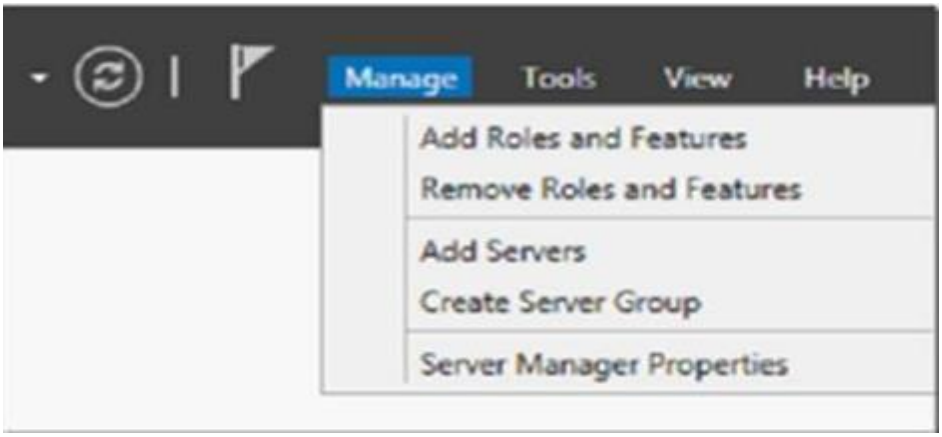
EXPERIMENT-1

Hyper-V-creating and configuring virtual machines?

Installing the roles for Hyper-V:

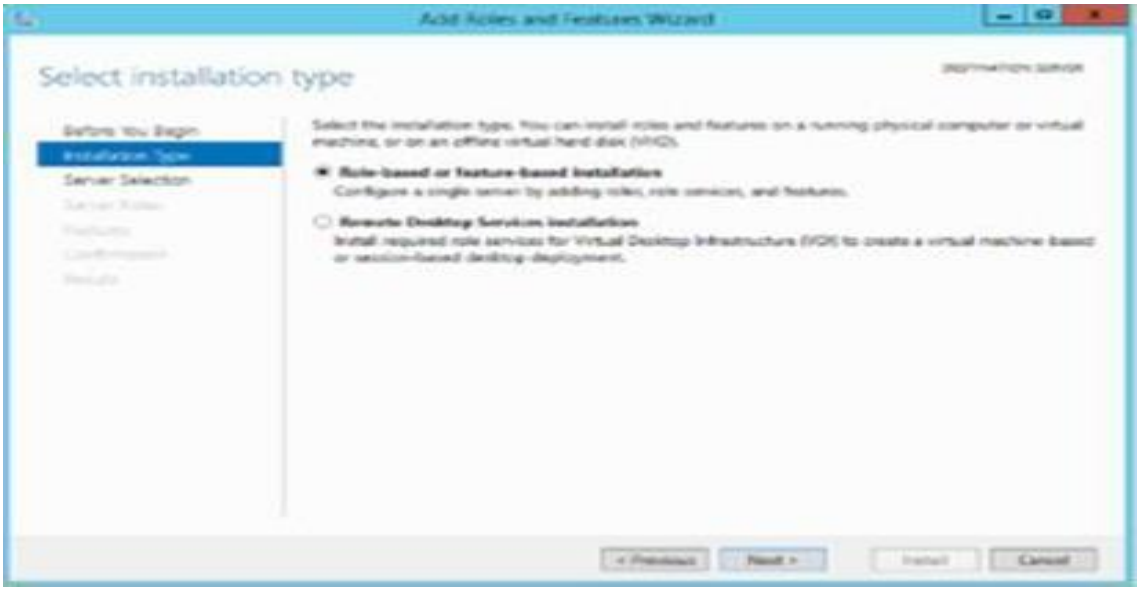
Open up Server Manager.

Once the server has initialised all its roles then click on Manage as shown above and then click on "Add Roles and Features"

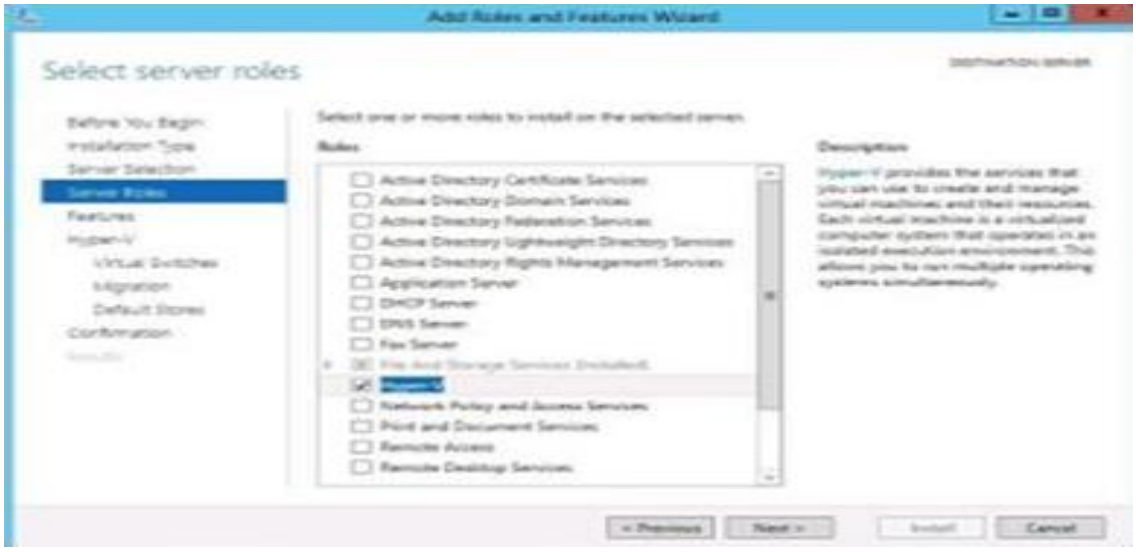


Read through the information (if you knew to this), to continue click Next.

Select "Role-Based or feature-based installation" and click Next.



Click on the checkbox next to Hyper-V.



After you have selected the role Hyper-V this window will come up. Click on add Features. > Click Next.> On the Feature screen click Next.

If you want to allow live migrations then click the checkbox above, otherwise accept the defaults and then click Next.

Specify the default location for your virtual harddisks by clicking the Browse button or accept the default locations and then click Next.

Click the checkbox to "Restart" the server automatically if required

Click Install.

Configuring Hyper-V:

You can open this shortcut either by using Server Manager or going to Control Panel -> Administrative Tools -> Hyper-V Manager.

This is the Hyper-V window that will open.
Click on Hyper-V Settings on the right hand side, the screen below will come up.

EXPERIMENT-2

Hyper-V-creating and configuring virtual machine storage?

Before you can allocate provisioned storage to hosts and cluster, it should be discovered and classified in the VMM fabric:

1. Discover and classify storage > Add and classify block storage devices > Add file storage
2. Allocate block storage to host groups. You can allocate an entire storage pool, or specific logical unit (LUN).
3. Make sure you've completed these steps before you allocate storage to hosts:

MPIO: If you're using fibre channel or iSCSI storage, the Multipath I/O (MPIO) feature must be enabled on each host.

- If MPIO is already enabled before you add the host, VMM will automatically enable it for supported storage arrays using Microsoft DSM. If you have vendor specific DSMs these will be used.
- If you add a host to VMM and enable MPIO later, you need to configure it manually to add the discover device hardware IDs.
- **HBA and zoning**: If you're using Fiber Channel storage array network (SAN), each host must have a host bus adapter (HBA) installed, and zoning must be correctly configured.
- **iSCSI**: If you are using an iSCSI SAN, make sure that iSCSI portals have been added, and that the iSCSI initiator is logged into the array.
- **Storage group**: Explain to your storage administrator how VMM manages storage.

Allocating storage

You can allocate file storage directly to hosts and clusters.

You can add LUNs to hosts and clusters:

If you already provisioned LUNs on a host group, you can assign these to hosts and clusters.

If you provisioned a storage pool on a host group, you can create LUNs during the procedure to add storage to a cluster.

After adding iSCSI storage to a host, you need to create a new session to the storage.

Allocate file storage to a standalone host

You can assign file shares on any host on which you want to create VMs that will use the file share as storage.

1. Click Fabric > **Servers** > **All Hosts**, and select the host or cluster node you want to configure.
2. Click **Host** > **Properties** > **Host Access**. Specify a Run As account. By default the Run If you used a domain account for the VMM service account, add the domain account to the local Administrators group on the file server.

- If you used the local system account for the VMM service account, add the computer account for the VMM management server to the local Administrators group on the file server. For example, for a VMM management server that is named VMMServer01, add the computer account VMMServer01$.
- Any host or host cluster that accesses the SMB 3.0 file share must have been added to VMM using a Run As account. VMM automatically uses this Run As account to access the SMB 3.0 file share.
- If you specified explicit user credentials when you added a host or host cluster, you can remove the host or cluster from VMM, and then add it again by using a Run As account.

3. Click **Host Name Properties** > **Storage** > **Add File Share**.
4. In **File share path**, select the required SMB 3.0 file share, and then click **OK**.
5. To confirm that the host has access, open the **Jobs** workspace to view the job status. Or, open the host properties again, and then click the **Storage** tab. Under **File Shares**, click the SMB 3.0 file share. Verify that a green check mark appears next to **Access to file share**.
6. Repeat this procedure for any standalone host that you want to access the SMB 3.0 file share, or for all nodes in a cluster

Assign a logical unit to a standalone host

Either assign an existing unit, or create a new one and assign it.

1. In **Fabric** > **Servers** > **All Hosts**, right-click the host that you want to configure > **Properties**.

2. If you want to create a new logical unit:

> On the toolbar, next to **Disk**, click **Add**. Next to **Logical unit** click **Create Logical Unit**.

> In Create Logical Unit > **Storage pool** choose the pool from which the create the logical unit. Specify a name (alphanumeric only), a description and the unit size. Click **OK** to finish.

3. To assign an existing logical unit to the host, on the toolbar, next to **Disk**, click **Add**, and select the logical unit you want to assign.

4. In the **Logical unit** list, verify that the logical unit that you just created is selected.

5. In **Format new disk**, if you want to format the disk, select **Format this volume as NTFS volume with the following settings**, and specify the settings. Note that if you select **Force format even if a file system is found** all existing data on the volume will be overwritten.

6. In **Mount Point**, select the mount options. Then click **OK** to assign the logical unit to host.

7. VMM registers the storage logical unit to the host and mounts the storage disk.

8. To configure additional disk settings open Disk Management on the host. To open Disk Management, click **Start**, type **diskmgmt.msc** in the search box, and then press ENTER. The new disk appears in the list of disks as a basic disk.

Configure storage for a Hyper-V cluster

1. Click **Fabric Servers** > **All Hosts**. Right-click the cluster you want to configure > **Properties**. In **Host Cluster Name** > **Properties** click a tab:

> **Available Storage**: for adding available storage, converting available storage to shared storage (CSV), or removing available storage.

> **Shared Volumes**: for adding cluster shared volumes (CSVs), converting CSVs to available storage, or removing CSVs. The cluster must run at least Windows Server 2016 to support CSVs.

2. Configure storage for the host cluster. Note that:

Convert volumes one at a time. After conversion, confirm that the logical unit appears on the **Shared Volumes** tab.

3. When you're ready to commit the changes, click **OK**.

Create an iSCSI session

1. On the target host, in the Services snap-in, make sure that the Microsoft iSCSI Initiator Service is started and set to Automatic.
2. In **Fabric** > **Servers** > **All Hosts Hosts**, right-click the host > **Properties**.
3. Under **iSCSI Arrays**, see if the storage array is already listed. If it is not, on the toolbar, next to **iSCSI Array**, click **Add**.
4. In the Create New iSCSI Session > **Array** , click the storage array you want to use.
5. Click **Create** to create a new session. Click Use advanced settings if you want to modify customized settings, including target listener, name, or the host NIC that you want to use.
6. The array that you added appears under **iSCSI Arrays**. Click the array to view more details.

EXPERIMENT-3

Hyper-V – Creating and configuring virtual networks?

Hyper-V Extensible Switch Types and Use Cases

Hyper-V supports the creation and use of three different Virtual Switch types:

External Virtual Switch

The External Virtual Switch is perhaps the most common switch that is created in the Hyper-V environment. The External Virtual Switch enables connecting virtual machines to the physical network. It allows network traffic to be able to egress from the virtual network out to the physical network connected to the Hyper-V host.

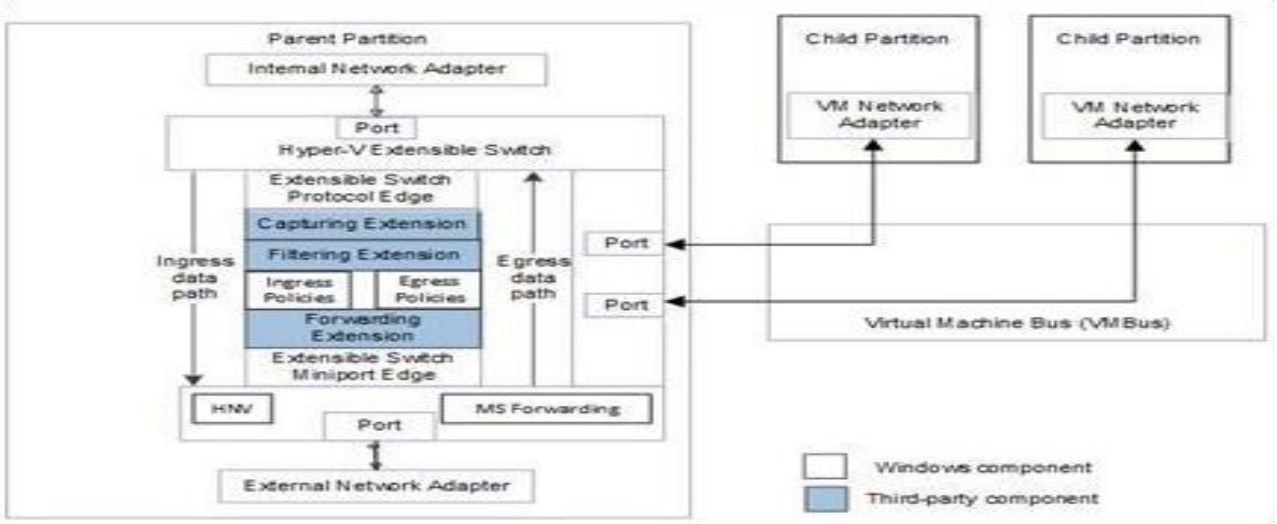
Internal Virtual Switch

The Internal Virtual Switch is a type of switch that allows created isolated virtual network environments on which to place Hyper-V virtual machines. The Internal Virtual Switch is a perfect choice for DEV/TEST/STG environments where entire networks may be simulated for which to house development or other virtual machines that you want to have isolated from production. All the virtual machines that are placed on the Internal Virtual Switch can be communicated to one another.

Private Virtual Switch

The Private Virtual Switch has a very specific purpose. When using this type of Hyper-V Virtual Switch, the host itself is not able to see IP communication

from the VMs that are attached to this type of Virtual Switch Internal and Private Virtual Switches.



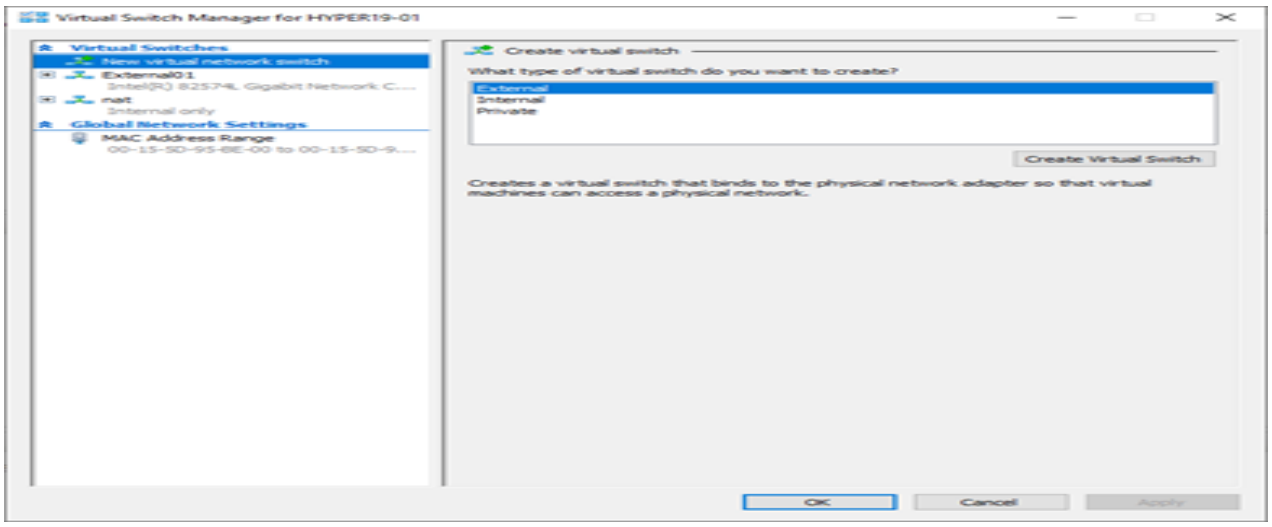
Components of the Hyper-V Extensible Switch in Windows Server 2012 R2 and higher

Converged Networking

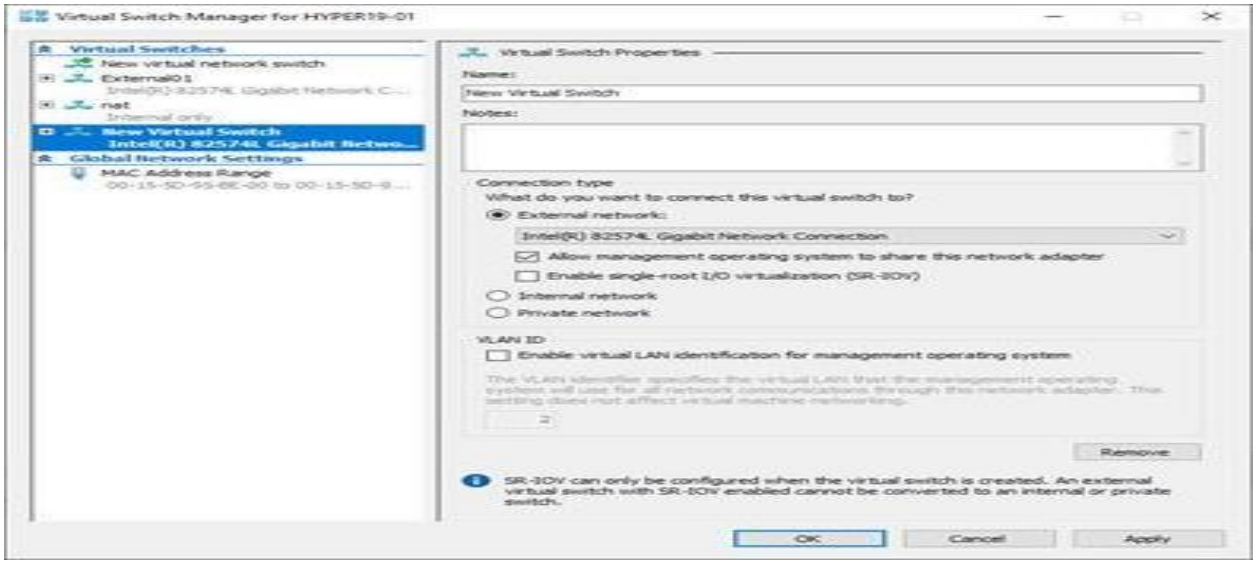
When thinking about the actual physical network adapters that exist on a Hyper-V host, the number of physical connections and uplinks can add up. With Windows Server 2016, Microsoft introduced a new type of supported network configuration from the host side called Converged Network that allows exposing RDMA through a host-partition virtual NIC. This allows the host partition services to access RDMA on the same NICs that are used for Hyper-V guest operating system network communication.

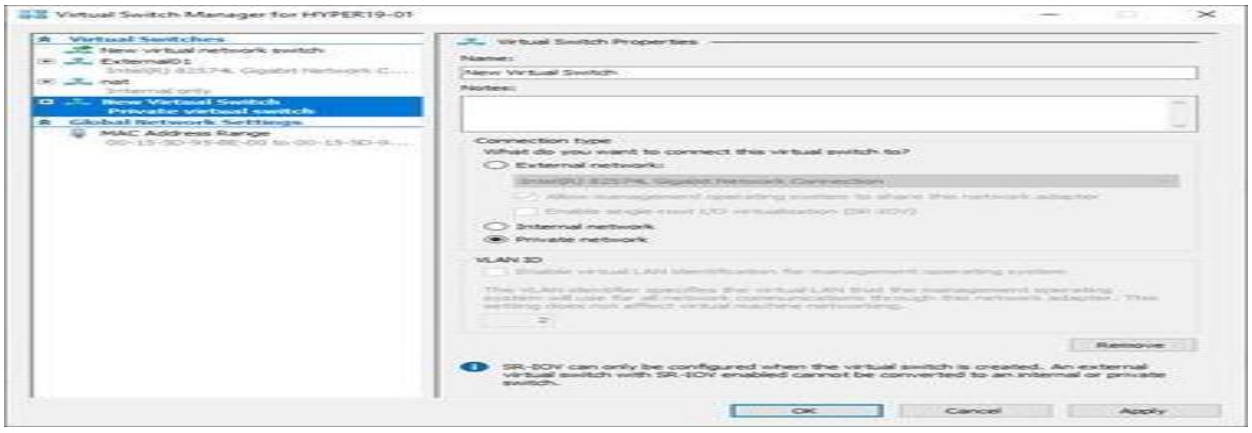
Creating A New Hyper-V Virtual Switch

In the Hyper-V Manager, creating a new Hyper-V Virtual Switch is accomplished in the Virtual Switch Manager found in the Hyper-V Manager utility. As you can see, you have the three different Virtual Switch types available – External, Internal, and Private.



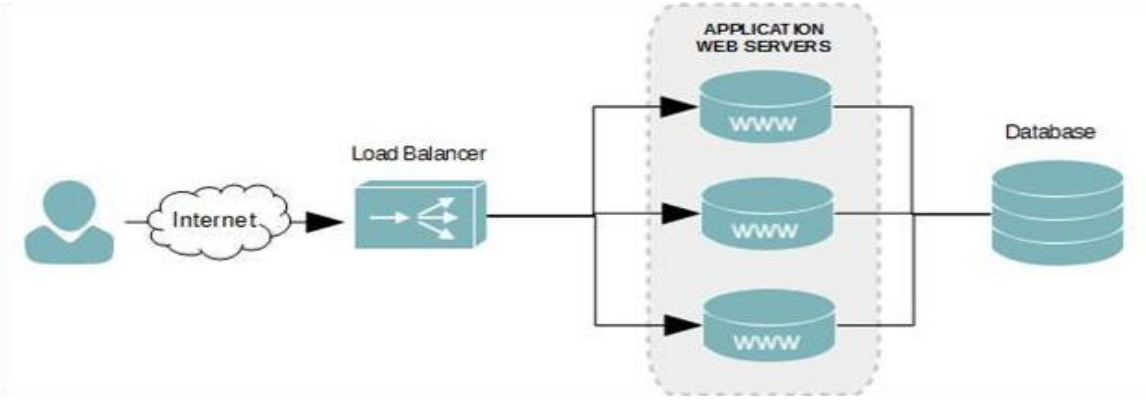
Creating a new virtual switch in Hyper-V using the Hyper-V Switch Manager.





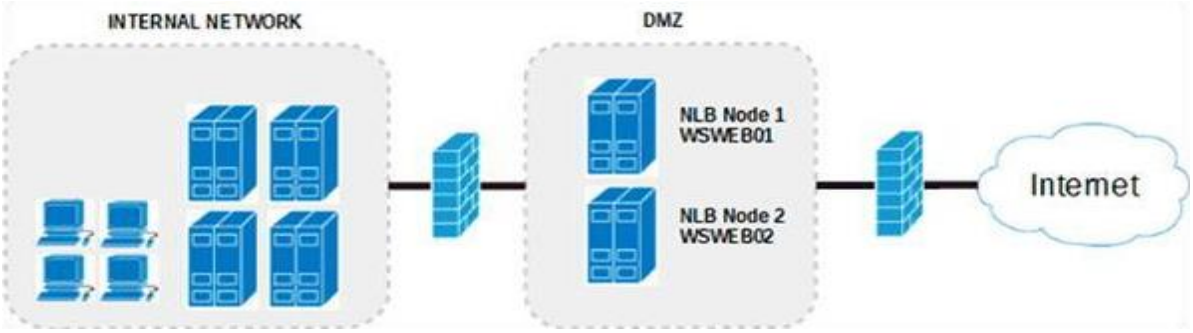
EXPERIMENT-4

Configure network load Balancing(NLB)?



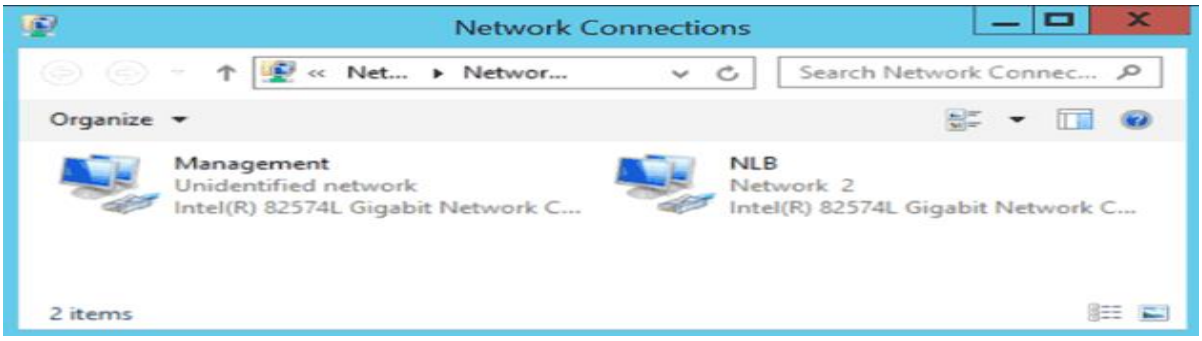
Network Infrastructure Scenario

I will be using the following infrastructure to create a load balanced web server using Microsoft's NLB feature.



Web Servers in a DMZ

The server will have two network interfaces and will be multi-homed. This allows us to dedicate one NIC to server management and the other to our website's Internet traffic. The servers will also reside inside of a DMZ to protect our Internal network.



Windows Server 2012 Network Interfaces

Both network interfaces have been renamed, as can see in the figure above, to make it easier to identify their functions. The Management interface is for internal remote connections, and the NLB is used by the cluster and accessed by users of the web site.

Web Servers

The two web servers will have the following configuration.

Hostname	Mangement NIC	NLB NIC	Role	Cluster	Cluster IP
WSWEB01	172.30.0.100	172.30.1.21	IIS	contoso.com	17.30.1.20
WSWEB02	172.30.0.101	172.30.1.22	IIS		

Multi-homed Network Routing

Our servers are all multi-homed, which means they each connect to two different networks. Since a default gateway can be configured on only one network interface, we need to create custom routes for the other. We'll

assign the default gateway to the Internet facing network interface and create custom routes for our internal network.

Without the custom routes, remote connections from the internal network, such as RDP, will find their way to our web servers; however, connections back to our client computer initiating the RDP session will not be able to find their way back. This, of course, prevents you from logging onto the server or managing it from the Internal network.

1. Open a Command prompt.

2. Run the route command to get the interface index value of the management network interface.

```
route print
```

3. At the beginning of the route command's output, you will see an interface list.

```
4. Microsoft Windows [Version 6.3.9600]

5. (c) 2013 Microsoft Corporation. All rights reserved.

7. C:UsersAdministrator>route print

9.   Interface List

10. 25...02 bf ac 1e 00 82 ......Intel(R) 82574L Gigabit Network Connection
    #2

11. 12...00 0c 29 16 8c 1a ......Intel(R) 82574L Gigabit Network Connection

12. 1...........................Software Loopback Interface 1

13. 13...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter

14. 14...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
```

15. 29...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2

16. By knowing the MAC address of our management network interface, which is **00 0c 29 16 8c 1a**, I've determined the interface index to be 12.

17. In my lab environment, there are three internal subnets that this server may receive a connection from on the management interface. I need to create a route for each of the following subnets.

Subnet	10.4.0.0 /24	10.5.0.0 /24	10.6.0.0 /24
Gateway	172.30.0.1		

18. Each route must be assigned to interface index 12 – our management interface in this tutorial. All routes must go through our gateway at 172.30.0.1. Use the route command to create the routes.

19.route -p add 10.4.0.0 mask 255.255.255.0 172.30.0.1 metric 1 if 12

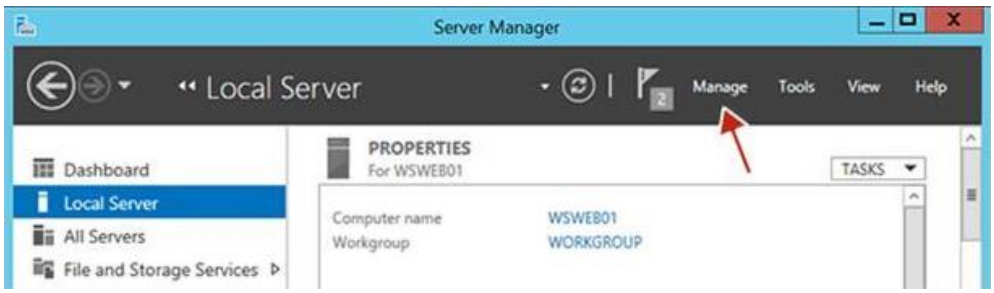
20.route -p add 10.5.0.0 mask 255.255.255.0 172.30.0.1 metric 1 if 12

21.route -p add 10.6.0.0 mask 255.255.255.0 172.30.0.1 metric 1 if 12

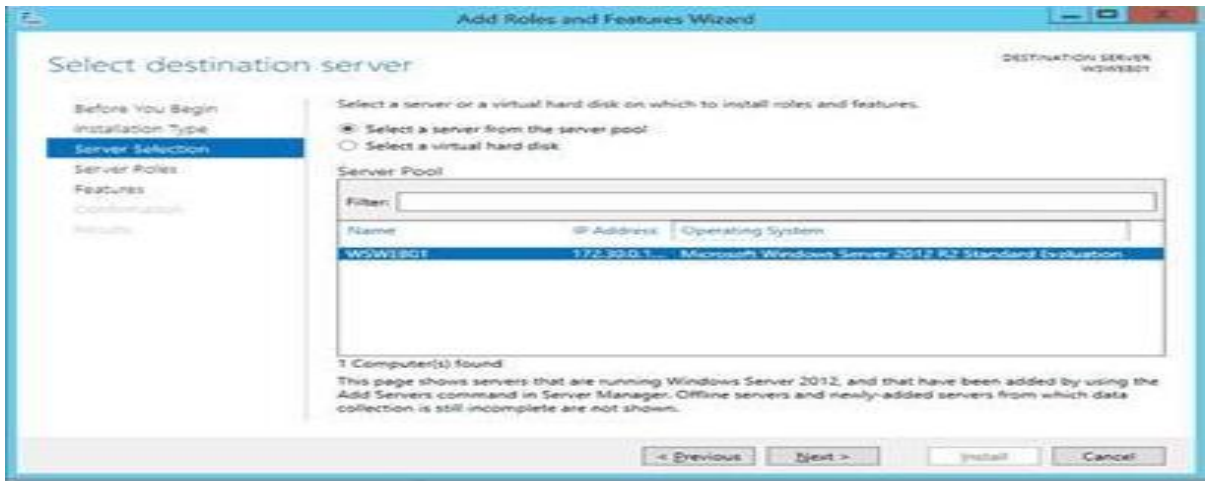
Install the NLB Feature

This step needs to be followed on all servers that will be added to the cluster. Log onto each using an account with administrative rights and follow the instructions below.

Launch Server Manager. > Click **Manage**.



Click **Add New Roles and Features**. > On the **Before you begin** screen, click **Next**. > On the S**elect installation type** screen, select the **Rolebased or Feature-based installation** radio button, and then click **Next**. > On the **Select destination server** screen, ensure the **Select a server from the server pool** radio is selected. Now ensure the current server is selected in the Server Pool.

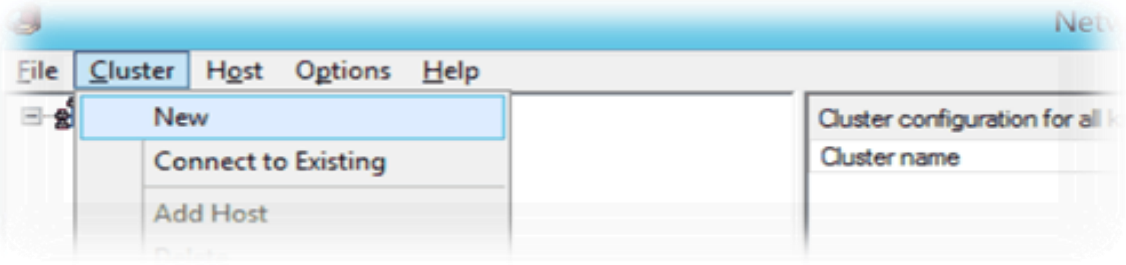


click **Install**. Select destination server > Click **Next**. > On the **Select server roles** screen, click **Next**. > On the **Select features** screen check the N**etwork Load Balancing** checkbox. > Click **Next**. > On the **Confirmation**

Create an NLB Cluster:-

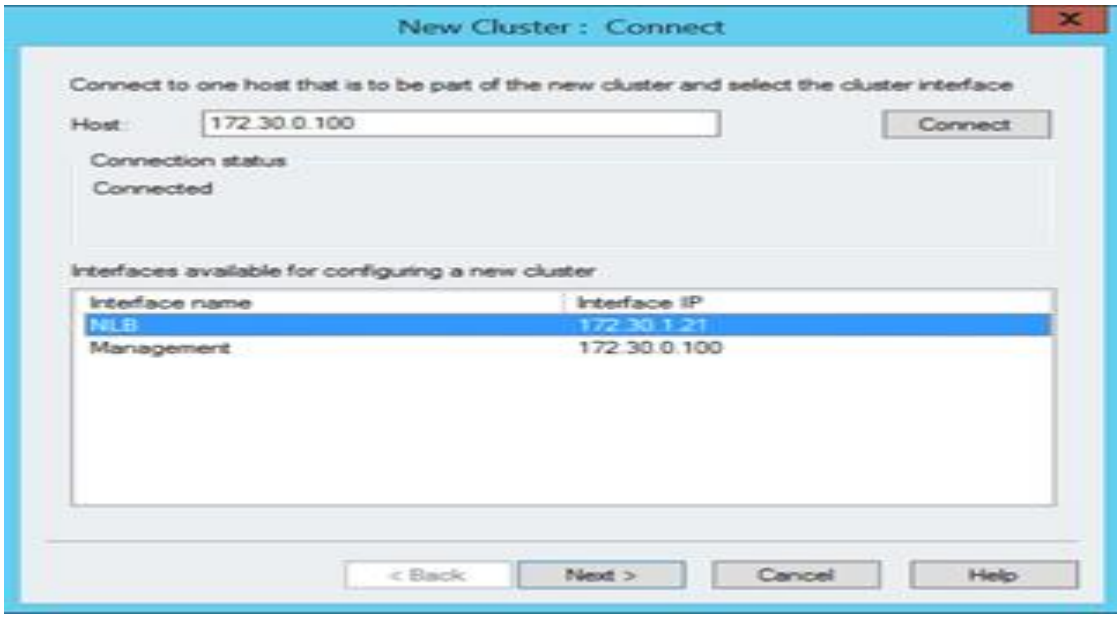
Launch the **Network Load Balancing Manager**. This can be done by clicking the **Tools** menu in the **Server Manager**.

From the top menu of the Network Load Balancing Manager, click **Cluster**, and then click **New**.



In the **Host** text field of the **New Cluster : Connect** dialog box, enter an IP address of the server you are currently logged onto.

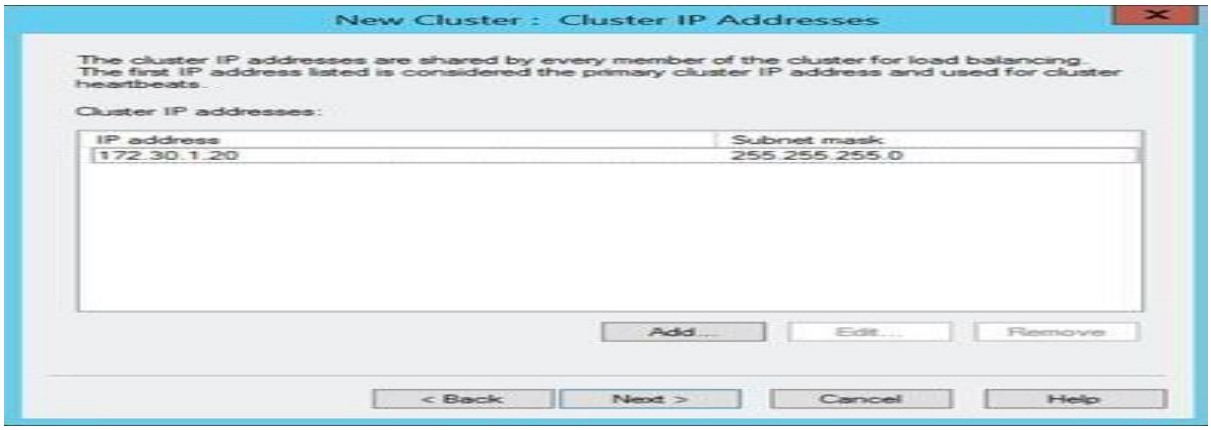
The **Interfaces available for configuring a new cluster** > Select the NLB interface and then click the **Next** button.



In the **New Cluster : Host Parameters** dialog box, click **Next**.

In the **New Cluster : Cluster IP Addresses** dialog bo box, click **Add...**

Enter the IP address and the subnet mask you want to assign to the web server cluster. When done, click **OK**.



Cluster Parameters dia, enter the FQDN you are going to assign to the cluster. > click **Next**.

In the **New Cluster** log box

We are only serving web content over port 80. Let's narrow the port rules down to only accept connections to the cluster over that port. Select the default rule and then click Edit.

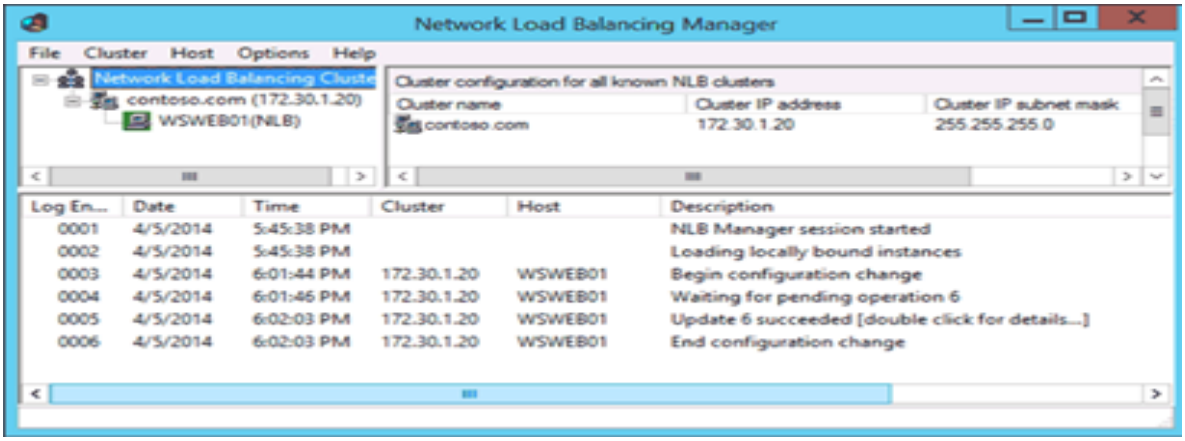
In the **Add/Edit Port Rule** dialog box, uncheck **All** under Cluster IP address. Ensure the IP address we've assign to the cluster is selected in the drop-down menu.

Under Port Range of the **Add/Edit Port Rule** dialog box, enter 80 in both the From and To text fields.

Under Protocols, select **TCP**. For this web balance cluster, we will not need UDP.

Keep the remaining default settings and then click **OK**.

The NLB cluster will now be created with a single node (WSWEB01).

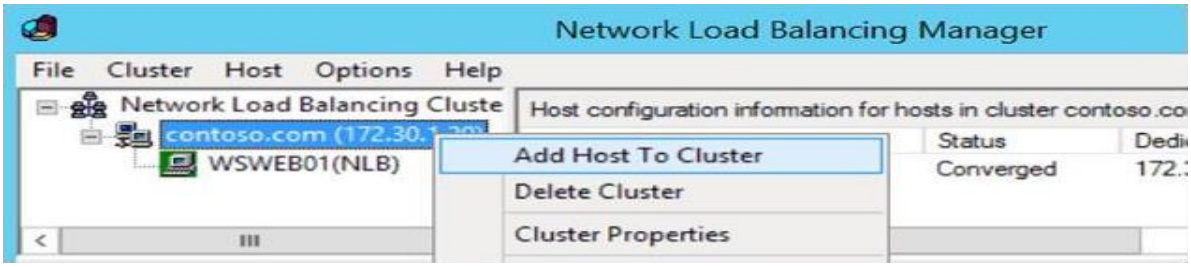


Add the Second Web Server:-

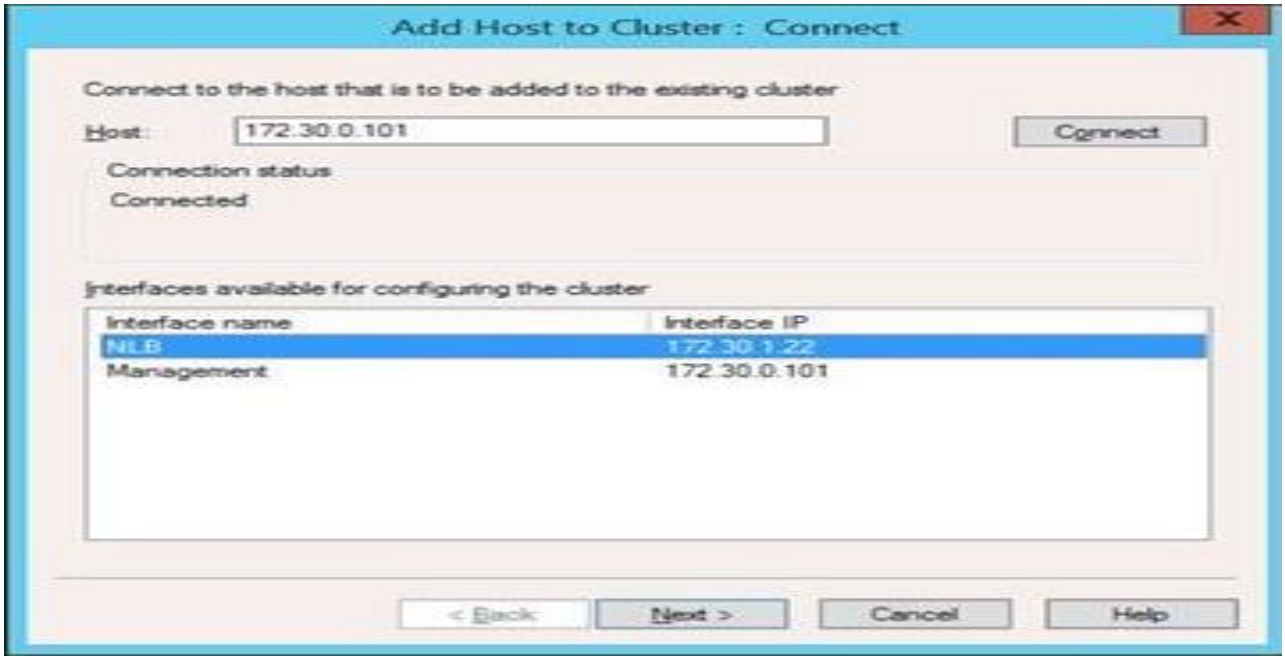
Load balance clusters typically have two or more nodes, and ours is no exception.

In the left tree-view panel of the **Network Load Balancing Manager**, select the name of the cluster we just created (contoso.com).

Right-click the cluster name and click **Add Host to Cluster**.



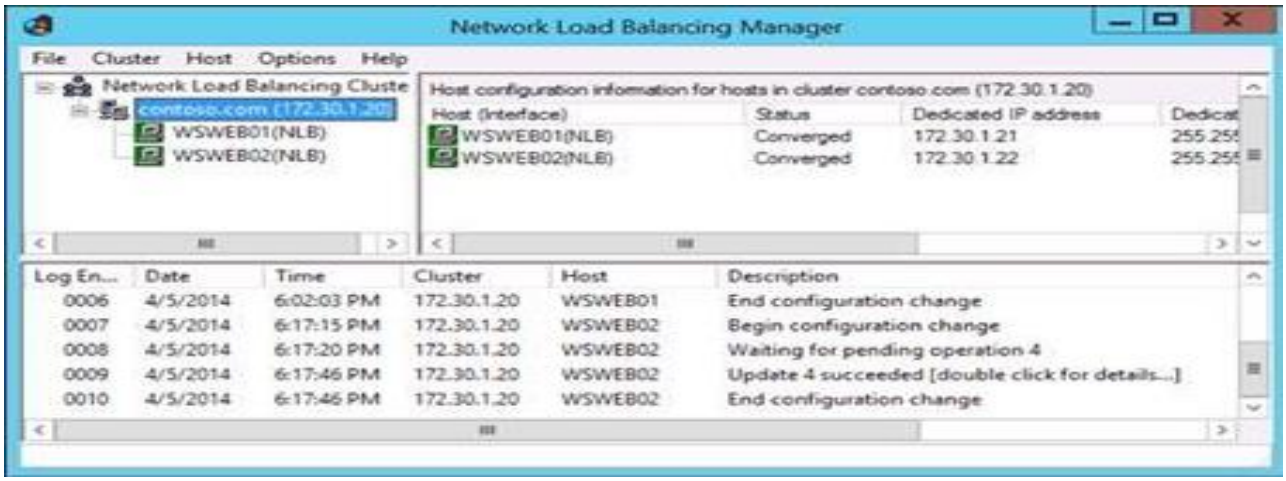
In the **Add Host to Cluster : Connect** dialog box, enter the IP address of the second web server.



5. In the **Add Host to Cluster : Host Parameters** dialog box, use the default values and click **Next**.

6. In the **Add Host to Cluster : Port Rules** dialog box, use the default values and click **Finish**. We've already defined everything when we created the cluster.

7. Our cluster is complete. After a few seconds, ours servers will be converged and be able to server our web application.



EXPERIMENT-7

Configure advanced file services?

You can configure the File Services, which enable you to create file shares on your vSAN datastore. You can enable vSAN File Services on a regular vSAN cluster, a vSAN stretched cluster, or a vSAN ROBO cluster.

Prerequisites

- 4 Core CPU
- 10 GB physical memory

You must ensure to prepare the network as vSAN File Service network:

If using standard switch based network, the Promiscuous Mode and Forged Transmits are enabled as part of the vSAN File Services enablement process. If using DVS based network, vSAN File Services are supported on DVS version 6.6.0 or later. Create a dedicated port group for vSAN File Services in the DVS.

Allocate static IP addresses as file server IPs from vSAN File Service network, each IP is the single point access to vSAN file shares.

For best performance, the number of IP addresses must be equal to the number of hosts in the vSAN cluster.
All the static IP addresses should be from the same subnet.
Every static IP address has a corresponding FQDN, which should be part of the Forward lookup and Reverse lookup zones in the DNS server.

Procedure

1. Navigate to the vSAN cluster and click **Configure** > **vSAN** > **Services**.
2. On the File Service row, click **Enable**.

3. Review the checklist on the Introduction page, and click **Next**.

4. In the File service agent page, select one of the following options to download the OVF file.

5. In the Domain page, enter the following information and click **Next**:

- **File service domain**: The domain name should have minimum two characters. The first character should be an alphabet or a number. The remaining characters can include an alphabet, a number, anunderscore (_), a period (.), a hyphen (-).
- **DNS servers**: Enter a valid DNS server to ensure the proper

EXPERIMENT-8

Configuration of File Services.

- **DNS suffixes**: Provide the DNS suffix that is used with the file services. All other DNS suffixes from where the clients can access these file servers should also be included. File Services does not support DNS domain with single label, such as "app", "wiz", "com" and so on. A domain name given to file services should be of the format this domain.registered root dnsname

AUTO FILL: This option is displayed after you enter the first IP address in the IP address text box. Click the AUTO FIL option to automatically fill the remaining fields with sequential IP addresses, based on the subnet mask and gateway address of the IP address that you have provided in the first row. You can edit the auto filled IP addresses.

LOOK UP DNS: This option is displayed after you enter the first IP address in the IP address text box. Click the LOOK UP DNS option to automatically retrieve the FQDN corresponding to the IP addresses in the IP address column.

Results

The OVF is downloaded and deployed. The file services domain is created and the vSAN file services is enabled. File servers are started with the IP addresses that were assigned during the vSAN File Services configuration process.

- The OVF is downloaded and deployed.
- The file services domain is created and the vSAN file services is enabled.
- The file servers are started with the IP addresses that were assigned during the vSAN File Services configuration process.
- A File Services VM (FSVM) is placed on each host.

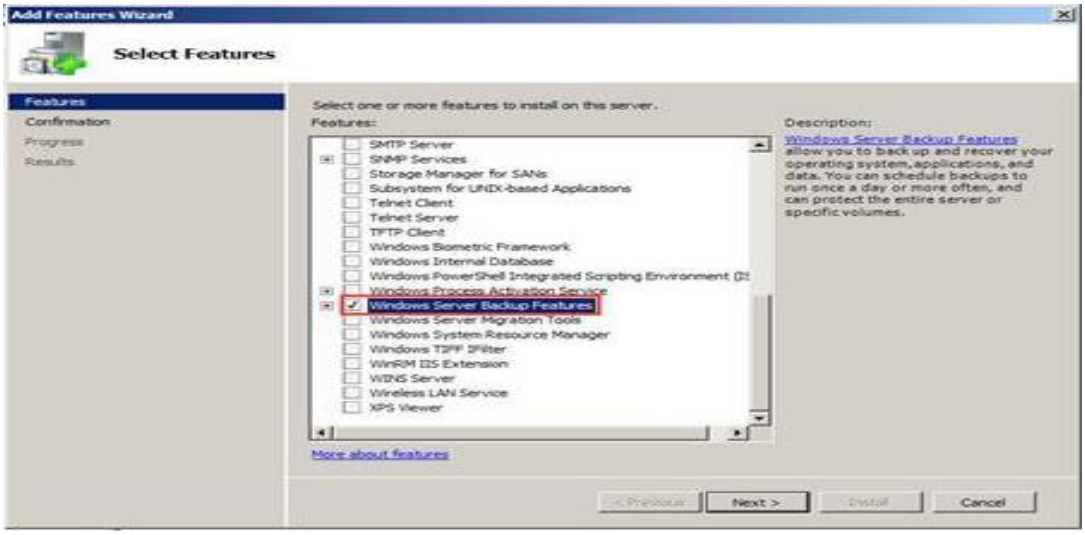
Access Granted!

EXPERIMENT-10

Configuring window server bws backup tool?

Install Windows Server Backup.

1. Open Server Manager.
2. In the pop-up window, choose **Features**.
3. Then click **Add Features** on the right-panel to continue.
4. Next, select the **Windows Server Backup Features** and click **Next**.
5. After that, click **Install**.



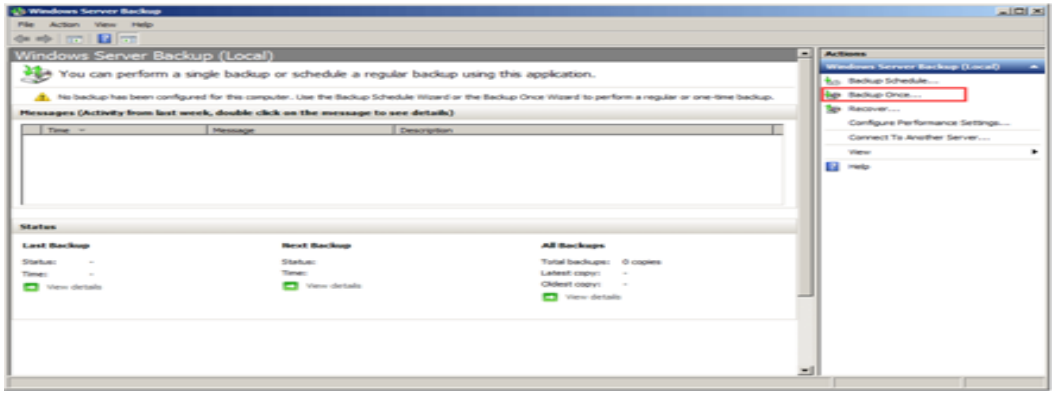
How to Perform Server Backup with Windows Server Backup?

Here, we will show you the step-by-step guide on using Windows Server Backup.

1. Open Run dialog.

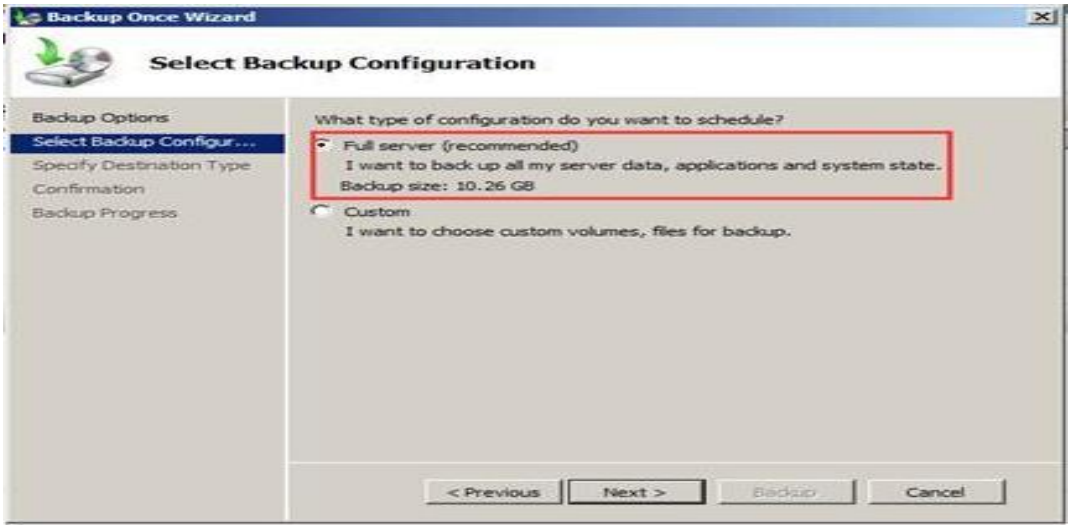
2. Type **wbadmin.msc** in the box and click **OK** to continue.

3. In the pop-up window, choose **Backup Once Wizard** on the right panel to continue.

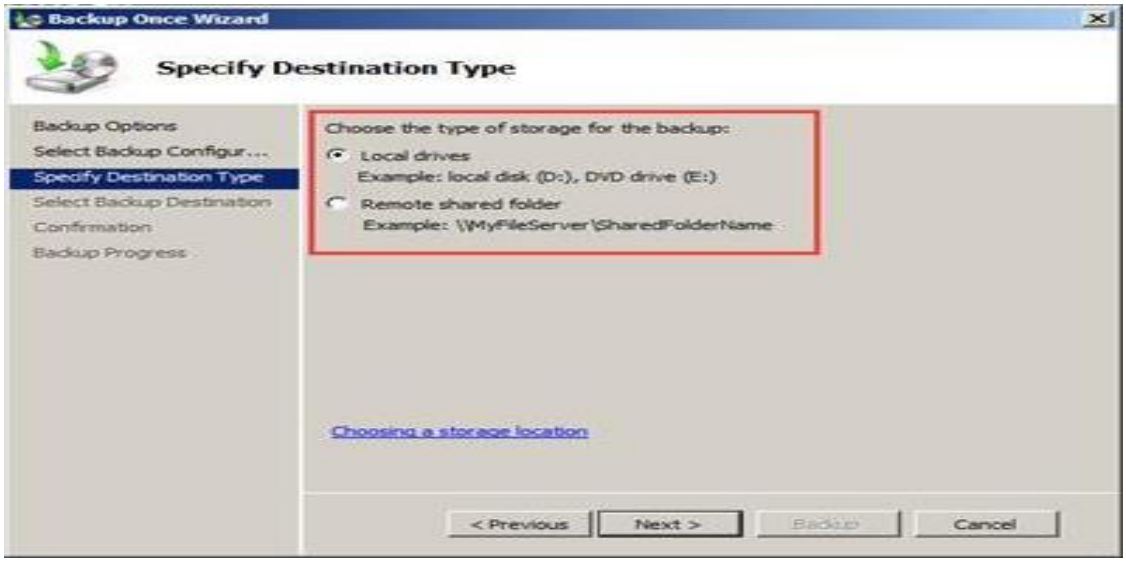


4. Then choose Backup options. Here, you need to choose **Different Options** and click **Next**.

5. Select Backup Configuration. The options include **Full Server: back up all Server data, applications and system state** and **Custom: choose custom volumes, files for backup**. Then click **Next**.

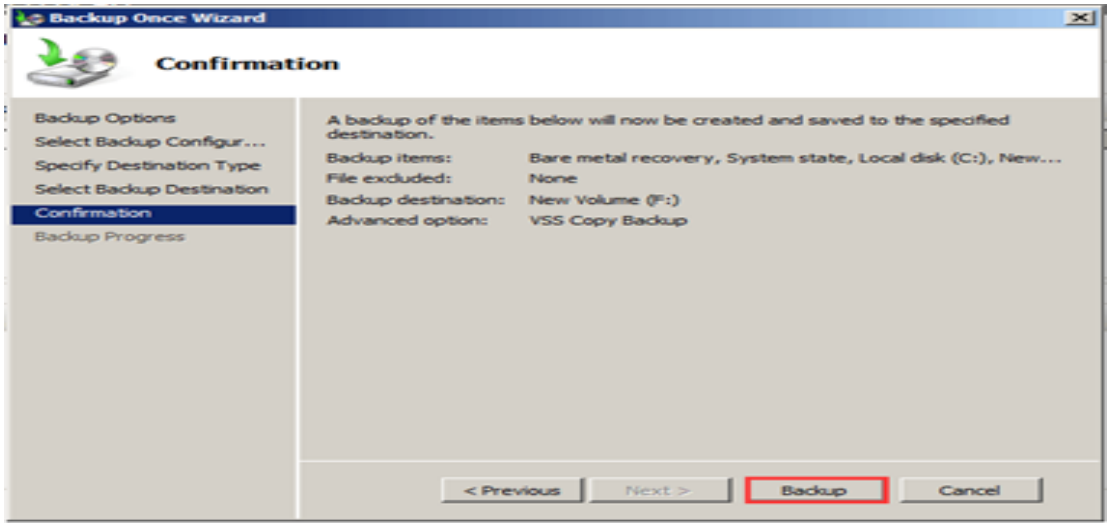


6. Then choose a destination type to save the backups. You can save it to a **local disk** or a remote shared drive. Then click **Next**.



7. If you choose a local drive to save the backup, next, you need to specify which volume to choose. Then click **Next**.

8. After selecting the backup source and destination, you need to confirm the backup settings. Then click **Backup** to start Windows Server backup.

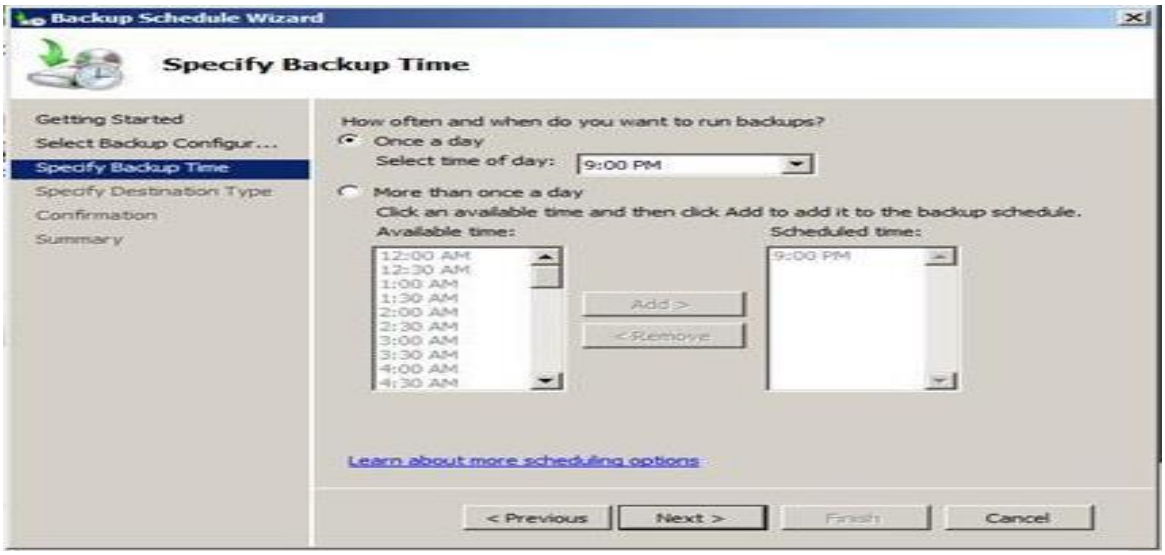


Once all steps are finished, Windows Server Backup software will start to back up the system and you may need to wait for a while for the process to be completed.

How to Perform Schedule Backup with Windows Server Backup?

Now, this part will show you the step-by-step guide on schedule server backup.

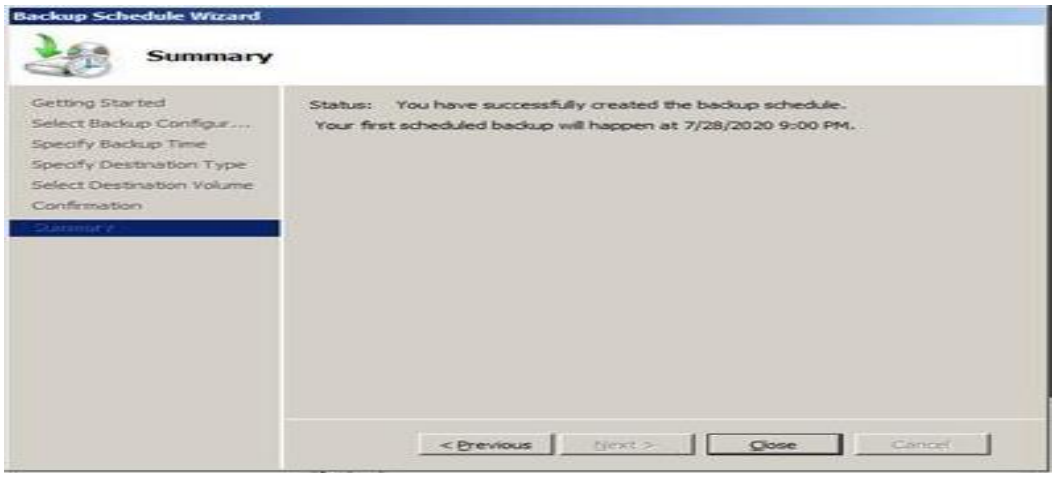
1. Open the Windows Server Backup.
2. Then choose the Backup **Schedule Wizard** on the right panel to continue.
3. Then click **Next**.
4. Next, choose a schedule backup configuration. You can choose either **Full Server** or **Custom**. Then click **Next**.
5. Then choose how often and when you want to run backups. You can select a specific time of a day or choose more than once a day to run backups. Then click **Next**.



6. Next, you are required to choose a destination to save the backup and click **Next**.

7. After that, click **Finish** to continue.

8. Windows Server Backup has successfully created the backup schedule. It will begin to back up Server at the scheduled time. At last, click **Close** to exit the wizard.

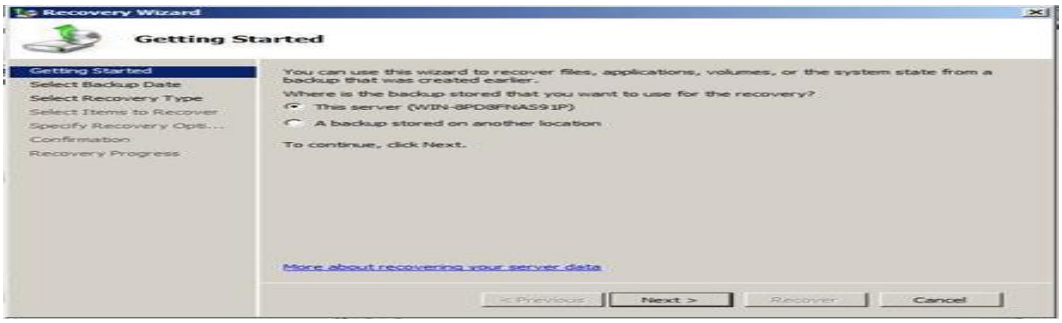


How to Restore from Server Backups?

1. Open Windows Server Backup.

2. Then choose **Recovery Wizard** on the right panel to continue.

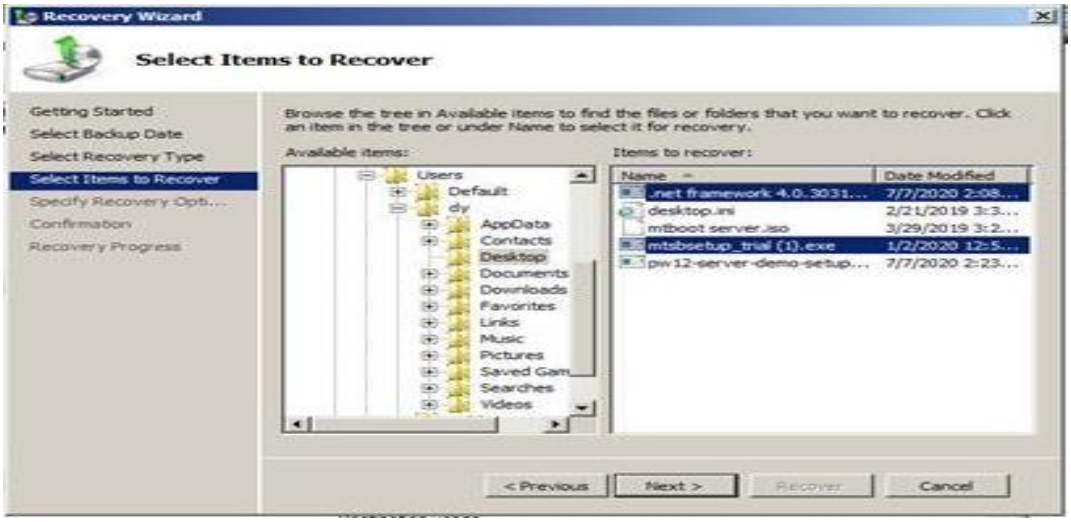
3. Then choose the backup that you want to use for the recovery. You can choose the Server or another backup location and click **Next**.



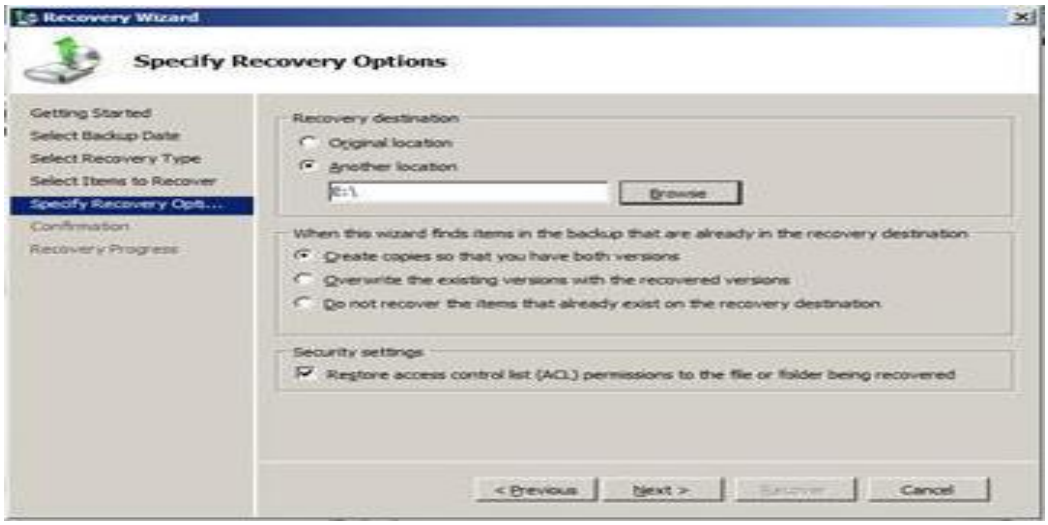
4. Select the backup date. You can choose it according to the backup created time and click **Next**.

5. Then choose what you want to restore. You can choose **Files and Folders**, **restore an entire volume** or **restore system state**.

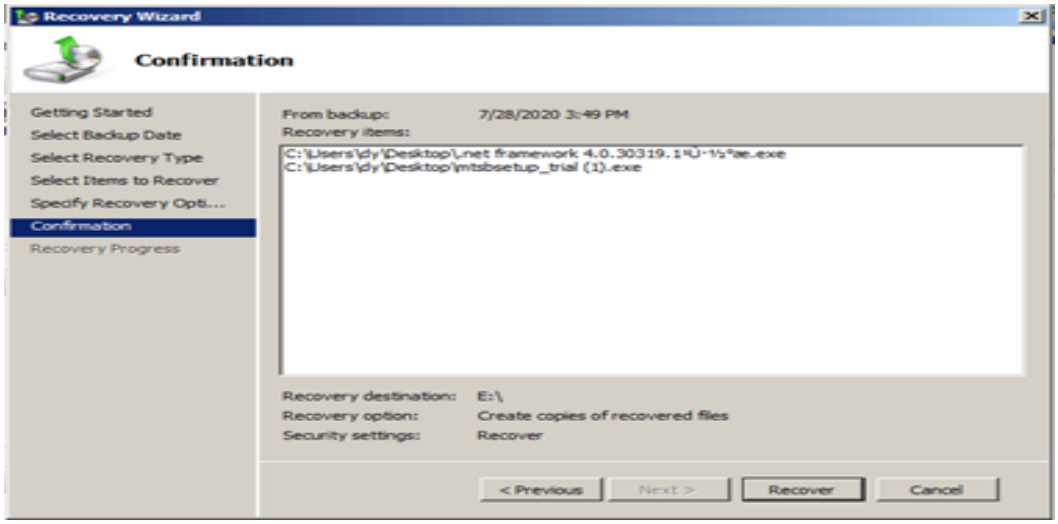
6. Here we show how to restore files and folders as an example. Browse the tree in available items to find the files or folder you want to recover. You can choose one item or choose several items together, then click **Next**.



7. Select a restore destination. You can restore the items to the original location or restore it to another location.



8. Then click **Recover** to start the restoring process.



When this process is finished, you have successfully restored the files and folders.

EXPERIMENT-12

Understanding Windows booting and troubleshooting booting issues?

BIOS phase

To determine whether the system has passed the BIOS phase, follow these steps:

If there are any external peripherals connected to the computer, disconnect them.

Check whether the hard disk drive light on the physical computer is working. If it's not working, this dysfunction indicates that the startup process is stuck at the BIOS phase.

Press the NumLock key to see whether the indicator light toggles on and off. If it doesn't toggle, this dysfunction indicates that the startup process is stuck at BIOS.

If the system is stuck at the BIOS phase, there may be a hardware problem.

Boot loader phase

If the screen is black except for a blinking cursor, or if you receive one of the following error codes, this status indicates that the boot process is stuck in the Boot Loader phase:

Boot Configuration Data (BCD) missing or corrupted

Boot file or MBR corrupted

Operating system Missing

Boot sector missing or corrupted

Bootmgr missing or corrupted

Unable to boot due to system hive missing or corrupted

To troubleshoot this problem, use Windows installation media to start the computer, press Shift + F10 for a command prompt, and then use any of the following methods.

Method 1: Startup Repair tool

The Startup Repair tool automatically fixes many common problems. The tool also lets you quickly diagnose and repair more complex startup problems. When the computer detects a startup problem, the computer starts the Startup Repair tool. When the tool starts, it performs diagnostics. These diagnostics include analyzing startup log files to determine the cause of the problem. When the Startup Repair tool determines the cause, the tool tries to fix the problem automatically.

To do this task of invoking the Startup Repair tool, follow these steps.

On the Install Windows screen, select Next > Repair your computer.

On the Choose an option screen, select Troubleshoot.

On the Advanced options screen, select Startup Repair.

After Startup Repair, select Shutdown, then turn on your PC to see if Windows can boot properly.

The Startup Repair tool generates a log file to help you understand the startup problems and the repairs that were made. You can find the log file in the following location:

%windir%\System32\LogFiles\Srt\Srttrail.txt

For more information, see Troubleshoot blue screen errors.

Method 2: Repair Boot Codes

To repair boot codes, run the following command:

BOOTREC /FIXMBR

BOOTREC /FIXBOOT

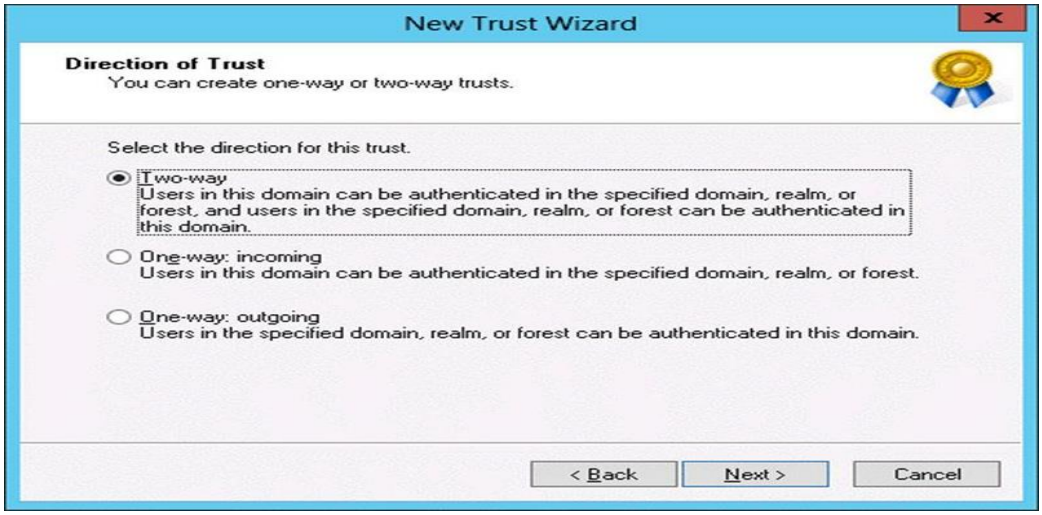
EXPERIMENT-14

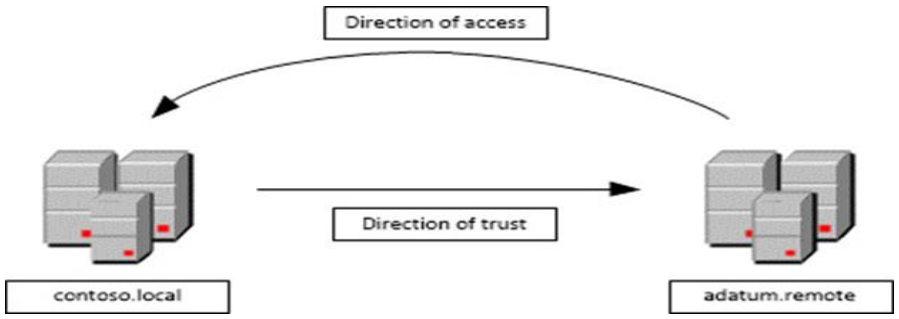
Active Directory Forest trust relationship?

Trust transitivity

Trust direction

When you create a new trust, you specify a trust direction You can choose a two-way (or bidirectional) trust or a unidirectional trust, which is either oneway incoming or one-way outgoing.



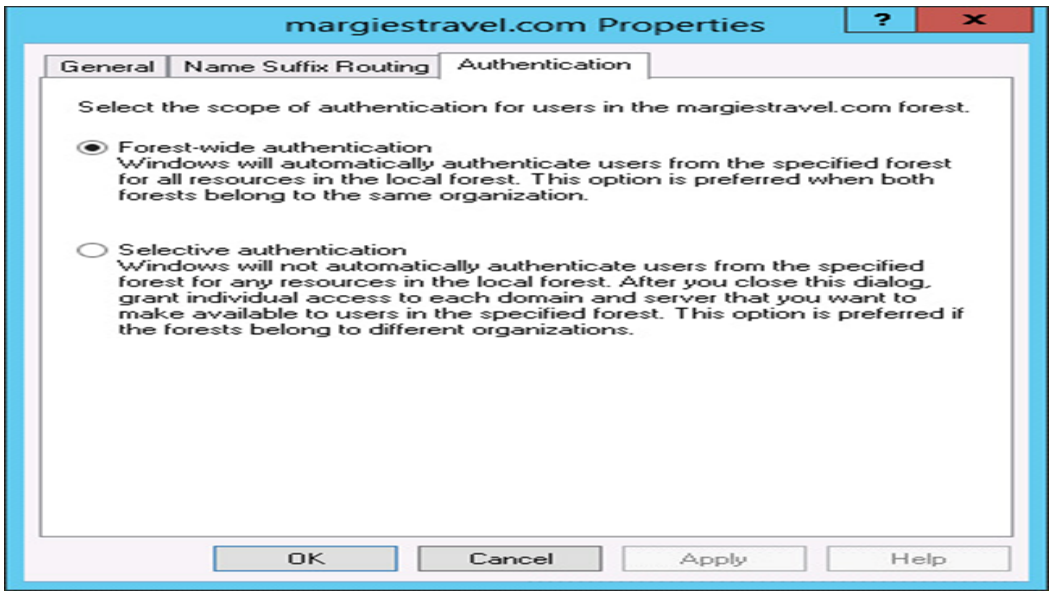


Forest trusts

When you configure a forest trust, one Active Directory forest trusts the other one. Forest trusts are transitive. When you configure a forest trust, you can allow any domain in the trusting forest to be accessible to any security principal in the trusted forest. Forest trusts require that each forest be configured to run at the Windows Server 2003 forest functional level or higher. Forest trusts can be bidirectional or unidirectional. You are most likely

to configure forest trusts if your organization has two or more Active Directory forests.

Forest-wide authentication When you choose forest-wide authentication, users from the trusted forest are automatically authenticated for all resources in the local forest. You should use this option when both the trusted and trusting forests are part of the same organisation. Figure 1-8 shows a forest trust configured with this type of authentication.

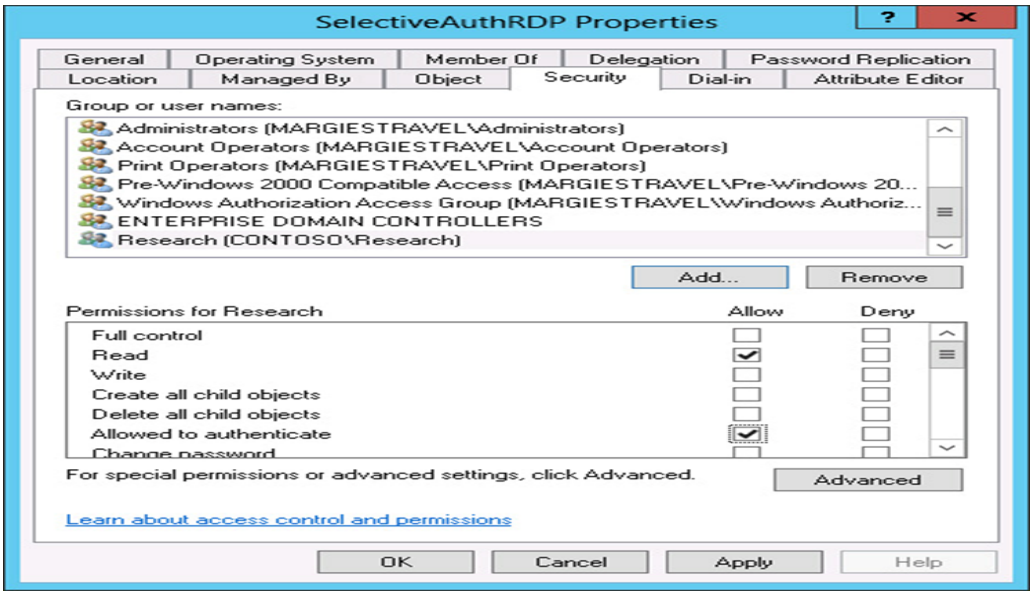


Selective authentication When you configure this option, Windows does not automatically authenticate users from the trusted forest. You can then configure specific servers and domains within the forest to allow users from the trusted forest to authenticate. Use this option when the two forests are from different organizations, or you have more stringent security requirements.

Configuring selective authentication

Configuring selective authentication means granting specific security principals in the trusted forest the Allowed to authenticate (allow) permission on the computer that hosts the resource to which you want to grant access. For example, assume you had configured a forest trust with selective authentication. You want to grant users in the Research universal group from the trusted forest access to a Remote Desktop Services (RDS) server in the trusting forest. To accomplish this goal, you can configure the properties of

the RDS server's computer account in Active Directory Users and Computers and grant the Research universal group from the trusted forest the Allowed to authenticate permission as shown in Figure 1-9. Doing this only allows users from this group to authenticate; you still have to grant them access to RDS by adding them to the appropriate local group on the RDS server.

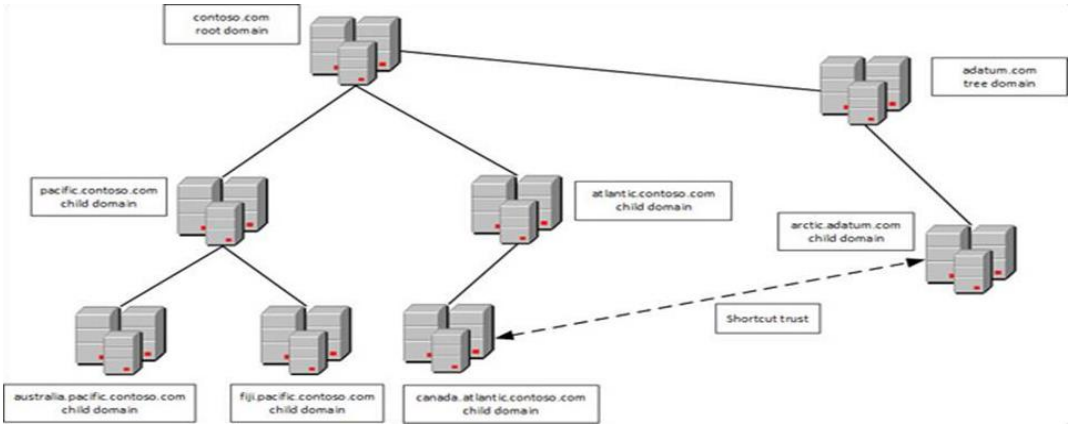


External trusts

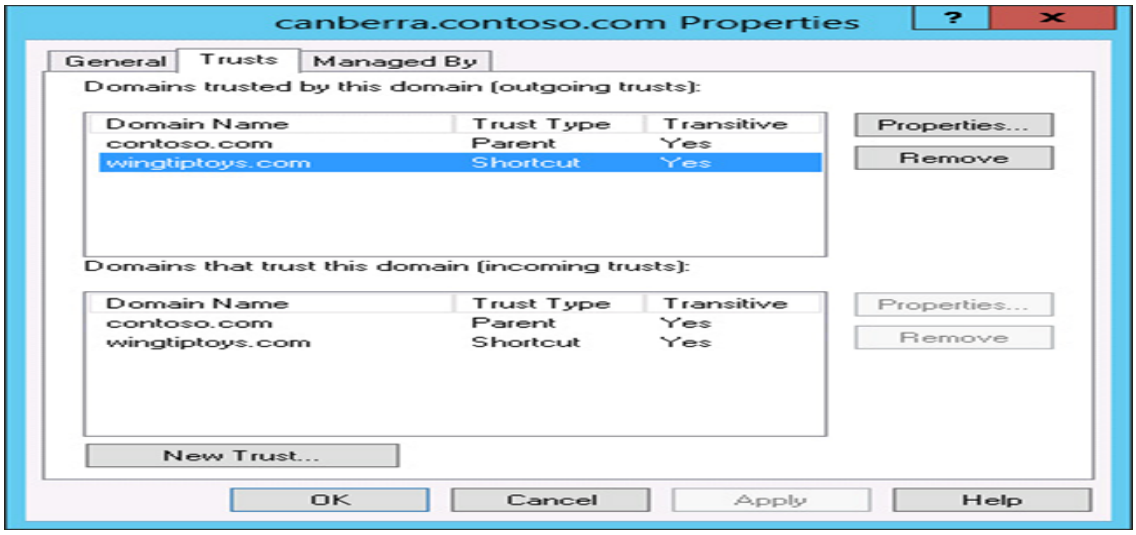
External trusts enable you to configure one domain in one forest to trust a domain in another forest without enabling a transitive trust.

Shortcut trusts

Shortcut trusts enable you to speed up authentication between domains in a forest that might be in separate branches or even separate trees.

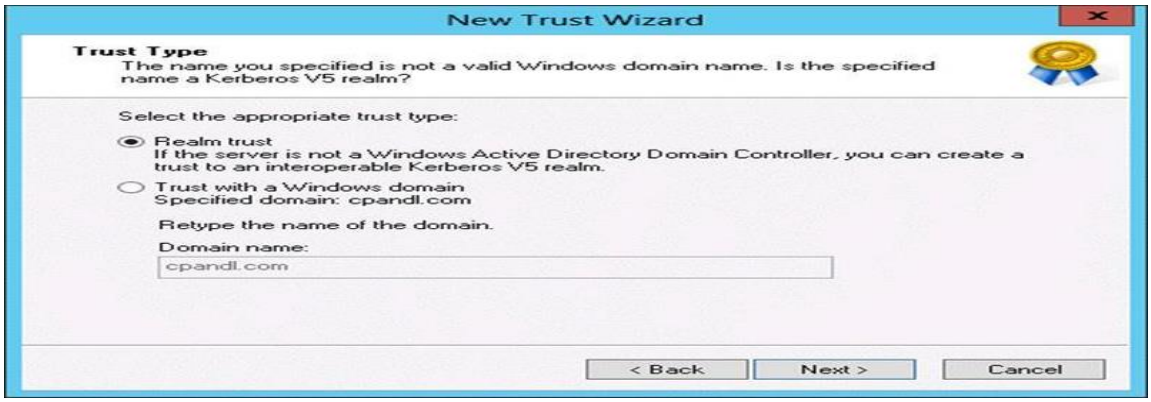


.



Realm trusts

You use a realm trust to create a relationship between an Active Directory Services domain and a Kerberos V5 realm that uses a third-party directory service. Realm trusts can be transitive or intransitive. They can also be unidirectional or bidirectional. You're most likely to configure a realm trust when you need to allow users who use a UNIX directory service to access resources in an Active Directory domain or users in an Active Directory domain to access resources in a UNIX Kerberos V5 realm.



EXPERIMENT-16

Active Directory Certificate services?

Active Directory Certificate Services (AD CS) is one of the server roles introduced in Windows Server 2008 that provides users with customizable services for creating and managing **Public Key Infrastructure (PKI)** certificates, which can be used for **encrypting** and digitally signing electronic documents, emails, and messages.

The applications supported by AD CS are secure wireless networks, Virtual Private Networks (VPN), Internet Protocol Security (IPSec), Network Access Protection (NAP), Encrypting File Systems (EFS), smart card logon, and more.

There are many features of AD CS, including:

1. **Certificate Authority (CA):** The **Certificate Authority** in AD CS is mainly concerned with managing and issuing public-key certificates. Multiple CAs can be linked to form a PKI. A typical PKI is a combination of software, hardware, standards, services, and policies to manage the digital certificates used in a PKI. A CA can be of two types:
2. **Certification Authority Web Enrollment:** The CA Web Enrollment in AD CS permits external clients, who are not part of the domain network, to connect to the CA via an Internet browser. CA Web Enrollment only supports interactive requests that the requester makes and uploads manually through the site.
3. **Online Responder:** The Online Responder is a Microsoft Windows Service that runs on the OCSP server with Network service privileges. In AD CS, the

online responder receives and processes requests regarding the status of the certificates.

4. **Network Device Enrollment Service:** The **Network Device Enrollment Service (NDES)** is a function of AD CS that has the ability to issue certificates to network devices managing traffic such as routers, firewalls, and switches. These devices are not Active Directory domain members and therefore don't possess exclusive Active Directory credentials. NDES enables one-time enrollment passwords for these network devices. These password requests are then sent to the CA for processing and the certificates obtained from the CA are forwarded to the device. Thus, NDES is used by the administrators for authentication of such networking devices.
5. **Certificate Enrollment Web Service:** The Certificate Enrollment Web Service in AD CS permits users and computers to enroll and renew certificates using the HTTPS protocol.

EXPERIMENT-17

Active Directory Rights Management Services (ADRMS)?

Installing AD RMS

The following steps illustrate how to install AD RMS:

✓ Go to Start Menu → **Administrative Tools** → **Server Manager**

✓ Click **Add Roles** and check the **Active Directory Rights Management Services** box from the list of server roles. Click on **Add Required Role Services** in the **Add Roles Wizard**, to proceed and click **Next**.

✓ In the left pane, select **AD RMS Cluster** to create one. Click **Next**.

✓ Select **Cluster Key Storage** and choose the **Use AD RMS centrally managed key storage** option and enter a Cluster Key Password.

✓ For **Cluster Address**, select **Use an SSL-encrypted connection** and mention the FQDN and click **Validate**.

✓ For **Server Authentication Certificate for SSL Encryption**, select **Choose an existing certificate for SSL encryption**

✓ Finally, under **SCP Registration**, choose **Register the AD RMS service connection point now** option and click **Next** on the window that follows.

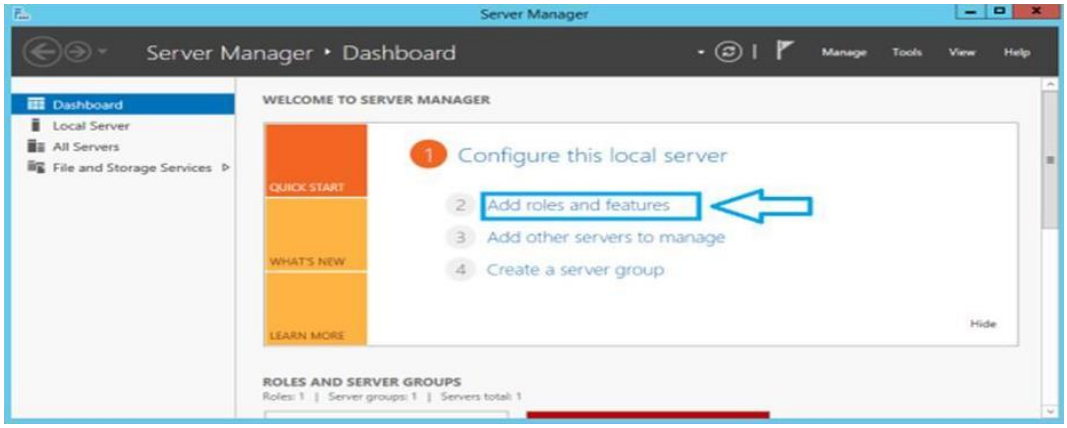
EXPERIMENT-18

Configuring CA backup and recovery?

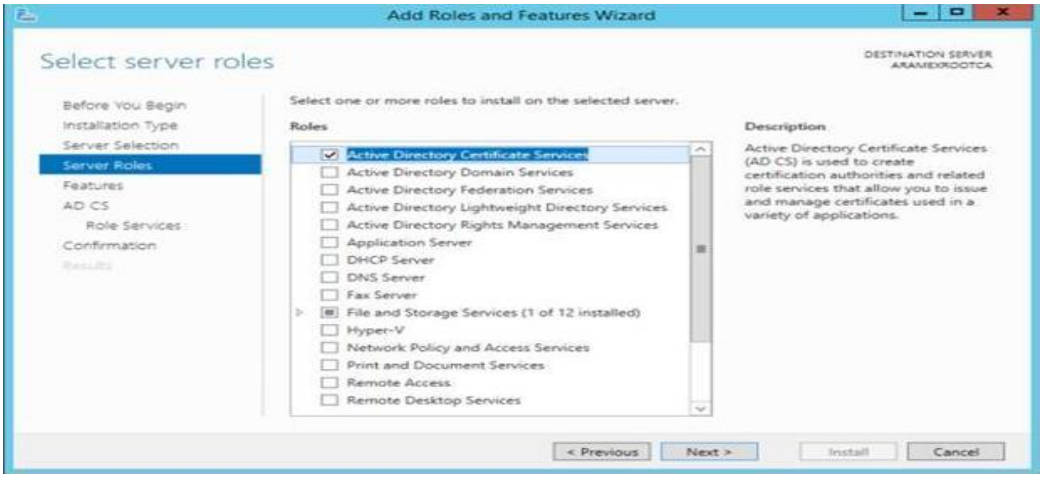
Backup and Restore Root CA to Windows 2012 R2 We may sometimes need to move/recover/upgrade Root CA due to OS corruption/upgradation or other requirements. It could be a tricky task since we need to retain the Private Key of Root CA otherwise it would create a problem of issued Certificates and our organisation may face issues without root ca.

Backup Old Root CA

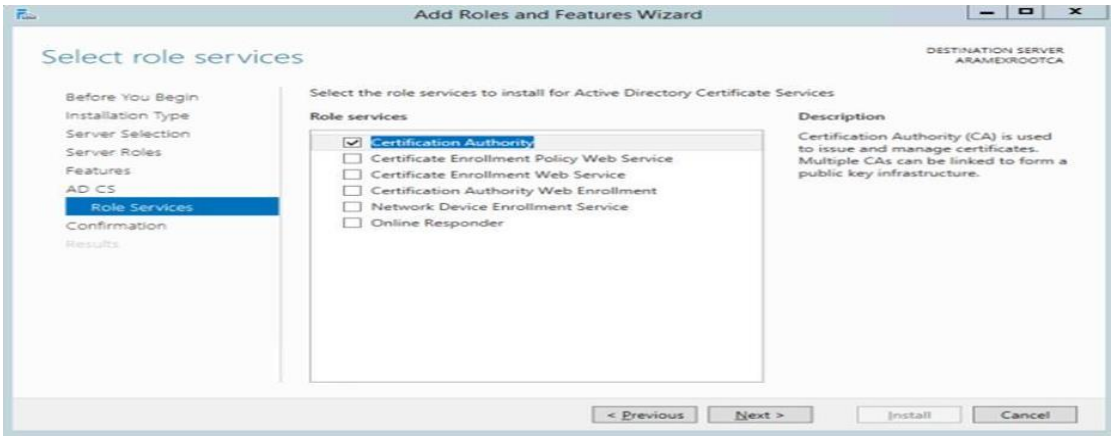
- Log on to your root CA, open the Certificate Authority console. ● Right click the CA name and go to All Tasks > Back up CA.



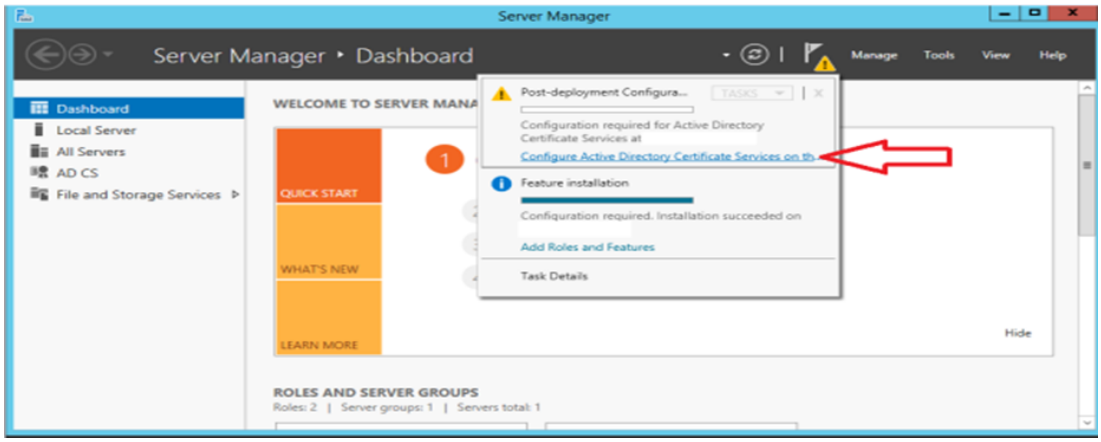
- Click Active Directory Certificate Services.



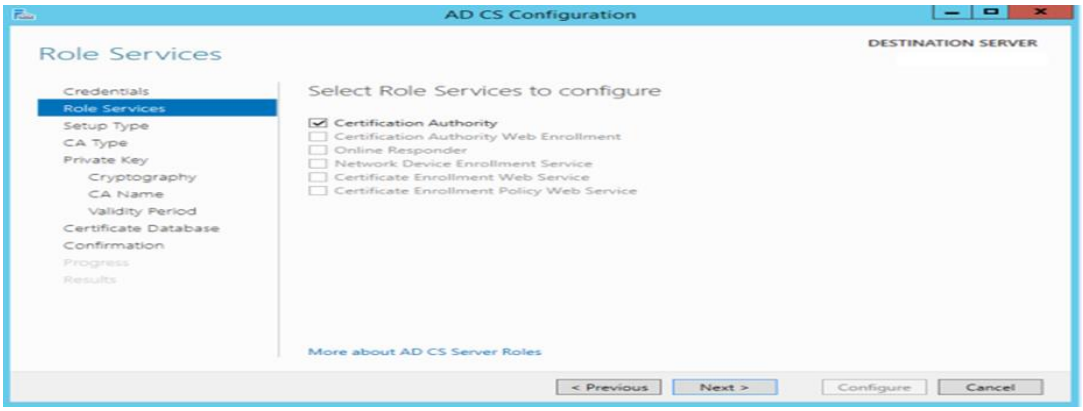
- Since this is Root CA, only pick the Certificate Authority role service. Complete the wizard till the end.

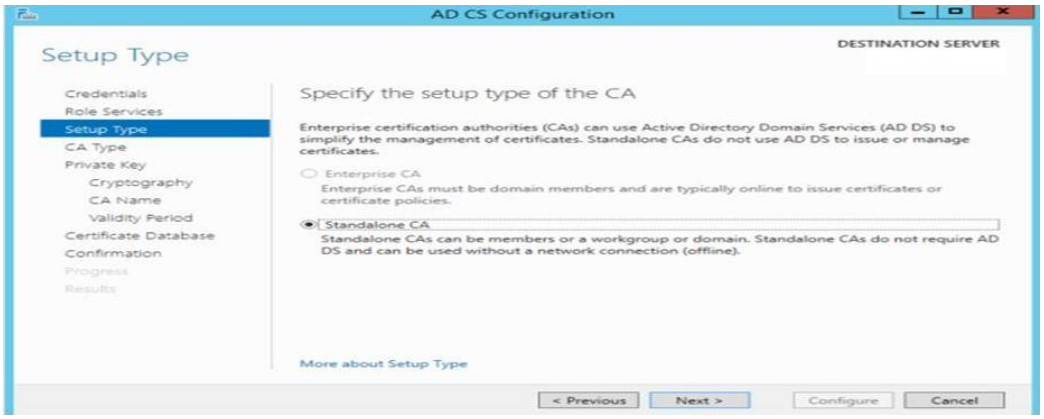


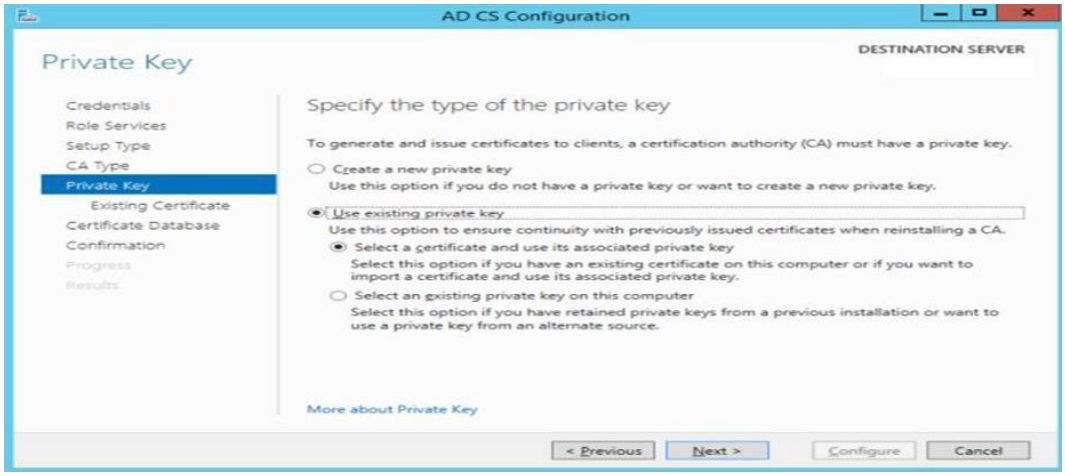
- Go to Server Manager again, click the flag icon that has a warning sign on it, and choose to Configure Active Directory Certificate Services.



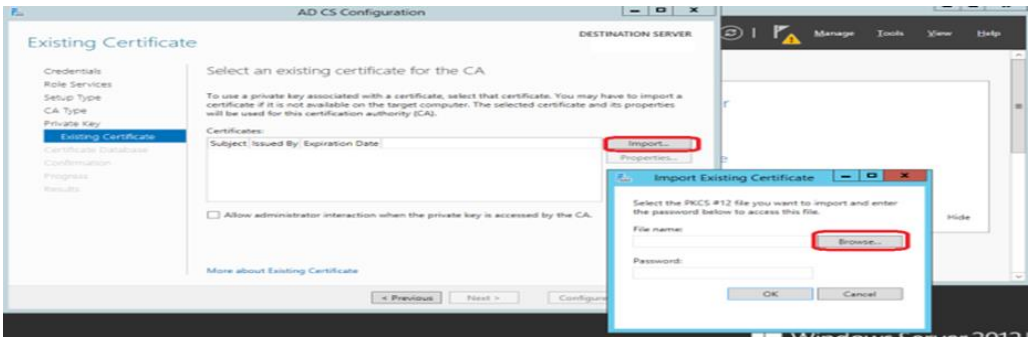
- Select Certification Authority for services to configure.



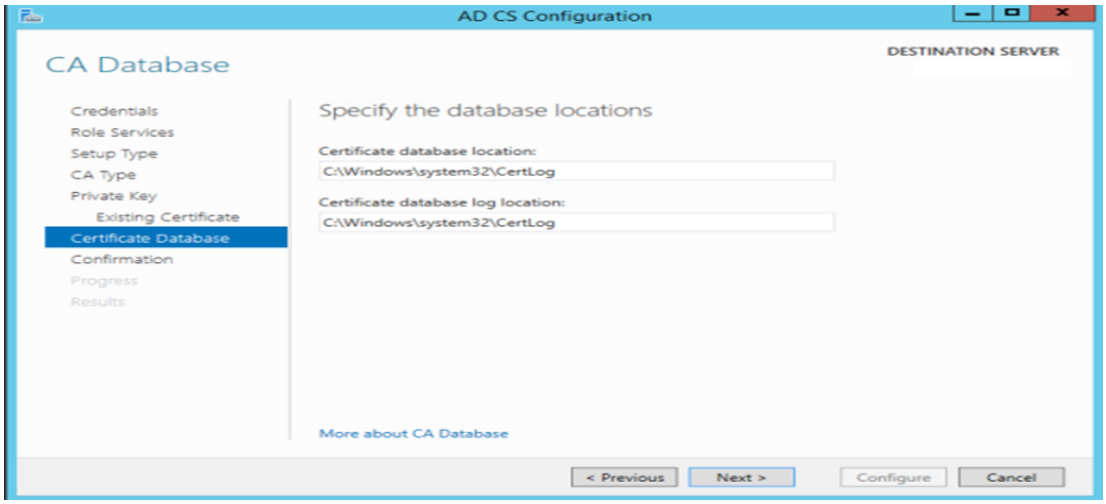


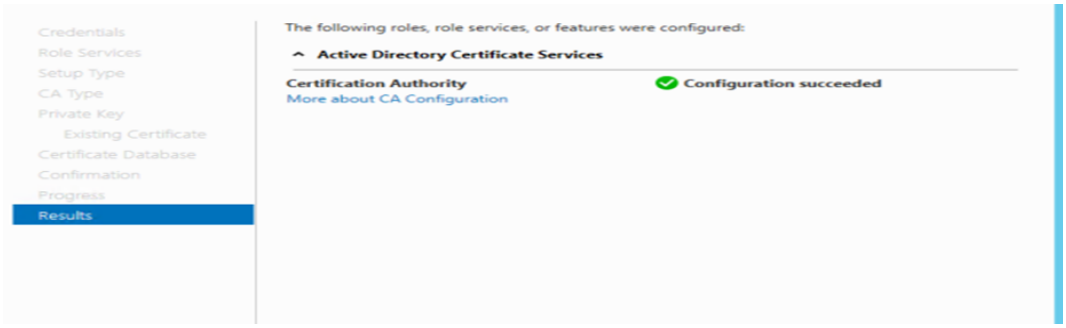


- In this step, you have to choose the old Root CA private key file that you have from your backup.

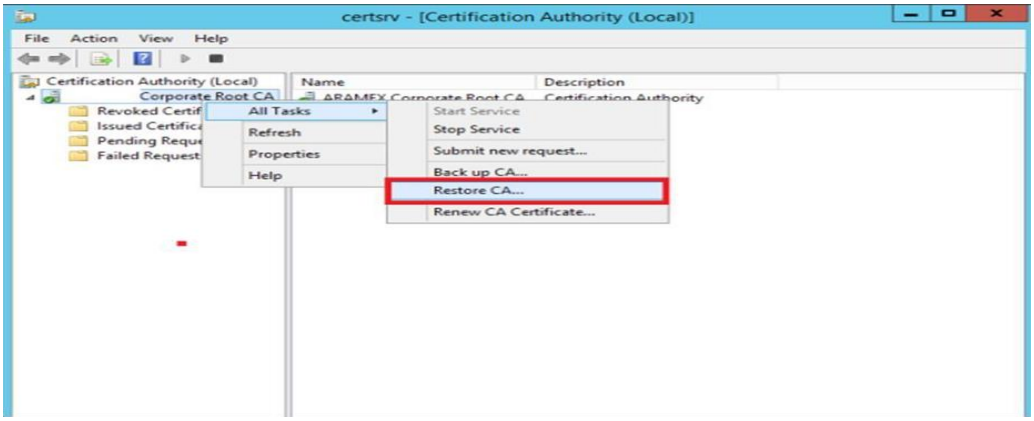


- In the Certificate Database location page, make sure to choose the same location the old Root CA has. Pre-create folders if you are using custom locations.





- Open the Certification Authority Console. Right click the CA name, and choose All Tasks > Restore CA.



- Choose only Certificate database and certificate database log. No need to choose Private key and CA certificate as this was restored during the installation.

EXPERIMENT-19

Design an automated server installation strategy?

Install MDT

MDT installation requires the following:

The Windows ADK for Windows 10 (installed in the previous procedure)

Windows PowerShell (version 5.1 is recommended; type $host to check)

Microsoft .NET Framework

On MDT01:

Visit the MDT resource page and click Download MDT.

Save the MicrosoftDeploymentToolkit_x64.msi file to the D:\Downloads\MDT folder on MDT01.

Note: As of the publishing date for this guide, the current version of MDT is 8456 (6.3.8456.1000), but a later version will also work.

Install MDT (D:\Downloads\MDT\MicrosoftDeploymentToolkit_x64.exe) with the default settings.

Create the OU structure

Switch to DC01 and perform the following procedures on DC01:

To create the OU structure, you can use the Active Directory Users and Computers console (dsa.msc), or you can use Windows PowerShell.

Copy the following list of OU names and paths into a CSV file and save it as ~\Setup\Scripts\oulist.csv.csv

Copy

OUName,OUPath

Contoso,"DC=CONTOSO,DC=COM"

Accounts,"OU=Contoso,DC=CONTOSO,DC=COM"
Computers,"OU=Contoso,DC=CONTOSO,DC=COM"

Groups,"OU=Contoso,DC=CONTOSO,DC=COM"

Admins,"OU=Accounts,OU=Contoso,DC=CONTOSO,DC=COM"

Service Accounts,"OU=Accounts,OU=Contoso,DC=CONTOSO,DC=COM"

Users,"OU=Accounts,OU=Contoso,DC=CONTOSO,DC=COM"

Servers,"OU=Computers,OU=Contoso,DC=CONTOSO,DC=COM"

Workstations,"OU=Computers,OU=Contoso,DC=CONTOSO,DC=COM"

Security Groups,"OU=Groups,OU=Contoso,DC=CONTOSO,DC=COM"

Next, copy the following commands into a file and save it as ~\Setup\Scripts\ou.ps1. Be sure that you are viewing file extensions and that you save the file with the .ps1 extension.

PowerShell

Copy

```
Import-CSV -Path $home\Setup\Scripts\oulist.csv | ForEach-Object {
        New-ADOrganizationalUnit -Name $_.ouname -Path $_.oupath
 Write-Host -ForegroundColor Green "OU $($_.ouname) is created in the location $($_.oupath)"
}
```

Lastly, open an elevated Windows PowerShell prompt on DC01 and run the ou.ps1 script:

PowerShell

Copy

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Force
Set-Location $home\Setup\Scripts
```

.\ou.ps1

This will create an OU structure as shown below.

OU structure.

To use the Active Directory Users and Computers console (instead of PowerShell):

On DC01:

Using the Active Directory Users and Computers console (dsa.msc), in the contoso.com domain level, create a top-level OU named Contoso.

In the Contoso OU, create the following OUs:

Accounts

Computers

Groups

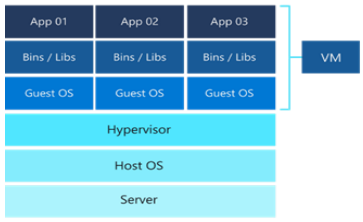
In the Contoso / Accounts OU, create the following underlying OUs:

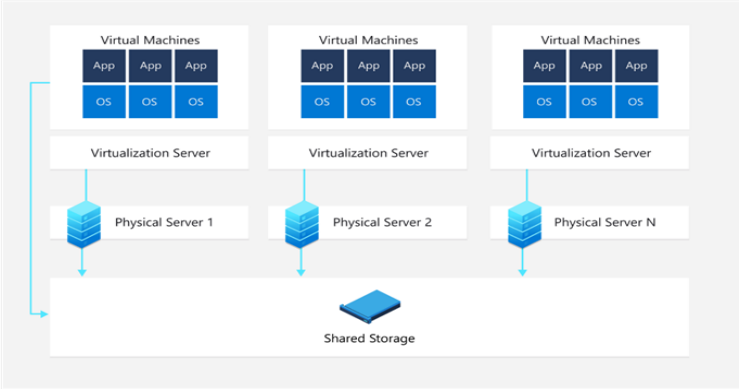
EXPERIMENT-20

Understanding virtual server deployment?

Virtual machines: virtual computers within computers

A virtual machine, commonly shortened to just VM, is no different than any other physical computer like a laptop, smart phone, or server. It has a CPU, memory, disks to store your files, and can connect to the internet if needed. While the parts that make up your computer (called hardware) are physical and tangible, VMs are often thought of as virtual computers or softwaredefined computers within physical servers, existing only as code.





Server virtualization works by abstracting or isolating a computer's hardware from all the software that might run on that hardware. This abstraction is accomplished by a hypervisor, a specialised software product. There are numerous hypervisors in the enterprise space, including Microsoft Hyper-V and VMware vSphere.

Virtualization uses software that simulates hardware functionality to create avirtual system, enabling organisations to run multiple operating systems andapplications on a single server.