Integrating a Shibboleth IdP with Microsoft Active Directory

Author: Ian Burgess

Contributors: Gemma O'Doherty & Joe Boyle

Version 1.0

29 July 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.

Document Scope

This document is a low-level technical document which discusses and describes a process for integrating a Shibboleth IdP with Microsoft Active Directory.

Introduction to the C2k Enterprise Active Directory

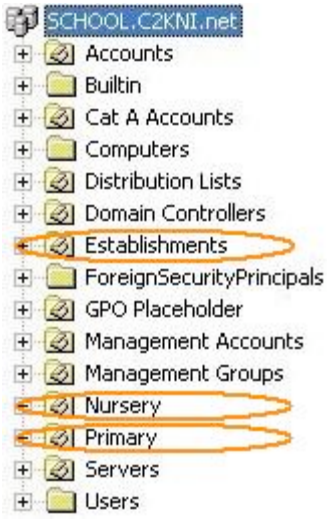
Before delving into the integration process it is worthwhile describing the environment which the authors integrated into the UK Federation. By understanding the starting point and subsequent integration it is hoped that readers will understand the rationale for certain decisions and be able to adapt the process to suit their own particular needs.

C2k is responsible for the provision of an information and communications technology (ICT) managed service to all schools in Northern Ireland. The managed service comprises of >80,000 networked computers, together with a rich mix of educational content and services.

From a technology perspective, C2k utilises a single directory service for authenticating and authorising all students, teaching staff and non-teaching staff. One Microsoft Active Directory forest with two domains hosts all necessary user accounts, computer accounts, security groups and distribution groups:

- *1 x forest "C2k EAD"*
  - *1 x domain "c2kni.net" - contains administrative user accounts*
  - *1 x domain "school.c2kni.net" - contains the bulk of accounts and groups*

The OU hierarchy of the "school.c2kni.net" domain contains a number of placeholder OUs which categorise the high-level user communities:



Name	Contains
Establishments	*Objects for Post Primary and Special Needs Schools*
Nursery	*Objects for Nursery Schools*
Primary	*Objects for Primary Schools*

Figure 1: 1st Level OU Hierarchy in the C2k EAD

A standardised naming convention and sub-structure is implemented underneath each of the three 1st-level placeholder OUs.

Each school in Northern Ireland is assigned a 7-digit DENI number. Table 1 shows the breakdown and values used for the first three digits in a DENI number.

1st digit	2nd digit	3rd digit
	0 Primary	
1 Belfast	1 Nursery	1 Controlled
2 Western Area	2 Secondary/Intermediate	2 Voluntary
3 North Eastern	3 Special	3 Voluntary Maintained
4 South Eastern	4 Grammar	
5 Southern		

Table 1: DENI Number Breakdown

The school DENI number(s) are used to create 2nd-level placeholder OUs underneath the relevant parent. Figure 2 shows the OU hierarchy for the school with the DENI number 4410085:

Figure 2: Sample School illustrating 2nd and 3rd Level OUs in the C2k EAD

The user accounts for Teaching Staff and Non-Teaching Staff exist in the relevant OUs.

The storage location for user accounts for Students is slightly more complicated with further intake year OUs being utilised underneath the Students OU. For example, if a student joined a school in 2007, their user account will be created in the "2007" OU that exists underneath the "Students" OU.

There are a number of features of the C2k EAD and its supporting infrastructure which helped to facilitate the implementation of a Shibboleth IdP.

- A well defined and agreed administrative model is used across the entire C2k EAD.
- A bespoke provisioning tool is used to control identity and access management within the C2k EAD. All user accounts are created by the provisioning tool; there is no manual creation of user accounts within the C2k EAD:
    - The tool ensures consistency and quality of data.
    - The tool automatically guarantees uniqueness of usernames.
    - The username assigned to a user when they are created in the C2k EAD lives with them throughout their time in the N. Ireland education system.

Integrating a Shibboleth IdP with Active Directory

This section describes a process for integrating a Shibboleth IdP with Active Directory at a logical level.

A later section in this document provides details on the physical aspects of integrating a Shibboleth IdP with Active Directory.

Attribute Mapping Exercise

It is possible, but extremely unlikely, that the information which must be published for users within the UK Federation will stored in the required format in Active Directory. More commonly an attribute mapping exercise will be undertaken to determine how information held in Active Directory can be transformed into a format that is suitable for use within the UK Federation. At the highest level there are three steps in the attribute mapping exercise:

1. Decide on the attributes to publish to other members of the UK Federation.
2. Identify the information that is stored in Active Directory.
3. Design how to map the information from Active Directory to that required in the UK Federation.

Each of these steps will now be discussed in more detail.

Attributes published to the UK Federation

Table 2 records the core attributes for the UK Federation and indicates those that C2k intend to publish.

Attribute	Publish	Initial C2k Decision
eduPersonScopedAffiliation	Y	Published to the UK Federation with the following value(s): • member@c2kni.net
eduPersonTargetedID	Y	Published to the UK Federation and distinct for each Service Provider
eduPersonPrincipalName	N	For each individual user account in the C2k EAD the values for the "sAMAccountName" and the individual portion of a secondary email address are the same: • sAMAccountName - bloggsj123 • secondary email - bloggsj123@c2kni.net If C2k map the username for user accounts (i.e. Active Directory attribute sAMAccountName) to eduPersonPrincipalName there is a concern that a Service Provider could easily harvest large numbers of valid email addresses.
eduPersonEntitlement	N	C2k will be interested in investigating usage of this attribute in the future. Across the C2k EAD extensive use is made of security groups to control access to resources. In the majority of cases the administration of the security groups is performed at the local school level. Local IT Administrators within a school have the ability to add and remove users in their school from school-specific security groups. As the design, implementation and usage of Shibboleth increases C2k anticipate the creation of Shibboleth specific security groups within each school.

Table 2: Initial set of Attributes published to the UK Federation

Note: C2k anticipate that this initial position will change as more services in the UK Federation are consumed and utilised by the user community.

Attributes held in Active Directory

The breadth of data held within an Active Directory varies from organisation to organisation.

The screen snapshot in Figure 3 shows the mandatory attributes that must be entered when creating a user account within an Active Directory:

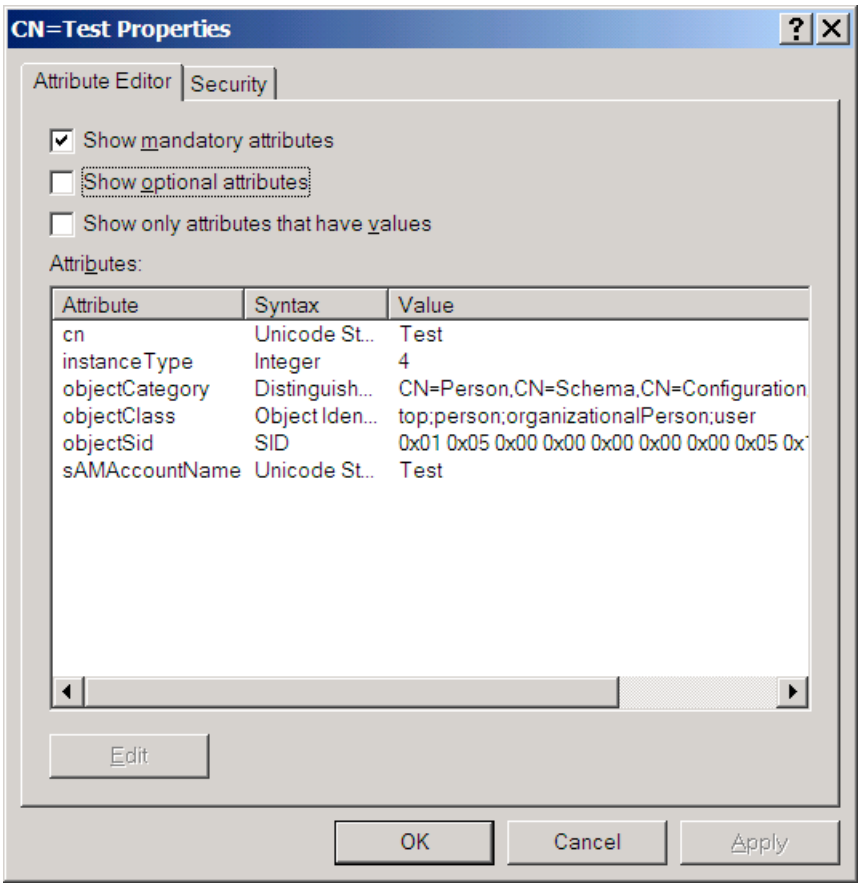


Figure 3: Minimum Attributes for an Active Directory User Account

Of the attributes listed above only the "cn" and "sAMAccountName" attributes are actually entered by the creator; the remainder are system controlled attributes.

A number of rules apply for the "cn" and "sAMAccountName" attributes:

- *"cn" must be unique within the OU*
- *"sAMAccountName" must be unique within the domain*

As well as publishing these two mandatory attributes, Table 3 identifies the other information that is stored for each user in the C2k EAD.

Data Stored	***Attribute in Active Directory***	***Comments and Examples***
Surname	*Sn*	
Salutation	*Title*	*Typically used for teachers e.g. Dr. Jones*
First/Chosen Name	*givenName*	

Data Stored	Attribute in Active Directory	Comments and Examples
Email	Mail	Each school in the C2k EAD is assigned a custom email address e.g. school.town.ni.sch.uk If the user has been granted access to email services their primary email address will be of the form - bloggsj123@school.town.ni.sch.uk
DENI Number	extensionAttribute1	
Unique user id / number in education	extensionAttribute2	A prefix in the data identifies which category the user belongs to: • Teacher • Non-Teaching • Student The remainder of the user id is a number that uniquely identifies the user.
Date of Birth	extensionAttribute3	
Intake year	extensionAttribute4	
Gender	extensionAttribute5	
Curriculum year	extensionAttribute6	
Sub-group within year	extensionAttribute7	Sub-group (or Form Group) within year e.g. 4A2
Secondary email address(es)	proxyAddresses	In the C2k EAD, schools have the ability to register and use additional DNS names e.g. school.org. If this approach has been adopted the users within the schools can have a secondary email address of the form - jbloggs123@school.org All users within the C2k EAD also belong to a single email namespace e.g. c2kni.net. In this case the user's email address will be of the form - jbloggs123@c2kni.net

Table 3: Attributes in the C2k EAD

Note: Some of the attributes listed in the table are not available natively in Active Directory; 15 extensionAttributes are only available after Exchange has been installed in the Active Directory forest.

Up to this point, when determining how information stored in an Active Directory can be utilised within the UK Federation, the focus has been on attributes associated with each individual user account. However, other information held within an Active Directory can also be utilised:

- The security groups that a user belongs to
- The location of a user account within the OU hierarchy

The Resolver.XML created by the Shibboleth for Windows Installer includes sample code for leveraging security group membership to populate the "eduPersonAffiliation" attribute.

Michael White's presentation on "Shibboleth at Stirling" includes details on how to leverage the OU hierarchy to populate the "eduPersonScopedAffiliation" attribute:

http://www.rsc-ne-scotland.ac.uk/mcshib/Presentations/mcshib8augmichaelwhite.ppt

Mapping AD Attributes to UK Federation Attributes

Having completed the first two steps in the attribute mapping exercise, the final step established the links between the source Active Directory date and the target UK Federation attributes.

Attribute	Options for Deriving Values from Active Directory
eduPersonScopedAffiliation	Can be statically defined for all users Can be derived from: • Security group membership • Location in OU hierachy
eduPersonTargetedID	Can be hashed from a unique source value associated with each user account. The Active Directory attributes objectSid or objectGUID could be used as the source value.
eduPersonPrincipalName	Could be mapped to the username or email address associated with a user account.
eduPersonEntitlement	Could be derived from security group membership.

Table 4: Options for Deriving Attribute Values from Active Directory

In the C2k implementation of a Shibboleth IdP the attributes to be published to the UK Federation are already generated by the default configuration of the Shibboleth for Windows Installer.

Shibboleth IdP Server

In general when a Shibboleth IdP Server communicates with Active Directory it performs two primary functions:

1. It authenticates users from Active Directory
2. It queries Active Directory for information about users and presents it to back to service providers

To allow the operation of these functions the documentation with the IdP installer for Active Directory states that the Shibboleth IdP Server should be a member server within an Active Directory forest/domain.

Unfortunately this approach conflicts with the security goals for the C2k infrastructure - "all systems that are members of the C2k Enterprise Active Directory must be connected to the internal C2k wide area network; specifically no member servers should be placed in the DMZs that connect to the Internet."

To progress the implementation of the Shibboleth IdP Server it was decided that this system would be configured as a standalone server; it would not be a member of the C2k EAD.

Active Directory User Account for the Shibboleth IdP

As stated earlier in this document, a Shibboleth IdP queries Active Directory for information about users. To query Active Directory the Shibboleth IdP will need a set of credentials i.e. username and password. A dedicated user account should be used for the following reasons:

- *It simplifies both the initial setup and on-going troubleshooting*
- *It facilitates targeted security analysis i.e. investigations can be concentrated on the actions of one particular account.*

A normal user account is sufficient for use by the Shibboleth IdP; it does not have to belong to any of the default or built-in groups in Active Directory such as "Account Operators" or "Administrators".

Depending on the security policy that applies to an infrastructure the Shibboleth account can also be set so that the "password never expires".

Install and Configure the Shibboleth IdP Software

If the Shibboleth for Windows Installer is run on a server that belongs to an Active Directory domain (i.e. a member server) the Control Information page of the Installer is automatically populated with information about the host Active Directory.

The C2k decision to set up the Shibboleth IdP Server as a standalone system (i.e. not a domain member) has implications for the installation of the Shibboleth IdP software. When executed in the C2k environment the Control Information page of the Installer has no suggested entries.

Table 5 shows sample input values for a configuration with separate internal (e.g. "ACME.LOCAL") and external (e.g. "acme.com") DNS zones.

Parameter	Input Value
AD Domain:	ACME.LOCAL
DNS Name for IDP:	shibboleth.acme.com
Scope to Assert:	acme.com
Kerberos:	DC01.ACME.LOCAL:88
LDAP:	DC01.ACME.LOCAL:389

Table 5: Sample input values for separate internal and external DNS zones

Table 6 shows sample input values for a split-brain DNS configuration. In a split-brain con DNS setup the same namespace (e.g. ACME.COM) is used both internally and externally.

Parameter	Input Value
AD Domain:	ACME.COM
DNS Name for IDP:	shibboleth.acme.com
Scope to Assert:	acme.com

Kerberos:	DC01.ACME.COM:88
LDAP:	DC01.ACME.COM:389

Table 6: Sample input values for a split-brain DNS configuration

After the setup of the Shibboleth for Windows Installer completes, the credentials for the user account used by the Shibboleth IdP to query Active Directory must be specified. The sample below highlights the values that must be modified in the resolver.xml file:

```
<JNDIDirectoryDataConnector id="directory">

              <Search filter="sAMAccountName=%PRINCIPAL%">

                            <Controls searchScope="SUBTREE_SCOPE" returningObjects="false"
/>

              </Search>

              <Property name="java.naming.factory.initial"
value="com.sun.jndi.ldap.LdapCtxFactory" />

              <Property name="java.naming.provider.url"
value="ldap://DC01.ACME.LOCAL:389/CN=Users,DC=ACME,DC=LOCAL" />

              <Property name="java.naming.security.principal" value="shibboleth@ACME.NET" />

              <Property name="java.naming.security.credentials" value="C0mplexP@ssw0rd" />

</JNDIDirectoryDataConnector>
```

An important line to highlight within this section is:

```
              <Property name="java.naming.provider.url"
value="ldap://DC01.ACME.LOCAL:389/CN=Users,DC=ACME,DC=LOCAL" />
```

The value for this property defines the starting point for search operations that the Shibboleth IdP uses when querying for information about users. If all users are located underneath the built-in Users container no modifications are required to this line.

If user accounts have been created underneath a custom OU (e.g. Accounts) the line should be modified as follows:

```
              <Property name="java.naming.provider.url"
value="ldap://DC01.ACME.LOCAL:389/CN=Accounts,DC=ACME,DC=LOCAL" />
```

In the C2k EAD the user accounts are distributed underneath three top-level OUs (e.g. Establishments, Nursery and Primary). This configuration required the following changes to enable the Shibboleth IdP to search the entire Active Directory:

```
              <Property name="java.naming.provider.url"
value="ldap://DC01.ACME.LOCAL:389/~~CN=Users,~~DC=ACME,DC=LOCAL" />
```
{Delete the highlighted text}

```
              <Property name="java.naming.security.principal" value="shibboleth@ACME.NET" />

              <Property name="java.naming.security.credentials" value="C0mplexP@ssw0rd" />

       <Property name="java.naming.referral" value="follow"/>
```

The initial arp.site.xml file that is created by the Shibboleth for Windows Installer releases the following attributes - eduPersonAffiliation & eduPersonScopedAffiliation.

An organisation may decide that it wants to release more attributes to service providers.

In the arp.site.xml the character sequence "<!--" identifies the start of a comment section, whilst the character sequence "-->" identifies the end of a comment section. Changing which core attributes are released by Shibboleth IdP is simply a process of adding, deleting or moving the comment identifiers.

To release the eduPersonTargetedID attribute edit the arp.site.xml file as follows:

```
<!-- We will *NOT* release ePTID, ePPN or ePE
```
{← Delete this line}

```
                        <Attribute name="urn:mace:dir:attribute-
def:eduPersonTargetedID">

                                    <AnyValue release="permit"/>

                        </Attribute>
```

```
<!-- We will *NOT* release ePPN or ePE
```
{← Insert this line}

```
                        <Attribute name="urn:mace:dir:attribute-
def:eduPersonPrincipalName">

                        </Attribute>

                        <Attribute name="urn:mace:dir:attribute-
def:eduPersonEntitlement">

                                    <AnyValue release="permit"/>

                        </Attribute>

-->
```

After the necessary edits have been completed, the TomCat5 service must be restarted for the changes to be applied to the Shibboleth IdP.

Implementing a Shibboleth IdP in C2k

This section describes the process and procedures by which C2k implemented a Shibboleth IdP in their infrastructure.

The entire process for installing and configuring a Shibboleth IdP server is summarised below:

1. *Network Connectivity*
    a. *Identify and configure a network location for the Shibboleth IdP e.g. either a common DMZ or dedicated Federation DMZ*
    b. *Open the necessary ports in internal and external firewalls*
2. *Installing and Configuring the Shibboleth IdP Server*
    a. *Install the Windows Server operating system*
    b. *Configure network name resolution (DNS and HOSTS file)*
3. *Testing Network Communications*
4. *Installing and Configuring the Shibboleth IdP Software*
    a. *Run the Shibboleth for Windows Installer*
    b. *Edit the Resolver.XML file*
    c. *Edit the ARP.Site.XML file*
    d. *Restart the TomCat5 service*
5. *Testing a Shibboleth IdP with TestShib*

Many of these steps will now be discussed and described in more detail.

Network Connectivity

There are a number of options for the exact placement of a Shibboleth IdP server within an infrastructure. Figure 4 illustrates one of the most common network zone architectures for a Shibboleth IdP.

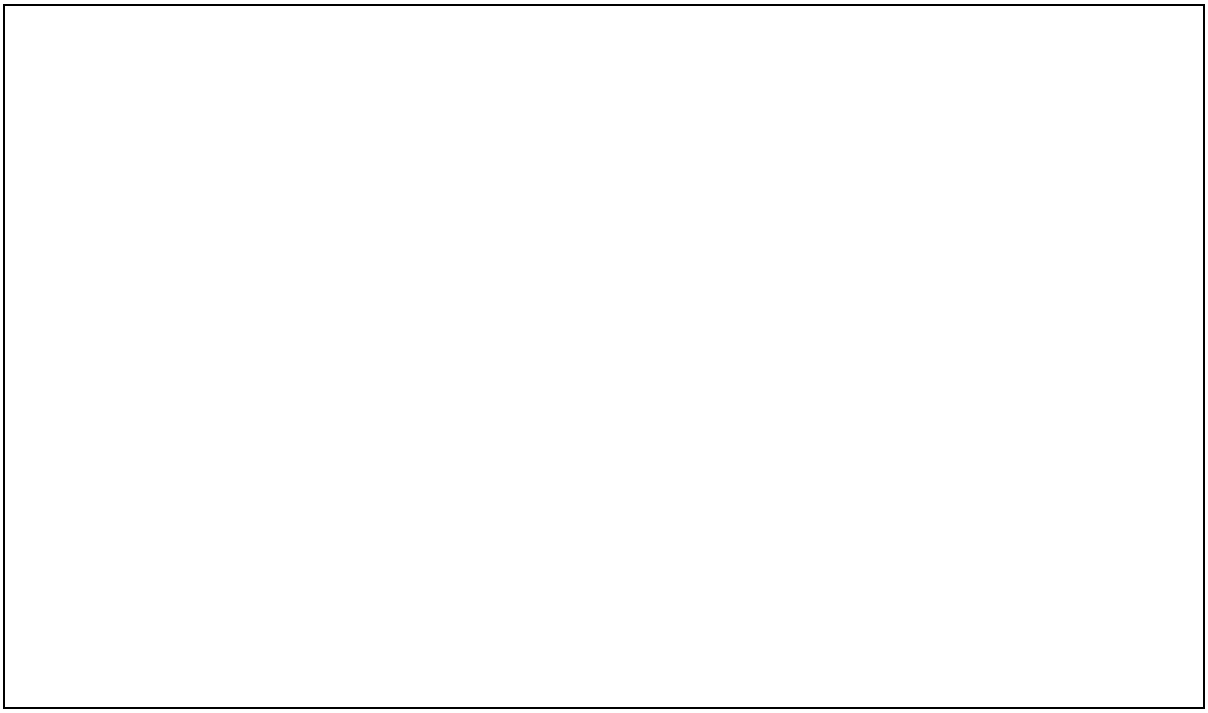


Figure 4: Typical Network Zone Architecture for a Shibboleth IdP

In this solution the Shibboleth IdP Server resides in a De-Militarised Zone (DMZ); the DMZ is usually connected to a dedicated network interface on an external firewall.

With this network configuration no direct access is allowed from the Internet to the Internal Infrastructure. The external and internal firewalls are configured to support the use of proxies and relays that reside in a DMZ. Rules on the external firewall control the communications that are allowed from the Internet to systems in the DMZ and vice versa. Rules on the internal firewall control the communications that are allowed from the DMZ to the Internal Infrastructure and vice versa.

Table 7 records the rules for the external firewall.

Source	Source Port	Target	Target Port	Action	Comment
Shibboleth IdP	*	External DNS Server	53/UDP	Permit	Allows the Shibboleth IdP to resolve names and IP addresses of systems on the Internet
Shibboleth IdP	*	*	80/TCP	Permit	Allows the Shibboleth IdP to initiate HTTP communications with systems on the Internet
Shibboleth IdP	*	*	443/TCP	Permit	Allows the Shibboleth IdP to initiate HTTPS/Secure Sockets Layer (SSL) communications with systems on the Internet
*	*	Shibboleth IdP	8442/TCP	Permit	Allows systems on the Internet to initiate communications with the browser facing ports of the Shibboleth IdP

Source	Source Port	Target	Target Port	Action	Comment
*	*	Shibboleth IdP	8443/TCP	Permit	Allows systems on the Internet to initiate communications with the Service Provider facing ports of the Shibboleth IdP

Table 7: Firewall Rules for External Firewall

Table 8 records the rules for the Internal Firewall.

Source	Source Port	Target	Target Port	Action	Comment
Shibboleth IdP	*	AD Domain Controller	88/TCP & 88/UDP	Permit	Allows the Shibboleth IdP to initiate Kerberos communications with the AD Domain Controller
Shibboleth IdP	*	AD Domain Controller	389/TCP	Permit	Allows the Shibboleth IdP to conduct LDAP queries against the AD Domain Controller

Table 8: Firewall Rules for Internal Firewall

Installing and Configuring the Shibboleth IdP server

The Windows Server 2003 operating system should be installed on the Shibboleth IdP Server. The latest service pack and security hot-fixes should also be installed.

Network name resolution must now be configured so that the Shibboleth IdP Server can identify and locate systems on the Internet and the Internal Infrastructure.

DNS is configured so that the Shibboleth IdP Server resolves names from an external DNS server. The external DNS server could be one operated by an ISP, or alternatively it could be a dedicated external DNS server owned and operated by an internal IT group.

In the case of C2k an added complexity is the use of the same DNS namespace (i.e. “c2kni.net”) on both the Internal Infrastructure and the Internet. This configuration is often referred to as “split-brain DNS”. Figure 5 illustrates where the different zones in a split-brain DNS configuration would be hosted.

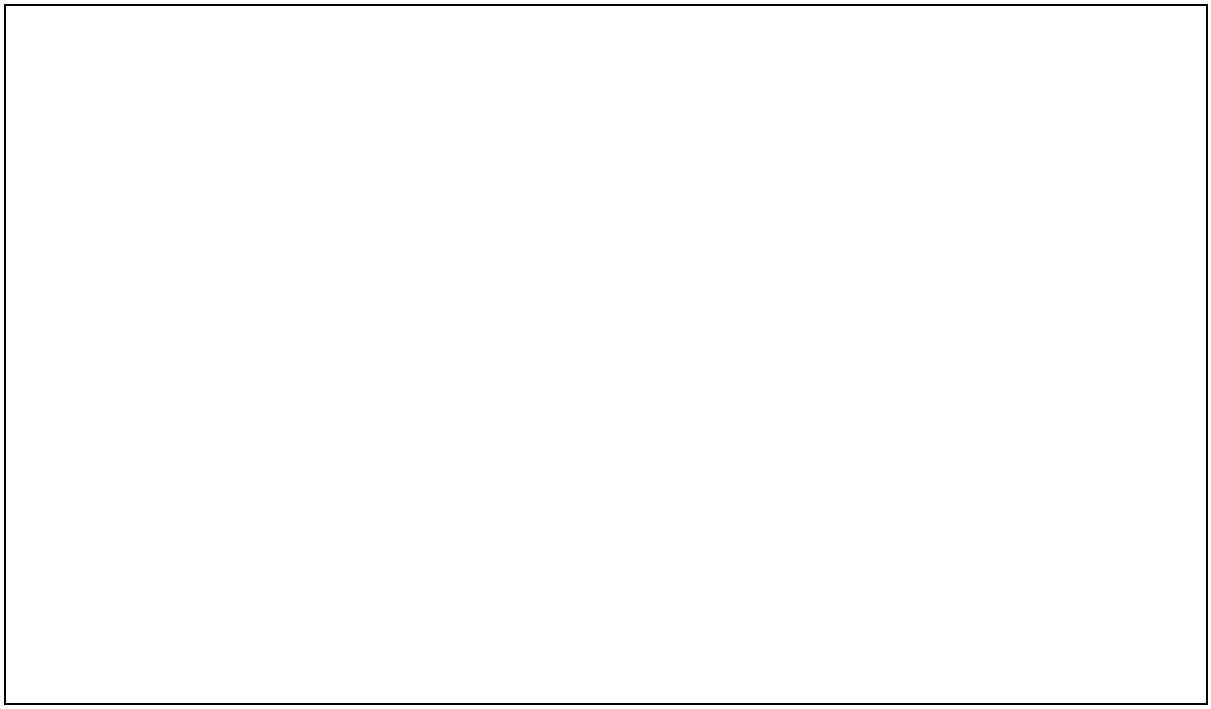


Figure 5: The Scope of DNS zones in a split-brain configuration

Also, the DNS records stored in the internal and external zones will differ greatly:

- *Internal DNZ zones contain entries for all internal systems e.g. file servers, workstations etc.*
- *External DNZ zones contain entries for all external systems e.g. web servers, Shibboleth servers etc.*

This setup presents a problem for the Shibboleth IdP Server because it needs to resolve names of systems on the Internet and resolve the name of a Domain Controller on the Internal Infrastructure. The Shibboleth IdP Server is setup to query an external DNS server which will know nothing about a Domain Controller in the Internal Infrastructure. A simple solution is to modify the "%windir%\System32\drivers\etc\hosts" file and add an entry for the Domain Controller which we want to locate e.g.

```
10.10.5.5          DC01.ACME.COM
```

Testing Network Communications

After the prerequisite networking and name resolution components have been configured a number of tools can be used to verify the correct configuration and operation of network communications.

Tool	***Usage***
PortQry	*Test connectivity from a Shibboleth IdP to Active Directory.*
Online Port Scanners	*Test connectivity from the Internet to a Shibboleth IdP server.*
Internet Browser	*To test HTTP access from the Shibboleth IdP to the Internet. HTTP is used to download the latest version of the XML metadata files from the UK Federation.*

Table 9: Network Testing and Troubleshooting Tools

"Appendix A – Useful Tools and Techniques" – describes how to use these tools to test and troubleshoot the different categories of network communications required to implement a Shibboleth IdP.

Installing and Configuring the Shibboleth IdP software

Use the guidance in an earlier section of this document to install and configure the Shibboleth IdP software.

Testing a Shibboleth IdP with TestShib

After completing all installation and configuration steps use the guidance at https://spaces.internet2.edu/display/SHIB/IdPActiveDirectory to test the operation of a Shibboleth IdP.

Appendix A - Useful Tools and Techniques

This appendix details a number of tools and techniques that the authors used when implementing the C2k Shibboleth IdP.

Network Tools

In a large support organisation other individuals or groups may configure the underlying network and security infrastructure. The individual responsible for configuring a Shibboleth IdP may be interested in performing a number of quick and simple validation tests after work has been completed by network or security teams.

The combination of PortQry and Online Port Scanning tools allows the testing of the internal and external network communications that are required to allow the successful deployment and operation of a Shibboleth IdP.

PortQry

PortQry is a command-line utility which helps to troubleshoot TCP/IP connectivity issues from a Shibboleth IdP to Active Directory.

"Where is the tool located?"

PortQry can be downloaded from:
http://www.microsoft.com/downloads/details.aspx?FamilyID=89811747-C74B-4638-A2D5-AC828BDC6983&displaylang=en

"How is the tool used?"

PortQry should be installed on the Shibboleth IdP server.

Use the following commands to verify connectivity to an Active Directory:

```
Portqry -n {IP address of DC} -e {port to query; 88 and 389}
```

Examples:

```
Portqry -n 10.10.5.5 -3 88

Portqry -n 10.10.5.5 -3 389
```

"Is there more information available on this tool?"

For more information please refer to the following articles:

How To: Mastering PortQry.exe (Part 1):
http://www.windowsecurity.com/articles/Mastering-PortQryexe-Part1.html

How To: Mastering PortQry.exe (Part 2):
http://www.windowsecurity.com/articles/Mastering-PortQryexe-Part2.html

Online Port Scanners

Online Port Scanners can be used to help troubleshoot TCP/IP connectivity issues from the Internet (either the UK Federation or TESTSHIB) to a Shibboleth IdP server.

Note: Online Port Scanner tests should only be run in the final stages of configuring a Shibboleth IdP; all prior internal and external connectivity configuration steps should be completed and tested.

"Where is the tool located?"

There are a number of online port scanners available on the Internet. When searching for an online port scanner, try to locate one which allows the querying of a single port number on the target system.

The author used the following online resource to test the implementation of the C2k Shibboleth IdP:

http://www.t1shopper.com/tools/port-scanner/

"How is the tool used?"

The usage will vary per online port scanner. Use the tool selected to check access to the ports (8442 & 8443) presented and used by the Shibboleth IdP:

- *8442 - Browser facing ports*
  i.e. ShibbolethV1SSOHandler & Shibboleth_StatusHandler
- *8443 - Service Provider (SP) facing ports*
  i.e. SAMLv1_AttributeQueryHandler & SAMLv1_1ArtifactQueryHandler

If the tests are successful messages like the following should be returned:

```
43.65.23.87 is responding on port 8442 ()

43.65.23.87 is responding on port 8443 (pcsync-https)
```

Active Directory Access

When fully operational, the Shibboleth IdP server will be making a number of queries against an Active Directory. The Microsoft LDP tool can be used to simulate and test the required connectivity and access from a Shibboleth IdP to Active Directory.

The Windows Server operating system by default performs high-level logging of queries executed against an Active Directory. Windows Server can be configured to log more detailed information, which is often useful in troubleshooting situations.

Verifying LDAP access using the LDP tool and logging LDAP access to an Active Directory will now be discussed in more detail.

LDP

LDP is an LDAP client that can browse and view objects stored in an Active Directory.

"Where is the tool located?"

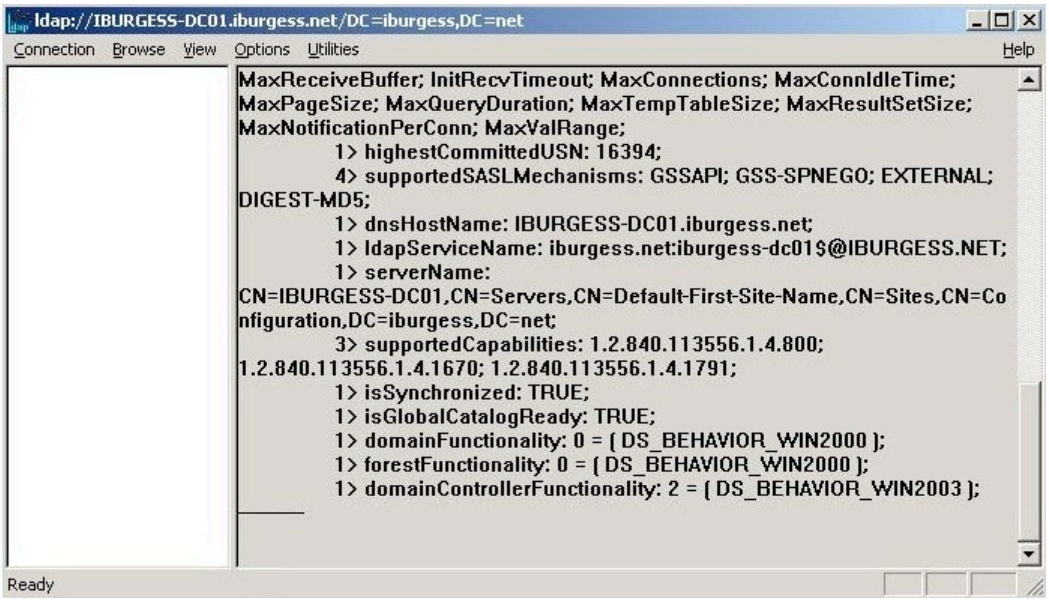
LDP is one of the Windows Server 2003 Support Tools. The tools can be installed by running \SUPPORT\TOOLS\SUPTOOLS.MSI on the Windows Server 2003 installation media.

LDP is built into Windows Server 2008; it is available if the Active Directory Domain Services (AD DS) server role is installed.

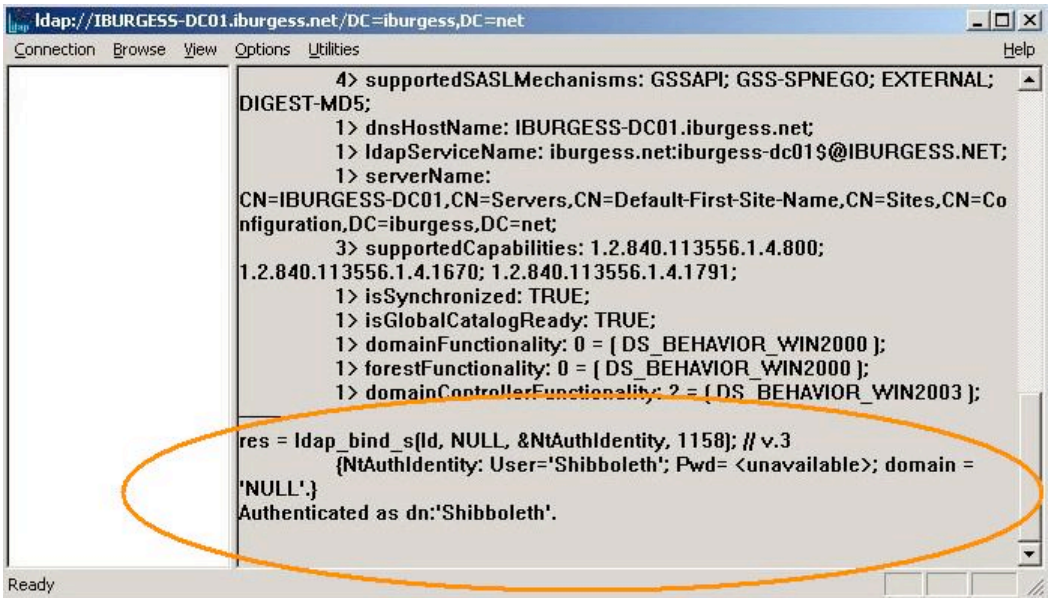
"How is the tool used?"

To verify LDAP connectivity from a Shibboleth IdP to Active Directory:

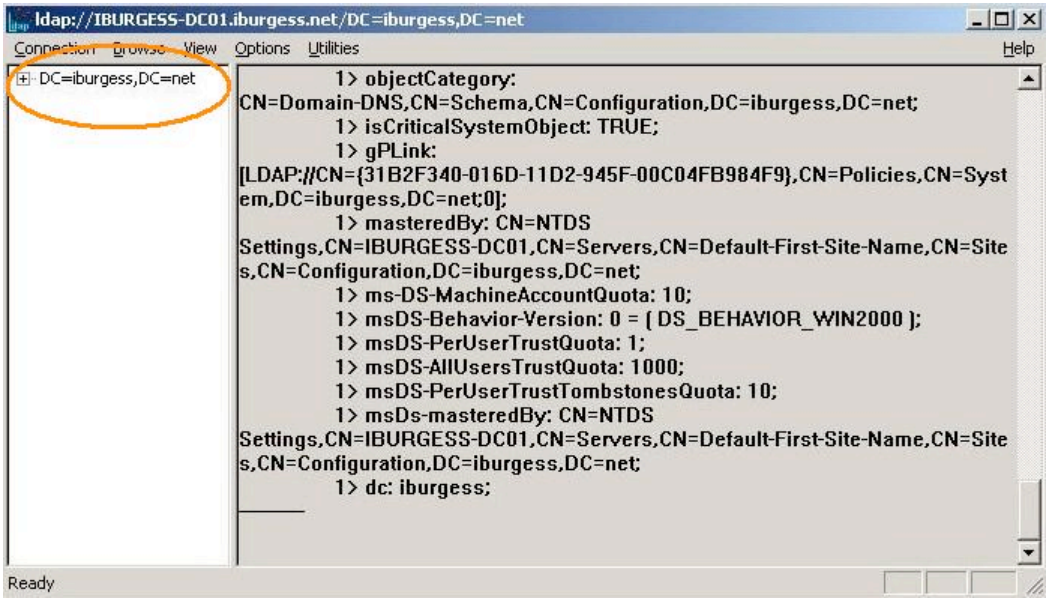
1. *Log onto the Shibboleth IdP*
2. ***Start → Run →** Type **LDP.EXE** and click on **OK***
3. *From the **Connection** drop-down menu select **Connect**...*
4. *In the Connect dialogue box enter the **Server:** to connect to. Type in the **IP address or hostname of the Active Directory domain controller** that the Shibboleth IdP will query and click **OK**. Information about the Active Directory is presented in the right-hand pane.*



5. *From the **Connection** drop-down menu select **Bind**...*
6. *In the Bind dialogue box enter the credentials (**User:** & **Password:**) of the Active Directory user account that is used by the Shibboleth IdP and click **OK**. In the right-hand pane a message indicates successful authentication by Active Directory.*

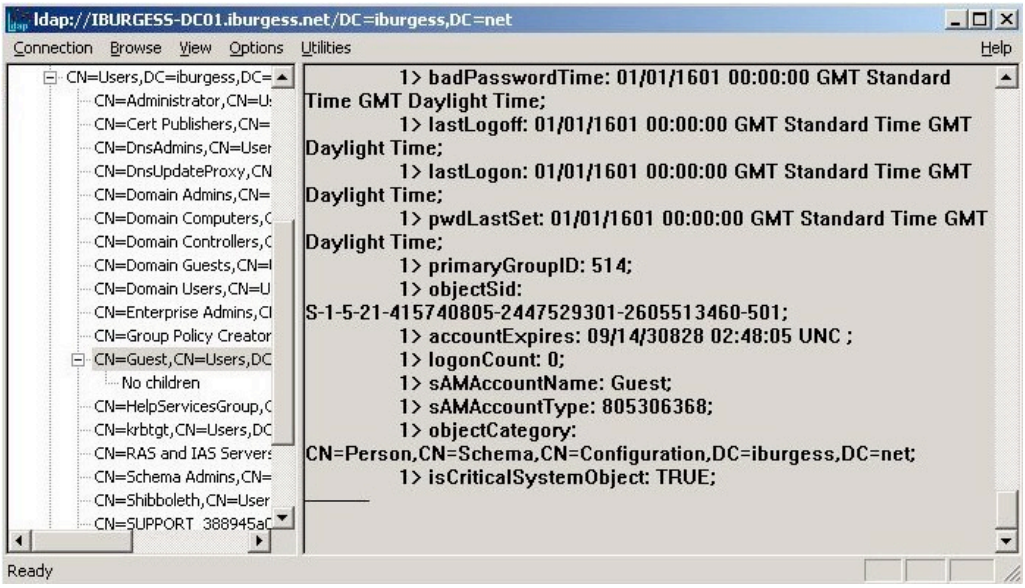


7. *From the **View** drop-down menu select **Tree***
8. *In the Tree View dialogue box select the **BaseDN**:. This is the entry point in the Active Directory from which browsing starts. It is OK to leave this blank and click **OK**. The left-hand pane should be updated with the name of the Active Directory domain, whilst the right-hand pane will be updated with more attributes associated with the domain.*



Note: The default starting point is the top level of an Active Directory hierarchy i.e. in the Active Directory technical community this is known as the Domain Naming Context (NC).

9. *Drill down through Active Directory by expanding/double-clicking entries in the left-hand pane. In the following screenshot example the user has navigated to the "Users" container and expanded the attributes for the "Guest" account.*



"Is there more information available on this tool?"

For more information please refer to the following articles:

- *Ldp*:
  http://technet2.microsoft.com/windowsserver2008/en/library/319a46f2-7a37-4274-9e24-c7558ce663e01033.mspx?mfr=true
- Ldp Overview:
  http://technet2.microsoft.com/windowsserver/en/library/4efcf47f-e3eb-46e4-9c6c-842b39eca2011033.mspx?mfr=true

Logging LDAP access

In day-to-day operation the Shibboleth IdP will be executing a number of queries against Active Directory. By default the Windows Server operating system logs a limited amount of information on the queries made for objects held within an Active Directory. The level of logging and monitoring of LDAP searches can be increased.

"Is there more information available on this tool?"

For more information please refer to the following articles:

Logging LDAP searches: AD and ADAM:
http://www.activedir.org/Articles/tabid/54/articleType/ArticleView/articleId/41/Logging-LDAP-searches-AD-and-ADAM.aspx
(please pay particular attention to the last three paragraphs)

Note: Also check the Testing Resolver.XML files with ResolverTest.BAT

Depending on organisational requirements and the configuration of Active Directory, the Resolver.XML file that is supplied by the Shibboleth for Windows Installer may need to be modified. If changes are made then their operation can be tested with an in-built test script - ResolverTest.BAT

"Where is the tool located?"

`ResolverTest.BAT` *can be found in* `C:\Program Files\Internet2\IdP\bin`

"How is the tool used?"

Launch a command prompt and navigate to the `C:\Program Files\Internet2\IdP\bin` *directory.*

Test changes made to resolver.XML use the following command:

```
Resolvertest.BAT --user=Administrator
 --resolverxml=C:/Program%20Files/Internet2/idp/etc/resolver.xml
```

***Note**: during testing in C2k, the ResolverTest.BAT script did not provide a value for the eduPersonTargettedID attribute. However the same tests against TESTSHIB showed that the attribute was being released by the Shibboleth IdP.*

Performance Monitoring and Troubleshooting information at the end of this section.

Shibboleth IdP Logging and Test Script

The Shibboleth for Windows Installer includes logging functionality and a test script. Both of these components are extremely useful when implementing the initial configuration of a Shibboleth IdP.

Shibboleth IdP Log Files

The Shibboleth IdP records log information in a number of plain text files.

"Where is the tool located?"

The primary log files to check in a Shibboleth IdP are:

- `C:\Program Files\Internet2\CaptiveTomcat5.5\logs\catalina.{date}.log`
- `C:\Program Files\Internet2\IdP\logs\shib-error.log`
- `C:\Program Files\Internet2\IdP\logs\shib-access.log`

"How is the tool used?"

The amount of information gathered can be increased by modifying the following line in the idp.xml file:

```
<ErrorLog level="WARN"
location="file:/C:/Program%20Files/Internet2/idp//logs/shib-error.log" />
```

Change the value of level from "WARN" to "DEBUG" e.g.

```
<ErrorLog level="DEBUG"
location="file:/C:/Program%20Files/Internet2/idp//logs/shib-error.log" />
```

***Note**: After testing has been completed reset the logging values back to their defaults and restart the TomCat5 service.*

Stopping and Starting the TomCat5 Service (Shibboleth IdP)

If changes are made to the .XML configuration files (e.g. idp.XML or resolver.XML) for a Shibboleth IdP, Tomcat must be restarted for the changes to take effect. The Shibboleth for Windows Installer runs Tomcat as a service.

"Where is the tool located?"

There are a number of methods for locating and managing the tomcat service:

1. ***Start → Administrative Tools → Services** MMC Snap-In → **Tomcat5***
2. *Launch* **`C:\Program Files\Internet2\CaptiveTomcat5.5\bin\tomcat5w.exe`**
3. *Command Prompt - the "***`NET START`***" command within a command prompt lists all running services*

"How is the tool used?"

1. *Services MMC Snap-In*
    a. *Right-click the **Tomcat5** service and select **Restart***
2. *Tomcat5.exe*
    a. *On the **General** tab*
        i. *Click on the **Stop** button*
        ii. *Click on the **Start** button*
3. *Command Prompt*
    a. **`"NET STOP TOMCAT5"`**
    b. **`"NET START TOMCAT5"`**

Testing Resolver.XML files with ResolverTest.BAT

Depending on organisational requirements and the configuration of Active Directory, the Resolver.XML file that is supplied by the Shibboleth for Windows Installer may need to be modified. If changes are made then their operation can be tested with an in-built test script - ResolverTest.BAT

"Where is the tool located?"

`ResolverTest.BAT` *can be found in* `C:\Program Files\Internet2\IdP\bin`

"How is the tool used?"

Launch a command prompt and navigate to the `C:\Program Files\Internet2\IdP\bin` *directory.*

Test changes made to resolver.XML use the following command:

```
Resolvertest.BAT --user=Administrator
 --resolverxml=C:/Program%20Files/Internet2/idp/etc/resolver.xml
```

***Note**: during testing in C2k, the ResolverTest.BAT script did not provide a value for the eduPersonTargettedID attribute. However the same tests against TESTSHIB showed that the attribute was being released by the Shibboleth IdP.*

Performance Monitoring and Troubleshooting

As the usage of a Shibboleth IdP increases one or more performance bottlenecks within the overall federation solution could be encountered. The guidance within this section suggests methods for monitoring the performance of both the Shibboleth IdP server and the Active Directory domain controller that is queried by the Shibboleth IdP server.

When focusing on the performance of the Domain Controller being queried, it is the author's view that the Windows Server 2008 Reliability and Performance Monitor tool provides more comprehensive LDAP performance reporting information than the Windows Server 2003 Performance Advisor. However the choice of which tool to run will depend entirely on the version of Windows Server running on the domain controllers within an Active Directory:

- *Windows Server 2003 Domain Controllers → use the Windows Server 2003 Performance Advisor*
- *Windows Server 2008 Domain Controllers → use the Windows Server 2008 Reliability and Performance Monitor*

Both tools will now be discussed in more detail.

Windows Server 2003 Performance Advisor

Server Performance Advisor (SPA) is a performance diagnostic tool for Windows Server 2003. It can provide reports for server roles such as Active Directory, Internet Information System (IIS), and DNS etc.

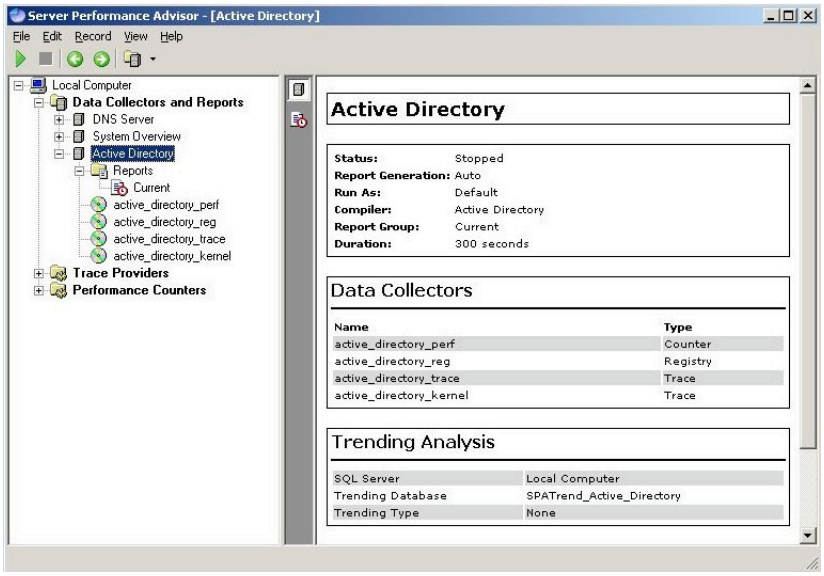
"Where is the tool located?"

SPA v2 can be downloaded from:
http://www.microsoft.com/downloads/details.aspx?familyid=09115420-8c9d-46b9-a9a5-9bffcd237da2&displaylang=en

"How is the tool used?"

The steps below provide a high-level summary of how to use RPM:

1. *Windows Server 2003 Domain Controller*
    - *Log onto the Domain Controller which the Shibboleth IdP queries*
    - *Launch SPA*
        - *Select and start the **Active Directory** Data Collector and Reports set*



2. *Client Workstation*
    - *Initiate the Shibboleth IdP action that is causing an issue*
    - *Wait for the Shibboleth IdP action to complete*
3. *Windows Server 2003 Domain Controller*
    - *Stop the Data Collector Set*
    - *View and analyse the report of the information collected*

Windows Server 2008 Reliability and Performance Monitor

As the name suggests, the Windows Reliability and Performance Monitor monitors and assesses the performance and reliability of a system.

"Where is the tool located?"

Reliability and Performance Monitor (RPM) ships with Windows Server 2008.

"How is the tool used?"

The steps below provide a high-level summary of how to use RPM:

1. *Windows Server 2008 Domain Controller*
    - *Log onto the Domain Controller which the Shibboleth IdP queries*
    - *Launch RPM*
        - *Select and start the **Active Directory Diagnostics** Data Collector Set*
2. *Client Workstation*
    - *Initiate the Shibboleth IdP action that is causing an issue*

- *Wait for the Shibboleth IdP action to complete*

3. *Windows Server 2008 Domain Controller*
   - *Stop the Data Collector Set*
   - *View and analyse the report of the information collected*

For more detailed guidance on using RPM please refer to the following article(s):

Tracking LDAP Searches with Windows Server 2008 Reliability and Performance Monitor:
http://www.activedir.org/Articles/tabid/54/articleType/ArticleView/articleId/49/Default.aspx

Disclaimer