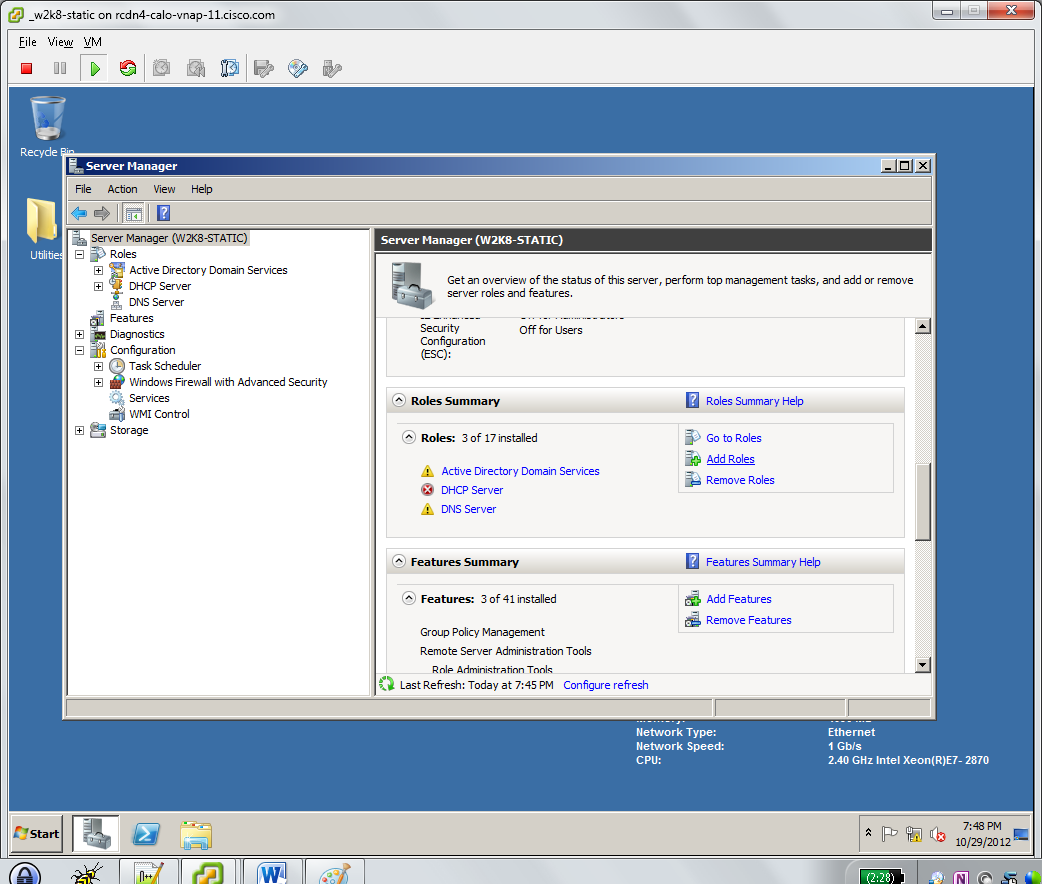
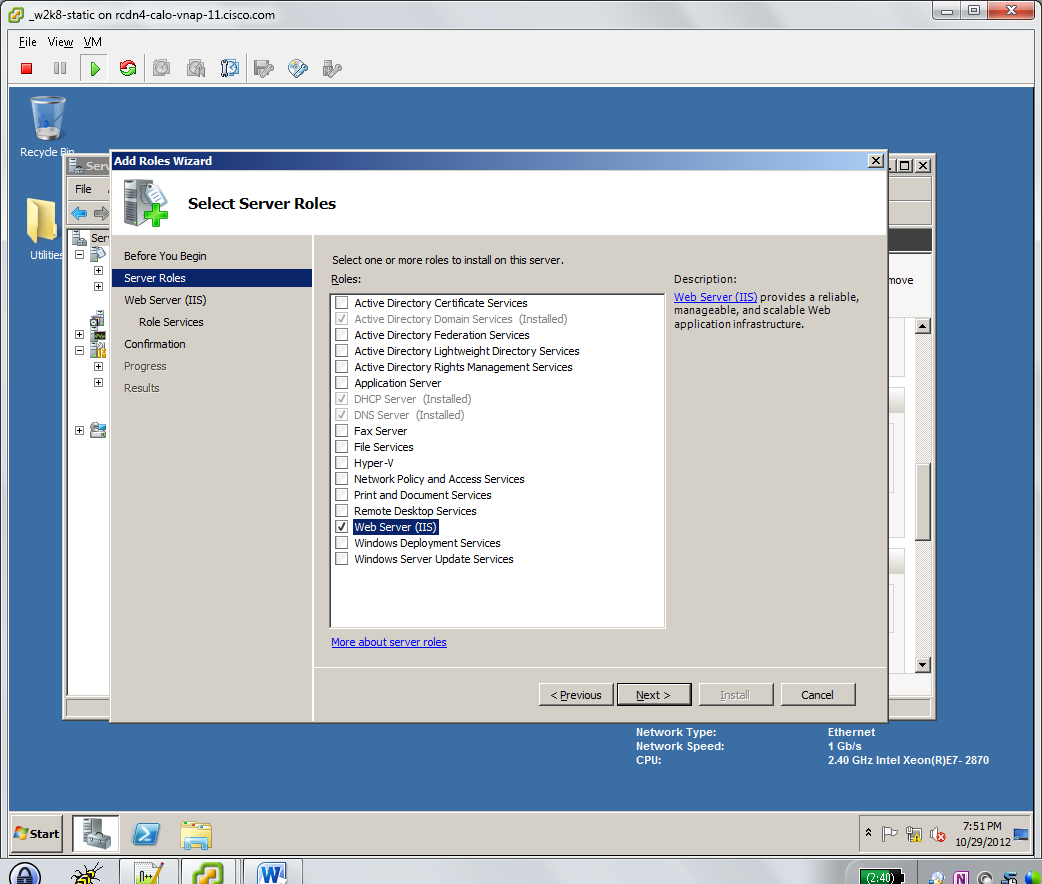
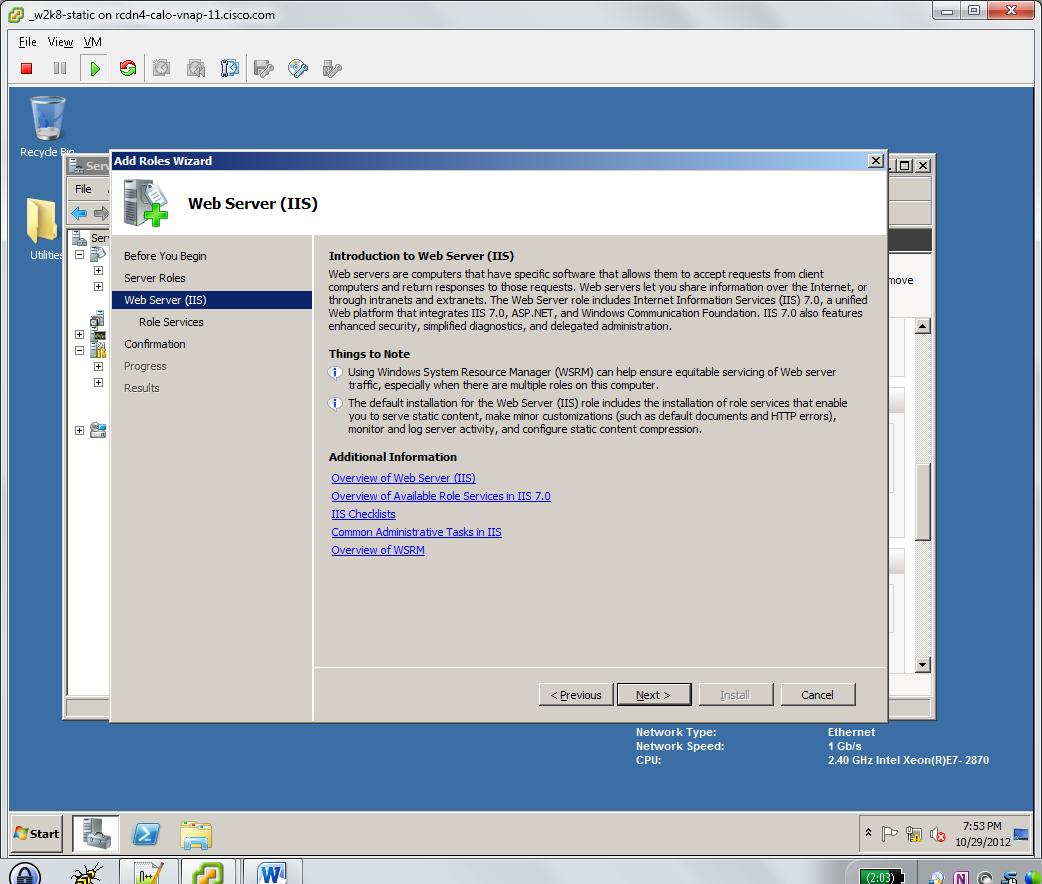
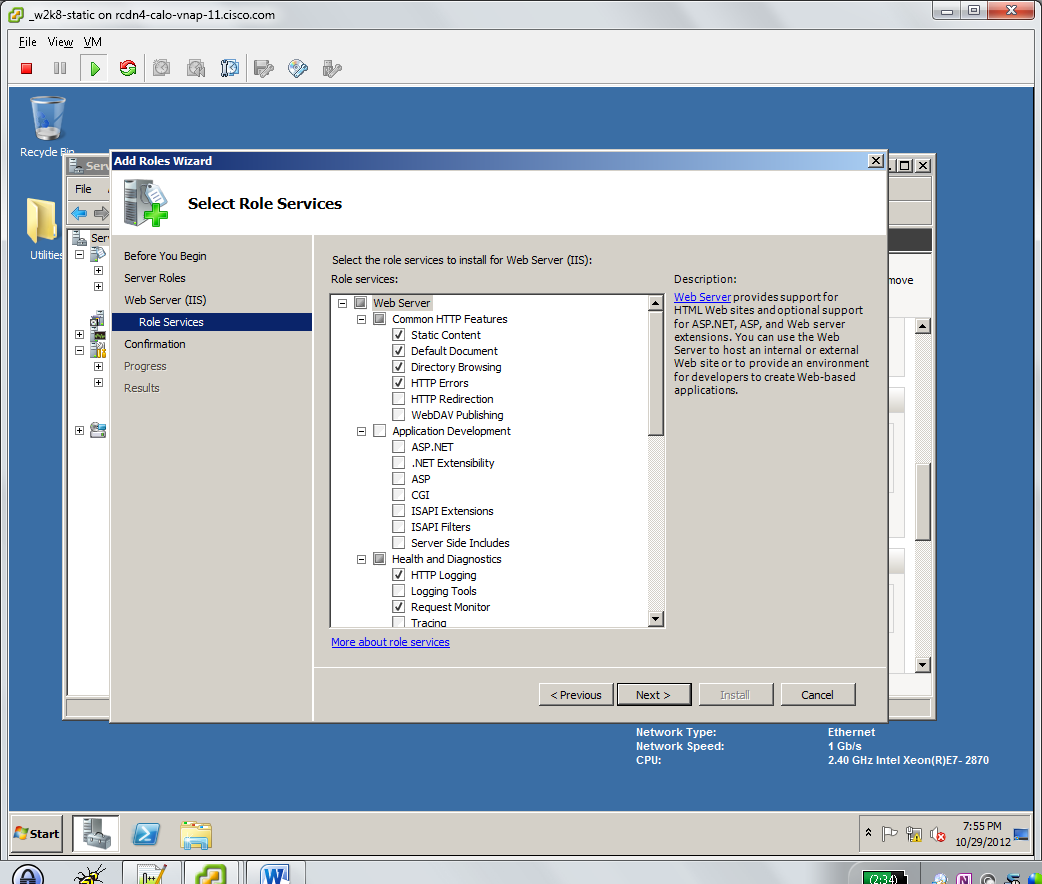
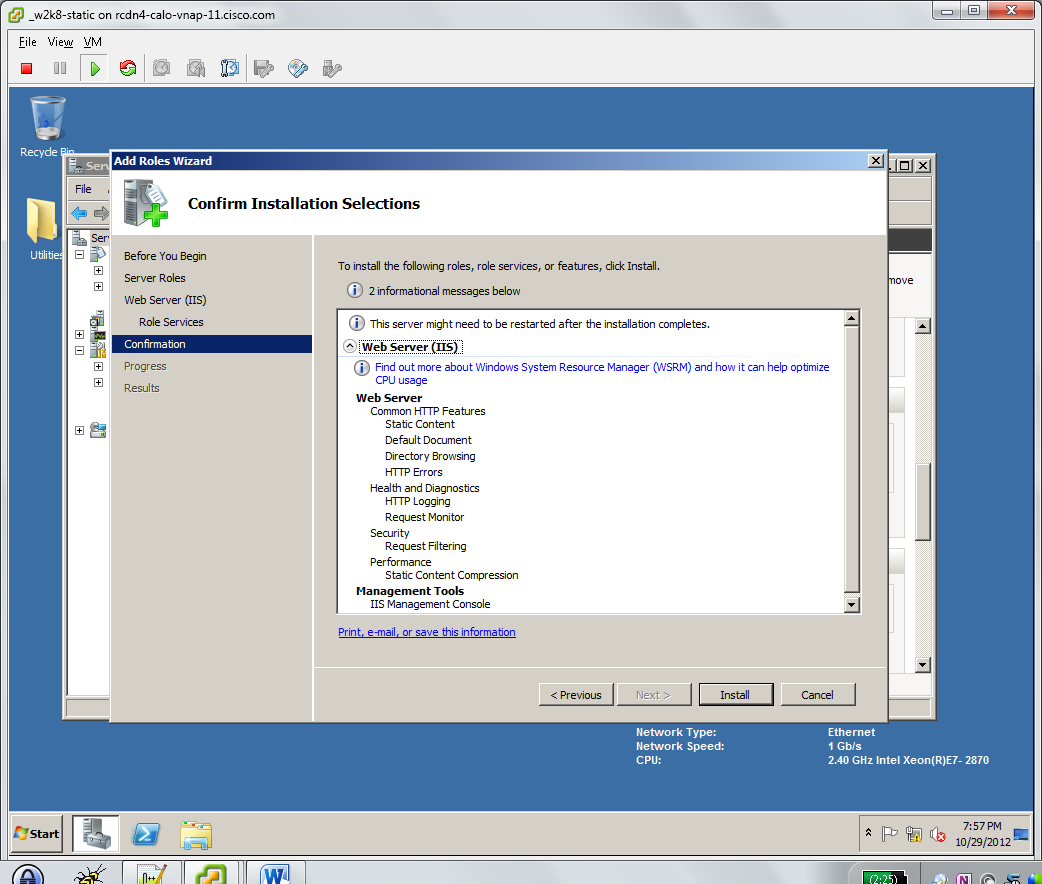
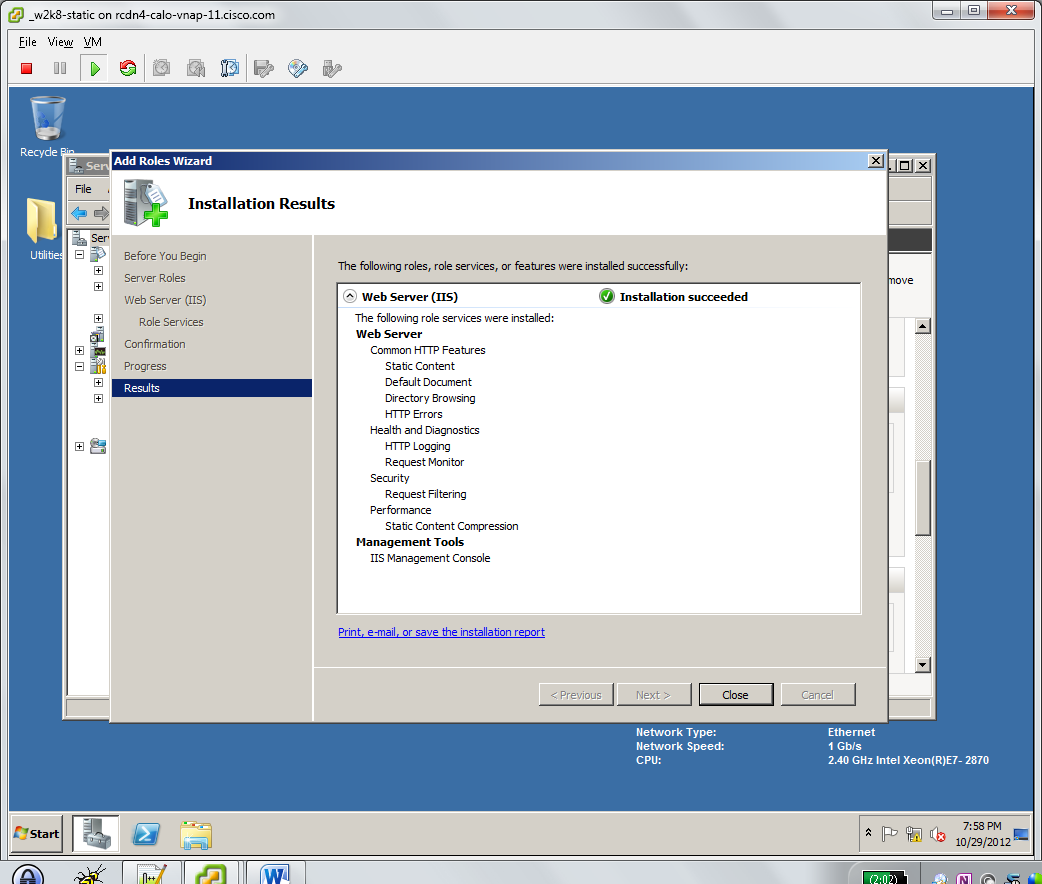
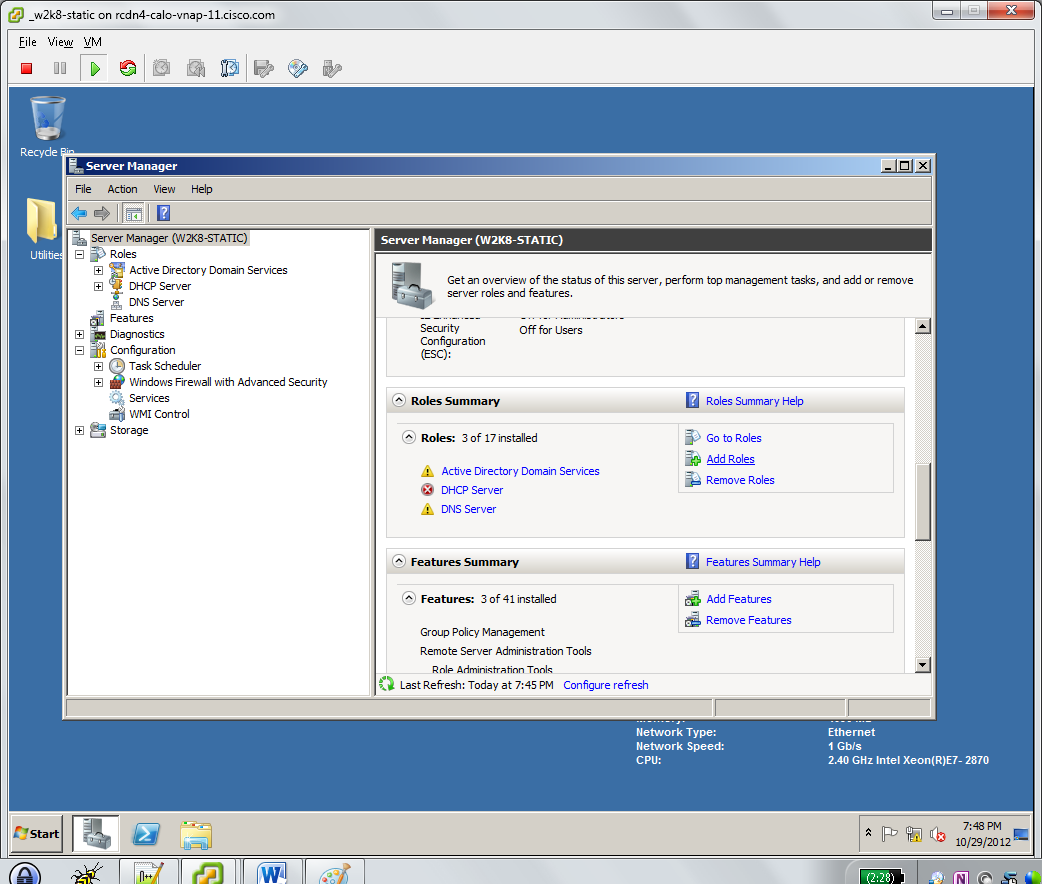
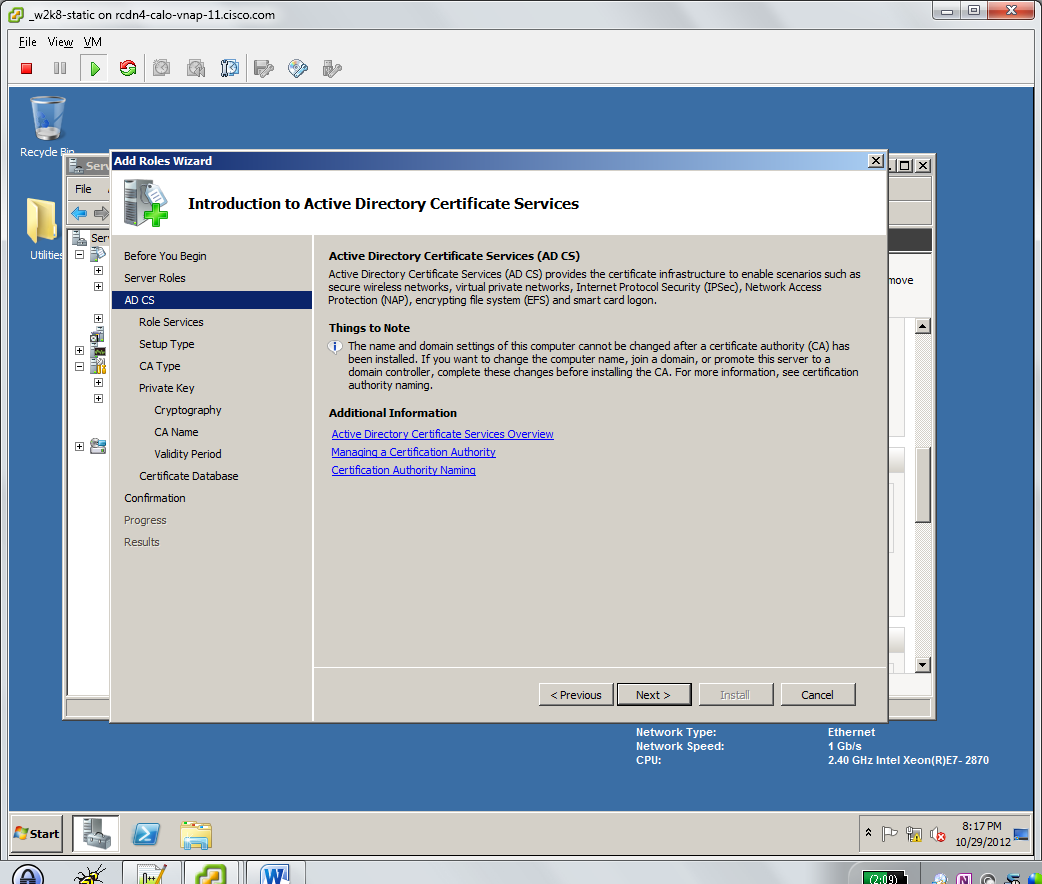
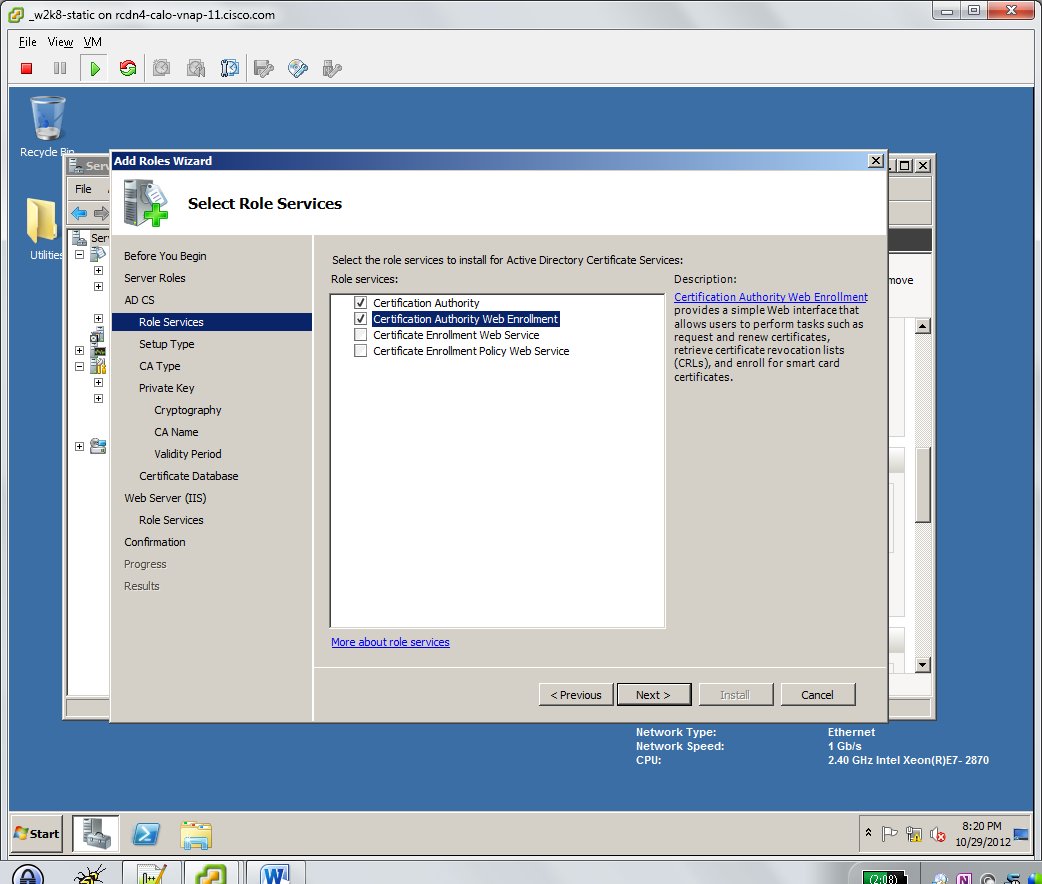
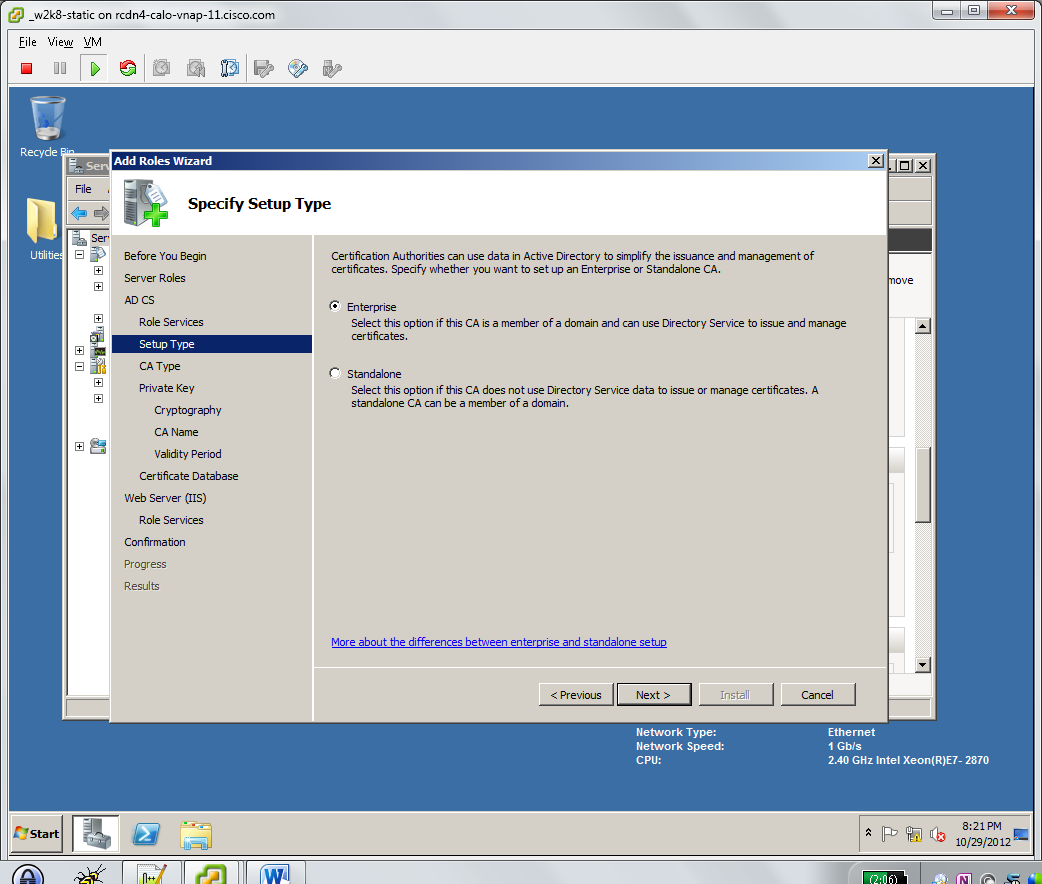
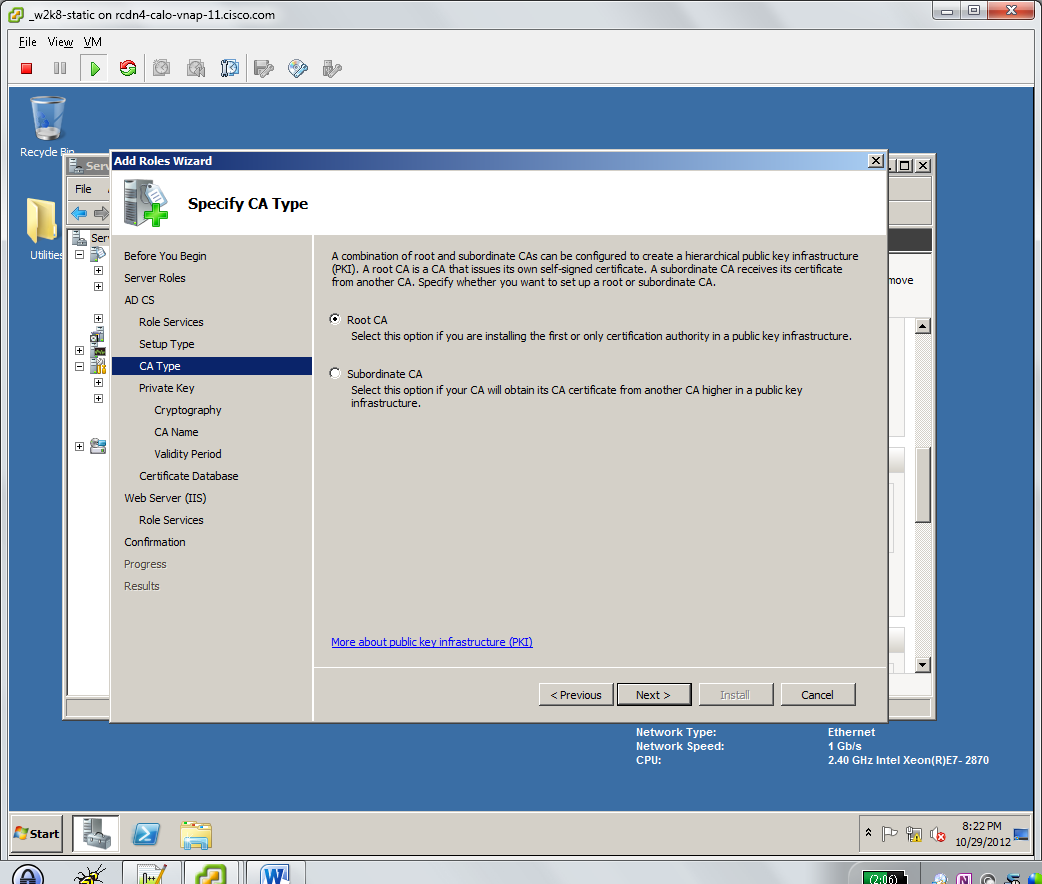
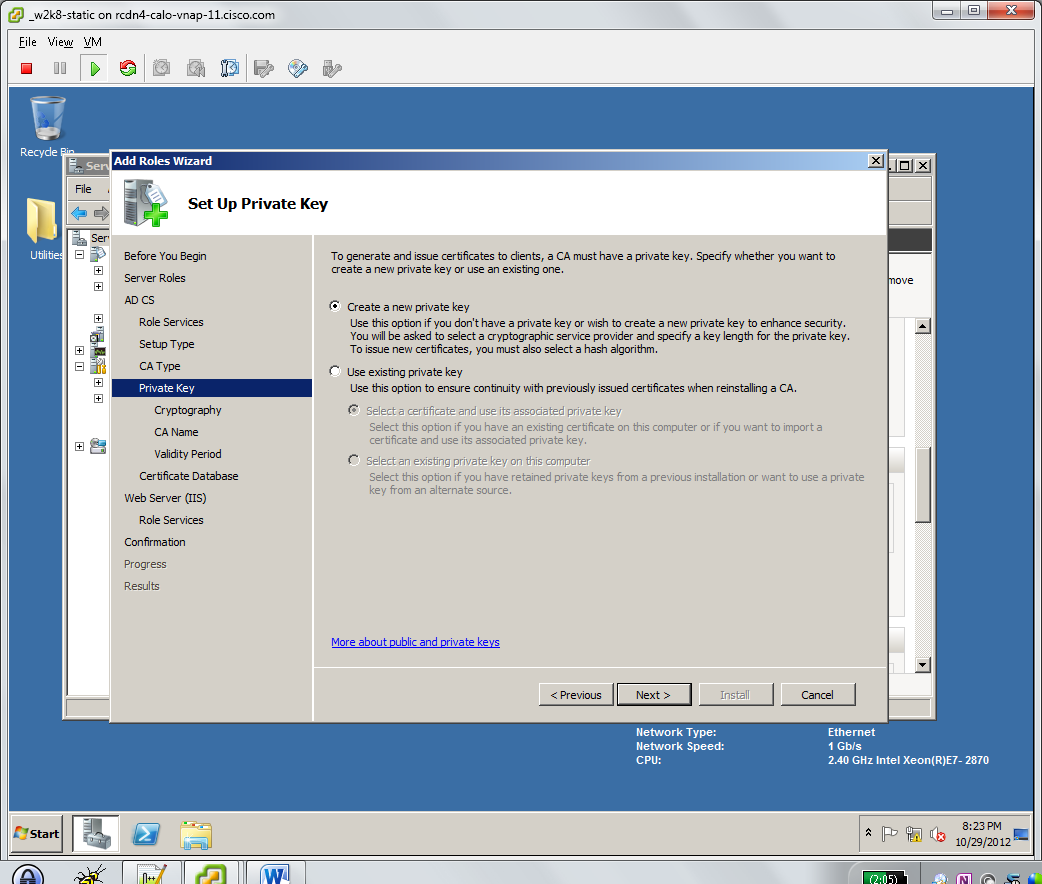
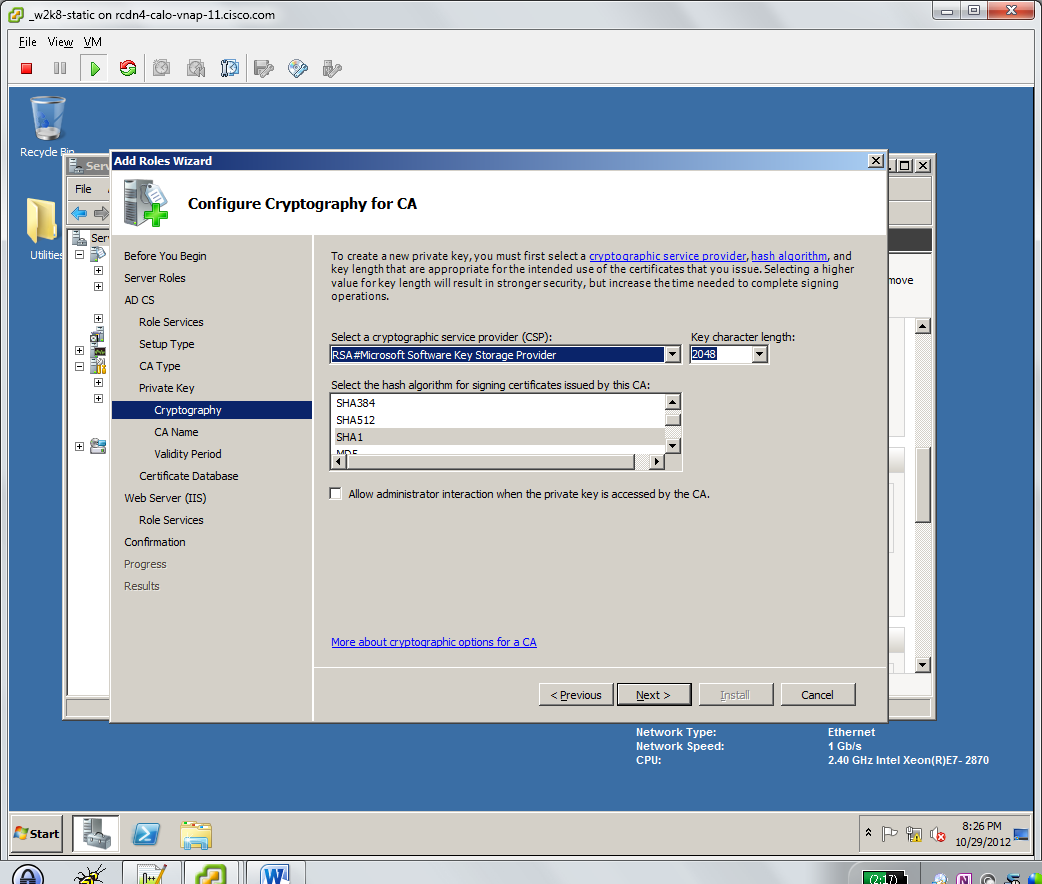
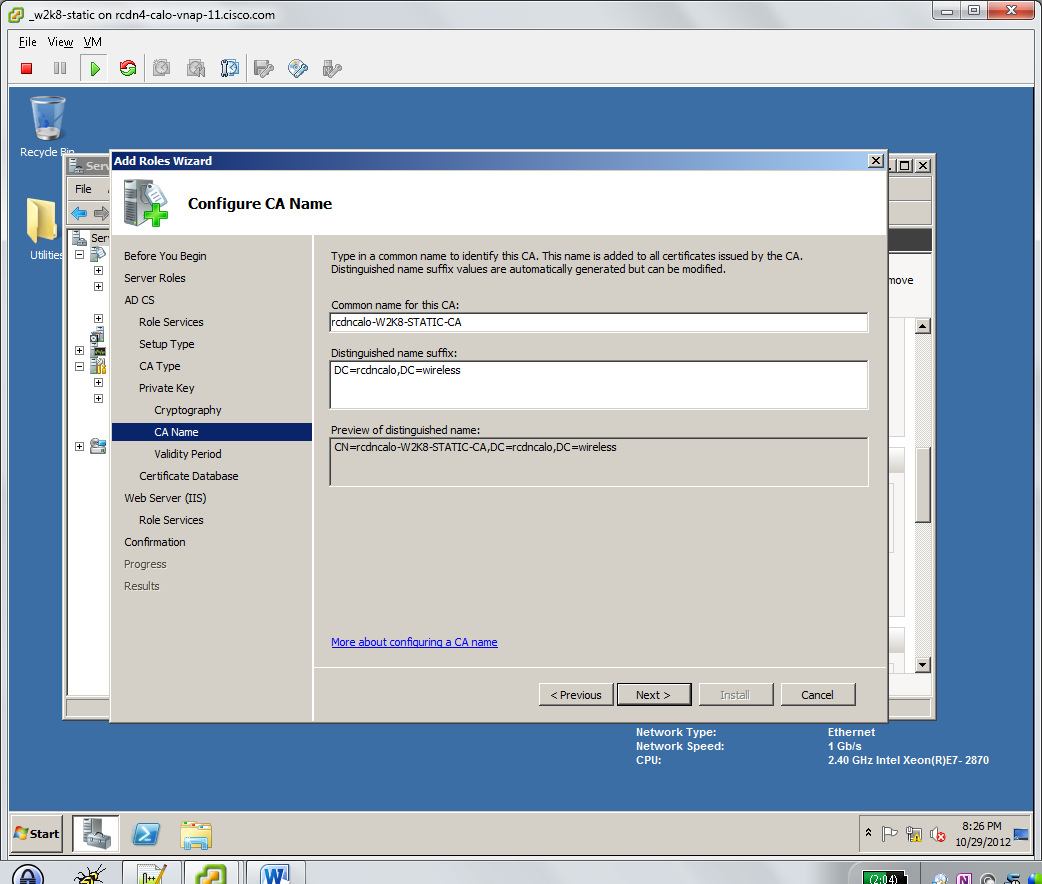
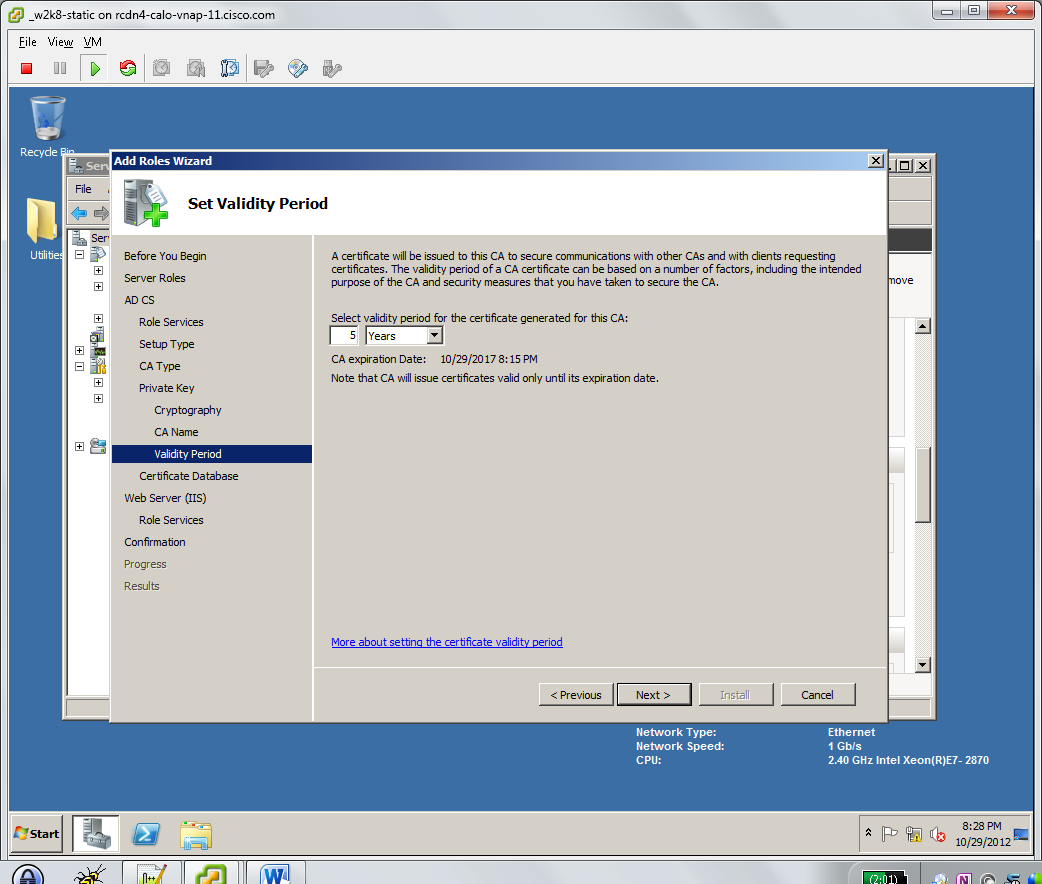
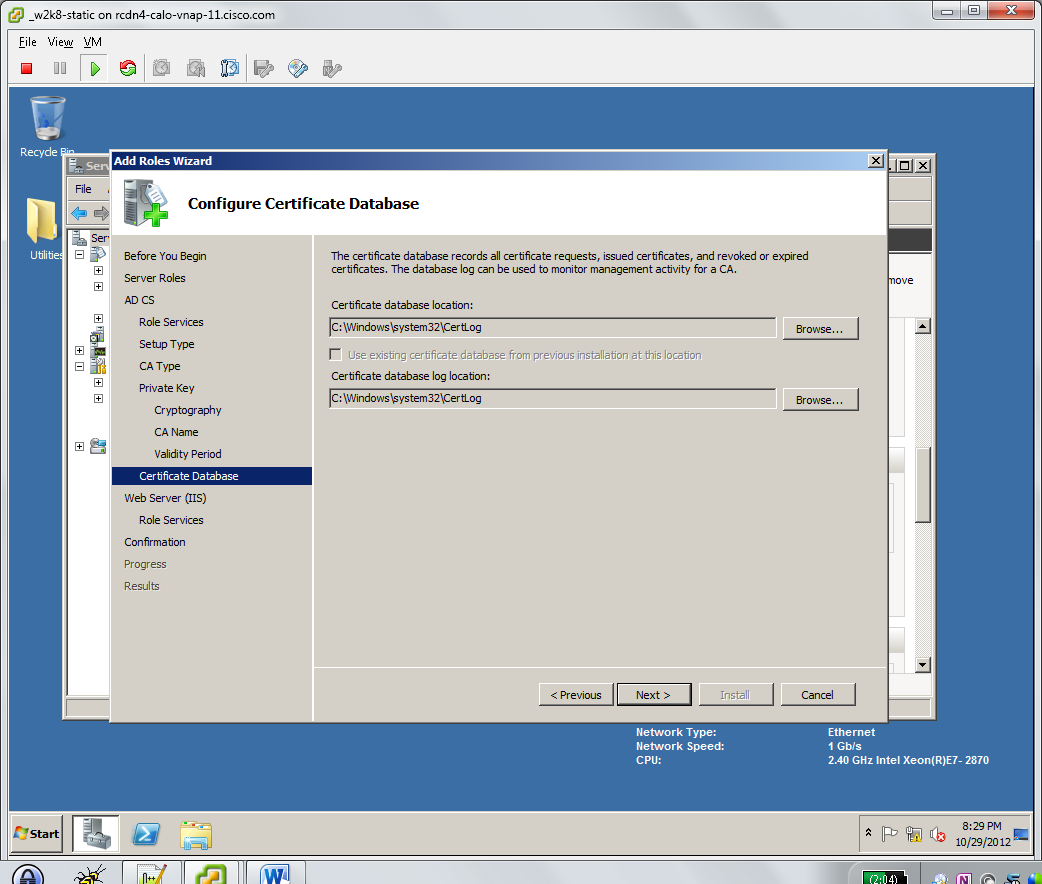
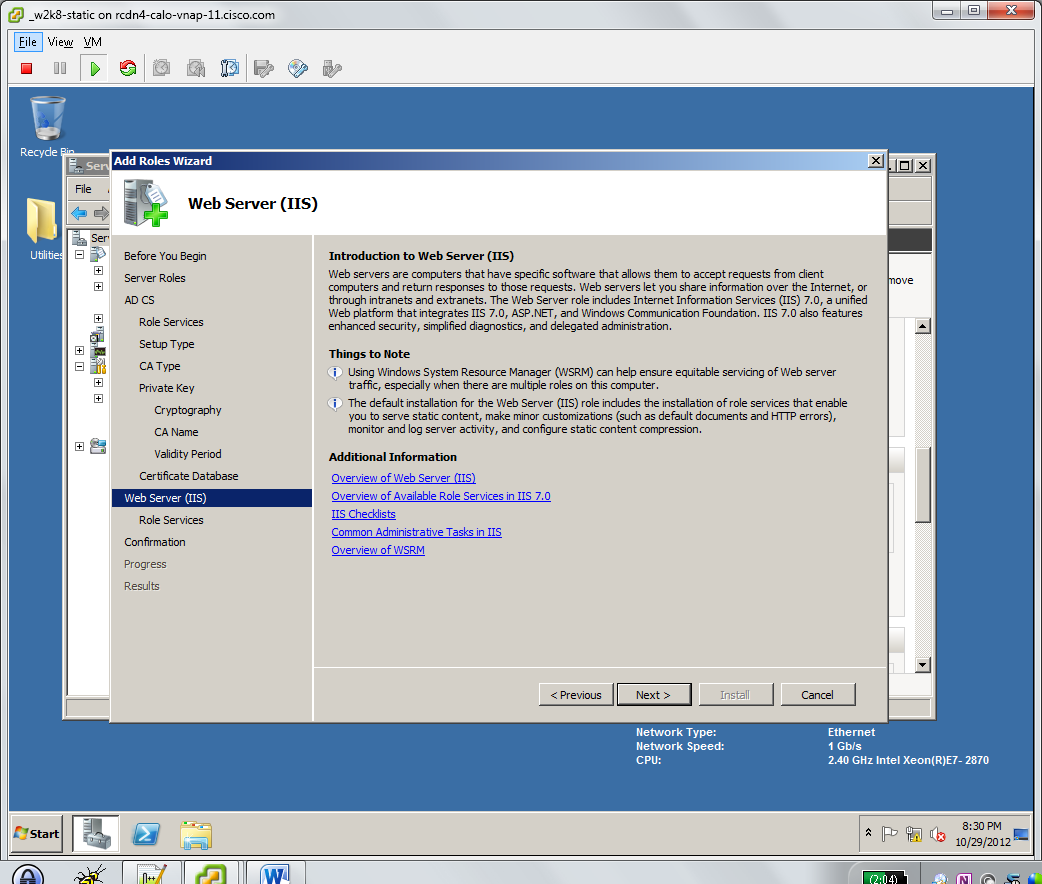
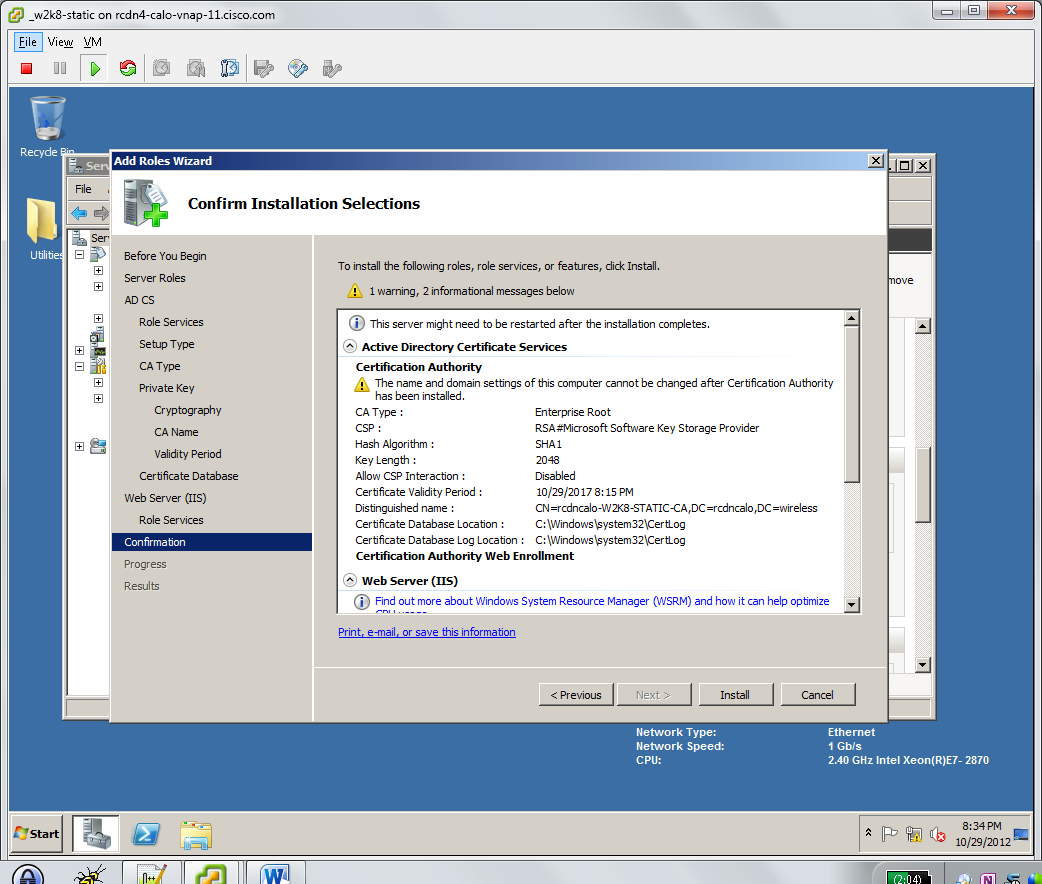
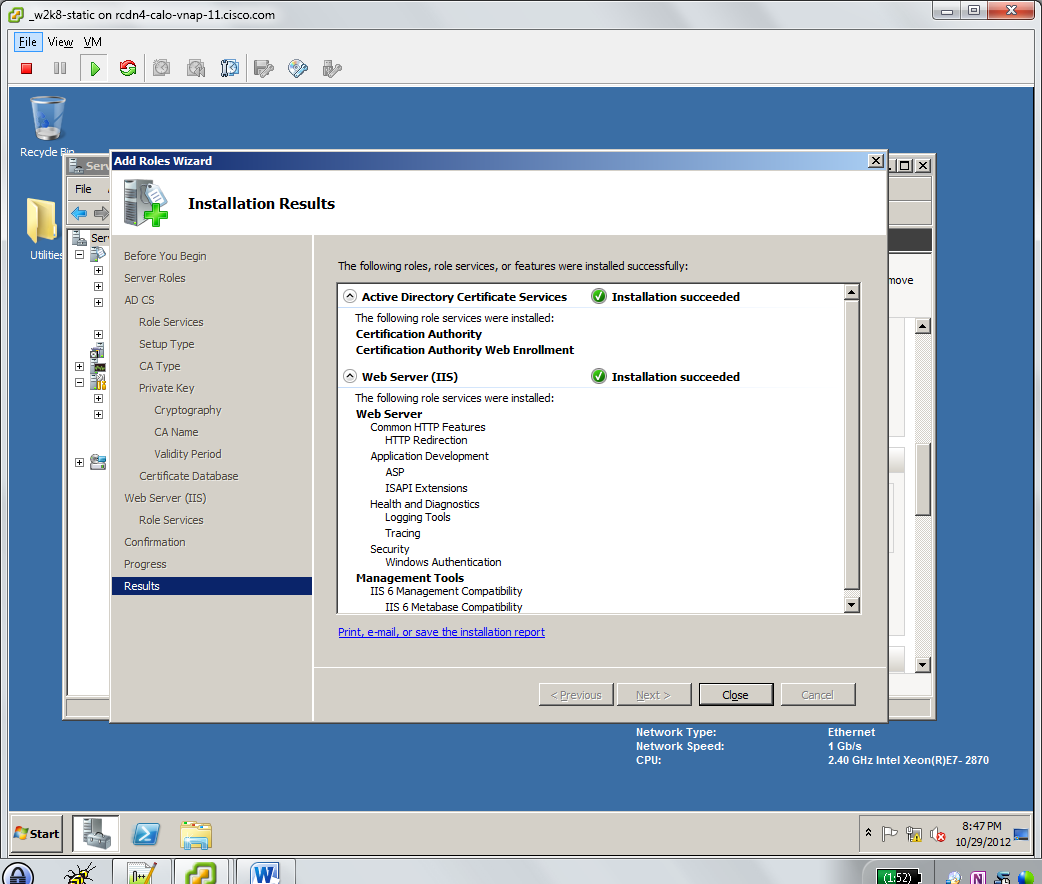
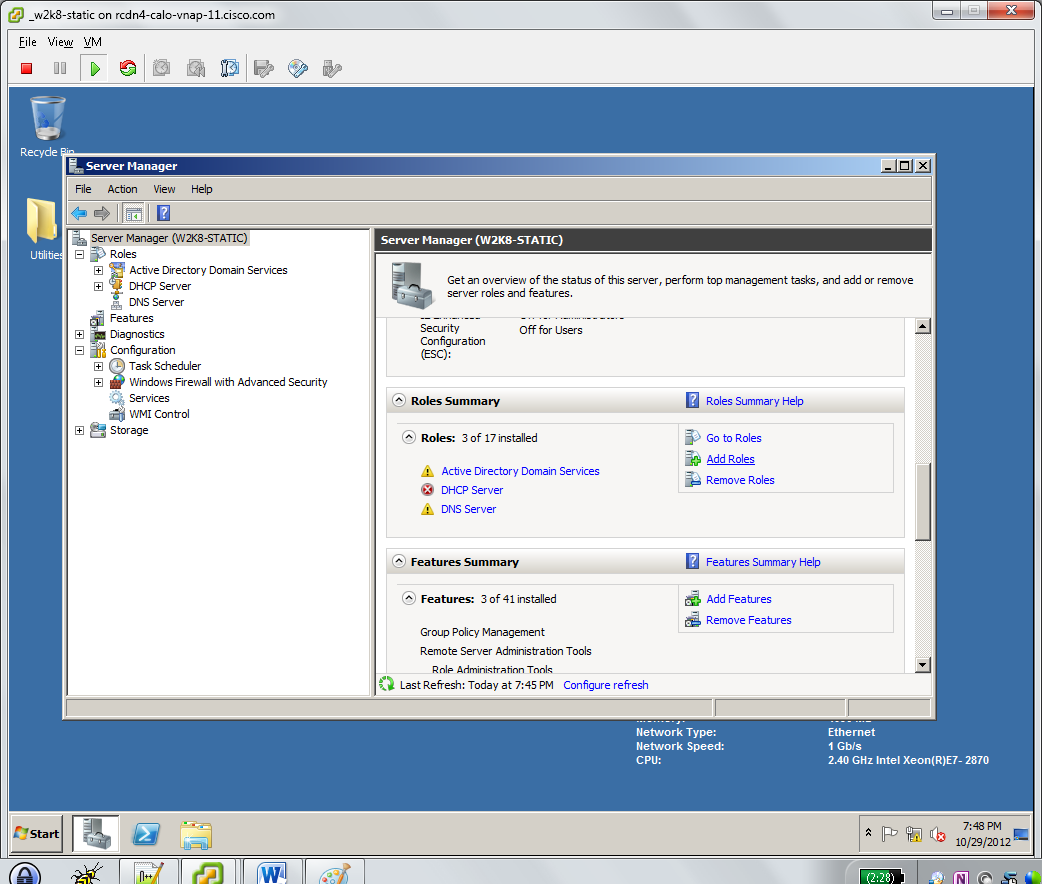
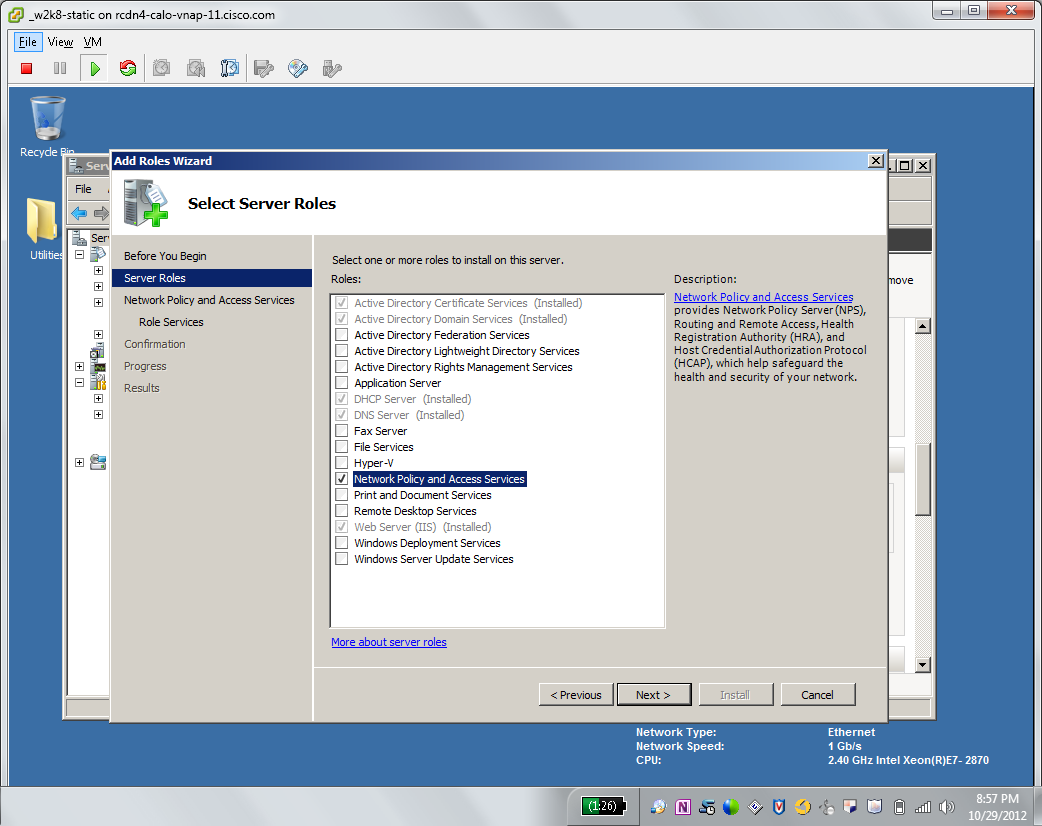
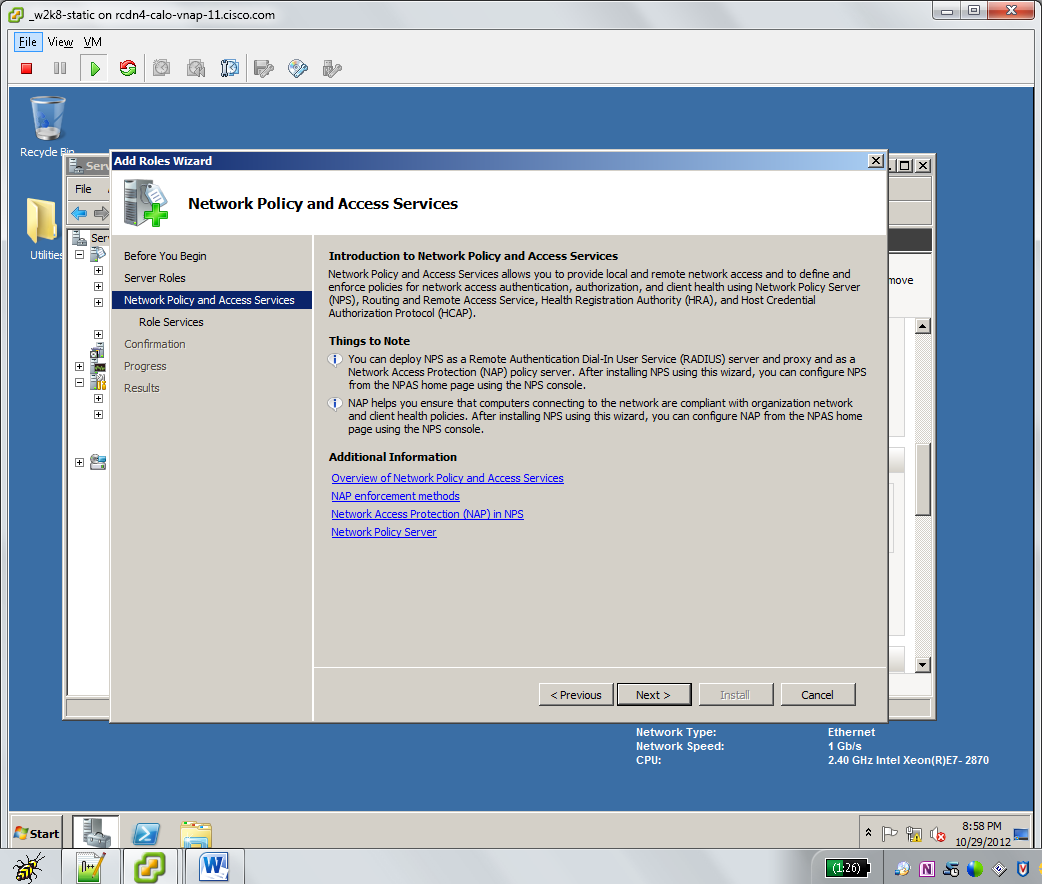
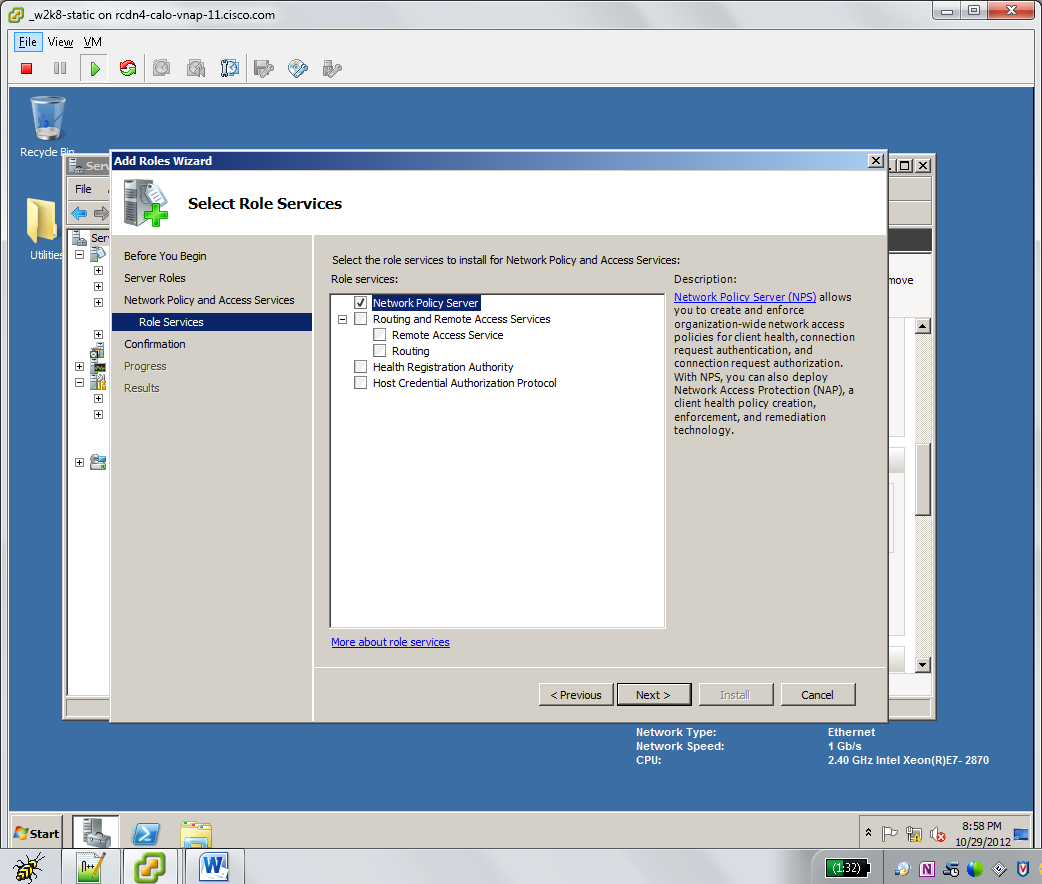
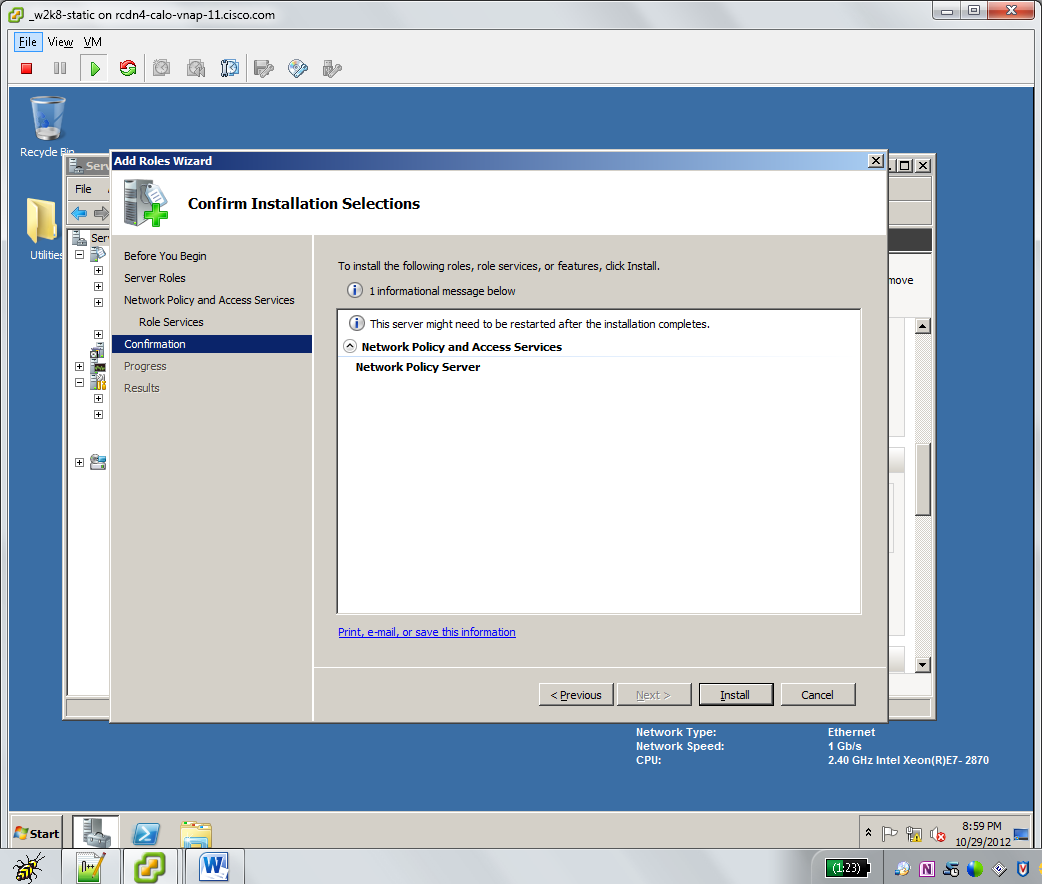
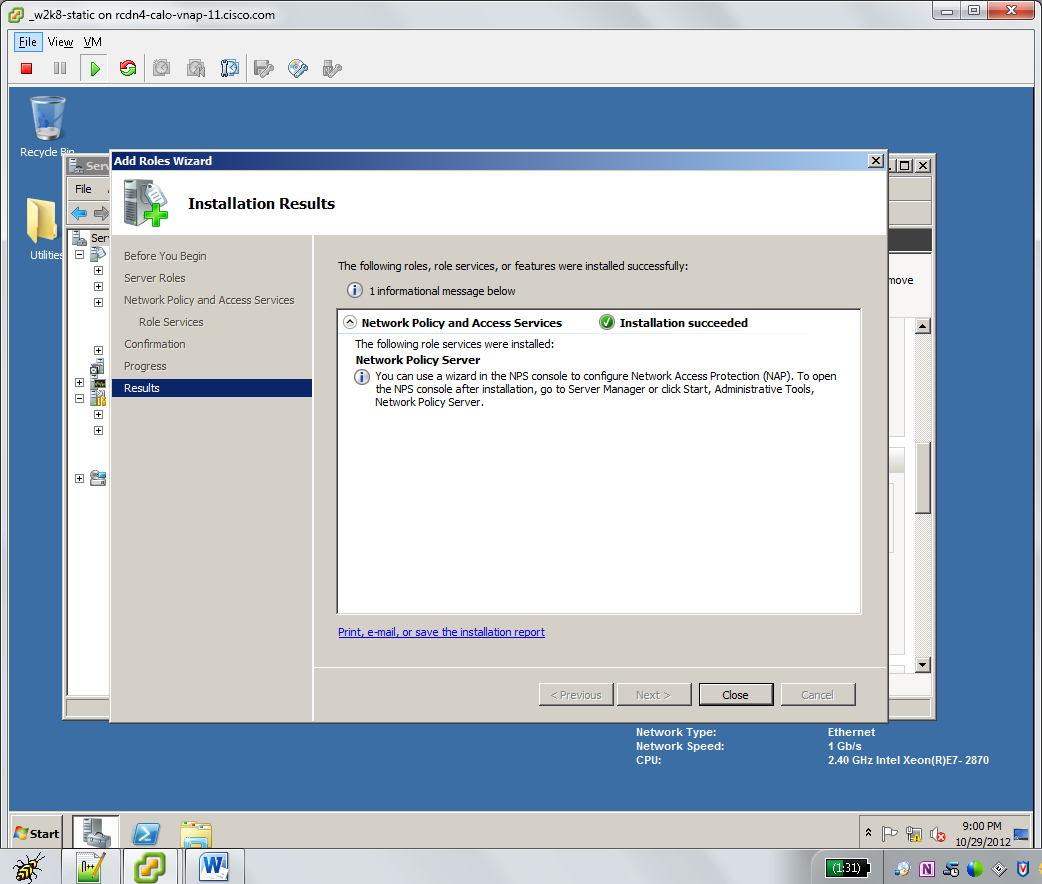
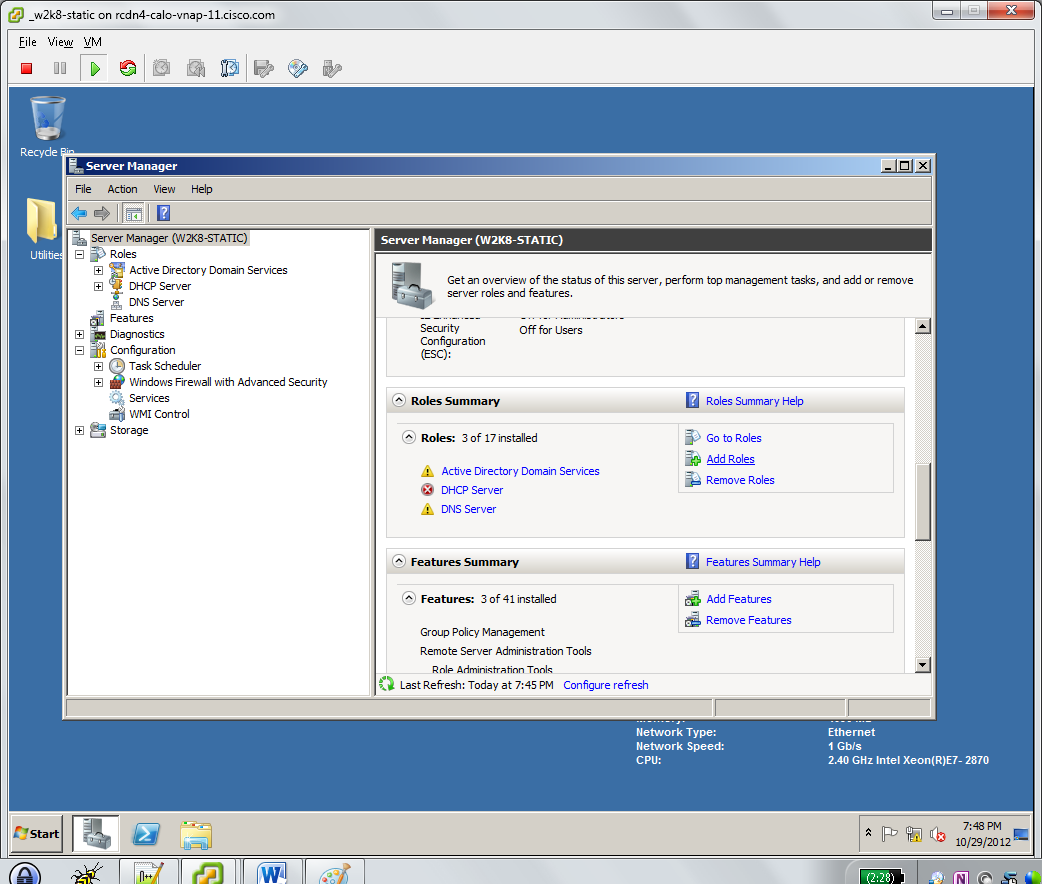
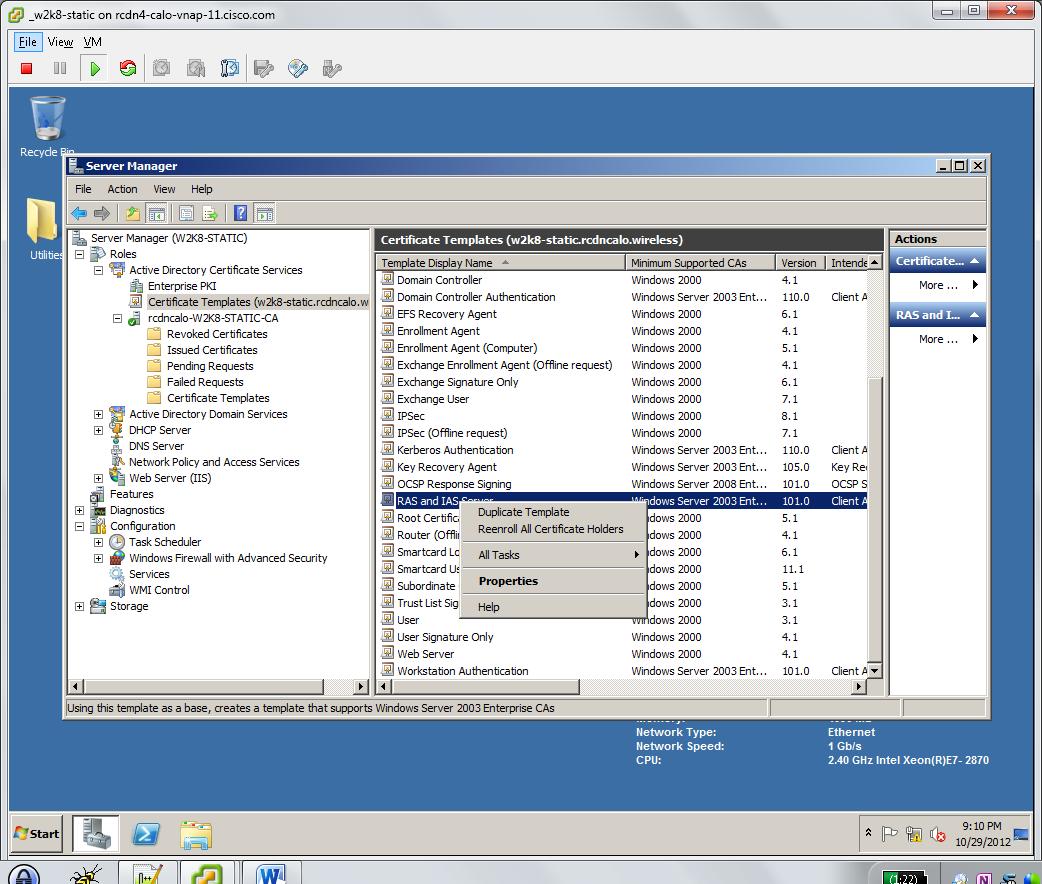
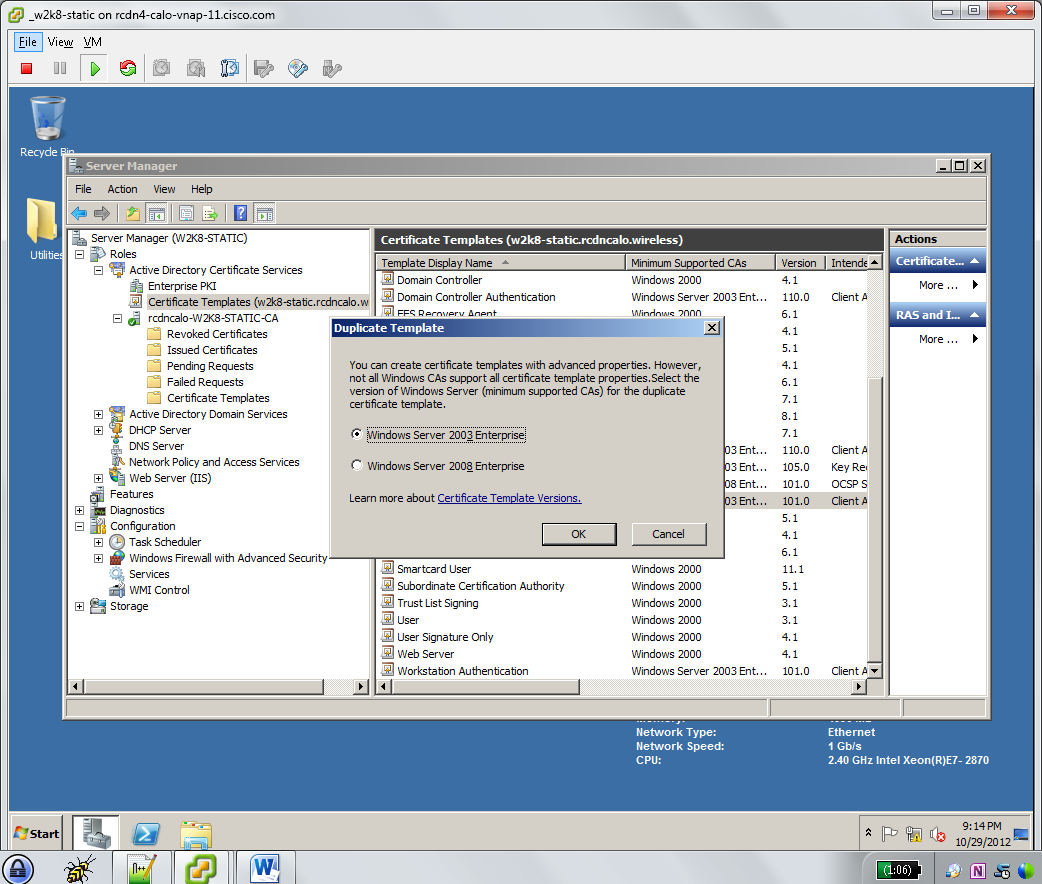
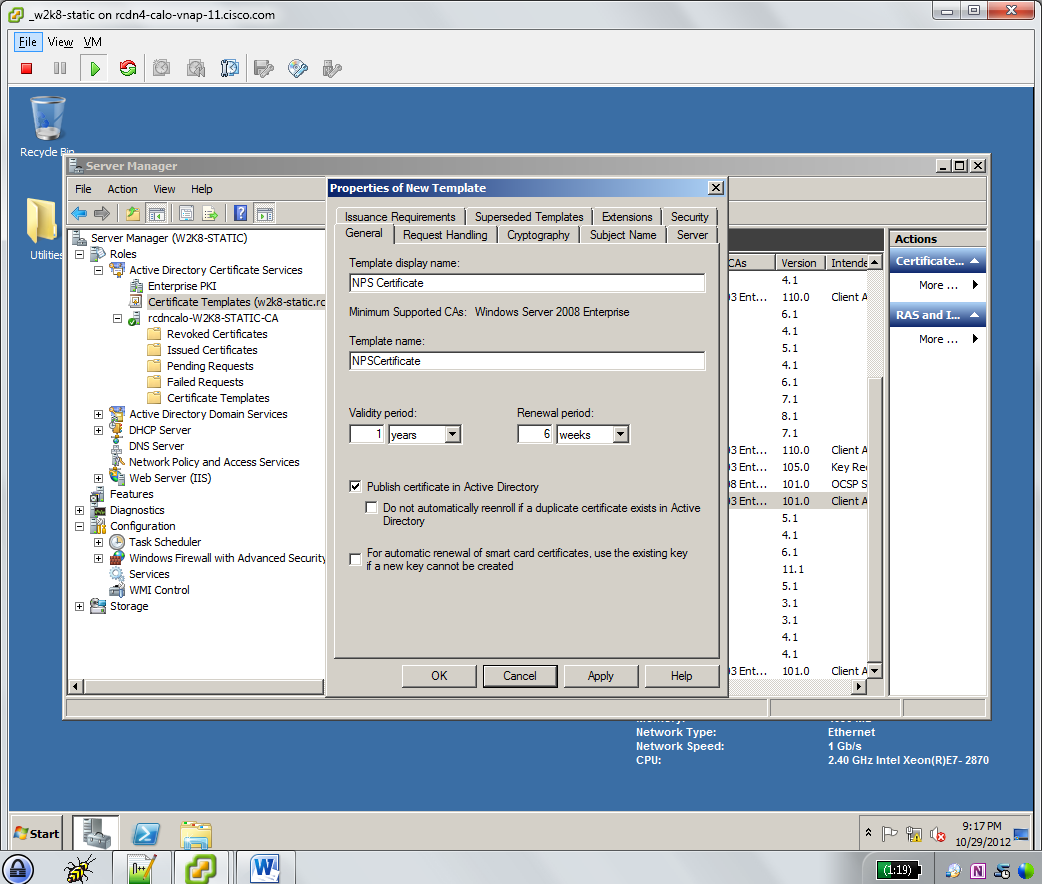
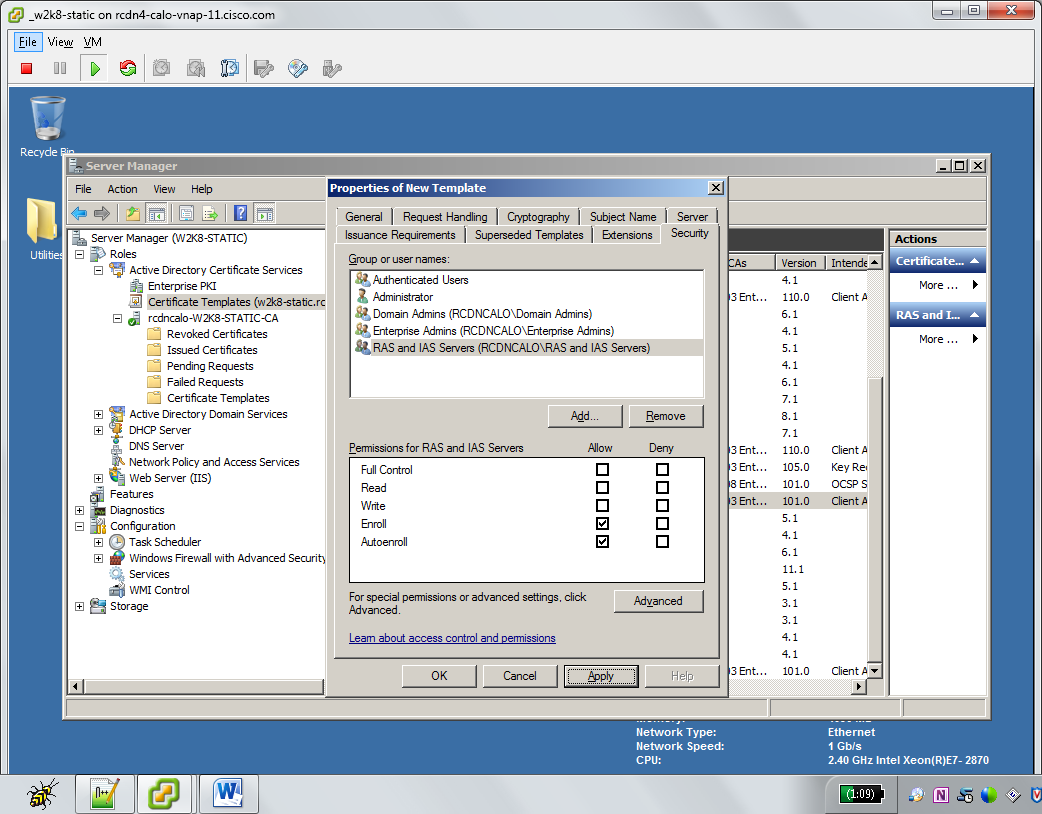
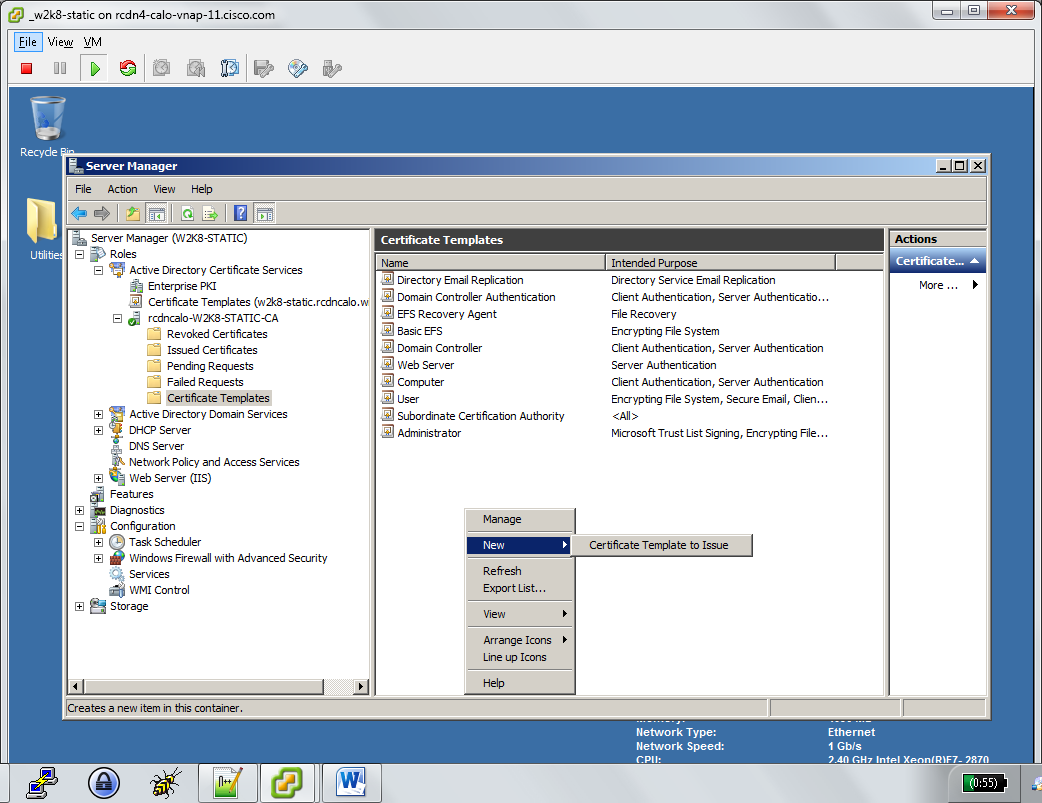
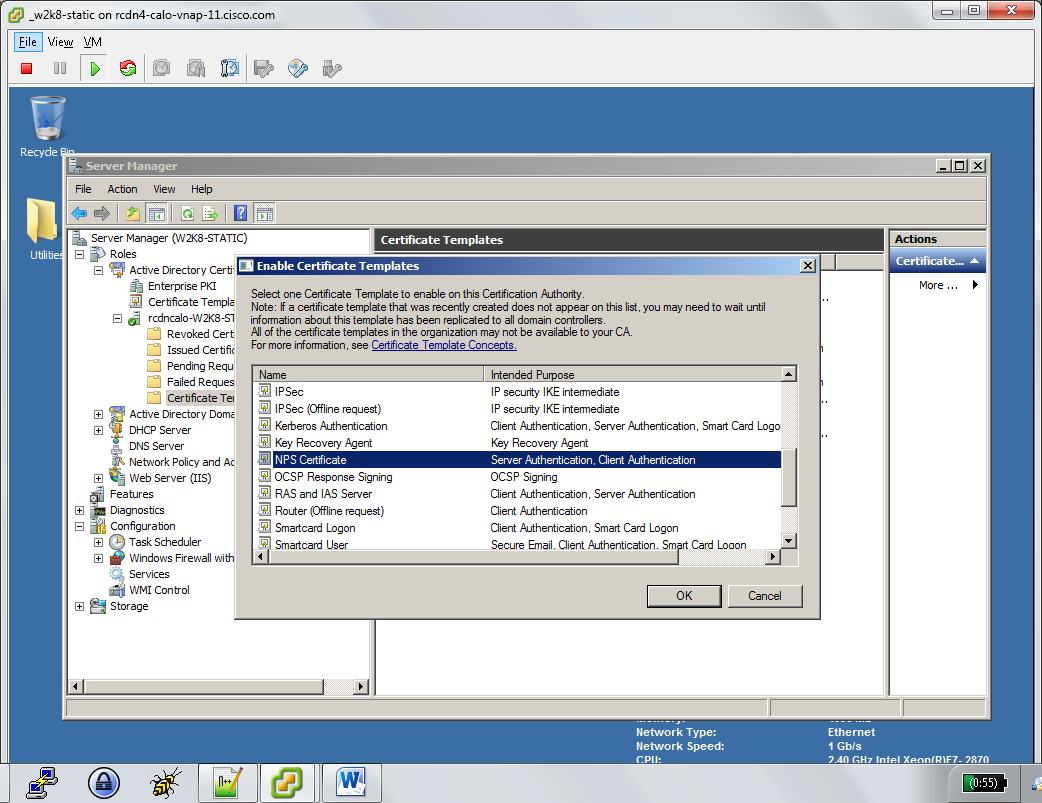
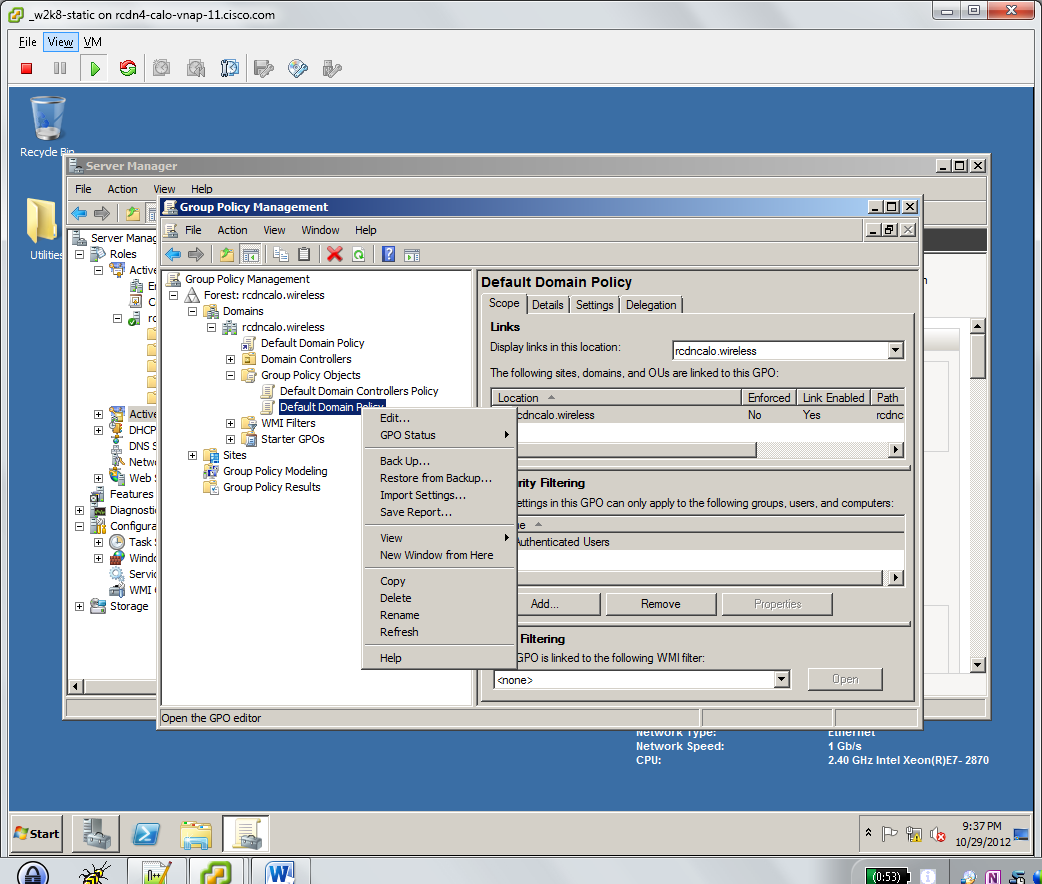
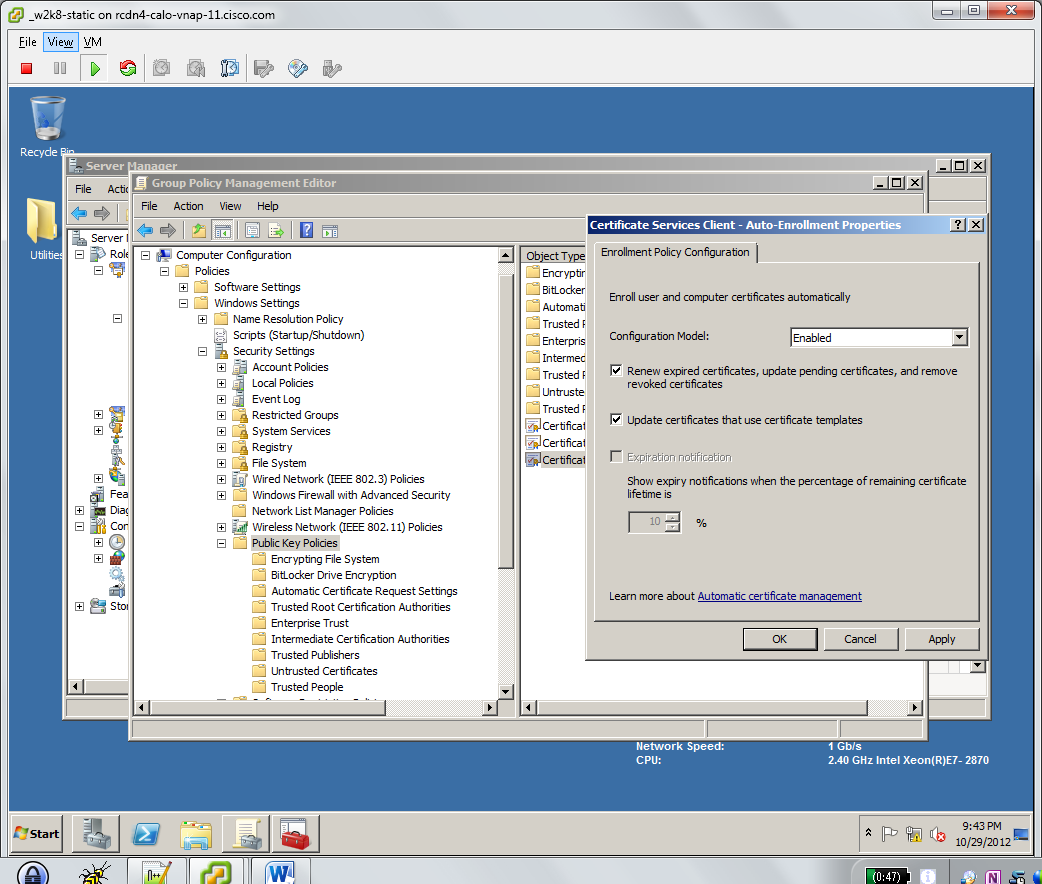
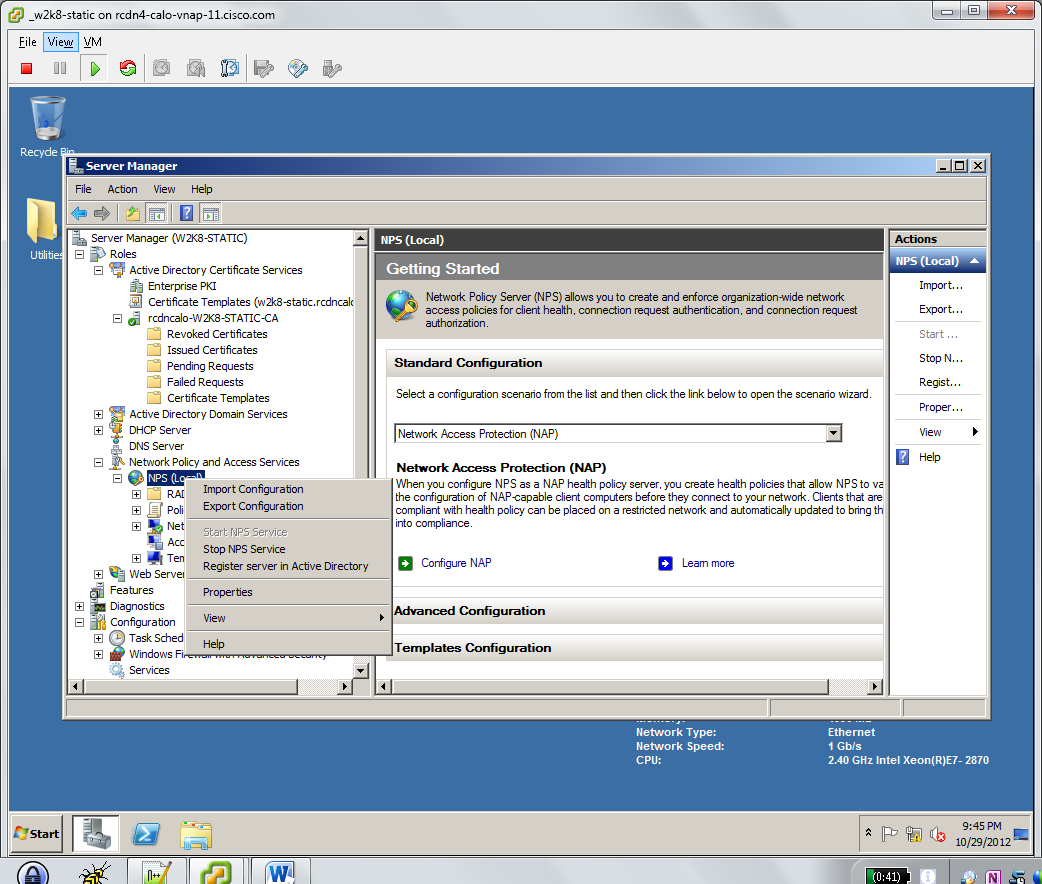
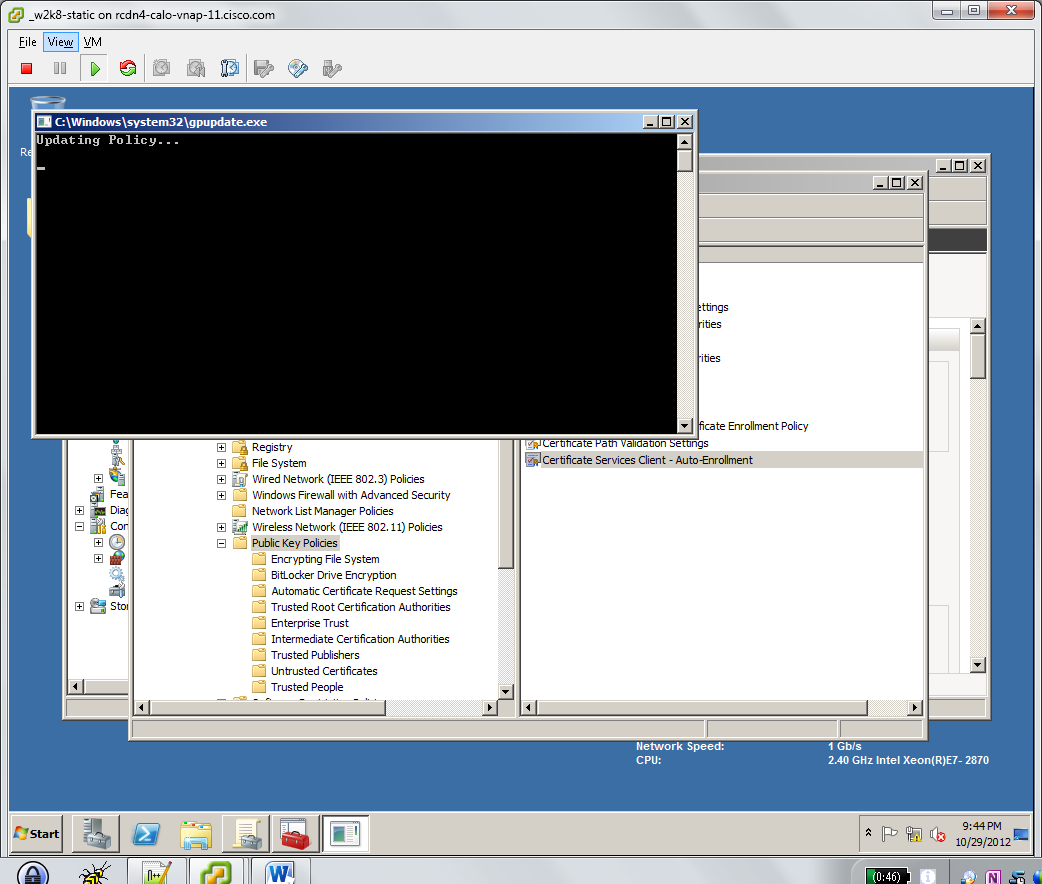
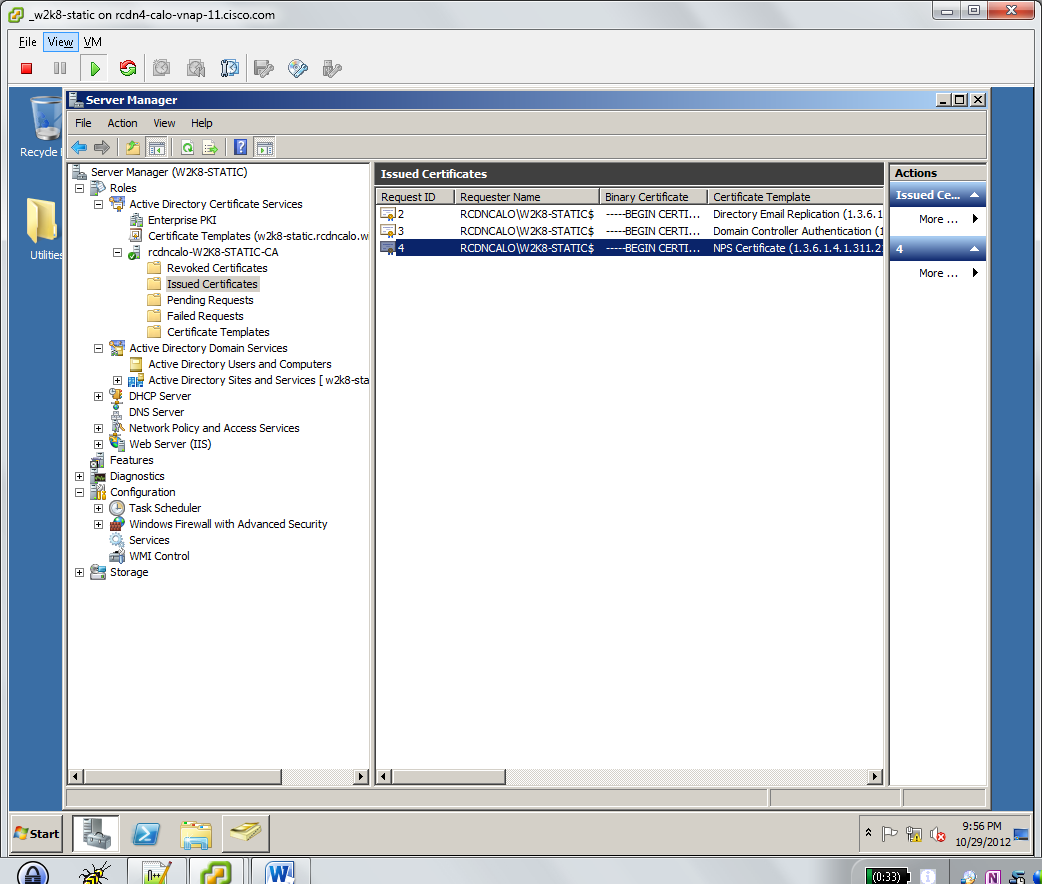
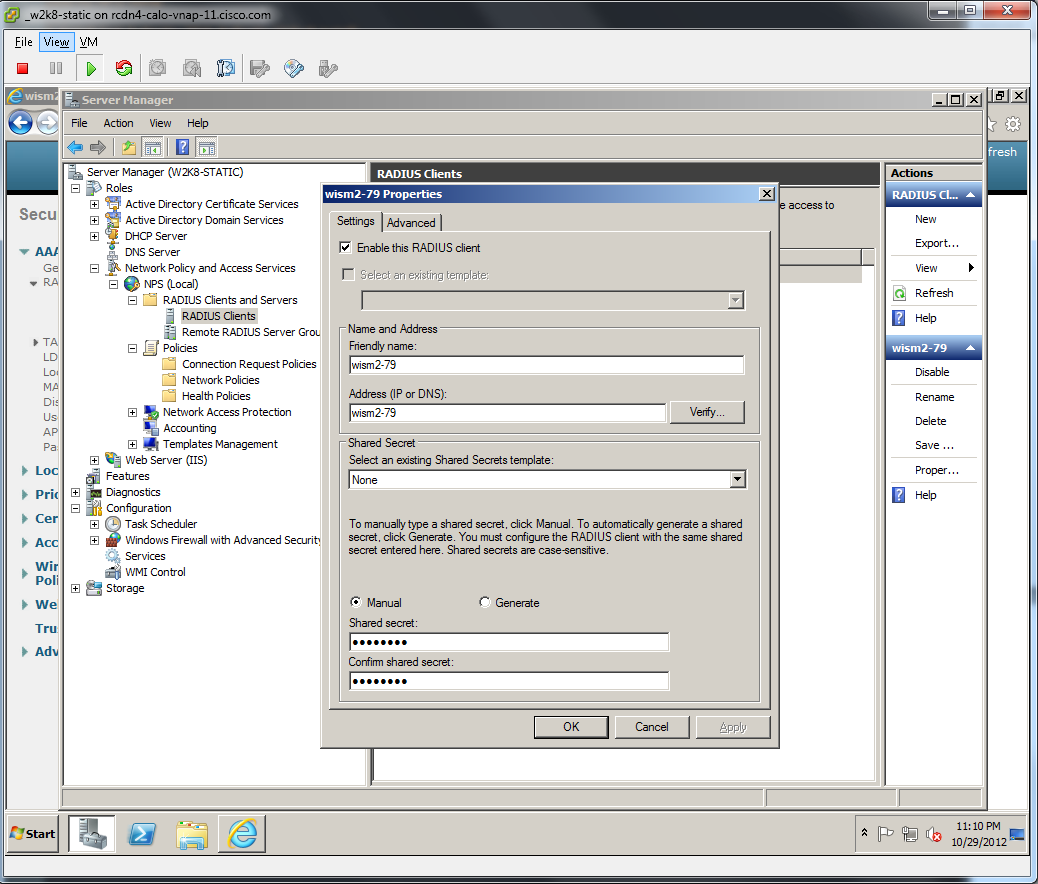
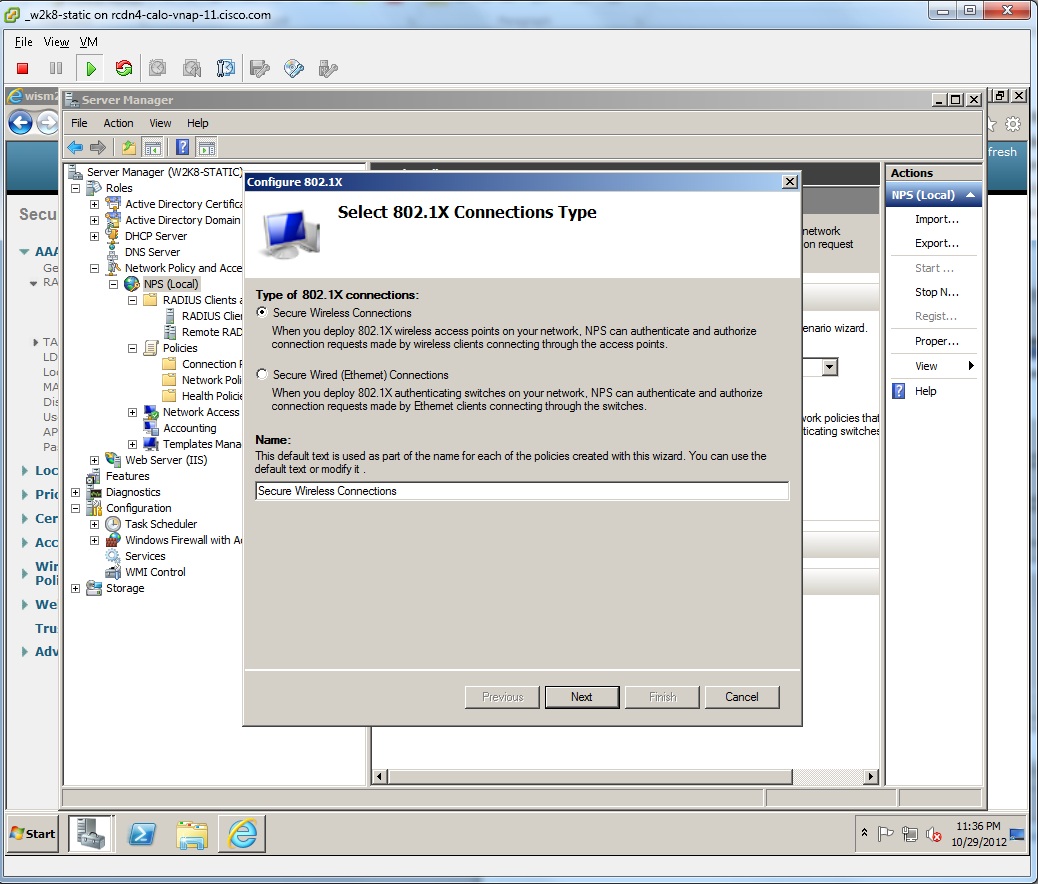
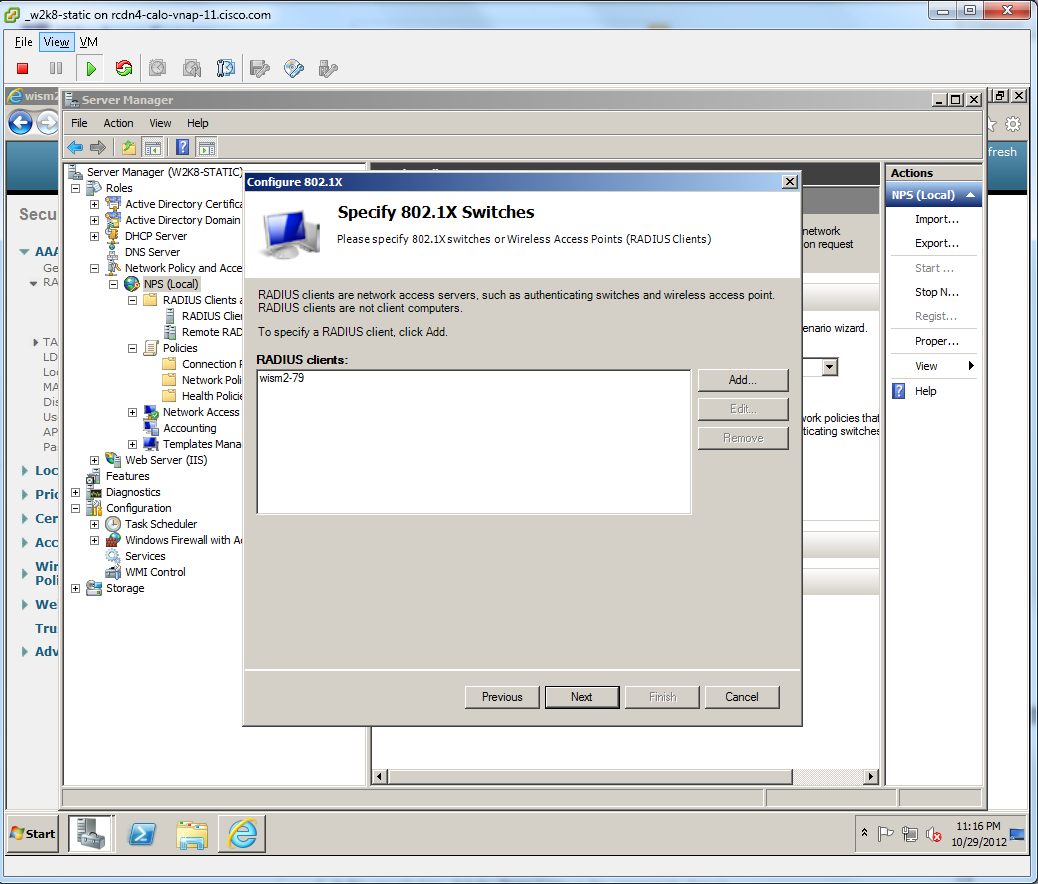
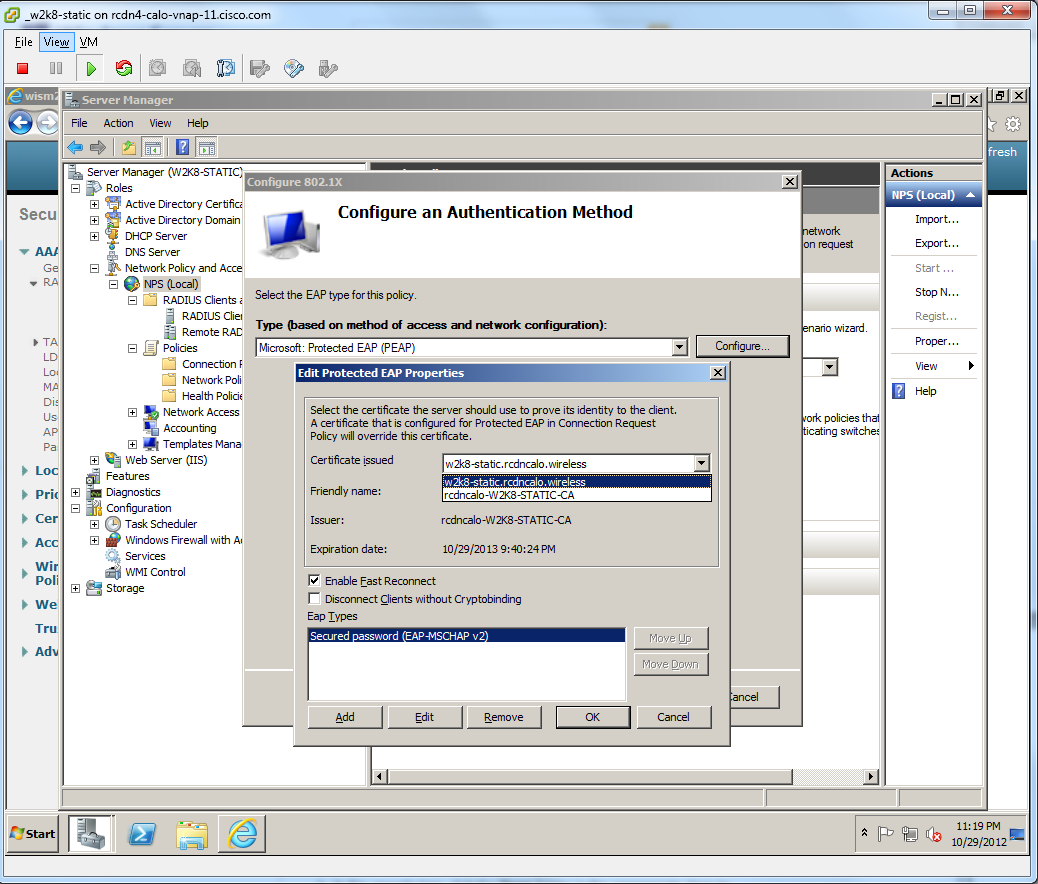
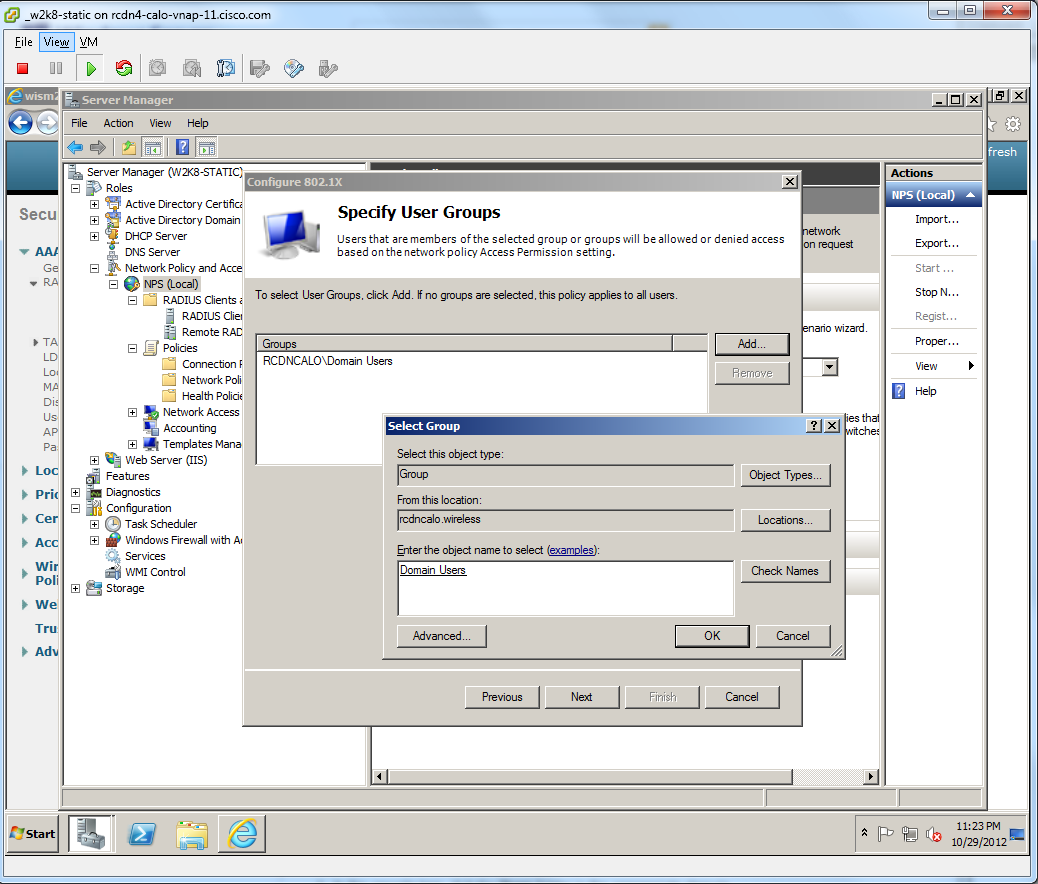
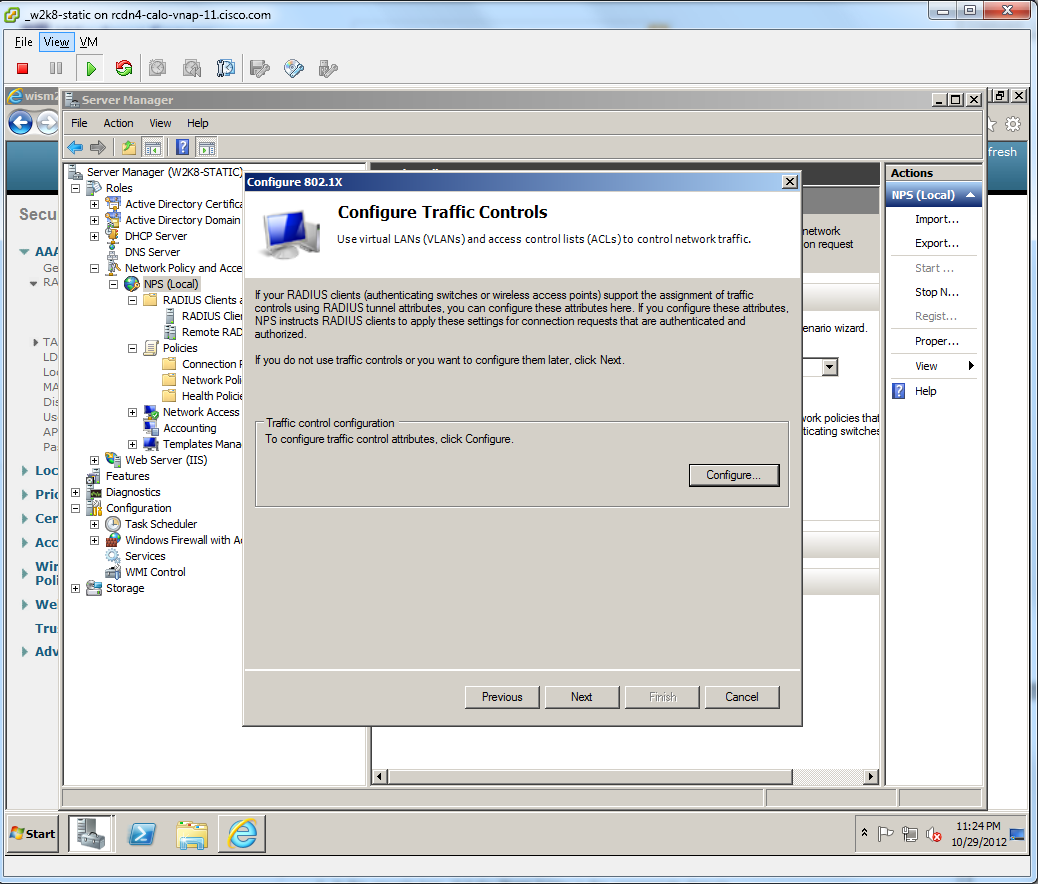
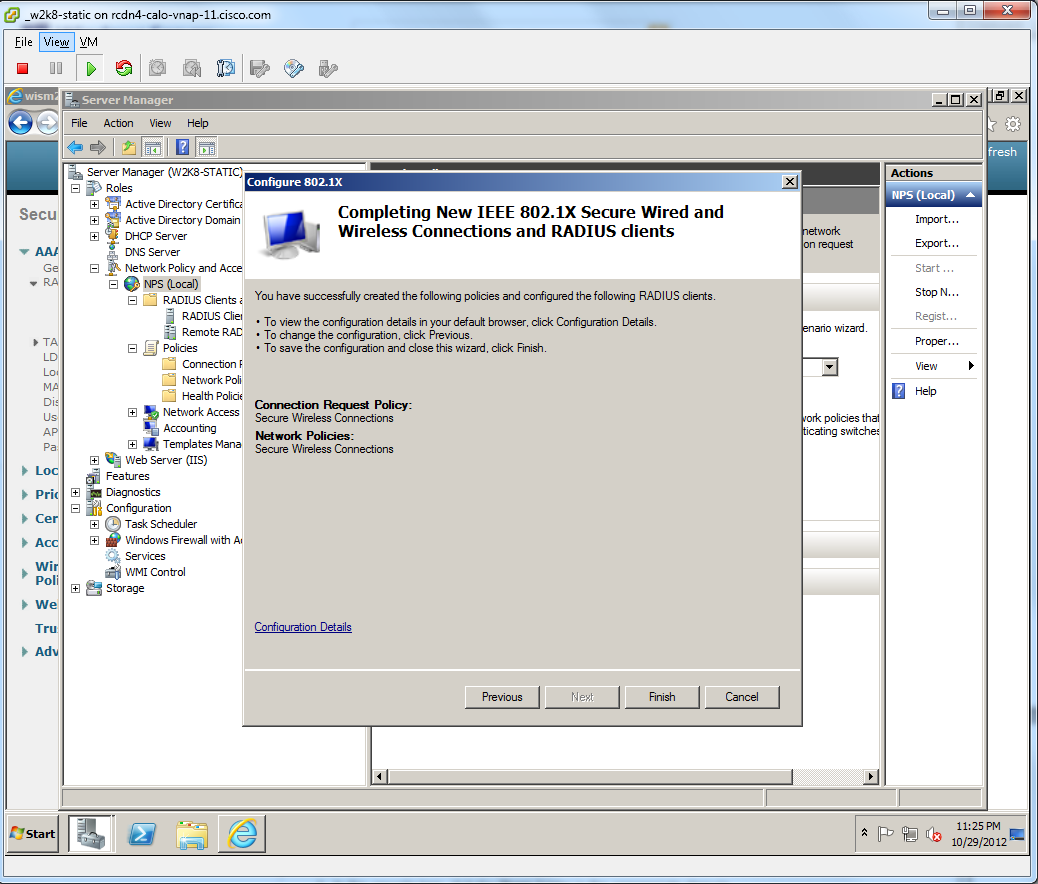
**Deploy a CA and NPS Certificate Server – Windows 2008 R2 Standard Server**

Resources:

* [http://technet.microsoft.com/en-us/library/cc771696.aspx](http%25253A%25252F%25252Ftechnet.microsoft.com%25252Fen-us%25252Flibrary%25252Fcc771696.aspx)
* [http://technet.microsoft.com/en-us/library/cc501466.aspx](http%25253A%25252F%25252Ftechnet.microsoft.com%25252Fen-us%25252Flibrary%25252Fcc501466.aspx)
* [http://technet.microsoft.com/en-us/library/cc730811.aspx](http%25253A%25252F%25252Ftechnet.microsoft.com%25252Fen-us%25252Flibrary%25252Fcc730811.aspx)

Prerequisites: Windows 2008 R2 Server, Active Directory Domain Services, Web Server (IIS).

1. **Install Web Server (IIS)**
   1. Open **Server Manager**
   2. Right Click **Roles** and select **Add Roles** or Click on **Roles Summary > Add Roles**
   3. Check **Web Server (IIS)** click **Next**  
      
   4. Click **Next**
   5. Accept the default web server role services, Click **Next**
   6. Confirm installation selections and make sure no errors are present. Click **Install**  
      
   7. Confirm installation results have no errors and resolve as necessary. Click **Close**  
      
2. **Install Active Directory Certificate Services**
   1. Open **Server Manager**
   2. Right Click **Roles** and select **Add Roles** or Click on **Roles Summary > Add Roles**
   3. Check **Active Directory Certificate Services**. Click **Next.**  
      
   4. Click **Next.**
   5. Check **Certification Authority** (default)
   6. Check **Certification Authority Web Enrollment.** Click **Add Required Role Services** if prompted.  
      
   7. Click **Next**
   8. Select **Enterprise.** Click **Next.**  
      
   9. Select **Root CA.** Click **Next.**  
      
   10. Select **Create a new private key.** Click **Next.**  
       
   11. Accept default encryption types, bit length, and hash algorithm. Click **Next**.  
       
   12. Leave default Common name and Distinguished name suffix. Click **Next.**  
       
   13. Modify validity period if desired. Click **Next.**  
       
   14. Accept certificate database defaults. Click **Next.**  
       
   15. IIS Introduction. Click **Next.**  
       
   16. Accept default web server roles services. Click **Next.**  
       
   17. Confirm installation selections and correct errors if necessary. **Note:** *you cannot change the name of your server after a Certificate Authority installation*. Click **Install**.  
       
   18. Confirm installation results have no errors and resolve as necessary. Click **Close.**
3. **Install NPS**
   1. Open **Server Manager**
   2. Right Click **Roles** and select **Add Roles** or Click on **Roles Summary > Add Roles**
   3. Check **Network Policy and Access Services**. Click **Next.**  
      
   4. Review Introduction if desired. Click **Next.**
   5. Check **Network Policy Server.** Click **Next.**  
      
   6. Review installation selections and correct errors as necessary. Click **Install.**  
      
   7. Review installation results and correct errors if necessary. Click **Close.**  
      
4. **Configure NPS CertificateTemplate and Autoenrollment**
   1. Open **Server Manager**
   2. Expand **Roles > Active Directory Certificate Services > Certificate Templates**. **Select RAS and IAS Server**. Right Click and choose **Duplicate Template.**  
      
   3. Select to Duplicate Template using your Domain Functional Level (from AD Directory Services Install). If uncertain, choose default **Windows Server 2003 Enterprise.** Click **OK**.  
      
   4. Type a **Template Display Name** that you will recognize for NPS. Adjust validity period to desired duration. Check **Publish certificate in Active Directory.**  
      
   5. Click the **Security**tab. In **Group or user names**, click **RAS and IAS Servers**.
   6. In **Permissions for RAS and IAS servers**, under **Allow**, select the **Enroll** and **Autoenroll** permission check boxes. Click **OK**.  
      
   7. From **Server Manager**. Select **Roles > Active Directory Certificate Services > *Your CA* > Certificate Templates.** Right Click in Certificate Templates task pane. Select **New > Certificate Template to Issue**.  
      
   8. Choose the name of the Certificate Template created previously. Click **OK.**
   9. Open **Group Policy Editor.** Click **Start > Administrative Tools > Group Policy Editor.** Expand Forest > Domains > $yourdomain > Group Policy Objects. Right Click **Default Domain Policy**. Click **Edit.**  
      
   10. Open **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, and then select **Public Key Policies.**
   11. In the details pane, double-click **Certificate Services Client - Auto-Enrollment**. The **Certificate Services Client - Auto-Enrollment Properties** dialog box opens.
   12. Change **Configuration Model** to **Enabled.**
   13. Select **Renew expired certificates, update pending certificates, and remove revoked certificates**
   14. Select **Update certificates that use certificate templates**
   15. Click **OK.**
   16. Register NPS in Active Directory. In **Server Manager**. Navigate to **Roles > Network Policy and Access Services > NPS (Local)**. Right Click **NPS (Local)** and choose **Register server in Active Directory.** Review authorization notification. Click **OK.** Computer now Authorized. Click **OK.**
   17. Force Group Policy Update. Click **Start > Run**. Type **gpupdate /force.** Allow update to finish.  
       
   18. Review Issued Certificates. Navigate to **Roles > Active Directory Certificates Services > *Your CA* > Issued Certificates.** We can now see the NPS Certificate has been issued to our machine **RCDNCALO\W2K8-STATIC$.** This was autoenrolled after registering NPS with Active Directory and forcing a Group Policy Update. This will be the Server side certificate used for applicable EAP Authentication Methods.
   19. Create RADIUS Clients adding your WLC(s). Open **Server Manager** Navigate to **Roles > Network Policy and Access Services > NPS (Local) > RADIUS Clients and Servers > RADIUS Clients.** Right Click and click **New**. Populate **Friendly name, Address (IP or DNS).** For Shared Secret, leave **Template** to **None.** Choose **Manual** and type **Shared Secret** and matching **Confirm shared secret.** Click **OK.** (example uses *cisco123)*.  
       
   20. Create new **802.1X Configuration.** Navigate to **Roles > Network Policy and Access Services > NPS (Local).** Click dropdown in **Standard Configuration** section then **Select** **RADIUS server for 802.1X Wireless or Wired Connections.** Click **Configure 802.1X.** For type of 802.1X Connections: select **Secure Wireless Connections.** Provide a **Name** for the policy or accept default **Secure Wireless Connections.** Click **Next.**  
       
   21. Confirm RADIUS client is present. This client was added previously. Add additional RADIUS clients as required. Click **Next.**  
       
   22. Select EAP method type for this policy. For PEAP choose **Microsoft: Protected EAP (PEAP)**. For EAP-TLS choose **Microsoft: Smart Card or other Certificate** (our example is configuring PEAP).Select **Configure**. Verify Certificate issued reflects the certificate that NPS autoenrolled. Our NPS certificate template provided a one year validity period, where-as the Root CA certificate is for five years. Notice the Certificate reflects the FQDN for the Windows Server we are installing NPS on: w2k8-static.rcdncalo.wireless. The other certificate is the actual Root CA that matches the name from the Root CA installation earlier which is not what we want to select. Click **OK**. Click **Next.**   
       
   23. Add desired Windows Groups. These can be machine or user groups. We are adding default **Domain Users** group for example. Click **OK.** Click **Next.**  
       
   24. Do not configure Traffic Controls at this time. This can be used for VLAN assignment and other VSA Attributes to provide AAA override settings to the WLC. Click **Next.**  
       
   25. Click **Finish.**
   26. Add RADIUS server to WLC. Navigate in the WLC GUI to **SECURITY > AAA > RADIUS > Authentication.** Click **New…** Provide **Server IP Address** for NPS server. Provide **Shared Secret** and **Confirm Shared Secret**. Click **Apply.**  
       