Single Sign On with Informix Dynamic Server Using Windows AD

Overview....2
Setup KDC (Windows AD) for IDS....2
  Add users....2
  Add hosts....2
  Register Service Principal....2
  Export and Merge keytab....3
    Export in Windows....3
    Merge in Unix....3
Setup IDS to use the KDC (Windows AD)....4
  SQLHOSTS....4
  Configure CSM....4
  Bring IDS server up....5
Setup clients to use the IDS server....5
  SQLHOSTS....5
Setting up KDC (Windows AD)....5
  Add users....5
Troubleshooting....7

Overview

Informix Dynamic Server (IDS) Single Sign On (SSO) support in Windows is implemented using Windows Kerberos implementation. Windows Kerberos implementation does not support GSSAPI but instead provides support for Microsoft-specific API, the Security Support Provider Interface (SSPI).

This document outlines the broad steps required to setup SSO using Windows AD. The steps required to setup AD is given as an example. Please contact your system administrator to get the requirements in your site.

This document illustrates setting up SSO for Informix Dynamic Server using the following setup:

INFORMIXSERVER	ol_ids_1150_1
IDS host	aixmach1.ibm.com
Kerberos domain	TESTMART.LENEXA.IBM.COM

Setup KDC (Windows AD) for IDS

Add users

1. Add user Informix
2. Add other users who will be authenticating with the KDC
3. Add INFORMIXSERVER as a user. Make sure that this user does not have "change password at next logon" set. You can use any user name for this purpose, but it is convenient and intuitive to use INFORMIXSERVER. This name should be unique, in that it must not clash with any host name that may be configured in the KDC.

Add hosts

Add the host machines that will be authenticating with the KDC. This will be the host running the IDS server

Register Service Principal

Kerberos authentication requires that services be set as Service Principal Names (SPNs) associated with a hostname.

SPNs are unique identifiers for services running on servers. It is registered in Active Directory under a user account as an attribute called Service-Principal-Name. The SPN is assigned to the account under which the service that the SPN identifies is running. Any service can look up the SPN for another service. When a service wants to authenticate to

another service, it uses that service's SPN to differentiate it from other services running on that computer.

The hostname should be a Fully Qualified Domain Name (FQDN) for the association. The FQDN for our example would be:

ol_ids_1150_1/aixmach1.ibm.com@TESTMART.LENEXA.IBM.COM

To add an SPN type the following at a command prompt:
setspn -A ServiceClass/Host:Port hostname

For example:

```
setspn –A ol_ids_1150_1/aixmach1.ibm.com@TESTMART.LENEXA.IBM.COM
aixmach1.ibm.com
```

Export and Merge keytab

Export the keytab of the SPN at the KDC and copy it to the Unix host and merge the keytab with the Kerberos keytab file on the machine

Export in Windows

Use the ktpass utility to export the keytab file. For example:

```
ktpass
   /out c:\temp\ol_ids_1150_1.keytab
   /princ ol_ids_1150_1/aixmach1ibm.com@TESTMART.LENEXA.IBM.COM
   /mapUser ol_ids_1150_1
   /mapOp set
   /pass ******  (enter password here)
   /crypto DES-CBC-CRC
   /pType KRB5_NT_PRINCIPAL
```

Copy the output file to the Unix host running IDS, for example to /tmp/ ol_ids_1150_1.keytab

Merge in Unix

Use the ktutil utility to import and merge the keytab file. Please contact your system administrators to get the location of the Kerberos utilities and the location of the Kerberos keytab file. The following example assumes that the ktutil utility is located in /usr/ Kerberos/sbin and that the Kerberos keytab is /etc/krb5.keytab.

For example:

```
/usr/kerberos/sbin/ktutil
ktutil: rkt /tmp/ol_ids_1150_1.keytab
ktutil: wkt /etc/krb5.keytab
```

```
ktutil: quit
```

Setup IDS to use the KDC (Windows AD)

SQLHOSTS

IDS uses CSM to exchange Kerberos credentials. Setup SQLHOSTS as in the following example:

```
ol_ids_1150_1   olsoctcp   aixmach1.ibm.com   srvportnum   s=7, csm = (GSSCSM).
```

The only addition is the SQLHOSTS option field which must contain

s=7, csm = (GSSCSM).

The flag s=7 tells IDS to use Kerberos SSO and the option csm=(GSSAPI) tells what CSM module to use. The name GSSAPI can be any name that you choose. This will be mapped to an actual CSM module in the next step.

Configure CSM

The concsm.cfg file defines the CSM configuration information. By default, the concsm.cfg file resides in $INFORMIXDIR/etc/. The IDS administrator (DBSA) can configure the location of CSM configuration by specifying the INFORMIXCONCSMCFG environment variable for IDS when it is started.

The syntax of entry in concsm.cfg is

csmname("client=clientlib, server=serverlib, "global_opts", "conn_opts")

- csmname is name to the communication support module
- clientlib and server lib value specifies the full path and name of the GSSCSM shared library
- there are no global options in the current release of the GSSCSM module
- connection option specifies whether confidentiality and integrity is used

- confidentiality is specified by connection option 'c = [01],' the vaule 1 indicating that confidentiality (encryption) is used, and 0 indicating that it is not.

- integrity is specified using connection option 'i = [01],' the value 1 indicating that integrity (using message authentication codes to ensure that the message received is the one that was sent) is used, and 0 indicating that it is not used.

Example concsm.cfg configuration

```
GSSCSM("/work/informixdir/lib/csm/igsss11a.so", "", "c=1,i=1")
```

The name GSSCSM in the above example must match the name given in the options column of the SQLHOSTS file.

Bring IDS server up

As user informix, bring the IDS server up. If the Kerberos ticket is not already obtained at logon, run "kinit" and supply the password for user informix when asked.

If the CSM options in the SQLHOSTS file change, the server must be restarted.

Setup clients to use the IDS server

SQLHOSTS

The clients must have the SQLHOSTS options "s=7,csm=(GSSAPI) set. In a Windows client, use the setnet32 utility to edit the options value in the SQLHOSTS entry. On a Unix client, edit the SQLHOSTS file.

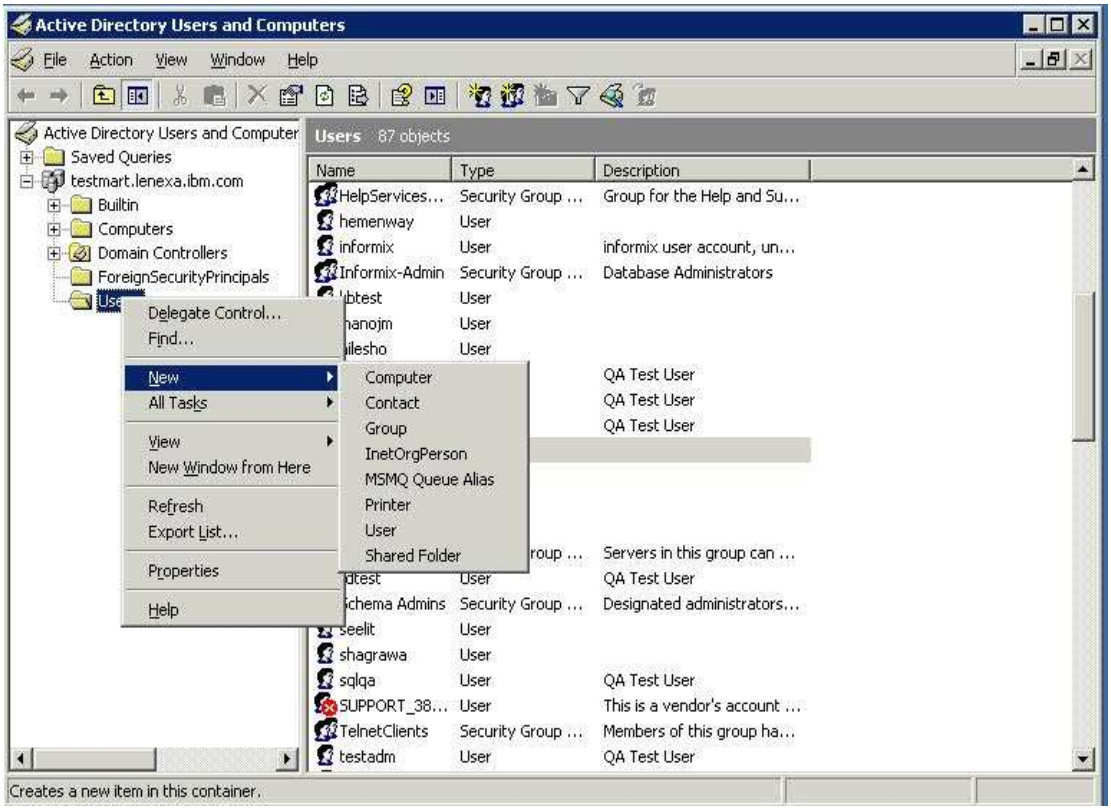
Setting up KDC (Windows AD)

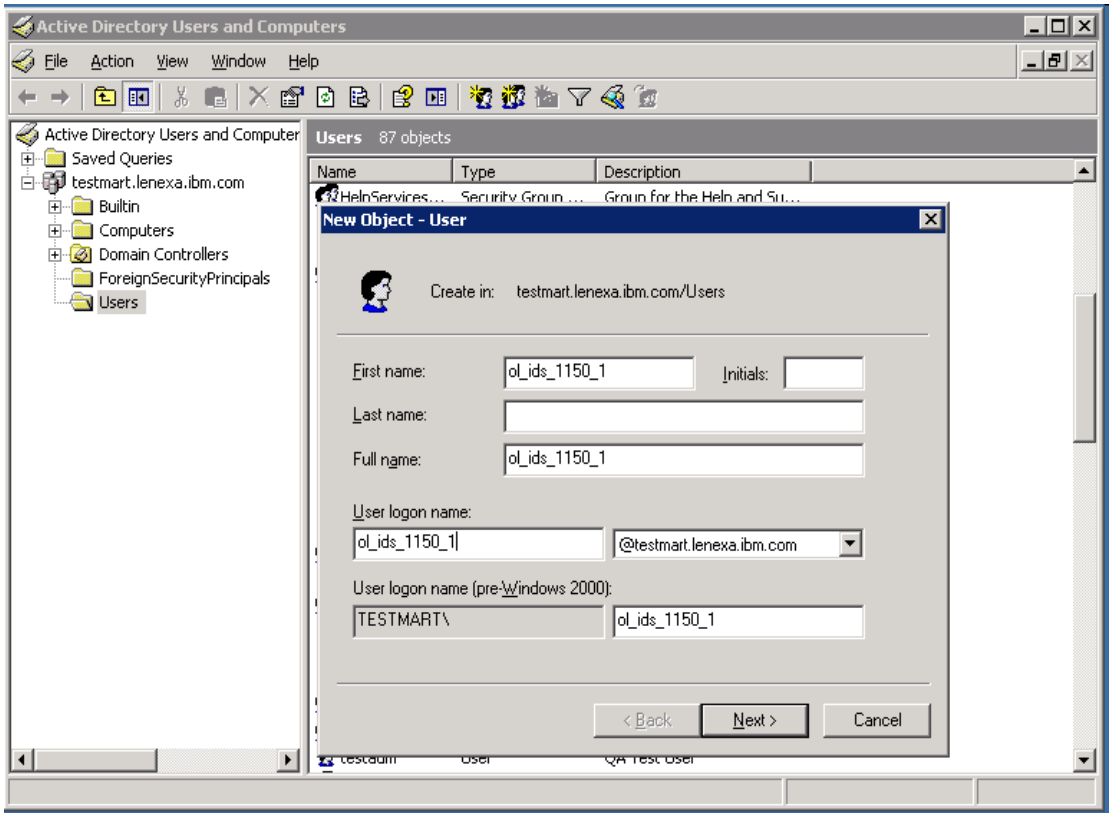
This section outlines the broad steps required to setup SSO using Windows AD. This is provided as guidance only. Please contact your system administrator to get the requirements in your site

Add users

Bring up the "Active Directory Users and Computers" dialog box. The path to it depends on the version of the Windows server. It can usually be found via start/ Administrative Tools/ Active Directory Users and Computers".

Right click on "users" folder on the navigation panel and select New/User as in the example below.


Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computer
Saved Queries
testmart.lenexa.ibm.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Delegate Control...
Find...
New
All Tasks
View
New Window from Here
Refresh
Export List...
Properties
Help
Computer
Contact
Group
InetOrgPerson
MSMQ Queue Alias
Printer
User
Shared Folder
Users 87 objects
Name Type Description
HelpServices... Security Group ... Group for the Help and Su...
hemenway User
informix User informix user account, un...
Informix-Admin Security Group ... Database Administrators
User
User
User
QA Test User
QA Test User
QA Test User
Servers in this group can ...
QA Test User
Designated administrators...
User
shagrawa User
sqlqa User QA Test User
SUPPORT_38... User This is a vendor's account ...
TelnetClients Security Group ... Members of this group ha...
testadm User QA Test User
Creates a new item in this container.


Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computer
Saved Queries
testmart.lenexa.ibm.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Users 87 objects
Name Type Description
New Object - User
Create in: testmart.lenexa.ibm.com/Users
First name: ol_ids_1150_1
Initials:
Last name:
Full name: ol_ids_1150_1
User logon name:
ol_ids_1150_1
@testmart.lenexa.ibm.com
User logon name (pre-Windows 2000):
TESTMART\
ol_ids_1150_1
< Back
Next >
Cancel

Troubleshooting

- Ensure that the users added to the KDC can log into the host machine as Kerberos users. If this does not work, please contact your system administrators.
- Windows machines that are part of an Active Directory domain automatically synchronize their clocks to the domain controller's clock through the Windows Time Service. Unix systems typically do not have NTP installed and configured out of the box, so manual configuration is required to keep these systems' clocks in sync.
- The Windows domain controller supports only the RC4 encryption type as well as the older DES encryption type. It does not support the newer Triple DES that MIT and Heimdal support.
- Ensure that the Reverse ARP resolution in the domain controller is setup correctly.