IBM Netcool OMNIbus WebGUI 8.1

Load Balancing Configuration

A step by step example

Author: Gheorghe Mihaela, IBM NSA Software Engineer | IBM Clouds Lab
Mihaela.Gheorghe1@ibm.com

Description

This guide has the purpose to illustrate a complete step by step example for a load balancing configuration for IBM Netcool OMNIbus WebGUI.

The steps described within this document are applicable for environments with DASH version 3.1.2 and higher. For creating this document, the tests were performed within an environment with WebGUI 8.1 Fix Pack 15 , DASH 3.1.3.2. and DB2 11.1.

They can be tested against any WebGUI 8.1.x environments as long as the DASH version is at least 3.1.2. and the installed DB2 is supported.

All the servers that will be part of the cluster MUST have the exact same versions and components installed.

Additional references:

https://www.ibm.com/support/knowledgecenter/en/SSSHTQ_8.1.0/com.ibm.netcool_OMNIbus.doc_8.1.0/webtop/wip/concept/web_ovr_loadbalancingcluster.html

https://www-01.ibm.com/support/docview.wss?uid=swg21983344

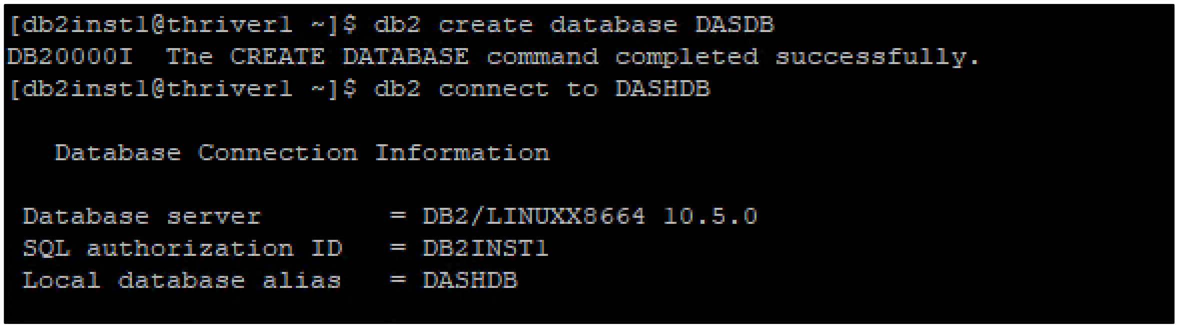
Configuration needed on the DB2 server

Login to DB2 with the DB2 instance owner user, in this example the default **db2inst1** user has been used.

Start DB2 database by running the following command: **db2start**

Create an empty database, you can name it for example **DASHDB**

db2 create database DASHDB
connect to DASHDB: **db2 connect to DASHDB**

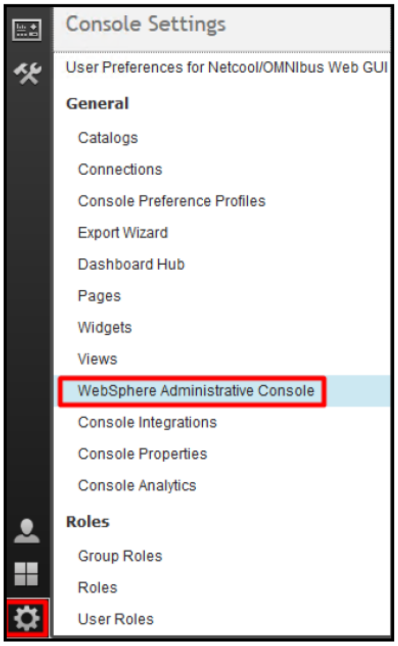


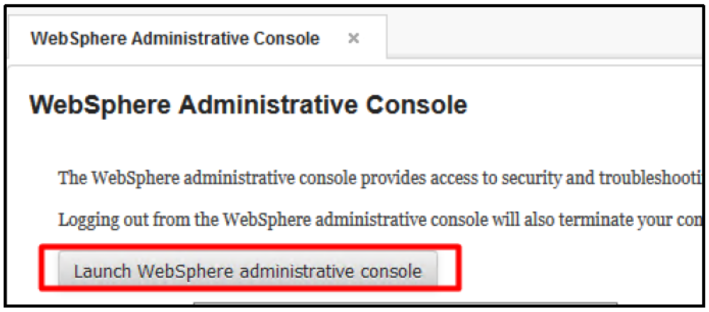
```
[db2inst1@thriver1 ~]$ db2 create database DASDB
DB20000I  The CREATE DATABASE command completed successfully.
[db2inst1@thriver1 ~]$ db2 connect to DASHDB

   Database Connection Information

 Database server        = DB2/LINUXX8664 10.5.0
 SQL authorization ID   = DB2INST1
 Local database alias   = DASHDB
```

Configuration needed on each WebGUI server

On the first WebGUI server:

1. Login to the WebGUI server and open WebSphere Administrative Console




WebSphere Administrative Console ×

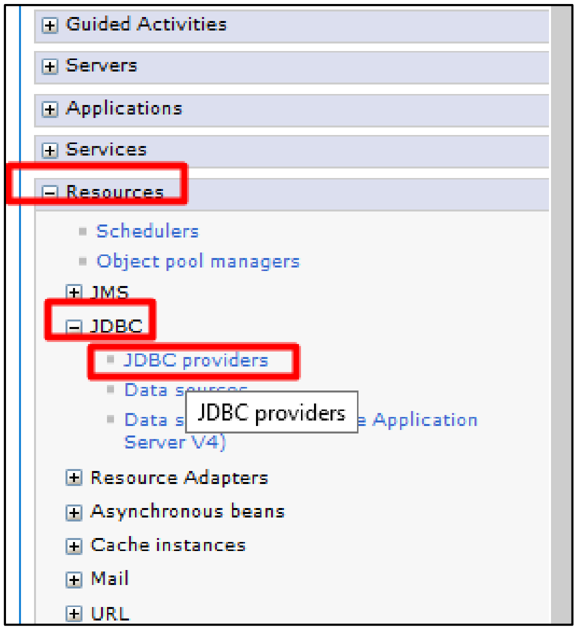
WebSphere Administrative Console

The WebSphere administrative console provides access to security and troubleshooti

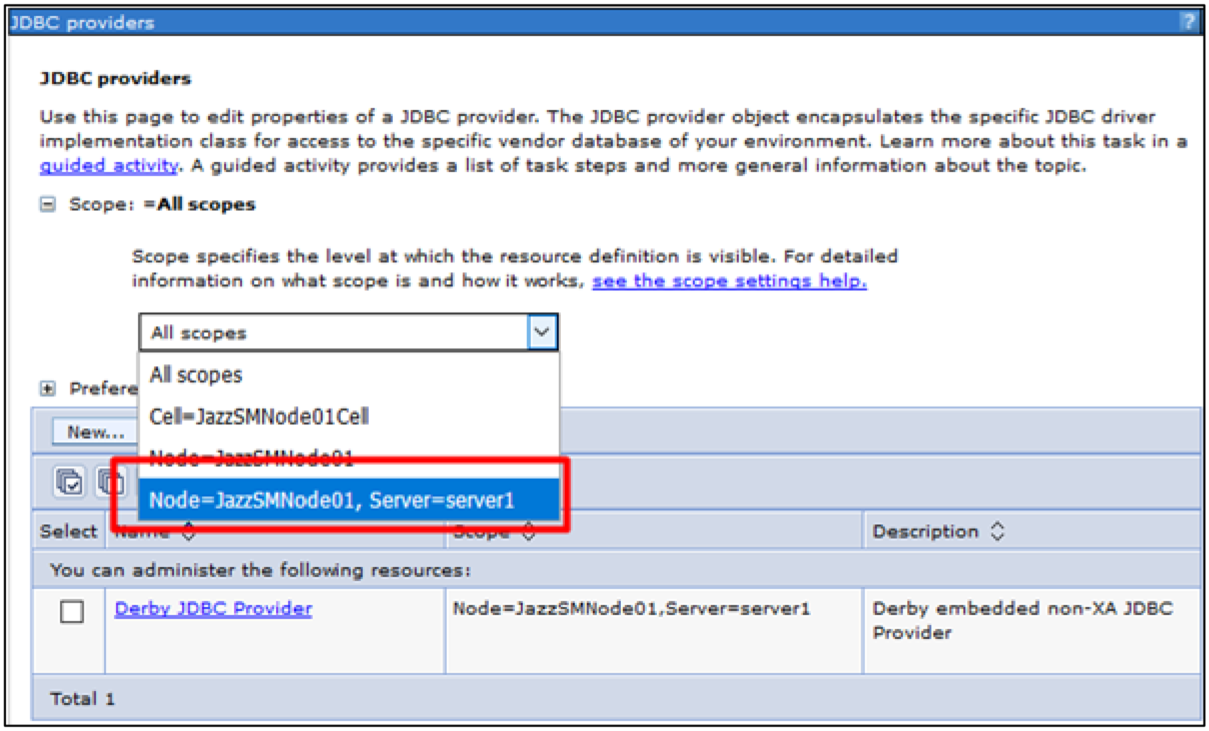
Logging out from the WebSphere administrative console will also terminate your con

Launch WebSphere administrative console

2. From WAS go to Resources -> JDBC -> JDBC providers



3. Select instead of "All scopes" the option Node=JazzSMNode01, Server=server1:



JDBC providers

JDBC providers

Use this page to edit properties of a JDBC provider. The JDBC provider object encapsulates the specific JDBC driver implementation class for access to the specific vendor database of your environment. Learn more about this task in a guided activity. A guided activity provides a list of task steps and more general information about the topic.

⊟ Scope: =**All scopes**

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, see the scope settings help.

All scopes

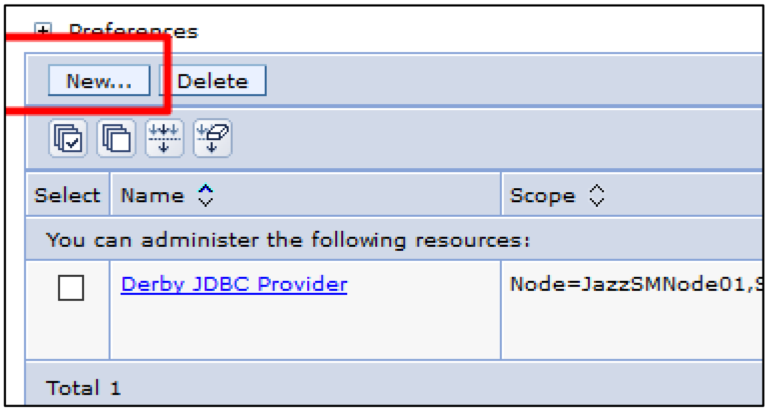
- All scopes
- Cell=JazzSMNode01Cell
- Node=JazzSMNode01
- Node=JazzSMNode01, Server=server1

⊞ Prefere

New...

Select	Name	Scope	Description
You can administer the following resources:			
□	Derby JDBC Provider	Node=JazzSMNode01,Server=server1	Derby embedded non-XA JDBC Provider
Total 1			

4. Create a new JDBC provider by clicking on the New option:

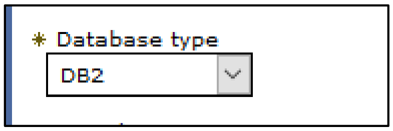


⊞ Preferences

New... Delete

Select	Name	Scope
You can administer the following resources:		
□	Derby JDBC Provider	Node=JazzSMNode01,S
Total 1		

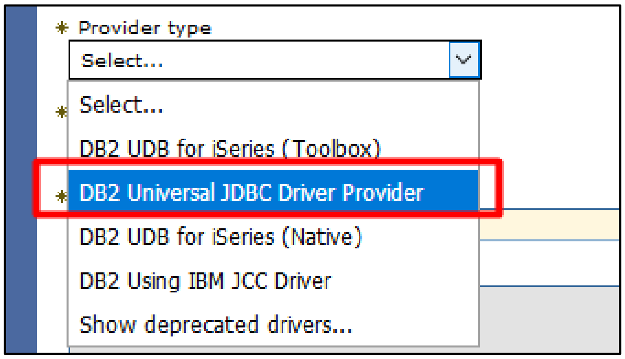
Select DB2 for database type:



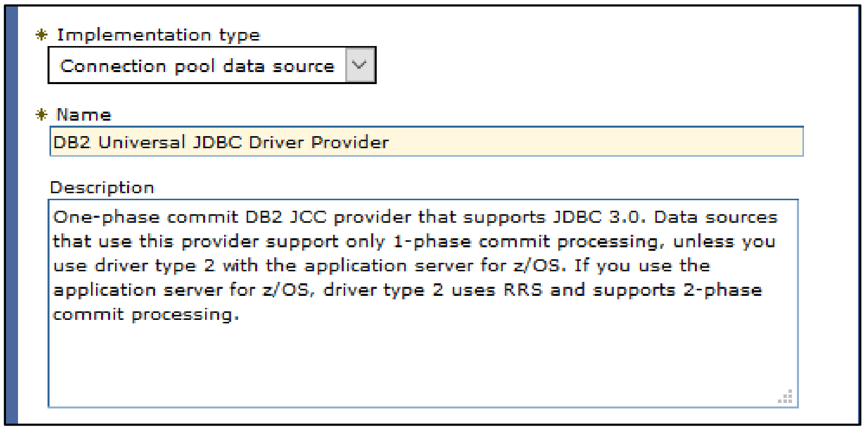
* Database type

DB2

For provider type select DB2 universal JDBC driver provider:


* Provider type
Select...
Select...
DB2 UDB for iSeries (Toolbox)
DB2 Universal JDBC Driver Provider
DB2 UDB for iSeries (Native)
DB2 Using IBM JCC Driver
Show deprecated drivers...

For implementation type select connection pool data source:



* Implementation type

Connection pool data source

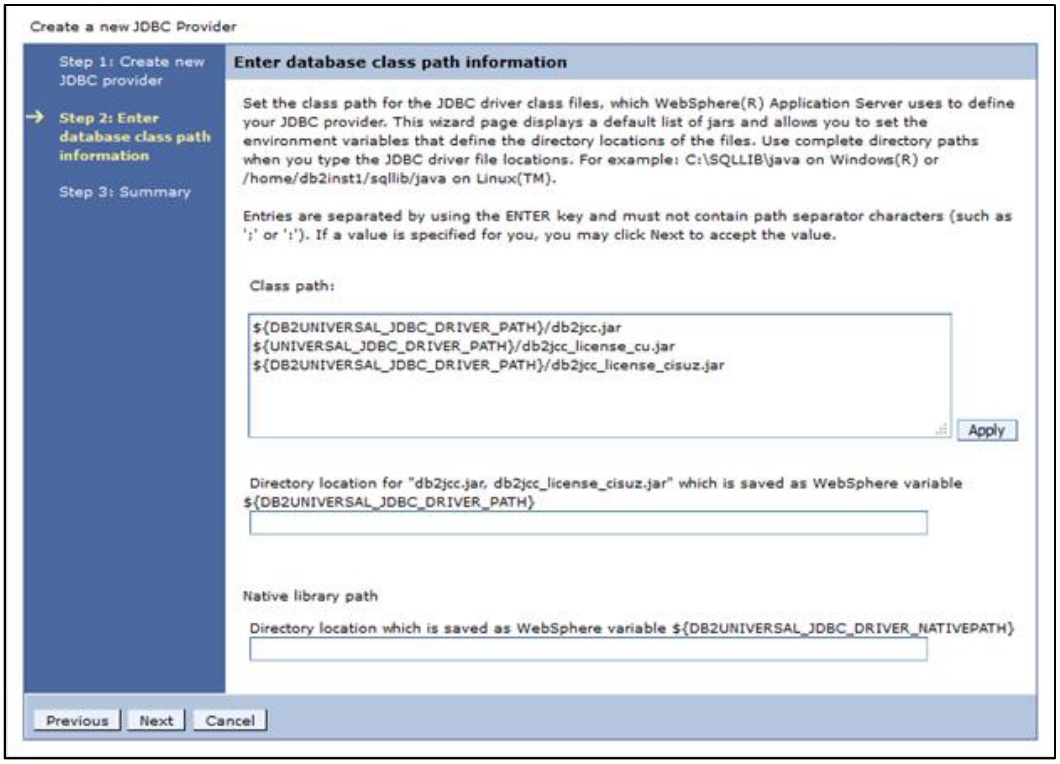
* Name

DB2 Universal JDBC Driver Provider

Description

One-phase commit DB2 JCC provider that supports JDBC 3.0. Data sources that use this provider support only 1-phase commit processing, unless you use driver type 2 with the application server for z/OS. If you use the application server for z/OS, driver type 2 uses RRS and supports 2-phase commit processing.

Click **next.**



Create a new JDBC Provider

Step 1: Create new JDBC provider
→ Step 2: Enter database class path information
Step 3: Summary

Enter database class path information

Set the class path for the JDBC driver class files, which WebSphere(R) Application Server uses to define your JDBC provider. This wizard page displays a default list of jars and allows you to set the environment variables that define the directory locations of the files. Use complete directory paths when you type the JDBC driver file locations. For example: C:\SQLLIB\java on Windows(R) or /home/db2inst1/sqllib/java on Linux(TM).

Entries are separated by using the ENTER key and must not contain path separator characters (such as ';' or ':'). If a value is specified for you, you may click Next to accept the value.

Class path:

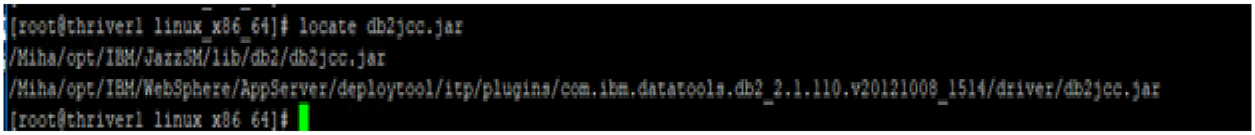
```
${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc.jar
${UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar
${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar
```

Directory location for "db2jcc.jar, db2jcc_license_cisuz.jar" which is saved as WebSphere variable ${DB2UNIVERSAL_JDBC_DRIVER_PATH}

Native library path

Directory location which is saved as WebSphere variable ${DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH}

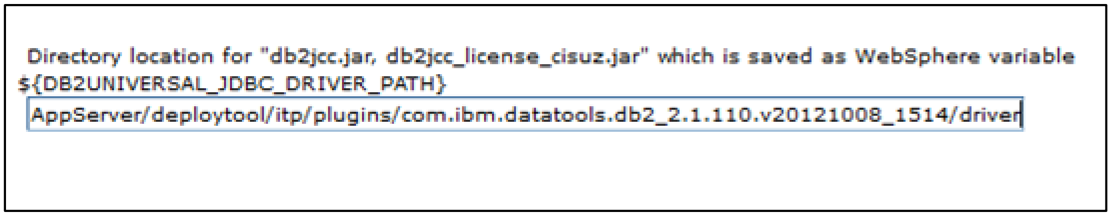
On the server search for **db2jcc.jar** file paths. There should be one under JazzSM directory which is required for native library path and one under WebSphere directory which is required for the first field.



```
[root@thriver1 linux_x86_64]# locate db2jcc.jar
/Miha/opt/IBM/JazzSM/lib/db2/db2jcc.jar
/Miha/opt/IBM/WebSphere/AppServer/deploytool/itp/plugins/com.ibm.datatools.db2_2.1.110.v20121008_1514/driver/db2jcc.jar
[root@thriver1 linux_x86_64]#
```

Enter the following path to the directory location for the mentioned jar files:

/Miha/opt/IBM/WebSphere/AppServer/deploytool/itp/plugins/com.ibm.datatools.db2_2.1.110.v20121008_1514/driver

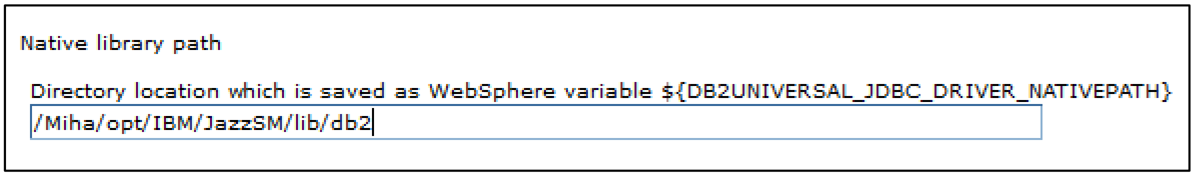


Directory location for "db2jcc.jar, db2jcc_license_cisuz.jar" which is saved as WebSphere variable ${DB2UNIVERSAL_JDBC_DRIVER_PATH}

AppServer/deploytool/itp/plugins/com.ibm.datatools.db2_2.1.110.v20121008_1514/driver

And the following path for the native directory:

/Miha/opt/IBM/JazzSM/lib/db2



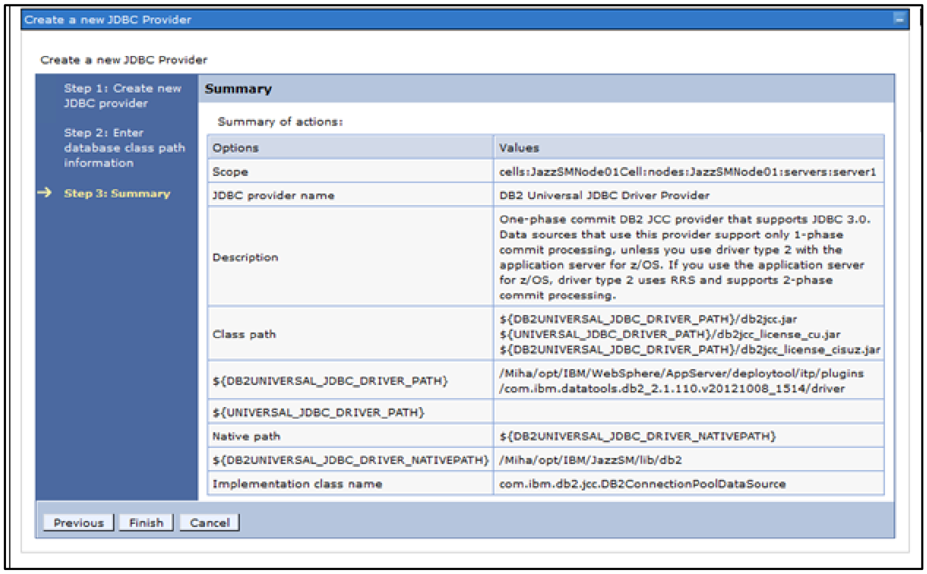
Native library path

Directory location which is saved as WebSphere variable ${DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH}

/Miha/opt/IBM/JazzSM/lib/db2

Click **next.**

Click **finish**.



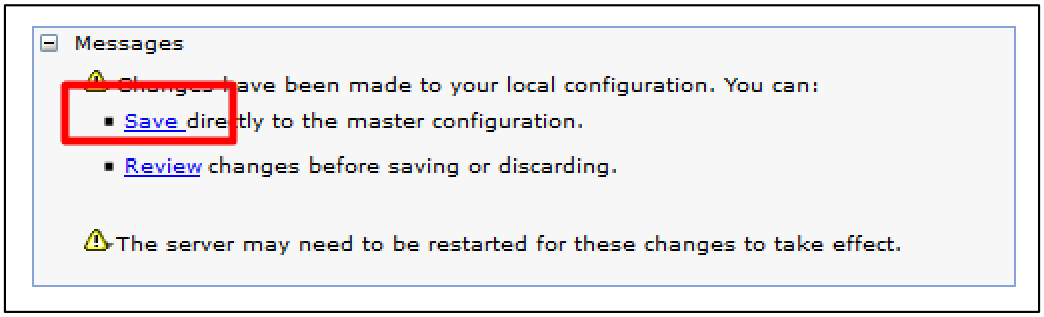
Create a new JDBC Provider
Create a new JDBC Provider
Step 1: Create new JDBC provider
Step 2: Enter database class path information
→ Step 3: Summary
Previous
Finish
Cancel

Summary

Summary of actions:

Options	Values
Scope	cells:JazzSMNode01Cell:nodes:JazzSMNode01:servers:server1
JDBC provider name	DB2 Universal JDBC Driver Provider
Description	One-phase commit DB2 JCC provider that supports JDBC 3.0. Data sources that use this provider support only 1-phase commit processing, unless you use driver type 2 with the application server for z/OS. If you use the application server for z/OS, driver type 2 uses RRS and supports 2-phase commit processing.
Class path	${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc.jar ${UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar ${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar
${DB2UNIVERSAL_JDBC_DRIVER_PATH}	/Miha/opt/IBM/WebSphere/AppServer/deploytool/itp/plugins /com.ibm.datatools.db2_2.1.110.v20121008_1514/driver
${UNIVERSAL_JDBC_DRIVER_PATH}	
Native path	${DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH}
${DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH}	/Miha/opt/IBM/JazzSM/lib/db2
Implementation class name	com.ibm.db2.jcc.DB2ConnectionPoolDataSource

Click ***Save*** to save the configuration (you will need to do this each time you get this screen):



Messages

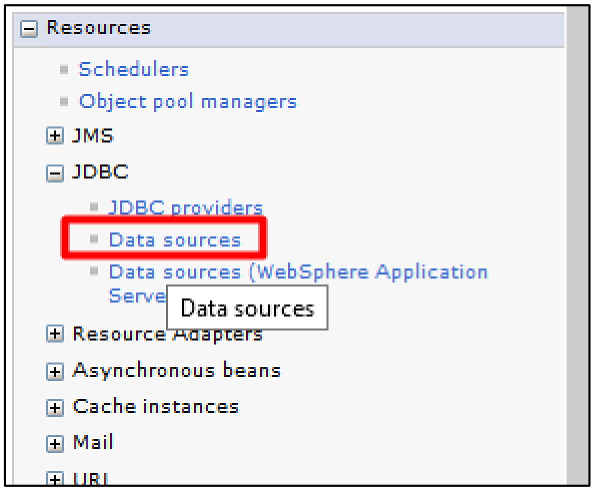
Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

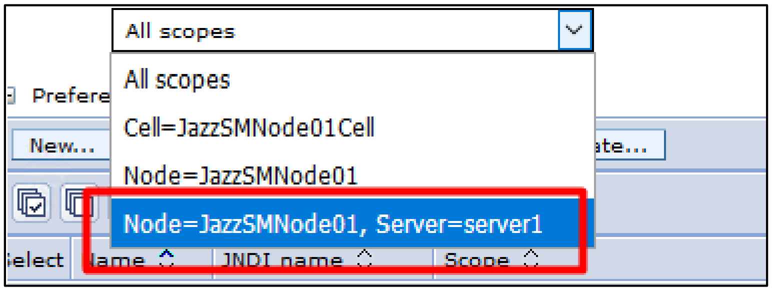
The server may need to be restarted for these changes to take effect.

5. Create a new Data Source for JDBC.

Go to "Resources" -> JDBC -> Data Sources

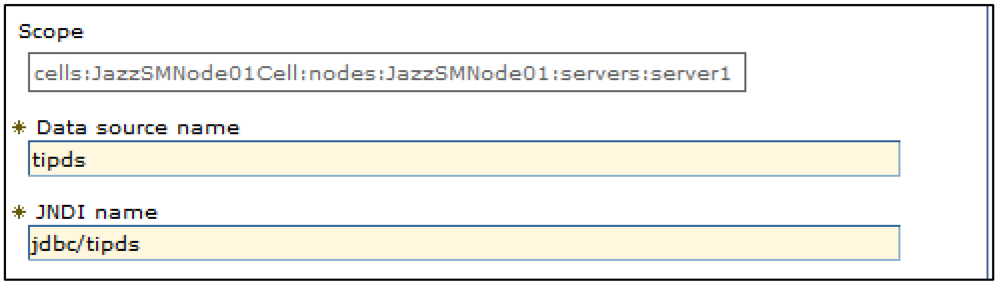


Select instead of "All scopes" the option Node=JazzSMNode01, Server=server1:



Click on "**New**"

Enter **tipds** (this should be always named as this) and **jdbc/tipds** for JNDI name (this should be always named as this):



Scope

cells:JazzSMNode01Cell:nodes:JazzSMNode01:servers:server1

* Data source name

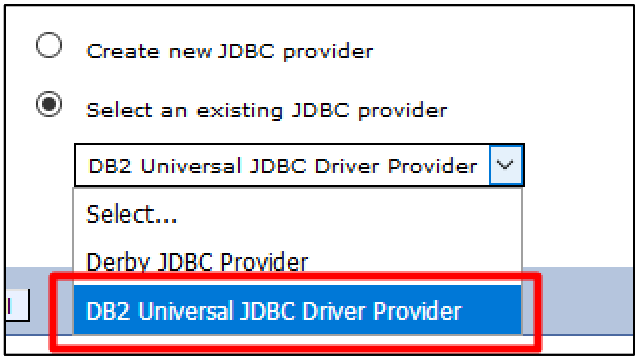
tipds

* JNDI name

jdbc/tipds

Click on **Next**.

Select the option "**Select an existing JDBC provider**" and select the "**DB2 universal JDBC driver provider"**:

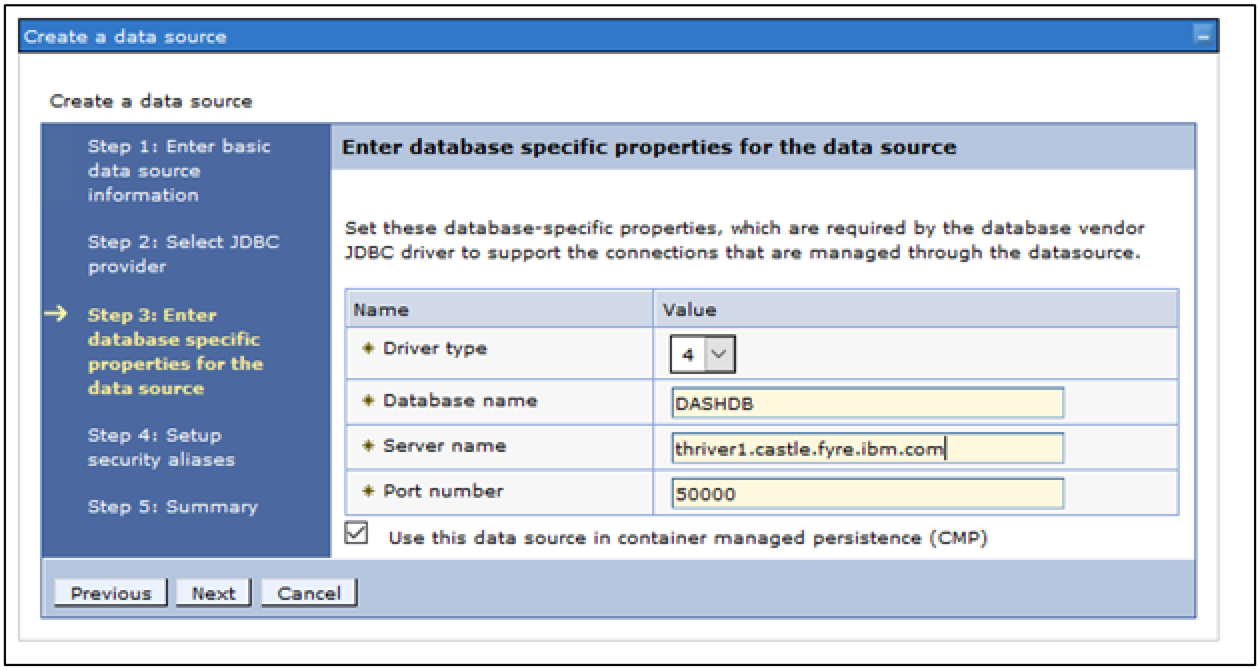


○ Create new JDBC provider

● Select an existing JDBC provider

DB2 Universal JDBC Driver Provider

Click on **Next**.



Create a data source

Step 1: Enter basic data source information

Step 2: Select JDBC provider

→ **Step 3: Enter database specific properties for the data source**

Step 4: Setup security aliases

Step 5: Summary

Enter database specific properties for the data source

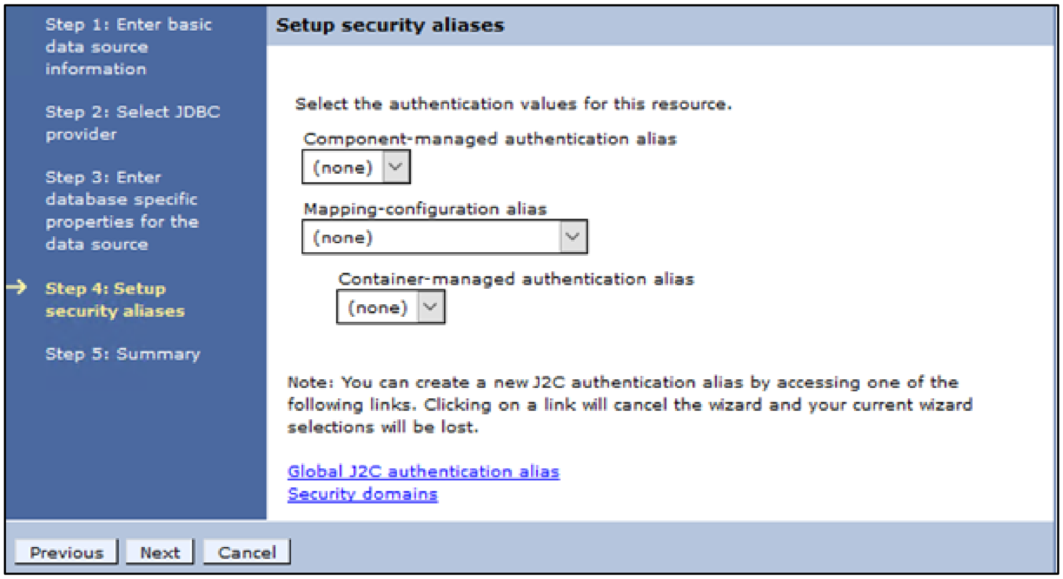
Set these database-specific properties, which are required by the database vendor JDBC driver to support the connections that are managed through the datasource.

Name	Value
* Driver type	4
* Database name	DASHDB
* Server name	thriver1.castle.fyre.ibm.com
* Port number	50000

☑ Use this data source in container managed persistence (CMP)

Within this screen you will have to enter the name of the database that you have created e.g. **DASHDB** and also the server hostname and the port number where DB2 is installed.

Click **next.**



Step 1: Enter basic data source information
Step 2: Select JDBC provider
Step 3: Enter database specific properties for the data source
→ **Step 4: Setup security aliases**
Step 5: Summary

Setup security aliases

Select the authentication values for this resource.

Component-managed authentication alias: (none)

Mapping-configuration alias: (none)

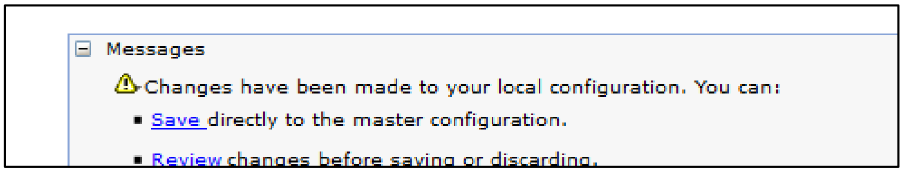
Container-managed authentication alias: (none)

Note: You can create a new J2C authentication alias by accessing one of the following links. Clicking on a link will cancel the wizard and your current wizard selections will be lost.

Global J2C authentication alias
Security domains

Within this screen you don't have to select anything, we'll complete this later.

Click **next.**
Click **finish.**
Click ***Save*** to store the configuration

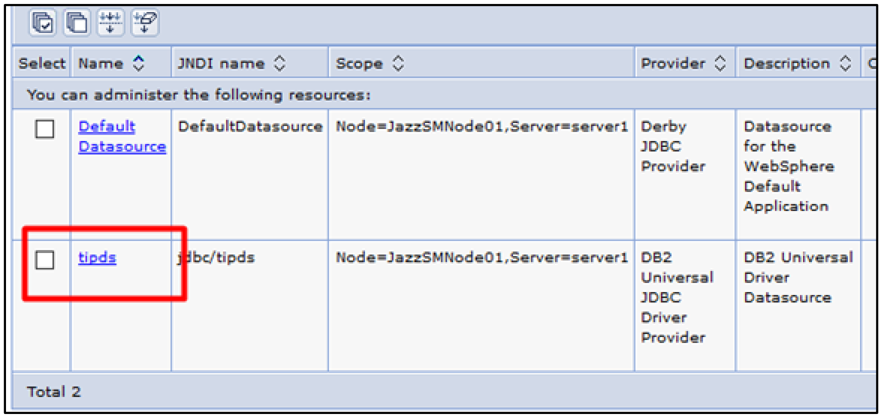


⊟ Messages

⚠Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

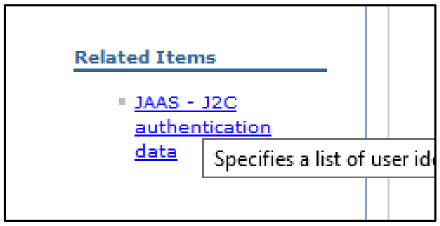
6. Click on the data source that was created e.g. "**tipds**":



Select	Name	JNDI name	Scope	Provider	Description
You can administer the following resources:					
□	Default Datasource	DefaultDatasource	Node=JazzSMNode01,Server=server1	Derby JDBC Provider	Datasource for the WebSphere Default Application
□	tipds	jdbc/tipds	Node=JazzSMNode01,Server=server1	DB2 Universal JDBC Driver Provider	DB2 Universal Driver Datasource

Total 2

Select "**JAAS - J2C authentication data**" under the **Related Items** section.

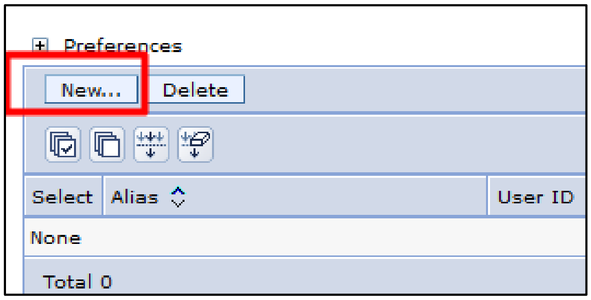


Related Items

- JAAS - J2C authentication data

Specifies a list of user id

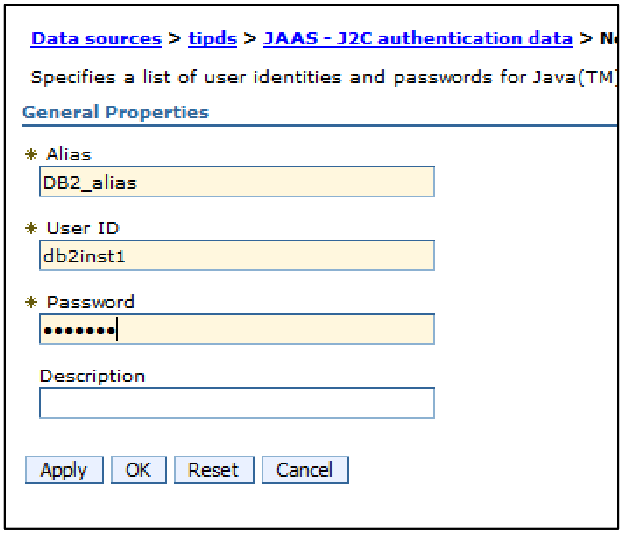
Click on **new:**



Select	Alias ⇕	User ID
None		
Total 0		

Enter a name as alias – in this example the following name was used: **DB2_alias**

Enter the **db2inst1** user (the instance owner user from DB2) and its password.



Data sources > tipds > JAAS - J2C authentication data > N

Specifies a list of user identities and passwords for Java(TM)

General Properties

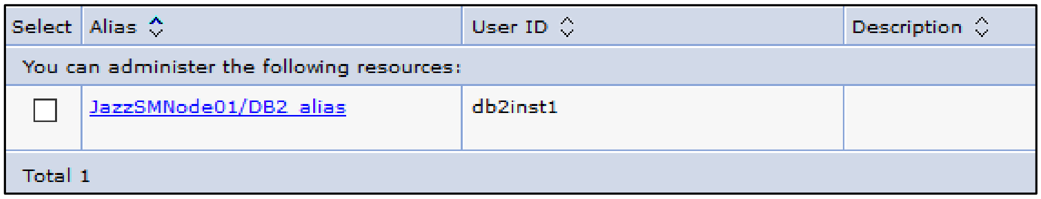
* Alias
DB2_alias

* User ID
db2inst1

* Password
•••••••

Description

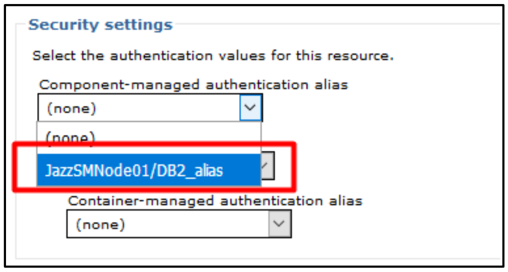
Click **ok.**
Save the configuration.



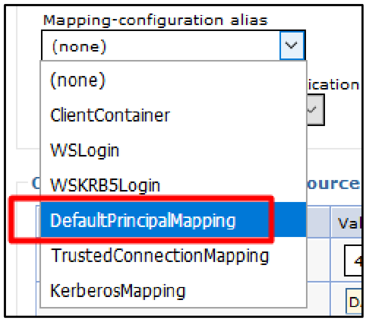
Select	Alias ⇕	User ID ⇕	Description ⇕
You can administer the following resources:			
□	JazzSMNode01/DB2_alias	db2inst1	
Total 1			

7. Return to the **tipds** data source and go to **Security Settings** section:

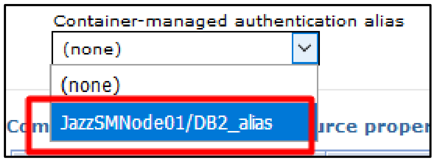
Select **JazzSMNode01/DB2_alias** for component-managed authentication alias:


Security settings
Select the authentication values for this resource.
Component-managed authentication alias
(none)
(none)
JazzSMNode01/DB2_alias
Container-managed authentication alias
(none)

Select **DefaultPrincipalMapping** for mapping-configuration alias:

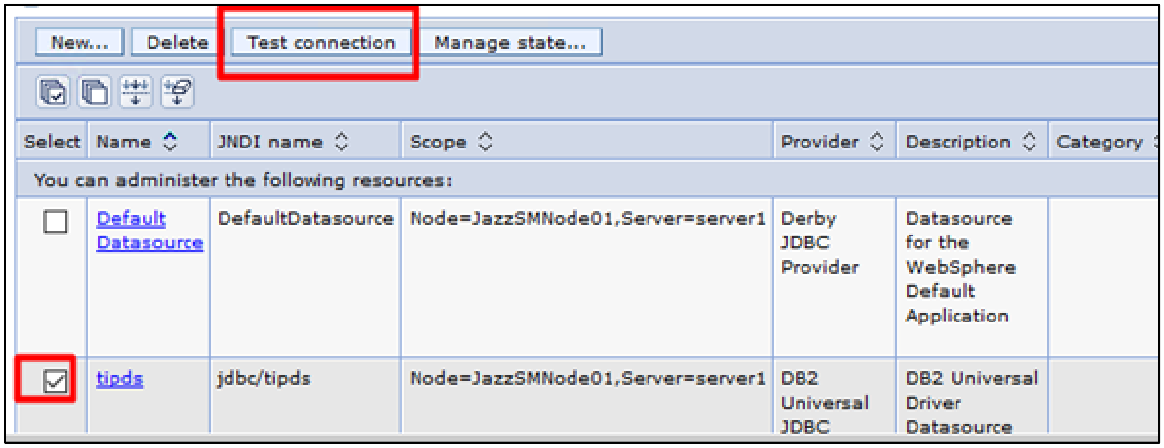


Select **JazzSMNode01/DB2_alias** for container-manager authentication alias:



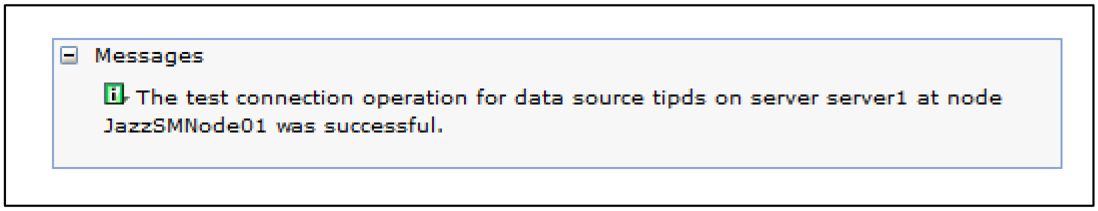
Click **ok.**
Click **Save** to store the configuration.

8. Check **tipds** data source connection:



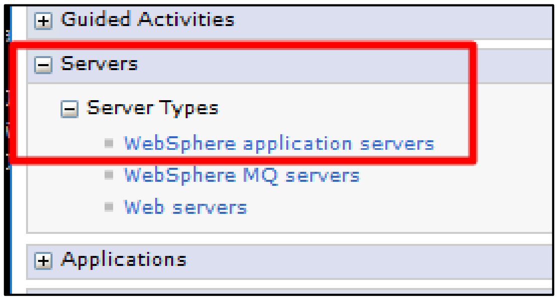
Select	Name	JNDI name	Scope	Provider	Description	Category
You can administer the following resources:						
☐	Default Datasource	DefaultDatasource	Node=JazzSMNode01,Server=server1	Derby JDBC Provider	Datasource for the WebSphere Default Application	
☑	tipds	jdbc/tipds	Node=JazzSMNode01,Server=server1	DB2 Universal JDBC	DB2 Universal Driver Datasource	

The output should be the below one:

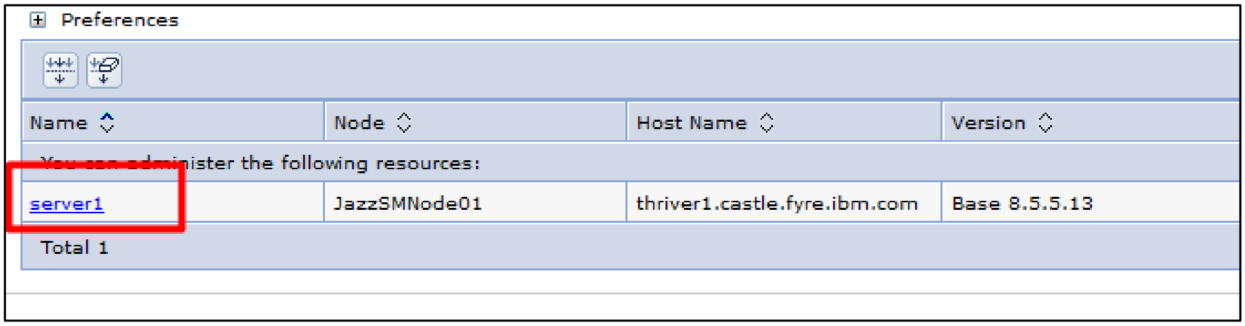

Messages

The test connection operation for data source tipds on server server1 at node JazzSMNode01 was successful.

9. From WAS menu -> Servers -> Server Types -> WebSphere application servers

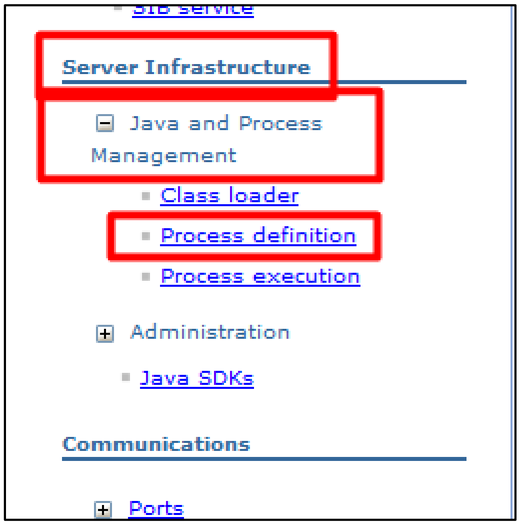


Click on **server1**:

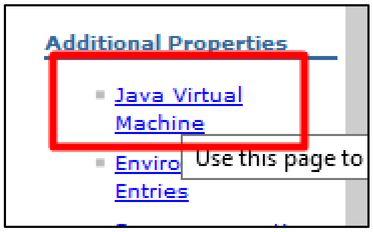


Name	Node	Host Name	Version
You can administer the following resources:			
server1	JazzSMNode01	thriver1.castle.fyre.ibm.com	Base 8.5.5.13
Total 1			

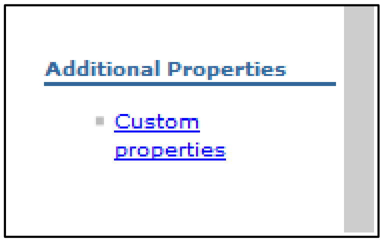
Under **Server Infrastructure** menu-> **Java and Process Management** => **Process Definition**



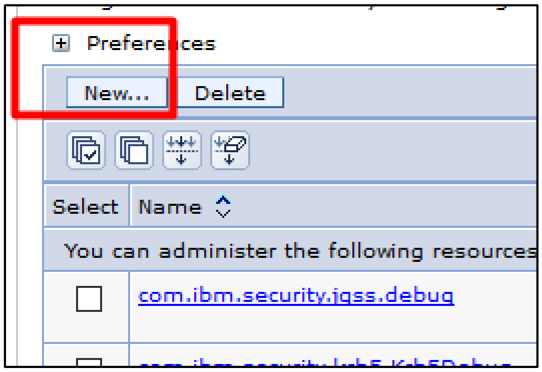
Click on **Java Virtual Machine** under the **Additional Properties** section:



Click on **Custom Properties** under the **Additional Properties** section:

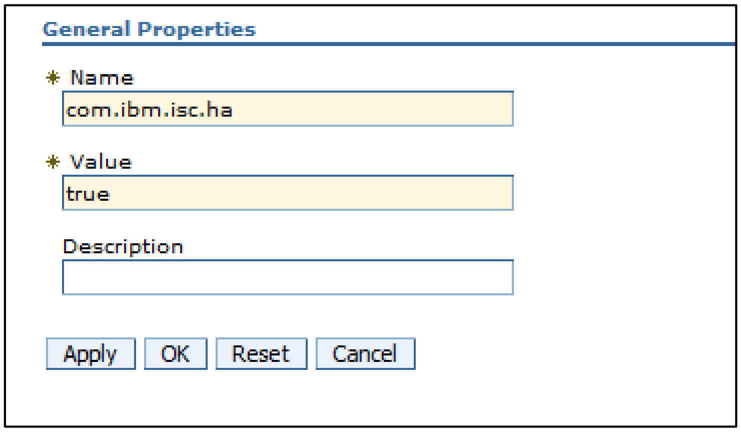


Click on **New**:



Select	Name
You can administer the following resources	
□	com.ibm.security.jgss.debug

Enter **com.ibm.isc.ha** for the Name property and **true** for the Value property:



General Properties

* Name: com.ibm.isc.ha

* Value: true

Description:

Click **apply** and **save**.

10. On the server, edit the **server.init** file from the webgui **etc** directory and set the following 2 properties as per above:

cluster.mode:on

timedtasks.enabled:true

Afterwards, you will need to restart webgui.

Then on the webgui server run the following command:

./consolecli.sh ListHANodes --username smadmin --password netcool

You should get your webgui server on the list.

Repeat all the above steps from 1 to 10 on all the other WebGUI servers that you want to add to this cluster setup.

Afterwards, with both servers configured you will need to enable server to server trust by following the steps described within the following link:

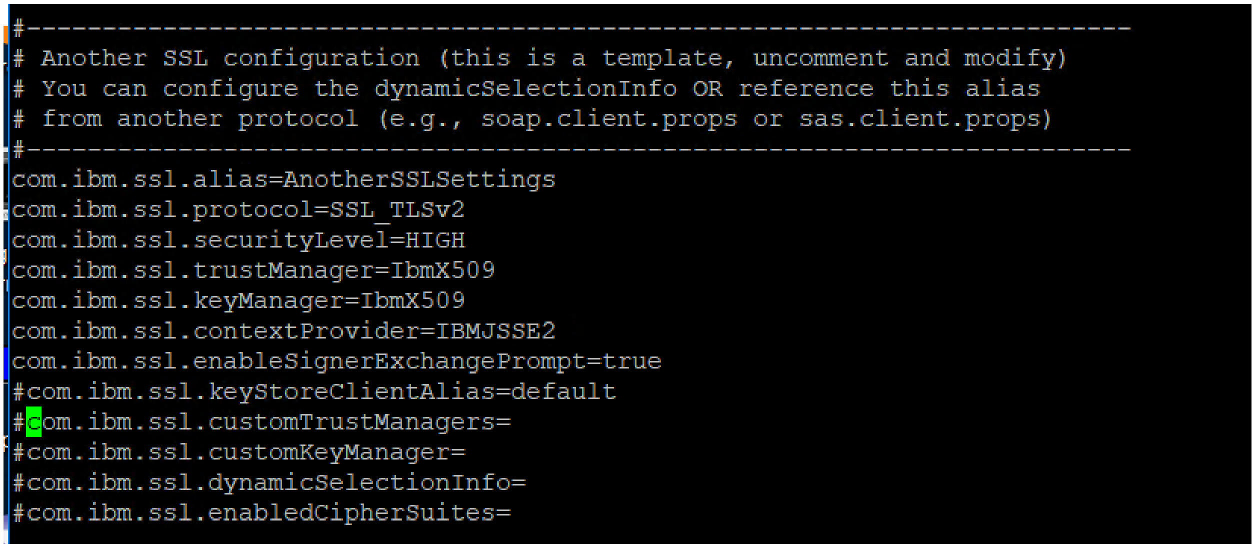
https://www.ibm.com/support/knowledgecenter/en/SSEKCU_1.1.2.1/com.ibm.psc.doc/tip_original/ttip_config_loadbal_trust.html

e.g. repeat the below steps from 1 to 5 for each WebGUI server:

1. Edit ssl.client.props properties file

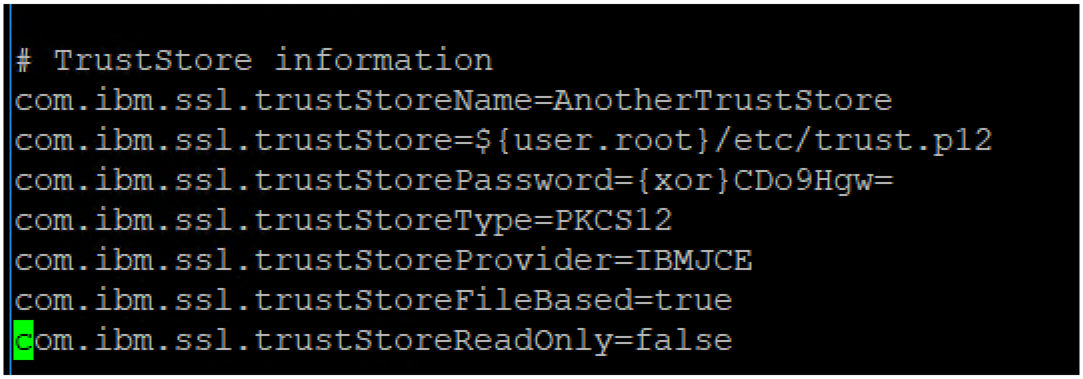
/Miha/opt/IBM/JazzSM/profile/properties/ssl.client.props

Uncomment the section that starts with **com.ibm.ssl.alias=AnotherSSLSettings** so that it looks like this:



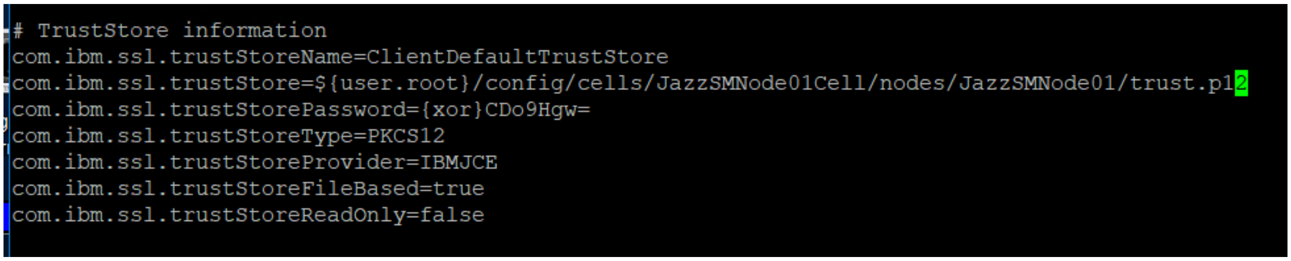
```
#------------------------------------------------------------------------
# Another SSL configuration (this is a template, uncomment and modify)
# You can configure the dynamicSelectionInfo OR reference this alias
# from another protocol (e.g., soap.client.props or sas.client.props)
#------------------------------------------------------------------------
com.ibm.ssl.alias=AnotherSSLSettings
com.ibm.ssl.protocol=SSL_TLSv2
com.ibm.ssl.securityLevel=HIGH
com.ibm.ssl.trustManager=IbmX509
com.ibm.ssl.keyManager=IbmX509
com.ibm.ssl.contextProvider=IBMJSSE2
com.ibm.ssl.enableSignerExchangePrompt=true
#com.ibm.ssl.keyStoreClientAlias=default
#com.ibm.ssl.customTrustManagers=
#com.ibm.ssl.customKeyManager=
#com.ibm.ssl.dynamicSelectionInfo=
#com.ibm.ssl.enabledCipherSuites=
```

2. Uncomment the section that starts with **com.ibm.ssl.trustStoreName=AnotherTrustStore** so that it looks like this:



```
# TrustStore information
com.ibm.ssl.trustStoreName=AnotherTrustStore
com.ibm.ssl.trustStore=${user.root}/etc/trust.p12
com.ibm.ssl.trustStorePassword={xor}CDo9Hgw=
com.ibm.ssl.trustStoreType=PKCS12
com.ibm.ssl.trustStoreProvider=IBMJCE
com.ibm.ssl.trustStoreFileBased=true
com.ibm.ssl.trustStoreReadOnly=false
```

3. Update the location of the trust store that the signer should be added to in the **com.ibm.ssl.trustStore** property of **AnotherTrustStore** by replacing the default value **com.ibm.ssl.trustStore=${user.root}/etc/trust.p12** with the correct path for your trust store. Example:



```
# TrustStore information
com.ibm.ssl.trustStoreName=ClientDefaultTrustStore
com.ibm.ssl.trustStore=${user.root}/config/cells/JazzSMNode01Cell/nodes/JazzSMNode01/trust.p12
com.ibm.ssl.trustStorePassword={xor}CDo9Hgw=
com.ibm.ssl.trustStoreType=PKCS12
com.ibm.ssl.trustStoreProvider=IBMJCE
com.ibm.ssl.trustStoreFileBased=true
com.ibm.ssl.trustStoreReadOnly=false
```

com.ibm.ssl.trustStore=${user.root}/config/cells/JazzSMNode01Cell/nodes/JazzSMNode01/trust.p12

4. Save file.
5. Restart webgui.

Repeat the same steps from 1 to 5 on the other servers.

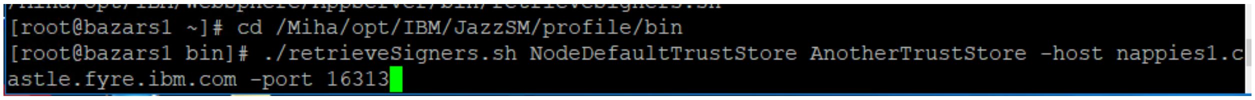
Afterwards, run the following command on each node for each *myremotehost* (that is, for every node that you want to enable trust with) in the cluster.

JazzSM_WAS_Profile/bin/retrieveSigners.sh NodeDefaultTrustStore AnotherTrustStore -host **myremotehost** -port **remote_SOAP_port**

where:
myremotehost is the name of the server to enable trust with;
remote_SOAP_port is the SOAP connector port number (16313 is the default). If you have installed with non-default ports, check *JazzSM_WAS_Profile*/properties/portdef.props for the value of SOAP_CONNECTOR_ADDRESS and use that.

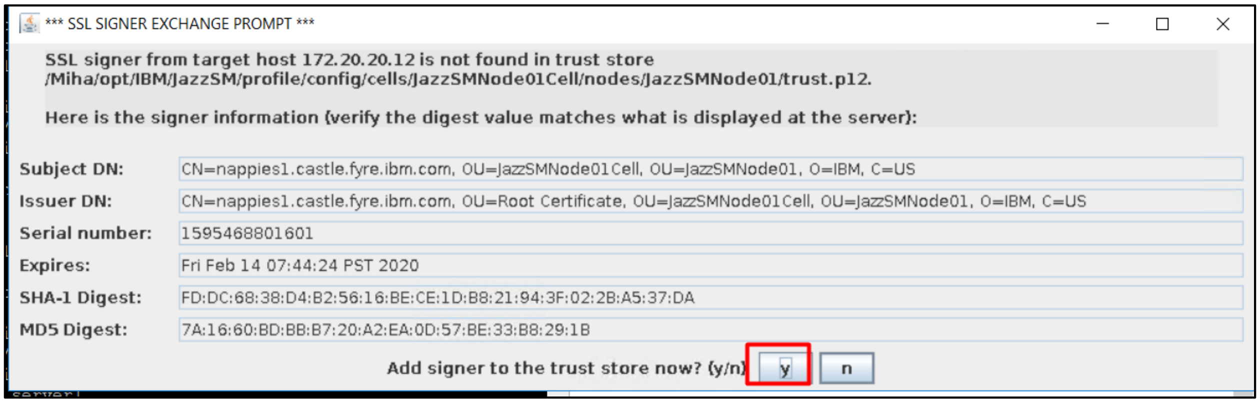
So, on server 1: run the following command – the host added in command line is the one from the second server:

./retrieveSigners.sh NodeDefaultTrustStore AnotherTrustStore -host **loaf1.castle.fyre.ibm.com** -port 16313



```
[root@bazars1 ~]# cd /Miha/opt/IBM/JazzSM/profile/bin
[root@bazars1 bin]# ./retrieveSigners.sh NodeDefaultTrustStore AnotherTrustStore -host nappies1.c
astle.fyre.ibm.com -port 16313
```

Click **yes** to add the signer to the trust store:



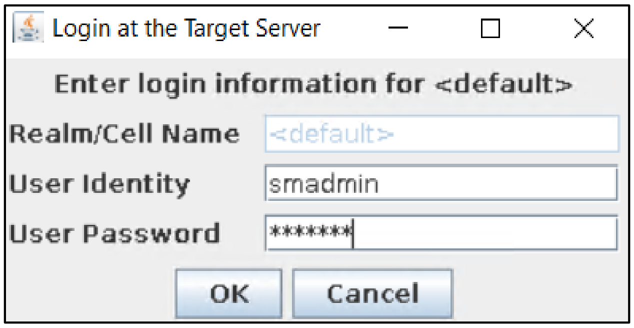
SSL signer from target host 172.20.20.12 is not found in trust store /Miha/opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/nodes/JazzSMNode01/trust.p12.

Here is the signer information (verify the digest value matches what is displayed at the server):

Subject DN:	CN=nappies1.castle.fyre.ibm.com, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US
Issuer DN:	CN=nappies1.castle.fyre.ibm.com, OU=Root Certificate, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US
Serial number:	1595468801601
Expires:	Fri Feb 14 07:44:24 PST 2020
SHA-1 Digest:	FD:DC:68:38:D4:B2:56:16:BE:CE:1D:B8:21:94:3F:02:2B:A5:37:DA
MD5 Digest:	7A:16:60:BD:BB:B7:20:A2:EA:0D:57:BE:33:B8:29:1B

Add signer to the trust store now? (y/n)

Enter **smadmin** credentials and click **ok**:

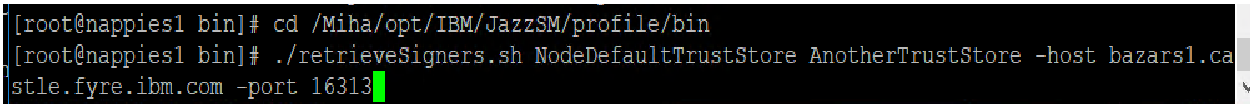


Enter login information for <default>

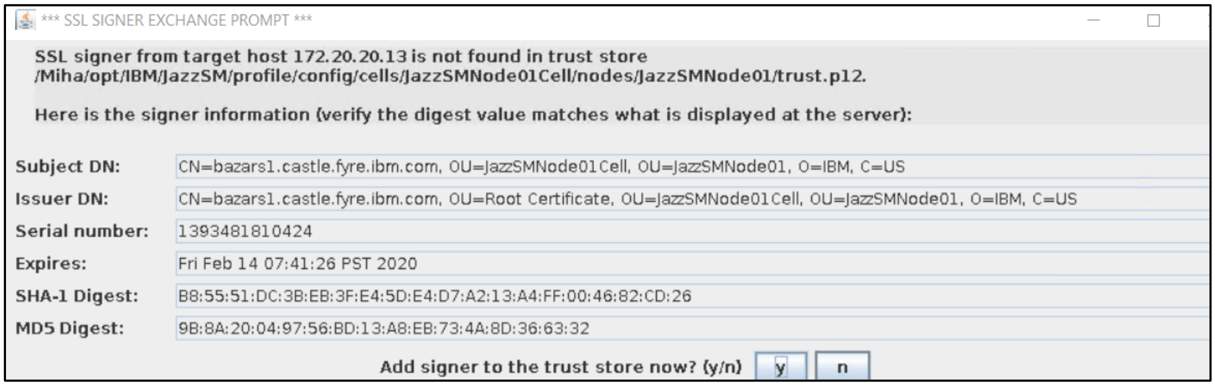
Realm/Cell Name	<default>
User Identity	smadmin
User Password	********

On server 2 – run the same but add the host of the webgui **server1**, example:

./retrieveSigners.sh NodeDefaultTrustStore AnotherTrustStore -host bazarz1.castle.fyre.ibm.com -port 16313



```
[root@nappies1 bin]# cd /Miha/opt/IBM/JazzSM/profile/bin
[root@nappies1 bin]# ./retrieveSigners.sh NodeDefaultTrustStore AnotherTrustStore -host bazars1.ca
stle.fyre.ibm.com -port 16313
```

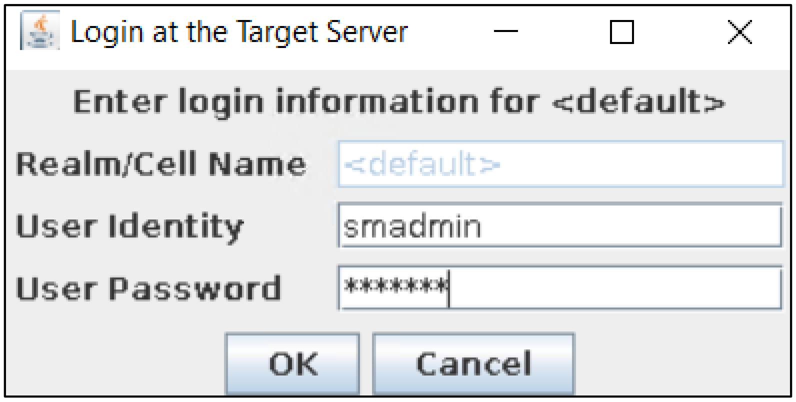


SSL signer from target host 172.20.20.13 is not found in trust store /Miha/opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/nodes/JazzSMNode01/trust.p12.

Here is the signer information (verify the digest value matches what is displayed at the server):

Subject DN:	CN=bazars1.castle.fyre.ibm.com, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US
Issuer DN:	CN=bazars1.castle.fyre.ibm.com, OU=Root Certificate, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US
Serial number:	1393481810424
Expires:	Fri Feb 14 07:41:26 PST 2020
SHA-1 Digest:	B8:55:51:DC:3B:EB:3F:E4:5D:E4:D7:A2:13:A4:FF:00:46:82:CD:26
MD5 Digest:	9B:8A:20:04:97:56:BD:13:A8:EB:73:4A:8D:36:63:32

Add signer to the trust store now? (y/n)



Login at the Target Server

Enter login information for <default>

Realm/Cell Name <default>

User Identity smadmin

User Password *******

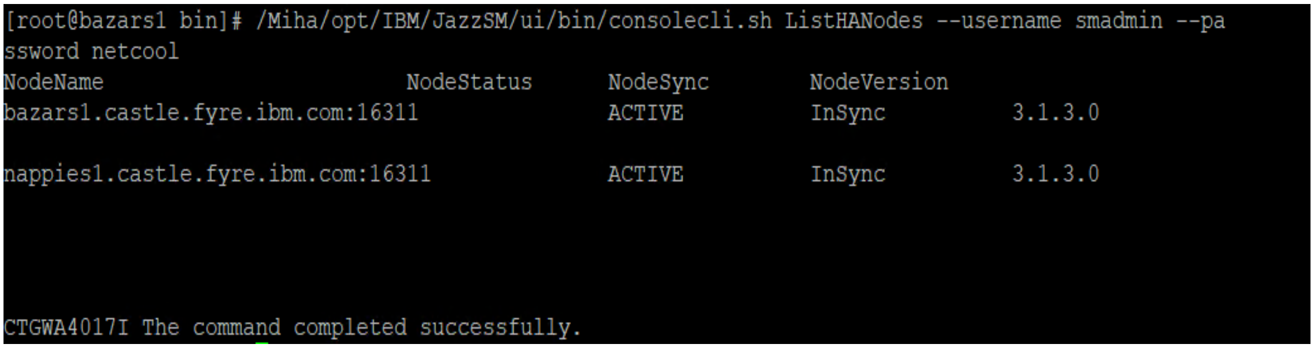
OK Cancel

Restart all webgui servers again.

At the end, you will have your HA environment configured.

Check status by running on each webgui server the following command:

./consolecli.sh ListHANodes –username smadmin –password netcool



```
[root@bazars1 bin]# /Miha/opt/IBM/JazzSM/ui/bin/consolecli.sh ListHANodes --username smadmin --pa
ssword netcool
NodeName                        NodeStatus      NodeSync        NodeVersion
bazars1.castle.fyre.ibm.com:16311               ACTIVE          InSync          3.1.3.0

nappies1.castle.fyre.ibm.com:16311              ACTIVE          InSync          3.1.3.0




CTGWA4017I The command completed successfully.
```

Hope you’ll find this useful for your HA configuration!