SERVER BASIC CONFIGURATION

PREPARED BY

Topics

- Configure local server properties
- Configure server roles
- Set up IP addressing service roles

Configure local server properties

Once you've installed your servers, you must take additional steps to enable them to perform the roles you chose for them in the network.

Server Roles and Requirements

Each server has a certain role to play, although in small networks a server performs multiple roles.

Some roles demand lots of memory, whereas others place a heavier load on that CPU.

Web Server

Web servers are used to provide access to information to users connecting to the server using a web browser, which is the client part of the application. A web server uses HTTP as its transfer mechanism.

To provide security to a web server it can be configured to require and use HTTPS, which uses SSL to encrypt the connection with no effort on the part of the user, other than being aware that the URL must use https rather than http.

Here are some of the components that should be maximized to ensure good performance in a web server:

- Disk Subsystem
- RAM
- CPU
- NIC

Application Server

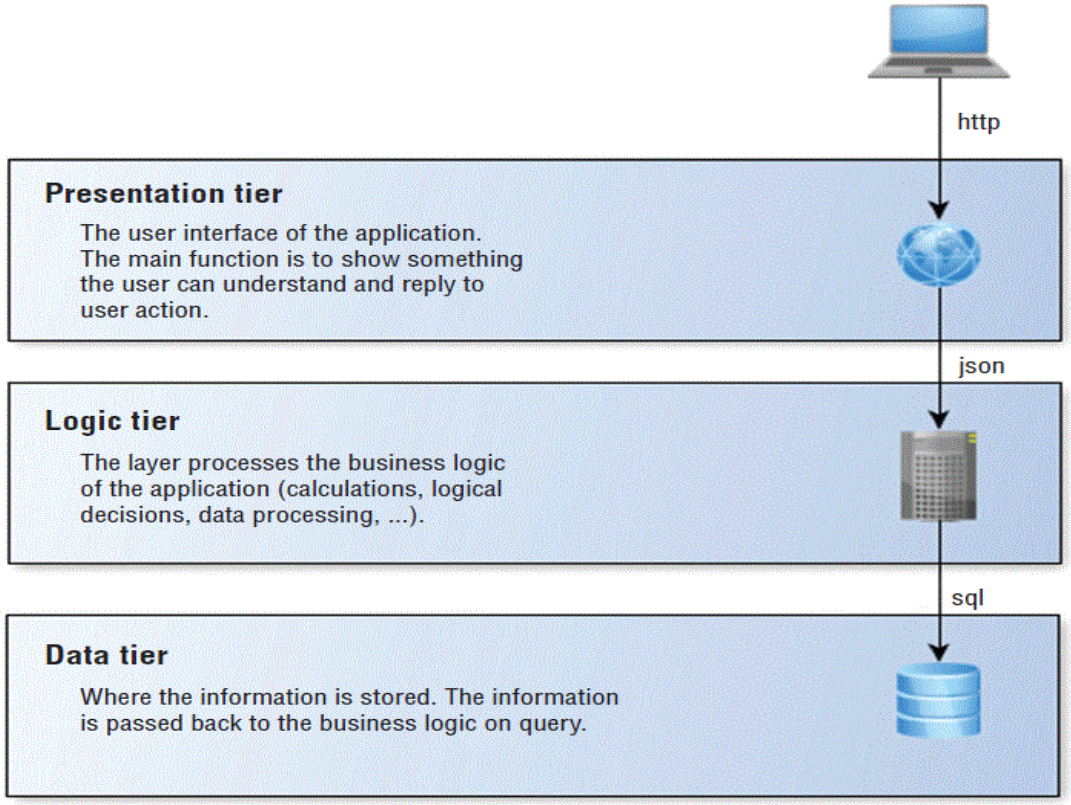
An application server is one that users connect to and then run their applications on.

In many cases this server is the middle tier in a three-tier architecture that accepts users' requests to its application and then communicates with a database server where content is stored.

Here are some of the components that should be maximized to ensure good performance in an application server:

- CPU
- NIC
- DISK
- MEMORY

Three tires


http
Presentation tier
The user interface of the application.
The main function is to show something
the user can understand and reply to
user action.
json
Logic tier
The layer processes the business logic
of the application (calculations, logical
decisions, data processing, ...).
sql
Data tier
Where the information is stored. The information
is passed back to the business logic on query.

Other Server

A Directory Services Server is one that accepts and verifies the credentials of users.

A Database Server is one that runs database software such as SQL Server or Oracle.

File servers are used to store files that can be accessed by the network users.

Print servers are used to manage printers, and in cases where that is their only role, they will manage multiple printers.

Mail servers run email server software and use SMTP to send email on behalf of users who possess mailboxes on the server and to transfer emails between email servers.

A server running Windows Routing and Remote Access Service (RRAS) can act as a remote access (dial-up) and virtual private network (VPN) server, while it is also able to act as a router.

Cont...

Dynamic Host Configuration Protocol (DHCP) servers are used to automate the process ofproviding an IP configuration to devices in the network.

Domain Name System (DNS) servers resolve device and domain names (website names)to IP addresses, and vice versa.

Proper Server Maintenance Techniques

Like all networking devices, servers need some attention from time to time.

Change Management

- All organizations need a change management process whereby every change goes through a formal evaluation process before it is implemented.

Patch Management

- we'll identify some of the types of updates that should be a part of a formal patch management policy. This policy should be designed to ensure that none of these types of updates fall through the cracks.
- **Operating System Updates**
- **Application Updates**
- **Security Software Updates**
- **Firmware Updates**
- **Device Driver Updates**

Microsoft Active Directory

Microsoft Active Directory Scope

- Understanding Directory Services
- Master "what is a domain?"
- ARBITRON.COM Domain Tree
- Domain Forests
- What is a domain controller?
- Is there a simple example of an Active Directory?
- Trust Relationships
- Users, Groups & Windows Permissions
- Practice What You Preach
- Organizational Units
- Group Policy Objects
- Why does PPM Standalone not work on Active Directory network?
- Active Directory & PPM
- So what have you learned so far?
- Apply what you have learned…
- The most important thing is…
- Questions?

Understanding Directory Services

- A ***directory*** is a stored collection of information about objects that are related to one another in some way.
- ***Network resources*** stored in a directory, also known as objects, can include:
  - File servers, printers, fax servers, applications, databases & users
- A ***directory service*** stores all information needed to use and manage these objects in a centralized location.
- The primary function of a directory is that users must be able to locate and use these objects and administrators must be able to manage how they are used.

Master "what is a domain?"

- A domain is a collection of computer, user and group objects defined by an administrator.

- These domain defined objects share common characteristics, security policies and relationships with other domains in the corporate network.

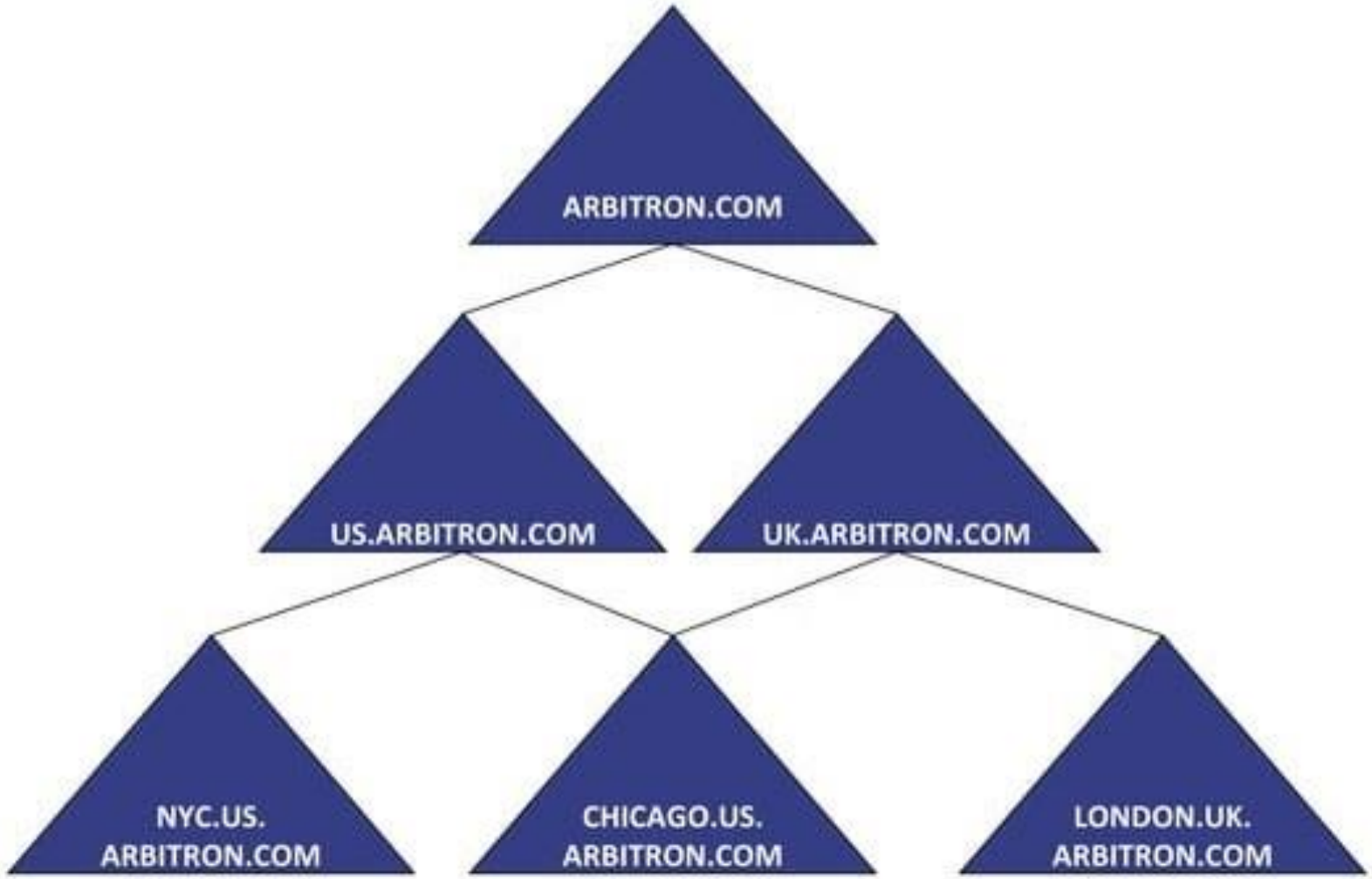
Trees

- A domain tree exists when one domain is the child of another domain. A domain tree must have a contiguous namespace, example birmingham.arbitron.com, columbia.arbitron.com

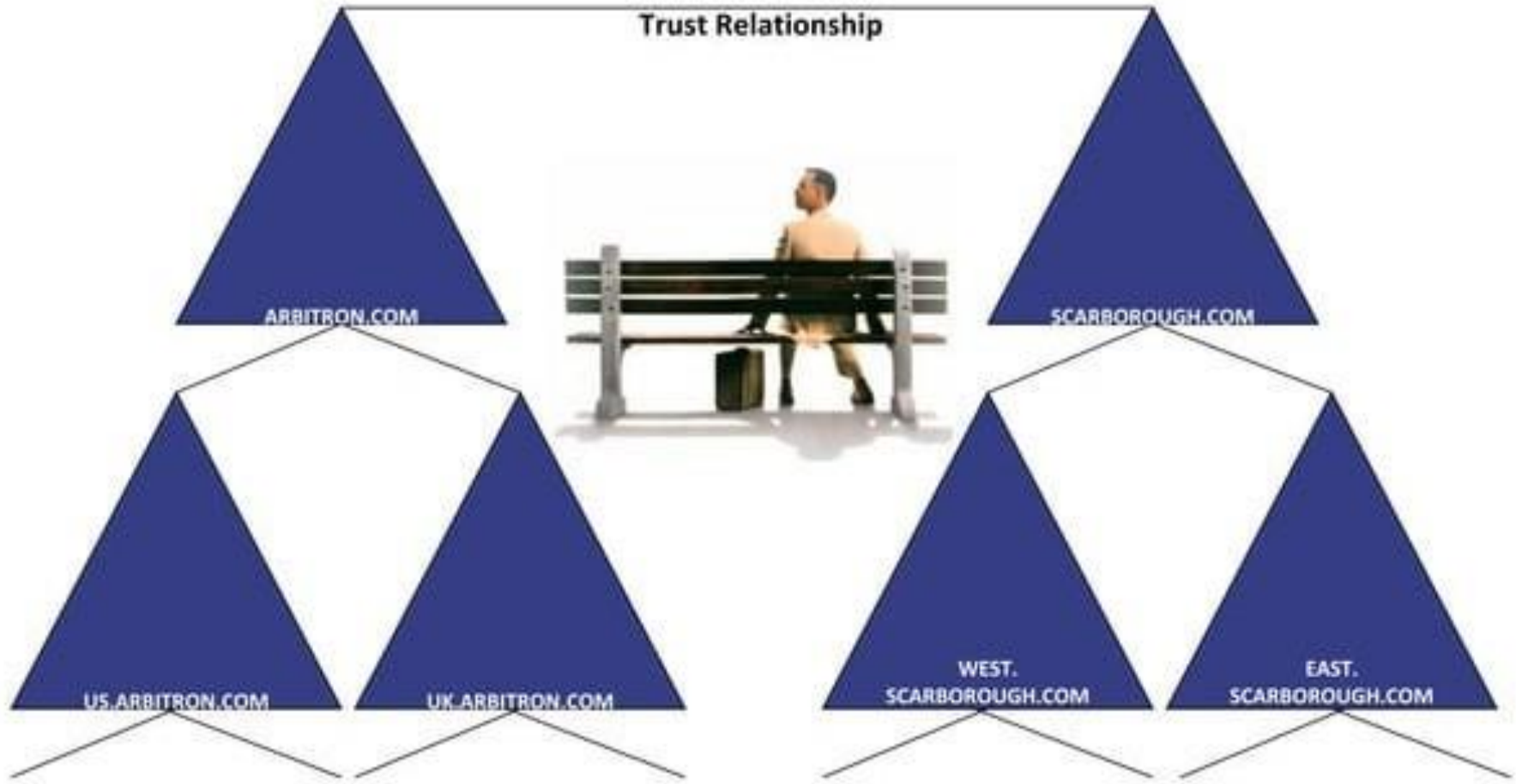
Forests

- A forest is a collection of trees that don't necessarily share a contiguous namespace, example arbitron.com, scarborough.com, insideradio.com

ARBITRON.COM Domain Tree



Domain Forests



What is a domain controller?

- A domain controller is a server that responds to security authentication requests (logging in, checking permissions, etc.) within a domain.
- Smaller companies will likely only have one domain controller whereas larger organizations will have multiple domain controllers. This allows user login requests and resources to be distributed across multiple servers and provides fault tolerance in the event one domain controller is down.
- Multiple domain controllers backup Active Directory information to each other on a periodic basis. ***Permission changes will have to be replicated to all domain controllers before all users can benefit.*** This is important if you change permissions in Chicago but the user you are working with is in Los Angeles.
- A single domain controller can manage multiple domain trees or forests.

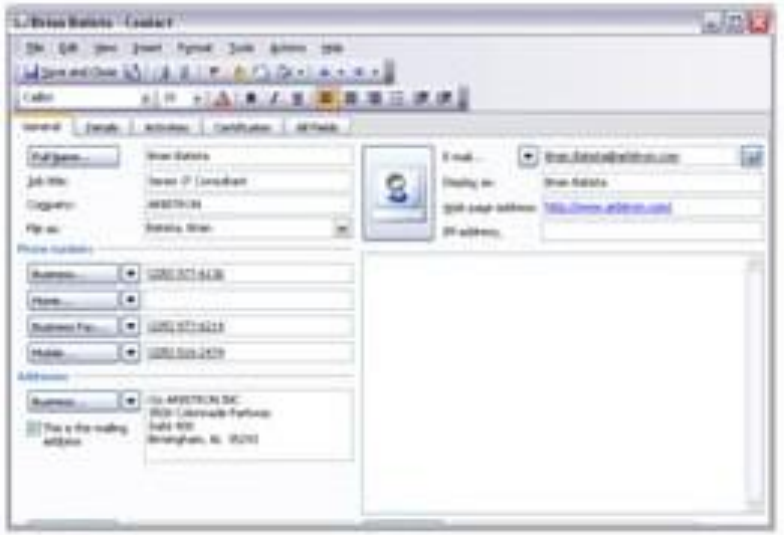
A domain controller implements the security and intrusion detection model of an organization. In short, a domain controller says…

"I am a cop, and you WILL respect my AUTHORITAH!"

Is there a simple example of an Active Directory?

- Yes, Microsoft Outlook Contacts!

- Outlook stores contact information and attributes you can search such as Name and Email address.



- Active Directory works under the same concept only with a much larger scope.

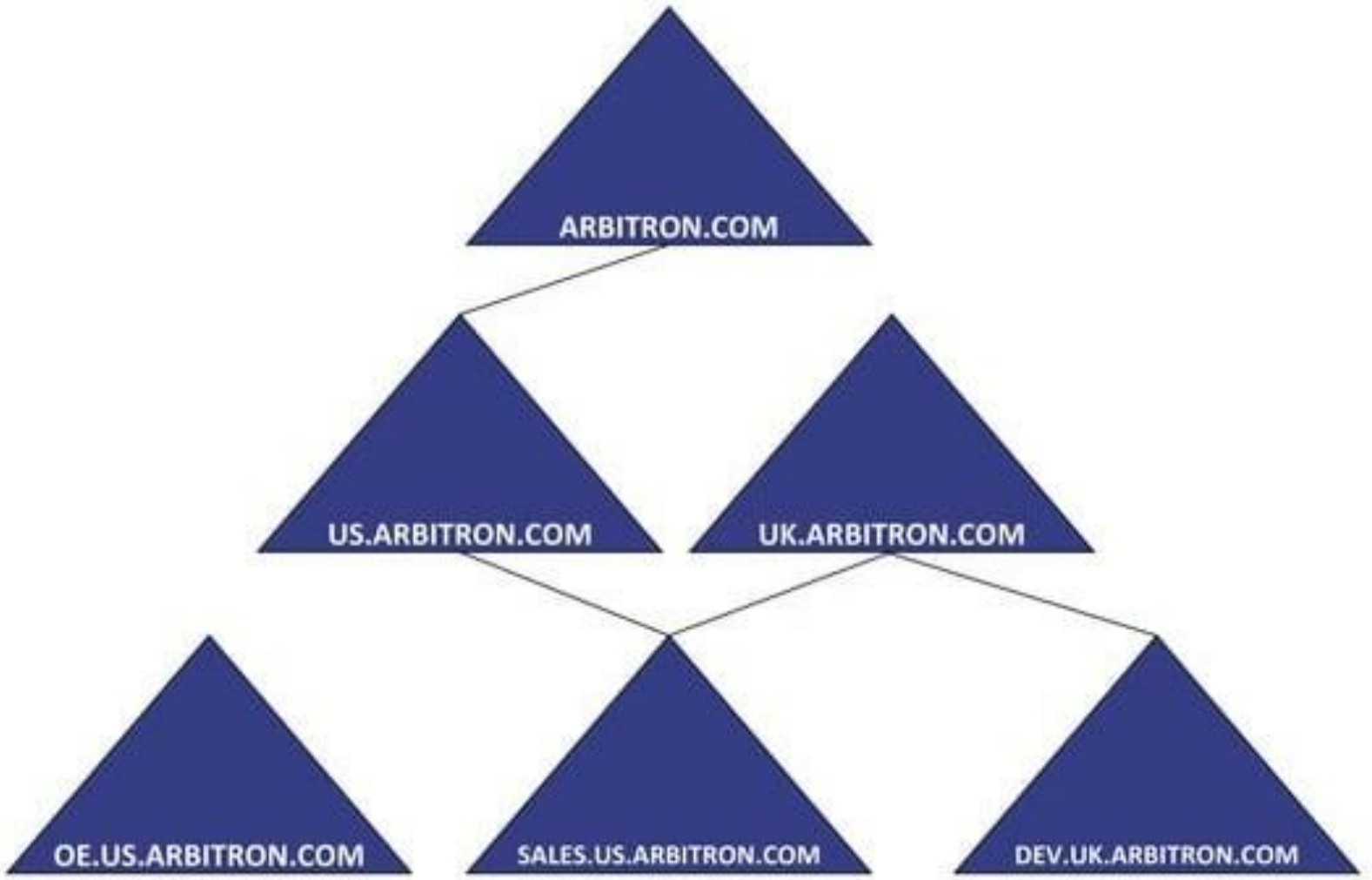
- Active Directory was designed to centralize large company networks into one repository where administrators can manage easily.

- With Active Directory users can search an infinite amount of resources without leaving their desks.

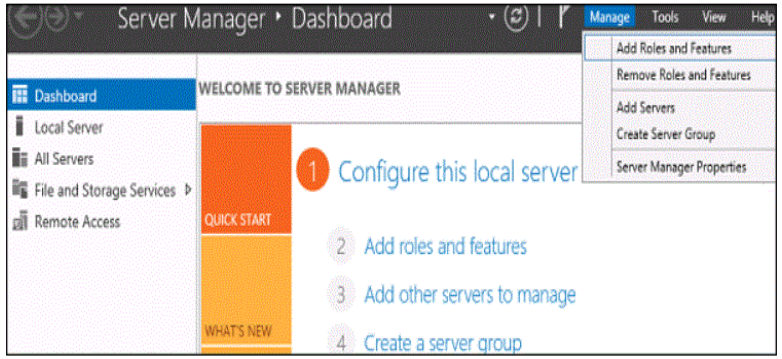
Trust Relationships

- Trust relationships between domains are how users from one domain can access resources in another domain.
- Trust relationships secure resources by grouping users and computers with like characteristics.
- A trust relationship must be established when a user from another domain needs access to your domain's resources.
- Active Directory domain trust relationships are two-way…
  - Meaning I trust you, you trust me.
- Formula to remember…
  - Domain A trusts Domain B. Domain B trusts Domain C. Therefore, Domain A trusts Domain C.

Domain Trust Relationships

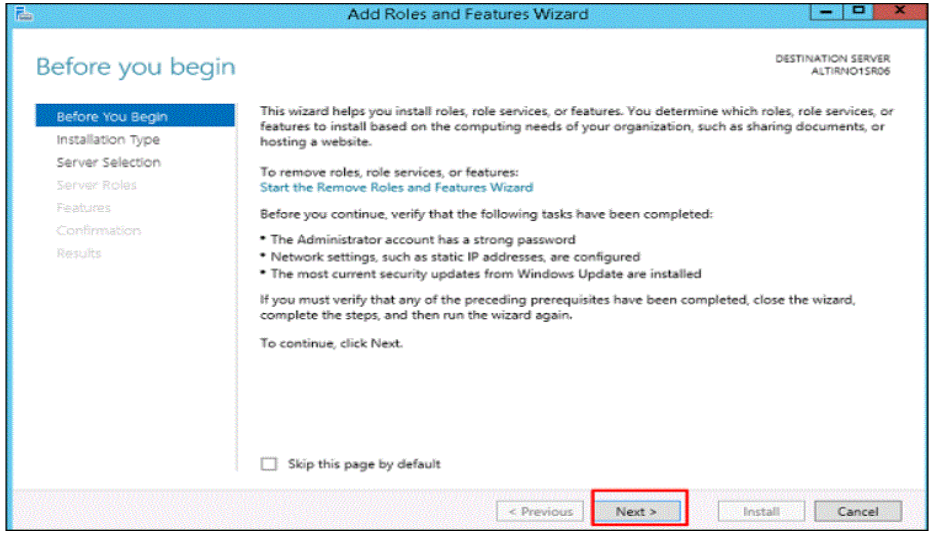


Step By Step Installation of Active Directory

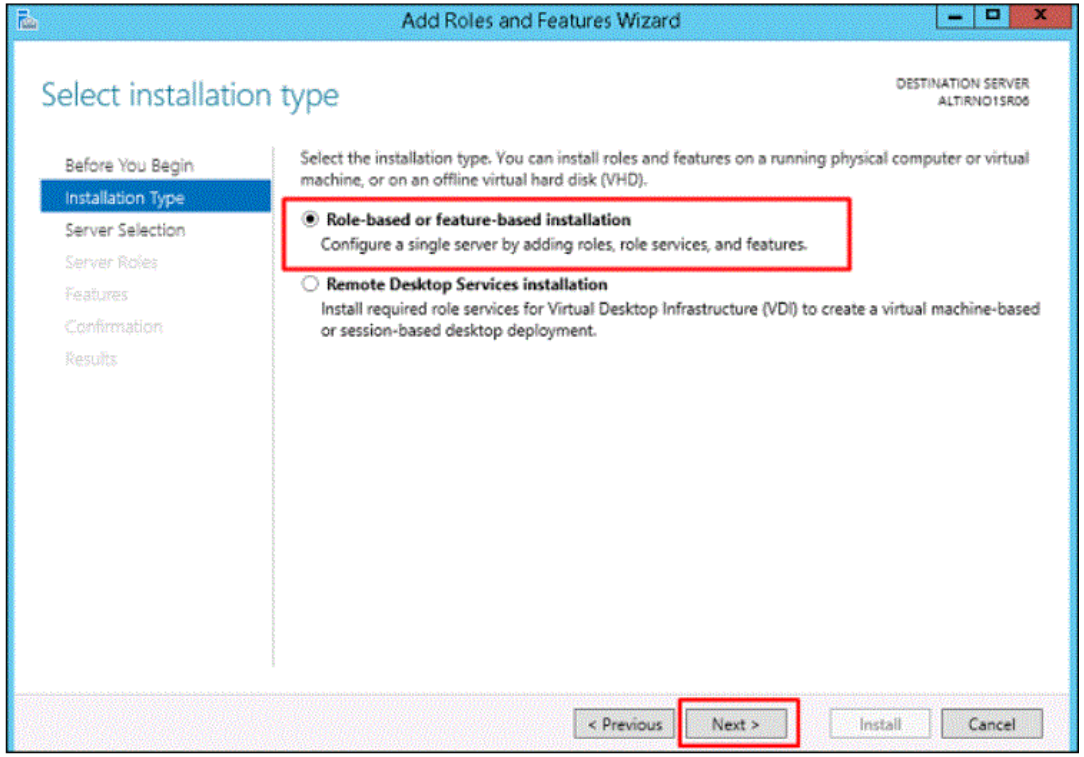


Step 1 – Go to "Server Manager" → Manage → Add Roles and Feature.

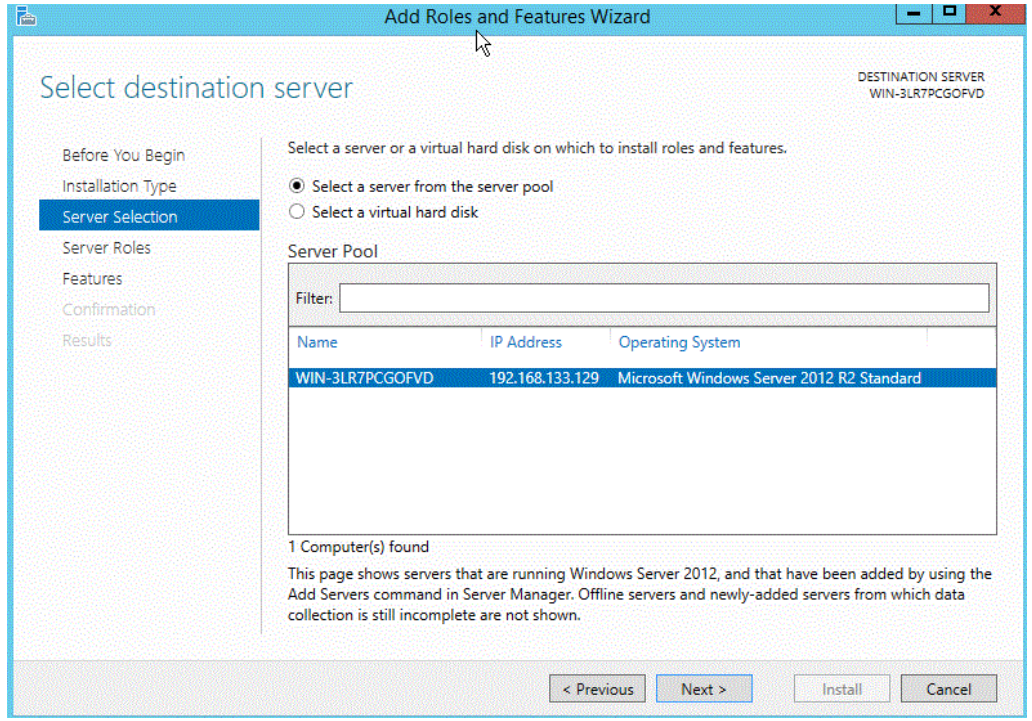
Step 2 – Click the Next button.



Step 3 – As we are installing AAD on this machine, we will select "Role-based or feature based Installation" → Next.

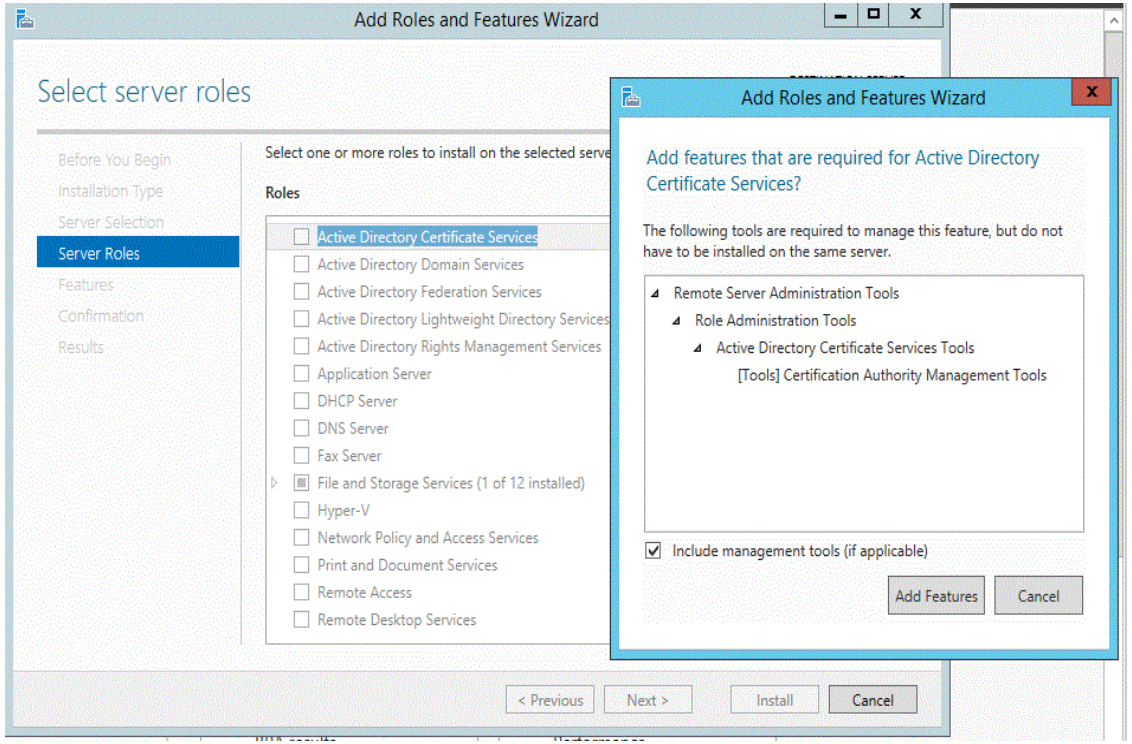


Step 4 – Click on “Select a server from the server pool”, this is the case when it will be installed locally.

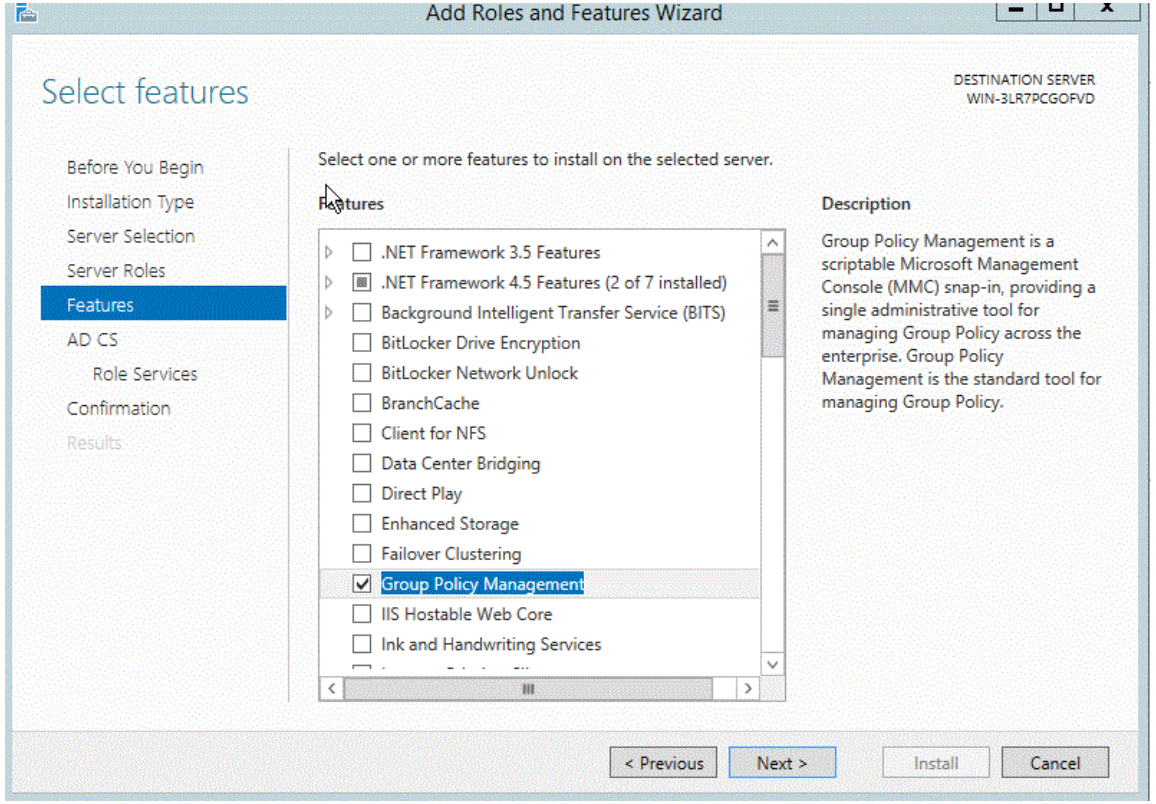


Step 5 – Check mark in the box next to **Active Directory Domain Services**. A box will be explaining additional roles services or features which are also required to install domain services.

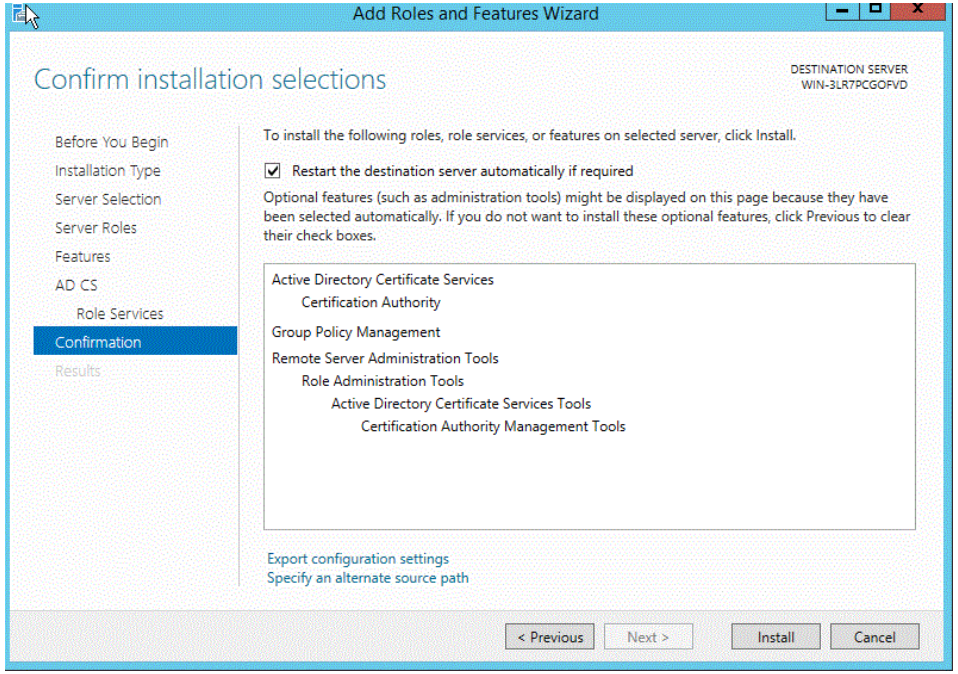
Step 6 – Click Add Features.



Step 7 – Check “Group Policy Management” → Next.

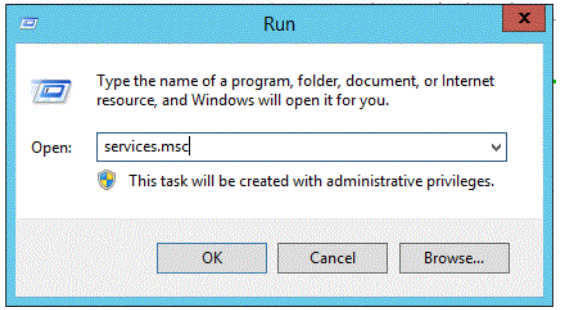


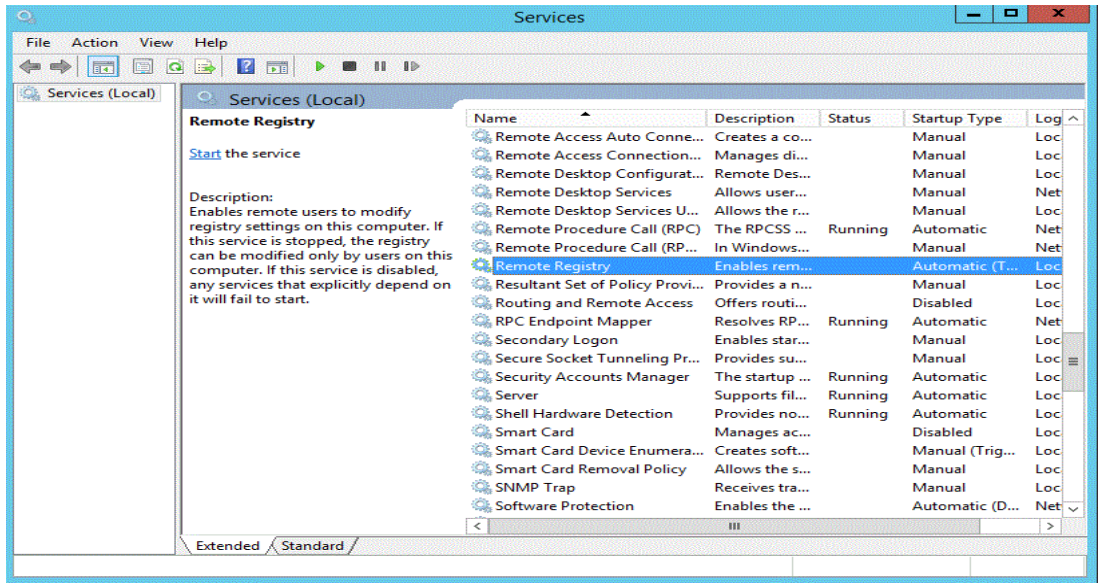
Step 8– Click “Install”.



Start the remote registry service

1. Go to START> Run then type “Services.msc”.



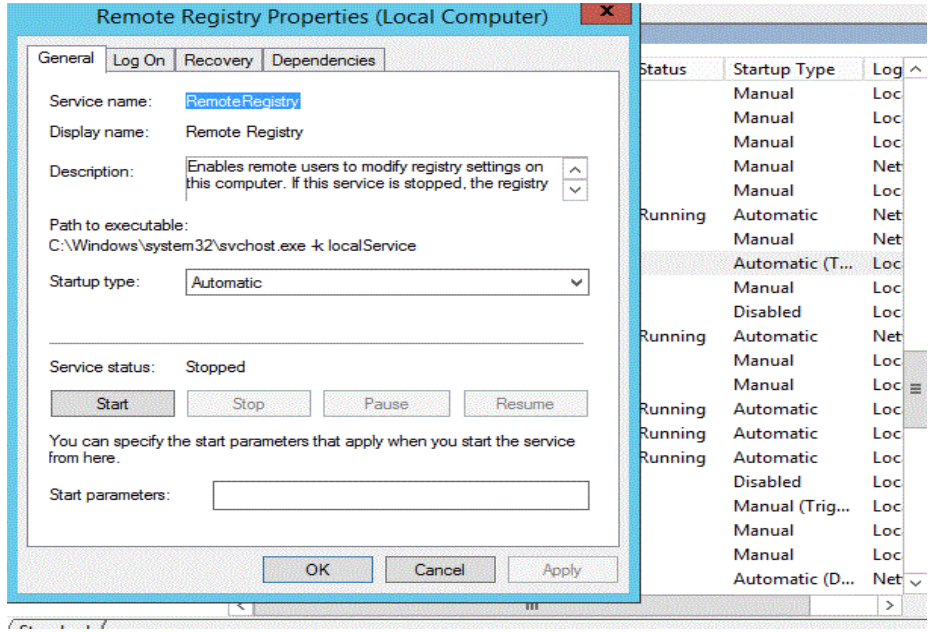


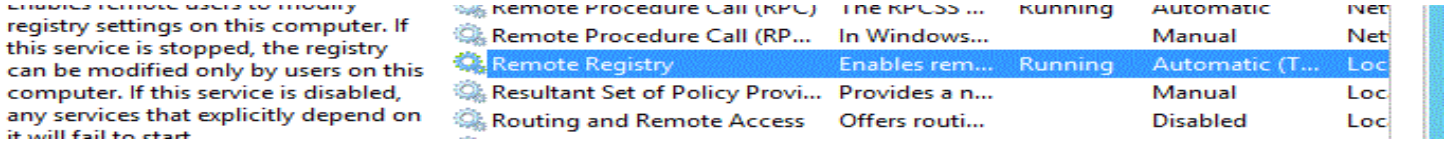
2. Right click on Remote Registry Services and then Select properties.

3. In General tab, Select Automatic from Startup Type drop-down menu.

4. Apply & Start.

5. After starting the same, Click OK.

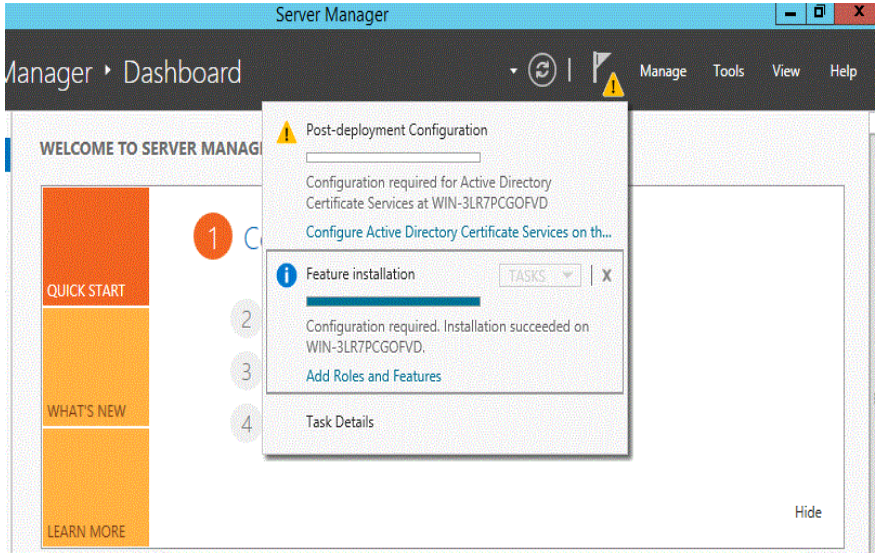




Configure Active Directory

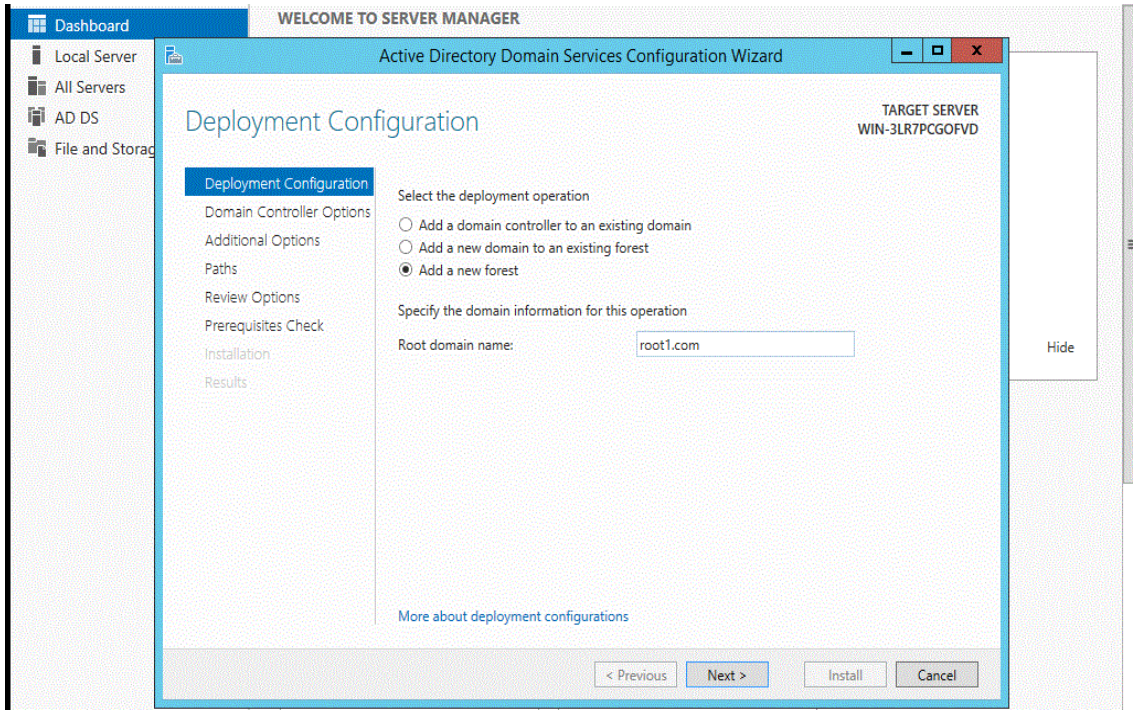
After you have installed the AD DS role, you must configure the server for your domain by using the following steps:

1. From the task bar, click Open the Server Manager.
2. Select the yellow notifications icon in the top navigation bar of the Server Manager window.
   - The Notifications Pane opens and displays a Post-deployment configuration notification. Click the Promote this server to a domain controller link that appears in the notification.



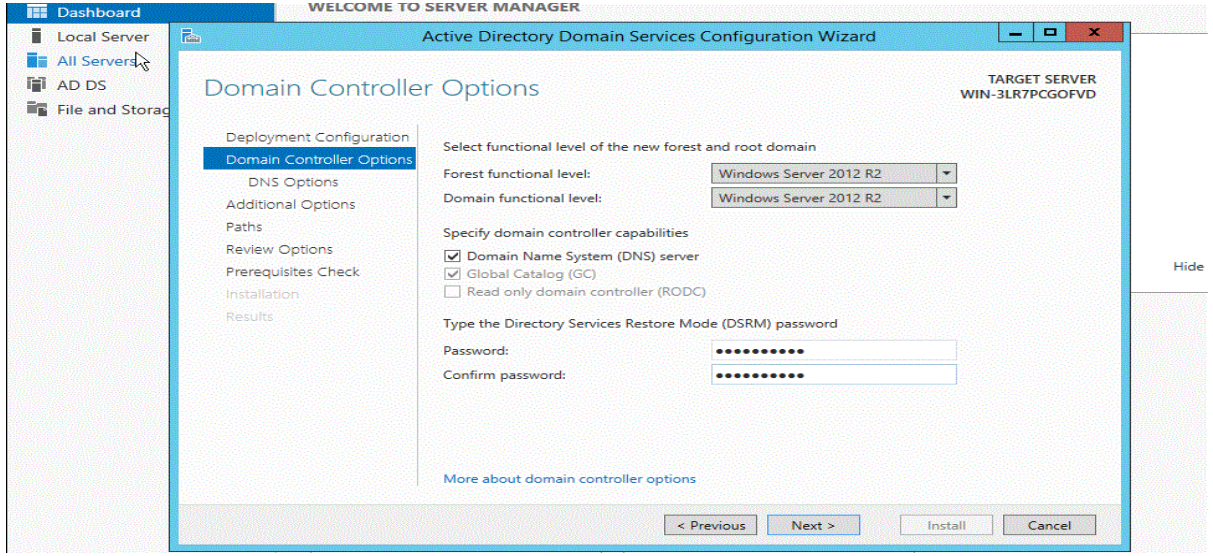
3. From the Deployment Configuration tab, select Radial options > Add a new forest. Enter your root domain name in the Root domain name field and click Next.

4. Select a Domain and a Forest functional level.



Note: These selections affect features and server domain controller eligibility. For further information on domains and forest functional levels, see the official Microsoft documentation.

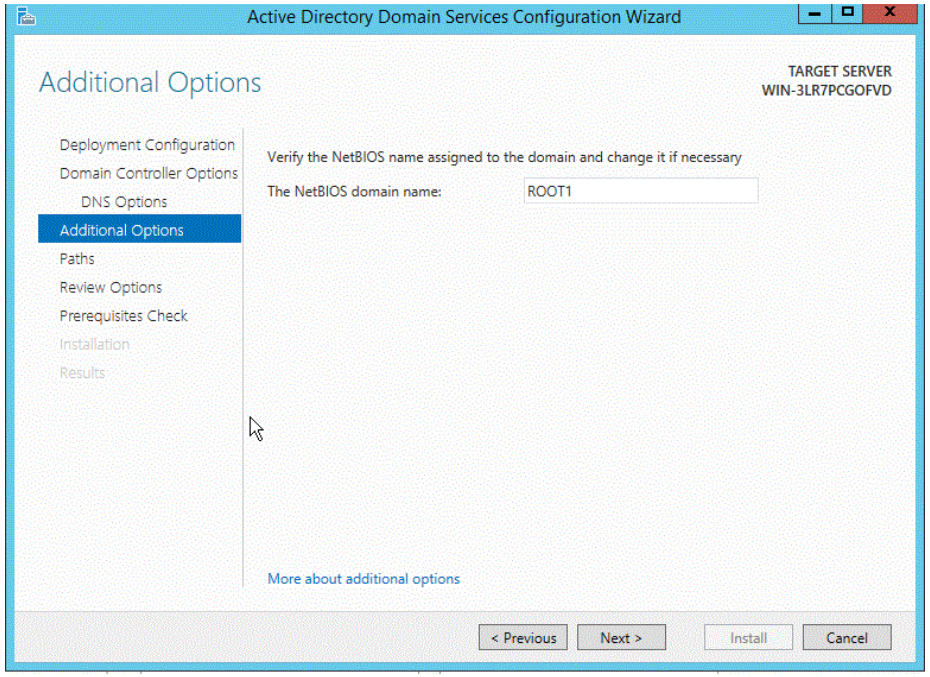
Enter a password for Directory Services Restore Mode (DSRM) in the Password field.



Note: The DSRM password is used when booting the Domain Controller into recovery mode.

5. Review the warning on the DNS Options tab and select Next.

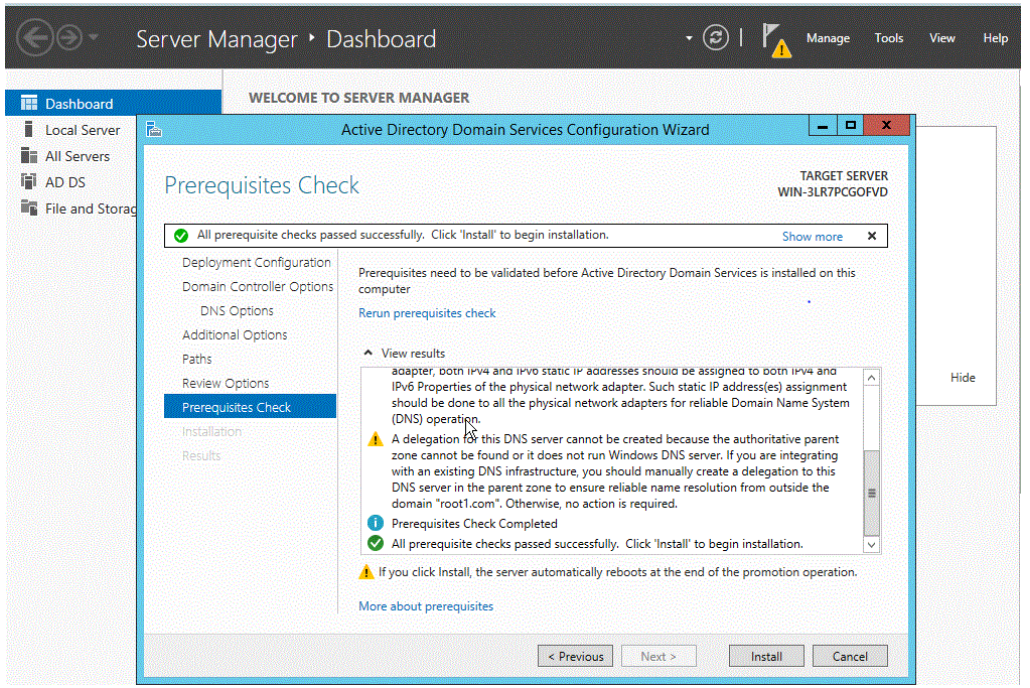
6. Confirm or enter a NetBIOS name and click Next.



7. Specify the locations of the Database, Log files, and SYSVOL folders, then click Next.

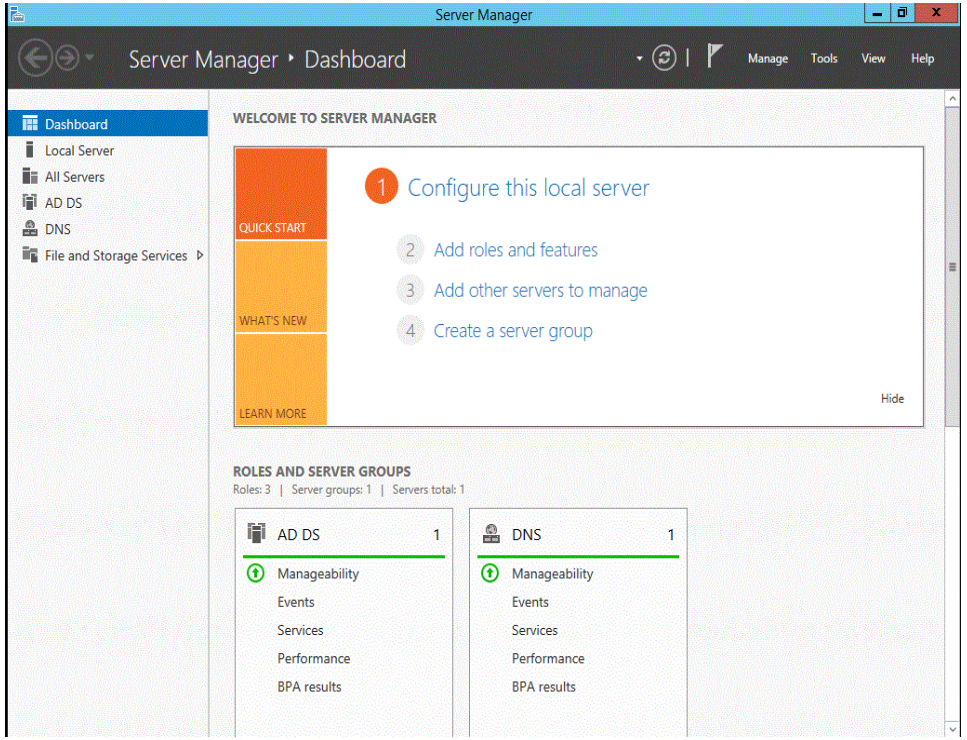
8. Review the configuration options and click Next.

9. The system checks if all of the necessary prerequisites are installed on the system. If the system passes these checks, click Install.



Note: The server automatically reboots after the installation is complete.

10. After the server reboots, reconnect to it by using Microsoft Remote Desktop Protocol (RDP).



Users, Groups & Windows Permissions

- User accounts
  - Represent each user that has access to login to a network

    Users must have an account/password created for them before they can login and access network resources.
- Group accounts
  - Provide access to resources for users who share common functions or geographic locations

    Individually granting users access to resources in unrealistic in large environments. Adding users to a group is the easiest way to grant access without having to create permissions each time. If the user leaves or no longer needs the resource simply remove the user from the group.
- Users can be members of multiple groups in Active Directory
  - Permissions in Windows networks are applied as *"most restrictive first"*

    If Dexter is a member of the PPMAT group that allows access to the PPM folder and is also a member of the Guests group that is denied access to the PPM folder he will not be able to access the PPM folder.

Uses of Active Directory Groups

Simplify Administration

To simplify administration by assigning share (resource) permission to groups rather than individual users in the active directory. When you assign permission to a group, all its members have the same access to the resource

Delegate Control

To delegate the control by assigning user rights to a group using Group Policies. In the future, you can add new members to the group who need the permission granted by this group.

Create Distribution List

One of the major use of groups with in active directory service is to create email distribution lists.

Domain Groups

The two Domain Groups consist of Security groups and Distribution groups and within these two groups we have three group scopes

Security Groups

Used with care, security groups provide an efficient way to assign access to resources on your network. Security groups have two main functions:

- Assign User Rights
- Grant Permissions to Resources

Distribution Groups

Distribution groups are designed to be used for e-mail specifically and cannot be granted Windows permissions.

Group Scopes in Active Directory

Universal Group

It can contain users and groups (global and universal) from any domain in the forest. Universal groups can be a member of domain local groups or other universal groups but NOT global groups.

Global Group

It can contain users, computers, and groups from same domain but NOT universal groups. It can be a member of global groups of the same domain, domain local groups or universal groups of any domain in the forest or trusted domains.

Domain Local Group

It can contain users, computers, global groups, and universal groups from any domain in the forest and any trusted domain, and domain local groups from the same domain. It can be a member of any domain local group in the same domain.

Universal Groups vs Domain Local Groups vs Global Groups

	Domain Local Groups	Global Groups	Universal Groups
Memberships	• Can contain users from any domain • Can contain Global groups from any domain • Can contain Universal groups from any domain • Can contain Domain Local groups but only from the same domain	• Can contain users from the same domain • Can contain Global groups from the same domain	• Can contain users from any domain within the forest where this Universal Group resides • Can contain Global groups from any domain within the forest where this Universal group resides • Can contain Universal groups from any domain within the forest where this Universal group resides
Permissions	• Permissions can only be assigned to members inside the domain	• Permissions can be assigned in any domain	• Permissions can be assigned in any domain or forest
Forest-Wide Replication	• Domain Local groups do not trigger forest-wide replication on any change in group memberships	• Global groups don't trigger forest-wide replication on any change in group memberships	• User accounts should not be added directly into a Universal group, as it triggers forest-wide replication on each addition and removal
Scope	• Can be perceived as resource groups to provide access to the domain	• Can be perceived as account groups primarily used to group users in the same domain	• Can be perceived as both resource and account groups
MemberOf	• Cannot be made a member of Global groups	• Can be made members of Domain Local groups to share the respective access to resources	• Can be a member of any group type in the forest.
Converted Into	• Can be converted to a Universal group (if no other Domain Local group exists as a member)	• Can be converted to a Universal group (if the group is not a member of any other Global group)	• Can be converted to a Domain Local group or a Global group (if no other Universal groups exist as members)

Users

One of the key points for using Active Directory is the users management. Every organization manages its users in different ways, setting for them name formats, assigning different permissions, etc.

Practice What You Preach!

- Aaron is an Radio Sales member at the *Best Freakin Radio Company Ever*. He belongs to the following Active Directory groups at his company:
  - PPMApps
  - Finance
  - HR_1
  - Remote Users
- *Best Freakin Radio Company Ever* had a network virus earlier in the week. The network was taken down as a security measure to prevent additional computers from becoming infected.
- Aaron has called Arbitron to say he cannot access the PPM folder or software on the *Applications* server due to an "Access is denied" error.
- What suggestions can you offer Aaron that may help him solve his issue?

Organizational Units

- Organizational Units (OU's) allow resources with common attributes such as access to resources to be managed and secured simultaneously.

- OU's group resources together that have similar permissions, access levels and functions such as…
  - The ***Finance*** OU contains users who need access to resources on the FINANCE1 server
  - The ***Sales*** OU contains users and printers that only the Sales department needs access to.
  - The ***Human Resources*** OU contains users who need access to the HR1 server exclusively since it contains payroll data and social security numbers.

- OU's could also organize resources by geographic location:
  - Birmingham

    Paul Dunlap, Chris Felder, Maria Petrey, Ted Frankenfield, Kelly Duvall, Tasia Martin, Tara Ward, BHMPrint01, BHMServer1
  - Columbia

    Dexter Beane, Nick Leaf, Allen Scott, CMBPrint, Nancy Pivec, CMBServer3

Group Policy Objects

- Group policy governs how a user is able to use Windows.
- Local application behavior is also governed with group policy such as local system services like PostgreSQL.
- Group policy objects are applied to Organizational Units in the Active Directory by an Administrator.
- When a user logs in the group policy settings are applied to all Active Directory objects in the OU the policy is applied to.

Questions?