RSA® Federated Identity Manager 4.2 Troubleshooting Guide

This document provides solutions to common problems that you may encounter with RSA® Federated Identity Manager 4.2 release.

Viewing Log Files

By default, the audit, system, and debug log files are available in the ***FIM-domain-directory*\rsa-fim-config\log** directory. You can change the names of these log files in the **log4j.xml** file. For instructions, see the *Administrator's Guide* (**admin.pdf**).

Debugging

Debug logging is disabled by default, so you must enable debug logging. You can also enable debug logging at runtime. For instructions on enabling debug logging, see the *Administrator's Guide* (**admin.pdf**).

If you want to view the second-level status codes that describe errors in more detail, set the property **fim.return.secondary.status.codes.with.error.responses** to **true** in the **fim.properties** file.

Common Symptoms and Fixes

Because RSA Federated Identity Manager is often used to perform web single sign-on (SSO), most Federated Identity Manager error messages are displayed in the browser window. Some of the common symptoms and fixes are described in the following topics.

Single Logout Does Not Work on Apache

Symptom

When you perform single logout in an environment that supports Apache as a web server, the single logout functionality does not work properly. For example, when you perform single logout using an HTTP URL, you can access the protected pages on the service provider or identity provider without being prompted for the user name and password. The reason for this behavior is that the default settings of the Apache **mod_jk** file do not contain the content expire parameter.

Note: If you are using the single logout service with an Internet Information Services (IIS) server where the content expire parameter is enabled, you will not face any problems.

Fix

Add the content expire parameter to Apache, as follows:

1. From the **//$apache home$/conf/** directory, open the **httpd.conf** file.
2. Add the following lines:

```
<IfModule mod_expires.c>
   ExpiresActive on
   ExpiresByType image/gif "access plus 1 months"
   ExpiresByType text/html "access 1 seconds"
   ExpiresDefault "access plus 1 seconds"
</IfModule>
```

3. Uncomment the following line:

```
LoadModule expires_module modules/mod_expires.so
```

4. Set the value of the content expire parameter to **Enabled**.
5. Restart the server.

Single Sign-On Fails due to Incorrect Authentication Policy Settings

Symptom

When you perform single sign-on (SSO) to access a web page, you get the following error message:

```
Error stack trace:
com.rsa.fim.profile.sso.SSOProfileException: The localAuthnURL
can not be obtained by mapping a local authentication method
 at
com.rsa.fim.profile.sso.SSOHelper.nullCheck(SSOHelper.java:393)
 at
com.rsa.fim.profile.sso.SSOHelper.handleNoTicket(SSOHelper.java
:760)
 at
com.rsa.fim.profile.sso.SSOProfileBean.processAuthnRequest(SSOP
rofileBean.java:583)
 at
com.rsa.fim.profile.sso.SSOProfile_5wyj3w_EOImpl.processAuthnRe
quest(SSOProfile_5wyj3w_EOImpl.java:206)
 at
com.rsa.fim.servlet.sso.SSOService.doGet(SSOService.java:82)
 at
javax.servlet.http.HttpServlet.service(HttpServlet.java:743)
 at
javax.servlet.http.HttpServlet.service(HttpServlet.java:856)
 at
weblogic.servlet.internal.StubSecurityHelper$ServletServiceActi
on.run(StubSecurityHelper.java:223)
 at
weblogic.servlet.internal.StubSecurityHelper.invokeServlet(Stub
SecurityHelper.java:125)...
```

SSO fails for one of the following reasons:

- The authentication policy settings are incorrect.
- An incorrect authentication policy is specified for the local entity.

Fix

1. Check the authentication policy settings:
   a. In the Administration Console, click **Policies > Authentication > Manage Existing**.
   b. Select the respective authentication policy, and click **Edit**.
   c. Specify the values for **Local to SAML Authentication Mappings** and **Auth URL** fields.
2. Select the correct authentication policy for the local entity:
   a. Click **Entities > Local Entities > Manage Existing**.
   b. Select the local entity, and click **Edit**.
   c. In the **Default Authentication Policy** field, select the above configured authentication policy.

For more information, see the *Administration Console Help*.

Single Sign-On Fails in a Cluster Setup due to Inability to Connect to RSA Access Manager Server

Symptom

When you perform single sign-on (SSO) to access a web page in a clustered environment, you see the following error message:

```
com.rsa.fim.exception.PluginException: Unable to connect to CT
Server using Admin API. Please verify Entitlements Server is
running and check Connection Configuration->Entitlements Server
settings. Error trying to connect to the Entitlements Server
 at
com.rsa.fim.plugin.impl.ct.connection.CTConnectionPlugin.init(C
TConnectionPlugin.java:44)
 at
com.rsa.fim.plugin.PluginFactory.initPlugin(PluginFactory.java:
201)
 at
com.rsa.fim.plugin.PluginFactory.getNewPluginObject(PluginFacto
ry.java:179)
 at
com.rsa.fim.plugin.PluginManager.checkOut(PluginManager.java:84
)
 at
com.rsa.fim.plugin.PluginManager.reloadPlugin(PluginManager.jav
a:152)
 at
com.rsa.fim.util.events.cluster.PluginReloadHandler.execute(Plu
ginReloadHandler.java:28)
```

```
 at
com.rsa.fim.util.events.cluster.ObjectMessageListener.onMessage
(FIMConfigUpdateHandler.java:92)
 at
weblogic.jms.client.JMSSession.onMessage(JMSSession.java:4060)
 at....
```

The reason for this error is that the configuration information contains localhost. When you run the Configure My System wizard, by default, all the plug-ins and connections for the Dispatcher Server or Entitlements Server are created with the hostnames set as localhost. Therefore, the runtime nodes are not able to connect to the admin server and you see the exception message.

Fix

You must replace the hostname that contains **localhost** with the fully qualified domian name (FQDN) of the machine where RSA® Access Manager is configured, and reload the RSA Access Manager connection.

SSO Fails in a Clustered Setup due to Incorrect Cluster Settings

Symptom

When you perform single sign-on (SSO) in a clustered environment, you get the following error message:

```
Error message: Cannot find requested objectWhile trying to
lookup 'com.rsa.fim.profile.common.FIMProfileHome' didn't find
subcontext 'com'. Resolved '' Error stack trace:
com.rsa.fim.exception.util.ServiceLocatorException: Cannot find
requested objectWhile trying to lookup
'com.rsa.fim.profile.common.FIMProfileHome' didn't find
subcontext 'com'. Resolved '' at
com.rsa.fim.util.ServiceLocator.getRemoteHome(ServiceLocator.ja
va:163) at
com.rsa.fim.servlet.ServletHelper.getFIMProfile(ServletHelper.j
ava:928) at
com.rsa.fim.servlet.discovery.WebAgentService.doGet(WebAgentSer
vice.java:91) at
javax.servlet.http.HttpServlet.service(HttpServlet.java:743) at
javax.servlet.http.HttpServlet.service(HttpServlet.java:856) at
weblogic.servlet.internal.StubSecurityHelper$ServletServiceActi
on.run(StubSecurityHelper.java:223) at
weblogic.servlet.internal.StubSecurityHelper.invokeServlet(Stub
SecurityHelper.java:125) at....
```

Fix

1. In the Administration Console, click **Cluster > Cluster Settings**.
2. Check that all the settings are specified correctly. Update the correct values in the **JNDI URLs** field.
3. Restart the admin server and the managed servers.

Single Sign-On Fails as the Plug-In Is Unable to Connect to the RSA Access Manager

Symptom

When you perform web single sign-on (SSO), you get the following error:

```
Error message: The name ID mapper plugin failed to operate
correctly: sirrus.runtime.RetryException:
getFedIdentityMapping( "
Unknown macro: {CT_NAME=panda, PROVIDER_TYPE=IDP,
MAPPED_DOMAIN=http}
" ) failed 6 consecutive times
(sirrus.runtime.ConnectionException: This connection to
AuthServer at 10.31.253.118:5615:anon:NO_AS_CLASS: is closed.)
Error stack trace: com.rsa.fim.profile.sso.SSOProfileException:
The name ID mapper plugin failed to operate correctly:
sirrus.runtime.RetryException: getFedIdentityMapping( "
Unknown macro: {CT_NAME=panda, PROVIDER_TYPE=IDP,
MAPPED_DOMAIN=http}
" ) failed 6 consecutive times
(sirrus.runtime.ConnectionException: This connection to
AuthServer at 10.31.253.118:5615:anon:NO_AS_CLASS: is closed.)
at
weblogic.rjvm.ResponseImpl.unmarshalReturn(ResponseImpl.java:19
5) at
weblogic.rmi.cluster.ClusterableRemoteRef.invoke(ClusterableRem
oteRef.java:338) at
weblogic.rmi.cluster.ClusterableRemoteRef.invoke(ClusterableRem
oteRef.java:252) at
com.rsa.fim.profile.common.FIMProfile_mzkd72_EOImpl_921_WLStub.
processAuthnRequest(Unknown Source) at
com.rsa.fim.servlet.sso.SSOService.doGet(SSOService.java:82) at
javax.servlet.http.HttpServlet.service(HttpServlet.java:743) at
javax.servlet.http.HttpServlet.service(HttpServlet.java:856) at
weblogic.servlet.internal.StubSecurityHelper$ServletServiceActi
on.run(StubSecurityHelper.java:223) at.....
```

The error occurs because the plug-in is not able to connect to RSA Access Manager.

Fix

1. Ensure that the plug-in connection information is configured properly in RSA Federated Identity Manager. For instructions, see the *Administration Console Help*.
2. Restart the RSA Access Manager server. For instructions, see the *Installation and Configuration Guide* (**install_config.pdf**).
3. Reload the RSA Access Manager connection from the Federated Identity Manager Administration Console. For instructions, see the *Administration Console Help*.

Single Sign-On Fails due to Mismatch in Timings

Symptom

When you perform single sign-on (SSO) to access a web page in a clustered environment, the authentication URL used by the authentication policy (specified as **Auth URL**) is displayed instead of the actual protected web page.

SSO fails for one of the following reasons:

- Timings on each node in the cluster are different.
- Clock timings on the RSA Federated Identity Manager server and RSA Access Manager server do not match.

Fix

1. Synchronize the timings on each node in the cluster.
2. Synchronize the clock timings on Federated Identity Manager and RSA Access Manager.
3. Restart Oracle WebLogic Server and the managed nodes.
4. Restart the RSA Access Manager servers.

Single Sign-On Fails due to Incorrect Configuration of Attribute Authority Using Desktop Federation

Symptom

When you perform single sign-on (SSO) to the client of the attribute authority using Desktop Federation (DF), you see the following error:

```
Error 401--Unauthorized
From RFC 2068 Hypertext Transfer Protocol -- HTTP/1.1:
10.4.2 401 Unauthorized
The request requires user authentication. The response MUST
include a WWW-Authenticate header field (section 14.46)
containing a challenge applicable to the requested resource.
The client MAY repeat the request with a suitable Authorization
header field (section 14.8). If the request already included
Authorization credentials, then the 401 response indicates that
authorization has been refused for those credentials. If the
401 response contains the same challenge as the prior response,
and the user agent has already attempted authentication at
least once, then the user SHOULD be presented the entity that
was given in the response, since that entity MAY include
relevant diagnostic information. HTTP access authentication is
explained in section 11.
```

SSO fails for one of the following reasons:

- The client is not properly configured for attribute authority or Desktop Federation.
- The identity provider is not properly configured for Desktop Federation Kerberos service.

Fix

You must configure the local intranet domains for the attribute authority and the Desktop Federation properly. For more information, see the *Installation and Configuration Guide* (**install_config.pdf**).

Single Sign-On and Single Logout Fail due to Name ID Mismatch

Symptom

When you perform single sign-on (SSO) or single logout, you get the following error:

```
Error stack
trace: com.rsa.fim.profile.logout.LogoutProfileException: The
provided NameID
does not match the stored NameID at
com.rsa.fim.profile.logout.LogoutHelper.getLocalNameID(LogoutHe
lper.java:764)
at
com.rsa.fim.profile.logout.LogoutProfileBean.processLogoutReque
st
(LogoutProfileBean.java:410) at
com.rsa.fim.profile.common.FIMProfileBean.processLogoutRequest
(FIMProfileBean.java:76) at
com.rsa.fim.profile.common.FIMProfile_mzkd72_EOImpl.processLogo
utRequest
(FIMProfile_mzkd72_EOImpl.java:652) at
com.rsa.fim.servlet.logout.LogoutService.doGet(LogoutService.ja
va:65) at
javax.servlet.http.HttpServlet.service(HttpServlet.java:743) at
javax.servlet.http.HttpServlet.service(HttpServlet.java:856) at
weblogic.servlet.internal.StubSecurityHelper$ServletServiceActi
on.run
(StubSecurityHelper.java:223) at
weblogic.servlet.internal.StubSecurityHelper.invokeServlet
(StubSecurityHelper.java:125) at
weblogic.servlet.internal.ServletStubImpl.execute(ServletStubIm
pl.java:283) at
weblogic.servlet.internal.ServletStubImpl.execute(ServletStubIm
pl.java:175) at
weblogic.servlet.internal.WebAppServletContext$ServletInvocatio
nAction.run
(WebAppServletContext.java:3245) at
weblogic.security.acl.internal.AuthenticatedSubject.doAs
(AuthenticatedSubject.java:321) at
weblogic.security.service.SecurityManager.runAs(SecurityManager
.java:121) at....
```

SSO or single logout fails for one of the following reasons:

- The name ID does not match the stored name ID.
- The name ID in the name ID plug-in does not match the name ID in the session plug-in.

Fix

- Ensure that the local name ID format used in the name ID plug-in and the session plug-in is the same:
  a. In the Administration Console on the identity provider, select **Components > Plug-ins > Manage Existing**.
  b. Select the DB Persistent Name ID plug-in, and, in the plug-in configuration, set the value for the **Local Name ID Format** field.
  c. Select the session plug-in, and, in the plug-in configuration, set the value for the **Local Name ID Format**, as specified in the preceding step.
- Change the value of the **Local Name ID Format** field:
  a. In the Administration Console on the identity provider, select **Components > Plug-ins > Manage Existing**.
  b. Select the name ID plug-in, and set the value of the **Local Name ID Format** field as **unspecified**.

Single Sign-On Fails over Secure Sockets Layer

Symptom

When you perform web single sign-on (SSO) over Secure Sockets Layer (SSL), you get the following error message:

```
Error message: Encountered a SOAP error during ArtifactResolve:
; nested exception is: java.io.FileNotFoundException:
C:\Documents and Settings\iis\.truststore (The system cannot
find the file specified) Error stack trace:
com.rsa.fim.exception.BindingProcessingException: Encountered a
SOAP error during ArtifactResolve: ; nested exception is:
java.io.FileNotFoundException: C:\Documents and
Settings\iis\.truststore (The system cannot find the file
specified) at
com.rsa.fim.binding.ArtifactBinding.extractSAMLMessage(Artifact
Binding.java:197) at
com.rsa.fim.servlet.ServletHelper.createProfileRequest(ServletH
elper.java:147) at
com.rsa.fim.servlet.sso.SSOService.doGet(SSOService.java:64) at
javax.servlet.http.HttpServlet.service(HttpServlet.java:743) at
javax.servlet.http.HttpServlet.service(HttpServlet.java:856) at
weblogic.servlet.internal.StubSecurityHelper$ServletServiceActi
on.run(StubSecurityHelper.java:223) at
weblogic.servlet.internal.StubSecurityHelper.invokeServlet(Stub
SecurityHelper.java:125) at
weblogic.servlet.internal.ServletStubImpl.execute(ServletStubIm
pl.java:283) at
weblogic.servlet.internal.ServletStubImpl.execute(ServletStubIm
pl.java:175) at
weblogic.servlet.internal.WebAppServletContext$ServletInvocatio
nAction.run(WebAppServletContext.java:3245) at
weblogic.security.acl.internal.AuthenticatedSubject.doAs(Authen
ticatedSubject.java:321) at ......
```

SSO fails for one of the following reasons:

- The truststores or keystores are not specified.
- The connection type is incorrect.

Fix

- If you are using server SSL, specify the truststore, and, if you are using mutual SSL, specify both the keystores and the truststores.
- Specify the connection type, as follows:
  a. In the Administration Console, select **Associations > Manage Existing**.
  b. Select the association, and click **Edit**.
  c. On the General Settings page, select the correct connection type.

Single Sign-On Fails due to Error in Cookie Creation

Symptom

When you perform web single sign-on (SSO), you get the following error message:

```
Error in cookie creation
```

SSO fails for one of the following reasons:

- The key generation algorithm (j2eeadaptor.encryption.algorithm*)* and encryption chaining mode (j2eeadaptor.encryption.chaining.mode*)* properties are not specified properly. propertiesThe values for the j2eeadaptor.encryption.algorithm and j2eeadaptor.encryption.chaining.mode properties specified for the identity provider do not match the values specified for the service provider.
- The path of the **key.txt** file is not properly set in the j2eeadaptor.encryption.key.file property.
- Access to the **key.txt** file is not provided to the IIS user.

Fix

- Specify the adaptor properties, as follows:
  a. From the ***FIM-Domain*\rsa-fim-config\properties** directory, open the **adaptor.properties** file.
  b. Specify correct values for the following properties:
     – j2eeadaptor.encryption.algorithm
     – j2eeadaptor.encryption.chaining.mode
     – j2eeadaptor.encryption.key.file
- Provide access to the **key.txt** file for the IIS user.

Single Sign-On Fails Because the Timings Are Not Synchronized

Symptom

When you perform web single sign-on (SSO) on any page and try to go back to the previous page, a replay attack exception error is displayed instead of redirecting you to the error URL.

```
Assertion is not in valid interval Error stack trace:
com.rsa.fim.profile.sso.SSOProfileException: Assertion is not
in valid interval at
com.rsa.fim.profile.sso.SSOHelper.checkInValidInterval(SSOHelpe
r.java:896) at
com.rsa.fim.profile.sso.SSOProfileBean.processResponse(SSOProfi
leBean.java:1523) at
com.rsa.fim.profile.common.FIMProfileBean.processResponse(FIMPr
ofileBean.java:50) at
com.rsa.fim.profile.common.FIMProfile_mzkd72_EOImpl.processResp
onse(FIMProfile_mzkd72_EOImpl.java:1156) at
com.rsa.fim.servlet.sso.AssertionConsumerService.doGet(Assertio
nConsumerService.java:78) at
com.rsa.fim.servlet.sso.AssertionConsumerService.doPost(Asserti
onConsumerService.java:40) at
javax.servlet.http.HttpServlet.service(HttpServlet.java:763) at
javax.servlet.http.HttpServlet.service(HttpServlet.java:856) at
weblogic.servlet.internal.StubSecurityHelper$ServletServiceActi
on.run(StubSecurityHelper.java:223) at
weblogic.servlet.internal.StubSecurityHelper.invokeServlet(Stub
SecurityHelper.java:125) at
weblogic.servlet.internal.ServletStubImpl.execute(ServletStubIm
pl.java:283) at
weblogic.servlet.internal.ServletStubImpl.execute(ServletStubIm
pl.java:175) at
weblogic.servlet.internal.WebAppServletContext$ServletInvocatio
nAction.run(WebAppServletContext.java:3245) at
weblogic.security.acl.internal.AuthenticatedSubject.doAs(Authen
ticatedSubject.java:321) at
weblogic.security.service.SecurityManager.runAs(SecurityManager
.java:121) at...
```

Fix

Ensure that the time on the identity provider and service provider is synchronized.

Single Sign-On Fails with IBM WebSphere Application Server and RSA Access Manager

Symptom

When you perform singe sign-on (SSO) in an RSA Federated Identity Manager deployment on the IBM WebSphere Application Server with Websphere as the authentication authority and RSA Access Manager as the access manager, you get the following error message:

```
Error 403-Unauthorized Access
```

The reason for this error is that the user mapping is not specified in the Websphere server for the resource.

Fix

1. In the Websphere Console, click **Users and Groups**.
2. Create the user mapping for the resource.

Note: You must specify the user mapping after redeploying the **.war** file.

Log On Page Appears Repeatedly

Symptom

When you perform web single sign-on (SSO) to access the service provider, you see the Log On page repeatedly.

The error occurs for one of the following reasons:

- The cookie domain name on both the identity provider and the service provider is the same.
- The FQDN on the identity provider or service provider machine has the loopback address set as 127.0.0.1 in the hosts file.
- The clock timings on RSA Federated Identity Manager and RSA Access Manager do not match.

Fix

You must specify the correct cookie domain name in Federated Identity Manager or RSA Access Manager, as follows:

1. In Federated Identity Manager, do the following:
   a. In the Administration Console, click **Components > Plug-ins > Manage Existing**.
   b. Select the RSA Access Manager session plug-in, and click **Edit**.
   c. Enter the correct cookie domain name.
      For instructions, see the *Administration Console Help*.
2. In RSA Access Manager, do the following:
   a. Edit the **webagent.conf** file.
   b. Set the parameter **cleartrust.agent.cookie_ip_check** to **false**.
      For instructions, see the *Installation and Configuration Guide* (**install_config.pdf**).

Unable to Access a Protected Page

Symptom

On accessing a protected web page and entering the correct credentials, you get an error message that you are unauthorized to access the web page. This is because the RSA Access Manager user account or password has expired.

Fix

You can use the RSA Access Manager Administration Console to verify whether the user account or password has expired. If either or both have expired, you have to renew the user acount, password, or both using the RSA Access Manager Administration Console. For more information, see the RSA Access Manager documentation.

Error on Using IP Address

Symptom

You get error messages if you specify the IP address while configuring RSA Federated Identity Manager.

The error occurs for one of the following reasons:

- Federated Identity Manager cannot create cookies using IP addresses.
- In a clustered deployment, the use of IP addresses in the load balancer is not supported.

Fix

You must specify the FQDN instead of the IP address.

Unexpected Behavior while Using Refresh on the Browser

Symptom

In the Administration Console, clicking the browser **Refresh** button leads to unexpected behavior. For example, if RSA Federated Identity Manager is deployed in a single-tier environment, and you do the following:

1. In the Administration Console, select **Components > Plug-ins > Add New > Web Agent Plugin.**
2. Add and save the plug-in information. The Plug-ins page lists all the plug-ins.
3. Click **Refresh** in the browser.

You see the following error message instead of the Plug-ins page. As a result, the Oracle WebLogic Server Administration Console gets filled with error messages.

```
***Exception from CreatePluginConfig Command.
org.jpox.exceptions.TransactionNotActiveException: Transaction
is not active. Yo u either need to define a transaction around
this, or run your PersistenceManage rFactory with
'NontransactionalRead' set to 'true' at
org.jpox.NonmanagedTransaction.getConnection(NonmanagedTransact
```

```
ion.ja va:235) at
org.jpox.NonmanagedTransaction.getConnection(NonmanagedTransact
ion.ja va:189) at
org.jpox.AbstractPersistenceManager.getConnection(AbstractPersi
stence Manager.java:369) at
org.jpox.store.rdbms.scostore.NormalMapStore.clear(NormalMapSto
re.jav a:572) at
org.jpox.store.mapping.MapMapping.postUpdate(MapMapping.java:20
1) at
org.jpox.store.rdbms.request.UpdateRequest.execute(UpdateReques
t.java :287) at
org.jpox.store.rdbms.table.ClassTable.update(ClassTable.java:21
64) at.....
```

Fix

Ensure that you do not use the browser **Refresh** button.

Incorrect Attribute Transfer of Common Name Attribute

Symptom

When you perform an attribute transfer of the CommonName attribute from an identity provider, the transfer does not work as intended. The reason for the incorrect attribute transfer is the mapping specified for the CommonName attribute in the attribute plug-in. By default, the CommonName attribute exists in your LDAP directory, and, when you specify the mapping using CommonName in the plug-in, this value replaces the value of the CommonName attribute in the LDAP directory.

Fix

1. In the LDAP directory, add an attribute called **RSACommonName**.
2. In the attribute plug-in, specify the mapping using **RSACommonName**. For example, RSACommonName=cn.

Note: Microsoft Active Directory Federation Services (AD FS) does not allow you to map the CommonName attribute to any other name.

Installation Fails in a Clustered Setup due to Incorrect Information on Servers and Nodes

Symptom

While installing RSA Federated Identity Manager in a clustered setup (Oracle WebLogic Server platform) by running the **Install.cmd**, **packRuntime.cmd**, and **unPackRuntime.cmd** scripts, you get the following error:

```
Error in JAVA_HOME.
```

The reason for this error is that these scripts internally use some scripts written in Oracle WebLogic Server, such as the pack and unpack commands, which cannot be located because of an incorrect path.

Fix

You must set the correct path on the admin server and the managed nodes, for the following environment variables:

- *path* for JAVA_HOME
- JAVA_HOME/bin path invoking the pack command in **packRuntime.cmd**
- bea\weblogic92\common\bin path invoking the unpack command in **unpackRuntime.cmd**

System Crashes while Using RSA Federated Identity Manager

Symptom

While using RSA Federated Identity Manager, your system crashes after displaying one of the following errors:

```
<ExecuteRequest failed
 java.lang.OutOfMemoryError.
java.lang.OutOfMemoryError
        at java.io.RandomAccessFile.readBytes(Native Method)
        at
java.io.RandomAccessFile.read(RandomAccessFile.java:315)
        at
weblogic.diagnostics.archive.FileUtils.readFile(FileUtils.ja
va:46)
        at
weblogic.diagnostics.archive.filestore.FileIndexMetaInfo.bui
ldIndex(FileIndexMetaInfo.java:403)
        at
weblogic.diagnostics.archive.filestore.FileIndexMetaInfo.bui
ldIndex(FileIndexMetaInfo.java:343)
        Truncated. see log file for complete stacktrace
```

or

```
<Multicast socket receive error: java.lang.OutOfMemoryError
: heap allocation failed
java.lang.OutOfMemoryError: heap allocation failed
        at java.net.PlainDatagramSocketImpl.receive0(Native
Method)
        at
java.net.PlainDatagramSocketImpl.receive(PlainDatagramSocket
Impl.java:136)
        at
java.net.DatagramSocket.receive(DatagramSocket.java:712)
        at
weblogic.cluster.FragmentSocket.receive(FragmentSocket.java:
202)
        at
weblogic.cluster.MulticastManager.run(MulticastManager.java:
400)
        Truncated. see log file for complete stacktrace
>
Exception in thread "CompilerThread1"
java.lang.OutOfMemoryError: requested 35344 bytes for
```

```
Chunk::new. Out of swap
space?http://<bugs.sun.com>/bugdatabase/view_bug.do?bug_id=5
075468..........
```

Fix

The Java Virtual Machine (JVM) internally has a hotspot compiler that tweaks the bytecodes to native code based on the number of times a specific code has been executed. This hotspot compiler fails when trying to optimize and allocate space. The solution must be provided in the JVM.

Troubleshooting IBM WebSphere Application Server Deployment

FIM uses different version of Derby jars instead of one installed with Websphere 7 default installation.

Fix

1. After installing FIM manually or using install script, replace Derby jars shipped with Websphere with the one shipped with FIM.
2. Copy the following files from **<PROFILE_DIR>\rsa-fim-config\lib directory** and replace the jar files in **<APP-SERVER-INSTALL-DIR>\derby\lib** directory:
   - derby.jar
   - derbyclient.jar
   - derbynet.jar
   - derbytool.jar

FIM ships few endorsed jars for Websphere 7.0.

Symptom

FIM ships few endorsed jars for Websphere 7.0.

- Websphere 7 uses only upgrade jars present in **<CDIMAGE>\WAS\WAS7-endorsed-lib** directory.

Fix

1. After installation on Websphere 7, go to **<APP-SERVER-INSTALL-DIR>\java\jre\lib\endorsed** directory and delete the following files:
   - xalan.jar
   - xercesImpl.jar
2. Copy the following files from **CDIMAGE>\WAS\WAS7-endorsed-lib** directory to **<APP-SERVER-INSTALL-DIR>\java\jre\lib\endorsed** directory:

- xalan-2.7.1.jar
- xercesImpl-2.9.1.jar
- xmlsec-1.5.1.jar

Troubleshooting Tomcat Application server Deployment

Reducing the startup time of Tomcat 7 application server during deployment.

Symptom

Tomcat 7 application server scans all the jar files during deployment, leading to increase in the startup time.

Fix

- Update the below mentioned list for the following property **tomcat.util.scan.DefaultJarScanner.jarsToSkip** in the **catalina.properties** file.

```
tomcat.util.scan.DefaultJarScanner.jarsToSkip=org.springframewo
rk.aop-3.1.1.RELEASE.jar,\
org.springframework.asm-3.1.1.RELEASE.jar,\
org.springframework.beans-3.1.1.RELEASE.jar,\
org.springframework.context-3.1.1.RELEASE.jar,\
org.springframework.core-3.1.1.RELEASE.jar,\
org.springframework.expression-3.1.1.RELEASE.jar,\
org.springframework.web.servlet-3.1.1.RELEASE.jar,\
org.springframework.web-3.1.1.RELEASE.jar
```

- Add one of the below property
  - Djava.security.egd=file:/dev/./urandom (SystemProperty)

  (or)

  - securerandom.source=file:/dev/./urandom (jre/lib/security/java.security file)

Troubleshooting Oracle WebLogic Server Deployment

FIM 4.2 doesn't start if Weblogic 11gR1 is installed with Derby Evaluation DB (Part of WLS Installer)

Symptom

The **saaj.jar** file is not shipped in Weblogic endorsed directory in this release.

For Weblogic 11gR1 the saaj.jar is not required as Weblogic already has updated version of this jar, but the same is required for Weblogic 10.3 MP2.

Fix

Copy saaj.jar from **<KIT>\cdimage\TOMCAT\jre\lib\endorsed** directory and put it in JDK's endorsed directory of your deployment.

June 2013

Trademarks