GLOBAL
University

Final Year Project Report

Full Unit – Final Report

Building a Heterogeneous LAN

Yehya Bassam Mneimne

A report submitted in part fulfilment of the degree of

BS in Computer Science

Supervisor: Dr. Ahmad Hammoud

Department of Computer Science
Global University

Aug, 12 2016

Declaration

This report has been prepared on the basis of my own work. Where other published source materials have been used.

Table of Contents

Abstract

This word document serves as what was needed for my senior project. Building a LAN with all requirements was a challenging project, taking into consideration that some prerequisite courses for fulfilling my senior are not taken yet, Like Network Infrastructure and MCP 1.

Project Specification

This report show how the project was accomplished, what are the problems faced, and how problems were solved. The following are the main points to accomplish the senior project.

- Formatting and installing latest version of Windows Server
- Installing and configuring latest version of MS Exchange Server
- Installing and configuring latest version of MS SQL Server
- Implementing a RAID 1 solution
- Primary Domain Controller (This server will go off due to hard disk failure)
- Backup Domain Controller (This server should be promoted to replace PDC)
- IP tables will be used as a firewall to control what protocols are allowed. For example:
    - users should not be able to reach the SQL Server using \\
    - users should be able to contact SQL server to run a query and get result
    - users should be able to access the shared folder
- Shared Folder where users store their files
    - Who can do what
- Implementing a Group Policy:
    - If any user added himself to any local administrators group at any computer that joined the domain, he/she will be removed automatically
    - Whenever a user logs in, s/he will find a drive Z that points to his/her shared folder
- Formatting and installing any version of Linux. A user using this Linux machine should be able to access his/her shared folder, after supplying his/her credentials
- Allowing users to reach internet, using their client machines. PDC is the only server attached to internet
- Installing DHCP & DNS on the PDC
- Installing a web server behind the firewall and allowing users to reach it using https (not http) to make sure the communication is encrypted. Windows Server should be used to issue a certificate. Then, this certificate will be applied to the web server

- Installing an open-source antivirus package
- Installing a wireless solution.
- You buy a small router (very cheap one), you give it internet, then you allow domain users to use internet
- Allowing users to connect to the server using remote desktop. Use Microsoft Load Balancer, which is a server that will receive all requests from users and redirect the user to the least busy server.

Project’s Content:

This report includes steps that were taken to accomplish specific goals. Every step is explained briefly to better understand the project.

- **Normal** – the style for the basic text of the document. Times New Roman font 11
- **Project Title** – the title style.
- **Heading 1, Heading 2, Heading 3** – styles for different levels of section headings.
- **Figure** – the style for a figure or table caption.
- **Code** – the style for program source code.
- **Bulleted List** – the style for a standard bulleted list such as this one.
- **Numbered** – similar to the bulleted list style except that the list is numbered.
- **Italics** – the style used to stress a specific element, or description of a figure.

Introduction

As s senior student, I was asked for a final project to complete my academic study in the university. Being an Information Technology student focuses on aiming to improve and learn as much as possible; Technology is always improving and updates are frequent.

Since depending on university courses was not enough, establishment of a self-educating environment was a priority and needed. This project taught me missing links I couldn’t learn by my own, they were captured through teaching session in class. A teacher once said to IT students: “You should always protect a network. To that you should assign a Linux Firewall with static configuration so that you, as an admin, have full control over the packets”. But the question is how-to?

Technical skills are gained, not learned. Before entering college, it’s crucial to learn more. Someone said, to master the field you should:

1. Know the concise definitions.
2. Know the functionality.
3. Know the purpose of its presence.

In other words, some self-minor studies alone was accomplished. This action helped me later, especially in mid-year college; I already have enough background information. Although these information are beneficial, the academic study shall not be underestimated, where learning occurs.

In mid-year college, I learned new things I never knew, like programming, Firewall configuration, and domain controller related tasks. This project will work as a one-unit study and revision for all what was covered throughout my years.

What is the Project?

The project is mainly building a LAN with full requirements. This scenario can be applied on all start-up companies, where most companies need an internal infrastructure domain connected network. First, a PDC (Primary Domain Controller) that acts as the main controller of the network, the backbone of the network, where maximum bandwidth, system resources, and protection is needed. PDC will concatenate all elements together, will be called later in this report as **objects** just to be more jargon-oriented and terminology related. Object can be users, computers, other DCs (Domain Controllers).

The PDC should always be available for service. For this use, an SDC (Secondary Domain controller) is implemented to perform backup operations and to maintain availability. A SDC can be any version of Windows Server. Users’ and Computers’ actions are monitored in a controlled manner. To help improve this control, a Linux Firewall is added to act as a routing point between the end-users and the DCs. Moreover, GPOs (Group Policy Objects) are implemented to OUs (Organizational Unit) to provide more and complex computer settings under the scope of security.

Project Environment and Resources:

Initially, the project was given to be done in one of the labs, where system resources are separated and won't be a barrier. However, this action is strictly violating the university policy, since these computers have explicit access to the university domain and this could be a security breach. A similar, stand-alone and proper environment was asked for implementing the project specifications and avoiding bottlenecks and lack in system performance. My proposal was not accepted, so the situation came to find my way out by using my own PC as a project environment with minimal implementation and system requirements.

Booting different operating systems on the same host is required in this scenario, so a *Virtual Machine* was installed on the local system.

Product: VMware® Workstation 12 Pro

Version: 12.0.0 build-2985596

Status: Licenced

Expiration: No expiration

VMware is a software that allows the host machine to split the physical server into multiple virtual machines. These machines can be any official operating system like Windows, Linux, Ubuntu, and Netware. "*All of which can be used concurrently on the same hardware*"[1]. Each virtual machine has its own unique settings.

[1] techtarget. (n.d.). *SeachVMware* . Retrieved from http://searchvmware.techtarget.com/definition/VMware-Server

Resources:

PDC Resource

As mentioned before, PDC should maintain availability, so it's recommended to reserve the highest proportion of the host machine. In the project the PDC's resources are:

- 2 GB of RAMs DDR3
- 2 CPU processors
- 60GB SCSI hard disk 1
- 2GB SCSI hard disk 2(RAID1)
- 2GB SCSI hard disk 3 (RAID1)
- NAT network adapter (Internal)
- NAT network adapter (External)

RAID1 and redundant network adapter

Using three hard disks was part of the project, as it will be discussed it later. However, I choose to add another NAT (Network Address Translation) to insure that PDC is separate from the local area network–for security reasons.

Firewall Resources

The Firewall in this scenario has limited functionality; filtering packets. Such system should not have an excess in resources, the following are used and recommended[2]:

- 1 GB of RAMs DDR3
- 1 CPU processors
- 20 GB SCSI hard disk 1
- NAT network adapter (Internal)
- NAT network adapter (External)

Note: The firewall should always have a minimum of two separate network adapter, to provide routing.

[2] pfSense. (2016). *Choose your hardware*. Retrieved from pfsense: https://www.pfsense.org/hardware/

Domain users’ Resources:

Running three different virtual machines on the same host will be an overhead, so Windows users will have the minimum resources, and the following are used:

- 1 GB of RAMs DDR3
- 1 CPU processors
- 20 GB SCSI hard disk 1
- NAT network adapter

Domain users are the end-user of the network, this implies that one network adapter is needed to establish a connection. The Network address is 192.168.74.0/24. Later on, I will explain the IP distribution to every user, and that is when a DHCP (Dynamic Host Configuration Protocol) was added to the network, so the users are no longer choosing an IP within the full range 0~254.

Project Implementation

This part of the report describes the procedure of my project in a serial manner.

Installing Latest version of Windows Server

Windows Server 2012 R2 brings many services into infrastructure with features and enhancements in virtualization, management, storage, networking, virtual desktop infrastructure, access and information protection, and the web and application platform. (Dan Holme, 2008;Stanek, 2008)

Nowadays, Windows Server 2016 will be released. Few months ago, when starting the project, Windows Server 2016 was not published yet, however, Windows Server 2012 R2 was available with new features and role that wasn't available on Windows Server 2008.

What is SQL Server

SQL server is a suite of software, and a product name as well. SQL server is a relational database system (RDBMS). It is used to store and manage data. Within this software, data is stored within tables. Data is stored is Tables consisting of columns and rows. Tables can be linked, or "Related", to one another. Tables and objects that belong to the same family or require similar security are collectively stored in a Database. (Microsoft Developer Network, 2016; Ramez Elmasri, 2004)

Installing Latest version of SQL Server

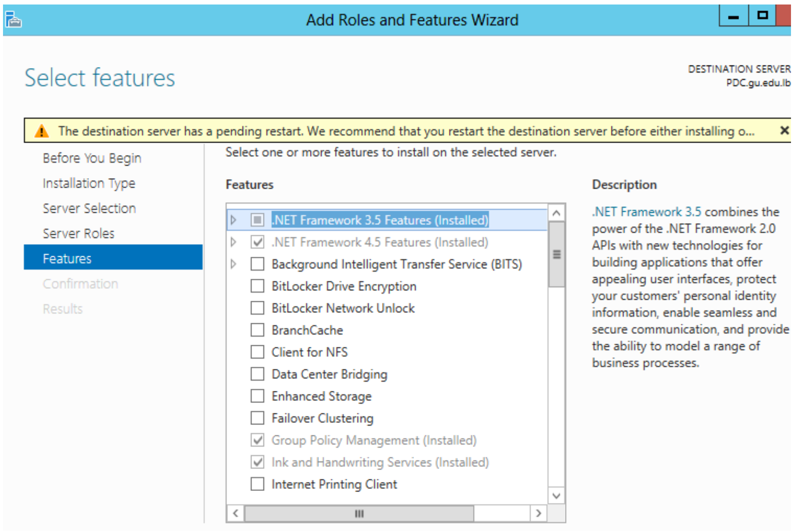
For both 32-bit and 64-bit editions of SQL Server 2014, the following considerations apply:

- Computers with the NTFS file format

- SQL Server Setup will block installations on read-only, mapped, or compressed drives

Prerequisite installation of .NET Framework 3.5 and .NET Framework 4.5.

First, SQLEXPR_X64_ENU.exe 135MB was downloaded. To install SQL, first install the database engine. The database engine is a core service for storing, processing and securing data. It provides controlled access and rapid transaction processing to meet the requirement most application data within the enterprise.



Select features

DESTINATION SERVER
PDC.gu.edu.lb

⚠ The destination server has a pending restart. We recommend that you restart the destination server before either installing o... ✕

Select one or more features to install on the selected server.

Features

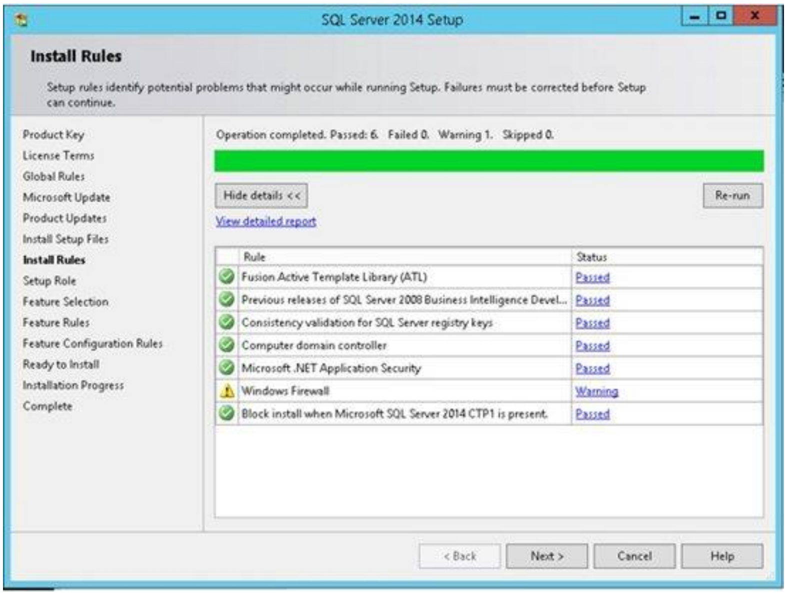
- ■ .NET Framework 3.5 Features (Installed)
- ☑ .NET Framework 4.5 Features (Installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache
- ☐ Client for NFS
- ☐ Data Center Bridging
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☑ Group Policy Management (Installed)
- ☑ Ink and Handwriting Services (Installed)
- ☐ Internet Printing Client

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.

Figure 1. Add Roles and Features Wizard

Feature	**Diskspace requirement**
Database Engine and data files, Replication, Full-Text Search, and Data Quality Services	811 MB
Analysis Services and data files	345 MB
Reporting Services and Report Manager	304 MB
Integration Services	591 MB
Master Data Services	243 MB
Client Components (other than SQL Server Books Online components and Integration Services tools)	1823 MB
SQL Server Books Online Components to view and manage help content[1]	375 KB



Install Rules

Setup rules identify potential problems that might occur while running Setup. Failures must be corrected before Setup can continue.

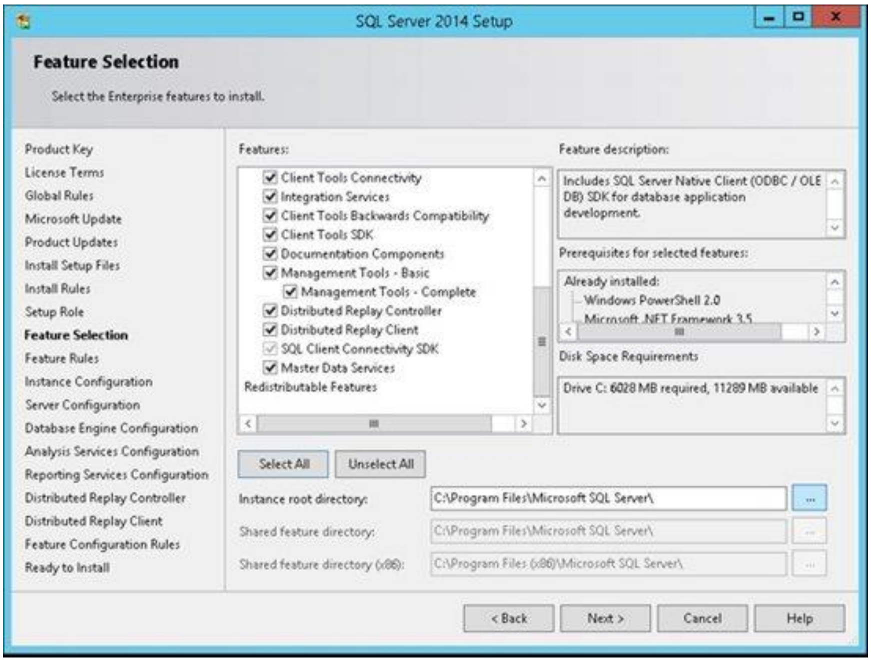
Operation completed. Passed: 6. Failed 0. Warning 1. Skipped 0.

	Rule	Status
✓	Fusion Active Template Library (ATL)	Passed
✓	Previous releases of SQL Server 2008 Business Intelligence Devel...	Passed
✓	Consistency validation for SQL Server registry keys	Passed
✓	Computer domain controller	Passed
✓	Microsoft .NET Application Security	Passed
⚠	Windows Firewall	Warning
✓	Block install when Microsoft SQL Server 2014 CTP1 is present.	Passed

Figure 2. Rules' Installation

The SQL Server installation program checks the machine to make sure it meets the hardware and software requirements to install SQL Server. If you get any Errors in the results, SQL installation wizard cannot continue.

In *figure 3*, you can choose what features to install. It is highly recommend not to choose all the features on a production server if you don't need them. Choose only the features that you need or might need. Conversely you might want to select all using a development server in order to give you more flexibility in the development environment. Once you choose to use another feature you will be able to add it in production later on.



SQL Server 2014 Setup

Feature Selection

Select the Enterprise features to install.

Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Setup Role
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Analysis Services Configuration
Reporting Services Configuration
Distributed Replay Controller
Distributed Replay Client
Feature Configuration Rules
Ready to Install

Features:

- ☑ Client Tools Connectivity
- ☑ Integration Services
- ☑ Client Tools Backwards Compatibility
- ☑ Client Tools SDK
- ☑ Documentation Components
- ☑ Management Tools - Basic
  - ☑ Management Tools - Complete
- ☑ Distributed Replay Controller
- ☑ Distributed Replay Client
- ☑ SQL Client Connectivity SDK
- ☑ Master Data Services

Redistributable Features

Feature description:

Includes SQL Server Native Client (ODBC / OLE DB) SDK for database application development.

Prerequisites for selected features:

Already installed:
Windows PowerShell 2.0
Microsoft .NET Framework 3.5

Disk Space Requirements

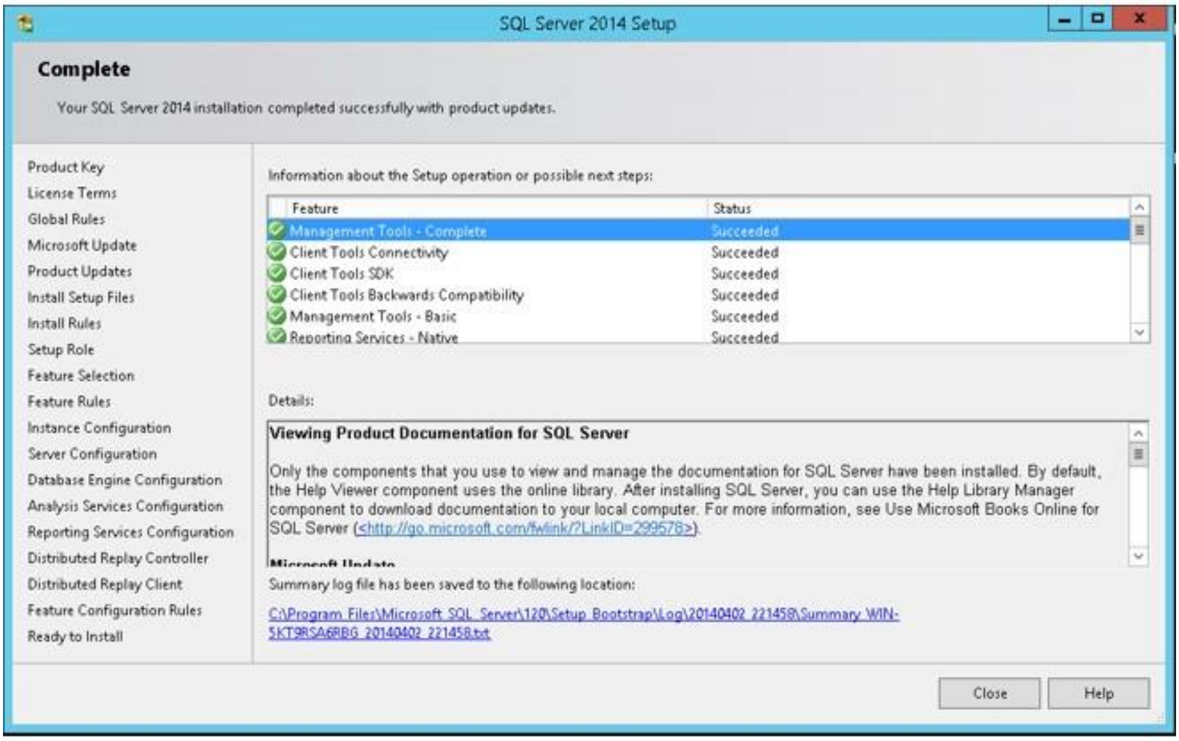
Drive C: 6028 MB required, 11289 MB available

Instance root directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

Figure 3. Feature Selection



SQL Server 2014 Setup

Complete

Your SQL Server 2014 installation completed successfully with product updates.

Information about the Setup operation or possible next steps:

Feature	Status
Management Tools - Complete	Succeeded
Client Tools Connectivity	Succeeded
Client Tools SDK	Succeeded
Client Tools Backwards Compatibility	Succeeded
Management Tools - Basic	Succeeded
Reporting Services - Native	Succeeded

Details:

Viewing Product Documentation for SQL Server

Only the components that you use to view and manage the documentation for SQL Server have been installed. By default, the Help Viewer component uses the online library. After installing SQL Server, you can use the Help Library Manager component to download documentation to your local computer. For more information, see Use Microsoft Books Online for SQL Server (<http://go.microsoft.com/fwlink/?LinkID=299578>).

Microsoft Update

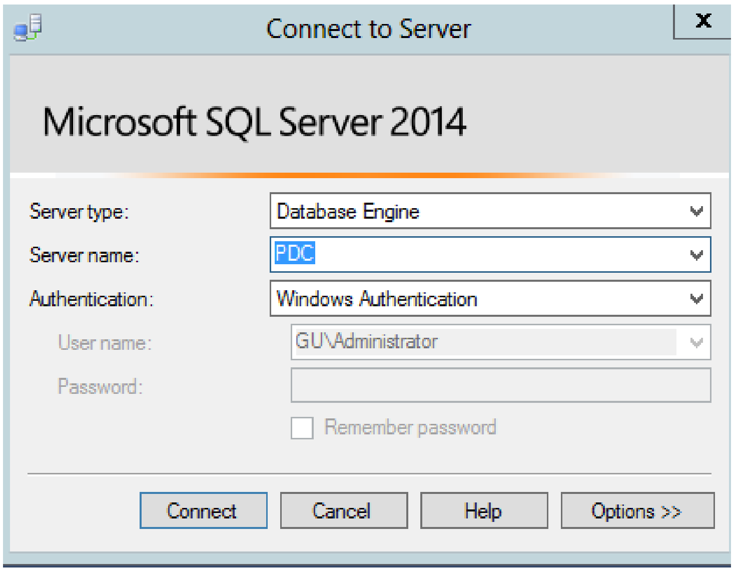
Summary log file has been saved to the following location:

C:\Program Files\Microsoft SQL Server\120\Setup Bootstrap\Log\20140402_221458\Summary_WIN-5KT9RSA6RBG_20140402_221458.txt

Figure 4. *Installation Completed*

Once the test is completed, figure 4 will show and insure the success or the failure of installing the selected features. If all test passed, then the prerequisites requirements like 4.5 Framework are already running on the system.

Finally, during this step shown in figure 5, by typing the instance name chosen previously, a successful connection will be established and the server will be ready to store data.



Connect to Server

Microsoft SQL Server 2014

Server type: Database Engine

Server name: PDC

Authentication: Windows Authentication

User name: GU\Administrator

Password:

□ Remember password

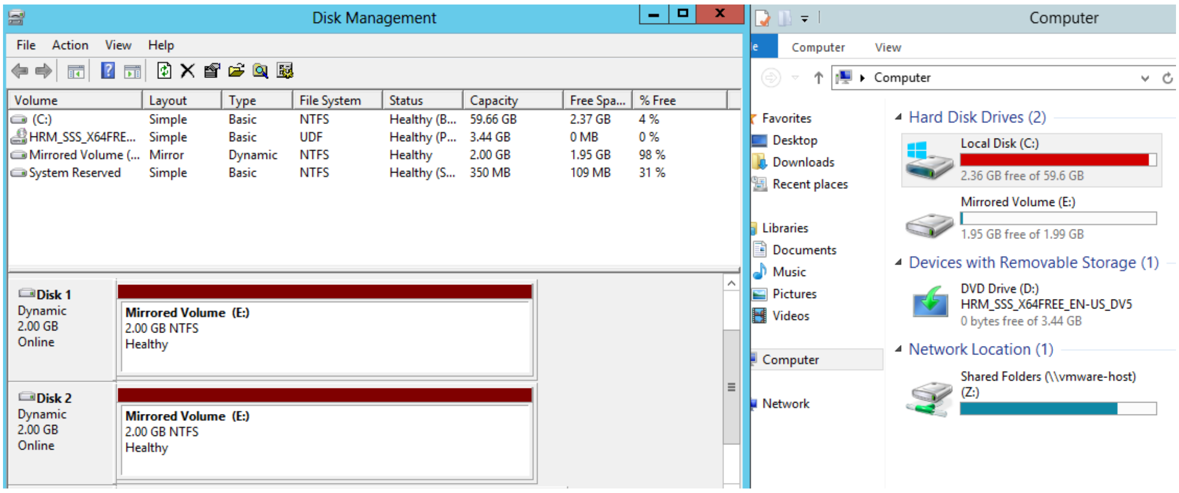
Figure 5. *Connect to instance*

Implementing Raid 1 Solution

It is a fault-tolerance configuration known as "disk mirroring." With RAID 1, data is copied seamlessly and simultaneously, from one disk to another, creating a replica, or mirror. If one disk malfunctioned, the other can keep working. It's the simplest way to implement fault tolerance and it's relatively low cost.

The downside is that RAID 1 causes a slight drag on performance. RAID 1 can be implemented through either software or hardware. A minimum of **two** disks is required for RAID 1 hardware implementations. With software RAID 1, instead of two physical disks, data can be mirrored between volumes on a single disk. One additional point to remember is that RAID 1 cuts total disk capacity in half: If a server with two 1TB drives is configured with RAID 1, then total storage capacity will be 1TB not 2TB.

How to Implement Raid 1



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	59.66 GB	2.37 GB	4 %
HRM_SSS_X64FRE...	Simple	Basic	UDF	Healthy (P...	3.44 GB	0 MB	0 %
Mirrored Volume (...	Mirror	Dynamic	NTFS	Healthy	2.00 GB	1.95 GB	98 %
System Reserved	Simple	Basic	NTFS	Healthy (S...	350 MB	109 MB	31 %

Disk 1
Dynamic
2.00 GB
Online

Mirrored Volume (E:)
2.00 GB NTFS
Healthy

Disk 2
Dynamic
2.00 GB
Online

Mirrored Volume (E:)
2.00 GB NTFS
Healthy

Hard Disk Drives (2)

Local Disk (C:)
2.36 GB free of 59.6 GB

Mirrored Volume (E:)
1.95 GB free of 1.99 GB

Devices with Removable Storage (1)

DVD Drive (D:)
HRM_SSS_X64FREE_EN-US_DV5
0 bytes free of 3.44 GB

Network Location (1)

Shared Folders (\\vmware-host)
(Z:)

Figure 6. Disk management and Computer console.

As shown in figure 6, Disk 1 and Disk 2 are the two mirrored SCSI HDD with 2GB capacity. To Implement RAID 1 the following procedure is required:

1. Boot up Windows, hit the start button, and in the search box type either "Create and" or "Disk man", and click "Create and Formant Hard Disk Partitions". This program is also accessible through Control Panel → System and Security → Administrative Tools → Create and Formant Hard Disk Partitions.
2. If these drives have never been used, it may ask you to initialize them, in which case you'll most likely be using "MBR"(Master Boot Record).
3. If the new disks do not say "Unallocated" in them, then delete their volumes by right-clicking on each disk's volume and going to "Delete Volume"
4. Now create the RAID: right-click on one of the disk, it doesn't matter which partition. Go to "New Mirror Volume"

Creating New Mirrored Volume

A series of prompts will ask you about some details of the new mirrored volume (array), like which disks are to be included, size of the volume, drive letter assignment, and volume name. In my example, Disk 1 and Disk 2 are used (Disk 0 being my original disk with the OS on it), the full size available (its default), drive letter E, quick format, and "WinMirror" as the volume name. A Mirrored Volume has been created in Windows Server 2012.

Installing Active Directory to PDC

A Directory service stores all information about resources on a network such as users, groups, computers, files, printers and applications. It provides all the services that makes the information available and useful. AD (active directory) stores info about resources in a hierarchy structure, it contains objects that represent the different types of network resources. Each object has attributes such as user's first name, last name and email address or a printer location. (Stanek, 2008) (Dan Holme, 2008) In my project, an active directory was made under the full qualified domain name GU.

To initialize AD on PDC, open the Server Manager from the task bar. From the Server Manager Dashboard, select Add roles and features. This will launch the Roles and Features Wizard allowing for modifications to be performed on the Windows Server 2012 instance. The following should be done to install active directory on the PDC:

1. Select Role-based or Features-based installation from the Installation Type screen and click next.

2. The current server is selected by default. Click Next to proceed to the Server Roles tab.

Note: Roles are the major feature sets of the server, such as IIS, and features provide additional functionality for a given role

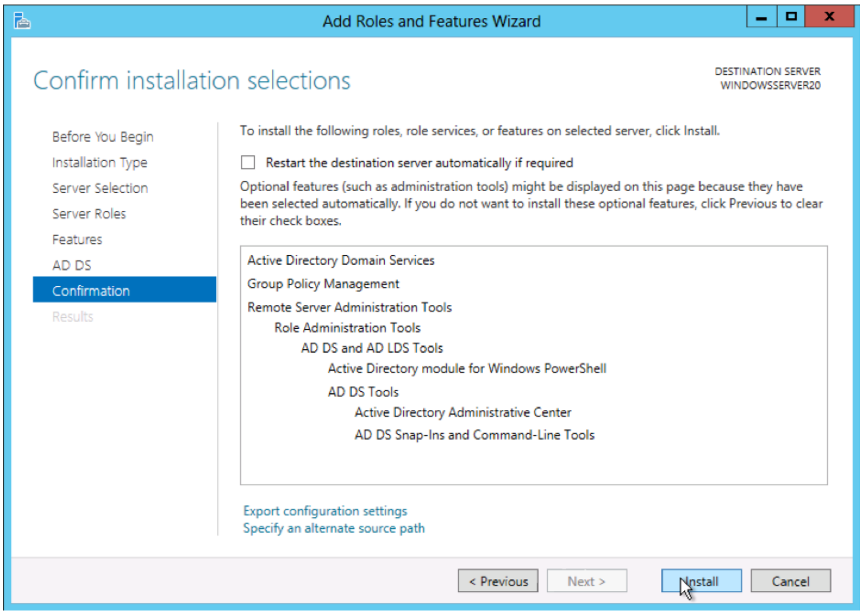
3. From the Server Roles page place a check mark in the box next to Active Directory Domain Services. A notice will appear explaining additional roles services or features are also required to install domain services, click Add Features.

Note: There are other options including, Certificate services, federation services, lightweight directory services and rights management. Domain Services is the glue that holds this all together and needs to be installed prior to these other services.

4. Review and select optional features to install during the AD DS installation by placing a check in the box next to any desired features; once done click next.

Review the information on the AD DS tab as shown in figure 7 and click next.

5. Review the installation and click Install.



Confirm installation selections

DESTINATION SERVER
WINDOWSSERVER20

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Domain Services
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
                Active Directory Administrative Center
                AD DS Snap-Ins and Command-Line Tools

Export configuration settings
Specify an alternate source path

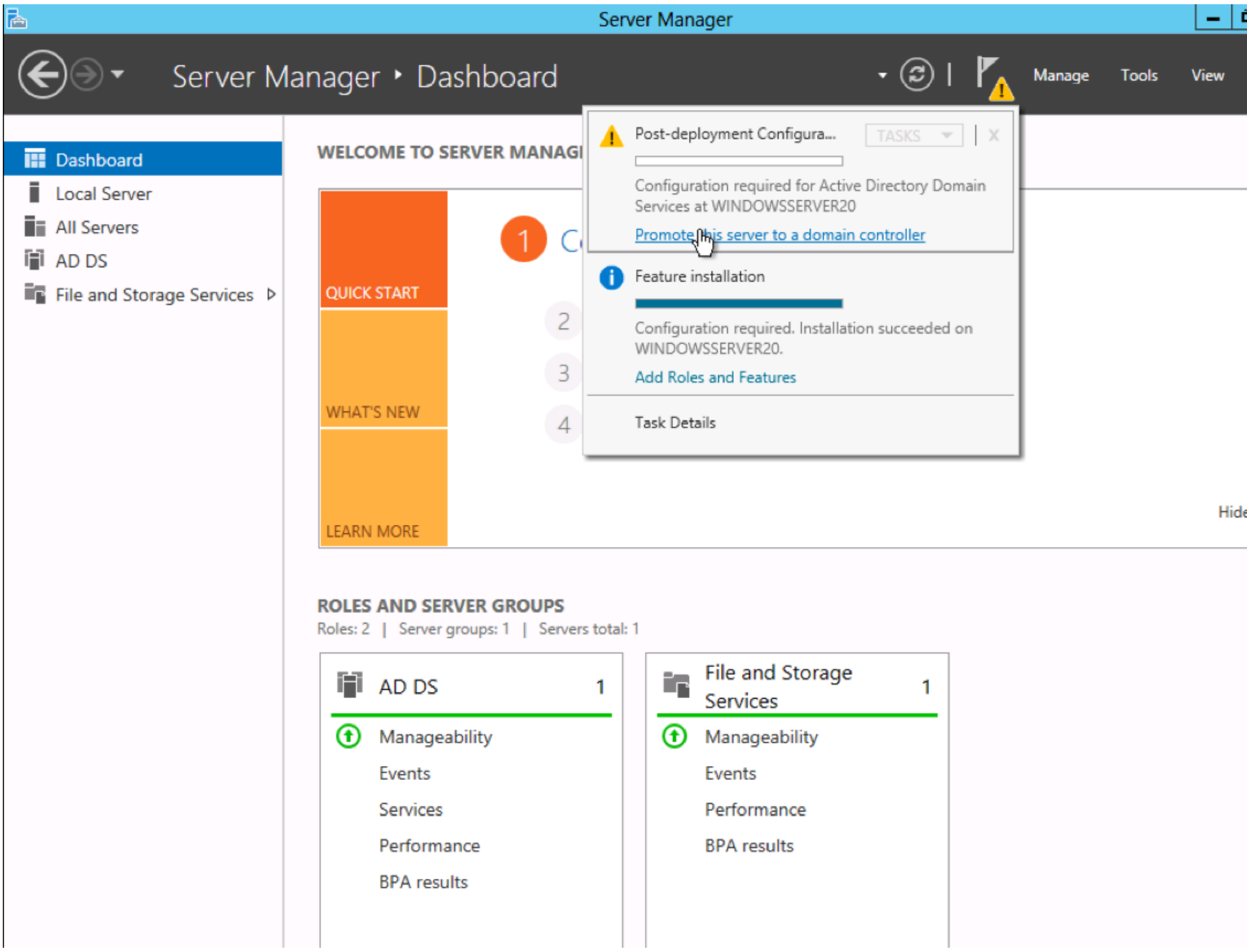
Figure 7. Active Directory Domain Service roles and features Confirmation console.

Note: The installation progress will be displayed on the screen. Once installed the AD DS role will be displayed on the 'Server Manager' landing page.

Configuring Active Directory

Once the AD DS role is installed, the server will need to be configured for the domain.

- If you have not done so already, open the Server Manager from the task bar.
- Open the Notifications Pane by selecting the Notifications icon from the top of the Server Manager. From the notification regarding configuring AD DS, click Promote this server to a domain controller.



Post-deployment Configura...

Configuration required for Active Directory Domain Services at WINDOWSSERVER20

Promote this server to a domain controller

Feature installation

Configuration required. Installation succeeded on WINDOWSSERVER20.

Add Roles and Features

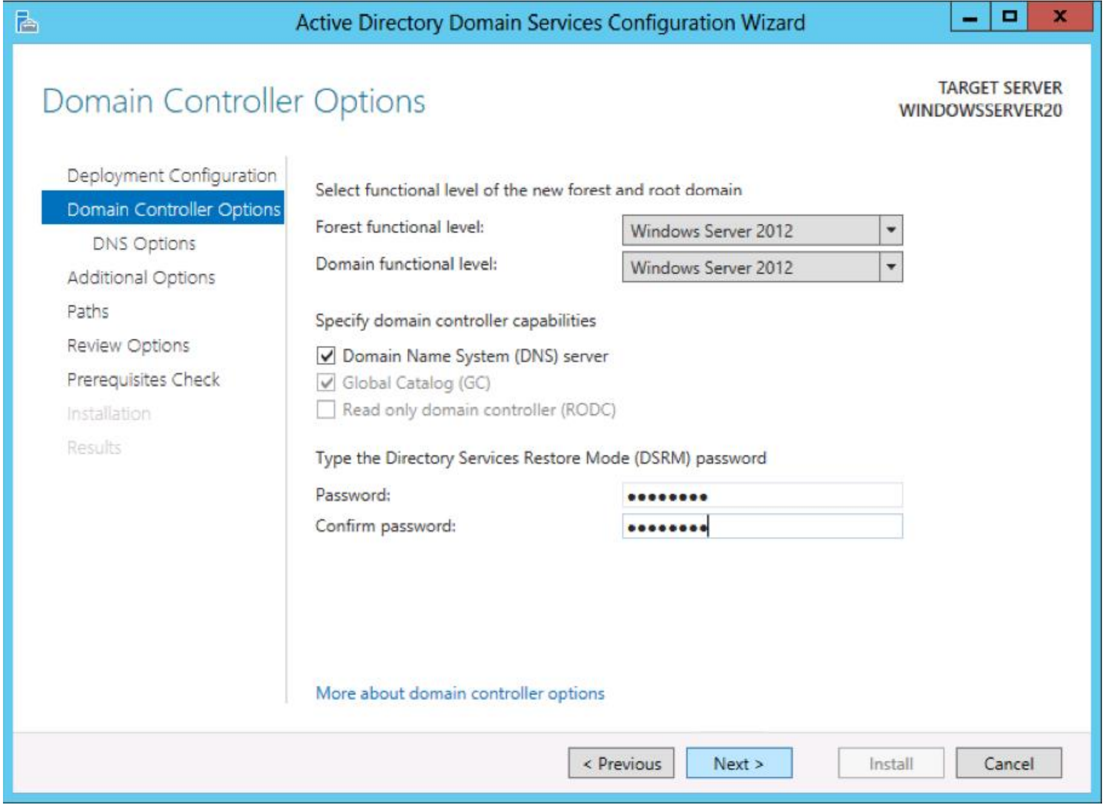
Task Details

Figure 8. Promoting This server to be a Domain Controller

- From the Deployment Configuration tab select add a new forest from the radial options menu. Insert root domain name into the Root domain name field.

- Review and select a Domain and Forest functional level. Once selected fill in a DSRM password in the provided password fields. The DSRM password is used when booting the Domain Controller into recovery mode.

Note: The selection made here will have lasting effects to features and server domain controller eligibility.



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
WINDOWSSERVER20

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012

Domain functional level: Windows Server 2012

Specify domain controller capabilities

☑ Domain Name System (DNS) server
☑ Global Catalog (GC)
□ Read only domain controller (RODC)

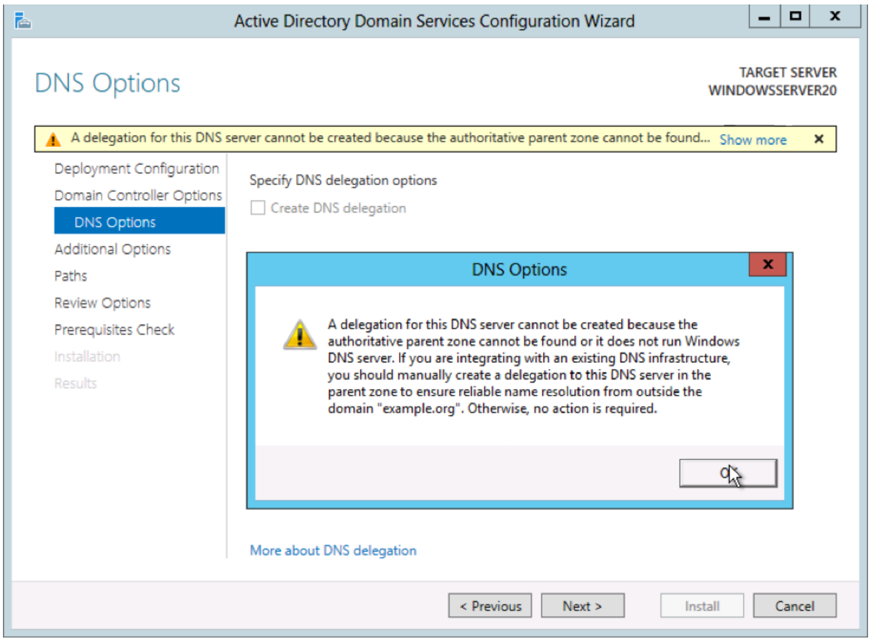
Type the Directory Services Restore Mode (DSRM) password

Password: ••••••••

Confirm password: ••••••••

Figure 9. Domain Controller Options

- Review the warning on the DNS Options tab and select next.



⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...

Specify DNS delegation options

□ Create DNS delegation

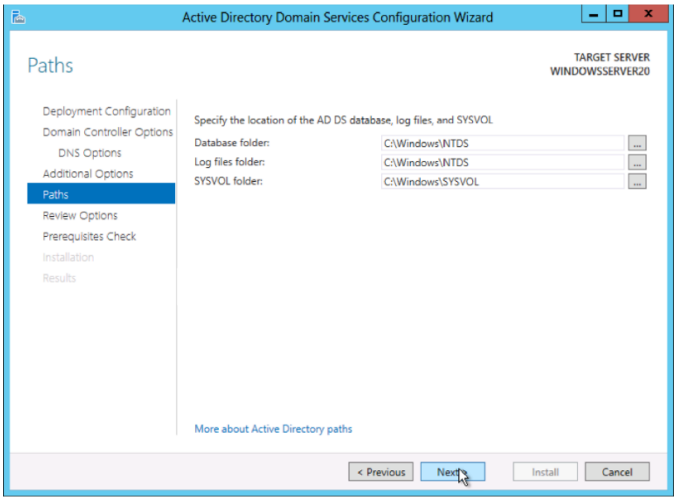
DNS Options

A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "example.org". Otherwise, no action is required.

Figure 10. DNS Options

- Confirm or enter a NetBIOS name “GU” and click next.

- Configure the location of the SYSVOL, Log files, and Database folders and click next.



Specify the location of the AD DS database, log files, and SYSVOL

Database folder: C:\Windows\NTDS

Log files folder: C:\Windows\NTDS

SYSVOL folder: C:\Windows\SYSVOL

Figure 11. Configuring AD DS paths

- Review the configuration options and click next.
- The system will check to ensure all necessary prerequisites are installed on the system prior to moving forward. If the system passes these checks you will proceed by clicking Install. (Server world, 2012)

Note: The server will automatically be rebooted once the installation completes.

After rebooting you will notice that an active directory has been installed, with the root name GU.

Add a Secondary Domain Controller

If you primary domain controller was to fail, you can still run ADD services on secondary domain controller. Just like what's done to add a Primary Domain Controller, a new virtual machine with windows server 2012 should be installed. Going through the same process until **promoting** the server by pressing on promote this server. (Fra, 2012)

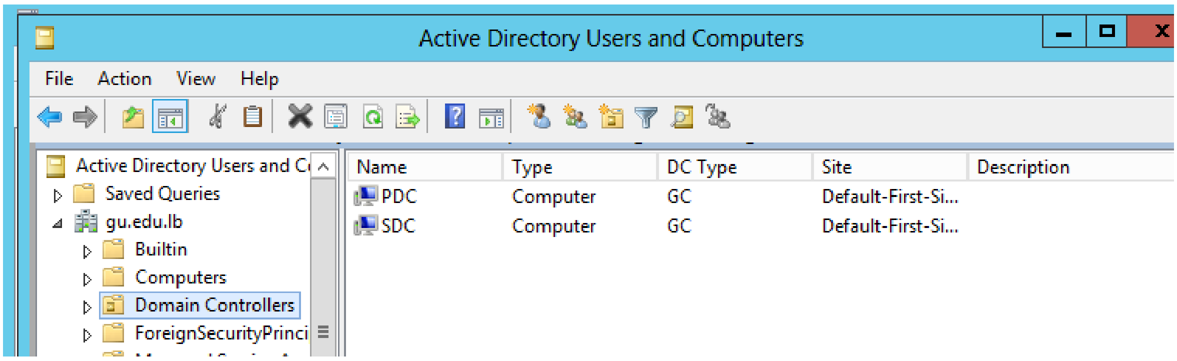
When the wizard pops-up, click next until prompted to select from **existing** forest[3], or add a new forest. So first:

- Select add a domain controller to an existing forest and press next
- Type any name of a running and active domain, in this case gu.edu.lb

  Since the new machine is not a member to the domain, currently logged in credentials, can't be used, so an alternative credentials shall be used which is GU admin.
- Now select the domain from domain site-pool[4],
- This server should be a backup domain controller, so the DNS and global catalogue should be enabled on this server
- The database, log files, SYSvol are recommended to be on different physical drives, but for practicing purposes leave them as default.
- Assign and confirm the DSRM(Password)
- A summary will show up just to check and validate if every configuration is matched. Then press finish and reboot.
- As soon as the installation finished and reboot has been done, you should notice two computers PDC and SDC. Under the GU active directory → Domain controllers OU as shown in the figure 12.

[3] A forest is A group of Active Directory trees

[4] A site allow replication within the same boundary



Name	Type	DC Type	Site	Description
PDC	Computer	GC	Default-First-Si...	
SDC	Computer	GC	Default-First-Si...	

Figure 12. Content of Domain Controllers' OU

Benefits of a BCD

In Windows NT 4 server domains, the Backup Domain Controller (BDC) is a computer that has a copy of the user accounts database. Unlike the accounts database on the Primary Domain Controller (PDC), the BDC database is a read-only copy. When changes are made to the master accounts database on the PDC, the PDC pushes the updates down to the BDCs. (Dan Holme, 2008)

Most domains will have at least one BDC, and often there are several BDCs in a domain. These additional domain controllers exist to provide fault tolerance. If the PDC fails, then it can be replaced by a BDC. In such circumstances, an administrator promotes a BDC to be the new PDC. BDCs can also authenticate user logon requests - and take some of the authentication load from the PDC (Dan Holme, 2008)

Implementation Problems [SOLVED]

The problem is when the servers couldn't replicate for connectivity issues. VMware provides separation between two physical machines, but the problem was within the VMware forwarding, the Primary DNS could not be contacted.

The following tasks were done to solve the problem:

- Trying New subnet
- Trying *to tracert* [5]the PDC
- Troubleshooting connection
- Turning **OFF** windows firewall on the PDC

[5] *Tracert is a cmd command that give info regarding trace, hop count, latency between source and destination.*

Installing Open Source anti-virus

When you start up Windows 8 and above versions for the first time, Windows Defender is on and working to protect your PC by scanning for malicious software. Windows Defender uses real-time protection to scan everything you download or run on your PC.

If Windows 8 and above is running on the machine, you can't get Microsoft Security Essentials, the open source anti-virus. But you don't need it because you already have Windows Defender by default, which provides the same level of protection. Windows Defender will turn itself off if you install another antivirus app. However, Windows recommend to stick on Windows Defender and no need for external antivirus.

Windows Update downloads updates for Windows Defender automatically to help keep the PC safe and protect it from attacks. (Microsoft, 2016)

Linux Firewall

A firewall is a system designed to prevent unauthorized access to or from a private network (which could be just one machine). (Afra, 2013)Firewalls can be implemented in hardware or software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets[6]. All messages entering or leaving the intranet pass through the firewall, which examines each message and allows, proxies, or denies the traffic based on specified security criteria. The firewalls listed in this article are overwhelmingly based on the iptables program. (pfSense, 2016)

What are iptables

Iptables is a command-line firewall utility that uses policy chains to allow or block traffic. When a connection tries to establish itself on the system, iptables looks for a rule in its list to match it to. If it doesn't find one, it resorts to the default action. (Afra, 2013) (pfSense, 2016)

Iptables almost always comes pre-installed on any Linux distribution. To update/install it, just retrieve the iptables package:

```
sudo apt-get install iptables
```

Types of Chains

iptables uses three different chains: input, forward, and output.

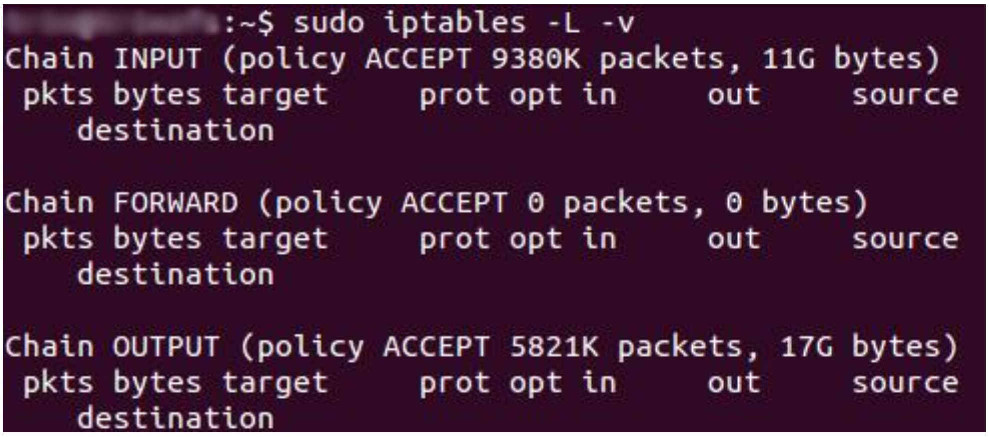
Input – This chain is used to control the behaviour for incoming connections. For example, if a user attempts to SSH into the PC/server, iptables will attempt to match the IP address and port to a rule in the input chain. (Afra, 2013; Ellingwood, 2014)

[6] Intranet: a local or restricted communications network, especially a private network created using World Wide Web software.

Forward – This chain is used for incoming connections that aren't actually being delivered locally. Think of a router – data is always being sent to it but rarely actually destined for the router itself; the data is just forwarded to its target. Unless you're doing some kind of routing, NATing, or something else on this system that requires forwarding, you won't even use this chain. (Afra, 2013; Ellingwood, 2014)

There's one way to check whether or not the system uses/needs the forward chain.

```
iptables -L -v
```



```
[redacted]:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 9380K packets, 11G bytes)
 pkts bytes target     prot opt in     out     source
   destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source
   destination

Chain OUTPUT (policy ACCEPT 5821K packets, 17G bytes)
 pkts bytes target     prot opt in     out     source
   destination
```

Figure 13. Chains in iptables

Output – This chain is used for outgoing connections knowing that the ping source is the firewall. For example, if you try to ping google.com, iptables will check its output chain to see what the rules are regarding ping and google.com before making a decision to allow or deny the connection attempt. (Afra, 2013; Ellingwood, 2014)

Implementing Firewall

In this scenario:

- Users should not be able to reach the SQL Server using \\
- Users should be able to contact SQL server to run a query and get result
- Users should be able to access the shared folder

The SQL Server is will be installed on the PDC to maximize performance, thus the local machine **cannot** handle four-running machines at the same time:

- Running Firewall
- Active domain-user
- PDC
- SQL Server

Implementation Problems [SOLVED]

One of the sophisticated problems was connecting an external OS to a windows domain controller. I've tried many packages that enable integration between Linux and Windows server where all ended to fail, until it was solved using **realm**[7] package.

Installing *realm on Linux Firewall* joining the domain

First, the firewall and the domain should be able to ping each other, if the ping is lost then check for connectivity issues. Installing **realm** is done through (Server world, 2012):

```
yum -y install realm
```

This action will install some required packages (automatically download).

- Next, the realm should do its negotiation and discovery:

```
realm discover Gu.edu.lb
```

- Once the domain is discovered, the following text should appear

```
  type: kerberos
  realm-name: Gu.edu.lb
  domain-name: Gu.edu.lb
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common
```

- join in Active Directory domain

```
realm join Gu.edu.lb

Password for Administrator: # AD's Administrator password
```

- make sure it's possible to get an AD user info or not

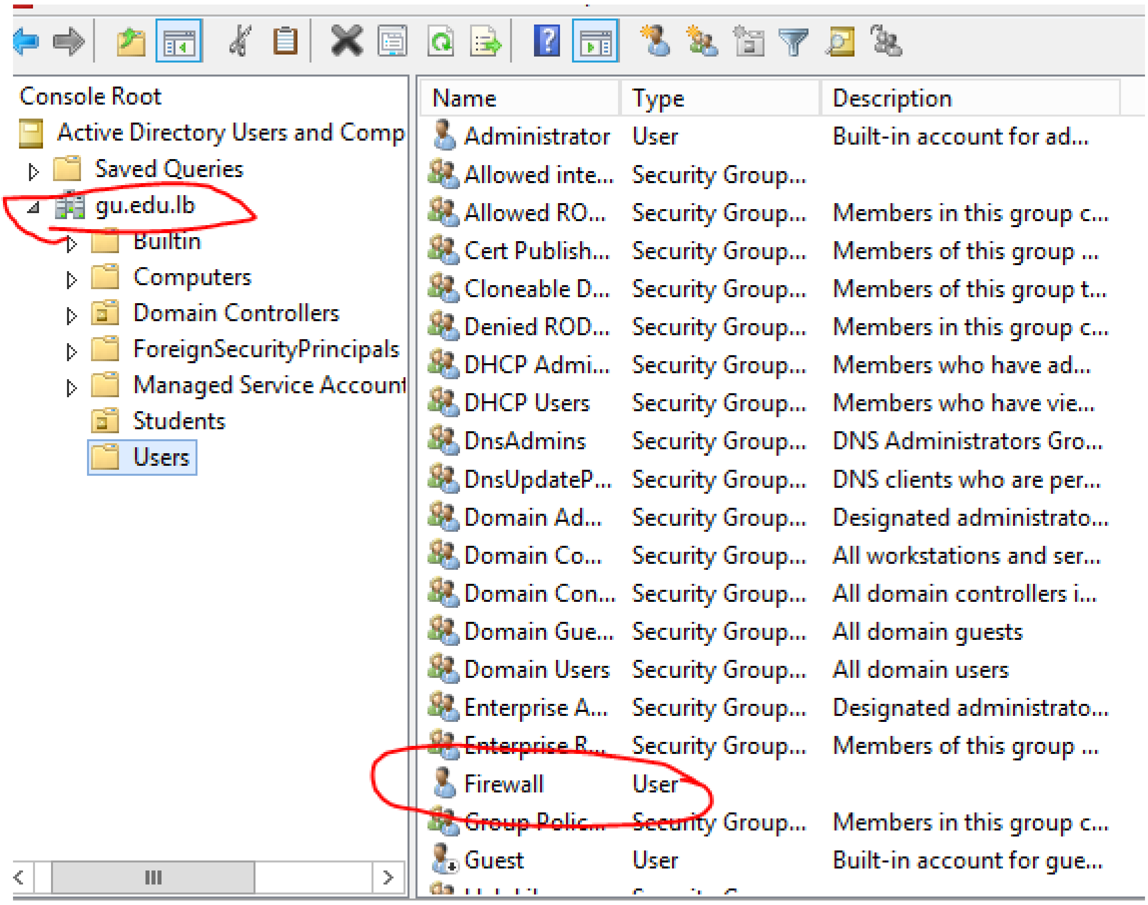
```
id firewall\\PDC

uid=1313201104(firewall@gu.edu.lb)
gid=1313200513(domainusers@gu.edu.lb)groups=1313200513(domain
users@gu.edu.lb)
```

[7] Realm is a discovering and joining identity domain

- make sure it's possible to switch to an AD user or not

```
su - firewall\\PDC

Creating home directory for firewall@gu.edu.lb

[firewall@Gu.edu.lb@dlp ~]$
```

Note: Firewall is a user already created under domain users' OU before discovering the domain as shown in figure 14.



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed inte...	Security Group...	
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DHCP Admi...	Security Group...	Members who have ad...
DHCP Users	Security Group...	Members who have vie...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise R...	Security Group...	Members of this group ...
Firewall	User	
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...

Figure 14. Content of Domain Users

Configuring Iptables

To configure iptables, open terminal and type su. The configuration process in this scenario will be divided to:

- Blocking UNC traffic
- Granting access to issue a Query

Blocking UNC traffic

Firewall is now active and connected to the domain. Best practices would have you restrict access to these ports. By default, these ports are usually only open to the Private Network:

- TCP Port 445
- TCP Port 137
- TCP Port 139
- UDP Port 137
- UDP Port 138

To block these ports open terminal on Linux, then type su (Super User), since iptables requires root privileges.

```
Iptables -A FORWARD -i eth0 -o eth1 -s 192.168.74.0/24 -d 
192.168.74.131 -p tcp -m multiport -dport 445,137,139 -j DROP

Iptables -A FORWARD -i eth0 -o eth1 -s 192.168.74.0/24 -d 
192.168.74.131 -p upd -m multiport -dport 137,138 -j DROP
```

Since the traffic is forwarded from users to PDC, the whole subnet was assigned to be drop. But not all traffic is drop, only UMC traffic coming from Ethernet0 to Ethernet 1.

-p: protocol

-s: source

-d: destination

-i: input packet

-o: output packet

-j: action

Granting access to issue queries on SQL Server and Shared folder

Mainly, there are no restrictions to on the user trying to issue the query, in other words the whole subnet has access to the SQL.

```
iptables -A FORWARD -p tcp -s 0/0 --sport 1024:65535 -d 192.168.74.131 --
dport 1433 -m state --state NEW,ESTABLISHED -j ACCEPT

iptables -A FORWARD -p tcp -s 192.168.74.131 --sport 1433 -d 0/0
--dport 1024:65535 -m state --state ESTABLISHED -j ACCEPT
```

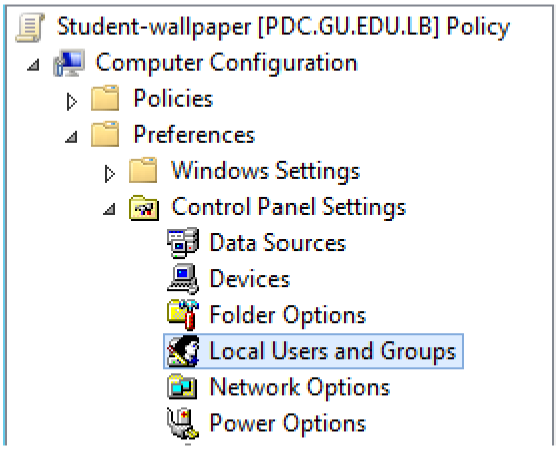
--state: state of connection.

As network traffic generally needs to be two-way ”incoming and outgoing” to work properly, it is typical to create a firewall rule that allows established and related incoming traffic, so that the server will allow return traffic to outgoing connections initiated by the server itself.

Group Policy

Group Policy is designed to simplify administration by allowing administrators to configure user and computer settings in Active Directory Domain Services and then have those policies automatically applied to computers and enforced for computer and user accounts throughout an organization. (Server world, 2012) Not only does this provide central management of computers, it also helps to automate key administrative tasks. Using Group Policy, you can accomplish the following tasks:

- Configure security policies for account lockout, passwords, Kerberos, and
- auditing
- Redirect special folders such as a user’s Documents folder to centrally managed
- network shares
- Lock down computer desktop configurations
- Define logon, logoff, shutdown, and start-up scripts
- Automate the installation of application software
- Maintain Microsoft Internet Explorer and configure standard settings



Student-wallpaper [PDC.GU.EDU.LB] Policy
- Computer Configuration
  - Policies
  - Preferences
    - Windows Settings
    - Control Panel Settings
      - Data Sources
      - Devices
      - Folder Options
      - Local Users and Groups
      - Network Options
      - Power Options

Figure 15. Group policy console

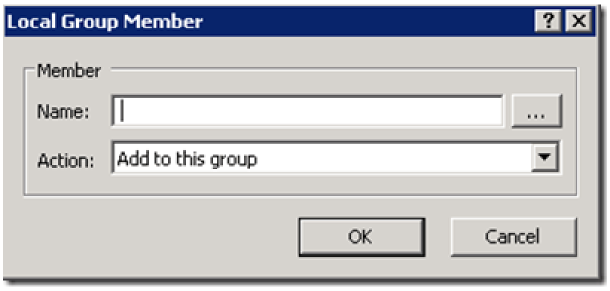
Restricting access to local admin group using GPO

The following steps will need to be applied to a GPO that is applied to the computer objects you want to control the local administrator groups:

- Open the Group Policy Management Console and edit the group policy that is applied to the scope of computers that you want to control.

- Go to the Computer Configuration →Preferences → Control Panel Settings → Local User and Groups option. See figure 16

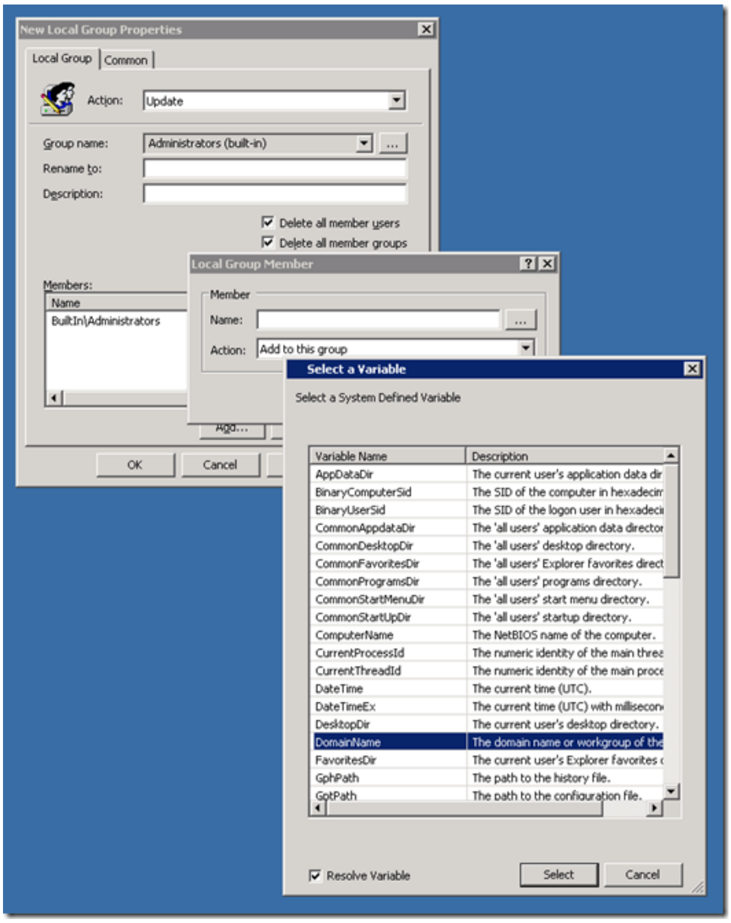
Figure 16. Adding group member



Name:

Action: Add to this group

- Click on Actions → New → Local Group
- You will be need to select "Administrators (built-in)" from the group name as this always selects the built-in administrators group.
- Tick both "Delete all member users" and "Delete all member groups". These two options will automatically remove any users or groups that are not explicitly being added to the group. This is only needed on item number one in the list of settings as that setting will be processed last.
- Now, you will need to make sure you are added back in the Domain Admin's and Local Administrator groups so that you don't totally lock yourself out of the computer. To do this, click the "Add…" button to bring up the "Local Group Member" dialogue box. Check figure 17
- type "BuiltIn\Administrator" in the Name field and click OK
- You should also add "DOMAINNAME\Domain Admins" as it is a good practice to have the DA account as a member of the local admin group on all computers in the domain. To do this, use the Domain Name variables. Click "add"



Action: Update

Group name: Administrators (built-in)

Rename to:

Description:

☑ Delete all member users

☑ Delete all member groups

Members:

Name
BuiltIn\Administrators

Name:

Action: Add to this group

Select a System Defined Variable

Variable Name	Description
AppDataDir	The current user's application data dir
BinaryComputerSid	The SID of the computer in hexadecim
BinaryUserSid	The SID of the logon user in hexadeci
CommonAppdataDir	The 'all users' application data director
CommonDesktopDir	The 'all users' desktop directory.
CommonFavoritesDir	The 'all users' Explorer favorites direct
CommonProgramsDir	The 'all users' programs directory.
CommonStartMenuDir	The 'all users' start menu directory.
CommonStartUpDir	The 'all users' startup directory.
ComputerName	The NetBIOS name of the computer.
CurrentProcessId	The numeric identity of the main threa
CurrentThreadId	The numeric identity of the main proce
DateTime	The current time (UTC).
DateTimeEx	The current time (UTC) with millisecon
DesktopDir	The current user's desktop directory.
DomainName	The domain name or workgroup of the
FavoritesDir	The current user's Explorer favorites c
GphPath	The path to the history file.
GptPath	The path to the configuration file.

☑ Resolve Variable

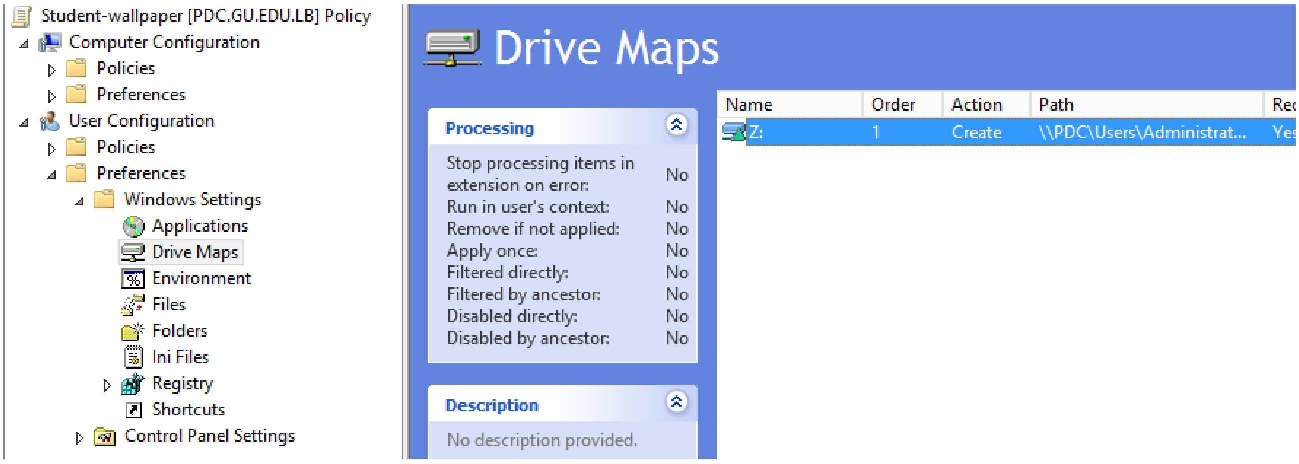
Figure 17. Selecting DomainName

- Now click in the "Name:" text field and then press F3. This will now bring up the "Select Variable" dialogue box. Click on the "Domain Name" field and press "Select" and then "OK". (Alternatively you could type %DomainName% in the name field and just press OK.) check figure 16

Public drive mappings

Newly created Group Policy objects apply to all authenticated users. The drive map preference items contained in the GPO inherits the scope of the GPO; leaving us to simply configure the preference item and link the GPO. Start by configuring the drive map preference item by choosing the Action of the item. Drive map actions include Create, Replace, Update, and Delete. These are the actions commonly found in most preference items. Create and Delete actions are self-explanatory (Stanek, 2008)

The configured location is a network share named data; hosted by a computer named PDC. The configured drive letter is the Z drive. All other options are left at their defaults. This GPO is linked at the gu.edu.lb domain. Check figure 18



Processing

Stop processing items in extension on error:	No
Run in user's context:	No
Remove if not applied:	No
Apply once:	No
Filtered directly:	No
Filtered by ancestor:	No
Disabled directly:	No
Disabled by ancestor:	No

Description

No description provided.

Name	Order	Action	Path	Rec
Z:	1	Create	\\PDC\Users\Administrat...	Yes

Figure 18. Mapping network drive Z to every User under the path \Administrator\Desktop\Users

Granting Linux Access to Shared Folder

Windows share can be mounted on RHEL system using `cifs` option of `mount` command as:

```
[root@host ~]# mount -t cifs -o username=<share user>,password=<share
password> //WIN_PC_IP/<share name> /mnt
```

However, In case the user is in windows domain then you can define the domain as follows:

```
[root@host ~]# mount -t cifs -o username=<share user>,password=<share
password>,domain=gu.edu.lb //192.168.74.131/<share name> /mnt
```

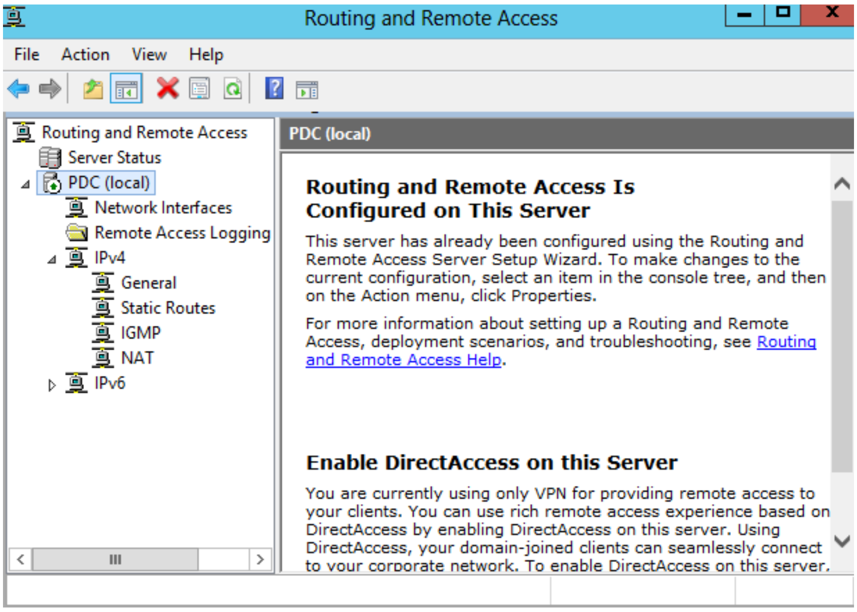
As previously explained, to discover a Windows domain, **realm** should be installed under the Linux machine.

Granting Internet access for domain users

To grant access for those who are authenticated within the site to any domain controller, a new role should be installed on the domain controller, which is the RRSA (Routing and Remote Access)

The steps are simple:

- Add the role and follow the wizard. Restarting the PDC is optional.
- Press tools in the server manager, and scroll to **routing and remote access**
- A dialog like figure 19 should appear
- Initially, this dialog should be empty. PDC server should have a red arrow down. Right click on the server name and select configure and enable routing and remote access. (Fra, 2012)



Routing and Remote Access Is Configured on This Server

This server has already been configured using the Routing and Remote Access Server Setup Wizard. To make changes to the current configuration, select an item in the console tree, and then on the Action menu, click Properties.

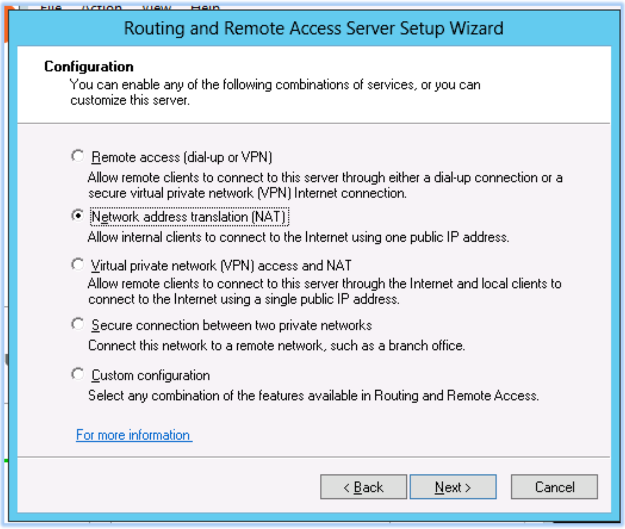
For more information about setting up a Routing and Remote Access, deployment scenarios, and troubleshooting, see Routing and Remote Access Help.

Enable DirectAccess on this Server

You are currently using only VPN for providing remote access to your clients. You can use rich remote access experience based on DirectAccess by enabling DirectAccess on this server. Using DirectAccess, your domain-joined clients can seamlessly connect to your corporate network. To enable DirectAccess on this server.

Figure 19. Routing and Remote access Console

- In the setup wizard, select network address translation (NAT)



Routing and Remote Access Server Setup Wizard

Configuration
You can enable any of the following combinations of services, or you can customize this server.

○ Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.

● Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.

○ Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.

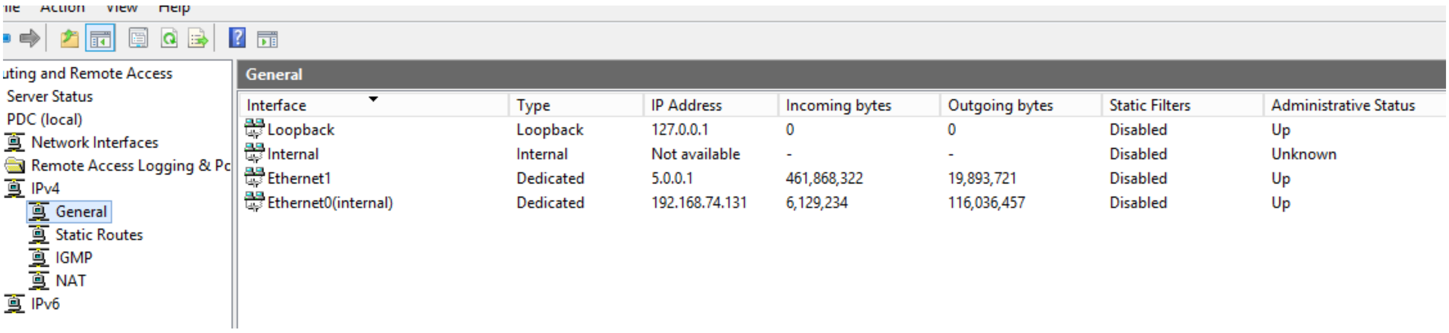
○ Secure connection between two private networks
Connect this network to a remote network, such as a branch office.

○ Custom configuration
Select any combination of the features available in Routing and Remote Access.

For more information

Figure 20. Routing and Remote Access Server Setup Wizard

- Finally, select the WAN interface as the public interface, and press finish.



uting and Remote Access
Server Status
PDC (local)
Network Interfaces
Remote Access Logging & Pc
IPv4
General
Static Routes
IGMP
NAT
IPv6

General

Interface	Type	IP Address	Incoming bytes	Outgoing bytes	Static Filters	Administrative Status
Loopback	Loopback	127.0.0.1	0	0	Disabled	Up
Internal	Internal	Not available	-	-	Disabled	Unknown
Ethernet1	Dedicated	5.0.0.1	461,868,322	19,893,721	Disabled	Up
Ethernet0(internal)	Dedicated	192.168.74.131	6,129,234	116,036,457	Disabled	Up

Figure 21. IPv4 General Routing and Traffic Information

As you can see in figure 21, there is two Ethernet interfaces, Ethernet1 and internal. On purpose the external IP was from different class subnet, for security reasons. Both links' status is UP means routing is occurring successively.

Installing DHCP and DNS

What is DHCP

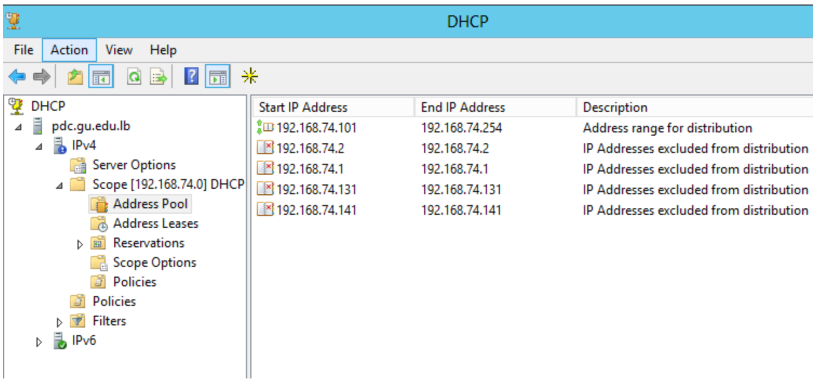
Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network. (Stanek, 2008; Afra, 2013; Server world, 2012)

DHCP assigns an IP address when a system is started, for example:

- A user turns on a computer with a DHCP client.
- The client computer sends a broadcast request (called a DISCOVER or DHCPDISCOVER), looking for a DHCP server to answer.
- The router directs the DISCOVER packet to the correct DHCP server.
- The server receives the DISCOVER packet. Based on availability and usage policies set on the server, the server determines an appropriate address (if any) to give to the client. The server then temporarily reserves that address for the client and sends back to the client an OFFER (or DHCPOFFER) packet, with that address information. The server also configures the client's DNS servers, WINS servers, NTP servers, and sometimes other services as well.
- The client sends a REQUEST (or DHCPREQUEST) packet, letting the server know that it intends to use the address.
- The server sends an ACK (or DHCPACK) packet, confirming that the client has been given a lease on the address for a server-specified period of time. (Stanek, 2008)

Configuring DHCP

There are two types in DHCP window, the first is IPv4 and second is IPv6. In this scenario, IPv4 are used. The first thing to do is to configure **scope**[8]**.** The best practice is to configure a scope of IP addresses before dynamic addresses are assigned. As you can see in figure 22, my address pool has a range of IPs starting from 192.168.74.101 to 192.168.74.254, however, some IPs are excluded since they are dedicated to servers such as: Firewall, PDC, SDC …



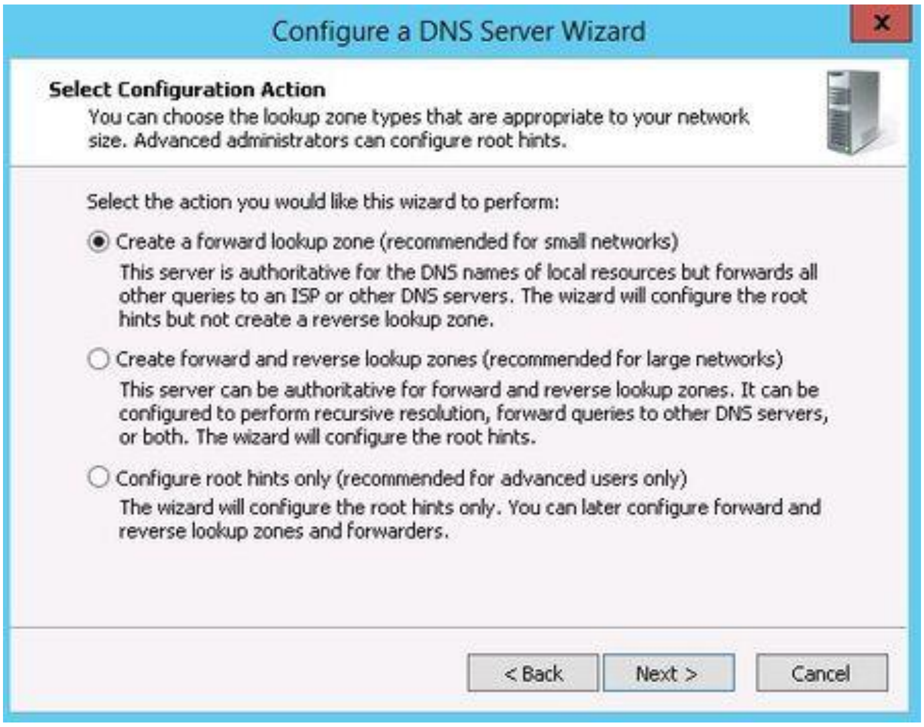
Start IP Address	End IP Address	Description
192.168.74.101	192.168.74.254	Address range for distribution
192.168.74.2	192.168.74.2	IP Addresses excluded from distribution
192.168.74.1	192.168.74.1	IP Addresses excluded from distribution
192.168.74.131	192.168.74.131	IP Addresses excluded from distribution
192.168.74.141	192.168.74.141	IP Addresses excluded from distribution

Figure 22. DHCP Console

[8] A scope is a range of IP addresses assigned to computers requesting a dynamic IP address

Configure DNS Server in Server 2012

Within Server Manager, to configure the DNS Server, click the Tools menu and select **DNS**. This brings up the DNS Manager window. Configure how the DNS server will work before adding any actual records. Select the DNS server to manage, then click the Action menu, and select **Configure a DNS Server**. This brings up the Configure a DNS Server wizard.



Select Configuration Action
You can choose the lookup zone types that are appropriate to your network size. Advanced administrators can configure root hints.

Select the action you would like this wizard to perform:

● Create a forward lookup zone (recommended for small networks)
This server is authoritative for the DNS names of local resources but forwards all other queries to an ISP or other DNS servers. The wizard will configure the root hints but not create a reverse lookup zone.

○ Create forward and reverse lookup zones (recommended for large networks)
This server can be authoritative for forward and reverse lookup zones. It can be configured to perform recursive resolution, forward queries to other DNS servers, or both. The wizard will configure the root hints.

○ Configure root hints only (recommended for advanced users only)
The wizard will configure the root hints only. You can later configure forward and reverse lookup zones and forwarders.

Figure 23. DNS Configuration Wizard

There are three options here. You can either: configure **a forward lookup zone** [9]only, create forward and **reverse lookup zone[10]**, or **configure root hints[11]** only.

For example, if a user is set up to print to a printer with an IP address of 10.20.12.114, but you need to know what name that printer goes by so you can find it, a reverse lookup can help.

If you already have DNS setup on the network, you'll probably want to continue using the same configuration you already have. If not, use forward and backward for most situations.

Click next afterwards.

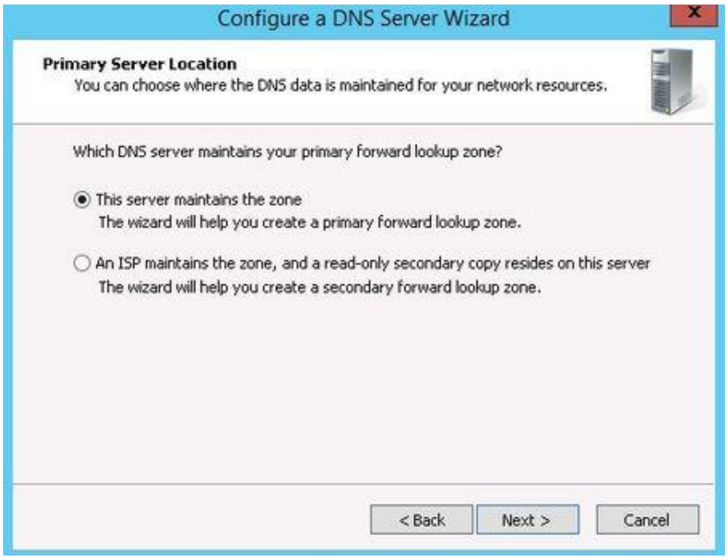
[9] A forward lookup zone allows you to do the standard DNS function of taking a name and resolving it into an IP address.

[10] A reverse lookup zone allows you to do the opposite, taking an IP address and finding its name

[11] Root hints only will not create a database of name records for lookups, but rather will just have the IP addresses of other DNS servers where records can be found

Now, you choose whether this server will maintain the zone, or if this server will have a read-only copy of the DNS records from another server.

Next enter the zone name. If this is the first DNS server, then this needs to be the root zone name for an entire organization. Click next when the name is entered.



Configure a DNS Server Wizard

Primary Server Location

You can choose where the DNS data is maintained for your network resources.

Which DNS server maintains your primary forward lookup zone?

● This server maintains the zone
The wizard will help you create a primary forward lookup zone.

○ An ISP maintains the zone, and a read-only secondary copy resides on this server
The wizard will help you create a secondary forward lookup zone.

Figure 24. Primary Server location

Now, you need to choose the file name where the DNS records will be stored. The default filename is to add a **.dns** extension to the name of the zone you chose in the previous window. Unless you have a corporate policy stating otherwise, stick with the convention to make things easier.

Next, you select how this server will respond to Dynamic Updates. Although there are three choices here, only two should actually be used in production. Select the first option to **allow only secure dynamic updates** if you are integrating the DNS with Active Directory. Select **do not allow dynamic updates** if the DNS is not integrated with Active Directory and you don't want to allow dynamic updates. Do not allow unsecured dynamic updates unless you really know what you are doing and have a very good reason for doing so.

Up next is the option to configure forwarders. If the DNS server ever gets a query for which it has no record, it can forward that request on to another DNS server to see if it has the answer. For example, in order to provide name resolution for internet connectivity, you can input the ISP name servers here, or use a DNS provider such as OpenDNS. The order forwarders are listed in is the order they are tried, so place the faster and most reliable forwarder at the top of the list.

Click next and the DNS server is now configured and ready for use.

Enabling RDS and Microsoft Load Balancer

Microsoft offers a service that used to be Microsoft terminal services, and now it’s RDS (Remote Desktop services). In this part, the installation will handle this role and setting up the environment to accept such requests, if a person logs in to IIS (Internet information Service) Webpage, they will be presented with web applications. (Load Balencer Inc., 2013)

RDS Installation

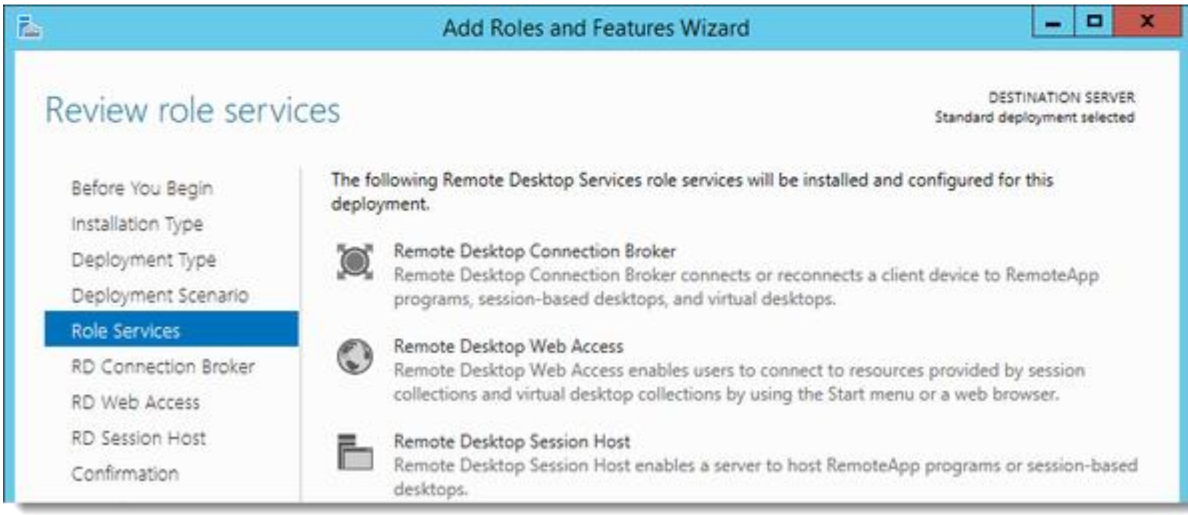
- Log on to the Domain Controller, and in Server Manager right-click the All Servers node and add the second server using the Add Servers command (or select the All Servers node, click Manage) Now that all servers needed in this deployment scenario are present, click Manage, and click Add Roles & Features. Click Next.

- Select Installation Type Select Remote Desktop Services installation. Click Next.

- Select Deployment Type Although Quick Start might be a valid option for a single server deployment, leave the default selected. This will explain the steps necessary to install Remote Desktop Services in greater detail. Click Next.

- Select Deployment Scenario. Select Session-based desktop deployment. The other option will be a different post in this series.
  Click Next.

  Review Role Services and Click Next



Review role services

DESTINATION SERVER
Standard deployment selected

The following Remote Desktop Services role services will be installed and configured for this deployment.

Remote Desktop Connection Broker
Remote Desktop Connection Broker connects or reconnects a client device to RemoteApp programs, session-based desktops, and virtual desktops.

Remote Desktop Web Access
Remote Desktop Web Access enables users to connect to resources provided by session collections and virtual desktop collections by using the Start menu or a web browser.

Remote Desktop Session Host
Remote Desktop Session Host enables a server to host RemoteApp programs or session-based desktops.

Figure 25. Review Role Services

- Specify RD Connection Broker server. Click the member server and click the Add button
  Click Next.
- Specify RD Web Access server
- Click the member server and click the Add button.
  Click Next.
- Confirm selections. Check Restart the destination server automatically if required.
  Click Deploy.
- View progress

  Wait until all role services are deployed and the member server has restarted.
  Click Close.

- In Server Manager click Remote Desktop Services and scroll down to the overview.

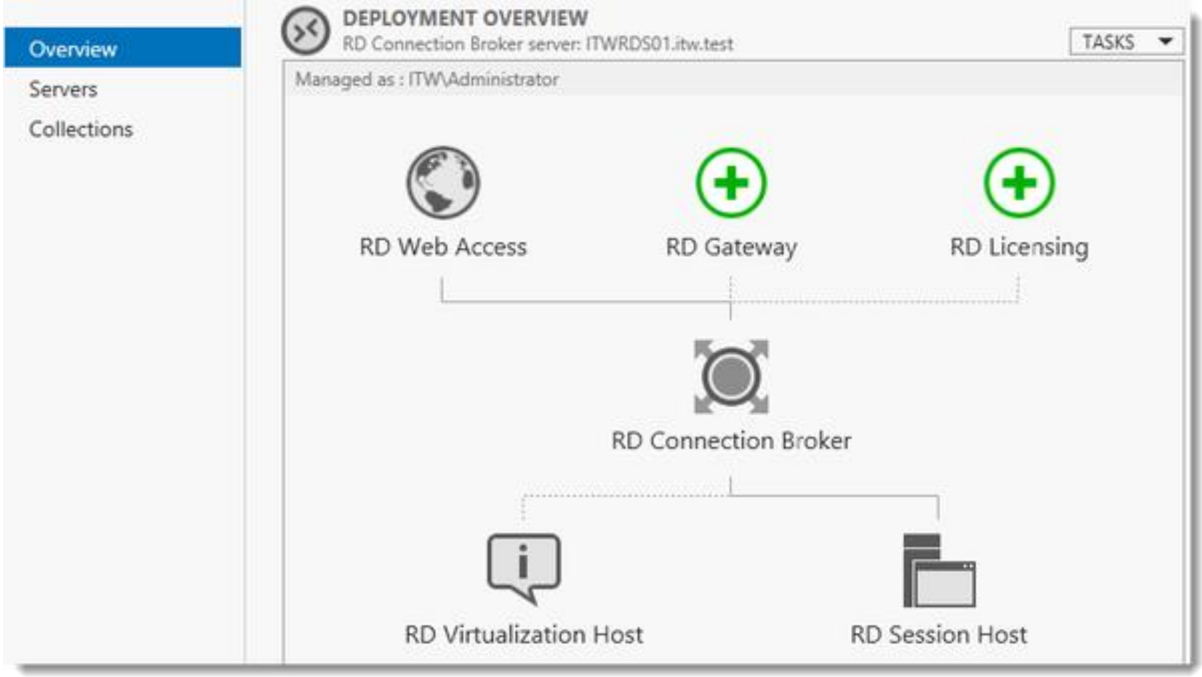


Figure 26. Deployment Overview

As you can see the deployment is missing a RD Gateway server and a RD Licensing server. Click the Add RD Licensing server button.

- Select a server. Click the domain controller and click the Add button. Click Next.
- Confirm selections Click Add.
- View progress Wait until the role service is deployed. No restart is needed. Click Close.

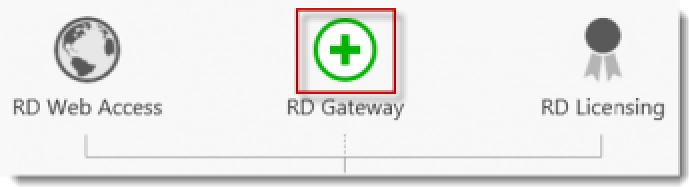


Figure 27. Adding RD Gateway server

Click the Add RD Gateway server button.

- Select a server. Click the member server and click the Add button. Click Next.
- Name the self-signed SSL certificate. The wizard creates a self-signed certificate. RD deal with certificates in this deployment in a little bit. Enter the external Fully Qualified Domain Name which you will also use for the Web Access URL. In my case, for lack of a better name, with “gateway.GU.nl. Click Next.
- Confirm selections Click Add.
- View progress

Wait until the role service is deployed. No restart is needed.

Notice that "gateway.it-worxx.nl" was configured for the deployment.
Also notice that even more certificate configuring is need, but we'll get to that later. Pay no attention to it for now.
Click Close.

- *Reviewing the Remote Desktop Services certificate requirements is optional*

In Server Manager, Remote Desktop Services, Overview, click Tasks and click Edit Deployment Properties.

Configuring the Deployment

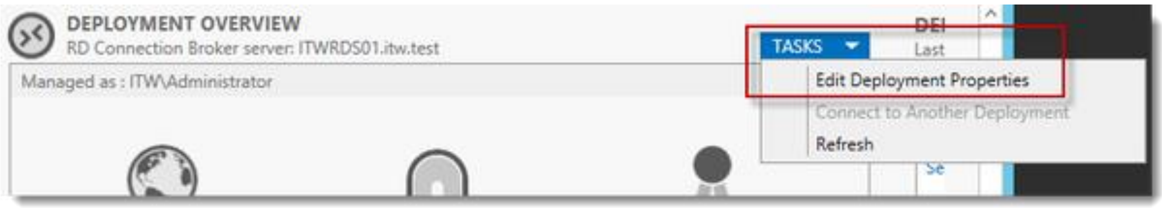
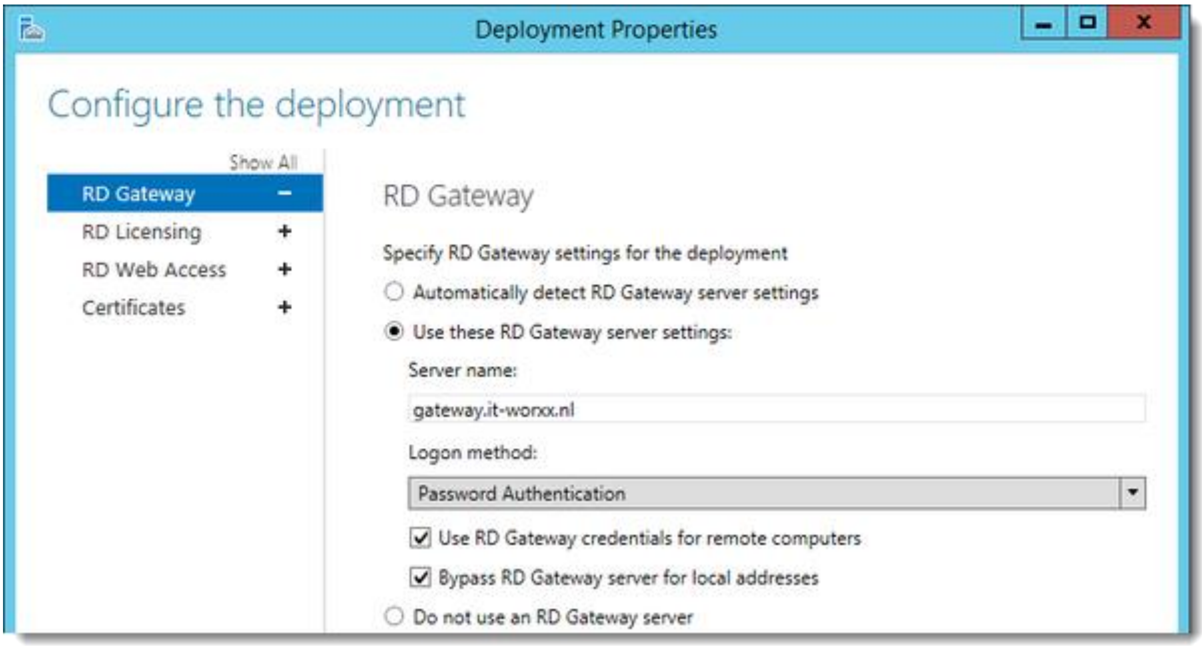

DEPLOYMENT OVERVIEW
RD Connection Broker server: ITWRDS01.itw.test
Managed as : ITW\Administrator
TASKS
Edit Deployment Properties
Connect to Another Deployment
Refresh

Figure 28. Editing the Deployment Properties



Configure the deployment

RD Gateway

Specify RD Gateway settings for the deployment

○ Automatically detect RD Gateway server settings

● Use these RD Gateway server settings:

Server name:

gateway.it-worxx.nl

Logon method:

Password Authentication

☑ Use RD Gateway credentials for remote computers

☑ Bypass RD Gateway server for local addresses

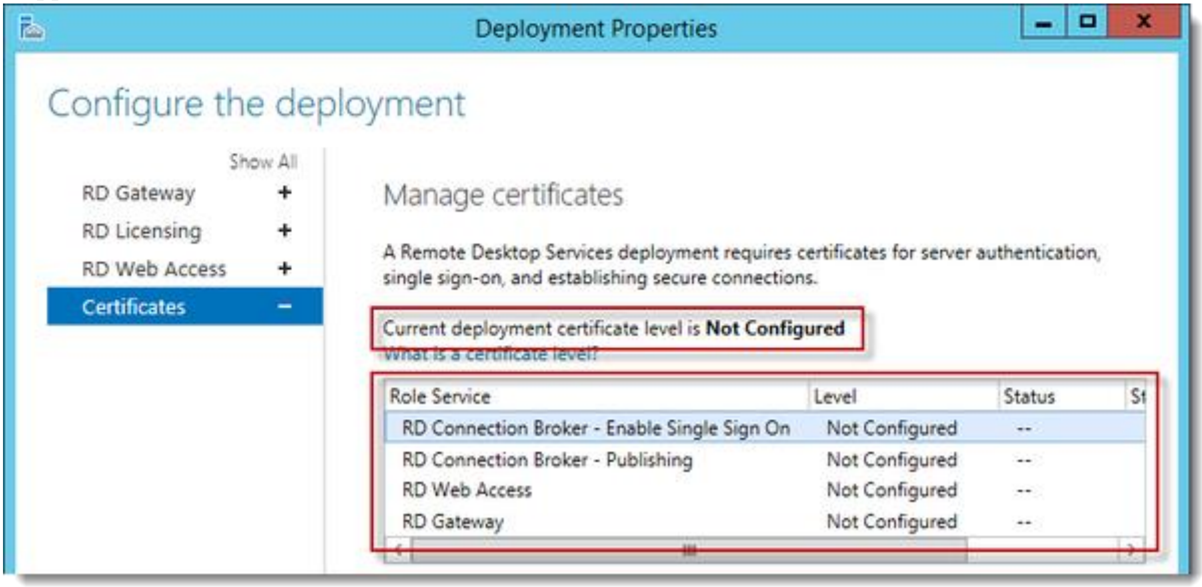
○ Do not use an RD Gateway server

Figure 29. RD Gateway settings.

Click RD Licensing.

- Configure the deployment. Notice that a RD License server is available, but no license type is selected yet. Select Per User, but since this is just a guide setup, it really doesn't matter.

Click RD Web Access. Configure the deployment. By default, the RD Web Access IIS application is installed in /RdWeb. Click Certificates.



Deployment Properties

Configure the deployment

Manage certificates

A Remote Desktop Services deployment requires certificates for server authentication, single sign-on, and establishing secure connections.

Current deployment certificate level is **Not Configured**

What is a certificate level?

Role Service	Level	Status	St
RD Connection Broker - Enable Single Sign On	Not Configured	--	
RD Connection Broker - Publishing	Not Configured	--	
RD Web Access	Not Configured	--	
RD Gateway	Not Configured	--	

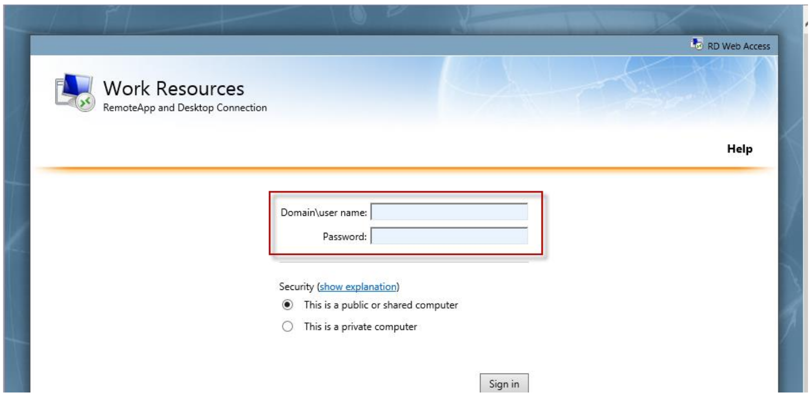
Figure 30. Configure the Deployment

Notice that the certificate level currently has a status of **Not Configured**.
As you can see, certificates are used for different goals within the deployment.
The RD Gateway certificate is used for Client to gateway communication and needs to be trusted by the clients. Either install the self-signed certificate on all clients, or use a certificate for which the complete certificate chain is already trusted by all clients. As it said in the wizard, the external FQDN should be on the certificate.
The RD Web Access certificate is used by IIS to provide a server identity to the browser clients.
The RD Connection Broker actually has two goals for which it needs certificates:

To enable single sign on (server to server authentication), and then for publishing (signing RDP files). If you can look in the deployment, you'll see that the Connection Broker is now configured to use, so change it to use an external FQDN as well.
If the same FQDN is used for all goals described above, need only one certificate, and one external IP address is needed.
Click OK

Testing the RDS

After Setting up configurations in DNS, test the web application. So first, open the browser, and type the Zone name, that you previously configured in DNS wizard. If the following web page opened (Figure 31), then you web app are online.



Domain\user name:
Password:

Security (show explanation)
● This is a public or shared computer
○ This is a private computer

Figure 31. Web Access is Online

Installing MS Exchange Server

Microsoft Exchange Server is a calendaring and mail server developed by Microsoft that runs exclusively on the Microsoft Windows Server product line.

How to Install Exchange Server 2016

Deployment of an Exchange Server 2013 server goes through three main stages. First Preparing Active directory if you are installing Exchange Server 2016 for the first time, then installing the Exchange Server 2016 pre-requisites on the server, and lastly running Exchange Server 2016 setup. (Network Microsoft Developer, 2016)

Preparing Active Directory for Exchange Server 2013

When you are installing Exchange Server 2013 for the first time, the Active Directory needs to be prepared. There are a series of requirements for Active Directory preparation to be successful: (Network Microsoft Developer, 2016)

- Schema master running Windows Server 2003 with SP2, or a later version of Windows Server
- At least one Global Catalogue server per site that Exchange will be installed in that is running Windows Server 2003 SP2 or later
- At least one Domain controller per site that Exchange will be installed in that is running Windows Server 2003 SP2 or later
- Forest functional mode of Windows Server 2003 or higher
- An account with Schema Admins, Domain Admins, and Enterprise Admins permissions to run Exchange setup

The Active Directory preparation requires the RSAT-ADDS tools

```
Import-Module ServerManager

Add-WindowsFeature RSAT-ADDS
```

However in this scenario, an installation of Exchange Server in the AD forest will occur for the first time. Running the following Exchange 2013 setup command is necessary to prepare Active Directory:

```
setup /PrepareAD /OrganizationName:"GU"/IAcceptExchangeServerLicenseTerms
```

Installing the Exchange Server 2013 Pre-Requisites

The prerequisites that are needed to install Exchange 2016 on computers running Windows Server 2012 or Windows Server 2012 R2 depends on which Exchange role you want to install.

To install prerequisites:

- Open Windows PowerShell.
- Run the following command to install the required Windows components.

```
Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience, NET-
Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-
Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-
PowerShell, Web-Mgmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-
Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-
Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-
Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console,
Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-
Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content,
Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation, RSAT-ADDS
```

Usually, it take a couple of minutes to install roles. Notice the result of the installation, if the test passed and succeeded, then a reboot is required.

After installing the prerequisites, the system is ready for the core pre-installation roles. These roles should be installed in the correct order.

1. NET Framework 4.5.2
2. Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit

Note that the PDC has some running services on it, like: RRSA, DHCP, etc… The NET Framework 4.5.2 is already installed, so the only required role is Microsoft Unified Communications Managed API4.0, Core Runtime 64-bit.

Installing Exchange Server 2013 Using the Setup Wizard

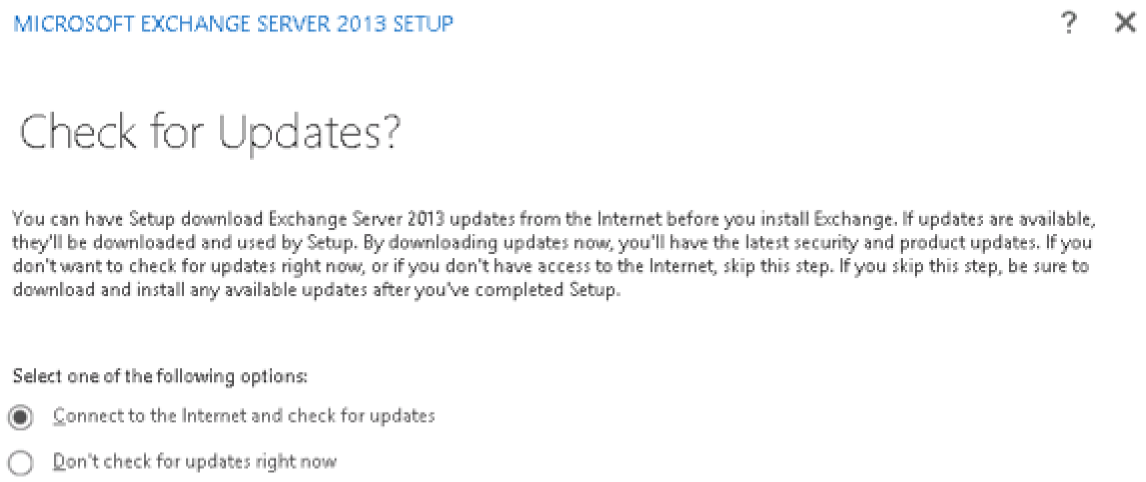
After installing the pre-requisites a restart of the server may be required. If you proceed without restarting then setup may be unable to proceed when it detects the pending restart.

From the location where the Exchange 2016 files are stored, run Setup.exe. Or by cmd, by typing the following command:

```
C:\Users\Administrator\Desktop\exchange >setup /PrepareAD
/IAcceptExchangeServerLicenseTerms /OrganizationName:GU
```

The following series are the steps to accomplish proper installation:

- First dialog gives the opportunity to check for updates to the setup files before proceeding, continue and pass the Introduction message. Check figure 32.



MICROSOFT EXCHANGE SERVER 2013 SETUP

Check for Updates?

You can have Setup download Exchange Server 2013 updates from the Internet before you install Exchange. If updates are available, they'll be downloaded and used by Setup. By downloading updates now, you'll have the latest security and product updates. If you don't want to check for updates right now, or if you don't have access to the Internet, skip this step. If you skip this step, be sure to download and install any available updates after you've completed Setup.

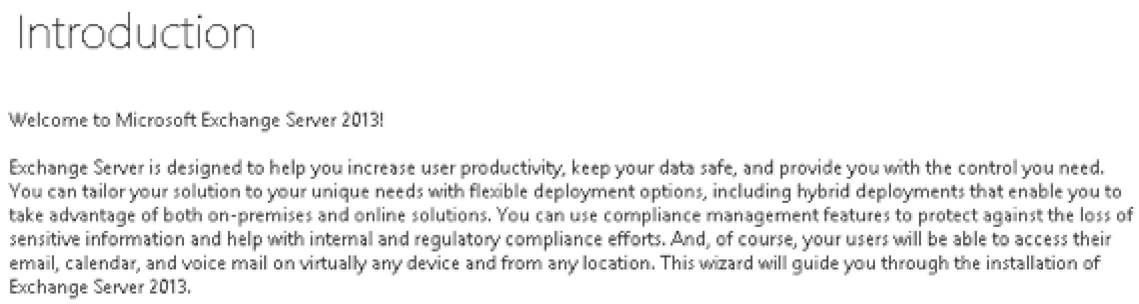
Select one of the following options:

● Connect to the Internet and check for updates

○ Don't check for updates right now

Figure 32. Checking for update

- In Exchange 2013 setup introduction, accept the license agreement in figure 33 and figure 34.

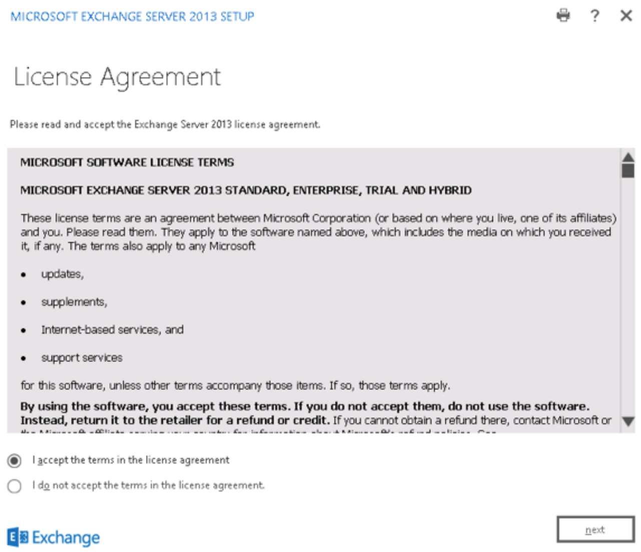


Introduction

Welcome to Microsoft Exchange Server 2013!

Exchange Server is designed to help you increase user productivity, keep your data safe, and provide you with the control you need. You can tailor your solution to your unique needs with flexible deployment options, including hybrid deployments that enable you to take advantage of both on-premises and online solutions. You can use compliance management features to protect against the loss of sensitive information and help with internal and regulatory compliance efforts. And, of course, your users will be able to access their email, calendar, and voice mail on virtually any device and from any location. This wizard will guide you through the installation of Exchange Server 2013.

Figure 33. Introduction setup



MICROSOFT EXCHANGE SERVER 2013 SETUP

License Agreement

Please read and accept the Exchange Server 2013 license agreement.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT EXCHANGE SERVER 2013 STANDARD, ENTERPRISE, TRIAL AND HYBRID

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

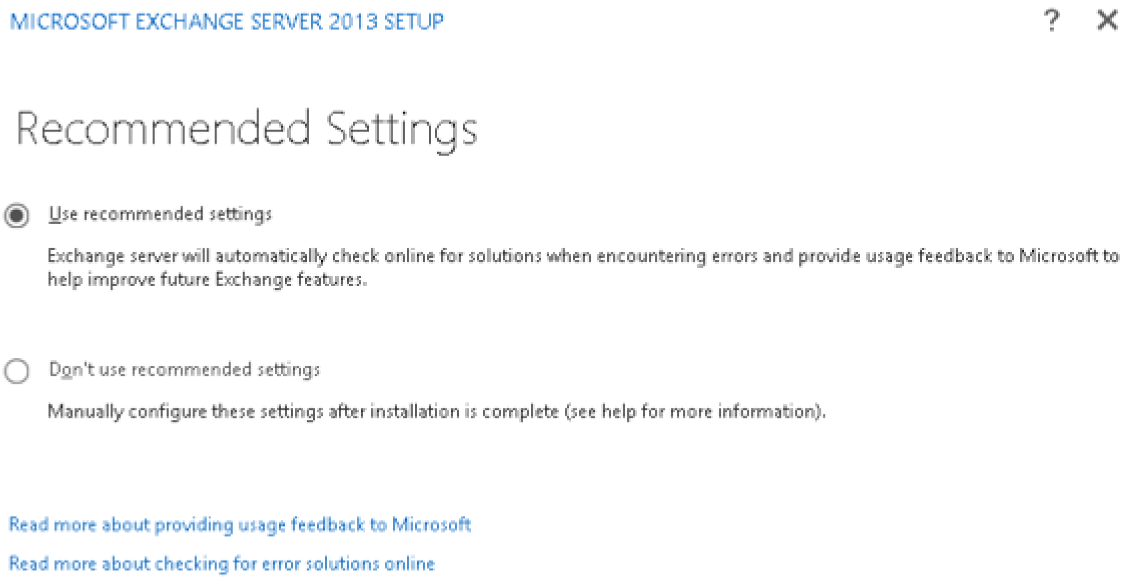
By using the software, you accept these terms. If you do not accept them, do not use the software. Instead, return it to the retailer for a refund or credit. If you cannot obtain a refund there, contact Microsoft or

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement.

Figure 34. License Agreement

- Choose whether or not to enable Error Reporting in figure 35 and proceed.



MICROSOFT EXCHANGE SERVER 2013 SETUP

Recommended Settings

● Use recommended settings

Exchange server will automatically check online for solutions when encountering errors and provide usage feedback to Microsoft to help improve future Exchange features.

○ Don't use recommended settings

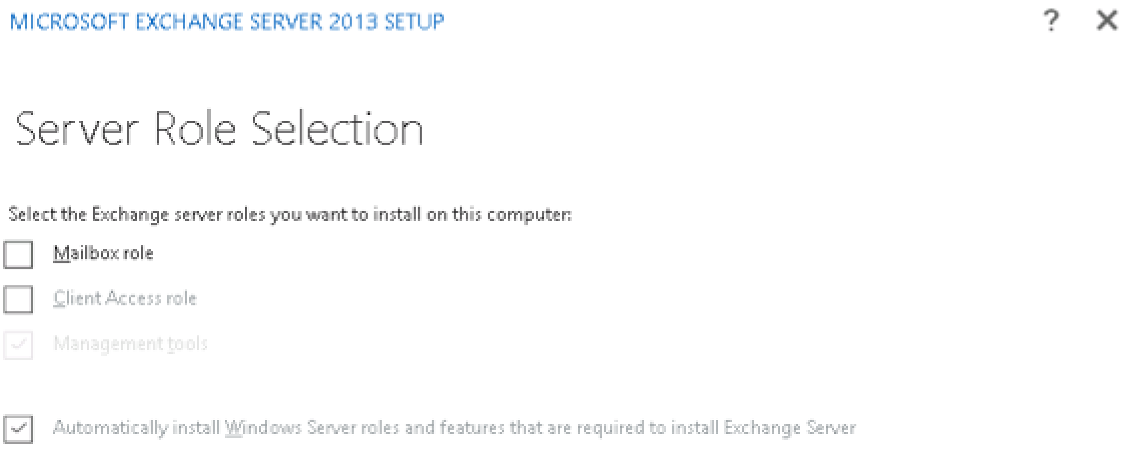
Manually configure these settings after installation is complete (see help for more information).

Read more about providing usage feedback to Microsoft

Read more about checking for error solutions online

Figure 35. Mailbox Settings

- Configure Exchange 2016 error reporting
- After a check that all the pre-requisites are installed the setup wizard will move on to the next step automatically (if the check was successful).
- Now choose the server roles to install. If this is the first server you're installing Microsoft recommends you install the Mailbox server role first. (Network Microsoft Developer, 2016)



MICROSOFT EXCHANGE SERVER 2013 SETUP

Server Role Selection

Select the Exchange server roles you want to install on this computer:

□ Mailbox role

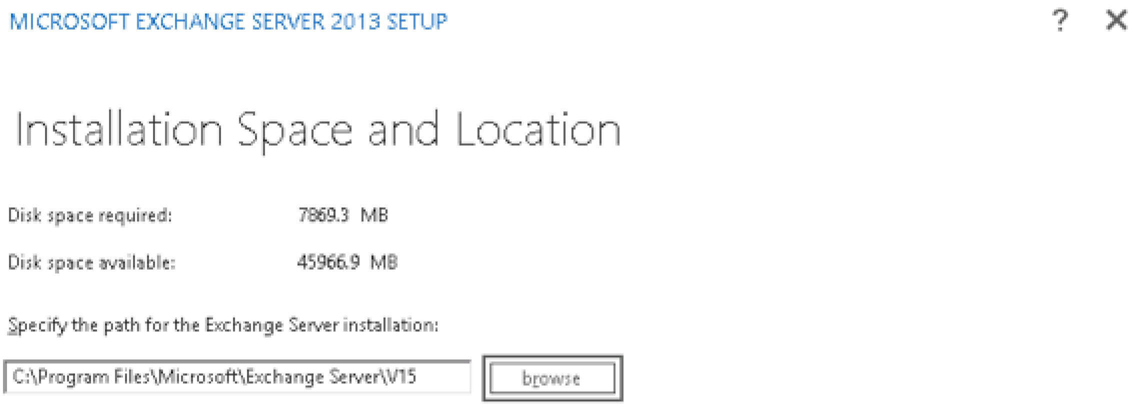
□ Client Access role

☑ Management tools

☑ Automatically install Windows Server roles and features that are required to install Exchange Server

Figure 36. Server Role Selection

- Verify that you have enough disk space for the installation, or choose a path that does have enough disk space, and click Next to continue.



MICROSOFT EXCHANGE SERVER 2013 SETUP

Installation Space and Location

Disk space required: 7869.3 MB

Disk space available: 45966.9 MB

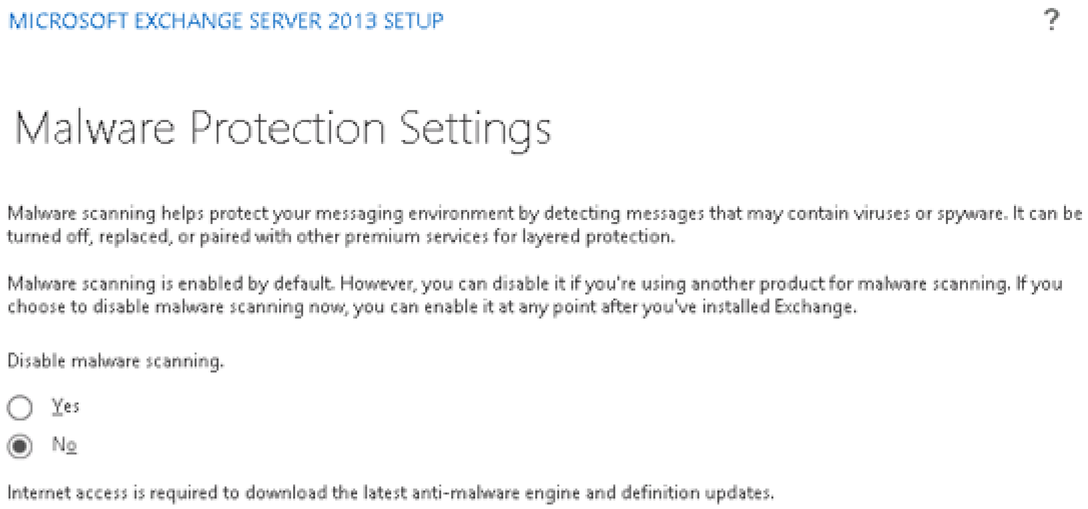
Specify the path for the Exchange Server installation:

C:\Program Files\Microsoft\Exchange Server\V15

Figure 37. Installation Space and Location

- If there is no existing Exchange organization in Active Directory, and you haven’t already prepared Active Directory for Exchange, you will be prompted to enter an Exchange organization name.

- When installing the Mailbox server role you are given the option to disable malware protection. If you disable it now you can enable it again later.



MICROSOFT EXCHANGE SERVER 2013 SETUP

Malware Protection Settings

Malware scanning helps protect your messaging environment by detecting messages that may contain viruses or spyware. It can be turned off, replaced, or paired with other premium services for layered protection.

Malware scanning is enabled by default. However, you can disable it if you're using another product for malware scanning. If you choose to disable malware scanning now, you can enable it at any point after you've installed Exchange.

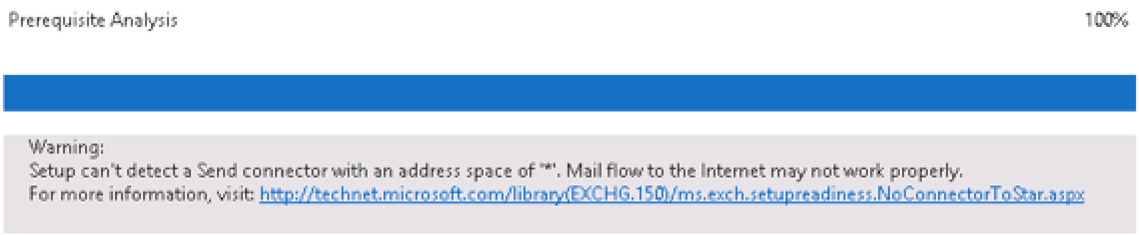
Disable malware scanning.

○ Yes
● No

Internet access is required to download the latest anti-malware engine and definition updates.

Figure 38. Malware Protection Settings

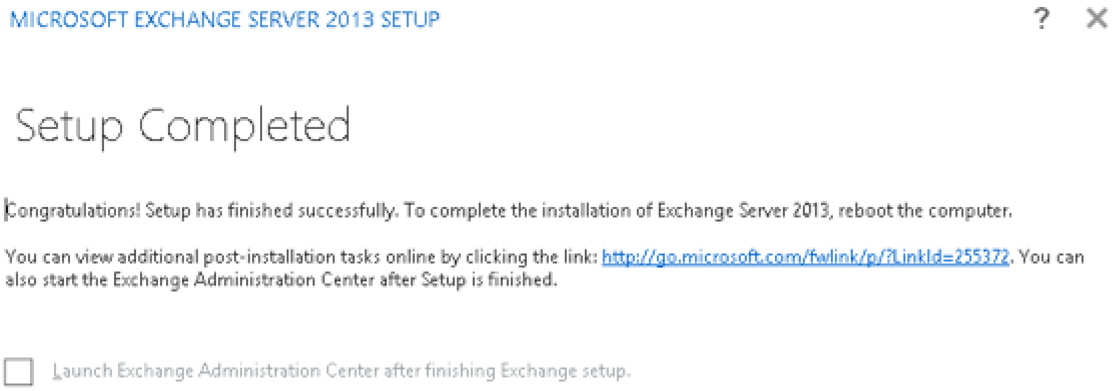
- Some readiness checks are performed. If this is the not the first server you're installing and there is no Send Connector defined for outbound email then you may see a warning, the server installation can still proceed.



Warning:
Setup can't detect a Send connector with an address space of "*". Mail flow to the Internet may not work properly.
For more information, visit: http://technet.microsoft.com/library(EXCHG.150)/ms.exch.setupreadiness.NoConnectorToStar.aspx

Figure 39. Warning Message

- Begin the installation of Exchange 2016



Setup Completed

Congratulations! Setup has finished successfully. To complete the installation of Exchange Server 2013, reboot the computer.

You can view additional post-installation tasks online by clicking the link: http://go.microsoft.com/fwlink/p/?LinkId=255372. You can also start the Exchange Administration Center after Setup is finished.

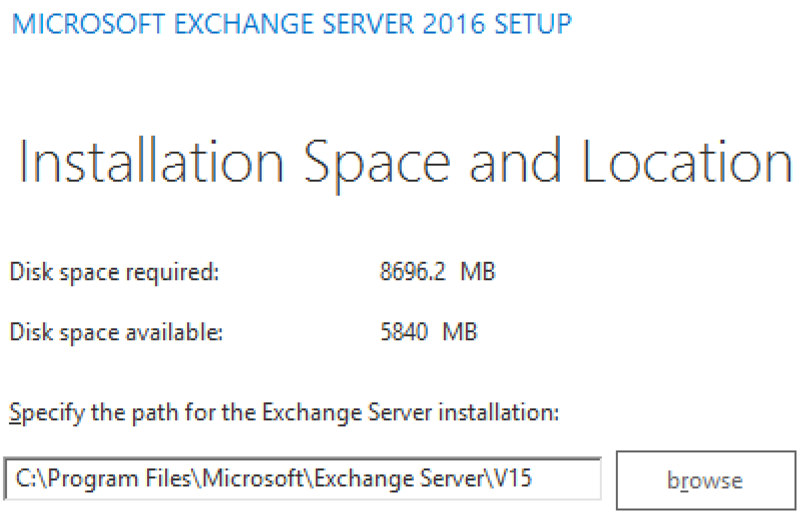
□ Launch Exchange Administration Center after finishing Exchange setup.

Figure 40. Setup Completed

- Figure 40 shows that the mailbox is successfully installed.

1.1.1 Installation Problems [Fixed]:

First problem was that my VM doesn't have enough space allocation for installation. Check figure 41.



MICROSOFT EXCHANGE SERVER 2016 SETUP

Installation Space and Location

Disk space required: 8696.2 MB

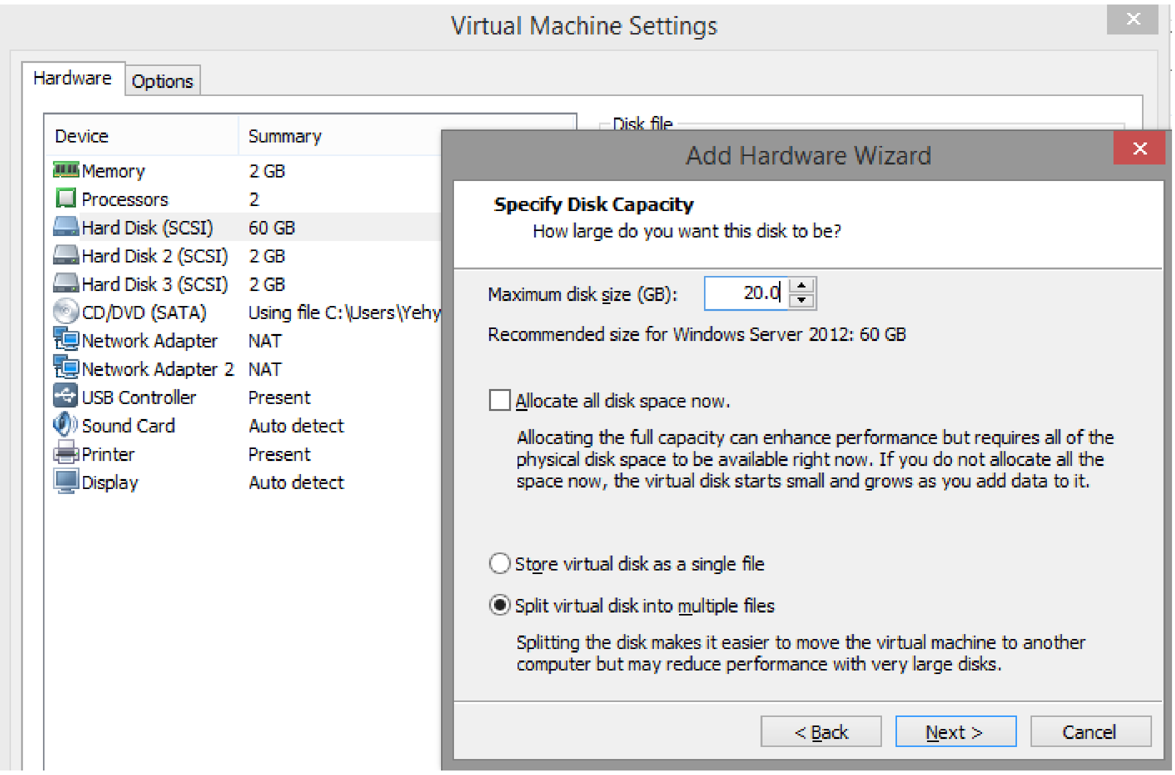
Disk space available: 5840 MB

Specify the path for the Exchange Server installation:

C:\Program Files\Microsoft\Exchange Server\V15

Figure 41. Not Enough Disk space

After shutting the PDC down, the HDD has been upgraded. A new drive was added to the virtual machine. Check figure 42.



Virtual Machine Settings

Device	Summary
Memory	2 GB
Processors	2
Hard Disk (SCSI)	60 GB
Hard Disk 2 (SCSI)	2 GB
Hard Disk 3 (SCSI)	2 GB
CD/DVD (SATA)	Using file C:\Users\Yehy
Network Adapter	NAT
Network Adapter 2	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Add Hardware Wizard

Specify Disk Capacity

How large do you want this disk to be?

Maximum disk size (GB): 20.0

Recommended size for Windows Server 2012: 60 GB

☐ Allocate all disk space now.

Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

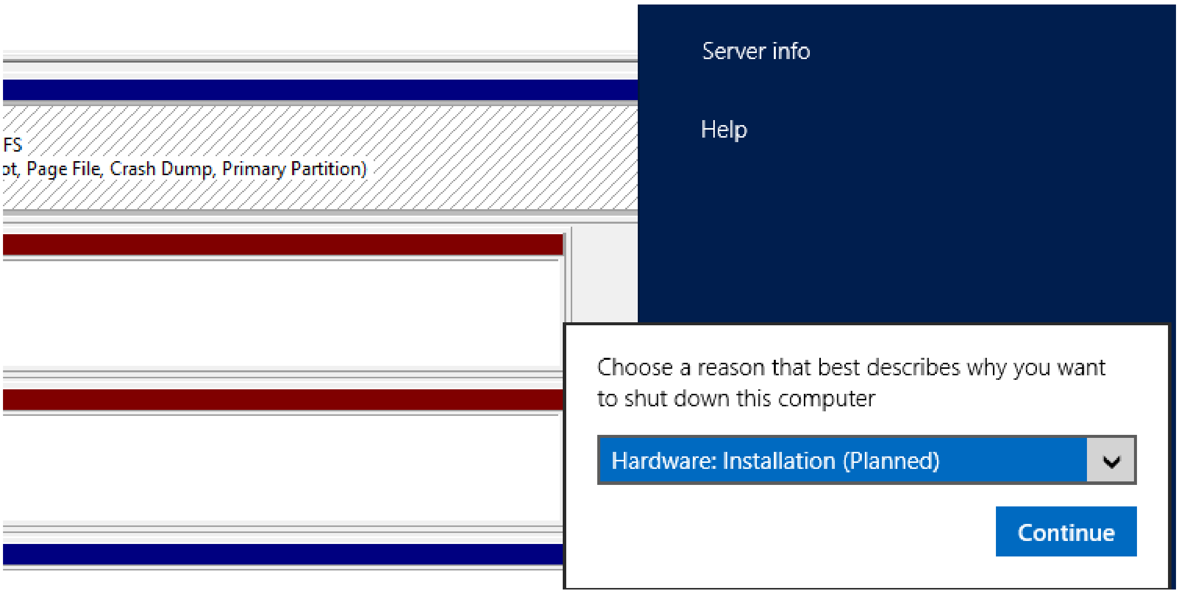
○ Store virtual disk as a single file

● Split virtual disk into multiple files

Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Figure 42. HDD upgrade

Rebooting the PDC requires a reason that describe the purpose. In this case, chose Hardware: Installation (planned) and press continue. Check figure 43.

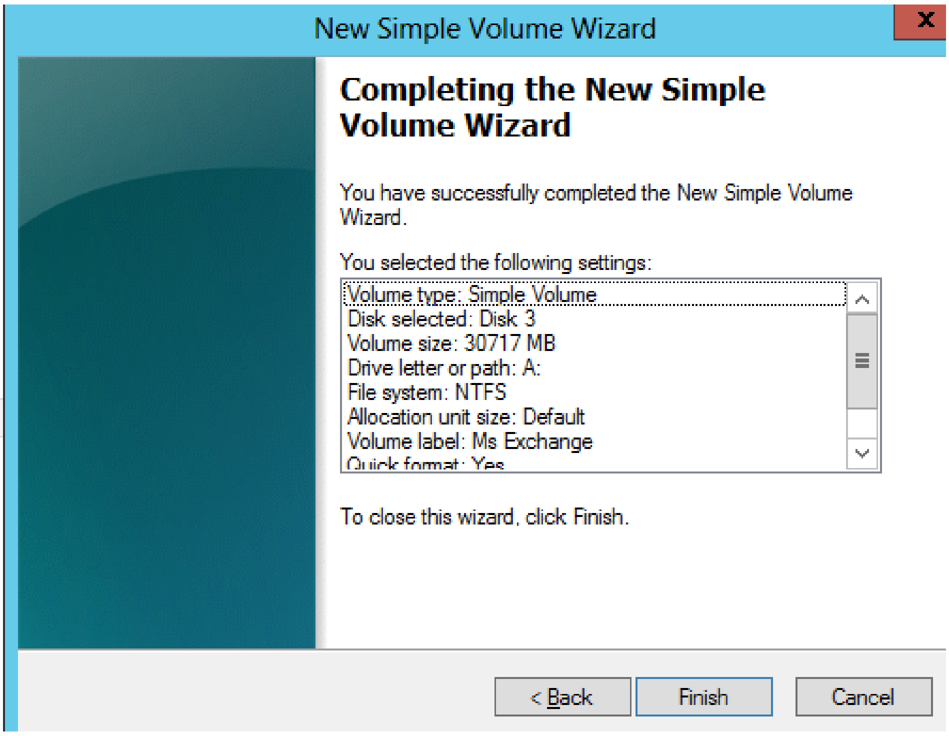


Choose a reason that best describes why you want to shut down this computer

Hardware: Installation (Planned)

Figure 43. Rebooting the PDC

After reboot, the disk is now in Offline state. Initializing the disk and configuring a new volume letter to it is required for accessing and allocating space. Check figure 44.



Completing the New Simple Volume Wizard

You have successfully completed the New Simple Volume Wizard.

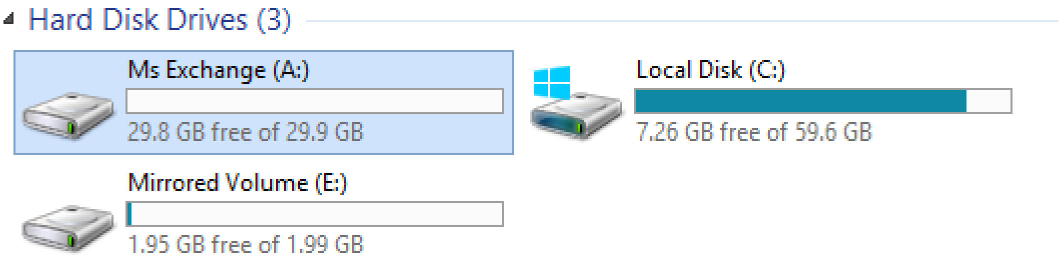
You selected the following settings:

Volume type: Simple Volume
Disk selected: Disk 3
Volume size: 30717 MB
Drive letter or path: A:
File system: NTFS
Allocation unit size: Default
Volume label: Ms Exchange
Quick format: Yes

To close this wizard, click Finish.

Figure 44. New HDD with 30GB

Finally after adding the hard disk, proceed for installation.



Hard Disk Drives (3)

Ms Exchange (A:)
29.8 GB free of 29.9 GB

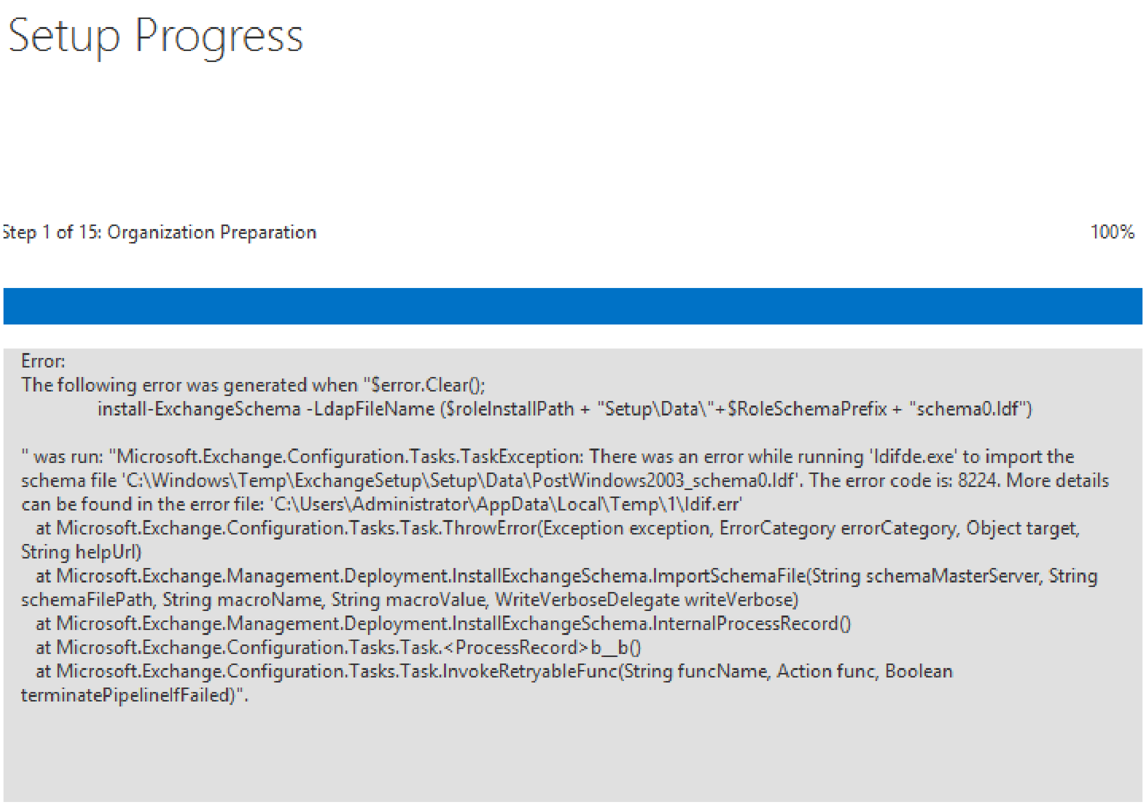
Local Disk (C:)
7.26 GB free of 59.6 GB

Mirrored Volume (E:)
1.95 GB free of 1.99 GB

Figure 45. Computer's HDDs

1.1.2 Installation Problems [Fixed]:

The following error shows every time the installation reaches prerequisite checks. Check figure 46.



Setup Progress

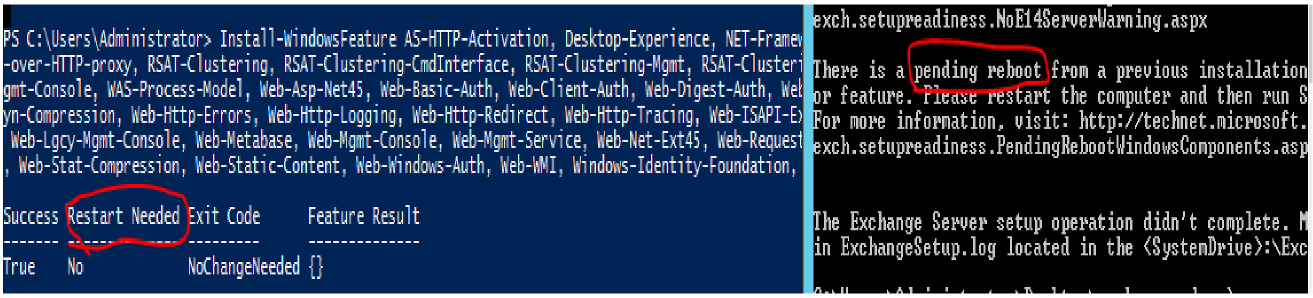
Step 1 of 15: Organization Preparation 100%

```
Error:
The following error was generated when "$error.Clear();
          install-ExchangeSchema -LdapFileName ($roleInstallPath + "Setup\Data\"+$RoleSchemaPrefix + "schema0.ldf")

" was run: "Microsoft.Exchange.Configuration.Tasks.TaskException: There was an error while running 'ldifde.exe' to import the
schema file 'C:\Windows\Temp\ExchangeSetup\Setup\Data\PostWindows2003_schema0.ldf'. The error code is: 8224. More details
can be found in the error file: 'C:\Users\Administrator\AppData\Local\Temp\1\ldif.err'
   at Microsoft.Exchange.Configuration.Tasks.Task.ThrowError(Exception exception, ErrorCategory errorCategory, Object target,
String helpUrl)
   at Microsoft.Exchange.Management.Deployment.InstallExchangeSchema.ImportSchemaFile(String schemaMasterServer, String
schemaFilePath, String macroName, String macroValue, WriteVerboseDelegate writeVerbose)
   at Microsoft.Exchange.Management.Deployment.InstallExchangeSchema.InternalProcessRecord()
   at Microsoft.Exchange.Configuration.Tasks.Task.<ProcessRecord>b__b()
   at Microsoft.Exchange.Configuration.Tasks.Task.InvokeRetryableFunc(String funcName, Action func, Boolean
terminatePipelineIfFailed)".
```

Figure 46. Error upon installation

This error message has error code. Searching for solutions lead for reinstalling the Ms Exchange through command-line interface.

Through the installation process, problems were faced. Some of these problems were in the prerequisite analysis.



```
PS C:\Users\Administrator> Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience, NET-Framew
-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clusteri
gmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web
yn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ex
 Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request
, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation,

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             NoChangeNeeded {}
```

```
exch.setupreadiness.NoE14ServerWarning.aspx

There is a pending reboot from a previous installation
or feature. Please restart the computer and then run S
For more information, visit: http://technet.microsoft.
exch.setupreadiness.PendingRebootWindowsComponents.asp


The Exchange Server setup operation didn't complete. M
in ExchangeSetup.log located in the <SystemDrive>:\Exc
```

Figure 47. Conflict between troubleshooting and installation.

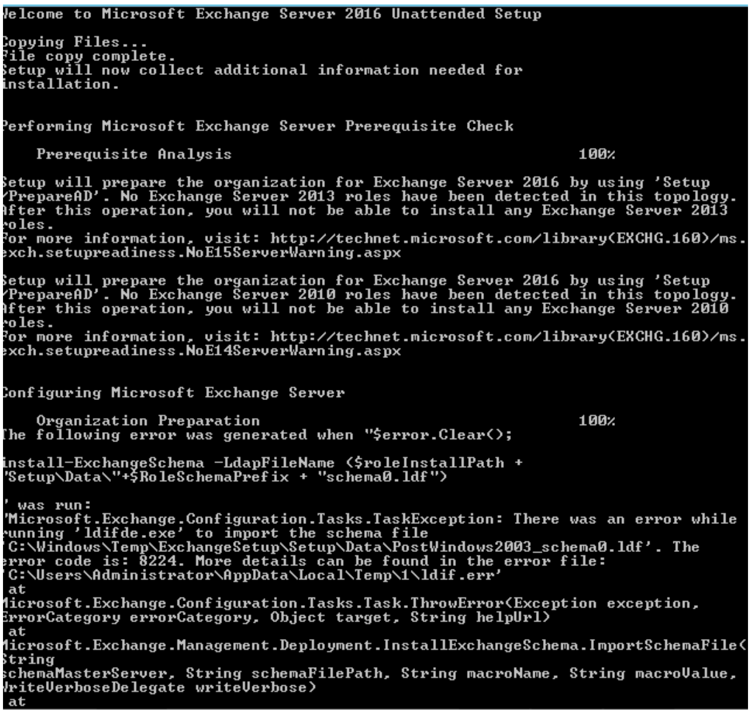
As shown in figure 44, there was a conflict that was not fixed. The blue screen on the left is the Windows power shell. Testing prerequisite is done through windows power shell. However, the result shows that PDC's core roles are existing and no restart needed. During command-line installation, the error on the right shows that a restart is required. After restarting the PDC, the following error keeps on showing, and Microsoft Exchange could not be installed using GUI.

1.1.2.1 Installing Exchange Server 2016 through CMD

As mentioned before, running a line of code can initiate a process for installing Exchange Server. To make sure that the environment is ready for installation, a couple of codes should be used first.

```
Setup /PrepareSchema /IAcceptExchangeServerLicenseTerms
/OrganizationName:GU
```

The same error has been encounter. However, this time the error message has a different error code, and some error log files generated as shown in figure 48. These error files has some important LDIF information.

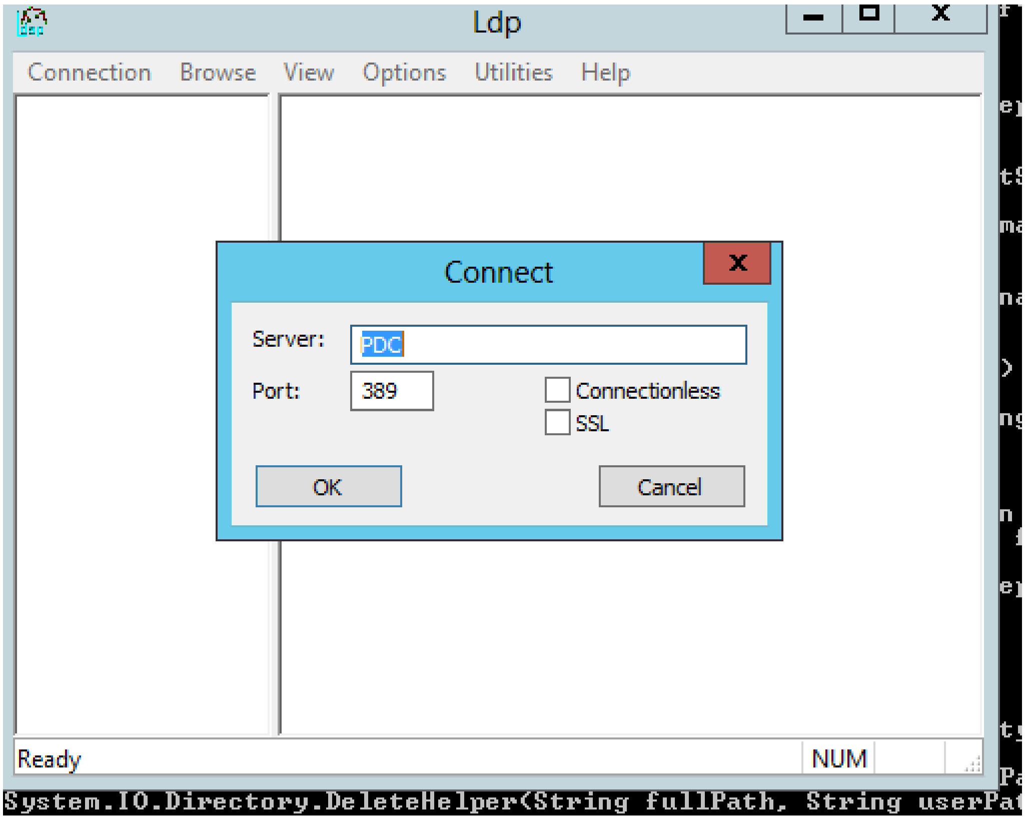


```
Welcome to Microsoft Exchange Server 2016 Unattended Setup

Copying Files...
File copy complete.
Setup will now collect additional information needed for
installation.


Performing Microsoft Exchange Server Prerequisite Check

    Prerequisite Analysis                                      100%

Setup will prepare the organization for Exchange Server 2016 by using 'Setup
/PrepareAD'. No Exchange Server 2013 roles have been detected in this topology.
After this operation, you will not be able to install any Exchange Server 2013
roles.
For more information, visit: http://technet.microsoft.com/library(EXCHG.160)/ms.
exch.setupreadiness.NoE15ServerWarning.aspx

Setup will prepare the organization for Exchange Server 2016 by using 'Setup
/PrepareAD'. No Exchange Server 2010 roles have been detected in this topology.
After this operation, you will not be able to install any Exchange Server 2010
roles.
For more information, visit: http://technet.microsoft.com/library(EXCHG.160)/ms.
exch.setupreadiness.NoE14ServerWarning.aspx


Configuring Microsoft Exchange Server

    Organization Preparation                                   100%
The following error was generated when "$error.Clear();

install-ExchangeSchema -LdapFileName ($roleInstallPath +
"Setup\Data\"+$RoleSchemaPrefix + "schema0.ldf")

" was run:
"Microsoft.Exchange.Configuration.Tasks.TaskException: There was an error while
running 'ldifde.exe' to import the schema file
'C:\Windows\Temp\ExchangeSetup\Setup\Data\PostWindows2003_schema0.ldf'. The
error code is: 8224. More details can be found in the error file:
'C:\Users\Administrator\AppData\Local\Temp\1\ldif.err'
 at
Microsoft.Exchange.Configuration.Tasks.Task.ThrowError(Exception exception,
ErrorCategory errorCategory, Object target, String helpUrl)
 at
Microsoft.Exchange.Management.Deployment.InstallExchangeSchema.ImportSchemaFile(
String
schemaMasterServer, String schemaFilePath, String macroName, String macroValue,
WriteVerboseDelegate writeVerbose)
 at
```

Figure 48. cmd error message

The Exchange Server setup operation didn't complete. More details can be foundin ExchangeSetup.log located in the <SystemDrive>:\ExchangeSetupLogs folder.

Using LDAP tool to connect to database, first open cmd and type ldp.exe, then connect to the Server as shown in figure 49 using port 389. The following is the error:



Server: PDC

Port: 389

□ Connectionless

□ SSL

```
System.IO.Directory.DeleteHelper(String fullPath, String userPat
```

Figure 49. Establishing connection to PDC for troubleshooting the error message

```
  The following error was generated when "$error.Clear();
        install-ExchangeSchema -LdapFileName ($roleInstallPath +
"Setup\Data\"+$RoleSchemaPrefix + "schema89.ldf")

" was run: "Microsoft.Exchange.Configuration.Tasks.TaskException: There
was an error while running 'ldifde.exe' to impor
t the schema file
'C:\Windows\Temp\ExchangeSetup\Setup\Data\schema89.ldf'. The error code
is: 8245. More details can be
found in the error file: 'C:\Users\rbbr\AppData\Local\Temp\ldif.err'
   at Microsoft.Exchange.Configuration.Tasks.Task.ThrowError(Exception
exception, ErrorCategory errorCategory, Object ta
rget, String helpUrl)
   at
Microsoft.Exchange.Management.Deployment.InstallExchangeSchema.ImportSche
maFile(String schemaMasterServer, String
schemaFilePath, String macroName, String macroValue, WriteVerboseDelegate
writeVerbose)
   at
Microsoft.Exchange.Management.Deployment.InstallExchangeSchema.InternalPr
ocessRecord()
   at Microsoft.Exchange.Configuration.Tasks.Task.<ProcessRecord>b__b()
   at
Microsoft.Exchange.Configuration.Tasks.Task.InvokeRetryableFunc(String
funcName, Action func, Boolean terminatePip
elineIfFailed)".


The Exchange Server setup operation didn't complete. More details can be
found in ExchangeSetup.log located in the
<SystemDrive>:\ExchangeSetupLogs folder.
```

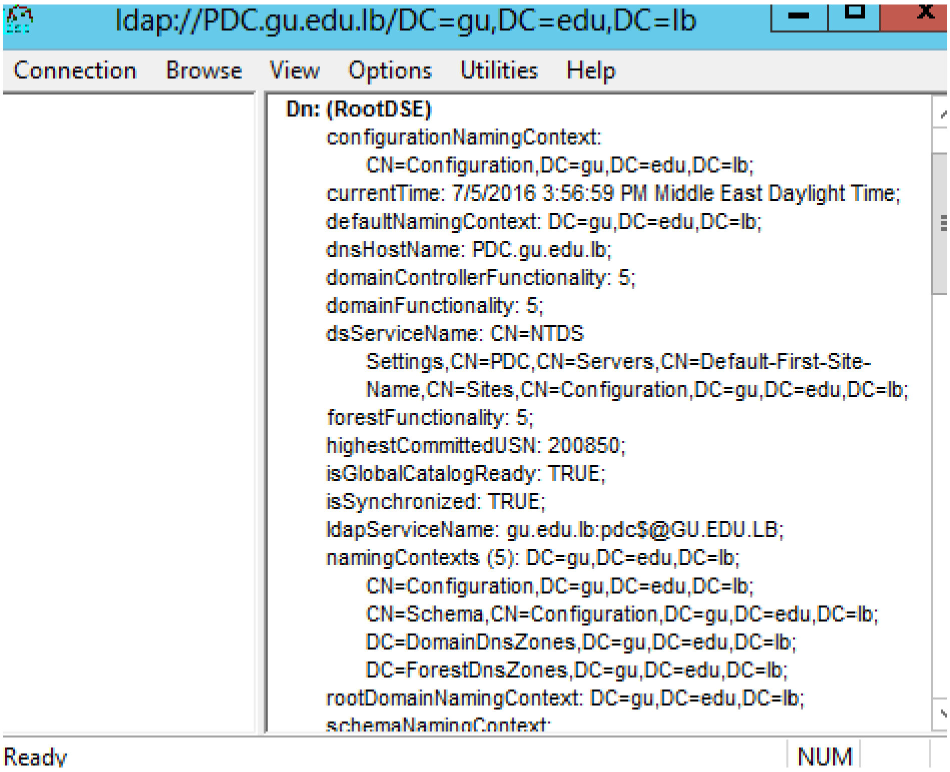
And the ldif log says:

```
Entry DN: CN=ms-DS-GeoCoordinates-
Altitude,CN=Schema,CN=Configuration,DC=Gu,DC=edu,DC=lb
Add error on entry starting on line 452: Unwilling To Perform

The server side error is: 0x20bb Schema update failed: duplicate OID.

The extended server error is:

000020BB: SvcErr: DSID-032603C0, problem 5003 (WILL_NOT_PERFORM), data
8379


An error has occurred in the program
```

What I did:

1. Backed the Domain.
2. Made sure I am logged in to the schema master DC, and are a member of Schema Admins and Enterprise Admins (not sure if this one is needed, but I was).
3. Opened up LDIF.err in a text editor to see exactly which attribute caused the error (in my case it was "ms-DS-GeoCoordinates-Altitude").
4. Run LDP.exe, connect to your schema master and bind to it.
5. Go to "Browse" > "Modify".
6. Leave the DN blank, and type "schemaUpgradeInProgress" into the *attribut*e field, and enter a "1" into the *value* field. Leave *operation* as "add" and click the "Enter" button, then "Run". This will mark the schema as being in the progress of being upgraded and will allow to do things that you normally wouldn't have permissions to.
7. Go to "View" > "Tree" and connect to the base DN where you had the error ("CN=Schema,CN=Configuration...").
8. On the left side of the window, find the specified erroneous attribute. For me, I found "CN=ms-DS-GeoCoordinates-Altitude\0ACNF:{*someGUID*}...". To fix the error, I needed to rename that attribute to the correct name.
9. Right click the entry to rename, and select "Modify DN".
10. Copy the name of the "Old DN", paste it into the "New DN" field but remove the "\0ACNF:{*someGUID*}" bit.
11. Click "Run", and the attribute should be renamed.
12. Mark the schema back as not being in the progress of an upgrade by doing steps 4-5 again, but setting the value as "0” instead of "1".

Unfortunately, same error kept on showing, check figure 50. But on the other side, a new information was found, which "Cannot authenticate user".
Installing Exchange Server will never occur if the currently logged on user doesn't have privilege.



```
Dn: (RootDSE)
    configurationNamingContext:
        CN=Configuration,DC=gu,DC=edu,DC=lb;
    currentTime: 7/5/2016 3:56:59 PM Middle East Daylight Time;
    defaultNamingContext: DC=gu,DC=edu,DC=lb;
    dnsHostName: PDC.gu.edu.lb;
    domainControllerFunctionality: 5;
    domainFunctionality: 5;
    dsServiceName: CN=NTDS
        Settings,CN=PDC,CN=Servers,CN=Default-First-Site-
        Name,CN=Sites,CN=Configuration,DC=gu,DC=edu,DC=lb;
    forestFunctionality: 5;
    highestCommittedUSN: 200850;
    isGlobalCatalogReady: TRUE;
    isSynchronized: TRUE;
    ldapServiceName: gu.edu.lb:pdc$@GU.EDU.LB;
    namingContexts (5): DC=gu,DC=edu,DC=lb;
        CN=Configuration,DC=gu,DC=edu,DC=lb;
        CN=Schema,CN=Configuration,DC=gu,DC=edu,DC=lb;
        DC=DomainDnsZones,DC=gu,DC=edu,DC=lb;
        DC=ForestDnsZones,DC=gu,DC=edu,DC=lb;
    rootDomainNamingContext: DC=gu,DC=edu,DC=lb;
    schemaNamingContext:
```

Figure 50. LDAP connection for administering the PDC

The user **GuAdmin** was added to **SchemaAdmins** group, and the installation is repeated. Figure 51 shows that the prerequisite test, and copying file phase have passed. However, figure 52 shows an error occurred during installation. The solution left was to install Exchange on a new VM.

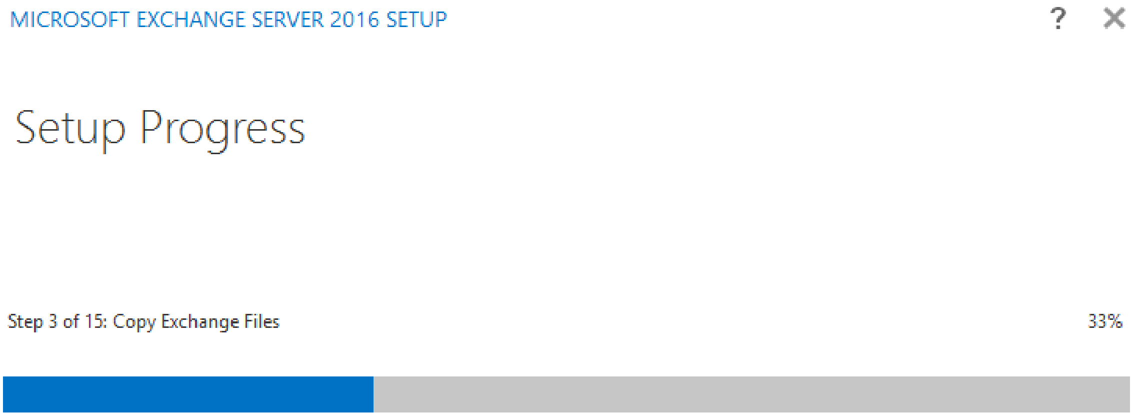
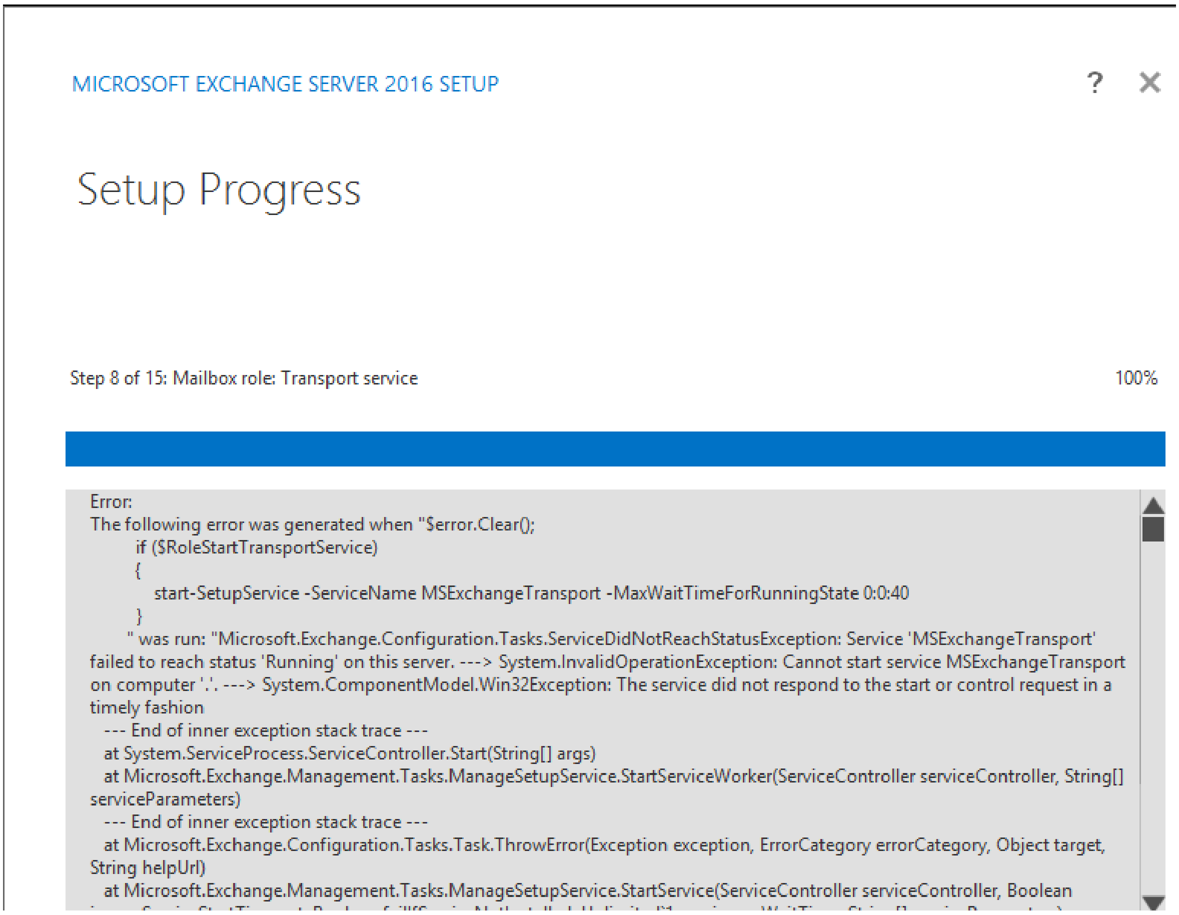

MICROSOFT EXCHANGE SERVER 2016 SETUP
?
✕
Setup Progress
Step 3 of 15: Copy Exchange Files
33%

Figure 51. Setup is in Progress



Setup Progress

Step 8 of 15: Mailbox role: Transport service 100%

```
Error:
The following error was generated when "$error.Clear();
        if ($RoleStartTransportService)
        {
           start-SetupService -ServiceName MSExchangeTransport -MaxWaitTimeForRunningState 0:0:40
        }
      " was run: "Microsoft.Exchange.Configuration.Tasks.ServiceDidNotReachStatusException: Service 'MSExchangeTransport'
failed to reach status 'Running' on this server. ---> System.InvalidOperationException: Cannot start service MSExchangeTransport
on computer '.'. ---> System.ComponentModel.Win32Exception: The service did not respond to the start or control request in a
timely fashion
   --- End of inner exception stack trace ---
   at System.ServiceProcess.ServiceController.Start(String[] args)
   at Microsoft.Exchange.Management.Tasks.ManageSetupService.StartServiceWorker(ServiceController serviceController, String[]
serviceParameters)
   --- End of inner exception stack trace ---
   at Microsoft.Exchange.Configuration.Tasks.Task.ThrowError(Exception exception, ErrorCategory errorCategory, Object target,
String helpUrl)
   at Microsoft.Exchange.Management.Tasks.ManageSetupService.StartService(ServiceController serviceController, Boolean
```

Figure 52. Error while installation

Installing 802.1x Wi-Fi Radius server

It is also referred to as WPA-802.1X mode, and sometimes just WPA (as opposed to WPA-PSK), this is designed for enterprise networks and requires a RADIUS authentication server. This requires a more complicated setup, but provides additional security (e.g. protection against dictionary attacks on short passwords). Various kinds of the Extensible Authentication Protocol (EAP) are used for authentication. WPA-Enterprise mode is available with both WPA and WPA2. (Afra, 2013; Server world, 2012)

Figure 53 describe how the authentication process occurs

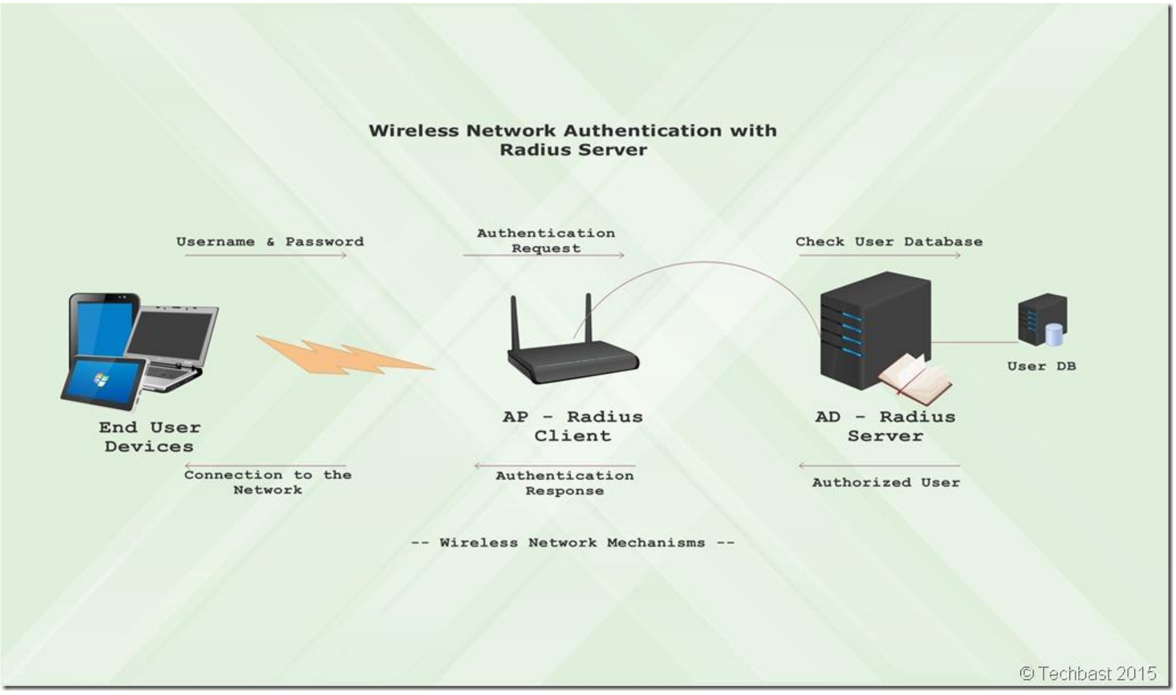


Figure 53. Wireless Network Authentication with 802.1x

WPA has been designed specifically to work with wireless hardware produced prior to the introduction of WPA protocol, which provides inadequate security through WEP (Stanek, 2008; Afra, 2013). WPA2 replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance (Server world, 2012). The benefits of using this type of encryption is:

- End-users can logon with usernames and passwords.
- End-users securely receive unique encryption keys at each session.
- Administrator can change the login credentials and revoke access per user.
- This mode provides better encryption key security.

In order to create an infrastructure for authentication, authorization, and accounting for protected wireless connections for an organization using Windows wireless clients, the following steps need to be completed:

- Configure the certificate infrastructure.
- Configure Active Directory for accounts and groups.
- Configure the wireless Access Point.
- Configure the NPS server on a computer.
- Configure Wireless Network (IEEE 802.11) Policies Group Policy settings.
- Configure wireless clients for EAP-TLS or PEAP-TLS.

Configuring the certificate infrastructure

Regardless of which authentication method used for wireless connections, computer certificates must be installed on the NPS servers. (Dan Holme, 2008)

For PEAP-MS-CHAP v2, there is no need to deploy a certificate infrastructure to issue computer and user certificates for each wireless client computer. Instead, you can obtain individual certificates for each NPS server from a commercial CA and install them on the NPS servers. (Microsoft Developer Network, 2016)

For computer authentication with EAP-TLS or PEAP-TLS, a computer certificate, also known as a machine certificate, must be installed on each wireless client computer. For user authentication with EAP-TLS or PEAP-TLS after a network connection is made and the user logs on, a user must use certificate on the wireless client computer. (Stanek, 2008)

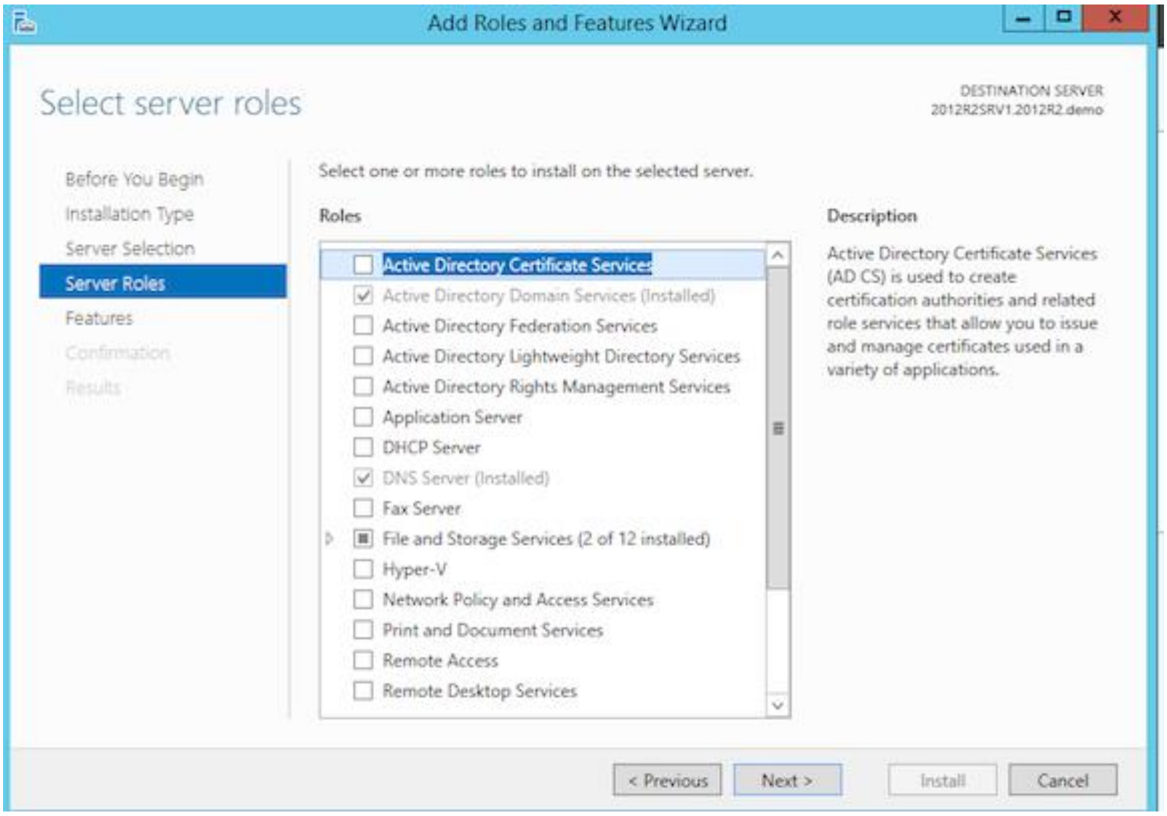
In order to create Certificate Infrastructure, the below steps should be taken:

- Installing a Certificate Infrastructure
- Installing Computer Certificates
- Installing User Certificates

Installing a Certificate Infrastructure

From the Windows Server 2012 R2 Server Manager, click Add Roles and Features.

- Select Active Directory Certificate Services.



Select server roles

DESTINATION SERVER
2012R2SRV1.2012R2.demo

Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☐ DHCP Server
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ▣ File and Storage Services (2 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

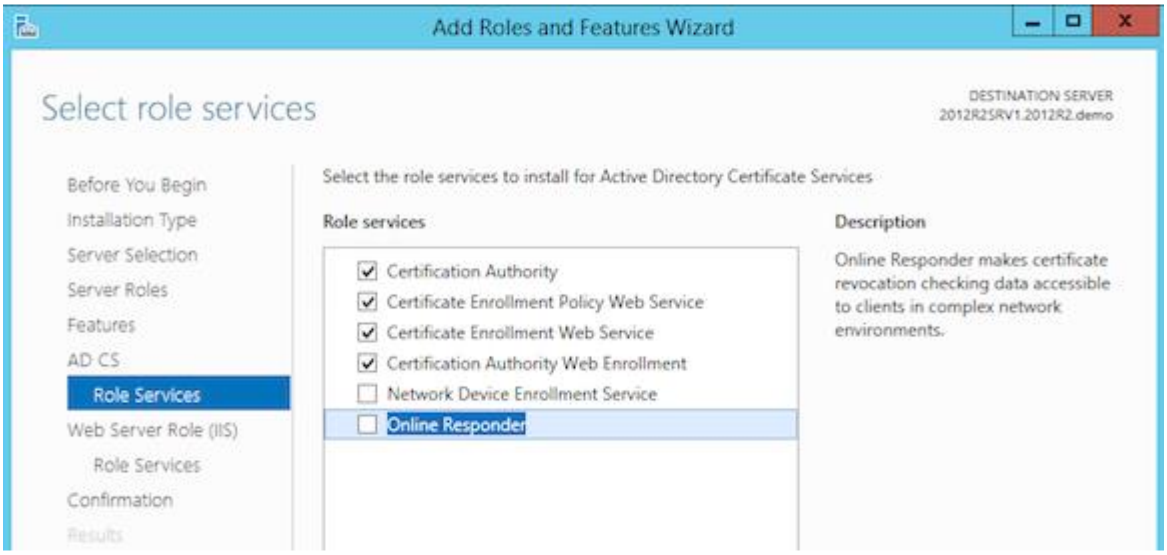
Figure 54. Server roles selection

- Install Active Directory Certificate Authority
- Click the Add Features in the popup window to allow installation of the Certification Authority Management Tools
- Install Active Directory Certificate Authority add roles

Select the following services:

- Certification Authority (this is your main CA)
- Certification Enrollment Policy Web Service
- Certificate Enrollment Web Service (web portal to request certificates)

Certification Web Enrollment



Select role services

DESTINATION SERVER
2012R2SRV1.2012R2.demo

Select the role services to install for Active Directory Certificate Services

Role services

- ☑ Certification Authority
- ☑ Certificate Enrollment Policy Web Service
- ☑ Certificate Enrollment Web Service
- ☑ Certification Authority Web Enrollment
- ☐ Network Device Enrollment Service
- ☐ Online Responder

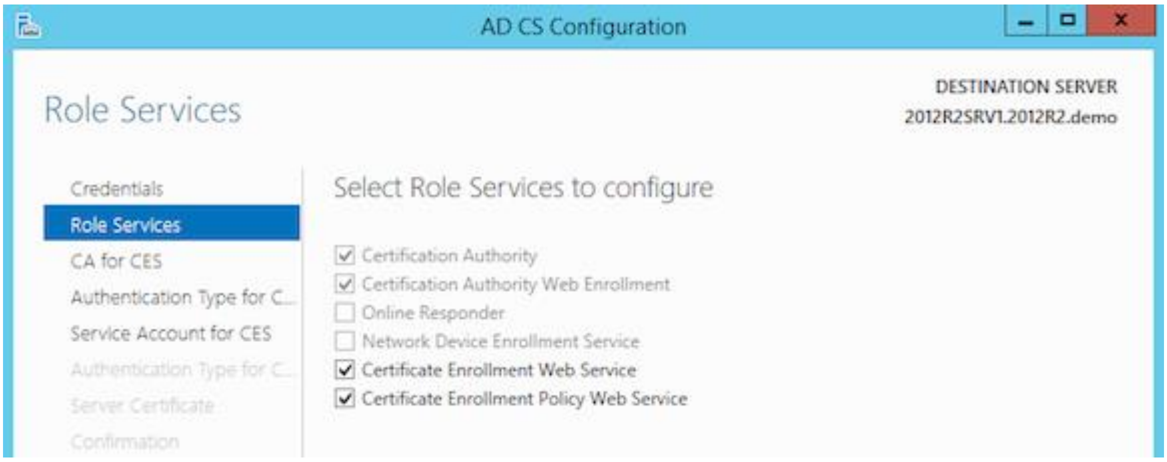
Description

Online Responder makes certificate revocation checking data accessible to clients in complex network environments.

Figure 55. Role Services selection

- Once installed, Select AD CS in your Server Manager

- Accept the default database locations or modify according your own requirements.
- This completes the configuration of the first two CA components. Let's continue with the other two. In the Select Role Services to configure, choose Certificate Enrollment Web Service and Certificate Enrollment Web Policy Service.



Role Services

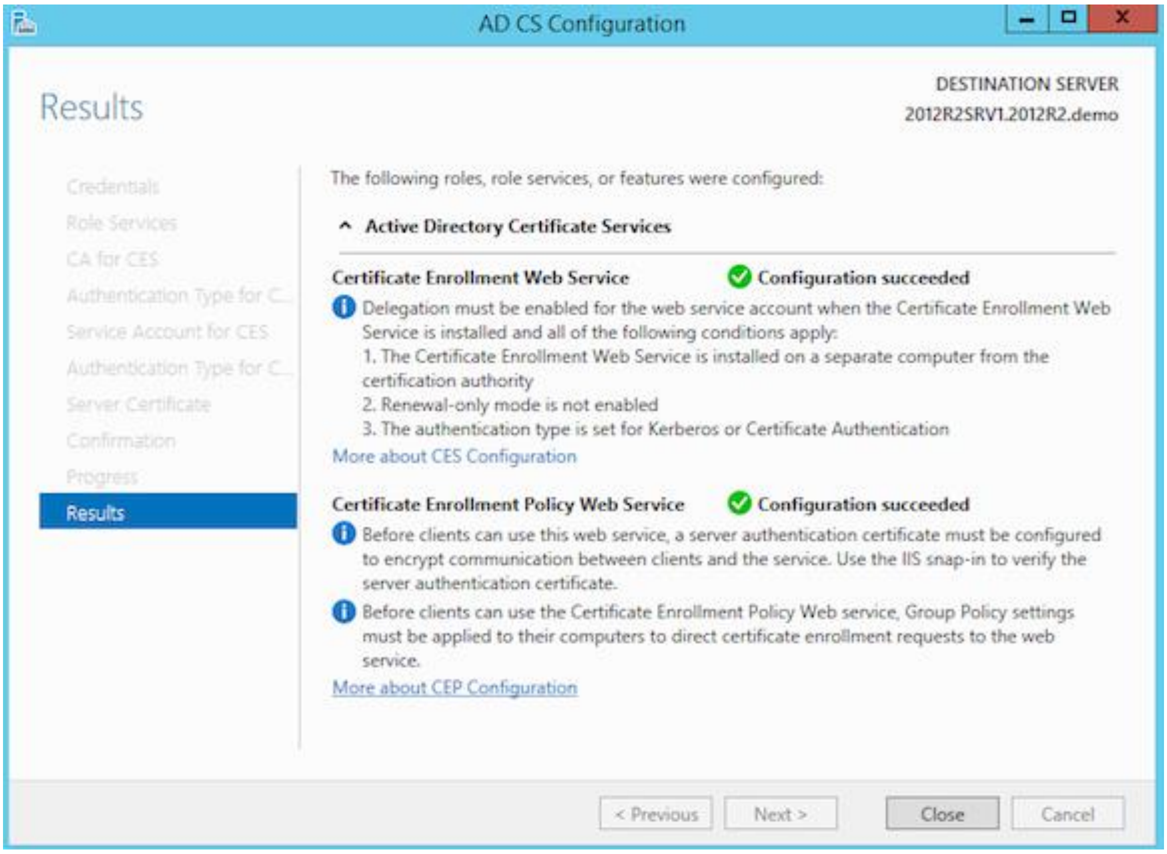
DESTINATION SERVER
2012R2SRV1.2012R2.demo

Select Role Services to configure

- ☑ Certification Authority
- ☑ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☑ Certificate Enrollment Web Service
- ☑ Certificate Enrollment Policy Web Service

Figure 56. Select Role Service to configure

Figure 57 shows that the configuration of all required Certificate Authority services succeeded.



The following roles, role services, or features were configured:

Active Directory Certificate Services

Certificate Enrollment Web Service ✓ Configuration succeeded

Delegation must be enabled for the web service account when the Certificate Enrollment Web Service is installed and all of the following conditions apply:
1. The Certificate Enrollment Web Service is installed on a separate computer from the certification authority
2. Renewal-only mode is not enabled
3. The authentication type is set for Kerberos or Certificate Authentication

More about CES Configuration

Certificate Enrollment Policy Web Service ✓ Configuration succeeded

Before clients can use this web service, a server authentication certificate must be configured to encrypt communication between clients and the service. Use the IIS snap-in to verify the server authentication certificate.

Before clients can use the Certificate Enrollment Policy Web service, Group Policy settings must be applied to their computers to direct certificate enrollment requests to the web service.

More about CEP Configuration

Figure 57. Results of AD CS Configuration

Installing Computer Certificates

To configure automatic certificate allocation from an enterprise CA:

- Open Active Directory Users and Computers.
- In the console tree, double-click Active Directory Users and Computers, right-click the domain name in which your CA lives, and then click Properties.
- On the Group Policy tab, click Default Domain Policy, and then click Edit.
- In the console tree, right-click Automatic Certificate Request Settings, point to New, and then click Automatic Certificate Request.
- Go to Computer Configuration/Windows Settings/Security Settings/Public Key Policies/Automatic Certificate Request Settings
- When the Automatic Certificate Request wizard appears, click Next.
- In Certificate templates, click Computer, and then click Next.
- Your enterprise root CA appears on the list.
- Click the CA, click Next, and then click Finish.

- To create a computer certificate for the CA computer, type the following at the command prompt:

```
gpupdate /target:Computer
```

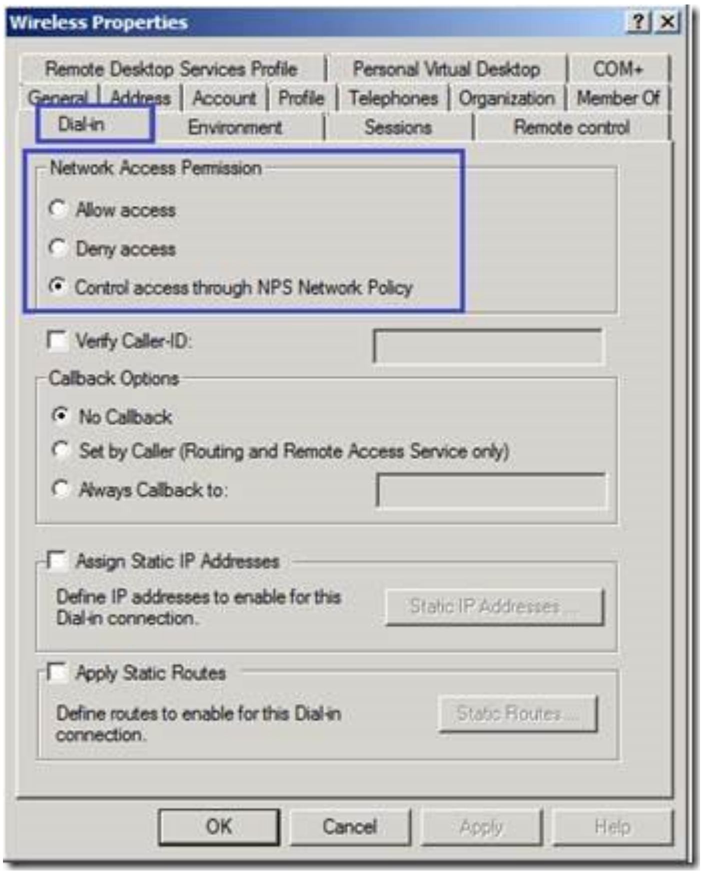
Installing User Certificates

Configuring Active Directory for Accounts and Groups

Once the Certificate Infrastructure is ready, you need to configure AD accounts and groups. To configure Active Directory user and computer accounts and groups for wireless access, do the following:

- Create a USER account for all users who would make wireless connections.
- Create a COMPUTER account for all computers that would use wireless connections.

· Set the remote access permission on user and computer accounts to the appropriate setting (either Allow access or Control access through Remote Access Policy) as shown in figure 58.



Wireless Properties

Network Access Permission
○ Allow access
○ Deny access
● Control access through NPS Network Policy

□ Verify Caller-ID:

Callback Options
● No Callback
○ Set by Caller (Routing and Remote Access Service only)
○ Always Callback to:

□ Assign Static IP Addresses
Define IP addresses to enable for this Dial-in connection.

□ Apply Static Routes
Define routes to enable for this Dial-in connection.

Figure 58.   Wireless Properties

Configuring the Wireless Access Point

The next step is to deploy the wireless Access Point, in this scenario the APN is U.S Robotics. The AP needs to be configured to support WPA, WPA2 or WEP encryption with 802.1X authentication. (Dan Holme, 2008) Additionally, configure RADIUS settings on your wireless AP switches with the following:

- The IP address or name of the RADIUS server
- The RADIUS shared secret
- UDP ports for authentication and accounting, and failure detection settings.

If the wireless APs require vendor specific attributes (VSAs) or additional RADIUS attributes, you must add the VSAs or attributes to the remote access policies of the IAS/NPS servers.

Configuring the NPS Server

Now the RADIUS Server needs to be configured. The steps needed are:

- Install the NPS server role on the server.
- Install the Certificate on the NPS.
- Add the access point as a RADIUS Client.
- Create the connection request policies and network policies required.

· The NPS server requires a certificate. You can use the RAS and IAS certificate template to create a new template to use for NPS servers. The link below discusses configuring this template and enabling it for auto-enrollment:

Configuring Wireless Network (IEEE 802.11) Policies Group Policy Settings

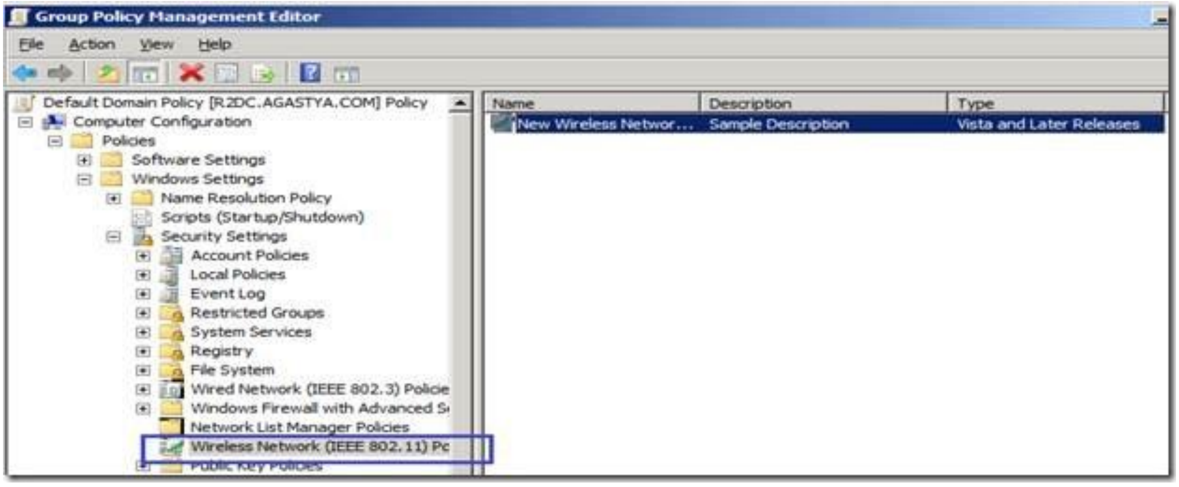
To configure Wireless Network Policies Group Policy settings, do the following:

1. Open the Active Directory Users and Computers snap-in.

2. In the console tree, double-click Active Directory Users and Computers, right-click the domain container that contains your wireless computer accounts, and then click Properties.

3. On the Group Policy tab, click the appropriate Group Policy object (the default object is Default Domain Policy), and then click Edit.

4. In the console tree, as shown in figure 59, open Computer Configuration, then Windows Settings, then Security Settings, then Wireless Network (IEEE 802.11) Policies.



Name	Description	Type
New Wireless Networ...	Sample Description	Vista and Later Releases

Figure 59. *GPOME console*

5. Right-click Wireless Network (IEEE 802.11) Policies and then click Create Wireless Network Policy. In the Wireless Network Policy Wizard, type a name and description.

6. In the details pane, double-click your newly created wireless network policy.

7. Change settings on the General tab as needed.

8. Click Add to add a preferred network.

9. On the Network Properties tab, type the wireless network name (SSID) and change wireless network key settings as needed.

10. Click the IEEE 802.1x tab. Change 802.1X settings as needed, including specifying and configuring the correct EAP type. Click OK twice to save changes

Configuring Wireless Clients Authentication

If you are using EAP-TLS or PEAP-TLS, you need to install computer and user certificates on wireless clients. If the domain is configured for auto-enrollment of computer certificates, each computer that is a member of the domain requests a computer certificate when Computer Configuration Group Policy is refreshed. To force a refresh of Computer Configuration Group Policy for a computer running Windows 7, Windows XP, or Windows Server 2003, restart the computer or type `gpupdate /target:computer` at a command prompt.

For user authentication with EAP-TLS, a locally installed user certificate or a smart card must be used. The locally installed user certificate must be obtained through auto-enrollment, Web enrollment, by requesting the certificate using the Certificates snap-in, by importing a certificate file, or by running a CAPICOM program or script.

If you have configured auto-enrollment of user certificates, then the wireless user must update their User Configuration Group Policy to obtain a user certificate. If you are not using auto-enrollment for user certificates, use one of the following procedures to obtain a user certificate:

- Submit a user certificate request via the Web
- Request a certificate with the Certificates snap-in

If you have configured settings for the Wireless Network (IEEE 802.11) Policies Group Policy extension and specified the authentication type wireless network, no other configuration is needed for wireless.

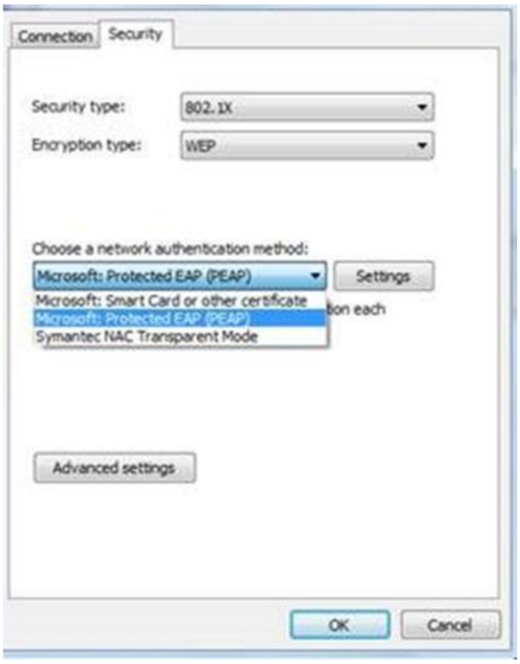
If you are not using GPO, you can manually configure the authentication on a wireless client running Windows 7, using the following steps:

1. From the Network and Sharing Center, click the Manage wireless networks task. In the Manage Wireless Networks window, double-click your wireless network name.

2. Click the Security tab. In Security type, select 802.1x, WPA-Enterprise, or WPA2-Enterprise. In Choose a network authentication method, from the drop down and then click Settings.

3. If using EAP-TLS or PEAP-TLS under the Smart Card or other Certificate Properties dialog box, select Use a certificate on this computer to use a registry-based user certificate or Use my smart card for a smart card-based user certificate.

If you want to validate the computer certificate of the NPS server, select Validate server certificate (recommended and enabled by default). If you want to specify the names of the NPS servers that must perform the TLS authentication, select Connect to these servers and type the names.



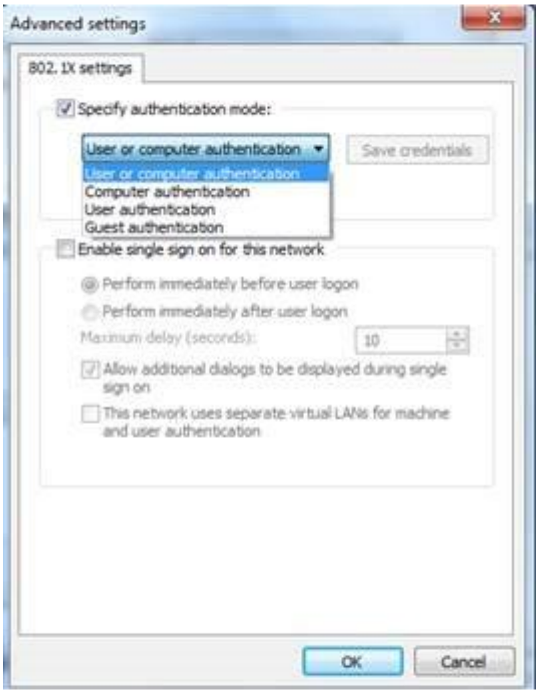
Security type: 802.1X

Encryption type: WEP

Choose a network authentication method: Microsoft: Protected EAP (PEAP)

Connection
Security
Microsoft: Smart Card or other certificate
Microsoft: Protected EAP (PEAP)
Symantec NAC Transparent Mode
Settings
tion each
Advanced settings
OK
Cancel

Figure 60. Security and Authentication tab



Advanced settings

802.1X settings

☑ Specify authentication mode:

User or computer authentication

□ Enable single sign on for this network

● Perform immediately before user logon

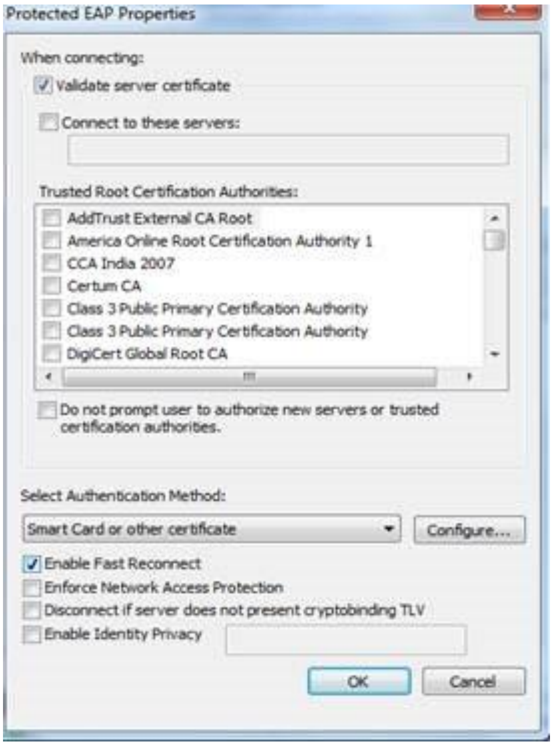
○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

Figure 61. Advanced 802.1X settings



Protected EAP Properties

When connecting:

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ AddTrust External CA Root

□ America Online Root Certification Authority 1

□ CCA India 2007

□ Certum CA

□ Class 3 Public Primary Certification Authority

□ Class 3 Public Primary Certification Authority

□ DigiCert Global Root CA

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Smart Card or other certificate

☑ Enable Fast Reconnect

□ Enforce Network Access Protection

□ Disconnect if server does not present cryptobinding TLV

□ Enable Identity Privacy

Figure 62. EAP Properties

4. Click OK twice.

To summarize, for EAP-TLS or PEAP-TLS, you need to have a certificate infrastructure to issue computer certificates to your NPS servers and both computer and user certificates to your wireless client computers. For PEAP-MS-CHAP v2, you only need to install computer certificates on the NPS servers, provided that the appropriate root CA certificates are already installed on the wireless clients. You will need to manage Active Directory users and groups for wireless access, configure NPS servers as RADIUS servers to the wireless APs, and configure the wireless APs as RADIUS clients to the IAS servers.

References

Afra, D. A. (2013). *Firewalls and Gateway*.

Dan Holme, N. R. (2008). Configuring Windows Server 2008 Active Directory. *Trainning Kit*, pp. 0-1037.

Ellingwood, J. (2014, May 2). *How the Iptables Firewall Works*. Retrieved from Digital Ocean: https://www.digitalocean.com/community/tutorials/how-the-iptables-firewall-works

Fra, M. (2012, 11 11). *Helping to Prevent Technological Defenestration*. Retrieved from Falcon IT Services: http://www.falconitservices.com/support/KB/Lists/Posts/Post.aspx?ID=77

Load Balencer Inc. (2013, April 5). Load Balancing Microsoft Remote Desktop Services Deployment Guide. *Installing Load Balancer*, p. 46.

Microsoft. (2016). *Windows Defender*. Retrieved from Microsoft: https://www.microsoft.com/en-lb/

Microsoft Developer Network. (2016). *Microsoft SQL Server*. Retrieved from MSDN: https://msdn.microsoft.com/en-us/library/mt590198(v=sql.1).aspx

Network Microsoft Developer. (2016, 03 28). *Install the Exchange 2016 Mailbox role using the Setup wizard*. Retrieved from TechNet: https://technet.microsoft.com/en-us/library/bb124778(v=exchg.160).aspx

pfSense. (2016). *Choose your hardware*. Retrieved from http://www.pfsense.org/hardware

Ramez Elmasri, S. B. (2004). *Fundamentals of Database Systems* (Vol. III). New York.

Server world. (2012, april 4). *Join in Windows Active Directory*. Retrieved from Server-world: http://www.server-world.info/en/note?os=Fedora_21&p=realmd

Stanek, W. R. (2008). Windows Server 2008 Inside Out. *Windows Server 2008 Overview and Planning*, pp. 0-1516.

techtarget. (n.d.). *SearchVMware*. Retrieved from http://searcgvmware.techtraget.com/definition/VMware-Server