Configuring Vintela SSO in Distributed Environments – Vintela Configuration Only

Applies to:

Primarily XI 3.x but can also be used for XIR2 SP2 and later

Summary

This paper combines all the steps from the XI 3.x admin guide(s) with the latest best practices and all the latest SAP notes regarding vintela, kerberos and java AD configuration.

Author: Tim Ziemba BSEE, MCSE

Company: SAP Business Objects

Created on: 10 December 2008

Author Bio

Veteran of varied IT/communications. Employed with SAP Business Objects Support in Lake Mary, FL since September 2005. Currently specializing in Authentication - XIR1, XIR2, XI 3.x BIP/IDD other areas include administration, migration, deployment and network troubleshooting.

Table of Contents

Please make sure you can perform the simple tests at the end of each section as they are designed in an order where 5 needs 4 which needs 3 which needs etc… There are 4 sections needed to get SSO working. Important notes are highlighted in RED code is in BLUE

Key Terms

Some terms or acronyms we will be referring to throughout this document

CMS – Windows service that is responsible for authorization when using vintela SSO

CMC- Web Admin tool used to configure the CMS service and other parameters for Business Objects Enterprise

CCM – Utility found on Business Objects Enterprise servers that can view Business Objects server/services/processes

SSO - Single Sign-On – The ability to access an application without entering login credentials also known as silent sign-on, automatic logon, etc

Vintela - 3rd party SSO tool packaged in with Business Objects products since XIR2 SP2 to provide quick easy SSO configuration. Since it is OEM'd no external products need to be installed for SSO to work.

JAS – a take off from WAS - Web Application Server - but in this context we are referring to Java Application Servers ONLY in order to differentiate from IIS .net and other JAS (tomcat, Websphere, Weblogic, Jboss, Oracle App Server, etc)

Service account – Refers to an Active Directory user with special permissions (such as a fixed non-changing password or SPN)

SPN – Service Principal Name refers to an additional alias and attribute to an AD account. Various tools can be used to add an SPN to an AD account. It's much like a UPN or sam accountname except there can be multiple SPN's per account. The SPN is a primary access point for kerberos applications.

UPN – User Principal Name in AD (i.e. user@domain.com).

Sam Account Name – common logon name in AD (i.e. domain\user)

HLB – Refers to Hardware Load Balancers (used to split the load between JAS) DNS redirects generally will follow the same rules as an HLB.

Troubleshooting Tools that may be needed

Kinit - Provided with java SDK, it can verify krb5.ini configuration by submitting TGS requests to the KDC

AD Explorer - Can be downloaded from Microsoft Sys internals , used to search and verify AD account attributes

MMC - Microsoft Management Console can be accessed from any windows 2000/2003 server

Packet Scanner – The built in Microsoft Netmon, free 3rd party ethereal/wireshark, or other utility that can trace and record network packets between various hosts.

Kerbtray – Microsoft utility used to display or purge kerberos tickets on a client workstation

NOTE: check out the references at the end of this document to links for the above tools and more.

Section1- Planning your Service account Configuration

Prior to configuring SSO you must create at least 1 service account. There are 3 completely separate roles for a service account. These roles can be shared with 1 account or spread across many. A best practice would be to use a common naming convention that will be introduced in this white paper. This can make troubleshooting easier and management simpler.

Vintela SSO account Used by JAS (enabled in web.xml) for launching the vintela filter. (Currently requires ktpass so SPN and UPN are the same value and to encrypt the password into a keytab file. Requires additional SPN's for all HTTP points of entry (JAS, HLB, etc). This account does not actually run any services or require any local permission unless combined with the CMS service account. For this doc we will assume groups have already been mapped and manual AD auth is already working.

Naming Convention for service account(s) (only suggested but helpful for troubleshooting and administration)

A) **One service account for all roles**/environments (use a name like BOSSOSVCACCT)

C) **One service account per environment** (Use BOSSOPROD, BOSSODEV, BOSSOQA)

You can have as many or as few service accounts as you would like. If SPN's are involved the less service accounts the less likely the chance for duplicate SPN's (this is an issue where AD cannot respond to kerberos requests due to conflict of the same aliases (SPN) created for multiple accounts). The per role option is excellent as well and will make tracing a little easier if packet scanning is required. **If you have any questions please open a message with support prior to executing these steps or you can post you questions on the SDN forums.**

After planning you naming convention and service accounts then you are ready to create your service accounts. Service accounts will need to be created in Active Directory by a Domain Admin. For the rest of this document we will assume the all in 1 service account but references will be made to the roles/environments. Screenshots will be created with the newest version of Enterprise (there may be slight differences if using older versions). To note this configuration is only possible with Business Objects XIR2 SP2 or later.

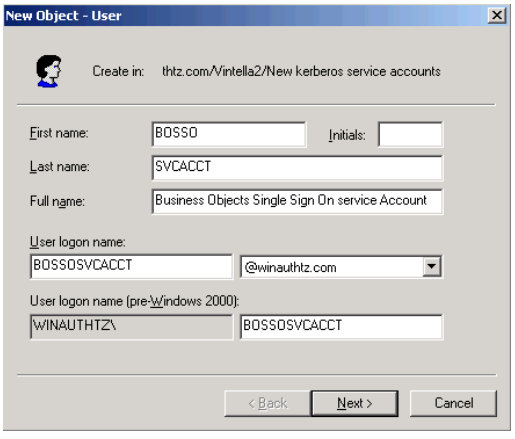
READ THIS FIRST

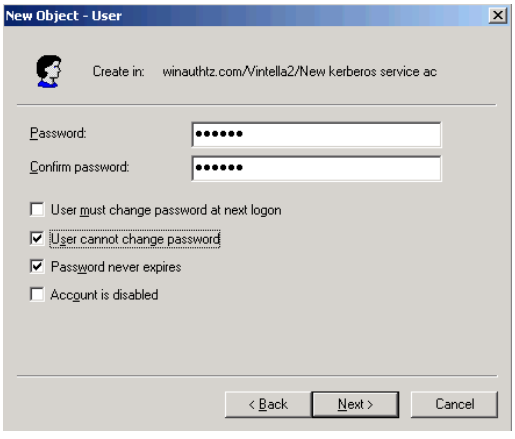
Even though there will be screenshots with steps completed in Active Directory throughout the rest of this document, please refer to your companies local AD/network Admins when attempting these steps. The steps documented were tested in house, but your local AD admin is the only one familiar with your companies AD and its policies. If any questions arise please use the business objects user forums or open a message with support.

Section 2 - Creating and preparing the service account for kerberos delegation

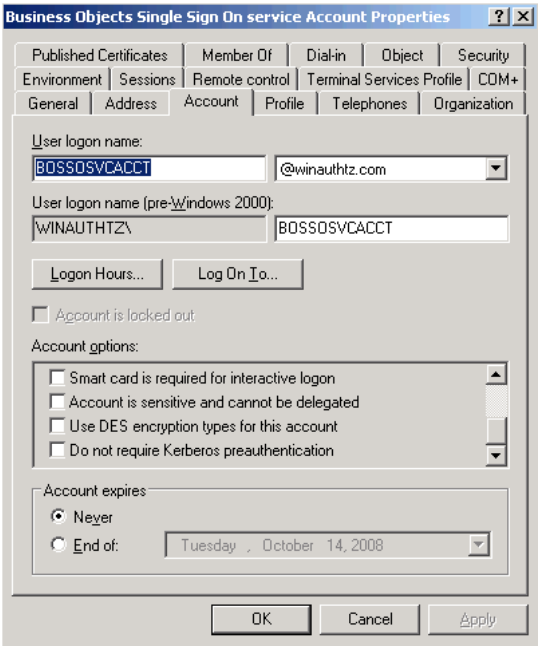
Below are suggestions for AD Domain Admin to create an account in AD. The following must be in place before you will be able to configure Business Objects for SSO.

Below screenshots depict the creation of an "all inclusive" service account





Account is BOSSOSVCACCT, password is set to never expire. Should a password expire, then the functionality dependant on that account will fail (see the roles above). You will also need to enable delegation after running ktpass (test2)



Some of our legacy Product Guides and Whitepapers required “Use DES encryption types for this account” to be enabled on kerberos service accounts. In most cases DES is not required or desired and should not be used in XI 3.0 or later.

When DES is not selected RC4 will be used by default with AD. In some cases on earlier versions of XIR2 with java SDK 1.4.2, RC4 may not work without updating the JDK to 1.5. Since XI 3.x comes with JDK 1.5 using RC4 is preferred. **For this document do NOT select “Use DES encryption types for this account”.**

Steps for running KTPass (only installed on a DC by default)

KTPASS is a built in kerberos command (on DC’s by default). With the options selected it will essentially perform 3 functions.

1) Create an RC4 encrypted keytab file with the password/filename specified in the command.

2) Rename the windows 2003 user name (UPN) to the value specified in the idm.princ.

3) Create an SPN for the service account with the value specified in the idm.princ.

In order for vintela (role 3) to use a service account the UPN and SPN must match.

KTPASS should be run on any account that will be used for vintela (just once per this doc and many times per legacy docs). Syntax that should be used is below.

```
ktpass -out myname.keytab -princ BOSSO/bossosvcacct.mydomain.com@REALM.COM -mapuser
bossosvcacct@REALM.COM -pass yourpw -kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

1. Replace myname with any name for your keytab such as BOSSO.keytab (also must be specified in web.xml)
2. Replace mydomain.com with the full domain name where the service account was created
3. Replace REALM.COM with the default domain (often the same value as above). This will be the value in your web.xml idm.realm (your default realm or domain in AD). Make sure this is in ALL CAPS whenever it is entered (java SDK’s may requires this)
4. Replace yourpw with your service account password (this password will also be used in your tomcat java options during the initial configuration)

Sample ktpass command:

ktpass -out vinsso.keytab -princ BOSSO/bossosvcacct.mydomain.com@WINAUTHTZ.COM -mapuser bossosvcacct@WINAUTHTZ.COM -pass password -kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT

here is a sample output – notice there are no errors or warnings (if an error or warning should appear check syntax and contact Business Objects support).

Targeting domain controller:bobj-w2k3-db-tz,winauthtz.com Successfully mapped BOSSO/bossosvcacct.winauthtz.com to bossosvcacct

Key created.

Output keytab to vinsso.keytab:Keytab version: 0x502

keysize 81 BOSSO/bossosvcacct.mydomain.com@MYDOMAIN.COM ptype 1 (KRB5_NT_PRINCIPAL) vno 255 etype 0x17 (RC4-HMAC) keylength 16 (0x91c0c7b367db3f2d6684b6690a5ff6e2)

NOTE: If you receive encryption not supported errors for RC4 try and download the windows 2003 SP2 ktpass version or later.

Verifying creation of the default SPN

the SPN (BOSSO/bossosvcacct.winauthtz.com) was configured properly, run a setspn –l on the service account

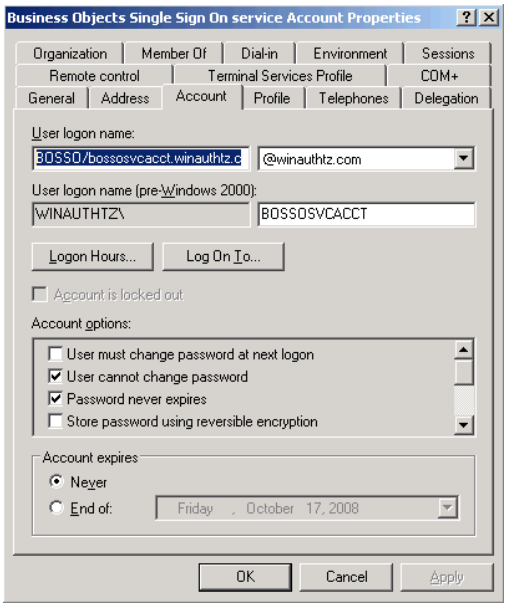
Setspn –l bossosvcacct should be…

Registered ServicePrincipalNames for CN=Business Objects Single Sign On service Account,OU=New kerberos service accounts,OU=Vintella2,DC=winauthtz,DC=com:

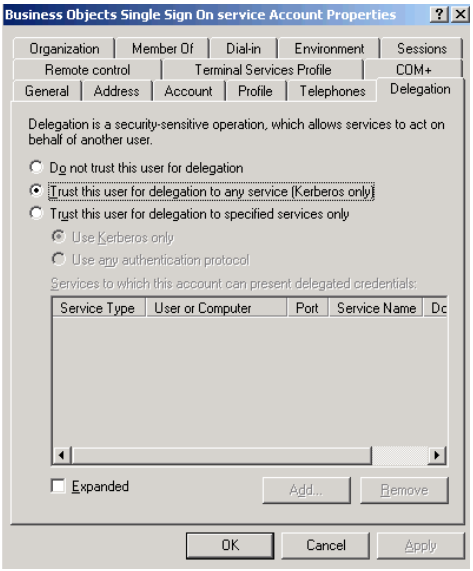
BOSSO/bossosvcacct.winauthtz.com

Verifying the account UPN was modified

Use the MMC to look up the account and verify the 2003 username is = to the SPN (screenshot below)



NOTE: This would also be a good time to verify delegation is enabled on the vintela SSO account. Screenshot below in 2003 native. If using 2000 or mixed mode AD then look for a checkbox under the account properties.



Locate the keytab file

Perform dir at the command prompt the keytab file should also be present

You should copy this file to any server that has a JAS installed that will be performing vintela SSO

By default it should be copied to the c:\winnt\ with the krb5 and bsclogin (created later in this doc)

Running setspn to create access points for SSO

Now we need to generate SPN's for all clients and possibly JAS (if using a fixed IP). When a client attempts to login to infoview it will use the URL (hostname/FQDN/IP) to generate a kerberos TGS request. In order for clients to make this request an SPN = to the hostname/FQDN/IP) must be added to the service account for it to succeed. Use the setspn command to create client SPN's

Setspn –a HTTP/hostname of each tomcat server

Setspn –a HTTP/FQDN of each tomcat server

Setspn –a HTTP/ip.ip.ip.ip of each tomcat server to allow vintela to work on the server

Examples…

Setspn –a HTTP/r31-rtm-tz bossosvcacct

Setspn –a HTTP/r31-rtm-winauthtz.com bossosvcacct

Setspn –a HTTP/10.55.220.100 bossosvcacct

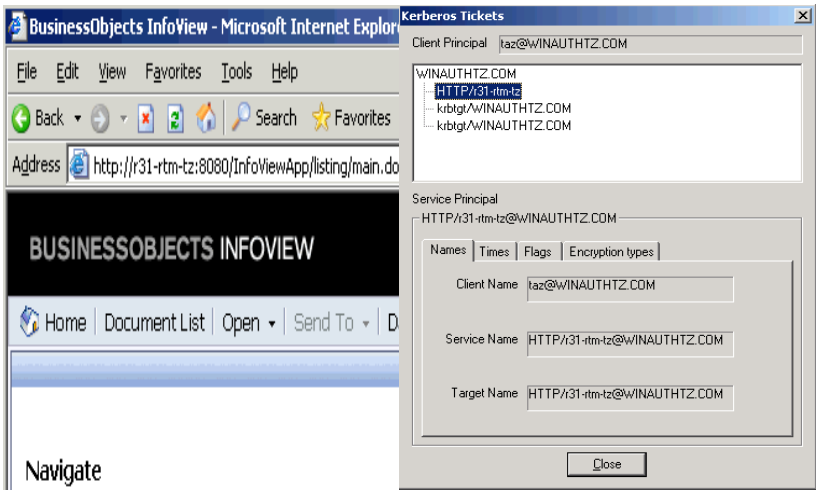
HTTP SPN's are going to generally be needed in pairs (FQDN and hostname). Each SPN acts as a point of entry for client requests. When performing SPNEGO (SSO) on the client the URL is used to generate a client TGS request

NOTE: When performing SPNEGO locally on a JAS it will default to NTLM and fail. A typical work around is to create an HTTP/ip.ip.ip.ip SPN and add it to the browsers local intranet sites. This will allow for testing SSO on the JAS.

At this point you can continue on to configure any and all Business Objects servers for SSO. The BOSSO/bossosvcacct.mydomain.com SPN can be used to configure manual AD authentication (CMC-SPN) and the web.xml (idm.princ). For more clarification see the samples below

Some examples below

Notice the http://r31-rtm-tz becomes http/r31-rtm-tz in kerbtray (link in reference section)

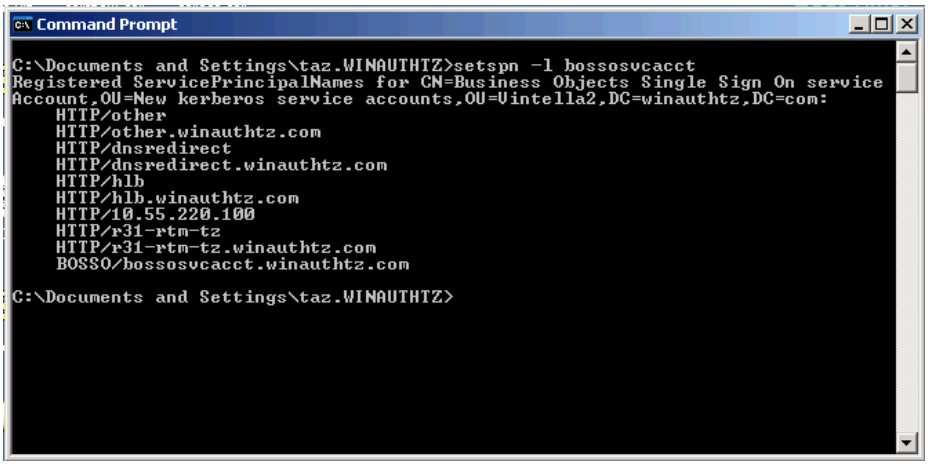


To View all created SPN's

When finished Run setspn –l bossosvcacct

To view all created SPN's

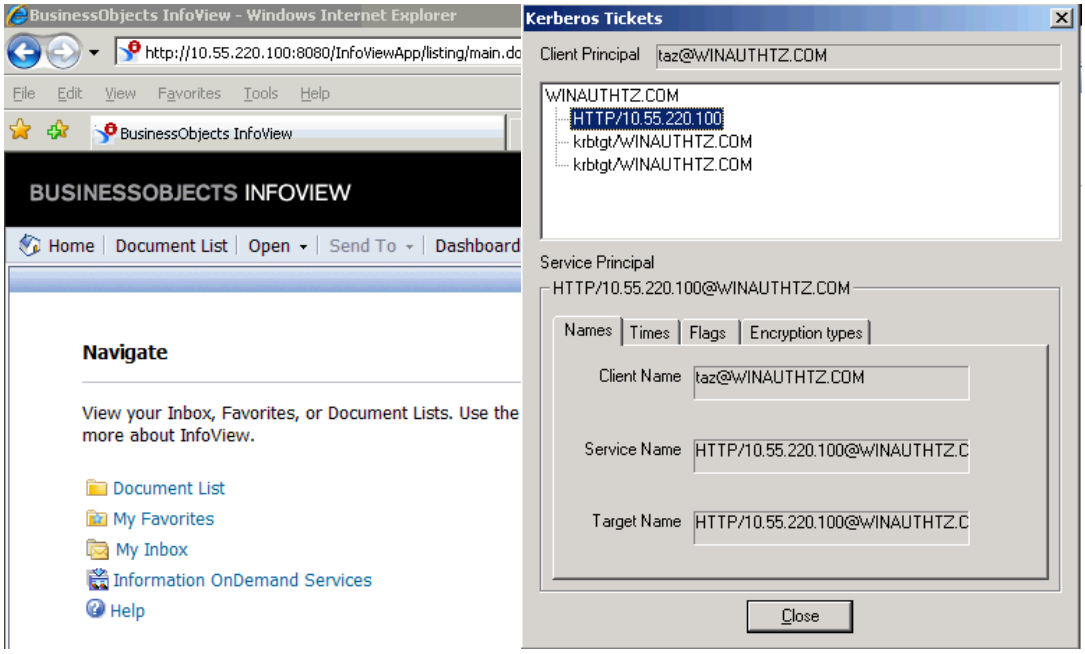
Sample output below in screenshot



The original SPN created during ktpass (BOSSO, plus HTTP pair SPN's for hlb, dns, r31-rtm-tz, and other).These simulate an environment with 1 tomcat server, that can be accessed via hardware load balancer (hlb), a redirect (DNS), and possibly something else (other).

There is also an IP SPN for the tomcat server. By default vintela does not work on the server. However when using an IP SPN we have been able to get tomcat to SSO on the local server.

Sample below



This example shows http://10.55.220.100 becoming http/10.55.220.100 in kerbtray (link in references)

Section 3 – Configuring and testing vintela 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 than default 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.

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

NOTE: Make a backup copy of any XML files prior to editing to insure default values can always be retrieved

In the server.xml you will want to define any "non-SSL HTTP/1.1 Connector on port 8080" or "SSL HTTP/1.1 Connector on port 8443" (if using SSL) have maxHttpHeaderSize="16384" or higher (if needed).

Sample

```
<!—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 – This is where the vintela filter is enabled. The changes below consider a default web.xml.

In most cases when using SSO you will want to change your authentication default to secWinAD, siteminder, must be set to false, and vintela to true

Sample

```
<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 default REALM (the one from the ktpass step) MUST be in ALL CAPS

Set your idm.princ to the default SPN (also from the ktpass step)

```
<!—
<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>WINAUTHTZ.COM</param-value>
   </init-param>
   <init-param>
      <param-name>idm.princ</param-name>
      <param-value>BOSSO/bossosvcacct.winauthtz.com</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

Verifying web.xml settings

If the settings don't seem to have an effect, open the web.xml with a browser such as IE. Review the changed settings (the values what are uncommented should show up in dark text. Commented values will appear grayed out).

Configuring Java Options for vintela server components

Then 3 more options must be added to the tomcat java options

The wedgetail.sso.password is the password for the vintela SSO account (ktpass step earlier)

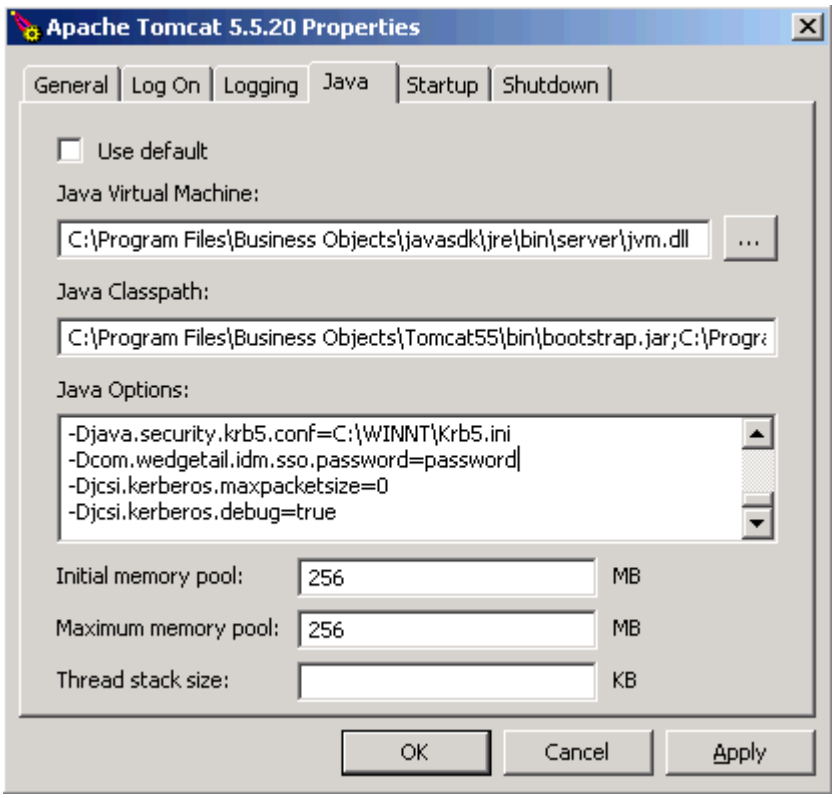
The max packet size will force SSO clients to use TCP (UPD issues discussed earlier)

The DJCSI.kerberos.debug options will enable a start up trace of the vintela filter.

-Dcom.wedgetail.idm.sso.password=password

-Djcsi.kerberos.maxpacketsize=0

-Djcsi.kerberos.debug=true



Verifying vintela filter is loaded successfully

stop tomcat, delete, or move the C:\program file\business objects\tomcat55\logs*.*

restart tomcat, wait 10-20 seconds or so (to allow the vintela filter to initialize). Search the std.out for "credentials obtained" (without the "") for the BOSSO/bossosvcacct.winauthtz.com@WINAUTHTZ.COM. This is also the UPN of the vintela SSO account or the combination of idm.princ@IDM.REALM from the web.xml

If the credentials are obtained then vintela filter is loading successfully. You may proceed attempt to test SSO from the client machines or from the server (NOTE: must have an IP SPN defined in section 2 and use the IP address in the URL)

Verifying a valid vintela idm.princ@IDM.REALM

If credentials are not obtained then you can compare the UPN (from Microsoft Management Console –mmc) = the idm.princ@IDM.REALM and you can take this value and test by running kinit (same steps as earlier)

C:\program files\business objects\javasdk\bin\kinit BOSSO/bossosvcacct.winauthtz.com

Sample success in the screenshot below

If you receive any errors please search our notes, the forums, or open a message with support

NOTE: If using XIR2 with java SDK 1.4.x this may not work with RC4 – per this doc. You should either upgrade your JDK to 1.5.x (note 1262507) or use the XIR2 vintela docs.

When kinit works, and credentials are obtained in the std.out then we can finish the configuration by testing SSO from the client side in the next section

Section 4 – Tracing tomcat & packet scanning client SSO issues

At this point you should have manual AD auth working for all applications (including infoview), the vintela filter loaded, and tested on the server. If not please finish the earlier sections before attempting to troubleshoot SSO

The following tracing options were tested in 3.1 with tomcat 5.5

Newly added to the 3.1 admin guide is

-sun.security.krb5.debug=true

This logging is for java AD (AKA manual logon). It shows much more than the **debug=true** that we add to the bsclogin.conf

For vintela we still use (when you see djcsi think vintela) both on XIR2 and XI 3.x

-Djcsi.kerberos.debug=true

For this logging to work you must not have a keytab file in the web.xml (or cached web.xml in tomcat 5.5). It will only trace when using the tomcat password option for vintela **(-Dcom.wedgetail.idm.sso.password=mypassword**) and the keytab is commented out

Troubleshooting client SSO issues

Use kerbtray to view and purge tickets on the client machine (even if the client is the server) On a successful login attempt you should receive 3 tickets (1 krbtgt for the user initial flag, 1 krbtgt for the user, and 1HTTP SPN for the URL in which vintela SSO was attempted) . Refer to the screenshots in section 2

Use wireshark, netmon, or other packet scanner on the client to capture kerberos traffic (port 88) and look for error messages. Check the support site or open a message with support if you cannot resolve.

For more detailed logs use netmon, or ethereal/wireshark on the client workstation. If you need help interpreting the logs please open a message with support. Packet scans can contain confidential information

and should not be posted on the SDN forums or other public places.

NOTE: Purge tickets with kerbtray prior to running a packet scan or important data may not be captured. Verify Delegation is enabled on the service account

If URL has a . such as an IP address or FQDN then it MUST be added to your browser local intranet sites. In multi forest environments use the FQDN ONLY+

Other Tests: For manual tests on XI 3.x use http://server:port/InfoViewApp/logonNoSso.jsp

On XIR2 http://server:port/businessobjects/enterprise115/desktoplaunch/InfoView/logonForm.do

If using multiple forests (XI 3.1 and later) then verify that DNS can resolve your remote forest forward lookup zone. In some cases this can be worked around by adding the FQDN of the URL in the local hosts file and local intranet sites. Verify a full tway forest trust exists between the domains.

If you receive Null on XI 3.x or java.lang.null.pointerexception in XIR2 verify that delegation is enabled (and not constrained) see section 1 test2.

Steps for packet scanning client requests

1) Install kerbtray and run it - C:\program files\resource kit\kerbtray.exe
2) Right click on the icon in the lower left hand corner and purge all tickets
3) Install and run your packet scanner (on the client machine)
4) Attempt SSO by accessing the vintela URL http://server:port/InfoViewApp/ http://server:port/businessobjects/enterprise115/desktoplaunch for/ XIR2
5) Wait about 10 seconds after the failure
6) Stop your scanner and save your file (.cap or .pcap). Open a message with support and attach the file with a description of the error or symptoms

Additional Steps - Cleanup tracing, add keytab, and forcing an AD site

At this point you have completed and tested each section (1-7) . You can now remove any tracing that was enabled

Remove the following(if they exist)…

-Djcsi.kerberos.debug=true java option (set by default in section 3)

Dcom.wedgetail.idm.sso.password=mypassword (only remove if you have a valid keytab configured)

Switch Tomcat 5.5 back to local system (if running under service account for verbose tracing)

Encrypting your service account password

Copy the vinsso.keytab (created during ktpass step) to the c:\winnt directory then specify the following in the web.xml (after the idm.princ setting). Once this is added you can remove the wedgetail.passowrd option from the tomcat java options. At this point your vintela SSO account password will now be encrypted with RC4.

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

Setting up an AD site

In large deployments it may also be necessary to use the idm.ad.site parameter to force vintela to login to a set of specific DC's. If so add this section next and add the following option to the tomcat java options

This may be required if vintela is trying to authenticate against DC's that are non local or on the other side of a firewall(discovered in packet scanning or Djcsi tracing).

```
<init-param>
<param-name>idm.ad.site</param-name>
<param-value>mysite</param-value>
</init-param>
```

Java options

```
-Djcsi.kerberos.site=mysite
```

References

XIR2 Java AD https://www.sdn.sap.com/irj/sdn/go/portal/prtroot/docs/library/uuid/e0edd98d-c43e-2b10-e09a-e0a89931cedc

XIR2 Vintela https://www.sdn.sap.com/irj/sdn/go/portal/prtroot/docs/library/uuid/3097fb98-c63e-2b10-e7b8-fb7253566373

XI 3.0 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

All steps in this document were performed in the following environment

AD 2003 functional level aka 2003 native (3rd party)

Windows 2003 server SP2 for the CMS and tomcat

XI 3.1

Tomcat 5.5 (integrated)

Java 1.5 (integrated)

VSJ 3.1 (integrated)

Copyright