Configuring Kerberos Manual Authentication and/or SSO in Distributed Environments (requires XI 3.1 SP3 or later)

Applies to:

Only XI 3.1 SP3 or later please see configuring Vintela SSO for earlier versions

Summary

This paper combines all the steps from the XI 3.1 admin guide(s) with the latest best practices and all the latest SAP KBs regarding vintela, kerberos and java AD configuration. **It is specifically written for XI 3.1 SP3 and will not work with earlier versions of XI.**

Author(s): Tim Ziemba BSEE, MCSE

Company: SAP Business Objects

Created on: 30 June 2010

Author Bio

IT/communications background prior to SAP/BO. Employed with SAP Business Objects Support in Lake Mary, FL since September 2005. Currently specializing in Authentication - XIR1, XIR2, XI 3.1 other areas include administration, migration, deployment and network troubleshooting.

Table of Contents

Section 1 - Creating and preparing the service account

1) Create a service account in Active Directory with a non-changing password

Running setspn to create SPN's for manual logon (CMS) and access points for SSO

Create an SPN for the CMS (such as BOCMS/serviceaccountname.serviceaccountdomain.com

Create pairs of SPN's for each web/app or load balancer (HTTP/hostname and HTTP/FQDN)

Create IP SPN's if needed (HPPT/IP.IP.IP.IP)

setspn –a BOCMS/serviceaccountname.serviceaccountdomain
The following SPN's are only needed for SSO
setspn –a HTTP/hostname of each tomcat or web/app server
setspn –a HTTP/FQDN of each tomcat tomcat or web/app server
Optional SPN's for server SSO and HLB's (if used)
setspn –a HTTP/ip.ip.ip.ip of each tomcat server to allow SSO to work on the server
setspn –a HTTP/otherFQDN/hostname/IP for any DNS redirects, or load balancers that will be used for SSO

To View all created SPN's

When finished Run setspn –l bossosvcacct to view all created SPN's

Section 2 - Configure the CMC and map in AD groups

Verify the AD plugin is enabled and groups are mapped. Verify users are showing up in CMC

Verify the SPN from above steps is added to the AD plugin

Verify the default domain is FQDN in all CAPS

Verify enable single Sign on is checked

Section 3 — Start the SIA/CMS under the service account

Add the service account to the local administrator's group on any server where the service account will be running a SIA/CMS.

Add the service account to the Act as part of the Operating System local policy

Stop the SIA and restart with the service account in domain\user format

To verify the service account is working

You should be able to login via client tools (deski, designer, business views, CCM, etc) at this point. If an error occurs please search our KB/notes if you have an error code or open a message with support**.**

Do not move on to the next section if you cannot login to client tools

Section 4 – Setting up the java SDK for AD (bsclogin and krb5.ini)

bsclogin.conf – to load the java login module and trace login requests.

You can copy the default bsclogin file from below (replace sun with ibm is using websphere or when the web/app is on AIX)

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required debug=true;
};
```

krb5.ini – to configure the KDC's that will be used for the java SDK login requests

```
[libdefaults]
default_realm = MYDOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tgs_enctypes = rc4-hmac
default_tkt_enctypes = rc4-hmac
udp_preference_limit = 1
[realms]
MYDOMAIN.COM = {
kdc = MYDCHOSTNAME.MYDOMAIN.COM
default_domain = MYDOMAIN.COM
}
```

Replace MYDOMAIN.COM with the same domain of your service account. All DOMAIN info must be in ALL CAPS. You may list as many KDC's as you want but for initial configuration it is recommended to just have 1 to simplify testing.

Replace MYDCHOSTNAME with the hostname or a domain controller.

To look up your information you can open a DOS window, execute the set command, then look up the logonserver and the USERDNSDOMAIN. Use these values for the MYDCHOSTNAME and MYDOMAIN.COM respectively.

Using this set command the LOGONSERVER.DNSDOMAIN.COM = the default KDC

To verify the krb5.ini can successfully receive a ticket (this does not verify multi-domain issues)

navigate from DOS command line to the Boinstall\javasdk\bin directory. By default this is c:\program files\business objects\javasdk\bin

Run kinit username hit enter and type your password. If the KDC in the krb5.ini is correct you should receive a ticket

KB 1245178 and **KB 1429745** for advanced krb5.ini settings

Section 5 – Configuring java Infoview and CMC (3.1 or later)

Add the following lines to the tomcat java options. Tomcat must be restarted to test.

```
-Djava.security.auth.login.config=c:\winnt\bsclogin.conf
-Djava.security.krb5.conf=c:\winnt\krb5.ini
```

Verify bsclogin.conf was added properly

After the restart the bsclogin (with debug=true option from earlier) will force user logon attempts to show up in the std.out. To verify the path is correct attempt to logon to infoview (with AD selected in the drop down) then view the std.out, scroll to the end and the username should appear in username@REALM.COM

If you have a **commit succeeded** then the java SDK portion is working for infoview. At this point a successful test user will be able to login to java infoview and CMC.

Enable SDK tracing if needed with the following java option

```
-Dbobj.logging.log4j.config=verbose.properties
```

The log files are located in documents and settings\tomcat user\.businessobjects

-Dsun.security.krb5.debug=true

The –Dsun logging will add additional levels of Kerberos trace information

If you only want manual AD logon then at this point you are done!

Section 6 – Configuring and testing SSO server side (web.xml and server.xml)

Server.xml — For Tomcat servers it is necessary to increase the default HTTP Header size in the server.xml. Kerberos login requests contain group information and this requires a larger header size. 16384 is usually large enough but if your AD contains users that are a member of many groups (50 or more AD groups). You may need to increase this size to 32768.

Default path is c:\program files\business objects\tomcat55\conf\server.xml

NOTE: Make a backup copy of any XML files prior to editing

In the server.xml you will want to define any "**maxHttpHeaderSize="16384**" or higher (if needed).

```
<!—Define a non-SSL HTTP/1.1 Connector on port 8080 →
<Connector URIEncoding="UTF-8" acceptCount="100" connectionTimeout="20000"
disableUploadTimeout="true" enableLookups="false" maxHttpHeaderSize="16384"
maxSpareThreads="75" maxThreads="150" minSpareThreads="25" port="8080" redirectPort="8443"/>
```

Web.xml – Default path is c:\program files\business objects\tomcat55\InfoViewApp\WEB-INF\web.xml

```
<context-param>
  <param-name>authentication.default</param-name>
  <param-value>secWinAD</param-value>
</context-param>
<context-param>
  <param-name>siteminder.enabled</param-name>
  <param-value>false</param-value>
</context-param>
<context-param>
  <param-name>vintela.enabled</param-name>
  <param-value>true</param-value>
</context-param>
```

- Remove open and close comments from auth filter (bold <!-- →)
- Set the idm.realm to your service account domain. MUST be in ALL CAPS
- Set your idm.princ to the service account
- Comment out the legacy logging (bold <!-- →)

```
<!—
<filter>
  <filter-name>authFilter</filter-name>
  <filter-class>com.businessobjects.sdk.credential.WrappedResponseAuthFilter</filter-class>
  <init-param>
    <param-name>idm.realm</param-name>
    <param-value>VTIAUTH08.COM</param-value>
  </init-param>
  <init-param>
    <param-name>idm.princ</param-name>
    <param-value>bossosvcacct</param-value>
  </init-param>
  <init-param>
    <param-name>idm.allowUnsecured</param-name>
    <param-value>true</param-value>
  </init-param>
  <init-param>
    <param-name>idm.allowNTLM</param-name>
    <param-value>false</param-value>
```

```
    </init-param>
<!—
    <init-param>
      <param-name>idm.logger.name</param-name>
      <param-value>simple</param-value>
      <description>
        The unique name for this logger.
      </description>
    </init-param>
    <init-param>
      <param-name>idm.logger.props</param-name>
      <param-value>error-log.properties</param-value>
      <description>
        Configures logging from the specified file.
      </description>
    </init-param>
  →
    <init-param>
      <param-name>error.page</param-name>
      <param-value>../logonNoSso.jsp</param-value>
      <description>
        The URL of the page to show if an error occurs during authentication.
      </description>
    </init-param>
  </filter>
  →
```

You must also remove the comments from the filter mapping (separate section)

```
  <!--
  <filter-mapping>
    <filter-name>authFilter</filter-name>
    <url-pattern>/logon/logonService.do</url-pattern>
  </filter-mapping>
  -->
```

Save the web.xml

NOTE: If in the same cluster deployed on the exact same version/patch then this file can be copied between machines. It may be copied from different environments again if the product/version are exactly the same and the CMS name is modified to = the destination environment.

It may not be copied if any patch is different, or any different/additional products (that modify the .war files) have been installed

Configuring Java Options for vintela server components

```
-Dcom.wedgetail.idm.sso.password=password
-Djcsi.kerberos.debug=true
```

Verifying vintela filter is loaded successfully

If the credentials are obtained for serviceaccount@IDM.REALM.COM then vintela filter is loading successfully.

Verifying a valid vintela idm.princ@IDM.REALM

If credentials are not obtained then you can test by running kinit (same steps as earlier)

```
C:\program files\business objects\javasdk\bin\kinit bossosvcacct
```

Make sure the browser is setup properly for client side testing **KB 1379894** (IE) and **KB 1263764** (firefox)

Troubleshooting client side issues must be done with 3rd party tools since SSO occurs external to business Objects and the web/app. **KB 1370926** will create log files. Open a message with support if you need help interpreting them under boj-bip-aut

Section 7 – Additional information and settings

Detailed troubleshooting and best practices can be found in **KB 1476374**

For manual logon use http://server:port/InfoViewApp/logonNoSso.jsp

If using multiple forests check **KB 1323391**

Additional Steps - Cleanup tracing, add keytab, Constrained Delegation

- debug=true in the bsclogin.conf (set by in section 4 you can also leave this on as well)
- -Dbobj.logging.log4j.config=verbose.properties (may have been added to java options turn it off)
- -Djcsi.kerberos.debug=true java option (set in section 7 also turn off when not needed)
- Dcom.wedgetail.idm.sso.password=pw (**only remove when you have a valid keytab configured below**)
- Switch Tomcat 5.5 back to local system (if running under service account for verbose tracing)

Do not setup constrained delegation or the keytab until SSO is verified working as troubleshooting is much more difficult when trying to add these too.

Encrypting your service account password with a keytab

Create a keytab with ktpass (found on DC's and can be downloaded from Microsoft)

```
ktpass -out bosso.keytab -princ serviceaccount@REALM.COM –pass user_password -kvno 255-ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

Sample

```
ktpass -out bosso.keytab -princ bossosvcacct@VTIAUTH08.COM –pass password -kvno 255-ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

Copy the bosso.keytab to the c:\winnt directory then add the following 4 lines in the web.xml

```
<init-param>
<param-name>idm.keytab</param-name>
<param-value>c:\winnt\bosso.keytab</param-value>
</init-param>
```

If you receive RC4 errors then you may need to get a newer version of ktpass from Microsoft. Please consult Microsoft regarding ktpass errors

See **KB 1359035** to test the keytab separately if SSO stops upon adding this setting

Setting up Constrained Delegation

See **KB 1184989** for setting up **constrained delegation** most steps are in Microsoft 1 in the web.xml

References

XI 3.1 Admin Guide http://help.sap.com/businessobject/product_guides/boexir3/en/xi3_bip_admin_en.pdf

ADExplorer http://technet.microsoft.com/en-us/sysinternals/bb963907

Netmon 3.2 http://www.microsoft.com/DOWNLOADS/details.aspx?FamilyID=f4db40af-1e08-4a21-a26b-ec2f4dc4190d&displaylang=en

Wireshark http://www.wireshark.org/download.html

kerbtray - http://www.microsoft.com/downloads/details.aspx?FamilyID=4e3a58be-29f6-49f6-85be-e866af8e7a88&displaylang=en

SAP SDN Business Objects User forums (requires free registration) https://www.sdn.sap.com/irj/sdn/businessobjects-forums

Additional Notes

AD 2008 functional level 2003 BO server Windows 2008 server SP2 for the CMS and tomcat (3rd party)

XI 3.1 SP3 Tomcat 5.5 (integrated) Java 1.5 (integrated) VSJ 3.3 (integrated)

Copyright