

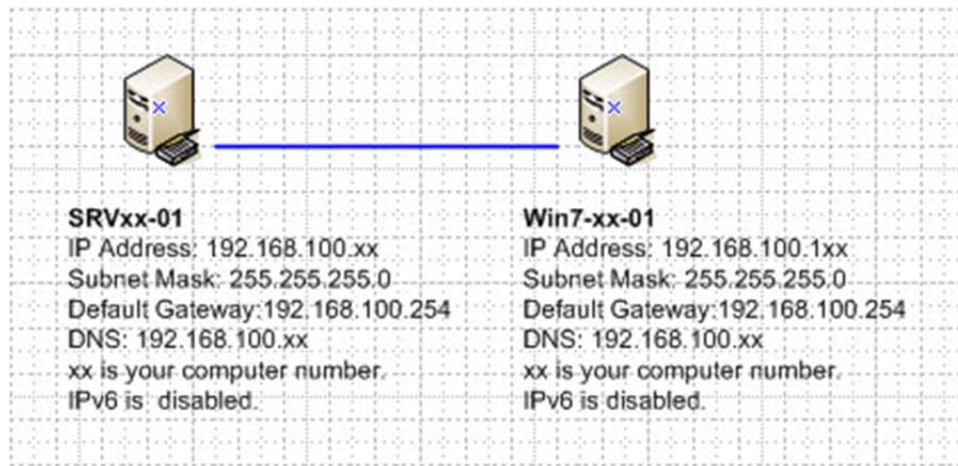
LAB 12: Creating a Domain with a Domain Controller

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 be a computer in the domain.

Lab Requirements:

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

Lab Setup: Initial

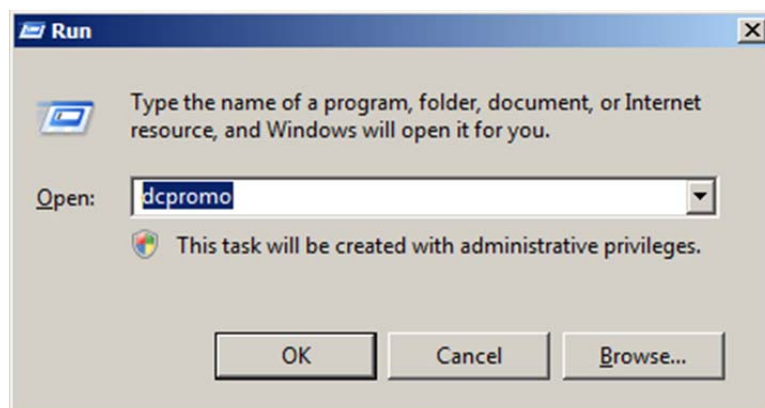


- **Exercise 1: Configuring IPv4 addresses.**

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

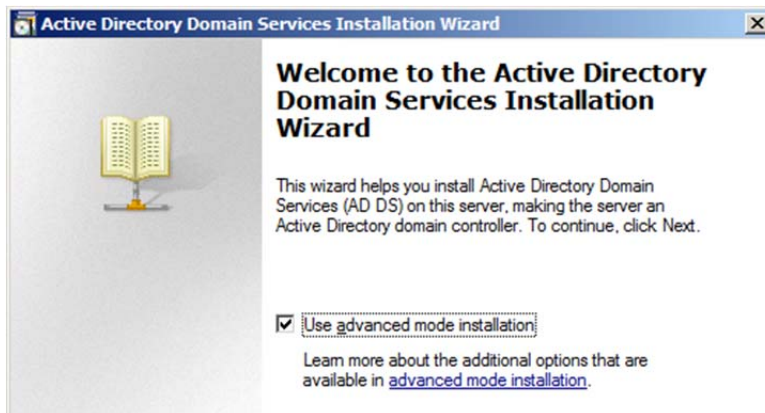
- **Exercise 2: Configuring the first domain controller in an Active Directory domain**

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

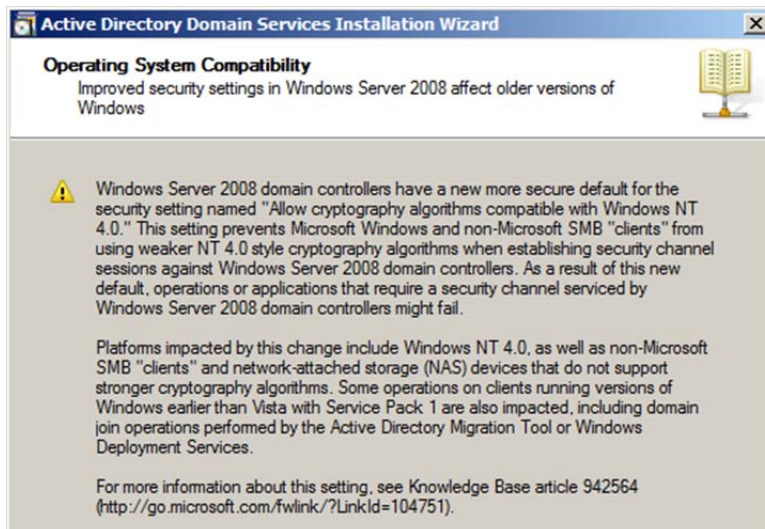


Active Directory Domain Services binaries are being installed. Please wait.

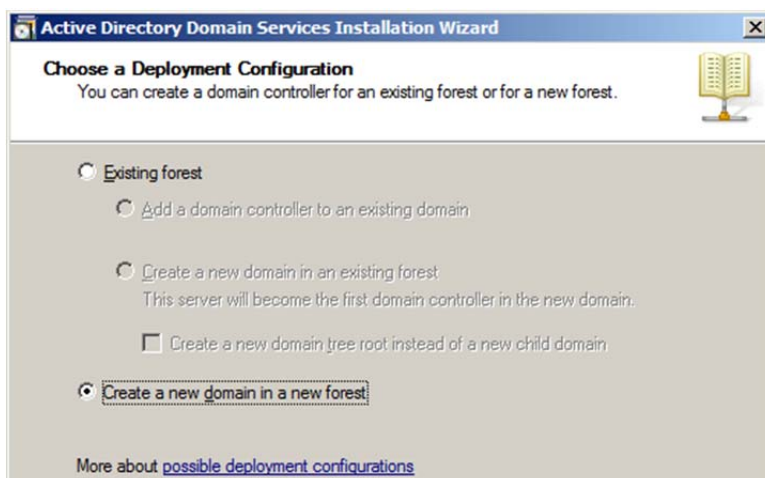
2. The **Active Directory Domain Services Installation Wizard** dialog box appears. Check the **Use advanced mode installation** option. Click **Next**.



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**.



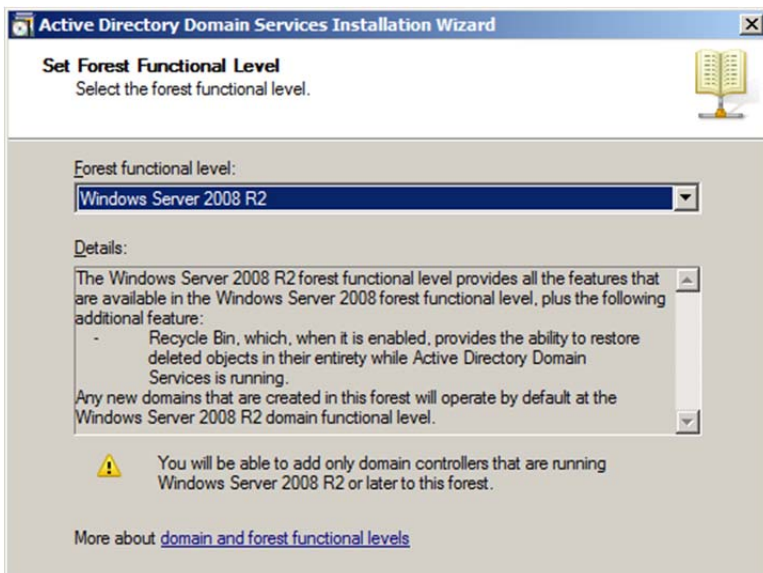
5. The **Name the Forest Root Domain** dialog box appears. Type **DOMAINxx.LOCAL**, xx is your computer number. Click **Next**.



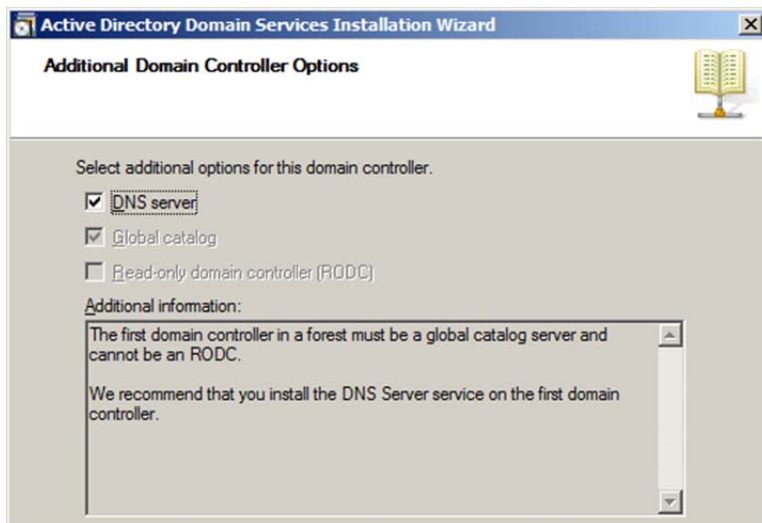
6. The **Domain NetBIOS Name** dialog box appears. Take the default setting and click **Next**.



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



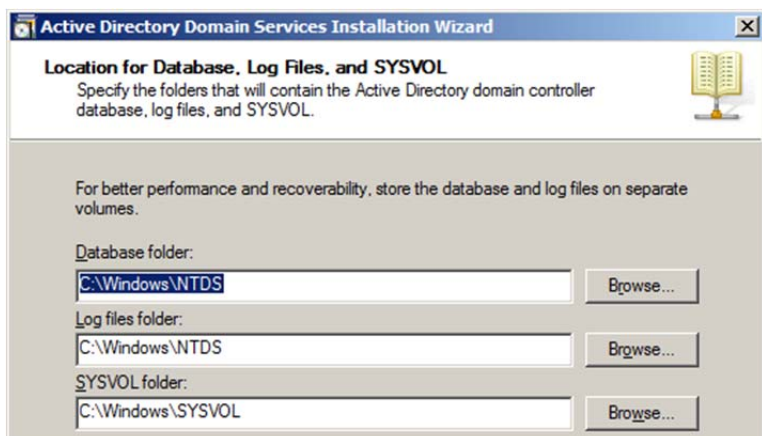
8. The **Additional Domain Controller Options** dialog box appears. Click **Next**.



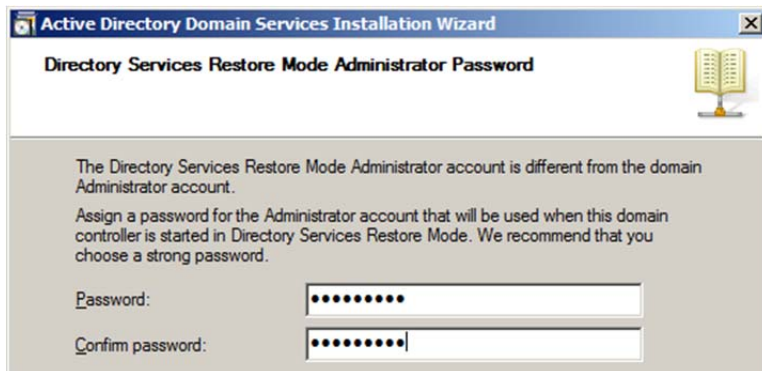
9. The DNS warning dialog box appears. Click **Yes**.



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**.



The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

Password: [Password field with 8 dots]

Confirm password: [Confirm password field with 8 dots]

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



Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "DOMAINxx.LOCAL". This is also the name of the new forest.

The NetBIOS name of the domain is "DOMAINXX".

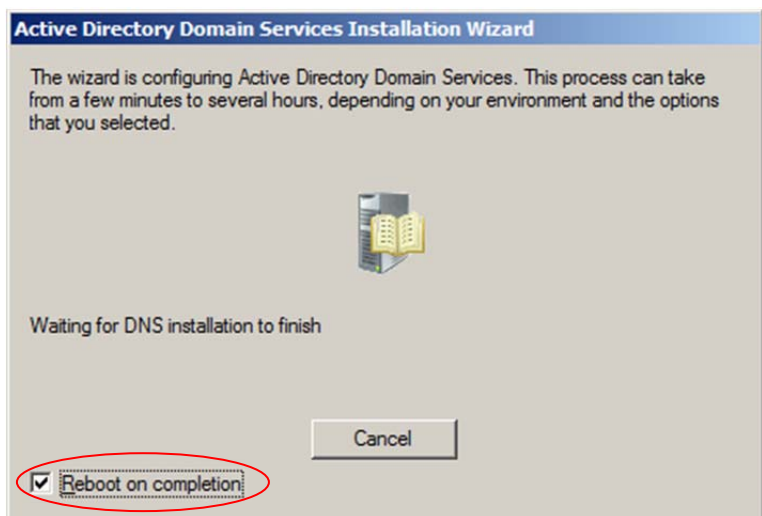
Forest Functional Level: Windows Server 2008 R2

Domain Functional Level: Windows Server 2008 R2

Site: Default-First-Site-Name

To change an option, click Back. To begin the operation, click Next.

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



The wizard is configuring Active Directory Domain Services. This process can take from a few minutes to several hours, depending on your environment and the options that you selected.

Waiting for DNS installation to finish

Cancel

☒ Reboot on completion

- **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**.

```

Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /all

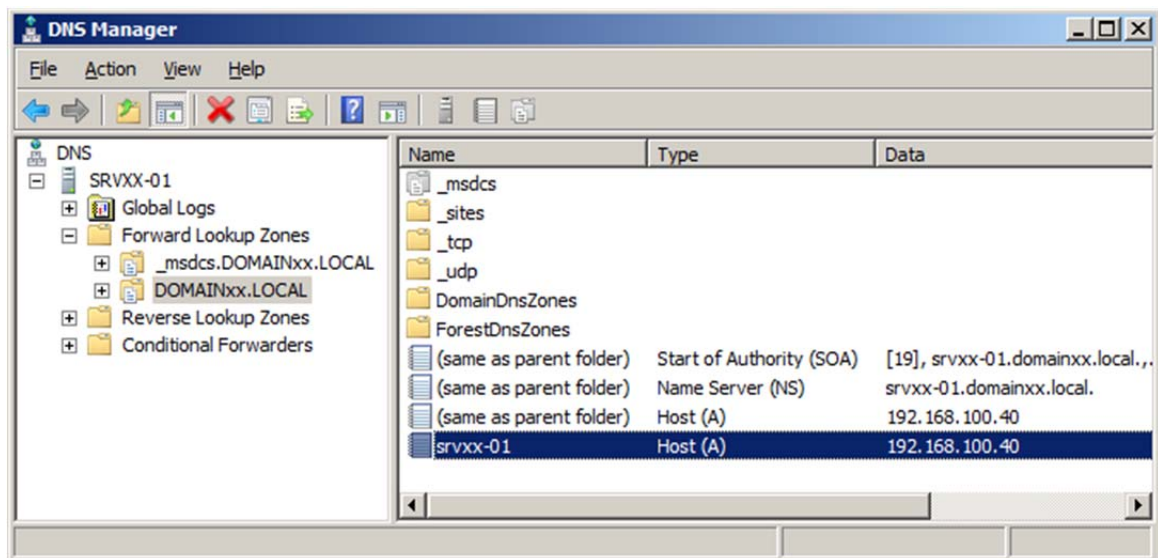
Windows IP Configuration

Host Name . . . . . : SRVxx-01
Primary Dns Suffix . . . . . : DOMAINxx.LOCAL
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : DOMAINxx.LOCAL

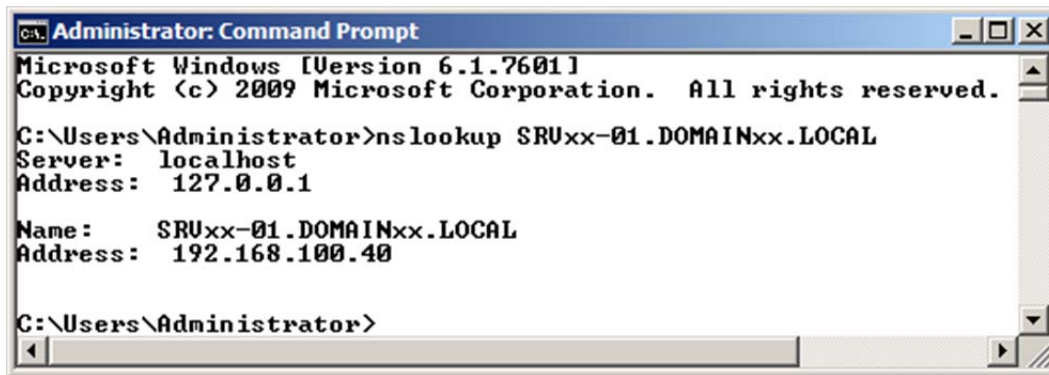
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-15-E3-78
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 192.168.100.40(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.254
DNS Servers . . . . . : 127.0.0.1
NetBIOS over Tcpip. . . . . : Enabled
  
```

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`.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

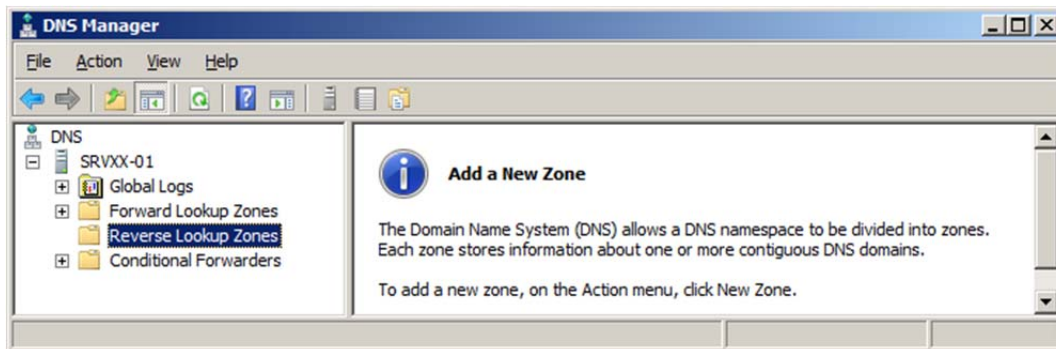
C:\Users\Administrator>nslookup SRVxx-01.DOMAINxx.LOCAL
Server: localhost
Address: 127.0.0.1

Name: SRVxx-01.DOMAINxx.LOCAL
Address: 192.168.100.40

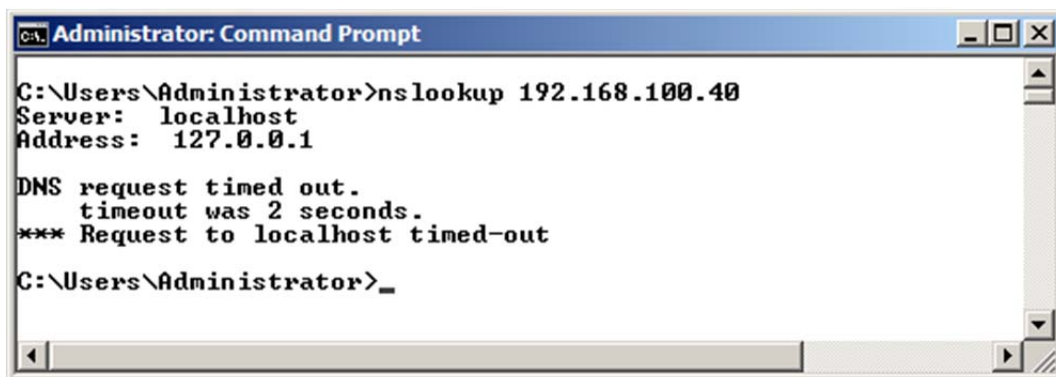
C:\Users\Administrator>
```

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`.



```
Administrator: Command Prompt

C:\Users\Administrator>nslookup 192.168.100.40
Server: localhost
Address: 127.0.0.1

DNS request timed out.
    timeout was 2 seconds.
*** Request to localhost timed-out

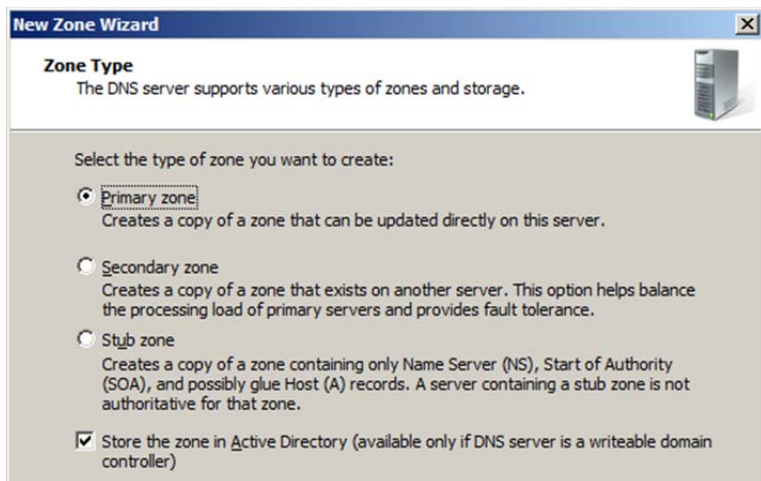
C:\Users\Administrator>
```

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.

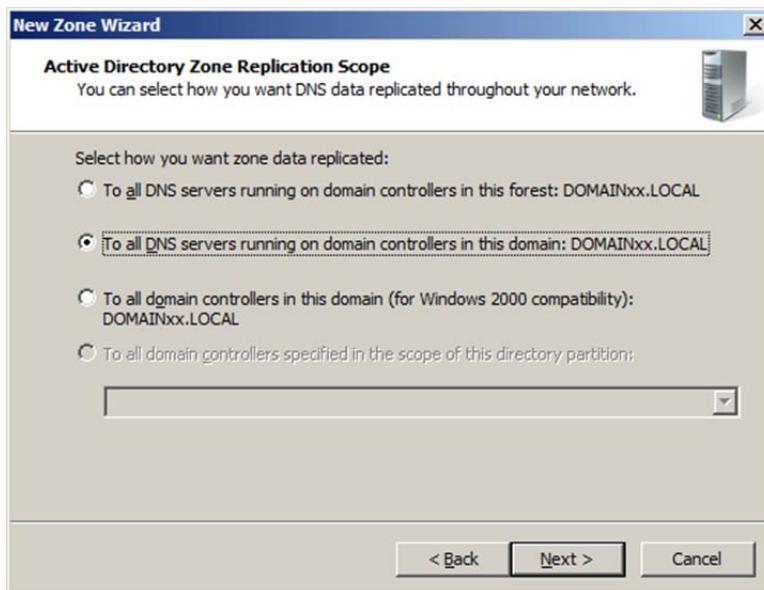
5. You will configure the Reverse Lookup Zone for your domain. Right-click **Reverse Lookup Zones**, and click **New Zone....** The **New Zone Wizard** dialog box appears. Click **Next**.



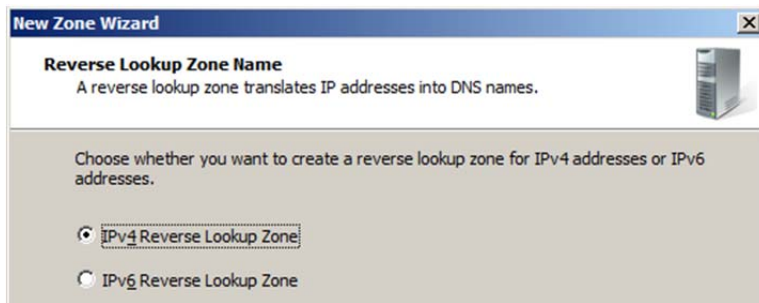
6. The **Zone Type** dialog box appears. Click **Next** without changing the option.



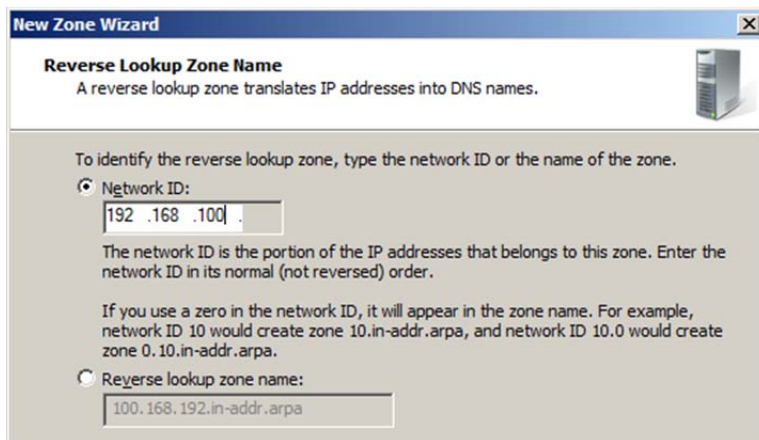
7. The **Active Directory Zone Replication Scope** dialog box appears. Click **Next** without changing the option.



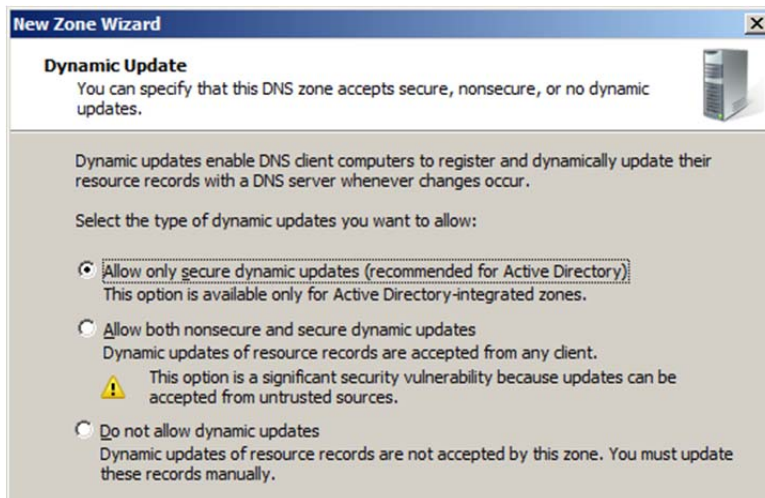
8. The **Reverse Lookup Zone Name** dialog box appears. Click **Next** without changing the option.



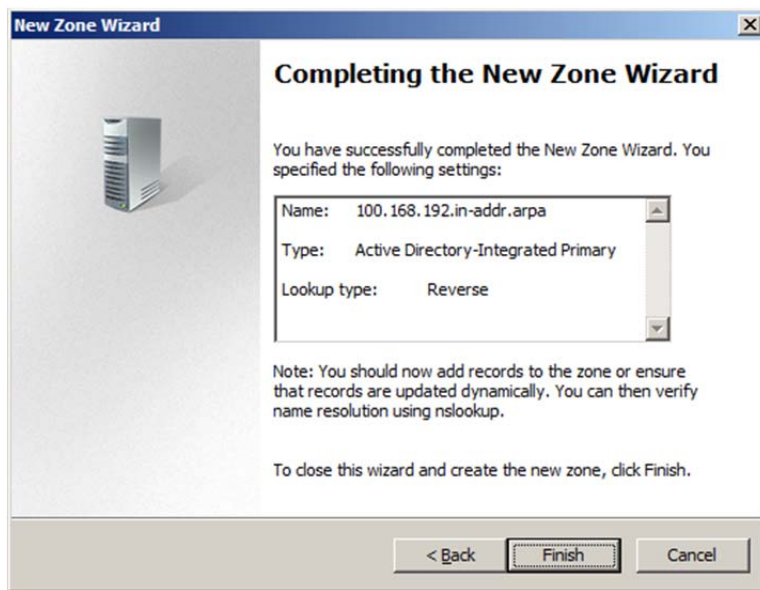
9. The **Reverse Lookup Zone Name** dialog box appears. Type **192.168.100** in the Network ID box. Click **Next**.



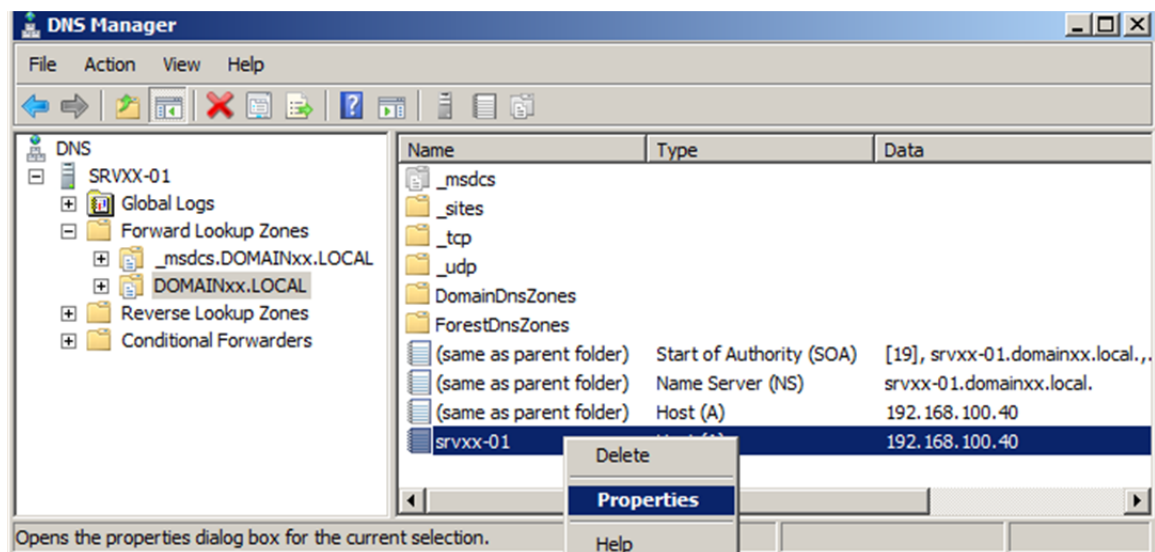
10. The **Dynamic Update** dialog box appears. Click **Next** without changing the option.



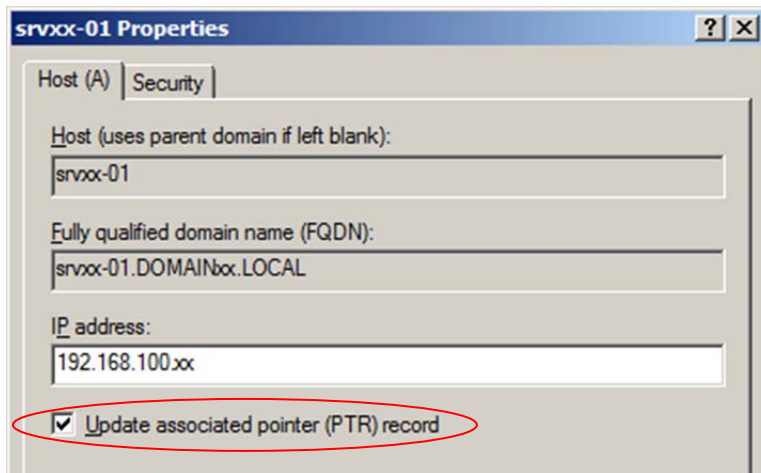
11. The Completing the New Zone Wizard dialog box appears. Click **Finish**.



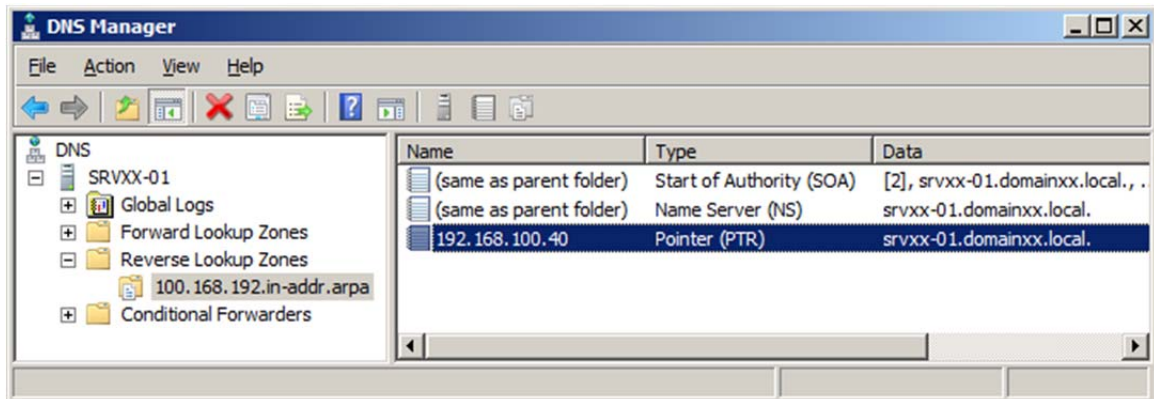
12. To update the **SRVxx-01** PTR record, right click **SRVxx-01** in the **Forward Lookup Zones > DOMAINxx.LOCAL**, and select **Properties**.



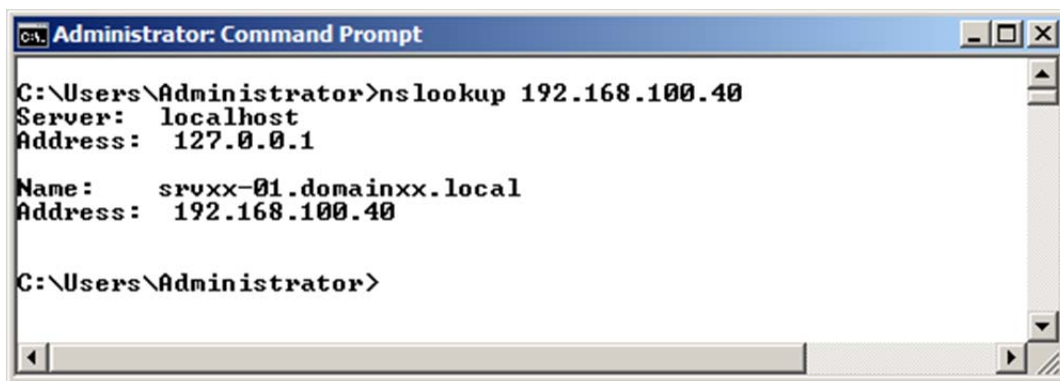
13. The **SRVxx-01 Properties** dialog box appears. Check the **Update associated pointer (PTR)** record option. Click **OK**.



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



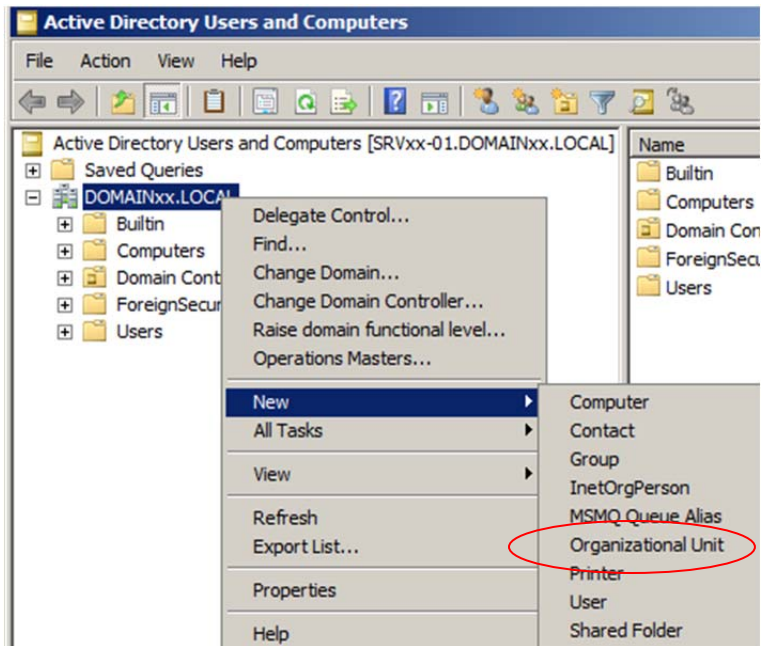
In the command prompt, type **nslookup 192.168.100.xx**.



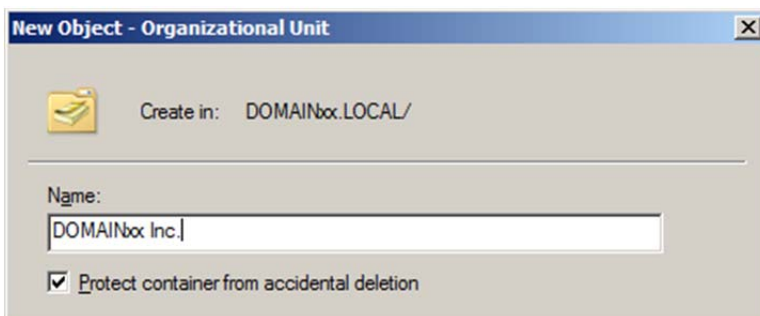
Now your local DNS server can provide the hostname of the IP address.

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

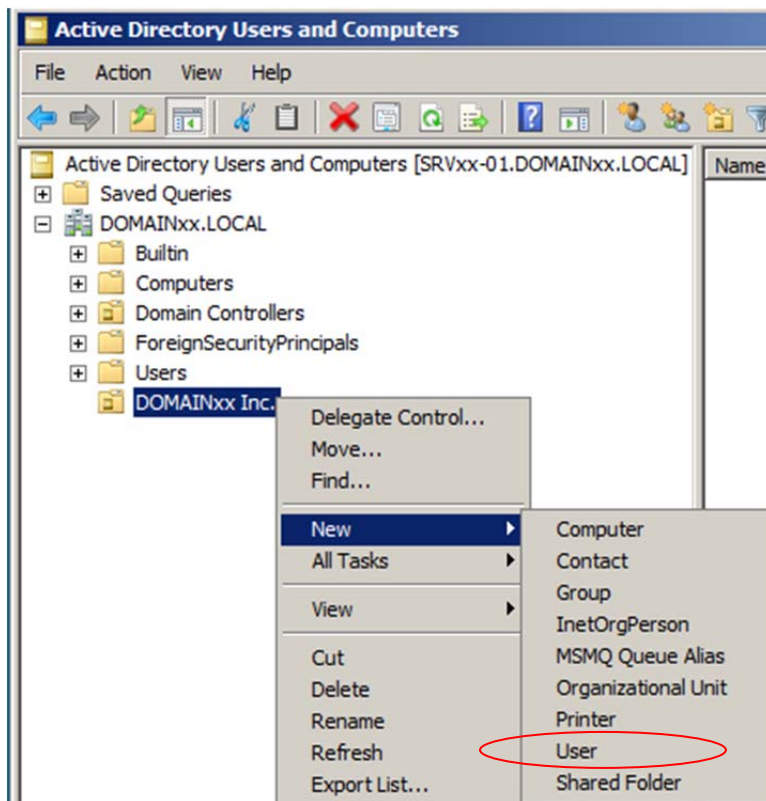
1. Open the **Active Directory Users and Computers** console (Start > All Programs > Administrative Tools > Active Directory Users and Computers). Right-click **DOMAINxx.LOCAL** and click **New > Organizational Unit**.



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



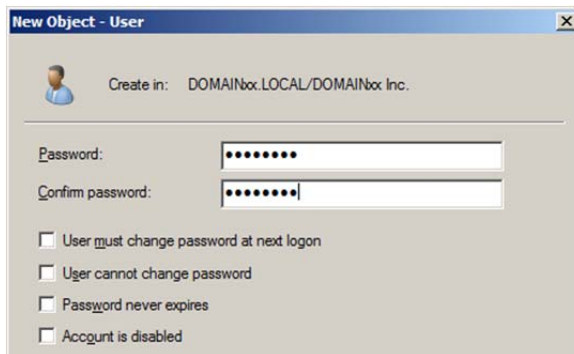
3. The **DOMAINxx Inc.** OU is created. Right-click **DOMAINxx Inc.** OU and click **New > User**.



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

A screenshot of the 'New Object - User' dialog box. The 'Create in:' field shows 'DOMAINxx.LOCAL/DOMAINxx Inc.'. Below this, there are several text input fields: 'First name:' with 'John', 'Initials:' with an empty field, 'Last name:' with 'Doe', and 'Full name:' with 'John Doe'. There are also fields for 'User login name:' with 'JDoe' and a dropdown menu showing '@DOMAINxx.LOCAL'. At the bottom, there are fields for 'User login name (pre-Windows 2000):' with 'DOMAINXX\' and 'JDoe'. The dialog box has a blue title bar and a close button in the top right corner.

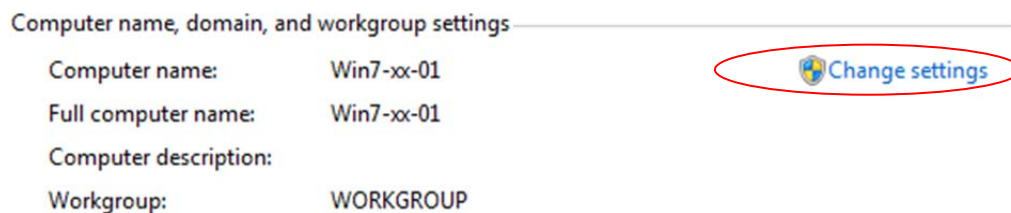
- The Password dialog box appears. Type **P@ssword** in the text boxes. Uncheck the first option. Click **Next**.



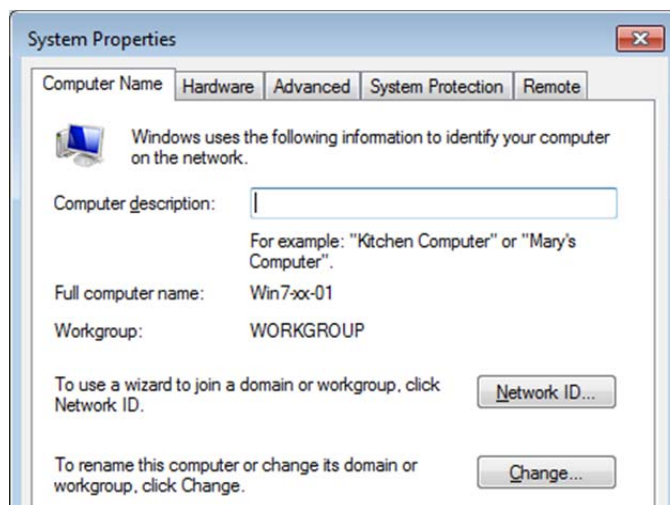
- The Summary dialog box appears. Click **Finish**. The **John Doe** user object appears in the **DOMAINxx Inc.** OU.

- Exercise 5: Joining a Active Directory domain**

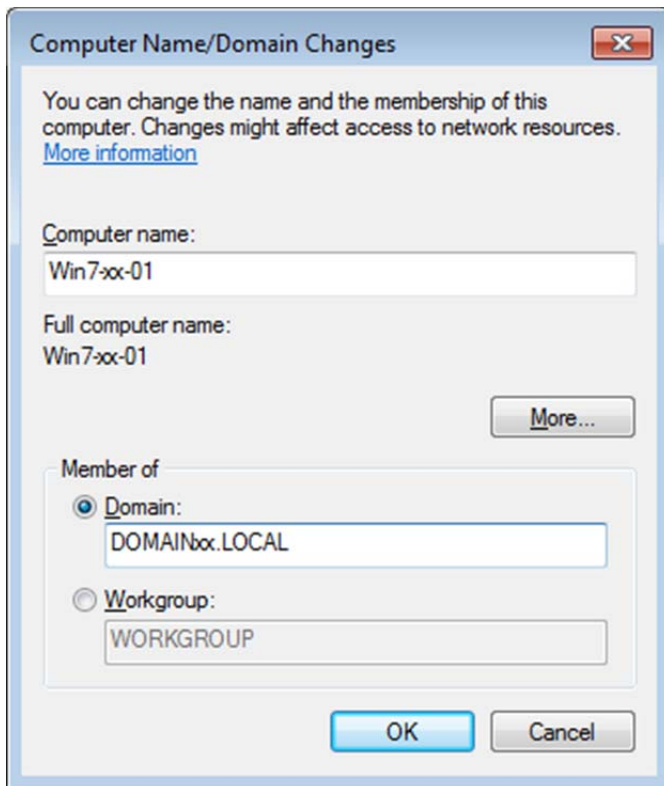
- Start the virtual machine **Win7-xx-01**.
- Open the command prompt and execute **PING 192.168.100.xx**. If you don't get any replies, check the TCP/IP settings on both machines.
- Open the **Control Panel**. Double-click **System** icon. Click **ChangeSettings** link under Computer name.



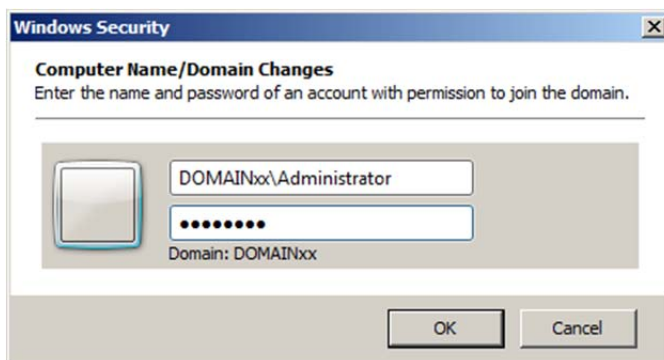
The **System Properties** dialog box appears. Click **Change....**



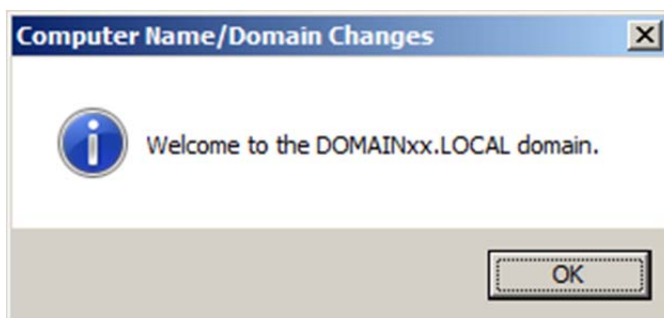
Select the **Domain:** option. Type **DOMAINxx.LOCAL** (xx is your monitor number). Click **OK**.



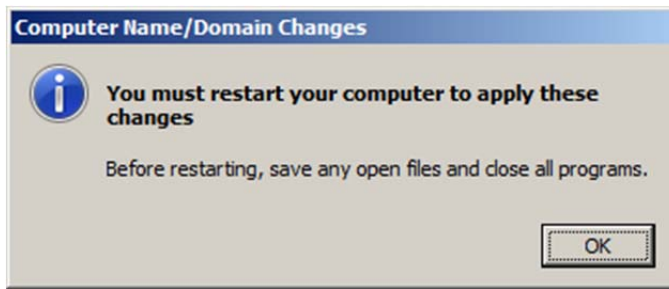
The **Windows Security** dialog box appears. Type **DOMAINxx\Administrator** in the User name box. Type **P@ssword** in the password box. If you use a different password, type your password for the account.



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

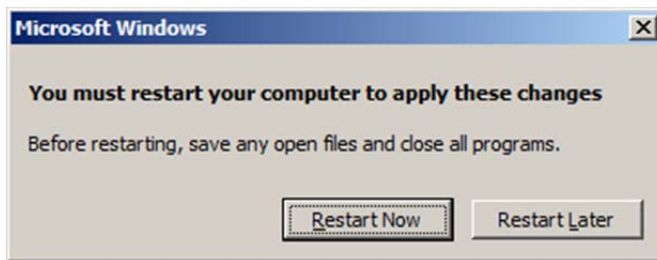


The Information dialog box appears. Click **OK**.



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

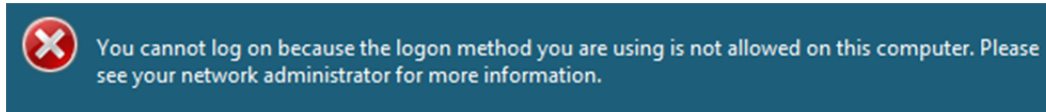
The Microsoft Windows dialog box appears. Click **Restart Now**. The system reboots. Now **Win7-xx-01** is a member server of **DOMAINxx.LOCAL**.



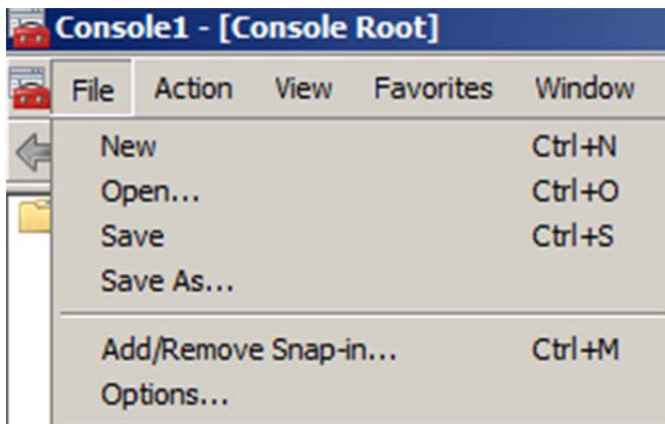
4. After sending **CTRL + ALT + DELETE** signal, The Local administrator account name (**Win7-xx-01\Admin** or the account you created) is displayed. You will need to logon as Domain administrator. Click **Switch User** and click **Other User**. Type **DOMAINxx\Administrator** in the User name box. Type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

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

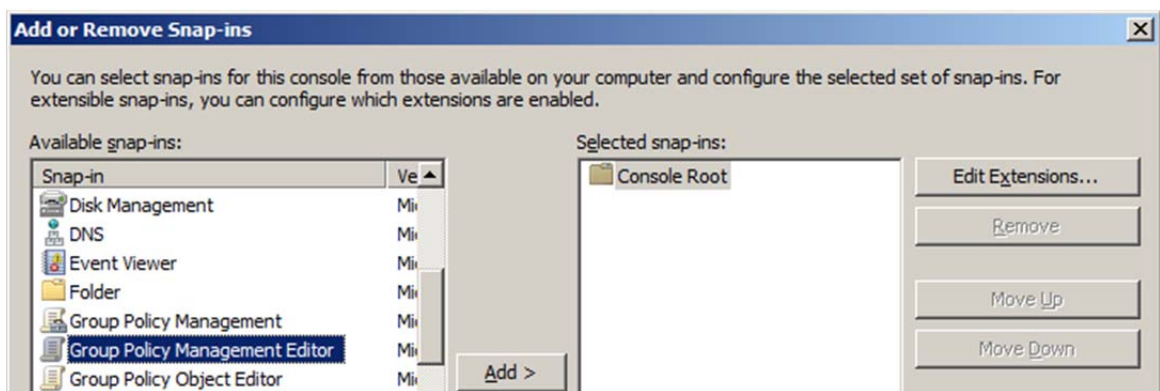
1. On **SRVxx-01**, log off and log on as **DOMAINxx\JDoe** user account. You should get the following message; this is because non-admin users can't log on to the domain controllers; John Doe is not an administrator. In a lab environment, since we are dealing with DCs only, we will allow non-admin users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



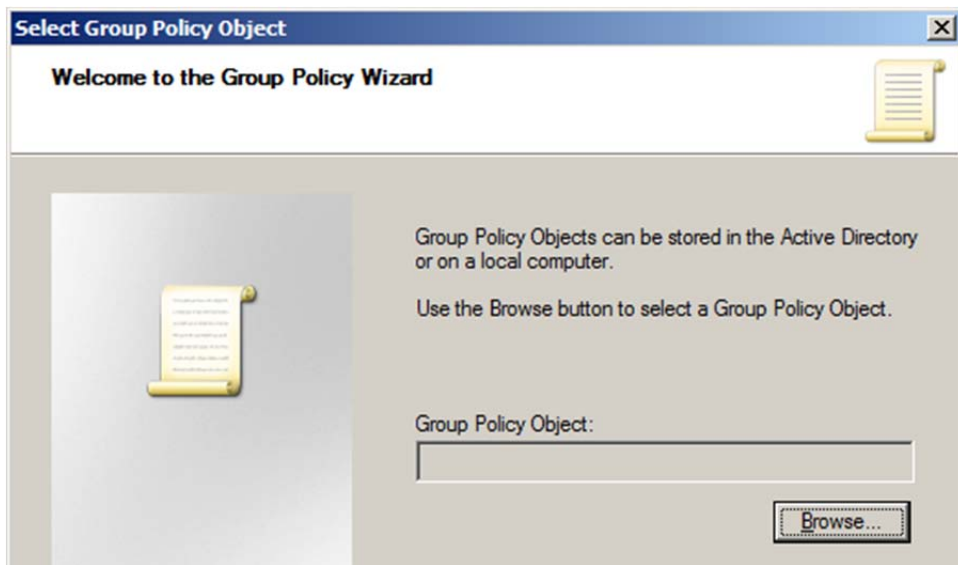
2. On **SRVxx-01**, Open **Start > Run**. Type **MMC** in the text box. The **Microsoft Management Console** window appears. Click **File > Add/Remove Snap-in...**



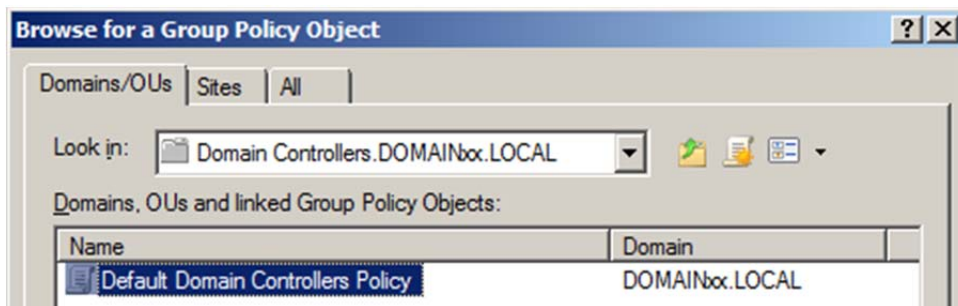
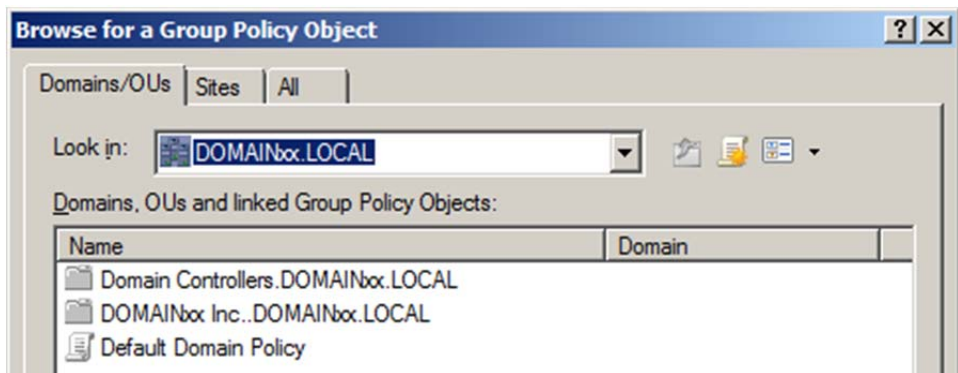
The **Add or Remove Snap-ins** dialog box appears. Select **Group Policy Management Editor** in the **Available snap-ins:** box, and click **Add >**.



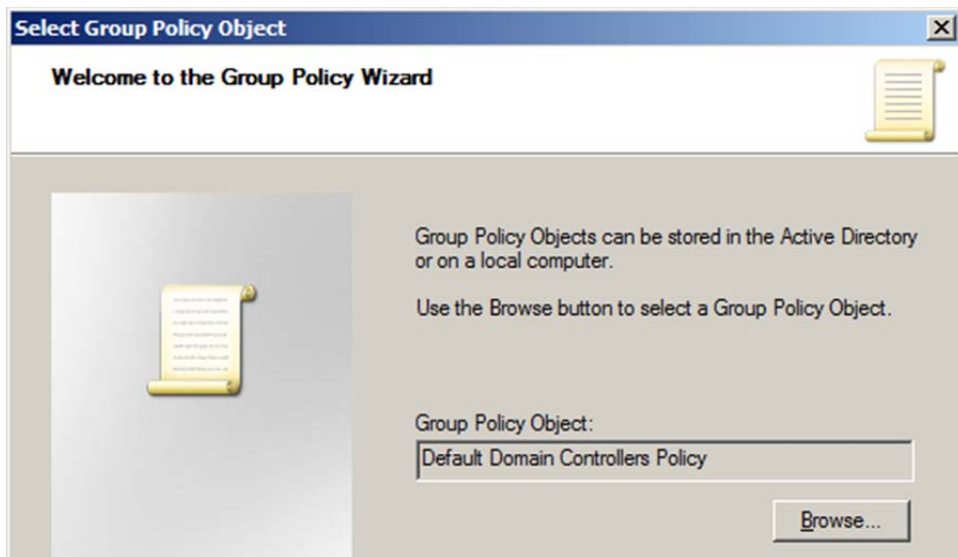
The **Select Group Policy Object** dialog box appears. Click **Browse...**



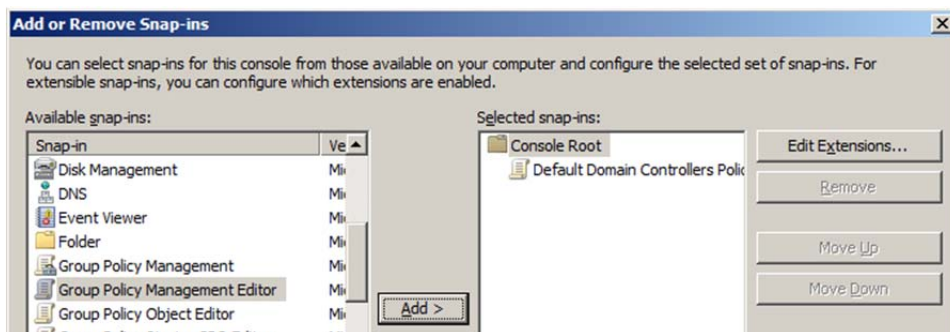
The Browse for a Group Policy Object dialog box appears. Double-click **Domain Controllers.DOMAINxx.LOCAL**, click **Default Domain Controllers Policy** and click **OK**.



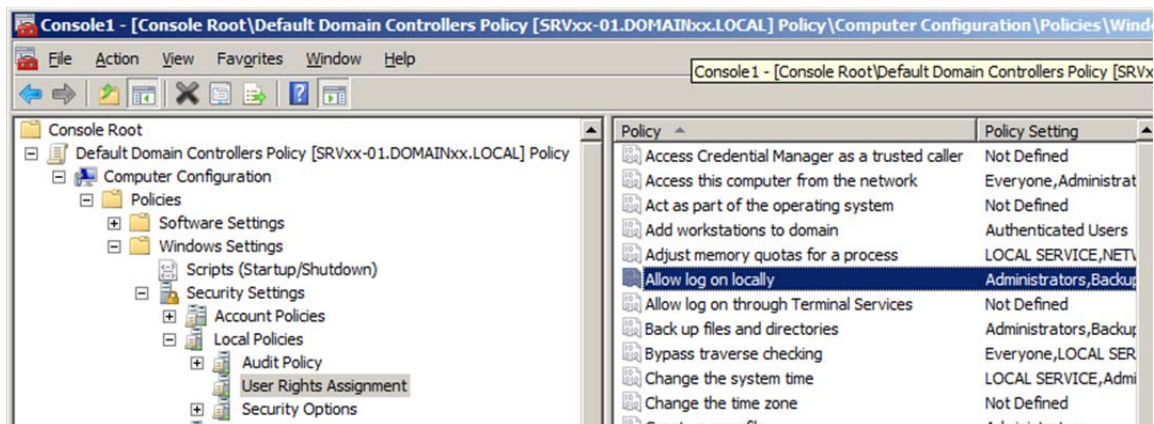
Click **OK**.



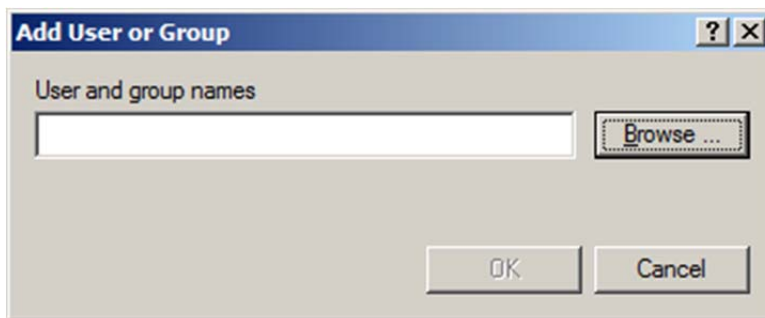
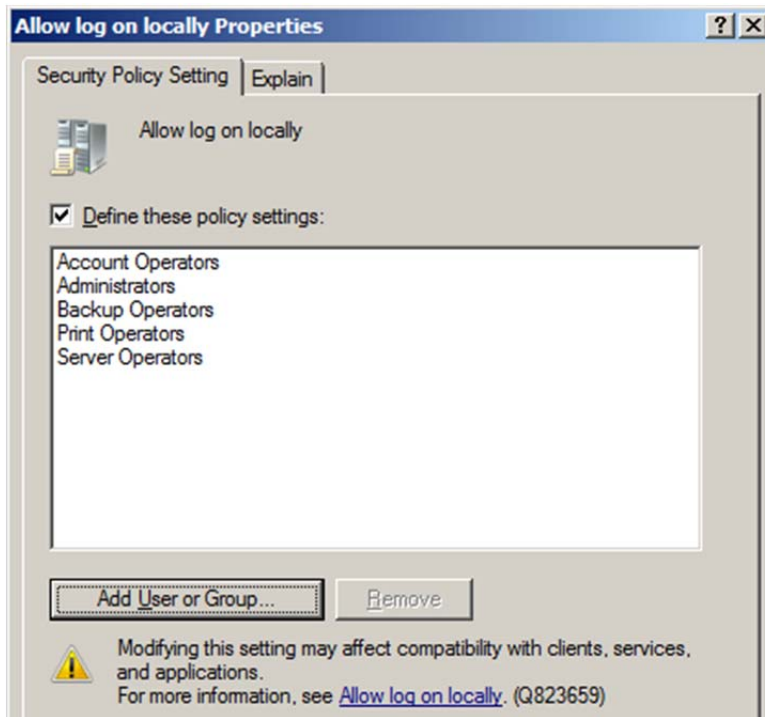
Click **OK**.



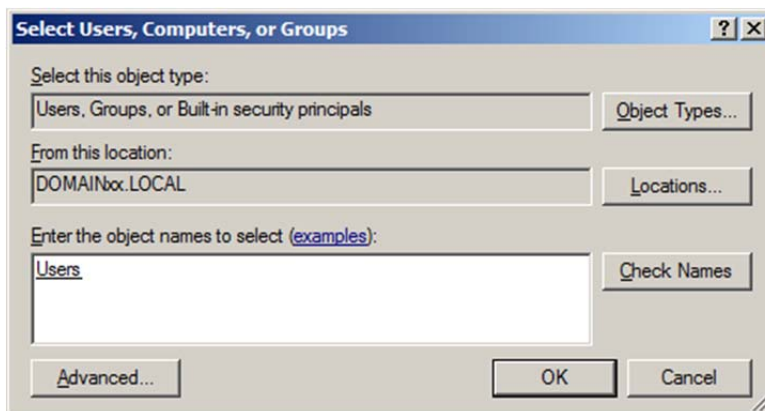
3. In the MMC **Console 1** window, navigate to the **User Rights Assignments** as shown below figure. Double-click **Allow log on locally**.

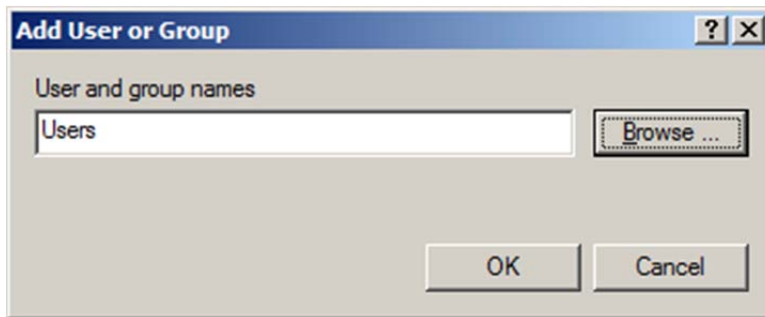


4. The **Allow log on locally Properties** dialog box appears. Click **Add Users or Group...**. The **Add User or Group** dialog box appears. Click **Browse...**.

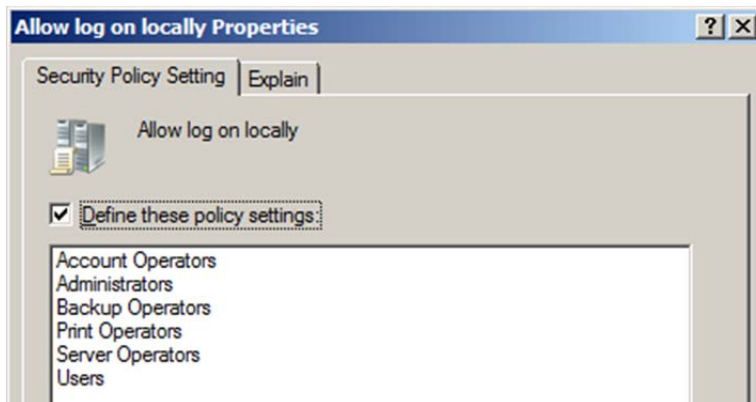


The **Select Users, Computers, or Groups** dialog box appears. Type **Users** in the text box and click **Check Names**. **Users** should be underlined. Click **OK**. In the **Add User or Group** dialog box, click **OK**.





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**.

```

Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.DOMAINXX>gpupdate
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.

C:\Users\Administrator.DOMAINXX>

```

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.