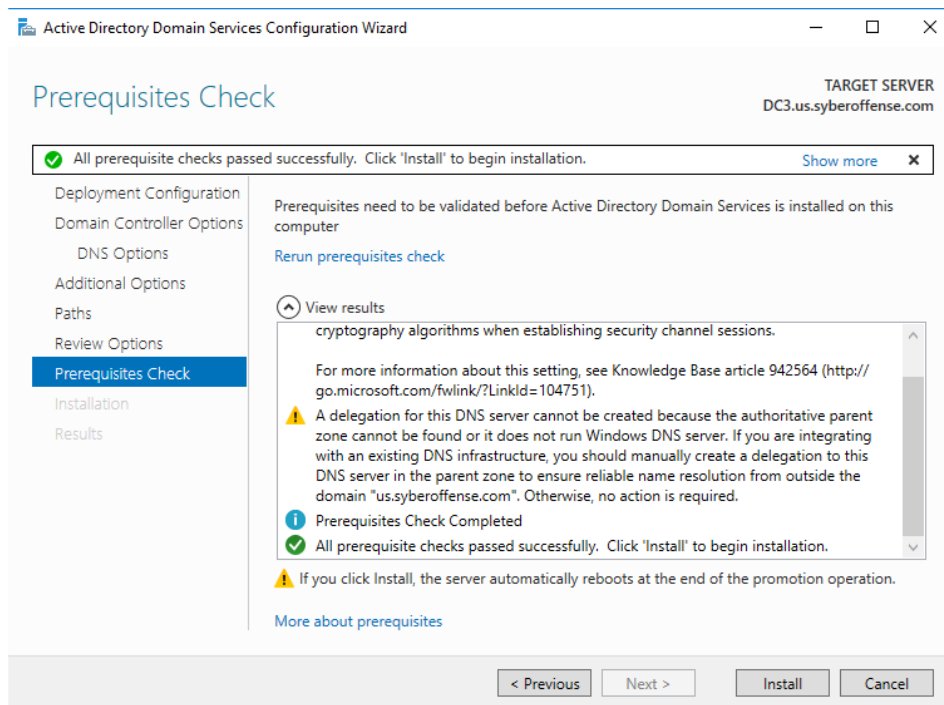
The screenshot shows the 'Paths' step of the Active Directory Domain Services Configuration Wizard. The left sidebar lists the steps: Deployment Configuration, Domain Controller Options, DNS Options, Additional Options, Paths (selected), and Review Options. The main area is titled 'Paths' and 'Specify the location of the AD DS database, log files, and SYSVOL'. It contains three input fields: 'Database folder:' with 'C:\Windows\NTDS', 'Log files folder:' with 'C:\Windows\NTDS', and 'SYSVOL folder:' with 'C:\Windows\SYSVOL'. Each field has a browse button (three dots). At the bottom, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'. The target server is 'DC3.us.syberoffense.com'.

On the next screen, confirm your choices. If all is right, click next.



The screenshot shows the 'Review Options' step of the Active Directory Domain Services Configuration Wizard. The left sidebar lists the steps: Deployment Configuration, Domain Controller Options, DNS Options, Additional Options, Paths, Review Options (selected), Prerequisites Check, Installation, and Results. The main area is titled 'Review Options' and 'Review your selections:'. It contains a list of configuration options: 'Configure this server as an additional Active Directory domain controller for the domain "us.syberoffense.com".', 'Site Name: Default-First-Site-Name', 'Additional Options:', 'Read-only domain controller: No', 'Global catalog: Yes', 'DNS Server: Yes', 'Update DNS Delegation: No', and 'Source DC: DC1.us.syberoffense.com'. At the bottom, there is a button for 'View script' and a note: 'These settings can be exported to a Windows PowerShell script to automate additional installations'. At the bottom of the wizard, there are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'. The target server is 'DC3.us.syberoffense.com'.

Wait for the verification to complete. Ignore all the yellow warning. Look for the green checkmark at the bottom and then click the install button.

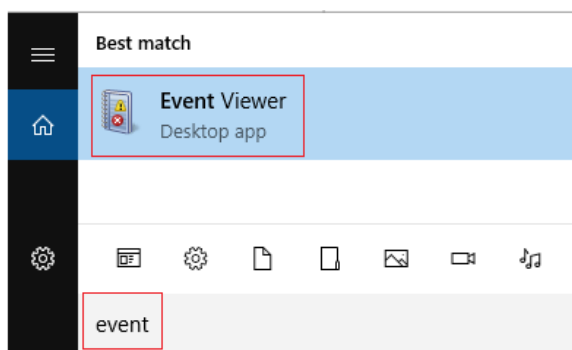


Once DC3 has completed its promotion to a domain controller, it will automatically reboot.

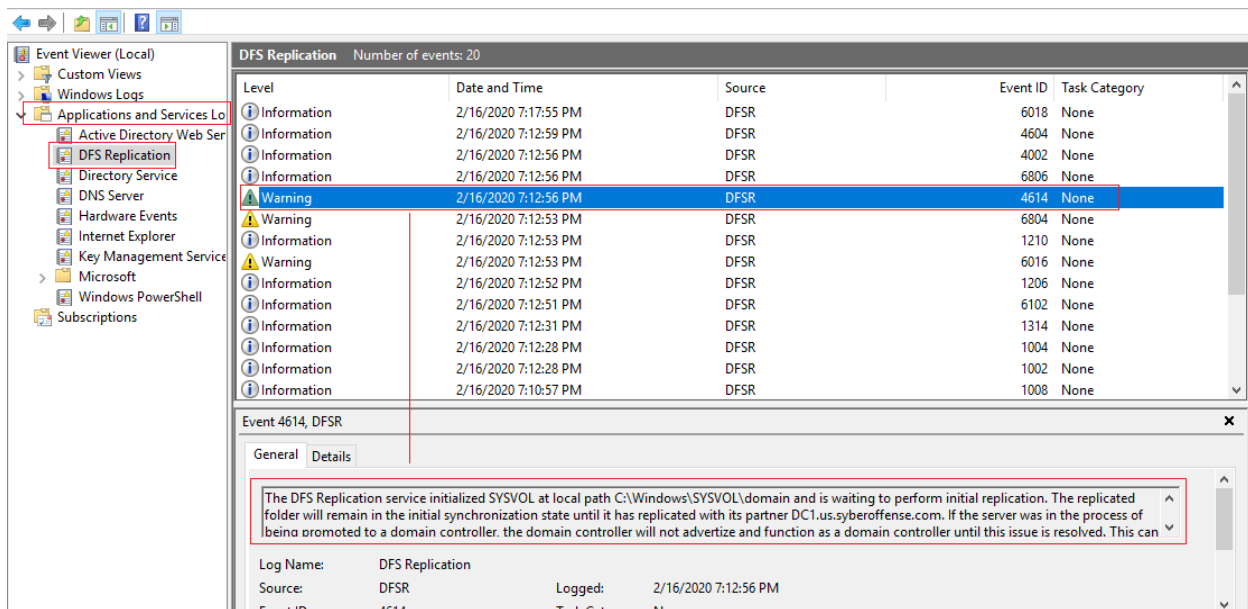
Once DC3 is up and running, give it time to replicate Active Directory with DC1.

## Check Event Logs for Any Replication Errors

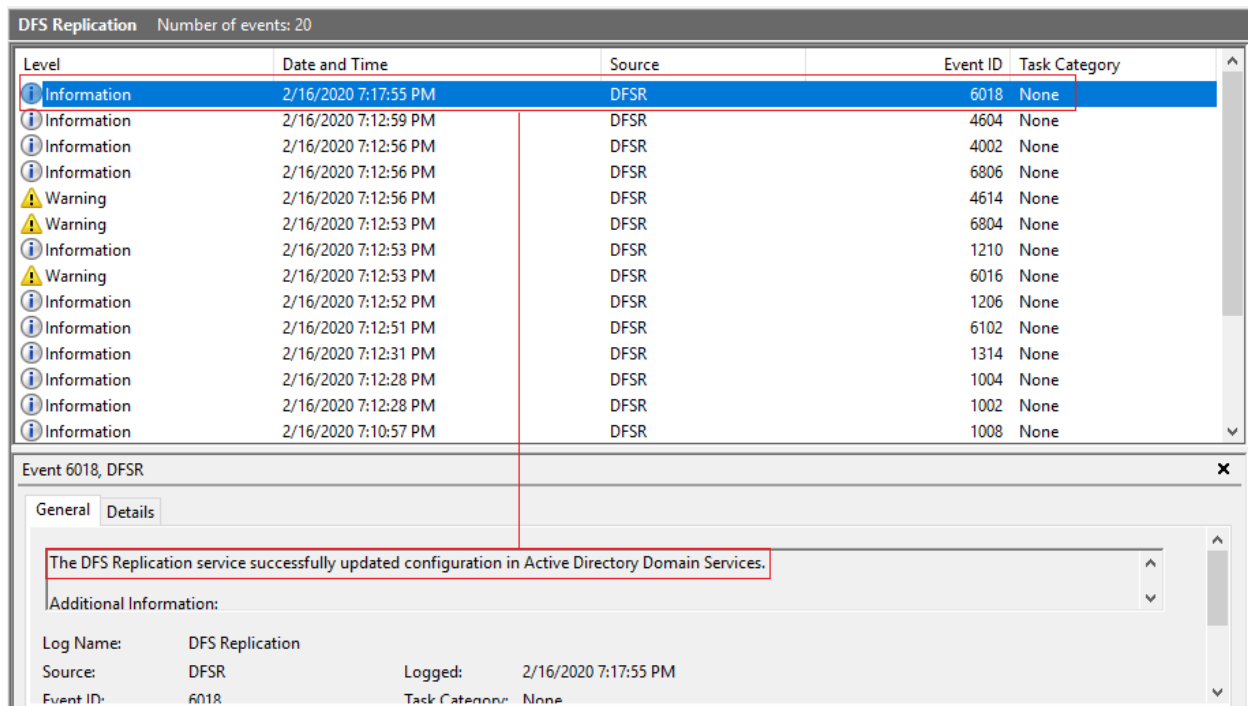
In the Windows search bar, type, 'event.' Click on Event Viewer.



From the left windowpane, open and expand the Applications and Service Logs. Click on DFS replication. Click on the first warning in the center windowpane. At the bottom of the center windowpane, you read the DFS replication is waiting to replicate.



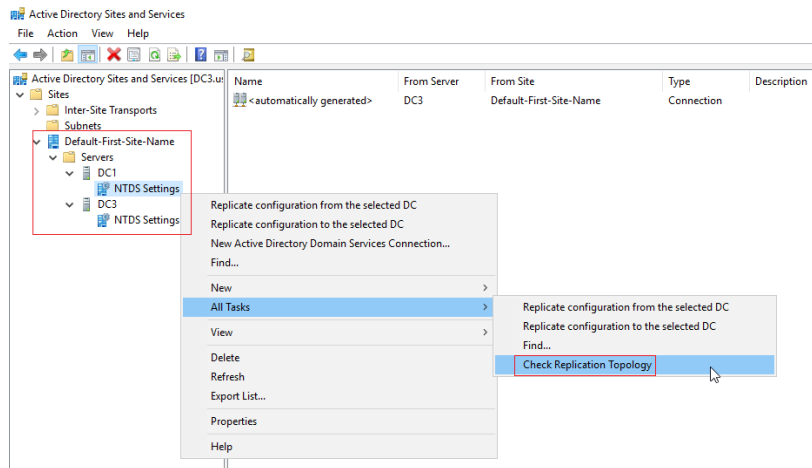
Now click and view the informational message. The DFS replication completed successfully. We will come back to the event viewer again once we take DC1 offline to see what replication errors message are present.



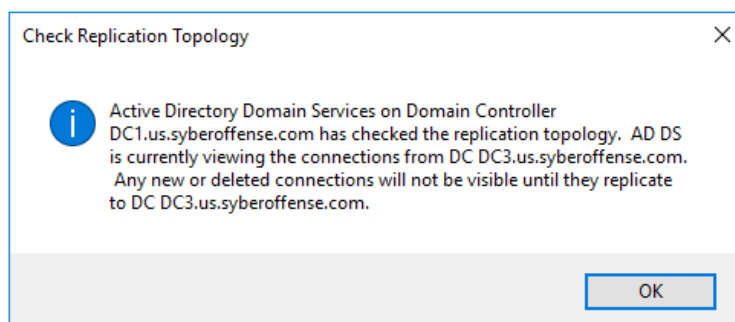
Close the event viewer.

From Server Manager, got to Tools and click on Active Directory Sites and Service. Expand Default-First-Site-Name. Expand the Server container. Expand the name of each server present.

Right-click on the NTDS Settings for each of the server and from the context menu, click on, Check Replication Topology.

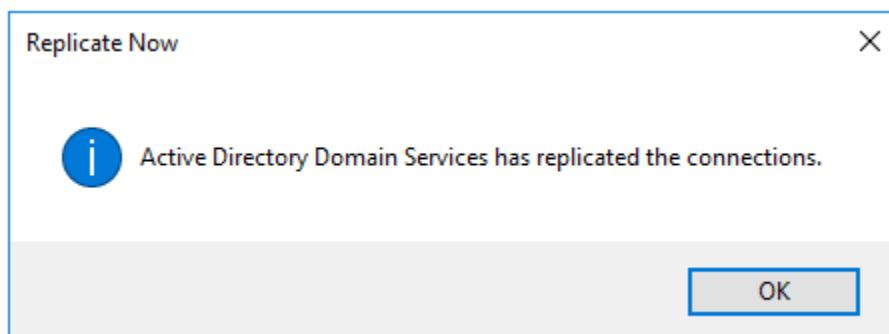


The following message is given. Click OK to close out the message.



From the left windowpane, click on the NTDS settings for DC1 And from the right windowpane, under the Name column, right-click where it says, 'Automatically generated' in brackets < >. From the context menu, select, 'Replicate Now'.

Note the following message.



Using site and Service, we can check on our replication topology and if need be, we can force one domain controller to replicate with another. This is the administrative tool for

troubleshooting site replication issues. When we talk about replication, we are talking about DC1 updating any changes with its active directory database with the other DCs in the domain.

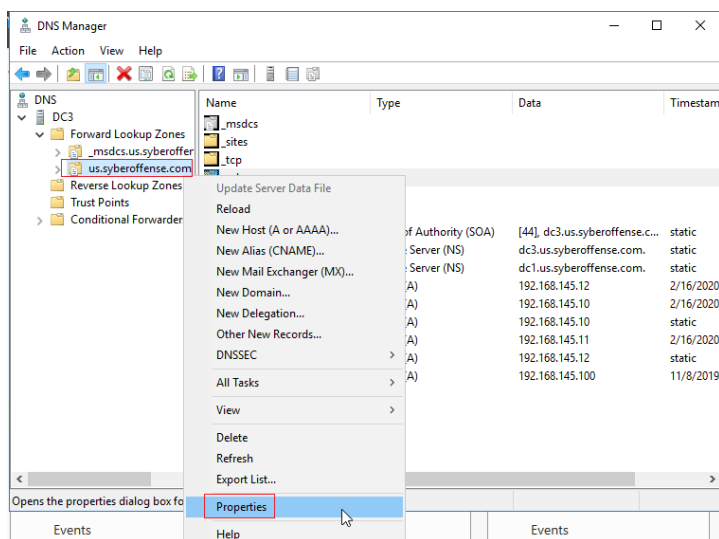
We will come back to this tool once we have taken DC1 offline. You can close out Sites and Services.

You can also check for any errors with your replication between DC1 and DC3 by opening the event viewer and examining the DFS replications logs. We periodically check the event viewer for indicators that there may be issues and not just with replication, but with any component of our windows server.

Let's prepare our DC3 to become a DNS secondary zone. DC3 will share the DNS database stored on DC1. Just as we have two domain controllers for redundancy of our forest root, we would also have at least two DNS servers running in the domain to ensure we have DNS available.

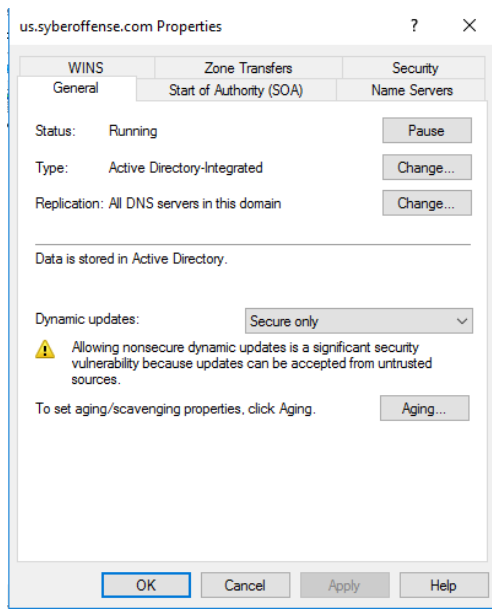
From Server Manager, click on Tools and from the list of available tools, click on DNS. This launches the DNS Management console. Since our DNS servers are all Active Directory Integrated, they are both equal. The Active Directory Integrated part means the DNS database is stored in Active Directory and replicated as changes to DNS are made, just like any other object in Active directory.

Expand the forward lookup zones container. Right-click on the container for your forward lookup zone and from the context menu, select properties.



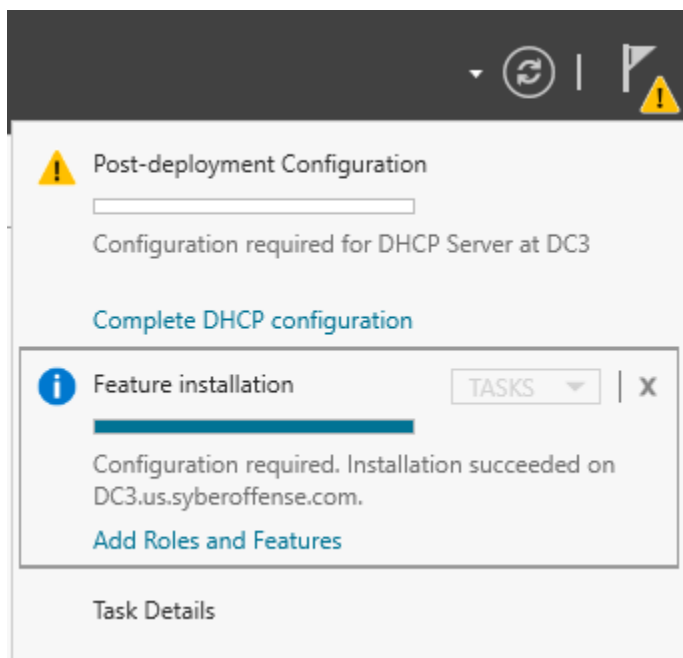
On the next screen is where you can change your zone type and the type of dynamic updates you will allow. No need to make any changes here. Click cancel.



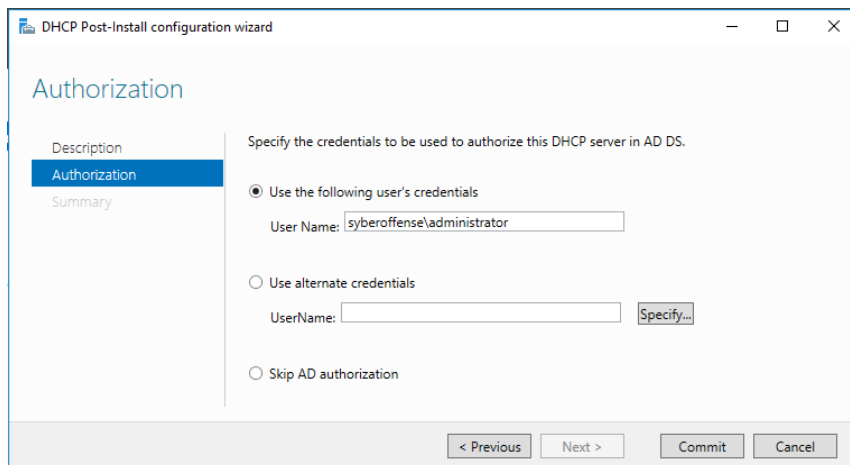


We next need to configure DHCP failover. This is our next level of redundancy. The DHCP role can be installed on any server in the domain but since DNS and DHCP work so well together, I prefer to install them both roles on a server running Active Directory. This is my preference for having the DHCP role running in the domain.

Using Server Manager on DC3 and Add the DHCP role. Once you installed the role, click on the warning message in Server Manager, and complete the DHCP configuration.



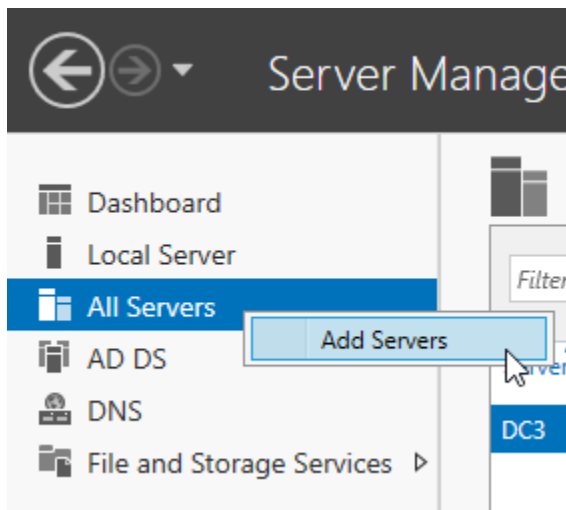
Accept all the defaults for the Post-install configuration wizard. And click commit.



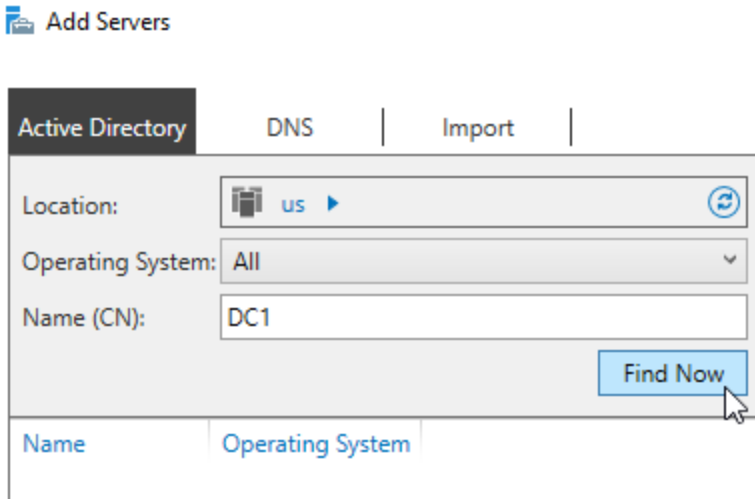
On the next screen, close the wizard.

We currently have DHCP running on DC1 and DC3. Since we are currently using the Server Manager on DC3, let's add DC1 to our Server Manager and manage DC1 from here.

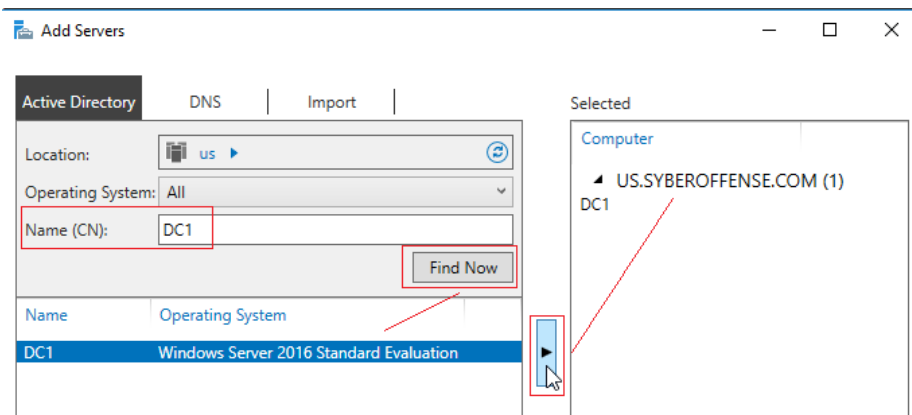
From your Server Manager console running on DC3, from the left windows pane, right-click on All Servers and from the context menu, click on, Add Servers.



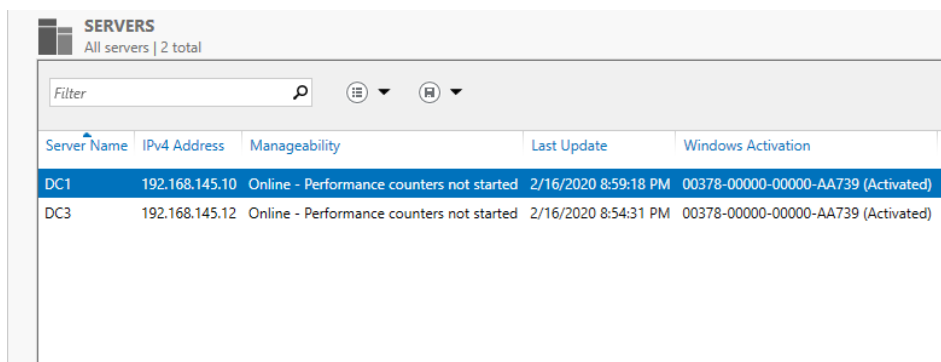
On the next screen, in the Name field, type the name of your forest root. Mine is called DC1. Click the Find Now button.



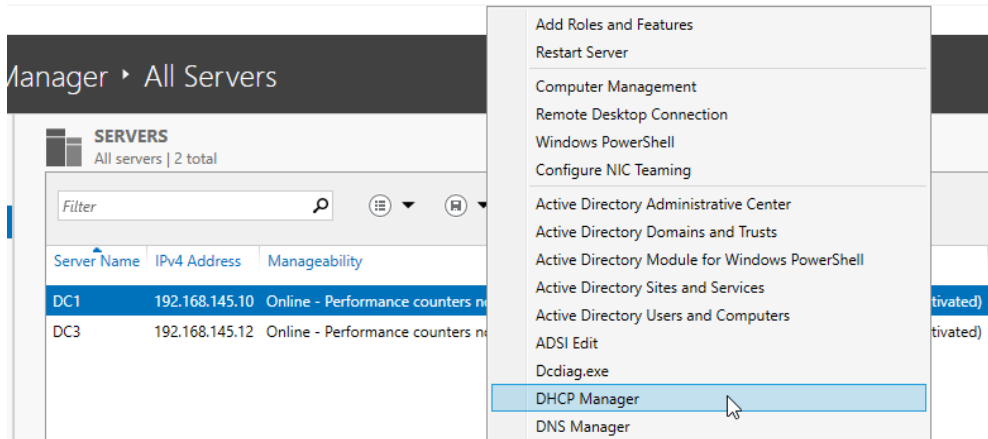
From the bottom windows pane, highlight the name of your forest root and use the move button to add it to the right windowpane. Click OK.



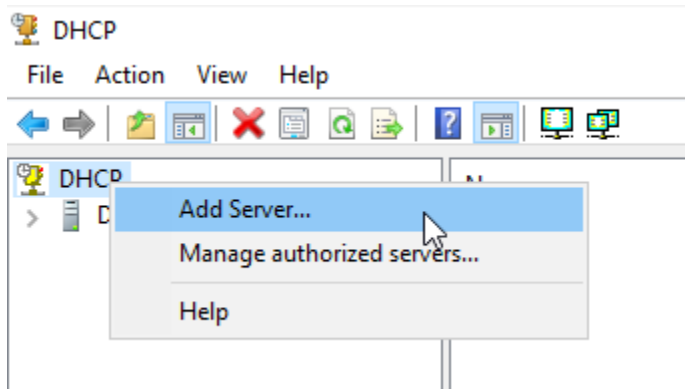
Back at Server windows, you will see your forest root has been added.



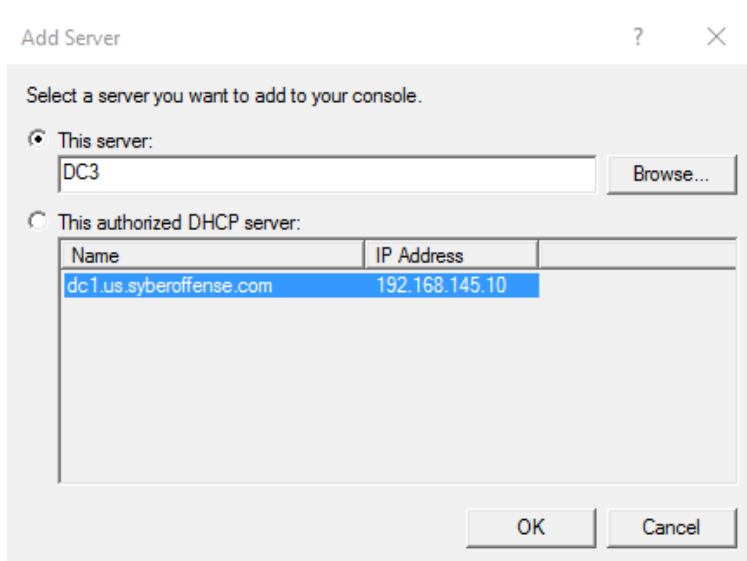
From the Server windowpane, you can now right-click and get access to all the roles running on DC1. From the context manager, select DHCP Manager.



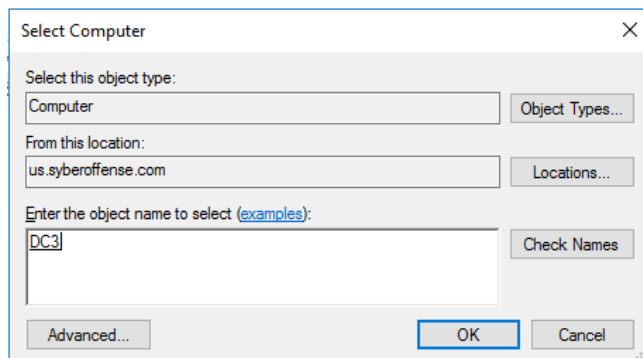
We now have access to the DHCP server on DC1. In the left window pane of your DHCP management console, Right-click on the top where it says, DHCP and from the context menu, select, Add Server.



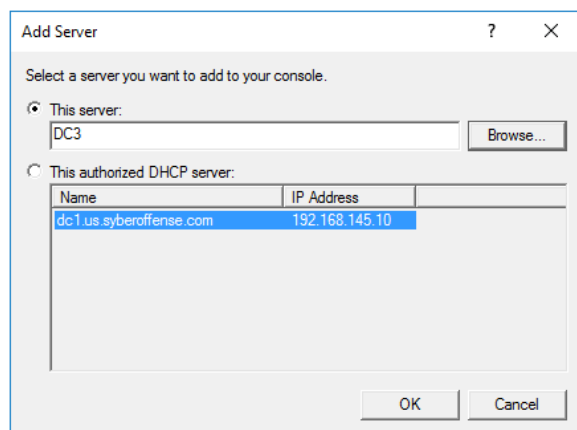
Type either the name or the IP address for your replica domain controller, DC3.



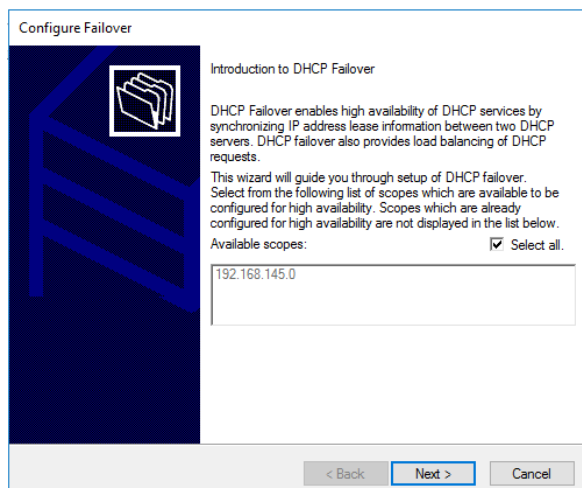
In Select Computer screen, type in the name of your replica domain controller. Click the Check Names button. If the server is registered with the appropriate records in the DNS database, it will be found and underlined. Click OK.

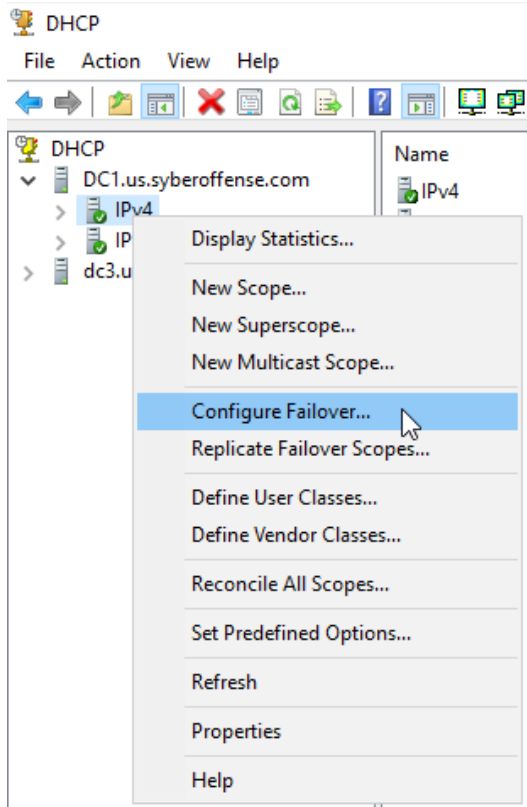


On the next screen, click OK one more time.

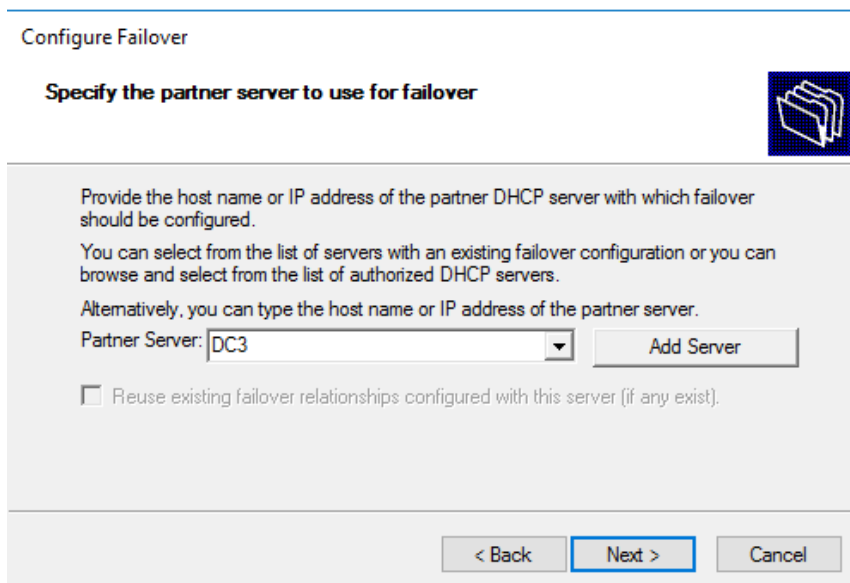


You now have two servers listed in the left windowpane. Expand DC1 or the forest root of your domain. Right-click on your IPv4 scope and from the context menu, select, Configure Failover. This launches the Configure Failover wizard. On the introduction screen, click Next.

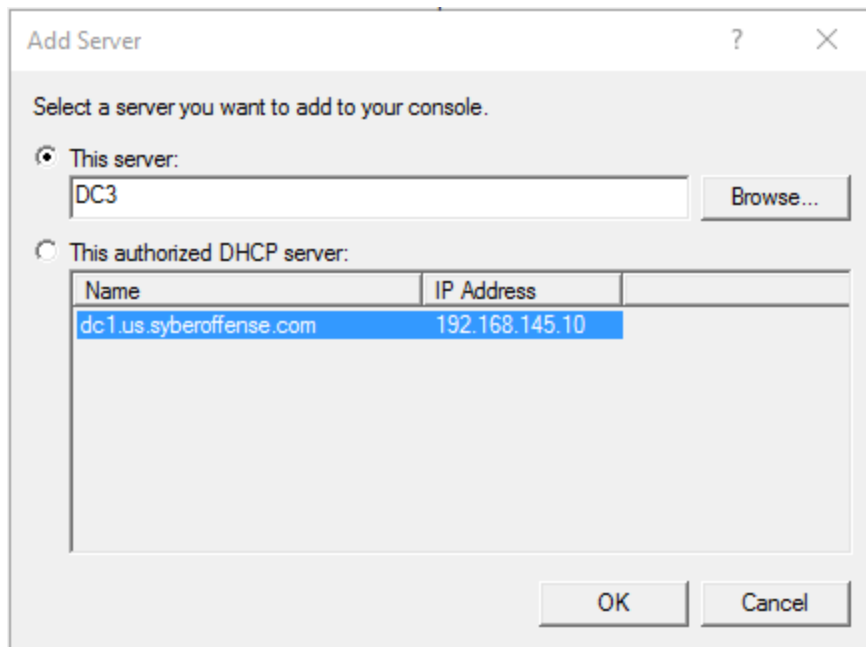




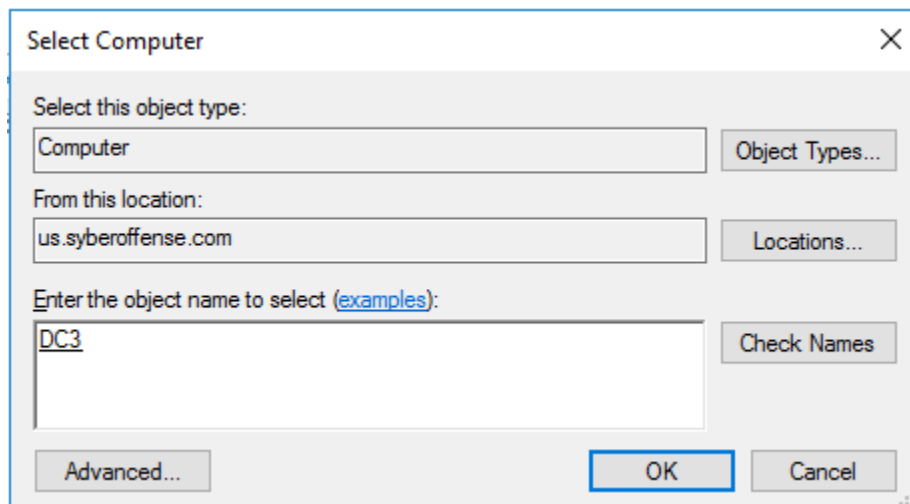
In the next window, types the name of your replica domain controller and click the Add Server button.



On the next screen, again type, the name of your replica domain controller and click on the Browse button.



In the next windows, type in the name of your replica domain controller and click on the Check Names button. Click OK.



Click OK again and on the next screen showing the FQDN for your replica domain controller, click next.

Configure Failover

**Specify the partner server to use for failover**

Provide the host name or IP address of the partner DHCP server with which failover should be configured.

You can select from the list of servers with an existing failover configuration or you can browse and select from the list of authorized DHCP servers.

Alternatively, you can type the host name or IP address of the partner server.

Partner Server:

☐ Reuse existing failover relationships configured with this server (if any exist).

< Back **Next >** Cancel

On the next screen, create a new failover relationship. Match your setting with the following window.

Configure Failover

**Create a new failover relationship**

Create a new failover relationship with partner dc3.us.syberoffense.com

Relationship Name:

Maximum Client Lead Time:  hours  minutes

Mode:

Hot Standby Configuration

Role of Partner Server:

Addresses reserved for standby server:  %

☒ State Switchover Interval:  minutes

☒ Enable Message Authentication

Shared Secret:

< Back **Next >** Cancel

On the last window, click finish.



**Configure Failover**

Failover will be set up between dc1 and dc3.us.syberoffense.com with the following parameters.

Scopes:

192.168.145.0

Relationship Name: dc1-dc3.us.syberoffense.com  
 Maximum Client Lead Time: 1 hrs 0 mins  
 Mode: Hot standby  
 State Switchover Interval: 5 mins

Hot Standby Configuration

Role of Partner Server: Standby  
 Addresses reserved for standby: 50%

< Back Finish Cancel

On the next window, The DHCP servers perform a configuration check. Click close.

**Configure Failover** ? X

Progress of failover configuration.

The log below shows the progress of the various tasks for configuring failover including any errors encountered.

Add scopes on partner server .....Successful  
 Disable scopes on partner server .....Successful  
 Creation of failover configuration on partner server .....Successful  
 Creation of failover configuration on host server .....Successful  
 Activate scopes on partner server.....Successful  
 Configure failover successful.

Close

DC3 is standing by as the replica for the forest root and as the backup DNS and DHCP server for the domain in the event, DC1 should have a catastrophic failure.

## Summary

Congratulation on taking the right step in mitigating the risk of a catastrophic failure if your forest root goes offline. With the use of virtualization and system states. We can have any number of servers running at the same time on a single medium-size server. In this lab. We saw how virtualization could be used to create a replica of our forest root. What about my file server? My SQL server? My Exchange server? We could virtualize replicas of these just as easily and they could all be running on a single medium-size server inside their own virtual environment.