14 Audit Sink and Audit Lookup Policies

14.1 Description

This tutorial demonstrates using the audit sink policy to store and retrieve audit records to an external database using JDBC. For the purpose of this tutorial, we will create a new database instance on the gateway to act as an external gateway. If you have the ability to connect an actual remote DB, you may modify the steps for DB creation to apply for your database.

14.2 Prerequisites

14.2.1 Environment

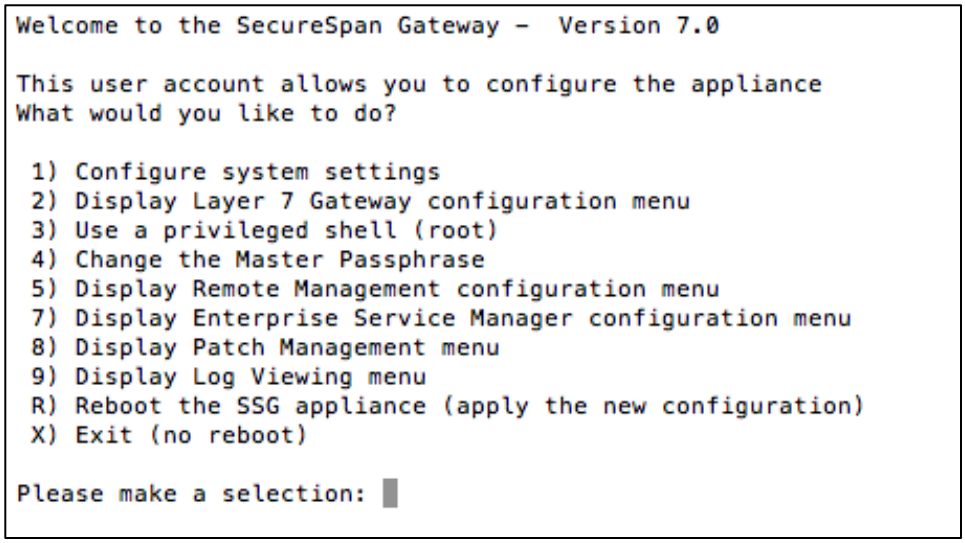
1. Layer 7 SecureSpan Gateway *(this tutorial was designed using a version 7.0 gateway; it may or may not work with earlier versions; it should work with later versions)*
2. Layer 7 Policy Manager *(this tutorial uses the Policy Manager software installation; the software installation version must match the gateway version; alternatively, users can use the Policy Manager browser-based version which always matches the gateway version that is connected to)*
3. soapUI *(this tutorial was designed using the free soapUI version 4.5.1; it may or may not work with other versions of soapUI; other clients can be used for this and other tutorials, but specific steps will not be provided for those other clients)*

14.2.2 Tutorials

1. 1 General Information
2. 2 Deploy Tutorial Services
3. 4 Test Tutorial REST Service
4. 6 Publish REST Service

14.3 Tutorial Steps

1. Login the gateway shell using your favorite SSH utility (i.e. Putty) using the username: "ssgconfig" and password: "7layer". Once logged in you will be presented with the gateway configuration menu as shown below:



2. Select "3) Use a privileged shell (root)" and hit enter.

3. Enter the root password: “7layer”
4. Change directory to the ssgconfig home directory by typing: “cd /home/ssgconfig”
5. Access the MySQL database shell by typing: “mysql”

```
[root@l7apimgmt ssgconfig]# mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 580
Server version: 5.5.28-enterprise-commercial-advanced-log MySQL Enterprise Serve
r - Advanced Edition (Commercial)

Copyright (c) 2000, 2012, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

6. Create a new database instance by typing: “create database auditsink_tutorial;”

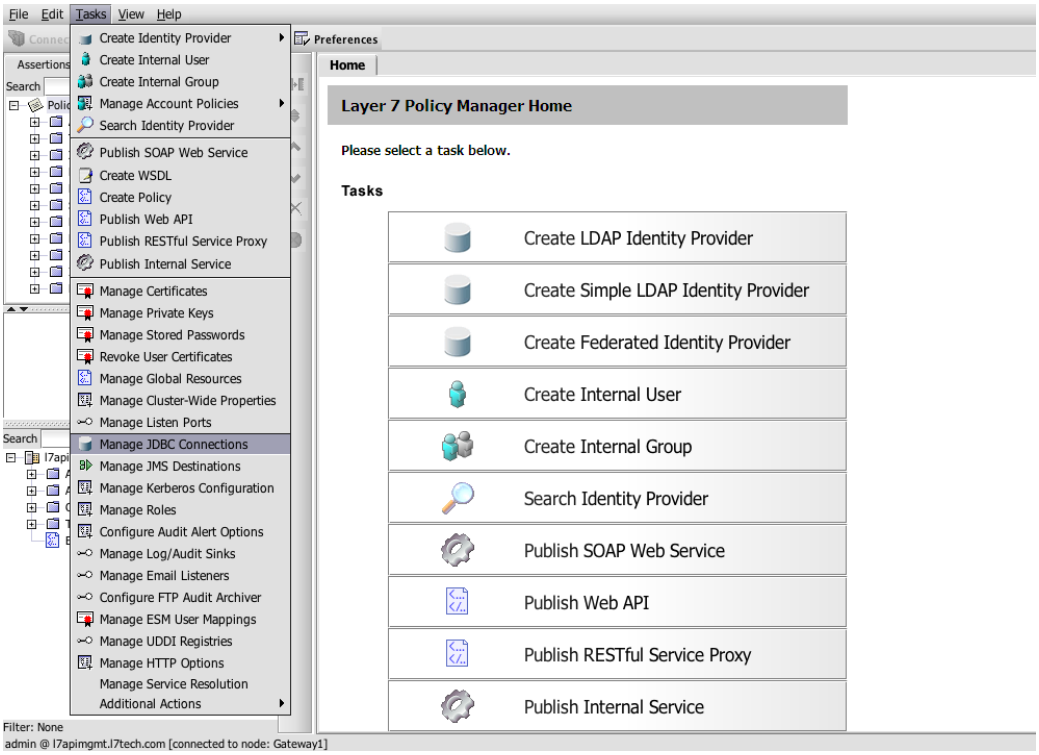
```
mysql> create database auditsink_tutorial;
Query OK, 1 row affected (0.00 sec)

mysql>
```

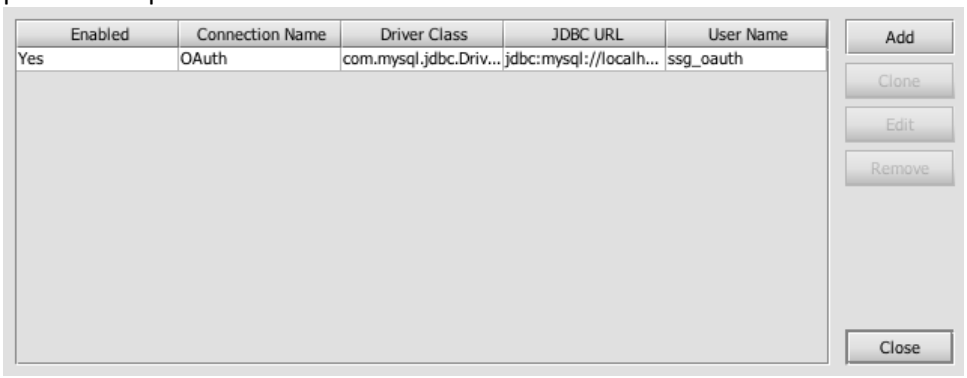
7. Exit the MySQL shell by typing: “\q”

```
mysql> \q
Bye
[root@l7apimgmt ssgconfig]#
```

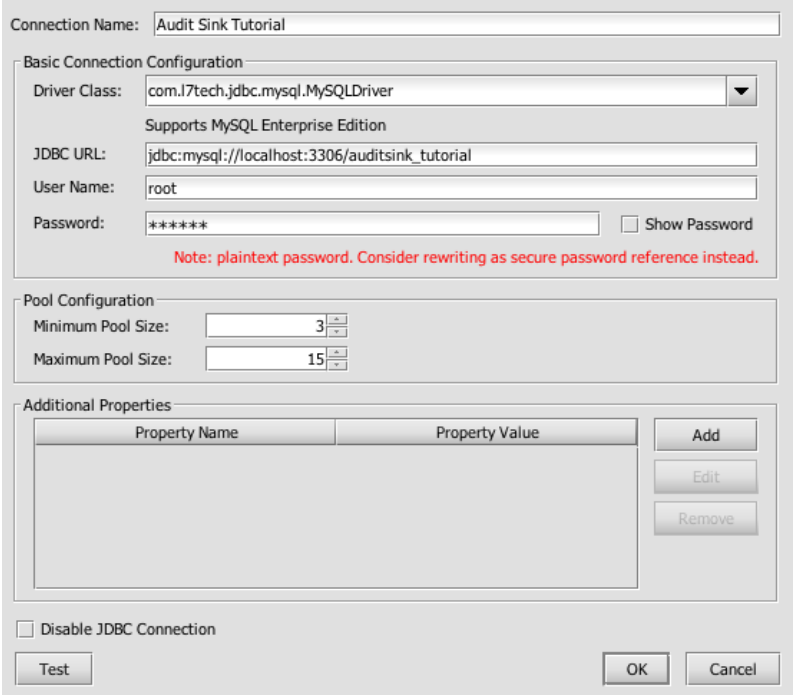
8. Exit the shell by typing: “exit”
9. Exit the menu by selecting: “X) Exit (no reboot)”
10. Connect to your gateway using Policy Manager (see tutorial ***1 General Information***).
11. Per ***1 General Information/Basic Policy Concepts/Policy Authoring/Policy Revisions***, set the active policy version of the ***Warehouse REST Tutorials*** service to the version that has been commented with, **Tutorial 8 Complete**.
12. Go to Tasks->Manage JDBC Connections



13. Press the “Add” button to add database connection for the audit sink database created in the previous steps.

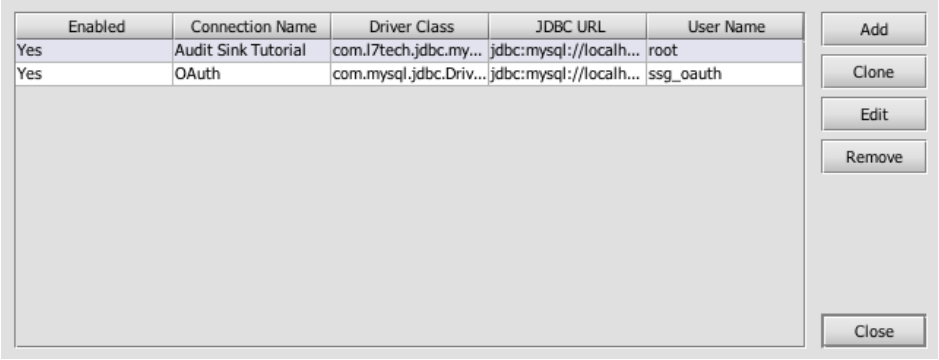


14. Enter the following information:
    - **a.** Connection Name: Audit Sink Tutorial
    - **b.** Driver Class: com.l7tech.jdbc.mysql.MySQLDriver
    - **c.** JDBC URL: jdbc:mysql://localhost:3306/auditsink_tutorial
    - **d.** User Name: root
    - **e.** Password: 7layer

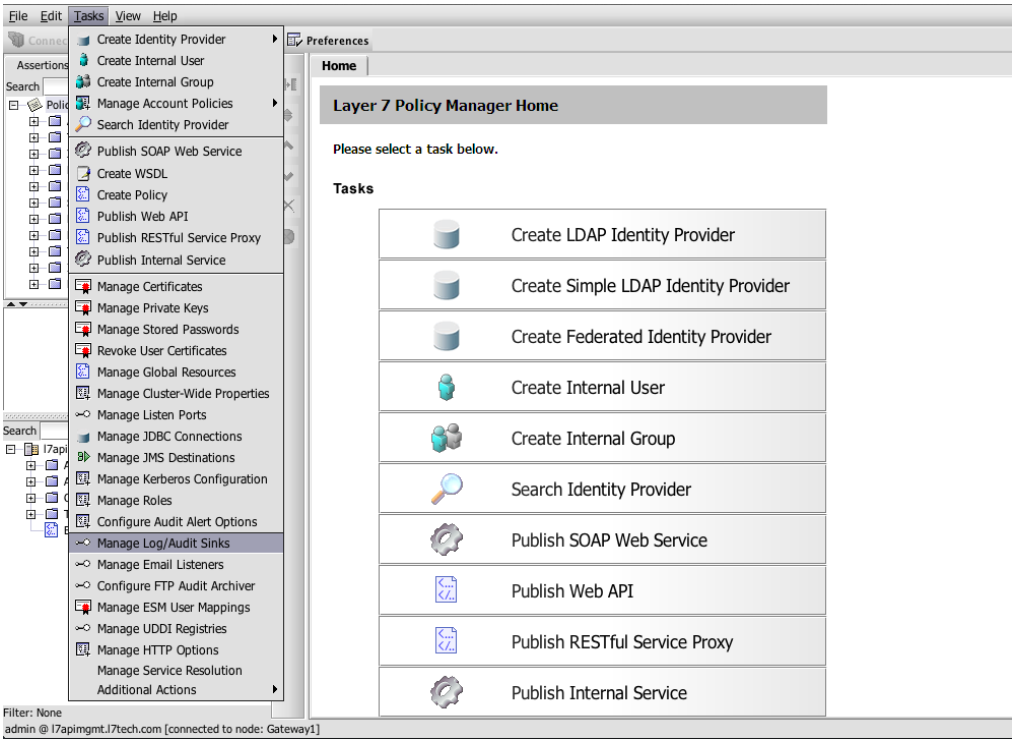


15. Press the “Test” button and ensure the connection test is successful.

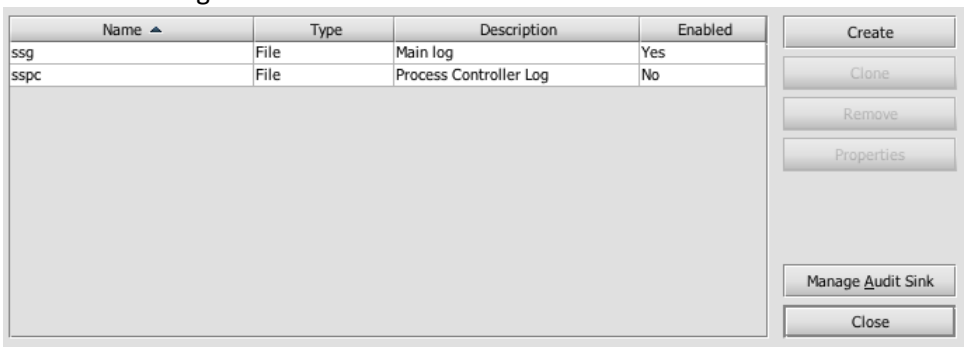
16. Press “OK” to close the JDBC Connection Test window.
17. Press “OK” to close the JDBC Connection Properties window and save the changes. You should now see the new connection listed in the Manage JDBC Connections window.



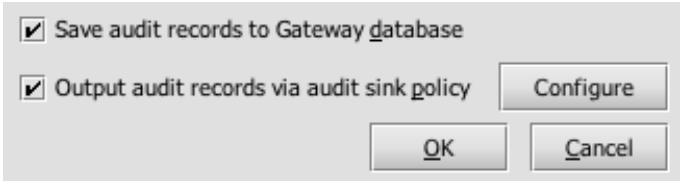
18. Press the “Close” button to close the Manage JDBC Connections window.
19. Go to Tasks->Manage Log/Audit Sinks



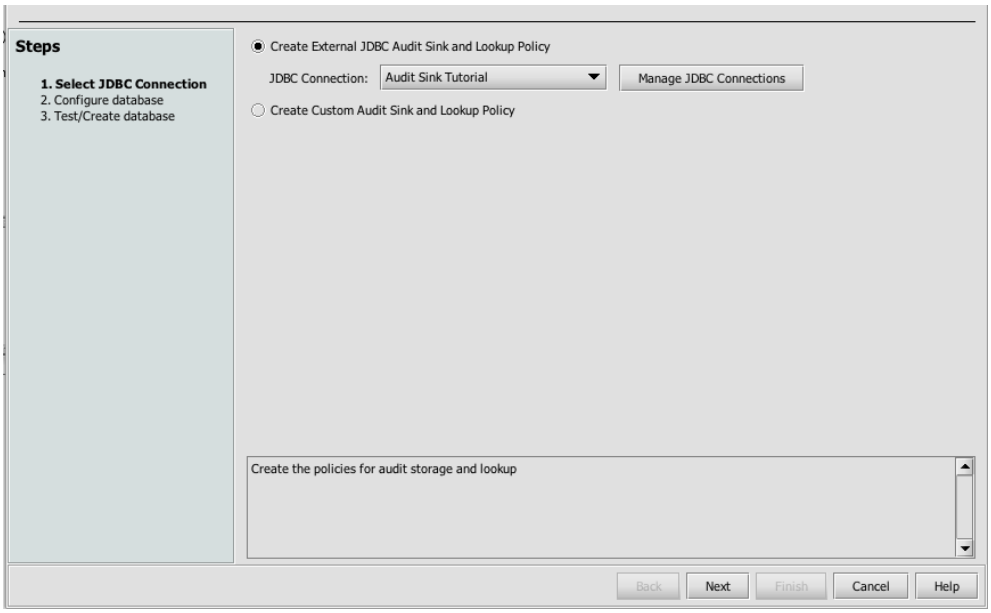
20. Select the Manage Audit Sink button



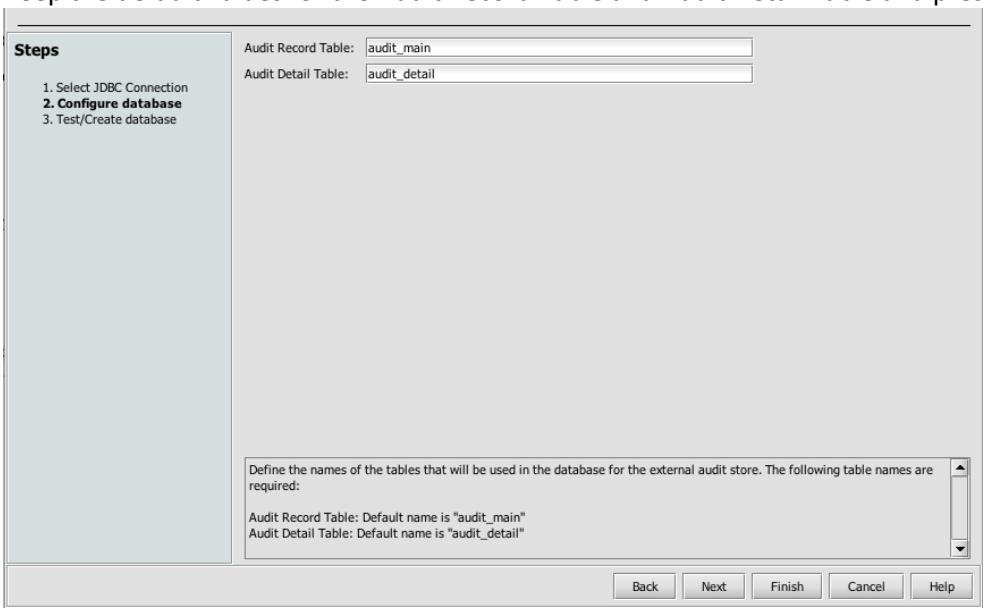
21. Check the “Output audit records via audit sink policy” checkbox and press the “Configure” button.



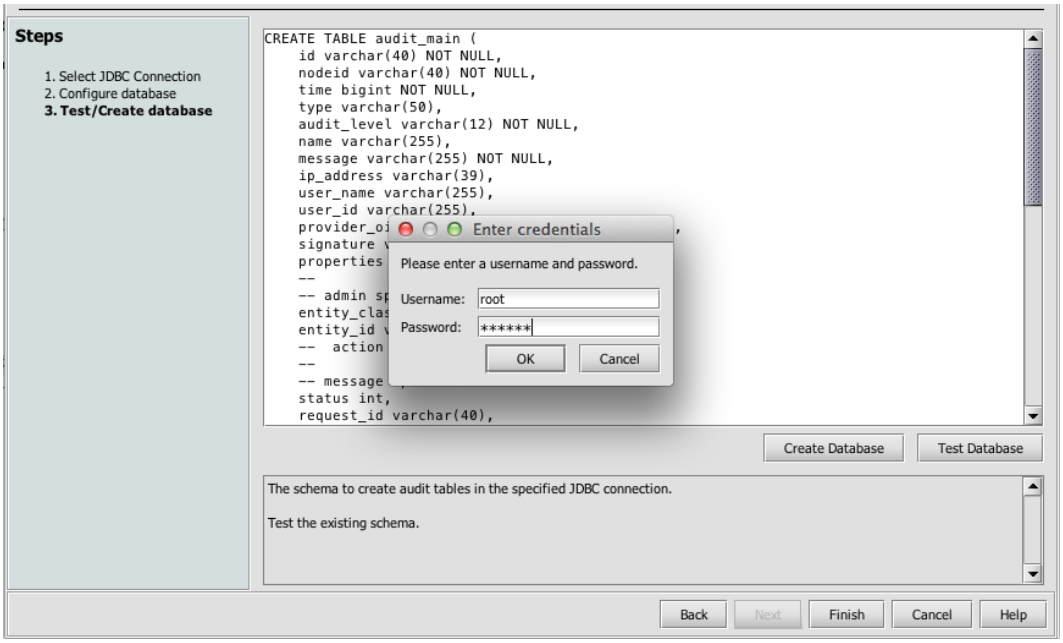
22. Press the “Configure” button to open the Configure External Audit Store Wizard.
23. Select the “Create External JDBC Audit Sink and Lookup Policy” radio button, select “Audit Sink Tutorial” for the JDBC Connection, and then press “Next”.



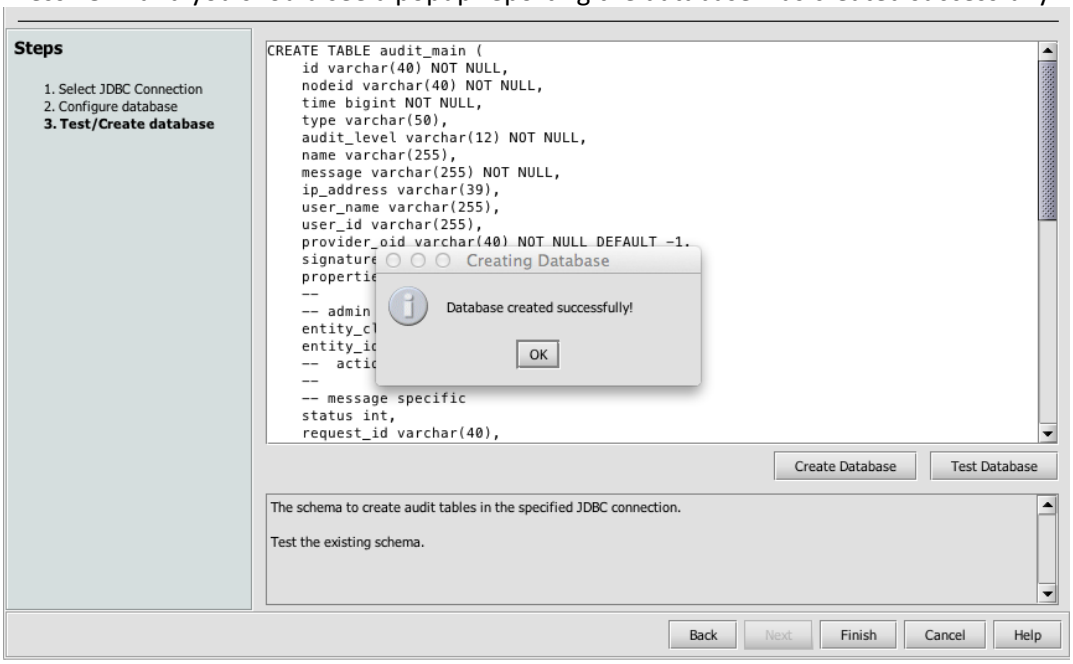
24. Keep the default values for the Audit Record Table and Audit Detail Table and press next.



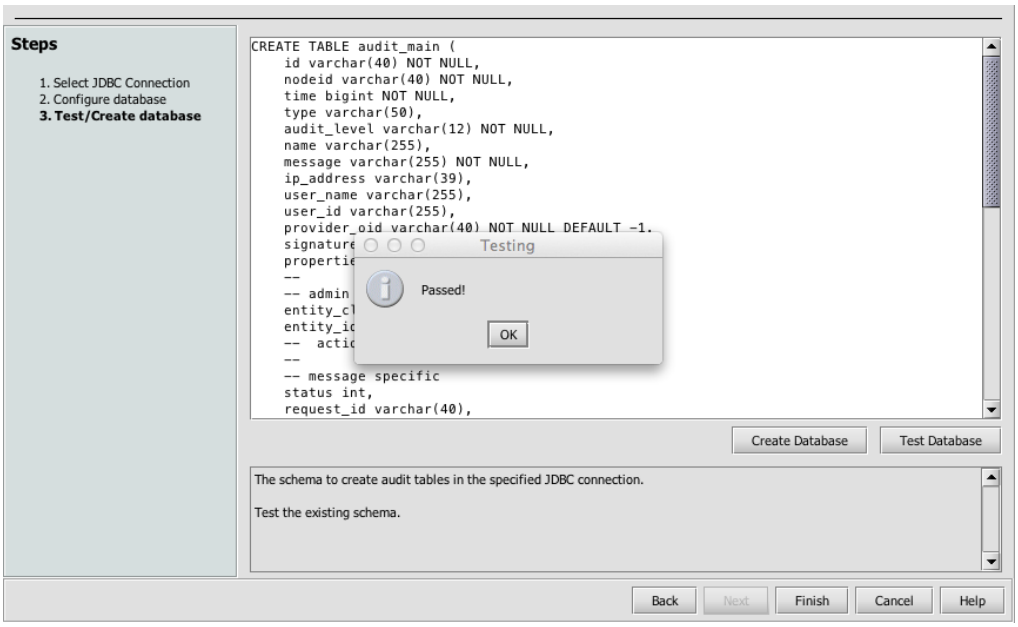
25. Press the “Create Database” button and enter the credentials for the database created in the previous steps (Username: root and Password: 7layer).



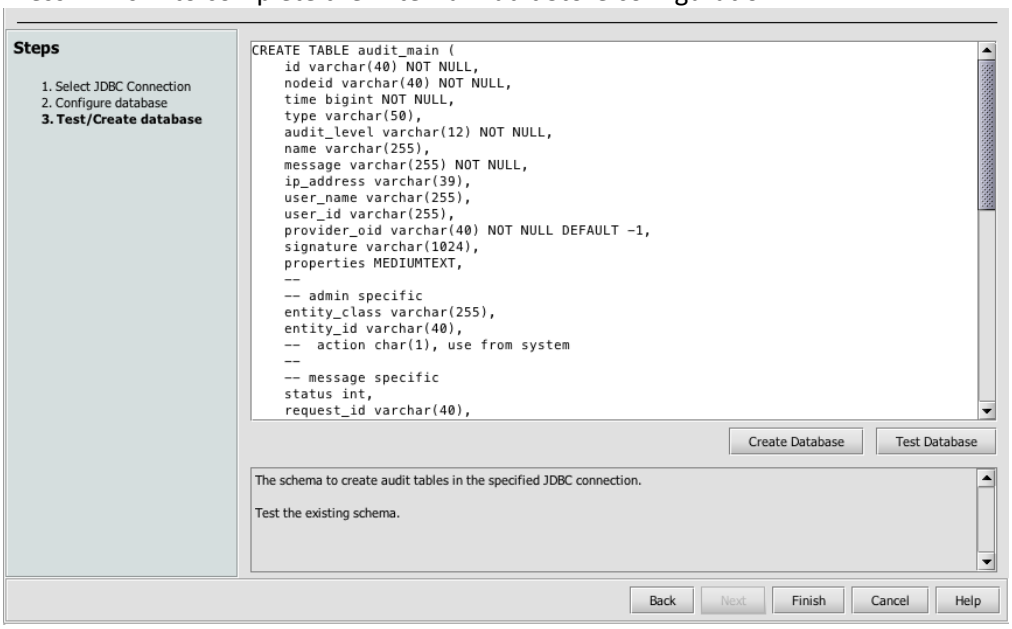
26. Press “OK” and you should see a popup reporting the database was created successfully.



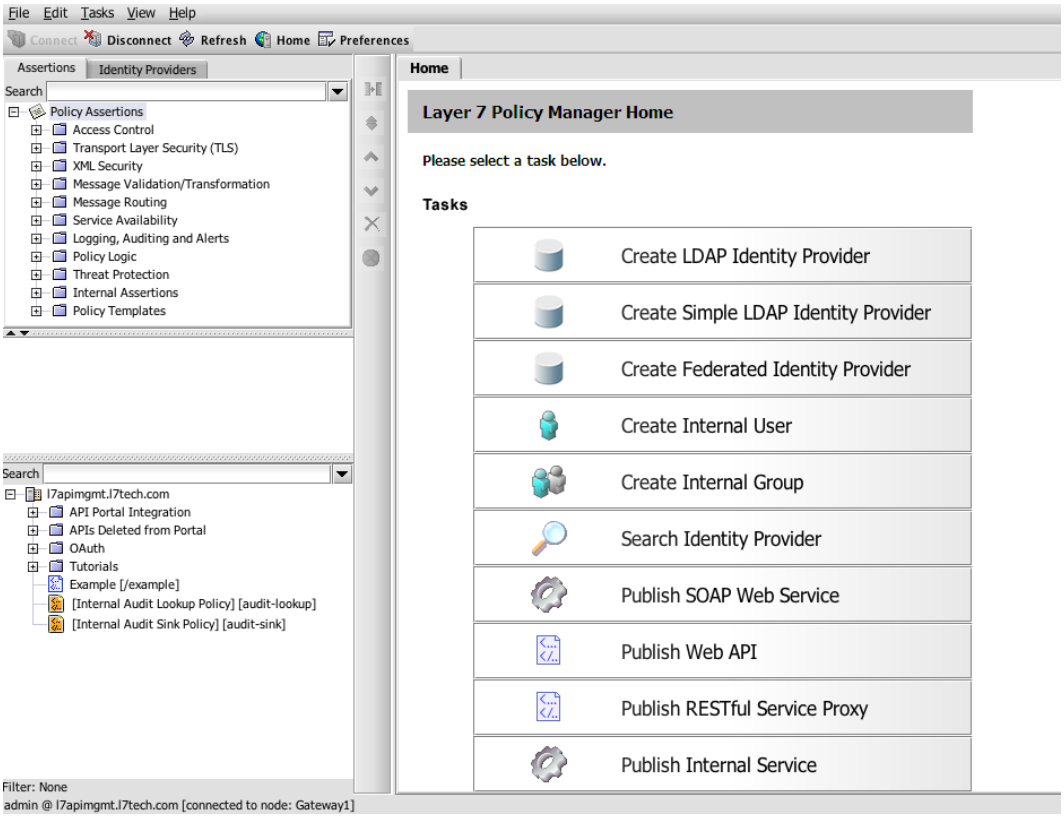
27. Press “OK” to close the Creating Database popup.
28. Press the “Test Database” button to validate the database. A popup indicating the testing has passed should appear.



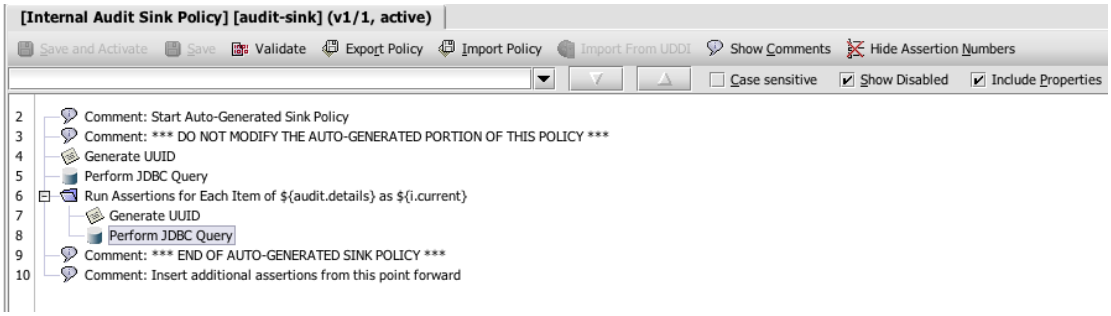
29. Press “OK” to close the Testing popup.
30. Press “Finish” to complete the External Audit Store configuration.



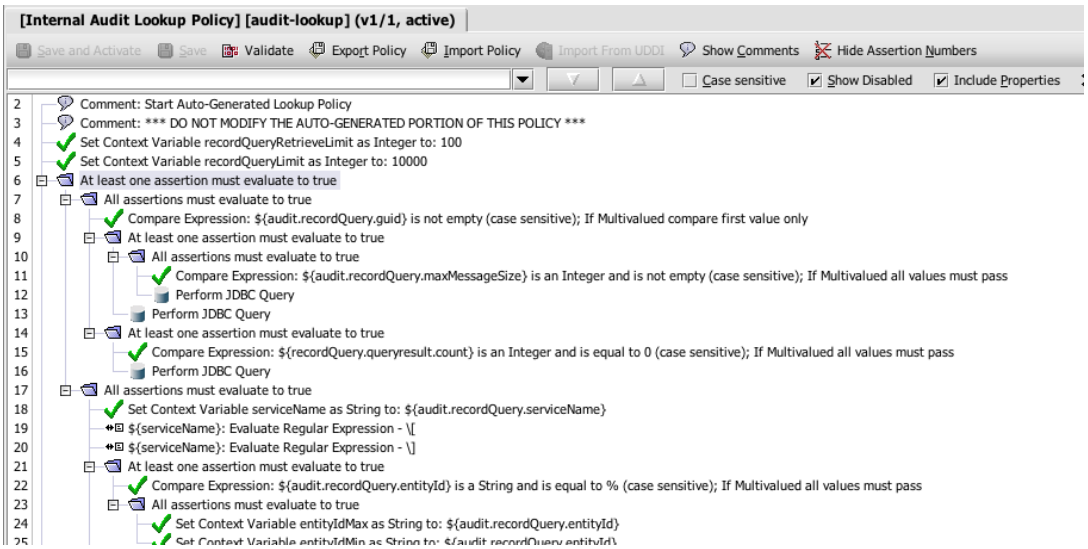
31. Press “OK” to close the Audit Sink Properties window.
32. Press “Close” to close the Manage Log Sinks window.
33. At this point, you will notice two new policies have been created called “[Internal Audit Lookup Policy][audit-lookup]” and “[Internal Audit Sink Policy][audit-sink]”



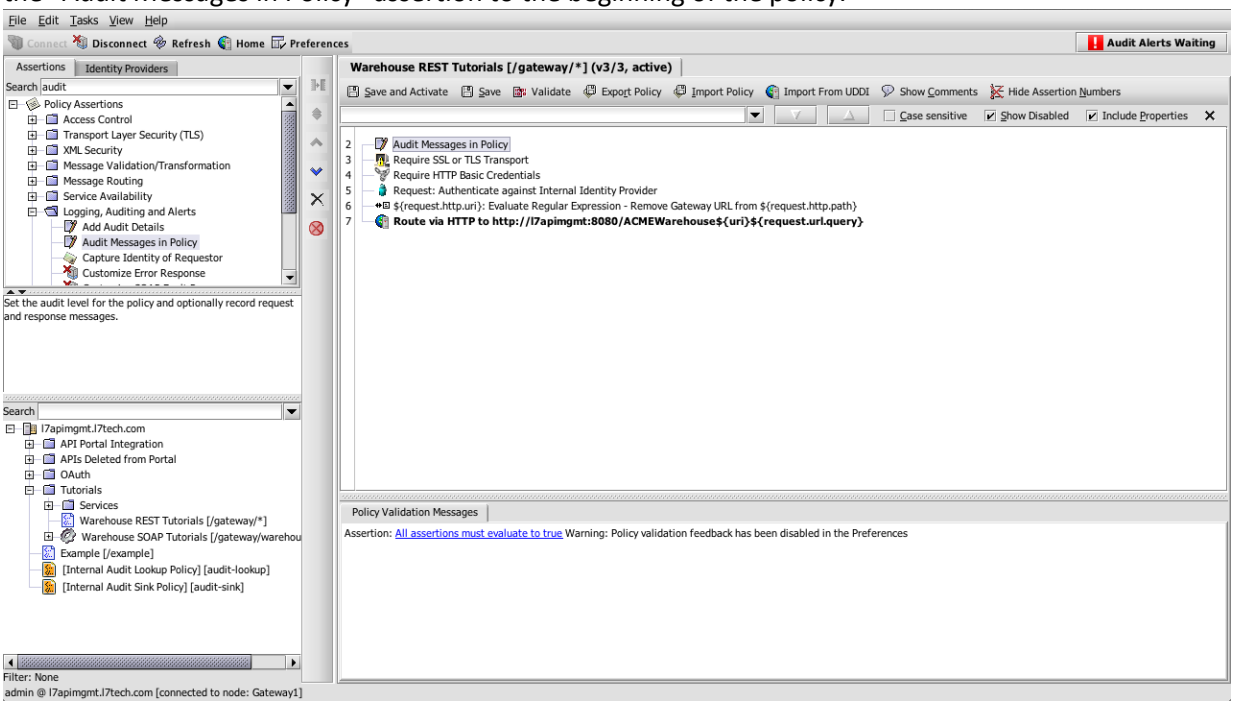
34. Open the Internal Audit Sink Policy by double-clicking on it. You will notice the policy does the following:
    a. Line 4: generates a unique ID to use for the key of the main audit table
    b. Line 5: Performs the JDBC operation to insert an entry into the main audit table
    c. Line 6: Loops through the audit details records that are present to:
        i. Line 7: generates a unique ID to use for the key of the audit details table
        ii. Line 8: Performs the JDBC operation to insert the entry into the audit details table



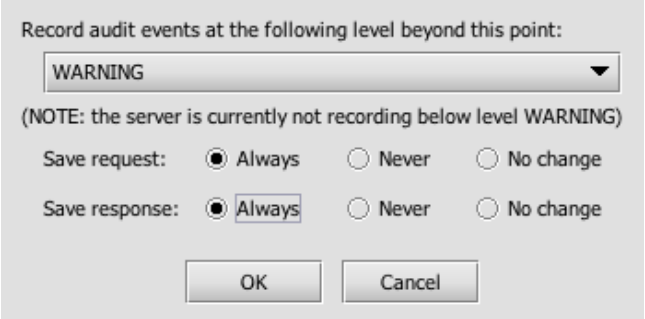
35. Open the Internal Audit Lookup Policy by double-clicking on it. You will notice that the policy is more involved than the Audit Sink Policy. The Lookup policy will query records from the main audit and audit detail tables to allow the display of the audit information within the Audit Log Viewer.



36. Open the Warehouse REST Tutorials service policy created in Tutorial 6. Edit the Policy and add the “Audit Messages in Policy” assertion to the beginning of the policy.

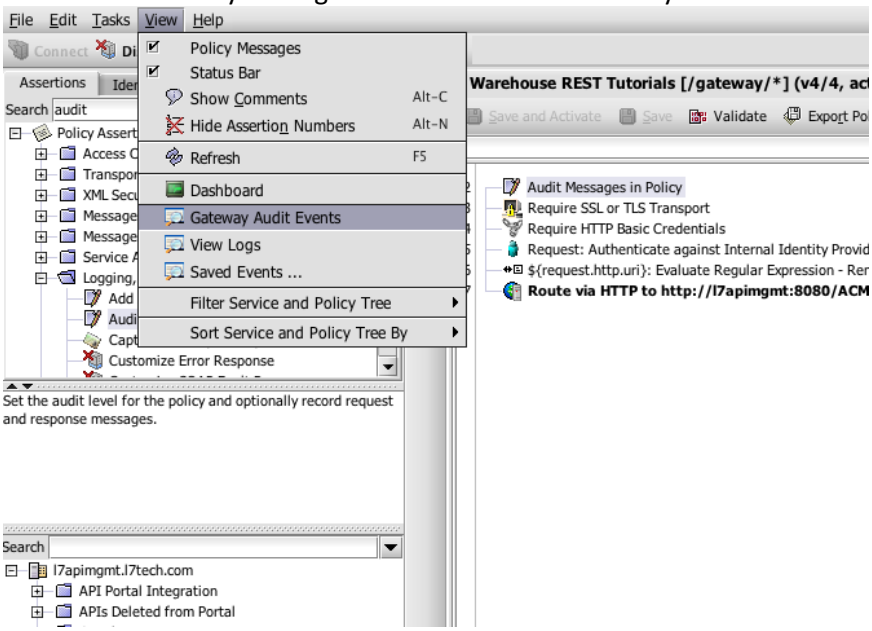


37. Double-click on the “Audit Messages in Policy” assertion within the Warehouse REST Tutorials service and ensure that it is set for WARNING and change the Save Request and Save Response values to both be set to “Always”.

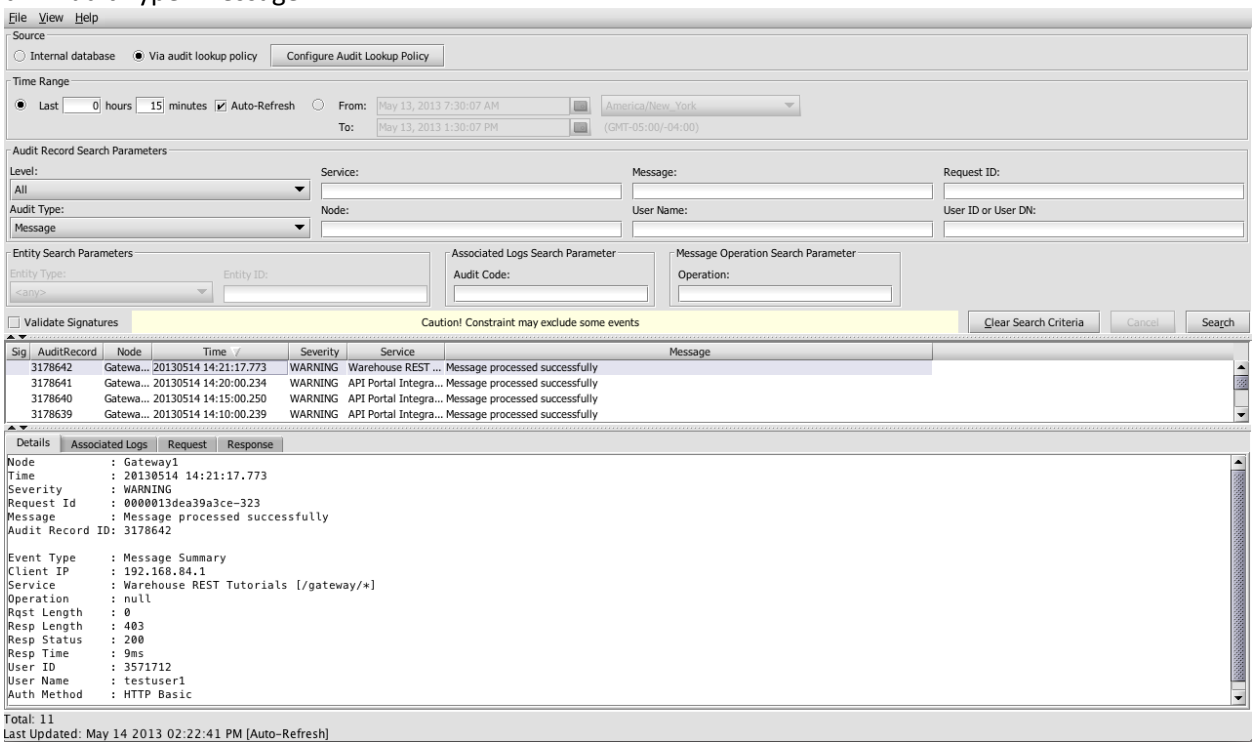


38. Press the “OK” button to close the Audit Properties window.
39. Press the “Save and Activate” button to save and activate the policy.
40. Use SOAPUI to make a call to the Warehouse SOAP service as was done in tutorial 6.

41. Return to the Policy Manager and select View->Gateway Audit Events



42. In the Gateway Audit Events window, set the following and then press the “Search” button:
    a. Source: “Via audit lookup policy”
    b. Time Range: Last 15 minutes
    c. Level: All
    d. Audit Type: Message



43. Select the line for the Warehouse REST service. You will notice the Details tab will display information about the request such as Client IP, Service, response time, etc. The Associated Logs will show additional log details. The Request tab will show the full request (empty in this case as there was no request message body). The Response tab will show the full response.
44. From the Gateway Audit Events window, select File->Exit to close the window and return to the main policy manager window.
45. You are done with this tutorial.

14.4 Additional Context

In this tutorial, we used the Audit Sink Policy to store and retrieve gateway audit events to both the local gateway audit store as well as an external database store (simulated by creating a new database instance on the local gateway image). While we used the default Audit Sink and Audit Lookup policies in this tutorial, it is possible to alter these policies to alter what information is stored and sent to an external audit source. It is also possible to send audit events externally using different protocols such as HTTP(s), JMS, FTP, email, and/or SNMP.

The information that is available to be captured is based on audit context variables. See the Policy Manager online help under the Policy Manager Overview -> Managing Log/Audit Sinks -> Working with the Audit Sink Policy for more details.