Configuring Operating System Profiles
Overview

By default, the Integration Service process runs all workflows using the permissions of the operating system user that starts Informatica Services. The Integration Service reads and writes files to locations specified by service process variables.

When you configure the Integration Service to use operating system profiles, the Integration Service process runs workflows with the permission of the operating system user you define in the operating system profile. The operating system profile contains the operating system user name, service process variables, and environment variables. The operating system user must have access to the directories you configure in the profile and the directories that the Integration Service accesses at run time. You can use operating system profiles for an Integration Service that runs on UNIX.

Using Operating System Profiles

To use an operating system profile, assign the profile to a repository folder or assign the profile to a workflow when you start a workflow. You must have permission on the operating system profile to assign it to a folder or workflow. Also, the user that runs a workflow must have permissions to use the operating system profile that is assigned to the workflow or folder. For example, you assign operating system profile Sales to workflow A. The user that runs workflow A must also have permissions to use operating system profile Sales. The Integration Service stores the output files for workflow A in locations specified in the service process variables of the operating system profile.

To manage permissions for operating system profiles, go to the Security page of the Administration Console. You can create, edit, delete, and assign permissions to operating system profiles in the Configure Operating System Profiles dialog box.

Operating System Profile Components

Configure the following components in an operating system profile:

- **Operating system user name.** Configure the operating system user that the Integration Service uses to run workflows.
- **Service process variables.** Configure service process variables in the operating system profile to specify different output file locations based on the profile assigned to the workflow.
- **Environment variables.** Configure environment variables that the Integration Services uses at run time.
- **Permissions.** Configure permissions for users to use operating system profiles.

Configuring Operating System Profiles

To use operating system profiles to run workflows, complete the following steps:

1. Enable operating system profiles in the Integration Service properties.
2. Set umask to 000 on every node configured to run the Integration Service.
3. Configure pmimpprocess on every node configured to run the Integration Service. pmimpprocess is a tool that the DTM process, command tasks, and parameter files use to switch between operating system users.
4. Create the operating system profiles.
5. Configure operating system profile properties.
6. Assign permissions on operating system profiles to users or groups.

You can assign operating system profiles to repository folders or to a workflow.
Step 1. Enable Operating System Profiles
1. In the Administration Console, select the Integration Service in the Navigator.
2. Click Edit in the Advanced Properties section of the Properties tab.
3. Enable the Uses Operating System Profiles option.
   You can select this option if the Integration Service runs on UNIX.

Step 2. Set umask
Set umask to 000 on every node configured to run the Integration Service. To apply changes, restart Informatica Services.

Step 3. Configure pmimpprocess
Configure pmimpprocess on every node configured to run the Integration Service. pmimpprocess is a tool that the DTM process, Command tasks, and parameter files use to switch between operating system users.

To configure pmimpprocess:
1. At the command prompt, switch to the following directory:
   `<PowerCenter installation directory>/server/bin`
2. Enter the following information at the command line to log in as the administrator user:
   `su <administrator user name>`
   For example, if the administrator user name is root enter the following command:
   `su root`
3. Enter the following commands to set the owner and group to the administrator user:
   `chown <administrator user name> pmimpprocess`
   `chgrp <administrator user name> pmimpprocess`
4. Enter the following commands to set the setuid bit:
   `chmod +g pmimpprocess`
   `chmod +s pmimpprocess`

Step 4. Create Operating System Profiles
To use operating system profiles for an Integration Service, create operating system profiles. You cannot edit the name or the system user name after you create an operating system profile. If you do not want to use the operating system user specified in the operating system profile, delete the operating system profile. After you delete an operating system profile, assign a new operating system profile to repository folders that the operating system profile was assigned to.

To create an operating system profile:
1. Click the Configure Operating System Profiles icon on the Security page of the Administration Console.
   The Configure Operating System Profiles dialog box appears.
2. Click Create Profile.
3. Enter the User Name, System User Name, and $PMRootDir.
4. Click OK.
**Step 5. Configure Properties of Operating System Profiles**

After you create an operating system profile, configure the operating system profile properties. To edit the properties of an operating system profile, select the profile in the Configure Operating System Profile dialog box and then click Edit.

The following table describes the properties of an operating system profile:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Read-only name of the operating system profile. The operating system profile name can be up to 80 characters. It cannot include spaces or the following special characters: `:/?*&lt;&gt;</td>
</tr>
<tr>
<td>System User Name</td>
<td>Read-only name of an operating system user that exists on the machines where the Integration Service runs. The Integration Service runs workflows using the system access of the system user defined for the operating system profile.</td>
</tr>
<tr>
<td>$PMRootDir</td>
<td>Read-only name of an operating system user that exists on the machines where the Integration Service runs. The Integration Service runs workflows using the system access of the system user defined for the operating system profile.</td>
</tr>
<tr>
<td>$PMSessionLogDir</td>
<td>Directory for session logs. It cannot include the following special characters: `*&lt;&gt;</td>
</tr>
<tr>
<td>$PMBadFileDir</td>
<td>Directory for reject files. It cannot include the following special characters: `*&lt;&gt;</td>
</tr>
<tr>
<td>$PMCacheDir</td>
<td>Directory for index and data cache files. You can increase performance when the cache directory is a drive local to the Integration Service process. Do not use a mapped or mounted drive for cache files. It cannot include the following special characters: `*&lt;&gt;</td>
</tr>
<tr>
<td>$PMTargetFileDir</td>
<td>Directory for target files. It cannot include the following special characters: `*&lt;&gt;</td>
</tr>
<tr>
<td>$PMSourceFileDir</td>
<td>Directory for source files. It cannot include the following special characters: `*&lt;&gt;</td>
</tr>
<tr>
<td>$PMExtProcDir</td>
<td>Directory for external procedures. It cannot include the following special characters: `*&lt;&gt;</td>
</tr>
<tr>
<td>$PMTempDir</td>
<td>Directory for temporary files. It cannot include the following special characters: `*&lt;&gt;</td>
</tr>
<tr>
<td>$PMLookupFileDir</td>
<td>Directory for lookup files. It cannot include the following special characters: `*&lt;&gt;</td>
</tr>
<tr>
<td>$PMStorageDir</td>
<td>Directory for run-time files. Workflow recovery files save to the $PMStorageDir configured in the Integration Service properties. Session recovery files save to the $PMStorageDir configured in the operating system profile. It cannot include the following special characters: `*&lt;&gt;</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Environment Variables</td>
<td>Name and value of environment variables used by the Integration Service at workflow run time.</td>
</tr>
</tbody>
</table>

**Configuring Service Process Variables for Operating System Profiles**

Service process variables set in an operating system profile override service process variables set in the Integration Service properties. If the Integration Service runs on a grid, the operating system user must have access to the service process variables configured in the operating system profile on every node in the grid.

Define absolute directory paths for $PMWorkflowLogDir and $PMStorageDir in the Integration Service properties. You configure $PMStorageDir in the Integration Service properties and the operating system profile. The Integration Service saves workflow recovery files to the $PMStorageDir configured in the Integration Service properties and saves the session recovery files to the $PMStorageDir configured in the operating system profile. Define the other service process variables within each operating system profile.

**Step 6. Assigning Permissions**

Assign permissions on an operating system profile to users and groups. Then, assign operating system profiles to repository folders or to a workflow. If the user that runs a workflow does not have permission on the operating system profile assigned to the workflow, the workflow fails.

Users inherit permissions on the operating system profile if they belong to a group that has permissions on the operating system profile. Users that have the Administrator role inherit permission on all operating system profiles. The Permissions tab of the operating system profile shows a list of all users with permissions on the operating system profile.

Click edit on the Permissions tab to edit permissions on the operating system profile. To add permissions on operating system profiles, select a user or group from the All Users and Groups area and click the right arrow. To remove permissions on operating system profiles, select a user or group from the Users and Groups with Permissions area and click the left arrow.

**Assign Operating System Profiles to Repository Folders or to a Workflow**

The Integration Service uses the operating system profile to run workflows in the folder. Operating system profiles allow the Integration Service to run a workflow and write output files using the setting of the operating system profile.

You must have permission on the operating system profile to assign it to a folder or workflow. In the Repository Manager, edit the folder properties to assign an operating system profile for the Integration Service to use. You can use the Start Workflow Advanced option in the Workflow Manager to override the operating system profile assigned to the folder.

When you copy a folder or back up a repository, the operating system profile assignment is not copied. After you copy a folder or restore a repository, you must assign an operating system profile to the folder.

**Troubleshooting Operating System Profiles**

**After I selected Use Operating System Profiles, the Integration Service failed to start.**

The Integration Service will not start if operating system profiles is enabled on Windows or a grid that includes a Windows node. You can enable operating system profiles on Integration Services that run on UNIX.

-or-

pmimpprocess was not configured. To use operating system profiles, you must set the owner and group of pmimpprocess to administrator and enable the setuid bit for pmimpprocess.
Author

Padma Heid
Technical Writer