Platform Application Center
Version 9 Release 1 Modification 1

Release Notes

GI13-1890-02

Platform Application Center
Version 9 Release 1 Modification 1

Release Notes

GI13-1890-02

Note
Before using this information and the product it supports, read the information in "Notices" on page 31.

First edition

This edition applies to version 9, release 1, modification 1 of IBM Platform Application Center (product number 5725G88) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. What's new

New supported browsers

Google Chrome for Windows version 26, 27, 28 is now supported.

New supported operating systems

The following operating systems are now supported for the Platform Application Center web server:

Linux for Power Systems™ Servers (Linux 2.6, glibc 2.3 or glibc 2.11): Red Hat Enterprise 5.6, 5.7, 5.8, 6.0, 6.1, 6.2, 6.3 and SUSE 11.0, 11.1, 11.2

DCV visualization session sharing with other users

For new installations, the following built-in application templates for NICE Desktop Cloud Visualization (DCV) now have two new fields: **Share visualization with** and **Share permissions**:

- AppDCV
- AppDCVonLinux
- CATIA

For upgrades, to use this feature, you will need to add the new fields to your application templates.

In the job submission form, these fields allows users to specify operating system user accounts with whom they want to share their visualization session and indicate whether the share is view-only or whether the other users have view and control access to the visualization.

Once the user submits the job, users that are specified in the **Share visualization with** field are able to view the job in the **Jobs** page, and can click **Visualize** to visualize the job with DCV. If the users are also allowed control of the visualization, they are able to manipulate the visualization window.

The user who submitted the job can modify who can visualize this job after job submission by clicking the **Share Visualization** button from the **Job Details** page. Users that are removed from the **Share visualization with** list are no longer able to see the job in the **Jobs** page. Note, however, that any open visualization windows are not automatically closed.

Enable DCV visualization session sharing in existing DCV application templates

To add the new **Share Visualization with** and **Share permission** fields to any of your existing DCV application templates:

1. Unpublish your application template.
2. Add a field in your application template and make sure that the field ID is SHARE_USER_LIST.

SHARE_USER_LIST is a reserved system ID to enable DCV session sharing and requires no changes to your existing submission script.

3. Add a radio button field in your application template and make sure that the field ID is SHARE_USER_VIEW_ONLY.

   Specify the values: View only, and View & Control.

   A value of true indicates the share is view-only to users listed in the SHARE_USER_LIST field. A value of false indicates users listed in the SHARE_USER_LIST field can view and control the session. SHARE_USER_VIEW_ONLY is a reserved system ID to define sharing permissions for DCV session sharing and requires no changes to your existing submission script.

4. Publish your application template.

Last local path saved for input and output files

Platform Application Center now saves the last local path that a user navigated to. This applies when a user adds input files in submission forms, and uses local directories to download or upload files in the **Jobs** page.

Single sign-on with X.509 authentication

Platform Application Center now supports client authentication with X.509 certificates, through the web browser and the Web Services API.

The X.509 certificate is used to verify the identity of the Platform Application Center server when HTTPS is used from a browser. After the certificate is imported into the browser, authentication is done through X.509 and users are not prompted to log in to Platform Application Center.

To use X.509 authentication with Platform Application Center, you need to configure the Platform Application Center web server and each client.

Usage Statistics for license entitlement

In **System & Settings** > **Usage Statistics**, you can now compare product usage against the licensed amounts for:

- IBM® Platform Application Center
- IBM Platform LSF®
- IBM Platform Dynamic Cluster
- IBM Platform License Scheduler

In the new configuration file `$GUI_CONFDIR/entitlement.conf`, specify values according to what your audit agreement states and restart Platform Application Center services. The charts indicate whether the licensed amounts are exceeded, when, and how often. The charts display the licensed amount, and the maximum sampled value for the past week, past month, and past year, as well as all-time high values.

Chapter 2. Differences between IBM Platform Application Center editions

IBM Platform Application Center(Platform Application Center) is available in two editions: Basic Edition and Standard Edition.

IBM Platform Application Center Basic Edition provides basic job submission, and job and host monitoring.

IBM Platform Application Center Standard Edition provides not only basic job submission and job and host monitoring, but also default application templates, role-based access control, reporting, customization, and remote visualization capabilities.

The following table highlights the differences between the editions.

Feature	IBM Platform Application Center Basic Edition	IBM Platform Application Center Standard Edition
Generic job submission	✓	✓
Job and host monitoring	✓	✓
Built-in reporting		✓
Specific application job submission		✓
Built-in application templates		✓
Custom applications and templates		✓
Custom job data repositories		✓
SDK to extend application templates and create custom pages		✓
Notifications when job status changes		✓
Branding customization capabilities		✓
Support for remote 2D/3D visualization		✓
Web Services API		✓
Role-based access control		✓
LSF Scheduler Dashboard		✓
Product Usage Statistics	✓	✓
Integration with IBM Platform Process Manager for web-based flow submission, monitoring and control		✓

Feature	IBM Platform Application Center Basic Edition	IBM Platform Application Center Standard Edition
Integration with IBM Platform Analytics reports for advanced web-based analysis and reporting on LSF data		✓
Integration with IBM Platform License Scheduler for web-based license usage monitoring	✓	✓

Chapter 3. Requirements

New installation requirements

Installation location requirements

Access to LSF

The installation location must have access to the IBM Platform LSF environment(LSF). LSF must be installed and accessible. Get the location of LSF and know the value of LSF_ENVDIR.

Memory requirements

Ensure the installation location has enough memory. The following indicates the Minimum recommended hardware for the Platform Application Center web server.

Item	Small cluster (Up to)	Medium cluster (Up to)	Large cluster (Up to)
Active jobs	5000	50,000	500,000
Job throughput	10,000 jobs/day	100,000 jobs/day	1 million jobs/day
Hosts	100	1000	6000
Active users	50	200	1000
Concurrent users	10	40	200
Time to keep job information and data (default)	14 days	14 days	14 days
Minimum recommended hardware for the Platform Application Center web server	1 CPU, 4 cores each Memory: 8 GB Disk type: Normal	2 CPUs, 4 cores each Memory: 16 GB Disk type: Faster	2 CPUs, 8 cores each Memory: 24 GB Disk type: Faster
Tuning required?	No	Yes	Yes

Disk space requirements

Disk size

Each host should have at least 800 MB of local disk space to install. To support ongoing logging of important data, 2 GB or more is recommended.

Job data

Make sure you have enough space for job data. By default, all job data is stored under the directory `/home/`.

Platform Application Center web server host

- For new installations, a requirement is that you do not have any existing versions of Platform Application Center installed.
- For upgrades, you must have installed Platform Application Center 8.0, 8.0.1, 8.0.2, 8.3, or 9.1.0.0

- For best performance, do not use the LSF master host as the Platform Application Center web server host.
- If failover is required, the Platform Application Center host must be one of the LSF master candidates.
- If failover is not required, any LSF server or client host can be the Platform Application Center web server host as long as the host can read the following:
  - $LSF_ENVDIR
  - $LSF_SERVERDIR
  - $LSB_SHAREDIR

Installation location requirements when using Platform Process Manager

If you have IBM Platform Process Manager(Platform Process Manager):

- If Platform Process Manager is locally installed, you must install Platform Application Center on the same host.
- If Platform Process Manager is installed on a shared filesystem, the Platform Application Center must be installed on a host that can access the shared filesystem.

Installation user account

You must be root to install.

Failover requirements

- Get the name of the LSF master and LSF master candidate hosts as indicated with the parameter LSF_MASTER_LIST in `lsf.conf`.
- You have two LSF master candidate hosts to act as failover hosts.
- You have enabled EGO in your cluster. This is required to support failover for Platform Application Center.
- You have a shared file system in which to install Platform Application Center. This is required in case the host on which Platform Application Center is installed goes down.
- If you are enabling MySQL failover:
  - You have MySQL Community Edition or MySQL Enterprise, version 5.5 or higher.
  - MySQL is installed locally on two LSF master candidate hosts, and it is installed in the same local directory on both hosts.
  - Both LSF master candidate hosts have the same MySQL version.

Database requirements

Supported databases

- MySQL 5.0, 5.1, 5.5, 5.6 Community Edition and Enterprise. For better performance, MySQL 5.6 is recommended.
- Oracle 10g, 11.2 Enterprise Edition for production clusters

MySQL requirements

- Check that MySQL is installed and running.
- Get the location of the MySQL JDBC driver. You will need it for installation. Versions 5.1.13 and higher are supported.

  If the MySQL JDBC driver is not installed, you can download it from:

`http://www.mysql.com/downloads/connector/j/`

Important: After download, you will need to manually extract the MySQL JDBC driver package to a local directory on the Platform Application Center host.

- Get the MySQL root user password. You will need it for installation. The default for MySQL is no password.

Oracle requirements

- Check your Oracle database is properly configured and running.
- Check you have a user name, password, and URL to access the database.
- Ensure you installed the latest JDBC driver (`ojdbc14.jar` or newer) for the Oracle database. This driver is available from the following URL:

  `http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/index.html`

LSF requirements

LSF and LSF add-ons product versions

Important: If you are using LSF 8.0, 8.0.1 or 8.3, you need to download and install the fix pack.

- Fix pack for LSF 8.3:

  http://www.ibm.com/support/fixcentral/swg/selectFixes?parent=Platform+Computing&product=ibm/Other+software/Platform+LSF&release=All&platform=All&function=fixId&fixids=lsf-8.3-build209549&includeSupersedes=0
- Fix pack for LSF 8.0.1:

  http://www.ibm.com/support/fixcentral/swg/selectFixes?parent=Platform+Computing&product=ibm/Other+software/Platform+LSF&release=All&platform=All&function=fixId&fixids=lsf-8.0.1-build209240&includeSupersedes=0

	Supported with			
	IBM Platform LSF	**IBM Platform Process Manager**	**IBM Platform Analytics**	**IBM Platform License Scheduler**
IBM Platform Application Center Basic Edition	• 9.1, 9.1.1, 9.1.1.1 Express® Edition • 9.1, 9.1.1, 9.1.1.1 Standard Edition • 8.3 Express Edition • 8.3 Standard Edition • 8.0.1 • 8.0	-	-	9.1

	Supported with			
	IBM Platform LSF	**IBM Platform Process Manager**	**IBM Platform Analytics**	**IBM Platform License Scheduler**
IBM Platform Application Center Standard Edition	• 9.1, 9.1.1, 9.1.1.1 Express Edition • 9.1, 9.1.1, 9.1.1.1 Standard Edition • 8.3 Express Edition • 8.3 Standard Edition • 8.0.1 • 8.0	9.1.1	9.1	9.1

Synchronize times between LSF and Platform Application Center

The clock time on both the LSF master and the Platform Application Center web server must be the same. Ensure these times are synchronized.

Ensure the LSF LSB_SHAREDIR is accessible

Platform Application Center requires read access to the LSF `work` directory, defined in the LSF configuration file `$LSF_ENVDIR/lsf.conf` with the parameter LSB_SHAREDIR.

Configure LSF events for Platform Application Center

You need to configure LSF to log events so that Platform Application Center can retrieve job information.

1. Log on to the LSF master host as the LSF administrator.
2. Set the LSF environment.
3. Edit the `$LSF_ENVDIR/lsbatch/`*`cluster_name`*`/configdir/lsb.params` configuration file.
   a. Add the parameter `ALLOW_EVENT_TYPE` and define the following events.

      If you do not plan to use Standard reports, use the following configuration. These are the required events for the **Jobs** page in Platform Application Center to work properly:

```
ALLOW_EVENT_TYPE=JOB_NEW JOB_STATUS JOB_FINISH2 JOB_START JOB_EXECUTE JOB_EXT_MSG JOB_SIGNAL JOB_REQUEUE JOB_MODIFY2
JOB_SWITCH METRIC_LOG
```

      If you plan on using Standard reports, use the following configuration:

```
ALLOW_EVENT_TYPE=JOB_NEW JOB_START JOB_START_ACCEPT JOB_STATUS JOB_FORWARD \
MIG JOB_ACCEPT JOB_SWITCH JOB_FINISH JOB_MODIFY2 UNFULFILL JOB_SIGACT \
JOB_SIGNAL JOB_EXECUTE JOB_REQUEUE JOB_CLEAN JOB_EXCEPTION JOB_EXT_MSG \
JOB_ATTA_DATA JOB_CHUNK SBD_UNREPORTED_STATUS PRE_EXEC_START JOB_FORCE \
JOB_MOVE JOB_RUN_RUSAGE METRIC_LOG
```

   b. Enable event streaming by setting `ENABLE_EVENT_STREAM=Y`.

      Event streaming in your LSF cluster is required so that data can be loaded into the Platform Application Center database.

      Important: The LSF stream file name must be `lsb.stream` to work with Platform Application Center. This is the default name.

   c. Check whether the parameter LSB_QUERY_PORT is set in `lsf.conf`. If LSB_QUERY_PORT is set, then set `NEWJOB_REFRESH=Y` in `lsb.params`.

This is required because when LSB_QUERY_PORT is set, newly submitted job information is not immediately available, and as a result, Platform Application Center is unable to display job details when a job is submitted.

4. Run **badmin reconfig** to reconfigure mbatchd.

LSF and IBM Platform MultiCluster

If using LSF with IBM Platform MultiCluster, ensure the first cluster name listed in the configuration file `lsf.shared` is the local cluster name, as this is used by LSF to detect the `lsb.stream` file location.

Additional requirements for LSF 8.x only

Install the Fix Pack for LSF 8.0.1 and 8.3:
Install the fix pack for LSF 8.0.1 and LSF 8.3.

- Fix pack for LSF 8.3:

  http://www.ibm.com/support/fixcentral/swg/selectFixes?parent=Platform+Computing&product=ibm/Other+software/Platform+LSF&release=All&platform=All&function=fixId&fixids=lsf-8.3-build209549&includeSupersedes=0

- Fix pack for LSF 8.0.1:

  http://www.ibm.com/support/fixcentral/swg/selectFixes?parent=Platform+Computing&product=ibm/Other+software/Platform+LSF&release=All&platform=All&function=fixId&fixids=lsf-8.0.1-build209240&includeSupersedes=0

Define how to manage the lsb.stream file for LSF 8.x:

1. Log in as LSF administrator to the Platform Application Center web server.
2. Set your Platform Application Center environment:

   For example:

   - For **csh** or **tcsh**:

     ```
     % source /opt/pac/cshrc.platform
     ```

   - For **sh**, **ksh**, or **bash**:

     ```
     $ . /opt/pac/profile.platform
     ```

3. Edit the `$PERF_CONFDIR/dataloader/lsbevents.properties` file and set:

   ```
   AUTO_DELETE_STREAM_FILE=Y
   REMAINED_STREAM_FILE=10
   ```

   The number in REMAINED_STREAM_FILE represents the number of files and can be smaller or larger depending on your site requirements.

System requirements

Supported operating systems

- Linux 2.6 glibc 2.3 x86 64 bit, Red Hat 5.6, 5.7, 5.8, and 6.0, 6.1, 6.2, 6.3
- Linux 2.6 glibc 2.3 x86 64 bit, SUSE 10.2, SUSE 11.0, 11.1, 11.2
- Linux for Power Systems Servers (Linux 2.6, glibc 2.3 or glibc 2.11): Red Hat Enterprise 5.6, 5.7, 5.8, 6.0, 6.1, 6.2, 6.3 and SUSE 11.0, 11.1, 11.2

Supported authentication

- Password File
- NIS
- LDAP

- AD (Active Directory)

Supported web browsers

Linux

- Firefox 3.6, 10.0

Windows

- Internet Explorer 8, 9
- Firefox 16, 17.07, 20, 21, 22
- Google Chrome 26, 27, 28

Important:

Adobe Flash version 8 or later is required to access report charts.

Supported Java Runtime Environment (JRE) in browser

- JRE 1.6.0_10 or higher is required.

  JRE1.6.0_25 or higher is required for Internet Explorer 9.
- For Exceed on Demand integrations, JRE 1.7 or higher is required on the browser for application templates to work properly.
- The JRE add-on must be enabled.

Important: A supported Java™ Runtime Environment(JRE) version must be enabled at the system level on the host on which the browser is running. Otherwise, Platform Application Center will not work properly. Select **Start** > **System** > **Control Panel** > **Java** and check that a supported version of the JRE is enabled.

Tested applications and versions

The following versions of supported applications have been tested with Platform Application Center:

Note: These are tested application versions. Job submission forms can be customized to support other versions.

Application	Tested Versions
ABAQUS	• 6.9-1
ANSYS	• V121 • V120 • V110 • V100
BLAST	• 2.2.20
CATIA	• V5R20 Windows 7
CFX	• CFX-5 (Ansys Suite)
CLUSTALW	• 2.1
CMGL_GEM	• 2008.12 • 2009.13

Application	Tested Versions
CMGL_IMEX	• 2008.11 • 2009.11
CMGL_STARS	• 2008.12 • 2009.11
DCV	• NICE DCV Server 2012.0-4557 on LSF compute hosts • RealVNC Visualization Edition (VE) 4.5.1 Viewer on user workstations
ECLIPSE	• 2009.1 • 2010
Exceed	• Exceed on Demand server 13.8 SP1 (Platform Application Center web server) • Exceed on Demand Client 13.8 SP1 **Important:** For Exceed application templates to work properly, JRE 1.7 or higher is required on the browser.
FLUENT	• 12.1.2 • 12.0.16 • 6.3.26
HMMER	• 3.0
LS-DYNA	• 971 • 970
MATLAB	• R2011a
NASTRAN	• MSC 2008
NWCHEM	• 6.0
RGS STAR-CCM+	• HP Remote Graphic Software 5.4.7/5.4.8 • 6.02

Download required Platform Application Center binaries

Download the IBM Platform Application Center(Platform Application Center) 9.1.1.0 package.

- If you have Platform Application Center Enterprise version, download IBM Platform Application Center Standard Edition.
- If you have Platform Application Center free version, download IBM Platform Application Center Basic Edition.

Upgrade requirements

Required installed Platform Application Center version

You must have installed Platform Application Center 8.0, 8.0.1, 8.0.2, 8.3, or 9.1.0.0

Download required Platform Application Center binaries

Download the IBM Platform Application Center(Platform Application Center) 9.1.1.0 package.

- If you have the Platform Application Center Enterprise version, download IBM Platform Application Center Standard Edition.
- If you have the Platform Application Center free version, download IBM Platform Application Center Basic Edition.

Synchronize times between LSF and Platform Application Center

The clock time on both the LSF master and the Platform Application Center web server must be the same. Ensure these times are synchronized.

Ensure the LSF LSB_SHAREDIR is accessible

Platform Application Center requires read access to the LSF `work` directory, defined in the LSF configuration file `$LSF_ENVDIR/lsf.conf` with the parameter LSB_SHAREDIR.

Configure LSF events for Platform Application Center

You need to configure LSF to log events so that Platform Application Center can retrieve job information.

1. Log on to the LSF master host as the LSF administrator.
2. Set the LSF environment.
3. Edit the `$LSF_ENVDIR/lsbatch/`*`cluster_name`*`/configdir/lsb.params` configuration file.
   a. Add the parameter `ALLOW_EVENT_TYPE` and define the following events.

      If you do not plan to use Standard reports, use the following configuration. These are the required events for the **Jobs** page in Platform Application Center to work properly:

```
ALLOW_EVENT_TYPE=JOB_NEW JOB_STATUS JOB_FINISH2 JOB_START JOB_EXECUTE JOB_EXT_MSG JOB_SIGNAL JOB_REQUEUE JOB_MODIFY2
JOB_SWITCH METRIC_LOG
```

      If you plan on using Standard reports, use the following configuration:

```
ALLOW_EVENT_TYPE=JOB_NEW JOB_START JOB_START_ACCEPT JOB_STATUS JOB_FORWARD \
MIG JOB_ACCEPT JOB_SWITCH JOB_FINISH JOB_MODIFY2 UNFULFILL JOB_SIGACT \
JOB_SIGNAL JOB_EXECUTE JOB_REQUEUE JOB_CLEAN JOB_EXCEPTION JOB_EXT_MSG \
JOB_ATTA_DATA JOB_CHUNK SBD_UNREPORTED_STATUS PRE_EXEC_START JOB_FORCE \
JOB_MOVE JOB_RUN_RUSAGE METRIC_LOG
```

   b. Enable event streaming by setting `ENABLE_EVENT_STREAM=Y`.

      Event streaming in your LSF cluster is required so that data can be loaded into the Platform Application Center database.

      Important: The LSF stream file name must be `lsb.stream` to work with Platform Application Center. This is the default name.

   c. Check whether the parameter LSB_QUERY_PORT is set in `lsf.conf`. If LSB_QUERY_PORT is set, then set `NEWJOB_REFRESH=Y` in `lsb.params`.

      This is required because when LSB_QUERY_PORT is set, newly submitted job information is not immediately available, and as a result, Platform Application Center is unable to display job details when a job is submitted.
4. Run **`badmin reconfig`** to reconfigure mbatchd.

Additional requirements for LSF 8.x only

Install the Fix Pack for LSF 8.0.1 and 8.3

Install the fix pack for LSF 8.0.1 and LSF 8.3.

- Fix pack for LSF 8.3:

  http://www.ibm.com/support/fixcentral/swg/selectFixes?parent=Platform+Computing&product=ibm/Other+software/Platform+LSF&release=All&platform=All&function=fixId&fixids=lsf-8.3-build209549&includeSupersedes=0

- Fix pack for LSF 8.0.1:

  http://www.ibm.com/support/fixcentral/swg/selectFixes?parent=Platform+Computing&product=ibm/Other+software/Platform+LSF&release=All&platform=All&function=fixId&fixids=lsf-8.0.1-build209240&includeSupersedes=0

Define how to manage the lsb.stream file for LSF 8.x

1. Log in as LSF administrator to the Platform Application Center web server.
2. Set your Platform Application Center environment:

   For example:

   - For **csh** or **tcsh**:

     ```
     % source /opt/pac/cshrc.platform
     ```

   - For **sh**, **ksh**, or **bash**:

     ```
     $ . /opt/pac/profile.platform
     ```

3. Edit the `$PERF_CONFDIR/dataloader/lsbevents.properties` file and set:

   ```
   AUTO_DELETE_STREAM_FILE=Y
   REMAINED_STREAM_FILE=10
   ```

   The number in REMAINED_STREAM_FILE represents the number of files and can be smaller or larger depending on your site requirements.

Chapter 4. Known Issues and Limitations

Category	Issue	Description
Application templates: CATIA	CATIA job does not display the Visualize icon and displays the message "Cannot open file" after upgrading Platform Application Center 8.3 to 9.1.1	This is caused by the fact that the file `CATIA.cmd` in 8.3 does not define ${CWD_OPT} in the **bsub** command. To fix this issue, edit the file `CATIA.cmd` in `$GUI_CONFDIR/application/draft/CATIA` or `$GUI_CONFDIR/application/published/CATIA` if your application is published, and add ${CWD_OPT} in JOB_RESULT to the bsub command. For example:`JOB_RESULT=`/bin/sh -c "bsub -B -N ${OUTPUT_FILE_LOCATION_OPT}` **`${CWD_OPT}`** `${JOB_NAME_OPT} ${COPY_FILE_OPT} ${RES_REQ_OPT} ${PRE_EXEC_OPT} ${POST_EXEC_OPT} start_catia.bat 2>&1 "``
DCV	A Linux DCV job does not run when a local operating system user's home directory is not `/home`	When the Platform Application Center web server and the DCV server are on different hosts, local operating system user accounts are used, and the user's home directory is not `/home`, Linux DCV jobs do not run. This is due to the fact that local operating system user accounts on a host are different user accounts, even though they may have the same name. Platform Application Center requires that a user's home directory and the job directory be shared and accessible to other users. Ensure local user home directories are shared to run a Linux DCV job.
Internet Explorer, Firefox	Platform Application Center host cannot have underscores in the host name	This is a known issue in Internet Explorer and Firefox. On Internet Explorer, setting cookies fails when the host name of the server contains underscores (_). This issue prevents users from logging in to Platform Application Center. On Firefox, this issue causes downloading and uploading files to fail. To work around the problem, change the host name to remove underscores or use the IP address to access the Platform Application Center server.
Internet Explorer 8 or 9 Compatibility View	Pages do not display properly with Internet Explorer 8 or 9 in Compatibility View	Pages do not display properly when using Internet Explorer 8 or 9 in Compatibility View. Workaround: 1. In Internet Explorer 8 or 9, select **Tools** > **Compatibility View Settings**. 2. In the dialog, make sure all these checkboxes are unchecked: • **Include updated website lists from Microsoft** • **Display intranet sites in Compatibility View** • **Display all websites in Compatibility View**

Category	Issue	Description
Jobs: job name	When the job name contains a forward slash "/" the job directory path is incorrect	For example, if the job name is `/tmp`, the job directory also becomes `/tmp` instead of the default `/home/user_name`. Workaround: Do not use a forward slash "/" in the job name. This is because the job name is used to name the job directory.
Jobs: job group	In the Jobs page, hovering the mouse on a striped state for a job group does not display the number of exited jobs	In the Jobs page, state column, hovering your mouse over a striped state for a job group does not indicate the number of exited jobs, even if there are exited jobs in the job group.
Jobs	File list display limitation	If a folder in a file list contains more than 4000 files or folders, can only can display a maximum of 4000 files in a file selection list.
Jobs: input files	Special characters in file names	Special characters single quote (`'`), double quote (`"`) and dollar sign ($) are not supported in file names. File management and file selection in Platform Application Center will not work properly for files with these characters in the file name.
Jobs: input files	When an input file contains include statements and the file is larger than 100 MB, Platform Application Center hangs	In **Jobs** > **Submission Forms**, when you add an input file with a size larger than 100 MB and it has include statements to other input files, Platform Application Center hangs. This is caused by a JVM memory overflow as the default setting is 64 MB. To increase the memory on the JVM: 1. In the **Java Control Panel**, select the **Java** tab and click the **View** button. The **Java Runtime Environment Settings** dialog is displayed. 2. In **Runtime Parameters**, change the value to at least 500 MB. For example: -Xmx500m
Jobs: input files	File upload from a browser on Windows 7 takes a long time	On Windows 7, it is recommended to tune Windows. From a command prompt, run this batch command as local administrator: `reg.exe ADD HKLM\SYSTEM\CurrentControlSet\services\AFD\Parameters /v DefaultSendWindow1 /t REG_DWORD /d 1640960 /f`
Job notifications	Job notification does not record status change from Exited to Pending	When job status changes from Exited to Pending the status change is not updated. For example, if you requeue an Exited job, status changes to Pending in LSF but the change is not displayed. When the job starts running, the status notification message changes to "Exited to Running". The Exited to Pending change is not shown.

Category	Issue	Description
Jobs: Safari browser	Included file names overlap in submission form	Applies only to Safari 5.1.7. In **Jobs** > **Submission Forms**, when a form has the **Use include files** field and you add include files, the include files name overlap.
Jobs: Safari browser	Selecting a job selects the whole window	Applies only to Safari 5.1.7. In **Jobs** > **Jobs** and **Jobs By State** pages, when you select a job, the whole window gets selected.
Jobs: Safari browser	Tooltip for job array status does not display correct information	Applies only to Safari 5.1.7. **Jobs** > **Job Data** > **By Job**, when you mouse over the job status in the Job Status column, the tooltip does not display for a job array.
Jobs: Safari browser	Filter rules do not display properly in the Jobs page	Applies only to Safari 5.1.7. In the Jobs page, when you click the ON button to display filter rules, the filter rules do not display properly.
LSF	Failed in an LSF library call: Internal library error when a job is submitted	This error occurs when a job is submitted through Platform Application Center. Platform Application Center uses the privileged ports 1 to 1024 to send requests to LSF. When too many requests are coming in to LSF at the same time, all ports are in use. As a result, LSF API calls fail and the library call message is displayed. To resolve this issue: 1. Log in as LSF administrator to any host in the cluster. 2. Edit the `lsf.conf` configuration file and set: `LSF_NON_PRIVILEGED_PORTS=Y` 3. Run **`badmin reconfig`** to reconfigure `mbatchd`.
LSF	When a job is submitted, Platform Application Center displays the message " Job submitted. Job details are temporarily unavailable"	This issue is caused when LSB_QUERY_PORT is set in `lsf.conf` and NEWJOB_REFRESH=N in `lsb.params`. Newly submitted job information is not immediately available, and as a result, Platform Application Center is unable to display job details when a job is submitted. 1. Log in as LSF administrator to any host in the cluster. 2. Edit the `lsb.params` configuration file and set: `NEWJOB_REFRESH=Y` 3. Run **`badmin reconfig`** to reconfigure `mbatchd`.
LSF	Cannot generate Service Level Agreement (SLA) reports	If LSF 8.0 is used with Platform Application Center, Service Level Agreement (SLA) reports for resource-based SLA cannot be generated. Only reports for time-based SLA can be generated.

Category	Issue	Description
Log files	/var/logs/messages has multiple lines added for each action in Platform Application Center	For each user request, an action will be logged in the operating system /var/logs/messages file. This causes the log file to increase in size very quickly. The workaround is to disable the system log for /bin/sh -c.
MySQL failover	After upgrading from Platform Application Center 8.0 to 9.1.1 and enabling failover and MySQL failover, cannot find the mysql service	When upgrading Platform Application Center 8.0 with failover to 9.1.1 and enabling MySQL failover, there is no `mysql` service displayed when services are displayed with the **`egosh service list`** command. This is due to the fact that the MySQL failover feature did not exist in Platform Application Center 8.0. Contact Technical Support for details on enabling MySQL failover in 9.1.1 in this situation.
MySQL	Jobs page is displaying with error message: Cannot convert value '2012-12-05 17:52:18.000000' from column 23 to TIMESTAMP	If you are using MySQL Server 5.6, the `driver mysql-connector-java-5.1.6.jar` does not work due to a bug inside the driver. This is mentioned as a bug fixed in the MySQL 5.1.7 JDBC Connector package: Connector/J failed to parse TIMESTAMP strings for nanos correctly. (Bug #39911) in http://dev.mysql.com/doc/refman/5.1/en/cj-news-5-1-7.html. Workaround: Download and install the MySQL 5.1.7 JDBC driver from: http://dev.mysql.com/downloads/connector/j/ .
Reports	Unable to produce or copy report to new custom report: Invalid report configuration file (Service Level Agreement(SLA)) message	Applies to MySQL and Oracle databases. In **Reports** > **Job Reports**, when a user selects the Service Level Agreement (SLA) report and clicks **Produce Report** or **Copy to New Custom Report**, the error message "Invalid report configuration file (Service Level Agreement(SLA)) is displayed.
Oracle, job groups, job arrays	Administrator user sees message "View restricted by Administrator" when attempting to view jobs in a job array or job group with Oracle database	Applies only to Oracle databases. The administrator is unable to view the jobs within a job array or job group from the **Jobs** page, **Jobs** subtab.
Oracle, DCV	When a DCV session is shared, filtering by user in the **Jobs** page displays "ORA-00933: SQL command not properly ended"	Applies only to Oracle databases. When a user shares his DCV session and another user attempts to view that user's job in the Jobs page by filtering by user, an error message is displayed and the user cannot view the job.
Online Help: Google Chrome	Search button wraps incorrectly in online help when using Google Chrome	When using Google Chrome, the online help Search button wraps incorrectly and is located below the search field.
Page display	Login dialog has layout issues and after login nothing is displayed or the navigation pane seems crumpled.	After logging in to Platform Application Center, nothing is displayed or the navigation pane seems crumpled. This issue is caused when Platform Application Center is upgraded from but the browser cache has not been cleared on user workstations. To resolve this problem, clear the cache of all browsers after a Platform Application Center upgrade.

Category	Issue	Description
VNC	VNC does not work after Platform Application Center uninstalled and reinstalled on the same host	If you install Platform Application Center and then for some reason uninstall and reinstall on the same host, VNC does not work. This is caused by the fact that the VNC server is still running. Manually clean up VNC processes after uninstalling Platform Application Center and before reinstalling.
VNC	Per-job remote Console is supported for shared disk installation only	For per-job remote consoles, Platform Application Center creates a VNC session file in `$GUI_WORKDIR`, which must be located a shared location (for example, `/opt/pac`). Platform Application Center cannot create a VNC session on compute nodes if `$GUI_WORKDIR` is a local directory. You must install Platform Application Center in a shared location enable failover to use the per-job remote consoles.
VNC	Cannot connect to server when opening a remote console	When a user tries to open a remote console through **Remote Consoles** > **Open my console**, a VNC console window is displayed, but cannot connect to the server. No VNC session is created on the master host. To work around the problem, check `$GUI_WORKDIR/.vnc` directory. Remove any `${user}` subdirectory for the user having a problem connecting. This will remove the VNC session file created in `$GUI_WORKDIR/.vnc/${user}`, and the user should be able to connect successfully.
VNC	Changing the window size does not take effect with **Session mode per user** in remote consoles when using VNC	In **Settings** > **Page Settings** under **Remote Consoles**, when you select **Session mode per user** and change the display size, it does not take effect, the display size is the same as before when using VNC. This situation arises when a user's VNC session already exists. Platform Application Center does not recreate the VNC session, it uses the existing one. To have display size changes take effect, clean up the VNC settings in the user's home directory and start a VNC session through Platform Application Center.
Web Services: `pacclient.py`	pacclient.py displays "@: Event not found." and "IOError" when the user password is "!@#In123"	When using **`pacclient.py`**, if your password has special characters, use a backslash (\)before specifying the password. For example, if your password is !@#In123, specify: `\!@#In123`

Category	Issue	Description

RGS	Linux run level 5 required for RGS jobs	LSF RGS jobs require run level 5 in order to use **startx** to start the RGS sender process. If the run level is not 5, the X-Windows server cannot start. Make sure the Linux run level on your system is set to 5 (the default may be 3 or some other value on your system).
		1. Edit /etc/inittab and modify the following:
		`# Default runlevel. The runlevels used by RHS are:`
		`# 0-halt (Do NOT set initdefault to this)`
		`# 1-Single user mode`
		`# 2-Multiuser, without NFS (The same as 3,`
		`# if you do not have networking)`
		`# 3-Full multiuser mode`
		`# 4-unused`
		`# 5-X11`
		`# 6-reboot (Do NOT set initdefault to this)`
		`#`
		`id:5:initdefault:`
		2. Reboot the machine to make the change take effect, or log on as root and start the X Server manually:
		`/sbin/init 5`

Process Manager	Job Flows Global View display limitation	In the **Job Flows** > **Global View**, there is a limit to the number of dependencies that can be displayed. If the number of dependencies is more than 48, the name will be missing on some items in the view. The issue appears only on Firefox 3.6 with Shockwave 10 Flash plug-in when the number of dependencies in the view is greater than 48.
Process Manager	Process Manager Job Templates are not supported	Platform Process Manager Job Templates are not supported in Platform Application Center. Use Platform Application Center application templates for job submissions to job flows.
Process Manager, X.509	Process Manager does not work when the user logs in through an X.509-enabled certificate: the message "Permission denied" is displayed and scripts are displayed	When a user uses X.509 authentication with Platform Application Center, the user is unable to access flows and Platform Process Manager related pages in Platform Application Center.

Chapter 5. Single sign-on with X.509 authentication

Platform Application Center supports client authentication with X.509 certificates, through the web browser and the Web Services API. The X.509 certificate is used to verify the identity of the Platform Application Center server when HTTPS is used from a browser. After the certificate is imported into the browser, authentication is done through X.509 and users are not prompted to log in to Platform Application Center.

X.509 with non self-signed certificates

Before you begin

Prepare server and user certificates and keys

About this task

If you have your own certificate authority to sign certificates, prepare the server and user certificates and keys.

Procedure

1. Create the server certificate and sign it.
2. Generate the user's keystore file with your site-specific information.

   Note:

   - CN must be the user's operating system user name on the Platform Application Center web server.
   - The storetype must be PKCS12, as this format is used by Platform Application Center.
   - The default keystore password on the Platform Application Center web server is `changeit`
   - If you are using a *.pfx file, you must convert the user certificate and keystore file for use by Platform Application Center. For example:

     ```
     openssl pkcs12 -in mycerts.pfx -out mycerts.pem
     openssl pkcs12 -export -in mycerts.pem -out mykeystore.p12
     ```

Configure the server for X.509 authentication

Step 1: Configure Tomcat for X.509

Procedure

1. Log in to the Platform Application Center web server as root.
2. Set your Platform Application Center environment.

   For example:

   - For **csh** or **tcsh**:

     ```
     # source /opt/pac/cshrc.platform
     ```

   - For **sh**, **ksh**, or **bash**:

     ```
     # . /opt/pac/profile.platform
     ```

3. Stop Platform Application Center.

   ```
   # pmcadmin stop
   ```

4. Edit $GUI_CONFDIR/server.xml and set the following attributes for <Connector port=.../> to the following values:
   - clientAuth="want"
   - algorithm="ibmX509"
   - sslProtocol="TLS"

   For example:

```
<Connector port="${CATALINA_START_PORT}" maxHttpHeaderSize="8192"</p><p>
           maxThreads="${CATALINA_MAX_THREADS}" minSpareThreads="25" maxSpareThreads="75"
           enableLookups="false" redirectPort="${CATALINA_HTTPS_START_PORT}" acceptCount="100"</i>
           sslProtocol="TLS" compression="on" compressionMinSize="2000" </i>
           clientAuth="want" algorithm="ibmX509"
           compressableMimeType="text/html,text/xml,text/css,text/javascript,text/plain" connectionTimeout="20000"
           disableUploadTimeout="true" URIEncoding="UTF-8"/>
```

   In <Connector port ..../>, check that the parameters keystoreFile, keystorePass, truststoreFile, and truststorePass are correct in your environment. If any of these attributes are not valid, the server-side certificate fails to authenticate. The user will not be able to log on to Platform Application Center. The following are the default values for Platform Application Center:
   - keystoreFile="/root/.keystore"
   - keystorePass="changeit"
   - truststoreFile="/opt/pac/jre/linux-x86_64/lib/security/cacerts"
   - truststorePass="changeit"

   Note: On PowerLinux™, the default value for truststoreFile is /opt/pac/jre/linux-ppc64/lib/security/cacerts
5. Start Platform Application Center.

```
# pmcadmin start
```

Step 2: Import certificates into Platform Application Center's trust store

Before you begin

You need server and user certificates and keys for this configuration. Refer to "Prepare server and user certificates and keys" on page 21 for more details.

Procedure

1. Log in to the Platform Application Center web server as root.
2. Set your JAVA_HOME to the JRE installed with Platform Application Center.

   For example:

```
setenv JAVA_HOME  /opt/pac/perf/jre/linux-x86_64
```

3. Import your Certificate Authority certificate into Platform Application Center's trust store.
   a. Import your Certificate Authority certificate.

      For example:

```
$JAVA_HOME/bin/keytool -delete -alias myca -keystore $PAC_TOP/jre/linux-x86_64/lib/security/cacerts

$JAVA_HOME/bin/keytool -import -v -storepass changeit -trustcacerts -alias myca -file /share/myCA/cacert.pem \
-keystore $PAC_TOP/jre/linux-x86_64/lib/security/cacerts
```

   b. Check that the certificate was applied by displaying the Certificate Authority certificate that is in the java trust store file.

```
JAVA_HOME/bin/keytool -list -keypass changeit -storepass changeit \
-keystore $PAC_TOP/jre/linux-x86_64/lib/security/cacerts | grep myca
```

4. Restart Platform Application Center.

```
# pmcadmin stop
# pmcadmin start
```

Configure the client for X.509 client authentication

Before you begin

You need user certificates and keys for this configuration.

- If you are using non self-signed certificates, refer to “Prepare server and user certificates and keys” on page 21 for more details.
- If you are using self-signed certificates, refer to “Prepare user certificates and keys” for more details.

Procedure

1. Import the user's keystore file into the user's browser on the client.

   The steps to import the user's keystore are different depending on the browser type:

   - Internet Explorer: Double-click the certificate file (for example, `my.p12`) to import it.
   - Mozilla Firefox: from the menu, select **Options** > **Options**, select **Advanced**, select the **Encryption** tab, click the button **View Certificates**, then click the button **Import**.
   - Google Chrome: Select the **Customize and control Google Chrome** icon, select **Settings**, click **Show Advanced Settings**, under **HTTPS/SSL**, click the button **Manage Certificates** and click the button **Import**.
2. Restart the browser.
3. Test connecting to Platform Application Center with the browser.

   Type in the Platform Application Center URL and use HTTPS. For example:

   ```
   https://hostA:8080/platform
   ```

   You should be able to view Platform Application Center pages without being prompted to log on.

X.509 with self-signed certificates

Before you begin

Prepare user certificates and keys

About this task

Before you configure the server or client for X.509 authentication, prepare the user certificates and keys. The following steps assume a self-signed certificate.

Procedure

1. Generate the user's keystore file with your site-specific information.

   Note:

   - CN must be the user's operating system user name on the Platform Application Center web server.
   - The storetype must be PKCS12, as used by Platform Application Center.
   - The default keystore password on the Platform Application Center web server is `changeit`

For example:

```
$JAVA_HOME/bin/keytool -genkey -v -alias myKey -keyalg RSA -storetype PKCS12 -keystore my.p12
-storepass changeit -keypass changeit -dname "CN=userA, OU=IBM Platform,
O=IBM Platform, L=Markham, ST=Ontario, C=CA" -validity 3650
```

2. Export the user certificate file from the keystore file that was created in the previous step.

   For example:

```
$JAVA_HOME/bin/keytool -export -alias myKey -file my.cert -keypass changeit
-storepass changeit -storetype PKCS12 -keystore my.p12
```

Note: If you are using a *.pfx file , you need to convert the user certificate and keystore file for use by Platform Application Center. For example:

```
openssl pkcs12 -in mycerts.pfx -out mycerts.pem
openssl pkcs12 -export -in mycerts.pem -out mykeystore.p12
```

Configure the server for X.509 authentication

Step 1: Configure Tomcat for X.509

Procedure

1. Log in to the Platform Application Center web server as root.
2. Set your Platform Application Center environment.

   For example:

   - For **csh** or **tcsh**:

     ```
     # source /opt/pac/cshrc.platform
     ```

   - For **sh**, **ksh**, or **bash**:

     ```
     # . /opt/pac/profile.platform
     ```

3. Stop Platform Application Center.

   ```
   # pmcadmin stop
   ```

4. Enable HTTPS.

   ```
   # pmcadmin https enable
   ```

5. Open `$GUI_CONFDIR/server.xml` and make sure these attributes for `<Connector port=.../>` are set to the following values:

   - `clientAuth="want"`
   - `algorithm="ibmX509"`
   - `sslProtocol="TLS"`

   For example:

```
<Connector port="${CATALINA_START_PORT}" maxHttpHeaderSize="8192"</p><p>
           maxThreads="${CATALINA_MAX_THREADS}" minSpareThreads="25" maxSpareThreads="75"
           enableLookups="false" redirectPort="${CATALINA_HTTPS_START_PORT}" acceptCount="100"</i>
           sslProtocol="TLS" compression="on" compressionMinSize="2000" </i>
           clientAuth="want" algorithm="ibmX509"
           compressableMimeType="text/html,text/xml,text/css,text/javascript,text/plain" connectionTimeout="20000"
           disableUploadTimeout="true" URIEncoding="UTF-8"/>
```

   In `<Connector port ..../>`, check that the parameters keystoreFile, keystorePass, truststoreFile, and truststorePass are correct in your environment. If any of these attributes are not valid, the server-side certificate fails to authenticate. The user will not be able to log on to Platform Application Center. The following are the default values for Platform Application Center:

   - `keystoreFile="/root/.keystore"`
   - `keystorePass="changeit"`
   - `truststoreFile="/opt/pac/jre/linux-x86_64/lib/security/cacerts"`

- `truststorePass="changeit"`

  Note: On PowerLinux, the default value for truststoreFile is `/opt/pac/jre/linux-ppc64/lib/security/cacerts`

6. Start Platform Application Center.

   ```
   # pmcadmin start
   ```

Step 2: Import user certificates into Platform Application Center's truststore

Before you begin

- You need user certificates and keys for this configuration. Refer to "Prepare user certificates and keys" on page 23 for more details.

Procedure

1. Log in to the Platform Application Center web server as root.
2. Set your JAVA_HOME to the JRE installed with Platform Application Center.

   For example:

   ```
   setenv JAVA_HOME  /opt/pac/perf/jre/linux-x86_64
   ```

3. Import the user's certificate into Platform Application Center's JRE keystore.

   Note:

   - The default password for the Platform Application Center truststore is changeit
   - You need to import each user's certificate into Platform Application Center's JRE keystore

   For example:

```
${JAVA_HOME}/bin/keytool -import -noprompt -trustcacerts -alias myKey -file my.cert
-keypass changeit -storepass changeit -keystore ${JAVA_HOME}/lib/security/cacerts
```

4. Restart Platform Application Center.

   ```
   # pmcadmin stop
   # pmcadmin start
   ```

Configure the client for X.509 client authentication

Before you begin

You need user certificates and keys for this configuration.

- If you are using non self-signed certificates, refer to "Prepare server and user certificates and keys" on page 21 for more details.
- If you are using self-signed certificates, refer to "Prepare user certificates and keys" on page 23 for more details.

Procedure

1. Import the user's keystore file into the user's browser on the client.

   The steps to import the user's keystore are different depending on the browser type:

   - Internet Explorer: Double-click the certificate file (for example, `my.p12`) to import it.
   - Mozilla Firefox: from the menu, select **Options** > **Options**, select **Advanced**, select the **Encryption** tab, click the button **View Certificates**, then click the button **Import**.

- Google Chrome: Select the **Customize and control Google Chrome** icon, select **Settings**, click **Show Advanced Settings**, under **HTTPS/SSL**, click the button **Manage Certificates** and click the button **Import**.

2. Restart the browser.
3. Test connecting to Platform Application Center with the browser.

   Type in the Platform Application Center URL and use HTTPS. For example:

   `https://hostA:8080/platform`

   You should be able to view Platform Application Center pages without being prompted to log on.

Using X.509 with Web Services

Convert user keys and certificates to PEM format for Python clients

Before you begin

You need user certificates and keys for this configuration.

- If you are using non self-signed certificates, refer to "Prepare server and user certificates and keys" on page 21 for more details.
- If you are using self-signed certificates, refer to "Prepare user certificates and keys" on page 23 for more details.

About this task

Python supports certificates and keys only in PEM format. If you will be using a Python client to connect to Platform Application Center, or `pacclient.py`, you need to convert your key and certificate files to PEM format.

Procedure

1. Convert your user key and certificate files to PEM format.
   a. Get the `.key.pem` file.

      For example:

      ```
      openssl pkcs12 -nocerts -in my.p12 -out .key.pem
      ```

   b. Get the `.cert.pem` file.

      For example:

      ```
      openssl pkcs12 -clcerts -nokeys -in my.p12 -out .cert.pem
      ```

   c. Remove the passphrase from the key.

      For example:

      ```
      openssl rsa -in .key.pem -out key_nopass.pem
      mv key_nopass.pem .key.pem
      ```

2. Copy the `.key.pem` and `.cert.pem` files to the same directory as your client program.

Test that X.509 works with Web Services

Before you begin

You will need to complete the following steps before you can test X.509 with Web Services.

1. You need user certificates and keys for this configuration.

- If you are using non self-signed certificates, refer to “Prepare server and user certificates and keys” on page 21 for more details.
- If you are using self-signed certificates, refer to “Prepare user certificates and keys” on page 23 for more details.

2. Convert your key and certificate files to PEM format. Python supports certificates and keys only in PEM format. For more information, refer to “Convert user keys and certificates to PEM format for Python clients” on page 26.
3. Configure your server and import client certificates into Platform Application Center's truststore.
   - If you are using non self-signed certificates, refer to “Step 1: Configure Tomcat for X.509” on page 21 and “Step 2: Import certificates into Platform Application Center's trust store” on page 22for more details.
   - If you are using self-signed certificates, refer to “Step 1: Configure Tomcat for X.509” on page 24 and “Step 2: Import user certificates into Platform Application Center's truststore” on page 25for more details.

About this task

You can use the example Python `pacclient.py` and `pac_api.py` to test X.509 connection to Platform Application Center with Web Services.

Procedure

1. Copy files from the Platform Application Center web server host to your client host, replacing `/opt/pac` with the directory in which you installed Platform Application Center.

   From `/opt/pac/gui/3.0/bin`, copy the following to your client host:

   - `pacclient.py`
   - `pac_api.py`

2. Copy the user's `.key.pem` and `.cert.pem` to the same directory as pacclient.py and pac_api.py.
3. On your client host, modify `pac_api.py` to avoid logon by adding the `http.add_certificate` line.

   For example:

```
def getJobListInfo(parameter):
        #url, token = getToken()
        url = 'https://ib05b01:8080/'
        token = ''
        x509Flag, keypemfile, certpemfile = checkX509PEMCert(url)

        if ( (x509Flag == False) & (len(token) <= 0) ):
                print "You must log on to PAC. To log on, run pacclient logon."
                return

        http = httplib2.Http()
        #if ( (x509Flag == True) & (len(token) <= 0) ):
                # X509Flag is True and token is empty, then add the key/cert files into http request.
        #       http.add_certificate(keypemfile, certpemfile, '')

        http.add_certificate('.key.pem', '.cert.pem', '')
```

4. Go to the directory in which `pacclient.py` is located and test the Python client by running `pacclient.py job`.

   There should not be any prompt to log on.

   For example:

```
./pacclient.py jobJOBID   STATUS   EXTERNAL_STATUS   JOB_NAME   COMMAND
       12183   Running       -            *037934810  sleep 1234444
```

Modify your client program to authenticate with X.509

The following are examples of how to modify your client code to connect to Platform Application Center and authenticate with X.509. The following examples assume that you have made the necessary configurations on the Platform Application Center web server.

Python client code example

Python supports only certificates and keys in PEM format. You must convert your key and certificate files to PEM format. For more information, refer to "Convert user keys and certificates to PEM format for Python clients" on page 26

Use the httplib2 function and add_certificate to use the key and certificate files for authentication.

For example:

```
http = httplib2.Http()
http.add_certificate('C:/workplace/.key.pem','C:/workplace/.cert.pem', '')
response, content = http.request('https://www.example.com/', 'GET',
body=body, headers=headers)
```

Java client code example

Use the Java API to send https requests for X.509 authentication. Notice that the keystore must be PKCS12 and the URL must specify https.

Example for HttpClient version 4.x:

```
// read in the keystore from the filesystem, this should contain a single keypair
KeyStore clientKeyStore = KeyStore.getInstance("PKCS12");
clientKeyStore.load(new FileInputStream(KEYSTORE_LOCATION), KEYSTORE_PASS.toCharArray());

// set up the socketfactory, to use our keystore for client authentication.
SSLSocketFactory socketFactory = new SSLSocketFactory(
  SSLSocketFactory.SSL,
  clientKeyStore,
  KEYSTORE_PASS,
  null,
  null,
  null,
  (X509HostnameVerifier) SSLSocketFactory.ALLOW_ALL_HOSTNAME_VERIFIER);

// create and configure scheme registry
SchemeRegistry registry = new SchemeRegistry();
registry.register(new Scheme("https", 8443, socketFactory));

// create a client connection manager to use in creating httpclient
ThreadSafeClientConnManager manager = new ThreadSafeClientConnManager(registry);

// create the client based on the manager, and use it to make the call
HttpClient httpClient = new DefaultHttpClient(manager);

// create the method to execute
HttpPost m = new HttpPost ("https://www.example.com/");

// execute the method
HttpResponse response = httpClient.execute(m);
```

Example for HttpClient version 3.x:

```
Example of using custom protocol socket factory for a specific host:
     Protocol authhttps = new Protocol("https",
          new AuthSSLProtocolSocketFactory(
              new URL("file:my.keystore"), "mypassword",
              new URL("file:my.truststore"), "mypassword"), 443);

     HttpClient client = new HttpClient();
     client.getHostConfiguration().setHost("localhost", 443, authhttps);
     // use relative url only
     GetMethod httpget = new GetMethod("/");
     client.executeMethod(httpget);

Example of using custom protocol socket factory per default instead of the standard one:
     Protocol authhttps = new Protocol("https",
          new AuthSSLProtocolSocketFactory(
              new URL("file:my.keystore"), "mypassword",
              new URL("file:my.truststore"), "mypassword"), 443);
     Protocol.registerProtocol("https", authhttps);

     HttpClient client = new HttpClient();
     GetMethod httpget = new GetMethod("https://localhost/");
     client.executeMethod(httpget);
```

Perl client code example

Use the Perl API to send https requests for X.509 client authentication.

You need the Crypt::SSLeay package. You can download it from: http://search.cpan.org/dist/Crypt-SSLeay/. This package supports the HTTPS protocol under LWP and allows an LWP::UserAgent object to use GET, HEAD, and POST requests.

For example:

```
use LWP::UserAgent;

# Client certificate with PEM format
$ENV{HTTPS_CERT_FILE} = 'cert.pem';
$ENV{HTTPS_KEY_FILE}  = 'keynopass.pem';
###################################
# Or Client certificate with PKCS12 format
$ENV{HTTPS_PKCS12_FILE}     = 'pkcs12.p12';
$ENV{HTTPS_PKCS12_PASSWORD} = 'PKCS12_PASSWORD';

my $ua  = LWP::UserAgent->new;
my $response = $ua->get('https://www.example.com/');
```

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Intellectual Property Law
Mail Station P300
2455 South Road,
Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application

programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

LSF, Platform, and Platform Computing are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Printed in USA

GI13-1890-02