RTQF Level: 5
Sector: ICT
Sub-sector: NETWORKING
Trainer: TUYISHIME Peter
Module: INSTALLATION, CONFIGURATION AND MANAGEMENT OF WINDOWS SERVER. (NEWWS501)

LU.1: PREPARE TO INSTALL A SERVER

1.1. Choose suitable operating system features and network (server) services

Current and common used Windows Servers

✚**Overview of window server**

Windows Server is a server operating system that enables a computer to handle network roles such as print server, domain controller, web server, and file server. As a server operating system, it is also the platform for separately acquired server applications such as Exchange Server or SQL Server.

✚Edition of windows server

This channel includes the following operating systems:

- **Windows Server** 2003 (April 2003)
- **Windows Server** 2003 R2 (December 2005)
- **Windows Server** 2008 (February 2008)
- **Windows Server** 2008 R2 (October 2009)
- **Windows Server** 2012 (September 2012)
- **Windows Server** 2012 R2 (October 2013)
- **Windows Server** 2016 (September 2016)

✚**Windows server roles**

- **Domain controller:** used to manage domains and domain objects; provides user authentication through Active Directory.
- **File server:** provides access to files stored on the **server**.
- **Print server:** provides network printing functionality.
- **DHCP server:** allocates IP addresses and provides configuration information to clients.

✚**Definition of Windows Server Features**

Features refer to additional capabilities of the Windows operating system itself, such as the .NET Framework or windows backup.

✚RAID configuration

RAID 5 is a redundant array of independent disks **configuration** that uses disk striping with parity. Because data and parity are striped evenly across all of the disks, no single disk is a bottleneck.

✚Feature on demand

Features on Demand is a **feature**, introduced in **Windows** 8 and **Windows Server 2012** , that allows you to remove role and **feature** files (sometimes called **feature** payload) from the operating system to conserve disk space, and install roles and **features** from remote locations or **installation media instead of from local ..**

✚Definition of Server Core

Windows Server Core *is* a minimal installation option for the ***Windows Server*** operating system (OS) that has no GUI and only includes the components required to perform ***server*** roles and run applications. ***Server Core*** is available in both the ***Windows Server*** Semi-Annual Channel and Long-Term Servicing Channel releases.

Learning Outcome1.2: Revise required installation options

Learning Outcome 1.3: Analyse data migration requirements

What is data migration?

Data Migration is the process of transferring data from one system to another while changing the storage, database or application.

1.3.1 Data migration requirements

Data Migration is the process of transferring data from one system to another while changing the storage, database or application. Typically, data migration occurs during an upgrade of existing hardware or transfer to a completely new system.

Types of Data Migration

- ✔ Storage migration.

- ✔ Cloud migration.

✔ Application migration.

Data migration involves 3 basic steps:

✔ Extract data
✔ Transform data
✔ Load data

Data migration requirements

After you have verified your source server meets the Requirements, verify that your target server meets the requirements below for data migration:

✔ Operating system

Windows operating system editions (Data center, Enterprise, Standard, Essential Business Server, Web Server, Foundation Server, Small Business Server, or Storage Server Edition).

✔ System memory

The minimum system memory on each server should be 1 GB. The recommended amount for each server is 2 GB.

✔ Disk space for program files

This is the amount of disk space needed for the Double-Take program files. For Windows 2008, this is approximately 375 MB.

✔ Disk space for data files

This is the amount of disk space needed for the source data files. This will be dependent on the applications you are running and the amount of data files you have.

✔ Server name

Server name must still be in ASCII format. If you have the need to use a server's fully qualified domain name, your server cannot start with a numeric character because that will be interpreted as an IP address.

✔ Protocols and networking

The server must meet the following protocol and networking requirements:

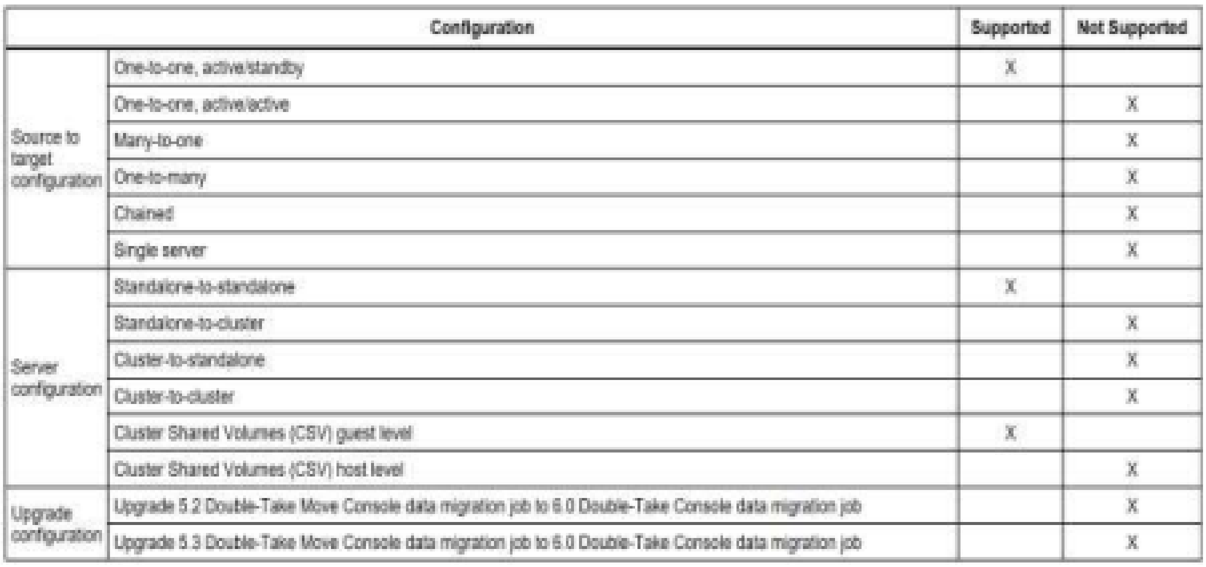
Your servers must have TCP/IP with static IP addressing. By default, Double-Take is configured for IPv6 and IPv4 environments. If you are using IPv6 on your servers, your clients must be run from an IPv6 capable machine.

✔ Cloud

Double-Take can be used to migrate data to an existing server in the cloud. Keep in mind that you should enable appropriate security measures, like VPN, to protect your data as it migrates to the cloud. Cloud migration is the process of moving data, applications or other business elements to a cloud computing environment

✔ Supported configurations

The following table identifies the supported configurations for a data migration job:



Configuration		Supported	Not Supported
Source to target configuration	One-to-one, active/standby	X	
	One-to-one, active/active		X
	Many-to-one		X
	One-to-many		X
	Chained		X
	Single server		X
Server configuration	Standalone-to-standalone	X	
	Standalone-to-cluster		X
	Cluster-to-standalone		X
	Cluster-to-cluster		X
	Cluster Shared Volumes (CSV) guest level	X	
	Cluster Shared Volumes (CSV) host level		X
Upgrade configuration	Upgrade 5.2 Double-Take Move Console data migration job to 6.0 Double-Take Console data migration job		X
	Upgrade 5.3 Double-Take Move Console data migration job to 6.0 Double-Take Console data migration job		X

✔ Creating a data migration job

With a data migration job, your servers can be in a NAT environment. However, you must make sure you have added your servers to the Double-Take Console using the correct IP address. Review the NAT configuration table in the Adding servers section before you start the job creation process.

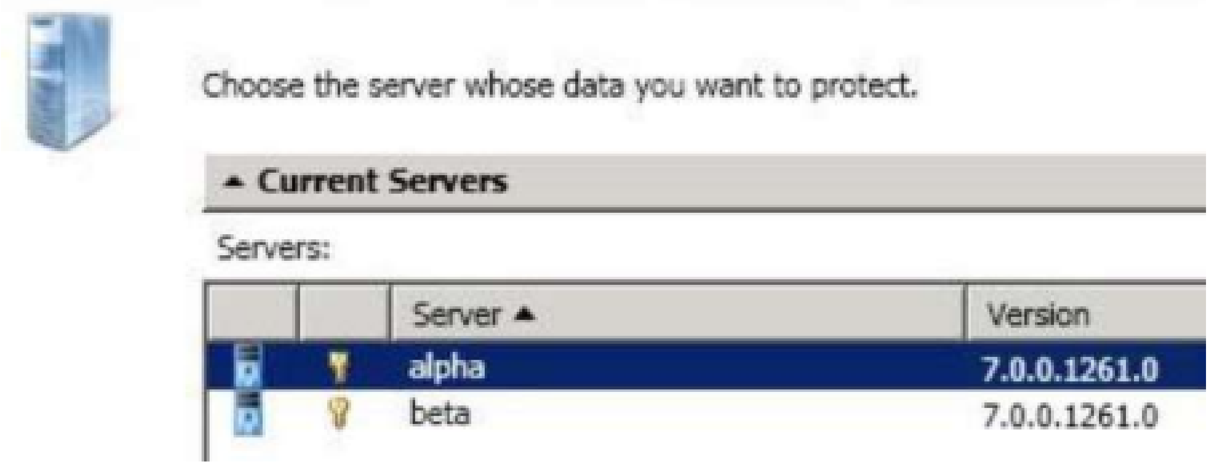
✔ Managing and controlling data migration jobs

-Click Get Started from the toolbar.

-Select Double-Take Move and click Next.

-Choose your source server. This is the server that contains the data that you want to migrate.

- choose source data



Choose the server whose data you want to protect.

▲ Current Servers

Servers:

		Server ▲	Version
		alpha	7.0.0.1261.0
		beta	7.0.0.1261.0

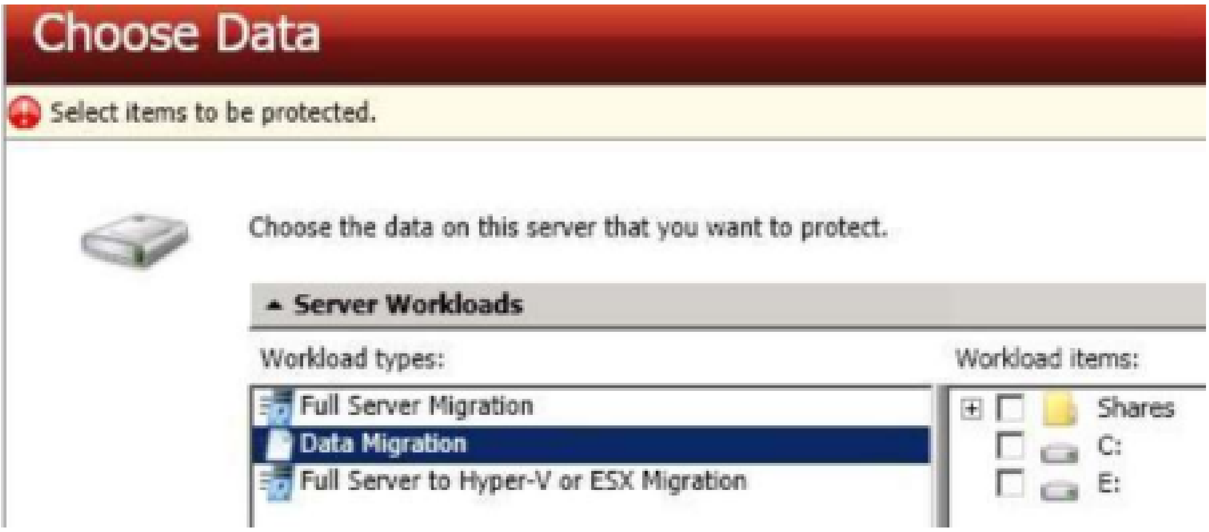
✔ **Current Servers**

This list contains the servers currently available in your console session.

✔ **Find a New Server**

If the server you need is not in the Current Servers list, click the Find a New Server heading.

- Click Next to continue.
- Choose the type of workload that you want to migrate.



Choose Data

Select items to be protected.

Choose the data on this server that you want to protect.

▲ Server Workloads

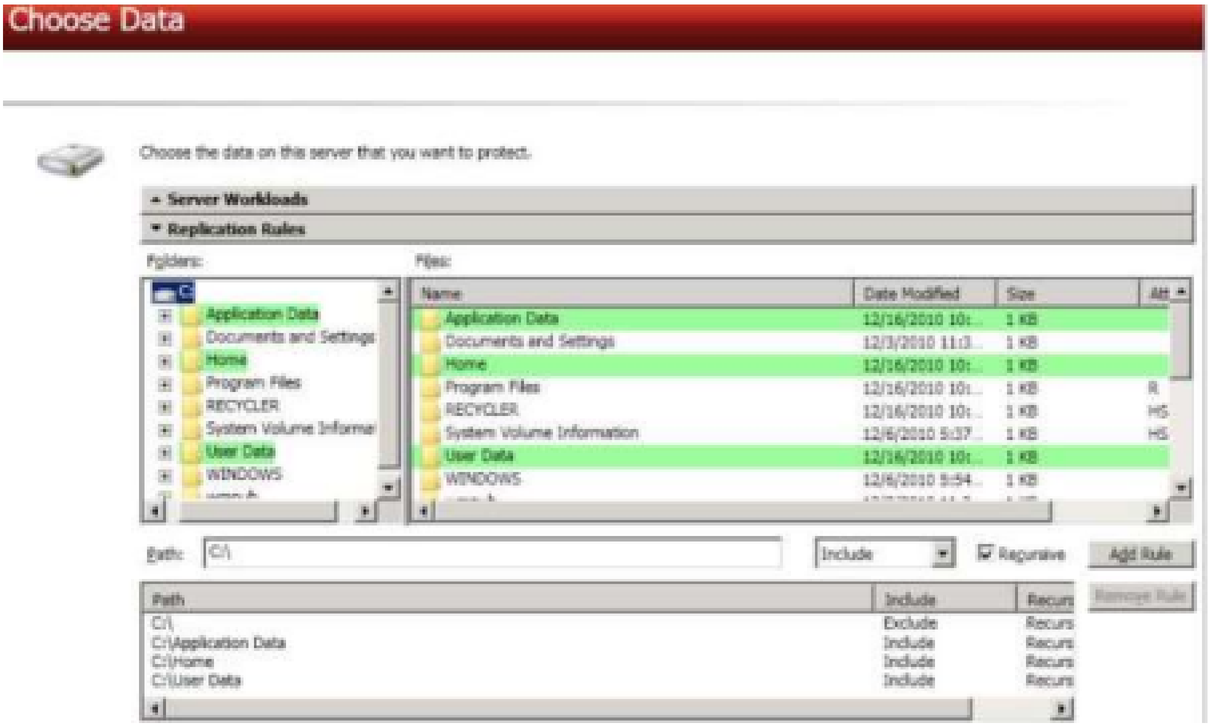
Workload types:

- Full Server Migration
- Data Migration
- Full Server to Hyper-V or ESX Migration

Workload items:

- ⊞ □ Shares
- □ C:
- □ E:

- To select your files and folders in more detail, click the **Replication Rules** heading and expand the volumes under **Folders**.



Choose Data

Choose the data on this server that you want to protect.

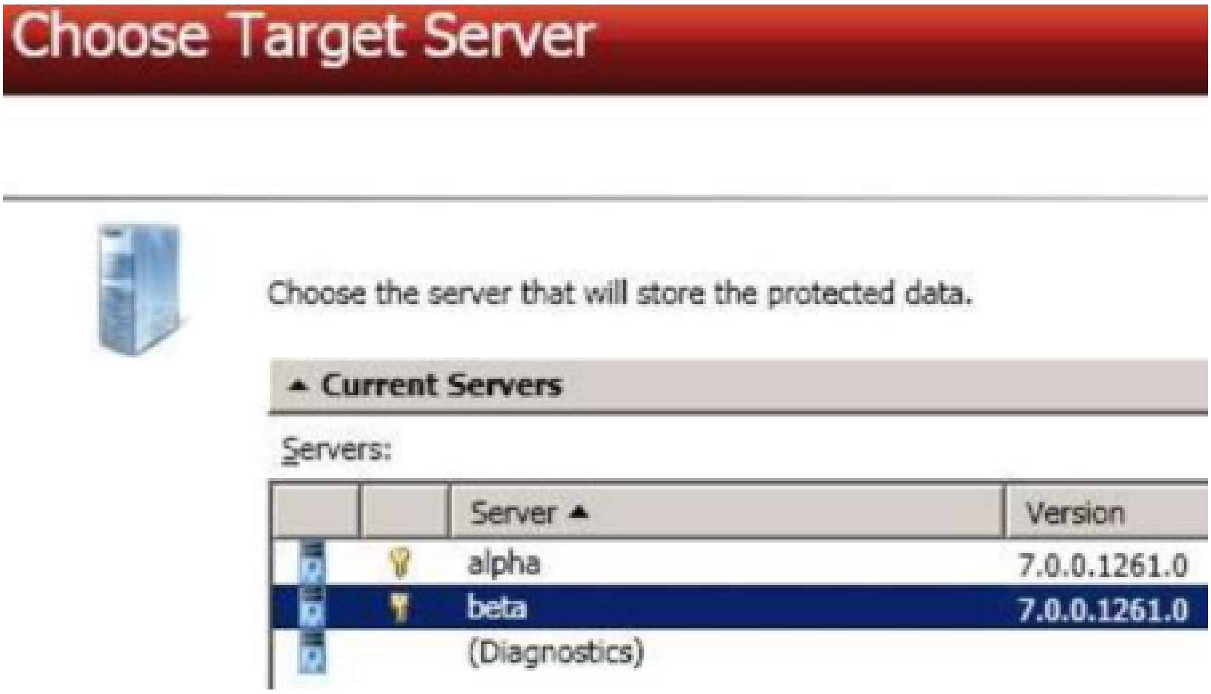
Name	Date Modified	Size	Att
Application Data	12/16/2010 10:...	1 KB	
Documents and Settings	12/3/2010 11:3...	1 KB	
Home	12/16/2010 10:...	1 KB	
Program Files	12/16/2010 10:...	1 KB	R
RECYCLER	12/16/2010 10:...	1 KB	HS
System Volume Information	12/6/2010 5:37...	1 KB	HS
User Data	12/16/2010 10:...	1 KB	
WINDOWS	12/6/2010 5:54...	1 KB	

Path: C:\ Include ☑ Recursive Add Rule Remove Rule

Path	Include	Recurs
C:\	Exclude	Recurs
C:\Application Data	Include	Recurs
C:\Home	Include	Recurs
C:\User Data	Include	Recurs

- Click **Next** to continue.

- Choose your target server. This is the server that will receive the migrated data from the source.



Choose Target Server

Choose the server that will store the protected data.

		Server ▲	Version
		alpha	7.0.0.1261.0
		beta	7.0.0.1261.0
		(Diagnostics)	

- Click Next to continue.

- You have many options available for your data migration job.

- Click Next to continue.

- Double-Take validates that your source and target are compatible.

- Once your servers have passed validation and you are ready to begin migration, click

Finish, and you will automatically be taken to the Manage Jobs page.

✔ cutting over data migration jobs

When the migration mirror has completed, the migration job may or may not terminate automatically depending on your selection for Wait for user intervention before cutover. If you disabled user intervention, the migration job will automatically terminate to complete the migration process. If you enabled user intervention, when the migration mirror is complete, the status will change to Protecting. Use this time to complete any necessary tasks. When you are ready to complete the migration, use the following instructions to cutover.

- On the Manage Jobs page, highlight the job that you want to cutover and click Failover or Cutover in the toolbar.

- Select the type of cutover to perform.

- Select how you want to handle the data in the target queue.

- When you are ready to begin cutover, click Cutover.

Learning Outcome 1.4: Back up local data in preparation for installation

1.4.1 Windows server backup

Windows Server Backup is a Feature of windows server or is built-in component of Windows Server 2008 R2 or other version that consists of a Microsoft Management Console (MMC) snap-in, command-line tools, and Windows PowerShell cmdlets.

1.4.2 Overview of Windows Server Backup

Windows Server Backup consists of a Microsoft Management Console (MMC) snap-in, command-line tools, and Windows PowerShell cmdlets that provide a complete solution for your day-to-day backup and recovery needs.

You can use Windows Server Backup to back up a full server (all volumes), selected volumes, the system state, or specific files or folders and to create a backup that you can use for bare metal recovery. You can recover volumes, folders, files, certain applications, and the system state. And, in case of disasters like hard disk failures, you can perform a bare metal recovery.

1.4.3 Checklist: Schedule Automatic Backups

With an automated backup program, backup software handles the task for you. You specify the time intervals at which you wish for server backup to be done. This takes the challenge of remembering to do it on your own away from you if you‟re willing to trust the software to complete its designed purpose. Example: NovaStor backup tool

Checklist:

✔ Check the capabilities of the existing backup system. Decide on how much you should you spend on backup.

✔ How many times a day and at what times you want to run backups.

✔ Whether you will use a volume, a single disk, multiple disks, or a remote shared folder to store the backups.

✔ Which files, folders, or volumes you want to back up and whether the backups will need to be used for bare metal, full server (all volumes), or system state recovery. ✔ Think of backup scenarios.

✔ Tune and automate the backup system.

1.4.4 Checklist: Perform a Manual Backup

A manual server backup is a backup done periodically by utilizing backup tools either provided by their servers or included in with their operating systems. It allows the user to see the backup being done. It is easy to initiate but consume time.

Checklist:

Before you begin, review concepts and requirements, and then determine the following:

✔ Where you will store the backup.

✔ Which volumes you want to back up and whether the backups will need to be used for operating system (critical volumes only), full server (all volumes), system state, or bare metal recovery.

✔ If you have not already done so, install Windows Server Backup.

✔ Run the Backup Once Wizard and follow the instructions in the wizard.

✔ After the backup is created, run a test recovery using the backup to confirm that you are able to recover the items that you intended.

1.4.5 Checklist: Recover Files, Folders, Applications, Volumes, or the Operating System

Before you begin, review concepts and requirements, and then determine the following:

✔ What you want to recover.

✔ What backup you will use to recover from.

✔ Where you want to recover to.

✔ If you have not already done so, install Windows Server Backup.

✔ If needed, attach any drives or make sure any remote shared folders that you need are available and that you have access to them. Also, make sure that you understand the limitations of different storage and recovery types.

✔ Run the Recovery Wizard and follow the instructions in the wizard that are specific to what you want to recover.

1.4.6 Installation of Windows Server Backup Tools

To access backup and recovery tools, you must install the Windows Server Backup Features and subordinate items that are available in the Add Features Wizard in Server Manager. This installs the following tools:

✔ Windows Server Backup Microsoft Management Console (MMC) snap-in Wbadmin command-line tool.

✔ Windows PowerShell cmdlets for Windows Server Backup

To install backup and recovery tools

1. Click Start, click Administrative Tools, click Server Manager, in the left pane click Features, and then in the right pane click Add Features. This opens the Add Features Wizard.
2. In the Add Features Wizard, on the Select Features page, expand Windows Server Backup Features, and then select the check boxes for Windows Server Backup and Command-line Tools.

3. On the Confirm Installation Selections page, review the choices that you made, and then click Install. If there is an error during the installation, it will be noted on the Installation Results page.
4. Then, to access these backup and recovery tools, do the following:

To access the Windows Server Backup snap-in, click Start, click Administrative Tools, and then click Windows Server Backup.

To access and view the syntax for Wbadmin, click Start, right-click Command Prompt, and then click Run as administrator. At the prompt, type: wbadmin /?

For instructions to access and view the Help for the Windows PowerShell Windows Server Backup cmdlets, see Using Windows Server Backup Cmdlets.

1.4.7 Backing Up Your Server

You can use Windows Server Backup to protect your operating system, system state, volumes, files, and application data. Backups can be saved to single or multiple disks, single or multiple volumes, DVDs, removable media, or remote shared folders. They can be scheduled to run automatically or manually.

1.4.8 Recovering Your Server

You can use the backups you have created with Windows Server Backup to recover your operating system, system state, volumes, applications and application data, backup catalog, and local files and folders. To do this, use the following tools:

- Recovery Wizard (in Windows Server Backup)
- Windows Setup disc or a separate installation of the Windows Recovery Environment -
Catalog Recovery Wizard (in Windows Server Backup)

You can also perform these tasks using the **Wbadmin** command.

1.4.9 Optimizing of Backup and Server Performance

You can use the Optimize Backup Performance dialog box to improve the performance of backups for full volumes, which can improve server performance. It is available from the homepage of the Windows Server Backup snap-in. However, these settings apply only if you are including entire volumes in the backup.

To adjust performance settings for Windows Server Backup

1. Click Start, click Administrative Tools, and then click Windows Server Backup. 2.
In the Actions pane of the snap-in default page, under Windows Server Backup,
click Configure Performance Settings. This opens the Optimize Backup Performance
dialog box.

3. In the Optimize Backup Performance dialog box, do one of the following:

✔ Click Normal backup performance.

✔ Click Faster backup performance.

1.4.10 Testing of backup Using Cmd

You must run **wbadmin** from an elevated command prompt. (To open an elevated command prompt, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.)

Or you may test using this way

Use the Wbadmin.exe available if you install the windwos server backup feature.

To perform a system state backup use:

Wbadmin start systemstatebackup –backuptarget:<targetDrive> -quiet

By adding a target drive it is:

Wbadmin start systemstatebackup –backuptarget:**D** -quiet

1.4.11. Resources for Backup and Recovery

Use the following resources on the Microsoft Web site:

✔ For technical information, see http://go.microsoft.com/fwlink/?LinkId=93236. ✔ For information about the Wbadmin command, see the Command Reference (http://go.microsoft.com/fwlink/?LinkId=140216).

✔ For information about backing up or recovering computers running Active Directory Domain Services, see http://go.microsoft.com/fwlink/?LinkId=143743. ✔ For information about Windows PowerShell commands (cmdlets) for Windows Server Backup, see http://go.microsoft.com/fwlink/?LinkId=143721.

✔ For in-depth troubleshooting information for events, see http://go.microsoft.com/fwlink/?LinkID=140218.

1.4.12. User Interface: Windows Server Backup

The Windows Server Backup Microsoft Management Console (MMC) snap-in contains the following wizards to help you schedule and create backups, and perform recoveries:

✔ Backup Schedule Wizard

✔ Backup Once Wizard

- ✔ Recovery Wizard
- ✔ Catalog Recovery Wizard

LU 2: INSTALL SERVER NETWORK OPERATING SYSTEM

Learning Outcome 2.1: Install network operating system (NOS) and update the NOS with all required patches

2.1. Windows Server

2.1.1 Installation Methods

The choice of installation method depends on whether you are a novice, expert, or advanced user. Those installation methods are:

✔ Installing Windows using Oracle Hardware Installation Assistant (Oracle Hardware Installation Assistant: OHIA). It needs to download Server Software.

✔ Installing Windows manually- using DVD's or a downloaded software. ✔ Installing Windows from a deployment server environment use of customized Windows installation image (WIM) on a system running Windows Deployment Services (WDS).

Once this installation image file has been created, you can boot your server from its network card and select the image from the WDS system for unattended deployment.

2.1.2 Installation Types

✔ **Clean Installation:** consists of the wipe out an existing operating system on existing partition or installation on a new partition.

✔ **In-Place Upgrade:** An in place upgrade takes an existing installation of Windows and upgrades it to a new installation.

✔ **Migration:** A migration involves two Windows installations (From a source to a destination) using either using the Side-by-side or Wipe and Load method. ✔ **Dual boot:** Dual boot or multi boot refers to a computer that has more than one operating system installed.

2.1.3 Choosing Whether to Upgrade or Migrate

✔ **Upgrade**

Upgrade versions are for users that already have a previous copy of Windows installed on

their computer, and who want to install the newer version on the same computer. Note:

Full Installation Media are sold to those who do not yet have a copy of Windows. ✔

Migration

Wipe-and-load method is used when we only have one computer. Temporarily you upload user settings on some other computer, you wipe out existing computer and then do a clean install on that computer. After the installation we can download saved settings from previous installation to complete the migration process. To do migration we can use User State Migration Tool or Windows Easy Transfer.

2.1.4 Hardware Requirements for Windows Server

Windows Server 2012 R2 Hardware Requirements

Component	Minimum Requirement	Microsoft Recommended
Processor	1.4 GHz	2 GHz or faster
Memory	512 MB RAM	2 GB RAM or greater
Available Disk Space	32 GB	40 GB or greater
Optical Drive	DVD-ROM drive	DVD-ROM drive

2.1.5 Using Windows Server Migration Tools

There are 2 way of installing these tools on your Windows Server 2012 server.

1. Use PowerShell by opening a Windows PowerShell command window as administrator. 2. Use the "Add Roles and Features Wizard" to add the Windows Server Migration Tools to your destination machine

Learning Outcome 2.2: Post-Install and Configure the Server

2.2.1 Overview of Post-Installation Configuration

After completing a manual installation of the Windows Server 2012 R2 and rebooting the server, you should review the following post installation tasks and, if necessary, perform the tasks that are applicable to your server. Checklist which can be used after installing Windows Server 2012 R2:

- **Server Configuration Tasks**

✔ Server Manager > Local Server

✔ Enable Remote Desktop

✔ Set IP address, gateway and DNS

✔ Change Time Zone

✔ IE Enhanced Security – Admin: Off; User: On

✔ Reboot

✔ Change Computer Name, and add a domain suffix, or join to the domain ✔ Server Manager > Local Server > Manage > Server Manager Properties Check: Do Not Start Server Manager Automatically at Startup

✔ Reboot

2.2.2 Configuration of server network settings (Configure the IP address)

Click Change adapter settings. Right-click on Local Area Connection and click on Properties. Select Internet Protocol Version 4 (TCP/IPv4) and click on Properties. Select "Use the following IP address" and enter the IP address, Subnet Mask, Default Gateway and DNS server.

2.2.3 Set the computer name

Click Start, right-click Computer, and then click Properties. The computer name appears under Computer name, domain, and workgroup settings. To change it click on change.

2.2.4 Join a domain

- On the Start screen, type Control Panel, and then press ENTER.
- Navigate to System and Security, and then click System.
- Under Computer name, domain, and workgroup settings, click Change settings. - On the Computer Name tab, click Change.

The join a domain option appears.

2.2.5 Configure the time zone

Right-click the time field in the lower right corner and then click the Adjust date/time option. In the settings window, you can change the time, date, and time zones of each Windows Server.

2.2.6 Enable automatic updates

Manually enable automatic updates on Windows 2012 and Windows 2008 Public Cloud Servers

✔ Connect to the Windows server.

✔ Click on the Windows icon in the lower-left corner.

✔ Click Control Panel > System and Security. ...

✔ Under the Windows Update section, click Turn automatic updating on or off.

2.2.7 Add roles and features

Steps

- In Server Manager, click Manage and then select Add Roles and Features to start the Add Roles and Features Wizard.

- On the Select installation type screen, select Role-based or feature-based installation. - Select the target server.
- On the Select features screen, check the box next to .Net Framework 3.5 Features.

2.2.8 Enable remote desktop

Click on the Settings button,

- Click on Server Info under Desktop.
- The Server Info launches the System Control Panel page. “Click Advance System Settings” on the right. This will launch the System Properties page.
- Select the appropriate option under Remote Desktop and click OK.

2.2.9. Configure Windows Firewall settings

Manage firewall settings

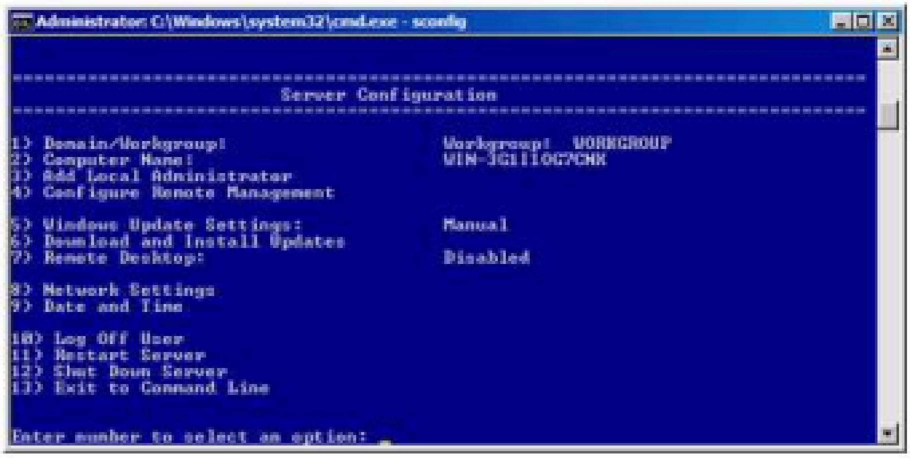
- Open the Server Manager from the task bar.
- On the right-hand side in the top navigation bar, click Tools and select Windows Firewall with Advanced Security.
- Review the current configuration settings by selecting Windows Firewall Properties from the MMC landing page.

2.2.10. Activation of Windows Server.

To begin the installation of the KMS host in the Windows Server 2012 / 2012R2 machine, begin by adding a role: On the next screen, select Role-based or feature-based installation: Select the server where the roles will be installed: On the Add Roles and Features Wizard, select Volume Activation Services.

2.2.11 Configuration of Server Core installation.

A useful command is sconfig, it allows you to quickly configure basic server settings. Simply type in **sconfig** on the command prompt and follow the on screen instructions:



Administrator: C:\Windows\system32\cmd.exe - sconfig

```
===============================================================================
                         Server Configuration
===============================================================================

1) Domain/Workgroup:                    Workgroup:  WORKGROUP
2) Computer Name:                       WIN-3G1I1OG7CNK
3) Add Local Administrator
4) Configure Remote Management

5) Windows Update Settings:             Manual
6) Download and Install Updates
7) Remote Desktop:                      Disabled

8) Network Settings
9) Date and Time

10) Log Off User
11) Restart Server
12) Shut Down Server
13) Exit to Command Line

Enter number to select an option: _
```

2.2.12 Network Interface Card Teaming

NIC Teaming, also known in the Microsoft world as Load Balancing/Failover (LBFO), allows you to install additional physical Ethernet network adapters (NICs) into your server and "team" or combine them together to make one virtual NIC that provides better performance and fault tolerance.

To create a NIC Team:

- In Server Manager, click Local Server.
- In the Properties pane locate NIC Teaming, and then click the link Disabled to the right. ...
- In Adapters and Interfaces, select the network adapters that you want to add to a NIC Team.
- Click TASKS, and then click Add to New Team.

2.2.13 Using DISM to Add Windows Features

What is DISM?

Deployment Image Servicing and Management (DISM) is a command-line tool that you can use to service offline images or running operating systems. Use it to install, uninstall, configure, and update Windows features, packages, drivers and international settings.

Use DISM to enable windows server backup feature for a running system.

LU 3. CONFIGURE AND ADMINISTER THE SERVER

3.1. Install and administer active directory, Organizational units (OUs).

3.1.1. Overview of Windows Server Management

3.1.1.1 Definition of Server Manager

Microsoft Windows Server Manager is a tool to view and manage server roles and make configuration changes. Server Manager allows administrators to manage local and remote servers without requiring physical access to the servers or enabling Remote Desktop Protocol connections.

3.1.1.2 Use the server manager console to perform the following tasks on both local servers and remote servers:

▪ **View role-related events.**

Access Event viewer

- ✔ Right click on the Start button and select Control Panel > System & Security and double-click Administrative tools.
- ✔ Double-click Event Viewer.
- ✔ In the console tree, right-click the appropriate log file.

▪ **Run the Best Practice Analyzer for a role.**

It is a tool that allows admins to scan individual server roles to determine if they are configured according to Microsoft‟s recommended best practices.

Steps:

Open the Server Manager

Navigate through the console tree to Server Manager/Roles/ (the role that you want to analyze).

When opened, the BPA is listed within the role‟s Summary section

▪ List the tools available from Server Manager.

▪ Restart Windows Server

Restart From GUI.

Click on the start button followed by the Power button, and then Restart.

Restart From Command Prompt.

```
C:\> shutdown -r
```

Restart From PowerShell.

```
PS C:\> Restart-Computer
```

Restart Remotely.

We can also use PowerShell to remotely reboot a Windows Server, again this is done with the „Restart-Computer‟ cmdlet, except we specify the name of the computer that we want to restart.

```
PS C:\> Restart-Computer -ComputerName "web01"
```

„web01‟ being the server

3.1.2 Administrative Tools and Remote Server Administration Tools

3.1.2.1. Remote Server Administration Tools

RSAT (Remote Server Administration Tools) is a Windows Server component for remote management of other computers also running that operating system.

Steps:

Start the Add Features Wizard in Windows Server 2008 or Windows Server 2008 R2 or the Add Roles and Features Wizard in Windows Server 2012 and later versions. Then, on the Select Features page, expand Remote Server Administration Tools, and then select the tools that you want to install.

3.1.2.2. Managing non-domain joined Windows Server with RSAT and Server Manager

A non-domain joined server is either one resided in workgroup or in non-trusted domain

Steps:

Add non-domain joined server to server manager. Use DNS tab in Add Server dialog to add non-domain joined server.

Once this is done, server will be added but you will likely will get Refresh Failed and also “Kerberos target resolution error” for newly added server. Which means that you are unable to communicate with this server.

1. Add non-domain joined server into trusted hosts on a management server. On management server (the one from which you run Server Manager) you have to add your target non-domain joined server to Trusted Hosts list by means of issuing the following PS command:

```
Set-Item wsman:localhost\client\trustedhosts Non-DomainJoinedServer1 -Concatenate -Force
```

Use this command to view your current Trusted Hosts list:

```
(Get-Item wsman:localhost\client\trustedhosts).value
```

2. Configure UAC to allow elevated remote sessions on a target non-domain joined computer. By default this is not allowed on a worgroup computers. You can this by issuing this PS command:

```
New-ItemProperty -Name LocalAccountTokenFilterPolicy -path
HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System -propertyType
DWord -value 1
```

You may check current setting with this command:

```
(Get-ItemProperty –Path
'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System').LocalAccountT
okenFilterPolicy
```

3.1.2.3 Configuring Services

a. Startup Types

The startup type allows you to choose how the service is started when the computer boots up and can be set to: Automatic, Automatic (Delayed), manual, or disabled. If a service is set to automatic, the service will start automatically as soon as you boot up your computer and require no intervention from you.

Meaning of each type:

Automatic: The service starts at system logon.

Automatic (Delayed): The service starts a short while after the system has finished starting up. ...

Manual: The service starts only when explicitly summoned.

Disabled: The service is disabled.

Steps to configure startup types:

- Head to Start.

- Type services.
- Select Services (under Results)
- Select a service to adjust by double-clicking.
- In the General tab, Startup type section, select Automatic (Delayed Start), Automatic, Manual or Disabled.

b. Service Recovery

In case a service fails, you can set up service recovery options as follows: On the right-hand side of the Services window, right-click the service that you want to set up recovery options for. In the context menu, select Properties. From the opened window, click the Recovery tab.

c. Service Accounts

Windows services can run as the following account types: Domain user account, Local user account, Local Service account, Network Service account, Virtual accounts, Managed Service Account, Local System account.

Security for service account types can be grouped by the level of security they offer:

Most-secure account types

Non-administrative local account, Non-administrative domain account, Built-in Local Service account, Built-in Network Service account, Built-in virtual service account. Managed Service Account

Less-secure account types

Administrative local account, Administrative domain account

Least-secure account type

Built-in Local System account

3.1.3 Active Directory Domain Services

3.1.3.1 Overview of AD DS

Active Directory Domain Services (AD DS) is a server role in Active Directory that allows admins to manage and store information about resources from a network, as well as application data, in a distributed database. AD DS can also help admins manage a network's elements (computers and end users) and reorder them into a custom hierarchy.

The structure of the hierarchy includes an AD forest, the forest's domains and organizational units in those domains. AD DS integrates security by authenticating logons and controlling who has access to directory resources.

The makeup of AD DS includes:

AD Users and Computers, AD Administrative Center, AD Domains and Trusts, AD Sites and Services, AD PowerShell module, a server for Network Information Service tools, Additional command-line tools and snap-ins.

3.1.3.2 Overview of Domain Controllers

A domain controller (DC) is a server that responds to security authentication requests within a Windows Server domain. It is a server on a Microsoft Windows or Windows NT network that is responsible for allowing host access to Windows domain resources.

A domain controller has an Active Directory database from which user accounts can be created and deleted, and security and access granted or revoked.

It provides domain-wide services to the users, such as security policy enforcement, user authentication, and access to resources.

3.1.3.3 Installing a Domain Controller

Steps

- ✔ If it is not already open, open the Server Manager window.
- ✔ Select Roles > Active Directory Domain Services.
- ✔ In the Summary section, click Run the Active Directory Domain Services Installation Wizard (dcpromo.exe).

Add a New Domain in Existing Forest in Windows Server 2016

- Open server manager dashboard and click Add roles and features.
- Read the prerequisites and click Next.
- Choose Role-based or feature-based installation and click Next.
- Choose the destination server on which you want to configure the new domain and click Next.

3.1.4 Active Directory Domain Services Objects

3.1.4.1 Managing User Accounts

Managing user accounts in Windows Server 2012 Essentials

- Open the Dashboard.
- Click Users on the navigation bar.
- Click Add a user account in the Tasks pane.
- Follow the prompts in the Add a User Account Wizard to create the user account.

3.1.4.2 Managing Groups

Groups help to easily manage more than one user simultaneously.

Create a New Server Group in Server Manager on Windows Server 2012

- Click Manage in the top-right of Server Manager and select Create Server Group from the menu.
- In the Create Server Group window, give the new group a name in the Server group name box.

3.1.4.3 Managing Computer Accounts

A computer account is an account that is stored in Active Directory and that uniquely identifies a computer in a domain. A computer account uses the same name as the computer joining the domain. It represents a physical entity such as a computer or person.

To create a new computer account:

- Open Active Directory Users and Computers.
- In the console tree, right-click Computers. Where? Active Directory Users and Computers/domain node/Computers. Or, right-click the folder in which you want to add the computer.

- Point to New, and then click Computer.
- Type the computer name.

3.1.4.4 Delegating Administration

Delegate administrator privilege in Active directory:

- Start the delegation of control wizard by performing the following steps: Open Active

Directory Users and Computers. ...

- Select the users or group to which you want to delegate common administrative tasks. To do so, perform the following steps: ...
- Assign common tasks to delegate. ...
- Click Finish.

3.2: Deploy and configure server roles

3.2.1 Dynamic Host Configuration Protocol

· Overview of the DHCP Server Role

3.2.1.1 Configuring DHCP Scopes

A DHCP scope is a valid range of IP addresses that are available for assignment or lease to client computers on a particular subnet. In a DHCP server, a scope is configured to determine the address pool of IPs that the server can provide to DHCP clients.

Scopes determine which IP addresses are provided to the clients. They should be defined and activated before DHCP clients use the DHCP server for its dynamic IP configuration. Users can configure as many scopes on a DHCP server as required in the network environment.

Use the following procedure to create and configure a DHCP scope.

1. Select Start-->Programs-->Administrative Tools-->DHCP.
2. In the console tree, click the DHCP server to which you wish to add the DHCP scope for the IP telephones. ...
3. Select Action-->New Scope from the menu.
4. Click the Next button.

3.2.1.2 Managing a DHCP Database

Managing a DHCP server database involves backing up the database, restoring the database

and reconciling the database. You can do all of these from within the DHCP manager by right-clicking on the DHCP server or they can be done from the command line.

Right-clicking on the server and selecting backup. You will be prompted for the location for storing the backup file. The default is \windows\system32\dhcp\backup.

The DHCP server automatically backs up its data every 60 minutes. These automatic backups are only used if the server detects that its database is corrupt. They cannot be used to manually restore the DHCP data or migrate the data to another server.

Restoring the DHCP database is as straightforward as backing it up. If the DHCP server is already running, you need to stop the DHCP Server Service, restore the database and then restart the DHCP Server Service. You will be prompted for the location of the file you want to restore from.

4.2.1.3 Securing and Monitoring DHCP

The common threats to DHCP servers are:

1. An unauthorized user could start a denial-of-service (DoS) attack by requesting and obtaining a large number of IP addresses.

2. An unauthorized user could use a rogue DHCP server to provide incorrect IP addresses to your DHCP clients.

To ensure that only authorized individuals or users connect to the DHCP server and obtain a DHCP lease, you should consider limiting physical access and wireless access to the network.

You should also consider configuring only the precise number of IP addresses required for each DHCP scope to make it less simple for hackers to intercept IP addresses. You can use the reservations feature to do this.

The DHCP server can be a single point of failure in networking environments that only have one DHCP server. You can increase the availability of DHCP servers and protect your DNS servers from DoS attacks by deploying two DHCP servers, and then using the 80/20 Rule if you have two DHCP servers located on different subnets.

The 80/20 Rule is applied as follows:

-Allocate 80 percent of the IP addresses to the DHCP server which resides on the local subnet.

-Allocate 20 percent of the IP addresses to the DHCP Server on the remote subnet.

If the DHCP server that is allocated with 80 percent of the IP addresses has a failure or is attacked, the other DHCP server would be able to assign DHCP clients with IP addresses.

4.2.2 Domain Name System (DNS)

It is the system by which Internet domain names and addresses are tracked and regulated.

3.2.2.1 Name Resolution for Windows Clients and Servers

Name resolution is a method of reconciling an IP address to a user friendly computer name. Originally networks used host files to resolve names to IP addresses. They came in the form of a text file that the computer accessed if name resolution was required.

3.2.2.2 Installing a DNS Server

To configure DNS by using the DNS snap-in in Microsoft Management Console (MMC), follow these steps:

1. Click Start, point to Programs, point to Administrative Tools, and then click DNS.
2. Right-click Forward lookup zones, and then click New Zone.
3. When the New Zone Wizard starts, click Next.

3.2.2.3 Managing DNS Zones

A managed zone is the container for all of your DNS records that share the same domain name, for example, example.com. Managed zones are automatically assigned a set of name servers when they are created to handle responding to DNS queries for that zone.

NS zones are used to delineate which DNS Servers are authoritative for resolving name resolution queries for a given section of the DNS hierarchy.

The following tasks are linked to their associated scripting samples:

Creating a DNS Zone, Modifying a DNS Zone, Deleting a DNS Zone, Adding a Zone IP Address,

Deleting a Zone IP Address, Pausing a Zone, Resuming a Zone, Updating a Zone, Reloading a Zone, Refreshing a Zone

Creating different scripts: https://docs.microsoft.com/en-us/windows/desktop/dns/dns-wmi provider-samples-managing-dns-zones

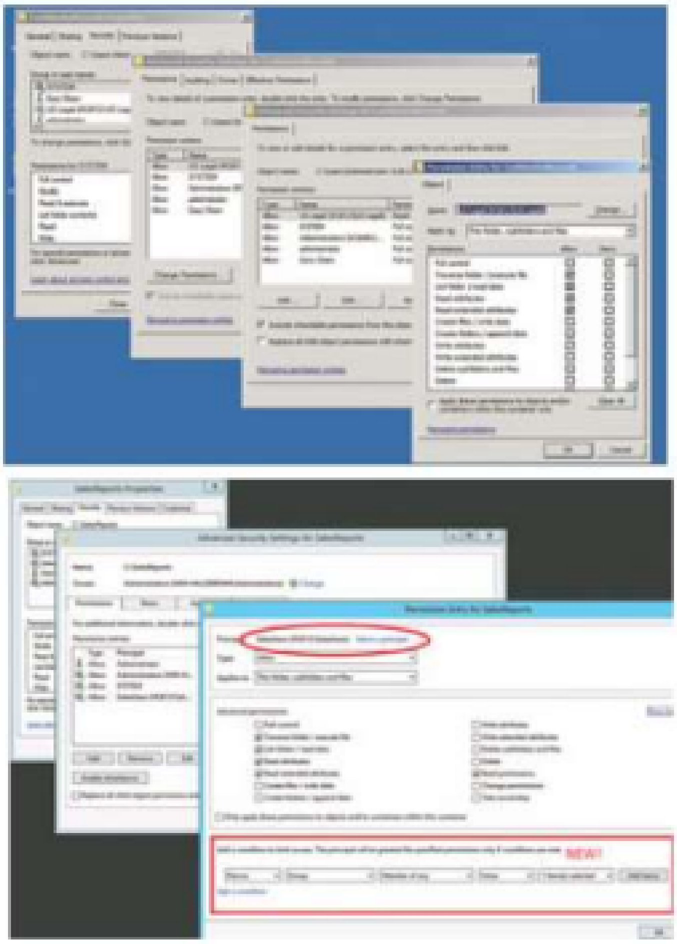
3.3: Configure the server roles and features: file and share access services

· File and Print Services

3.3.1 Securing Files and Folders

Microsoft has added some nice features in the file system of Windows Server 2012 and using Active Directory Rights Management Services (AD RMS) with other features, you can apply file classification so the file carries the rights without having to apply security groups.

To what you can do in win Server 2008, the conditional statement at the bottom in Windows Server 2012 is added.



Windows User 28
(Advanced permissions in Windows Server 2008 are shown on top, while the newer advanced permissions in Windows Server 2012 are shown on bottom.)

Install AD RMS Role

-Choose Add roles and features from the Dashboard or from the Tools dropdown menu.

-Skip past the intro screen and select Role-based or feature based installation. -Select Destination Server (select the VHD or server to which you want to install).

-Select Server Roles | Select Active Directory Rights Management. This will pop up a list of prerequisite services to install (.NET 4.5, IIS and so on). Click the Add Features button, then click Next.

-Select Features | Select Windows Internal Database. Click Next.

-Web Server Role (information only). Click Next.

-Role Services (AD RMS is selected) Click Next.

-Confirmation (click Install). No need to check the box to restart the server automatically as AD RMS does not require a reboot for installation or removal.

Following the installation, Server Manager will show AD RMS in the menu

To install and configure Active Directory Rights Management Services to lock down your organization's files and shares:

3.3.2 Protecting Shared Files and Folders by Using Shadow Copies

Shadow Copy (also known as Volume Snapshot Service, Volume Shadow Copy Service or VSS) is a technology included in Microsoft Windows that can take manual or automatic backups of computer files and volumes, even when they are in use. It runs as a Windows service named Volume Shadow Copy.

Shadow Copy technology requires the file system to be NTFS in order to create and store shadow copies. Shadow Copies can be created on local and external (removable or network) volumes by any Windows component that uses this technology, such as when creating a scheduled Windows Backup or automatic System Restore point.

Open the File Explorer and right-click on the volume where you want to enable Volume Shadow Copies. Select Configure Shadow Copies: Select the volume and click Enable: Microsoft suggests to use a dedicated drive to store Volume Shadow Copies in case of high-load.

3.3.3 Configuring Work Folders

Work Folders is a new feature of Windows Server 2012 R2 that allows users to have access to individual corporate data folders, no matter where the users are and from what device they are connecting.

Work Folders: Prerequisites

In order to install Work Folders, you need the following configured (as a minimum):

-Windows Server 2012 R2 Standard or Enterprise

-Windows 8.1 (Any versions) or Windows 8.1 RT

For external and production solutions, you also need the following:

-Public CA issued SSL certificate (internally generated SSL cert will do for domain-joined clients or in demo scenarios)

-Automatic server discovery DNS settings

-Reverse Proxy (preferred, but not required)

Installing Work Folders Server Role

No matter if the Work Folders will be used only internally or both internally and externally, the first step is installing the Work Folders Server Role.

-From the Server Manager, **choose Add Roles and Features**.

-From the Select Server Roles, go to File and Storage Services / File and iSCSI Services, then select Work Folders.

-A pop-up will inform you about the additional IIS Hostable Web Core component that will be installed as well.

Creating Work Folders Security Groups

Work Folders are working much like regular NTFS folders from a security perspective. To grant/deny access, you rely on global security groups within Active Directory.

In this example, let‟s create an Active Directory group called "Work Folders Users," that is allowed full access rights to the Work Folders directories.

-Logon to your Server 2012 R2 domain controller, go to the Active Directory Users and Computers console, and choose Create new group by using icon in toolbar or right-click / new / group).

-Select Global and Security as options and give it a name and description (Work Folders Users).

-Create and Configure Work Folders Data Folders

In this last step, create and configure a sync share for work folders, granting access rights to the earlier created AD security group.

-From the Server 2012 R2 member server in the domain, go to Server Manager / File and Storage Services / Work Folders.

-Start the New Sync Share Wizard or click Task / New Sync Share.

-Select your 2012 R2 server and select Enter a local path. Browse to the directory you want to make available as sync share (c:\data\sample work folders directory, in my example).

-Select user alias@domain as the structure for user folders. With this option selected, if a domain user logs on, his folder structure is created as user@domain. In the other case, only the username would be visible, making it more difficult to distinguish users from different domains.

-In the Sync Access step of the configuration wizard, click Add… and select Work Folders

Users from the Active Directory list of groups. Make sure the Disable inherited permissions and grant users exclusive access to their files is enabled.

-In the Device Policies window, check Encrypt Work Folders and automatically lock screen, and require a password. Encrypt work folders makes sure the synced folders to the local device will be encrypted. The latter sets certain additional security parameters for the device from which you want to use work folders sync.

-Click Next to complete the Work Folders Sync Share creation.

Source: https://www.petri.com/configure-work-folders-windows-server-2012-r2

(read about how to configure SSL Certificate)

3.3.4 Configuring Network Printing

A Printer is one of the most important devices for an office network and being a system administrator you should be able to deploy it.

Prerequisites

Following are the requirements:

- The Administrator account must have a strong password.
- A static IP is configured.
- The latest windows updates are installed.
- The firewall is turned off.
- Installing the Print Server

Step 1: Open the server manager dashboard from the task bar. Click on 'Add roles and features'.

Step 2: Click on 'Next'.

Step 3: Choose Role-based or feature-based installation and click Next. Step 4:

Choose the destination printer server for this configuration and click Next.

Step 5: Choose Print and document services from server roles and when a new window appear, click Add Features.

Step 6: Click Next.

Step 7: Leave the default selections and click Next.

Step 8: Click Next.

Step 9: Choose Print Server and click Next.

Step 10: Click on Install

Step 11: Click: Close after successful installation.

Configuring the Print Server

Step 1: Open the print server management console. Right-click on Printers located under your print server machine and click Add Printer.

Step 2: Attach the printer to your computer. Choose the right port where your printer is connected.

Step 3: Choose "Use an existing printer driver on the computer" if you have an existing printer drivers otherwise choose "Install a new driver" and follow the wizard. Click Next.

Step 4: Give a friendly name to your printer and share it with other users on network. Click Next

Step 5: Click Next to finish the printer installation.

Step 6: Click Finish.

Step 7: Again, go to printer management console and right click on the printer icon. Click Manage Sharing. Go to sharing tab and check mark both options as shown in figure. Click Apply and then OK.

You have successfully configured and deployed your print server. This printer will be visible to other users on your network.

LU 4: MONITOR AND TEST THE SERVER

4.1: Test the server performance

- **Monitoring of Server**

Supervising activities in progress to ensure they are on-course and on-schedule in meeting the objectives and performance targets.

✔ **CPU Usage:**

CPU Performance and Monitoring is one of the most important aspects for what we do in computing every day.

▪ **Memory Consumption**
▪ **I/O Network**
▪ **Disk Usage**

✔ **Process:**

A process is an instance of a program running in a computer. It is close in meaning to task , a term used in some operating systems. An application that is being shared by multiple users will generally have one process at some stage of execution for each user.

✔ **Port scanning:**

A **port scan** is a method for determining which ports on a network are open.

As ports on a computer are the place where information is sent and received, port scanning is analogous to knocking on doors to see if someone is home.

✔ **Response Time:**

Is the amount of **time** it takes for a **server** to respond to a request from client.

 Windows server built-in monitoring tools:

✔ **Task Manager:** It is an interesting tool that enables you to:

▪ Verify and monitor resources performance and usage (RAM, CPU) for your server. ▪ Manage processes, applications and services.

▪ Manage users connected to your server

✔ Event Viewer:

The Windows Event Viewer shows a log of application and system messages, including errors, information messages, and warnings. It‟s a useful tool for troubleshooting all kinds of different Windows problems.

Note that even a properly functioning system will show various warnings and errors in the logs you can comb through with Event Viewer.

While there are a lot of categories, the vast amount of troubleshooting you might want to do pertains to three of them:

- Application: The Application log records events related to Windows system components, such as drivers and built-in interface elements.
- System: The System log records events related to programs installed on the system.
- Security: When security logging is enabled (it‟s off by default in Windows), this log records events related to security, such as logon attempts and resource access.

✔ Reliability and Performance Monitor:

This enables you to monitor how a computer running the Windows Server 2012 and Windows Server 2012 R2 operating system uses CPU, memory, disk, and network resources.

Performance Monitor is a system monitoring program introduced in Windows. It monitors various activities on a computer such as CPU or memory usage.

✔ Reliability and Performance Monitor.

Whereas Event Viewer allows you to monitor system and application events, Reliability and Performance Monitor(RPM) allows you to monitor and log the reliability and performance of your computer.

✔ Data collector sets

Data Collector Sets are part of the Performance Monitor tool. It provides an automated way to capture a systems overall performance.

It monitors the four subsystems, Processor, Network, Disk and Memory. It allows you to configure and schedule performance counter, event trace, and configuration data collection so that you can analyze the results and view performance reports.

4.2: Use troubleshooting tools and techniques to diagnose and correct server issues

 Troubleshoot windows server

✔ Resources for Top Areas of Support for Windows Server

✔ Best Practices Analyser

✔ Events and Errors

Learning Outcome 4.4: install, configure and maintain the antivirus for the proper protection of the systems

 Troubleshoot windows server

✔ Resources for Top Areas of Support for Windows Server

✔ Best Practices Analyser

✔ Events and Errors

 Anti-viruses on windows server

✔ System protected