Tivoli Netcool Supports

Guide to

The SCOM2007 Probe

On Windows

by

Jim Hutchinson

Document release: 2.0

Table of Contents

1 Introduction

1.1 Overview

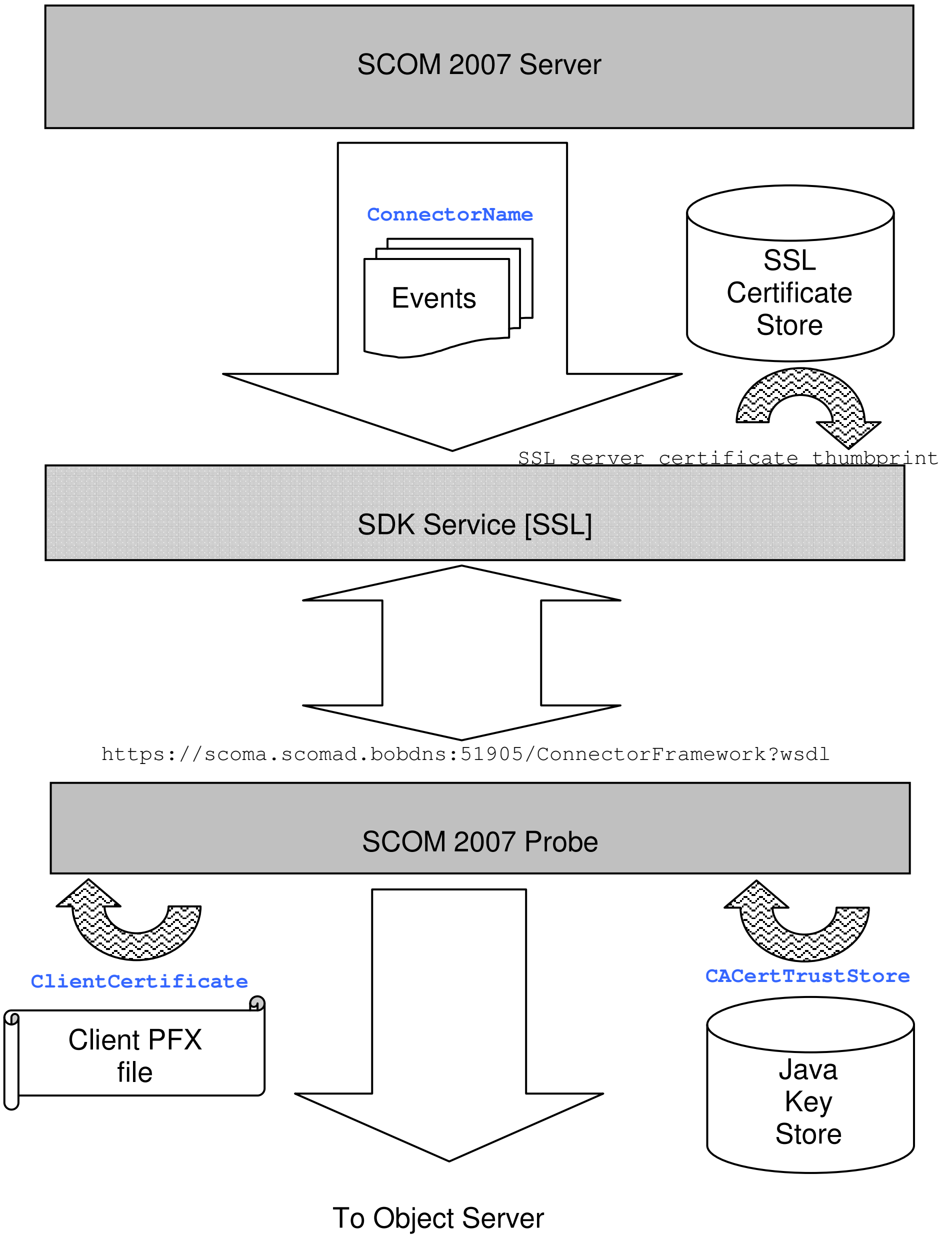
The SCOM 2007 probe is now only available for Windows. Other platform support was removed due to problems with configuration. Microsoft support should be contacted where issues related to SSL Certificates or SDK service configuration and patching.

The SCOM 2007 probe is designed to connect to the SCOM 2007 servers SDK Service [web service] and includes bi-directional features provided by a command line interface. Connectivity to the SDK Service is via SSL [only] and requires the configuration of both Client and Server SSL Certificates. Once connected the probe is sent data by the SCOM 2007 Server based upon the ConnectorName specified in the SCOM 2007 probes properties file.

Support for Windows 2008 and 64-bit Windows was introduced in the latest release of the probe, although it is recommended that 32-bit java is used exclusively, where possible.

Issues have been observed when the SCOM 2007 probe is installed locally on Windows 2008 64-bit servers. In this environment it is recommended that the probe is configured remotely, ideally in a 32-bit environment and if required, migrated onto the SCOM 2007 server after preliminary testing.

SCOM 2007 Server and Probe interaction



2 SCOM2007 probe installation

2.1 Patch Dependencies

IBM patches

probe-nonnative-base-10 or above
probe-command-port-3 or above

Third party patches

Java 1.5
JAXWS RI 2.1.1
WSIT 1.0 (milestone 4)
Unrestricted JCE Policy files for SDK 1.4 (for AIX)

Perl 5.6 or later for the command line interface tools used by the desktops

2.2 Installation

The SCOM 2007 probes documentation and readme files should be used to install and configure the probe. This document is intended to supplement this documentation and to provide enhanced troubleshooting techniques.

2.3 Java environment

2.3.1 Ensuring java version 1.5 is used

The probe user's path should include the version of java required by the probe. The PATH setting is seen when the 'set' command is run in a command window whilst logged in as the probe user.

2.3.2 Required JARS

The required jar files should be placed in a discrete SCOM probe directory to improve troubleshooting and maintenance.

Required JARS:-

JAXWS 2.1.1 :

- activation.jar
- jaxb-api.jar
- jaxb-impl.jar
- jaxb-xjc.jar
- jsr173_api.jar
- sjsxp.jar

WSIT 1.0

- webservices-api.jar
- webservices-extra-api.jar
- webservices-extra.jar
- webservices-rt.jar
- webservices-tools.jar

3 SCOM2007 probe configuration

3.1 Windows BAT script

If problems are experienced when running the probe from the command-line, it is possible to check the systems configuration by copying and editing the probes bat script found in %OMNIHOME%\probes\win32. Ensure that the original file is backed-up before making any edits.

The recommended configuration is provided in the appendix for completeness.

Create a new directory in the C: directory for use by the SCOM 2007 probe.
C:\ SCOM2007PROBE

Create and install the required jar files in a sub-directory, then update the CLASSPATH setting in the BAT script.
e.g.
C:\ SCOM2007PROBE\JARS

Create a new log directory to log debug messages to and update the property file accordingly;
e,g,
C:\ SCOM2007PROBE\DEBUG

Create a new directory to store the SSL certificates and keystores in;
e.g.
C:\ SCOM2007PROBE\SSL

3.2 Windows Services

Once the probe is tested from the command line and confirmed as working, it can be installed under Windows service or added to process autoimation.

e.g.

```
nco_p_scom2007 /install -propsfile C:\SCOM2007PROBE\scom2007.props
```

4 Debugging

There are three types of debugging available;

- Normal Probe
- Non-native Probe
- Java SSL handshake

4.1 Probe Log File

- The log file messages are self-explanatory except the Error: message that indicates something is not right with the connection to the specified SCOM 2007 server(s);

```
Error: Unable to get events: The probe couldn't
connect to any of the Scom2007 servers specified in
the hosts file
```

This message indicates a problem with accessing the SCOM 2007 server or an issue with the SSL Certificates being used by the client and/or server.

- Check connectivity to the SDK server from the probe host

  ping host / telnet host port / Internet Explorer to SDK service

- Enable Java SSL debugging if the SDK service is available

4.2 Non-native Probe logs

4.2.1 Enabling

In order to troubleshoot the java part of the SCOM 2007 probe, the non-native logging needs to be increased to debug. To do this set the two log file paths and enable debugging as follows;

```
NCO_P_NONNATIVE_TRANSCRIPT=C:\SCOM2007PROBE\DEBUG\nonnative.log
NDE_FORCE_LOG_MODULE=C:\SCOM2007PROBE\DEBUG\nde_forced.log
NDE_DEFAULT_LOG_LEVEL=debug
```

These environment variables are set using the Windows user interface as normal.

Only new command windows will use the new settings. The ‘set’ command can be used to check that they are set correctly before attempting to run the probe from the command line.

4.3 Java Debuging

4.3.1 Enabling Java SSL debugging

The SCOM 2007 probe runs java which accepts SSL debug options for SSL;

```
REM *** args to execute the probe
set PROGARGS=javaw -Djavax.net.debug=ssl:handshake:verbose
```

4.3.2 Enabling Full Java debugging

The SCOM 2007 probe also accepts the full [all] debug option which can be used for more in depth debugging and includes SSL debug logging;

```
REM *** args to execute the probe
set PROGARGS=javaw -Djavax.net.debug=all:handshake:verbose
```

4.4 Useful ‘grep’ commands

4.4.1 Looking for error messages

```
grep –i error: nonnative.log
```

```
Error: Failed to create ConnectorFrameworkDataAccess object :
javax.xml.ws.WebServiceException: Failed to access the WSDL at:
https://scoma.scomad.bobdns:51905/ConnectorFramework?wsdl. It failed with:
Error: Failed to connect to SCOM 2007 interface
Error: Unable to get events: The probe couldn't connect to any of the Scom2007
servers specified in the hosts file
```

4.4.2 Confirming SSL Client certificate is available

```
grep –i found nonnative.log
```

```
found key for : 1
Found trusted certificate:
```

4.4.3 Examining Java SSL handshakes

```
grep '\*\*\*' nonnative.log
```

```
*** ClientHello, TLSv1
*** ServerHello, TLSv1
*** Certificate chain
*** CertificateRequest
*** ServerHelloDone
*** Certificate chain
*** ClientKeyExchange, RSA PreMasterSecret, TLSv1
*** Finished
*** Finished
*** ClientHello, TLSv1
*** ServerHello, TLSv1
*** Finished
*** Finished
*** ClientHello, TLSv1
*** ServerHello, TLSv1
*** Finished
*** Finished
```

```
Ignoring “***” and "Unknown command" lines
```

5 Microsoft Certificate Authority Certificates

The following example is for the creation of Microsoft CA certificates on a tiered Certificate Authority.

	SCOMA	SCOM1
CA Server Type	Root CA	Issuing CA
SCOM 2007 Server	Yes	
SDK Service	Yes	
Domain Server	Yes	

Name	Example
Issuing CA hostname	SCOM1
SDK Service hostname	SCOMA
SDK Service FQDN	SCOMA.SCOMAD.bobdns
UPN	scomuser
E-mail address	scomuser@SCOMAD.bobdns

5.1 *User certificate generation:*

5.1.1 User Template Generation

On the Issuing CA [SCOM1] perform the following steps :

- Open the “Certification Authority” tool (under “Administrative Tools”)
- Select “Certificate Templates”
- Right-click and select “Manage”
- Select the “**User**” template from the list of templates
- Right-click and select “Duplicate Template”
- Name the new template e.g. “Probe User”
- The following options are selected under the TAB’s :
    - General :
        - “Publish certificate in Active Directory”
    - Request Handling (**allow export**):
        - Purpose is “Signature and encryption”
        - “Include symmetric algorithms allowed by the subject”
        - Minimum Key size is 1024
        - “**Allow private key to be exported**” [➽]
        - “**Enroll subject without requiring any user input**” [➽]
    - Subject Name :
        - “Build from this Active Directory information”
        - Subject name format : ‘Fully Distinguished Name’
        - Include e-mail name in subject name [➽]
        - E-mail name [➽]
        - User principal name (UPN) [➽]
    - Issuance Requirements : nothing
    - Superseded Templates : nothing
    - Extensions : the following extensions are included
        - Application Policies
        - Certificate Template Information
        - Issuance Policies
        - Key Usage
    - Security (**add enrol to probe user**): [➽]
        - Add the probe user to the list of Group and User names e.g. scomuser (scomuser@SCOMAD.bobdns)
          Such that the assigned user (scomuser) has the following permissions : read [➽]/write [➽]/**enroll** [➽]

Click Apply and then OK

5.1.2 Client Certificate Option

To Create the newly created option (SCOM 2007 Probe User) in the Issuing CA server:

- Select the “Certificate Templates” in the Certificate Authority Tool
- Select ‘New’, and select ‘Certificate Template’
- Select the newly created template, e.g. SCOM 2007 Probe User
- Select ok

To force propagation of the template, perform the following steps :

- At the root of the “Certification Authority” Tool, select the Issuing CA e.g. “SCOM1”
- Right-click and select “All Tasks” -> “Stop Service”.
- Start the Issuing CA service up again, by right-clicking on the Issuing CA e.g. “SCOM1” and selecting “All Tasks” -> “Start Service”.
- On a command-line, run : `gupdate /force`

5.1.3 Generate Client Certificate

To generate a client certificate based on the new template:

- On the **probe server** or other computer within the **CA's domain** as the **user** to issue the certificate for.

  e.g. on hostname SCOMA as user scomuser

- Open a browser window and go to the **Issuing CA's** URL :

  e.g. http://scom1.scomad.bobdns/certsrv

- Select "Request a certificate"
- Select "Advanced certificate request"
- Select "Create and submit a request to this CA"
- In the 'Advanced Certificate Request window, select the newly created certificate template, e.g. 'Probe User'
- Keep the default values, and select "Submit"
- In the following page, click "Install this certificate"

The certificate should then appear in the Certificate snap-in under 'Local User'.

This certificate needs to be exported to be used by the probe locally or on a remote host.

- Select the certificate, and right-click on it, then select "All tasks" and "Export"
- In the pop-up window, select "Yes, export the private key"
- Under "Export File Format", "Personal Information Exchange – PKCS #12 (.PFX)" should be selected [➼]
- Select "Include all certificates in the certification path if possible" [➼]
- Select "Enable strong protection" [➼]
- Under "Password", type-in an export password (this password will be the one used by the probe property **ClientCertificatePassword** after it is encrypted using nco_g_crypt)

  e.g. netcool
- Specify a filename, and the certificate will be exported (Probe property **ClientCertificate**).

  e.g. SCOMProbeUserCert.pfx

5.2 Server certificate generation

5.2.1 Server Template Generation

As with the procedure described in Client certificate generation, create a template on the Issuing CA (e.g. SCOM1) by duplicating a standard template, in this case the “Web Server” template.

e.g. “SDK Web Server”

On the Issuing CA [SCOM1] perform the following steps :

- Open the “Certification Authority” tool (under “Administrative Tools”)
- Select “Certificate Templates”
- Right-click and select “Manage”
- Select the “Web Server” template from the list of templates
- Right-click and select “Duplicate Template”
- Name the new template e.g. “SDK Web Server”
- General : keep the default
- Request Handling (allow export) :
    - Purpose should be “Signature and encryption”
    - Minimum key size should be : 1024
    - **Select “Allow private key to be exported” [➽]**
- Subject Name :
    - “Supply in the request” should be selected
- Issuance Requirements : nothing
- Superseded Templates : nothing
- Extensions : the following extensions are included
    - Application policies (Server Authentication)
    - Certificate Template Information
    - Issuance Policies
    - Key Usage
- Security (**add enroll**/**add hostname**):
    - The **SDK Service** user (e.g. **scomuser**)
      read [➽],
      write[➽]
      enroll [➽]
    - Add the **hostname** of the **SDK service** server (e.g. **SCOMA)**
      read [➽],
      write[➽]
      enroll [➽]

Click Apply and then OK

5.2.2 Server Certificate Option

To Create the template option in the Issuing CA server:

- Select the “Certificate Templates” in the Certificate Authority Window
- Select ‘New’, and select ‘Certificate Template’
- Select the newly created template, e.g. SDK Service Web Server
- Select ok

To force propagation of the template, perform the following steps :

- At the root of the “Certification Authority” Tool, select the Issuing CA e.g. “SCOM1”
- Right-click and select “All Tasks” -> “Stop Service”.
- Start the Issuing CA service up again, by right-clicking on the Issuing CA e.g. “SCOM1” and selecting “All Tasks” -> “Start Service”.
- On a command-line, run : `gupdate /force`

5.2.3 Generate Server Certificate

To generate a server certificate based on the new template:

On the **SDK service server** (SCOMA) as the **SDK Service user** (scomuser):

- Open the Issuing CA’s web page :
  e.g. http://scom1.scomad.bobdns/certsrv
- Select “Request a certificate”
- Select “Advanced certificate request”
- Select “Create and submit a request to this CA”
- In the “Advanced Certificate Request” page, select the following options :
  - Certificate Template : select the newly created template
    e.g. “SDK Web Server”
  - Specify the “Identifying information for offline template:”
    e.g. FQDN and user mail address for this example would be;

    Name : SCOMA.SCOMAD.bobdns

    E-mail : scomuser@SCOMAD.bobdns

    Company : IBM

    Department : Tivoli

    City : London

    State : England

    Country : GB
  - **Mark Keys as exportable [➽]**
  - **Under “Key Options”, click “Store certificate in local computer” [➽]**
  - Under “Additional options:”, specify the FQDN (DNS) attribute in the Attributes field : (CMC [*] / SHA-1)
    - **SAN:dns=SCOMA.SCOMAD.bobdns**
- Click “Submit”, the certificate is installed in the Certificate snap-in under “Local Computer”

5.3 SSL Certificate Deployment

5.3.1 CA keystore File

- Download the RootCA certificate

Open the RootCA webpage on the RootCA machine with a browser.

e.g. on SCOMA, the url is : http://scoma.scomad.bobdns/certsrv

Select the following task :

“**Download a CA certificate, certificate chain, or CRL**”

In the webpage, select the Root CA in the “CA certificate” list.

The “Encoding method” selected should be “DER”.

Select the “Download CA certificate” option.

In the pop-up window, select “save” and save the file on the computer.

The default name for the certificate is : certnew.cer

- Import the CA certificate into a CA keystore

Run the keytool command :

```
keytool -import -trustcacerts -alias RootCA -file certnew.cer -keystore
MSCACERTS
Enter keystore password:  changeit
Owner: CN=EnterpriseRootCA, DC=SCOMAD, DC=bobdns
Issuer: CN=EnterpriseRootCA, DC=SCOMAD, DC=bobdns
Serial number: 798302fe72406dab49231ad581ba4e01
Valid from: Wed Jul 02 11:25:10 BST 2008 until: Tue Jul 02 11:32:43 BST
2013
Certificate fingerprints:
         MD5:  01:10:2D:33:53:27:76:F8:22:0C:28:07:00:90:8F:77
         SHA1: 93:A8:39:66:C4:C4:31:9D:B5:E3:29:48:6F:01:04:57:BC:31:BD:E8
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

5.3.2 SDK Service SSL Certificate

To use the server certificate for the SDK Service refer to the SCOM 2007 probe documentation for full details of this procedure:

Extract the thumbprint string from the SDK Service server certificate using the Microsoft SSL Certificate GUI [run-> mmc];

e.g.

```
SCOMA.SCOMAD.bobdns -> c4411fcff88be2b6234a030673ec9586381b1429
```

This server certificate thumbprint is referenced in the probe documentation;

e.g. for an SDK Service running on port `51905`

```
httpcfg query ssl
httpcfg delete  ssl -i 0.0.0.0:51905
httpcfg set  ssl -i 0.0.0.0:51905 -h c4411fcff88be2b6234a030673ec9586381b1429 -
n LOCAL_MACHINE -c MY -f 2
```

Check that the SDK service is available by accessing the Connector Framework from a web browser logged in as the SDK service user (**scomuser**). Ensure that the browser is configured correctly so that pages are always reread rather than read from a cache.

e.g.

https://scoma.scomad.bobdns:51905/ConnectorFramework?wsdl

5.3.3 SCOM 2007 Server Certificate locations

Examples SSL Certificate locations:-

Certificates (Local Computer) - Personal - Certificates

- SCOM 2007 Server Certificate
- Root CA Server Certificate

Certificates (Current User) - Personal - Certificates

- SCOM 2007 Server Certificate
- Root CA Server Certificate
- SCOM 2007 probe user Client Certificate

6 Example Probe Configuration

6.1.1 scom2007.hosts

```
scoma.scomad.bobdns:51905
```

6.1.2 scom2007.props

```
HostsFile                      : "C:\\Program
Files\\IBM\\Tivoli\\netcool\\omnibus\\probes \\scom2007.hosts"
RegistrationIdRecoveryFile     : "C:\\Program Files\\IBM\\Tivoli\\netcool\\omnibus
\\var\\scom2007.reco"
CACertTrustStore               : "C:\\SCOM2007PROBE\\SSL\\CACERTS"
ClientCertificate              : "C:\\SCOM2007PROBE\\SSL\\client.pfx"
ClientCertificatePassword      : "BHBGFJFGHLDACLCGCOFPBACG"
CleanUpOnShutdown              : "true"
ConnectorName                  : "Netcool probe"
```

6.1.3 Using nco_g_crypt

If the certificate password contains non-alpha-numeric characters then the password needs to be entered on the command line;

e.g.

```
nco_g_crypt
Password: *!£$%^&*
HOAIEPENFEBC
```

7 Windows 2008 Considerations

7.1 Netsh replaces httpcfg

The equivalent netsh command to attach the server certificate thumbprint is;

```
netsh http show sslcert
netsh http delete sslcert ipport=0.0.0.0:51905
netsh http add sslcert ipport=0.0.0.0:51905
certhash=0000000000003ed9cd0c315bbb6dc1c08da5e6 appid={GUID}
clientcertnegotiation=enable
```

The 'appid' parameter is a GUID that is used to identify the owning application, in this case the SDK service.

The AppID GUID that corresponds to the named executable is obtained via the regedit tool.

Registry Entry [run->***regedit***]

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\<**Executable_name**>

Other equivalent netsh commands are:

```
netsh http show sslcert
netsh http delete sslcert ipport=0.0.0.0:51905
```

7.2 Local or Remote SCOM 2007 probe?

Microsoft Support have recommend that clients [SCOM 2007 probe] are installed remote from the SCOM 2007 SDK service. This is due to problems with internal communications between the client and server, after the SSL authentications are completed. The symptom for the probe is for it not to be able to connect to the SCOM 2007 after a given period [minutes], with the probe reporting connection problems;

- ‘Connection has been shutdown’
- ‘Connection reset’

7.3 Number of events issue

There is a known bug with the way the SCOM 2007 SDK server interacts with the SCOM 2007 probe, which causes a problem when large amounts of events need to be passed through the connection [the latest test fix patch is required to resolve this issue];

```
APAR IZ98802 - Probe now poll the alerts base on number set in
BatchSize property
```

8 Appendix

8.1 Useful links

Creating PKCS#12 certificates with Microsoft CA's;

http://technet.microsoft.com/en-us/library/cc135718.aspx

Microsoft Support Recommended links;

Example SSL certificate creation;

How to add a Subject Alternative Name to a secure LDAP certificate

http://support.microsoft.com/kb/931351

Creating Certificate Requests Using the Certificate Enrolment Control and CryptoAPI

http://msdn.microsoft.com/en-us/library/ms867026.aspx

How to configure the SCOM 2007 server for SSL;

http://support.microsoft.com/kb/957562

SCOM 2007 server overview;

http://technet.microsoft.com/en-us/library/bb735400.aspx

8.2 Example SCOM 2007 Server : SDK Service

Directory : C:\program files\System Center Operations Manager 2007

Filename : Microsoft.Mom.Sdk.ServiceHost.exe.config

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
 <system.diagnostics>
  <sources>
   <source name="System.ServiceModel" switchValue="Information,
ActivityTracing"
    propagateActivity="true">
    <listeners>
     <add type="System.Diagnostics.DefaultTraceListener" name="Default">
      <filter type="" />
     </add>
     <add name="McfTracing">
      <filter type="" />
     </add>
    </listeners>
   </source>
   <source name="System.ServiceModel.MessageLogging" switchValue="Information,
ActivityTracing">
    <listeners>
     <add type="System.Diagnostics.DefaultTraceListener" name="Default">
      <filter type="" />
     </add>
     <add name="McfTracing">
      <filter type="" />
     </add>
    </listeners>
   </source>
  </sources>
  <sharedListeners>
   <add initializeData="c:\Microsoft.Mom.Sdk.ServiceHost_tracelog"
    type="System.Diagnostics.XmlWriterTraceListener, System, Version=2.0.0.0,
Culture=neutral, PublicKeyToken=b77a5c561934e089"
    name="McfTracing" traceOutputOptions="LogicalOperationStack, DateTime,
Timestamp, ProcessId, ThreadId, Callstack">
    <filter type="" />
   </add>
  </sharedListeners>
 </system.diagnostics>
    <runtime>
        <gcServer enabled="true"/>
    </runtime>
    <appSettings>
       <!-- use appSetting to configure base address provided by host -->
       <add key="baseAddressMcfV3"
value="https://scoma.SCOMAD.bobdns:51905/ConnectorFramework" />
    </appSettings>
    <system.serviceModel>
<diagnostics>
    <messageLogging logEntireMessage="true" logMalformedMessages="true"
        logMessagesAtServiceLevel="true" logMessagesAtTransportLevel="true" />
</diagnostics>
<bindings>
      <wsHttpBinding>
          <binding name="McfDefaultBinding"
maxReceivedMessageSize="2147483647">
              <readerQuotas maxDepth="2147483647"
maxStringContentLength="2147483647"
                  maxArrayLength="2147483647" maxBytesPerRead="2147483647"
maxNameTableCharCount="2147483647" />
              <security mode="Transport">
```

```
                  <transport clientCredentialType="Certificate" />
              </security>
          </binding>
      </wsHttpBinding>
  </bindings>
        <behaviors>
            <serviceBehaviors>
                <behavior name="ConnectorFrameworkServiceBehavior">
                    <serviceDebug httpHelpPageEnabled="true"
includeExceptionDetailInFaults="true" />
                    <serviceMetadata httpGetEnabled="true"
httpGetUrl="http://scoma.SCOMAD.bobdns:51906/ConnectorFramework"
                        httpsGetEnabled="true" />
                    <serviceThrottling maxConcurrentSessions="1000" />
                    <serviceCredentials>
                        <clientCertificate>
                            <authentication
mapClientCertificateToWindowsAccount="true" />
                        </clientCertificate>
                    </serviceCredentials>
                </behavior>
            </serviceBehaviors>
        </behaviors>
        <services>
            <service behaviorConfiguration="ConnectorFrameworkServiceBehavior"

name="Microsoft.EnterpriseManagement.ConnectorFramework.ServiceDataLayer.Connec
torFrameworkDataAccess">
                <endpoint address="" binding="wsHttpBinding"
bindingConfiguration="McfDefaultBinding"
                    name="Main"
contract="Microsoft.EnterpriseManagement.ConnectorFramework.IConnectorFramework
" />
            </service>
        </services>
    </system.serviceModel>
</configuration>
```

8.3 Example Windows BAT script

```
@echo off

setlocal
REM *** MUST ADD JRE TO PATH FOR SERVICES
set PATH=C:\Program Files\Java\jre1.5.0_15\bin;%PATH%

REM *** Enable debugging as required
REM SET NCO_P_NONNATIVE_TRANSCRIPT=C:\SCOM2007PROBE\DEBUG\nonnative.log
REM SET NDE_FORCE_LOG_MODULE=C:\SCOM2007PROBE\DEBUG\nde_forced.log
REM SET NDE_DEFAULT_LOG_LEVEL=debug

REM *** remove spaces from OMNIHOME variable or they screw things up
call :get_new_omnihome "%OMNIHOME%"

REM *** set up classpath variables for the MOM probe

if exist "%OMNIHOME%\probes\win32\nco_p_scom2007.jar" (
set CLASS_DIR=%NEWOMNIHOME%\probes\win32
)

set PROBE_CLASSPATH=%CLASS_DIR%\nco_p_scom2007.jar
set NSPROBE_CLASSPATH=%CLASS_DIR%\NSProbe.jar
set COMMANDPORT_CLASSPATH=%CLASS_DIR%\CommandPort.jar

REM *** Hard code SCOM_INCLUDES
set SCOM_INCLUDES=C:\SCOM2007PROBE\JARS\activation.jar
set SCOM_INCLUDES=C:\SCOM2007PROBE\JARS\jaxb-api.jar;%SCOM_INCLUDES%
set SCOM_INCLUDES=C:\SCOM2007PROBE\JARS\jaxb-impl.jar;%SCOM_INCLUDES%
set SCOM_INCLUDES=C:\SCOM2007PROBE\JARS\jaxb-xjc.jar;%SCOM_INCLUDES%
set SCOM_INCLUDES=C:\SCOM2007PROBE\JARS\jsr173_api.jar;%SCOM_INCLUDES%
set SCOM_INCLUDES=C:\SCOM2007PROBE\JARS\sjsxp.jar;%SCOM_INCLUDES%
set SCOM_INCLUDES=C:\SCOM2007PROBE\JARS\webservices-api.jar;%SCOM_INCLUDES%
set SCOM_INCLUDES=C:\SCOM2007PROBE\JARS\webservices-extra-api.jar;%SCOM_INCLUDES%
set SCOM_INCLUDES=C:\SCOM2007PROBE\JARS\webservices-extra.jar;%SCOM_INCLUDES%
set SCOM_INCLUDES=C:\SCOM2007PROBE\JARS\webservices-rt.jar;%SCOM_INCLUDES%
set SCOM_INCLUDES=C:\SCOM2007PROBE\JARS\webservices-tools.jar;%SCOM_INCLUDES%

REM *** args to execute the probe
set PROGARGS=javaw -Djavax.net.debug=ssl:handshake:verbose -Xrs -cp
%PROBE_CLASSPATH%;%NSPROBE_CLASSPATH%;%SCOM_INCLUDES%;%COMMANDPORT_CLASSPATH% nco_p_scom2007

REM *** don't need these any more, so ditch them in case we run over the windows limit on env
vars (!)
set CLASS_DIR=
set PROBE_CLASSPATH=
set NSPROBE_CLASSPATH=
set AXIS_CLASSPATH=

REM *** default value for the instance (if not requested)
set INSTANCEOPTIONS=/INSTANCE NCOSCOM2007Probe

REM *** service related options requested by the user
set SERVICEOPTIONS=

REM *** removal of service options requested by the user
set REMOVEOPTIONS=

REM *** additional commmand line actions used on install only
set CMDLINE=

REM *** args specified by user of the script (e.g command line args)
set EXTRAARGS=

REM *** analyse the command line arguments
REM *** Beginning of arg loop
:loopargs

if "%1" EQU "" (
       goto endofargs
```

```
)

if /i "%1" EQU "/INSTALL" (
        set SERVICEOPTIONS=%SERVICEOPTIONS% %1
        set CMDLINE=/CMDLINE
        shift
        goto loopargs
)
if /i "%1" EQU "/REMOVE" (
        set REMOVEOPTIONS=%REMOVEOPTIONS% %1
        shift
        goto loopargs
)
if /i "%1" EQU "/NOAUTO" (
        set SERVICEOPTIONS=%SERVICEOPTIONS% %1
        shift
        goto loopargs
)
if /i "%1" EQU "/DEPEND" (
        set SERVICEOPTIONS=%SERVICEOPTIONS% %1 %2
        shift
        shift
        goto loopargs
)
if /i "%1" EQU "/GROUP" (
        set SERVICEOPTIONS=%SERVICEOPTIONS% %1 %2
        shift
        shift
        goto loopargs
)
if /i "%1" EQU "/ACCOUNT" (
        set SERVICEOPTIONS=%SERVICEOPTIONS% %1 %2
        shift
        shift
        goto loopargs
)
if /i "%1" EQU "/PASSWORD" (
        set SERVICEOPTIONS=%SERVICEOPTIONS% %1 %2
        shift
        shift
        goto loopargs
)
if /i "%1" EQU "/INSTANCE" (
        set INSTANCEOPTIONS=%1 %2
        shift
        shift
        goto loopargs
)
if /i "%1" EQU "/CMDLINE" (
        REM *** %2 so we dont carry the word /CMDLINE (and remove the quotes, as we will
already have quotes around it)
        for %%v in (%2) do set UNQUOTED=%%v
        set EXTRAARGS=%EXTRAARGS% %UNQUOTED%
        shift
        shift
        goto loopargs
)
if /i "%1" EQU "/BACKOFF" (
        set SERVICEOPTIONS=%SERVICEOPTIONS% %1 %2
        shift
        shift
        goto loopargs
)

REM *** to get here, this must be nothing to with service args (and not CMDLINE args)
set EXTRAARGS=%EXTRAARGS% %1
shift
goto loopargs

:endofargs

REM  *** now install or run the probe as requested but with the probe's required classpath
arguments etc. added
if "%SERVICEOPTIONS%" EQU "" (
        REM *** no service options, so is it a request to remove the service?
        if "%REMOVEOPTIONS%" EQU "" (
                REM not remove so just run the probe as a console application
                nco_p_nonnative %PROGARGS% %EXTRAARGS%
        )  else (
                REM *** we want to remove the service
                nco_p_nonnative %REMOVEOPTIONS% %INSTANCEOPTIONS%
        )
) else (
        REM *** service options selected, so it must (and hopefully is!) install
        nco_p_nonnative %SERVICEOPTIONS% %INSTANCEOPTIONS% %CMDLINE% "%PROGARGS% %EXTRAARGS%"
)

goto :EOF

REM *** convert OMNIHOME into 8.3 notation
:get_new_omnihome
set NEWOMNIHOME=%~fs1
goto :EOF
```

8.4 Running the probe under Windows Services

Although the probe script has the right environment the system may not. In order to configure the system for the right settings you must consider the environment set within the bat script and the install command;

```
REM *** service options selected, so it must (and hopefully is!) install
nco_p_nonnative %SERVICEOPTIONS% %INSTANCEOPTIONS% %CMDLINE% "%PROGARGS% %EXTRAARGS%"
```

Therefore the system's environment must contain the java [javaw] path;

```
C:\Program Files\Java\jre1.5.0_15\bin
```

And the **`SCOM_INCLUDES`** variable must be added and include all the required JAR files;

```
C:\Program Files\Tivoli\netcool\omnibus\probes\win32\nco_p_scom2007.jar
C:\Program Files\Tivoli\netcool\omnibus\probes\win32\NSProbe.jar
C:\Program Files\Tivoli\netcool\omnibus\probes\win32\CommandPort.jar
C:\SCOM2007PROBE\JARS\activation.jar
C:\SCOM2007PROBE\JARS\jaxb-api.jar
C:\SCOM2007PROBE\JARS\jaxb-impl.jar
C:\SCOM2007PROBE\JARS\jaxb-xjc.jar
C:\SCOM2007PROBE\JARS\jsr173_api.jar
C:\SCOM2007PROBE\JARS\sjsxp.jar
C:\SCOM2007PROBE\JARS\webservices-api.jar
C:\SCOM2007PROBE\JARS\webservices-extra-api.jar
C:\SCOM2007PROBE\JARS\webservices-extra.jar
C:\SCOM2007PROBE\JARS\webservices-rt.jar
C:\SCOM2007PROBE\JARS\webservices-tools.jar
```

Additionally all the probe property paths must be explicitly set;

```
HostsFile                     : "C:\\Program
Files\\IBM\\Tivoli\\netcool\\omnibus\\probes\\scom2007.hosts"
RegistrationIdRecoveryFile    : "C:\\Program
Files\\IBM\\Tivoli\\netcool\\omnibus\\var\\scom2007.reco"
CACertTrustStore              : "C:\\SCOM2007PROBE\\SSL\\CACERTS"
ClientCertificate             : "C:\\SCOM2007PROBE\\SSL\\client.pfx"
ClientCertificatePassword     : "BHBGFJFGHLDACLCGCOFPBACG"
CleanUpOnShutdown             : "false"
ConnectorName                 : "Netcool probe"
```