IBM Security

Intelligence. Integration. Expertise.

IBM® SECURITY PRIVILEGED IDENTITY MANAGER

Migrating data from version 1.x to version 2.1.0

Authors

Tay Zhun Chong
Li LinLin
Haan-Ming Lim

Version 1.0

April 2017

Contents

IBM Security

Intelligence. Integration. Expertise.

Migrating data from IBM Security Privileged Identity Manager version 1.x to version 2.1.0

(1) Prepare your ISPIM 1.x environment for migration

Use the following roadmap to prepare your IBM Security Privileged Identity Manager version 1.x environment for migration:

	Procedure	Reference
1.	Install the data migration tool to export Privileged Credential Management (PCM) data. • Stop the ITIM application when you are installing the data migration tool. • Ensure that the data migration tool installation is completed and the ITIM application is restarted before you resume normal ISPIM operations.	See Adding an operation for data exporting

(2) Exporting data from ISPIM 1.x environment

You can choose to perform the exporting of data way ahead of the planned migration and run through the migration steps that are involved on a **ISPIM 2.1.0 test environment**. This task allows you get yourself familiarize before the actual migration.

Before executing the actual migration, ensure that you have the latest set of data exported by running through the data export again.

2.1 Exporting Privileged Credential Management Data

To export Privileged Credential Management (PCM) data from ISPIM version 1.x, you must configure a life cycle rule. See Configuring a life cycle rule for the operation for instructions on configuring a life cycle rule and to view the list of data objects that are exported.

If there are changes made to the ISPIM data objects in the Administrative Console (itim/console), ensure that you export the latest data by running the life cycle rule again before the actual migration to version 2.1.0 begins.

Note: The following data are not exported:

- Accounts that are not in the credential vault are not exported.
- Disabled policies are not exported. A warning message is shown in **View Requests**, if there are disabled policies found.

- Assignment attributes are not exported. It is not supported in ISPIM 2.1.0.
- Shared Access Policy with members as "All users in the organization" are not exported. However, you can create that policy manually in Service Center.

2.2 Exporting Single Sign-on Data

2.2.1 Exporting IBM Security Privileged Identity Manager policies in IMS Server

Note down the ISPIM policies that will be retained after migrating to the ISPIM 2.1.0 environment. You will need to manually set these policies on the newly set up ISPIM 2.1.0 environment for migration.

1. On the IMS Server environment, log in to AccessAdmin as a system administrator. For example, pim manager or itim manager.
2. Under System Menu, click **System policies > IBM Security Privileged Identity Manager Configuration Policies**.
3. Note down the following policies, if it is modified:
   - **Enable session recording?**
   - **Session recording image capture option**
   - **Session recording keyboard capture option**
   - **Action to take when the client computer cannot connect to the server**
   - **Maximum number of failed connection attempts to the server**
   - **Time interval between connection attempts to the server**
   - **Allow empty justification on credential check-out**

Important: You do **not** need to note down the following policies because the following policies are not needed for migration:

- **IBM Security Identity Manager URL**
- **IBM Security Identity Manager Authentication Service ID**
- **Privileged Session Recorder Server URL**

2.2.2 Exporting Access Profiles from IMS Server

Important: Ensure that you export only custom AccessProfiles. Custom AccessProfiles are AccessProfiles that are created by you or modified out-of-the-box (OOTB) profiles. It is suggested that you use the IBM Security Privileged Identity Manager OOTB profiles in version 2.1.0.

To export the **custom** Access Profiles, proceed with the steps as follows,

1. In a Windows system, install **ISAM ESSO Access Agent** and **Access Studio**. For instructions on installation, see AccessAgent and AccessStudio installation roadmap.
2. Connect the ISAM ESSO AccessAgent to the IMS Server.
3. Log in to ISAM ESSO AccessAgent as a system administrator. For example, pim manager or itim manager.
4. Launch AccessStudio.
5. Click **File** > **Import data from IMS**.
6. Select the AccessProfiles that you want to migrate to the new server in the left panel.
   Note: To select more than one AccessProfile, hold the Ctrl key.
7. Right-click the selected AccessProfiles and select **Save to a file**. For example, `PIM1x.eas`
   Note: Widgets that are associated with an AccessProfile are uploaded automatically.

2.3 Exporting Privileged Session Recorder Data

It is not required to export the Privileged Session Recorder (PSR) data because the ISPIM 2.1.0 environment will be configured, during migration, to connect to the existing ISPIM 1.x PSR database. All recordings will be retained and accessible from the new ISPIM 2.1.0 environment.

For more information on the preparation required on the ISPIM 2.1.0 environment, see Section 3.

(3) Prepare your ISPIM 2.1.0 environment for migration

Use the following roadmap to prepare your IBM Security Privileged Identity Manager version 2.1.0 environment for migration:

	Procedure	Reference
1.	Prepare the data tier for ISPIM 2.1.0 environment. **Important - Privileged Session Recorder (PSR) database:** • The current ISPIM 1.x PSR database will eventually be used by the new ISPIM 2.1.0 environment later in the migration process. This is part of the migration steps that will be covered later in the guide. See Section 4.1 for more information. ○ For now, to complete the set up for ISPIM 2.1.0, proceed to create a database for PSR in the new data tier so that the ISPIM configuration can be completed. • When you are setting up the Privileged Session Recorder database, ensure that the **database administrator ID/username** is the same as the one defined in the ISPIM 1.x environment. This check ensures that the schema on both the Privileged Session Recorder databases (1.x and 2.1.0) are the same. **Suggestion**: If you want to set up the data tier for ISPIM 2.1.0 to share the same database server as ISPIM 1.x, complete the following steps: 1. Create a new database instance on the ISPIM 1.x database server. 2. Create the ISPIM 2.1.0 Identity, Single Sign-On, and PSR databases on the newly created instance.	See Prerequisite Software
2.	Install IBM Security Privileged Identity Manager version 2.1.0. Restart the appliance after the setup is completed.	See Setting up the virtual appliance
3.	Proceed to complete the ISPIM configuration when the appliance has successfully restarted.	See Setting up a stand-alone or primary node for IBM Security Privileged Identity Manager

	Important: When you are configuring the Session Recorder database, the database administrator ID used will be the same as the one defined in the ISPIM 1.x environment. This step ensures that the schema on both Session Recorder database is the same.	
4.	Install Fix Pack 3 on the ISPIM 2.1.0 environment: a. Access the fix pack management page by logging in to *https://<servername>:9443/fixpacks*. b. Browse to `2.1.0-ISS-ISPIM-VA-FP0003.fixpack` and apply the fix pack. c. Restart the virtual appliance.	See IBM Security Privileged Identity Manager fix pack 2.1.0-ISS-ISPIM-VA-FP0003
5.	Prepare the environment to import custom AccessProfiles and to verify the status of the migration. a. In a Windows system, install **Privileged Access Agent 2.1.0** and AccessStudio. b. Connect AccessAgent to the ISPIM version 2.1.0 with Fix Pack 3 appliance.	See AccessAgent and AccessStudio installation roadmap

(4) Migrating data from ISPIM 1.x to ISPIM 2.1.0 FP3

Note: During the migration process, ensure that all end users of ISPIM do not have access until the migration to ISPIM 2.1.0 Fix Pack 3 environment is completed.

Before you begin:

- All credentials must be checked in. Verify credentials are checked in from the Administrative Console.
    - Login to administrative console (itim/console).
    - Click **Manage Shared Access > Manage Credential Vault.**
    - Ensure that no credentials are checked out by reviewing the list of credentials shown here.
- Ensure that you have the latest set of exported data from the data migration tool.
- *Only applicable if you are migrating Privileged Session Recorder (PSR)*:
    - Ensure that there are no active recordings, and all recordings are completed. Verify this in the Privileged Session Recorder console.
    - **Back up** the Privileged Session Recorder version 1.x database.

4.1 Migrating Privileged Session Recorder data

Note: If you are not migrating Privileged Session Recorder data, proceed to section **4.2 Migrating Single Sign-On data**.

1. In the virtual appliance dashboard, reconfigure the ISPIM 2.1.0 PSR database settings to the ISPIM 1.x PSR database server.
    a. On the ISPIM 2.1.0 Fix Pack 3 virtual appliance, login to Local Management Interface (LMI) via *https://<servername>:9443*
    b. Click **Configure > Database Server Configuration > Session Recording Data Store > Reconfigure**
    c. For the ISPIM 2.1.0 PSR database configuration, update the hostname and port number to the ISPIM 1.x PSR database, where the old session recorder database resides.
    d. Update the Database Administrator password.
    e. Save the configuration and wait for the reconfiguration to complete.
2. By using the virtual appliance command line interface, reset the recorder index. Open the virtual appliance command line interface (CLI).
   Type the following commands, pressing Enter after each line:
    a. `ispim`
    b. `recorder`
    c. `reset_index`.

4.2 Migrating Single Sign-on data

4.2.1 Migrating IBM Security Privileged Identity Manager policies in IMS Server

Before you begin: Ensure that you have the ISPIM policies from Section 2.2.1.

1. Log in to AccessAdmin as a system administrator. For example, pim manager.

2. Under **System Menu**, click **System policies** > **IBM Security Privileged Identity Manager Configuration Policies**.
3. Set the respective ISPIM policies with the values from Section 2.2.1.

4.2.2 Migrating Access Profiles

Important: Ensure that you migrate only custom AccessProfiles. Custom AccessProfiles are AccessProfiles that are created by you or modified OOTB profiles. It is suggested that you use the IBM Security Privileged Identity Manager OOTB profiles in version 2.1.0.

Before you begin: Ensure that you have a Windows system with Privileged Access Agent 2.1.0 and AccessStudio installed, and connected to a ISPIM 2.1.0 server.

1. Log in to the Privileged Access Agent as a system administrator. For example, pim manager or itim manager.
2. Launch AccessStudio.
3. Click **Open file** and browse to the `PIM1x.eas` file (this file is generated from Section 2.2.2 by exporting the Access Profiles).
   Note: Click **No** if there is a prompt to save changes.
4. Select the AccessProfiles and widgets that you want to upload in the left panel.
5. Right-click the selected AccessProfiles and select **Upload to IMS**.
   Note: Once the upload is successful, AccessProfiles or widgets with the same name are overwritten in IMS Server.

4.3 Migrating Privileged Credential Management (PCM) data

Important: Before you begin, ensure you have the latest list of exported data that was provided by the data migration tool from Section 2.1.

4.3.1 Importing users with the Identity Feed service

1. Upload the user feed file. For example, `Users.csv`.
   a. In the Virtual Appliance dashboard, click **Configure Privileged Identity Manager**.
   b. In **Manage Server Settings**, click **Upload Feed File**.
   c. Click **New**.
   d. Browse to the feed file and click **Save Configuration**.
2. Create the Identity Feed service.
   a. In the Administrative Console, click **Manage Services**.
   b. Click **Create**.
   c. In **Select Type**, select **Comma Separated File (CSV) identity feed** and click **Next**.
   d. Fill in the details in the **Service Information** tab. For example, `/userdata/identity/feeds/<file name>.`
   Note: By default, users are created under the default organization. If you want to create users under a different organization unit, use **Placement rule**.
   e. Click **Finish**.
3. Create users.
   a. In the Administrative Console, click **Manage Services**.
   b. Click **Refresh**.
   c. Click the arrow on the service that was created in the previous step.
   d. Click **Reconcile Now**.
4. Manually reconfigure the memberships.
   a. In the Administrative Console, click **Manage Groups**.
   b. Using `Membership.csv`, manually assign the users to the respective groups.

4.3.2 Importing other objects with the bulk upload tool

Before you begin: Ensure that you have manually migrated the organization structure.

Note: The values for ORG_PDN must be modified to the actual pseudo DN of the target system. See ORG_PDN attribute description.

1. In the Administrative Console, upload the modified CSV file. See Uploading a CSV file with the administrative console.
2. The files must be uploaded in the following order,
   a. `Resources.CSV`
   b. `IdentityProviders.CSV`
   c. `Credentials.CSV`
   d. `CredentialPools.CSV`
   e. `Access.CSV`
3. You can check the status in **View Requests** > **View All Requests** after one file is uploaded. To see the details of the request, click **Shared Access Bulk Load** > **Result details**.

Notes:

Organization

- Values of ORG_PDN in the CSV file must be modified manually.

Identity Provider

- Previously known as "Service", Bulk upload might not work properly if the adapter on the original server (ISPIM 1.x) has a different version from that on the target server (ISPIM 2.1.0). In that case, you need to edit the output file.
- Key based authentication is not supported in ISPIM 2.1.0. A warning is shown in **View Requests** if a service is configured in that way (ISPIM 1.x).
- For Custom IDP type, the adapter profile needs to be imported to ISPIM before bulk upload.

Access

- Previously known as “Role” and “Shared Access Policy”.

4.3.3 Importing other objects manually

The following objects must be created manually in ISPIM 2.1.0 if there are any customization for these in the older ISPIM 1.x environment.

In the Administrative Console, create the following objects manually:

1. Custom Group
2. Membership
3. View
4. Workflow
5. Email Template
6. Lifecycle Rule
7. Design
8. Organization structure

(5) Verifying the migrated data

Note: To verify scenarios that involves Privileged Access Agent, you can use the Windows workstation that was mentioned in Section 3 for the verification steps.

5.1 Verifying the Single Sign-on data and AccessProfiles

1. Login to the single sign-on administrative console.
2. Verify that the IBM Security Privileged Identity Manager policies is properly assigned.
3. Login to a Privileged Access Agent with a migrated user.
4. Verify that the custom profiles are working as intended.

5.2 Verifying the Privileged Session Recorder data

1. Login to a Privileged Access Agent with a migrated user.
2. Record a session with Privileged Access Agent by performing an automated check-in or check-out of credentials.
3. In the Administrative Console, use an existing user that is in the **Session Recorder Auditor** group or add a user to the **Session Recorder Auditor** group. For example, `annie`. See Adding members to groups.
4. Log in to the **Privileged Session Recorder console** with the user that you added. For example, `annie`.
    a. Verify that you can see the list of migrated session recording data.
    b. Verify that the recording playback is correct by playing the session recording you made in step 2.

Note: The session recording data might take a while to load for the initial search.

5.3 Verifying the Privileged Credential Management data

1. Log in to the Service Centre (`ispim/ui`) as an administrator. For example, **admin**.
   Note: This user interface is introduced in ISPIM 2.1.0 for administrator to onboard and manage the shared access credentials. For a list of new consoles, see Shared access consoles.
2. Verify the imported data objects by navigating to the following sections:
    a. **Manage Credentials** – For verifying the credentials imported
    b. **Manage Resources** – For verifying the resources imported.
    c. **Manage Identity Providers** – For verifying the services imported.
    d. **Manage Access** – For verifying the shared access policies imported.
3. Log in to Administrative Console (`itim/console`) as the same administrator user.
4. Verify that the credential pools are imported successfully.

The migration to ISPIM 2.1.0 FP3 environment is successful once all the data is verified. Proceed to reinstall the ISAM ESSO Access Agent on all the end user’s workstations with Privileged Access Agent 2.1.0.

Post-migration tasks

Reinstall AccessAgent on all the client workstations to point to the new ISPIM 2.1.0 FP3 environment.

1. Uninstall the ISAM ESSO AccessAgent on the client workstation.

2. Install the new Privileged Access Agent 2.1.0 on the client workstations and configure it to the new ISPIM 2.1.0 FP3 environment.

Note: If you encounter any issues and the migration must be stopped, use the following procedure to perform a recovery:

1. Restore the Privileged Session Recorder database backup to the ISPIM 1.x database server.
2. Restart the ISPIM 1.x environment to restart all the ISPIM services.