Opsware™ Process Automation System

Version 2.2, Administering Opsware Process Automation System

For Process Automation System Administrators

Table of Contents

Overview

Administering PAS includes:

- Managing security, which comprises managing Security: Users, Groups, Capabilities, and Permissions

  You can map PAS user roles either to external groups or roles or to individual user accounts.

- Enabling PAS to run Ops flows against remote machines and integrate them with other applications.
- Changing such configurations for Central and Studio as:
  - The Studio host server, communications port number, and protocol used.
  - The database user account and password.
  - The maximum size of the Jetty service Wrapper.log file.
- Backing up OpsForce.

For information on administering Ops flow runs, see Help for Central.

Security: Users, Groups, Capabilities, and Permissions

Many of the PAS security features take place in the background. From the point of view of the PAS administrator, author, and user, PAS security deals with:

- Security of communications between PAS system components and between those components and the flows' target systems.

  The aspect of this that is relevant to authors is the use of the HTTPS protocol and SSH for PAS communications.

- User authentication, or logging in.

  You can configure PAS to use external Active Directory, LDAP, or Kerberos authentication of user logins. To accomplish this configuration, you use the Central **Administration** tab. For information on doing so, see Help for Central.

  Note: In order to make communications secure, you can configure Active Directory to run over the Secure Sockets Layer, using the LDAPS protocol. For information on doing so, see Configuring Active Directory or LDAP over SSL (LDAPS protocol).

- Managing PAS users and groups and controlling the operations and flows that they can run.

  In PAS, groups are the basic unit for managing access to flows and controlling what they can do with the flows, but you could manage them with individual users as well. You manage groups' and users' rights by granting them:

  - Capabilities (types of actions that users can perform).

    To give your flow authors the capability to author flows, for instance, you might create a group, "Authors", which you would assign the AUTHOR capability. You manage users, groups, and capabilities from the Central Web application. For information on doing so, see Help for Central.

  - Access to specific objects (such as folders, flows, operations, and system accounts within Studio).

For example, for an author to make and test changes to a flow that has subflows, he or she needs to have the AUTHOR capability as well as the READ, WRITE, and EXECUTE permissions for the flow and the LINK permission for any subflow that is used in the flow.

For a Central user to run a certain flow (flow X), you would add the Central user to the LEVEL_ONE, LEVEL_TWO, or LEVEL_THREE group, any of which comes with the capabilities needed to run flows, and you would assign him or her the EXECUTE permission for flow X.

Authors assign permissions for flows and associated objects in Studio. For information on doing so, see Help for Studio.

The following graphic shows how the concepts of users, groups, capabilities, and permissions interact to let administrators and authors define how individuals can react with which objects.

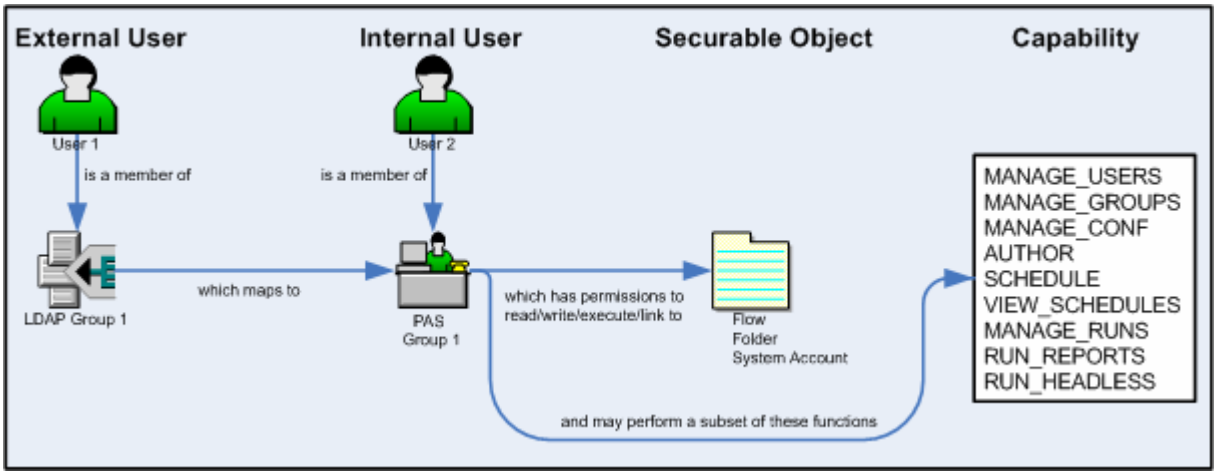

Figure 1 - Components of access control in PAS

- Protecting the confidentiality of sensitive credentials.

  System accounts are PAS objects that a user can invoke in order to run a flow in a location that requires specific authentication and permissions that the flow user might not have, without the user's being able to see the credentials he or she is using to run the flow. This means that flow users can run flows wherever necessary, but without the user's having to enter the credentials necessary to get access to the flows' targets, while the credentials remain protected.

Configuring Active Directory or LDAP over SSL (LDAPS protocol)

Machines ordinarily communicate with Active Directory using Lightweight Directory Access Protocol (LDAP, a clear-text protocol). To encrypt communications, you can set PAS to communicate with Active Directory over Secure Sockets Layer (SSL). The LDAPS protocol is the LDAP protocol encrypted with SSL.

Important: If you are configuring LDAP to run over SSL, see your LDAP administrator about exporting a certificate, then complete the following procedure, skipping steps 1 through 9.

To configure Active Directory to communicate with LDAPS

1. On the AD machine, start Microsoft Management Console (mmc.exe).
2. To add the Certificates snap-in:
   a. From the **File** menu, select **Add/Remove Snap-in.**
   b. In the **Add/Remove Snap-in** dialog, click **Add.**
   c. In the **Add Standalone Snap-in** dialog, select **Certificates** and click **Add.**
   d. Select **Computer Account** and then click **Next.**
   e. In the **Select Computer** dialog box, click **Finish.**
   f. In the **Add standalone Snap-in** dialog, click Close, and in the **Add/Remove Snap-in** dialog click **OK.**
3. In the MMC console, open **Certificates (Local Computer)** and its subfolders **Personal\Certificates.**
4. In the right panel, find the certificate for the AD.

   For example, if the AD is "ad.mycompany.com", you should see a certificate with:

   - The same name as the AD.
   - An intended purpose of **Client Authentication.**
   - A **Domain Controller** certificate template.
5. Right-click the certificate, point to **All Tasks,** then click **Export.**
6. When the Certificate Export Wizard starts, click **Next.**
7. Make sure that **No, do not export the private key** is selected, then click **Next.**
8. In the **Export File Format** page, select **DER encoded binary X.509 (CER)** and click **Next.**
9. In the **File to Export** page, select the location and name of the exported certificate.

   The certificate file has a .cer extension.
10. Copy the exported certificate file to a location on the server machine on which you have installed Central.
11. On the Central machine, stop the RSCentral service.
12. Open a command-line window and run the following two commands:

    ```
    cd %PAS_HOME%\jre1.5\bin
    keytool –keystore "%PAS_HOME%\jre1.5\lib\security\cacerts" –import –file <path_to_cert_from_step9> -alias <some_alias>
    ```

    In this command, **alias** is used to identify the certificate. For example, it could be named something like "mycompany_ad_cert".
13. When prompted for the certificate store's password, type "changeit".

    "changeit" is the default password. For information on using "keytool" to change the password, see the keytool documentation.
14. When you are prompted to confirm that this certificate should be trusted, type **Yes**.
15. To verify that the certificate was imported, run the following command:

    ```
    keytool –keystore "%PAS_HOME%\jre1.5\lib\security\cacerts"
     –list -alias <some_alias>
    ```

    The default certificate store password is "changeit".

    You should see a summary of the certificate.

16. In %PAS_HOME%\Central\conf, open the Central.properties file in a text editor.
17. Locate the line that begins with “ADAuthGroupBased.URL” and set it to specify the LDAPS protocol, by modifying it to read as follows:

    ```
    ADAuthGroupBased.URL=LDAPS://<your_AD>:<port> ;
    ```

    For example, if your AD is ad.mycompany.com and you have configured it to use the default port 636, the line should read as follows:

    ```
    ADAuthGroupBased.URL=LDAPS://ad.mycompany.com:636 ;
    ```
18. Restart RSCentral service.

Configuring PAS for extended functionality

Extended functionality in PAS is the use of Ops flows that can execute actions:

- On machines that are on different domains or on the other side of firewalls from the Central Web server (the machine on which you installed the Central Web application).
- That use other Web services or application programming interfaces (APIs).

Such actions are carried out by RAS operations, which are enabled, or hosted, by one of two Web services that are installed during the PAS Web application installation:

- Java Remote Action Service (JRAS)
- .NET Remote Action Service (NRAS)

A RAS operation therefore requires a reference that directs it to JRAS or NRAS. The reference, which you configure in Studio, is made up of a name and the URL of the JRAS or NRAS. You also must add the reference in the RAS operation. (For information on adding a JRAS or NRAS reference in a RAS operation, see Help for Studio.)

There are two considerations that may affect how you install JRAS and NRAS.

1. Where you need to install JRAS and NRAS and their content.

   The Central installation installs JRAS and NRAS on the Central server. However, to run an operation against a machine that is on a different domain or the other side of a firewall from the Web server, JRAS or NRAS must be installed on the machine against which you’re going to run the operation.

2. Which applications you will run the operation against.

   The following applications have special additional requirements:

   - Microsoft Operations Manager (MOM)

     Operations that run against MOM can only run on a MOM server and require NRAS to integrate with MOM. The instance of NRAS must be installed on the MOM server.

   - Microsoft Exchange Server

     Operations that run against Exchange Server can only run on a machine that has the Exchange Server management tools installed and require NRAS to integrate with Exchange Server. The instance of NRAS must be installed on the Exchange server.

   - Windows Server Clustering Services

Operations that run against Clustering Services can only run on an Enterprise Edition Windows 2003 Server or a machine that has the Windows 2003 Server Administrator Pack installed. These operations require NRAS to integrate with Clustering Services. The instance of NRAS must be installed on the Windows Server that is running the Clustering Services.

- HP OpenView

  Operations that run against HP OpenView can only run on a machine that is running HP OpenView and require JRAS to integrate with HP OpenView. The instance of JRAS must be installed on the HP OpenView machine.

These applications require special content (IAction code), which is installed by the JRAS and NRAS content-upgrade programs JRASContentSetup.exe and NRASContentSetup.exe.

The JRAS and NRAS content-upgrade programs require the versions of JRAS and NRAS that are installed by the independent installation programs JRASSetup.exe and NRASSetup.exe. These versions are different from the versions of JRAS and NRAS that are installed by default.

Therefore, after you install the PAS Web server, you can run operations that:

- Run against machines on the PAS Web server's domain (and are not on the other side of a firewall from the PAS Web server).
- Do not require support for MOM, Exchange Server, Clustering Services, or HP OpenView.

On the other hand, you need to install either JRAS and its content-upgrade program or NRAS and its content-upgrade program in order to run an operation against:

- A machine that is on a different domain or on the other side of a firewall from the PAS Web server.

  You only need to install JRAS or NRAS on one machine on the other domain or on the far side of the firewall in order to run a JRAS-dependent or NRAS-dependent operation on other machines there.

- MOM, Exchange Server, Clustering Services, or HP OpenView.

The following table summarizes this discussion.

If the operation you want to run	**Then you need to run these installation programs**
Does not require either JRAS or NRAS.	Nothing beyond the Central installation
Requires either JRAS or NRAS. Runs within the local installation of PAS. Does not run against applications that require special RAS IAction content.	Nothing beyond the Central installation, because the operation can use the NRAS or JRAS content that was installed as part of the Central installation
Runs against a machine on a different domain or across a firewall from the PAS Web server. Does not run against applications that require special RAS IAction content.	The following, run on the machine against which you will run the operation: JRASSetup.exe or NRASSetup.exe

	as appropriate
Runs within the local installation of PAS. Runs against applications that require special RAS IAction content.	The following, run locally: JRASSetup.exe and JRASContentSetup.exe OR NRASSetup.exe and NRASContentSetup.exe as appropriate
Runs against a machine on a different domain or across a firewall from the PAS Web server. Runs against applications that require special RAS IAction content.	The following, run on the machine against which you will run the operation: JRASSetup.exe and JRASContentSetup.exe OR NRASSetup.exe and NRASContentSetup.exe as appropriate

The following sections describe installing JRAS and NRAS and their content, and testing the installations.

Installing JRAS and JRAS content

Because JRAS is installed as part of the Central install, this installation need only be done on machines on which Central has not been installed.

To install the JRAS server

1. On the Opsware PAS CD, locate JRASSetup.exe and copy it to the machine on which you're going to install it.
2. Start the copy of JRASSetup.exe that you just created.
   The Opsware JRAS Setup Wizard starts with the **Welcome** page.
3. Click **Next.**
4. On the **License Agreement** page, read the agreement, click **I accept the agreement,** and then click **Next.**
   The **JRAS Configuration** page appears. On this page, you specify:
   - A location for the Java Virtual Machine that this wizard creates.
   - A communication port number for JRAS.
5. In the **JVM Path** box, leave the default installation path.
   OR
   Specify a different location where Java.exe resides.
6. In the **Port Number** box, leave the default port number or specify a new one, and then click **Next.**
   The **JRAS Optional Packages** page appears.
7. Select either or both of the following items of optional content for installation:

- Base Content, which comprises the IActions that are used in the Opsware Accelerator Packs.
- SDK Examples, which contain sample code you use to build your own IActions.

8. Click **Next.**
9. On the **Select Destination Location** page, click **Next** to accept the default installation path for JRAS.

   OR

   Click **Browse,** specify a different location where you want JRAS installed, and then click **Next.**
10. On the **Select Start Menu Folder** page, either accept the default **Start** menu folder in which you want the JRAS shortcut to reside or specify a different one, and then click **Next.**

    The **Ready to Install** page appears, displaying the location where JRAS will be installed and other information on the choices you have made.
11. To proceed, click **Install.**

    The installation program tracks progress on the installation progress page.
12. When the installation completes, click **Finish.**

To install JRAS-specific content

1. At the source of the Opsware installation files, navigate to and run JRASContentSetup.exe.

   The Opsware JRAS Content Updater Setup Wizard starts with the **Welcome** page.
2. Click **Next.**
3. On the **License Agreement** page, read the agreement, click **I accept the agreement,** and then click **Next.**

   The **Select Components** page appears, on which you choose the type of installation and/or which components you want to install.

   - A full installation installs both base content (the IActions required for Opsware Accelerator Packs) and HP OpenView operations.
   - A compact installation installs only base content.
   - In a custom installation, you choose which components you want to install.
4. Choose a full, compact, or custom installation.

   OR

   Select the components you want to install. The kind of installation changes automatically depending on which components you select.
5. Click **Next.**

   The **Ready to Install** page appears, displaying the location where JRAS content will be installed and other information on the choices you have made.
6. To proceed, click **Install.**
7. When the installation completes, click **Finish.**

To test the JRAS server installation

- Using a Web browser, access the following URL to confirm that the Web service is running.

  `http://<Hostname>:<Portnumber>/JRAS/services/RCAgentService?wsdl`

  where

  - <Hostname> is the name of the PAS Web application server
  - <Portnumber> is the name of the default port used for JRAS on the Web application server

    If you accept the default port number in the JRAS Setup, this number is 4085.

  If the Web service is running, a WSDL/XML document appears.

Installing the .NET Remote Action Service

The .NET Remote Action Service (NRAS) installation program creates and places files in the default IIS Web root directory.

Because NRAS is installed as part of the Central installation, you only need to perform the NRAS installation on machines on which you have not installed Central.

To install NRAS

1. At the source of the Opsware installation files, navigate to and run PASNRASInstaller.exe.
2. On the **Welcome** page, click **Next.**
3. On the **License Agreement** page, read the agreement, click **I accept the agreement,** and then click **Next.**
4. On the **NRAS Optional Packages** page, select either or both of the following items of optional content for installation:
   - **Base Content,** which comprises the IActions that are used in the Opsware Accelerator Packs.
   - **SDK Example,** which contain sample code you use to build your own IActions.
5. On the **Network Settings** page, specify an IP address that NRAS will use for communications.
6. On the **Select Destination Location** page, click **Next** to accept the default installation path for NRAS.

   OR

   Click **Browse,** specify a different location where you want the NRAS installed, and then click **Next.**
7. On the **Select Start Menu Folder** page, either accept the default **Start** menu folder in which you want the NRAS shortcut to reside or specify a different one, and then click **Next.**

   The **Ready to Install** page appears, displaying the location where NRAS will be installed and other information on the choices you have made.
8. To proceed, click **Install.**

   The installation program tracks progress on the installation progress page.
9. When the installation completes, click **Finish.**

To test the NRAS server installation

- Using a Web browser, access the following URL to confirm that the Web service is running.

  `http://<Hostname>:<Portnumber>/NRAS/services/RCAgentService.asmx`

  where

  - <Hostname> is the name of the PAS Web application server
  - <Portnumber> is the name of the default port used on the Web application server.

    If you accepted the default port number when you installed the NRAS server, the default port number is 4080.

  If the Web service is running, a WSDL/XML document appears.

To obtain access to the NRAS interface within Studio

- Open Studio and configure a remote action service.

  For information on configuring a remote action service, see Help for Studio.

Changing Central configurations

Central configurations that you can change include:

- Which authentication providers are enabled and specific settings for how PAS uses them.

  PAS supports the following authentication providers:

  - Active Directory (AD)
  - Lightweight Directory Access Protocol (LDAP)
  - Kerberos

  For information on enabling authentication with one or more of these providers, see Help for PAS Central. (Because topic names can change, search for “external authentication”.)
- Mapping external groups to internal PAS groups.
- The password of the database user account that PAS uses.

  Warning: When changing passwords and assigning accounts to user roles, remember that the Central.properties file is not encrypted. The only protection for this file is the security of the file’s location in your system.
- The maximum size of the Jetty service Wrapper.log file.

  If you install Central as a Windows service, then by default the maximum size for Wrapper.log is 64 megabytes (MB). When the file reaches that size, the file begins to *roll*—that is, the oldest entry is deleted as each new entry is added. For information on changing the maximum size of Wrapper.log, see the procedure, “To change the maximum size of the Jetty service Wrapper.log.

Changing the password of the database user

After changing the password of the database user in the database management system, complete the following procedure.

To change the password of the database user

1. In a text editor, open \%PAS_HOME%\Central\conf\Central.properties.

2. Find the following line, append the new password, and then save and close the file.

   ```
   hibernate.connection.password=
   ```

Changing the maximum size of the Wrapper.log file

To change the maximum size of the Jetty service Wrapper.log file

1. In the Jetty home directory, navigate to \extra\win32 and then open wrapper.conf.

   If you accepted the defaults in the Central installation program, the Jetty home directory is a subdirectory of the PAS home directory (which by default is C:\Program Files\Opsware\PAS).

2. Locate the property “wrapper.logfile.maxsize” and specify the maximum size in bytes that the log file should reach before it starts rolling.

   You can abbreviate the size value of this property by adding k (for kilobytes) to the end of the size.

   Important: Setting the value to zero (0) disables rolling, and the file will grow indefinitely.

3. Save and close the file.

Changing Studio configurations

In the \iConclude\conf\Studio.properties file, you can change the following aspects of the Studio:

- Central host server
- Default communication port used
- Choice of HTTP: or HTTPS: (secure sockets) as the Internet protocol

To change the Studio.properties file

1. Use a text editor to open %PAS_HOME%\Studio\conf\Studio.properties
2. Edit the following lines to make the desired changes:
   - To change the name of the host server (the server on which the Web application is located), change **localhost** in the following line to the name or IP address of the host server.

     ```
     dharma.repaircenter.host=localhost
     ```

   - To change the port number that PAS uses, change **8080** in the following line to the desired port number.

     ```
     dharma.repaircenter.port=8080
     ```

   - By default, PAS uses the https Internet protocol. To specify that PAS use the http Internet protocol, change **https** in the following line to **http**.

     ```
     dharma.repaircenter.proto=https
     ```

Backing up PAS

Backing up PAS involves backing up your Ops flows, operations, system accounts, selection lists, and other PAS objects, and backing up the PAS database. You back up

PAS objects in Studio by backing up the repository and then placing a copy of the repository's backup in a secure location.

To back up PAS

1. In Studio, back up each repository (**Create Backup** command, on the **Repository** menu), using the procedure given in Help for Studio.

   Each repository is backed up as a .jar file.
2. Make a copy of each repository's .jar file and store the copy in a secure location.
3. Back up the Central database and store the backup in a secure location.

   Dashboard charts are stored in the Central database, so the database backup includes Dashboard charts.

Index