IBM Netcool Operations Insight - Fundamentals Training

Course Corrections Document

May 27, 2022

TOD43G (Classroom)
TOD43GI (Self-paced)
TOD43IG (Self-paced)

About this document

This document contains information about issues that were encountered during deliveries of this course. These issues will be addressed in subsequent updates of the material.

You should review this document before the start of class, and use this list as the first point of reference if issues arise.

LDAP self-signed SSL certificate fix

Symptoms

- No users except smadmin can log into DASH.

- The following messages are in /home/dsrdbm01/idsslapd-dsrdbm01/logs/ibmslapd.log (on the VM hosting the LDAP server):

  ```
  GLPSSL019E The SSL layer has reported an unidentified internal error, SSL extended
  error code:10.
  GLPSRV004I Terminating server.
  ```

- The IBM LDAP server starts in configuration-only mode.

- The IBM LDAP administration server cannot start.

Cause

The SSL certificate that allows secure communication between LDAP and WebSphere Application Server is expired.

The password for the LDAP keystore database is also expired.

Solution

> **Important:** This document uses `host1.tivoli.edu` as an example host name. Use the actual host name in your environment where the LDAP server is running when you apply this fix.

Run the following steps on host1.tivoli.edu to recreate the SSL certificate.

1. Start the key management tool.

   a. Open a terminal window on host1.tivoli.edu.

   b. Run the following command to switch to the root user. The password is **object00**.

   ```
   su – root
   Password: object00
   ```

   c. Run the following commands to start the Key Management tool.

   ```
   cd /opt/ibm/ldap/V6.3.1/appsrv/bin/

   ./ikeyman.sh
   ```

2. Recreate the SSL certificate.
   a. Click the **Open** icon.
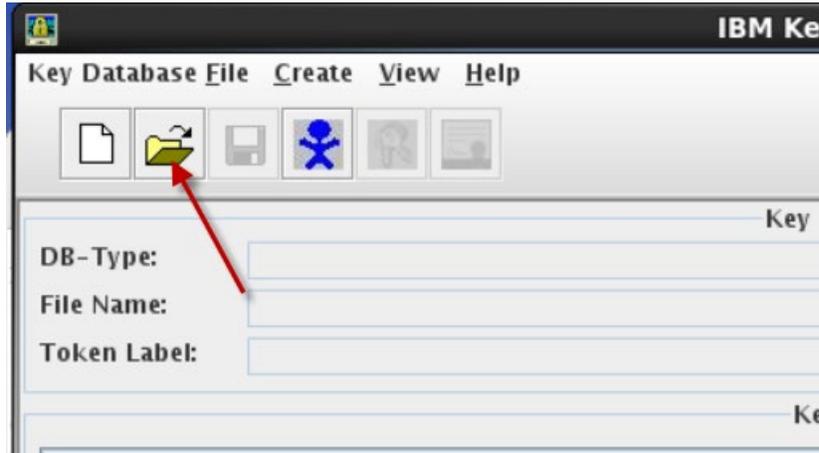
   b. Open the **ldapsslkey.kdb** database. This database is in the **/opt/ibm/ldap/V6.3.1/etc/** directory.
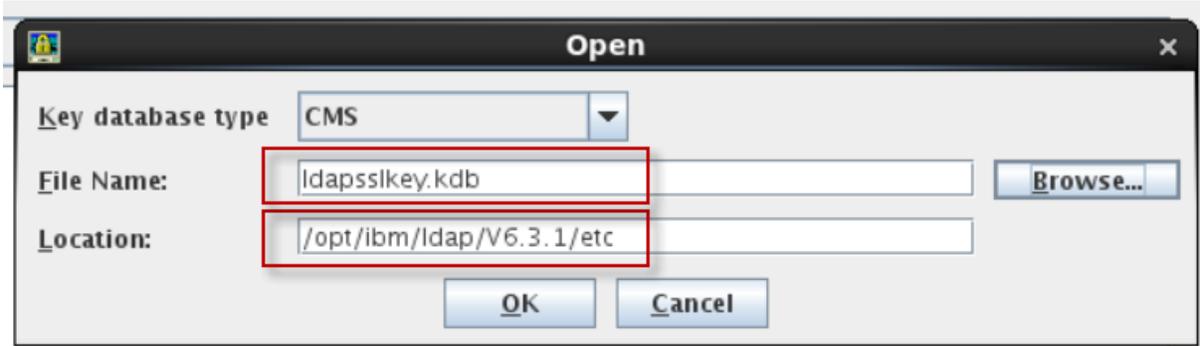
   c. Enter **object00** as the password.

   d. Click **OK** on the password expired message.
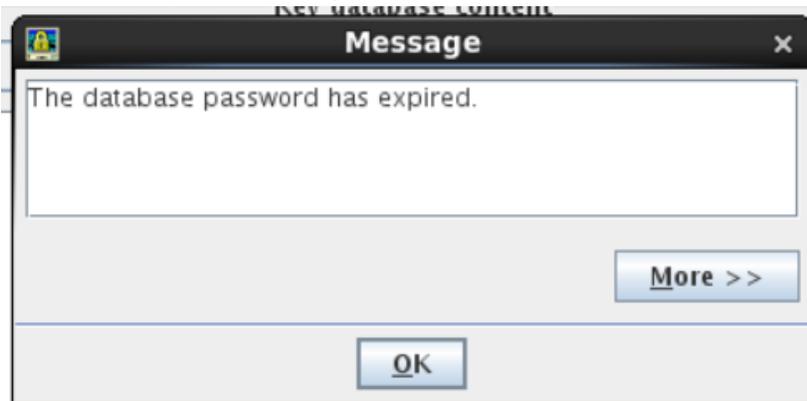
e. Click **Yes** to change the password.

f. Enter **object00** as the password.

g. Enter **object00** again to confirm.

h. Confirm that **Expiration time** is not selected. This ensures that that password does not expire.

j. Click **OK**.
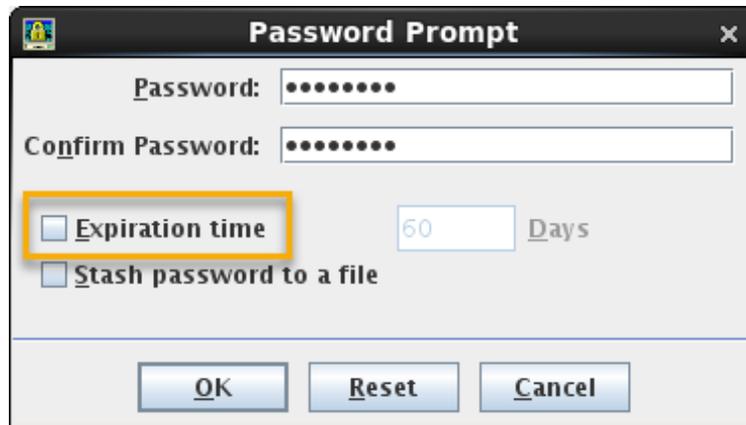
k. Select the **ldapsslkey** certificate.

l. Click **Delete**.

Token Label:

Key database content

Personal Certificates ▼

* ldapsslkey

Receive...

Delete

View/Edit...

Export/Import...

m. Click **Yes** to confirm.

Confirm ✕

? Are you sure you want to delete the selected item?

Yes   No

n. Click **New Self-Signed**.

New Self-Signed...

Extract Certificate...
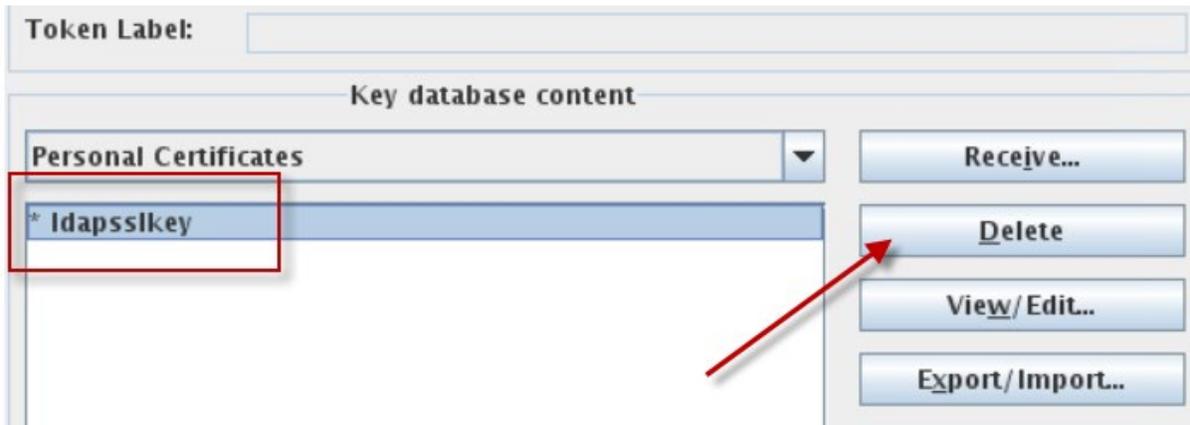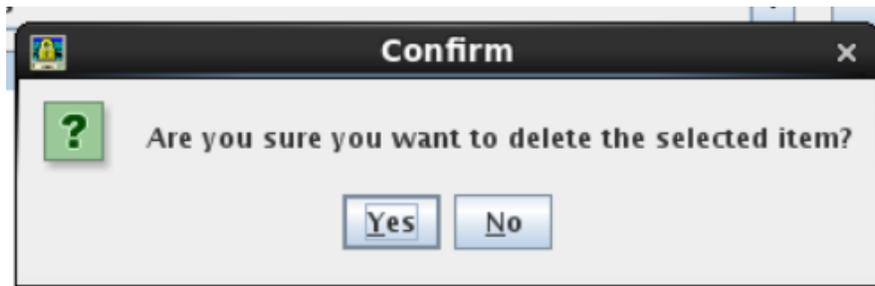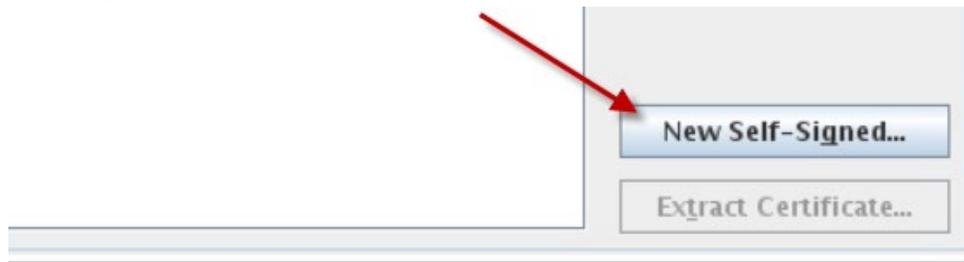
o. Enter **ldapsslkey** as the **Key Label**.

p. Enter your host name as the **Common Name**, if it is not already present.

Important: This document uses `host1.tivoli.edu` as an example host name. Use the actual host name in your environment where the LDAP server is running when you apply this fix.

---

q. Enter **7300** as the **Validity Period**.

r. Click **OK**.

s. Click **Key Database File > Exit**.

3. Start the LDAP server and the Administration server.

   a. Run the following command to start the SDS Instance Administration tool.

   `/opt/ibm/ldap/V6.3.1/sbin/idsxinst`

   b. Notice that the server state is **Started (config only)**.

   c. Click **Start/Stop**.
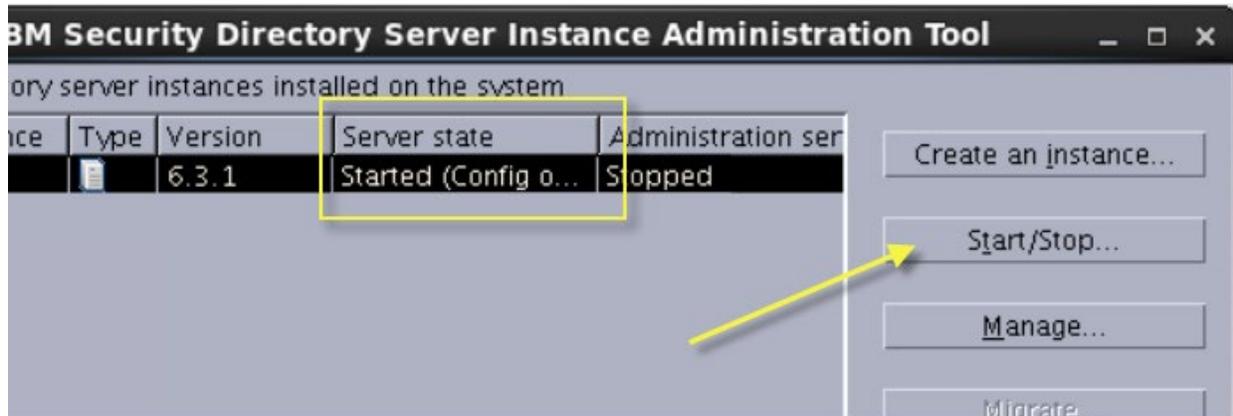
d. Click **Stop server**. After a moment, the server stops.
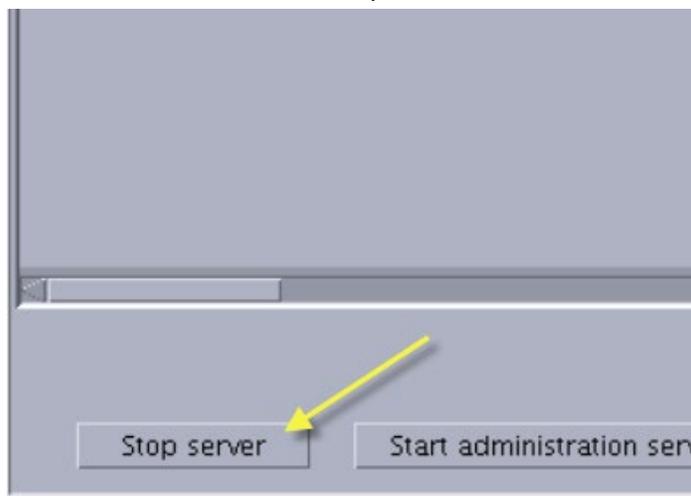
e. Click **Start server**. After a moment, the server starts.
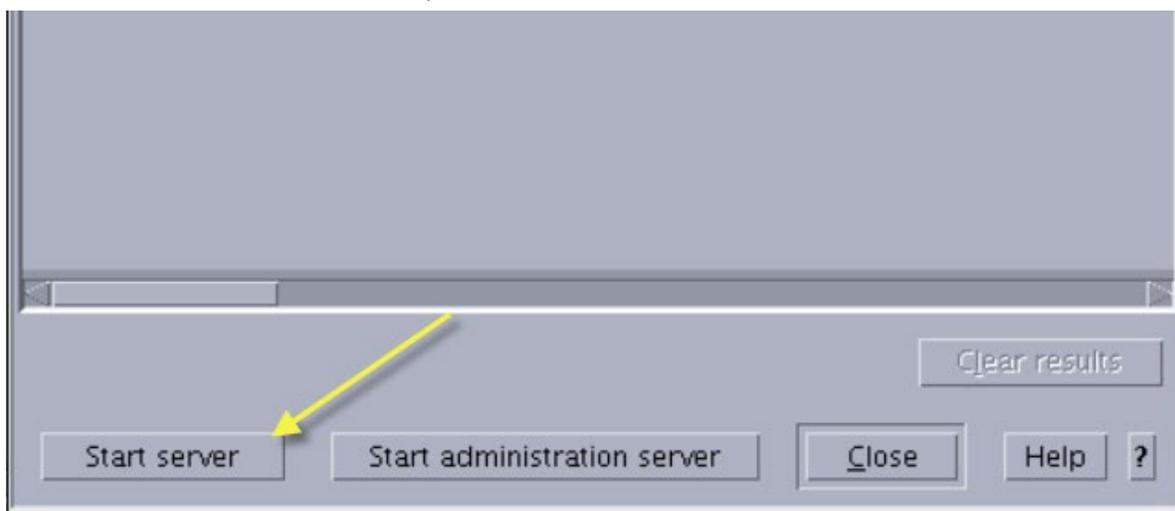
f. Click **OK** to confirm.
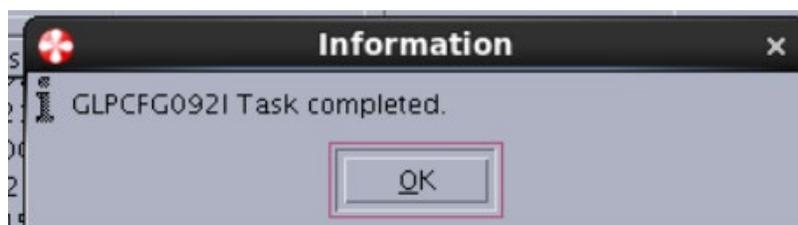
g. Click **Start administration server**. After a moment, the server starts.
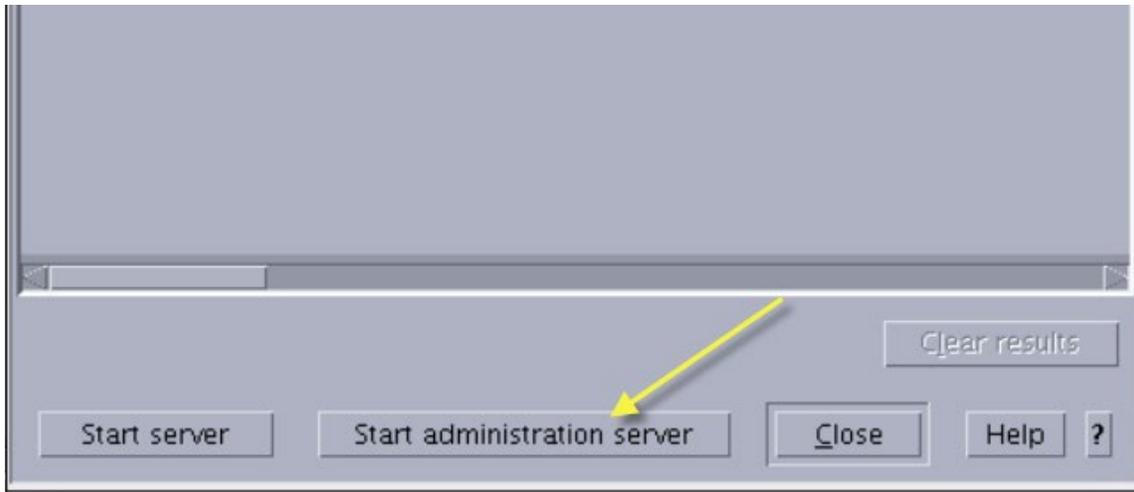
h. Click **OK** to confirm.

i. Confirm that the state of both servers is **Started**.

j. Click **Close** to exit the Manage server state window.
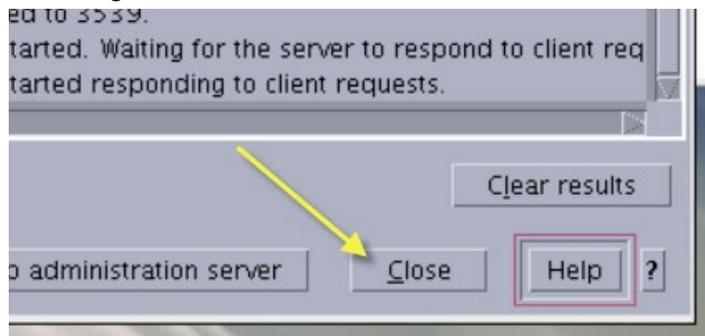
k. Click **Close** to exit the SDS Instance Administration tool.
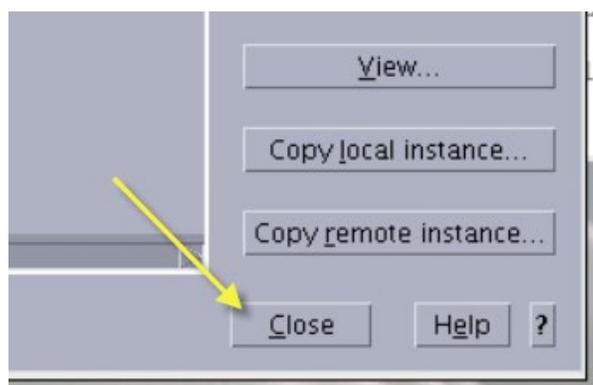
Verification

Run the following steps to verify that the LDAP server is working properly.

1. Run the following two commands on **host1.tivoli.edu** as the root user to query the LDAP server.

    ```
    cd /opt/ibm/ldap/V6.3.1/bin
    ```

    ```
    ./ldapsearch -v -D cn=root -w object00 -h host1.tivoli.edu -p 389 -b dc=ibm,dc=com uid=*
    1.1
    ```

    If the LDAP server is working correctly, the output of the preceding command should look like the following example.

    ```
    uid=tcruser1,ou=tipusers,cn=tipRealm,dc=ibm,dc=com
    uid=tcruser2,ou=tipusers,cn=tipRealm,dc=ibm,dc=com
    uid=tipuser1,ou=tipusers,cn=tipRealm,dc=ibm,dc=com
    uid=tipuser2,ou=tipusers,cn=tipRealm,dc=ibm,dc=com
    uid=root,cn=tipRealm,dc=ibm,dc=com
    cn=Tinisha Fowble,ou=tipusers,cn=tipRealm,dc=ibm,dc=com
    ...output omitted...
    30 matches
    ```

2. Verify that the **ncoadmin** user can log in to DASH.

   a. Go to the **host2.tivoli.edu** lab image, or to the image where DASH is running.

   b. Open a Firefox browser within the lab image.

   c. Go to the following URL. You might need to replace the fully qualified domain name (FQDN) in this example with the FQDN of the host where DASH is running.

   https://host2.tivoli.edu:16311/ibm/console/logon.jsp

   d. Log in with the user name **ncoadmin** and the password **object00**.

   e. Verify that the **ncoadmin** user can log in to DASH.

IBM Tivoli Network Manager not running properly

Symptoms

The **itnm_status** command returns an error message or shows that some processes are not running.

Cause

The image for this course was created with conservative allocation of RAM that sometimes causes ITNM to not start correctly while other processes are starting simultaneously.

Solution

1. Run the following command to force all of the ITNM processes to stop.

   ```
   pkill ncp
   ```

2. Wait 30 seconds.

3. Confirm that all ncp processes have stopped by running the following command.

   ```
   pgrep -fl ncp
   ```

4. Run the following command to restart ITNM.

   ```
   itnm_start
   ```

5. Wait 30 seconds and then run the following command. Repeat the command every 30 seconds until you see that all ncp processes are running.

   ```
   itnm_status
   ```

6. **Note**: If you seen an error message about Apache Zookeeper not starting because of the existence of a specific file, delete the file mentioned in the error message, and then repeat the preceding steps.

Student Notebook items

None reported.

Course presentation items by unit

None reported.

End of document