Shibboleth Best Practice Guide Guidance for Installing and Running Shibboleth on Windows

Colin Bruce
Coventry University

18 September 2008

Contents

These guides have been prepared by organisations who participated in the JANET Shibboleth on Windows project. These guides are provided for general information purposes and are not intended to be definitive or exhaustive guides to the configuration, installation and implementation of Shibboleth On Windows.

Introduction

This document provides information that is intended to help those installing, configuring and testing Shibboleth on a Windows server. It is not an installation, configuration or testing guide – there are other documents that provide such information. Instead it is a document which provides additional information that may complement these guides.

Installation

Research

When deploying new hardware or software it is tempting to put the CDROM in a server and run setup. The installer is quick and easy to use. However, once Shibboleth is installed some configuration is required. This will be much easier if those carrying out the installation know and understand the terminology. Some useful sites to get a good understanding of Shibboleth are:

http://www.ukfederation.org.uk/
http://shibboleth.internet2.edu/
http://shibboleth.internet2.edu/get-started.html

Virtualisation

Consider using a virtual server rather than a physical server to run your Shibboleth Identity Provider (IDP). There are commercial and open source virtualisation systems. One example is Xen which is open source. A useful link about Xen is:

http://www.xen.org/

Collaboration

Involve colleagues from the Institution's Library or other e-Learning units at an early stage. They will probably be responsible for the user interface and will have to deal with any queries that arise from the implementation. They are also usually responsible for providing access to remote resources.

Network Requirements

Ports 80, 443, 8442 and 8443 need to be open in both directions for Shibboleth to work successfully. Port 443 provides https but any port can be used instead. However, it is often difficult to convince network people to open some other port for HTTPS traffic.

ISA Firewalls

Microsoft ISA is often used as a web proxy server. This can cause problems when HTTPS traffic is on a port other than port 443 or 563, for example the 8443 port that Shibboleth uses. On the face of it the problem is easily solved by creating new definitions for ports 8442 and 8443. For example we might create new port definitions for ports 8442 and 8443. Then it seems it is just a matter of creating ISA rules to allow traffic on these new ports through the firewall. However, this does not work. The solution is to change the "tunnel port range" to include the port values you wish to use. This can be done by running the following VB Script.

```
''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''
' Copyright (c) Microsoft Corporation. All rights reserved.
' THIS CODE IS MADE AVAILABLE AS IS, WITHOUT WARRANTY OF ANY KIND. THE ENTIRE
' RISK OF THE USE OR THE RESULTS FROM THE USE OF THIS CODE REMAINS WITH THE
' USER. USE AND REDISTRIBUTION OF THIS CODE, WITH OR WITHOUT MODIFICATION, IS
' HEREBY PERMITTED.
''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''
''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''
' This script creates a new tunnel port range containing a single user-specified
' port to allow clients to send requests, for example, SSL requests, to that
' port.
' This script can be run from a command prompt by entering the
' following command:
'     CScript AddTPRange.vbs RangeName PortNumber
''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''''
Option Explicit
```

```
' Define the constants needed.
Const Error_TypeMismatch = &HD
Const Error_AlreadyExists = &H800700B7
Const Error_OutOfRange = &H80070057

Main(WScript.Arguments)

Sub Main(args)
    If(args.Count <> 2) Then
        Usage()
    Else
       AddTPRange args(0), args(1)
    End If
End Sub

Sub AddTPRange(newRangeName, newTunnelPort)

    ' Create the root object.
    Dim root  ' The FPCLib.FPC root object
    Set root = CreateObject("FPC.Root")

    'Declare the other objects needed.
    Dim isaArray     ' An ISA Server array object
    Dim tpRanges     ' An FPCTunnelPortRanges collection
    Dim newRange     ' An FPCTunnelPortRange object
    Dim port         ' An Integer

    ' Get a reference to the array and to
    ' the collection of tunnel port ranges.
    Set isaArray = root.GetContainingArray()
    Set tpRanges = isaArray.ArrayPolicy.WebProxy.TunnelPortRanges

    ' Create a new tunnel port range.
    On Error Resume Next
    port = CDbl(newTunnelPort)
    If Err.Number = Error_TypeMismatch Then
        WScript.Echo "A number must be entered for the port to be included."
        WScript.Quit
    End If
    Err.Clear
    Set newRange = tpRanges.AddRange(newRangeName, port, port)
    If Err.Number = Error_AlreadyExists Then
       WScript.Echo "A port range with the name specified already exists."
       WScript.Quit
    ElseIf Err.Number = Error_OutOfRange Then
        WScript.Echo "The range of permissible ports is from 1 through 65535."
        WScript.Quit
    End If
    On Error GoTo 0

    ' Save the changes to the collection of tunnel port ranges
    ' with fResetRequiredServices set to True to restart the Firewall service.
    tpRanges.Save True
    WScript.Echo "Done!"
End Sub

Sub Usage()
    WScript.Echo "Usage:" & VbCrLf _
        & "  " & WScript.ScriptName & " RangeName TunnelPort" & VbCrLf _
        & "" & VbCrLf _
        & "  RangeName  - Name of the tunnel port range to be added" & VbCrLf _
        & "  TunnelPort - Port to be included in the new tunnel port range"
    WScript.Quit
End Sub
```

Further information about this and other scripts to show what ranges are in use or to delete ranges can be found in the Microsoft Technet article at:

http://technet.microsoft.com/en-us/library/cc302450.aspx

This article also includes example code which is shorter than the example shown above. However, the examples quoted in the articles do not appear to work. The one quoted above does.

Configuration

Forms Based Authentication
Many of the users of your Shibboleth Identity Provider will have limited IT experience. Consequently it is worth using forms based authentication rather than the default Windows login box. The Shibboleth on Windows installer configures this by default but it is worth modifying the form so that it is more suitable for non-IT people. For example, add links to your user registration system (if you have one) so that they can apply for an account if they don't have one already or reset their password. If you have an online help desk system, add a link to that as well. Remember that your colleagues who are using your identity provider may not be on your campus so you need to provide them with all the facilities they need in order to do their work remotely. Instructions for modifying the login page can be found in:

http://gilbert.dev.ja.net/groups/shib/wiki/702ee/Changing_the_Look_on_the_Login_Page.html

Attribute Release Policy
The attribute release policy determines what attributes are exposed and to which sites. In most cases the release policy allows a small number of attributes to be exposed to everyone. The global attribute release policy is defined in:

```
C:\Program Files\Internet2\IdP\etc\arps\arp.site.xml
```

assuming you installed Shibboleth in C:\Program Files. Different Service Providers may require various values in the attribute eduPersonEntitlement. However, some (e.g. EDUServ) cannot accept values in eduPersonEntitlement that they do not understand. As a result the attribute release policy for these attributes has to be modified for these providers so that they do not receive the attributes they do not understand. This can be done by creating a rule that blocks specific values to specific Service Providers. For example, suppose you release a value such as AAA#ShibGlobal to EDUServ and a value such as urn:mace:dir:entitlement:common-lib-terms to another Service Provider with both values in eduPersonEntitlement, so the full value of the attribute is:

```
AAA#ShibGlobal;urn:mace:dir:entitlement:common-lib-terms
```

EDUServ will treat this as an error since the string urn:mace:dir:entitlement:common-lib-terms does not match any of the attribute values that it understands. The solution is to block this value when the attribute is being exposed to EDUServ. This can be done by adding the following rule to the global Attribute Release Policy.

```
<Rule>
   <Description>Attribute Release Policy for EDUServ.</Description>
   <Target>
      <Requester>urn:mace:eduserv.org.uk:athens:federation:uk</Requester>
   </Target>
   <Attribute name="urn:mace:dir:attribute-def:eduPersonEntitlement">
      <Value release="deny">urn:mace:dir:entitlement:common-libterms</Value>
   </Attribute>
 </Rule>
```

The attribute value to be blocked (which in the example is underlined) may have to be changed to suit your particular installation.

Testing

Janet Test Sites
Use the JANET test sites once Shibboleth is installed and after making any changes. Two such sites are:

https://ledi.edina.ac.uk:8885/cgi-bin/printenv
https://target.iay.org.uk/secure/printenv.cgi

Be aware that there is a slight problem with the first site in that it does not show eduPersonEntitlement even though that attribute is exposed. The second site does show that attribute correctly.

Errors and Failures
It is likely that as your Identity Provider is developed there will be things that do not work as expected. For example, it might not authenticate correctly even though the correct password is being entered or an attribute that should be released is not doing so. This can be very frustrating and the log files that Shibboleth generates on the Identity Provider may not contain enough information to resolve the problem in some circumstances. However, the log files that the Service Provider you are testing against may be. When this happens it is useful to test against one of the test sites listed above and then contact the UK Federation Help Desk with the date and time that you carried out the test. They can usually provide the relevant extract from the logs they have gathered and that can be immensely useful when diagnosing errors and failures.

Running

Log Files
The Shibboleth log files are stored in the directory:

```
C:\Program Files\Internet2\IdP\logs
```

assuming the standard location C:\Program Files was used when installing the package. The amount of information written to these files is defined in the "<Logging>" section of the file `Idp.xml` in `C:\Program Files\Internet2\IdP\etc`. The default values are Warn and Info for "`ErrorLog level`" and "`TransactionLog`" level respectively. The amount of information recorded can be increased by changing both these values to "`Debug`". However, this can produce very large log files so once the issue being investigated has been resolved the values should be returned to their defaults.

Metadata File
The metadata file must be kept up to date. If it is not updated, Service Providers that have been added to the UK Federation will not be visible to people authorised by your Identity Provider. The installer automatically adds a scheduled task to download the metadata on an hourly basis but if some Service Providers are not available it is worth checking that this download is working and being done regularly.

Time Synchronization
Time synchronization is very important to Shibboleth. If the clocks on the Identity Provider and Services Provider differ by more than a few minutes, Shibboleth will be unable to authenticate users correctly. Even though people type their correct passwords they will be told that their password is incorrect. If your Shibboleth server is in a Windows Domain its clock is likely to be correct. However, if it is not and especially if it is a virtual server then some time synchronization system will be required. If you find that everyone is being told their password is wrong even though they are typing it very carefully, time synchronization is a possible cause of the problem.