Configuring your Active Directory Infrastructure for Express for Lync 2.0

Overview

Active Directory (AD) is the basis for any Microsoft Infrastructure. It is a directory service that is included with all versions of Microsoft Windows Server products. An AD domain controller authenticates and authorizes all users and computers within a Microsoft Windows domain network. It can be used to supply group and security policies for all computers in the domain environment.

For more information about Active Directory, please see visit the links below:

- Wikipedia Explanation of Active Directory
- Microsoft White Paper on identity access
- Microsoft Technet description of changes to AD in Windows Server 2012

Express for Lync requires that an Active Directory infrastructure be setup. It also requires the installation of Active Directory Certificate Services for the handling of TLS certificates throughout the Lync 2013 Deployment.

If you already have a domain controller deployed, you can skip the setup of the Domain Controller virtual machine and continue to the section which shows you how to configure certificate services for your lync deployment.

**NOTE:** Please view this link in order to determine if your domain controller meets the requirements for Lync Server 2013.

Activating the Domain Controller Virtual Machine

The Express for Lync Domain Controller virtual machine can be activated by using the Windows Hyper-V Manager applet. Please follow the instructions below to activate the VM:

1. Access the Windows Start Screen by pressing on the Windows key on your keyboard.
2. Click on the Hyper-V Manager tile to launch the Hyper-V manager.
3. In the Windows Hyper-V Manager window, select the Virtual Machine labelled "WinSrvr2012DC". Right click on it, and select "Settings...".

4. In the settings window, on the left hand side you will notice configuration options. Scroll down to "Automatic Start Action" and select "Always Start the Virtual Machine automatically". This will always start the domain controller when the Express for Lync appliance boots up. Click OK to accept the changes.

5. Double click on the virtual machine labelled "WinServer2012DC" to launch the Remote Terminal Window. Click on the start button to start the virtual machine. The start button is the Green icon at the top of the virtual machine connection window.

Install and Configure Windows Server 2012 as the Primary Domain Controller
Install the Active Directory Domain Controller Role

In order for Windows Server to gain the role of the domain controller, it must go through the domain controller promotion (dcpromo) process. Follow the steps below in order to activate the domain controller role:

1. At the virtual machine welcome screen, go to the action menu, and click on the menu item “Ctrl+Alt+Delete” to bring up the login screen. Enter the following credentials to login:
   username: administrator
   password: sangoma1!

2. Once logged in, click on the “Server Manager” icon from the Windows Start Screen. This will launch the Server Manager MMC snap-in.

3. From the server manager window, click on “Add Roles and Features”. This will launch the “Add Roles and Features Wizard”. 
4. In the “Add Roles and Features Wizard”, click Next to begin the Active Directory installation.

5. In the next screen, make sure that “Role Based or Feature Based Installation” is marked and click Next to continue.

6. At the server selection screen, make sure the server you are working on is selected. Please note that usually this server will be selected as it is the first system in the server pool.

7. At the role selection screen, make sure the following roles are checked off:
   - Active Directory Domain Services
   - DNS Server
   
   Please note, when selecting the roles above, you will be notified that some other feature requirements are needed for the roles. Accept the features it suggests.
Also note that the DNS Server role requires that the Domain Controller VM be set to a static IP address. If it is set to DHCP, then the Add Role and Feature wizard will warn you to adjust it.

8. No other features are required. Click Next to proceed to the AD DS configuration. (This may take a few minutes for the proceeding Next to appear as AD checks for other ADs)

9. The next two screens will inform you that you are setting up both AD DS and DNS Server. Click Next to both screens to proceed to the confirmation screen.

10. At the confirmation screen, make sure “Restart the destination server automatically if required” is checked off. This will reboot the virtual machine if required when all the roles are installed. Click Install to begin the installation process.

11. Once the wizard has completed, you will notice the Results window asking you to promote the server to a domain controller. Click on that link to start the Domain Controller promotion process.

Configure the Active Directory Domain Controller Role
1. In the Active Directory Domain Services Configuration wizard, you will be asked to create a new domain or add to an existing domain, please select Add a New Forest. In the Root Domain Name textbox, enter the domain name you would like to use for your Lync Deployment and your entire Active Directory infrastructure. For this guide, I will be using lynctest.local.

2. In the next screen, the wizard will ask you what functional level would you like the forest to run on. Leave these at defaults unless you absolutely require changing them. Set a restore mode password as well just in case you would ever need to make changes to the Active Directory forest. For more information on Domain and Forest Functional Levels, please go to http://technet.microsoft.com/en-us/library/cc771294.aspx. Also, make sure that Domain Name Server and Global Catalog Server have been checked off as these are required for the Primary Domain Controller (PDC) Role.

3. In the DNS Options, you will notice a a warning stating a DNS Delegation source cannot be found. Please ignore this as the DNS Server roles have not been created yet and will be created once the AD Infrastructure is setup. Click Next to proceed.

4. The next screen will ask you for the NetBIOS name. This should be left at whatever default the wizard provides. Click Next to continue.
5. The next screen will ask you about what paths you would like the directory service to be installed to. Make sure they are all left at their defaults. If for some reason something has changed, make sure they are the same as the screenshot below.

![Active Directory Domain Services Configuration Wizard](image)

6. The next screen will ask you to review your settings. Review them and click Next to proceed.
7. The Active Directory wizard will now do a pre-requisite check on the server to make sure that it can be installed. You will notice a few warnings being provided due to the DNS server, IP address being DHCP, and cryptography algorithms. These can be ignored as they are not related to this install. Click Install if the pre-requisite check has passed.

![Active Directory Domain Services Configuration Wizard](image)

8. The installer will start the installation. The Domain Controller will need to reboot during the installation process. This process can take at minimum 20 minutes to complete. Please be patient during this process. Once completed, you would need to log into the machine with your new domain administrator account. At the Windows Welcome screen, press ctrl-alt-delete to login. The username and password are the exact same credentials as the ones you used to prior to upgrading the server to a domain controller. DO NOT LOSE ACCESS TO THIS ACCOUNT AS THIS ACCOUNT NOW BELONGS TO BOTH THE ENTERPRISE AND DOMAIN ADMINISTRATOR GROUPS.

---

**Install and Configure Active Directory Certificate Services**

**Install Active Directory Certificate Services Role**
1. Once logged in, click on the “Server Manager” icon from the Windows Start Screen. This will launch the Server Manager MMC snap-in.

2. From the server manager window, click on “Add Roles and Features”. This will launch the “Add Roles and Features Wizard”.

3. In the “Add Roles and Features Wizard”, click Next to begin the Active Directory installation.
4. In the next screen, make sure that “Role Based or Feature Based Installation” is marked and click Next to continue.

5. At the server selection screen, make sure the server you are working on is selected. Please note that usually this server will be selected as it is the first system in the server pool.

6. At the role selection screen, make sure the following roles are checked off:
   - Active Directory Certificate Services
   - Internet Information Services (IIS)
   Please note, when selecting the roles above, you will be notified that some other feature requirements are needed for the roles. Accept the features it suggests.
7. At the feature selection screen, check off the following roles:
   .NET Framework 3.5

![Select features][1]

8. When the Active Directory Certificate Services wizard comes up, click Next to continue.
9. In the Certificate Services Role selection, select "Certificate Authority Web Enrollment". A window will pop up asking you to add some more features like below:

![Add features][2]

Click Add Features to accept the extra roles and features that is required. Once returned to the screen below, click Next to proceed

![Select role services][3]

10. When the IIS role services come up, click Next to proceed and accept the defaults. Click Next again to proceed to the confirmation screen.
11. At the Confirmation window, make sure "Restart the destination server if required" is checked off and click "Install" to start the installation.
11. **If you are having an issue installing the .NET Framework features, you would need the original Windows Server 2012 ISO image. You can download the image directly from Microsoft by clicking this link.**

Once the installation is complete, click Close to end the wizard.

12. Configure Active Directory Certificate Services

In order to configure certificate services, please follow the steps below:

1. Click on the “Server Manager” icon from the Windows Start Screen. This will launch the Server Manager MMC snap-in.
2. From the top right hand corner, click on the flag with the alert sign below and click on "Configure Active Directory Certificate Services".

3. In the Active Directory Certificate Services wizard, enter the domain credentials you would like to use to configure the role. The user account used MUST be a member of the Enterprise Admins group. Enter the account you would like to use, or leave the default and click Next to proceed.

4. In the role services window, select the "Certificate Authority" option and the "Certificate Authority Web Enrollment" option. Click Next to proceed.
5. In the setup type, choose “Enterprise CA”. Click Next to continue.

6. In this next screen, make sure “Root CA” is highlighted and click Next to proceed.

7. When asked to specify the type of private key, select the “Create new private key” button and click Next to proceed.
8. At the cryptography options screen, make sure the key length is 2048 and the hash algorithm is set to “SHA1”.

9. When asked to specify the name of the CA, leave it all at defaults. Click Next to proceed.

10. At the CA validity period screen, adjust the length of time you would like your private key to remain valid. The default is 5 years. Unless you absolutely need a different validity period, leave the default and click Next to proceed.
11. In the CA Database screen, leave the database locations default. Click Next to proceed.

12. At the confirmation screen, go through the Certificate Authority configuration to ensure that all the settings are correct. Once you are happy with the configuration, click “Configure” to being the process.

13. Once the configuration has completed, click on Close to close the AD CS Configuration wizard.

Enable Active Directory Certificate Services Auto-Enrollment Setting

Active Directory Certificate Services needs the Auto-Enrollment setting enabled for Lync Server 2013. This setting will automatically enroll all user and computer accounts, and provide them with the certificates required to connect to the domain. To enable it, please follow the instructions below:
1. From the Windows Start screen, select the Control Panel Tile.

2. Double click on "Administrative Tools" to bring up the Administrative tools control panel.

3. From the Administrative Tools window, double click on "Group Policy Management" to bring up the Group Policy Management MMC.

4. To get to the "Default Domain Controllers Policy", you would need to navigate through the following menu list: Forest: <AD Forest> -> Domains -> <AD Forest Name> -> Domain Controllers -> Default Domain Controllers Policy.

5. Right click on the Default Domain Controllers Policy and select "Edit" from the menu. This will launch the Group Policy Editor.
6. In the group policy editor, navigate down the following menu list to get to the Certificate Service Auto-Enrollment policy: Computer Configuration->Policies->Windows Settings->Security Settings->Public Key Policies.

7. Double click on the Certificate Services Client - Auto Enrollment policy to open the configuration window. Set the Configuration Model to "Enabled", and click on OK to accept the changes. Once done you may close both the Group Policy Editor and the Group Policy Management MMC console.