Installing and configuring
Microsoft Lync Server 2013

Peter Dorner
Advisory Architect
IBM

January 26, 2014

Version History

Blockpoint/Version	Date	Contributor	Revision Activity Description
1.0/v.00	01/26/2014	Peter Dorner	Initial Version – AD preparation, SQL mirror configuration

Contents

Introduction

The following document is a build out for a hypothetical company called PS-United. The company based in Miami, FL with one single Active Directory Forest along with one subnet and a recently built Exchange 2013. The build out is providing simple HA but no site resiliency. The company recently purchased a PBX which has to be integrated to the new Lync environment in order to use the Lync client for making phone calls.

Lync components

1. Lync Front End Server Pool

One Lync server pool with 2 Front End server will be configured to provide basic failover. The pool will provide the following functionality to the clients:

- User authentication
- Address book service
- Instant Messaging and presence information
- Audio and video conferencing
- Mediation server to provide connection to the existing PBX phone system

2. High Availability

High Availability (HA) is provided within the pool with multiple FE server. In case of a server failure due to the DNS setup and the resilience within the pool users will be connected to the other available server.

3. Lync File Share Server

The Lync File Share is used to generate and publish the Lync address book and store IM attachments. In this case no HA nor disaster recovery will be implemented, however if needed deploying a DFS infrastructure can provide both feature using DFS replication between the member servers.

4. Backend Database Servers

Lync has a requirement for a SQL server to store different databases associated with different Lync services. Lync2013 supports database mirroring for HA. Two servers with the Lync database mirror and a third SQL Witness server is used to provide the same data for both databases. In the event of a database server failure Lync will access to another server.

5. Load Balancing

Load balancing can be provided in two ways. DNS and hardware load balancing. This document does not cover hardware load balancer setup.

6. The following roles will not be used

Lync Edge Server - The purpose of edge server pool is to provide the communication mechanism for instant messaging based communication to public IM providers.

Director - The Director role is required for enhanced security; it provides a role to validate authentication requests within the DMZ for external users. In the event of a denial of service attack, the attack would end at the director role.

Persistent Chat – Persistent chat server enables users to join multiparty, topic based conversations. A separate Persistent chat Front End server runs the service and a Persistent Chat Back End server stores the chat history and chat informations.

DNS Name Resolution

Microsoft Lync has specific DNS requirements, in addition to the standard host A record requirements for individual servers and clusters, additional CNAME and SRV records are required for load balancing and the advertisement of Lync services to the end clients. The DNS configuration is listed later in this document.

Autodiscover

Clients use Autodiscover to find the Lync pool. No SRV record is used for Autodiscover. A DNS A record pointing to the Lync pool will be used.

Initial network configuration:

Server name	Role	IP	Windows Version
	Miami		
LyncDC-MIA-01	DC, GC, DNS, Operations Master	192.168.2.11/24	Windows Server 2008 R2 Enterprise with SP1
LyncDC-MIA-01	DC, GC, DNS	192.168.2.12/24	Windows Server 2008 R2 Enterprise with SP1
LyncCAS-MIA-01	Exchange 2013 CAS	192.168.2.21/24	Windows Server 2008 R2 Enterprise with SP1
LyncMBX-MIA-01	Exchange 2013 Mailbox	192.168.2.31/24	Windows Server 2008 R2 Enterprise with SP1
LyncFE-MIA-01	Lync 2013 Enterprise FE server	192.168.2.41/24	Windows Server 2008 R2 Enterprise with SP1
LyncFE-MIA-02	Lync 2013 Enterprise FE server	192.168.2.42/24	Windows Server 2008 R2 Enterprise with SP1
LyncBE-MIA-01	Lync 2013 BE server – SQL 2012 Enterprise	192.168.2.51/24	Windows Server 2008 R2 Enterprise with SP1
LyncBE-MIA-02	Lync 2013 BE server – SQL 2012 Enterprise	192.168.2.52/24	Windows Server 2008 R2 Enterprise with SP1
LyncWN-MIA-01	Witness server for SQL and FileShare server for Lync – SQL 2012 Express	192.168.2.71/24	Windows Server 2008 R2 Enterprise with SP1
LyncCa-MIA-01	CA server	192.168.2.61/24	Windows Server 2008 R2 Enterprise with SP1

Windows Server 2008 forest and domain functional level
Internal domain name: ps-united.com
External domain name: ps-united.com
Single Tier PKI Infrastructure

External and Internal Exchange FQDNs:
OWA for Miami   Miami.ps-united.com
Autodiscover for Exchange   autodiscover.ps-united.com
Autodiscover for Lync   lyncinternaldiscover.ps-united.com

Prerequsites

For Hyper-V based virtual machines

On the Domain Controllers (DNS servers) for proper DNS resolution you need to run the following commands otherwise the replication will failing between the sites using Hyper-V virtual switches

dnscmd /Config /EnableEDnsProbes 0

On all servers change the Network Card settings under Computer Management and disable the following:

IPv4 Large Send Offload
Checksum Offload

Lync Server Prerequisites

- .NET 3.5 Framework
- .NET 4.5 Framework
- Microsoft Silverlight
-
- Windows Management Framework 3.0
- Windows Identity Foundation 3.0
  - Front End
    - KB2646886 – install after all IIS 7.5 components are installed
  - Persistent chat
    - Microsoft Message Queuing

The following IIS modules are required for the FE and Director servers

- Static content
- Default document
- HTTP errors
- ASP.NET
- .NET extensibility
- Internet Server API (ISAPI) extensions
- ISAPI filters
- HTTP logging
- Logging tools
- Tracing

- Windows authentication
- Request filtering
- Static content compression
- Dynamic content compression
- IIS management console
- IIS management scripts and tools
- Anonymous authentication
- Client certificate mapping authentication

Use the following PowerShell command to install the required IIS modules:

```
Import-Module ServerManager
Add-WindowsFeature Web-Static-Content, Web-Default-Doc, Web-
Http-Errors, Web-Asp-Net, Web-Net-Ext, Web-ISAPI-Ext, Web-ISAPI-
Filter, Web-Http-Logging, Web-Log-Libraries, Web-Http-Tracing,
Web-Windows-Auth, Web-Filtering, Web-Stat-Compression, Web-Dyn-
Compression, Web-Mgmt-Console, Web-Scripting-Tools, Web-Basic-
Auth, Web-Client-Auth -Restart
```

Add the Remote System Administration Tools and the Desktop Experience Windows feature by running the following cmdlets:

```
Import-Module ServerManager
Add-WindowsFeature RSAT-ADDS, Desktop-Experience
```

Install the Windows Media Format Runtime

```
%systemroot%\system32\dism.exe /online /add-package
/packagepath:%windir%\servicing\Packages\Microsoft-Windows-
Media-Format-Package~31bf3856ad364e35~amd64~~6.1.7601.17514.mum
/ignorecheck
```

Preparing the schema, forest and the domain.

Before you can begin install Lync Server Management Shell by running the Setup.exe from the Lync DVD.
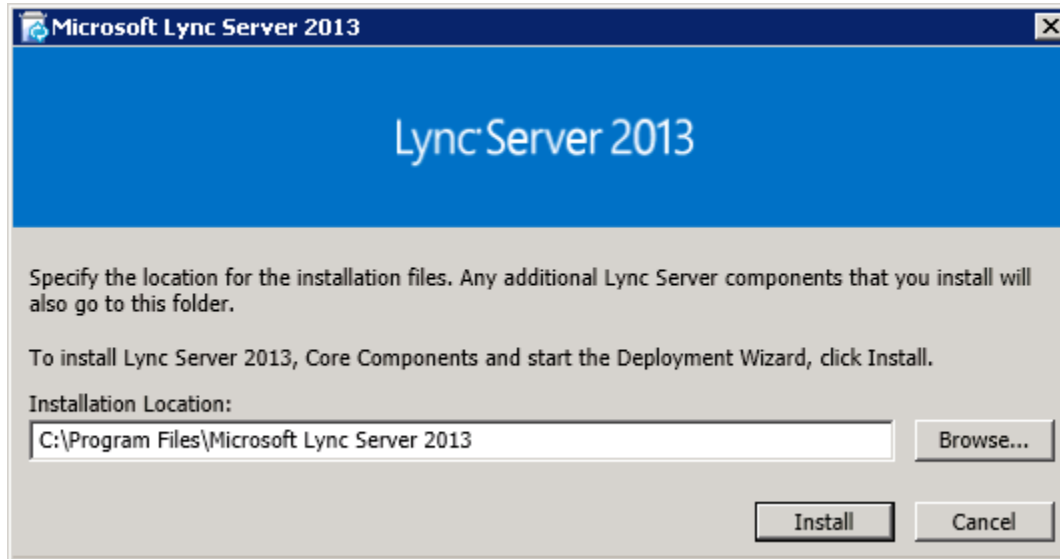
When it finished close the Lync Server Deployment Wizard and open **Lync Server Management Shell** from the Start Menu
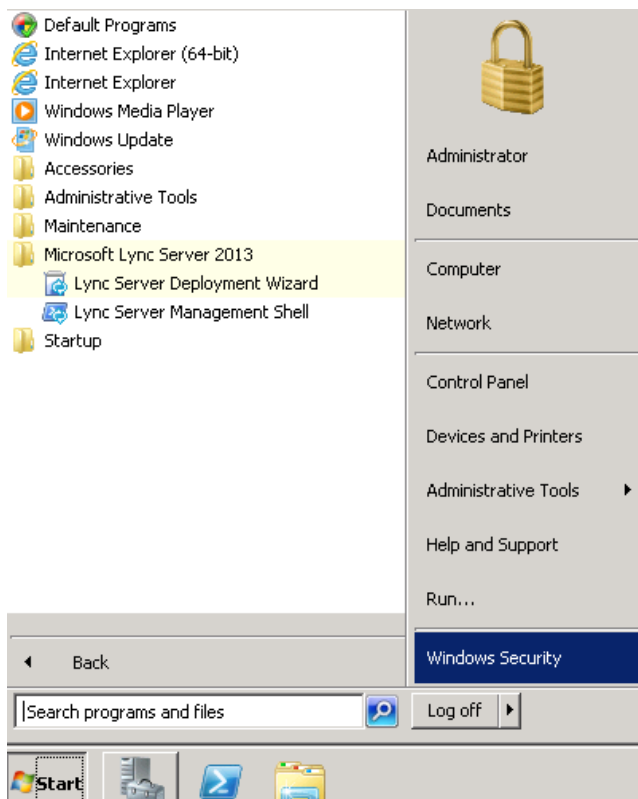
Schema update will running against the holder of the schema master FSMO, the account you use need to be member of the Schema Admin group. You need the Active Directory Domain Service Tools are installed before you begin.
Run the following cmdlet from the Lync Shell

Schema upgrade - `Install-CsAdServerSchema`
Forest prep - `Enable-CsAdForest`
Domain prep - `Enable-CsAdDomain`

You can prepare your domain using the GUI. To do this start the **Lync Server Deployment Wizard** from Start Menu and select the **Prepare Active Directory** option. The preparation steps are straight forward using the wizard.

Add the Lync server administrators to the CSAdministrator and RTCUniversalServerAdmins group
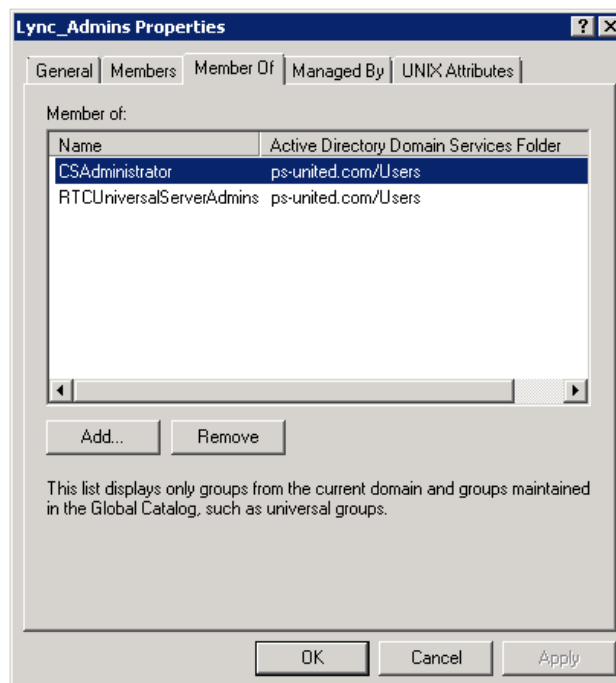
Verifying the new forest, schema and domain version

To verify the schema update check the **CN=ms-RTC-SIP-SchemaVersion** where the **rangeUpper** value should be 1150 and the **rangeLower** 3 or run the `Get-CsAdServerSchema` cmdlet
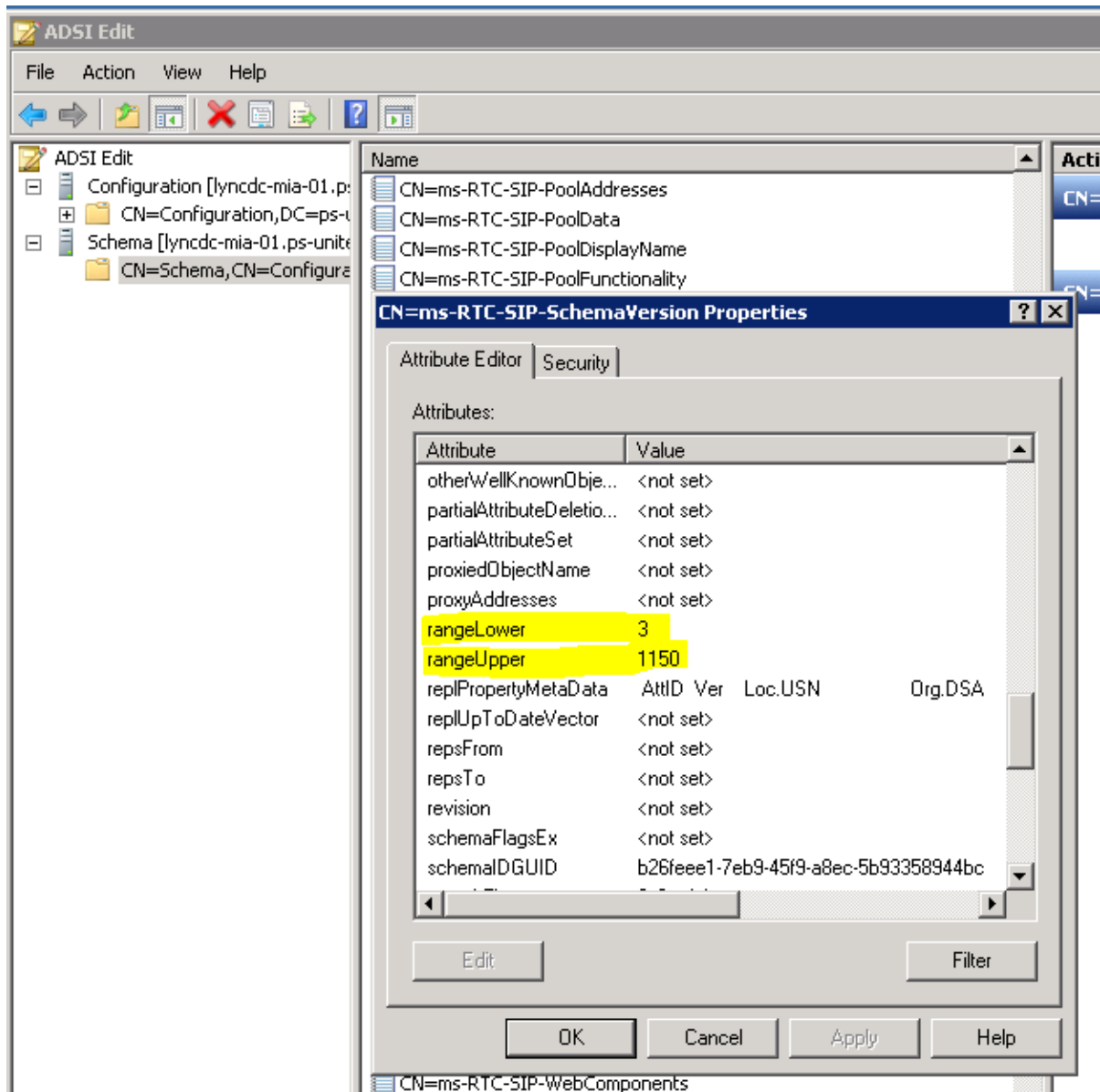
For forest preparation verification open Active Directory Users and Computers under the Users OU you should security groups starting with CS and RTC. The complete list of the new groups shown the following table

RTC Groups	CS Groups
RTCComponentUniversalServices	CSAdministrator
RTCHSUniversalServices	CSArchivingAdministrator
RTCProxyUniversalServices	CSHelpDesk
RTCSBAUniversalServices	CSLocationAdministrator
RTCUniversalConfigReplicato	CsPersistentChatAdministrator
RTCUniversalGlobalReadOnlyGroup	CSResponseGroupAdministrator
RTCUniversalGlobalWriteGroup	CSResponseGroupManager
RTCUniversalReadOnlyAdmins	CSServerAdministrator
RTCUniversalSBATechnicians	CSUserAdministrator
RTCUniversalServerAdmins	CSViewOnlyAdministrator
RTCUniversalServerReadOnlyGroup	CSVoiceAdministrator
RTCUniversalUserAdmins	
RTCUniversalReadOnlyGroup	

Command-line verification run the `Get-CsAdServerSchema` cmdlet
For more details of the forest preparation run the following

```
Get-CsAdForest -Report C:\ForestPrep.html
```


Domain verification
```
Get-CsAdDomain
Get-CsAdDomain -Report "C:\DomainPrepReport.html"
```

# Configuring Back End server for High Availability

The Back End (BE) servers are database servers running Microsoft SQL and hosting the databases for archiving, monitoring and persistent chat. These databases can be collocated, however it's not recommended to share these with other non-Lync databases. The BE servers also serves a backup store for the pool's user and conference data. A single BE server is supported, however SQL  failover, HA and/or disaster recover (DR) is recommended. In this case SQL mirroring will provide both the server and database HA. The BE servers don't have any Lync software installed.

Before the installation we create a SQL server service account, this account need to be part of the local administrator group on each SQL server with a strong password which never expires.
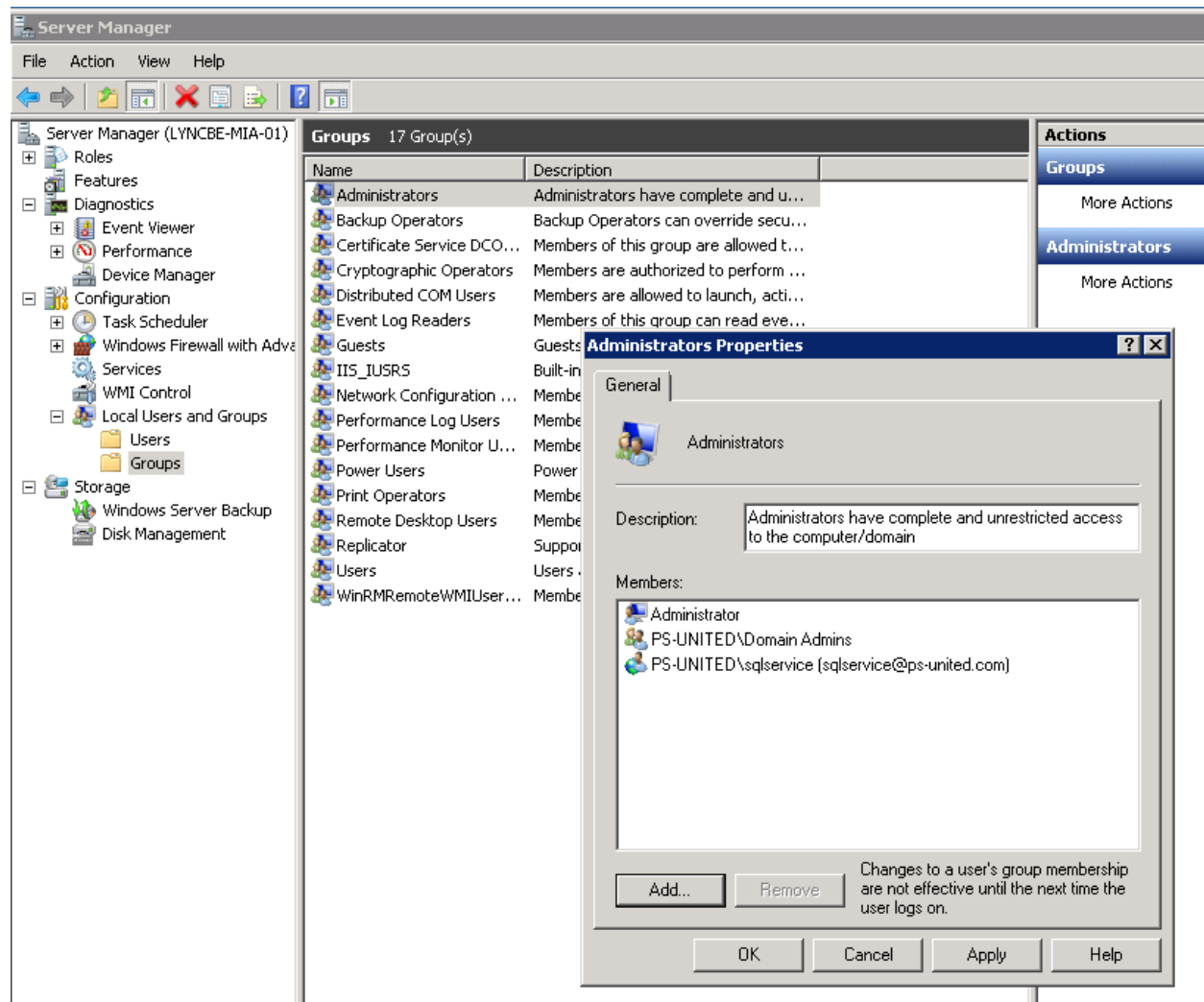


Install .NET 3.5 via the Add Features option from Server Manager.
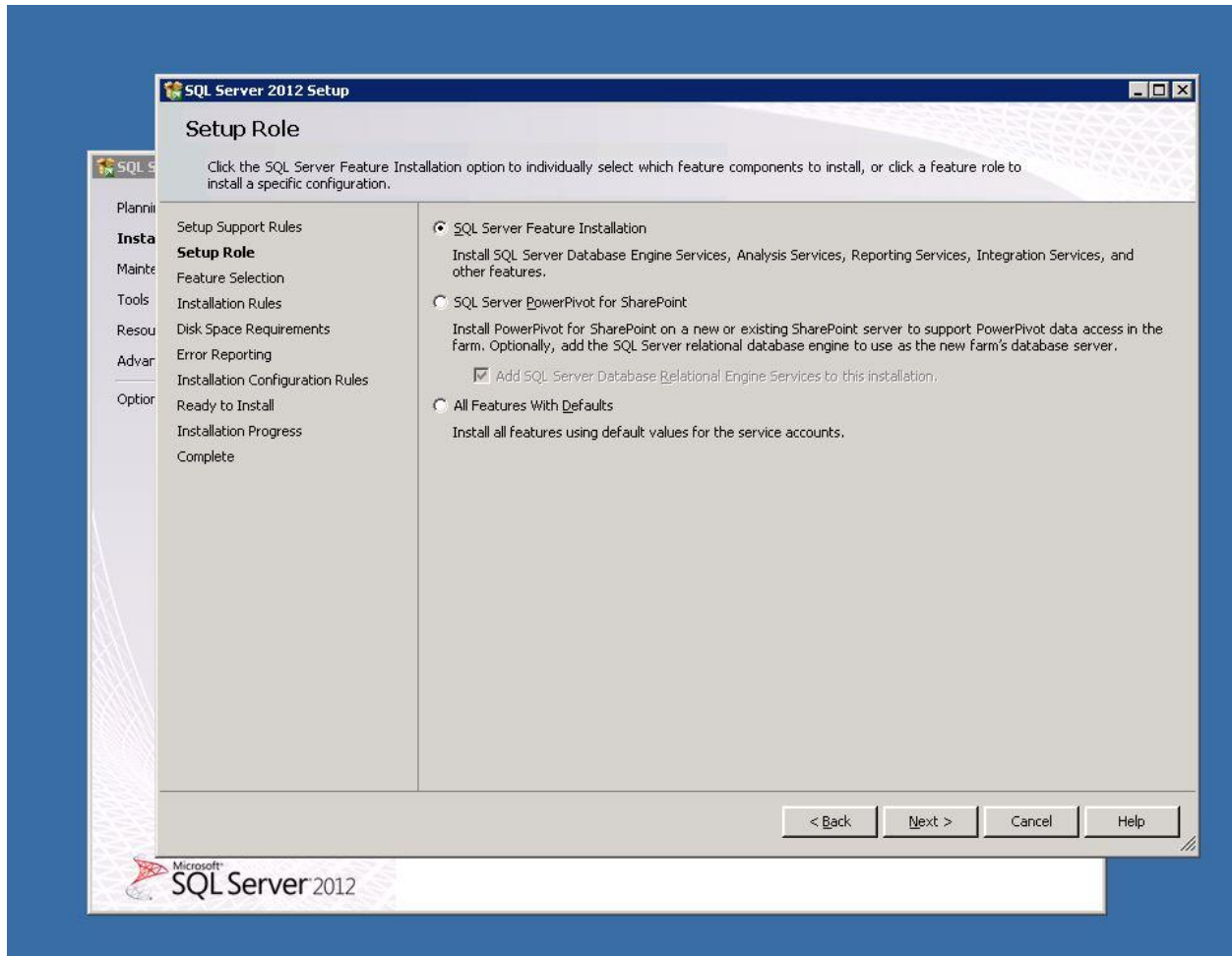
## Installing the SQL Servers

Start the installation by selecting the **New SQL Server stand-alone installation or add feature to an existing installation option**
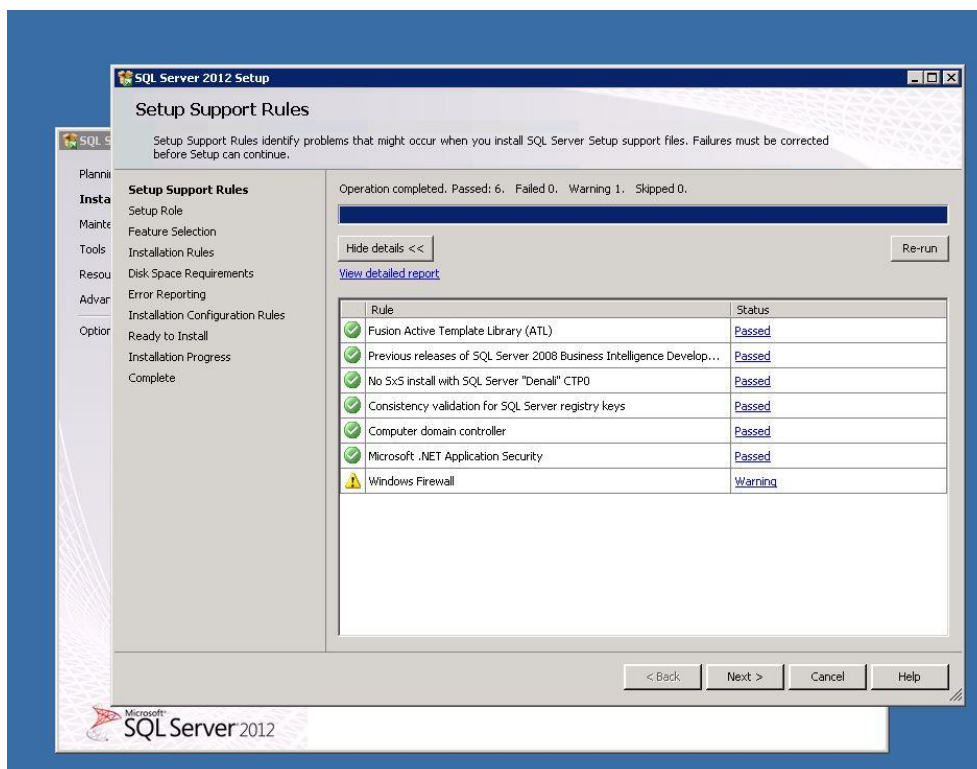
On the next page enter the product key and go **Next**

Read the License and select **Next**
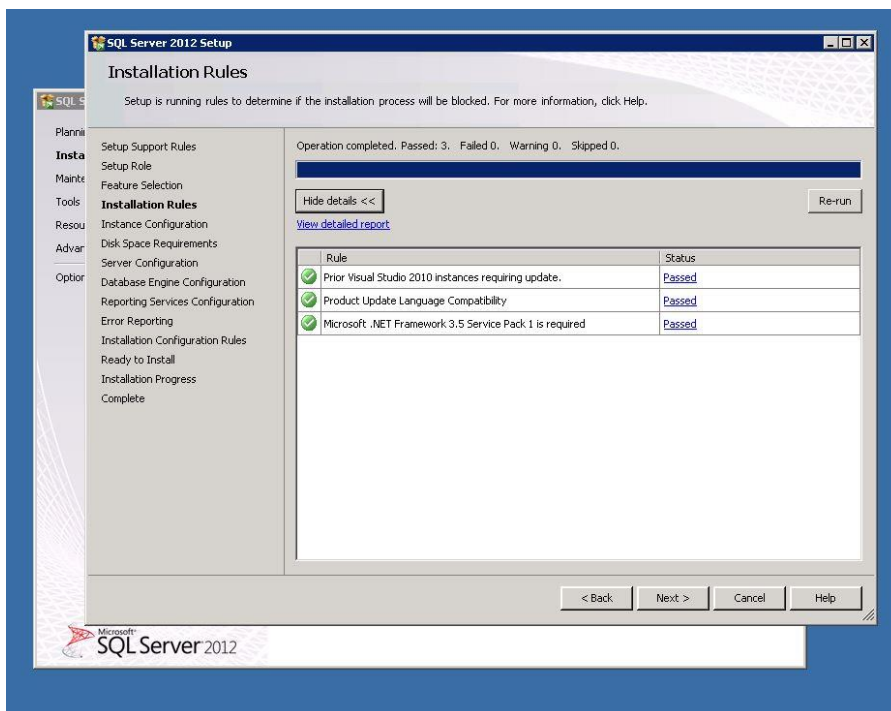
Select **SQL Feature installation**



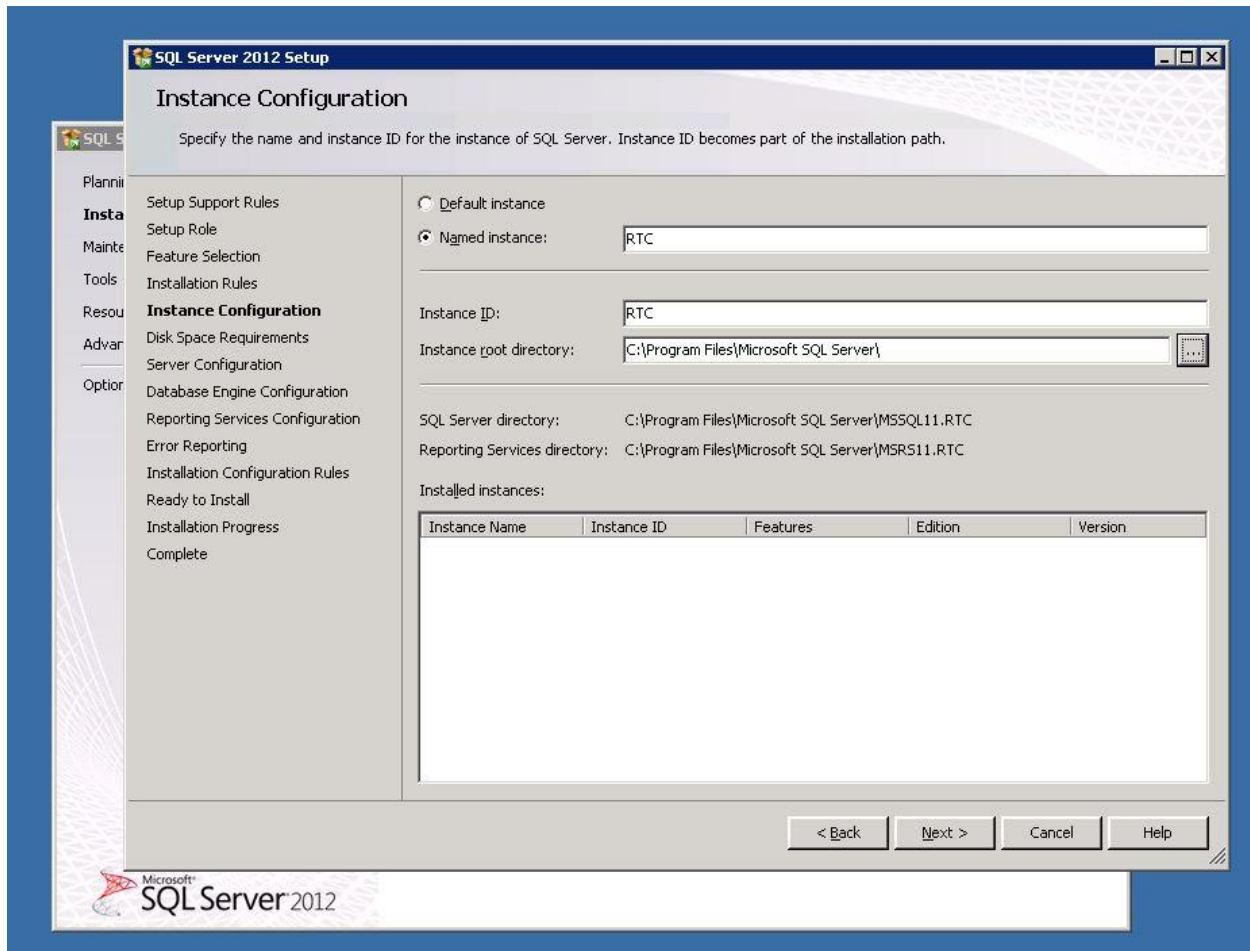Select the following features on the features selection page

- Database Engine Services
  - SQL Server Replication
- Reporting Services – Native
- Data Quality Client
- SQL Server Data Tools
- Client Tools Connectivity
- Management Tools – Basic
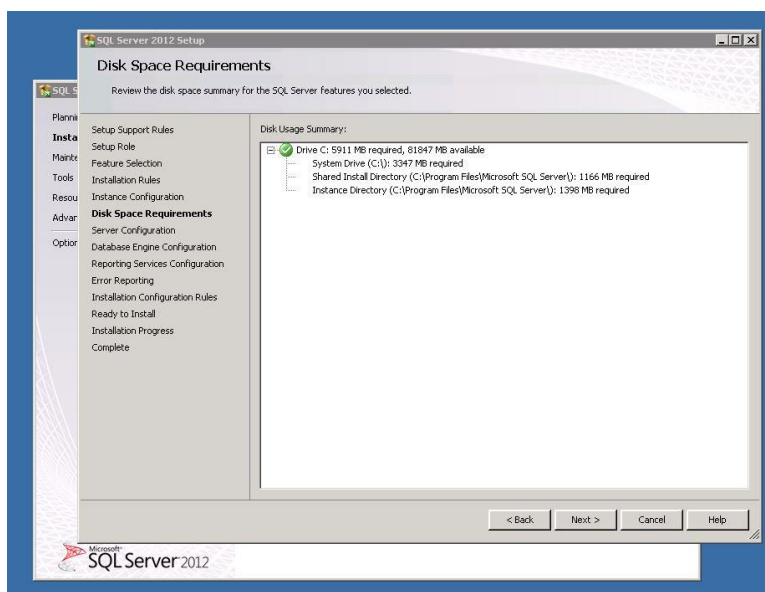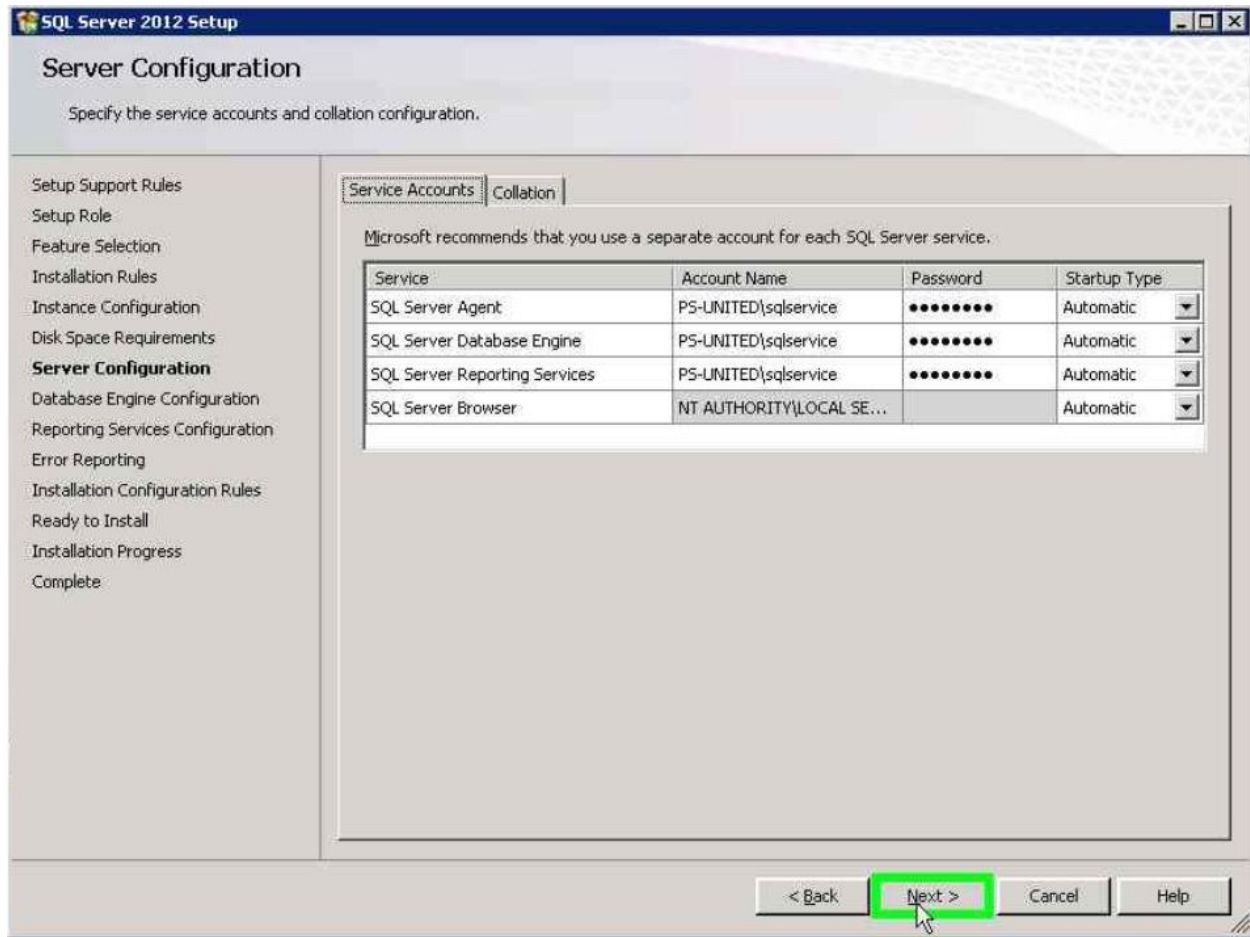  - Management Tools - Complete
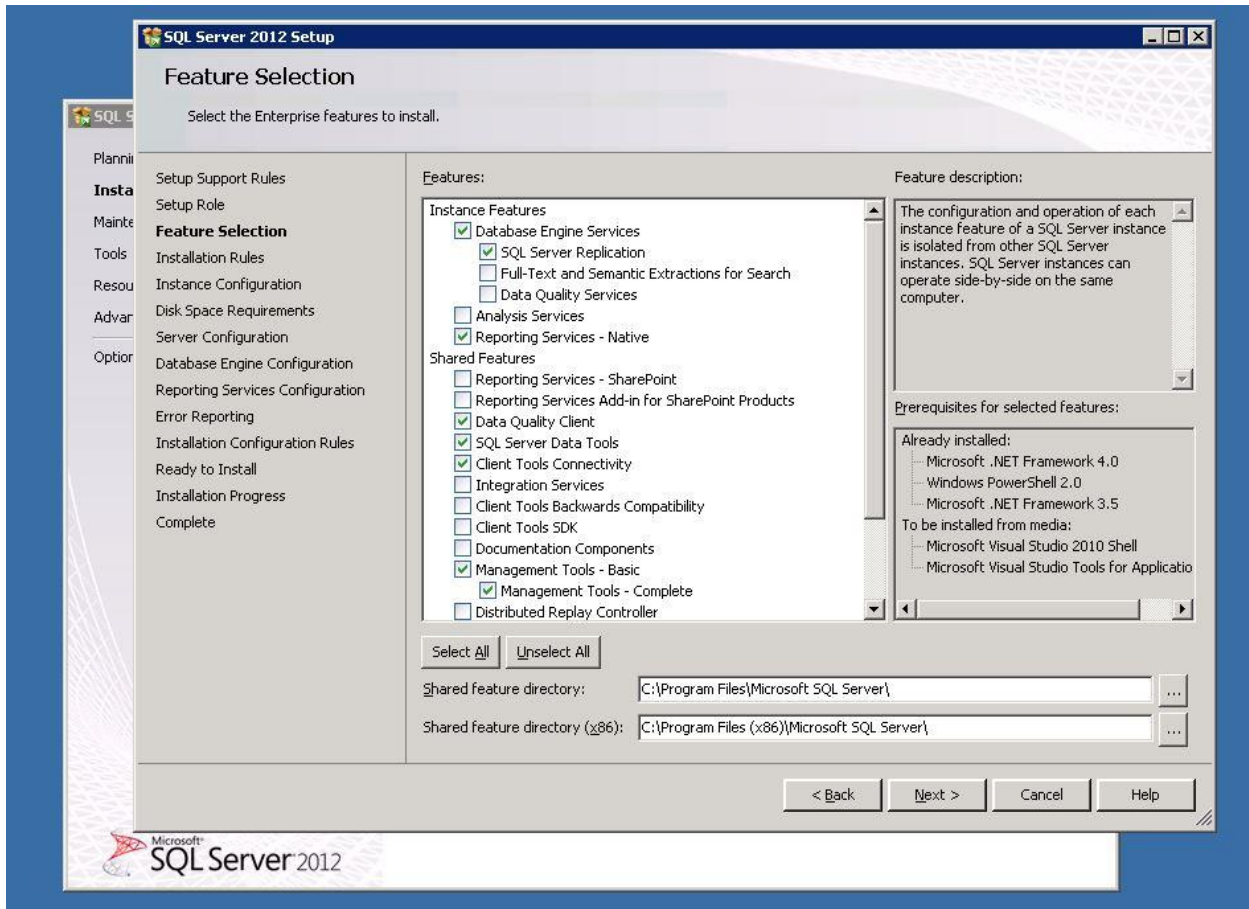
Select **Next**

Select **Named Instance** on the Instance Configuration page and call it **RTC**
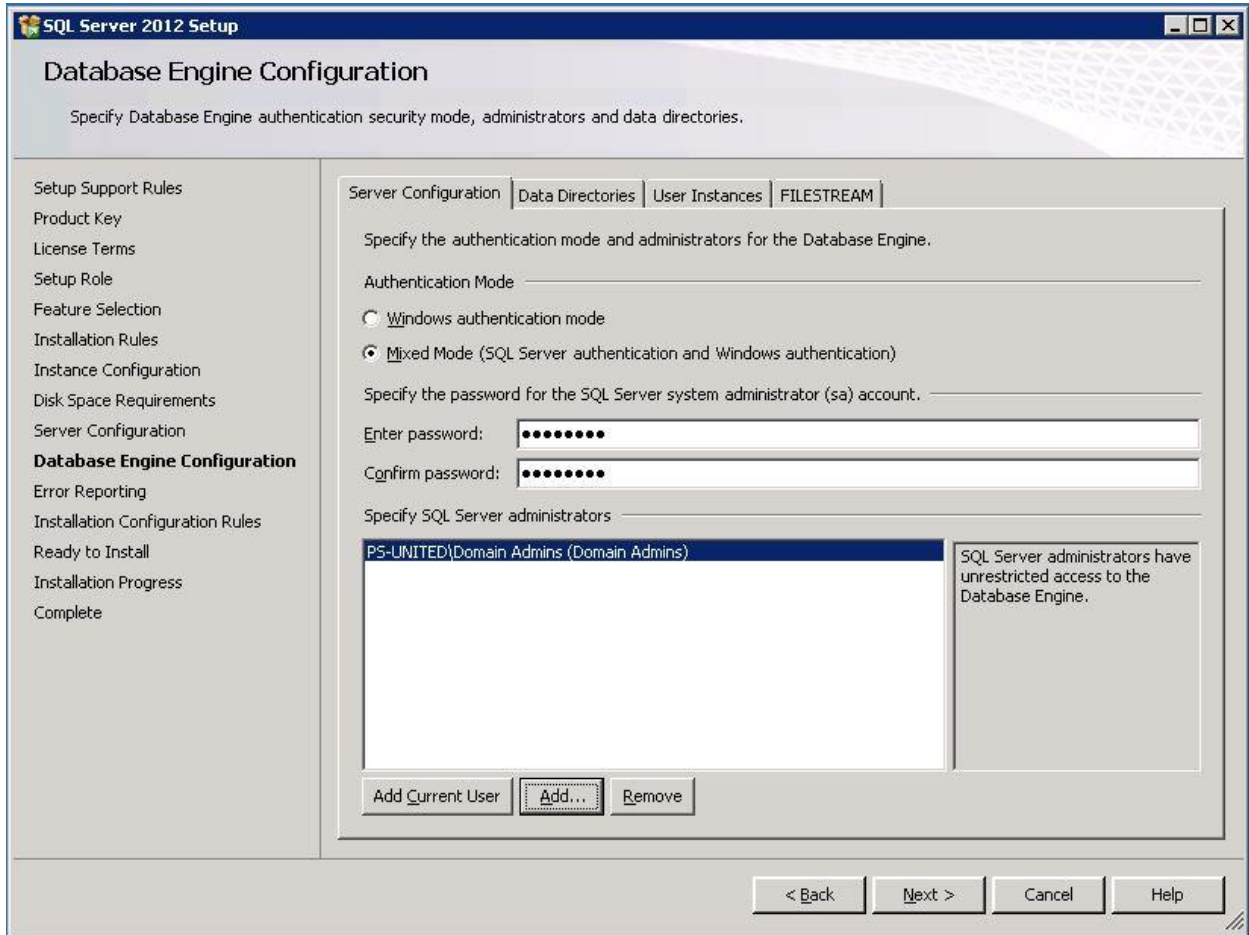


On the summary page select **Next**

Set the domain account you created for SQL Server Agent, SQL Server Database Engine and SQL Server Reporting Services.
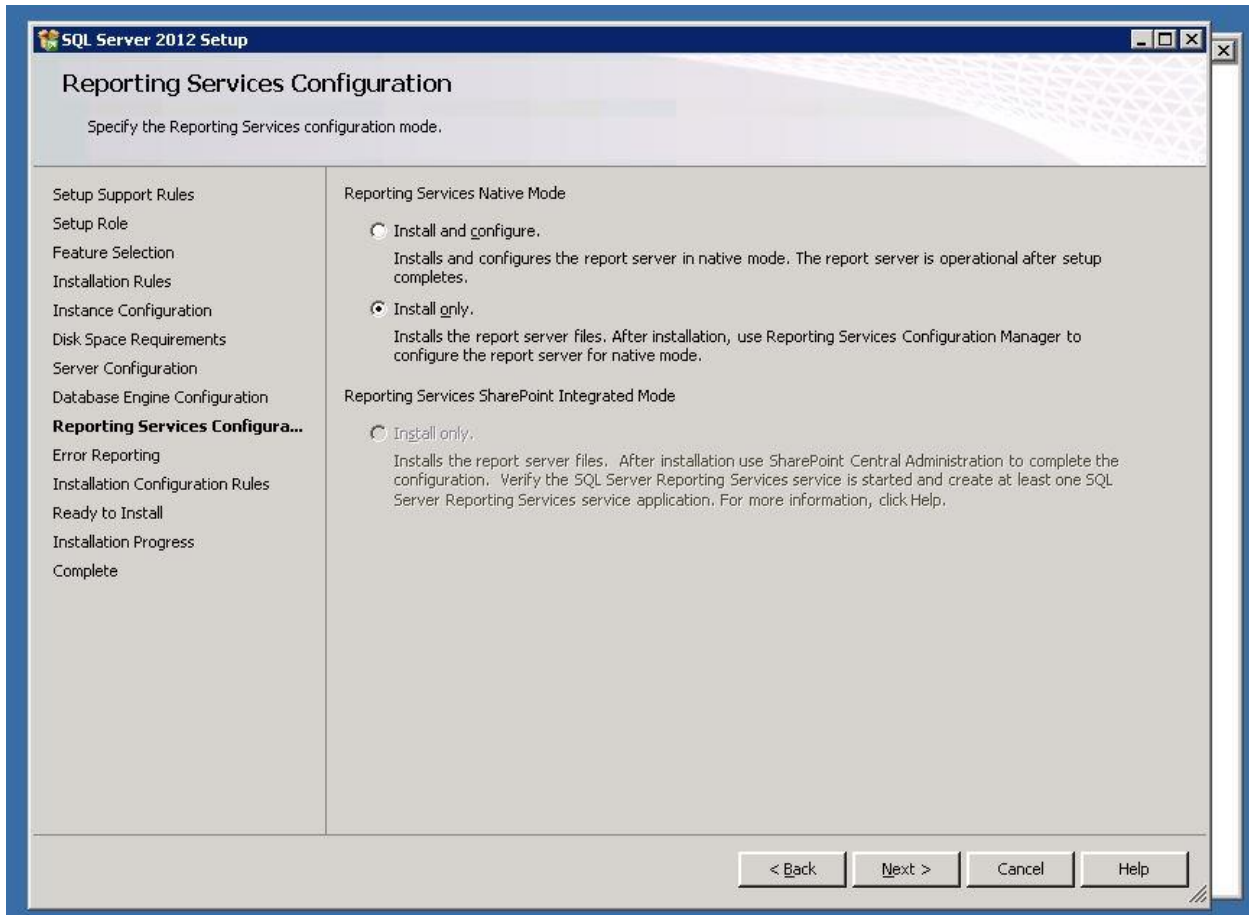
Select **Mixed Mode authentication** and set a password for the SA account. Also here you can add the administrators/administrator group who can manage the SQL Server
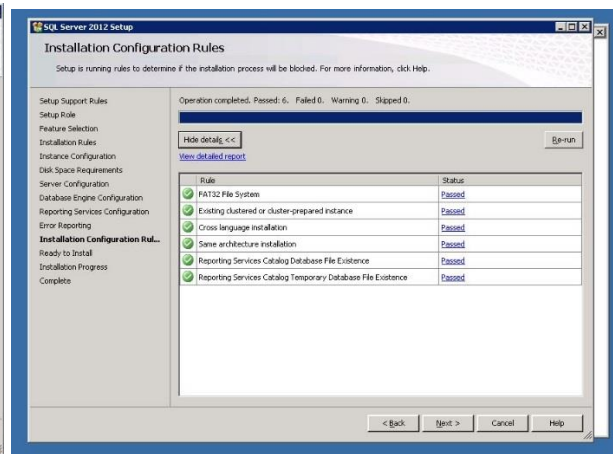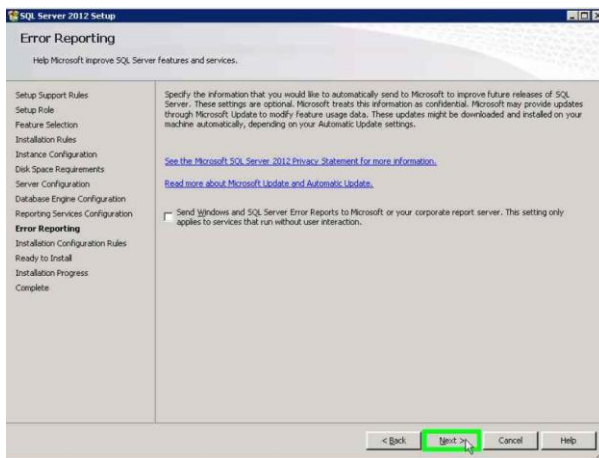


On the Data Directories tab set the Database locations, in this case lave the defaults.
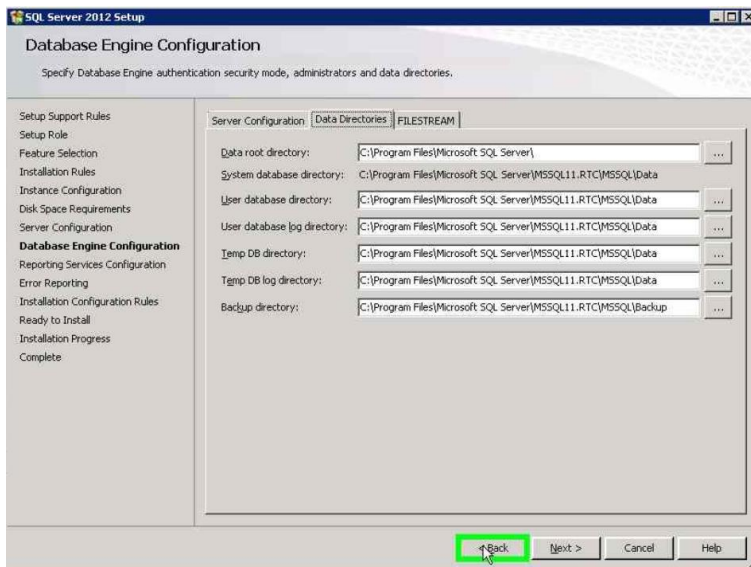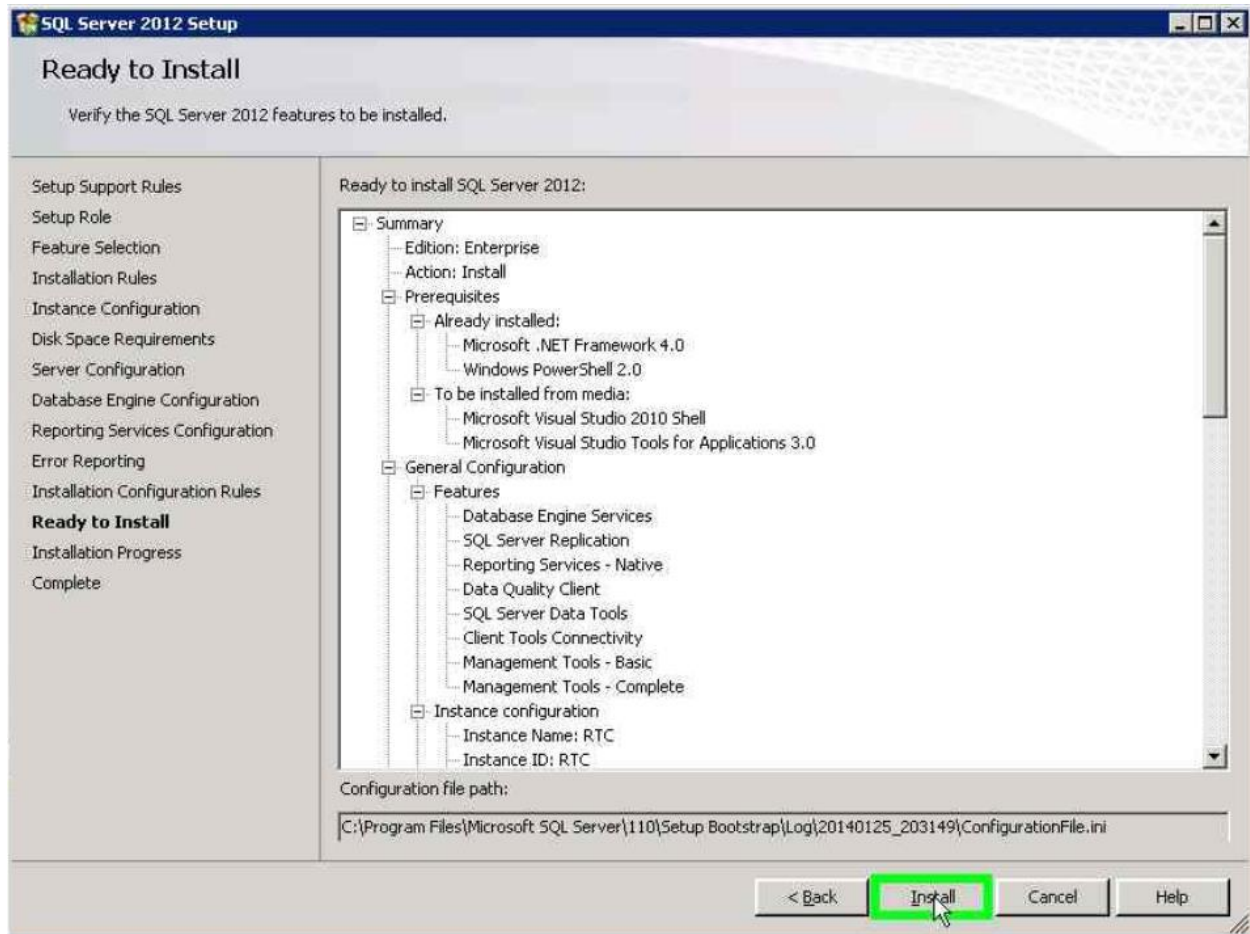
Select **Install Only** for the Reporting services we will configure it later when all SQL Servers are installed.



Select **Next** and **Next** on the following two pages

Start the **installation** of the SQL Server



Repeat steps above to install the second SQL Server
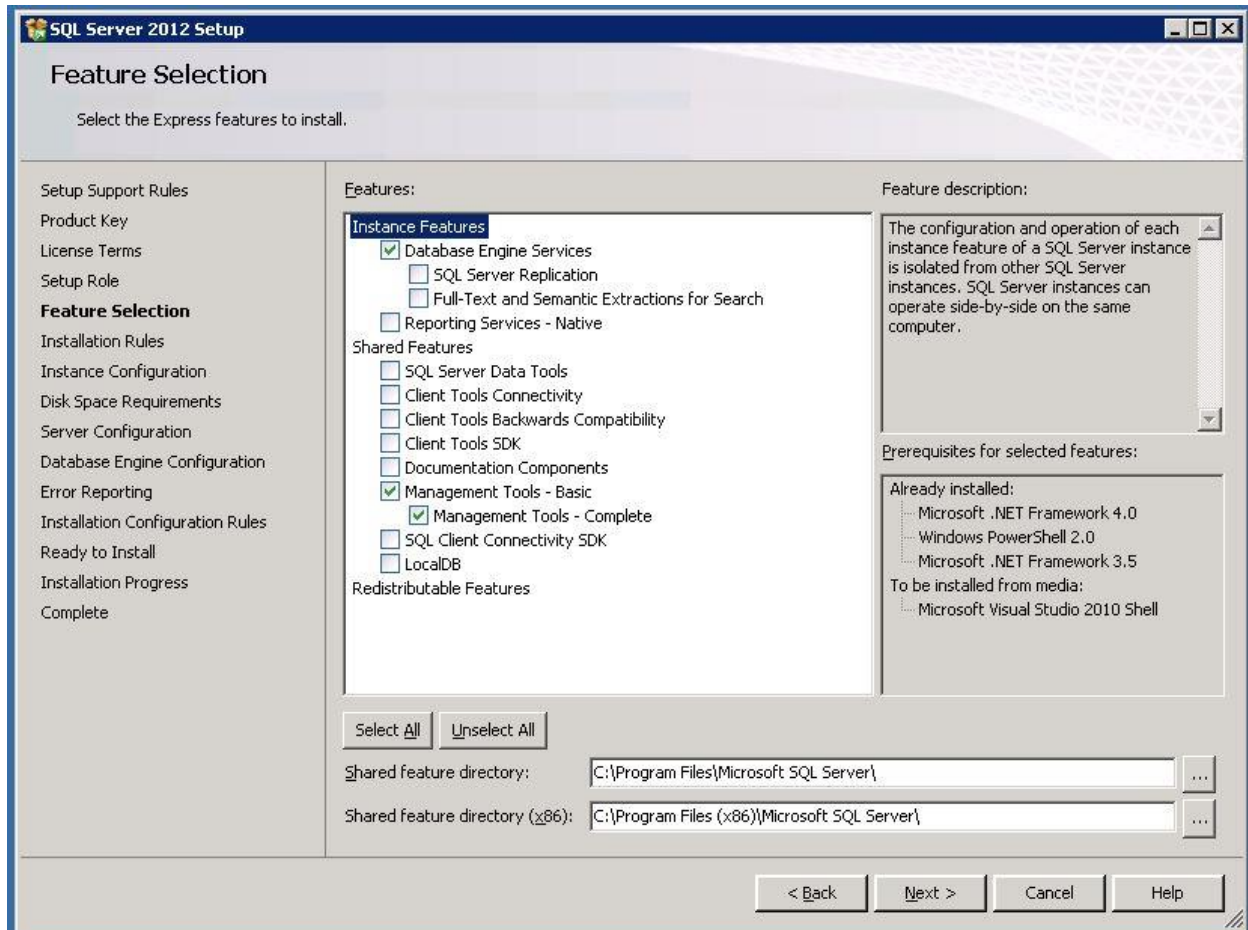
## *Installing SQL Witness server*

Install SQL Server as you did for the BE server I highlight only the differences or you can install SQL Express version as we only use this for witness and need only the database engine, the witness server will not use and of the features of a Standard/Enterprise version.

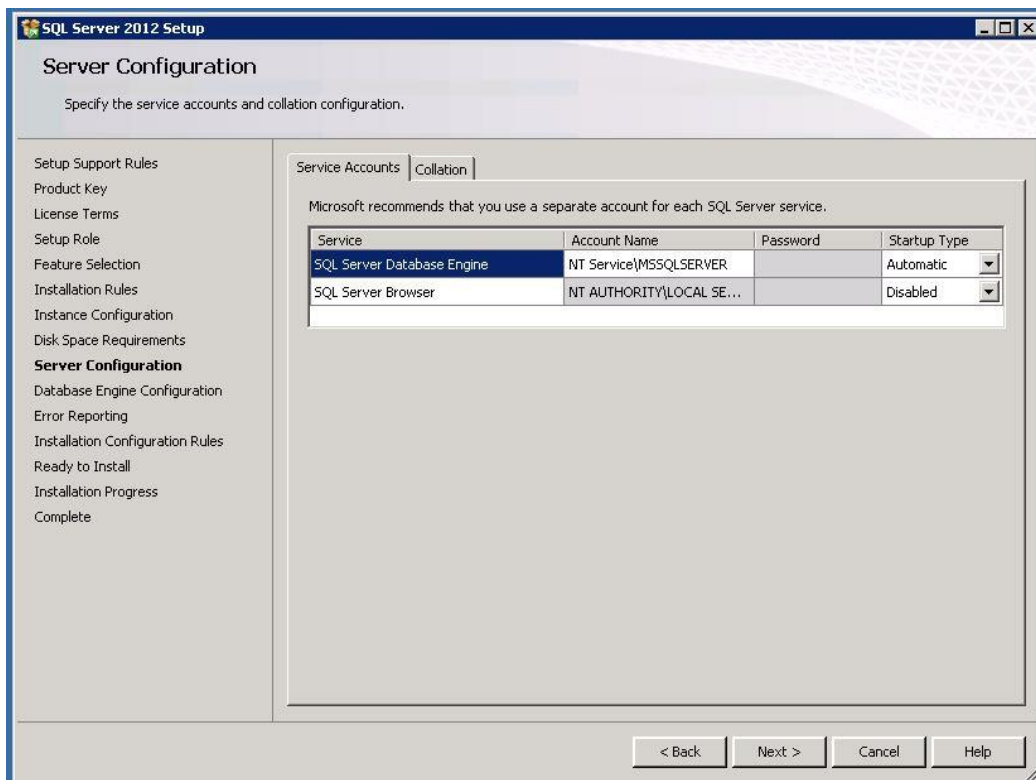Install only the **Database Engine** and the **Management Tools**
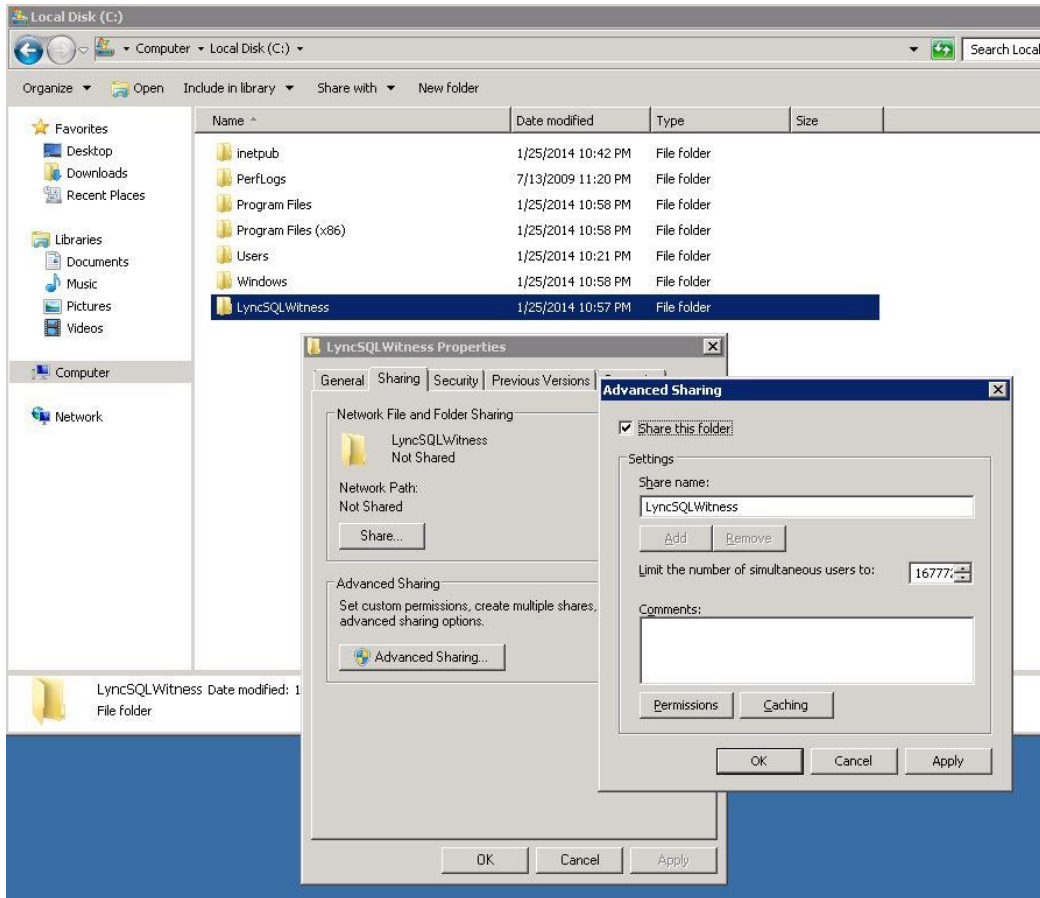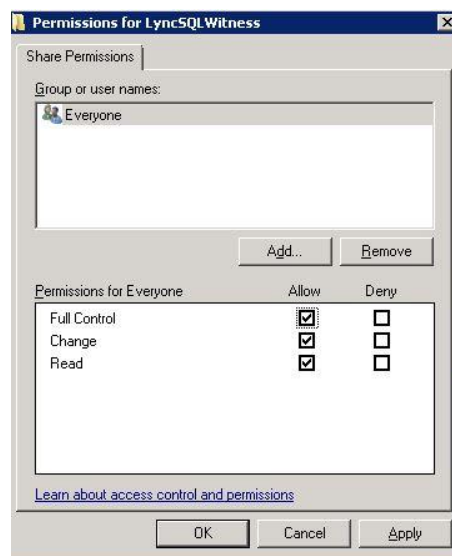
User the **Default Instance**
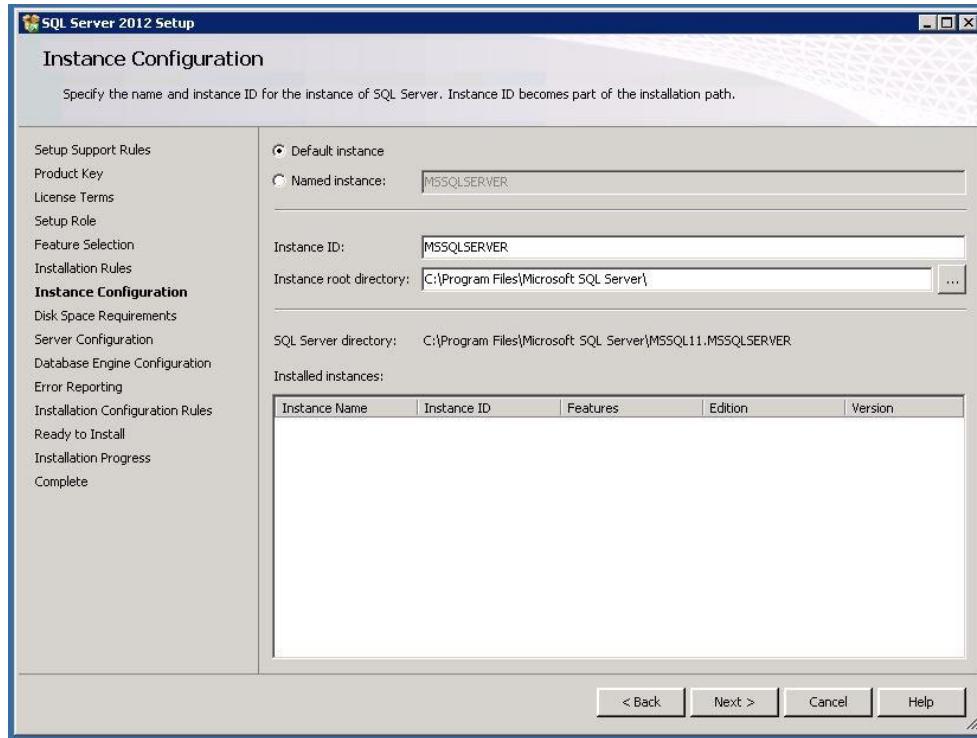


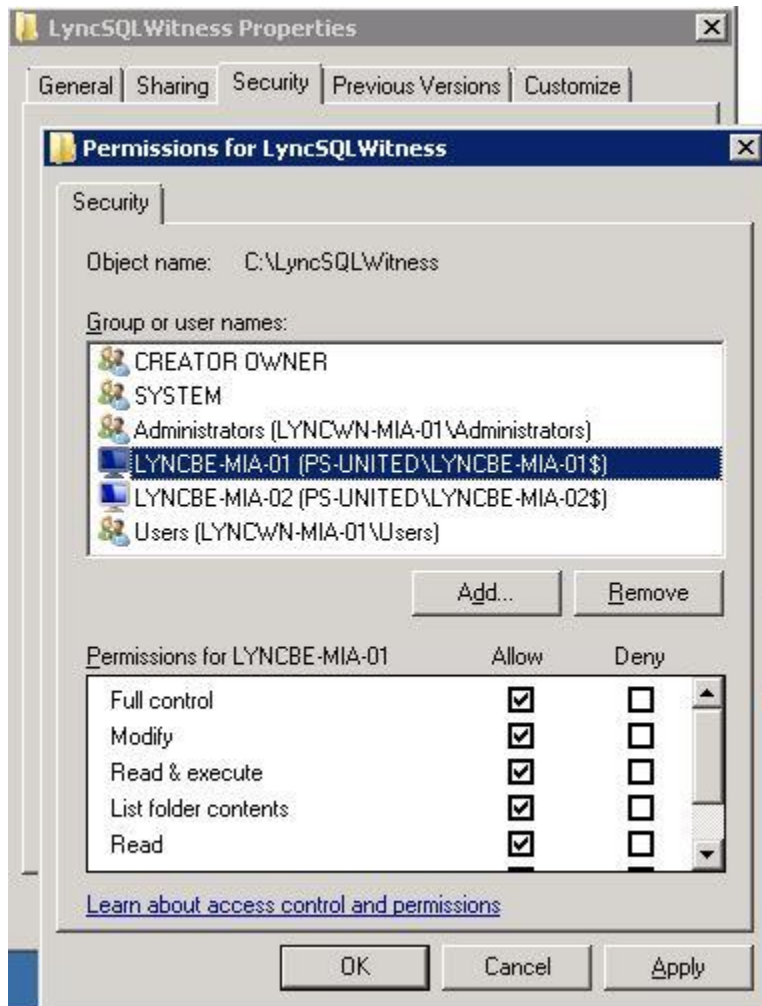Use the **default accounts** and finish the installation.

Create a share called LyncSQLWitness that SQL will use



Give Everyone full control as a share permission we will restrict access through the NTFS permissions

Add the two BE SQL Server with Full Control on the NTFS Permission (Security) tab

## *Configuring SQL for Lync 2013 deployment*

### Configuring Windows Firewall

We need to configure the built-in Windows firewall so the SQL cluster can communicate with each other and with the witness. Run the following PowerShell commands on all SQL server including the witness or use the GUI to configure the firewall.

*Server2008 R2*

```
netsh advfirewall firewall add rule name="Allow inbound SQL
Server" dir=in action=allow protocol=TCP LocalPort=1433
RemoteIP=localsubnet

netsh advfirewall firewall add rule name="Allow inbound SQL
Administrator Connection" dir=in action=allow protocol=UDP
LocalPort=1434 RemoteIP=localsubnet

netsh advfirewall firewall add rule name="Allow inbound SQL
Administrator Connection" dir=in action=allow protocol=TCP
LocalPort=1434 RemoteIP=localsubnet

netsh advfirewall firewall add rule name="Allow inbound SQL
Server Broker" dir=in action=allow protocol=TCP LocalPort=4022
RemoteIP=localsubnet

netsh advfirewall firewall add rule name="Allow inbound SQL
Server RPC" dir=in action=allow protocol=TCP LocalPort=135
RemoteIP=localsubnet

netsh advfirewall firewall add rule name="Allow inbound SQL
Server Analysis" dir=in action=allow protocol=TCP LocalPort=2383
RemoteIP=localsubnet

netsh advfirewall firewall add rule name="Allow inbound SQL
Server Browser" dir=in action=allow protocol=TCP LocalPort=2382
RemoteIP=localsubnet

netsh advfirewall firewall add rule name="Allow inbound SQL
Server Mirroring01" dir=in action=allow protocol=TCP
LocalPort=5022 RemoteIP=localsubnet

netsh advfirewall firewall add rule name="Allow inbound SQL
Server Mirroring02" dir=in action=allow protocol=TCP
LocalPort=7022 RemoteIP=localsubnet
```

```
netsh advfirewall firewall add rule name="Allow Inbound SQL
HTTP" dir=in action=allow protocol=tcp localport=80
remoteip=192.168.2.0/24

netsh advfirewall firewall add rule name="Allow Inbound SQL
HTTPS" dir=in action=allow protocol=tcp localport=443
remoteip=192.168.2.0/24

netsh advfirewall firewall add rule name="Allow Inbound SQL
Server Program" dir=in action=allow program="C:\Program
Files\Microsoft SQL Server\MSSQL11.RTC\MSSQL\Binn\sqlservr.exe"
remoteip=localsubnet
```


Enable the predefined rules listed below

- File and Printer Sharing (NB-Datagram-In)
- File and Printer Sharing (NB-Name-In)
- File and Printer Sharing (NB-Session-In)
- File and Printer Sharing (SMB-In)

- Remote Administration (NP-In)
- Remote Administration (RPC)
- Remote Administration (RPC-EPMAP)

- Windows Management Instrumentation (ASync-In)
- Windows Management Instrumentation (DCOM-In)
- Windows Management Instrumentation (WMI-In)

Windows Server 2012

```
New-NetFirewallRule -DisplayName "Allow Inbound SQL Server" –
Direction Inbound –Protocol TCP –LocalPort 1433 -RemoteAddress
LocalSubnet -Action Allow

New-NetFirewallRule -DisplayName "Allow inbound SQL
Administrator Connection" -Direction Inbound –Protocol UDP –
LocalPort 1434 -RemoteAddress LocalSubnet -Action Allow

New-NetFirewallRule -DisplayName "Allow inbound SQL
Administrator Connection" -Direction Inbound –Protocol TCP –
LocalPort 1434 -RemoteAddress LocalSubnet -Action Allow

New-NetFirewallRule -DisplayName "Allow inbound SQL Server
Broker" -Direction Inbound –Protocol TCP –LocalPort 4022 -
RemoteAddress LocalSubnet -Action Allow

New-NetFirewallRule -DisplayName "Allow inbound SQL Server RPC"
-Direction Inbound –Protocol TCP –LocalPort 135 -RemoteAddress
LocalSubnet -Action Allow

New-NetFirewallRule -DisplayName "Allow inbound SQL Server
Analysis" -Direction Inbound –Protocol TCP –LocalPort 2383 -
RemoteAddress LocalSubnet -Action Allow

New-NetFirewallRule -DisplayName "Allow inbound SQL Server
Browser" -Direction Inbound –Protocol TCP –LocalPort 2382 -
RemoteAddress LocalSubnet -Action Allow

New-NetFirewallRule -DisplayName "Allow inbound SQL Server
Mirroring01" -Direction Inbound –Protocol TCP –LocalPort 5022 -
RemoteAddress LocalSubnet -Action Allow

New-NetFirewallRule -DisplayName "Allow inbound SQL Server
Mirroring02" -Direction Inbound –Protocol TCP –LocalPort 7022 -
RemoteAddress LocalSubnet -Action Allow

New-NetFirewallRule -DisplayName "Allow Inbound SQL HTTP" –
Direction Inbound –Protocol TCP –LocalPort 80 -RemoteAddress
192.168.2.0/24 –Action Allow
```

```
New-NetFirewallRule -DisplayName "Allow Inbound SQL HTTPS" -
Direction Inbound -Protocol TCP -LocalPort 443 -RemoteAddress
192.168.2.0/24 -Action Allow

New-NetFirewallRule -DisplayName "Allow Inbound SQL Server
Program" -Direction Inbound -Program "C:\ProgramFiles\Microsoft
SQL Server\MSSQL11.RTC\MSSQL\Binn\sqlservr.exe" -RemoteAddress
LocalSubnet -Action Allow
```

Enable the following pre-defined rules

- File and Printer Sharing (NB-Datagram-In)
- File and Printer Sharing (NB-Name-In)
- File and Printer Sharing (NB-Session-In)
- File and Printer Sharing (SMB-In)
- Inbound Rule for Remote Shutdown (TCP-In)
- Inbound Rule for Remote Shutdown (RPC-EP-In)

Configuring the Reporting Services

The following steps need to be done on both BE server.

Start the Reporting Services Configuration Manager from the Start Menu and select the **Web Service URL** option to configure the web access using IP 192.168.2.51. If a certificate is installed you can select to use and encrypt the communication
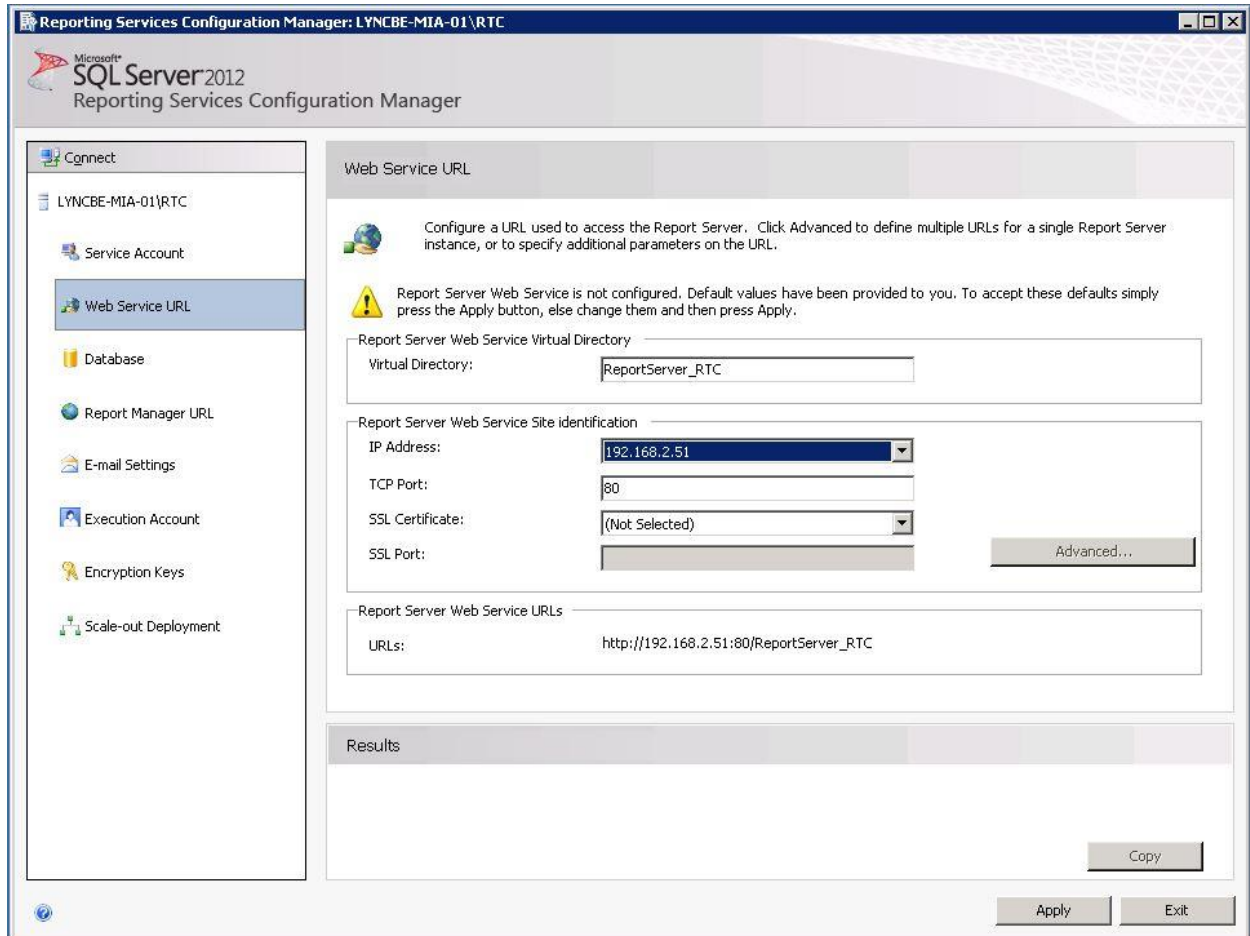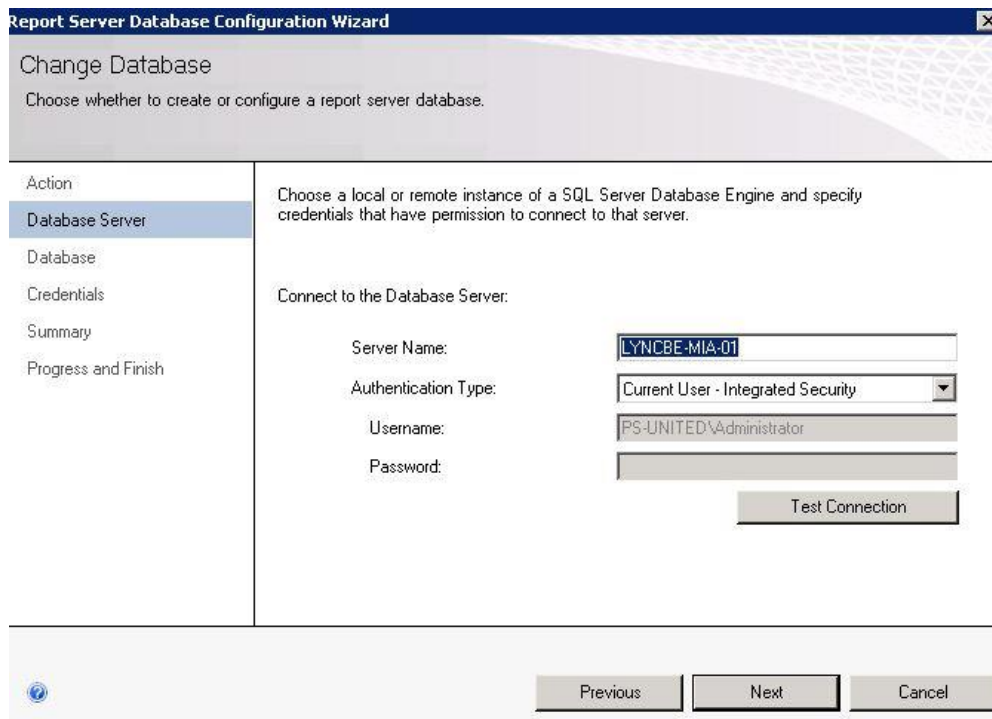
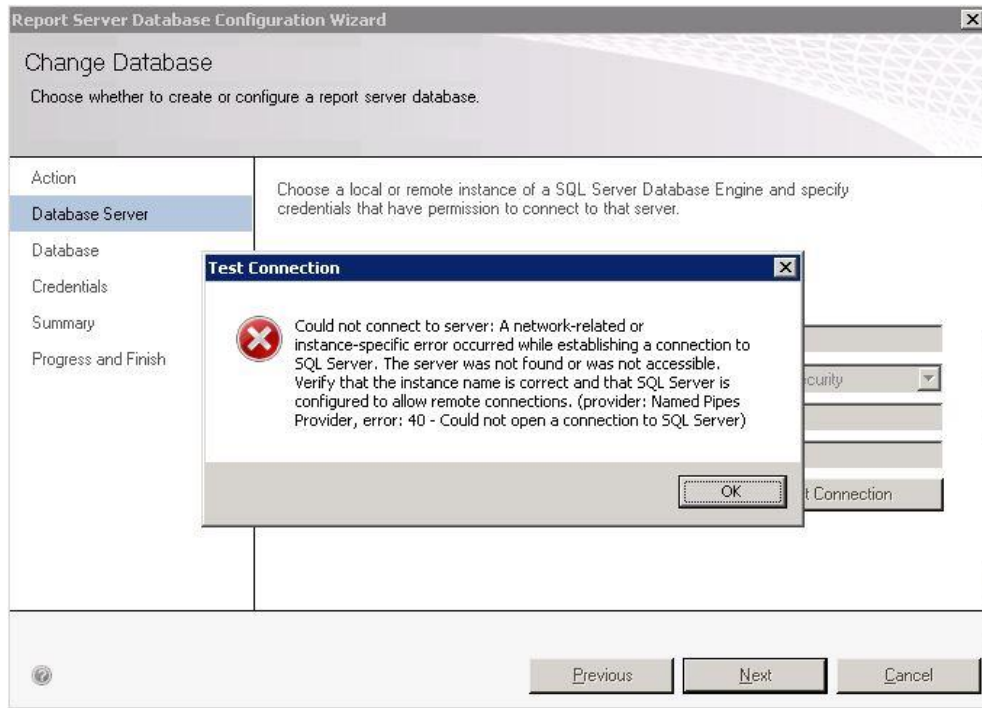Go to the database tab and select **Change Database**
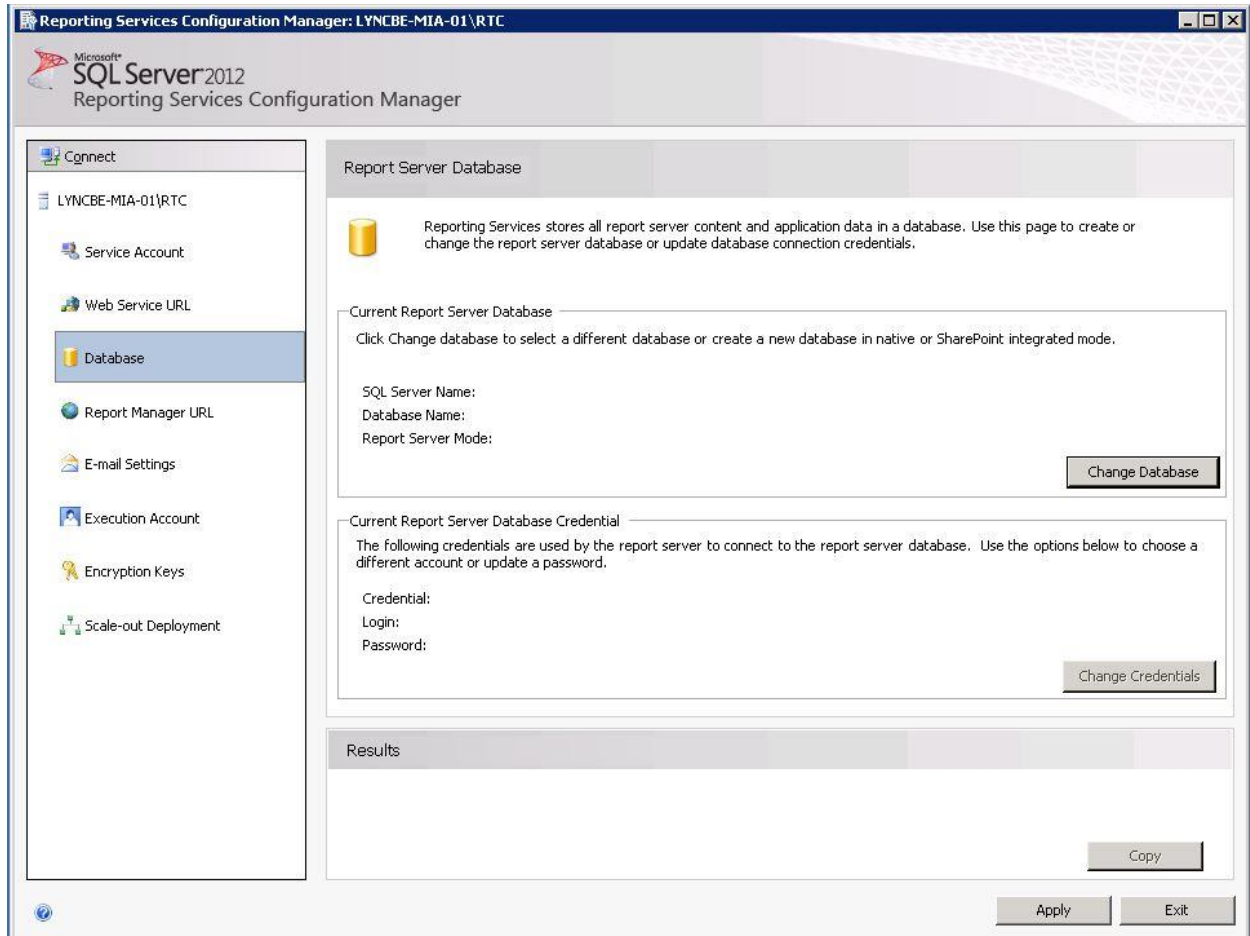
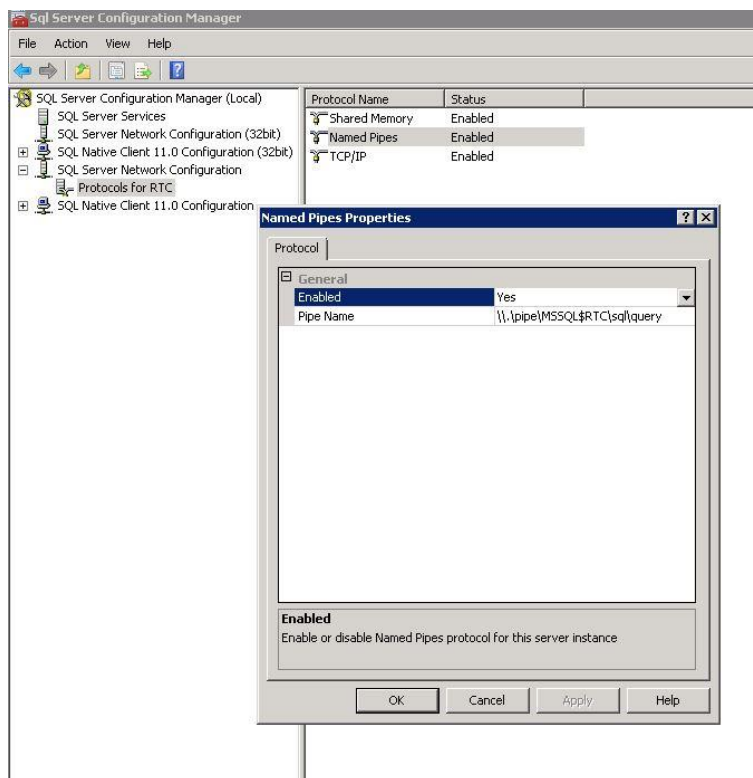Select **Create a new report server database**
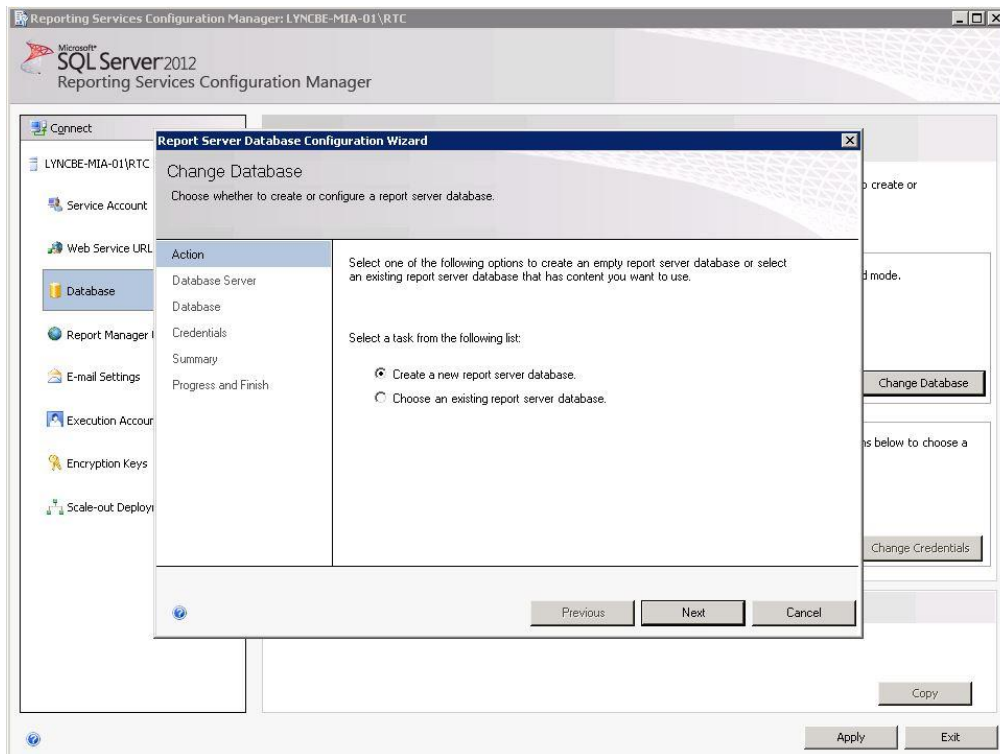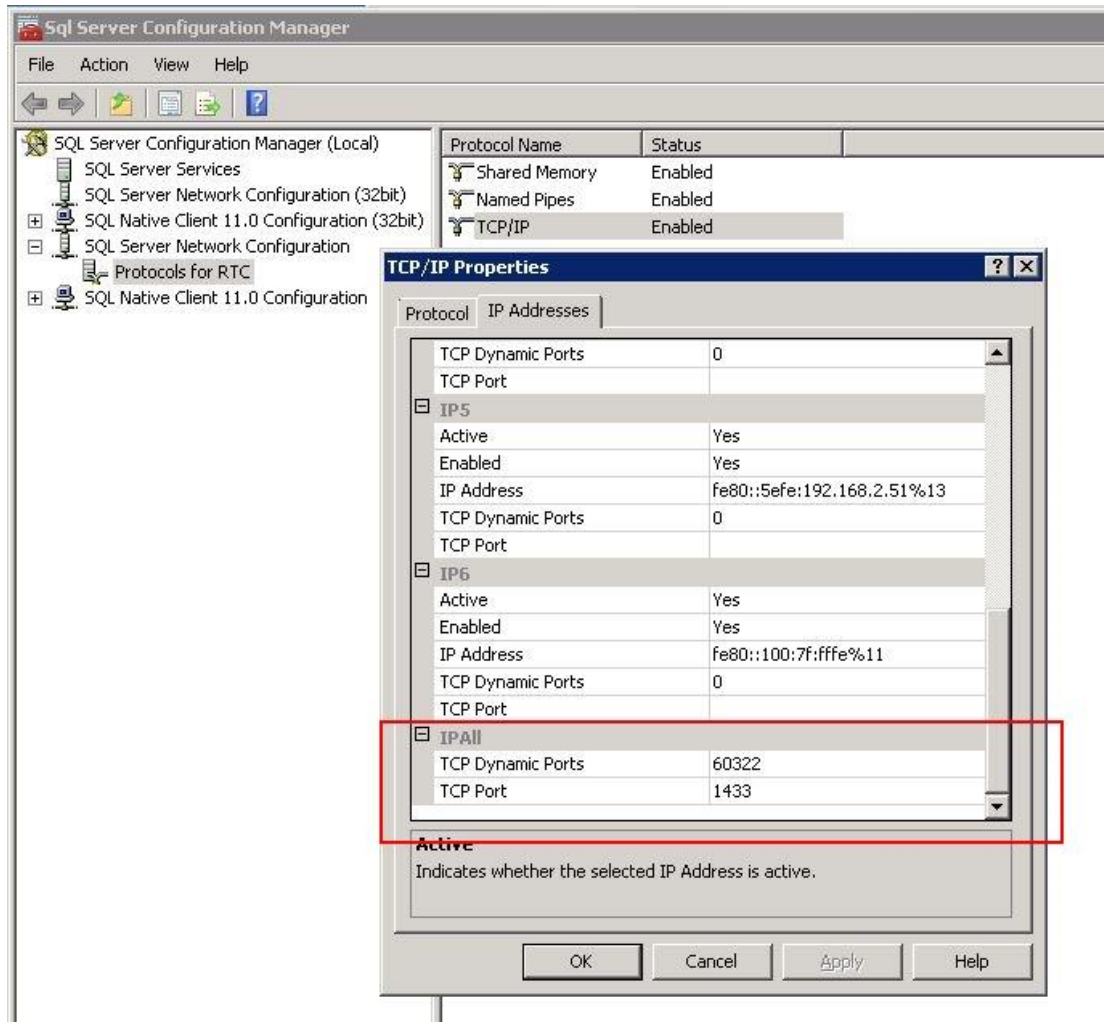

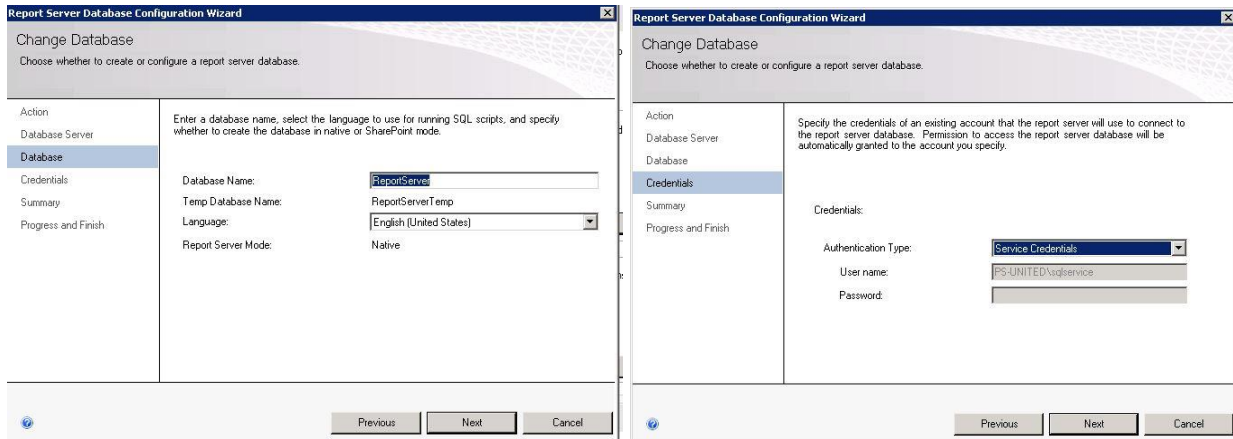Leave the default and **test connection**

If it fails

Make sure you opened the firewall and check that Named pipes are enabled under the SQL Server Configuration Manager
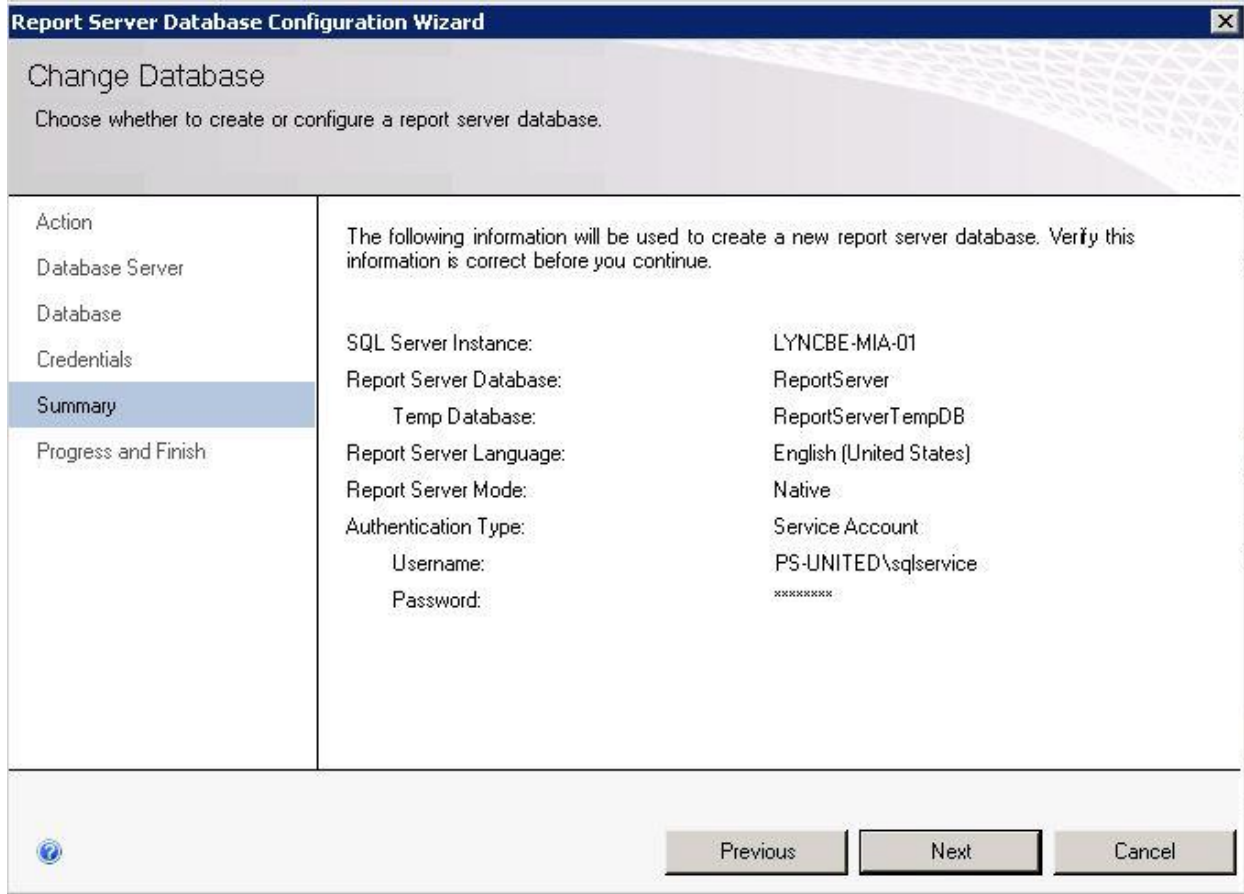
Check the TCP/IP port settings

Leave the Database name and service credentials default

Check the settings on the summary page and select **Next**

Report Server Database Configuration Wizard

Change Database

Choose whether to create or configure a report server database.

Action

Database Server

Database

Credentials

Summary

Progress and Finish

The following information will be used to create a new report server database. Verify this information is correct before you continue.

SQL Server Instance:	LYNCBE-MIA-01
Report Server Database:	ReportServer
Temp Database:	ReportServerTempDB
Report Server Language:	English (United States)
Report Server Mode:	Native
Authentication Type:	Service Account
Username:	PS-UNITED\sqlservice
Password:	xxxxxxxx

Previous   Next   Cancel

When the configuration finished go to the **Report Manager URL** and **Apply** the settings
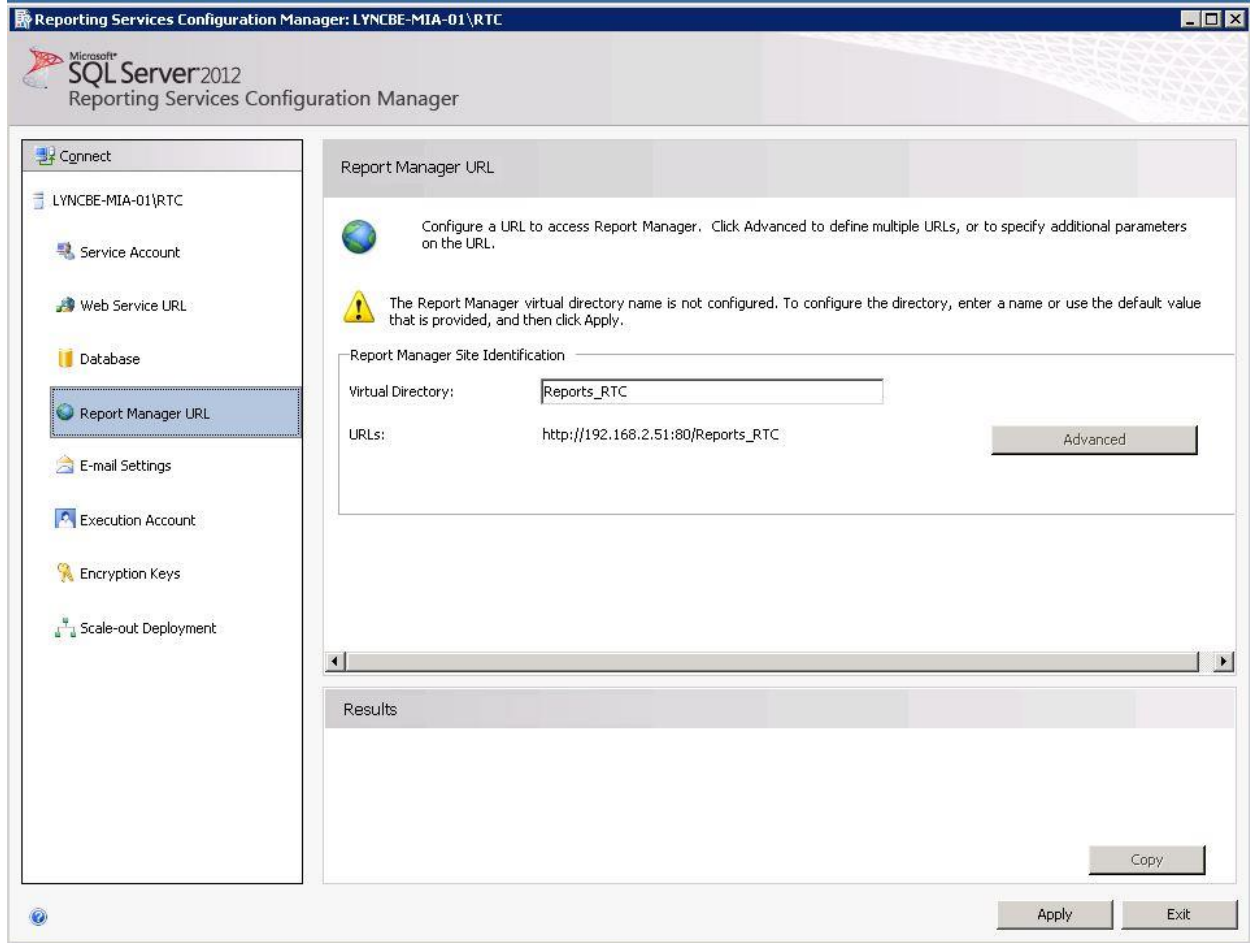
Check the web services configuration by opening the link on the Report Manager URL page. The SQL Server Reporting Home Services webpage should pop-up.
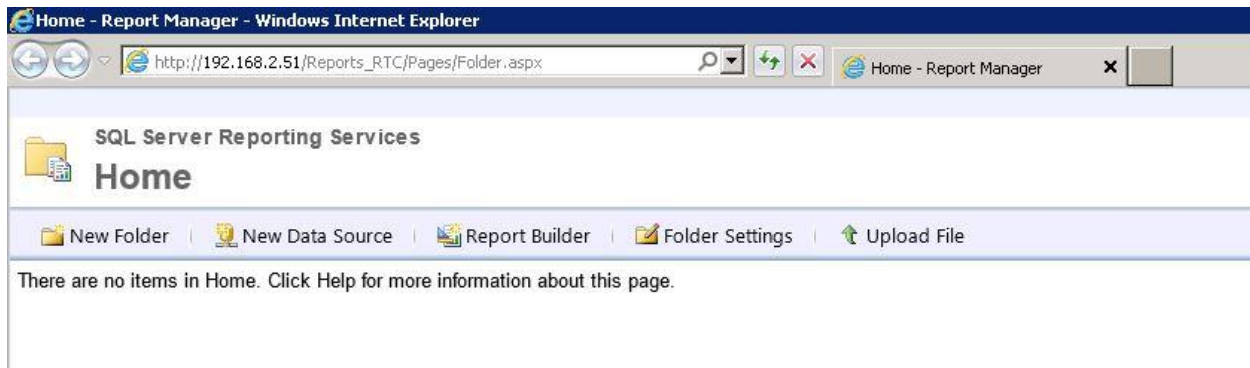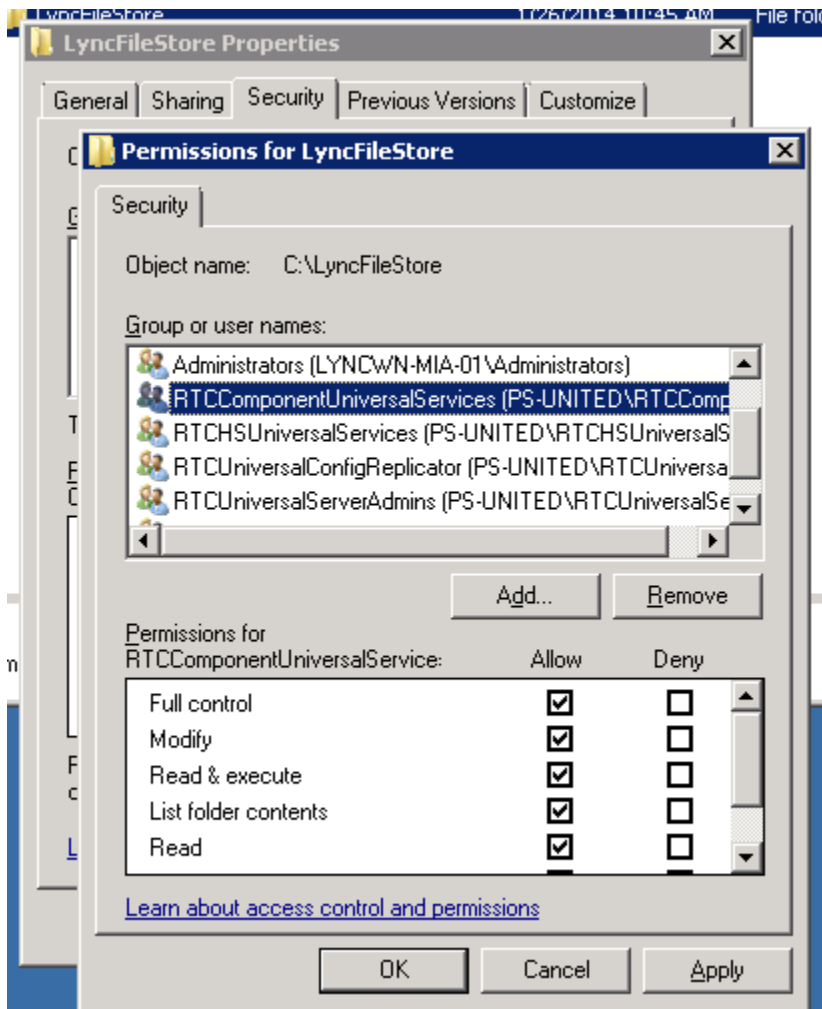
Configuring Lync File store

In this scenario we configure only a single file share, the configuration is the same on a DFS environment. The holder of this file share will be the SQL Witness server because there is no load in our test environment that would require a separate dedicated server.

Create a folder called LyncFileStore then share it. Give Full control for the following groups using the Security tab.

- RTCComponentUniversalService
- RTCHSUniversalServices
- RTCUniversalConfigReplicator
- RTCUniversalServerAdmin

Useful Links

- Lync 2013 planning tool
  http://www.microsoft.com/en-us/download/details.aspx?id=36823
- Lync 2013 Capacity Calculator
  http://www.microsoft.com/en-us/download/details.aspx?id=36828
- Lync 2013 Resource Kit
  http://www.microsoft.com/en-us/download/details.aspx?id=36821
- Lync 2013 Pre-Call diagnostic Tools
  http://www.microsoft.com/en-us/download/details.aspx?id=40733
- Lync 2013 Debugging Tools
  http://www.microsoft.com/en-us/download/details.aspx?id=35453
- Lync 2013 Poster
  http://www.microsoft.com/en-us/download/details.aspx?id=39968

References

- Microsoft TechNet
  http://technet.microsoft.com/en-us/library/gg398616.aspx
- TechNet blog
  http://blogs.technet.com
- TechNet Wiki
  http://social.technet.microsoft.com/wiki
- Mastering Microsoft Lync Server 2013 by Keith Hanna and Nathan Winters
  http://www.amazon.com/Mastering-Microsoft-Lync-Server-2013/dp/1118521323
- Getting Started with Microsoft Lync Server 2013 by Fabrizio Volpe
  http://www.packtpub.com/getting-started-with-microsoft-lync-server-2013/book