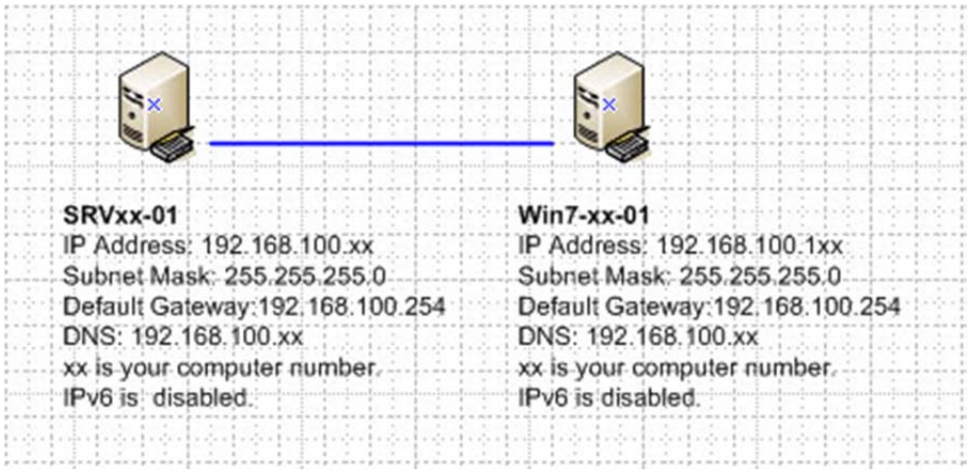
LAB 12: Creating a Domain with a Domain Controller

In this lab, you will create a domain with a domain controller and a Windows 7. You will configure **SRVxx-01** as the domain controller and DNS server and **Win7-xx-01** will a computer in the domain.

Lab Requirements:

Completion of Lab 01, 02, 03, 04, and 05

Lab Setup: Initial

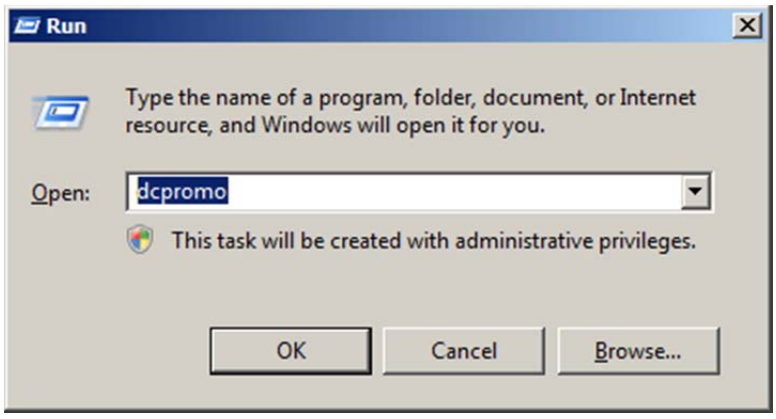


- **Exercise 1: Configuring IPv4 addresses.**

1. On each virtual machine, restore the **After installation** snapshot.
2. On each virtual machine, disable IPv6 and configure IPv4 address according the Lab Setup.

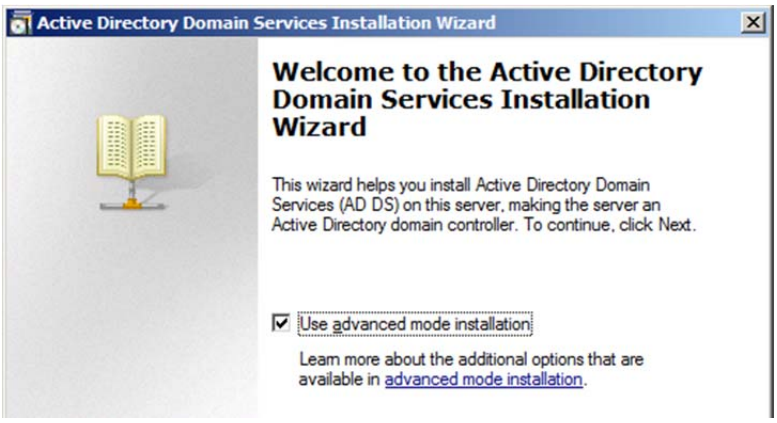
- **Exercise 2: Configuring the first domain controller in an Active Directory domain**

1. On SRVxx-01, open **Start > Run** prompt and type **dcpromo** in the text box. Click **OK**.

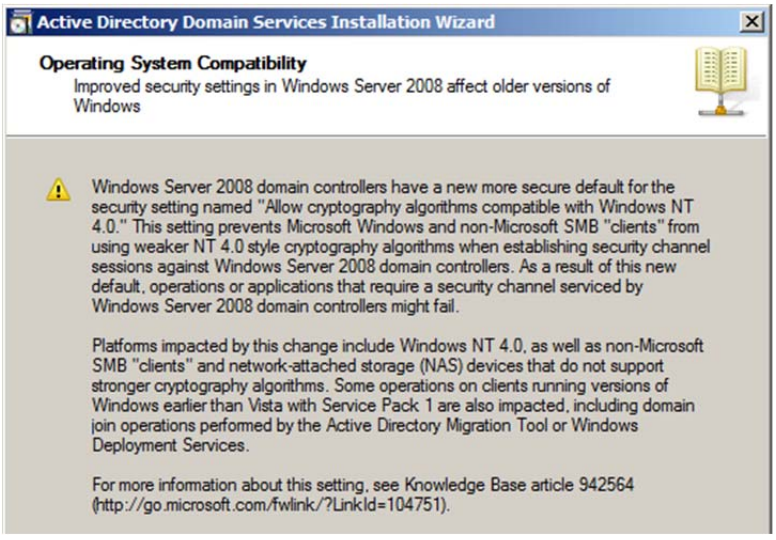


Active Directory Domain Services binaries are being installed. Please wait.

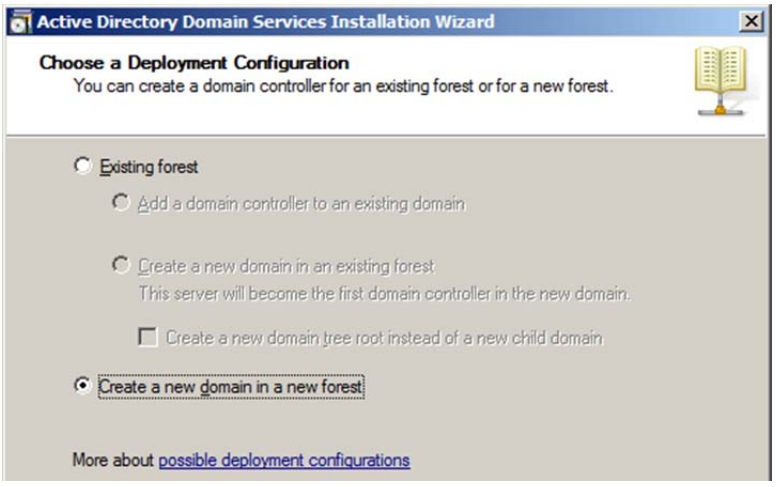
2. The **Active Directory Domain Services Installation Wizard** dialog box appears. Check the **Use advanced mode installation** option. Click **Next**.



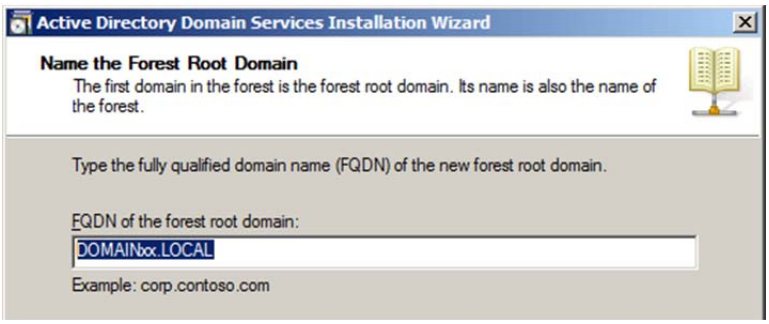
3. The **Operating System Compatibility** dialog box appears. Click **Next**.



4. The **Choose a Deployment Configuration** dialog box appears. Select the **Create a new domain in a forest** option. Click **Next**.

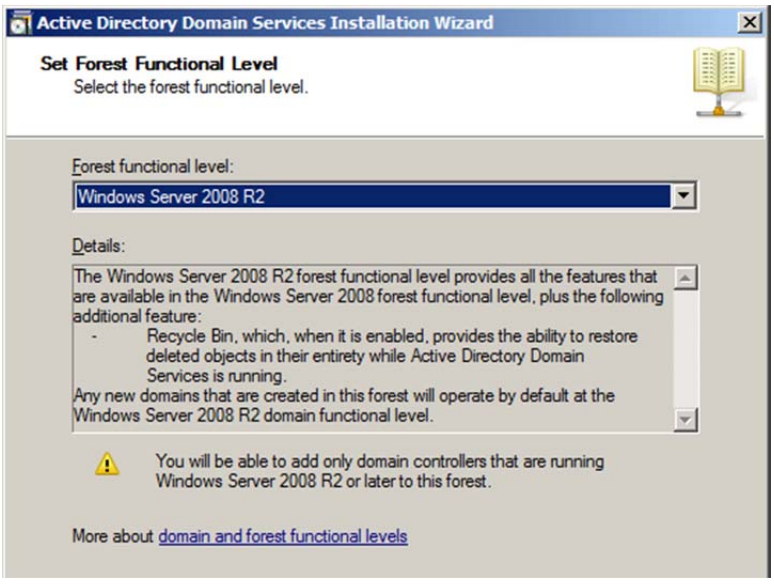


5. The **Name the Forest Root Domain** dialog box appears. Type **DOMAINxx.LOCAL**, **xx** is your computer number. Click **Next**.

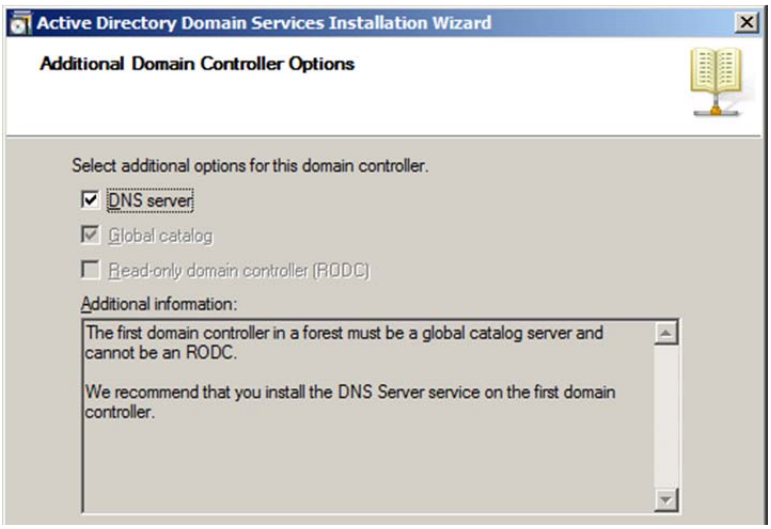


6. The **Domain NetBIOS Name** dialog box appears. Take the default setting and click **Next**.

7. The **Set Forest Functional Level** dialog box appears. Select **Windows 2008 R2** and click **Next**.

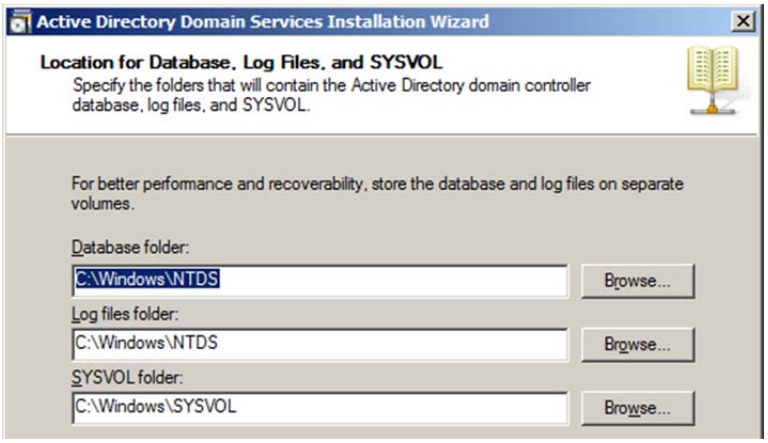


8. The **Additional Domain Controller Options** dialog box appears. Click **Next**.

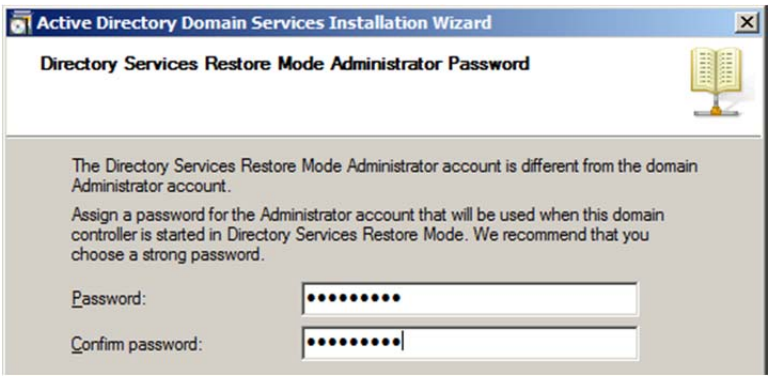


9. The DNS warning dialog box appears. Click **Yes**.

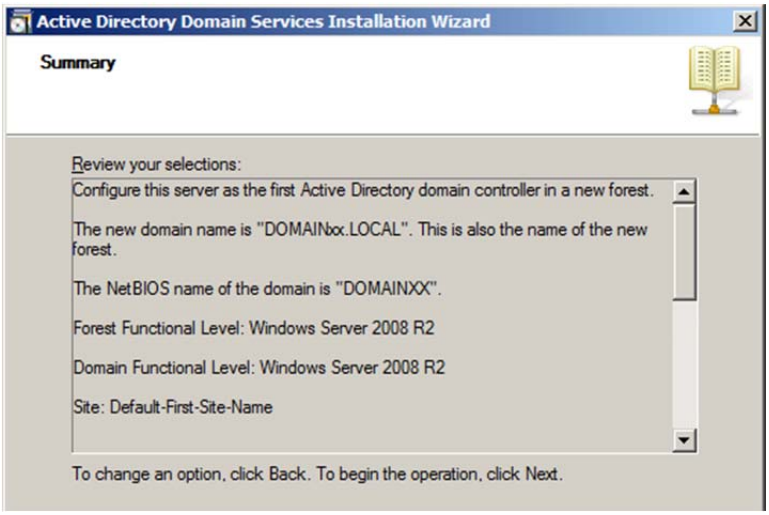
10. The **Location for Database, Log Files, and SYSVOL** dialog box appears. Take the default settings and click **Next**.



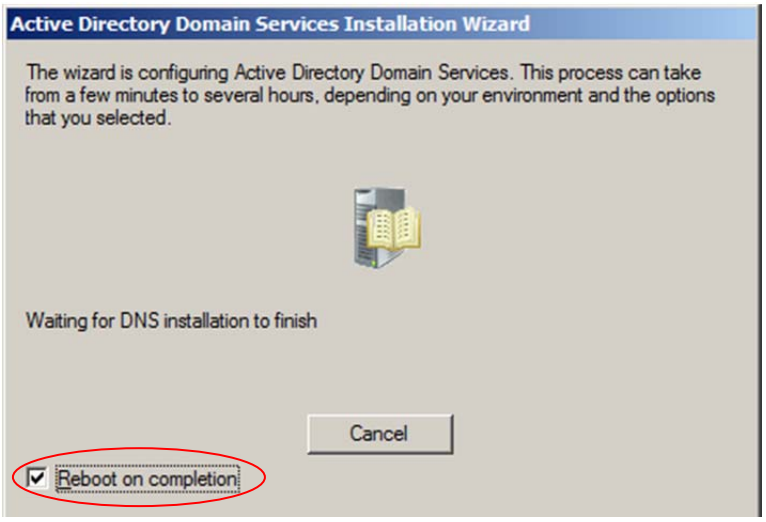
11. The **Directory Service Restore Mode Administrator Password** dialog box opens. Type **P@ssword** and click the **Next**.



12. The **Summary** dialog box opens. Click **Next**.



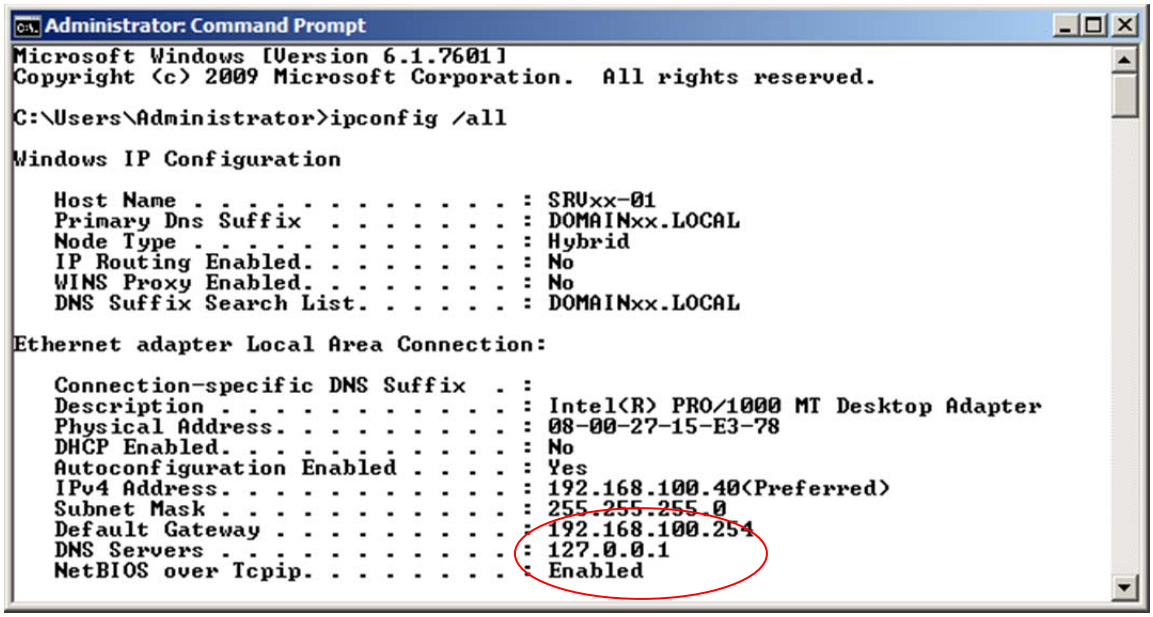
13. The **wizard** is configuring Active Directory Domain Services. Check the **Reboot on completion** option. Please wait.



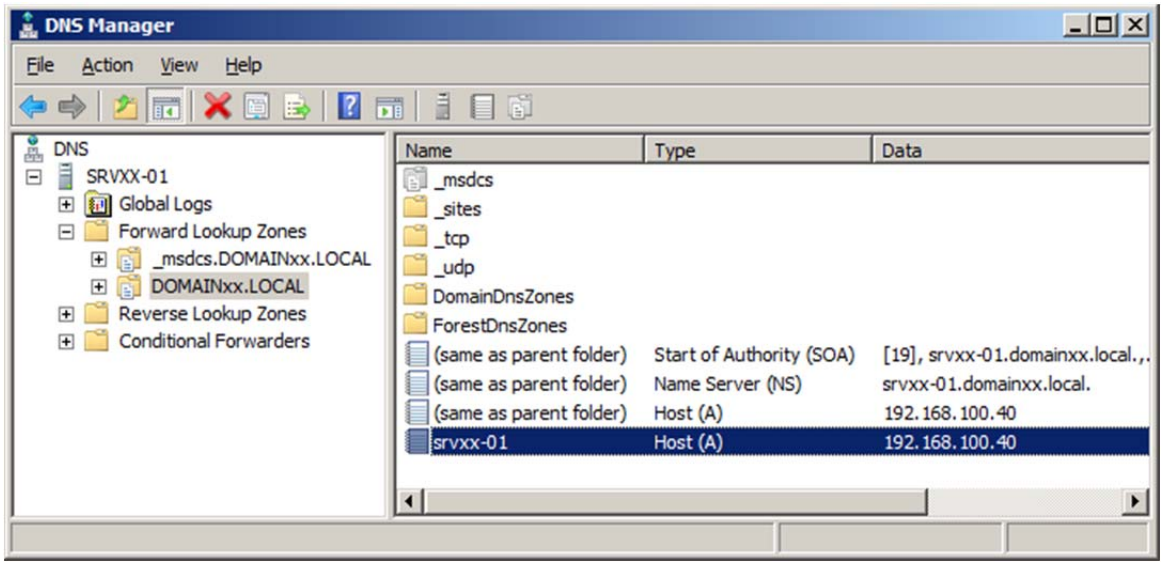
- **Exercise 3: Configuring DNS**

1. On **SRVxx-01**, login.

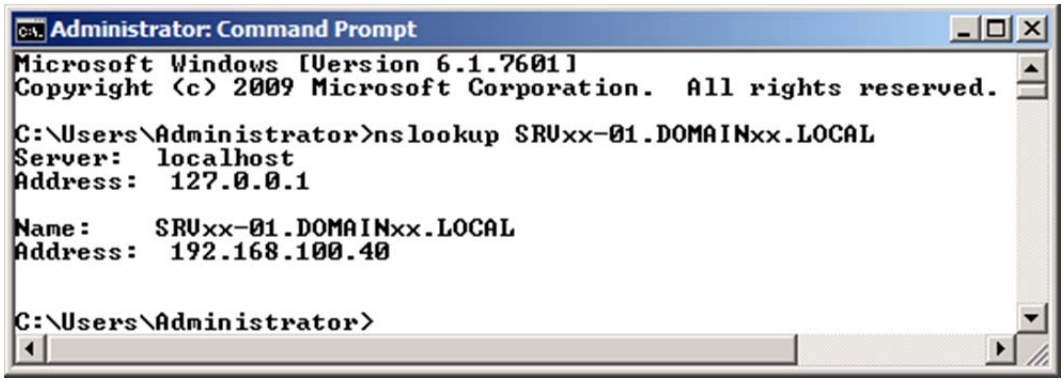
2. Open a command prompt and type **IPCONFIG /ALL**. The DNS IP address has been set to **127.0.0.1**, which points to itself; **SRVxx-01**.



3. Click **Start > All Programs > Administrative Tools > DNS**. Navigate to **DOMAINxx.LOCAL**. **DOMAINxx.LOCAL** has been configured in the Forward Lookup Zones.

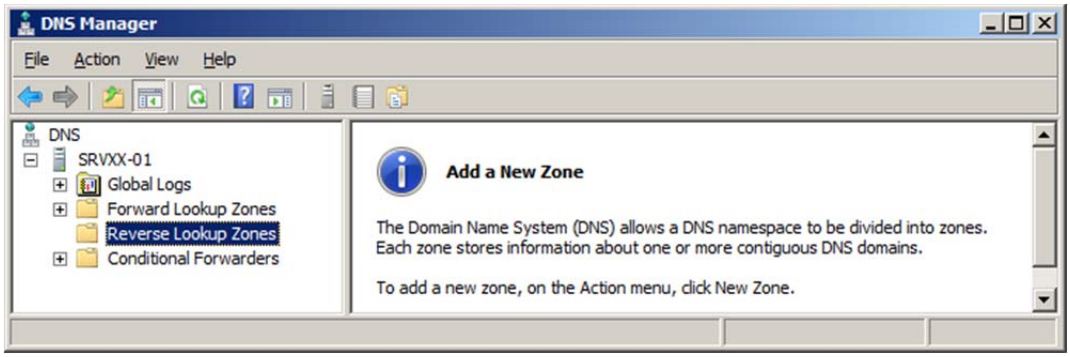


4. Open a command prompt and type **`nslookup SRVxx-01.DOMAINxx.LOCAL`**.

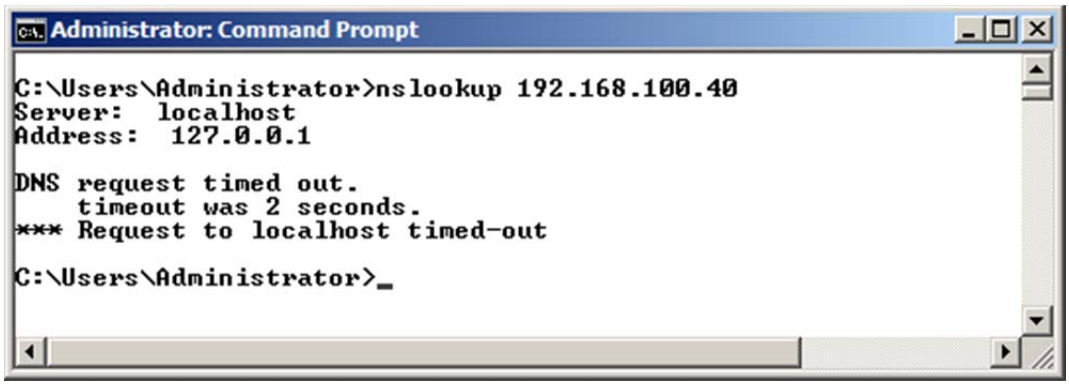


Server: localhost and **Address: 127.0.0.1** is the DNS server that is providing the name resolution service. Your local DNS server searches the Forward Lookup Zones to provide the IP address of **SRVxx-01.DOMAINxx.LOCAL**.

Click the **Reverse Lookup Zone** in the **DNS Manager**; you will see that nothing has been configured.



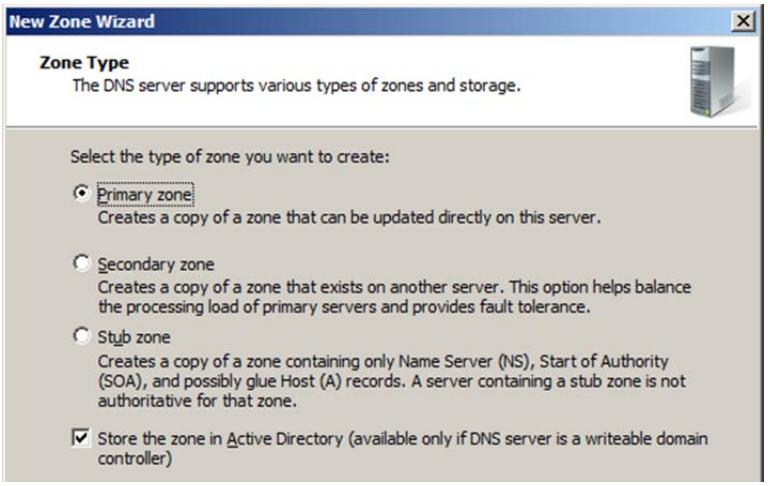
In the command prompt, type **`nslookup 192.168.100.xx`**.



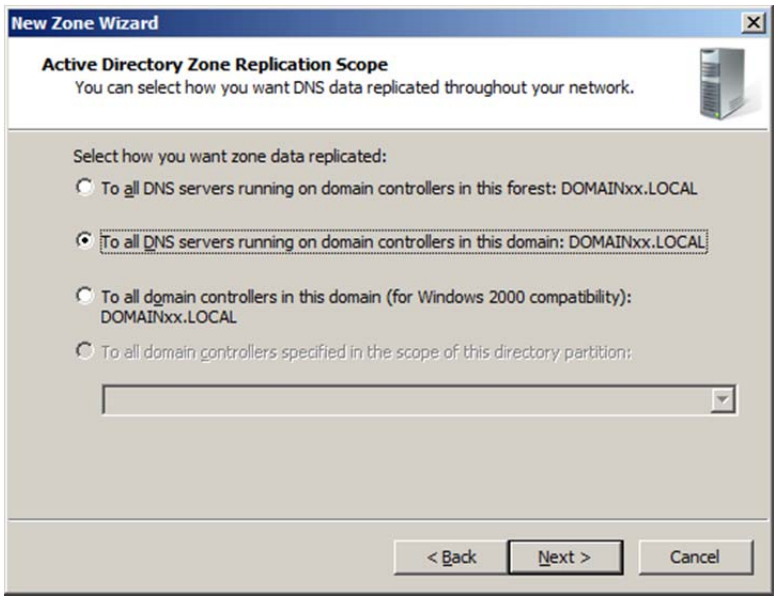
The output shows that DNS request timed out. This is because a Reverse Lookup Zone doesn't exist for your domain. Now you will configure a Reverse Lookup Zone.

5. You will configure the Reverse Lookup Zone for your domain. Right-click **Reverse Lookup Zones**, and click **New Zone…**. The **New Zone Wizard** dialog box appears. Click **Next**.

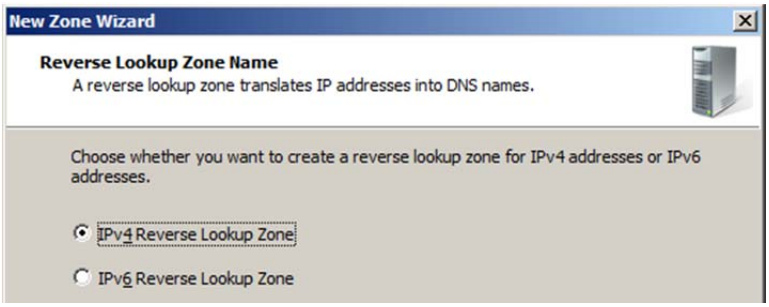
6. The **Zone Type** dialog box appears. Click **Next** without changing the option.



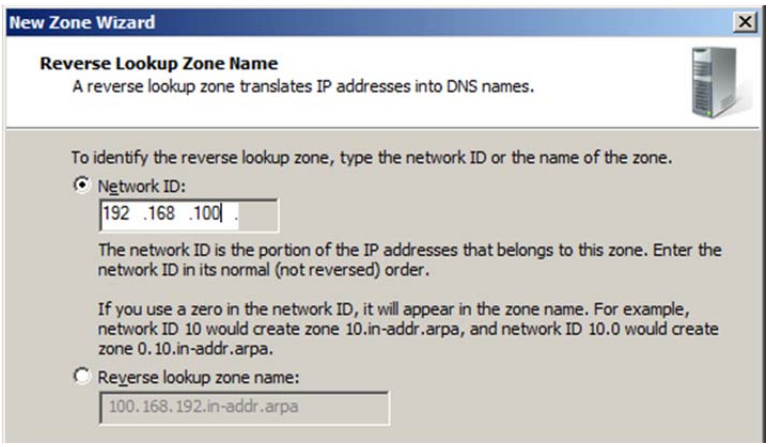
7. The **Active Directory Zone Replication Scope** dialog box appears. Click **Next** without changing the option.



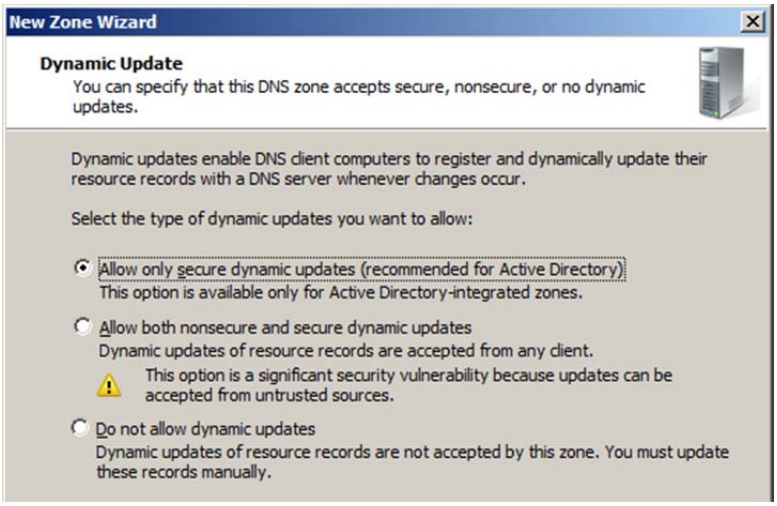
8. The **Reverse Lookup Zone Name** dialog box appears. Click **Next** without changing the option.



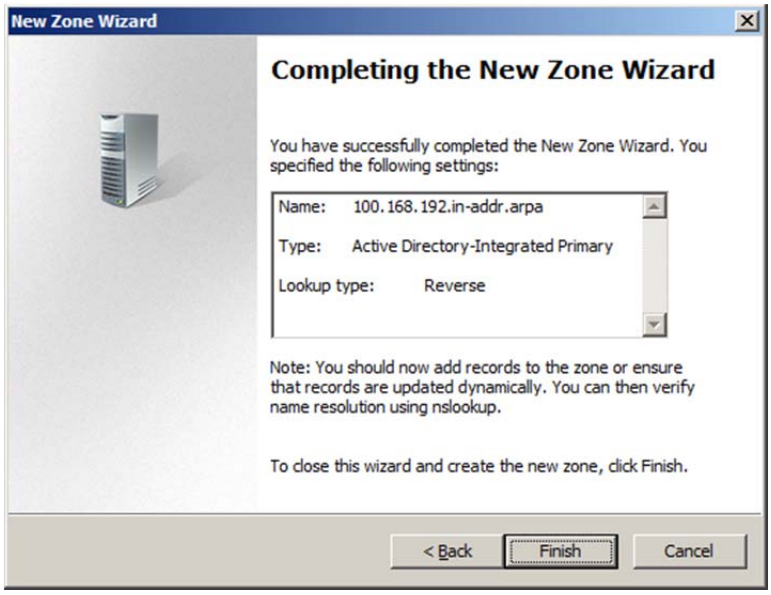
9. The **Reverse Lookup Zone Name** dialog box appears. Type **192.168.100** in the Network ID box. Click **Next**.



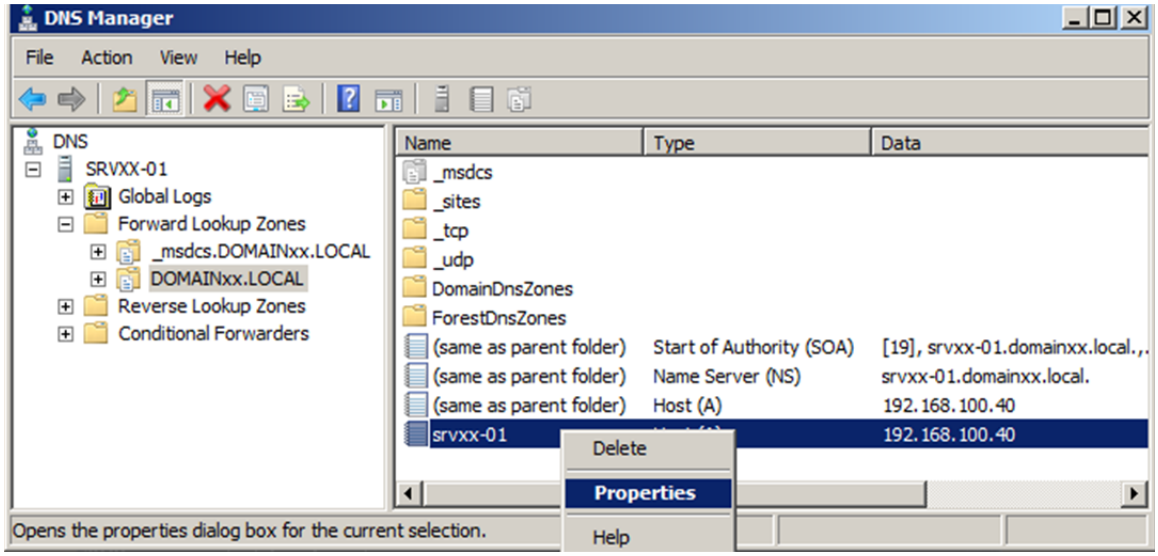
10. The Dynamic Update dialog box appears. Click **Next** without changing the option.



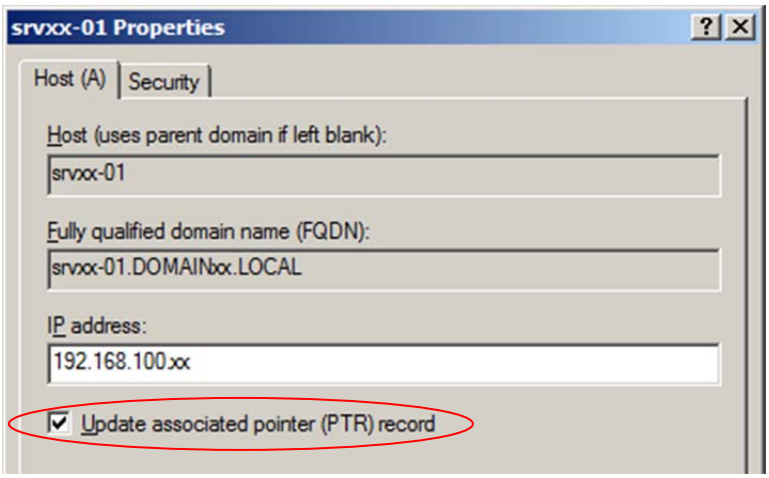
11. The Completing the New Zone Wizard dialog box appears. Click **Finish**.



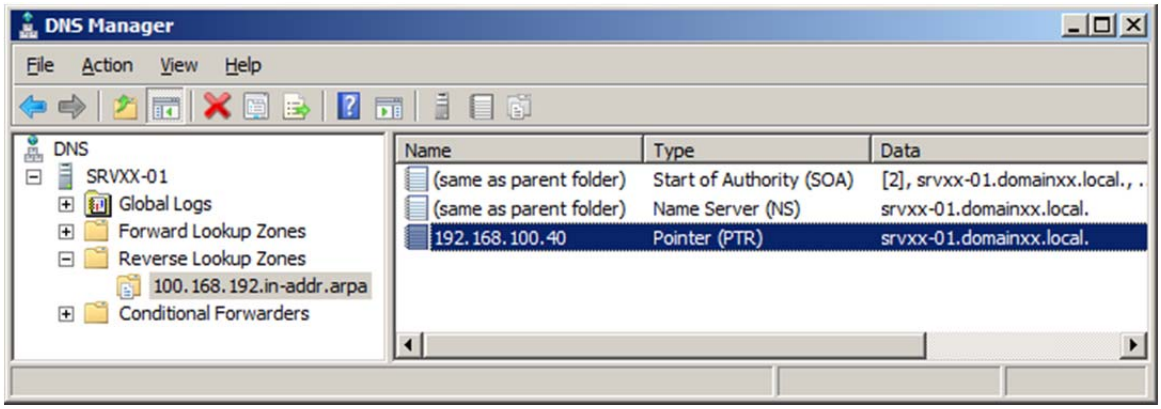
12. To update the **SRVxx-01** PTR record, right click **SRVxx-01** in the **Forward Lookup Zones > DOMAINxx.LOCAL**, and select **Properties**.



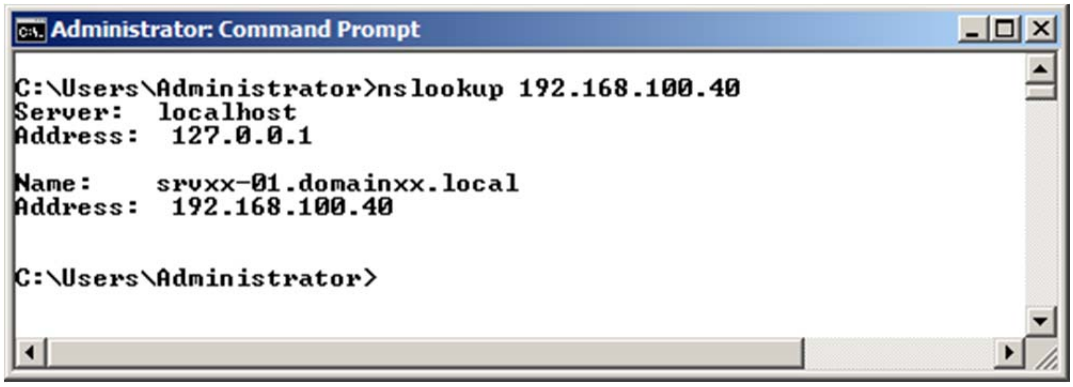
13. The **SRVxx-01 Properties** dialog box appears. Check **the Update associated pointer (PTR) record** option. Click **OK**.



In the **Reverse Lookup Zones > 100.168.192.in-addr.arpa**, you see the PTR record for **SRVxx-01**.



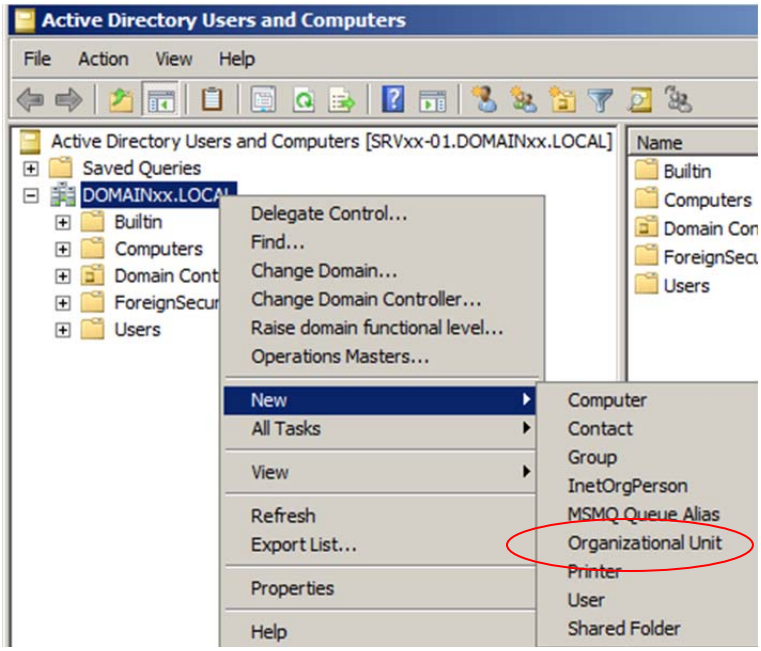
In the command prompt, type **`nslookup 192.168.100.xx`**.



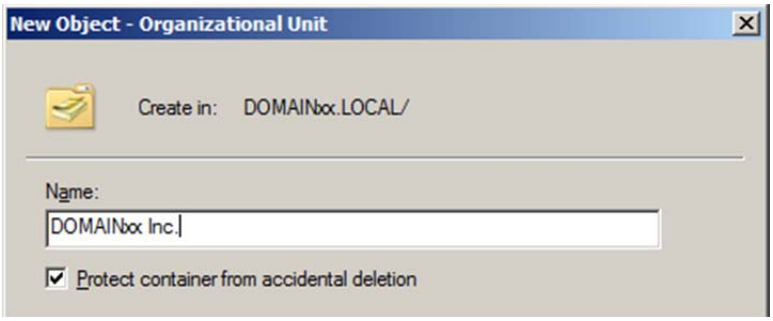
Now your local DNS server can provide the hostname of the IP address.

- **Exercise 4: Creating an Organizational Unit and User Object**

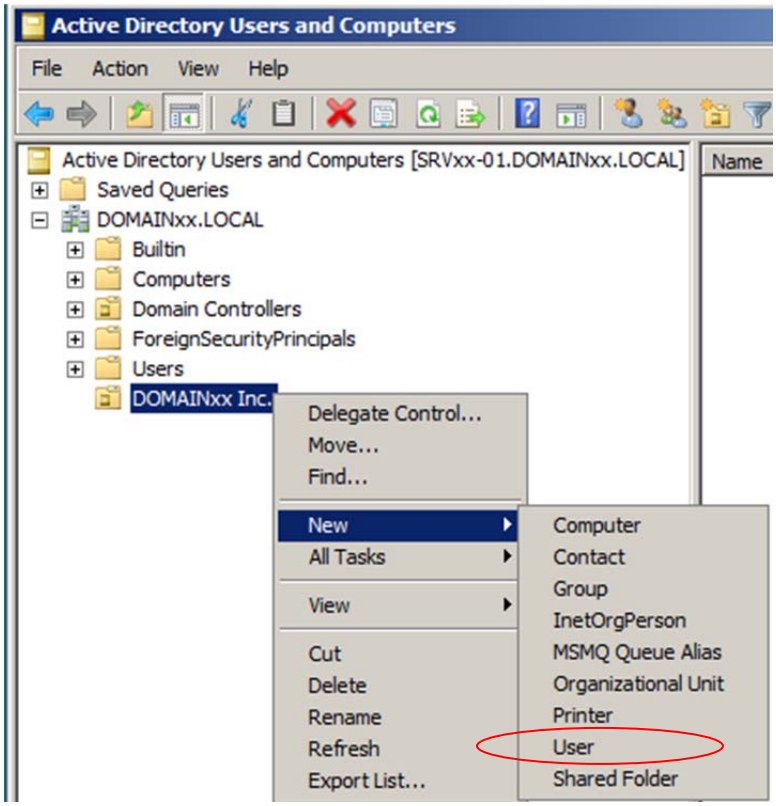
1. Open the **Active Directory Users and Computers** console (Start > All Programs > Administrative Tools > Active Directory Users and Computers). Right-click **DOMAINxx.LOCAL** and click **New > Organizational Unit**.



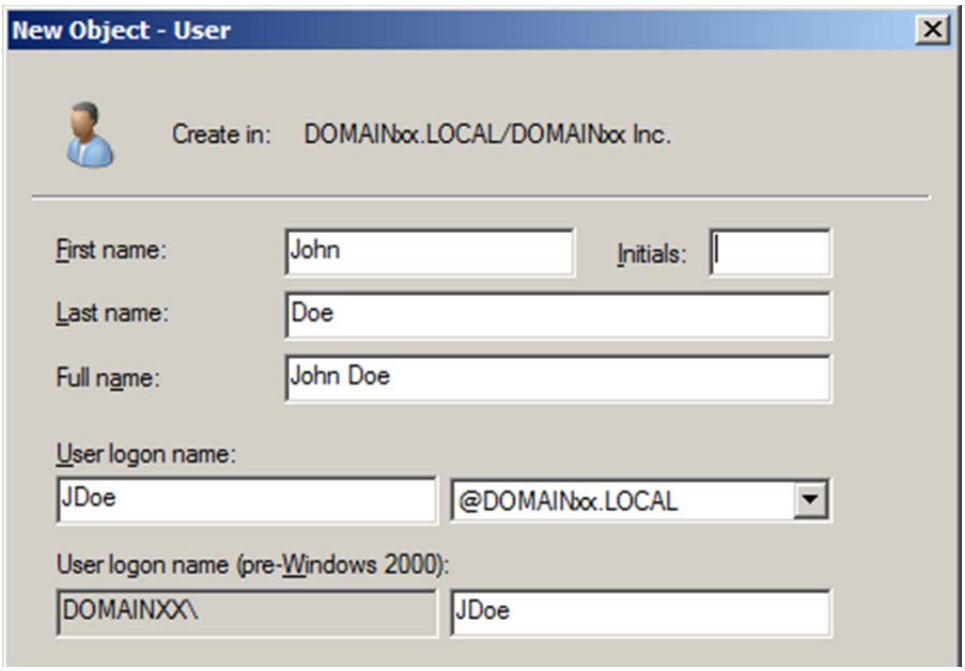
2. The **New Object – Organizational Unit** dialog box appears. Type **DOMAINxx Inc.** in the **Name** box and click **OK**.



3. The **DOMAINxx Inc.** OU is created. Right-click **DOMAINxx Inc.** OU and click **New > User**.



4. The **New Object – User** dialog box appears. Fill the textboxes as show in the below figure and click **Next**.



5. The Password dialog box appears. Type **P@ssword** in the text boxes. Uncheck the first option. Click **Next**.

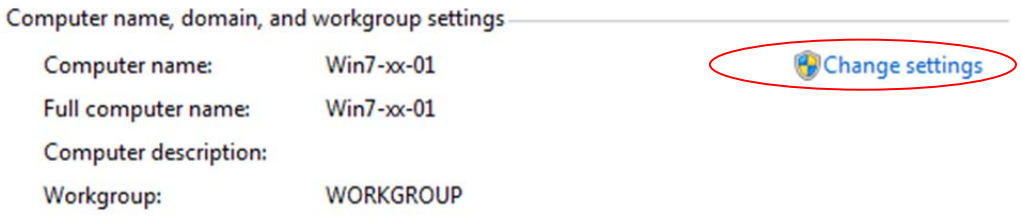
6. The Summary dialog box appears. Click **Finish**. The **John Doe** user object appears in the **DOMAINxx Inc.** OU.

- **Exercise 5: Joining a Active Directory domain**

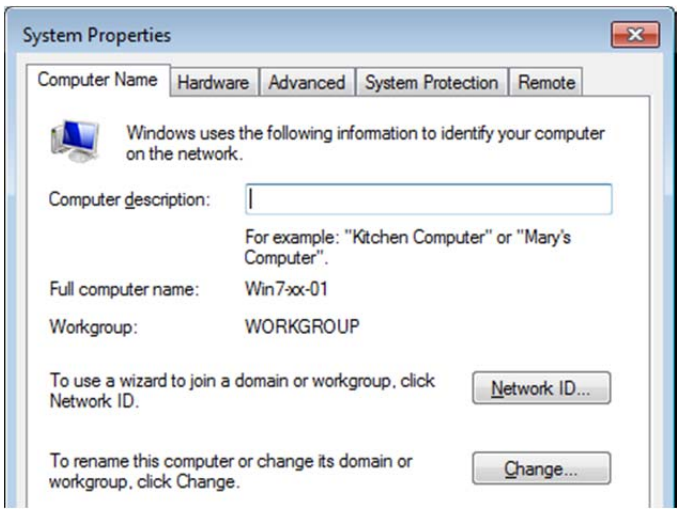
1. Start the virtual machine **Win7-xx-01**.

2. Open the command prompt and execute **PING 192.168.100.xx**. If you don't get any replies, check the TCP/IP settings on both machines.

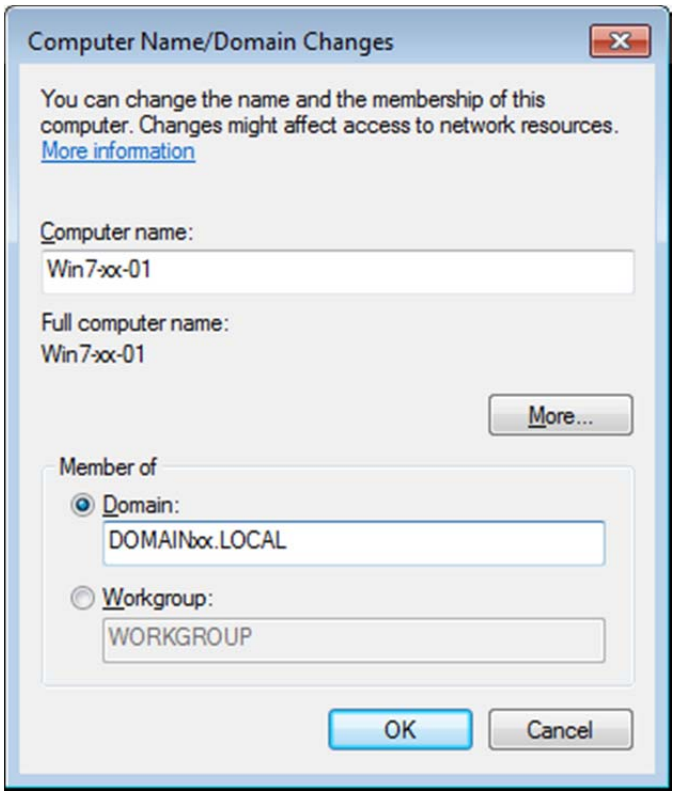
3. Open the **Control Panel**. Double-click **System** icon. Click **ChangeSettings** link under Computer name.



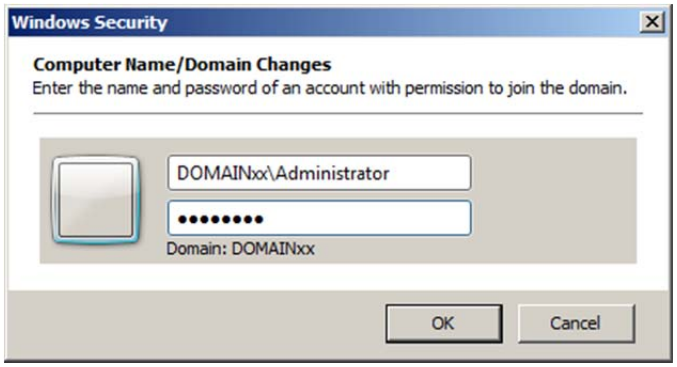
The **System Properties** dialog box appears. Click **Change…**.



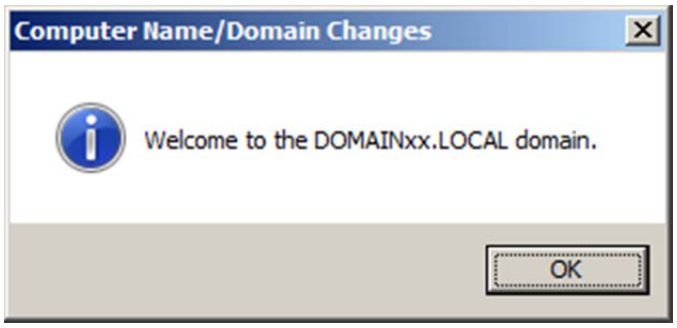
Select the **Domain:** option. Type **DOMAINxx.LOCAL** (xx is your monitor number). Click **OK**.



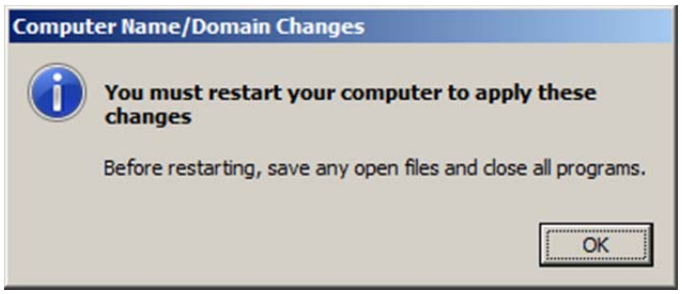
The **Windows Security** dialog box appears. Type **DOMAINxx\Administrator** in the User name box. Type **P@ssword** in the password box. If you use a different password, type your password for the account.



The Information dialog box appears. Click **OK**.

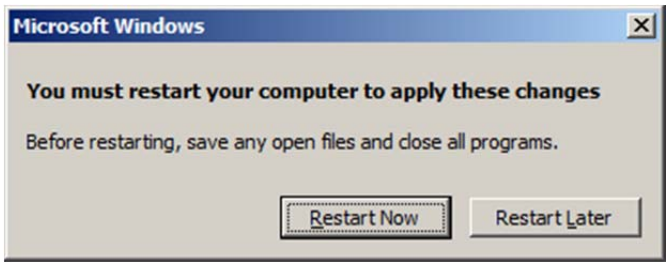


The Information dialog box appears. Click **OK**.



Click **Close** on the **System Properties** dialog box.

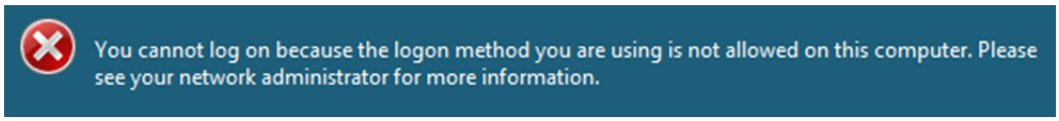
The Microsoft Windows dialog box appears. Click **Restart Now**. The system reboots. Now **Win7-xx-01** is a member server of **DOMAINxx.LOCAL**.



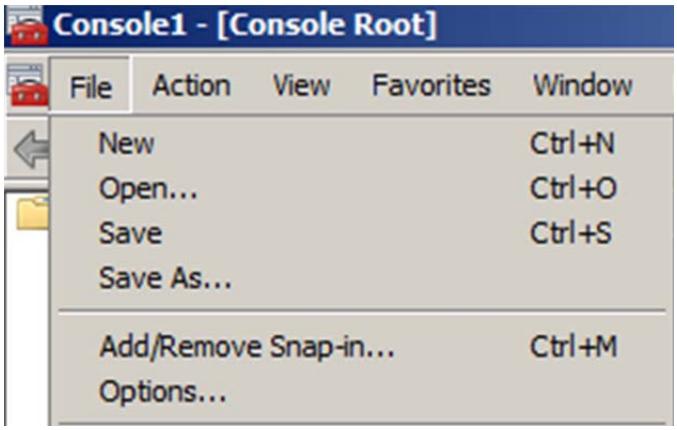
4. After sending **CTRL + ALT + DELETE** signal, The Local administrator account name (**Win7-xx-01\Admin** or the account you created) is displayed. You will need to logon as Domain administrator. Click **Switch User** and click **Other User**. Type **DOMAINxx\Administrator** in the User name box. Type **P@ssword** in the Password box. Press **Enter**.

- **Exercise 6: Allowing non-domain admin users to log on to the domain controllers**

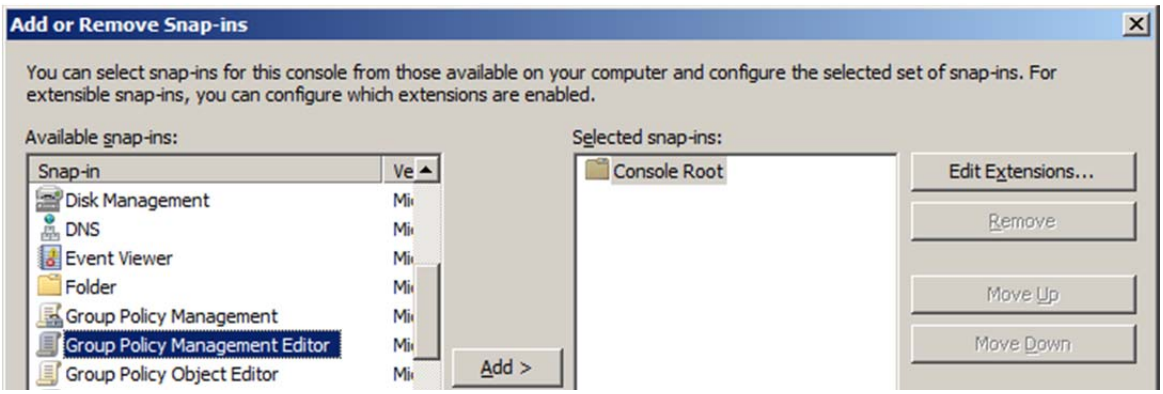
1. On **SRVxx-01**, log off and log on as **DOMAINxx\JDoe** user account. You should get the following message; this is because non-admin users can't log on to the domain controllers; John Doe is not an administrator. In a lab environment, since we are dealing with DCs only, we will allow non-admin users to log on to the DCs for testing.



2. On **SRVxx-01**, Open **Start > Run**. Type **MMC** in the text box. The **Microsoft Management Console** window appears. Click **File > Add/Remove Snap-in…**.

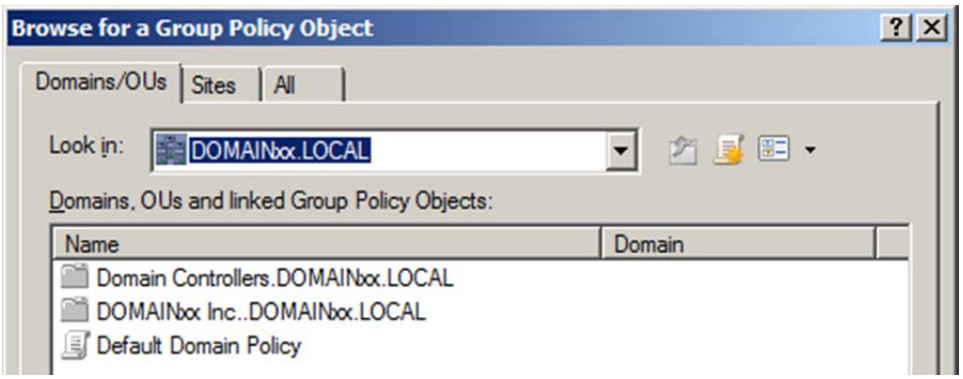


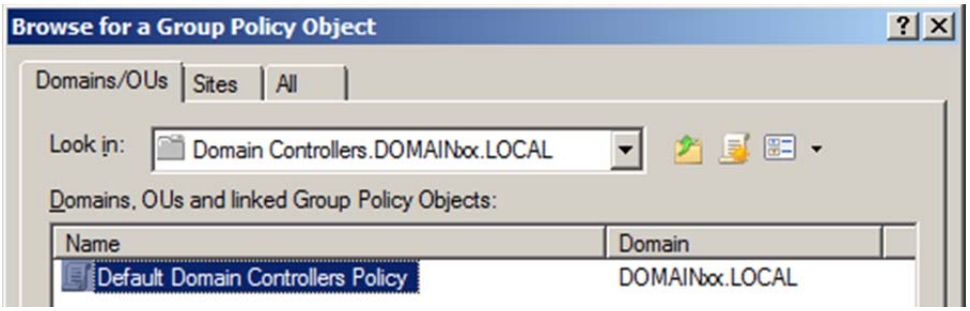
The **Add or Remove Snap-ins** dialog box appears. Select **Group Policy Management Editor** in the **Available snap-ins:** box, and click **Add >**.



The **Select Group Policy Object** dialog box appears. Click **Browse…**.

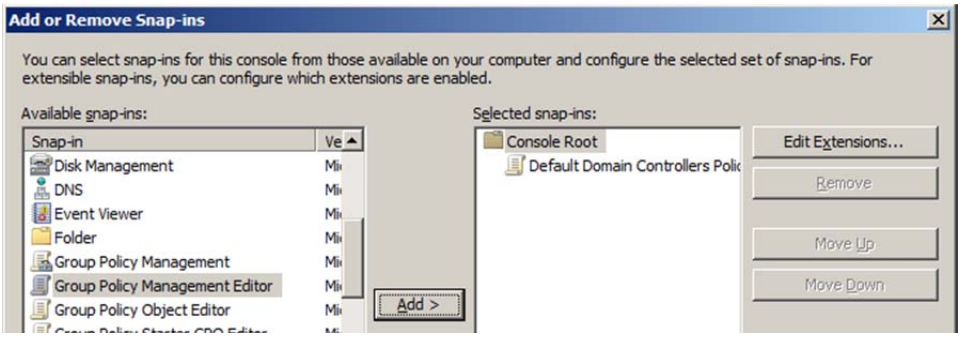
The Browse for a Group Policy Object dialog box appears. Double-click **Domain Controllers.DOMAINxx.LOCAL**. click **Default Domain Controllers Policy** and click **OK**.



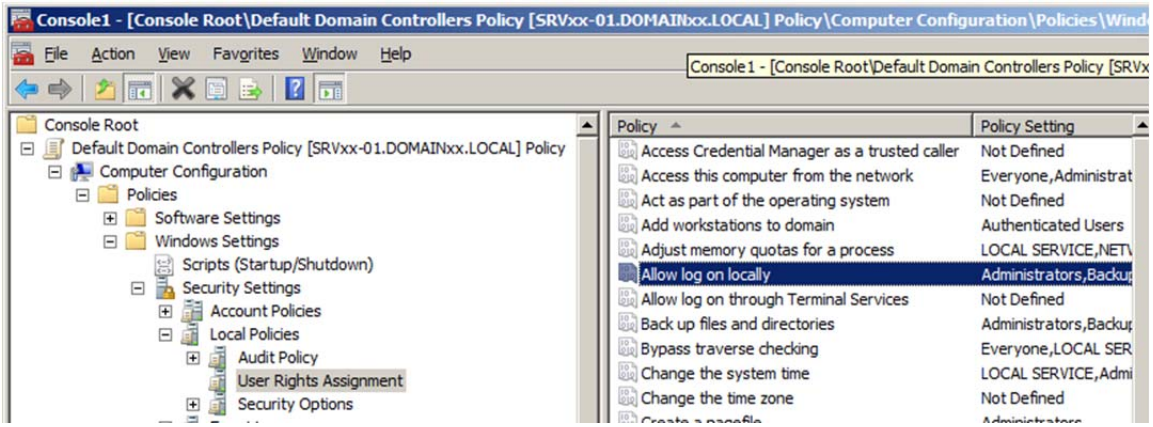


Click **OK**.

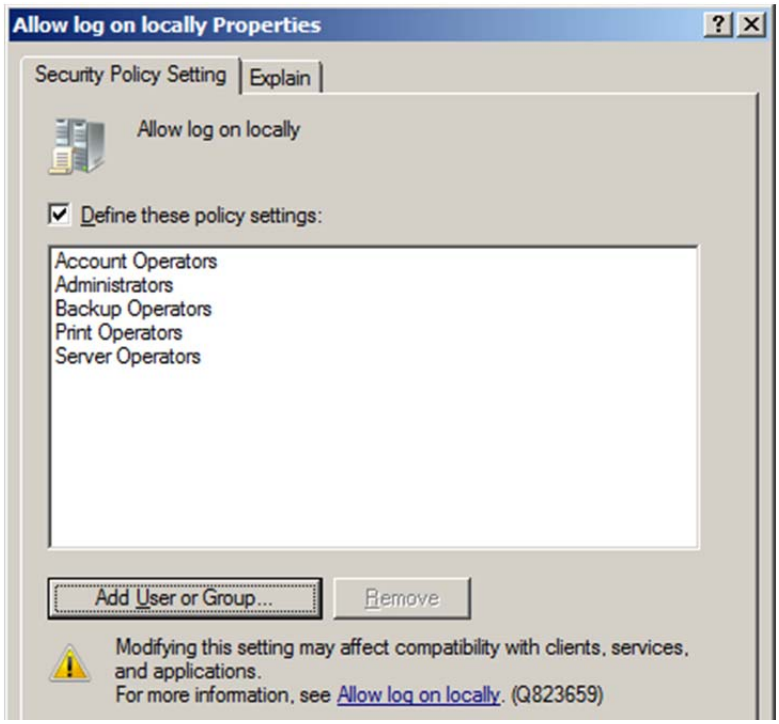
Click **OK**.

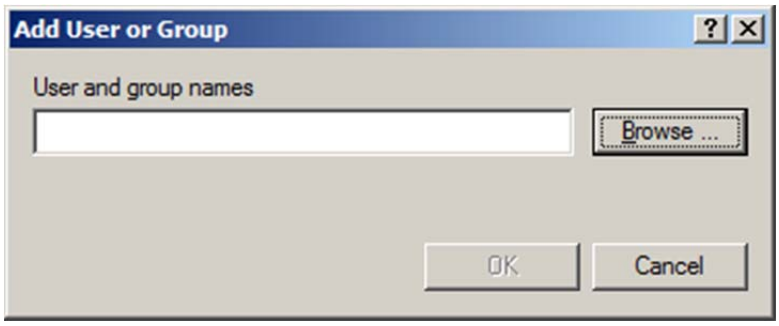


3. In the MMC **Console 1** window, navigate to the **User Rights Assignments** as shown below figure. Double-click **Allow log on locally**.

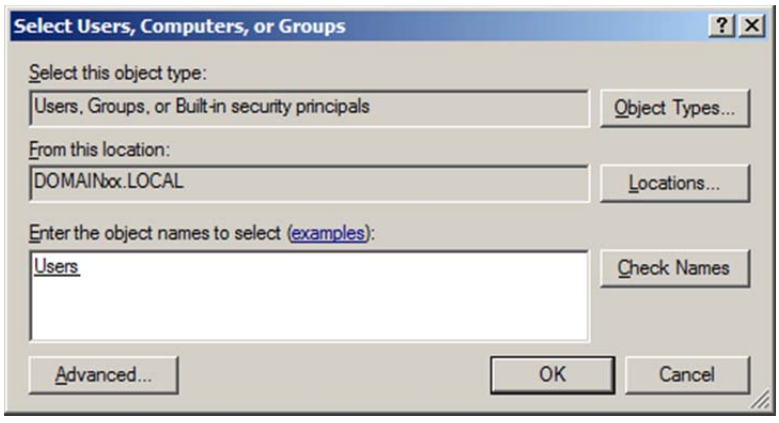


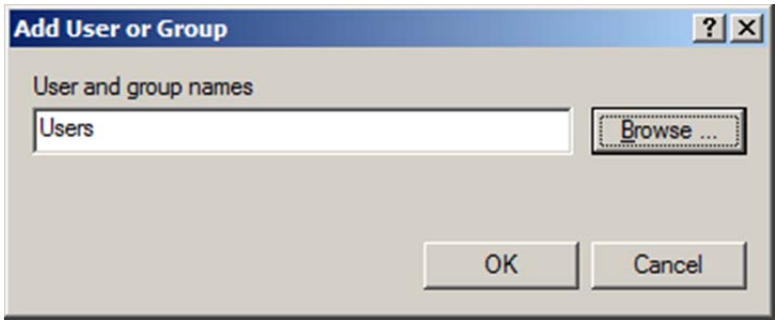
4. The **Allow log on locally Properties** dialog box appears. Click **Add Users or Group…**. The A**dd User or Group** dialog box appears. Click **Browse…**.



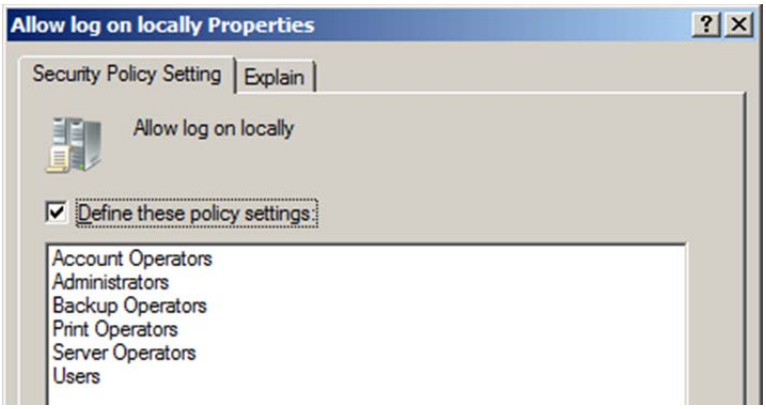


The **Select Users, Computers, or Groups** dialog box appears. Type **Users** in the text box and click **Check Names**. **Users** should be underlined. Click **OK**. In the **Add User or Group** dialog box, click **OK**.



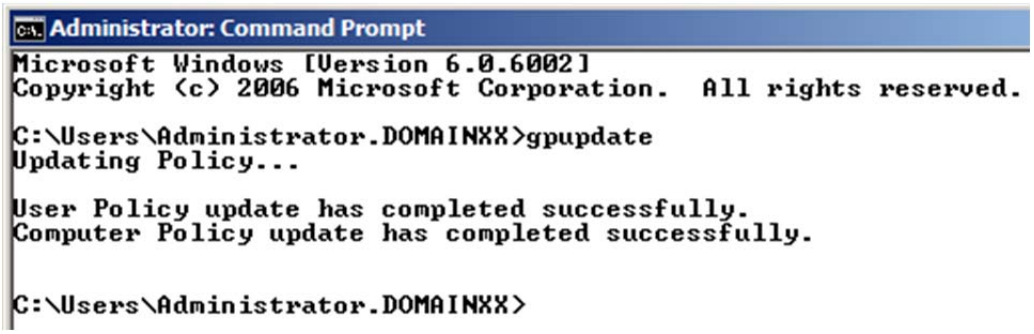


In the **Allow log on locally Properties** dialog box, **Users** group appears. Click **OK**.



5. Save the **Console 1** on the desktop.

6. On **SRVxx-01,** open a command prompt and execute **gpupdate**.



7. On **SRVxx-01**, log off and log on as **DOMAINxx\JDoe**. John Doe should be able to log on successfully. John Doe is a member of Domain Users group and Domain Users group is a member of Users group. So, when you assign **Allow log on locally** user right to Users group, John Doe will inherit the user right.