Lab 8: NAP - Mission Impossible

# For this lab

## Discuss:

* What the hardest part of the lab was and why you thought it was hard
* Any problems you had with the lab and what was done to fix the issues (even if the instructor fixed the issue. Pay attention!)
* Improvements you would make to the lab (Two minimum)

## Questions to answer

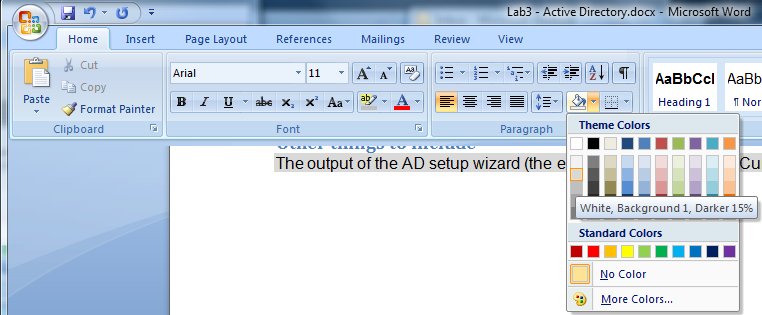
* Did you have to go back and fix the GPO for NAP configuration?
* Did you have to replace the SSL certificate for IIS?
* Was this lab too hard? (yes, this is a rhetorical question) If so, what do you think could be done to make it easier?

## Screenshots and other items to include with the report

* Screenshot of the netsh and ipconfig commands
* Screenshot of the WMIC computer rename command results
* The contents of the unattend.txt file
* Screenshot of successful enrollment for computer and SHA certificate
* The text results of the certutil.exe -setreg policy\EditFlags +EDITF\_ATTRIBUTEENDDATE command
* Screenshot of the Completing NAP Enforcement Policy and RADIUS Client Configuration page.
* Screenshot of the HRA certificate on the Client1 and Client2 computers
* Screenshot of the napstat status window
* Screenshot of an EventID22, HRA event

Other things to include

The contents of the **unattend.txt** file and the text results of the **certutil.exe -setreg** command in 10-point Currier new font, with paragraph shading of **White, Background 1, Darker 15%** for the contents of the file (See the screenshot for paragraph formatting help and the second paragraph for an example). DO NOT USE A SCREEN SHOT!



**How to shade the contents of the unattend.txt file**

[DCInstall]

ReplicaOrNewDomain=blah

NewDomain=blah.blah

NewDomainDNSName=who.knows

ForestLevel=16

DomainNetbiosName=bob

DomainLevel=4026

SafeModeAdminPassword=lassie

**Example output from unattend.txt file**

**NOTE: the commands in this lab can be easily miss-typed. Pay careful attention to the commands and make sure they are successful *before* continuing!**

## What you should have Before Starting

* You should have a fully functional Domain Controller (DC server)
* You should have a Windows 2008r2 Enterprise Full install server that is a member of the domain (NAP server)
* You should have a client Windows 7 machine named Client-lastname
* You should have a windows 2008r2 core server named SERVER-Lastname (File Server)

## On the Windows 7 management workstation

#### Group membership

1. Go to Start --> Administrative tools --> Active Directory Users and Computers.
2. Right-click on the name of the domain you created and select new --> Group. Call the group **NAP exempt computers**. Create additional groups called **NAP Client Computers**, **Boundary Network** and **Secure Network**
3. Open **NAP exempt computers** and click on the **Members** tab
   1. Click on add.
   2. Click on **Object Types. . .**
   3. Put a check box next to **Computers** and click on OK.
   4. Type in the name of your Domain Controller, NAP Server and file server, click on **Check Names**.
   5. Click on **OK**. You should have three computers listed – DC-lastname, NAP-lastname and SERVER-lastname.
   6. Click on **OK** again to close the window.
4. Open **NAP client computers** and click on the **Members** tab
   1. Click on add.
   2. Click on **Object Types. . .**
   3. Put a check box next to **Computers** and click on OK.
   4. Type in the name of your client computer (the Windows 7 machine), click on **Check Names**.
   5. Click on **OK**. You should have one computers listed – CLIENT-lastname.
   6. Click on **OK** again to close the window.
5. Open **Boundary Network** and click on the **Members** tab
   1. Click on add.
   2. Click on **Object Types. . .**
   3. Put a check box next to **Computers** and click on OK.
   4. Type in the name of your Domain Controller and NAP Server, click on **Check Names**.
   5. Click on **OK**. You should have two computers listed – DC-lastname, NAP-lastname.
   6. Click on **OK** again to close the window.
   7. At the end of the lab, these computers will be reachable from non-secure computers.
6. Open **Secure Network** and click on the **Members** tab
   1. Click on add.
   2. Click on **Object Types. . .**
   3. Put a check box next to **Computers** and click on OK.
   4. Type in the name of your File Server and client computer, click on **Check Names**.
   5. Click on **OK**. You should have two computers listed –SERVER-lastname and CLIENT-lastname.
   6. Click on **OK** again to close the window.
   7. At the end of the lab, these computers will only be reachable using IPSEC Health Security Certificates.
7. Close **Active Directory users and Computers**.
8. Reboot the Domain Controller, then all other computers for the group membership changes to take effect.

## On the NAP Windows 2008 server

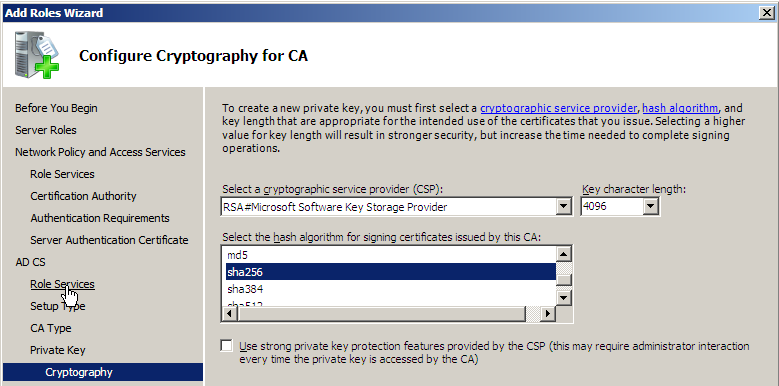
Log in using the domain administrative account you created: Firstname0Lastname (you must log in using an account that is a member of the **Domain Admins** group). A common mistake is to log in as a *local* user on the server.

#### Enable remote management tools

1. Open server manager and select **Features**.
2. Find and enable **Group Policy Management.**
3. Expand **Remote Server Administration Tools** 🡪 **Role Administration Tools** 🡪 **AD DS and AD LDS Tools 🡪 AD DS Tools**. Enable **AD DS Snap-Ins and Command-Line Tools**.
4. Click on **Next** then **Install**.

#### Certificate Service installation

1. Click on **Roles** in the navigation pane and select **Add Roles** from the details pane.
2. Click on **Next**.
3. Click on the checkbox next to **Active Directory Certificate Services** to select it.
4. Click **Next**.
5. Click on **Next** again on the screen introducing AD Certificate Services.
6. Click on **Next**.
7. Leave the default CA setup type set to **Enterprise**. Click on Next.
8. Leave the default CA type to **Root CA**. Click on Next.
9. Leave the default Private key set to **Create a new private key**. Click on Next.
10. On the Configure Cryptography for CA page, leave the default **RSA#Microsoft Software Key Storage Provider**. Click on the drop-down box under Key character length: and select **4096**. Change the hash algorithm to **sha256** (you may need to scroll down to see this option).

****

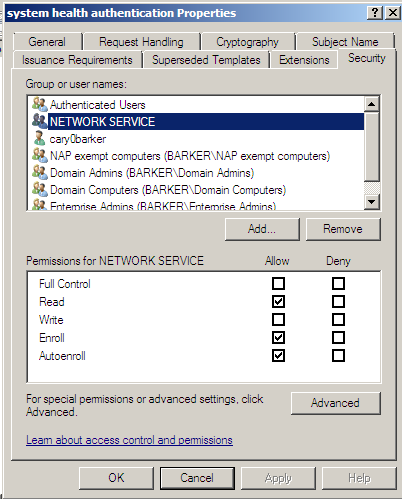
**Configuring the CA cryptography**

1. When prompted for the **SA Validity Period**, leave the default (5 Years) and click **Next**.
2. Click Next 3 times through the Certificate services folder locations, IIS configuration and components screens.
3. Click on **Install**. (Note: you will receive one warning about not being able to change name or domain settings - this is normal).

### Configure Certificate services and the NPS

#### Configure Certificate Template

1. Click Start and type in **certtmpl.msc** to open up certificate Templates.
2. In the right-hand pane, right-click on **Workstation Authentication** and select **Duplicate Template**.
3. For compatibility, choose **Windows Server 2008, Enterprise Edition**. Click on **OK**.
4. For the Display name, type in **System Health Authentication.** Make sure there is a check in the box next to **Publish certificate in Active Directory**.
5. Click on the **Extensions** tab.
6. Click on **Edit**.
7. Click on **Add.** . .
8. Scroll down and select **System Health Authentication** and click on **OK**.
9. Click on **OK** again.
10. Click on the **Security** tab.
11. Click on **Add. . .**
12. Type in **NAP exempt computers** (the group you created earlier) and click on **OK**.
13. Click on **Add. . .**
14. Type in **NETWORK SERVICE** (this is the service account the HRA runs under) and click on **OK.**
15. Make sure to add check marks below **Allow** for the **Enroll** and **Autoenroll** permissions to the **NAP exempted computers** and the **NETWORK SERVICE** groups.
16. Click on **OK**.
17. Close the console.

****

**Permissions for the *NAP exempted computers* and *NETWORK SERVICE* groups**

#### Publish the Certificate Template

1. Click on Start and type in **certsrv.msc**.
2. Expand the CA. Right-click on **Certificate Templates** and select New 🡪**Certificate Template to Issue**.
3. Click on **System Health Authentication** and select **OK**.
4. Verify the **System Health Authentication** template appears and one of the roles is listed as **System Health Authentication**.
5. Close the console

#### Certificate on NAP server

1. Open GPMC (gpmc.msc)
2. Expand the **Forest** --> **Domains** --> **Your Domain**
3. right-click on the **Default Domain Policy** and select **Edit.**
4. Expand **Computer Configuration** 🡪 **Policies** 🡪 **Windows Settings** 🡪 **Security Settings** 🡪 **Public Key Policies**
5. Double-click on **Certificate Services Client - Auto-Enrollment**
6. Next to **Configuration Model**, click on the drop-down box and select **Enabled**. Put a check in the boxes next to **Renew expired certificate, update pending certificates, and remove revoked certificates** and **Update certificates that use certificate templates**.
7. Click on **OK**
8. Close GPMC.
9. Click **Start** and type in **gpupdate /force**

#### Request and Verify computer certificate was installed.

1. Click on **Start** and type **mmc**
2. Click on **File** 🡪 **Add/Remove Snap-in**.
3. Click on **Certificates** and click on the **Add** button. Click on the Radio button next to **Computer account** and click on **Next**. Leave the default **Local computer** and click on **Finish** then **OK**.
4. In **Certificates (Local Computer)** 🡪 **Personal** 🡪 **Certificates** you will now find a certificate in the details pane. Verify that certificates for **System Health Authentication** and **Client Authentication** appear under the general tab. If they don’t, do the following:
   * In the Console tree, expand Certificates (Local Computer), right-click on **Personal 🡪 All Tasks** 🡪 **Request New Certificate**.
   * Click on **Next, Next** again, put a check in the box next to **Computer** and **System Health Authentication** then click on **Enroll**. (The computer certificate is needed for IIS later)
   * Click on **Finish**.
5. On the screen showing you have a certificate for System Health Authentication, grab a screenshot and include it in your lab report.
6. Close the MMC console. (select no when prompted to save the console)

#### Allow HRA to request/issue/manage certificates

1. Click on **Start** 🡪 **Administrative tools** 🡪 **Certification Authority**
2. Right-click on the CA server and select **properties**.
3. Click on the **Security** tab and select **Add**.
4. Type in **Network Service** and click on **OK**.
5. Make sure the following check boxes under the **allow** column are checked:
   * **Issue and Manage Certificates**
   * **Manage CA**
   * **Request Certificates**
6. Click on **OK**
7. Run the below commands as administrator. The result of the commands is in the following diagram (REF: http://technet.microsoft.com/en-us/library/dd296906.aspx)

* Open an administrative cmd prompt: Click on **Start** 🡪 **All Programs** 🡪 **Accessories**. Right-click on **Command Prompt** and select **Run as administrator**. Enter the two below commands (Note, the first command wraps to a second line - it must be entered as one line in the command prompt or it will fail!)
* **certutil.exe -setreg policy\EditFlags +EDITF\_ATTRIBUTEENDDATE**
* **net stop certsvc && net start certsvc**

C:\Windows\system32>Certutil.exe -setreg policy\EditFlags +EDITF\_ATTRIBUTEENDDATE

SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\barker-NAP-BARKER-CA\Pol

icyModules\CertificateAuthority\_MicrosoftDefault.Policy\EditFlags:

Old Value:

EditFlags REG\_DWORD = 11014e (1114446)

EDITF\_REQUESTEXTENSIONLIST -- 2

EDITF\_DISABLEEXTENSIONLIST -- 4

EDITF\_ADDOLDKEYUSAGE -- 8

EDITF\_BASICCONSTRAINTSCRITICAL -- 40 (64)

EDITF\_ENABLEAKIKEYID -- 100 (256)

EDITF\_ENABLEDEFAULTSMIME -- 10000 (65536)

EDITF\_ENABLECHASECLIENTDC -- 100000 (1048576)

New Value:

EditFlags REG\_DWORD = 11016e (1114478)

EDITF\_REQUESTEXTENSIONLIST -- 2

EDITF\_DISABLEEXTENSIONLIST -- 4

EDITF\_ADDOLDKEYUSAGE -- 8

EDITF\_ATTRIBUTEENDDATE -- 20 (32)

EDITF\_BASICCONSTRAINTSCRITICAL -- 40 (64)

EDITF\_ENABLEAKIKEYID -- 100 (256)

EDITF\_ENABLEDEFAULTSMIME -- 10000 (65536)

EDITF\_ENABLECHASECLIENTDC -- 100000 (1048576)

CertUtil: -setreg command completed successfully.

The CertSvc service may need to be restarted for changes to take effect.

C:\Windows\system32>net stop certsvc && net start certsvc

The Active Directory Certificate Services service is stopping.

The Active Directory Certificate Services service was stopped successfully.

The Active Directory Certificate Services service is starting.

The Active Directory Certificate Services service was started successfully.

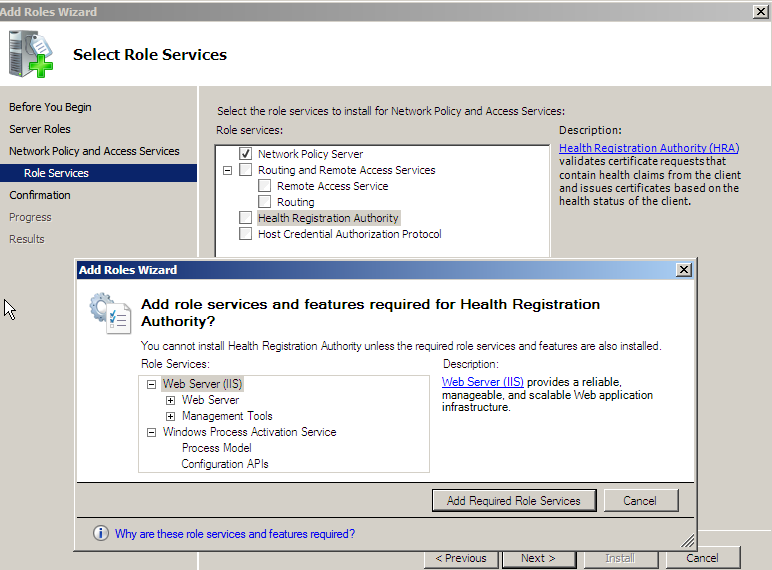
C:\Windows\system32>

**output of the certutil command setting the attributeenddate flag.**

1. Copy the text results of the two above commands and include them in your lab report.

### Install NPS

1. Click on Start --> server manager.
2. Click on Roles then click on the link **Add Roles**.
3. Click on **Next**.
4. Put a Check in the checkbox next to **Network Policy and Access Services** role.
5. Click on **Next**. Click on **Next** again.
6. Put a Check in the checkboxes next to **Network Policy Server** and **Health Registration Authority**.
7. Click on **Add Required Role Services** when prompted.



**Additional service dependencies**

1. Click on **Next**
2. Click on the radio button next to **use the local CA to issue health certificates for this HRA server** and click **Next**.
3. On the Choose Authentication Requirements for the Health Registration Authority screen, select **No, allow anonymous requests for health certificates**.
4. Select **Don't use SSL or choose a certificate for SSL encryption later**. Click on **Next**.
5. Click on **Next** two times.
6. Click on **Install**.
7. When the install finishes, verify there were no problems listed then click on **Close**.
8. Reboot the computer.

#### Configure the NPS HRA to use the Certificate server

1. Log in with an administrative account
2. Open Server Manager
3. Expand **Roles** 🡪 **Network Policy and Access Services** 🡪 **Health Registration Authority** 🡪 **Certification Authority**.
4. Your Certification Authority should already be there. Click on it then Click on **Properties** in the **Action** pane on the right.
5. Click on the radio button next to **Use enterprise certification authority**
6. Click on the drop-down box under **Authenticated compliant certificate template**. Select **SystemHealthAuthentication** from the drop-down list.
7. Click on the drop-down box under **Anonymous compliant certificate template**. Select **SystemHealthAuthentication** from the drop-down list.
8. Click on **OK**.

#### Configure NAP

1. Click on Start and type in **nps.msc** (or **Start** 🡪 **Administrative Tools** 🡪 **Network Policy Server**)
2. Click on the link labeled **Configure NAP**.
3. Under **Select Network Connection Method**, **select IPSEC with Health Registration Authority**. Leave the name set to **NAP IPSEC with HRA**. Click on **Next**.
4. On the **Specify NAP Enforcement Servers Running HRA** page, click **Next** (we are not using RADIUS).
5. On the **Configure Machine Groups** page click **Next**.
6. On the **Define NAP Health Policy** page, verify there are checks in the checkboxes next to **Windows Security Health Validator** and **Enable auto-remediation of client computers**. Click **Next**.
7. On the **Completing NAP Enforcement Policy and RADIUS Client Configuration** page, grab a screenshot to include with your lab report.
8. Click on Finish

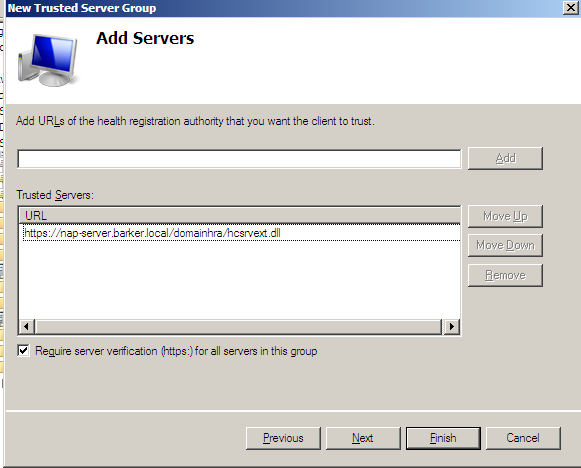
#### Configure System Health Validator to look at the Windows Firewall only

1. In the NPS console, expand **Network Access Protection** 🡪 **System Health Validators**
2. Double-click on **Windows Security Health Validator** in the details pane to open it.
3. Click in **Settings** under **Settings**.
4. Double-click on **Default Configuration** to edit it.
5. Make sure all check marks are removed except **A firewall is enabled for all network connections**.
6. Click on **OK**.

#### Configure Group Policy and filter for NAP client computer group

1. Click on Start and type in **gpmc.msc** (or **Start** 🡪 **Administrative tools** 🡪 **Group Policy Management**).
2. Expand **Forest** 🡪 **Domains** 🡪 Domain name. Right-click on the domain name and select **Create GPO in this domain, and Link it here…**
3. Name the GPO **NAP client configuration**. Click on **OK**.
4. The GPO will appear under the domain name on the navigation pane on the left.
5. Click on the **NAP client configuration GPO**. In the details pane you will see a security filtering section.
6. In the Security Filtering section, click on **Authenticated Users** then click on the **Remove** button. Click on OK when asked to remove the delegated privilege.
7. Click on the **Add…** button
8. Type in **NAP client computers** and click on **OK**.
9. Right-click on the **NAP client configuration** GPO and select **Edit**.
10. Expand **Computer Configuration** 🡪 **Policies** 🡪 **Windows Settings** 🡪 **Security Settings** 🡪 **System Services.**
11. Find the **Network Access Protection Agent** service and double-click on it.
12. Click on the checkbox next to **Define this policy setting**. Select **Automatic** then click on **OK**.
13. Expand **Network Access Protection** 🡪 **NAP client Configuration** 🡪**Enforcement Clients**.
14. Double-click on **IPSec Relaying Party**. Put a check in the checkbox next to **Enable this enforcement client**.
15. Click on OK.
16. Expand **NAP Client Configuration** 🡪 **Health Registration Settings** 🡪 **Trusted Server Groups**.
17. Right-click on **Trusted Server Groups** and select **New**.
18. Under Group Name type in **Trusted HRA Server** and click on **Next**.
19. On the Add Servers page, type in **https://**, the FQDN of the NAP server, including the domain name; also include the string **/domainhra/hcsrvext.dll**. For example if your server name is NAP-server and the domain name is barker.local, the entry would be:

**https://nap-server.barker.local/domainhra/hcsrvext.dll**

****

**Entering the URL of the HSA**

1. Click on **Add.**
2. Make sure you typed in the URL correctly. If you typed it in wrong nothing will work.
3. Click on **Finish**
4. Expand **Computer Configuration** 🡪 **Policies** 🡪 **Administrative Templates** 🡪 **Windows Components** 🡪 **Security Center**.
5. Double-click on Turn on Security Center (Domain PCs only). Click on **Enabled** and select **OK**.
6. Close GPMC.

#### And the most painful part: verify the IIS certificate is valid. Fix the certificate if it isn't valid.

(REF: http://www.jwsecure.com/dan/2008/07/04/debugging-a-nap-hra-on-an-enterprise-ca/)

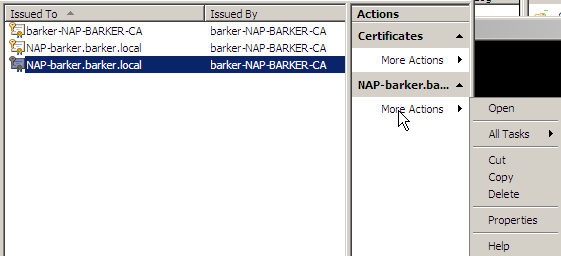
On another computer in your domain:

1. run gpupdate /force
2. open a web page and browse to the SSL website of the NAP server. (example: <https://nap-barker.barker.local>)

If you get an error "Internet Explorer cannot display the web page" you will need to perform the steps below. If you get a web page displaying a big IIS7 logo surrounded by welcome in different languages you can skip this section!

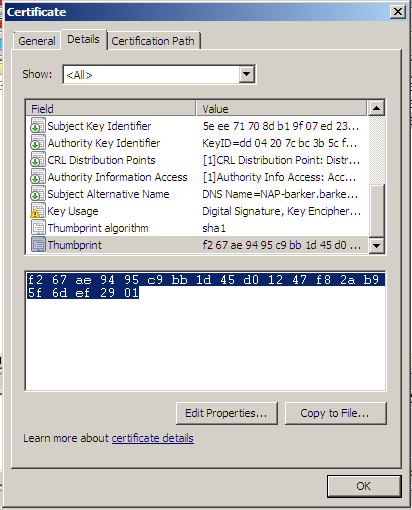
Find a certificate to use for IIS

1. Click on **Start** and type **mmc**
2. Click on **File** 🡪 **Add/Remove Snap-in**.
3. Click on **Certificates** and select **Add**. Click on the Radio button next to **Computer account** and click on **Next**. Leave the default **Local computer** and click on **Finish**. Click on **OK**.
4. In the Console tree, expand **Certificates (Local Computer)** 🡪 **Personal 🡪 Certificates**
5. In the details pane, use the horizontal scroll bar to find the **Intended purposes** column. (You may need to expand this column by clicking and dragging to the right on the divider between this column and another column).
6. Click on the line that has **Server Authentication** listed as one of the purposes. In the **Actions** pane (all the way to the right) click on **More Actions** below the name of the certificate.



**Clicking on More actions to look at the certificate properties**

1. Click on **Open**
2. Click on the **Details** tab.
3. Scroll down and click on **Thumbprint**. Highlight and copy (<Ctrl> + c) the contents of the thumbprint (you will need this to add the certificate to IIS)

****

**Copying the certificate thumbprint**

1. Paste the contents of the thumbprint in notepad. Keep for comparison.
2. Go to **Start 🡪 Administrative tools 🡪 Internet Information Services (IIS) Manager**.
3. Expand **ServerName 🡪 Sites 🡪 Default Web Site**.
4. In the Actions pane click on **Bindings. . .**
5. Click on **Add…**
6. From the drop down box under **Type:** select **https**. Under **SSL certificate**, choose the one that matches the hostname of your server. Click on **View…**, click on the **Details** tab and check the thumbprint against the thumbprint in notepad.
7. Click on **Close**.
8. Try going to the server's SSL site again, this time it should work.

****

**What you should see in Internet Explorer**

### Client computer

#### Test NAP configuration

1. Reboot your Windows 7 computer
2. Log into the Windows 7 client computer with an administrator account
3. Run **gpupdate /force** from the cmd prompt.
4. Click on Start and type in cmd. Type in **netsh nap client show grouppolicy**. You should see a series of entries. Make sure you see **Admin=Enabled** under **IPSec Relaying Party**

C:\Windows\system32>netsh nap client show grouppolicy

NAP client configuration (group policy):

----------------------------------------------------

NAP client configuration:

----------------------------------------------------

**Something went wrong. Check your NAP settings in the NAP client Configuration GPO**

C:\Windows\system32>netsh nap client show grouppolicy

NAP client configuration (group policy):

----------------------------------------------------

NAP client configuration:

----------------------------------------------------

Cryptographic service provider (CSP) = Microsoft RSA SChannel Cryptographic Provider, keylength = 2048

Hash algorithm = sha1RSA (1.3.14.3.2.29)

Enforcement clients:

----------------------------------------------------

Name = DHCP Quarantine Enforcement Client

ID = 79617

Admin = Disabled

Name = Remote Access Quarantine Enforcement Client

ID = 79618

Admin = Disabled

Name = IPSec Relying Party

ID = 79619

Admin = Enabled

Name = TS Gateway Quarantine Enforcement Client

ID = 79621

Admin = Disabled

Name = EAP Quarantine Enforcement Client

ID = 79623

Admin = Disabled

Client tracing:

----------------------------------------------------

State = Disabled

Level = Disabled

Trusted server group configuration:

----------------------------------------------------

Group = Trusted HRA Server

Require Https = Enabled

URL = https://NAP-server.barker.local/domainhra/hcsrvext.dll

Processing order = 1

Ok.

C:\Windows\system32>

**Something went right. good job!**

1. Next, type in **netsh nap client show state**. You should see a series of entries. Make sure you see **Initialized=Yes** under **IPSec Relaying Party** (highlighted in red below).

C:\Windows\system32>netsh nap client show state

Client state:

----------------------------------------------------

Name = Network Access Protection Client

Description = Microsoft Network Access Protection Client

Protocol version = 1.0

Status = Enabled

Restriction state = Not restricted

Troubleshooting URL =

Restriction start time =

Extended state =

Enforcement client state:

----------------------------------------------------

Id = 79617

Name = DHCP Quarantine Enforcement Client

Description = Provides DHCP based enforcement for NAP

Version = 1.0

Vendor name = Microsoft Corporation

Registration date =

Initialized = No

Id = 79618

Name = Remote Access Quarantine Enforcement Client

Description = Provides the quarantine enforcement for RAS Client

Version = 1.0

Vendor name = Microsoft Corporation

Registration date =

Initialized = No

Id = 79619

Name = IPSec Relying Party

Description = Provides IPSec based enforcement for Network Access Pro

tection

Version = 1.0

Vendor name = Microsoft Corporation

Registration date =

Initialized = Yes

Id = 79621

Name = TS Gateway Quarantine Enforcement Client

Description = Provides TS Gateway enforcement for NAP

Version = 1.0

Vendor name = Microsoft Corporation

Registration date =

Initialized = No

Id = 79623

Name = EAP Quarantine Enforcement Client

Description = Provides EAP based enforcement for NAP

Version = 1.0

Vendor name = Microsoft Corporation

Registration date =

Initialized = No

System health agent (SHA) state:

----------------------------------------------------

Id = 79744

Name = Windows Security Health Agent

Description = The Windows Security Health Agent checks the compliance

of a computer with an administrator-defined policy.

Version = 1.0

Vendor name = Microsoft Corporation

Registration date =

Initialized = Yes

Failure category = None

Remediation state = Success

Remediation percentage = 0

Fixup Message = (3237937214) - The Windows Security Health Agent has fi

nished updating its security state.

Compliance results =

Remediation results =

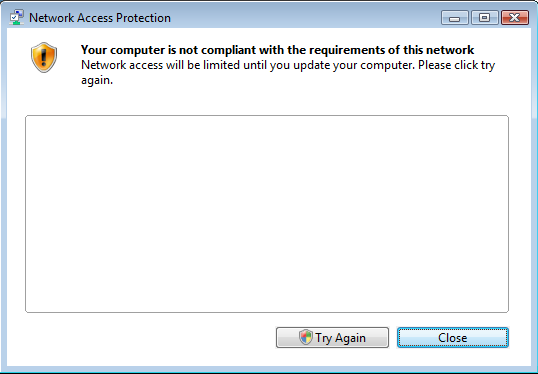
Ok.

C:\Windows\system32>

### Final verification NAP is working

#### On the Windows 7 computer (Client-Lastname)

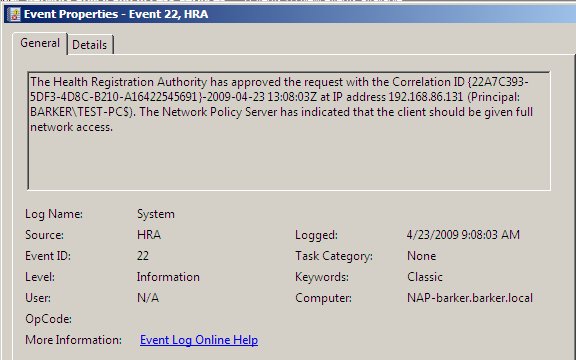
1. Click on **Start** and type **mmc**
2. Click on **File** 🡪 **Add/Remove Snap-in**.
3. Click on **Certificates** and select **Add**. Click on the Radio button next to **Computer account** and click on **Next**. Leave the default **Local computer** and click on **Finish**.
4. In the Console tree, expand **Certificates (Local Computer)** 🡪 **Personal 🡪 Certificates**
5. Verify there is a certificate present
6. Take a screenshot of the certificate and include it in your lab.
7. Click on Start and type in **napstat**. You will see a new icon in the system tray with a notification saying **This computer meets the requirements of this network**. Click on the icon to open the details window.
8. Take a screenshot of the notification window and include it in your lab report. (The screenshot below shows you what you get when the computer is not compliant).

****

**A computer not meeting the security requirements of the HRA.**

#### On the NAP server

1. In Server manager expand **Diagnostics** **🡪 Event Viewer** 🡪 **Custom Views** **🡪 Server Roles** 🡪 **Network Policy and Access Services**.
2. Look for EventID 22 - this indicates a client successfully used the HRA and has been approved.
3. Double-click on this event and take a screenshot. Include this screenshot in your lab.

****

**Example of a Client computer successfully contacting the HRA and getting approved**

END

## Troubleshooting:

### Certificate problems on IIS

C:\Users\cary0barker>netsh http show sslcert

SSL Certificate bindings:

-------------------------

IP:port : 0.0.0.0:443

Certificate Hash : 8dea252510e4c184b5ed86f8ced44f9b3bcf0d86

Application ID : {4dc3e181-e14b-4a21-b022-59fc669b0914}

Certificate Store Name : My

Verify Client Certificate Revocation : Enabled

Verify Revocation Using Cached Client Certificate Only : Disabled

Usage Check : Enabled

Revocation Freshness Time : 0

URL Retrieval Timeout : 0

Ctl Identifier : (null)

Ctl Store Name : (null)

DS Mapper Usage : Disabled

Negotiate Client Certificate : Disabled

C:\Users\cary0barker>certutil -store MY 8dea252510e4c184b5ed86f8ced44f9b3bcf0d86

MY

================ Certificate 1 ================

Serial Number: 3e8f1d5dc2f80c83446d0ca1ac9fc90a

Issuer: CN=barker-NAP-BARKER-CA, DC=barker, DC=local

NotBefore: 4/22/2009 8:43 PM

NotAfter: 4/22/2014 8:53 PM

Subject: CN=barker-NAP-BARKER-CA, DC=barker, DC=local

CA Version: V0.0

Signature matches Public Key

Root Certificate: Subject matches Issuer

Cert Hash(sha1): 8d ea 25 25 10 e4 c1 84 b5 ed 86 f8 ce d4 4f 9b 3b cf 0d 86

Key Container = barker-NAP-BARKER-CA

Provider = Microsoft Software Key Storage Provider

Encryption test FAILED

CertUtil: -store command completed successfully.

C:\Users\cary0barker>

RUN AS ADMINISTATOR

C:\Windows\system32>netsh http delete sslcert ipport=0.0.0.0:443

SSL Certificate successfully deleted

C:\Windows\system32>

C:\Windows\system32>netsh http add sslcert ipport=0.0.0.0:443 certhash=f267ae949

5c9bb1d45d01247f82ab95f6def2901 appid={4dc3e181-e14b-4a21-b022-59fc669b0914} cer

tstore=MY

SSL Certificate successfully added

C:\Windows\system32>netsh http show sslcert

SSL Certificate bindings:

-------------------------

IP:port : 0.0.0.0:443

Certificate Hash : f267ae9495c9bb1d45d01247f82ab95f6def2901

Application ID : {4dc3e181-e14b-4a21-b022-59fc669b0914}

Certificate Store Name : MY

Verify Client Certificate Revocation : Enabled

Verify Revocation Using Cached Client Certificate Only : Disabled

Usage Check : Enabled

Revocation Freshness Time : 0

URL Retrieval Timeout : 0

Ctl Identifier : (null)

Ctl Store Name : (null)

DS Mapper Usage : Disabled

Negotiate Client Certificate : Disabled

C:\Windows\system32>

### Client computers

Look in the Event log for NAP: Computer management 🡪 System Tools 🡪 Event Viewer 🡪 Windows Logs 🡪 Application and Services Logs 🡪 Microsoft 🡪 Windows 🡪 Network Access Protection 🡪 Operational.

Verify the NAP group policy is getting applied to the client computer (verify **NAP client configuration** is listed under Applies Group Policy Objects). From an administrative command prompt run **gpresult /SCOPE COMPUTER /R**

C:\Windows\system32>gpresult /SCOPE COMPUTER /R

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0

Copyright (C) Microsoft Corp. 1981-2001

Created On 4/23/2009 at 10:35:26 AM

RSOP data for BARKER\cary0barker on TEST-PC : Logging Mode

-----------------------------------------------------------

OS Configuration: Member Workstation

OS Version: 6.0.6001

Site Name: Default-First-Site-Name

Roaming Profile: N/A

Local Profile: C:\Users\cary0barker

Connected over a slow link?: No

COMPUTER SETTINGS

------------------

CN=TEST-PC,CN=Computers,DC=barker,DC=local

Last time Group Policy was applied: 4/23/2009 at 10:28:33 AM

Group Policy was applied from: DC-barker.barker.local

Group Policy slow link threshold: 500 kbps

Domain Name: BARKER

Domain Type: Windows 2000

Applied Group Policy Objects

-----------------------------

Default Domain Policy

NAP client configuration

The following GPOs were not applied because they were filtered out

-------------------------------------------------------------------

Local Group Policy

Filtering: Not Applied (Empty)

The computer is a part of the following security groups

-------------------------------------------------------

BUILTIN\Administrators

Everyone

BUILTIN\Users

NT AUTHORITY\NETWORK

NT AUTHORITY\Authenticated Users

This Organization

TEST-PC$

NAP client computers

Domain Computers

System Mandatory Level

C:\Windows\system32>

### On the NAP server

Look at the events for the HRA: In Server manager expand **Diagnostics** 🡪 **Custom Views** 🡪 **Network Policy and Access Services**

If there are no events, make sure that the **NETWORK SERVICE** and **NAP exempt computers** groups have the proper permissions to the **System Health Authentication** certificate template. Otherwise, Google any error events for find ways to resolve the problem(s).

### In general

* Make sure the system time on the computers in this lab are in synch. If the time is off by too far, certificates may not work and/or machines may have problems accessing the domain.
* Make sure the computers can PING each other
* Make sure DNS is working by using nslookup.

## Sites for help/troubleshooting:

http://www.microsoft.com/windowsserver2008/en/us/nap-main.aspx

http://technet.microsoft.com/en-us/library/cc730902.aspx

http://www.jwsecure.com/dan/2008/07/04/debugging-a-nap-hra-on-an-enterprise-ca/

http://technet.microsoft.com/en-us/library/dd314161.aspx

LAB 6 Evaluation Criteria

NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| COMPONENT | POINTS | | POINTS EARNED | COMMENTS |
| **Overall look and feel** | | | | |
| **Title Page** | 3 |  | | Title page neat, clean, includes lab # and lab title, Student’s name, date, e-mail address, class and section number are included. |
| **Table of Contents** | 2 |  | |  |
| **Executive Summary** | 5 |  | |  |
| **Professional Appearance** | 5 |  | | Professional overall look, font etc – readability spelling and grammar |
| **Header** | 2 |  | | – Lab Title |
| **Footer** | 2 |  | | – page, course # and student name |
| **Section Headings** | 2 |  | |  |
| **Numbered & Labeled Figures** | 2 |  | | Tables, Diagrams, Screenshots etc labeled and numbered |
| **Numbered Pages** | 2 |  | |  |
| **Content** | | | | |
| **Body Content** | 5 |  | | Clear and well organized point by point description of the actions taken  Each component should have its own section. |
| **Tables/Diagrams** | 5 |  | | Any tables and diagrams in 10-point Currier new font, with paragraph shading of White, Background 1, Darker 15% . A description must follow each table or diagram. |
| **System Configuration/Reports** | | | | |
| **Proper function of**  **Windows Vista**  **Windows 2008** | 10 |  | | The following configuration is in place:  System is functioning as it should at the end of the lab – (keep in mind that some labs may be designed to break something and/or make it not work like you would expect) |
| **Questions/Discussion addresses issues brought up in the Lab** | 15 |  | | Systems are properly configured for:   * Screenshots included * Certificate services and templates configured properly * NAP and HRA configured properly * Group policy properly configured |
| **Total:** | 60 |  | |  |