Documentation corrections for Tivoli Storage Productivity Center 4.2.2.2

Contents

Documentation corrections for Tivoli Storage Productivity Center V4.2.2.2

This section describes the documentation corrections for IBM® Tivoli® Storage Productivity Center V4.2.2.2.

IBM Tivoli Storage Productivity Center information center

IC84898 - Information Center topic "Configuring Tivoli Storage Productivity Center for DS8000 LDAP authentication"

In *Procedure for configuring Tivoli Storage Productivity Center*, the following text in step 2 is incorrect:

https://hostname:port/ibm/console/logon.jsp Where hostname defines the server that is running IBM Tivoli Integrated Portal and port defines the port number for Tivoli Integrated Portal. The default port is 16310.

In *Configuring DS8000 for LDAP authentication*, the following text in step 2 is incorrect:
To access the DS8000 GUI, expand **Element Manager**. Click **DS800**. In the content pane, select the DS8000® you want. In **Select Action**, select **Launch Default Element Manager**.
To see the corrected procedure, go to “Configuring Tivoli Storage Productivity Center for DS8000 LDAP authentication” on page 3.

IC84898 - Information Center topic "Configuring multiple Tivoli Storage Productivity Center servers with one DS8000 R4.2"

The following sentence in step 4 is incorrect:

Run the wsadmin command to export LTPA keys from `TPC_server1` into a file on `TPC_server2`.

The following directory path in step 6 is incorrect:
`c:\Program Files\IBM\Tivoli\TIP\bin>wsadmin -user tpcsuperuser`
To see the corrected procedure, go to “Configuring multiple Tivoli Storage Productivity Center servers with one DS8000 R4.2” on page 7.

IC84898 - Information Center topic "Setting up dual Tivoli Storage Productivity Center servers for high availability"

The text in step 7 is incorrect:

You need to synchronize the second authentication service (on `TPC_server2`) with the correct LTPA keys:

```
C:\Program Files\IBM\Tivoli\TIP\bin>wsadmin $AdminTask importESSLTPAKeys
-pathname LTPA_keys_file_name
-password LTPA_keys_password
```

To see the corrected procedure, go to “Setting up dual Tivoli Storage Productivity Center servers for high availability” on page 8.

82049 - Information Center topic "Enabling secure communication between Tivoli Storage Productivity Center and the LDAP repository"

Step 2 is missing information and should read as follows:

On the Tivoli Integrated Portal logon page, log on using the appropriate user ID and password. Your user name must have administrator permissions and must be the same user name that you used in the **Primary administrative user name** field on the Federated repositories page.

IBM Tivoli Storage Productivity Center and IBM Tivoli Storage Productivity Center for System z information centers

IC86478 - Information Center topic "The user account is locked after the DS Storage Manager password for the HMC is changed"

If the DS Storage Manager password for the Hardware Management Console (HMC) is changed, you must update the password in Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication. To see the procedures for updating the password in these applications, go to “The user account is locked after the DS Storage Manager password for the HMC is changed” on page 10

82049 - Information Center topic "Enabling secure communication between Tivoli Storage Productivity Center and the LDAP repository"

Step 2 is missing information and should read as follows:

On the Tivoli Integrated Portal logon page, log on using the appropriate user ID and password. Your user name must have administrator permissions and must be the same user name that you used in the **Primary administrative user name** field on the Federated repositories page.

Workaround for defect 80844

To validate your LDAP user name and upgrade to Tivoli Storage Productivity Center, complete the following steps:

1. Run the `ChangeWASAdminPass` script as described in Changing the WebSphere administrative user password for the Device server.
2. Run the `updateWASUserPassword script`:

   On the Windows operating system:

   ```
   updateWASUserPassword.bat TIP_installation_directory
   previous LDAP user_name previous LDAP password
   new LDAP username new LDAP password
   ```

   where *new LDAP username* and *new LDAP password* are the user name and password that you changed in Version 4.2.1.

   On the UNIX or Linux operating systems:

   ```
   updateWASUserPassword.sh TIP_installation_directory
   previous LDAP user_name previous LDAP password
   new LDAP username new LDAP password
   ```

   where *new LDAP username* and *new LDAP password* are the user name and password that you changed in Version 4.2.1.
3. Log in to Tivoli Integrated Portal and complete the following steps to change the password:
   a. Open an Internet Explorer or Mozilla Firefox web browser and type the following information in the address bar:

      `http://hostname:port`

   b. Log in to Tivoli Integrated Portal by using the appropriate user ID and password. Your user ID must have administrator permissions.
   c. In the Tivoli Integrated Portal navigation tree, click **Security** > **Secure administration, applications, and infrastructure**.
   d. On the Secure administration, applications, and infrastructure page, ensure that **Federated Repositories** is displayed in the **Available Realm Definitions** list and click **Configure**.

e. On the **Federated repositories** page, under **Server User Identity**, select **Server identity that is stored in the repository**, and enter the newly changed password.

f. Click **Save**.

4. Stop the services in this order:
   - Storage Resource agent
   - Replication server
   - Device server
   - Data server
   - Tivoli Integrated Portal

   For more information about stopping Tivoli Storage Productivity Center services, see Stopping the IBM Tivoli Storage Productivity Center services.
5. Start the Tivoli Storage Productivity Center services in this order:
   - Tivoli Integrated Portal
   - Data server
   - Device server
   - Replication server
   - Storage Resource agent
   - For more information about starting Tivoli Storage Productivity Center services, see Starting the IBM Tivoli Storage Productivity Center services.

Configuring Tivoli Storage Productivity Center for DS8000 LDAP authentication

You must configure IBM Tivoli Storage Productivity Center to use LDAP for single sign-on support for the DS8000 R4.2.

Overview

Configuring Tivoli Storage Productivity Center and DS8000 for single sign-on involves these general steps:

For Tivoli Storage Productivity Center

1. Extract the certificate. This certificate is used for securing communication between the Authentication Client on the HMC and the Authentication Service (server component) on Tivoli Storage Productivity Center.
2. Create a truststore which includes the certificate from step 1.
3. You need to know the URL for the Authentication Service.

For DS8000

1. Create a Storage Authentication Service (SAS) policy with information collected from Tivoli Storage Productivity Center and the LDAP server.
2. Test the Storage Authentication Service policy using a valid LDAP user mapped to a DS8000 user role in the policy.
3. Activate the Storage Authentication Service policy using a valid LDAP user mapped to the DS8000 administrative user role in the policy.

Procedure for configuring Tivoli Storage Productivity Center

This procedure assumes that Tivoli Storage Productivity Center is set up with the LDAP repository.

To configure Tivoli Storage Productivity Center, complete these steps:

1. You need to know the URL for the Authentication Service.

   Note: An example of the Authentication Service URL is:

   `https://`*`TIP_server_host`*`:16311/TokenService/services/Trust`

   Here is an example:

   ```
   https://tpcserver1.storage.mycompany.com:16311/TokenService/services/Trust
   ```

   The port for the Authentication Service (16311) is one plus the default Tivoli Integrated Portal port (16310). If you change the default port, for example, 17522, then the port number to use for the Authentication Service is one plus the Tivoli Integrated Portal port. In this example, the port number would be:

   ```
   https://tpcserver1.storage.mycompany.com:17523/TokenService/services/Trust
   ```
2. Start Internet Explorer and log in to IBM Tivoli Integrated Portal by entering the following text in the address field:

   https://hostname:port/ibm/console/logon.jsp

   where *hostname* defines the server that is running Tivoli Integrated Portal and port defines the port number for Tivoli Integrated Portal. The default port is 16316. Contact your Tivoli Storage Productivity Center administrator to verify the host name and port number. You can log in to Tivoli Integrated Portal with your LDAP user ID and password.
3. Create the truststore in Tivoli Integrated Portal. When logged into IBM Tivoli Integrated Portal, go to the Personal Certificates page for the Default keystore. Click **Security > SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal Certificates**. On this page, select the **default** certificate and click **Extract**. On the next page, enter the following information:

   Certificate file name

   Enter a file name for the extracted certificate. This file automatically gets created in `TIP_installation_directory/profiles/TIPProfile/etc/`.

   For Windows, the default directory is `C:\TIP_installation_directory\profiles\TIPProfile\etc\`.

   Accept and select the default data type. Click **OK**.
4. Create the truststore file and import the certificate into the truststore file using the **ikeyMan** tool.

   a. Launch the **ikeyMan** tool.

      For example on Windows:

      ```
      c:\Program Files\IBM\tivoli\tip\bin\ikeyman.bat
      ```

   b. Click **Key Database File > New**. On the New panel, enter the following information and click **OK**:

      Key database type

      Enter or leave the default JKS.

      File Name

      Enter a file name. For example, enter tpc_ess.jks.

Note: The default location is:

```
c:\Program Files\IBM\tivoli\tip\bin\
```

Location
Enter a location. For example, enter `c:\tpc\`. Click **OK**.

c. The next panel prompts you to specify a password for this truststore. Specify a password that you can remember. Click **OK**.

d. On the next panel, click **Add**. This action opens the Add CA certificate from a file panel. Click **Browse** and select the certificate file you created in step 3 on page 4. Click **Done**, then click **OK**.

   Note: Look for the certificate file, change the Files of Type to **All files**. Click **Open**.

e. You see a prompt to specify a label. Provide any label. An example of a label is: ESS_Cert. Click **OK**.

f. The ESS_Cert is now one of the certificates listed.

g. Exit the **`ikeyman`** tool and locate the truststore file (for this example, `tpc_ess.jks`). You need this truststore file and the password for configuring the LDAP-based policy on DS8000.

h. You are now finished with Tivoli Integrated Portal and the truststore setup.

5. Find the user ID and password that is used in LDAP to use for the DS8000 Storage Authentication Service policy configuration page.

   This user ID is used for authenticating with the Authentication Service. It can be any user ID in LDAP, or a user ID that is also used by Tivoli Storage Productivity Center. This user ID is used as the "Application Client User ID" for a Storage Authentication Service policy on the DS8000.

6. Find the name of a group in LDAP with which you can log in to Tivoli Storage Productivity Center and the DS8000. You would use this LDAP group on the DS8000 also, for mapping to DS8000 roles.

   You can go to the Tivoli Storage Productivity Center **Role-to-Group Mapping** node to find out which LDAP group is mapped to the role in Tivoli Storage Productivity Center.

   To find the LDAP group name, open the Tivoli Storage Productivity Center GUI and click **Tivoli Storage Productivity Center > Configuration > Role-to-Group Mapping**.

   The information gathered in steps 1, 3, 4, 5, and 6 is used on the DS8000 Storage Authentication Service policy creation page.

7. Configure DS8000 R 4.2.

Configuring DS8000 for LDAP authentication

Follow these steps:

1. Add the IP address of the DS8000 Hardware Management Console to the Internet Explorer list of trusted sites using the following steps:
   a. Open the Internet Explorer by clicking the Internet Explorer icon located on the Quick Launch toolbar.
   b. From the Internet Explorer toolbar, click **Tools** > **Internet options**.
   c. Click the **Security** tab, click the **Trusted sites** icon and then click **Sites**.
   d. In the **Add this web site to the zone** field, type the IP address of the DS8000 Hardware Management Console (HMC). Click **Add** and the IP address is added to the **Websites** field.

   e. Click **Close** and then click **OK** to exit the Internet Options window, and then close the Internet Explorer.
2. To access the DS8000 GUI, complete the following steps:
   a. In the Tivoli Storage Productivity Center GUI, expand the **Element Manager** tree.
   b. Click DS8000.
   c. Complete one of the following steps:
      - In the content pane, select a DS8000 system.
      - Click **DS8000 Element Manager > Select Action > Add Element Manager**.
   d. In **Select Action**, select **Launch Default Element Manager**. This action opens the DS8000 Storage Manager GUI so that you can administer DS8000. Enter the user name and password and click **OK**.
3. On the DS8000 Storage Manager Welcome page, click **Real-time manager > Monitor System > User Administration**.
4. On the User and Authentication Policy Administration Summary page, select a Complex Name. Under the Select action menu, select **Create Storage Authentication Service Policy**.
5. The Authentication Service Configuration page is displayed. Enter the following information:
   - Policy Name
   - Authentication Service URL (primary)
   - Authentication Service Client User ID
   - Authentication Service Client Password
   - Confirm Authentication Service Client Password

   Click **Next**.

   Note: An example of the authentication URL is:

   ```
   https://TIP_server_host:16311/TokenService/services/Trust
   ```

   Here is an example:

   ```
   https://tpcserver1.storage.mycompany.com:16311/TokenService/services/Trust
   ```

   The port for the Authentication Service (16311) is one plus the default Tivoli Integrated Portal port (16310). If you change the default port, for example, 17522, then the port number to use for the Authentication Service is one plus the Tivoli Integrated Portal port. In this example, the port number would be:

   ```
   https://tpcserver1.storage.mycompany.com:17523/TokenService/services/Trust
   ```
6. The Truststore file Information page is displayed. Enter the following information:
   - Truststore File Location
   - Truststore File Password
   - Confirm Truststore File Password

   Click **Next**.
7. The Map External Users and User Groups to DS8000 User Roles page is displayed. Enter the following information:
   - External Entity Name
   - External Entity Type
   - DS8000 User Role

Click **Add**. The entry is entered in the table at the bottom of this page. Select the entry you created and click **Next**.

8. The Verification page is displayed. Verify the information and click **Next**.
9. The Summary page is displayed. Click **Activate the Policy** if you want to activate the policy immediately. If you want to test the policy before activating it, do not select **Activate the Policy** and click **Finish** to create the policy. This scenario assumes that you want to test the policy before activating it. You see a message dialog indicating whether the policy was successfully created or not. If the policy was successfully created, close the message dialog.
10. The Manage Authorization Policy page is displayed. Select a policy. Under the Select action menu, click **Test Authentication Policy**.
11. The Test Storage Authentication Service Policy page is displayed. Enter the following information:
    - External User Name
    - External User Password

    Provide an LDAP user ID and password for External User Name and External User Password. The user ID must already be mapped to a valid DS8000 user role in the Storage Authentication Service policy. This user ID does not have to be in the Administrator group. Click **OK**.
12. The Manage Authentication Policy page is displayed. Select the policy you want. Under the Select action menu, click **Activate Authentication Policy**.
13. The Activate Storage Authentication Service Policy page is displayed. Enter the following information:
    - External User Name
    - External User Password

    Provide an LDAP user ID and password for External User Name and External User Password. The user ID must already be mapped to a valid DS8000 user role in the Storage Authentication Service policy. This user ID must be in the Administrator group. Click **OK**. The policy is now activated. Close the page.

Configuring multiple Tivoli Storage Productivity Center servers with one DS8000 R4.2

You can configure multiple Tivoli Storage Productivity Center servers to use LDAP for single sign-on support for the DS8000 R4.2.

Procedure for configuring multiple Tivoli Storage Productivity Center servers

Follow these steps:

1. Configure one server as described in “Configuring Tivoli Storage Productivity Center for DS8000 LDAP authentication” on page 3. This server is called `TPC_server1`.
2. Install a second Tivoli Storage Productivity Center server with the same LDAP information as the first server. The second server is called `TPC_server2`.
3. Open a command prompt window. Go to the following directory:

   TIP_installation_directory/bin
4. Run the **wsadmin** command to export LTPA keys from `TPC_server1` into a file on `TPC_server2`.

```
wsadmin -user TIP_admin_ID -password TIP_admin_password -lang jython
-port TIP_SOAP_port -host TPC_server1_hostname_or_IP_address
-f "TPC_install_dir_on_TPC_server2/tip/scripts/exportLTPAKeys.py"
"LTPA_keys_file_name" LTPA_keys_password
```

An example is:

```
c:\Program Files\IBM\Tivoli\TIP\bin>wsadmin -user tpcsuperuser
-password tpcsuperuser -lang jython
-port 16313 -host 9.56.98.41
-f "c:/program files/ibm/tpc/tip/scripts/exportLTPAKeys.py"
"c:/share/ltpaKeys_serv1" ltpa123
```

This creates a file named `ltpaKeys_serv1` containing the LTPA keys of `TPC_server1`. The LTPA keys are imported into `TPC_server2`.

Note: Use forward slashes.

5. In the same command window, run the following command to import the LTPA keys into IBM Tivoli Integrated Portal and then into the Device server.

   ```
   wsadmin -user TIP_admin_ID -password TIP_admin_password -lang jython
   -f "TPC_install_dir_on_TPC_server2/tip/scripts/importLTPAKeys.py"
   "LTPA_keys_file_name" LTPA_keys_password
   ```

   An example is:

   ```
   c:\Program Files\IBM\Tivoli\TIP\bin>wsadmin -user tpcsuperuser
   -password tpcsuperuser -lang jython
   -f "c:/program files/ibm/tpc/tip/scripts/importLTPAKeys.py"
   "c:/share/ltpaKeys_serv1" ltpa123
   ```

   Note: Use forward slashes.

6. Change to the Device server WebSphere® bin folder and run the same command there.

   ```
   c:\Program Files\IBM\TPC\device\apps\was\bin>wsadmin -user tpcsuperuser
   -password tpcsuperuser -lang jython
   -f "c:/program files/ibm/tpc/tip/scripts/importLTPAKeys.py"
   "c:/share/ltpaKeys_serv1" ltpa123
   ```

   Note: Use forward slashes.

7. The LTPA keys in `TPC_server1` and `TPC_server2` are now synchronized. You can complete a successful single sign-on launch from `TPC_server2` to the DS8000 R4.2. The DS8000 uses the same policy that was set up when you set up `TPC_server1`.

   The same steps can be used to start the same DS8000 from any number of IBM Tivoli Storage Productivity Center servers.

   Note: This is not a high-availability setup because the policy in DS8000 is still pointing to only one Embedded Security Service, which is that of `TPC_server1`.

Setting up dual Tivoli Storage Productivity Center servers for high availability

This section describes how to set up dual Tivoli Storage Productivity Center servers for high availability.

Procedure

Follow these steps:

1. Configure one Tivoli Storage Productivity Center server as described in "Configuring Tivoli Storage Productivity Center for DS8000 LDAP authentication" on page 3. In this example, this server is called `TPC_server1`.
2. Install a second Tivoli Storage Productivity Center server with the same LDAP information as the first server. In this example, this server is called `TPC_server2`.
3. Open a command prompt window. Go to the following directory:

   ```
   TIP_install_directory/bin
   ```
4. Run the following WebSphere command to export the LTPA keys from `TPC_server1` into a file on `TPC_server2`.

   ```
   wsadmin -user TIP_admin_ID -password TIP_admin_password
   -lang jython
   -port TIP_SOAP_port
   -host TPC_server1_hostname_or_IP_address
   -f "TPC_install_directory_on_TPC_server2/TIP/scripts/exportLTPAKeys.py"
   "LTPA_keys_file_name" LTPA_keys_password
   ```

   Here is an example:

   ```
   C:\Program Files\IBM\Tivoli\TIP\bin> wsadmin -user tpcsuperuser
   -password tpcsuperuserpassword
   -lang jython
   -port 16313
   -host 9.54.91.40
   -f "c:/Program Files/IBM/TPC/TIP/scripts/exportLTPAKeys.py"
   "c:/share/ltpakeys_serv1" ltpa123
   ```

   This creates a file named ltpakeys_serv1 which contains the LTPA keys of `TPC_server1`. The LTPA keys are imported into `TPC_server2`.

   Note: Use forward slashes with the **-f** parameter.
5. In the same command window, run the following WebSphere command to import the LTPA keys into Tivoli Integrated Portal and then into the Device server.

   ```
   wsadmin -user TIP_admin_ID -password TIP_admin_password
   -lang jython
   -f "TPC_install_directory_on_TPC_server2/tip/scripts/importTPAKeys.py"
   "LTPA_keys_file_name" LTPA_keys_password
   ```

   Here is an example:

   ```
   C:\Program Files\IBM\Tivoli\TIP\bin>wsadmin -user tpcsuperuser
   -password tpcsuperuserpassword
   -lang jython
   -f "c:/program files/ibm/tpc/tip/scripts/importLTPAKeys.py"
   "c:/share/ltpakeys_serv1" ltpa123
   ```

   Note: Use forward slashes with the **-f** parameter.
6. Change to the Device server WebSphere bin folder and run the same command there.

   ```
   c:\Program Files\IBM\TPC\device\apps\was\bin>wsadmin -user tpcsuperuser
   -password tpcsuperuserpassword
   -lang jython
   -f "c:/program files/ibm/tpc/tip/scripts/importLTPAKeys.py"
   "c:/share/ltpakeys_serv1" ltpa123
   ```

   Note: Use forward slashes with the **-f** parameter.
7. You need to synchronize the second authentication service (on `TPC_server2`) with the correct LTPA keys:

```
C:\Program Files\IBM\Tivoli\TIP\bin>wsadmin -user tpcsuperuser
-password tpcsuperuserpassword
-lang jython
-c "AdminTask.importESSLTPAKeys
('[-pathname c:/share/ltpakeys_serv1 -password ltpa123]')"
```

Restart the second Tivoli Integrated Portal server (on `TPC_server2`).

8. The LTPA keys in `TPC_server1` and `TPC_server2` are now synchronized.
9. If you are using the Java client. add the SSL certificates for all servers to the truststore file. Follow these steps:
   a. Log in to Tivoli Integrated Portal on `TPC_server1` and extract the certificate. In this example, the certificate is named `cert1.cer`.
   b. Log in to Tivoli Integrated Portal on `TPC_server2` and extract the certificate. In this example, the certificate is named `cert2.cer`.
   c. On `TPC_server1`, take the `cert1.cer` and `cert2.cer` certificates at one location and use the Java keytool command to create a truststore.
   d. Go to `c:\Program Files\IBM\Tivoli\tip\java\bin` and add these two certificates:

      ```
      keytool -import -alias TPCServer1
        -file c:\cert1.cer
        -keystore c:\ess.truststore.jks
        -storetype jks
        -storepass password
      ```

      ```
      keytool -import -alias TPCServer2
        -file c:\cert2.cer
        -keystore c:\ess.truststore.jks
        -storetype jks
        -storepass password
      ```

   e. Verify that the two certificates exist in the keystore by running this command:

      ```
      keytool -list
      -keystore c:\ess.trustore.jks
      -storepass password
      ```

      This command must list the two aliases (`TPCServer1` and `TPCServer2`) in the keystore.
   f. Copy the `ess.trustore.jks` keystore to `c:\Program Files\IBM\TPC\device\conf` on `TPC_server1` and `TPC_server2`.

The user account is locked after the DS Storage Manager password for the HMC is changed

If the DS Storage Manager password for the Hardware Management Console (HMC) is changed, you must update the password in Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication.

If you do not update this password in Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication, the DS Storage Manager user account for the HMC might be locked after these applications attempt to connect to the storage system with the incorrect password.

Update the password in the Tivoli Storage Productivity Center and Tivoli Storage Productivity Center for Replication GUIs as shown in the following table.

Interface	Action
Tivoli Storage Productivity Center for Replication	Update the password on the storage connection details page for the storage system as shown in the following steps: 1. In the GUI navigation tree, click **Storage Systems**. 2. On the Storage Systems page, click the **Connections** tab. 3. On the **Connections** tab, select the storage connection that you want to update. 4. On the Connection Details page, enter the password in the **Password** field, and then click **Apply**.
Tivoli Storage Productivity Center	Update the password on the storage connection details page for the storage system as shown in the following steps: 1. In the stand-alone GUI navigation tree, expand **Administrative Services** > **Data Sources**. 2. Click **Storage Subystems**. 3. Click the **Magnifying Glass** icon next to the storage system that you want to update. 4. On the storage system details page, enter the password in the **Password** field, and then click **File** > **Save**.
Tivoli Storage Productivity Center	This task is required only if both of the following conditions are true: • You are using the launch-in-context feature to start the element manager, DS Storage Manager, from Tivoli Storage Productivity Center. • You are not using single sign-on with LDAP authentication to connect to the element manager. LDAP authentication is required for Tivoli Storage Productivity Center to connect to 4.2 and later. Update the password for the element manager as shown in the following steps. If you have multiple users who are accessing the element manager and their password was changed, you must update the password for each user. 1. In the stand-alone GUI navigation tree, expand **IBM Tivoli Storage Productivity Center**. 2. Click **Configuration Utility**. 3. In the Configuration Utility, click the **Element Manager** tab. 4. In the **DS8000 Element Manager** section, select the storage system that you want to update. 5. In the **Select Action** list, select **Modify Element Manager**. 6. In the **Modify Element Manager** window, enter the password in the **Password** field, and then click **Save**.