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

```
[db2instl@thriverl ~]$ db2 create database DASDB
DB20000I The CREATE DATABASE command completed successfully.
[db2instl@thriverl ~]$ db2 connect to DASHDB
Database Connection Information
Database server = DB2/LINUXX8664 10.5.0
SQL authorization ID = DB2INST1
Local database alias = DASHDB
```

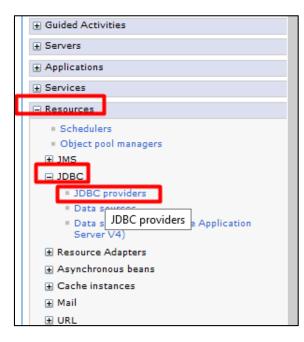
Configuration needed on each WebGUI server

On the first WebGUI server:

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



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



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

JDBC providers		2
JDBC providers Use this page to edit properties of a JDBC	provider. The JDBC provider object encaps	ulates the specific JDBC driver
	ecific vendor database of your environment a list of task steps and more general infor	
Scope: =All scopes		
	h the resource definition is visible. For deta d how it works, <u>see the scope settings help</u>	
Cell=JazzSMNode01Cell		
Node=JazzSMNode01	server1	
Select Name 🗘	ocope 0	Description 🗘
You can administer the following resource	es:	
Derby JDBC Provider	Node=JazzSMNode01,Server=server1	Derby embedded non-XA JDBC Provider
Total 1		

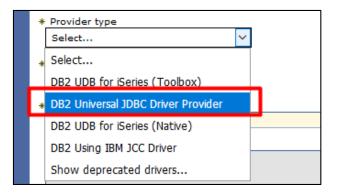
4. Create a new JDBC provider by clicking on the New option:

_	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	2
	DB2	\sim
'		

For provider type select DB2 universal JDBC driver provider:



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.

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



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
```

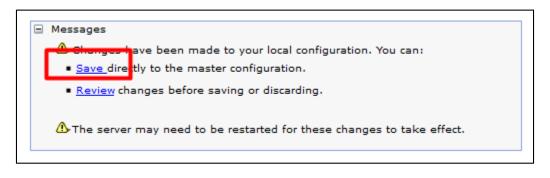
```
Directory location which is saved as WebSphere variable ${DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH}
/Miha/opt/IBM/JazzSM/lib/db2
```

Click next.

Click finish.

Step 1: Create new JDBC provider	Summary		
	Summary of actions:		
Step 2: Enter database class path	Options Values		
information	Scope	cells:JazzSMNode01Cell:nodes:JazzSMNode01:servers:server1	
Step 3: Summary	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	\${D82UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc.jar \${UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar \${D82UNIVERSAL_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):

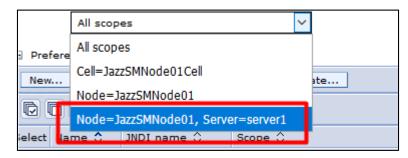


5. Create a new Data Source for JDBC.

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



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



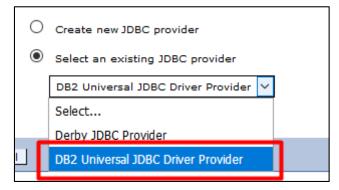
Click on "New"

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":



Click on Next.

	Step 1: Enter basic data source	Enter database specific	c properties for the data source	
	information			
	Step 2: Select JDBC provider	Set these database-specific properties, which are required by the database vendor JDBC driver to support the connections that are managed through the datasource.		
>	Step 3: Enter	Name	Value	
	database specific properties for the	+ Driver type	4 ~	
	data source	+ Database name	DASHDB	
	Step 4: Setup security aliases	* Server name	thriver1.castle.fyre.ibm.com	
	Step 5: Summary	* 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	Setup security aliases
data source information	
Step 2: Select JDBC	Select the authentication values for this resource.
provider	Component-managed authentication alias
Step 3: Enter database specific properties for the data source	Mapping-configuration alias (none)
→ Step 4: Setup security aliases	Container-managed authentication alias (none)
Step 5: Summary	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.
	Security domains
Previous Next Can	cel

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: <u>Save</u> directly to the master configuration. 	
 <u>Save</u> directly to the master configuration. 	Messages
	🛆 Changes have been made to your local configuration. You can:
	 <u>Save</u> directly to the master configuration.
Review changes before saving or discarding.	Review changes before saving or discarding.

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

C						
Select	Name 🛟	JNDI name 🗘	Scope 🗘	Provider 🗘	Description 🗘 C	
You o	an administe	r the following resou	irces:			
	<u>Default</u> <u>Datasource</u>	DefaultDatasource	Node=JazzSMNode01,Server=server1	Derby JDBC Provider	Datasource for the WebSphere Default Application	
	<u>tipds</u>	jibc/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.



Click on new:

🗉 Preferer	ces		
New	Delete		
	#		
Select Alia	s 🗘		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.

<u>Data sources</u> > <u>tipds</u> > <u>JAAS - J2C auther</u> Specifies a list of user identities and pass	
General Properties	
* Alias DB2 alias	
* User ID	
db2inst1	
* Password	
•••••	
Description	
Apply OK Reset Cancel	

Click **ok**.

Save the configuration.

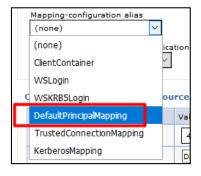
Select	Alias 🗘	User ID 🗘	Description 🗘					
You can administer the following resources:								
	JazzSMNode01/DB2 alias	db2inst1						
Total	Total 1							

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 th	e authentica	tion values f	or this resource	
Compor	ent-manag	ed authentica	ation alias	
(none)		\sim		
(none)			_	
JazzSM	lode01/DB2	_alias 🖌		
Con	ainer-mana	aged authenti	ication alias	
(no	ne)	~		

Select **DefaultPrincipalMapping** for mapping-configuration a lias:



Select JazzSMNode01/DB2_alias for container-manager authentication alias:

	Container-managed authentication alias						
	(none)	~					
	(none)	_					
Com	JazzSMNode01/DB2_alias	irce proper					

Click ok.

Click **Save** to store the configuration.

8. Check tipds data source connection:

New Delete Test connection Manage state Image: Image state i						
Select	Name 🗘	JNDI name 🗘	Scope 🗘	Provider 🗘	Description 🗘	Category 3
You c	You can administer the following resources:					
	<u>Default</u> <u>Datasource</u>	DefaultDatasource	Node=JazzSMNode01,Server=server1	Derby JDBC Provider	Datasource for the WebSphere Default Application	
	<u>tipds</u>	jdbc/tipds	Node=JazzSMNode01,Server=server1	DB2 Universal JDBC	DB2 Universal Driver Datasource	

The output should be the below one:



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

∃ Guided Activities	
Servers	
 Server Types 	
WebSphere application servers	
WebSphere MQ servers	
= Web servers	
Applications	

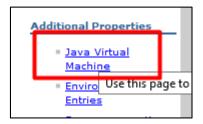
Click on **server1**:

	Preferences				
	+++ + +				
	Name 🛟		Node 🗘	Host Name 🗘	Version 🗘
r	- Yeu een edmig	ister the follo	wing resources:		
ſ	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:

			· · ·
Г	🗄 Pref	ere	ces
L	New		Delete
	Q (***
	Select	Nar	me 🗘
	You ca	an a	dminister the following resources
		<u>cor</u>	n.ibm.security.jgss.debug
			- the second to be Referred and

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

Name	
com.ibm.isc.ha	
• Value	
true	
Description	
Apply OK Reset Cancel	

Click apply and save.

10. On the server, edit the **server.init** file from the webgui **etc** directory and set the following 3 properties as per above:

cluster.mode:on

timedtasks.enabled:true

cluster.hostname:<server_hostname>

Make sure to add the correct hostname of your WebGUI/DASH server for each server.

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

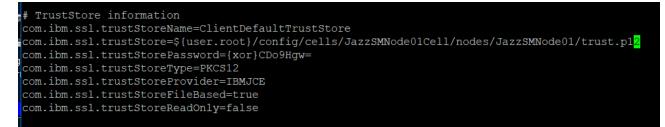
Uncomment the section that starts with **com.ibm.ssl.alias=AnotherSSLSettings** so that it looks like this:

, #
Another SSL configuration (this is a template, uncomment and modify)
<pre># You can configure the dynamicSelectionInfo OR reference this alias # form another mattered (a non-selectionInfo or reference this alias)</pre>
<pre># from another protocol (e.g., soap.client.props or sas.client.props) #</pre>
" 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
<pre>#com.ibm.ssl.keyStoreClientAlias=default</pre>
<mark>c</mark> om.ibm.ssl.customTrustManagers=
#com.ibm.ssl.customKeyManager=
<pre>#com.ibm.ssl.dynamicSelectionInfo=</pre>
<pre>#com.ibm.ssl.enabledCipherSuites=</pre>

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:



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 EX	🔬 *** SSL SIGNER EXCHANGE PROMPT *** – 🗆 🗙						
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 si	gner 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:	MD5 Digest: 7A:16:60:BD:BB:B7:20:A2:EA:0D:57:BE:33:B8:29:1B						
i	Add signer to the trust store now? (y/n)						

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

🛓 Login at the Target Server 🛛 🗆 🗙						
Enter login information for <default></default>						
Realm/Cell N	lame	≺defa	ault>			
User Identit	y	smad	min			
User Passw	ord	*****	o k			
	ок	0	Cancel			

On server 2 – run the same but add the host of the webgui **server 1**, 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 EXCHANGE PROMPT *** —								
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) y n							

🛓 Login at the Target	Server	_		\times				
Enter login information for <default></default>								
Realm/Cell Name	<default< th=""><th>></th><th></th><th></th></default<>	>						
User Identity	smadmir	1						
User Password ******								
ОК	Car	ncel						

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:

 $./consolecli.sh\,List HANodes\,-username\,smadmin-password\,netcool$

<pre>[root@bazars1 bin]# /Miha ssword netcool</pre>	/opt/IBM/JazzSM/ui/b	in/consolecli.	sh ListHANodes -	-username smadminpa
NodeName	NodeStatus	NodeSync	NodeVersion	
bazars1.castle.fyre.ibm.c	ACTIVE	InSync	3.1.3.0	
nappies1.castle.fyre.ibm.	com:16311	ACTIVE	InSync	3.1.3.0
CTGWA4017I The command co	mpleted successfully			

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