Windows Server Foundation

Lesson 00:

IGATE is now a part of Capgemini

People matter, results count.

Capgemini

CONSULTING.TECHNOLOGY.OUTSOURCING

Document History

Date	Course Version No.	Software Version No.	Developer / SME	Reviewer(s)	Approver	Change Record Remarks
11-August–2016	1.0	2012	Amal Thambi	Saran, Rajdeep	Mahima Sharma	Crested as per the Infra BU requirement

Course Goals

Course Goals

- This course is designed for entry level Infra resources to enable the skills required for provisioning and maintaining a Windows Server environment.

Pre-requisites

This course requires that you meet the following prerequisites:

- The audience should have completed IS Windows Fundamentals

Intended Audience

- For Entry level Infrastructure Services(IS) resources

Day Wise Schedule

- Day 1

Lesson 1: Deploying & managing server 2012

Lesson 2:Introduction to ADDS

Lesson 3:Name Server of Windows

- Day 2

Lesson 4:DNS Zones and DNS Record Management

Lesson 5: Implementing DHCP Server

Lesson 6:Implementing File and Print Services

- Day 3

Lesson 8:Backup and Restore

Lesson 9:Windows Server Updates & Windows Firewall

Lesson 10: Windows Deployment Services

- Day 4

Lesson 11: WSUS

Lesson 12: IIS

Table of Contents

Table of Contents

Table of Contents

Table of Contents

References

- **Books:**

  Mastering Windows Server 2012 – Wiley Publications

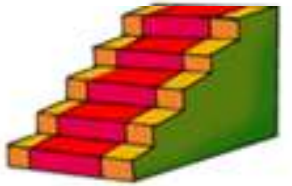
  MCSE 2012: 2012 R2 3-In-1 Complete Study Guide - Sybex Publications

- **Websites**

  http://technet.microsoft.com

Next Step Courses

- **Windows server 2016 Administration**



Other Parallel Technology Areas

- **Red Hat Linux Server**

Windows Essentials

Lesson 1 Deploying & managing server 2012

Module Overview

1.1. Windows Server 2012 Overview

1.2. Installing Windows Server 2012

1.3. Post-Installation Configuration of Windows Server 2012

1.4. Overview of Windows Server 2012 Management

1.5. Introduction to Windows PowerShell

1.6. Overview of TCP/IP

1.7. Understanding IPv4 & IPv6 Addressing

1.1. Windows Server 2012 Overview

- Windows Server 2012 R2 is the next version of Windows Server

- Delivers global-scale cloud services into your infrastructure with features and enhancements in virtualization, management, storage, networking, virtual desktop infrastructure, access and information protection, and the web and application platform.

What is new in server 2012

- Increased scalability and performance
- Virtualization features, such as those in Microsoft® Hyper-V® Server 2012 Replica, Live migration and Live Storage Migration
- Improved Windows PowerShell® and scripting support
- High-performance SMB 3.0 file shares
- Multi-server platform
- Built-in NIC teaming
- Enhanced Cloud Support
- Storage Spaces
- IP Address Management(IPAM)
- and many others

1.2. Installing Windows Server 2012

- **Windows Server 2012 Editions**
  - Standard
  - Datacenter
  - Foundation
  - Essentials
- **HW Requirements**
  - Processor architecture : 64 bit
  - Processor speed : 1.4 GHz
  - Memory (RAM) : 512 MB
  - Hard disk drive space : 32 GB
- **Installation Source:**
  - Optical media
  - USB media
  - Mounted ISO image
  - Network share
  - Windows Deployment Services (WDS)
  - System Center Configuration Manager
  - Virtual Machine Manager templates
- **Installation Type : New Install, Upgrade and Migrate**
- **Server Core Installation vs Server with a GUI Installation**

1.3. Post-Installation Configuration of Windows Server 2012

- Configure the IP address.
- Set the computer name.
- Join an Active Directory domain.
- Configure the time zone.
- Enable automatic updates.
- Add roles and features.
- Enable remote desktop.
- Configure Windows Firewall settings.

Booting process troubleshooting (Blue screen of death)

- Blue Screen of Death (also known as a blue screen or BSoD) is an error screen displayed on a Windows computer system after a fatal system error, also known as a system crash: when the operating system reaches a condition where it can no longer operate safely.

Troubleshooting BSOD

- Boot into Safe Mode
- Run a virus scan
- Perform a Repair Installation of Windows
- Roll back your recently installed drivers
- Roll back your recently installed Windows updates
- Clear up hard disk space
- Apply new updates and drivers
- Reinstall Windows
- Replace faulty hardware

Tools - bcdedit, bcdboot, systeminfo, msinfo32,fsutil

- **bcdedit** is a command-line tool for managing BCD stores. It can be used for a variety of purposes, including creating new stores, modifying existing stores, adding boot menu options, and so on.
- **bcdboot** tool is a command-line tool that enables you to manage system partition files. You can use the tool in the following scenarios: Setting up a system partition when you deploy new computers. For more information.
- **systeminfo** displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties (such as RAM, disk space, and network cards)
- **msinfo32** displays a comprehensive view of your hardware, system components, and software environment.
- **fsutil** Performs tasks that are related to file allocation table (FAT) and NTFS file systems

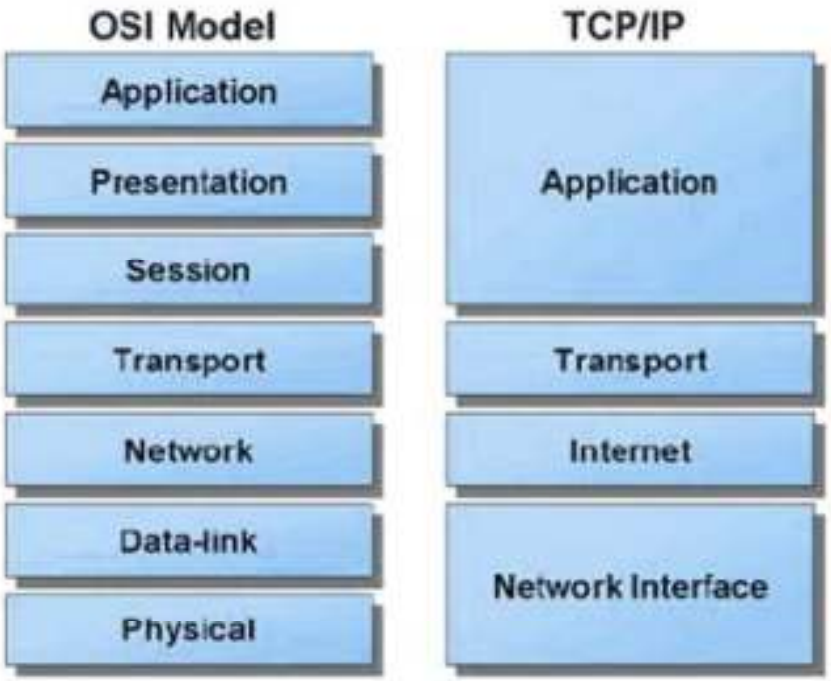
1.4. Overview of Windows Server 2012 Management

- Installing Windows Server
- Install and Configure required Roles and Features
- Monitor system performance
- Update system with the latest updates available from Microsoft
- User administration
- Verify that peripherals are working properly
- Quickly arrange repair for hardware in occasion of hardware failure
- Create and Configure file systems for Storage
- Create a backup and recover policy
- Perform recovery in case of Failure
- Configure High-Availability and Load-Balancing
- Monitor network communication
- Implement the policies for the use of the computer system and network
- Setup security policies for users. A sysadmin must have a strong grasp of computer security (e.g. firewalls)

1.5. Introduction to Windows PowerShell

- Introduced in 2006
- Windows PowerShell is a task automation and configuration management framework from Microsoft
- Consists of a command-line shell and associated scripting language built on the .NET Framework
- Functionalities provided:
  - Cmdlets (pronounced "command-lets")
  - Functions
  - Workflows

1.6. Overview of TCP/IP

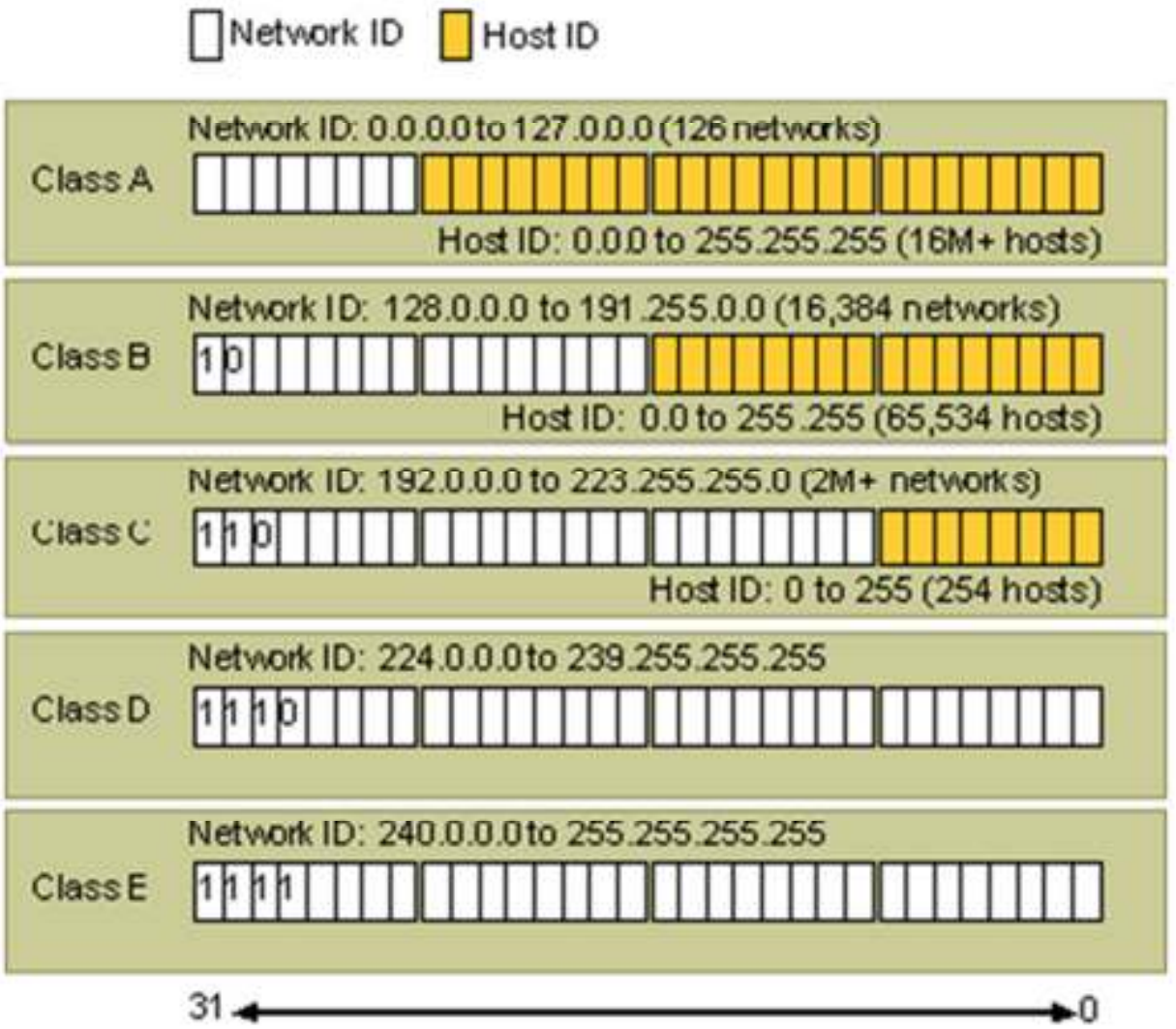


Capgemini
CONSULTING. TECHNOLOGY. OUTSOURCING

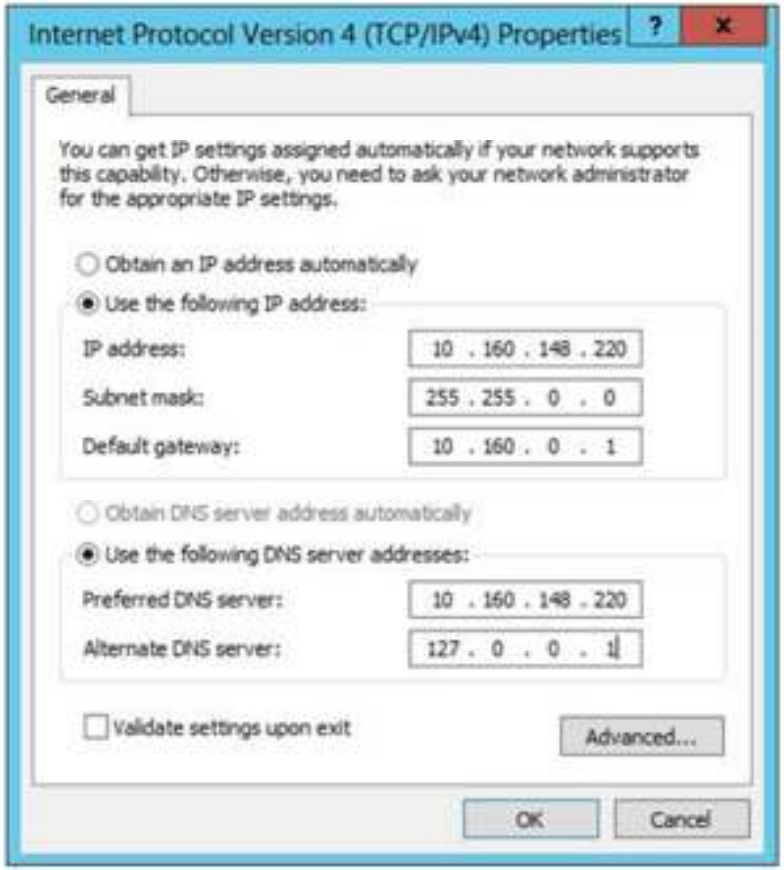
1.7. Understanding IPv4 & IPv6 Addressing

- Two types of IP Addressing
  - IPv4
  - IPv6

IPv4 Addressing

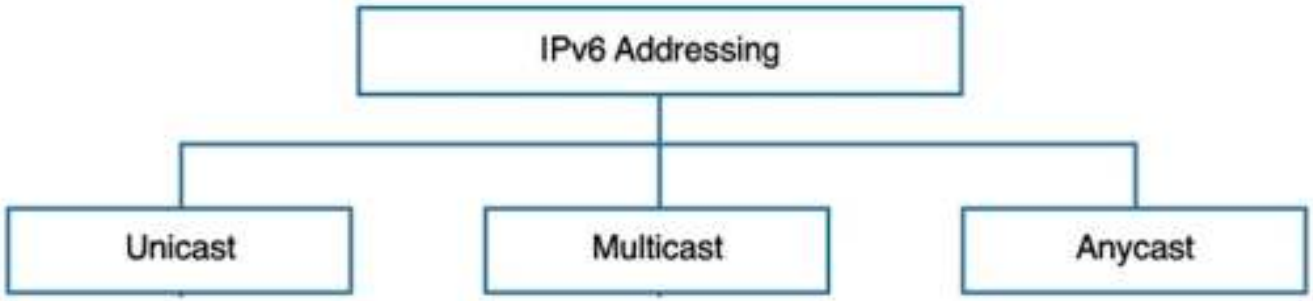


Configure IPv4

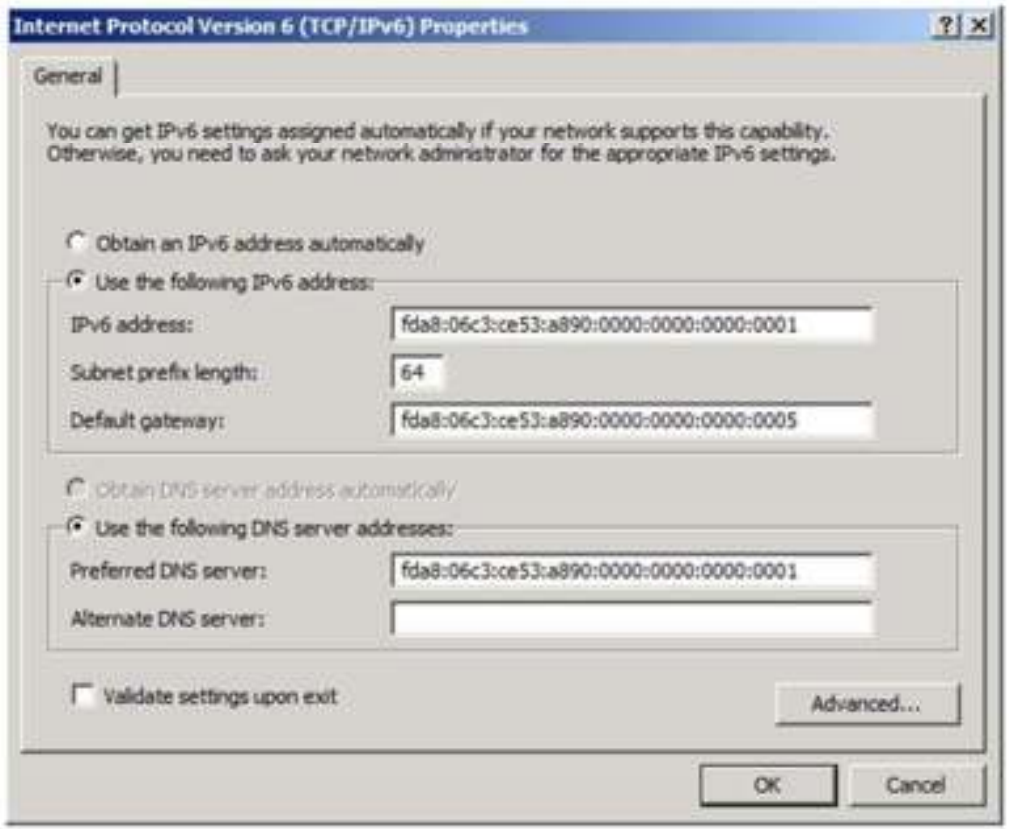


- netsh interface ipv4 set address name="Local Area Connection 2" static 172.16.254.2 255.255.255.192 172.16.254.1 store=persistent
- netsh interface add route prefix=172.16.1.0/24 interface="Local Area Connection 2" nexthop=172.16.254.254
- netsh interface ipv4 set dnsservers name="Local Area Connection 2" source=static address="172.16.254.250" validate=no

IPv6 Addressing



Configure IPv6 Address



- netsh interface ipv6 add address "Local Area Connection" 2001:db8:290c:1291::1
- netsh interface ipv6 add route ::/0 "Local Area Connection" fe80::2aa:ff:fe9a:21b8
- netsh interface ipv6 add dnsserver "Local Area Connection" 2001:db8:99:4acd::8

Summary

- **In this Module you have learnt:**
  - What is new in server 2012
  - How to install server 2012
  - Booting process troubleshooting (Blue screen of death)
  - Tools- bcdedit, bcdboot, systeminfo, msinfo32,fsutil
  - Basic server configuration
  - IPV 4 & 6 Configuration

Lab Exercise

- **INSTALLATION OF SERVER 2012**
- **Basic powershell commands**
- **IPV6 configuration**

Assignment

1. Explore purpose of utility like - bcdedit, bcdboot, systeminfo, msinfo32,fsutil
2. Booting system under safe mode and boot

Review Questions

1. **What should you do as an administrator when you encounter BSOD?**
2. **How can I configure IP address through commandline?**
3. **When I should use bcdedit?**

Windows Essentials

Lesson 2 Introduction to ADDS

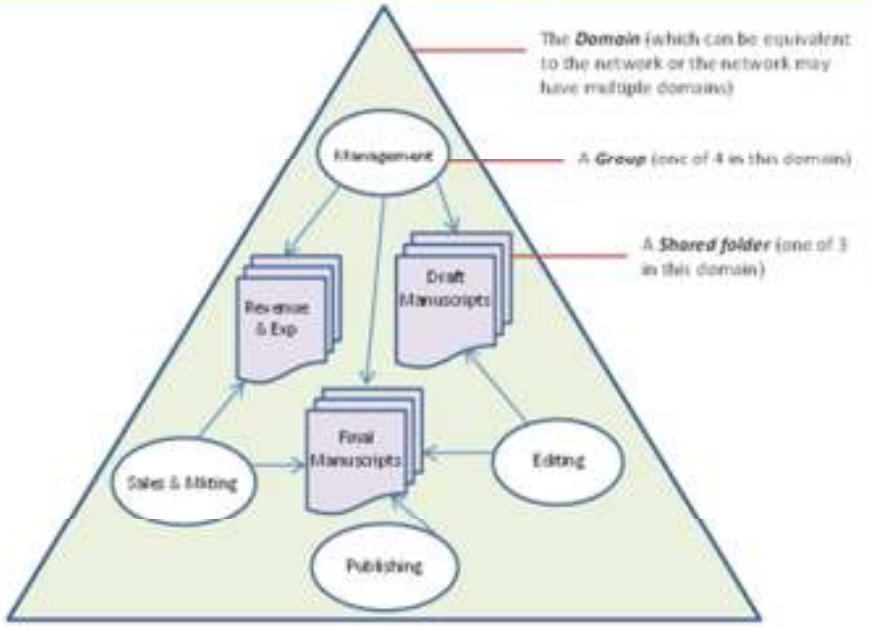
Module Overview

2.1. Overview of AD DS

2.2. Overview of Domain Controllers

2.3. Installing a Domain Controller

2.1. Overview of AD DS



- Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management.

Active Directory Administration Snap-ins

- **Active Directory Users and Computers**
  - used to manage users, groups, computers, printers and shared folders
- **Active Directory Domains and Trusts**
  - manage trust relationships
  - configure domain and forest functional levels
- **Active Directory Sites and Services**
  - Manage replication, network topology and related services
- **Active Directory Schema**
  - Manage AD Schema

Active Directory Administrative Center

- **Active Directory Administrative Center provides a task-orientated interface for managing Active Directory. To start this tool, click Start, Administrative Tools, Active Directory Administrative Center.**
- **You can use this tool to do the following:**
  - Connect to one or more domains
  - Create and manage user accounts
  - Create and manage groups
  - Create and manage organizational units
  - Perform global searches of Active Directory
- **Active Directory Administrative Center is installed by default on Windows Server 2008 R2 and is available on Windows 7 when you install the Remote Server Administration Tools (RSAT). This tool uses Windows PowerShell to perform administration tasks and relies on the .NET Framework**

Custom Consoles and Least Privilege

- Custom console is used to create a customized set of administrative consoles depending upon your work responsibilities.
- Creating a custom MMC can provide a convenient method for managing Windows Servers and the services they provide.
- Having one "dashboard" from which to manage Active Directory, Group Policy, DNS, DHCP, WSUS, WDS, and other services provides speed, simplicity, and a bit of self-documentation for whatever you have running on your server.

Secure Administration with Least Privilege, Run As Administrator, and User Account Control

- **It is recommended to use accounts for working Windows server/client**
  - A Standard user account
  - A Account with administrative privilege
- **Never use the Administrator account to log on.**
- **Use always the Standard user, and whenever some operations are requiring the Admin privileges, elevate your privilege by using "Run As" the administrative account.**

Use Windows PowerShell to Administer Active Directory

- Windows PowerShell is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and associated scripting language built on the .NET Framework
- enabling administrators to perform administrative tasks on both local and remote Windows systems
- administrative tasks are generally performed by cmdlets

New Features in 2012 ADDS

- Virtualization that just works
- Simplified deployment and upgrade preparation
- Simplified management
- AD DS Platform Changes
- GUI for Recycle Bin
- UI for Fine-Grained Password Policies
- Windows PowerShell History Viewer
- Windows PowerShell Cmdlets for Active Directory Replication

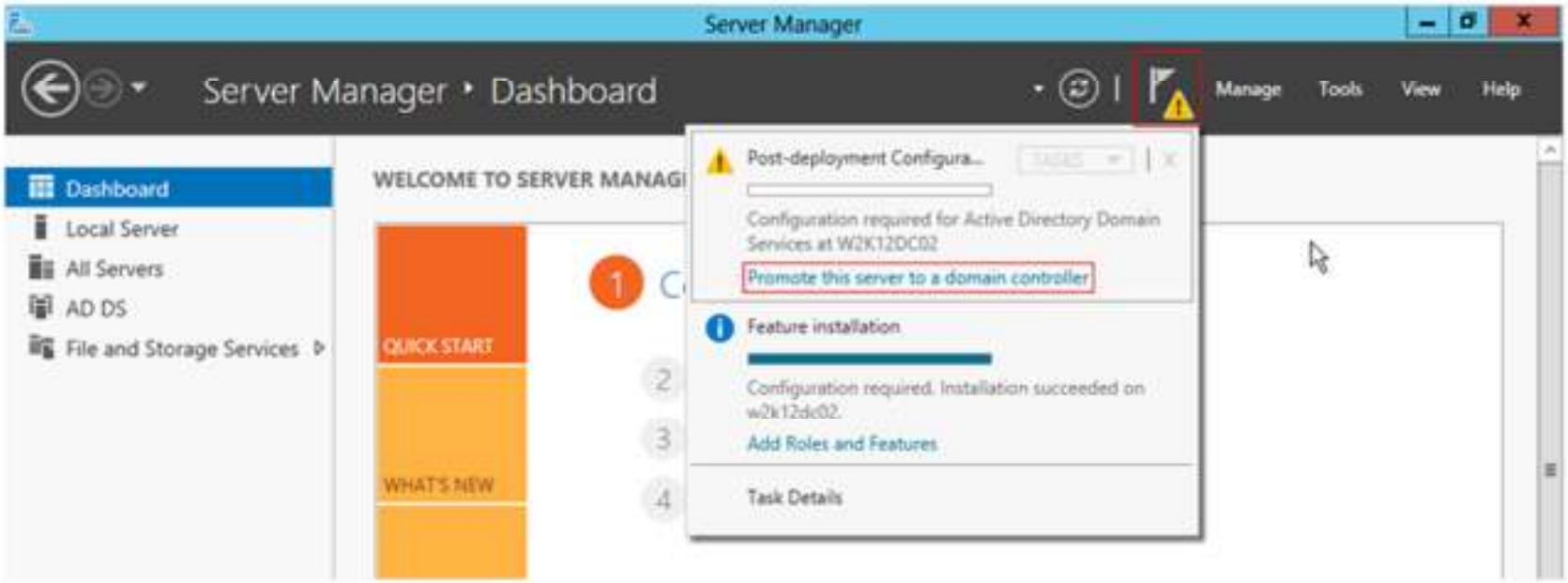
2.2. Overview of Domain Controllers

- A server running Active Directory Domain Services (AD DS) is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.
- One server, known as the primary domain controller, manages the master user database for the domain. One or more other servers are designated as backup domain controllers. The primary domain controller periodically sends copies of the database to the backup domain controllers. A backup domain controller can step in as primary domain controller if the PDC server fails and can also help balance the workload if the network is busy enough.
- In a domain, Domain Controllers needs to take care of 5 Flexible single master operation Roles. It can be load-balanced across the available number of DCs in the domain.

Active Directory Structure

- **Active Directory networks are organized using four types of divisions or container structures. These four divisions are**
  - Forests
  - Domain
  - Organizational units
  - Sites

2.3. Installing a Domain Controller



1. Install ADDS
2. Create a Domain in the Server to promote it as a Domain Controller

User Account

- **Active Directory user accounts represent physical entities, such as people.**
- **You can also use user accounts as dedicated service accounts for some applications.**
- **User accounts are also referred to as security principals.**
- **Security principals are directory objects that are automatically assigned security identifiers (SIDs), which can be used to access domain resources.**
- **A user account primarily:**
  - Authenticates the identity of a user.
  - Authorizes or denies access to domain resources.

User Account Management

- **Administrator can**
  - Rename/Move/Delete a user account
  - Reset a user account
  - UnLock a user account
  - Enable/Disable a user account

Create Users with Templates

- Enable you to standardize common user properties, such as group memberships
- It is important to realize that not all attributes are copied.
- One should ensure that template accounts are disabled, so that no one will misuse.

What Is a Managed Service Account

- The managed service account is designed to provide crucial applications such as IIS with the isolation of their own domain accounts, while eliminating the need for an administrator to manually administer the service principal name (SPN) and credentials for these accounts.
- It is a managed domain accounts that provides automatic password management and simplified SPN management.

Group Type

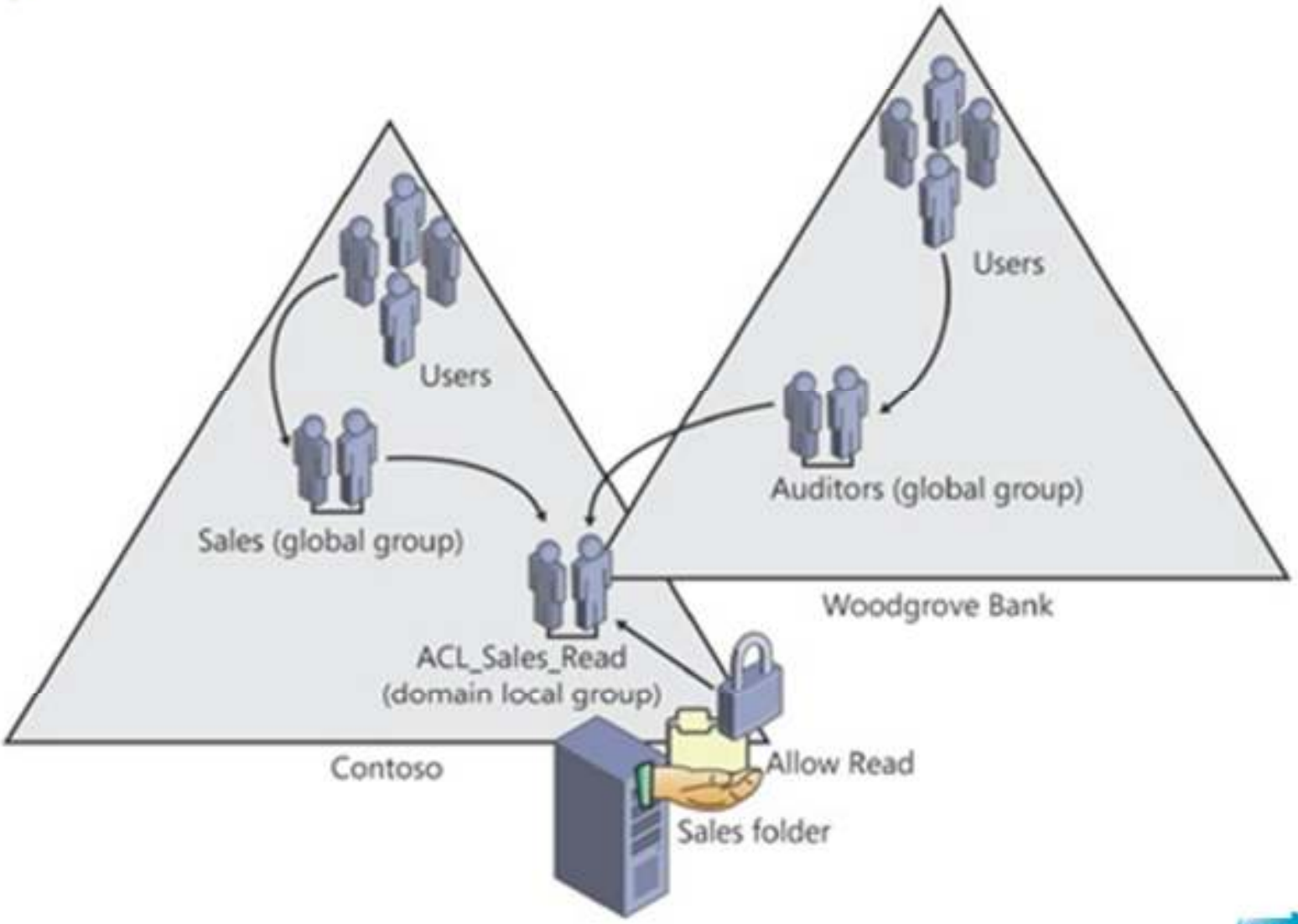
- **There are two types of groups in AD DS:**
  - distribution groups
    - use distribution groups to create e-mail distribution lists
  - security groups
    - use security groups to assign permissions to shared resources

Group Scope

Group Scope	Members from Same Domain	Members from Domain in Same Forest	Members from Trusted External Domain	Can be Assigned Permissions to Resources
Local	U, C, GG, DLG, UG and local users	U, C, GG, UG	U, C, GG	On the local computer only
Domain Local	U, C, GG, DLG, UG	U, C, GG, UG	U, C, GG	Anywhere in the domain
Universal	U, C, GG, UG	U, C, GG, UG	N/A	Anywhere in the forest
Global	U, C, GG	N/A	N/A	Anywhere in the domain or a trusted domain

U	User
C	Computer
GG	Global Group
DLG	Domain Local Group
UG	Universal Group

Group Management Strategy



Default Groups

- are security groups that are created automatically when you create an Active Directory domain. You can use these predefined groups to help control access to shared resources and delegate specific domain-wide administrative roles.
- Default groups, such as the Domain Admins group, are security groups that are created automatically when you create an Active Directory domain.
- Following are come of the commonly used default groups:
  - Enterprise Admins
  - Schema Admins
  - Administrators
  - Domain Admins
  - Server Operators
  - Account Operators
  - Backup Operators
  - Print Operators

Special Identities

- **Membership is purely controlled by Windows**
- **Can be given permissions on resources**
- **Example Special Identities:**
  - Anonymous Logon
  - Authenticated Users
  - Everyone
  - Interactive
  - Network

Workgroups, Domain, and Trust

- **In Workgroup Computer, System Accounts Manager(SAM) is the authority for authentication.**
  - Identities created will be local to that computer
- **In domain computer, Active directory is the authority for authentication**
  - Computers will have a trust relationship with the domain

Requirements for Joining a computer to the domain

- One should have permission in ADDS that allow you to join a computer to the domain
- Also one should be a member of Administrators group on the computer that needs to be joined to the domain

Prestage a computer account

- It is highly recommended that you should prestage the computer in the correct OU in the domain before you join the computer to the domain.
- By this way the policies intended to be applied for that OU computer/user will be applied immediately after joining the domain.
- If you have prestaged a computer then you don't need to move the computer to the appropriate OU after joining the domain.
- You can also specify who can join that computer to the domain

Secure computer Creation and Joins

- Prestage the computer in the correct OU before you join it to the domain
- Configure a default computer container
- Remove the default ability of normal domain users to join computers to the domain

Computer Account and Secure Channel

- **secure channel provides an encrypted way of communication between clients and domain controllers**
- **Every member computer will have a sAMAccountName and password. This is used to establish the secure channel between the member computer and the domain controller.**
- **Secure Channel might get broken due to the following reasons:**
  - Reinstalling the computer
  - Restoring a computer from an older backup
  - Computer and Domain disagrees the password

Recognize Computer Account problems

- **Computer Account Problems might pose several symptoms:**
  - Error messages at the time of logging-in in the login screen.
  - Event log errors with the keywords password, trust, secure channel, relationship with the domain or domain controller
  - Missing computer account in Active Directory

Reset a computer Account

- **You can reset a computer account in several ways:**
  - Active Directory Users and Computers
  - DSMod
  - NetDom
  - NLTest
  - PowerShell

Summary

- **In this Module you have learnt:**
  - What is ADDS
  - Difference between 2008 and 2012 ADDS

Lab Exercise

- **Installing ADDS Role**
- **Promoting server to Domain**

Review Questions

- **What is FSMO?**
- **What is a Site?**
- **What could be the AD structure of Capgemini?**

Windows Essentials

Lesson 3 Name Server of Windows

Module Overview

3.1. Windows DNS

3.2. Pre requisite of DNS

3.3. How to install a DNS in Windows Server 2008?

3.4. Server Services for Name Resolution

3.5. Client Services for Name Resolution

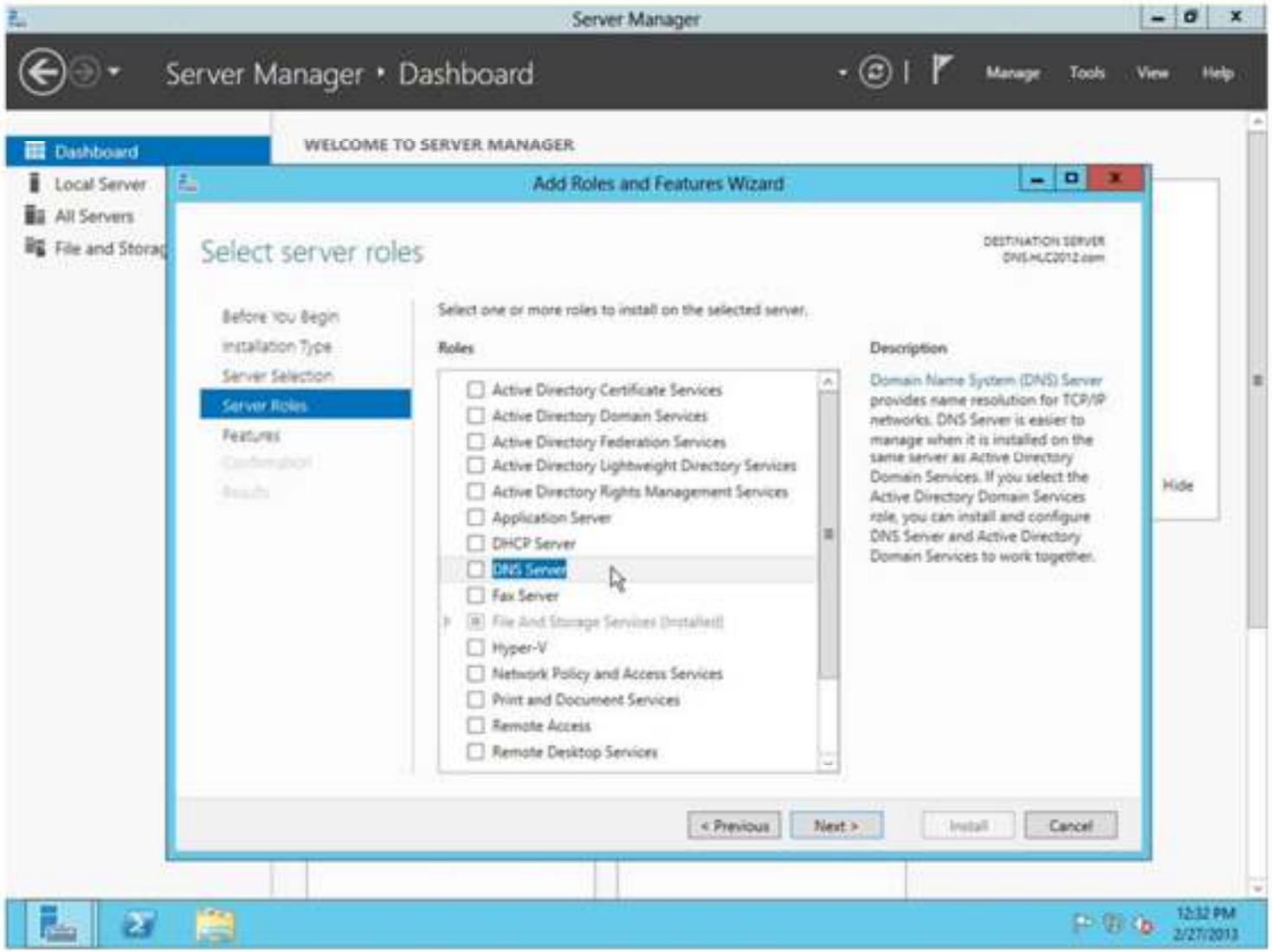
3.1. Windows DNS

- Domain Name System (DNS) is a hierarchical, distributed database that contains mappings of DNS domain names to various types of data, such as Internet Protocol (IP) addresses.
- DNS allows you to use friendly names, such as www.microsoft.com, to easily locate computers and other resources on a TCP/IP-based network.
- DNS is an Internet Engineering Task Force (IETF) standard.
- ADDS will require DNS for its functioning.

3.2. Pre requisite of DNS

- We need to install DNS role in order to make a Windows Server as a Domain Name Server
- It can be installed as a separate server or can be added along with other roles of a Windows Server
- It is recommended to have more than 1 DNS Server, so that in case of failure of the main DNS, other DNS server can provide the name resolution service.
- I can be installed in a full-fledged GUI Server or a Server Core installation.

3.3. How to install a DNS in Windows Server 2008?



Capgemini
CONSULTING. TECHNOLOGY. OUTSOURCING

3.4. Server Services for Name Resolution

- **DNS Server Service**
  - The DNS Server service enables DNS name resolution. It answers queries and update requests for DNS names. DNS servers locate devices that are identified by their DNS names and locate domain controllers in AD DS.
- **Location of Zone Files**
  - %systemroot%\system32\dns

3.5. Client Services for Name Resolution

- **DNS Client Service**
  - The DNS Client service resolves and caches Domain Name System (DNS) names for your computer. The DNS Client service must run on every computer that performs DNS name resolution. DNS name resolution is needed to locate domain controllers in AD DS domains.

NSLookup to troubleshoot name resolution

- NSLOOKUP is a basic command line utility for DNS queries, it's built into Windows and should be a tool you're familiar with.

- NSLOOKUP FQDN
- NSLOOKUP FQDN 208.67.222.222
- nslookup -querytype=mx bbc.co.uk

Summary

- **In this Module you have learnt:**
  - What is Windows DNS?
  - What are the pre requisites for DNS
  - How to install a DNS in Windows Server 2012?
  - What are the services in Server Side for DNS and location of DNS files
  - What are the services in Client Side for DNS

Lab Exercise

- Installation & Configuration of DNS role in windows server 2012
- Using of Nslookup to verify resolving of DNS
- Query of other records(MX,SRV etc)

Review Questions

- **What will be the problem if we don't have DNS?**
- **Can we combine DNS role with other Server roles?**

Windows Essentials

Lesson 4 DNS Zones and DNS Records Management

Module Overview

4.1. What is a Zone?

4.2. Type of Zone?

4.3. What is Forward Zone? - When it is Used

4.4. What is Reverse Zone? - When it is Used

4.5. How the IP and Name are mapped to each other?

4.6. What is DNS Record?

4.7. What are the types of Record we have?

4.8. When to use each Record?

4.9. How to create each type of Record?

4.1. What is a Zone?

A zone is the authoritative source for information about each DNS domain name that is included in the zone.

A zone starts with a single DNS domain name.

4.2. Type of Zone?

- Primary zone
- Secondary zone
- Stub zone

4.3. What is Forward Zone? - When it is Used

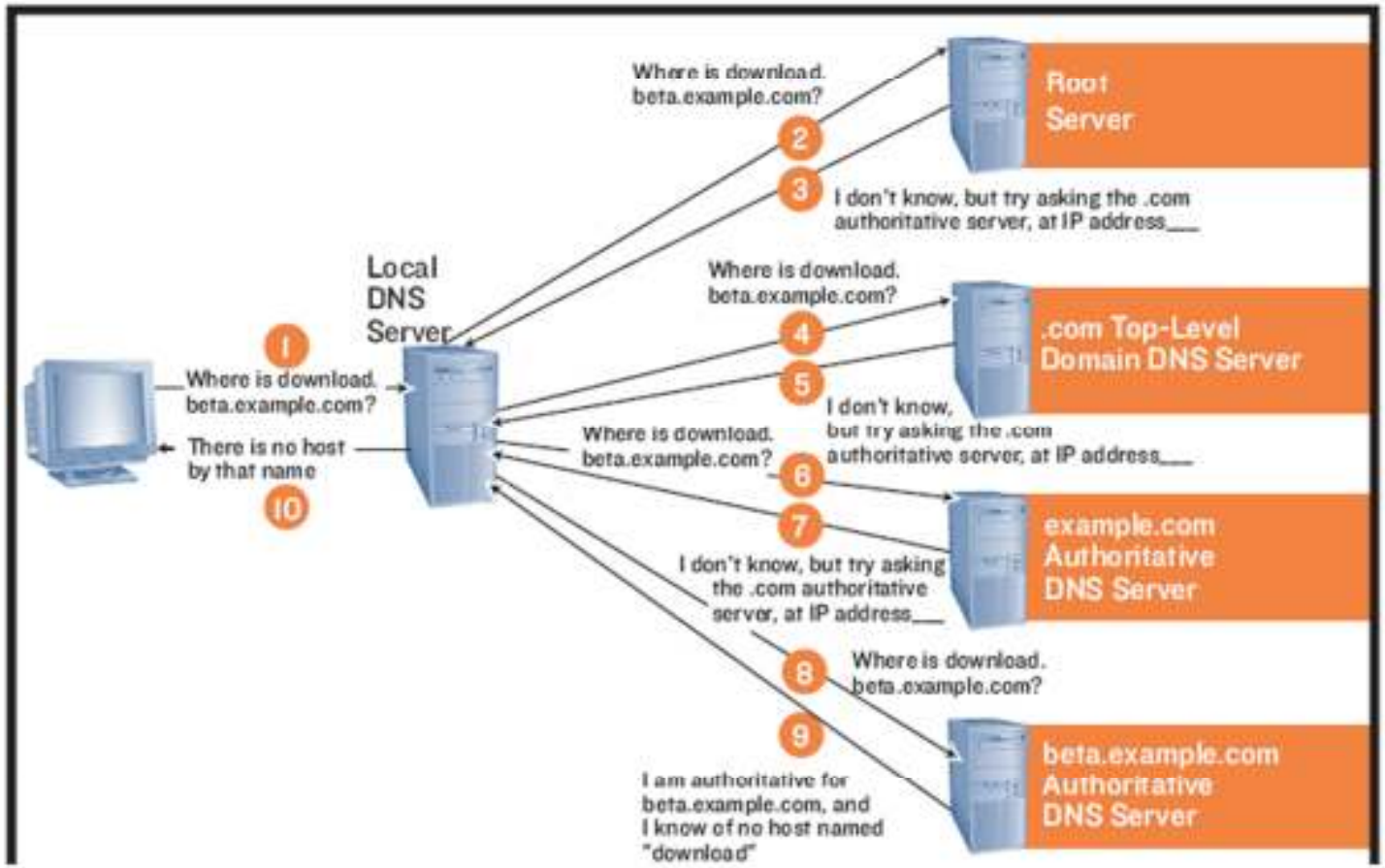
- A forward lookup zone is the most common type of zone. DNS clients can use this zone to obtain such information as IP addresses that correspond to DNS domain names or services that is stored in the zone. Another type of zone, a reverse lookup zone, provides mapping from IP addresses back to DNS domain names.
- When the Domain Name System (DNS) server role is installed as part of creating a domain controller by installing Active Directory Domain Services (AD DS), the forward lookup zones that are required to support the domain are automatically created.
- Creating a forward lookup zone is only necessary when you create a DNS server that is not running on a domain controller or if you need to create a DNS domain that is not part of your Active Directory domain structure.

4.4. What is Reverse Zone? - When it is Used

- DNS also provides a reverse lookup process, in which clients use a known IP address and look up a computer name based on its address. A reverse lookup takes the form of a question, such as "Can you tell me the DNS name of the computer that uses the IP address 192.168.1.20?"

- Used in some networked applications, where they are used to perform security checks.

4.5. How the IP and Name are mapped to each other?



4.6. What is DNS Record?

- Computers that need to be accessed from Active Directory and DNS domains must have DNS records.
- Although there are many different types of DNS records, most of these record types aren't commonly used.

4.7. What are the types of Record we have?

- A (address)
- CNAME (canonical name)
- MX (mail exchange)
- PTR (pointer)

4.8. When to use each Record?

- **A Records**
  - You would want to use an A Record for your DNS entry if you have an IP address that the domain/subdomain should point to or if you want to establish a domain/subdomain to be used as the place to point a CNAME
- **CNAME**
  - we can use CNAMEs for customers as a means of being able to change the IP address of a server or cluster of servers transparently and without users having to make their own DNS adjustments.
- **MX Record**
  - MX mechanism provides the ability to run multiple mail servers for a single domain, and allows administrators to specify an order in which they should be tried.
- **PTR (pointer)**
  - PTR records are mainly used to check if the server name is actually associated with the IP address from where the connection was initiated.

4.9. Demo: How to create each type of Record?

- How to create an A record?
- How to create a CNAME record?
- How to create a MX Record?
- How to create a PTR record?

Summary

- **In this Module you have learnt:**
  - Concept and need of zone
  - what are the different types of zone?
  - What is Forward Zone ? - When it is Used
  - What is Reverse Zone ? - When it is Used
  - Mapping of IP to name
  - What is DNS Records?
  - Different types of records ?
  - What is the use of each records?
  - Creation of each records·

Lab Exercise

- Creation, deletion& modification of zone
- Mapping of IP to name(Verify using nslookup)
- Creation of different DNS records

Review Questions

Windows Essentials

Lesson 5 Implementing DHCP Server

Module Overview

6.1. Overview of the DHCP Server Role

6.2. Configuring DHCP Scopes

6.3. Managing a DHCP Database

6.4. Securing and Monitoring DHCP

6.1. Overview of the DHCP Server Role

- When you deploy Dynamic Host Configuration Protocol (DHCP) servers on your network, you can automatically provide client computers and other TCP/IP based network devices with valid IP addresses

6.2. Configuring DHCP Scopes

- A scope is an administrative grouping of IP addresses for computers on a subnet that use the Dynamic Host Configuration Protocol (DHCP) service.
- The administrator first creates a scope for each physical subnet and then uses the scope to define the parameters used by clients.

DHCP reservation

- DHCP reservation is a process in which a particular IP address is mapped with one computer that is typically a server that needs to have a same IP address permanently.
- When this is done, every time the target DHCP client computer requests an IP address from the DHCP server, the mapped IP address is assigned to it. Since the IP address is reserved for a particular computer while specifying DHCP reservation, it is not assigned to any other computer even if it is the only address available in the DHCP address pool.

DHCP Filtering

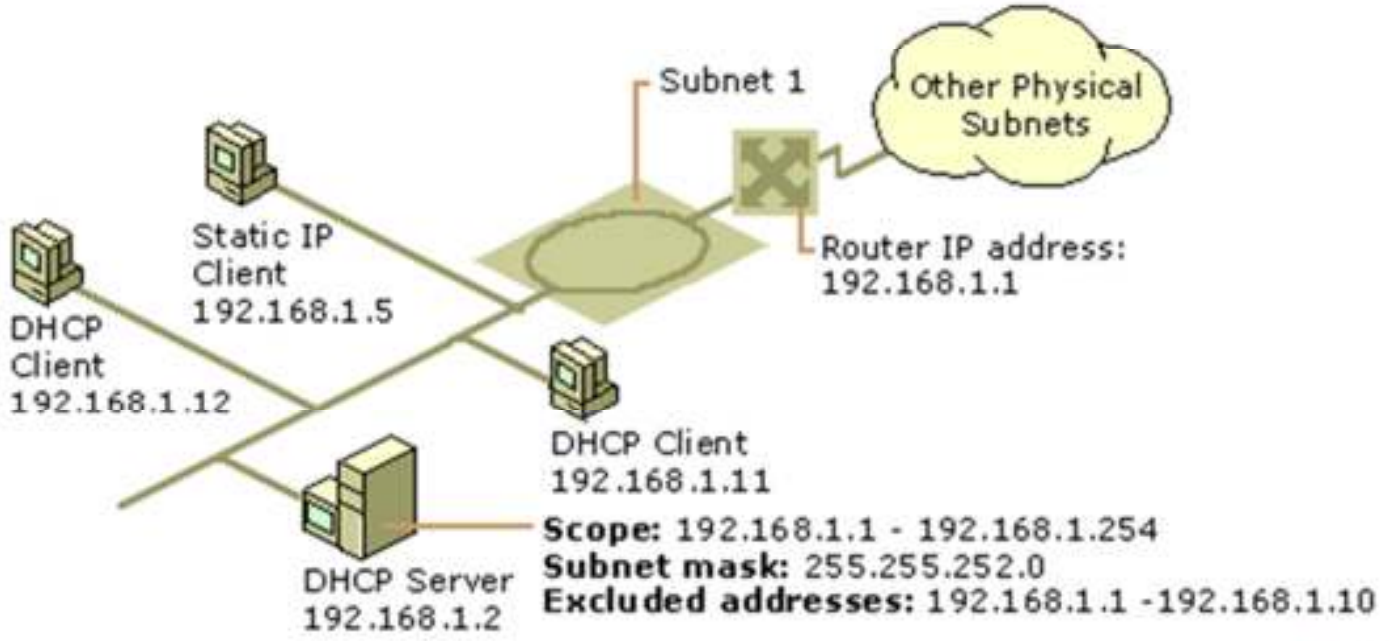
- A DHCP server offers its services to the DHCP clients based on the availability of MAC address filtering.
- Once the Allow filter is set, all DHCP operations are based on the access controls (allow/deny).
- You can add a valid MAC address to either the Allow or Deny filters, but not both.

DHCP Policy

- Allows you to create IPv4 policies that specify custom IP address and option assignments for DHCP clients based on a set of conditions.
- allows you to group DHCP clients by specific attributes based on fields contained in the DHCP client request packet. Policy Based Assignment (PBA) enables targeted administration and greater control of the configuration parameters delivered to network devices with DHCP.

Superscopes

- A superscope allows a DHCP server to provide leases from more than one scope to clients on a single physical network.
- Before you can create a superscope, you must use DHCP Manager to define all scopes to be included in the superscope. Scopes added to a superscope are called member scopes.



Capgemini
CONSULTING. TECHNOLOGY. OUTSOURCING

Using the 80/20 rule for scopes

- For balancing DHCP server usage, a good practice is to use the "80/20" rule to divide the scope addresses between the two DHCP servers.
- If Server 1 is configured to make available most (approximately 80 percent) of the addresses, then Server 2 can be configured to make the other addresses (approximately 20 percent) available to clients.

6.3. Managing a DHCP Database

- The DHCP server database is a dynamic database that is updated as DHCP clients are assigned or as they release their TCP/IP configuration parameters.

6.4. Securing and Monitoring DHCP

- DHCP is an unauthenticated protocol, which means that when users connect to the network they are not required to provide credentials in order to obtain a lease.
- An unauthenticated user can obtain a lease for any DHCP client whenever a DHCP server is available to provide a lease, and any option values that the DHCP server provides with the lease, such as WINS server or DNS server IP addresses, are available to the unauthenticated user.

1. The first step in designing a secure address allocation service is to limit the number of people authorized to have either physical or logical access to the address allocation server and to ensure that unauthorized persons do not have physical or wireless access to the network.
2. DHCP Server Authorization :There is an Active Directory feature that prevents rogue Windows 2000-based DHCP servers from running. When a DHCP server running Windows 2000 or later starts, it first checks Active Directory to confirm its authorization to run. If the server has explicitly been authorized as a DHCP server, it is allowed to run. By default, the DHCP server checks its authorization every sixty minutes.

DHCP backup and restore

- **Maintaining a backup of the Dynamic Host Configuration Protocol (DHCP) database protects you from data loss in the event of data corruption or a hard disk failure.**
- **There are three backup methods supported by the DHCP Server service:**
  - Synchronous backups that occur automatically. The default backup interval is 60 minutes.
  - Asynchronous (manual) backups, performed by using the Backup command in the DHCP snap-in.
  - Backups using Windows Backup (Ntbackup.exe) or other backup software.

Summary

- **In this Module you have learnt:**
  - Configuring DHCP Scopes
  - Managing DHCP Scopes, Reservations, Filters and Policies
  - Superscope and 80/20 Rule

Lab Exercise

- **Install & Configure DHCP Server**
- **DHCP backup and restore**

Review Questions

1. **Why will we require DHCP server in Capgemini Network?**
2. **What is the DHCP Server of your PC?**
3. **What if your PC couldn't reach DHCP server to get address?**

Windows Essentials

Lesson 6 Implementing File and Print Services

Module Overview

6.1. Overview of FSRM

6.2. Using FSRM to Manage Quotas, File Screens, and Storage Reports

6.3. Implementing Classification and File Management Tasks

6.4. Overview of DFS and DFS Replication

6.1. Overview of FSRM

- File Server Resource Manager is a suite of tools for Windows Server® 2008 that allows administrators to understand, control, and manage the quantity and type of data that is stored on their servers.

6.2. Using FSRM to Manage Quotas, File Screens, and Storage Reports

- **Quota Management** Information about creating quotas that set a soft or hard space limit on a volume or folder tree.
- **File Screening Management** Information about creating file screening rules that block files from a volume or a folder tree.
- **Storage Reports Management** Information about generating storage reports that can be used to monitor disk usage patterns, identify duplicate files and dormant files, track quota usage, and audit file screening.

Quota Management

- **On the Quota Management node of the File Server Resource Manager Microsoft® Management Console (MMC) snap-in, you can perform the following tasks:**
  - Create quotas to limit the space allowed for a volume or folder, and generate notifications when the quota limits are approached or exceeded.
  - Generate auto apply quotas that apply to all existing subfolders in a volume or folder and to any subfolders that are created in the future.
  - Define quota templates that can be easily applied to new volumes or folders and then used across an organization.

File Screening Management

- **On the File Screening Management node of the File Server Resource Manager MMC snap-in, you can perform the following tasks:**
  - Create file screens to control the types of files that users can save, and generate notifications when users attempt to save unauthorized files.
  - Define file screening templates that can be applied to new volumes or folders and that can be used across an organization.
  - Create file screening exceptions that extend the flexibility of the file screening rules.

Storage Reports Management

- **On the Storage Reports Management node of the File Server Resource Manager MMC snap-in, you can perform the following tasks:**
  - Schedule periodic storage reports that allow you to identify trends in disk usage.
  - Monitor attempts to save unauthorized files for all users or a selected group of users.
  - Generate storage reports instantly.

6.3. Implementing Classification and File Management Tasks

- **Classification**
  - Classification properties are used to categorize files and can be used to select files for scheduled file management tasks.
  - There are many ways to classify a file. One way is to create a classification property that assigns a value to all files within a specified directory.
  - Another way is to create rules to decide what value to set for a given property.
- **File management tasks**
  - Automate the process of finding subsets of files on a server and applying simple commands.
  - These tasks can be scheduled to occur periodically to reduce repetitive costs. Files that will be processed by a file management task can be defined through any of the following properties:
    - Location
    - Classification properties
    - Creation time
    - Modification time
    - Last accessed time

Shadow Copies

- Shadow Copies of Shared Folders provides point-in-time copies of files that are located on shared resources, such as a file server.
- With Shadow Copies of Shared Folders, users can view shared files and folders as they existed at points of time in the past.

6.4. Overview of DFS and DFS Replication

- Distributed file System (DFS) is a set of client and server services that allow an organization using Microsoft Windows servers to organize many distributed SMB file shares into a distributed file system. DFS provides location transparency and redundancy to improve data availability in the face of failure or heavy load by allowing shares in multiple different locations to be logically grouped under one folder, or DFS root.

- Distributed File System Replication (DFSR) service is a state-based, multimaster replication engine that supports replication scheduling and bandwidth throttling. DFSR uses a compression algorithm known as remote differential compression (RDC). RDC is a "diff-over-the wire" client/server protocol that can be used to efficiently update files over a limited-bandwidth network. RDC detects insertions, removals, and rearrangements of data in files, enabling DFSR to replicate only the changed file blocks when files are updated.

Print Services

- Print Services enables you to share printers on a network, as well as to centralize print server and network printer management tasks.
- It also enables you to migrate print servers and deploy printer connections using Group Policy

Summary

- **In this Module you have learnt:**
  - Creating and Configuring a File Share
  - Configuring Shadow Copies

Lab Exercise

- Install & configure File servers
- Configure DFS
- Configure FSRM(File screening,quotas)
- Collect Storage Reports

Review Questions

1. **Why I need FSRM?**
2. **Why I need to have DFS?**
3. **On what scenarios shadow copies can be helpful?**

Windows Essentials

Lesson 7 Backup and Restore

Module Overview

7.1. Data Protection Overview

7.2. Implementing Windows Server Backup

7.1. Data Protection Overview

- As administrator we need to have recovery plan for the below:
  - operating system
  - system state
  - Volumes
  - Files
  - application data.
- Backups can be saved to single or multiple disks, single or multiple volumes, DVDs, removable media, or remote shared folders.
- They can be scheduled to run automatically or manually.

7.2. Implementing Windows Server Backup

- Windows Server Backup consists of a Microsoft Management Console (MMC) snap-in, command-line tools, and Windows PowerShell cmdlets that provide a complete solution for your day-to-day backup and recovery needs.
- You can use Windows Server Backup to back up a full server (all volumes), selected volumes, the system state, or specific files or folders—and to create a backup that you can use for bare metal recovery.
- You can recover volumes, folders, files, certain applications, and the system state. And, in case of disasters like hard disk failures, you can perform a bare metal recovery. (To do this, you will need a backup of the full server or just the volumes that contain operating system files, and the Windows Recovery Environment—this will restore your complete system onto your old system or a new hard disk.)
- You can use Windows Server Backup to create and manage backups for the local computer or a remote computer. And, you can schedule backups to run automatically.
- Windows Server Backup is intended for use by everyone who needs a basic backup solution—from small business to large enterprises—but is even suited for smaller organizations or individuals who are not IT professionals.

Demo

- Perform backup of Data in Windows Server
- Perform recovery of files in Windows Server

Summary

- **In this Module you have learnt:**
  - Backing Up Data on a Windows Server 2012 R2 Server
  - Restoring Files Using Windows Server Backup

Lab Exercise

Backup and restore

Review Questions

1. **What needs to be backed up?**
2. **How often we need to backup?**
3. **What are the tools that windows server provides for backup/recovery?**

Windows Essentials

Windows Server Updates & Windows Firewall

Module Overview

8.1. Patch, Hotfix and Service pack

8.2. Use of applying security updates; Use of windows firewall

8.1. Patch, Hotfix and Service pack

- **Patch** is a piece of software designed to fix or improve a computer program or its supporting data
- A **hotfix** is a single, cumulative package that includes information that is used to address a problem in a software product. Typically, hotfixes are made to address a specific customer situation. The term "hotfix" originally referred to software patches that were applied to "hot" systems; that is, systems which are live, currently running, and in production status rather than development status.
- A **service pack (SP)** is a Windows update, often combining previously released updates, that helps make Windows more reliable. Service packs, which are provided free of charge on this page, can include security and performance improvements and support for new types of hardware.

8.2. Use of applying security updates and Use of windows firewall

- **Use of applying security updates**
  - By not applying a patch you might be leaving the security loophole in the OS/application open for hackers and malware to come in.
  - In order to keep the server secured, an administrator need to apply the latest security updates released by Microsoft/Vendor on a regular basis, before something exploits the security flaw in your system.
- **Use of windows firewall**
  - Windows Firewall is a built-in, host-based, stateful firewall
  - Windows Firewall drops incoming traffic that does not correspond to either traffic sent in response to a request of the computer (solicited traffic) or unsolicited traffic that has been specified as allowed (excepted traffic).
  - Windows Firewall helps provide protection from malicious users and programs that rely on unsolicited incoming traffic to attack computers.
  - Also drop outgoing traffic and is configured using the Windows Firewall with Advanced Security snap-in, which integrates rules for both firewall behavior and traffic protection with Internet Protocol security (IPsec).

Demo

- How to download and install a patch/Hotfix/ServicePack?
- How to configure your firewall to protect your server?

Summary

- **In this Module you have learnt:**
  - How to download updates and install When Microsoft will release security updates

Lab Exercise

- **Download and install updates**

Review Questions

1. **Why do we need to apply patches?**
2. **What is the latest service pack available for Windows Server?**
3. **What is the best time to apply an update?**
4. **Do I need to turn-on automatic update? Justify your answer**

Windows Essentials

Lesson 9 Windows Deployment Services

Module Overview

9.1. Overview of Windows Deployment Services

9.2. Managing Images

9.3. Administering Windows Deployment Services

9.1. Overview of Windows Deployment Services

- Windows Deployment Services enables you to deploy Windows operating systems.
- You can use it to set up new computers by using a network-based installation. This means that you do not have to install each operating system directly from installation media, for example a DVD or USB drive.

9.2. Managing Images

- **The image types used in Windows Deployment Services are:**
  - Install image. The operating system image that you deploy to the client computer.
  - Boot image. The Windows Preinstallation Environment (Windows PE) image that you boot a client into before you install the install image.

9.3. Administering Windows Deployment Services

- **As and Administrator, he needs to know at least the following basic activities in WDS:**
  1. Install/Remove WDS role
  2. Add/Remove Images

Summary

- **In this Module you have learnt:**
  - What is WDS
  - How to Deploy OS image using WDS
  - What is Boot Image

Lab Exercise

- **Implementing WDS**
- **Deploy OS image.**
- **Administering Windows Deployment Services**

Review Questions

1. **What are the benefits of using WDS?**
2. **What are the different types of images?**

Windows Essentials

Lesson 10 WSUS

Module Overview

10.1. Implementing Update Management

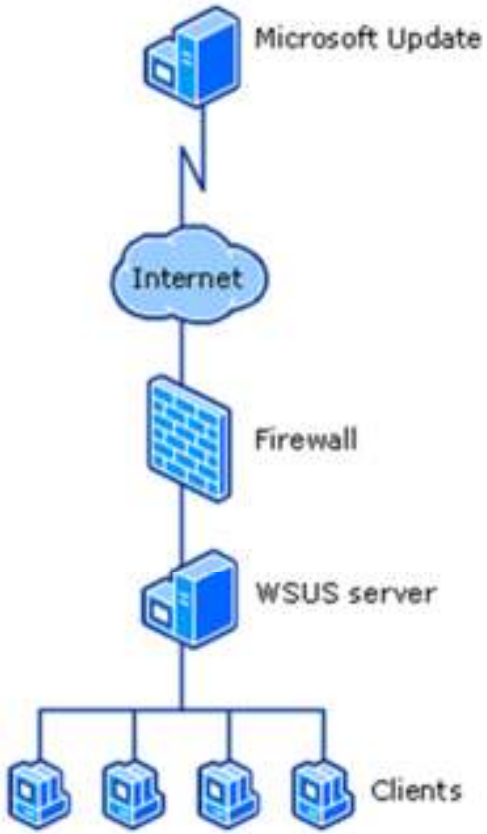
10.2. What is use of Storing in central place?

10.1. Implementing Update Management

- With Update Management enables information technology administrators to deploy the latest Microsoft product updates to computers that are running the Windows operating system.
- WSUS implements Update Management framework for windows.
- By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network.

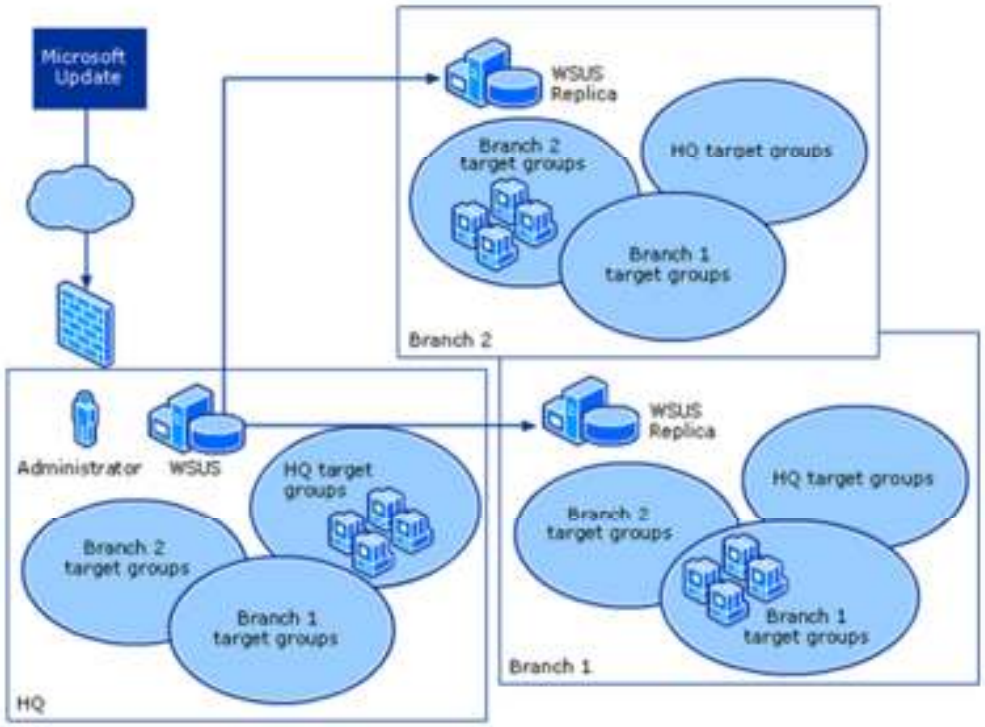
10.2. What is use of Storing in central place?

- Storing updates in a central place helps in distributing the updates throughout the organization.
- Clients doesn't need to individually download the updates from Microsoft for applying update. It saves time and bandwidth



Centrally managed WSUS

- For more complex Scenarios, Centrally managed WSUS servers utilize replica servers. Replica servers are not administered separately, and are used only to distribute approvals, groups, and updates. The approvals and targeting groups you create on the master server are replicated throughout the entire organization



Capgemini
CONSULTING. TECHNOLOGY. OUTSOURCING

Demo

- Install WSUS

Summary

- **In this Module you have learnt:**
  - Overview of WSUS
  - Installing WSUS

Lab Exercise

- **Install WSUS**

Review Questions

1. **Why do I need WSUS?**
2. **What are the benefits of WSUS?**
3. **What is WSUS replication?**

Windows Essentials

Lesson 11 IIS

Module Overview

11.1 Protocols used in IIS

- HTTP
- HTTPS
- FTP

11.2 Introduction of Web server

- A web server is a computer system that processes requests via HTTP, the basic network protocol used to distribute information on the World Wide Web.
- The term can refer to the entire system, or specifically to the software that accepts and supervises the HTTP requests.
- Uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients.

- Intranet vs Internet
  - Intranet is system in which multiple PCs are connected to each other. PCs in intranet are not available to the world outside the intranet. company or organization has their own Intranet network and members/employees of that company can access the computers in their intranet. Every computer in intranet is identified by a unique private IP address.
  - Internet is a world-wide / global system of interconnected computer networks. Every computer in internet is identified by a unique public IP address.

e.g) Apache, Tomcat, IIS

11.3 Introduction of Internet Information Services

- Internet Information Services (IIS, formerly Internet Information Server) is an extensible web server created by Microsoft for use with Windows NT family.
- IIS supports HTTP, 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.

- Window Server 2008 R2 – IIS 7.5
- Windows Server 2012 – IIS 8.0
- Windows Server 2012 R2 – IIS 8.5
- Windows Server 2016 – IIS 10

11.4 Installation of IIS

1. Open the Server Manager and click Add Roles and Features
2. Go on until you reach the Server Roles tab
3. Select Web Server (IIS)
4. Ignore the Features tab and go on
5. Click Next
6. The default configuration will be fine. Click Next
7. Click Install
8. Installation will be completed
9. Go back to the Server Manager. Select Internet Information Services (IIS) Manager from the Manage menu
10. Click Add Website
11. Specify at least the site name and path. Click Ok
12. Your first site is ready to be accessed

11.5 Managing IIS

- We need to use IIS Manager to manage IIS
- We can start/stop/configure/manage/backup/restore IIS with the IIS Manager

Demo

- Start IIS
- Stop IIS
- Add MIME Type
- Create and Deploy a small Webpage

Summary

- **In this Module you have learnt:**
  - Overview of IIS
  - Installing IIS
  - Managing IIS

Lab Exercise

- **Install and Manage IIS**

Review Questions

1. **Why do I need IIS?**
2. **How to manage IIS?**