POLYTECHNIC UNIVERSITY OF THE PHILIPPINES
COLLEGE OF COMPUTER AND INFORMATION SCIENCES
DEPARTMENT OF COMPUTER SCIENCE | DEPARTMENT OF INFORMATION TECHNOLOGY

System Administration and Maintenance

INSTRUCTIONAL MATERIAL FOR STUDENTS

Compiled by:

CARLO G. INOVERO
BSIT 4-1N
BSIT 4-1

Introduction to System Administration

Operating Systems

Objectives

In this chapter, the following objectives will be discussed:

- Installation, Configuration, and Maintenance of Microsoft Windows Server 2019
- Installation, Configuration, and Maintenance of Apple MacOS Server

Introduction to Windows Server: https://www.youtube.com/watch?v=zSRBctvCHJ8

Windows Server

Windows Server is a brand name for a group of server operating systems released by Microsoft since 2003. The first Windows server edition to be released under that brand was Windows Server 2003. However, the first server edition of Windows was Windows NT 3.1 Advanced Server, followed by Windows NT 3.5 Server, Windows NT 3.51 Server, Windows NT 4.0 Server, and Windows 2000 Server. Windows 2000 Server was the first server edition to include Active Directory, DNS Server, DHCP Server, Group Policy, as well as many other popular features used today.

Windows Server 2019 Installation Guide

Creating the Media Installer for Windows Server 2019

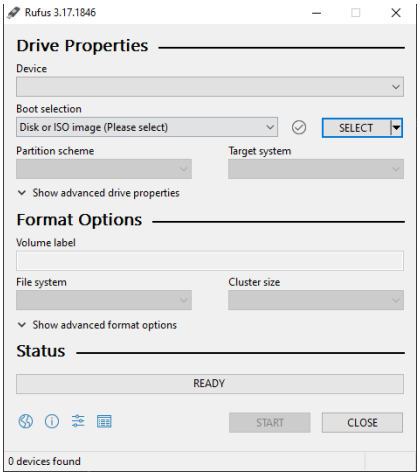
Step 1: Download and Install Rufus in this link:
https://github.com/pbatard/rufus/releases/download/v3.17/rufus-3.17.exe

Step 2: Download the Microsoft Windows Server 2019 ISO File in this link:

https://www.microsoft.com/en-US/evalcenter/evaluate-windows-server-2019?filetype=ISO

Step 3: Open Rufus and plug in an empty USB Drive

Step 4: Select the USB drive and the downloaded ISO, then click Start



Installation Guide:

Video Reference: Microsoft Windows Server 2019 Installation
https://www.youtube.com/watch?v=fRBV-NzYAZw

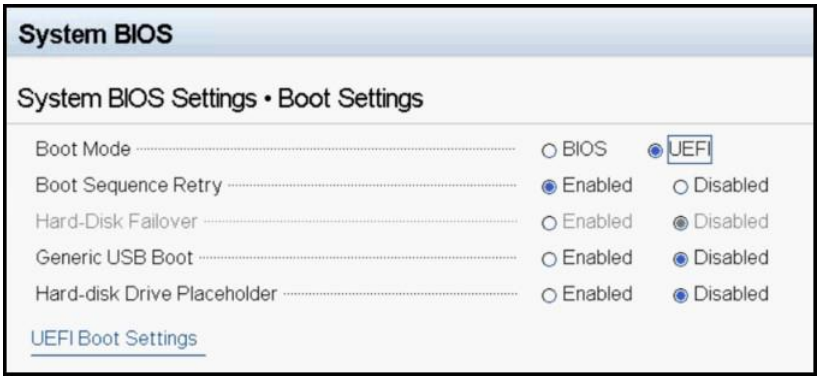
Step 1: Connect a keyboard, monitor, mouse, and other required peripherals to your system.

Step 2: Turn on your system and the connected peripherals.

Step 3: Press F2 to go to the System Setup page

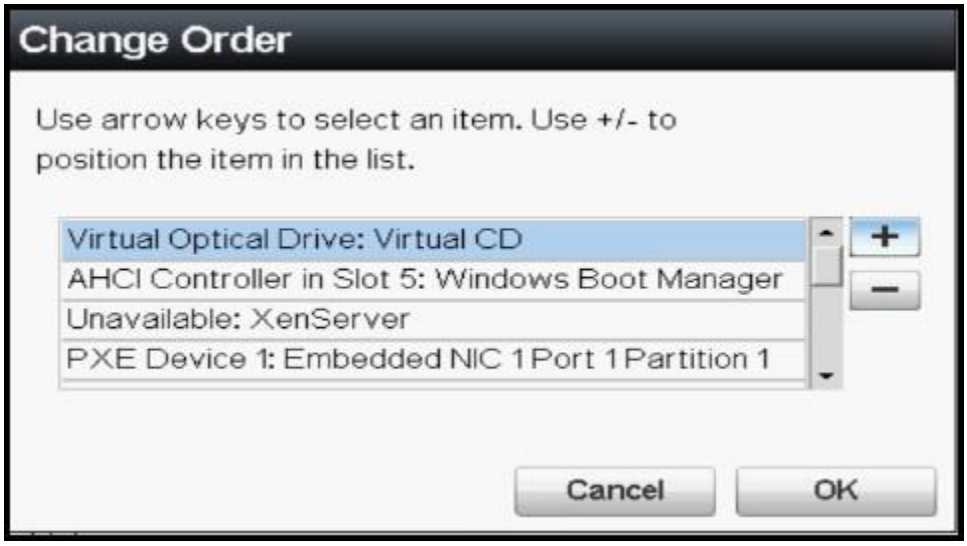
Step 4: On the System Setup page, click System BIOS, and then click Boot Settings

Step 5: Ensure that UEFI is selected as the Boot Mode.



Step 6: Click UEFI Boot Settings, and then click UEFI Boot Sequence

Step 7: In the Change Order window, ensure that Virtual Optical Drive: Virtual CD is selected as your boot device, and then click OK



Step 8: Click Back.

Step 9: Click Finish, and then click Yes

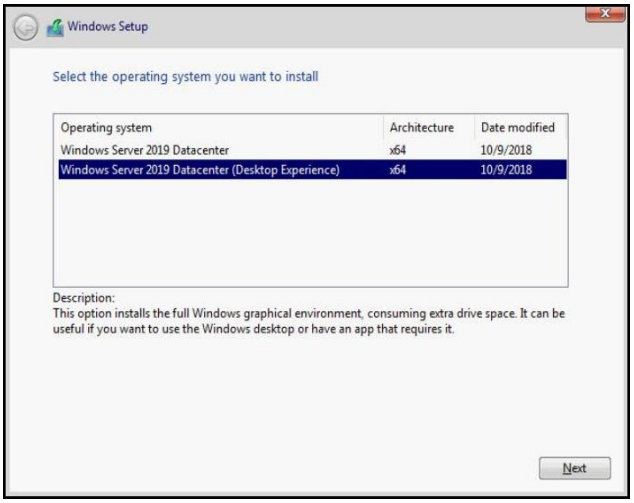
Step 10: Click Finish to exit the System Setup page, and then click Yes to reboot the system.

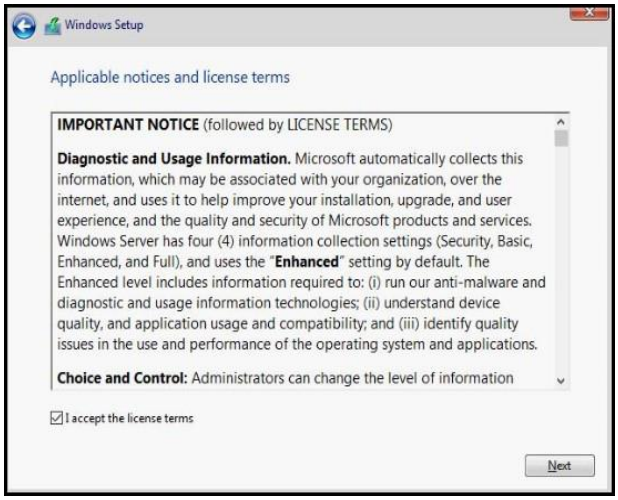
Step 11: Insert the Microsoft Windows Server 2019 media into the DVD drive.

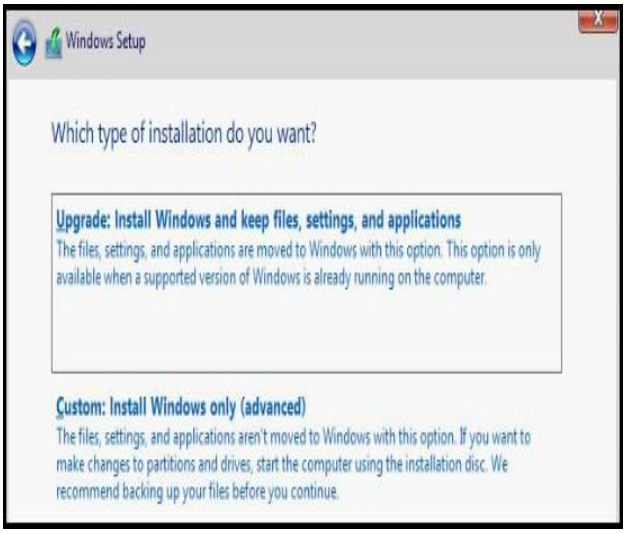
When the system starts to read the media, the following message is displayed

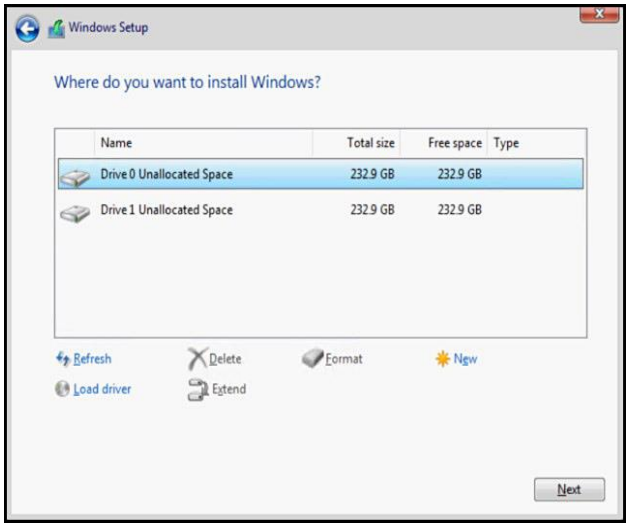
Step 12: After the files are loaded, select the language in which you want to install the OS

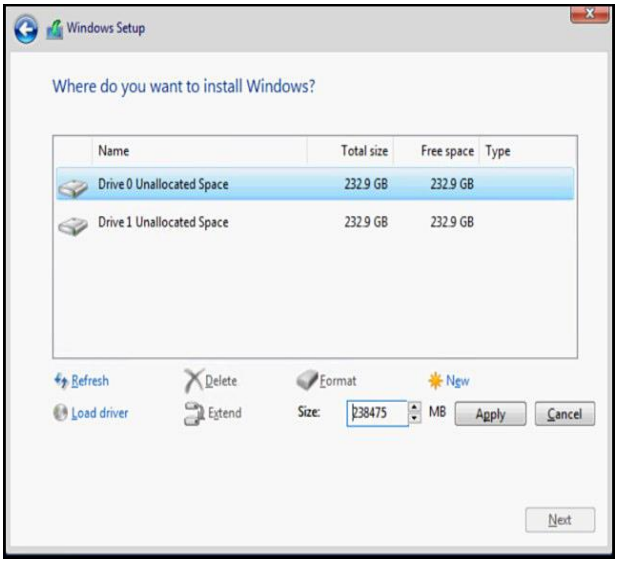
Step 13: Select the language, time and currency format, keyboard or input method, and then click Next, then follow the steps as shown in the images below:

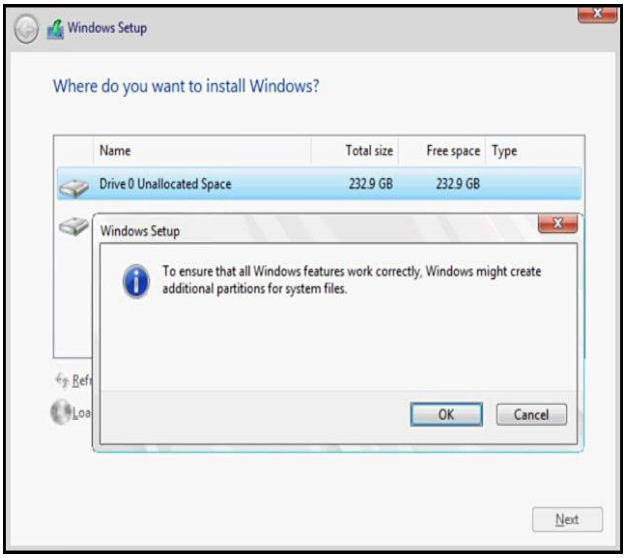

Windows Setup
Select the operating system you want to install
Operating system
Architecture
Date modified
Windows Server 2019 Datacenter
x64
10/9/2018
Windows Server 2019 Datacenter (Desktop Experience)
x64
10/9/2018
Description:
This option installs the full Windows graphical environment, consuming extra drive space. It can be useful if you want to use the Windows desktop or have an app that requires it.
Next

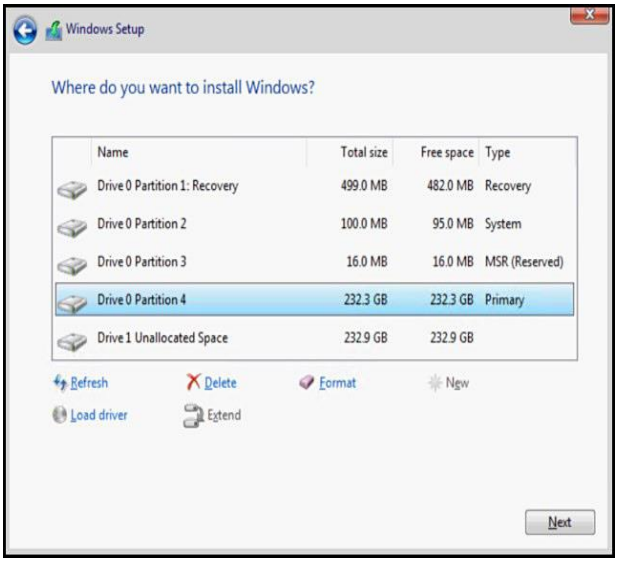

Windows Setup
Applicable notices and license terms
IMPORTANT NOTICE (followed by LICENSE TERMS)
Diagnostic and Usage Information. Microsoft automatically collects this information, which may be associated with your organization, over the internet, and uses it to help improve your installation, upgrade, and user experience, and the quality and security of Microsoft products and services. Windows Server has four (4) information collection settings (Security, Basic, Enhanced, and Full), and uses the "Enhanced" setting by default. The Enhanced level includes information required to: (i) run our anti-malware and diagnostic and usage information technologies; (ii) understand device quality, and application usage and compatibility; and (iii) identify quality issues in the use and performance of the operating system and applications.
Choice and Control: Administrators can change the level of information
I accept the license terms
Next

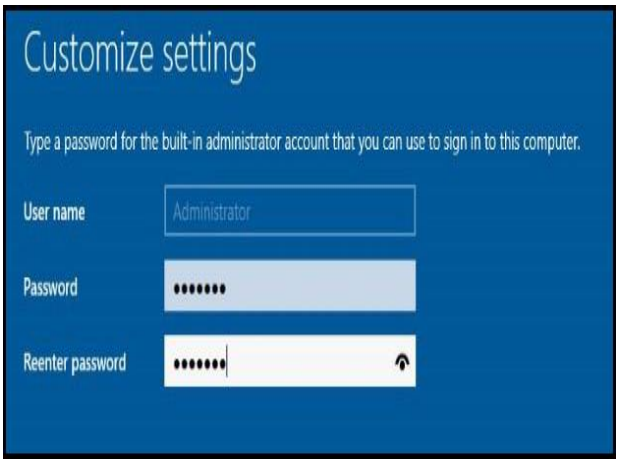

Windows Setup
Which type of installation do you want?
Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.
Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.


Windows Setup
Where do you want to install Windows?
Name
Total size
Free space
Type
Drive 0 Unallocated Space
232.9 GB
232.9 GB
Drive 1 Unallocated Space
232.9 GB
232.9 GB
Refresh
Delete
Format
New
Load driver
Extend
Next


Windows Setup
Where do you want to install Windows?
Name
Total size
Free space
Type
Drive 0 Unallocated Space
232.9 GB
232.9 GB
Drive 1 Unallocated Space
232.9 GB
232.9 GB
Refresh
Delete
Format
New
Load driver
Extend
Size:
238475
MB
Apply
Cancel
Next


Windows Setup
Where do you want to install Windows?
Name
Total size
Free space
Type
Drive 0 Unallocated Space
232.9 GB
232.9 GB
Windows Setup
To ensure that all Windows features work correctly, Windows might create additional partitions for system files.
OK
Cancel
Next



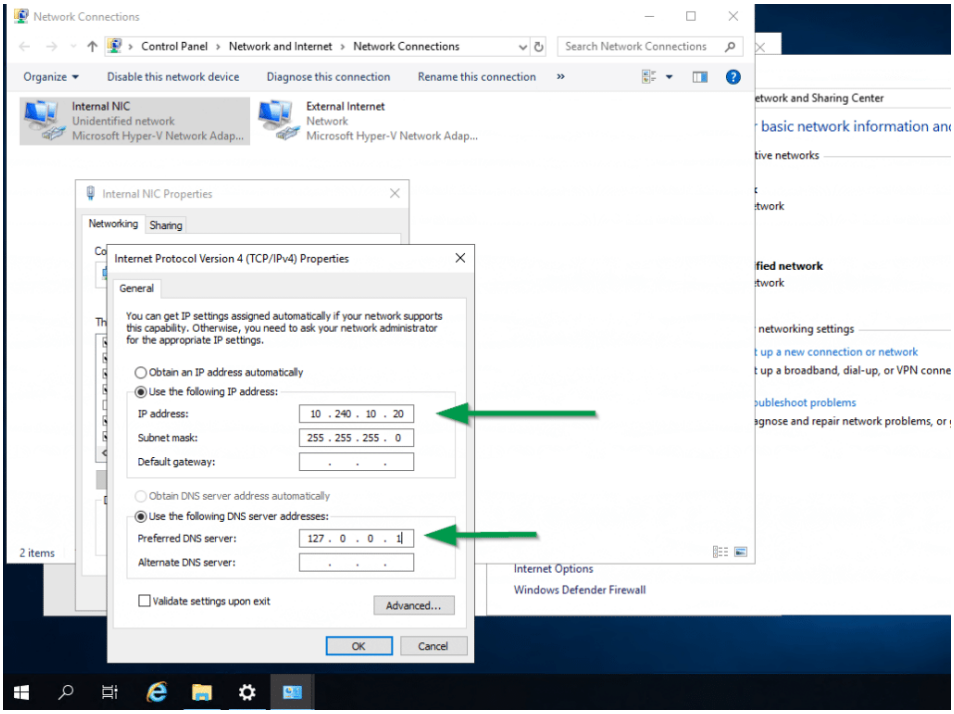


Step 14: After the system reboots, press Ctrl+Alt+Delete to log in to the system

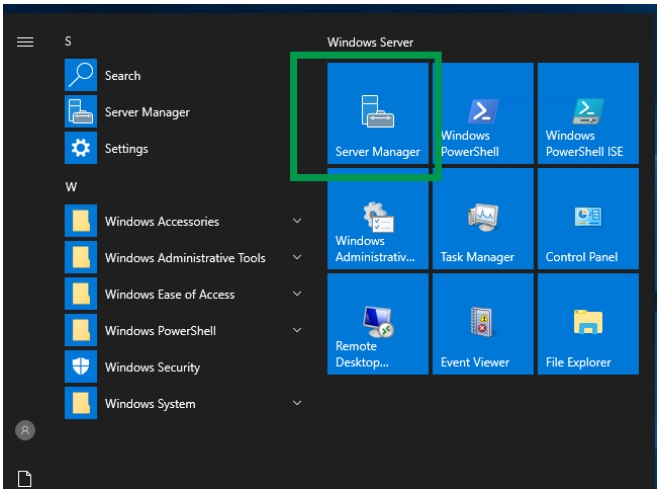
Step 15: Type the administrator password, and then press Enter

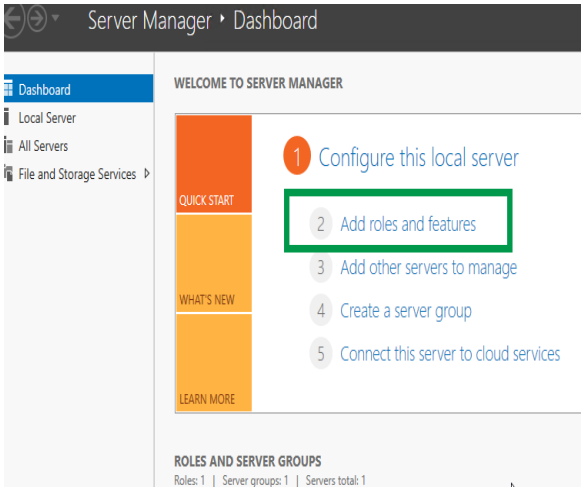
Windows Server 2019 Configuration Guide

Step 1: Set a static IP address for the TCP/IPv4 virtual machine INTERNAL NIC as shown here in the example below. Use your own private IP address subnet range. use a 10.x.x.x or 172.16.x.x or 192.168.x.x IP range



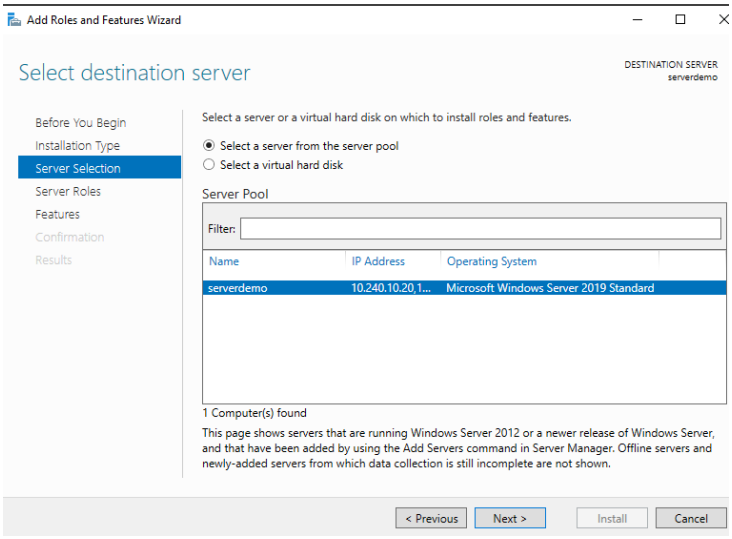
Step 2: Launch “Server Manager” from the start menu and select “Add Roles and Features“.



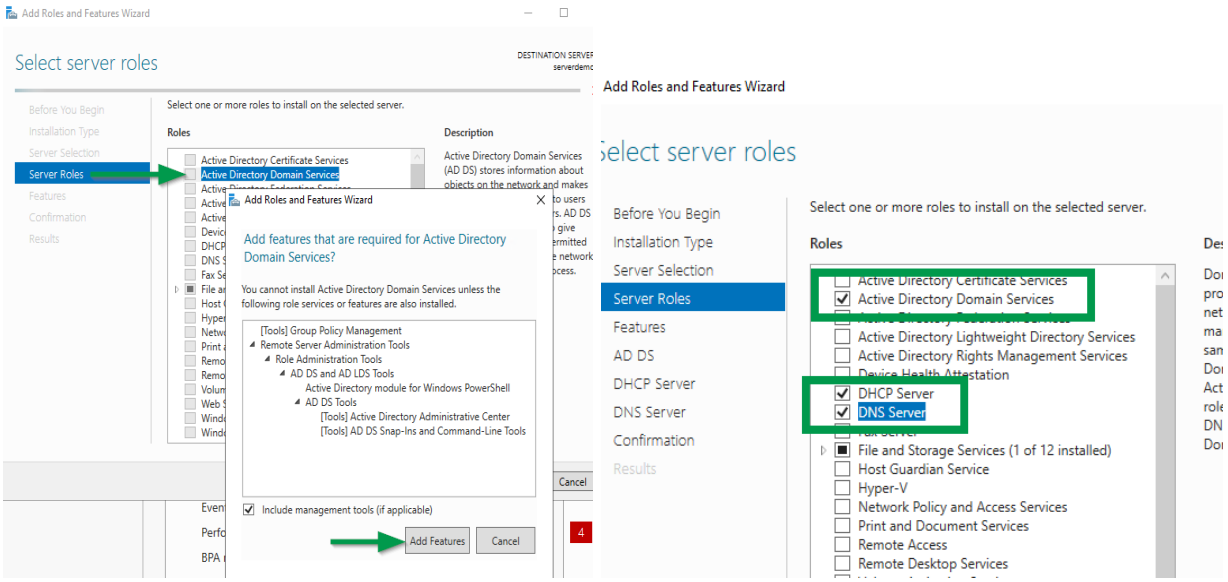


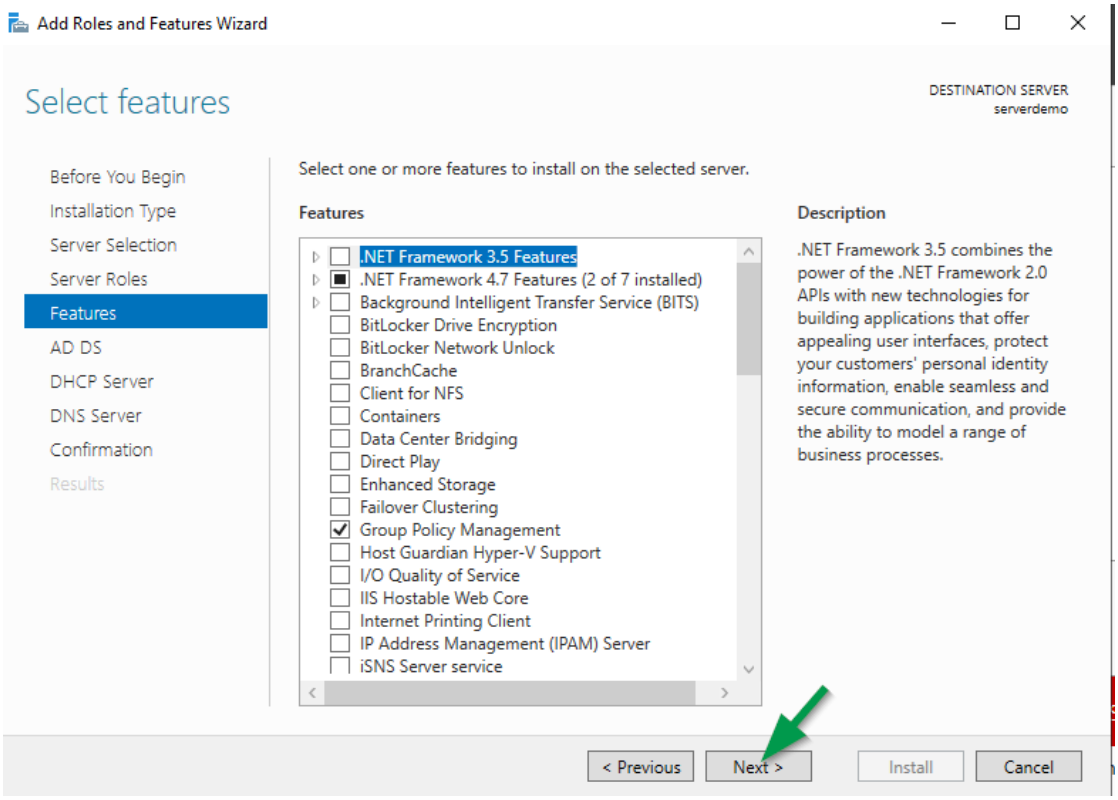
Step 3: Click Next at the “Before You Begin” screen, and “Next” at the “Select installation type” screen. Be sure the installation type is set to the default “Role-based or feature-based installation“.

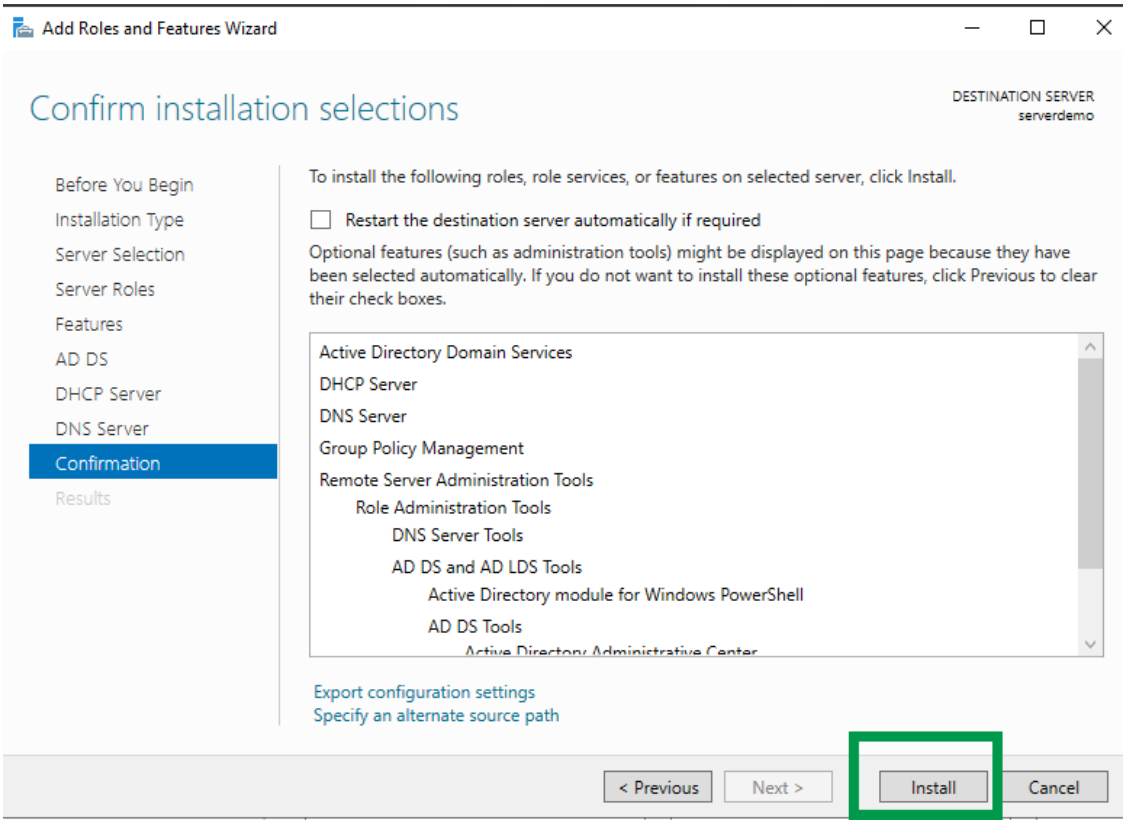
Step 4: At the “Select destination server” click Next to select your local server.



Step 5: At the “Server Roles” screen be sure to select “Active Directory Domain Services“, “DHCP“, and “DNS“. Select “Add Features” for each one and click Next.


Add Roles and Features Wizard
Select server roles
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Description
Add Roles and Features Wizard
Add features that are required for Active Directory Domain Services?
You cannot install Active Directory Domain Services unless the following role services or features are also installed.
[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
Include management tools (if applicable)
Add Features
Cancel
Add Roles and Features Wizard
Select server roles
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DHCP Server
DNS Server
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
DHCP Server
DNS Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services

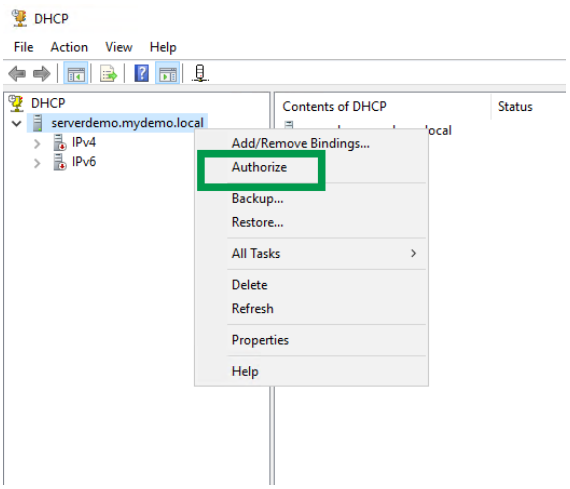

Add Roles and Features Wizard
Select features
DESTINATION SERVER
serverdemo
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DHCP Server
DNS Server
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.7 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Containers
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
Host Guardian Hyper-V Support
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
iSNS Server service
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel

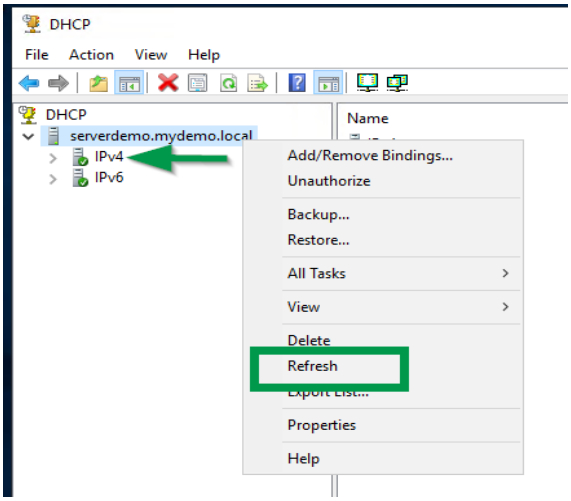


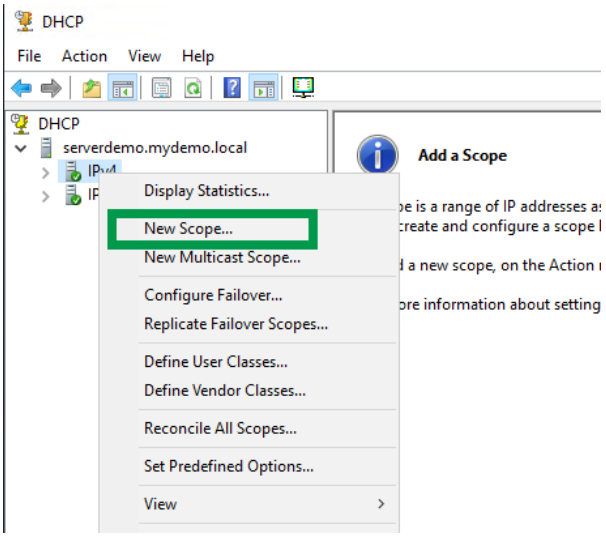
Configure DHCP Server Options and Authorize Server

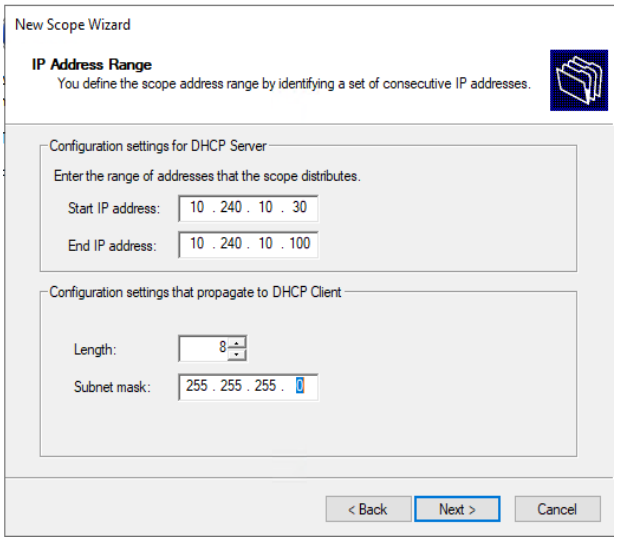
The final step that needs to be performed is authorizing the DHCP server and creating / enabling the DHCP client scope.

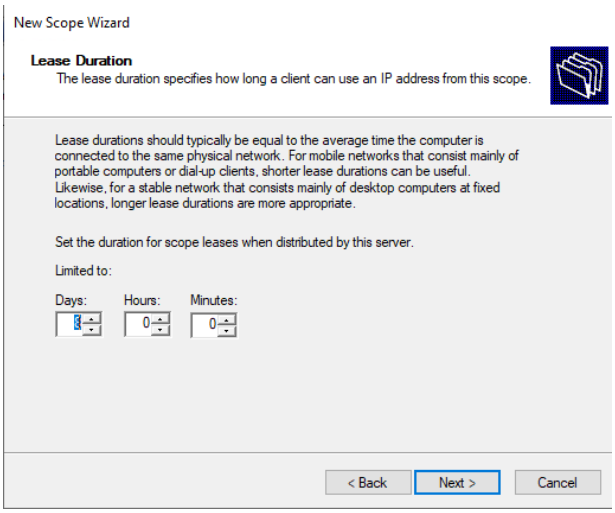
Launch DHCP Manager from the start menu > Windows Administrative Tools. Exp[and your DHCP server, right-click on the server name and select “Authorize“. Right-click on the server again and select “Refresh”. You should see all green check boxes now.

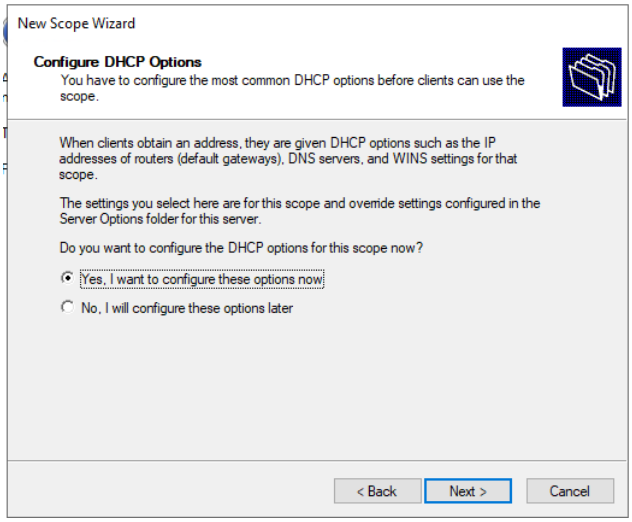

DHCP
File Action View Help
DHCP
serverdemo.mydemo.local
IPv4
IPv6
Contents of DHCP
Status
Add/Remove Bindings...
Authorize
Backup...
Restore...
All Tasks
Delete
Refresh
Properties
Help


DHCP
File Action View Help
DHCP
serverdemo.mydemo.local
IPv4
IPv6
Name
Add/Remove Bindings...
Unauthorize
Backup...
Restore...
All Tasks
View
Delete
Refresh
Properties
Help


DHCP
File Action View Help
DHCP
serverdemo.mydemo.local
Add a Scope
Display Statistics...
New Scope...
New Multicast Scope...
Configure Failover...
Replicate Failover Scopes...
Define User Classes...
Define Vendor Classes...
Reconcile All Scopes...
Set Predefined Options...
View


New Scope Wizard
IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.
Configuration settings for DHCP Server
Enter the range of addresses that the scope distributes.
Start IP address: 10 . 240 . 10 . 30
End IP address: 10 . 240 . 10 . 100
Configuration settings that propagate to DHCP Client
Length: 8
Subnet mask: 255 . 255 . 255 . 0
< Back
Next >
Cancel


New Scope Wizard
Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful.
Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.
Set the duration for scope leases when distributed by this server.
Limited to:
Days: 8
Hours: 0
Minutes: 0
< Back
Next >
Cancel


New Scope Wizard
Configure DHCP Options
You have to configure the most common DHCP options before clients can use the scope.
When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.
Do you want to configure the DHCP options for this scope now?
Yes, I want to configure these options now
No, I will configure these options later
< Back
Next >
Cancel

Microsoft Windows Server 2019 Maintenance Guide

Update Guide (Option 1):

1. Navigate to Settings > Update & Security > Windows Updates.
2. Click Check for Updates. Windows downloads and installs all available updates.
3. The update statuses are Downloading, Pending Install, and Pending Restart.
4. The server reboots outside of the active hours, 8:00 AM to 5:00 PM, unless otherwise specified. You also have the option to schedule the reboot.

Update Guide (Option 2):

1. Open PowerShell® and type sconfig.
2. Type 6 to open the Windows Updates menu.
3. Type a to look for all available updates or r to search for only recommended updates.
4. All available updates now display in the list.
5. Type n to close the menu without installing any updates.

MacOS Server Introduction

MacOS Server, formerly Mac OS X Server and OS X Server, is a series of Unix-like server operating systems developed by Apple Inc., based on macOS and later add-on software packages for the latter. macOS Server adds server functionality and system administration tools to macOS and provides tools to manage both macOS-based computers and iOS-based devices.

MacOS Server Requirements:

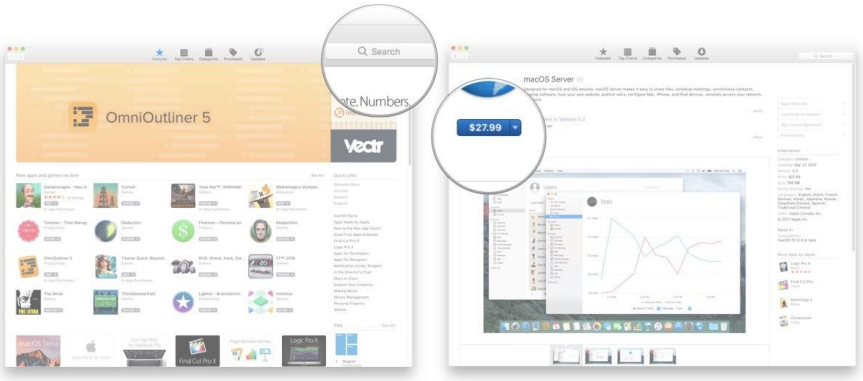
- Have macOS 11.3 or later installed
- Have at least 4 GB of RAM
- Have at least 10 GB of storage space
-

MacOS Server Installation Guide

Step 1: Launch the Apple App Store application.

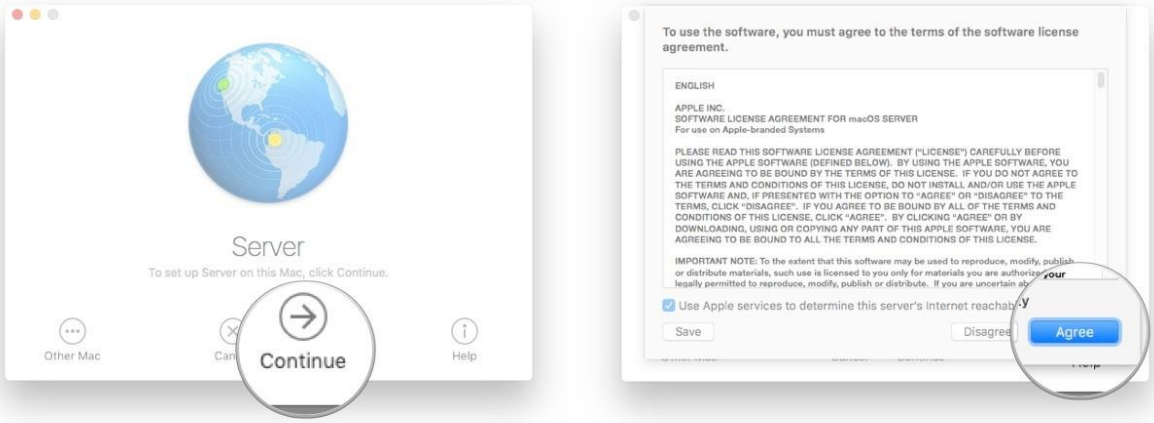
Step 2: Download macOS Server — or type "macOS Server" into the search bar, top right, if that link doesn't work for you.

Step 3: Click Buy macOS Server.



Step 4: When the macOS Server automatically starts up, click Continue

Step 5: Agree to the User Agreement



MacOS Server Configuration Guide

Step 1: On your Mac, click the Finder icon in the Dock to open a Finder window, then click Network in the Locations section of the sidebar.

If no items appear in the Locations section of the sidebar, hold the pointer over the word Locations, then click the arrow .

Step 2: In the Finder window, double-click the computer you want to connect to, then click Connect As.

If you're connecting to a Mac that has screen sharing turned on, and you have the appropriate privileges, you can also click Share Screen.

Step 3: Select how you want to connect to the Mac:

Guest: You can connect as a Guest user if the shared computer permits guest access.

Registered User: Connect to the other Mac using a valid login name and password. If “Only these users” is selected on the other Mac, make sure the login name you’re using is on the list of allowed users.

Using an Apple ID: Connect to the other Mac using an Apple ID. You must be set up in Users & Groups preferences with this Apple ID, on both this Mac and the other Mac.

If necessary, enter your user name and password, then select volumes or shared folders on the server.

In some cases you need the network area or workgroup for the shared computer. If you don’t have this information, contact the computer’s owner or your network administrator.

Step 4: Reconnecting to Other Servers

- Choose Apple menu > Recent Items, then choose from the list of recent servers.
- In the Finder , choose Go > Connect to Server, click the pop-up menu to the far right of the Server Address field, then choose a recent server.
- Add shared computers, network areas, and workgroups to the Finder sidebar. Select the item, then choose File > Add To Sidebar.
- Add a shared computer or server to your list of favorites. In the Finder, choose Go > Connect to Server, enter the network address, then click the Add button.

MacOS Server Maintenance Guide

Step 1: Launch the App Store

Step 2: Download macOS Sierra — or type "macOS Sierra" into the search bar, top right, if that link doesn't work for you.

Step 3: Click the Download Button

Step 4: Wait for the download to complete

Step 5: Click the Continue button when the macOS Sierra installer starts.

Step 6: Click Agree to accept the User Agreement.

Step 7: Click Install on the hard drive you want to use (if you have multiple options.)

Step 8: Wait for the upgrade to complete.

Introduction to MacOS Server: https://www.youtube.com/watch?v=VuSn2OO2TW0

Operating System Installation

Depending on the type of operating system, the installation method differs. The installation of Windows, Mac, Linux, and Solaris operating systems will be covered in this chapter.

Linux OS Installation

Linux is a free and open-source operating system that allows anyone with programming skills to customize and construct their own operating system to meet their own needs. It has gotten more user-friendly over time and now supports a variety of features such as

- Dependable when utilized with servers
- Antivirus is not required.
- For many years, a Linux server can run nonstop with the boot.

This section contains information about installing the Red Hat Enterprise Linux (RHEL), SUSE Enterprise Linux System (SLES) and Oracle Enterprise Linux (OEL) operating systems and system-specific drivers onto your server.

Table 1: OS Installation Task Map

Task	Installation Task	Instruction
Set up the client's server	Install server hardware and configure the service processor	Server Installation Guide
Prepare the client's system for OS installation	Set the display environment. If necessary, erase the primary boot disk.	Operating System Installation Overview and Preparation (oracle.com)
Set up the system for a RAID or non-RAID configuration based on the SAS controller card	The client's server supports two SAS controller cards. RAID setup is different for each card.	Configuring RAID (oracle.com)
Review the Server Product Notes	The product notes contain late-braeking news about the Linux OS software and patches.	Server Product Notes
Install the Linux OS	Choose an installation method and locate the installation instructions.	OS Installation Methods - Linux

Install the system-specific drivers from the Tools and Drivers CD.	Install the system-specific drivers needed to run the Linux OS on your server.	Installing the System-Specific Drivers
Run the up2date or SUSEWatcher utility.	Patches are available from the SunSolve Patch Portal at: http://www.sunsolve.sun.com	Running the up2date Utility for the RHEL OS or Running the SuSEWatcher Utility for the SLES OS

OS Installation Methods - Linux

- Sun Installation Assistant (SIA)

  The Sun Installation Assistant (SIA) is a convenient, front-end application designed to assist you in installing supported versions of Linux and Windows on your server. SIA supplements the standard installation utilities and procedures that ship with your operating system; it does not replace them.
- CD/DVD Media

  You can install a Linux OS using the local server DVD drive or a USB connected CD or DVD drive connected to the server.

  To Install Linux Using Local CD/DVD Drive:

  See the instructions for basic installation in the document that corresponds to the OS you are installing:

  - Red Hat Enterprise Linux Installation Guide for the x86, Itanium, and AMD64 Architectures at http://www.redhat.com/docs/manuals/enterprise/
  - SUSE Linux Enterprise Server Administration and Installation at http://www.novell.com/documentation/suse.html
  - Oracle Enterprise Linux 4 Installation at http://www.oracle-base.com/articles/linux/OracleEnterpriseLinux4Installation.php
  - Oracle Enterprise Linux 5 Installation at: http://www.oracle-base.com/articles/linux/OracleEnterpriseLinux5Installation.php

- Network or PXE

  This section describes how to boot the Linux from a PXE network environment.

  Before beginning the installation, take note of the prerequisites for the OS that you plan to install.

  - Red Hat Linux and Oracle Enterprise Linux Prerequisites
  - SUSE Linux Enterprise Server Prerequisites

  To Install Linux Using PXE:

  1. Ensure that the PXE network environment is properly set up and the SLES installation media is available for PXE boot.

  2. Reset the power on the server.

     For example:

     - From the ILOM web interface, select Remote Control --> Remote Power Control, then select the Power Cycle option from the Host action drop-down menu.
     - From the local server, press the Power button (approximately 1 second) on the front panel of the server to power off the server, then press the Power button again to power on the server.
     - From the ILOM CLI on the server SP, type: reset /SYS

     The BIOS screen appears.

  3. Press F8 to specify a temporary boot device.
     The Please Select Boot Device menu appears listing the available boot device.

  4. In the Boot Device menu, select the PXE installation boot device (physical port) that is configured to communicate with your network installation server.
     The network bootloader loads, and a boot prompt appears. Wait for the five second time-out and the installation kernel will begin to load.

  5. Proceed with the installation as described in the OS documentation.
     - Red Hat Enterprise Linux Installation Guide for the x86, Itanium, and AMD64 Architectures at http://www.redhat.com/docs/manuals/enterprise/
     - SUSE Linux Enterprise Server Administration and Installation at http://www.novell.com/documentation/suse.html

- Oracle Enterprise Linux 4 Installation at http://www.oracle-base.com/articles/linux/OracleEnterpriseLinux4Installation.php
- Oracle Enterprise Linux 5 Installation at: http://www.oracle-base.com/articles/linux/OracleEnterpriseLinux5Installation.php

- Remote KVMS

  This method uses the RKVMS capability of the ILOM or ELOM to install the Linux OS on your server from a remote networked system. The CD/DVD drive of the remote system (virtual CD-ROM) is used to access the OS media, and all output of the server is displayed on the remote system (remote console).

  Additional information about the RKVMS can be found in the ELOM or ILOM documentation.

  Requirements for Remote KMVS (RKVMS) over IP installation include:
  - Remote system connected to the network.
  - One of the following browsers on the remote system: Internet Explorer, Mozilla, or Firefox.
  - CD/DVD drive connected to the remote system.
  - Media for installing the OS of your choice.
  - SP of your server set up as instructed in the server installation guide.
  - User must be logged into the remote system as root.

  To Install Linux Using Remote KVMS Over IP With Virtual CD/DVD

  1. On a remote system, open a browser, and enter the IP address of the service processor for the server on which you want to install the OS.
     - The ILOM or ELOM login screen appears.

  2. At the login screen, enter the username and password for an account with administrator privileges, and click Login.
     - The web GUI main menu appears.

  3. Disable the session timeout:
     a. From the main menu, click the System Information tab, and then click the Session Time-Out submenu tab.
        - The Session Time-Out screen appears.
     b. Click the Disable Timeout radio button, and then click Submit.

  4. From the main menu, click the Remote Control tab and select Redirection.
     - The Screen appears with a Launch Redirection button.

  5. Click the Launch Redirection button to open a remote console window.
     - A screen appears with a Launch button. It also identifies your current host name, IP address, and user name.

6. Click Launch.

7. Mount the OS CD/DVD or ISO file to be installed on the server onto the virtual CDROM.

   For ILOM:

   a. In the Devices menu, select the following:
      - CD ROM if you are using a physical CD.
      - CD ROM Image if you are using an ISO file.

   b. Depending on your selection, a dialog directs you to select either a CD/DVD drive, or a file.

   For ELOM:

   a. In the remote console screen, select Storage and then select Mount Devices.
      - The Device Configuration screen appears.

   b. In the Storage 1 Source drop-down list, select the CD/DVD drive to be used for installing the OS.

8. Click Submit.

9. Reboot the system.
   - The system will boot from the virtual CD.

10. Proceed with the installation as described in the OS documentation.
    - Red Hat Enterprise Linux Installation Guide for the x86, Itanium, and AMD64 Architectures at http://www.redhat.com/docs/manuals/enterprise/
    - SUSE Linux Enterprise Server Administration and Installation at http://www.novell.com/documentation/suse.html
    - Oracle Enterprise Linux 4 Installation at http://www.oracle-base.com/articles/linux/OracleEnterpriseLinux4Installation.php
    - Oracle Enterprise Linux 5 Installation at: http://www.oracle-base.com/articles/linux/OracleEnterpriseLinux5Installation.php

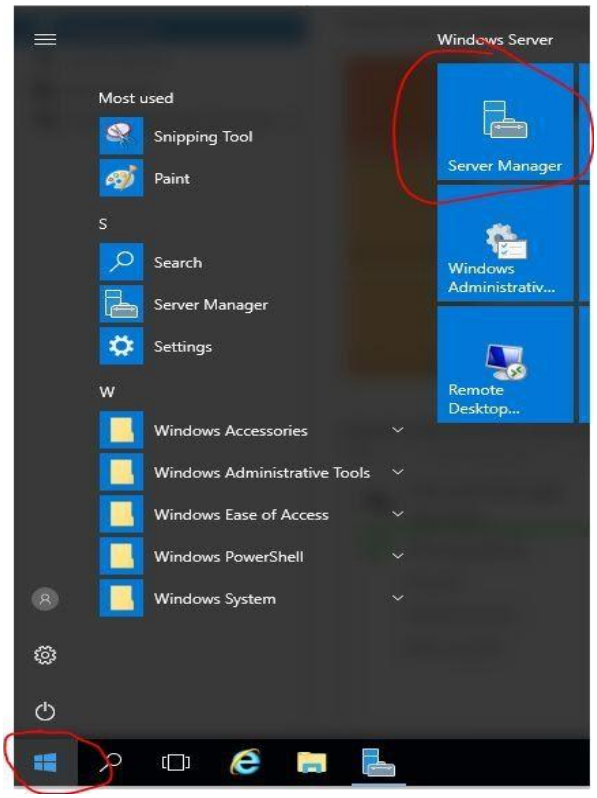
Read more on: https://docs.oracle.com/cd/E19150-01/820-1853-16/Chap5.html

INSTALL AND CONFIGURE DHCP SERVER ON WINDOWS SERVER

A DHCP server (Dynamic Host Configuration Protocol) is a server that automatically assigns IP addresses to computers and other devices on the network. Without a DHCP server, each device on the network would need to be manually configured with an IP address.

Every device on the network needs an IP address to access network resources such as the internet, applications and even making phone calls. With a DHCP server this entire process is automated and can be managed from a centralized server. When mobile devices move from one office to another it may require a new IP address. DHCP handles this automatically providing a new IP addresses when the device moves to another location. Without a DHCP server there would be an overwhelming amount of manual configuration assigning IP addresses to devices on the network. A DHCP server is a huge time saver.

Recommended Tool: SolarWinds IP Address Manager



How to Install DHCP Server

These guides was created using Windows Server 2016. The steps should be similar for other server versions.

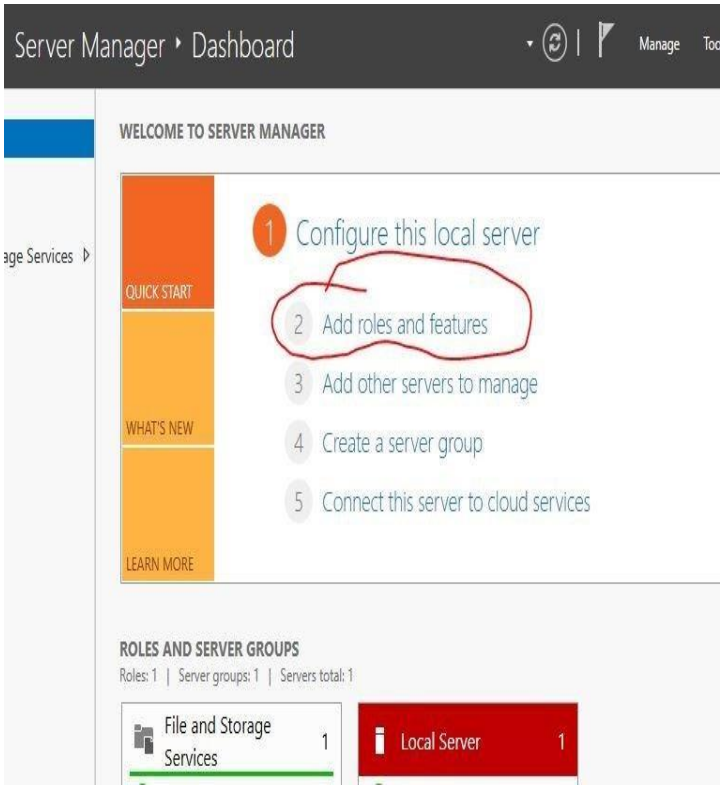
Step 1: Open Server Manager

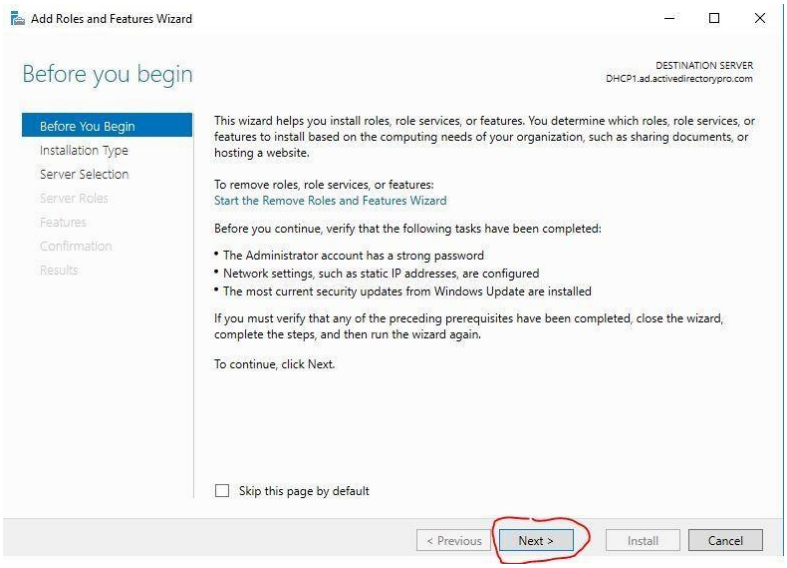
Click the start button then click the Server Manager

Step 2: Add roles and features

On the server manager dashboard click “Add roles and features” This will start the add roles and features wizard

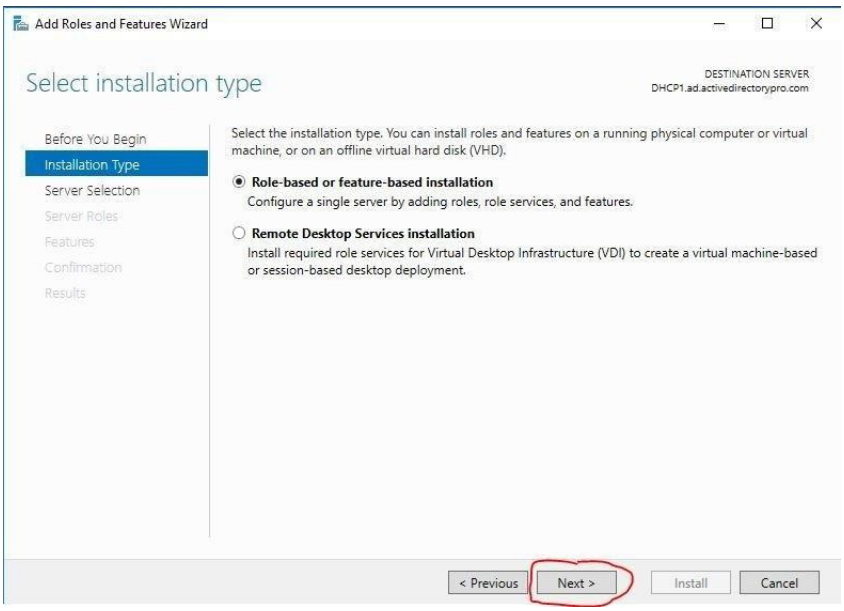
Click next on the before you begin page.





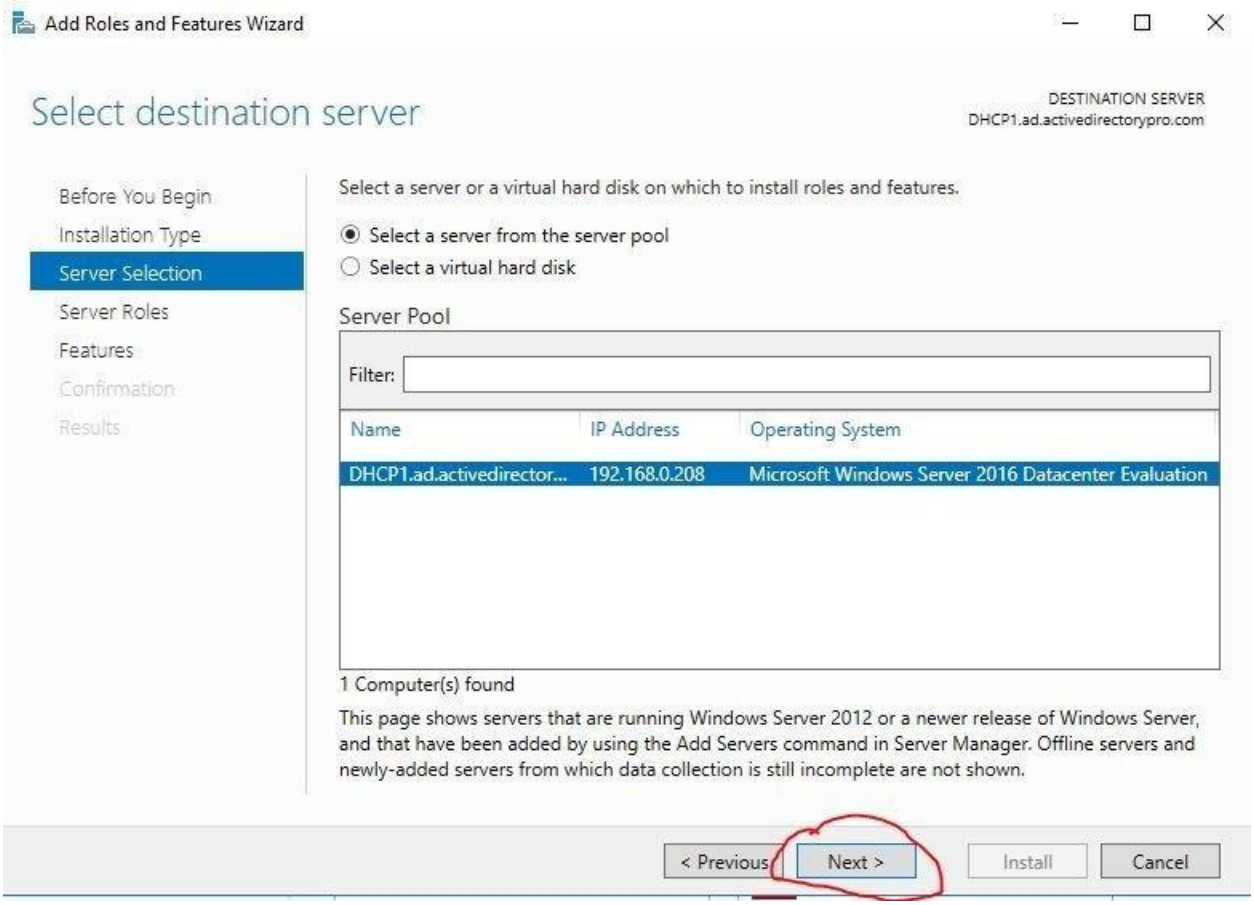
Step 3: Select Role-based or feature-based installation

Make sure “Role-based or feature-based installation is selected and click next



Step 4: Select destination server

On this page choose the server you want the DHCP service installed on. In this example I'll be choosing the local server.

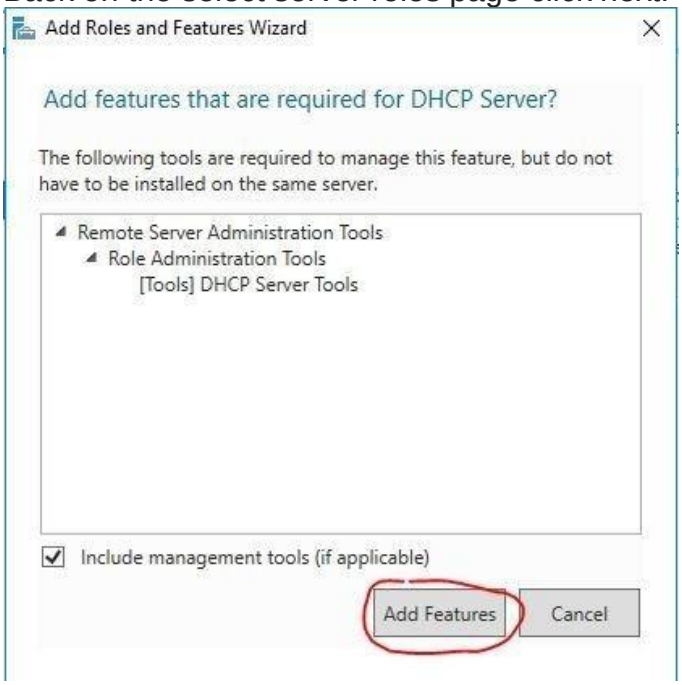


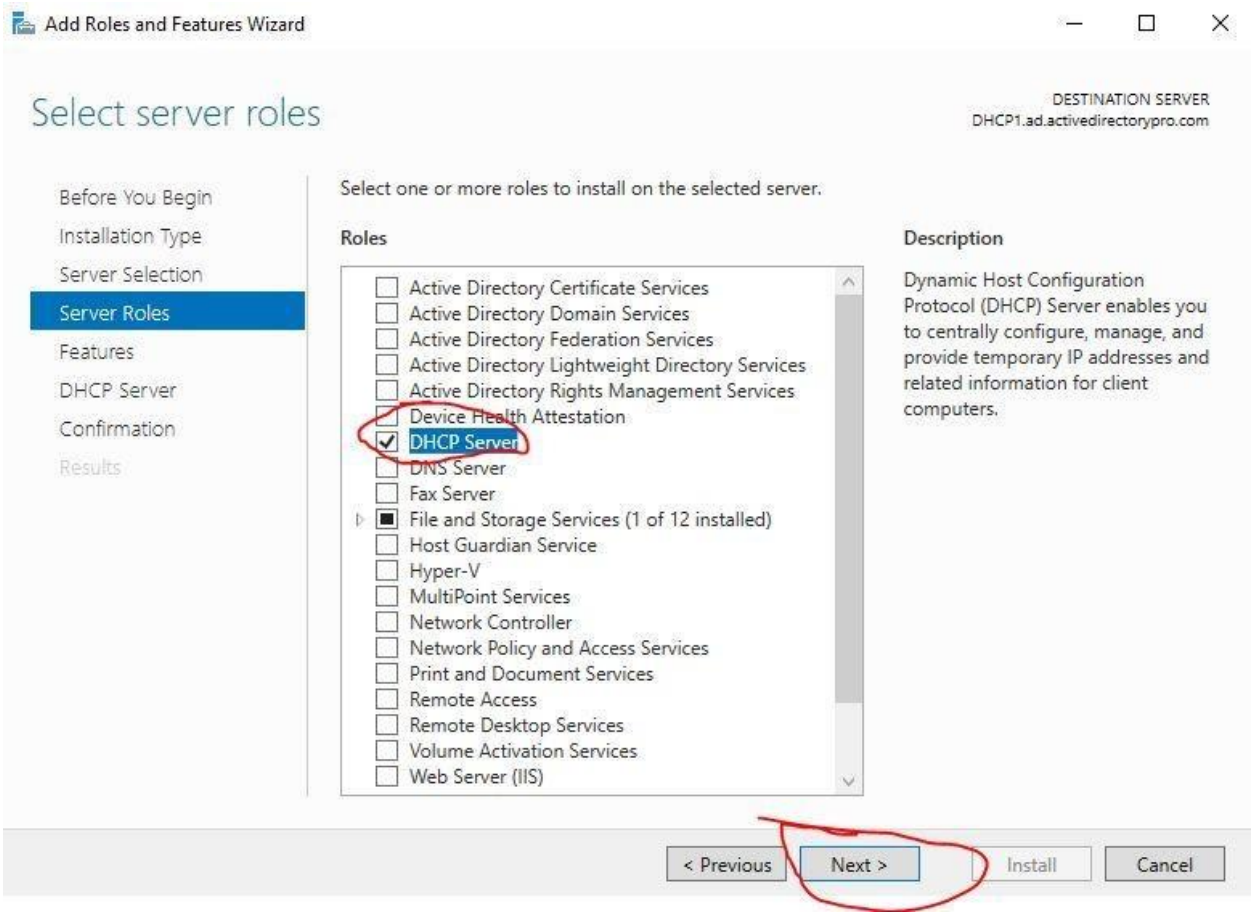
Step 5: Select server roles

On this page you want to select the DHCP server roles and click next.

When you select the roll, you will get a pop up asking to add features that are required for DHCP server. Click add features

Back on the select server roles page click next.



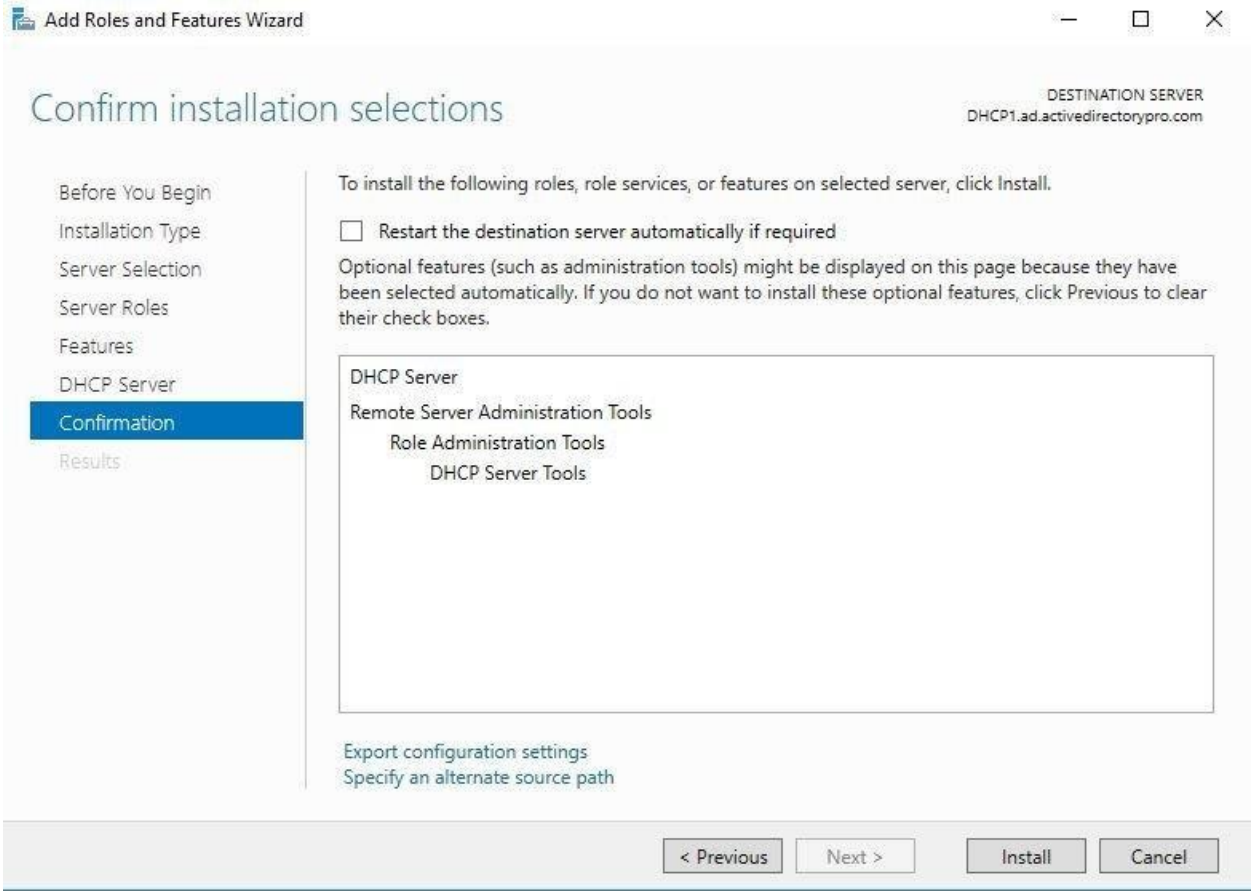


Step 6: Feature, DHCP Server

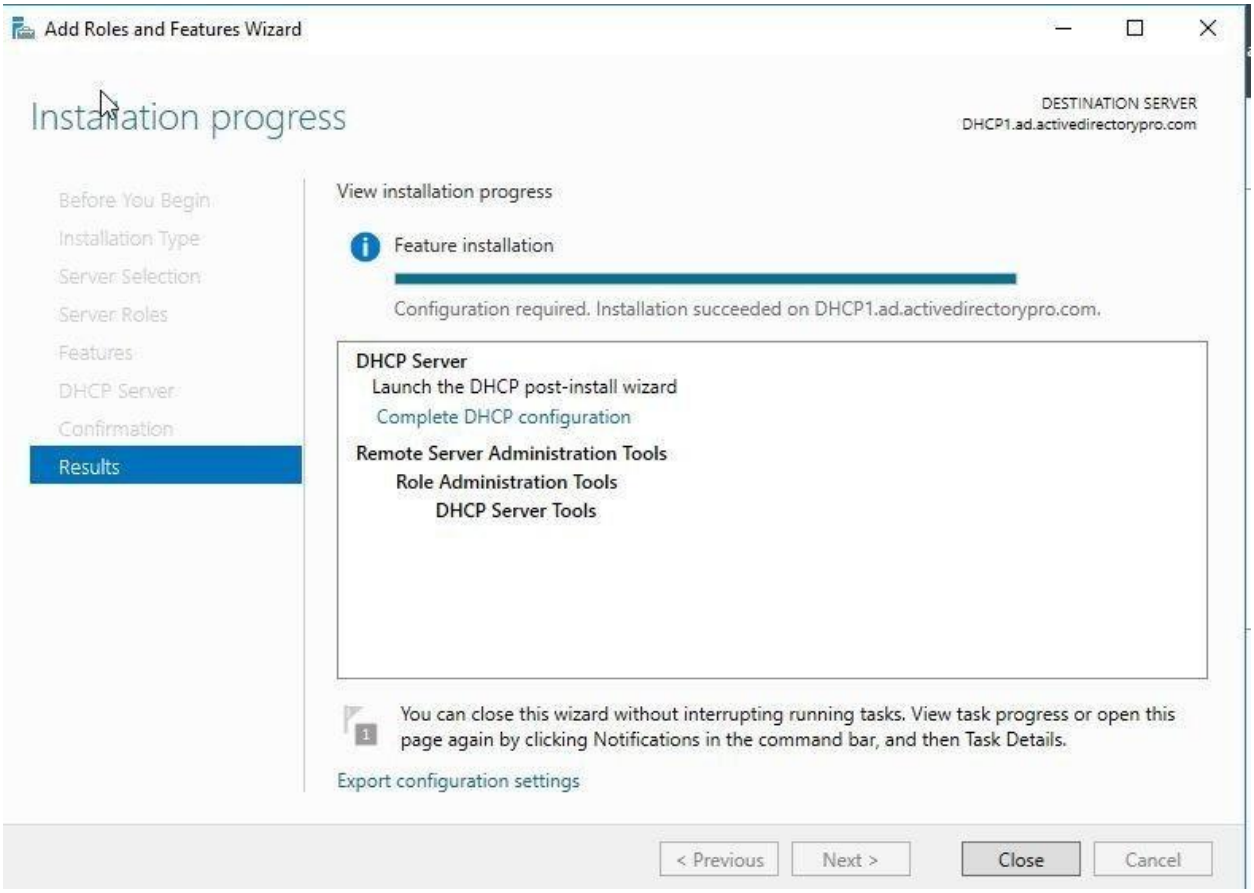
On the features screen click next
On the DHCP server click next

Step 7: Confirmation

On the confirmation page you can select to automatically restarted the server if required. On 2016 server it does not require a restart.



Click install and the install will start.
You will get an install progress page; it will say install succeeded when complete.



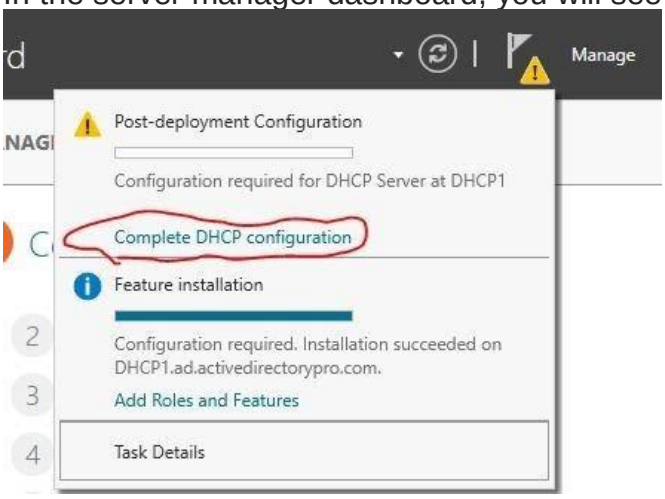
That completes the install of the DHCP role. Move onto the next section for steps on configuring the DCHP server.

CONFIGURE DHCP SERVER

If you followed the steps above you should now have the DHCP service installed.
But it still needs to be configured.

Step 1: Server Manager

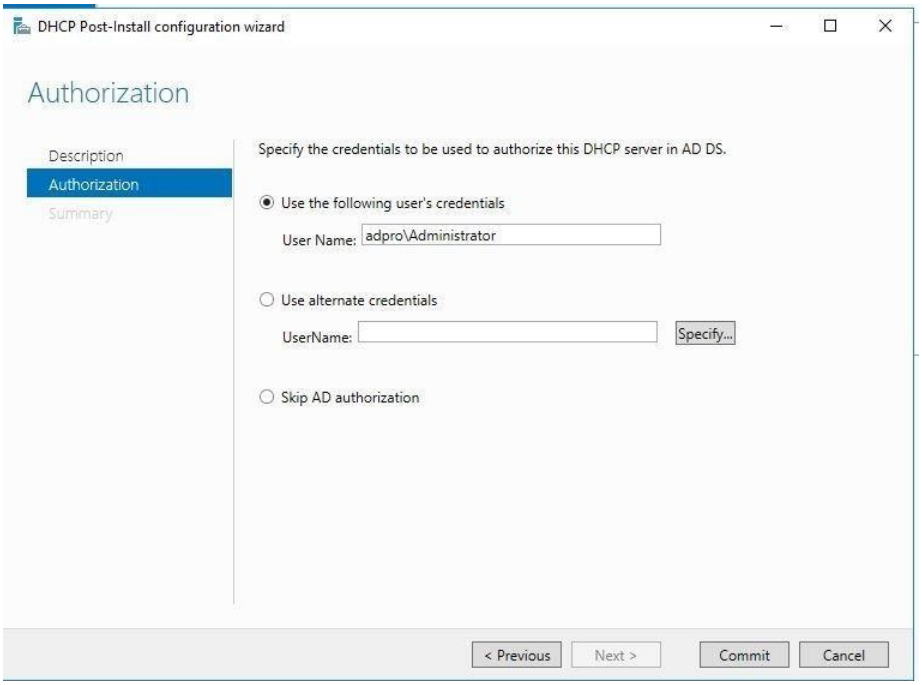
- In the server manager dashboard, you will see a yellow notification at the top left.



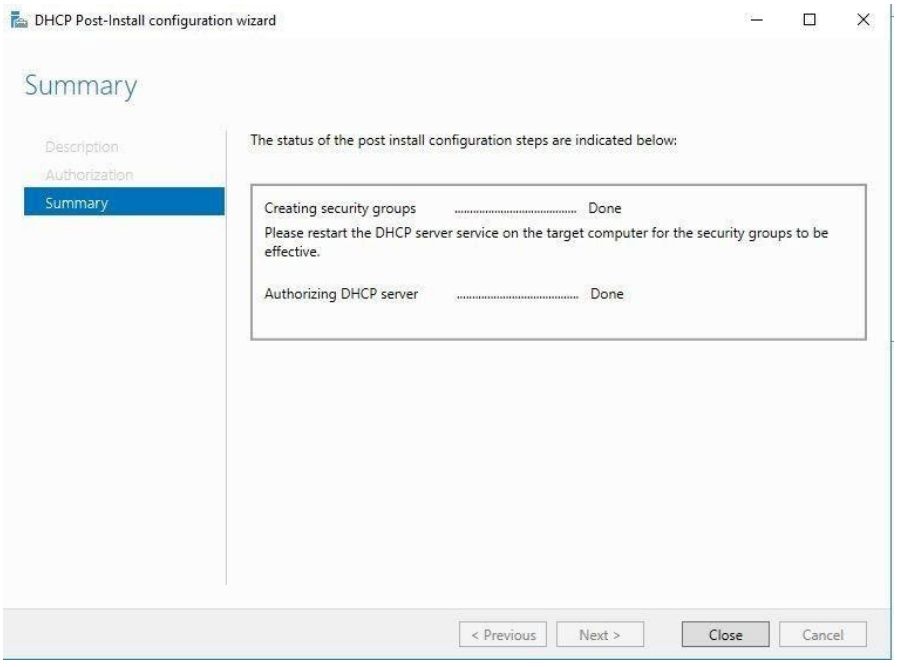
- Click on it
- Now click on “Complete DHCP configuration”

Step 2: Post-Install configuration wizard

- On the description screen click next
- On the authorization page use AD credentials if the server is joined to the domain.
- Choose “Skip AD authorization” if the DHCP server is standalone and not joined to the domain.
- Click commit



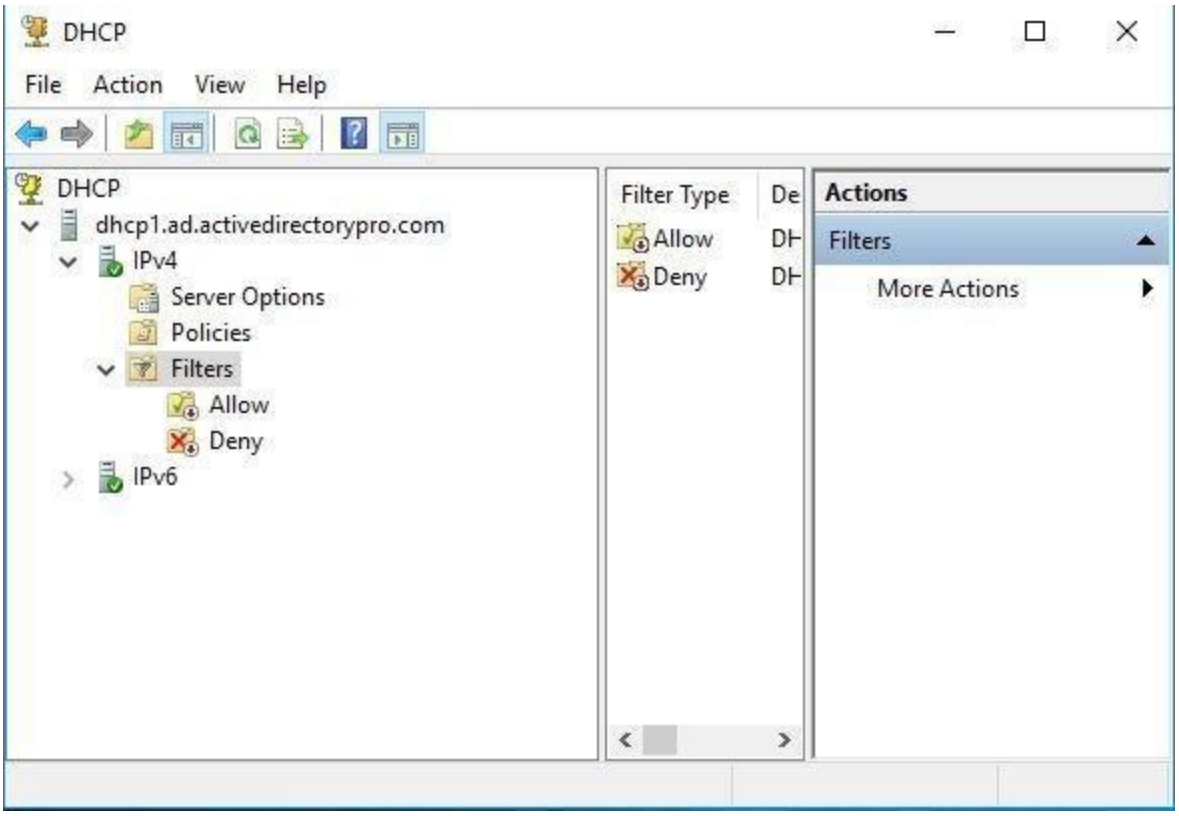
- You will see a summary page of the configuration steps
- Click close



Now you can open the DHCP management console to configure DHCP scopes and other options.

To access the DHCP management console **click start -> Windows Administrative Tool -> DHCP**

The DHCP management console

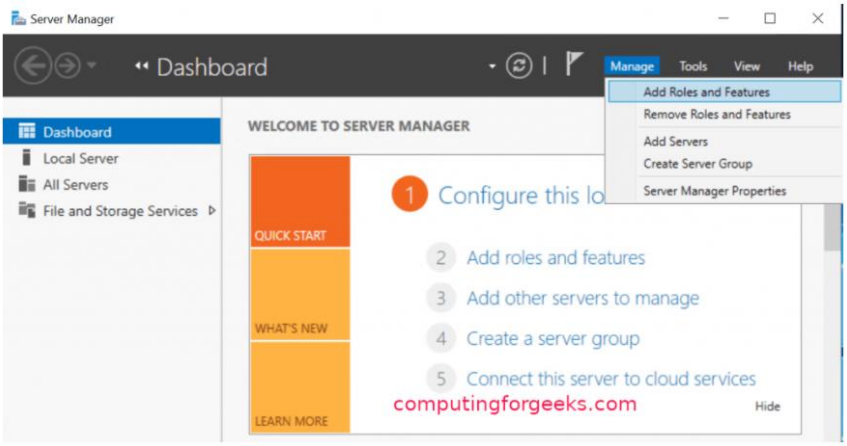


The next steps are to configure a new scope, configure scope options and ensure clients can access the DHCP server. I'll cover these steps in another post.

INSTALL AND CONFIGURE DNS SERVER ON WINDOWS SERVER

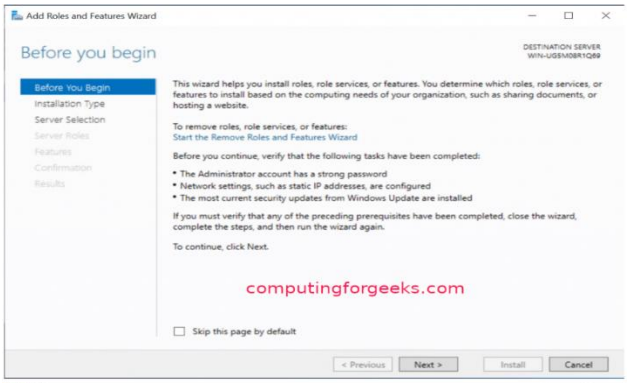
From Microsoft, Domain Name System (DNS) is one of the industry-standard suites of protocols that comprise TCP/IP, and together the DNS Client and DNS Server provide computer name-to-IP address mapping name resolution services to computers and users. DNS is part of the application layer of the TCP/IP reference model and is very important in day to day operation of computers all over the world. We are going to install DNS Server on windows server 2019 and later do configurations such as adding PTR, A/AAAA records among others. Before proceeding, make sure you have configured static IP Address on your server.

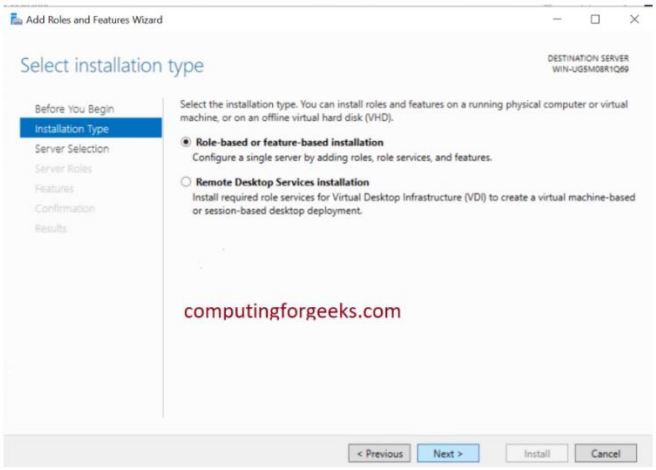
Step 1: Open Server Manager and Add Roles and Features



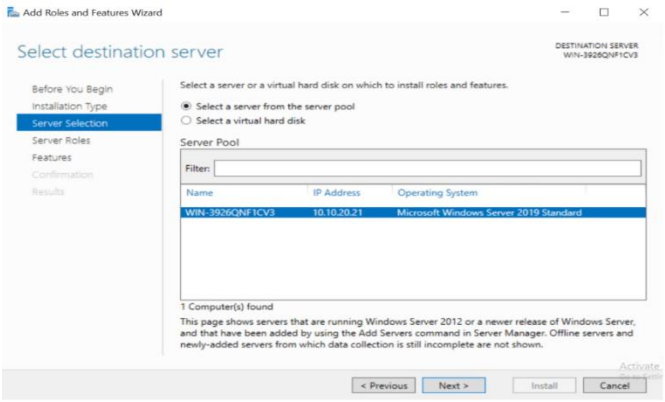
Click "**Next**" on the page that follows.

Select **“Role-based or feature-based installation“**

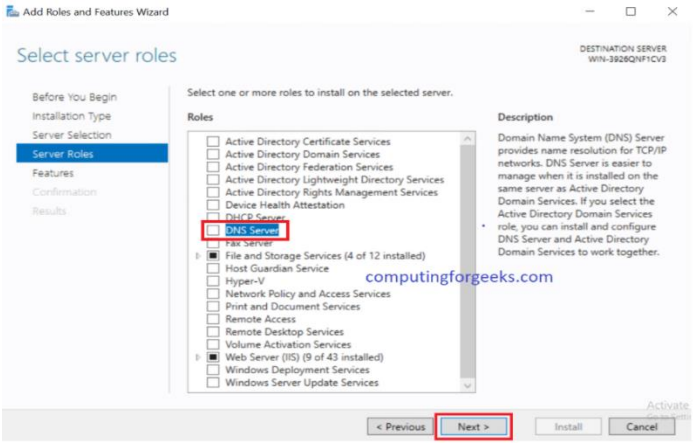




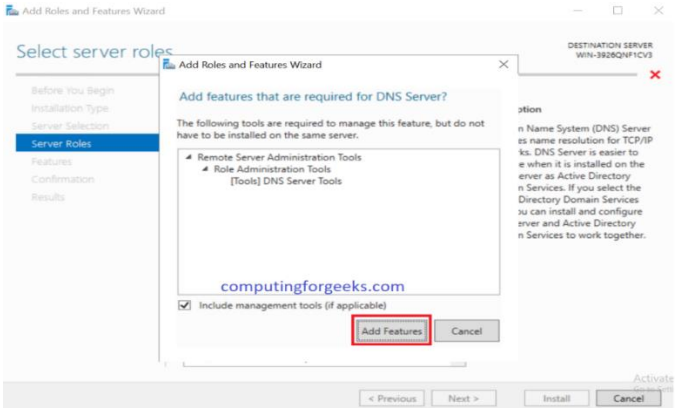
Select **Server** to install DNS into and hit **“Next “**



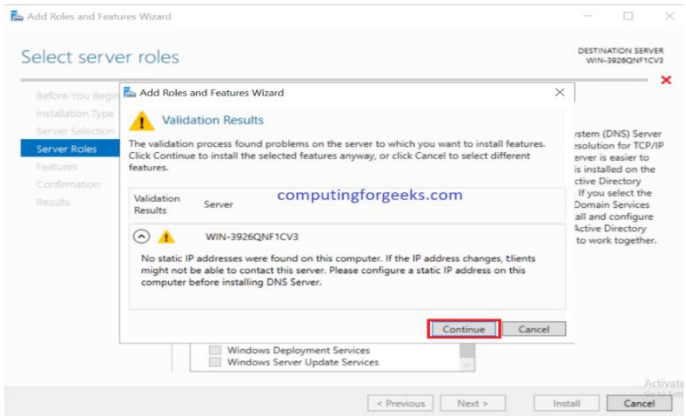
Step 2: Select DNS Server and Add Features

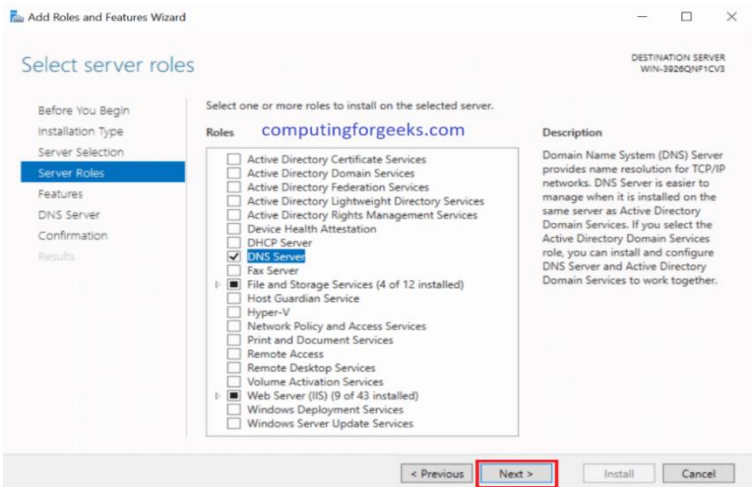


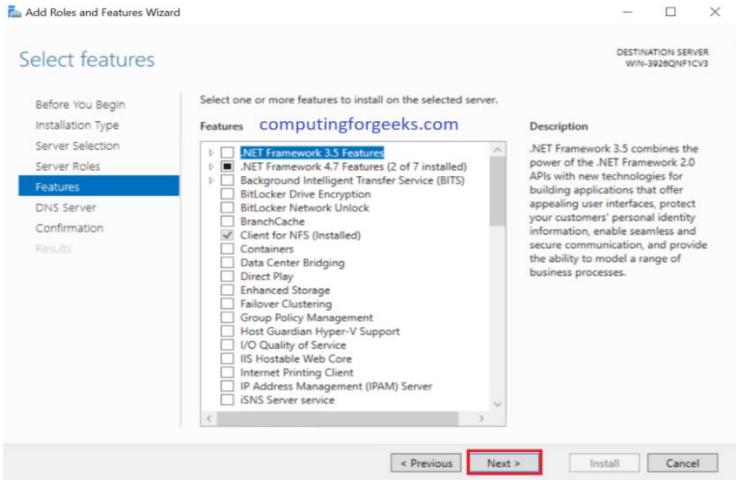
Click on **Add features**

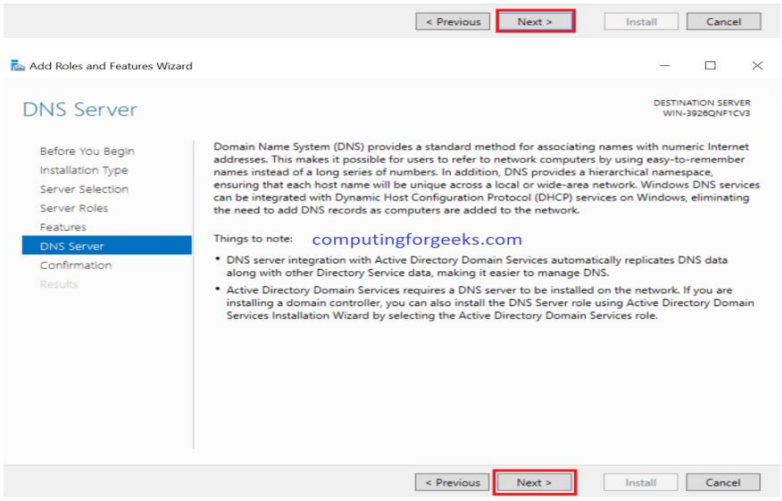


Click “**Next**” on the next three consecutive screens.



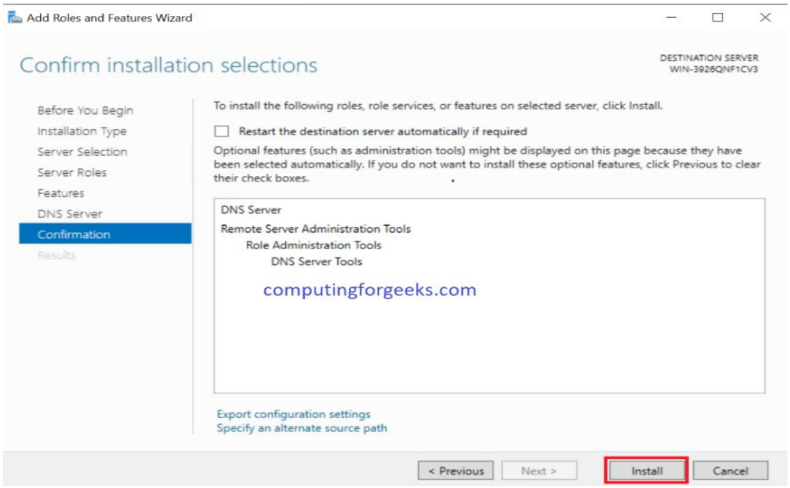




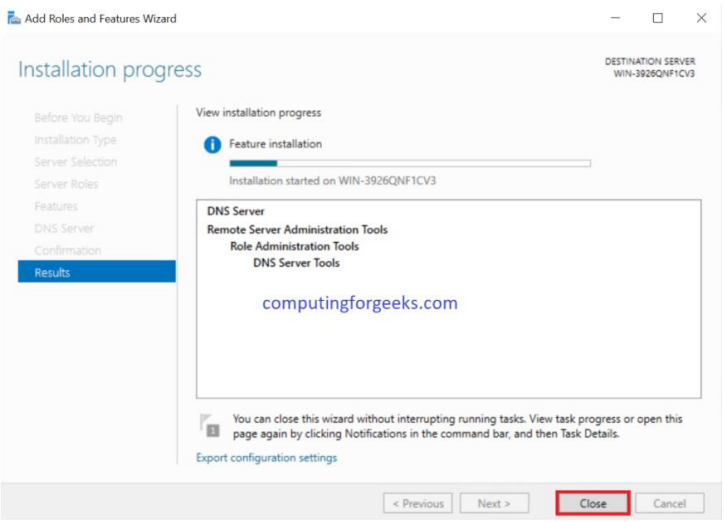


Step 3: Confirm and Install

Confirm your selections then hit “Install “



Step 4: Wait for the Installation then hit “Close”



Step 5: Configure Zones & Add records

Applications and Maintenance

Introduction

An application can be deployed in one of several ways. These deployment kinds include the installation files and information needed to install software on devices. A deployment type also has rules, such as detection techniques and requirements. For example, web database applications now supply the majority of the technologies and services we use on the Internet. This is the modern kind of application that can be delivered to any number of diverse, dispersed users who use any platform, operating system, or browser software.

Objectives

At the end of this chapter, the students must be able to:

a. Summarize several methods to push a custom configuration of applications to users.
b. Assess an application's ability to continue to meet a given organizational need.
c. Learn how to install database, web and client services, as well as how to configure and maintain them.

Database Installation, Configuration and Maintenance

What is MySQL (database)?

MySQL is an Oracle-backed open source relational database management system (RDBMS) based on Structured Query Language (SQL). MySQL runs on virtually all platforms, including Linux, UNIX and Windows. Although it can be used in a wide range of applications, MySQL is most often associated with web applications and online publishing.

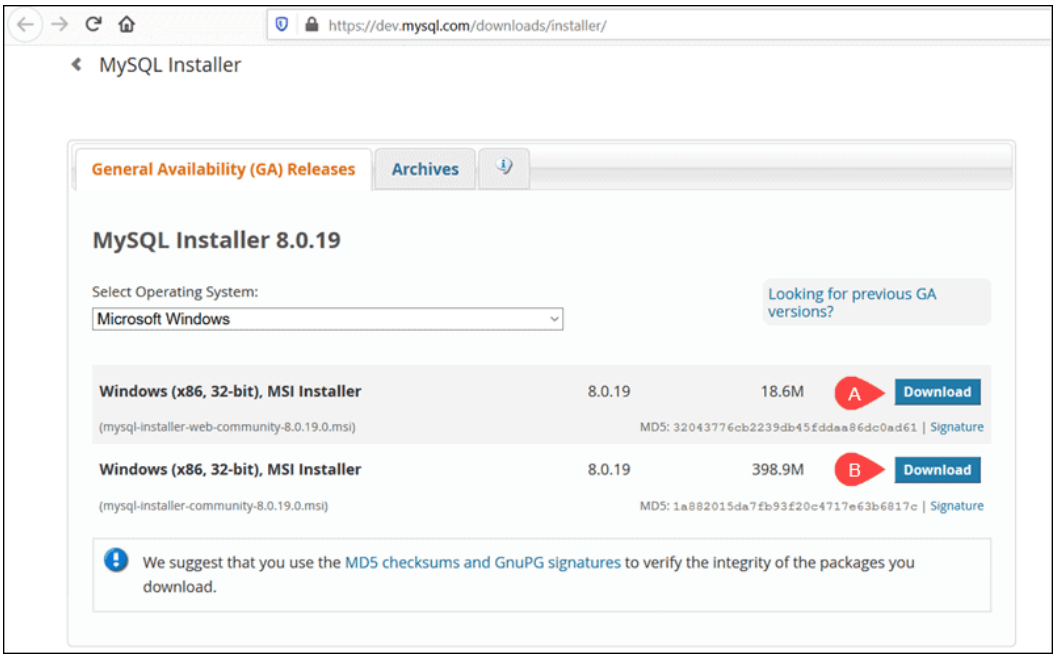
Today, MySQL is the RDBMS behind many of the top websites in the world and countless corporate and consumer-facing web-based applications, including Facebook, Twitter and YouTube.

MySQL Database Installation Guide

This topic will introduce to the student how to install and configure a database for Microsoft Windows.

*IMPORTANT - MySQL 8.0 Server requires the Microsoft Visual C++ 2019 Redistributable Package to run on Windows platforms. Users should make sure the package has been installed on the system before installing the server. The package is available here: http://www.microsoft.com/en-us/download/default.aspx

1. Download **MySQL Installer** from https://dev.mysql.com/downloads/installer/ and execute it.



You are given the option to download either the Web Community version or the Full MySQL package.

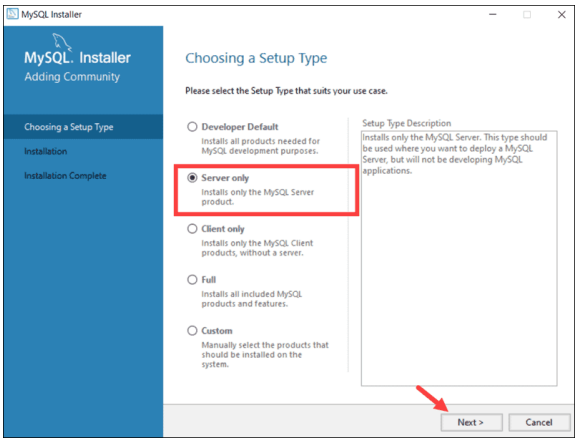
- The Web version (A) contains only the MySQL Installer and configuration files. You can customize and add additional MySQL products at a later point.
- The Full version (B) contains all MySQL Windows products, including the MySQL Server.

Select and download your preferred version. In this example, we selected the **Full MySQL Package** (B).

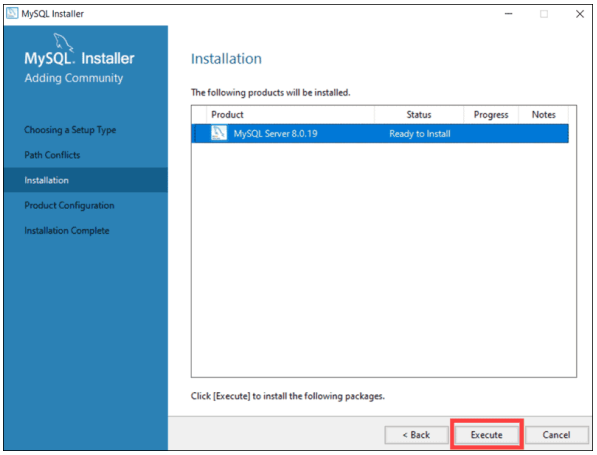
2. Determine the setup type to use for the initial installation of MySQL products. For example:

- **Developer Default**: Provides a setup type that includes the selected version of MySQL Server and other MySQL tools related to MySQL development, such as MySQL Workbench.
- **Server Only**: Provides a setup for the selected version of MySQL Server without other products.
- **Custom**: Enables you to select any version of MySQL Server and other MySQL products.
- **Full**: Installs all available MySQL products.

In the example below, we select the **Server Only** option and click **Next**.



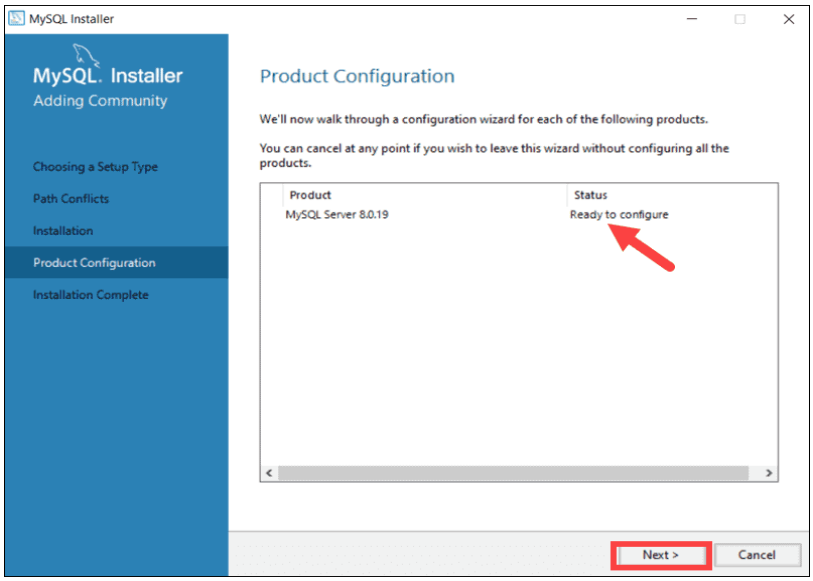
3. At this point, the system tries to resolve possible inconsistencies. It might inform you that additional packages need to be installed for the process to continue (e.g., Microsoft Visual C++ 2019 Redistributable Package). You can also run into Path installation inconsistencies if you have previous MySQL installations on your Windows Server.



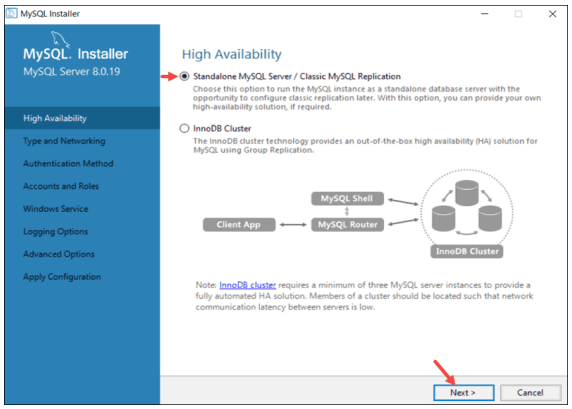
Luckily the **MySQL Installer** auto-resolves issues and installs the latest binary compatible version of missing software. You are now ready to start the installation process in earnest. Click **Execute** to begin the installation process.

MySQL Server Configuration guide with MySQL Installer

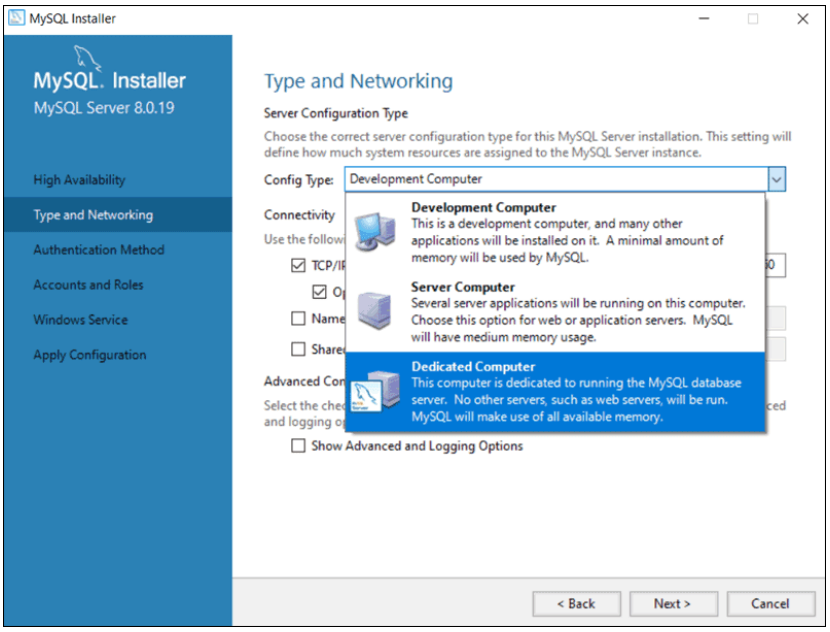
1. The MySQL Server 8.0.19 is now ready to be configured. Initiate the process by clicking **Next**.



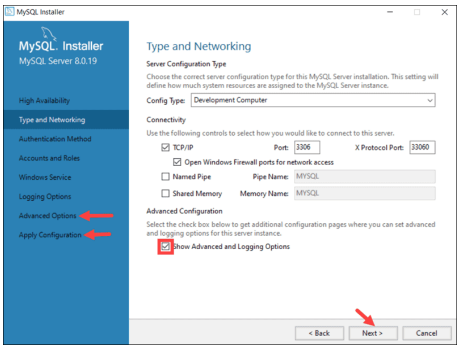
2. **High Availability**. The first configuration option affects database availability. It allows you to decide if you want to set up a Standalone MySQL Server or an InnoDB server cluster to improve availability. In this instance, we selected the classic, single server option.



3. **Type and Networking**. The **Type and Networking** section is used to define several essential features. The *Config Type* option lets you choose between three server configuration types. *Development Computer*, *Server Computer*, and *Dedicated Computer* define whether the server is dedicated solely to running your MySQL database or is going to share the underlying system with other applications. In this example, we decided to create a dedicated MySQL server.

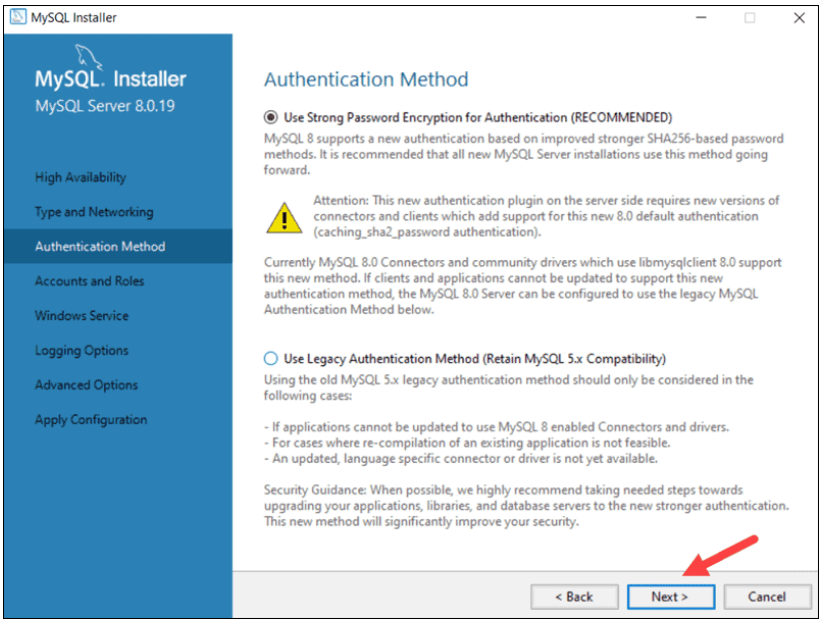


The **Type and Networking** tab can also define the port the MySQL server is listening on. The default setting is port number 3306 and can be changed to suit your needs. By checking the Show Advanced and Logging Option box, you can set additional logging options at a later stage.

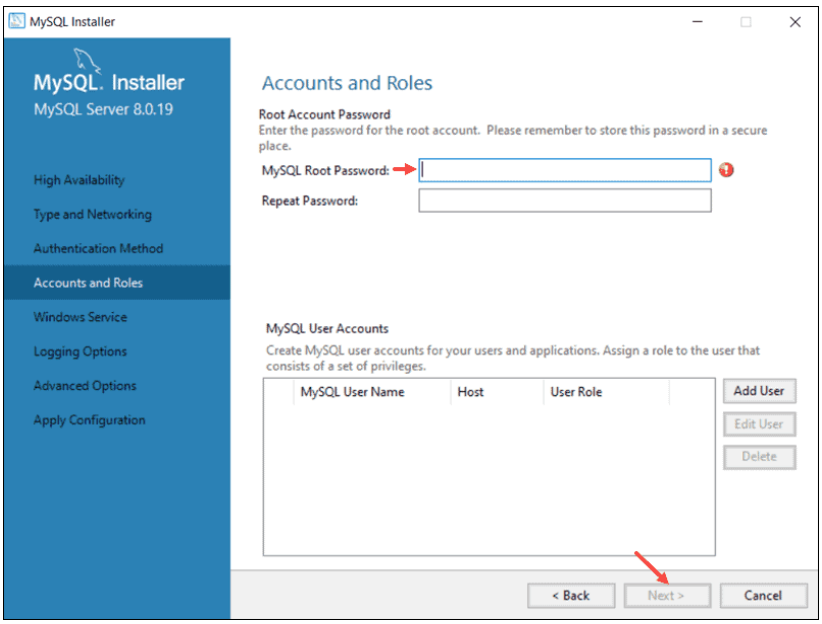


Click **Next** once you've selected the options you feel meet your requirements.

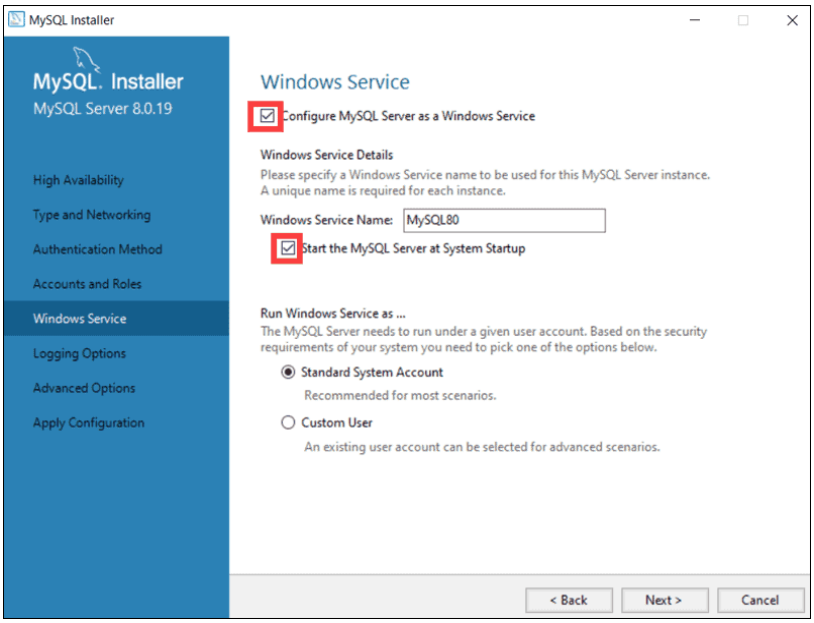
4. **Authentication Method**. It is possible to choose between two authentication methods, the recommended *Strong Password Encryption*, and the *Legacy Authentication Method*. Select the recommended **Use Strong Password Authentication** option.



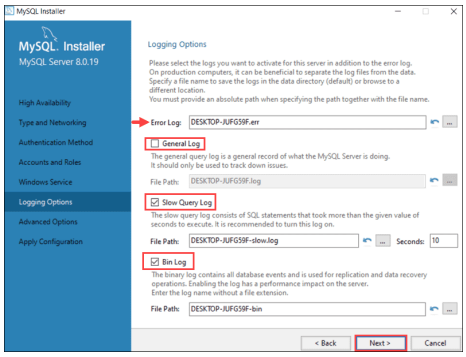
5. **Accounts and Roles**. You are now prompted to enter a password for your MySQL root user. You can also create additional roles for various users and purposes. This is only an initial setup, and credentials can be edited once the installation is complete.



6. **Windows Service**. By defining MySQL as a Windows Service, it can now start automatically whenever the Windows system boots. If you decide to start MySQL as an executable application, you would need to configure it manually.

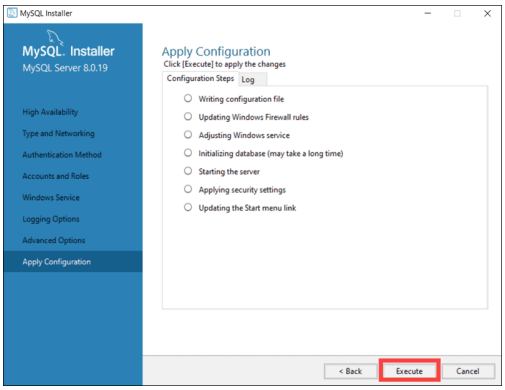


7. **Logging Options (Optional)**. If you have selected the Show Advanced Logging option in the **Type and Networking** tab, you are now able to set up MySQL log preferences. Logging options let you select the types of logs you want to activate and define the log directories. Click **Next** to reach the **Advanced Options** section.

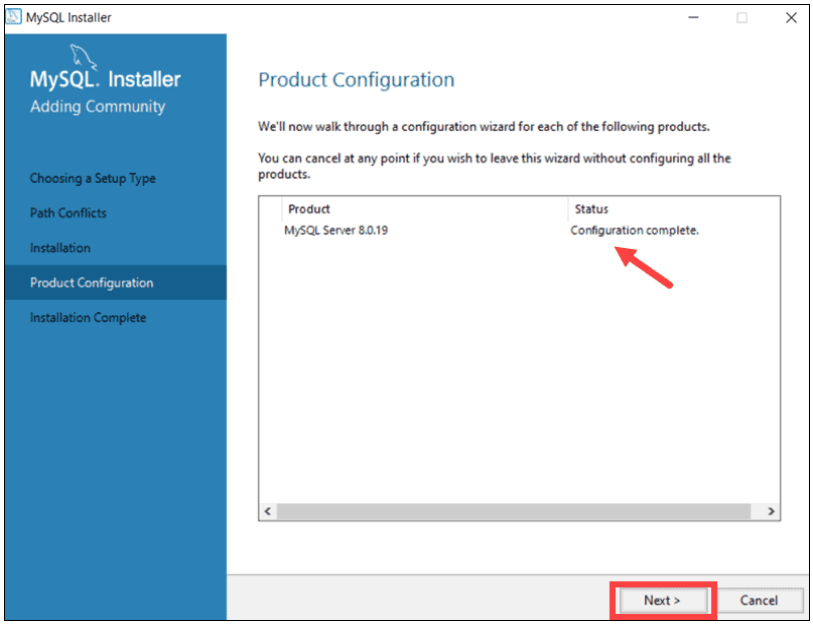


8. **Advanced Options (Optional)**. **Advanced Options** include setting a unique server identifier, and the type of case (Lower/Upper) to be used for *Table Names*. These settings are only available if you have checked the *Show Advanced Options* box in the **Type and Networking** tab.

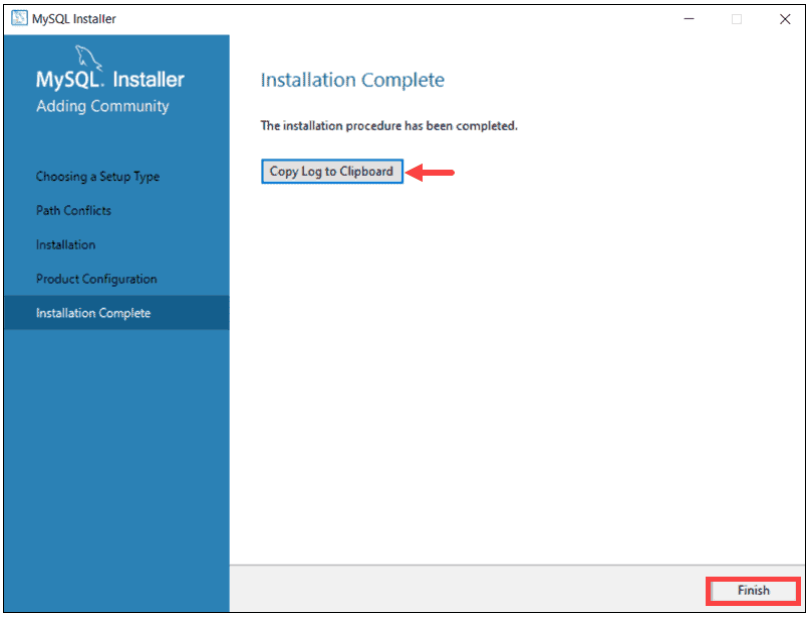
9. **Apply Configuration**. You have successfully configured the MySQL server and need to confirm for the MySQL Installer to apply the configuration. An overview of the configurations steps appears on the screen. Click **Execute** to apply the configuration.



The system informs once the configuration process is completed. Select **Next** to continue the installation process.



10. **Complete MySQL Installation on Windows Server**. After clicking **Next**, you are given the option to copy the installation process log to the Windows Clipboard. Click **Finish** to complete the MySQL server installation on Windows.



MySQL Database Maintenance

As a recommended best practice, customers should periodically optimize the Retain tables in order to achieve optimum query and update performance. This can have a big impact on the performance of archive jobs, deletion jobs, etc. It is also a good idea to optimize the memory settings for MySQL. The following maintenance tasks are frequently performed on a MySQL database:

- Backup. A backup is not a typical maintenance job. But it behaves more or less like one. The backup should be done regularly depending on the restore/PITR (Point in Time Recovery) requirements. Make sure, that in the backup all the necessary files (data files, transaction log files, configuration files and binary log files) are included. To prove that the backup process is working properly a regular restore should be performed. This can ideally be combined with the set-up of new database instances for developers or testing.
- Clean-up binary logs. The binary logs can be cleaned-up in two ways:

1. Passive by MySQL itself:

```
#    my.cnf

expire_logs_days    = 7
```

b. Active by the customers environment:

```
mysql> PURGE MASTER LOGS TO 'binarylog.000999';

mysql> PURGE MASTER LOGS BEFORE '2008-07-29 22:46:26';
```

Make sure NO binary logs are purged which are still needed by a slave. In this situation the slave is lost and has to be set-up from scratch. Make also sure binary logs are not removed by a file system operation (rm bin-log.*). Otherwise, the database gets confused.

- Optimize tables. After large UPDATE or INSERT/DELETE operations or long-time tables are blown up and contain a lot of unused space. This unused space can be partially reclaimed by optimizing the table again. This operation internally copies the whole table and therefore can take a long time!

```
mysql> OPTIMIZE TABLE <table_name>;
```

- Purge query cache. When there are SELECT queries with different sizes of result sets the query cache gets de-fragmented. This is shown by a lot of free space in the query cache but also a lot of not cached queries. Here it makes sense to purge the query cache from time to time.

```
mysql> FLUSH QUERY CACHE;
```

- Rotate binary logs. Binary logs can only be rotated by size. Sometimes you want to have them rotated by time. You can do this as follows (for example with a cron job):

```
mysql> FLUSH LOGS;
```

Web and Client Services Installation, Configuration and Maintenance

What is Internet Information Services (web server)?

Internet Information Services (IIS, formerly Internet Information Server) is an extensible web server software created by Microsoft for use with the Windows NT family. IIS supports HTTP, HTTP/2, HTTPS, FTP, FTPS, SMTP and NNTP. It has been an integral part of the Windows NT family since Windows NT 4.0, though it may be absent from some editions (e.g., Windows XP Home edition), and is not active by default.

An IIS web server accepts requests from remote client computers and returns the appropriate response. This basic functionality allows web servers to share and deliver information across local area networks (LAN), such as corporate intranets, and wide area networks (WAN), such as the Internet.

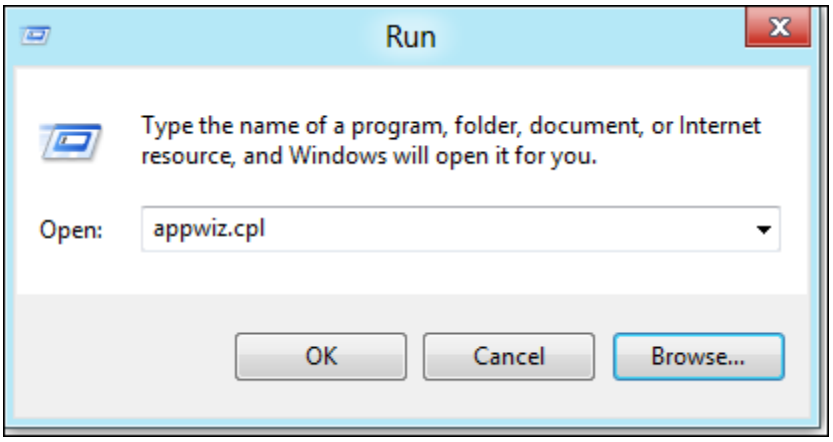
A web server can deliver information to users in several forms, such as static web pages coded in HTML; through file exchanges as downloads and uploads; and text documents, image files and more.

IIS Web Server Installation Guide

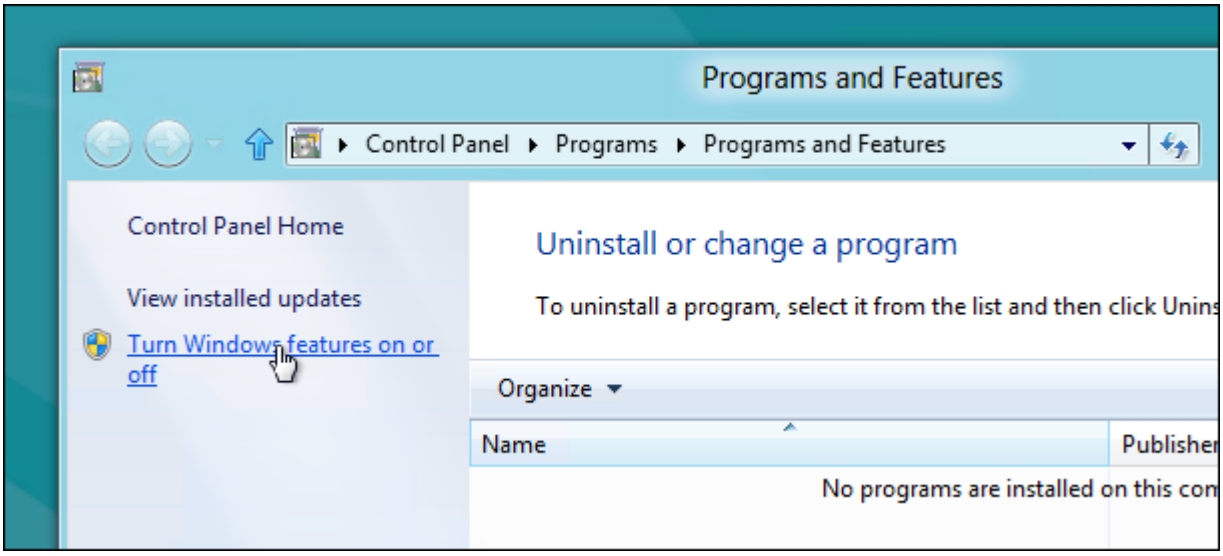
This topic will introduce to the student how to install and configure a web server for Microsoft Windows.

*NOTE - Windows 10 installs IIS version 10 instead of version 8. It's the same exact process either way.

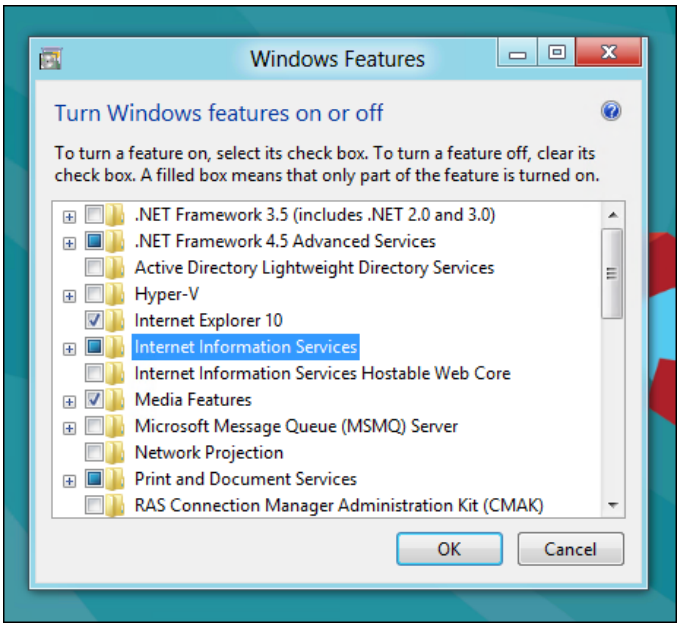
1. Keeping with Microsoft modular design of, uhm, everything these days, IIS in Windows is still an optional "Windows Feature". To install it, press the **Windows + R** key combination to bring up a run box, then type appwiz.cpl and press enter.



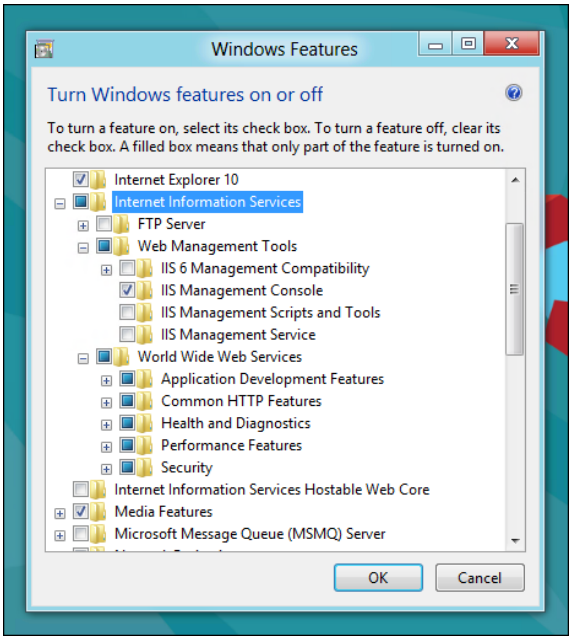
2. This will open the Program and Features part of Control Panel, on the left-hand side click on the “Turn Windows features on or off” link.



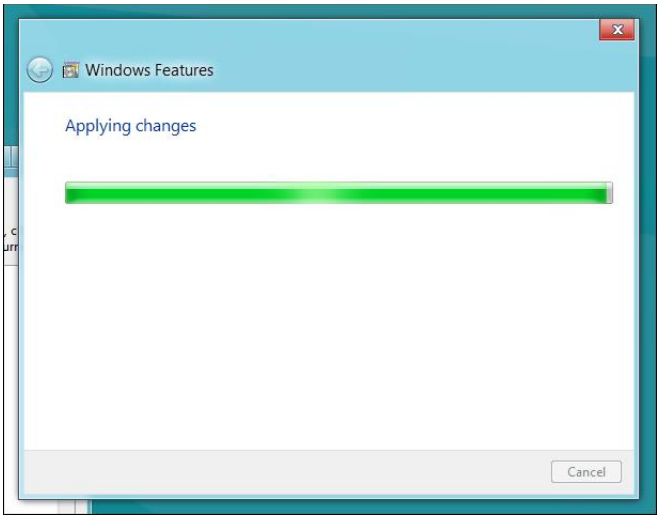
3. Now click on the Internet Information Services check box.



4. If you're a developer you are going to want to expand it and explore the sub-components as well. By default, it installs all the stuff needed to host a website, and you are probably going to need some of the more developer centric components as well. Click **OK**.

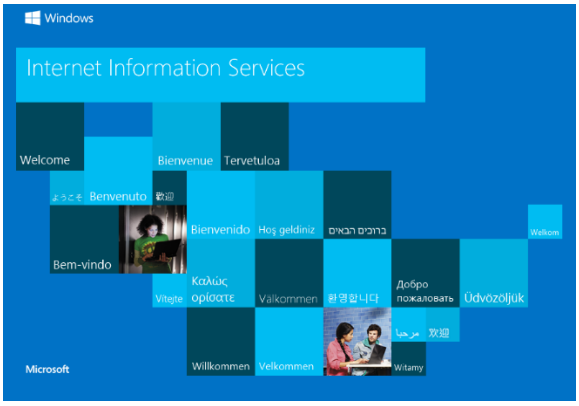


5. After clicking **OK**, this dialog will appear on your screen for a while.



6. Restart your computer.

7. After restarting your computer, open your browser and type “localhost” in the search bar and press **Enter**. If you can see the picture below, you successfully installed IIS.

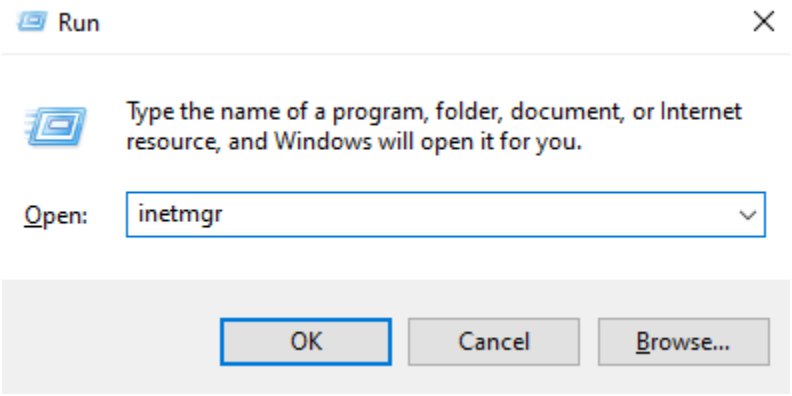


IIS Web Server Configuration

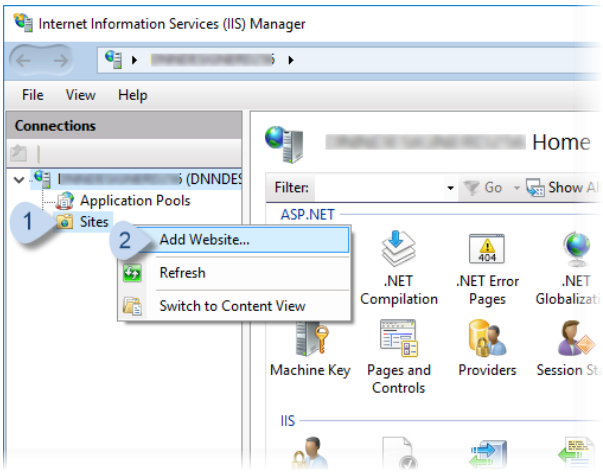
You can create a new website or set up an existing one for use with DNN. Choose one of the next two steps.

1. To **create a new website** and point it to the DNN installation folder:

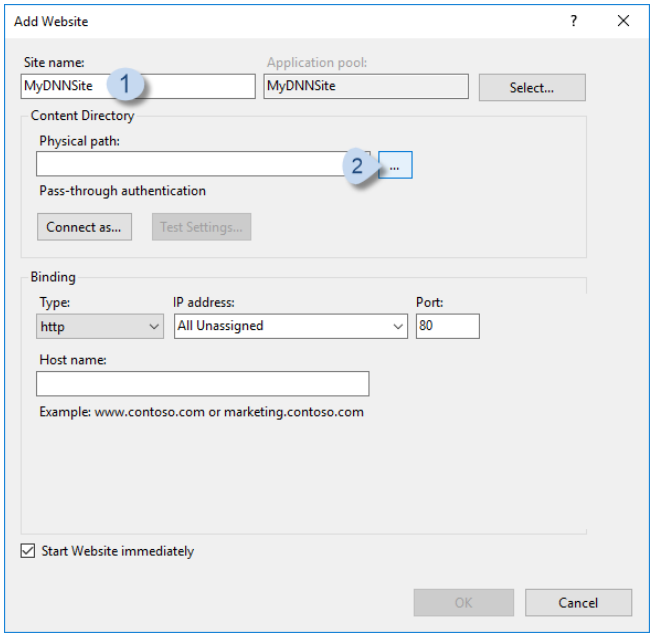
a. Go to Control Panel > Administrative Tools > Internet Information Services (IIS) Manager or press **Windows + R** and type inetmgr and hit **Enter**.



b. In the Connections panel, expand your host tree, right-click on Sites, and choose Add Website.

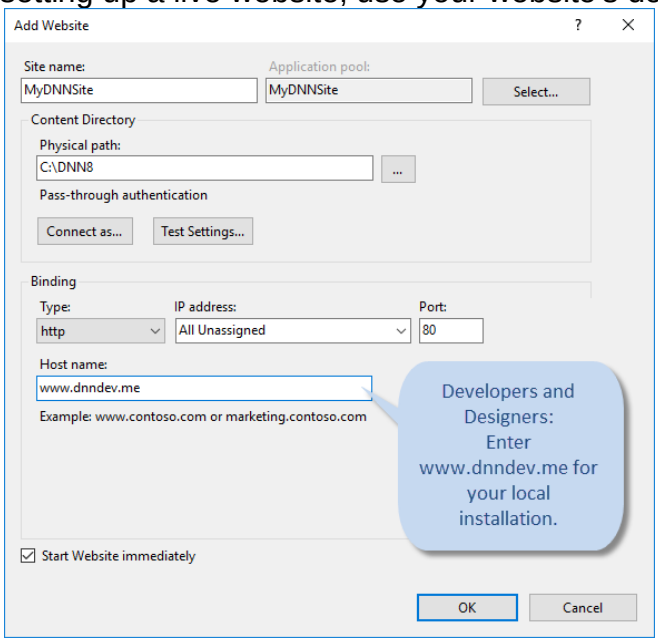


Enter the new website's name and choose the location.



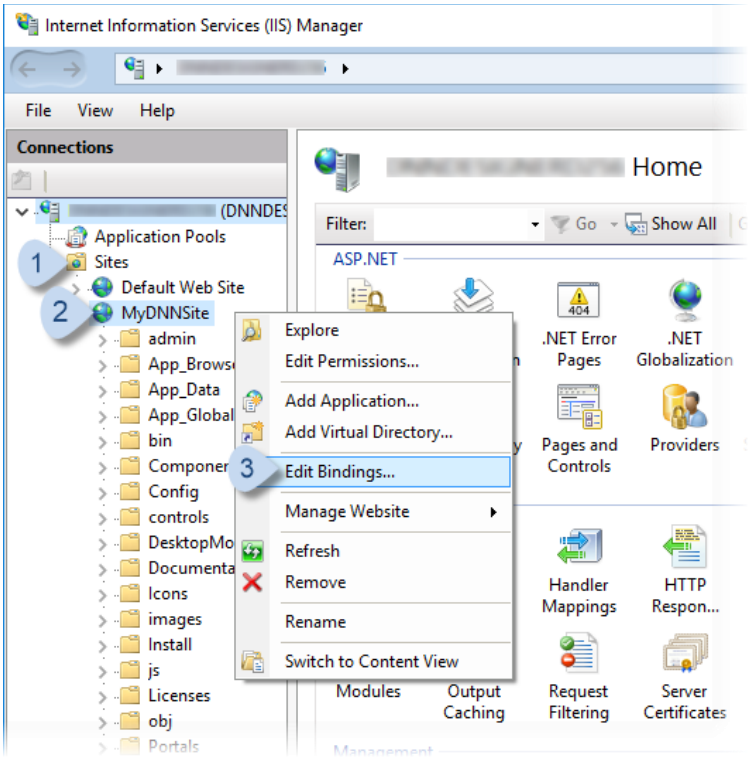
d. Enter the Host name.

Developers and Designers: If setting up a local development environment, you can use www.dnndev.me (or any subdomain). DNNDEV.ME is a registered domain which points to the loopback address of 127.0.0.1, so it will always resolve locally.
Administrators: If setting up a live website, use your website's domain.



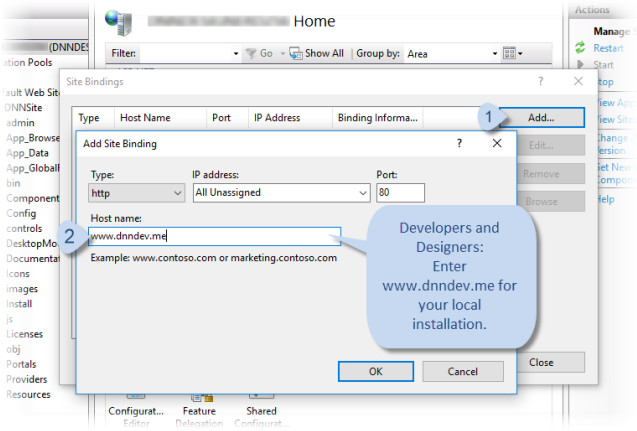
2. To use an **existing IIS website**:

a. In the **Connections** panel, right-click on the name of the existing website, and choose **Edit Bindings**....



b. In Site Bindings, click/tap Add.... In Add Site Binding, enter the Host name.

Developers and Designers: If setting up a local development environment, you can use www.dnndev.me (or any subdomain). DNNDEV.ME is a registered domain which points to the loopback address of 127.0.0.1, so it will always resolve locally.



Administrators: If setting up a live website, use your website's domain.

3. If you do not use **NETWORK SERVICE** as the user account to run your website, verify that **IIS AppPool\AppPoolName** has **Full** or **Modify** permissions for the DNN installation folder.

The account **IIS AppPool\AppPoolName** is automatically created by IIS.

IIS Web Server Maintenance

The log files that IIS generates can, over time, consume a large amount of disk space. Logs can potentially fill up an entire hard drive. To mitigate this problem, many users turn off logging completely. Fortunately, there are alternatives to doing so, such as the following:

- Enable folder compression
- Move the log folder to a remote system

1. Enable folder compression.

   IIS log files compress to about 2% of their original size. Enable compression of a log file as follows. You must be an administrator to perform this procedure.

   1. Click the File Manager icon in the icon bar.
   2. Move to the folder containing IIS log files (by default, %SystemDrive%\inetpub\logs\LogFiles).
   3. Right-click on the folder and click Properties.
   4. On the General tab of the Properties page, click Advanced.
   5. Click Compress contents to save disk space, and then

click OK.

6. Click Apply, and then select whether to compress the folder only, or the folder, its subfolders, and its files.
7. Click OK. Verify that the folder contents are compressed. The name of the folder and the name of each file should be colored blue, and the size of a compression file should be smaller.

This is a simple way to lower disk usage. It is not a final solution, however, because disk usage still grows over time, and could eventually fill up the hard drive.

If the folder already contains a significant amount of data, it could take the computer a while to compress its contents. Also note that this one-time process could slow down the computer during the initial compression, so if this is a production server, perform this operation during off-peak hours to prevent service degradation.

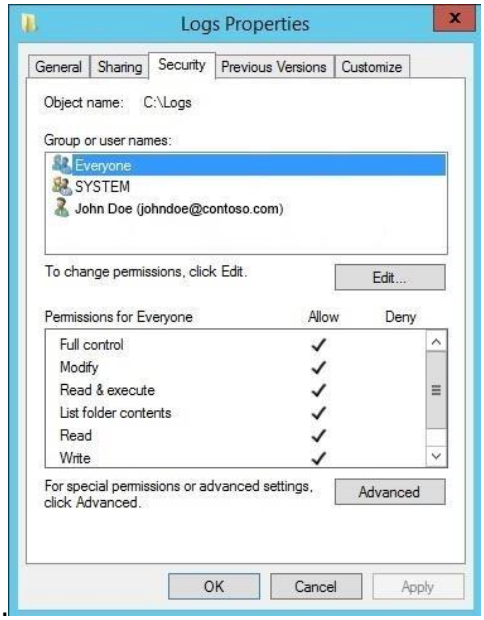
2. Move the log folder to a remote system.

IIS log files are stored by default in the %SystemDrive%\inetpub\logs\LogFiles folder of your IIS server. The folder is configured in the Directory property on the Logging page for either the server or an individual site. To lessen the problem of log disk usage, you can move your IIS log files to a folder on another server that has more space. This server can either be in the same domain as the local IIS server, or a different domain. You can save log files remotely either for the entire server or for individual Web sites.

This solution can help the security of the system, because if a local hard drive crashes, the log data is still available on remote storage. In addition, the log files can be consumed by analysis systems.

Change the location of an IIS log file to a remote share as follows:

1. Create a log-file directory on a remote server that is in the same domain as your local Web server running IIS.



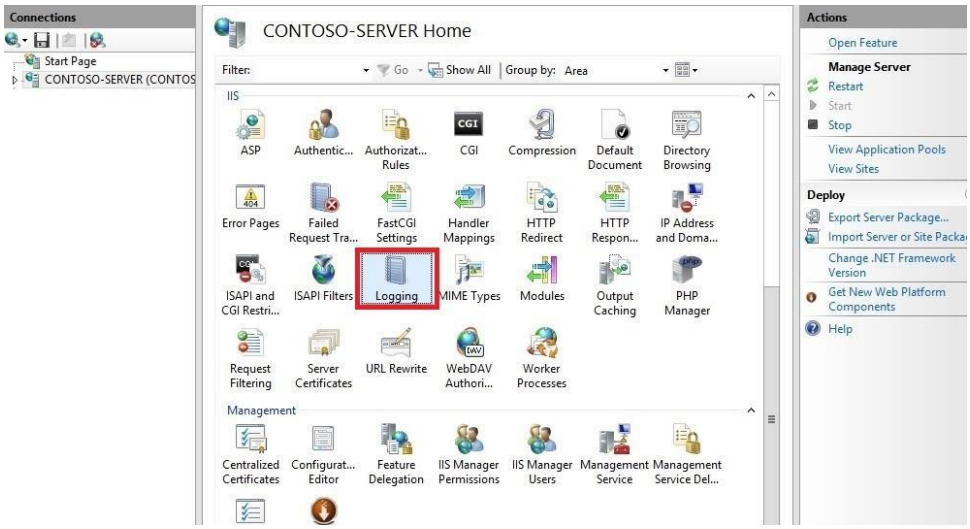
2. In the folder's **Properties** page, on the **Sharing** tab, click **Share** so that the directory is shared. On the **Security** tab, assign groups and users with the appropriate permissions. Ensure that the appropriate groups and users are able to read and write to the log files.

   Note: If you want to write log files to a remote server in a different domain, see Setting Up a Null Session for Cross-Domain Logging.

3. Open **IIS Manager** on your local Web server.

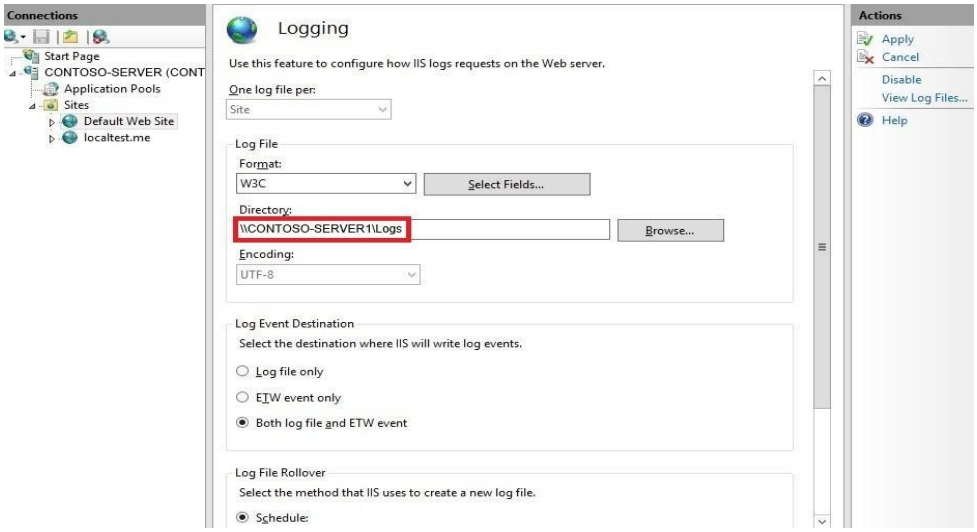
4. In **IIS Manager**, in the **Connections** pane, click the server or a Web site.

5. Double-



click **Logging**.

6. In the **Directory** text box, enter the full UNC path of the directory that you created on the remote server. For example, type \servername\Logs, where "servername" represents the name of the remote server, and "Logs" represents the name of the share where the log files are stored.



7. In the **Actions** pane, click **Apply**, and then click **OK**. All Web sites within the directory should begin logging data to the remote share.

Activities/Assessment:

1. What are maintenance steps and performance steps for MySQL server/database?
2. In your own words, why is SQL Server database maintenance required?
3. What is the objective of the web server in web programming?
4. What is the distinction between an application server and a web server?

Applications and Maintenance

Introduction

Client-server denotes a relationship between cooperating programs in an application, composed of clients initiating requests for services and servers providing that function or service. The application server is a framework, an environment where applications can run, no matter what they are or what functions they perform. An application server can develop and run web-based applications. There are many different types of application servers, including Java, PHP, and .NET Framework application servers. Application servers provide many advantages. They provide data and code integrity by allowing for a more centralized approach to updates and upgrades to applications. They provide security by centralizing the management of data access and the authentication process. Performance can be improved for heavy usage applications by limiting network traffic.

Objectives

- Summarize several methods to push a custom configuration of applications to users.
- Assess an application's ability to continue to meet a given organizational need.
- Discuss database, web and network server and client configurations.

What is Server Service?

Server Service, also known as LanmanServer, a component of the Microsoft Windows Server operating systems that allows a server to share file and print resources with clients over the network. When a redirector on a client requests a shared resource from a server, the Server service on the server responds and routes the resource to the client.

How Does It work?

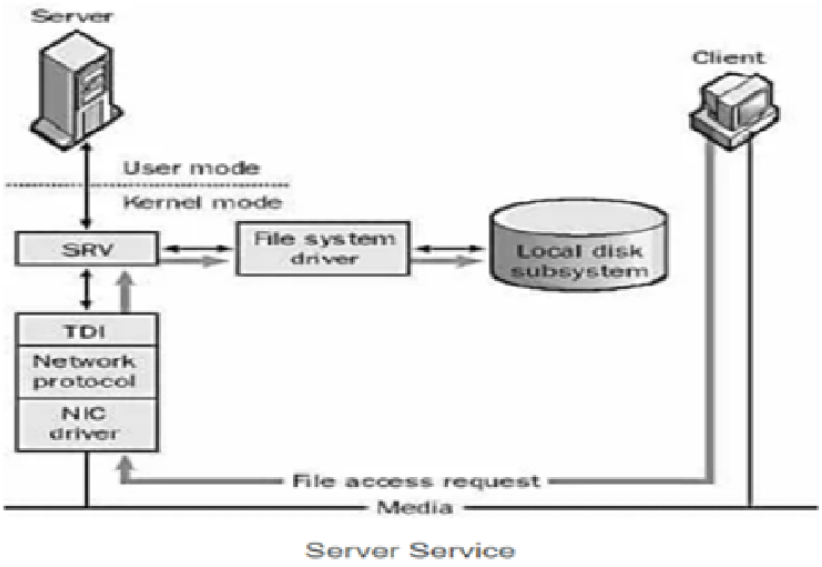
The Server service is implemented as a file system driver and resides above the transport driver interface (TDI) layer, which allows it to interact independently with any installed network transport protocols on the system. The Server service responds to requests just as any other file system driver does, allowing users to read and write data to and from remote network shares.

The Server service consists of two files:

Server (or SRV): A service that runs within the general Service Control Manager (services.exe) process

Srv.sys: A file system driver that operates in kernel mode and handles all low-level functions of the Server service, such as file reads and writes

If a remote network client makes a request to the Server service on the local computer, asking to read a file from the local file system, the request is received by the network interface card (NIC) driver and passed up the protocol stack to srv.sys, which forwards the read request to the appropriate local file system driver. The file system driver calls the disk subsystem driver to read the file, and the disk subsystem driver returns the file contents to the file system driver, which passes it back to srv.sys. Srv.sys passes the information back down the protocol stack to the NIC driver, which forwards it over the network to the requesting client.



Database Server Service/Database as a Service (DBaaS)

Database as a service (DBaaS) is a cloud computing managed service offering that provides access to a database without requiring the setup of physical hardware, the installation of software or the need to configure the database. Most maintenance and administrative tasks are handled by the service provider, freeing up users to quickly benefit from using the database.

DBaaS service variations

In a standard computing environment, the database server is part of the on-premises computing infrastructure and is installed, managed and run completely by an organization's IT staff.

In contrast, the DBaaS model is a fee-based subscription service in which the provider maintains the physical infrastructure and database and delivers it as a

private cloud service. The service typically covers high-level administrative burdens such as installation, initial configuration, maintenance and upgrades. Additional database administration (DBA) services, such as backup and performance management may also be provided. Control over the content and usage of the database is the responsibility of the customer.

DBaaS uses

The DBaaS model is ideal for small to medium-sized businesses that do not have well-staffed IT departments. Offloading the service and maintenance of the database to the DBaaS provider enables small to medium-sized businesses to implement applications and systems that they otherwise could not afford to build and support on-premises.

Database Server Configuration

You must customize the database server properties and features by setting configuration parameters, create storage spaces, and configure connectivity. You can automate startup. You customize the database server properties by setting or modifying configuration parameters in the onconfig file. You can use the IBM® OpenAdmin Tool (OAT) for Informix® to monitor and update your configuration. OAT provides suggestions for configuration parameter values to optimize your database server configuration. The current version of IBM Informix does not use some configuration parameters that are used in earlier versions of the server.

If you choose to configure a database server during installation, many configurations parameter and environment variables are set and a set of storage spaces are created automatically. Alternatively, you can manually configure the database server.

When you start the database server for the first time, disk space is initialized and the initial chunk of the root dbspace is created. Any existing data in that disk space is overwritten. Shared memory that the database server requires is also initialized. When you subsequently start the database server, only shared memory is initialized. Although the root dbspace is the default location of log files and databases, you can store log files and databases in other storage spaces to prevent the root dbspace from running out of space.

- **Storage space creation and management**
  You can create multiple storage spaces to store different types of objects, such as, data, indexes, logs, temporary objects, instead of storing everything in the root dbspace. The way that you distribute the data on disks affects the performance of the database server. You can configure the database server to both automatically minimize the storage space that data requires and automatically expand storage space as needed. You can segregate storage and processing resources among multiple client organization by configuring multitenancy.

- **Automatic performance tuning**
  You can set configuration parameters and Scheduler tasks to enable the database server to automatically adjust values that affect performance. By default, many automatic tuning configuration parameters and Scheduler tasks are set to solve common performance issues.
- **Feature configuration**
  You can configure the database server to support the types of optional functionality that you need.
- **Connectivity configuration**
  The connectivity information allows a client application to connect to the database server on the network. You must prepare the connectivity information even if the client application and the database server are on the same computer or node.
- **Limit session resources**
  You can limit the resources available to individual sessions to more evenly distribute system usage, and prevent resource monopolization.
- **Automate startup and shutdown on UNIX**
  You can modify startup and shutdown scripts on UNIX to automatically start and shut down the database server.
- **Automate startup on Windows**
  You can automate startup of the database server on Windows.

Regardless of the type of application, managing a client consists mainly of configuring its connection with the server components of SQL Server. Depending on the requirements of your site, client management can range from little more than entering the name of the server computer to building a library of custom configuration entries to accommodate a diverse multiserver environment.

The SQL Server Native Client DLL contains the network libraries and is installed by the setup program. The network protocols are not enabled during setup for new installations of SQL Server. Upgraded installations enable the previously enabled protocols. The underlying network protocols are installed as part of Windows Setup (or through Networks in Control Panel). The following tools are used to manage SQL Server clients:

- **SQL Server Configuration Manager**
  Both client and server network components are managed with SQL Server Configuration Manager, which combines the SQL Server Network Utility, SQL Server Client Network Utility, and Service Manager of previous versions. SQL Server Configuration Manager is a Microsoft Management Console (MMC) snap-in. It also appears as a node in the Windows Computer Manager snap-in. Individual network libraries can be enabled, disabled, configured, and prioritized using SQL Server Configuration Manager.

Setup

Run SQL Server setup to install the network components on a client computer. Individual network libraries can be enabled or disabled during setup when Setup is started from the command prompt.

- **ODBC Data Source Administrator**

  The ODBC Data Source Administrator lets you create and modify ODBC data sources on computers running the Microsoft Windows operating system.

Connecting from Another Computer

To enhance security, the Database Engine of SQL Server Developer, Express, and Evaluation editions cannot be accessed from another computer when initially installed. This lesson shows you how to enable the protocols, configure the ports, and configure the Windows Firewall for connecting from other computers.

- **Enabling Protocols**

To enhance security, SQL Server Express, Developer, and Evaluation install with only limited network connectivity. Connections to the Database Engine can be made from tools that are running on the same computer, but not from other computers. If you are planning to do your development work on the same computer as the Database Engine, you do not have to enable additional protocols. Management Studio will connect to the Database Engine by using the shared memory protocol. This protocol is already enabled.

If you plan to connect to the Database Engine from another computer, you must enable a protocol, such as TCP/IP.

How to enable TCP/IP connections from another computer

a. On the Start menu, point to All Programs, point to Microsoft SQL Server, point to Configuration Tools, and then click SQL Server Configuration Manager.

Note

- You might have both 32 bit and 64 bit options available.
- Because SQL Server Configuration Manager is a snap-in for the Microsoft Management Console program and not a stand-alone program, SQL Server Configuration Manager does not appear as an application in newer versions of Windows. The file name contains a number representing the version number of the SQL Server. To open Configuration Manager from the Run command, here are the paths to the last four versions when Windows is installed on the C drive.

Version	Path
SQL Server 2017 (14.x)	C:\Windows\SysWOW64\SQLServerManager14.msc
SQL Server 2016 (13.x)	C:\Windows\SysWOW64\SQLServerManager13.msc
SQL Server 2014 (12.x)	C:\Windows\SysWOW64\SQLServerManager12.msc
SQL Server 2012 (11.x)	C:\Windows\SysWOW64\SQLServerManager11.msc

b. In SQL Server Configuration Manager, expand SQL Server Network Configuration, and then click Protocols for <InstanceName>.
The default instance (an unnamed instance) is listed as MSSQLSERVER. If you installed a named instance, the name you provided is listed. SQL Server 2012 Express installs as SQLEXPRESS, unless you changed the name during setup.
c. In the list of protocols, right-click the protocol you want to enable (TCP/IP), and then click Enable.

- **Configuring a Fixed Port**

To enhance security, Windows Server 2008, Windows Vista, and Windows 7 all turn on the Windows Firewall. When you want to connect to this instance from another computer, you must open a communication port in the firewall. The default instance of the Database Engine listens on port 1433; therefore, you do not have to configure a fixed port. However, named instances including SQL Server Express listen on dynamic ports. Before you can open a port in the firewall, you must first configure the Database Engine to listen on a specific port known as a fixed port or a static port; otherwise, the Database Engine might listen on a different port each time it is started. For more information about firewalls, the default Windows firewall settings, and a description of the TCP ports that affect the Database Engine, Analysis Services, Reporting Services, and Integration Services.

Configure SQL Server to listen on a specific port

a. In SQL Server Configuration Manager, expand SQL Server Network Configuration, and then click on the server instance you want to configure.
b. In the right pane, double-click TCP/IP.
c. In the TCP/IP Properties dialog box, click the IP Addresses tab.
d. In the TCP Port box of the IPAll section, type an available port number. For this tutorial, we will use 49172.

e. Click OK to close the dialog box, and click OK to the warning that the service must be restarted.
f. In the left pane, click SQL Server Services.
g. In the right pane, right-click the instance of SQL Server, and then click Restart. When the Database Engine restarts, it will listen on port 49172.

- **Opening Ports in the Firewall**

Firewall systems help prevent unauthorized access to computer resources. To connect to SQL Server from another computer when a firewall is on, you must open a port in the firewall.

After you configure the Database Engine to use a fixed port, follow the following instructions to open that port in your Windows Firewall. (You do not have to configure a fixed port for the default instance, because it is already fixed on TCP port 1433.)

Web Services

There are many different services that fit within the category of Web services. The first one is a Web server. The Web server is software that runs on our hardware server and serves web pages using the HTTP protocol. When we type in a URL in our browser, we access the Web server that holds files in HTML format, along with images and other types of files.

Web Server

A Web Server mainly refers to server hardware or a software device that stores the web content and is used to host the web sites and produce the same as results when requested by the clients on the World Wide Web. To store, process and deliver the web pages when requested by the clients is the most prominent and technically the key feature and purpose of a Web Server.

These web servers generally tend to carry one or more websites. The requests sent by the clients over the World Wide Web are generally processed by the Web Server over Hypertext Transfer Protocol (HTTP) and the Web Pages are mostly delivered as HTML documents. Web servers are at the very core of the concept of web hosting. A web server is always connected to the internet and each of these connected servers has a certain unique address. The hosting providers are able to manage multiple domains on a single server because of the web servers.

Different types of web servers are available in the market for the developers to choose from, depending upon their preferences. The most prominent types of Web Servers available in the market are:

- Apache HTTP Server Web Server
- Internet Information Services (IIS) Web Server

- Lighttpd Web Server
- Sun Java System Web Server
- Jigsaw Server Web Server
- LiteSpeed server Web Server
- Node.js Web Server

Web server configuration

Plug-in configuration involves configuring the web server to use the binary plug-in module that WebSphere® Application Server provides. Plug-in configuration also includes updating the plug-in XML configuration file to reflect the current application server configuration. The binary module uses the XML file to help route web client requests.

After installing a supported web server, you must install a binary plug-in module for the web server by installing the Web Server Plug-ins. The plug-in module lets the web server communicate with the application server. The Web Server Plug-ins Configuration Tool allows you to configure the web server and create a web server definition in the configuration of the application server. The Web Server Plug-ins Configuration Tool uses the following files to configure a plug-in for the web server that you select:

- The web server configuration file on the web server machine, such as the httpd.conf file for IBM® HTTP Server.
- The binary web server plug-in file on the web server machine.
- The plug-in configuration file, plugin-cfg.xml, on the application server machine that you propagate (copy) to a Web server machine.
- The default (temporary) plug-in configuration file, plugin-cfg.xml, on the web server machine.
- The configureweb_server_name script that you copy from the web server machine to the application server machine.

See the following descriptions of each file.

Web server configuration file

The web server configuration file is installed as part of the web server. The Web Server Plug-ins Configuration Tool must re-configure the configuration file for a supported web server. Configuration consists of adding directives that identify file locations of two files:

- Binary web server plug-in file
- Plug-in configuration file, plugin-cfg.xml

Binary web server plug-in file

replace the default file.

Configureweb_server_name script for the web server definition

The Web Server Plug-ins Configuration Tool creates the configureweb_server_name script on the web server machine in the plugins_root/bin directory. If one machine in a remote scenario is running under an operating system like AIX® or Linux® and the other machine is running under Windows, use the script created in the plugins_root/bin/crossPlatformScripts directory. The script is created for remote installation scenarios only.

Copy the script from the web server machine to the app_server_root/bin directory on a remote application server machine. You do not have to copy the script on a local installation. Run the script to create a web server definition in the configuration of the application server.

When using the IBM HTTP Server, configure the IBM HTTP Administration Server also. The IBM HTTP Administration Server works with the administrative console to manage web server definitions. Also, use the administrative console to update your web server definition with remote web server management options. Click **Servers > Server Types > Web servers > web_server_name** to see configuration options. For example, click **Remote Web server management** to change such properties as:

- Host name
- Administrative port
- User ID
- Password

Important: Always open a new command window before running this script. You can avoid a potential problem by doing so.
The problem is a potential conflict between a shell environment variable, the WAS_USER_SCRIPT environment variable, and the actual default profile. The script always works against the default profile. If the WAS_USER_SCRIPT environment variable is set, however, a conflict arises as the script attempts to work on the profile identified by the variable.
The variable is easy to set accidentally. Issue any command from the profile_root/bin directory of any profile and the variable is set to that profile.
If you have more than one profile on your system, the potential exists that the default profile and the profile identified by the variable are different profiles. If so, a conflict occurs and the script might not create the web server definition in the correct profile, or might not create the web server definition at all.

Reset the variable in either of two ways:

- Close the command window where the variable is set and open a new one.
- Change directories to the profile_root/bin directory of the default profile and source the setupCmdLine.sh script:
  - **Windows:**
    1. Open a command prompt window.
    2. Change directories to the app_server_root\bin directory.
    3. Issue the setupCmdLine.bat command.
  - **Linux/Solaris/AIX/HP-UX**
    1. Open a command shell window.
    2. Change directories to the app_server_root/bin directory.
    3. Issue the ./setupCmdLine.sh command. Notice the space between the periods. The special format for this command sources the command to make the setting active for all processes started from the command shell.

If a web server definition already exists for a standalone application server, running the script does not add a new web server definition. Each standalone application server can have only one web server definition.

You cannot use the administrative console of a standalone application server to add or delete a Web server definition. However, you can do both tasks using the administrative scripting interface:

- Add a web server definition through the wsadmin facility using the configureweb_server_name script. The script uses a Java™ Command Language (Jacl) script named configureWebserverDefintion.jacl to create and configure the web server definition.
- Delete a web server definition using wsadmin commands.

Replacing the default plug-in configuration file with the file from the web server definition (propagation)

The default file uses fixed parameter values that might not match the parameter values in the actual file on the application server. The default file is a placeholder only. The file cannot reflect changes that occur in the application server configuration. The file also cannot reflect nondefault values that might be in effect on the application server. The application server must have the following values in the actual plugin-cfg.xml file. If so, the default file can successfully configure the binary plug-in module. Then, the plug-in module can successfully communicate with the web server and the application server. Suppose that the application server does not have the following values in the actual plugin-cfg.xml file. In that case, the default file configures the binary plug-in module incorrectly. The plug-in module can always communicate with the web server. But with an improper configuration file, the plug-in module cannot communicate successfully with the application server.

The following are fixed parameter values in the temporary plug-in configuration file.

- **Virtual host name**
  Default value: default_host
  This virtual host is configured to serve the DefaultApplication. This value is probably the same as the value in the real plugin-cfg.xml file. However, suppose that you create another virtual host for serving applications and install the DefaultApplication on it. If so, the actual plugin-cfg.xml file is regenerated. The web server cannot access the DefaultApplication. (The application includes the snoop servlet and the hitcount servlet.)
  To access applications on the new virtual host, propagate the real plugin-cfg.xml file. Propagation is copying the updated file from the application server machine to the web server machine.
- **HTTP transport port**
  Default value: 9080
  The 9080 value is the default value for the HTTP transport port for the default_host virtual host. This value is probably the same as the value in the updated file. However, this value changes for every profile on the application server machine. The HTTP transport port value must be unique for every application server.
  To communicate over a different port, propagate the real plugin-cfg.xml file.
- **Web server listening port**
  Default value: 80
  The 80 value is the default value for the port that controls communication with the web server. However, each application server profile must have a unique port value to communicate to a web server. The actual port value might be 81 or another number.
  To communicate over a different port, propagate the real plugin-cfg.xml file.

- **HTTPS transport port**
  Default value: 9443
  The 9443 value is the default value for the HTTPS (secure) transport port for the default_host virtual host. This value is probably the same as the value in the updated file. However, this value changes for every profile on the application server machine. The HTTPS transport port value must be unique for every application server.
  To communicate over a different secure port, propagate the real plugin-cfg.xml file.
- **Applications installed on the server1 application server**
  All of the default servlets and applications are included in the default file.
  To serve an application that you developed with the web server, propagate the real plugin-cfg.xml file.

Network Service

Network Services/Managed Network Services are the services of management of networks by IT service providers for their clients. The scope of network services extends from LAN/WLAN management, unified communications to Network Consulting Services and Network implementation services. Network Services include IP addressing, Domain Name System (DNS), primary domain email service, Internet access, web content filtering, security products such as firewalls, VPN termination and intrusion prevention systems (IPS), and the necessary tools and staff to support these services. Network Services will provide limited wireless connectivity for agencies (see the Wireless Services description in the following sections).

The advantages of network services/managed network services to client companies are as follows:

- Client companies can focus on their core competencies and save substantial sums of money in building and maintaining network capabilities
- Client companies can minimize their risks of network failure or data loss due to the same by offloading the risk to network service providers
- Ease in meeting compliance requirements of regulatory authorities owing to expertise of service providers in the same

Support

Application support is the daily process of running an application, including ensuring the app achieves service-level objectives and supporting users when issues arise. Application support services need to be well-equipped to keep the app running smoothly. There are several different levels of application support that should be provided:

First Level Application Support

This level includes basic troubleshooting to establish the cause of a problem. For example, if the network is down, the app cannot run. L1 support is often known as the first-line support, because these individuals are on the front lines gathering customer data and understanding the issue based on the problems reported to identify the root cause. This can also include general application monitoring.

Second Level Application Support

Second Level Support includes the actual resolution of incidents, generally by a professional who is either an expert in the application or the infrastructure supporting it. L2 support is often more expensive because of the technical expertise required to support L1 team members, raise issues, and identify potential solutions.

Third Level Application Development Support

Finally, at the third level, incidents are resolved by those who have a deep knowledge of the application, typically the developers of the application. For organizations outsourcing their application development, this layer of support may not be possible, and it's important for business leaders to take that into consideration when selecting a partner.

This may be known in some models as high-end or back-end support, and require highly skilled specialists who can address escalates from L1 and L2 employees and study and develop unknown issues to create methods to resolve them. Sometimes, this may mean a code or database change to resolve the issue.

Assessment/Activities

1. Discuss what is Server Service and how it works.
2. Discuss what is Database Server Configuration.
3. Discuss what is Web Server Configuration.
4. Explain how to connect client to database and web server.

Administrative Activities

Introduction:

In the most general sense, administrative duties are the tasks and activities that are part of the daily operations of a business. They include answering calls, taking messages, managing correspondence, ordering supplies, and keeping the shared office areas organized and functional. Duties also may include creating reports, inputting and managing data, managing files, basic bookkeeping and other financial tasks. Many of these duties are managed by administrative assistants, whose job it is to help an individual or team by taking on some or all of their clerical tasks, but many entry and midlevel positions also include a fair amount of administrative work.

Objectives:

a. Explain the benefits of content management within an organization.
b. Explain the need for content deployment
c. Identify and explain the responsibilities associated with server administration and management.
d. Explain the benefits of managing users and groups.

Content Management

What is Content Management?

Content management (CM) is the process for collection, delivery, retrieval, governance and overall management of information in any format. The term is typically used in reference to administration of the digital content lifecycle, from creation to permanent storage or deletion. The content involved may be images, video, audio and multimedia as well as text.

Content management process

Content management practices and processes can vary by purpose and organization. This can lead to differences in steps or terminology.

The stages of the content management lifecycle are:

1. Organization: The first stage where categories are created, taxonomies designed and classification schemes developed.
2. Creation: Content is classified into architectural categories.
3. Storage: Content format and storage decisions are made based on ease of access, delivery, security and other factors dependent on the organization's needs.
4. Workflow: Rules are designed to keep content moving through various roles while maintaining consistency with the organization's policies.

5. Editing/Versioning: This step involves managing multiple content versions and presentation changes.
6. Publishing: The stage where content is delivered to users, which can be defined as website visitors or internal publishing via the Intranet for employees.
7. Removal/Archives: The final stage where content is deleted or moved to an archive when it is infrequently accessed or obsolete.

Content Management System (CMS)

A content-management system (CMS) is a publication system for web sites. For example, a newspaper CMS might facilitate the process of reporters creating stories, which are then queued to editors, edited, and approved for publication. The CMS releases the article at a specific time, placing it on the web site, updating tables of contents, and taking care of other details. For an IT site, the CMS might permit plug-ins that give portal features, such as summaries of recent outages. A number of features are required to implement a functional CMS.

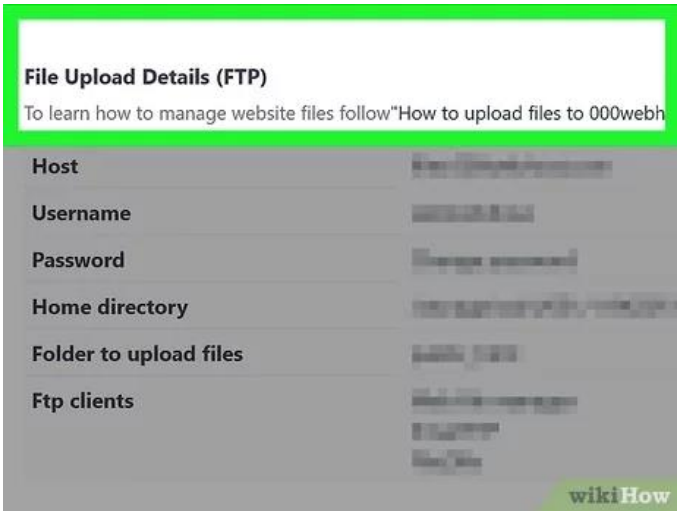
A CMS specifically consists of three layers: repository, history, and presentation. The repository layer is generally a database but may also be a structured file system with metadata. The content is stored in this layer. The history layer implements version control, permissions, audit trails, and such functionality as assigning a global document identifier to new documents. The history layer may be a separate journal or database or may be stored in the repository. The presentation layer is the user interface. In addition to allowing document interactions, such as browsing or editing, the presentation layer may implement document controls, such as read-only access or permissions.

Web Content Management

Web content management: Web content management is used to create, manage and display webpages. A web content management system (WCMS) is a program that provides organizations with a way to manage digital information on a website without prior knowledge of web programming and can include components for a specific industry, such as a content management application (CMA) that automates the production of HTML.

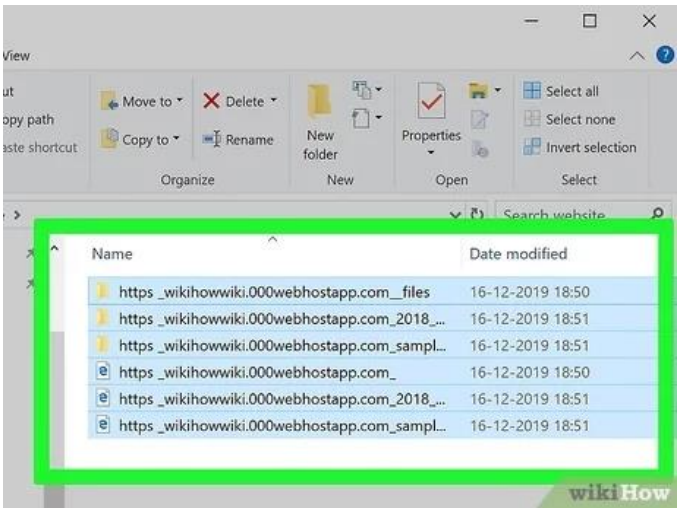
Content Deployment on Windows

1. **Find your hosting service's FTP information**

2. 

Before you can upload your website, you'll need to know your username, password, and website address for your hosting service's FTP server. This can usually be found in the "FTP" section of the hosting service's dashboard.

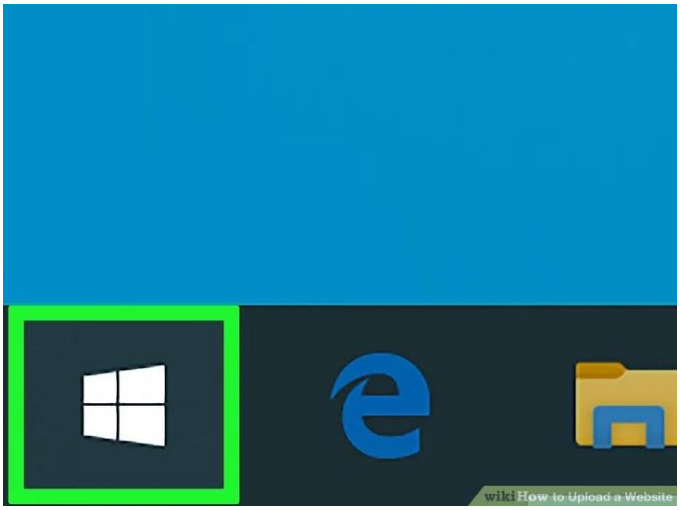
- Common examples of hosting services include GoDaddy and Hostinger. You must be logged in to see this information.
- If your website doesn't support FTP, you'll need to upload it directly to your hosting service's control panel instead.



Copy your website's files

Open the folder in which your website's files are stored, then click and drag your mouse across the files to highlight them and press Ctrl + C to copy them.

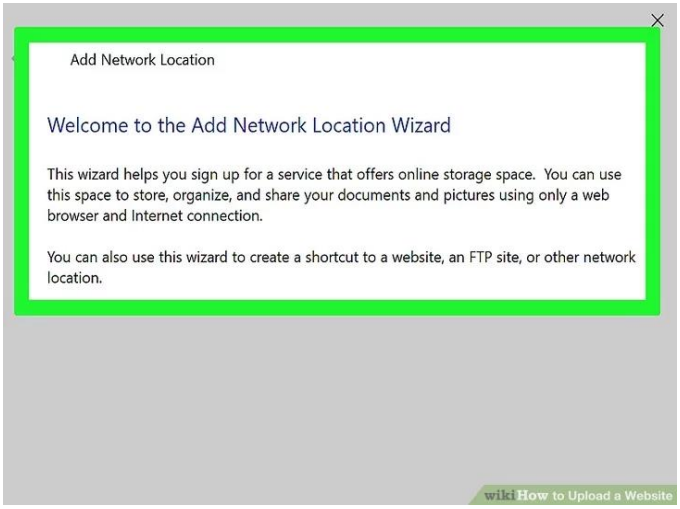
- The website's files typically include an index file, a cascading style sheet (CSS) file, and an images folder.



3. **Open This PC**

Double-click This PC on your computer's desktop, or type this pc into Start and then click This PC at the top of the search results. The "This PC" window will open.

4. Create a new FTP network folder

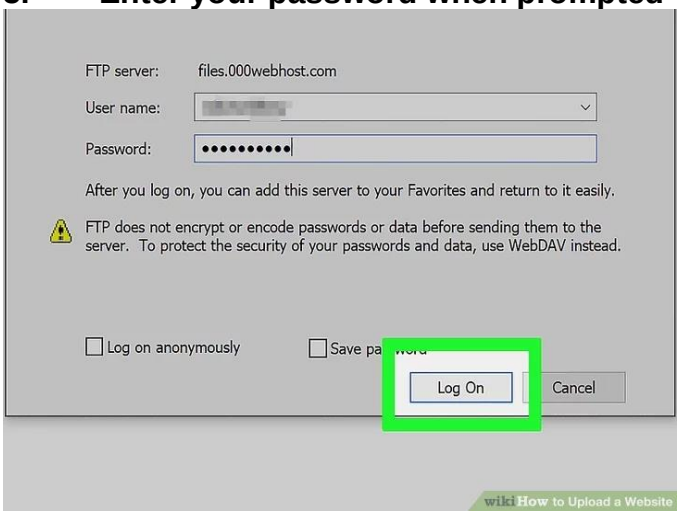


You can connect to your website hosting service's FTP folder by doing the following:

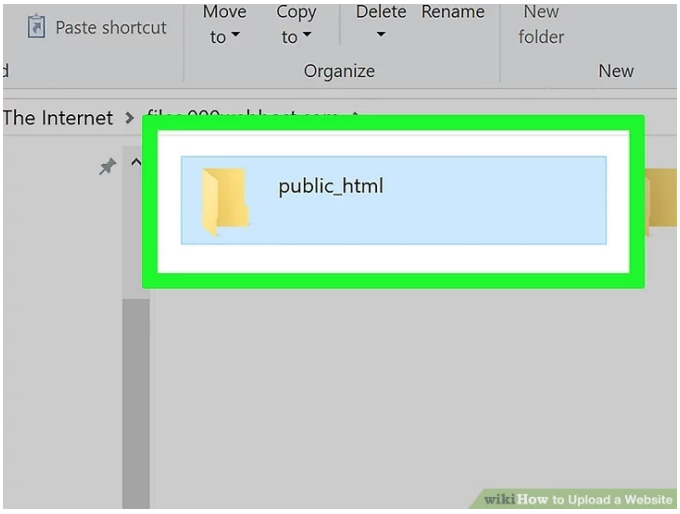
- Click the Computer tab.
- Click Add a network location, then click Next twice.
- Enter your hosting service's FTP address, then click Next.

- Uncheck the "Log on anonymously" box, then enter your FTP username and click Next.
- Enter a name for the network, click Next, and click Finish.

5. Enter your password when prompted

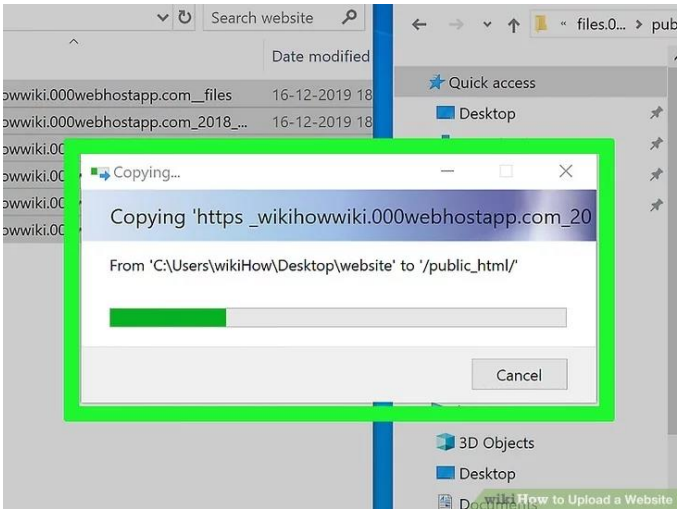


Once the FTP folder opens, you'll be prompted to type in the password which was listed on your hosting service's FTP page.



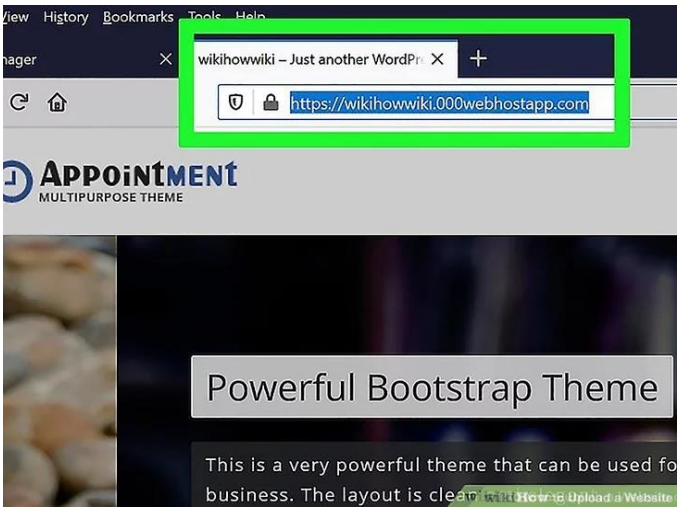
6. Open the "public_html" folder

In the FTP folder, double-click the "public_html" (or "html", or "root") folder to open it.



7. Paste in your website's files

Click a blank space in the folder, then press Ctrl+V to paste the files into the folder.



8. Access your website

In your computer's web browser, go to your website's domain address. As long as your website's files have finished uploading to your website's FTP folder, your website should be live.

Server Administration

A server is simply a computer that grants other computers access to centralized data or resources. There are various types of servers, and a few factors determine which kind of server admin someone requires. In a nutshell, hiring server administrators is a crucial step to ensure your system works as expected.

The only way to avoid hiring the services of a server administrator is by choosing a cloud-based system that allows you to store and manage your data online. In that case, you'd need to look for a company that offers web hosting to ensure the platform is secure from hacking. Now let us break it down further.

Nowadays it's really easy to set up a server, with many essential server management functions you need via auto-install. Servicing your server is a different matter. Because keeping tabs on maintenance plus performance and utilization levels can be time-consuming. It gets even more difficult to perform server administration when your operations include multiple servers. Tapping into a single vendor can trap you; consider using a mix of vendors for your server operating systems.

Manual management across big installations is time-consuming. You just can't manually log into server administration consoles on a machine by machine basis. Server management software is therefore crucial to successful management procedure. Most of these tools come with remote administration and machine monitoring thus, enabling you to manage machines across a range of sites in an efficient manner.

User and group management

User management describes the ability for administrators to manage user access to various IT resources like systems, devices, applications, storage systems, networks, SaaS services, and more. User management is a core part of any identity and access management (IAM) solution, in particular directory services tools. Controlling and managing user access to IT resources is a fundamental security essential for any organization. User management enables admins to control user access and on-board and off-board users to and from IT resources. Subsequently a directory service will then authenticate, authorize, and audit user access to IT resources based on what the IT admin had dictated.

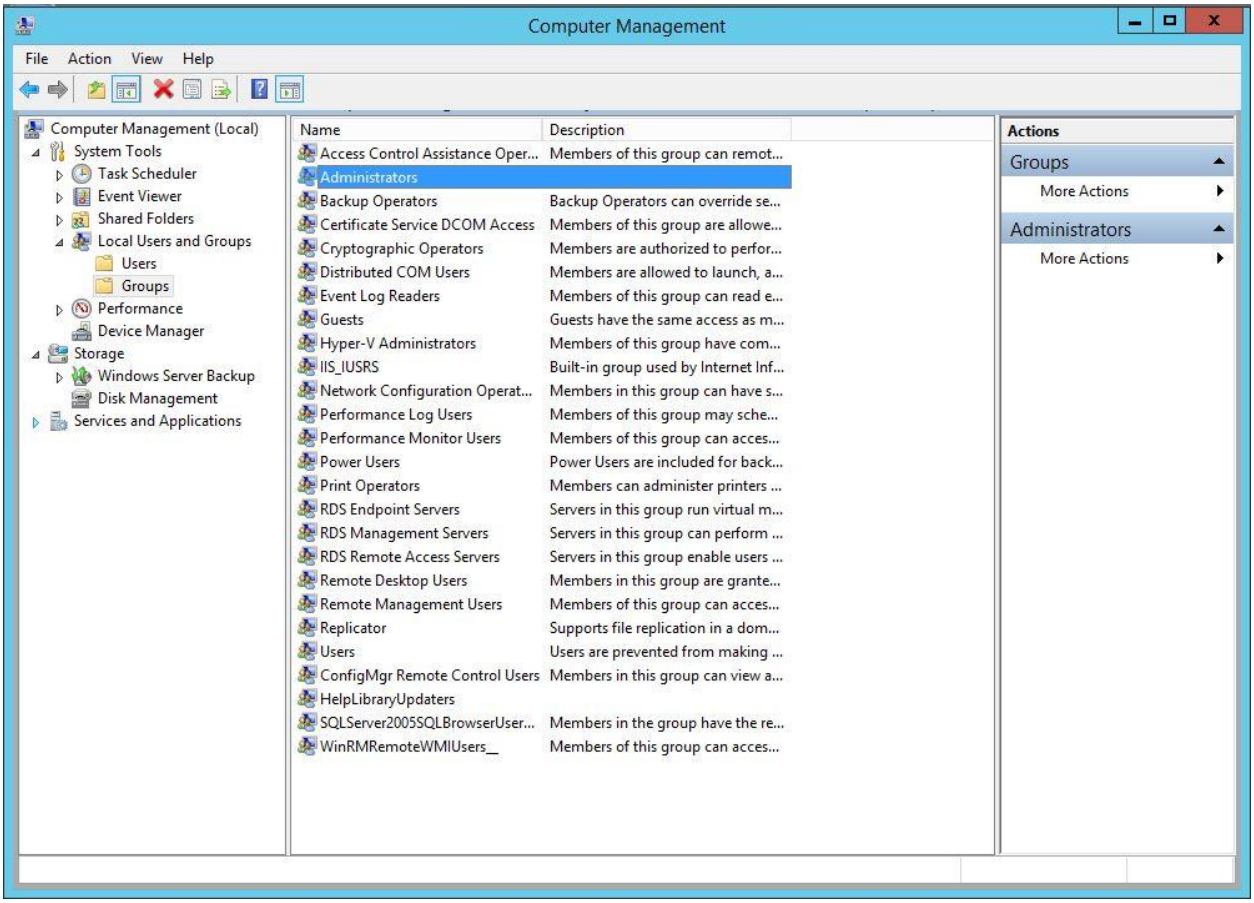
User Groups

User Groups is a group of users that share the same security access level to server resources. For example, if there are several interns in your company, you may want to limit them to read-only permissions to a company folder, read/write permissions to a public folder, and no permissions to Remote Web Access. In the past, you could only do this in the Dashboard by opening the property page of each intern user and updating

these settings one by one. With the integration of user groups, you can simply create a group named Interns, add each intern user to the group, and configure the permission settings only once for the entire group.

If you have integrated Windows Azure Active Directory with a server running the Windows Server Essentials Experience server role, when you create a new user group you can also assign an existing or new Microsoft Online Services security group to it. The local user group and the online security group will keep their membership in sync: if you add or remove a local user in the local user group, the corresponding online user will automatically be added or removed in the online user group.

Different User Groups



Here are the some types of the users stated above

Access Control Assistance Operators - Members of this group can remotely query authorization attributes and permissions for resources on this computer.

Administrators - Administrators have complete and unrestricted access to the computer/domain.
Backup Operators - Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Cryptographic Operators - Members are authorized to perform cryptographic operations.
Device Owners - Members of this group can change system-wide settings.
Distributed COM Users - Members are allowed to launch, activate and use Distributed COM objects on this machine.
Event Log Readers - Members of this group can read event logs from local machines.
Guests - Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted.
Users - Users are prevented from making accidental or intentional system-wide changes and can run most applications.
Network Configuration Operators - Members in this group can have some administrative privileges to manage configuration of networking.

Distribution Groups

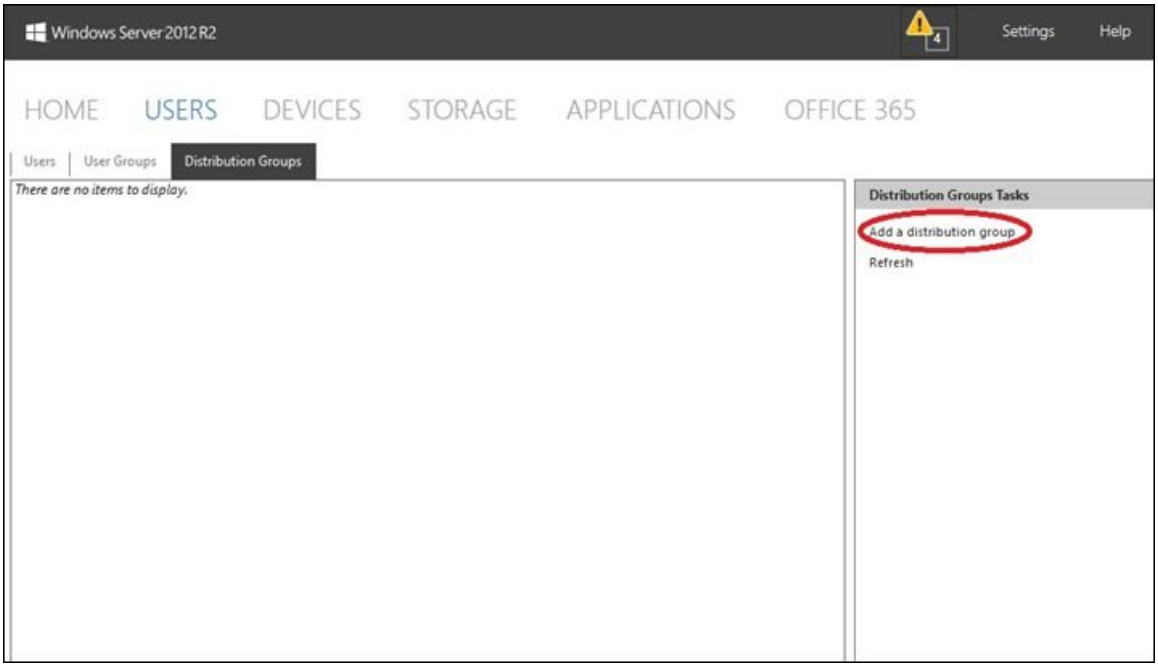
Distribution Groups is a feature that Office 365 Exchange Online provides. It is a collection of users that appears in the shared address book. When an email message is sent to a distribution group, it goes to all members of the group. Using distribution groups enables you to:

- Easily send an email message to a lot of people at once.
- Help people inside and outside your organization communicate and collaborate more easily.
- Not exceed the maximum number of recipients per message.

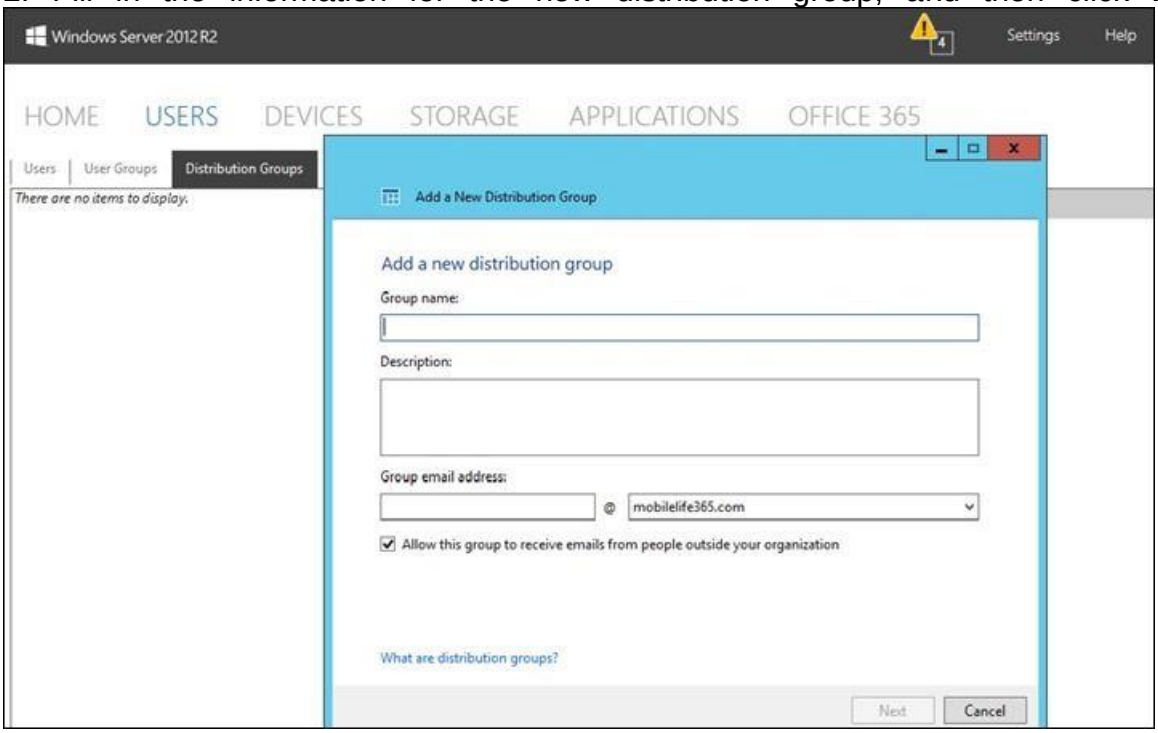
Creating a new user group or distribution group in Windows Server

The process for creating a new user group or distribution group is very similar. To create a user group, follow the same steps but start on the User Groups tab. After Essentials is integrated with Office 365, distribution group-related tasks will show up on the **Users>Distribution Groups** tab in the Essentials Dashboard. Use the following steps to create a new distribution group:

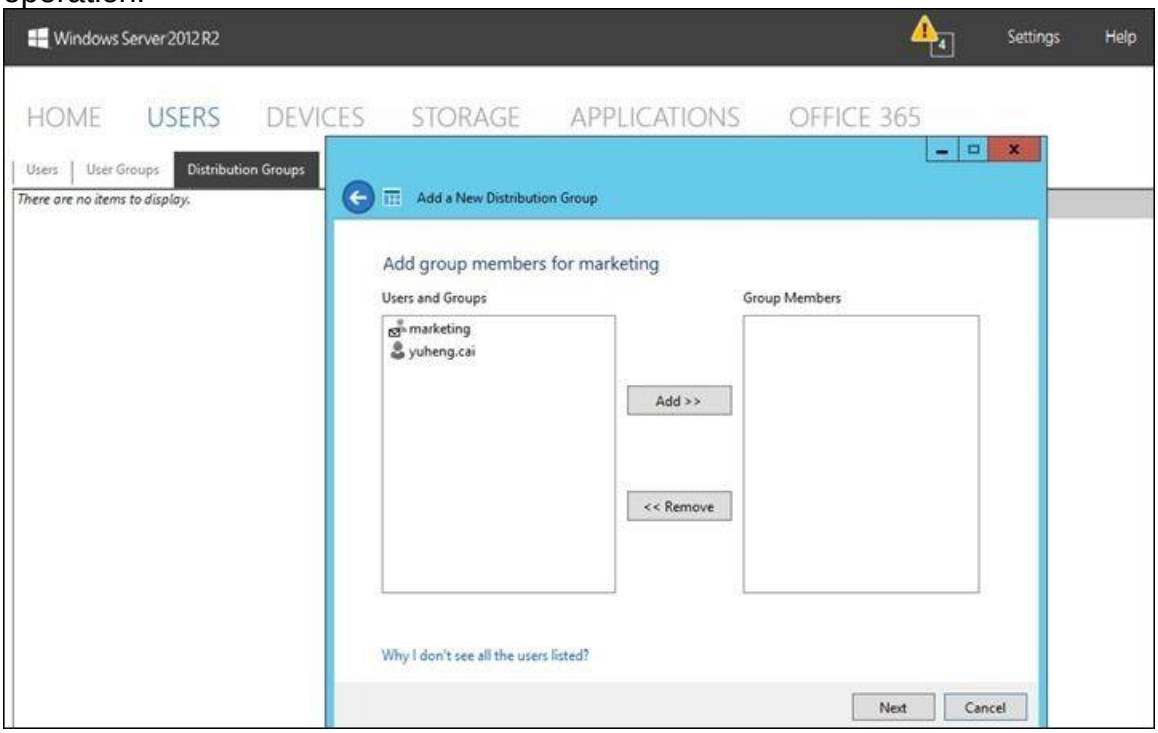
1. In the right pane, select the **Add a distribution group** task.



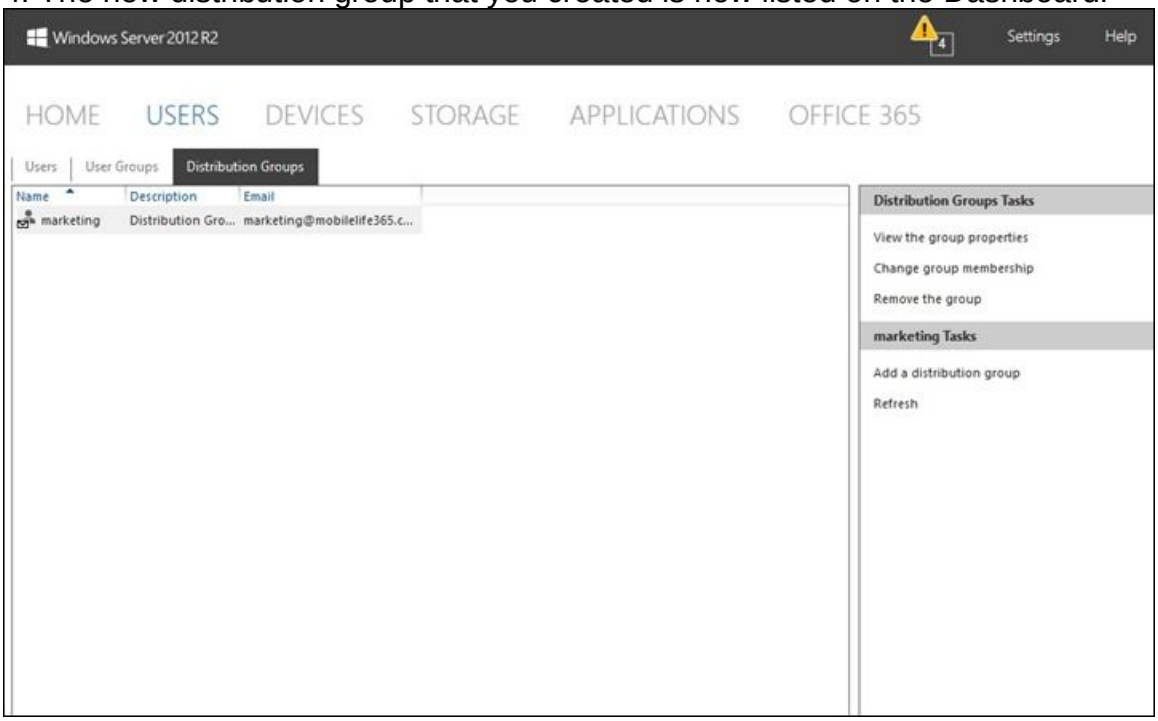
2. Fill in the information for the new distribution group, and then click **Next** .



3. Add group members to the distribution group, and then click **Next** to complete the operation.



4. The new distribution group that you created is now listed on the Dashboard.



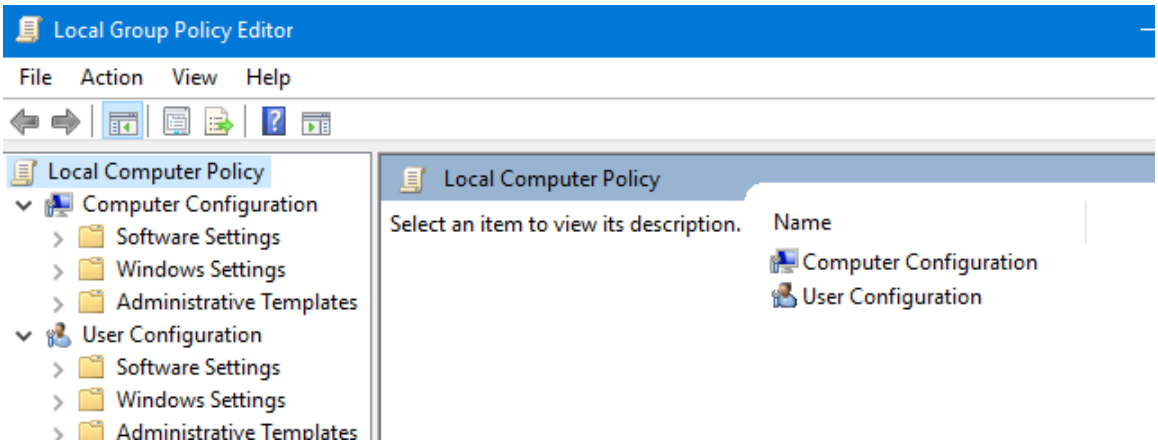
What is a Group Policy Object (GPO)?

A Group Policy Object (GPO) is a group of settings that are created using the Microsoft Management Console (MMC) Group Policy Editor. GPOs can be associated with a single or numerous Active Directory containers, including sites, domains, or organizational units (OUs). The MMC allows users to create GPOs that define registry-based policies, security options, software installation and much more.
The Benefits of Group Policy for Data Security

The benefits of Group Policy are not limited solely to security, there are a number of other advantages that are worth mentioning.

- **Password Policy:** Many organizations are operating with relaxed password policies, with many users often having passwords set to never expire. Passwords that aren't regularly rotated, are too simple or use common passphrases are at risk of being hacked through brute force. GPOs can be used to establish password length, complexity and other requirements.
- **Systems Management:** GPOs can be used to simplify tasks that are at best mundane and at worst critically time consuming. You can save yourself hours and hours of time configuring the environment of new users and computers joining your domain by using GPOs to apply a standardized, universal one.
- **Health Checking:** GPOs can be used to deploy software updates and system patches to ensure your environment is healthy and up to date against the latest security threats.

What is the Local Group Policy?



Local group policy.

By definition, the *Group Policy* is a Windows feature that offers you a centralized way of managing and configuring the Windows operating system, the programs and user settings from the computers that are connected to the same domain. *Group Policies* are most useful if you are a network administrator and you need to enforce certain rules or settings on the computers or users found in the network that you manage.
Local Group Policy is a variant of *Group Policy* that also lets you control individual computers, as opposed to all the computers that are registered on a domain. A good example is your home computer with Windows 10, Windows 8.1 or Windows 7. That means that this tool can be useful to home users as well as to network administrators. To put it into simple terms, you should think about *Local Group Policy* as a set of rules that govern how Windows works on your computer or device.

Can I use the Local Group Policy Editor?

Because *Local Group Policy Editor* is a rather advanced tool, you should know that it's not available in the *Home* or *Starter* editions of Windows. You can access it and use it only in:

- Windows 10 Pro and Windows 10 Enterprise
- Windows 7 Professional, Windows 7 Ultimate and Windows 7 Enterprise
- Windows 8.1 Professional and Windows 8.1 Enterprise

A few examples of what you can do with the Local Group Policy Editor

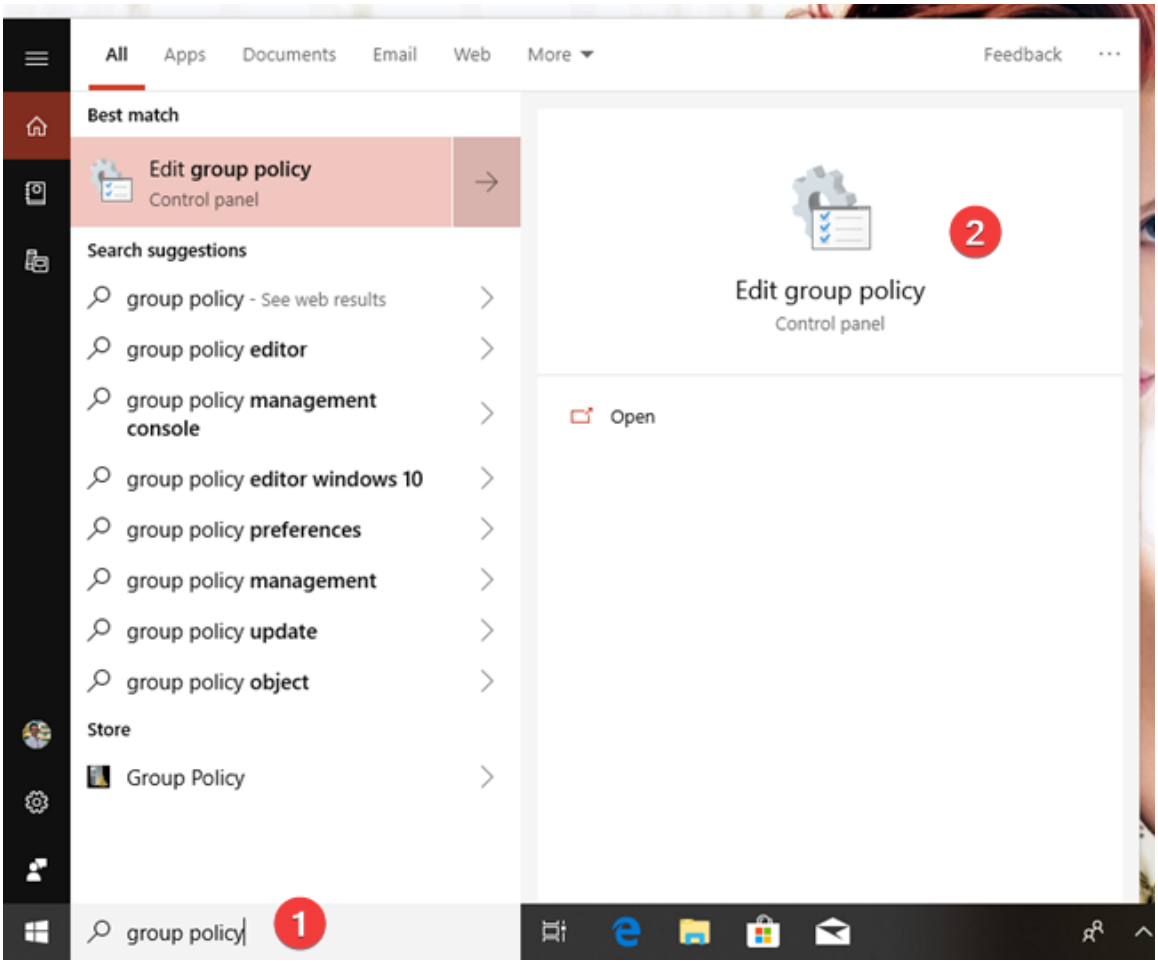
Let's list a few examples of what you can do with *Local Group Policy Editor*. You can configure Windows settings and you can enforce them so that the users on your computer cannot change them afterward. Here are just a few examples:

- Allow users to access only some of the applications found on your computer.
- Block users from using removable devices (ex. USB memory sticks) on the computer.
- Block users' access to the *Control Panel* and to the *Settings* app.
- Hide specific elements from the *Control Panel*.
- Specify the wallpaper used on the *Desktop* and block users from changing it.
- Block users from enabling/disabling LAN connections or block them from changing the properties of the computer's LAN (Local Area Network) connections.
- Deny users to read and/or write data from CDs, DVD, removable drives etc.
- Disable all the keyboard shortcuts that start with the *Windows* key. For instance, *Windows* + *R* (which opens the *Run* windows) and *Windows* + *X* (which opens the power user menu) stop working.

These are just a few examples. The *Local Group Policy Editor* from Windows allows you to configure many other settings.

How to open the Local Group Policy Editor in Windows

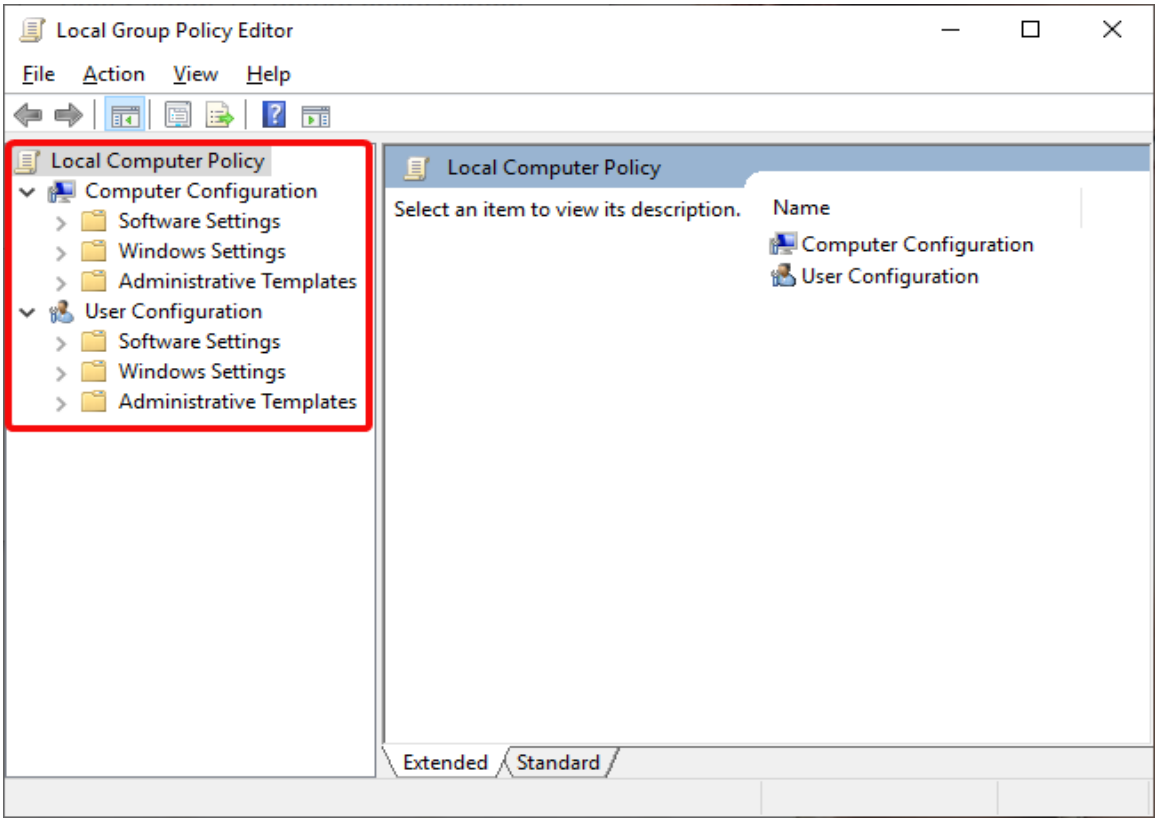
In Windows, an easy way to open the *Local Group Policy Editor* is to use the search. Enter *"gpedit.msc"* as a search text and then click the *"gpedit"* search result.



How to work with the Local Group Policy Editor

The *Local Group Policy Editor* is split into two panels: the left panel contains the *Local Group Policy* settings displayed in categories, while the right side panel shows the contents of the active category. The *Local Group Policies* are categorized into two large sections:

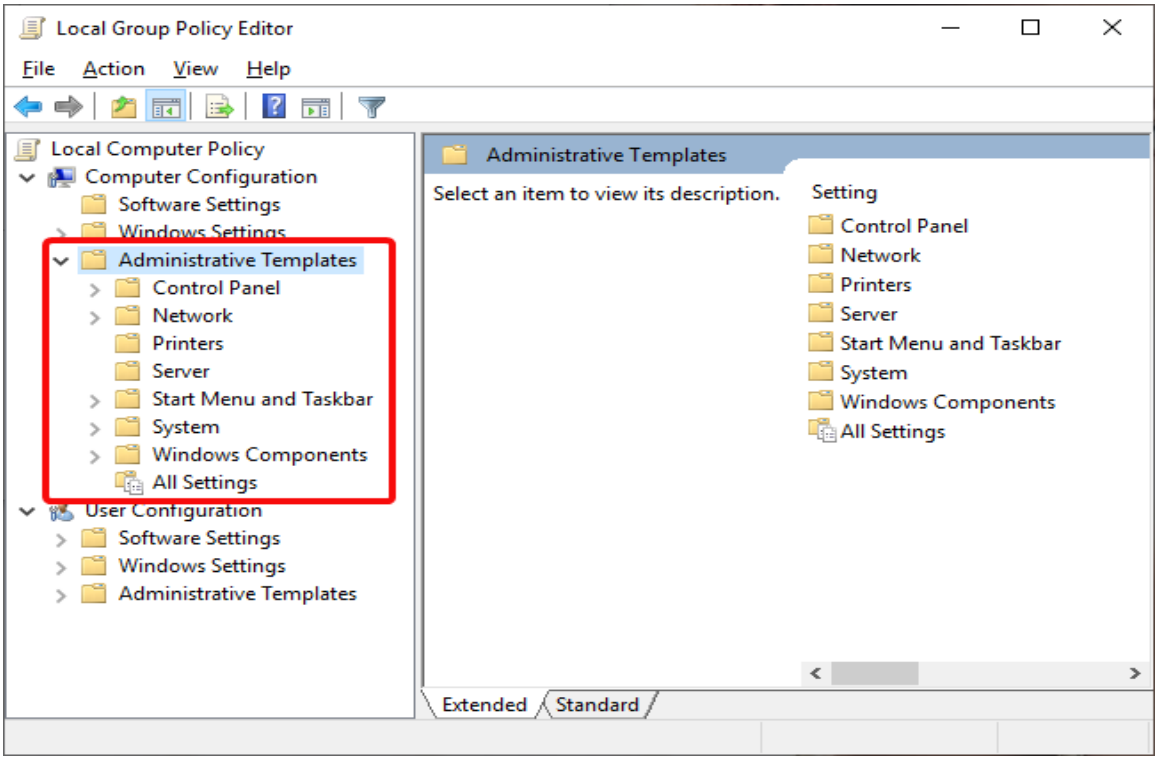
- *Computer Configuration* - holds *Local Group Policy* settings that control policies that are applied computer-wide, regardless of the user or users logged in.
- *User configuration* - holds *Local Group Policy* settings that control user policies. These policies are applied to users, rather than the whole computer. While it's outside the scope of this guide, you should know that user policies are applied for users regardless of which computer from your network they log into.



Local Group Policy Editor categories

Both the *Computer Configuration* and the *User Configuration* categories are split into three sections:

- *Software Settings* - contains software policies and, by default, it should be empty.
- *Windows Settings* - holds Windows security settings. It's also the place where you can find or add scripts that should run when Windows starts or shuts down.
- *Administrative Templates* - has lots of settings that control many aspects in terms of how your computer works. This is the place where you can see, change and even enforce all kinds of settings and rules. To give you a few examples, you can manage how the *Control Panel, Network, Start Menu, and Taskbar* work and what users can change when using them.



Administrative Templates in Local Group Policy Editor

How to edit Windows policies using the Local Group Policy Editor

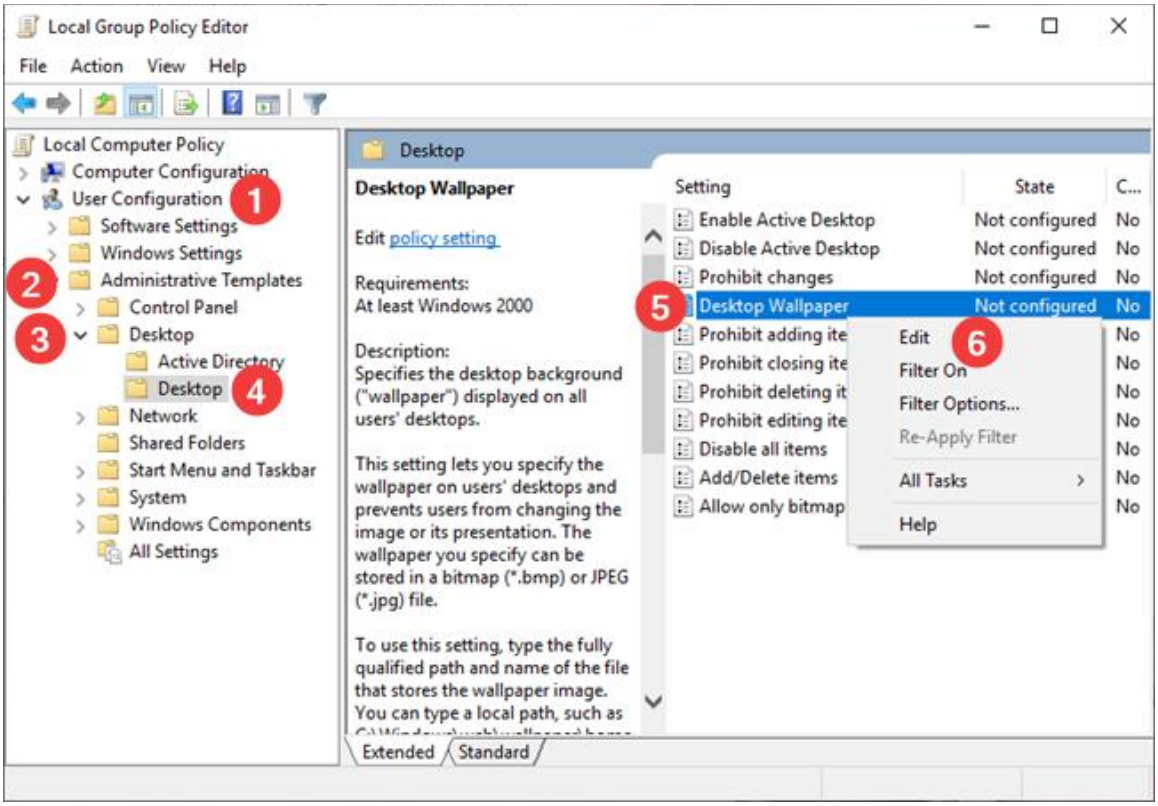
In order for you to easily understand the process involved in editing policies, we are going to use an example. Let's say that you want to set a specific default wallpaper for your desktop, one that's going to be set for all existing or new users on your Windows computer.

To get to the *Desktop* settings, you will have to browse the *User Configuration* category from the left panel. Then, go to the *Administrative Templates*, expand *Desktop* and select the inner *Desktop* settings. On the right panel, you will see all the settings that you can configure for the currently selected *Administrative Template*. Note that, for each setting available, you have two columns on its right side:

- The *State* column tells you which settings are *Not configured* and which are *Enabled* or *Disabled*.
- The *Comment* column shows you the comments you or another administrator made for that setting.

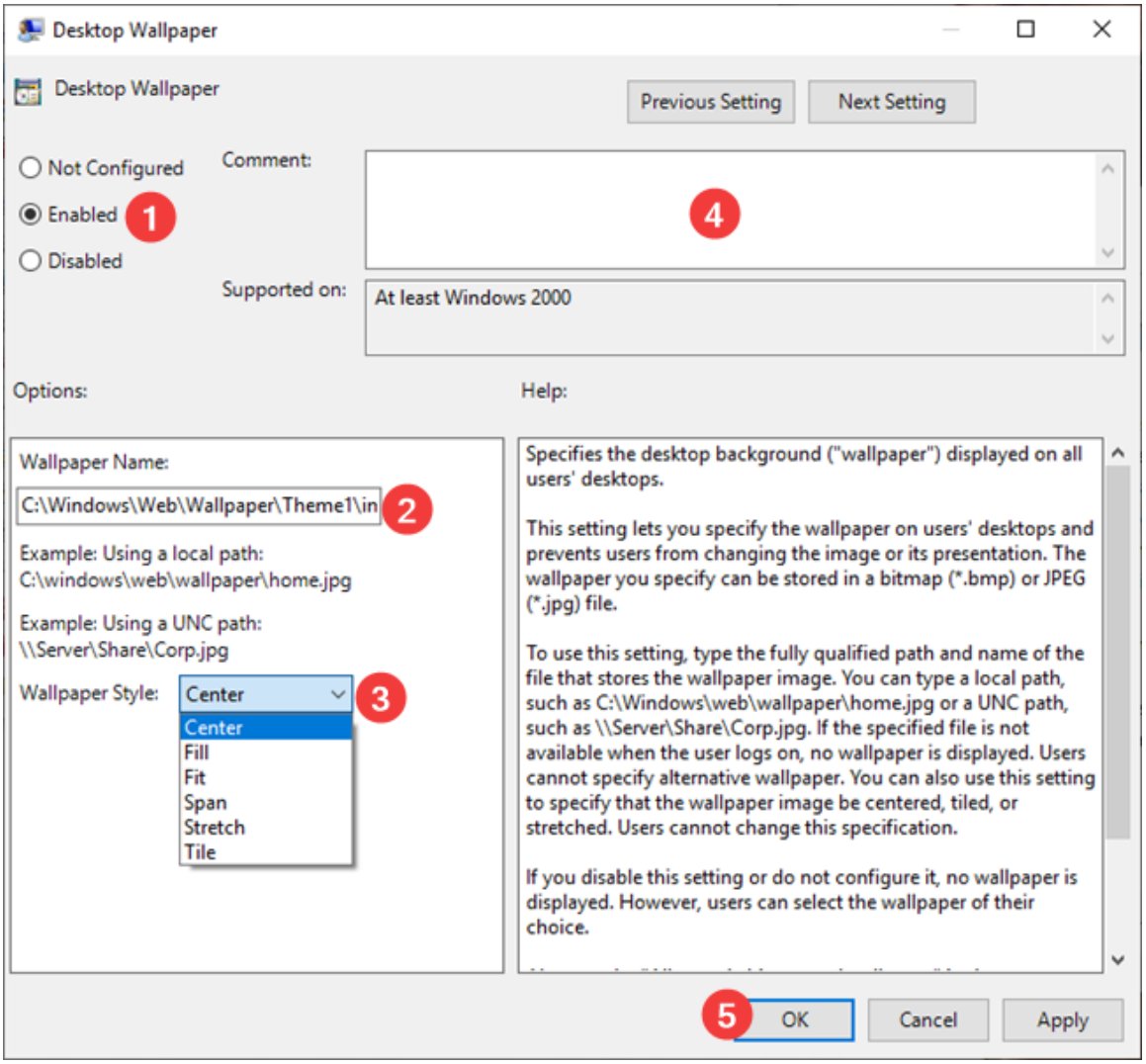
The left side of this panel also shows detailed information about what a specific setting does and what are its effects on Windows. This information is displayed in the left part of the panel, whenever you select a certain setting. For instance, if you select the *Desktop Wallpaper*, on the left you will see that it can be applied on Windows versions from *Windows 2000* on, and you can read its *Description*, which tells you that you can specify *"the desktop background ('wallpaper') displayed on all users' desktops. [...]"*. If

you want to edit a setting, in our case the *Desktop Wallpaper*, double click/tap on that setting, or right click/tap and hold on it and then select *Edit* from the contextual menu.



Desktop Wallpaper in Local Group Policy Editor

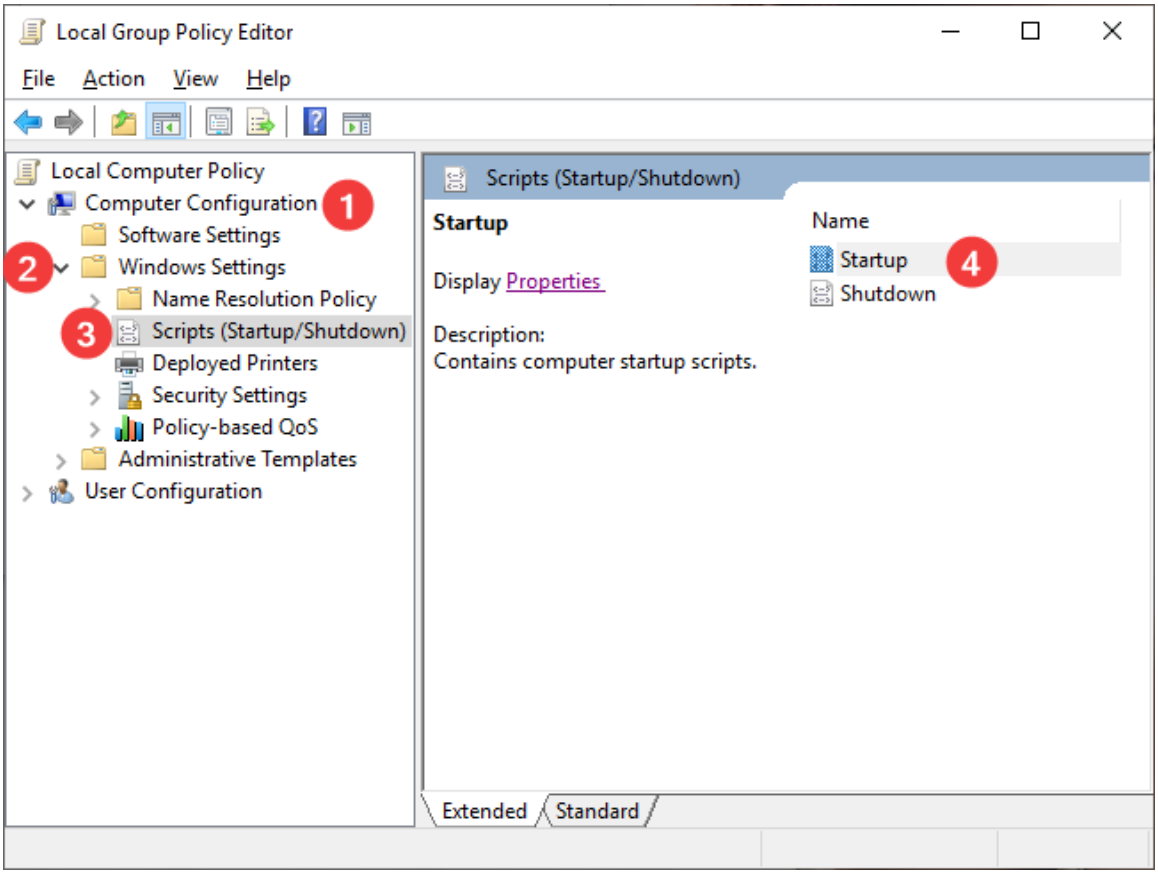
A new window that bears the name of the setting you selected is now opened. Inside that window, you can choose to *Enable* or *Disable* the setting, or you can choose to leave it *"Not configured"*. If you want to enable the setting, first select it as *Enabled*. Then, read its *Help* section and, if there's also an *Options* section, make sure you fill in the details that are asked of you. Note that this window can include different options, depending on the setting you choose to edit. For instance, in our example about specifying a *Desktop Wallpaper*, we have to provide the path to the image file we want to set as wallpaper and we must select how we would like it to be positioned. Then, we can add a comment (if we want to - this is entirely optional) and, finally, we have to press the *Apply* or the *OK* button in order to activate our setting.



Set up Desktop Wallpaper in Local Group Policy Editor

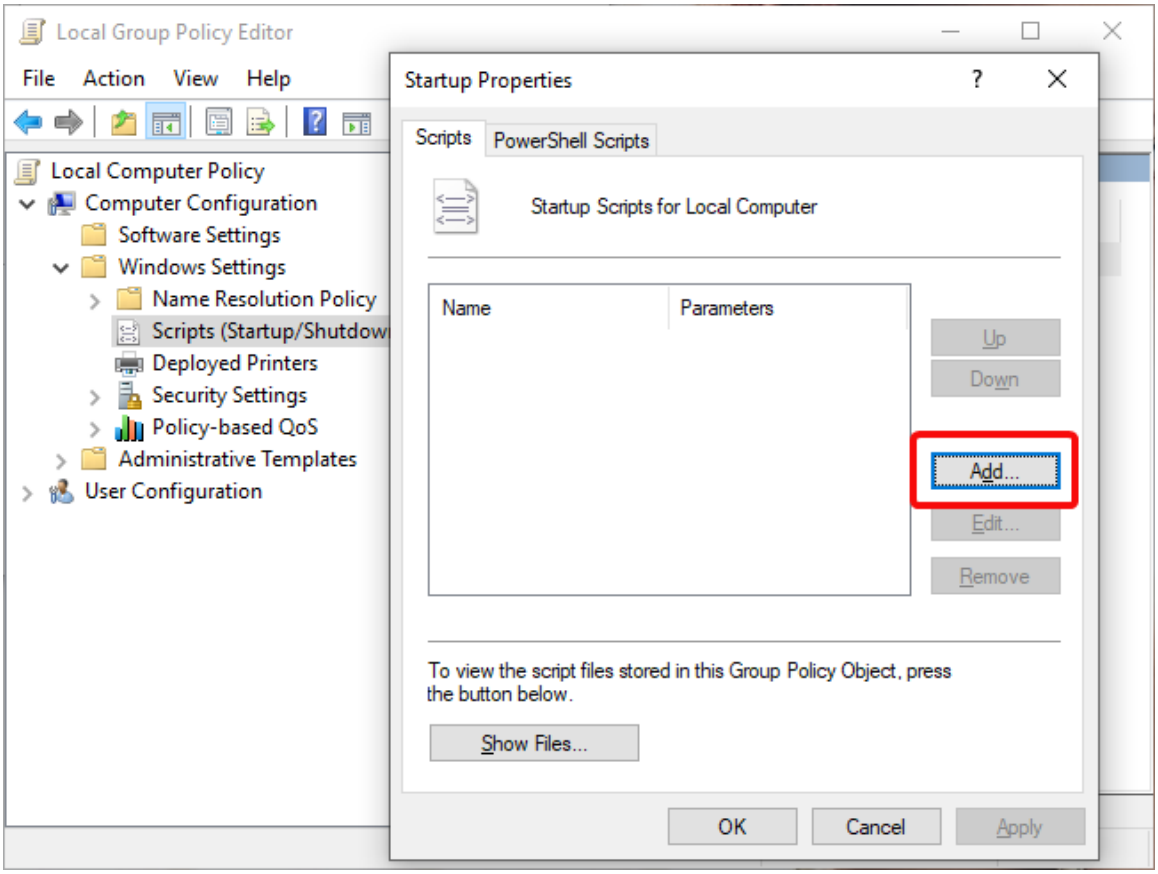
Disabling a setting or changing its status to *"Not Configured"* involves the simple selection of one of these options. As we mentioned earlier, different settings have different options. For instance, the *Scripts* you can set Windows to run when it starts or when it shuts down might look completely different.

Click or tap on *Computer Configuration*, then on *Windows Settings* and *Scripts (Startup/Shutdown)*. Select the *Startup* or *Shutdown* in the right panel, and click on tap the link *Properties* in the right panel. Alternatively, double-click *Startup* or *Shutdown*.



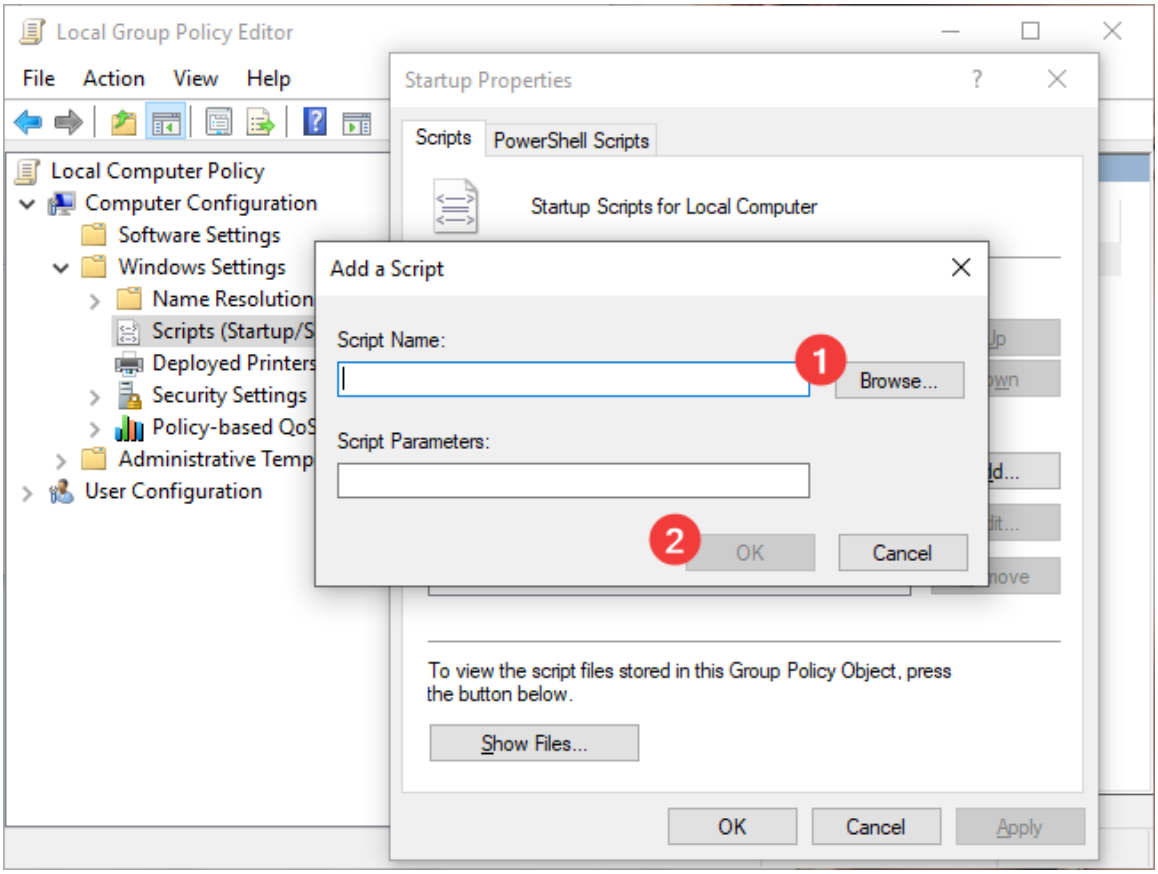
Startup and Shutdown Scripts in Local Group Policy Editor

Click or tap on *"Add…"* to add new scripts to the selected process.



Add scripts to Startup in Local Group Policy Editor

In this case, you won't *Enable* or *Disable* anything. Instead, you can add or remove various scripts from being run at Windows *Startup* or *Shutdown*.



Add a Script to Startup in Local Group Policy Editor

When you finish, click or tap *OK*.

Chapter Assessment:

1. Which issues need to be considered differently when providing external web services versus internal services to your organization?
2. Give an example of user management.
3. Is user management a need or is it just situational? Provide 1-2 sentences explanation.
4. What are the responsibilities of a server administrator?
5. Discuss the different server management tools

Backup Management, Security Management and Disaster Recovery

Introduction

Data is considered one of the most valuable assets of every company as it allows to effectively measure and record a wide range of business activities. It is an addition to the responsibilities of system administrators to manage the backup and security of these data as well as to prevent any disaster from harming it. Ensuring the safety of the company's data will not only avoid jeopardizing the business but also optimize the work environment of the company.

Objectives

At the end of this chapter, the students must be able to:

1. Create policies governing IT systems
2. Design and deliver training sessions on IT systems and policies

---

Backup Management

In the event of a primary data failure, backups create a copy of the data that can be retrieved. These failures can be caused by hardware or software faults, data corruption, or human error, such as a malicious attack or an unintentional deletion. As a result, system backup and recovery is an important skill for both system administrators and the companies they work for.

Managing backups after they've been created is an important aspect of a backup and recovery plan. This is because databases, and data stored on disk in general, can become corrupted just from sitting on a disk. Further risk is introduced when third-party data synchronization components and snapshotting technologies are used. Backup management entails deleting obsolete backups and performing periodic checking to ensure that backups are usable and available.

- **Factors in Developing Backup Strategies**

1. **Cost** – Backups costs money. One should consider to buy hardware and software, as well as pay for maintenance agreement and staffs.
2. **Backup Location** – Depending on one's budget, on-site and off-site backups are both recommended.

3. **Backup Method** - Each backup method requires a different quantity of storage, which affects prices, as well as a varied amount of time, that can affect both the length of the backup procedure and recovery times.
4. **Backup and Recovery Flexibility** - When it comes to backups, it's common to want to back up everything, but this isn't always the case when it comes to recovery. The ability to scale recovery from restoring a single file to recovering an entire server is required.
5. **Backup Schedule** – Backups should be automated and executed on a regular basis, rather than relying on someone remembering to do it manually. They should be set to run regularly enough to capture both frequently changing and rarely changing data. Backups should be scheduled to coincide with the needs of the production workflow. Here's where recovery point and recovery time objectives come into play; these targets shouldn't be universal; instead, they should be tailored to the demands of each system. Each system's backup schedule could be different.
6. **Scalable** - Backup system should be able to handle expected data volumes. One should have a procedure in place to ensure that new servers, apps, and data repositories are backed up.
7. **Backup Security** - Backups must be accessible when needed, but not just anyone should have access to them. It is critical to ensure that backups are secure against tampering in order to protect your organization.
8. **Recovery time objective** (RTO) - refers to maximum amount of time the business can afford to be without access to the data or application—or, how quickly you need to recover the data and application.
9. **Recovery point objective** (RPO) - refers to the amount of data you can afford to lose and effectively dictates how frequently you need to back up your data to avoid losing more.

- **Identifying data to backup**

But where do you start in backing up data? The first thing to figure out is what data are needed to be backup and understand file structure. These data if processed are called information which can provide insights and inferences. Correlated information which are stored on secondary or non-volatile storage like magnetic disks, optical disks and tapes are what file is. One should start at backing up these files that are absolutely necessary for business operations, such as E-mails, sales databases, financial spreadsheets, server configurations, and databases.

- **Identifying the location to backup data**

Data can be backed up either to remote systems, or locally to on-site servers. Both approaches have advantages and disadvantages, assisting in reducing certain hazards.

➢ **Locally to on-site Servers**

The physical proximity of the data is an advantage of onsite backup systems. The data may now be accessed much more quickly as a result of this. In addition, because you are not transferring data outside of your internal network, you won't require as much outbound bandwidth. Also, if you need to restore data from backups, you should be able to do it fast because the data is readily available. However, disasters such as structure fire are unanticipated. The systems we were backing up, as well as the backup server, can be destroy easily.

➢ **Offsite backups**

Offsite backups are therefore highly recommended. Making backups of crucial data and transmitting them offline to distant servers in a separate physical location is part of this process. Another backup server in a different office, or a cloud-hosted backup service, could be used. There are, however, trade-offs.

Offsite backups help us plan for disasters that can wipe out data from an entire workplace, but transmitting data offsite requires you to send it outside of your network. This implies you'll have to think about encryption and bandwidth. Depending on organization's budget it is recommended one to have both on-site and off-site servers.

➢ **3-2-1 Backup Strategy**

3-2-1 strategy dictates: two on-site (but on different storage media) and one off-site (for a total of three copies).

Consider keeping a backup copy of essential application data in your data center for speedy recovery and a second copy on a different infrastructure (e.g., tape or disk media) to avoid a single point of failure. Then you upload your data to an off-site cloud on a regular basis; this is your third copy. If necessary, this duplicate can be "disconnected," creating an "air gap" to protect against cyber hacking or ransomware.

- **Backup devices and services**

  - **Tape drive**

    Tape is the oldest backup medium in use today. It offers low-cost, high-capacity data storage, but relatively slow read/write performance makes tape a poor choice for incremental backup, continuous data protection (CDP) or any other backup method that updates backups whenever data changes (see the 'Common methods and solutions' section below).

    Tape is also more prone to physical wear and damage than other storage media so it needs to be closely managed and constantly tested to ensure that it will work when it's time for recovery. For these reasons, tape is a better choice for nightly or weekly backups or for cost-effectively archiving data that your organization wants or needs to keep but doesn't need in order to quickly bring the business back online in the event of an outage or disaster.
  - **Hard disk drives (HDDs) or solid-state drives (SSDs)**

    Most data today are backed up to a hard disk drive (HDD) or solid-state drive (SDD), whether that drive is a standalone external drive or part of a backup server (see below). Both offer much faster read/write performance than tape, making them a good choice for continually-updated backups and short-RTO/RPO backup scenarios.

    SDDs are increasingly popular because they offer faster read/write times than HDDs, require less physical space to store the same amount of data, and consume less power (even if they are more expensive to purchase per gigabyte). If HDDs and SDDs have a drawback, it's that they aren't particularly scalable—if you need more backup capacity, you have to purchase and install a new physical disk.
  - **Backup server**

    A backup server is a dedicated server built specifically for backing up files stored on multiple client computers on the same network. The server is outfitted with significant disk storage and specialized software for scheduling and managing backups. Backup server disks are often configured for redundancy to protect backup data and ensure that backups continue in the event of a disk failure. An onsite backup server can be a cost-effective backup solution for a small office but does not protect backup data against local outages or physical disasters.
  - **Cloud backup**

    Cloud backup backs up your data and applications via a corporate network or internet connection to a physical or (more likely) virtual backup server at a remote data center operated by your company, a hosting provider, or a cloud services provider.

- **Understanding Cloud Options**

Cloud backup is a service that backs up and stores data and apps on a business's servers on a distant server. Businesses use cloud backup to keep files and data accessible in the case of a system outage, outage, or natural disaster.

- **Cloud Storage**

  Cloud storage is essentially a remote filesystem that you may access. It's up to you how you use the available space; depending on the capabilities of the cloud provider, you may be able to access it as a local filesystem. Its capacity is unlimited, unlike local filesystems. Also in cloud storage, one only pays for what the organization use. Another benefit of cloud storage is that most cloud providers service many regions, allowing you to store data in a separate area.

- **Cloud Sync**

  Cloud sync copies folders from your local filesystem to a cloud-based file system. This is frequently used to share files so that they can be accessed from anywhere, effectively turning them into production data rather than backup data. Cloud sync may or may not allow you to view older versions of data, depending on the manufacturer.

- **Cloud Backup**

  Cloud backup works similarly to regular backup software, but the objective is the cloud rather than a local drive. The software backs up changes to the cloud on a regular basis, with previous versions retained. Backup software that runs in the cloud or in your local data center can be used to enable cloud backup. When it comes to when and how data is duplicated, cloud backup gives you more control than cloud sync. Compression and deduplication are frequently used in cloud backup to reduce the size and expense of backed-up data, and encryption may be used for security.

- **Cloud Disaster Recovery**

  In the event of a disaster, cloud disaster recovery gives the additional support needed to retrieve files and virtual machine images. High levels of automation are used in Disaster Recovery as a Service (DRaaS) to quickly bring systems up in the cloud.

- **Common methods and solutions**

The following is a list of the most commonly used backup and restore methods. The method or mix of methods you choose will depend on the factors mentioned earlier (RTO, RPO, scalability, security, geographic distance requirements) :

- **Full-image backup**

  Full-image only backup periodically backs up a complete copy the data source you want to protect. To restore lost data, you simply replace it with the most-recent full-image backup. Full-image restores are fast, but because full-image backups can be time-consuming and can't be performed as frequently as other backups, this method isn't well suited to shorter RTOs/RPOs.

- **Incremental**

  Incremental backup starts with a full-image backup and then performs periodic backups of only the data that changed since the most-recent backup; typically, after a set number of incremental backups, another full-image backup is performed and the cycle starts again. To restore data, you first apply the most-recent full-image backup and then apply each subsequent incremental backup to the desired RPO. Incremental saves backup time by allowing fewer full backups and speeds restore times for recently-changed files.

- **Differential**

  Differential backup backs up all data that has changed since the last full-image backup. To restore data, you first apply the most-recent full-image backup and then the most-recent differential backup. Backup time increases with each successive differential backup, but restoring requires applying just two backup files—the latest full image backup and the differential backup).

- **Continuous data protection (CDP)**

  Also called continuous backup or real-time back-up, CDP instantly saves a copy of every change to your data to a separate storage device and tracks each of those saves. CDP eliminates the interruption of discrete backups since backup happens constantly. And because CDP can restore data from the most recent change or from any specific point in time, it provides the most comprehensive and granular protection for your data.

- **Bare-metal backup**

  Bare-metal backup backs up an entire computer or server—applications, data, operating system, etc.—in a way that allows it to be restored to bare metal hardware (hardware without a previously installed operating system or preinstalled software).

- **Instant recovery**

  A backup and restore method for virtual machines (VMs), instant recovery maintains a continually-updated backup VM for the production VM. When it's time to restore, the system redirects to workload to the backup VM in real time so that users can continue working without interruption while IT staff restore the original VM. Instant recovery offers the advantages of zero RTO

and RPO but, in many cases, the performance of the backup VM is somewhat slower than that of the original VM.

- **Example scenarios**
  - **Full-image backup and Incremental backup**

    Here is an example to explain full-image backup and incremental backup, and how they might work as part of an organizational backup strategy:

    - On Monday, the team completes an initial full backup of all files on the designated hard drive.
    - On Wednesday, the team completes an incremental backup of only the files that have changed since Monday — the last backup that was completed.
    - On Friday, the team completes another incremental backup of just the files that have changed since Wednesday — the last backup that was completed. They repeat this again on Sunday.
    - On Monday, the process begins again with another full back up to the designated hard drive.

    By doing this, the team saves space in the drive. However, if they need to restore, it may cost them time. In the alternative, the team might adopt this plan:

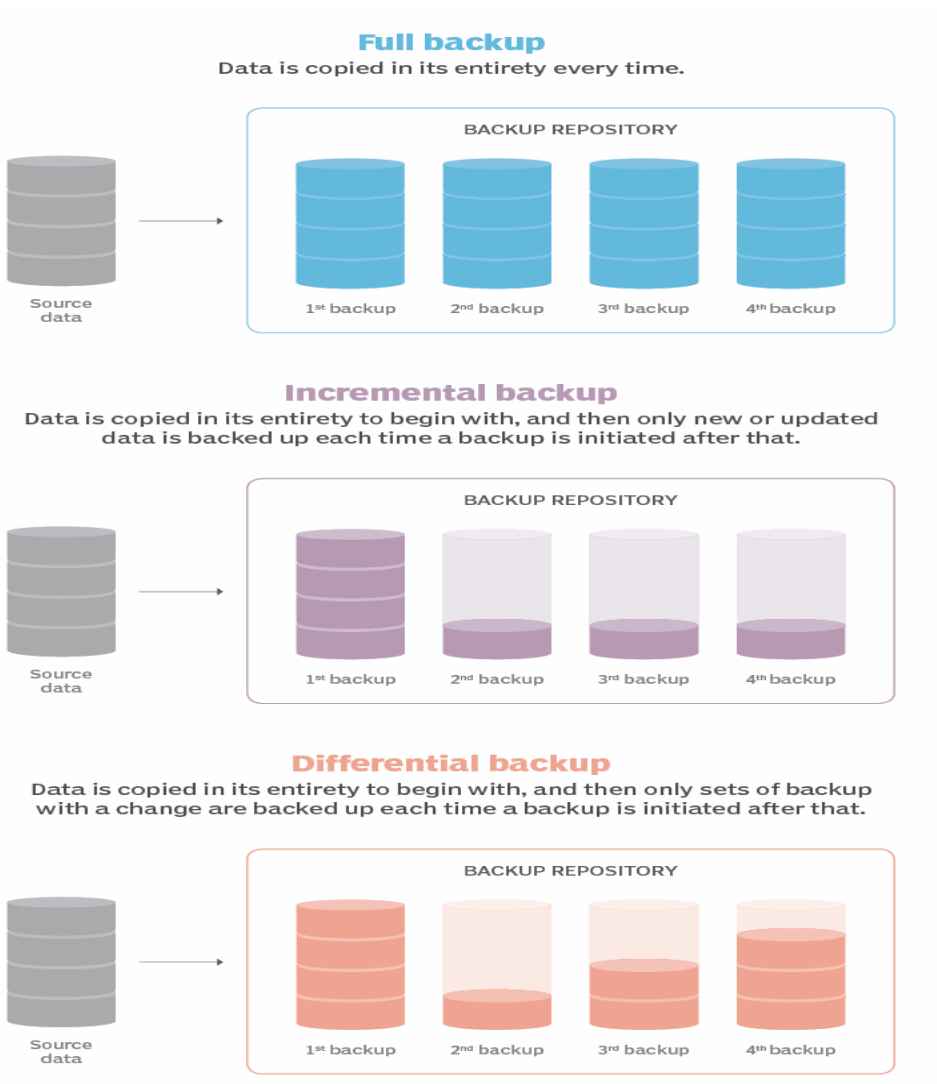
    - On Monday, the team completes an initial full backup of all files on the designated hard drive.
    - On Wednesday, the team completes differential backup of all files that have changed since Monday — the last full backup that was completed.
    - On Friday, the team completes another differential backup of all files that have changed since Monday — the last full backup that was completed. The backup from Wednesday is ignored because that is merely the latest differential backup. They repeat this again on Sunday, going back to the last full backup.
    - On Monday the process begins again with another full backup to the designated hard drive.

    This second strategy does require more space, but it is more of a compromise between the daily plan to run full backups and the reliance on incremental backups between spaced out full backups.

  - **Differential Backup**

    Suppose that you wanted to create a full-image backup on Monday and differential backups for the rest of the week. Tuesday's backup would contain all of the data that has changed since Monday. It would, therefore, be identical to an incremental backup at that point. On Wednesday, however, the

differential backup would back up any data that had changed since Monday as well.

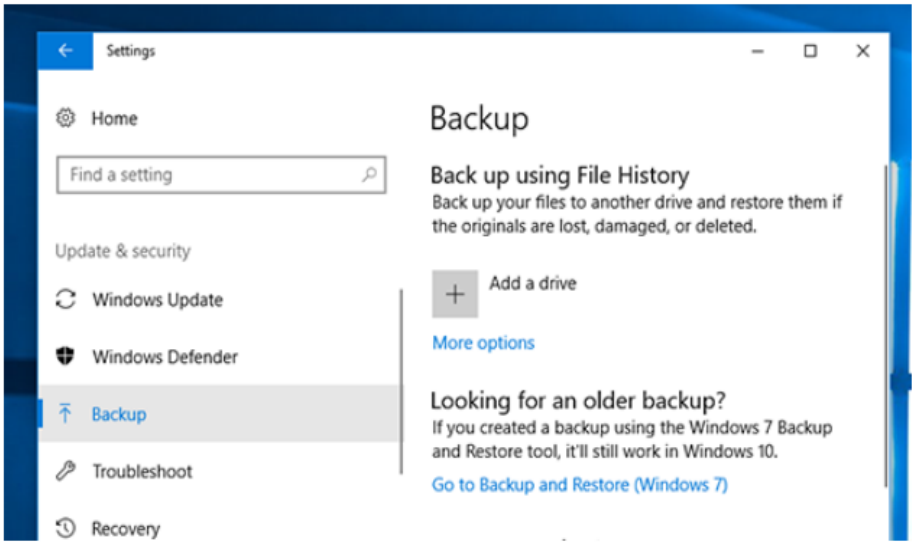


- **Special use cases**
  - **Windows 10 Backup and Restore**

    Windows 10 Backup and Restore makes periodic full image backups of your files on a schedule you specify. It can also create a backup image of your entire system—OS, applications, files, settings, etc.—so that you can recover everything if needed. An additional tool called File History can be set to automatically save multiple versions of a file so you can recover the file to a desired version or point in time.

Back up your PC with File History

Use File History to back up to an external drive or network location. Select **Start** > **Settings** > **Update & Security** > **Backup** > **Add a drive**, and then choose an external drive or network location for your backups.



Restore your files with File History

If you're missing an important file or folder that you've backed up, here's how to get it back:

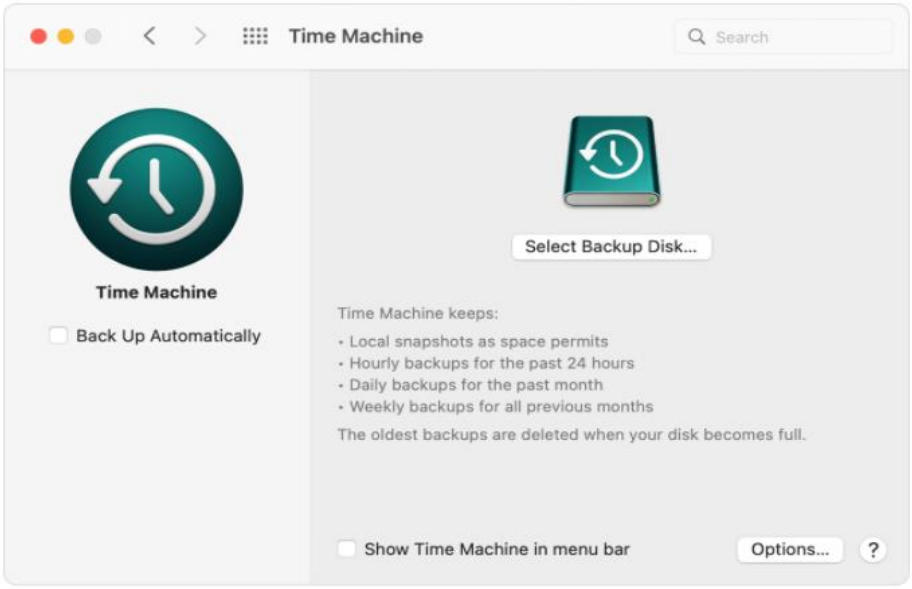
1. In the search box on the taskbar, type **restore files**, and then select **Restore your files with File History**.
2. Look for the file you need, then use the arrows to see all its versions.
3. When you find the version you want, select **Restore** to save it in its original location. To save it in a different place, right-click **Restore**, select **Restore to**, and then choose a new location.

- **Time Machine**

  Built into the Apple MacOS, Time Machine automatically performs hourly, daily, and weekly backups of your entire Mac system. It can save the backup to your Mac, an external drive, or to an AirPort Time Capsule (if you have one—Apple no longer makes them). When it's time to restore files, Time Machine lets you flip through dated backups to choose the recovery point you want. You can also back up files on your Mac—such as documents, photos, and songs—to iCloud.

Create a Time Machine backup

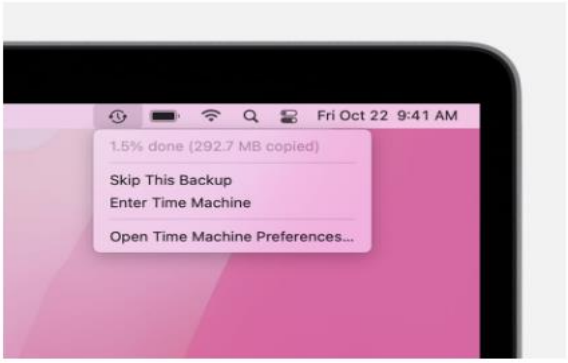
1. Connect an external storage device, such as a USB or Thunderbolt drive. Learn more about backup disks that you can use with Time Machine.
2. Open Time Machine preferences from the Time Machine menu in the menu bar. Or choose Apple menu > System Preferences, then click Time Machine.
3. Click Select Backup Disk.



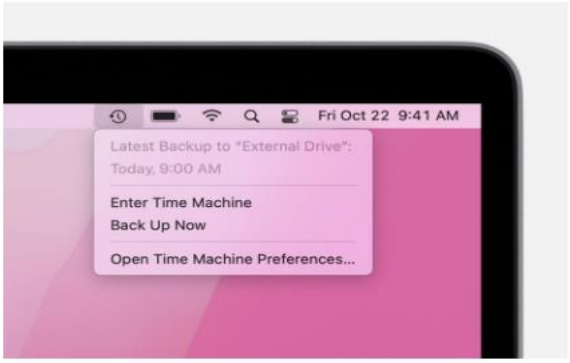
4. Select the name of your disk, then click Use Disk. Time Machine immediately begins making periodic backups—automatically and without further action by you.

If you want to start a backup manually, without waiting for the next automatic backup, choose Back Up Now from the Time Machine menu in the menu bar.

Use the same menu to check the status of a backup or skip a backup in progress. For example, if a backup is underway, the menu shows how much of it is done. When a backup is not underway, the menu shows the date and time of the latest backup.



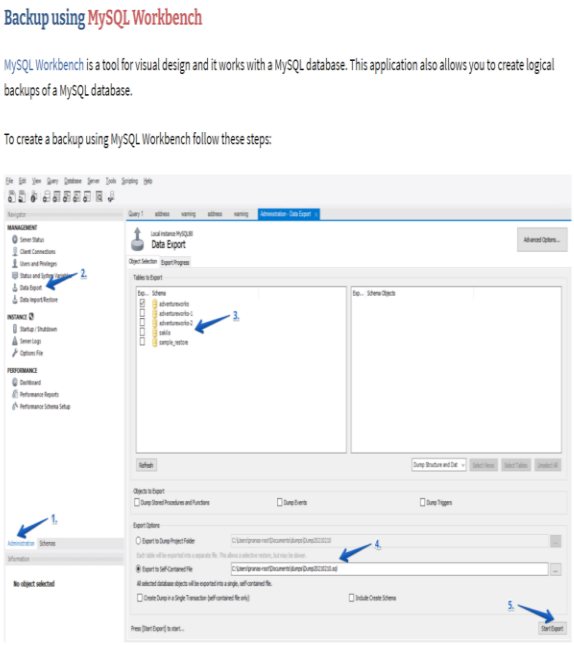
Backup is underway



Latest backup

- **SQL database backup and restore**

You can back up and restore MySQL, PostgreSQL, and SQL databases easily from the command line or with third-party tools available separately.



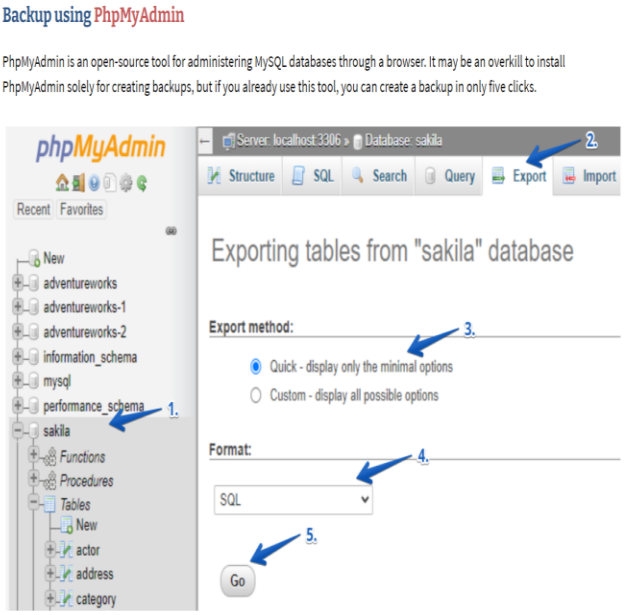
1. Go to the Administration tab, on the Navigation panel (on the left by default)
2. Select Data Export
3. From the Data Export tab in the Tables To Export section, select the databases and tables that will be added to the backup file
4. From the Export Option section, select the format for the exported data. Either each table will be exported to a separate .sql file, or one common .sql file will be created.

   Exporting each table to a separate file can be useful if you need to restore not the entire database, but some specific tables. But, as a rule, this is not necessary, and it is easier to work with one backup file.

5. Press the Export button to create a backup file.

The export section is essentially a graphic interface to the mysqldump utility. Although you cannot automate the creation process using MySQL Workbench, this tool is convenient for manually creating a backup and for migrating data.

Also, you can use MySQL Workbench as a parameter constructor for mysqldump. When you click the Export button, a log of the export execution will be displayed, in which there will be a mysqldump command with the parameters specified in the interface.



1. Select the database in the left panel
2. Go to the Export tab
3. To back up the entire server, select Quick. If you want to backup specific databases, then you must select Custom to see additional settings.
4. Select SQL format, which is the best for backup.
5. Click GO.

- **Backup Capabilities**

Following are some backup features that can help speed the recovery in specific cases:

- **Snapshots** – A snapshot is a copy of a dataset taken at a certain time. Snapshots, unlike backups, are usually saved on the same device as the original data. This makes them suitable for quick recovery, but they cannot be recovered from if the device fails.
- **Replication** – Data updates are replicated to a second site almost instantly. If the primary device fails, this enables for recovery with nearly no downtime. The second site, on the other hand, only has the most recent copy of the data, so it doesn't support recovery of data that's been corrupted or lost, or if you need an older version.
- **Deduplication** - Data are stored in several locations throughout an organization. By finding and removing duplicate data, deduplication minimizes the size of backups. The disadvantage however is that recovery times are made lengthier by the need to reverse this process.

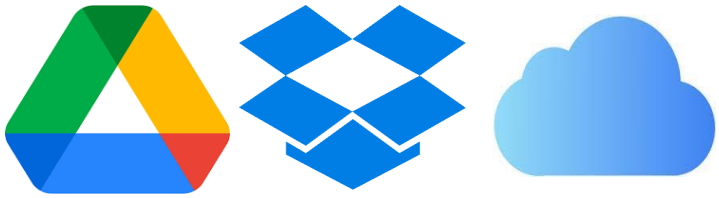
- **Backup Testing**

With a clear understanding of above areas, one can start to put together a test plan for how to make sure you are prepared for worst-case scenarios. The following are the list of tests to run with backup solution:

- Run a test of how long it takes to back up a given quantity of data
  - Run a restore of this same information and record the results.
- Run an application backup
  - Run a restore of this same application and record the results.
- Run a Virtual Machine (VM) backup
  - Make sure to test out your VM restore types.
- Run an offsite restore test
  - If your data is in a cloud or remote location, you should know how long it takes to recover from that location.

Lastly, making sure to establish a regular testing schedule, ideally once a quarter is important.

- **Users Backup**



While it is important to have a backup solution for infrastructure and critical systems, one should also think about users and their valuable files. Ensuring reliable backups for client devices is a bit more challenging than infrastructure devices. There likely to be lots of more client devices to backup compared to infrastructure ones. Plus, there are laptops, phones and tablets that won't be in the office all the time. One solution to user backups is to use a cloud service designed for syncing and backing up files across platforms and devices. Some examples of these are Dropbox, Apple iCloud and Google Drive, which are simple and straightforward to use. There are no complicated scheduling or configuration compared to infrastructure backups. They make it easy for users to configure what files or folders they want to have backed up and then ensure the files are synchronized with what's stored in the cloud.

Security Management

Information serving as one of the valuable assets of a company is important to be protected at all times from unwarranted modification, disclosure, or usage. Thus, preventive measures must be taken to ensure that the following won't be compromised:

- **Confidentiality** - Data confidentiality is concerned with preventing unwanted access to sensitive information such as nonpublic personal information (PII) or cardholder data (CD). Because confidential information can be used for identity theft and fraud, malicious actors frequently target it. Sensitive company information, such as trade secrets, can also be classified as confidential data.
- **Integrity** - Data integrity is concerned with the accuracy of data and the prevention of modifications to data submitted into a database or other resource. Data quality must be maintained by preventing malicious or unintentional changes to data that could affect data owners.
- **Availability** - To ensure that consumers can access information when they need it, data availability focuses on information accuracy, completeness, and consistency. Data storage, disaster recovery, and business continuity policies and processes must all be established.

The importance of keeping the privacy of a company's employees and clients should be taken as a serious matter. For the insurance of protecting the company and client data from security breaches, information security policies are made and fully enforced within the organization.

- **Cyber Security Threats**

A cyber security threat is any harmful attack that attempts to gain unauthorized access to data, disrupt digital activities, or damage data. Corporate spies, hacktivists, terrorist groups, hostile nation-states, criminal organizations, lone hackers, and disgruntled employees are all examples of cyber dangers. Cyber attackers can steal information or get access to a person's or company's financial accounts using sensitive data, among other potentially detrimental actions. Threats to cyber security include the following:

- **Malware**

  Spyware, ransomware, viruses, and worms are examples of malevolent software. When a user clicks on a malicious link or attachment, malware is activated, and harmful software is installed. Cisco reports that malware, once activated, can:

  - Block access to key network components (ransomware)
  - Install additional harmful software
  - Covertly obtain information by transmitting data from the hard drive (spyware)
  - Disrupt individual parts, making the system inoperable

- **Emotet**

  An advanced, modular banking Trojan that primarily serves as a downloader and dropper for other banking Trojans. Emotet is still one of the most expensive and devastating malwares.

- **Denial of Service**

  A denial of service (DoS) attack floods a computer or network, preventing it from responding to queries. A distributed DoS (DDoS) attack accomplishes the same goal, except it comes from a computer network. To disrupt the "handshake" procedure and carry out a DoS, cyber criminals frequently deploy a flood assault. Further methods may be utilized, and some cyber criminals take advantage of the period when a network is down to launch other attacks. According to Jeff Melnick of Netwrix, an information technology security software business, a botnet is a sort of DDoS in which millions of devices can be infected with malware and controlled by a hacker. Botnets, sometimes known as zombie systems, are designed to target and overpower a target's processing capabilities. Botnets are dispersed around the globe and difficult to track down.

- **Man in the Middle**

  When hackers inject themselves into a two-party transaction, this is known as a man-in-the-middle (MITM) assault. According to Cisco, after blocking transmission, they can filter and take data. When a visitor utilizes an unsecured public Wi-Fi network, MITM attacks are common. Attackers create a barrier between the visitor and the network, then use malware to install software and steal data.

- **Phishing**

  Phishing attacks use a forged communication, such as an email, to persuade the recipient to open it and follow the instructions therein, such as submitting a credit card number. “The goal is to steal sensitive data like credit card and login information or to install malware on the victim’s machine”, according to Cisco.

- **SQL Injection**

  A Structured Query Language (SQL) injection is a sort of cyberattack that occurs when malicious code is injected into a SQL server. When a server is infected, it releases data. It's as simple as typing the malicious code into a search field on a susceptible website.

- **Password Attacks**

  A cyber attacker can gain access to a variety of information with the appropriate password. Other sorts of password attacks include accessing a password database or straight guessing, which Data Insider defines as "a tactic cyber attackers utilize that relies largely on human contact and often entails persuading people into breaching common security procedures".

- **Methods to prevent cyber security attacks**

1. Back up your data

Backing up your business's data and website will help you recover any information you lose if you experience a cyber incident or have computer issues. It's essential that you back up your most important data and information regularly. Fortunately, backing up doesn't generally cost much and is easy to do.

It's a good idea to use multiple back-up methods to help ensure the safety of your important files. A good back up system typically includes:

- daily incremental back-ups to a portable device and/or cloud storage
- end-of-week server back-ups
- quarterly server back-ups
- yearly server back-ups

Regularly check and test that you can restore your data from your back up. Make it a habit to back up your data to an external drive or portable device like a USB stick. Store portable devices separately offsite, which will give your business a plan b if the office site is robbed or damaged. Do not leave the devices connected to the computer as they can be infected by a cyber-attack.

Alternatively, you can also back up your data through a cloud storage solution. An ideal solution will use encryption when transferring and storing your data, and provide multi-factor authentication for access.

2. Secure your devices and network

- **Make sure you update your software**

  Ensure you program your operating system and security software to update automatically. Updates may contain important security upgrades for recent viruses and attacks. Most updates allow you to schedule these updates after business hours, or another more convenient time. Updates fix serious security flaws, so it is important to never ignore update prompts.

- **Install security software**

  Install security software on your business computers and devices to help prevent infection. Make sure the software includes anti-virus, anti-

spyware and anti-spam filters. Malware or viruses can infect your computers, laptops and mobile devices.

- **Set up a firewall**

  A firewall is a piece of software or hardware that sits between your computer and the internet. It acts as the gatekeeper for all incoming and outgoing traffic. Setting up a firewall will protect your business's internal networks, but do need to be regularly patched in order to do their job. Remember to install the firewall on all your portable business devices.

- **Turn on your spam filters**

  Use spam filters to reduce the amount of spam and phishing emails that your business receives. Spam and phishing emails can be used to infect your computer with viruses or malware or steal your confidential information. If you receive spam or phishing emails, the best thing to do is delete them. Applying a spam filter will help reduce the chance of you or your employees opening a spam or dishonest email by accident.

3. **Encrypt important information**

   Make sure you turn on your network encryption and encrypt data when stored or sent online. Encryption converts your data into a secret code before you send it over the internet. This reduces the risk of theft, destruction or tampering. You can turn on network encryption through your router settings or by installing a virtual private network (VPN) solution on your device when using a public network.

4. **Ensure you use multi-factor authentication**

   Multi-factor authentication (MFA) is a verification security process that requires you to provide two or more proofs of your identity before you can access your account. For example, a system will require a password and a code sent to your mobile device before access is granted. Multi-factor authentication adds an additional layer of security to make it harder for attackers to gain access to your device or online accounts.

5. **Manage Passphrases**

Use passphrases instead of passwords to protect access to your devices and networks that hold important business information. Passphrases are passwords that is a phrase, or a collection of different words. They are simple for humans to remember but difficult for machines to crack.

A secure passphrase should be:

- long - aim for passphrases that are at least 14 characters long, or four or more random words put together
- complex - include capital letters, lowercase letters, numbers and special characters in your passphrase

- unpredictable - while a sentence can make a good passphrase, having a group of unrelated words will make a stronger passphrase
- unique - don't reuse the same passphrase for all of your accounts
  If you use the same passphrase for everything and someone gets hold of it, all your accounts could be at risk. Consider using a password manager that securely stores and creates passphrases for you.

➢ **Administrative privileges**

To avoid a cybercriminal gaining access to your computer or network:

- change all default passwords to new passphrases that can't be easily guessed
- restrict use of accounts with administrative privileges
- restrict access to accounts with administrative privileges
- look at disabling administrative access entirely

  Administrative privileges allow someone to undertake higher or more sensitive tasks than normal, such as installing programs or creating other accounts. These will be very different from standard privileges or guest user privileges. Criminals will often seek these privileges to give them greater access and control of your business.

  To reduce this risk, create a standard user account with a strong passphrase you can use on a daily basis. Only use accounts with administrative privileges, when necessary, limit those who have access, and never read emails or use the internet when using an account with administrative privileges.

6. Monitor use of computer equipment and systems

Keep a record of all the computer equipment and software that your business uses. Make sure they are secure to prevent forbidden access.

Remind your employees to be careful about:

- where and how they keep their devices
- the networks they connect their devices to, such as public Wi-Fi
- using USB sticks or portable hard drives - unknown viruses and other threats could be accidentally transferred on them from home to your business.

Remove any software or equipment that you no longer need, making sure that there isn't any sensitive information on them when thrown out. If older and unused software or equipment remain part of your business network, it is unlikely they will be updated and may be a backdoor targeted by criminals to attack your business.

Unauthorized access to systems by past employees is a common security issue for businesses. Immediately remove access from people who don't work for you anymore or if they change roles and no longer require access.

7. Implementing information Security Policies

A cyber security policy helps your staff to understand their responsibilities and what is acceptable when they use or share:

- data
- computers and devices
- emails
- internet sites

8. Protect your customers

It's vital that you keep your customers information safe. If you lose or compromise their information it will damage your business reputation, and you could face legal consequences.

Make sure your business:

- invests in and provides a secure online environment for transactions
- secures any personal customer information that it stores

If you take payments online, find out what your payment gateway provider can do to prevent online payment fraud.

- **Implementing Information Security Policies**

In order to instigate the importance of information security within an organization, policies must be implemented. The following are some of the policies to ensure information security:

- **Security Policies**
  To be able to identify and prevent information from being compromised and from abusing business-related data, application, computer systems and networks.

- **Acceptable Use Policies**
  This ensure there are proper and complete guidelines for instructing users on acceptable and unacceptable computing usage.

- **Copyright and Licensing Policies**
  - Implement procedures to ensure software license and copyright compliance.

- Ensure users do not copy software unless permitted by the licensing agreement.
- Conduct annual audit on installed software to determine compliance

- **Factors need to be considered when writing an Information Security Policy**
  - How to control access to information
  - How to prevent “snooping”
  - How to prevent a data breach
  - How to prevent data leakage
  - How to mitigate human error risk
  - How to prevent malicious actors from gaining access and changing information
  - How to establish change control processes
  - How to prevent unintended transfer errors
  - How to ensure no misconfigurations or security errors impact information
  - How to harden hardware to prevent a compromise
  - How to audit processes and procedures to ensure traceability
  - How to prevent natural disasters, human error, or storage erosion from impacting physical integrity
  - How to prevent human error or malicious attacks that impact logical integrity
  - How to maintain the data pieces’ unique values to protect entity integrity
  - How to establish processes that keep data stored and used uniformly to protect referential integrity
  - How to measure format, type, and amount of data entered into a database to protect domain integrity
  - How to create rules that address user needs to maintain user-defined integrity

- **Endpoint Security**

In addition to information security policies, an endpoint security software specifically built for enterprise clients is also required to safeguard all of their endpoints such as servers, laptops, mobile phones, and IoT devices. Endpoint security detects cyberthreats and secures weak endpoints on a company network, preventing harmful behavior.

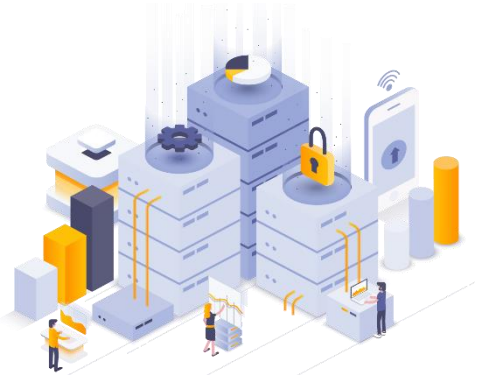
Endpoint security provides a more complete level of protection that spans throughout the entire network. This covers all network-connected devices (endpoints), which can all be utilized as security entry points.

Endpoint security uses a combination of firewalls, antivirus, anti-malware, and Host Intrusion Prevention systems to halt these threats and safeguard your network.

The difference between endpoint security and antivirus software is the scope of protection offered. With antivirus software, the only point of protection is the individual user's device that has antivirus installed.

Disaster Recovery

Disaster recovery is an organization's method of regaining access and functionality to its IT infrastructure after events like a natural disaster, cyber-attack, or even business disruptions related to the COVID-19 pandemic. A variety of disaster recovery (DR) methods can be part of a disaster recovery plan. DR is one aspect of business continuity.



- **Types of Disaster Recovery**

Businesses can choose from a variety of disaster recovery methods, or combine several:

- **Back-up:** This is the simplest type of disaster recovery and entails storing data off site or on a removable drive. However, just backing up data provides only minimal business continuity help, as the IT infrastructure itself is not backed up.
- **Cold Site:** In this type of disaster recovery, an organization sets up a basic infrastructure in a second, rarely used facility that provides a place for employees to work after a natural disaster or fire. It can help with business continuity because business operations can continue, but it does not provide a way to protect or recover important data, so a cold site must be combined with other methods of disaster recovery.
- **Hot Site:** A hot site maintains up-to-date copies of data at all times. Hot sites are time-consuming to set up and more expensive than cold sites, but they dramatically reduce down time.
- **Disaster Recovery as a Service (DRaaS):** In the event of a disaster or ransomware attack, a DRaaS provider moves an organization's computer processing to its own cloud infrastructure, allowing a business to continue operations seamlessly from the vendor's location, even if an organization's servers are down. DRaaS plans are available through either subscription or pay-per-use models. There are pros and cons to choosing a local DRaaS provider: latency will be lower after transferring to DRaaS servers that are closer to an organization's location, but in the event of a widespread natural disaster, a DRaaS that is nearby may be affected by the same disaster.
- **Back Up as a Service:** Similar to backing up data at a remote location, with Back Up as a Service, a third-party provider backs up an organization's data, but not its IT infrastructure.
- **Datacenter disaster recovery:** The physical elements of a data center can protect data and contribute to faster disaster recovery in certain types of disasters. For instance, fire suppression tools will help data and computer

equipment survive a fire. A backup power source will help businesses sail through power outages without grinding operations to a halt. Of course, none of these physical disaster recovery tools will help in the event of a cyber attack.

- **Virtualization:** Organizations can back up certain operations and data or even a working replica of an organization's entire computing environment on off-site virtual machines that are unaffected by physical disasters. Using virtualization as part of a disaster recovery plan also allows businesses to automate some disaster recovery processes, bringing everything back online faster. For virtualization to be an effective disaster recovery tool, frequent transfer of data and workloads is essential, as is good communication within the IT team about how many virtual machines are operating within an organization.
- **Point-in-time copies:** Point-in-time copies, also known as point-in-time snapshots, make a copy of the entire database at a given time. Data can be restored from this back-up, but only if the copy is stored off site or on a virtual machine that is unaffected by the disaster.
- **Instant recovery:** Instant recovery is similar to point-in-time copies, except that instead of copying a database, instant recovery takes a snapshot of an entire virtual machine.

- **Disaster Recovery Plan**

Organizations of all sizes generate and manage massive amounts of data, much of it mission critical. The impact of corruption or data loss from human error, hardware failure, malware, or hacking can be substantial. Therefore, it is essential to create a disaster recovery plan for the restoration of business data from a data backup image. It is important to have these 5 elements in making a disaster recovery plan:

1. **Disaster recovery team:** This assigned group of specialists will be responsible for creating, implementing and managing the disaster recovery plan. This plan should define each team member's role and responsibilities. In the event of a disaster, the recovery team should know how to communicate with each other, employees, vendors, and customers.
2. **Risk evaluation:** Assess potential hazards that put your organization at risk. Depending on the type of event, strategize what measures and resources will be needed to resume business.
3. **Business-critical asset identification:** A good disaster recovery plan includes documentation of which systems, applications, data, and other resources are most critical for business continuity, as well as the necessary steps to recover data.
4. **Backups:** Determine what needs backup (or to be relocated), who should perform backups, and how backups will be implemented. Include a recovery point objective (RPO) that states the frequency of backups and a recovery time objective (RTO) that defines the maximum amount of downtime allowable after a disaster. These metrics create limits to guide the choice of IT strategy, processes and procedures that make up an organization's disaster recovery

plan. The amount of downtime an organization can handle and how frequently the organization backs up its data will inform the disaster recovery strategy.

5. **Testing and optimization:** The recovery team should continually test and update its strategy to address ever-evolving threats and business needs. By continually ensuring that a company is ready to face the worst-case scenarios in disaster situations, it can successfully navigate such challenges.

- **Benefits of a Disaster Recovery Plan**

Obviously, a disaster recovery plan details scenarios for reducing interruptions and resuming operations rapidly in the aftermath of a disaster. It is a central piece of the business continuity plan and should be designed to prevent data loss and enable sufficient IT recovery.

Beyond the clear benefit of improved business continuity under any circumstances, having a company disaster recovery plan can help an organization in several other important ways.

1. **Cost-efficiency** - Disaster recovery plans include various components that improve cost-efficiency. The most important elements include prevention, detection, and correction, as discussed above. Preventative measures reduce the risks from man-made disasters. Detection measures are designed to quickly identify problems when they do happen, and corrective measures restore lost data and enable a rapid resumption of operations.
2. **Increased productivity** - Designating specific roles and responsibilities along with accountability as a disaster recovery plan demands increases effectiveness and productivity in your team. It also ensures redundancies in personnel for key tasks, improving sick day productivity, and reducing the costs of turnover.
3. **Improved customer retention** - Customers do not easily forgive failures or downtime, especially if they result in loss of sensitive data. Disaster recovery planning helps organizations meet and maintain a higher quality of service in every situation. Reducing the risks your customers face from data loss and downtime ensures they receive better service from you during and after a disaster, shoring up their loyalty.
4. **Compliance** - Enterprise business users, financial markets, healthcare patients, and government entities, all rely on availability, uptime, and the disaster recovery plans of important organizations. These organizations in turn rely on their DRPs to stay compliant with industry regulations.
5. **Scalability** - Planning disaster recovery allows businesses to identify innovative solutions to reduce the costs of archive maintenance, backups, and recovery. Cloud-based data storage and related technologies enhance and simplify the process and add flexibility and scalability.

- **Developing a Disaster Recovery Plan**

There are several steps in the development of a disaster recovery plan. Although these may vary somewhat based on the organization, here are the basic disaster recovery plan steps:

Risk assessment

First, perform a risk assessment and business impact analysis (BIA) that addresses many potential disasters. Analyze each functional area of the organization to determine possible consequences from middle of the road scenarios to “worst-case” situations, such as total loss of the main building. Robust disaster recovery plans set goals by evaluating risks up front, as part of the larger business continuity plan, to allow critical business operations to continue for customers and users as IT addresses the event and its fallout.

Evaluate critical needs

Next, establish priorities for operations and processing by evaluating the critical needs of each department. Prepare written agreements for selected alternatives, and include details specifying all special security procedures, availability, cost, duration, guarantee of compatibility, hours of operation, what constitutes an emergency, non-mainframe resource requirements, system testing, termination conditions, a procedure notifying users of system changes, personnel requirements, specs on required processing hardware and other equipment, a service extension negotiation process, and other contractual issues.

Set disaster recovery plan objectives

Create a list of mission-critical operations to plan for business continuity, and then determine which data, applications, equipment, or user accesses are necessary to support those functions. Based on the cost of downtime, determine each function’s recovery time objective (RTO). This is the target amount of time in hours, minutes, or seconds an operation or application can be offline without an unacceptable business impact.

Determine the recovery point objective (RPO), or the point in time back to which you must recover the application. This is essentially the amount of data the organization can afford to lose. Assess any service level agreements (SLAs) that your organization has promised to users, executives, or other stakeholders.

Collect data and create the written document

Collect data for your plan using pre-formatted forms as needed. Data to collect in this stage may include:

- lists (critical contact information list, backup employee position listing, master vendor list, master call list, notification checklist)
- inventories (communications equipment, data center computer hardware, documentation, forms, insurance policies, microcomputer

hardware and software, office equipment, off-site storage location equipment, workgroup hardware, etc.)
- schedules for software and data files backup/retention
- procedures for system restore/recovery
- temporary disaster recovery locations
- other documentation, inventories, lists, and materials
- Organize and use the collected data in your written, documented plan.

Test and revise

Next, develop criteria and procedures for testing the plan. This is essential to ensure the organization has adopted compatible, feasible backup procedures and facilities, and to identify areas that should be modified. It also allows the team to be trained, and proves the value of the DRP and ability of the organization to withstand disasters.

Finally, test the plan based on the criteria and procedures. Conduct an initial dry run or structured walk-through test and correct any problems, ideally outside normal operational hours. Types of business disaster recovery plan tests include: disaster recovery plan checklist tests, full interruption tests, parallel tests, and simulation tests.

Assessment

Read each question carefully, and then circle the answer that best fits the question.

1. Backup of the source data can be created

   a. On the same device
   b. On a different PC
   c. At some other location
   d. All of the mentioned

2. Which of the following backup technique is most space efficient?

   a. Full-image backup
   b. Incremental backup
   c. Differential backup
   d. Options b and c

3. Which of the following qualifies as best DR (Disaster Recovery) site?

   a. Same campus
   b. Same city
   c. Same country
   d. Different country

4. It is a series of bytes that is organized into blocks.

a. APK File
b. Text File
c. Object File
d. Source File

5. Which of the following is false?

a. The more important the data, the greater the need for backing it up
b. A backup is as useful as its associated restore strategy
c. Storing the backup copy near to its original site is best strategy
d. Automated backup and scheduling is preferred over manual operations

6. Which of the following is not a vulnerability to information security?

a. Flood
b. Without deleting data, disposal of storage media
c. Unchanged default password
d. Latest patches and updates not done

7. An advanced, modular banking Trojan that primarily serves as a downloader.

a. DOS
b. MITM
c. Emotet
d. SQL Injection

8. During a disaster, data security should be:

a. Put on the backburner while the recovery is handled
b. Attended to on an as-needed basis
c. Consistent with security during regular operations
d. All of the above

9. Having an outside DR adviser can be beneficial to recovery planning.

a. True
b. False

10. Based on the cost of downtime, determine each function’s RTO.

a. Evaluation of Critical Requirements
b. Risk Assessment
c. Disaster Recovery Plan Objectives
d. Final Documentation

Resource Management and Automation Management

Automatic Job Scheduling

Introduction

Alignment between IT and other lines of business has long been a challenge, but new solutions that provide visibility and intelligence into the volume and priority of projects managed by IT are enabling true collaboration. To make the most of limited resources, progressive companies are focusing on resource management within the IT department.

Objectives

At the end of this chapter, the students must be able to:

1. Compose a timeline for an IT project, given a budget and list of resources.
2. Compare and contrast the benefits of automation management.
3. Compare and contrast proactive administrative activities and reactive administrative activities.

Resource Management

Resource management is the practice of planning, scheduling, and allocating people, money, and technology to a project or program. The goal of resource management is to use the best combination of resources to satisfy requirements while also realizing these same resources are likely in demand elsewhere in the business. It is, in essence, the process of allocating resources to maximize organizational value. Good resource management results in the right resources being available at the right time for the right work.

Importance of Resource Management

Resource management is critical for organizations to ensure they are optimizing and allocating resources to the right initiatives. Companies and businesses could undertake all kinds of planning, but the ability to deliver projects on schedule and on budget would fall under speculation if resources are unavailable.

Good resource management is also a way to set realistic goals and map out when things can be done. A resource overview can assist businesses in making the most of their team's time, identifying resource shortages, and solve various conflicts. In fact, having resource management closely tied with projects, executives can tell which roles bring in the most revenue and profit to their companies.

Resource Management Techniques

While resources span multiple categories, people are the most complex to manage because there are so many elements that play into how they can best be optimized, including skill sets, availability, location and cost. Organizations use the following

resource management techniques to maximize resource efficiency, often relying on software to provide transparency to help leaders make smarter resource decisions.

- **Resource Allocation -** involves more than just assigning resources to projects. It considers the skills the team brings to the table along with their availability. Allocation reports will enable leaders to filter resources by skills and capacity to not only see who is available now but also when certain skills will be available in the future for better planning and fewer delays.
- **Resource Utilization -** enables leaders to gain visibility into the capacity of the team over a period of time and identify whether resources are being over or underutilized. Utilization reports reveal where resources are spending their time so leaders can see if there are opportunities to improve their effectiveness, productivity, and performance while keeping their workloads manageable.
- **Resource Leveling -** used to balance demand and supply. It is an important process to maximize resources across one or more projects based on their skills, getting the most value out of the resources you already have before you consider adding headcount or hiring a contractor. People often have different skill sets, many of which are underutilized. The goal of this resource management technique is to understand all of the team member's skills and where they may be of use to be able to fill gaps so you can minimize your resource spend.
- **Resource Forecast -** enables people to make predictions, identify potential conflicts, and prioritize resources on a timeline.

Resource Management Plan Stages

Resource management is the process of determining which resources are needed, in what quantities, and when, to complete a project. This method not only aids in determining how projects will be executed, but it also aids in estimating project costs and timelines.

1. **Determine the Resources Needed for the Project.** The first stage in resource management is determining which resources are required to fulfill the project. This information can come from project and resource knowledge, such as understanding the project's goals and tasks and comparing them to resource skillsets, or from prior successful lookalike projects as a guide. Using a template from previous successful projects not only helps to eliminate upfront project management labor, but it also helps to better forecast future success.
2. **Match the Right Resources to the Right Tasks.** Effective resource management entails matching your project's requirements with the resource best suited to meet them. Make sure the tasks you set align with the skillsets of the resource and that the resource has the available time to complete the project.
3. **Budget the Right Amount of Time for Each Resource**. It takes a special skill to schedule just the right amount of time for certain tasks to be completed. The most efficient utilization of resources is critical to the company's prosperity. Project managers must, however, avoid overscheduling their resources; otherwise, deadlines will be missed, and job quality will suffer.

4. **Schedule Resources Based on Projected Availability.** To effectively plan resources, the project manager should take into account not only what has to be done on the present project, but also any ongoing or recurrent projects that the resource's time is already committed to complete. Making the best scheduling decisions for your project can be aided with a resource management application that displays current hour availability, tentative allotment, and booked hours.
5. **Expect to Make Adjustments.** It's necessary to accept that not everything will go as planned when dealing with the human element of resource management. Recognize that you may need to make changes as a result of slow approvals, scope changes, or other unforeseen obstacles. Based on resource availability and workload, resource management software can assist in making smart modifications.
6. **Perform Post-Project Analysis.** Compare your estimated resources and scheduling to the actual resources used after you've finished. Were any of your predictions off the mark? Is there anything you need to modify about the way you distribute resources in the future? Aside from reviewing the reports, it's also a good idea to check in with your resources to see whether they thought the project went well and if they have any suggestions on how to improve the process in the future.

Need for Automated Resource Management

Historically, most IT departments have functioned on a “first-in, first-out” system, in which requests for support and development are responded to based on the order in which they were received. Additionally, when new tasks come in specified as high or critical priority, employees are expected to drop existing projects to focus on the high-priority task, then return to their previous assignments. As a result, the other work gets behind schedule, often without any visibility to the overall owner.

This style of system process is inefficient for several reasons, it causes the IT departments to be overwhelmed, resource capacity is being overestimated, goals of the business are not being addressed, and finally, task-switching leads to lost productivity.

Automation Management

Automation Management is the use of instructions to create a repeated process that replaces an IT professional's manual work in data centers and cloud deployments. Software tools, frameworks and appliances conduct the tasks with minimum administrator intervention. The scope of IT automation ranges from single actions to discrete sequences and, ultimately, to an autonomous IT deployment that takes actions based on user behavior and other event triggers.

Automation Management is different from orchestration, but commonly, the terms are used together. Automation accomplishes a task repeatedly without human intervention. Orchestration is a broader concept wherein the user coordinates automated tasks into a cohesive process or workflow for IT and the business. For example, an IT administrator enables workload scaling with automated instance creation, operating system (OS) installs and storage provisioning. They orchestrate the automation tasks in a workflow

with a specific order of operations for each task. Orchestration can also include permissions and roles enforcement, approval gates and more.

Benefits of Automation

When we look at big infrastructures that help automate a difficult process or workflow, such as the deployment of a new host, it is clear that having designed such a system has reaped considerable benefits. Even while we may begin the process of automating a certain operation with the only purpose of saving ourselves some typing, we discover the same advantages on a much smaller scale. The following are the key advantages we gain from deploying an automated management.

Repeatability

Repeatability is an indicator that the results can be trusted and that the test is being performed properly every time. Without repeatable results, retesting might be required, which can be very costly. Improper specimen identification, measurement, and alignment all play a part in creating non-repeatable results. Procedural errors, where different operators do not perform tests the same way throughout the day and from shift-to-shift, are also a source of inaccurate test data. A well-trained operator is crucial to ensuring the integrity and accuracy of results, and when operators change jobs or turnover becomes an issue, significant resources need to be expended on training new operators while production time is lost. A fully-automated system, on the other hand, requires minimal training and provides reliable and accurate results.

Reliability

Reliability is defined as the ability of a system to perform and maintain its functions in routine circumstances. Improving reliability means ensuring systems are more available for continuous operation than they typically are. Outage or failure of systems can lead to a non-availability, resulting in lost productivity and sales.

Related to overall reliability is the ability to have quick return-to-service when a hardware or software component fails. Some level of system failure is inevitable and being able to maintain a very low mean time to recovery (MTTR) is an equally important benchmark to overall uptime.

The complexity of the technology required to support today's retail and hospitality environments increase the difficulty of maintaining an acceptable reliability level. It's often necessary to deploy a range of systems and networks consisting of a mixture of legacy and modern application hosting both in-store and in the cloud. A rapidly evolving set of business requirements is driving the deployment of systems to support increased customer engagement, rich-media, new payment types, and better security, all the while creating complex configurations. And, these applications need to work across a large number of geographically dispersed

locations across multiple time zones. Keeping everything working properly with uptime in the 99.9 percentile and extremely quick MTTR is extremely difficult.

Flexibility

The general definition of flexibility is: being responsive to change, adaptable. In fact, being flexible in terms of automated manufacturing is basically being able to adapt your process to different options. The best way to describe flexibility would be to describe the total opposite of it, rigidity. Having a rigid manufacturing process consists of having a single product that can be produced in a given operation. If the process needs to be modified, it cannot be quickly adapted. Most of the time, rigid processes need a complete changeover when another kind of product must be produced.

Automation Pitfalls

Worker Displacement

A main disadvantage often associated with automation, worker displacement, has been discussed above. Despite the social benefits that might result from retraining displaced workers for other jobs, in almost all cases the worker whose job has been taken over by a machine undergoes a period of emotional stress. In addition to displacement from work, the worker may be displaced geographically. In order to find other work, an individual may have to relocate, which is another source of stress.

Human Dependence

There are potential risks that automation technology will ultimately subjugate rather than serve humankind. The risks include the possibility that workers will become slaves to automated machines, that the privacy of humans will be invaded by vast computer data networks, that human error in the management of technology will somehow endanger civilization, and that society will become dependent on automation for its economic well-being.

Increased Complexity and Impact

Automation often introduces or increases complexity. Unless carefully implemented and meticulously documented, an automated system can become a black box to your peers. Fewer people will understand how the task is actually accomplished or where to look when things inevitably break. “Complex systems fail in complex ways.”

Automation also vastly increases the impact of any failure you may en- counter, as it allows us to perform tasks across the entire infrastructure. While a manually executed command may well be mistyped, it will often have a limited impact. After all, this is often precisely *why* we wanted to automate the given task! But now

consider the failure scenario: accidentally removing a user account from a single machine, for example, is easy to fix and may not impact that system's operations; accidentally removing all user group associations from all of your infrastructure's hosts, on the other hand, may cause widespread system failure and be much harder to revert.

Loss of Audit Trail

Any but the simplest of infrastructures requires operations on a num- ber of different resources: information about host groups are stored in and accessed from one database, subsets of hosts are accessed in order to manipulate resources in another segregated access zone, and so on. For human interactions, all of these actions are (hopefully) explicitly authenticated and logged, allowing us to track who initiated what changes where and when. When we add automation into the mix, we frequently have to create a so- called "service account", an account that is not associated with a person, but that exists to allow automated tools to perform certain actions. Many automated solutions will use this account to access systems or internal resources, and even though considered an "unprivileged" account, it probably has sufficient access permissions to cause significant damage. What's more, it's unlikely that actions by this user can (easily) be tracked back to a human, an important auditability requirement.

In this case, the ability to orchestrate complex changes across large sets of hosts may lead to a loss of the audit trail. Granted, it is possible to retain the ability to track commands and actions, but even when that is not flat out neglected, with every added level of automation this becomes more and more cumbersome. Identifying who specifically initiated a chain of events, and ascertaining whether the correct access was applied becomes increasingly difficult.

Loss of Accountability

Even if we may not be able to track every single command executed by any automated system, we need to be able to identify on a higher-level what changes were *initiated* by whom. In today's massive infrastructures, automated systems make decisions about which servers to shut down, which ones to direct production traffic to, or which IP addresses or networks to automatically block. These decisions are made automatically, based on traffic patterns, system monitoring, and a number of other factors.

While we need to allow for this level of automation in order to meet the rapidly rising demands on our infrastructure, we *also* have a conflicting requirement of accountability. Every action performed on our systems need not be tied directly to a human, but the decision engine that automatically applies the given heuristics needs to regularly be reviewed and allow for an audit trail.

Remember: due to the ease with which our automated tools allow us to administer large numbers of machines, the size and impact of any outages will be significantly increased as well! Untangling the web of decisions made that led to a system wide outage becomes harder and harder due to the increased complexity of both the

run-time systems as well as the failure modes. In the end, we need to be able to identify exactly *why* the system failed in the way that it did. What was the *root cause*?
Similarly, from a security perspective, it is imperative to be able to tell who initiated a certain action – not in order to "blame" that person for causing an outage, but to be able to identify a possibly compromised account or e.g., overly broad access permissions. Government issued guidelines or regulations may require your organization by law to be able to provide a full audit trail of certain actions. With the help of automation, we can actually improve our auditability and accountability, but these factors do need to be considered and integrated into the tool or product right from the beginning.

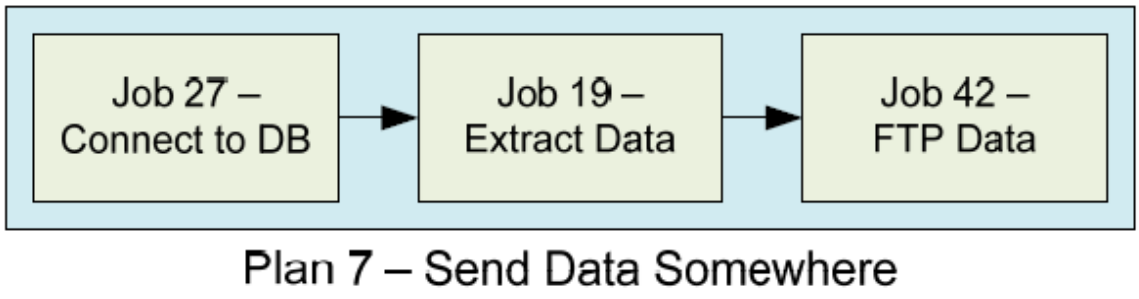
Safeguards

The complexity we inherit as a by-product of all the benefits of automation should not be underestimated. With every additional automated step, we broaden the possible impact of our tool. Not only can more things go wrong, but failure may propagate or escalate at scale. As a result, the need for safeguards together with the discovery of and alerting on error conditions increases at the same rate.
Simple tools rarely require human interaction, but may at times allow for confirmation from the user before taking a particular action; as an example, consider the -i flag to the cp(1), mv(1), and rm(1) utilities. As we combine such tools (or write our own) to provide more automation, such safeguards are often seen as a hindrance, and we avoid them where possible. After all, the whole point of automating a task is to avoid human interactions. But as we do so, we also increase the risk of more widespread damage when (not *if*!) things do go awry. Smart tools make use of well-defined thresholds when applying large changes: a tool may allow you to update or delete records in your inventory database without interaction (assuming proper authentication), but may ask for additional confirmation or even higher privileges when performing the same action on *all* records.

Automatic Job Scheduling

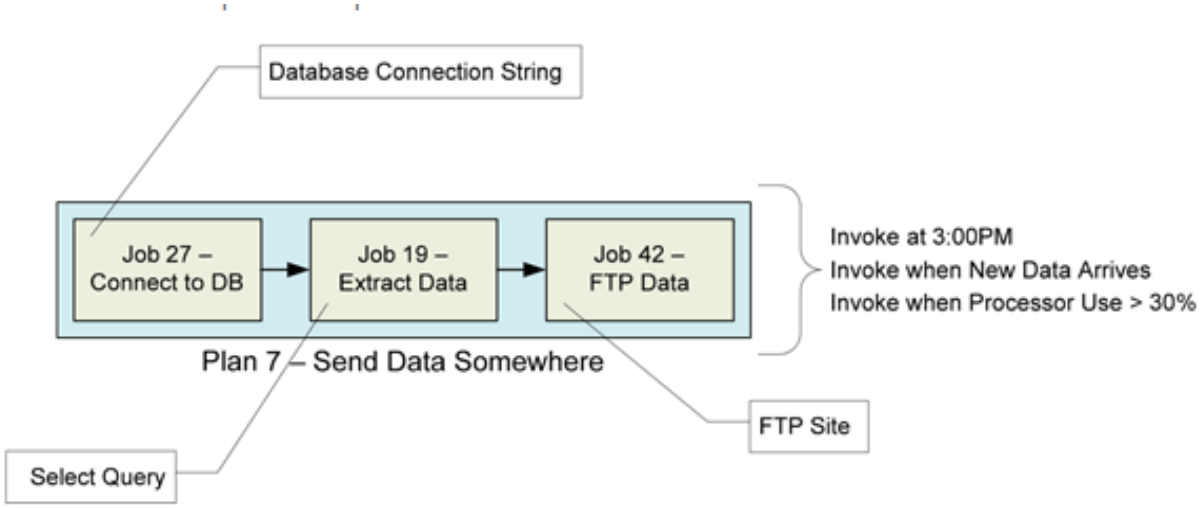
Before defining Job Scheduling, let us define first the meaning of the job. *Job* represents some sort of automation that occurs within an IT system. It is an action to be executed. It can be a running batch file, script file, shell command, or executing database job or transformation. Essentially, anything that enacts a change on a system is wrapped into this object we'll call a job.

Now if each job accomplishes one thing, this means that I can string together multiple jobs to fully complete some kind of action. We'll call that string an IT plan. A plan represents *a series of related jobs that can be executed* with the intended goal of carrying out some change.



In this figure, you can see how three different jobs are connected to create the plan. Job 27 connects to an Oracle database. It passes its result to Job 19, which then extracts a set of data from that database. Once extracted, the data needs to be sent somewhere. Job 42 completes that task, as it FTPs the data to a location somewhere.

The next thing we will talk about is the *schedule*. A schedule is applied to the job to tell it when to run.



Let's assume that in the previous figure, "Plan 7" relates to some data transfer that needs to happen inside The Project. In this case, let's assume that the data transfer occurs between its SQL Server and UNIX mainframe. The figure above shows a graphical representation of how this might be applied. There, you can see how three different schedules could potentially be attached to the newly-created plan:

- Invoke the plan at 3:00 PM
- Invoke the plan when a set quantity of new data arrives
- Invoke the plan when processor utilization is less than 30%

Any of these three schedules can be appropriate, depending on the needs of the system and its components. For example, the first schedule might be appropriate if a daily data dump is all that's necessary. In that case, a date/time-centric schedule might be all that's necessary to complete the action.

The second and third tasks highlight some of the more powerful scheduling options that could also drive the invocation of the plan. In the first, the plan is executed not based on any time of day. Rather, it executes when a set quantity of new data has been added to the database. This could be a smart solution if you want these two databases to stay roughly in sync with each other. It is really powerful when you consider how difficult that kind of schedule would be to create if you were using just the native SQL or UNIX tools alone.

That third schedule is particularly interesting because it could be used alone or in combination with the second. That third schedule instructs the plan to run only if the server isn't terribly busy. Using it in combination with the second allows you to maintain a level of synchronization while still throttling the use of the server. A good job scheduling solution will include a wide range of conditions that you can apply to plans to direct when they should kick-off.

In conclusion, Job scheduling tools enable IT to automate the execution of tasks based on date-and-time scheduling or other methods of execution such as event-based triggers. Job scheduling tools eliminate the need for manual kick-offs, reducing delays and giving IT more time to spend on higher-value projects.

Organizations wishing to automate unrelated IT workload could also use more sophisticated attributes from a job scheduler, for example:

- Real-time scheduling in accordance with external, unforeseen events
- Automated restart and recovery in case of failures
- Notifying the operations personnel
- Generating reports of incidents
- Audit trails meant for regulation compliance purposes

In-house developers can write these advanced capabilities; however, these are usually offered by providers who are experts in systems-management software.

In scheduling, many different schemes are used to determine which specific job to run. Some parameters that may be considered are as follows:

- Job priority
- Availability of computing resource
- License key if the job is utilizing a licensed software
- Execution time assigned to the user
- Number of parallel jobs permitted for a user
- Projected execution time
- Elapsed execution time
- Presence of peripheral devices
- Number of cases of prescribed events

Proactive Administrative Activities vs Reactive Administrative Activities

Proactive is defined as creating or controlling a situation by causing something to happen rather than responding to it after it has happened. The opposite of proactive, reactive, is defined as acting in response to a situation rather than creating or controlling it. So, the difference between a proactive administrative and reactive administrative is:

- Proactive administration is ensuring your system is operating at full capacity that will help you avoid the need for repairs or gaps in protection down the road.
- Reactive administration is where the vast majority of your time is spent responding to incidents.

Many administrators argue that they have little time to be proactive because they spend so much time putting out fires, something that makes them reactive. Spending the majority of your time putting out fires certainly shows that you are performing a task that needs to be performed. At some point though someone might wonder if a more skilled administrator might be able to stop the fires occurring in the first place.

It is up to you if you want to be a proactive or reactive administrator, but if you want to be proactive rather than reactive, one of the solutions you are looking for is *automation*. Set up sequences of automated actions that would mirror the typical actions of an experienced operator or systems administrator.

For example, you might typically try something three times to address the problem and only then choose to be notified about it, if an automatic fix was unsuccessful. You can easily set this up using monitoring software to automate your appropriate sequences of actions to handle most routine issues and reduce the “noise” that you face on a daily basis.

You might also need a reliable method of automatically escalating a specific problem after a certain time period has elapsed or the issue has not been responded to within a certain time frame. For example, during the day you might escalate to the IT support team or automatically raise a ticket to the helpdesk team. Out-of-hours you might escalate to the on-call support person or a third party to resolve.

Course Materials:

Watch
The Keys to Effective Resource Management with Microsoft Project
https://www.youtube.com/watch?v=0J80BxwKNys

Workload Automation and Job Scheduling - The RunMyJobs Automation Journey
https://www.youtube.com/watch?v=cMj9bEfpRhQ

The Basics of Enterprise Job Scheduling
https://www.youtube.com/watch?v=-1g1uX37I3w

Activities / Assessments (Chapter Activity)

1. Explain what is resource management and why it is important?
2. Give a sample scenario where repeatability is demonstrated in an automated system.
3. Why do you believe some administrators choose to be a reactive administrator rather than proactive administrators?

System Management and Support

Introduction

Systems management refers to the centralized administration of the IT (Information Technology) in an organization. The concept covers a broad set of subsystems that are needed to monitor and manage IT systems correctly. Managing IT systems is essential for organizing and running your business. Good system management is the backbone of an IT-based organization. This chapter will tackle the basic fundamentals of System and User Support, as well as the basic principles of System Documentation Writing.

Objective:

- To learn how to manage and provide user and system support
- To know the fundamental principles of System Documentation Writing
- Prioritize a list of administrative activities for IT, to support an organization's mission statement
- List the priorities of System Support teams.

System Management

System management is the system offering system which functions to realize the management of system offering needs, requirements, products, solutions and abilities. The purpose of system management is to enable and assure the management and abilities of the system management capabilities of the enterprise are controlled, balanced and aligned to the mission and needs of the enterprise as a whole.

Elements of System Management

Systems Management consists of a wide range of IT functions or subsets aimed at maintaining or improving infrastructure, network, applications, services, OSs, among many others. Systems Management oversees many IT requirements such as, (but not limited to):

- **Application Monitoring** - The Application Performance Management (APM) is a subset of the Systems Management. It deals with the monitoring and management of the performance of applications. This subset helps detect complex problems, deals with life-cycles, and level of service.
- **Asset Inventory** - To keep a record of hardware or software assets. This subset helps in asset lifecycle management, keeps a record of hardware, including firmware, versions, OSs, and their licenses. For software asset inventorying, it keeps versioning, patching, and licenses in control.

- **Log Management** - and Performance Analytics This subset helps manage the overall performance of the systems through log analyzing. It helps you collect, correlate, and analyze the system's data to give you an insight into the performance.
- **Network Monitoring and Management** - This includes monitoring of network devices, such as routers, switches, wireless access points, and end points. Network monitoring helps managers identify failures quickly and improve performance accordingly.
- **System Administration Monitoring** - and management of servers, storage, databases, virtualization, cloud, printers, PCs, and mobiles. This subset gives you full administration over systems configuration and the disaster recovery and backups.
- **IT Security and Compliance** - Security information and event management. This task is in charge of running anti-virus and malware tools, intrusion detection, data loss, and prevention systems and helping with any regulatory compliance.
- **Automation** - This might include automated backups and restores, automated workloads, or desired configuration states. A network automation software can also give you insights into faults, performance, availability, bandwidth, and IP address management.
- **Help and Service Desk Management** - Some benefits of this service are the ability to create and track issue tickets from a single place and have an IT expert solve them. IT teams can track issues, changes, and faulty assets.

Challenges in System Management

A systems management can sometimes make management more complex and less productive. It requires a learning process and some investment to make it work.

- **Training -** Employees need the right training to use these tools effectively. Deploying and using centralized systems management require time and effort. This is related to the size of the business and the existing expertise of the IT staff.
- **Increase cost -** Implementing and maintaining an IT and systems management requires an increased cost. Some of the best tools on the market are not so cheap, and the free ones take time to install and learn.
- **Interoperability -** Many systems management software is able to integrate and operate with different hardware or software vendors. Unfortunately, all of them have different data interpretations, which makes the interoperability, challenging.

System Documentation

In system administration terms, documentation means keeping records of where things are, explaining how to do things, and making useful information available to the

system users. Documentation is a way of creating an institutional memory that lets a System Administration team increase its knowledge and skill level.

Documentation provides information to customers to enable them to be self-sufficient. Documentation for system administration processes improves consistency, reduces errors, makes it easier to improve those processes over time, and makes tasks easier to delegate.

Documents should be kept in a repository so they can be shared and maintained. Wikis are a very useful system for hosting repositories because they make it easy to create and update documents and do not require HTML knowledge. Plug-ins extend wikis to do more services.

Importance of System Documentation

1. **Helps improve processes.** Identify bottlenecks and inefficiencies by documenting the exact processes. You'll quickly see what processes that you need to improve or get rid of.

2. **Helps train employees**. You can use process documents to help new employees understand their job roles and familiarize themselves with the processes they'll be involved in. Even experienced employees can still refer to these documents whenever they want to make sure that they are executing the process right.

3. **Helps preserve company knowledge**. Keep a record of processes known only to a few people specialized in doing them. That way even when they leave, the newcomers can resume the work easily.

4. **Helps mitigate risks** and maintain operational consistency.

5. Detailed process documentation is also **a vital part of patents and trade secrets.**

Writing System Documentation

You wish to provide information for your organization, your users, or colleagues. As a reader of system documentation, you are in search of information. This exchange of knowledge is direct communication between the author of the documents and the reader.

Know Your Audience

We write documentation for ourselves. This is the simplest case, as we know our target audience well – or so we think! For the most part, we are writing things down so we can repeat them later on, so we don't forget, so we have a point of reference in the future. This means that we have a pretty good idea what the prospective reader might expect to find, what they might know about the infrastructure etc.

***We write documentation for other system administrators*.** This case is still fairly straight forward. We expect our target audience to be very technical and have a very good understanding of our systems. For example, we write down the steps of a procedure that our colleagues may not normally perform, or we document the setup of a system component we are in charge of that is crucial to the overall operations of our organizations so that they may use this document as a reference when we are not available.

We write documentation for other technical people. Our services are used by a number of people in our organization. Some of these are very technical expert users, software developers or other engineers, perhaps. In order to allow these people to get information about our systems quickly, we provide end-user documentation which allows more efficient use of the resources we make available.

We write documentation for our users. The systems we maintain provide a certain service and thus has users, some of whom may be internal to our organization and others which may be outside customers. It is not rare that the people in charge of maintaining the systems provide documentation to these end-users in one way or another to allow them to utilize the service or help them find help when things break down.

We write documentation for other people everywhere. System administrators rely on the Internet at large to find answers to the rather odd questions they come up with in the course of their normal work day. Frequently we encounter problems and, more importantly, find solutions to such problems that are of interest to other people, and so we strive to share our findings, our analyses, and our answers.

Different Document Types

Knowing your audience and understanding what you wish to communicate to them are the most important aspects to understand before starting to write documentation. From these two main points derive a number of subsequent decisions that ultimately influence not only the process flow but also the structure of the document. Drawing parallels to software engineering once more, where we decide on the programming language or library to use based on its suitability to actually solve the given problem, we find that here, too, we need to use the right tool for the job. We cannot structure our end-user manual as a checklist, nor can we provide online help or reference documentation as a formal paper.

Each document type calls for a specific writing style, a unique structure and flow of information. In this section, we will take a look at some of the most common distinct categories of system documentation.

Different Document Types	Purpose	Target Audience	Structure
Processes and Procedures	• describe in detail how to perform a specific task; document the steps to follow to achieve a specific goal; • illustrate site-specific steps of a common procedure	• all system administrators in the organization	• simple, consecutive steps • checklist; • bullet points with terse additional information
Policies	• establish standards surrounding the use of available re- sources	• all users of the given systems	• full text, including description and rationale
Online Help and Reference	• list and index available resources • illustrate common tasks; • describe common	• all users of the given systems; • possibly restricted set of privileged users (depending on the resources indexed	• simple catalog or itemization; • short question-and-answer layout; • simple sentences with example invocations

	problems and provide solutions		
Infrastructure Architecture and Design	• describe in great detail the design of the infrastructure; illustrate and document information flow; • document reality	• other system administrators in the organization	• descriptive sentences with detailed diagrams; • references to rationale and decision making process behind the designs.
Program Specification and Software Documentation	• describe a single software tool, its capabilities and limitations. • Illustrate common useage • Provide pointers to additional information.	• All users of the tool, inside and outside of the organization.	• short, simple, descriptive sentences; • example invocations including sample output; • possibly extended rationale and detailed description command or syntax reference etc. via in-depth guide

Collaboration

Unlike other kinds of writing, creating and maintaining system documentation is not a solitary task. Instead, you collaborate with your colleagues to produce the most accurate information possible and allowing end users to update at least some of the documents you provide has proven a good way to keep them engaged and improve the quality of your information repository. Depending on the type of document, you may wish to choose a different method of enabling collaboration.

- **Usability;** how easy is it for you and your colleagues to edit the documents, to keep them up to date?
- **Collaboration;** how easy is it for others to make corrections, to comment on the content, to suggest and provide improvements?
- **Revision Control;** how easy is it to review a document's history, see what has changed between edits, see who made what changes when?

- **Access Control;** how easy is it for you to grant or deny access to individuals, teams, the organization, the public?
- **Searchability;** how easy is it for you and your users to discover the documents?

Formats

Finally, a word on the format of your documentation. Be aware of how your users might read the documents you provide. Frequently, it is necessary to be able to search documents offline, to forward them via email, to link to them, or to copy and paste portions. With that in mind, be mindful of the format in which you generate and present your information.

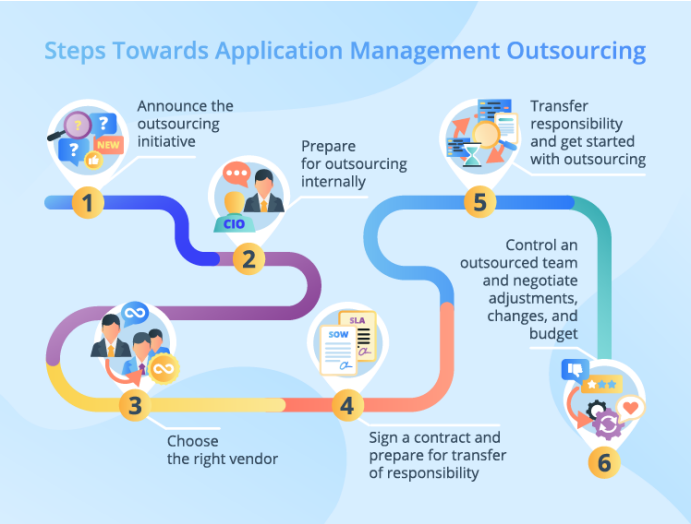
To increase the readability of your documents use a short line-length and the copious use of paragraphs. Viewing a single large block of run-away text with no line breaks immediately puts stress on the reader, as absorbing the information provided therein requires a high degree of concentration and eye movement.

- Breaking up your text into smaller paragraphs helps the reader relax and facilitates reading comprehension, speed, and ease.
- Write the text as you would read it out aloud, with paragraphs allowing the reader to catch their breath for a second.
- If you are writing a longer technical document, you can further structure it using headlines, numbered sections, subsections etc. using different ways to underline or emphasize the section titles.
- You can use itemization, bulleted or numbered lists, or indentation to make your text easy to read.
- Use short sentences, just like one single block of text is hard to read, so are never ending sentences with multiple conditionals and subclauses.
- Use proper punctuation. A period will almost always suffice; semicolons may be used as needed, but exclamation points are rarely called for!
- Resist the temptation to use images instead of text. If you are unable to distill the concepts or thoughts into language, then you have likely not fully understood the problem.
- Use illustrations as supplementary, not instead of information.
- Text ought to be your primary content: it can can easily be skimmed, indexed and searched, glanced through in a matter of seconds, and parts of a paragraph be re-read with ease;
- a screencast or video, to cite an extreme example, must be watched one excruciating minute at a time (not to mention the challenges non-textual media pose to visually impaired users).

System Management

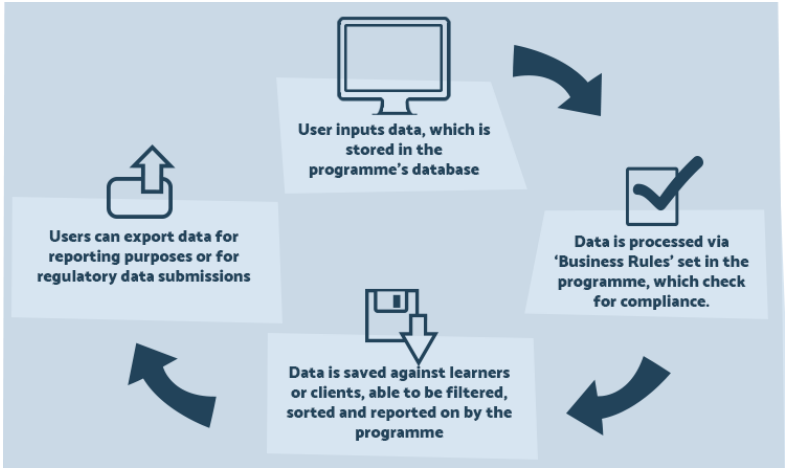
Application Management

Application Management (AM) is the lifecycle process for software applications, covering how an application operates, its maintenance, version control, and upgrades from cradle to grave. Application management services are an enterprise-wide endeavor providing governance designed to ensure applications run at peak performance and as efficiently as possible, from the end-user experience to integration with enterprise back office functions such as database, ERP, and SaaS cloud functions such as CRM.



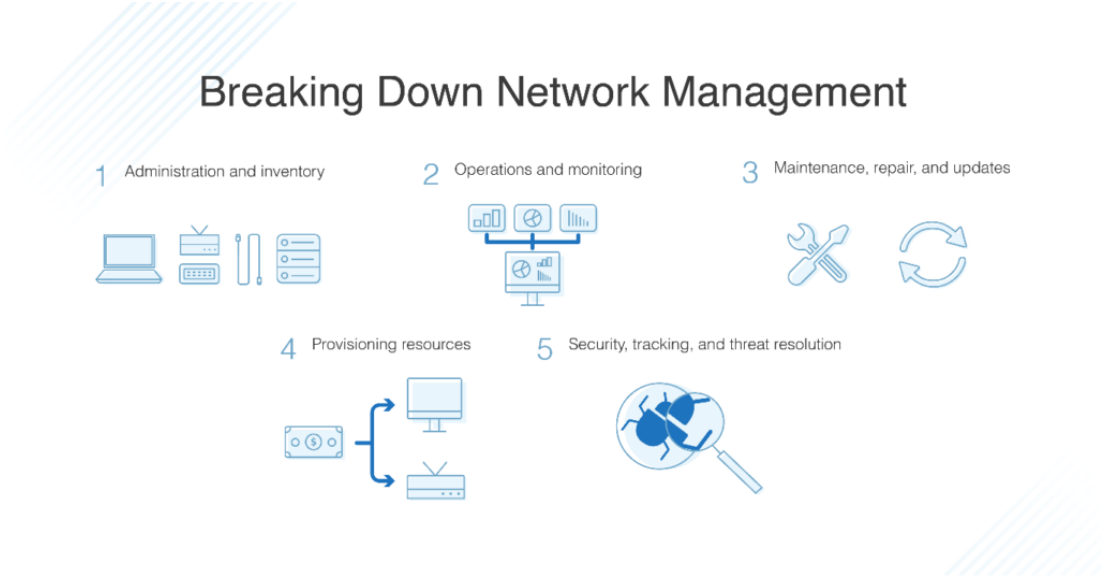
Client Management

Client management allows businesses to seamlessly manage their relationships with potential and existing customers. This includes managing sales, streamlining processes, and scheduling targeted customer communications. As a result, companies can better serve their customers, develop a better client relationship, and improve their profitability.

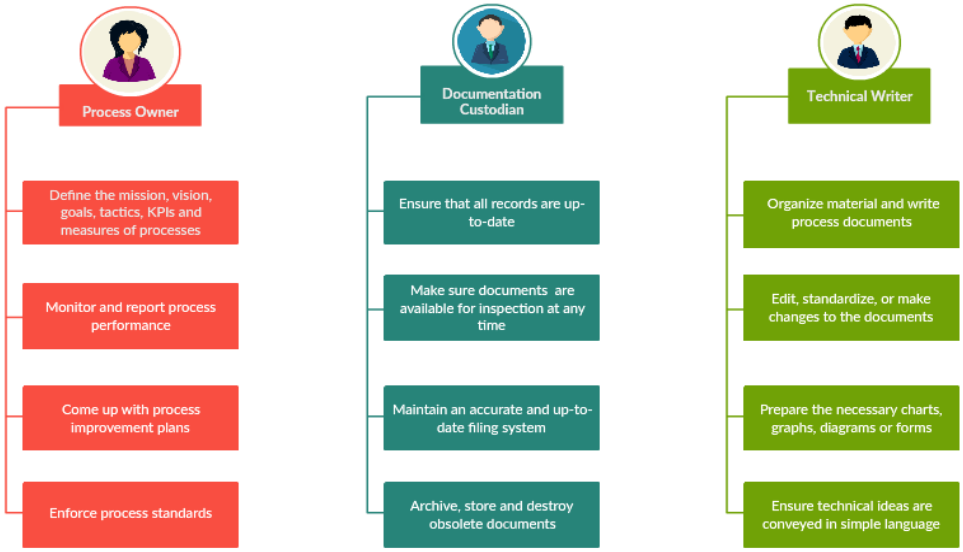


Network Management

A network management system (NMS) is an application or set of applications that lets network engineers manage a network's independent components inside a bigger network management framework and performs several key functions. An NMS identifies, configures, monitors, updates and troubleshoots network devices -- both wired and wireless -- in an enterprise network. A system management control application then displays the performance data collected from each network component, allowing network engineers to make changes as needed.



People Involved in the Documentation Process



System Documentation Template

The four basic elements of a System Documentation are the following: *TITLE, METADATA, WHAT, AND HOW.*

1. **Title**: A simple title that others will understand.
2. **Metadata:** The document's author's contact information, and the revision date or history. People reading the document will be able to contact the author with questions, and when you get promoted, your successors will honor you as the person who gifted them with this document. The revision date and history will help people understand whether the document is still relevant.
3. **What:** A description of the contents of the document or the goal that someone can achieve by following the directions. One or two sentences is fine.
4. **How:** The steps to take to accomplish the goal. For any step that seems mysterious or confusing, you might add a why, such as "Re-tension the tape (Why? Because we find that on a full backup, we get tape errors less often if we have done so, even with a new tape)."

Steps in Creating a System Documentation

Step 1: Identify and Name the Process

Figure out which process you are going to document first. Determine its purpose (why and how the process will benefit the organization) and provide a brief description of the process.

Step 2: Define the Process Scope

Provide a brief description of what is included in the process and what is out of the process scope, or what is not included in it.

Step 3: Explain the Process Boundaries

Where does the process begin and end? What causes it to start? And how do you know when it's done? Get these boundaries well defined.

Step 4: Identify the Process Outputs

Establish what will be produced by the process or what result the process will achieve once it is completed.

Step 5: Identify the Process Inputs

List down what resources are necessary to carry out each of the process steps.

Step 6: Brainstorm the Process Steps

Gather all information on process steps from start to finish. Either start with what triggers the process or start at the end of the process and track back the steps to the starting point.

The brainstorming session should involve those who are directly responsible for the process tasks or someone with extensive knowledge of it, as they can provide precise data.

Step 7: Organize the Steps Sequentially

Take the list of steps you've come up with and put them in a sequential order to create a process flow.

Keep the number of steps to a minimum and if a step includes more than one task, list them under the main step.

Step 8: Describe who is Involved

Decide each individual who will be responsible for the process tasks. Define their roles. Keep in mind to mention their job title rather than their name.

Also be considerate about those who would be referencing the document. Write it in a way that any employee with a reasonable knowledge can read and understand it.

Step 9: Visualize the Process

This is to improve clarity and readability of your documentation. Using a process flowchart, neatly visualize the process steps you've identified earlier.

Additional Documentation Uses

- **Self-help desk**: This area contains current status, major upcoming changes, and the ability to create tickets. It also contains links to other sources, such as the HOWTOs, FAQs, and monitoring system.
- **Internal group-specific documents**: Each group may want to have internal documentation that describes how to perform tasks that only that group can execute. This documentation has a narrow audience and may be less polished than documents aimed at a wider audience.
- **How-to documents**: A how-to or HOWTO document is a short document that describes how to accomplish a particular task.
- **Frequently asked questions**: The FAQs list the most common queries about a particular topic, along with their answers. The answers may point to a HOW TO document or self-help tools.
- **Reference lists**: Reference lists are accumulated lists of things that are not accessed often but that serve a specific purpose. For example, there might be a list of corporate acronyms, vendor contact information details, and hardware compatibility lists.
- **Procedures**: Have a repository for procedures, checklists, runbooks, and scripts. Also have a location for storing pre- and post-testing results and any other documents required for compliance with operational standards.
- **Technical library**: Store vendor documentation, technical articles, and so on, in a single repository that everyone can access.

Help Desk

Introduction

Every organization has a helpdesk. It may be physical, such as a walk-up counter, or virtual, such as by phone or email. Sometimes, the helpdesk function is unofficial, being the portion of each day spent directly helping customers. Small SA teams, with just one or two people, frequently have no official helpdesk, but that situation isn't sustainable. As the organization grows, small SA teams become big SA teams, and big SA teams become enterprise organizations. Organizations sometimes don't realize that they need to institute a formal helpdesk until it is too late.

What does a Help Desk do?
It provides a medium for contact for users to receive assistance when troubleshooting and solving problems. They are responsible in attending to the users' needs in a timely and professional manner. Help Desk support often works around the system and computer users within the company. They will also train the users on the basics of the system and computer functionalities.

Responsibilities of a Help Desk Administrator

- Managing service requests, problems and incidents
- Addressing IT concerns of all departments in the organization
- Tracking client/user issues
- Enabling employee onboarding

Support Staff

Sizing a helpdesk staff is very difficult because it changes from situation to situation. Universities often have thousands of students per helpdesk attendant. Corporate helpdesks sometimes have a higher ratio or sometimes a lower ratio. In a commercial computer science research environment, the ratio is often 40:1, and the first tier SAs have a similar skill level as second-tier SAs at other helpdesks, to meet the more highly technical level of questions. E-commerce sites usually have a separate helpdesk for internal questions and a "customer-facing" helpdesk to help resolve issues reported by paying customers. Depending on the services being offered, the ratio can be 10,000:1 or 1,000,000:1.

Support Process

Helpdesk staff should have well-defined processes to follow. In a smaller environment, this is not as important, because the processes are more ad hoc or are undocumented because they are being used by the people who built them. However, for a large organization, the processes must be well documented. Very large helpdesks use scripts as part of their training. Every service sup- ported has an associated flow of dialogue to follow to support that service. For example, the script for someone calling to request

remote access service captures the appropriate information and tells the operator what to do, be it enable remote access directly or forward the request to the appropriate service organization. The script for a request to reset a password would, for security reasons, require callers to prove who they are, possibly by knowing a unique piece of personal information, before a new password would be set.

Scope of system support

- **What is being supported?** Only the PCs or the LAN itself? Are all PCs supported, no matter which OS is being used, or only certain OSs and certain revisions? Which applications are being supported? How are unsupported platforms handled?
- **Who will be supported?** A particular department, building, division, enterprise, university? What if a person has offices in multiple buildings, each with its own helpdesk? Are only people who pay supported? Are only people of a certain management level and higher (or lower) supported?
- **Where are the customers?** This question is similar to who if one is supporting, for example, everyone in a particular building or location. However, where also includes support of traveling customers, customers visiting third-party sites, customers performing demos at trade shows, and people working from home.
- **When is support provided?** Are the hours of operation 8 AM to 6 PM, Monday through Friday? How are things handled outside of these hours? Do people have to wait until the helpdesk reopens, or is there a mechanism to reach SAs at home? If there is no support in the off-hours, what should facilities management do if environmental alarms sound or if a fire occurs?
- **How long should the average request take to complete?** Certain categories of requests should be instant; others will take longer. Establishing these goals sets expectations for the staff and customers. Customers expect everything to be immediate if they aren't told that certain tasks should be expected to take longer. A tiered structure might list certain things that are to be fast (5 minutes), slow (1 hour), and multiple days (requests for new service creation).

Chapter Review and Activities:

1. Describe a helpdesk staff structure.

2. Which topics seem to come up most often in customer requests at your site? What percentage might be handled by a self-help desk with some HOWTO documents?

3. Describe the people involved in the Documentation Process

3. Which documents in your organization would most benefit from having a template? Design the template.