Appendix A: Troubleshooting

This appendix offers troubleshooting steps to help solve common problems while using Prime Central. Refer to the troubleshooting procedures in this appendix before contacting the Cisco Technical Assistance Center (TAC) at http://www.cisco.com/tac.

This section contains the following topics:

Troubleshooting the Prime Central Integration Layer

Log files contain detailed information about request processing and exceptions and are your best diagnostic tool for troubleshooting the Prime Central integration layer.

Prime Central integration layer files are located in the following directory: *primeusr-home-directory*/esb_<*ID*> (~/esb_<*ID*> if you are logged in as primeusr).

- servicemix.log—Most recent log file.
- servicemix.log.1—Second oldest log file.
- servicemix.log.2—Third oldest log file.

Prime Central integration layer logger properties are located in ~/esb_<*ID*>/etc/org.ops4j.pax.logging.cfg. Useful properties include:

- log4j.appender.out.maxFileSize=10MB—Size of each servicemix.log file.
- log4j.appender.out.maxBackupIndex=10—Maximum number of log files. The oldest file has index 10; for example, servicemix.log.10.

The file also identifies the class package and log level to log; for example, log4j.logger.com.cisco.prime=DEBUG.

The Prime Central integration layer control script itgctl saves configuration and log information in ~/esb_<*ID*>/diagnostics/diagnostics.[*YYYYMMDDHHMMSS*].tar.gz.

Problem The Prime Central integration layer is not running.

Solution Use the **itgctl status** command to check the status of the Prime Central integration layer.

Problem The Prime Central configuration changed, but the Prime Central integration layer does not retrieve the changes.

Appendix A: Troubleshooting

Solution The Prime Central integration layer must be restarted before it can retrieve the following types of Prime Central configuration changes:

- Modifications to the applications.
- A new application registers with Prime Central.
- An existing application is removed from Prime Central.
- The Prime Central *suiteadmin* user credentials change.

Enter the following commands to restart the Prime Central integration layer:

```
itgctl stop
itgctl start
```

Problem An application or the Prime Central integration layer is shown as Unavailable or is missing from the Suite Monitoring or User Management portlets.

Solution Review the Prime Central integration layer log files for Central Authentication Service (CAS) exceptions or application connection problems. If you find CAS exceptions, enter the following commands to restart the Prime Central integration layer:

```
itgctl stop
itgctl start
```

Problem The Prime Central integration layer log files report any of the following problems:

- CAS unavailable
- Authentication unavailable
- Unable to establish session to domain managers

Solution All Prime Central components use CAS for authentication services. The CAS server runs on the Prime Central portal. If you encounter CAS problems, verify that the Prime Central portal is up and running. Then, check the connectivity between the application server and the Prime Central portal. Finally, restart the Prime Central integration layer.

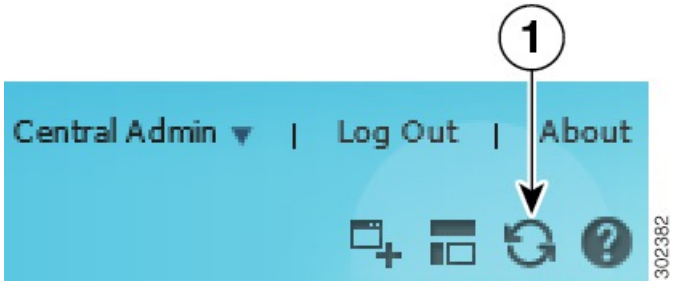
Problem An application times out or is unavailable. The log file reports an aggregation timeout for requests.

Solution For the first startup, use ping or tracert to verify routing to the application. Then, improve application performance. Finally, increase the Prime Central integration layer request aggregation timeout value.

Problem If you are using the User Management portlet while an application is brought up or down in Prime Central, you might receive Prime Central integration layer timeout errors.

Solution On the Prime Central home page, click the **Refresh Current Page** icon (see the following figure).

Figure 1: Home Page > Refresh Current Page Icon



Problem When you use the **itgctl stop** command to stop the integration layer, the following error message is generated:

```
Stop Prime Central - Integration Layer..... Warning: Karaf process can not be killed, may
need to remove the process manually.. Done
```

Solution As the primeusr user, enter the following command to kill the Apache Karaf process manually:

```
ps -ef | grep karaf | grep -v grep | cut -f2 -d' ' | xargs kill -9
```

Problem You want to determine the role and profile associated with every integration layer instance that resides on a host.

Solution Enter the following command:

```
itgctl list
```

Problem After upgrading to Prime Central 1.5.2 and running the **itgctl status** command, Prime Central indicates that the Integration Layer's status is `UP`, even though the Suite Monitoring portlet indicates that the Integration Layer's status is `DOWN`.

Solution Do the following:

1. Log in to Prime Central as the root user.
2. Go to the /etc/security directory and open the limits.conf file.
3. Verify that the following values are set. If not, make the necessary changes and save the file:

   - primeusr soft nofile—51200
   - primeusr hard nofile—65536
   - primeusr soft nproc—204800
   - primeusr hard nproc—204800
   - oracle soft nproc—51200
   - oracle hard nproc—51200
   - oracle soft nofile—30720
   - oracle hard nofile—65536
   - oracle soft stack—10240
   - hard memlock—4831838208
   - soft memlock—4831838208

Problem After upgrading to Prime Central 1.5.2, the Suite Monitoring portlet sometimes displays the integration layer's status as `Down` even though it has been started.

Solution The problem was observed on a server with the following applications and components installed:

- Prime Central 1.2 with a local embedded database
- Prime Central Fault Management 1.2
- Cisco Prime applications that are part of the Prime Carrier Management August 2013 release (Prime Network 4.0, Prime Optical 9.8, Prime Provisioning 6.5, and Prime Performance Manager 1.4)

After populating these applications with network data, complete the upgrade to Prime Central 1.5.2. Then, with Prime Central running, open the Suite Monitoring portlet and it indicates that the status for the integration layer, as well as the Prime applications, is `Down`.

To correct the problem, restart the integration layer by running the following commands:

- **itgctl stop**
- **itgctl start**

Problem In Suite Monitoring portlet, an application or the Prime Central integration layer Status is shown as `DOWN` intermittently.

Solution Prime Central Integration layer uses a predefined timeout period of 5 seconds for processing all the ping responses from connected DMs. If there are any network delays or resource issues, Suite Monitoring DM's status may show as `Down` for a short period.

To increase timeout value, do the following:

1. Log in as **primeusr**.
2. Uncomment **pingAggrTimeout** property in the below file and change to an appropriate value, which should be < 30000:

   $PRIMEHOME/esb_<ID>/etc/`com.cisco.prime.esb.system.cfg`

   For example : pingAggrTimeout=25000
3. Uncomment **pingTimeout** property in the below files and change to an appropriate value, which should be < 30000:

   $PRIMEHOME/esb_<ID>/etc/`com.cisco.prime.esb.ppm.cfg`

   $PRIMEHOME/esb_<ID>/etc/`com.cisco.prime.esb.ffusr.cfg`

   $PRIMEHOME/esb_<ID>/etc/`com.cisco.prime.esb.fmusr.cfg`

   $PRIMEHOME/esb_<ID>/etc/`com.cisco.prime.esb.agora.cfg`

   For example : pingTimeout=25000

Troubleshooting the Prime Central Portal

The Prime Central portal features single-sign on (SSO), meaning that when you log in to the portal, you do not have to log in separately to each application within your domain.

Log files contain detailed information about request processing and exceptions and are your best diagnostic tool for SSO troubleshooting.

SSO files are located in $XMP_HOME, which is *primeusr-home-directory*/XMP_Platform/cas.log. The log files increment with age:

- cas.log—Most recent log file.
- cas.log.1—Second oldest log file.
- cas.log.2—Third oldest log file.

Appendix A: Troubleshooting

SSO logger properties are located in $XMP_HOME/tomcat-7.0.23/webapps/SSO/WEB-INF/classes/log4j.xml. Useful properties include:

```
<appender name="cas" class="org.apache.log4j.RollingFileAppender">
    <param name="File" value="cas.log" />
    <param name="MaxFileSize" value="512KB" /> - Size of each cas.log file
    <param name="MaxBackupIndex" value="3" /> - Max number of log files
</appender>

<logger name="org.jasig" additivity="true">
    <level value="ERROR" /> - File also identifies the packages of classes to log and what
    log level
    <appender-ref ref="cas" />
</logger>
```

Problem On Internet Explorer, portlets might spin without opening. This problem occurs occasionally when you:

- Clear your browser cache and reload the entire application.
- Log in to Prime Central immediately after clearing your browser cache.

Solution On the Prime Central home page, click the **Refresh Current Page** icon (refer to this Figure 1: Home Page > Refresh Current Page Icon).

Problem After logging in to the Prime Central portal, menu options are missing.

Solution Do the following:

1. Log out of the Prime Central portal.
2. Clear your browser cache.
3. Open your default browser and log back in to the Prime Central portal.

Problem After updating the email address or phone number in the My Account portlet, there is no confirmation message.

Solution Do the following:

1. From the Prime Central menu, choose **Administration > User and Privilege Management > Users**. The User Management portlet opens.
2. Refresh the page.
3. Select the user with the updated email address or phone number and click **Edit**.
4. Verify the updated email address or phone number.

Problem A device is missing from the Common Inventory portlet.

Solution Do the following:

1. Verify that all Prime Central components are operational:
    1. Log in to Prime Central and choose **Administration > System > Suite Monitoring**.
    2. In the Suite Monitoring portlet, click the **Prime Central** tab and verify that the Prime Central integration layer status is Up.
    3. Click the **Applications** tab and verify that the application status is Up.

Appendix A: Troubleshooting

2. Check the device inventory when logged in as the centraladmin user:
    1. Log in to Prime Central as the centraladmin user.
    2. If the Common Inventory device table shows “No data available,” and if an attempt has already been made to synchronize the inventory, skip to Step 4.
3. If the centraladmin user can see the missing device but another user cannot, you must assign device scopes or NEs to that user:
    1. See the application documentation for details:
        - Prime Network—See "Creating New Device Scopes to Control Device Access" in the Cisco Prime Network Administrator Guide, Chapter 6, "Controlling Device Access and Authorization Using Device Scopes."
        - Prime Optical—See "Modifying a Prime Optical User's Properties" in the Cisco Prime Optical User Guide, Chapter 8, "Managing Security."
    2. After the device scope change persists on the application, you must synchronize the scope data. In the Common Inventory device table, click the **Synchronize** icon. Click the **Scope** radio button; then, click **Sync Now**. Wait for at least 15 minutes.
4. If the device is still missing from the Common Inventory device table, verify that the device exists on the source application:
    1. Log in to Prime Central as the centraladmin user.
    2. Choose **Administration > Discovery/Adding Devices > Prime Network** or **Prime Optical**.
    3. If the device is present, verify that its status is In Service or Up and it has been discovered by the application. If the device was added recently, wait for at least 15 minutes for it to be discovered.
    4. If the device is not present, add it on the application. Wait for it to be discovered and In Service (Prime Optical) or Available/Up (Prime Network).
5. When the device is discovered by the individual applications, synchronize the device inventory:
    1. Log in to Prime Central as the centraladmin user.
    2. In the Common Inventory device table, click the **Synchronize** icon.
    3. Click the **Inventory and Scope** radio button.
    4. Click **Sync Now**.
6. If the device is still missing from the Common Inventory portlet:
    1. Enter the following command to log in to the Prime Central shell:

        ```
        ssh -l primeusr prime-central-server
        ```
    2. Change directories to the $XMP_HOME directory and enter the following commands:

        ```
        tar -czvf common_inv_logs.tar.gz common_inventory.log
        /opt/primecentral/apache-servicemix-4.4.1-fuse-00-08/data/log/servicemix.log
        ```
    3. Send the log files to the Cisco TAC.

Problem If you are using Internet Explorer, when you zoom in or out to less than or greater than 100% screen resolution, the User Management and Common Inventory filters become blurry. This problem occurs only when you use the Filter option; no other views in either portlet blur when you zoom in or out.

Solution In Internet Explorer, do not zoom in or out when filtering data in the User Management and Common Inventory portlets. Alternately, use Firefox to launch Prime Central.

Problem In the My Account portlet and Add User wizard, if you change your password to include a trailing space at the end, Prime Central removes the last space character automatically. The next time you log in to Prime Central with the password that includes the trailing space, your password is denied.

Solution When creating a password, do not include a trailing space at the end.

Problem After you log in to the Prime Central portal, the login progress icon spins indefinitely or you see the "CAS is Unavailable" error message.

Solution Restart the Prime Central portal.

Problem After adding a QvPC device in Prime Network, if you are unable to view associated Virtual Machine, Hypervisor Data for the virtual cards of this device in Prime Central Common Inventory portlet.

Solution Do the following:

1. From the Prime Central menu, choose **Assure > Services > Data Center**. The Data Center page opens.
2. Click the **Compute**, **Network**, or **Storage** tab.
3. Click the **Synchronize** icon.

Note Only administrators can see the Synchronize icon, which is hidden for all other users.

4. In the Synchronize dialog box, do the following:
    1. Click the **Scope and Logical Inventory** radio button.
    2. Click **Sync Now**.
5. In the Common Inventory device table, click the **Synchronize** icon. Click the **Scopes and Inventory** radio button; click **Synchronize all data** radio button, then, click **Sync Now**. Wait for the Synchronization to complete.

Problem: Not able to switch to BulkUser, facing permission denied issue.

Solution: Use the **#userdel bulkuser** command to delete the BulkUser manually and then follow the steps that are mentioned in the Creating a Bulk User

Troubleshooting Prime Central Security

Problem False positives are indicated during a scan for security vulnerabilities.

Solution Prime Central components communicate over a highly secure message bus using the secure socket layer (SSL), a strong encryption algorithm, and two-way, certificate-based authentication. We recommend that you work with Cisco TAC to verify whether any found issues require further attention.

Troubleshooting Prime Network

Problem After registering with Prime Central, Prime Network is shown in the Suite Monitoring portlet > Applications tab, but its state is Down.

Solution Do the following:

1. Verify that the Prime Central integration layer configuration has been generated for Prime Network. Make sure the com.cisco.prime.esb.ana.cfg file has valid values for anaComURI and anaPtpServer.
2. Verify that the Prime Network gateway is up and accepting connections (BQL).
3. Check the servicemix.log file and capture any ana-bnd exceptions.
4. To bypass CAS authentication, configure anaPtpUser and anaPtpPw in com.cisco.prime.esb.ana.cfg.
5. Look for deserialization errors caused by a version mismatch between Prime Network and the Prime Central integration layer.
6. To troubleshoot transformation issues, look for the JMS queue name in the format DM_*operation-name*_net://net:*XXX*.

Troubleshooting Prime Optical

Problem After registering with Prime Central, Prime Optical is not shown in the Suite Monitoring portlet > Applications tab.

Solution Do the following:

1. Check the DMIntegrator.log file to see if the Prime Optical registration failed or succeeded.
2. Check if an incorrect hostname was entered for the Prime Central database during the Prime Optical registration. In the DMIntegrator.log file, check the value of the [SERVER:] property, which should be the hostname of the server where the Prime Optical database is installed.

Problem After registering with Prime Central, Prime Optical is shown in the Suite Monitoring portlet > Applications tab, but its state is Down.

Solution Do the following:

1. If the Prime Optical server did not start, log in to the Prime Optical workstation as the root user and enter the **opticalctl status** command. The output should show the CTM Server, SMService, and CORBAGWService services. If those services are not running, enter the **opticalctl start** command to start them.
2. As the primeusr UNIX OS user, log in to the Prime Central workstation and enter the **itgctl restart** command to reconfigure the Prime Central integration layer.
3. Wait for some time; then, check if the Prime Optical state changes to Up in the Suite Monitoring portlet > Applications tab.

If the problem persists, do the following:

1. Verify that the Prime Central integration layer configuration has been generated for Prime Optical. In the com.cisco.prime.esb.ctm.cfg file, make sure the file has valid values for ctmComURI ctmCorbaServer. If not, restart the Prime Central integration layer to configure Prime Optical.

Appendix A: Troubleshooting

2. On the Prime Optical server, enter the command **showctm -v** to see if the CORBAGWService is up.
3. Check the servicemix.log file and capture any ctm-bnd exceptions. If you see CAS exceptions, verify that the Prime Central portal is up and running. Then, check the connectivity between the application server and the Prime Central portal. Finally, restart the Prime Central integration layer.
4. See the Cisco Prime Optical 10.6 User Guide to create the GateWay/CORBA User on Prime Optical. Use ctmCorbaUser=*gateway-corba-user* and ctmCorbaPw=*gateway-corba-user-password* in the com.cisco.prime.esb.ctm.cfg file. Restart the Prime Central integration layer.

Problem Prime Optical is shown as Up in the Suite Monitoring portlet > Applications tab, but the menu options to launch Prime Optical are missing.

Solution Do the following:

1. In the User Management portlet, check whether the user has Prime Optical in his application access privileges.
2. If necessary, edit the user and check the **Grant Access to Prime Optical** check box in the Application Access Privilege screen.

Problem Cannot cross-launch Prime Optical from Prime Central.

Solution Do the following:

1. Verify that the Prime Optical server is up and running. As the root user, log in to the Prime Optical workstation and enter the **opticalctl status** command. The output should show the CTM Server, SMService, and Apache Web Server services, which are required to cross-launch Prime Optical from Prime Central.
2. The Prime Optical client is launched through Oracle Java Web Start technology. Verify that JRE 1.6 is installed on the client workstation, and that JNLP files are opened with Java Web Start.
3. When the Prime Optical client is launched for the first time on the client workstation, the client is downloaded, installed, and launched. Consequently, the first launch might take several minutes. If the client launches too slowly, the first opening might fail. Retry the cross-launch.
4. If the client is downloaded and launched, but closes without any messages, collect the Cisco/PrimeOptical_96/debug/CTMC-debug*.log files from the client workstation and contact the Cisco TAC.

Problem You receive an “Unable to connect” error when you try to cross-launch Prime Optical from the Prime Central portal or from Prime Network Vision.

Solution Send an update command through the browser by entering the following URL:

http://*portal-server:portal-http-port***/cxl/jnlpupdate?dm=***COM-URI*

where:

- *portal-server* is the hostname of the Prime Central portal host.
- *portal-http-port* is the portal port number.
- *COM-URI* is the Prime Optical identifier and can be found in the Prime Central Suite Monitoring portlet.

For example, if the Prime Central portal is running on the “prime_portal” host on port 8443 and the identifier for Prime Optical is 4, enter:

```
http://prime_portal:8443/cxl/jnlpupdate?dm=opt://opt:4
```

Troubleshooting Prime Performance Manager

Problem After registering with Prime Central, Prime Performance Manager is not shown in the Suite Monitoring portlet > Applications tab.

Solution Do the following:

1. On the Prime Performance Manager server, check the /opt/CSCOppm-gw/prime-integrator/DMIntegrator.log file to see if the Prime Performance Manager registration failed or succeeded.
2. Check if an incorrect hostname was entered for the Prime Central database during the Prime Performance Manager registration. In the DMIntegrator.log file, check the value of the [SERVER:] property, which should be the hostname of the server where the Prime Central database is installed.
3. If incorrect Prime Central database information was entered, re-enter the **/opt/CSCOppm-gw/bin/ppm primecentralintegration** command on the Prime Performance Manager gateway server. Use the correct database information.
4. If a previous incorrect instance of Prime Performance Manager exists in the Suite Monitoring portlet, do the following:
    1. In the Suite Monitoring portlet, click the **Applications** tab.
    2. Click the **Prime Performance Manager** radio button.
    3. Click **Delete**.
    4. After Prime Performance Manager has been removed from Prime Central, enter the **/opt/CSCOppm-gw/bin/ppm primecentralintegration** command on the Prime Performance Manager gateway server.

Problem After registering with Prime Central, Prime Performance Manager is shown in the Suite Monitoring portlet > Applications tab, but its state is Down.

Solution Do the following:

1. Restart Prime Performance Manager to complete the Prime Central registration. As the root user, log in to the Prime Performance Manager gateway server and enter the **/opt/CSCOppm-gw/bin/ppm restart** command. Log in to the Prime Performance Manager unit workstations and enter the **/opt/CSCOppm-unit/bin/ppm restart** command. Enter the **ppm status** command to check the operational status of Prime Performance Manager.
2. As the primeusr UNIX OS user, log in to the Prime Central workstation and enter the **itgctl restart** command to reconfigure the Prime Central integration layer.
3. Wait for some time; then, check if the Prime Performance Manager state changes to Up in the Suite Monitoring portlet > Applications tab.

Problem Prime Performance Manager is shown as Up in the Suite Monitoring portlet > Applications tab, but the menu options to launch Prime Performance Manager are missing.

Solution Do the following:

1. In the User Management portlet, check whether the user has Prime Performance Manager in the application access privileges.

2. If necessary, edit the user and check the **Grant Access to Prime Performance Manager** check box in the Application Access Privilege area.

Problem Cannot cross-launch Prime Performance Manager from Prime Central.

Solution Do the following:

1. Verify that the Prime Performance Manager gateway server is up and running. As the root user, log in to the Prime Performance Manager server and enter the **ppm status** command. All services should be running. If not, enter the **ppm restart** command to restart Prime Performance Manager.
2. If the problem persists, enter the **ppm tac** command on the Prime Performance Manager gateway server to collect the debug files. Then, contact the Cisco TAC.

Troubleshooting Prime Provisioning

Problem After logging in to Prime Central, if you click the **Add Portlets** icon and add the Device SR Count or SR Summary portlets, a Prime Provisioning login screen might appear. Because you are already logged in to Prime Central, you should not be prompted to log in a second time.

Solution This problem occurs when a user does not have the Application Access Privilege set to Prime Provisioning. The user can click the Add Portlets icon and add the Device SR Count or SR Summary portlets, at which point the Prime Provisioning login screen appears.

To give the user access to Prime Provisioning, do the following:

1. From the Prime Central menu, choose **Administration > User and Privilege Management > Users**.
2. In the User Management portlet, select the user that you want to edit and click **Edit**.
3. In the Enter User Info screen, click **Next**.
4. In the Application Access Privilege area, make sure the **Grant Access to Prime Provisioning** check box is checked. Click **Next**.
5. In the Assign Groups & Group Roles screen, click **Next**.
6. In the Assign Additional Individual User Roles screen > Prime Central tab, make sure the **Administrator** check box is checked. In the Prime Provisioning tab, click the desired radio button. Click **Next**.
7. In the Summary screen, click **Finished**. The updated user is displayed in the Users tab. When that user opens the Device SR Count or SR Summary portlets, he is not prompted to log in a second time.

Problem After registering with Prime Central, Prime Provisioning is shown in the Suite Monitoring portlet > Applications tab, but its state is Down.

Solution Do the following:

1. Use the **./prime.sh** command to check the list of running servers and verify that all services have started:

```
Name                State           Gen   Exec Time                Success  Missed
nspoller            started         1     Dec 16 01:55:08 EST      817      0
dbpoller            started         1     Dec 16 01:55:08 EST      824      0
httpd               started         1     Dec 16 01:55:13 EST      829      0
rgserver            started         1     Dec 16 01:55:58 EST      817      0
cnsserver           started         1     Dec 16 01:55:13 EST      823      0
```

2. If some services have stopped, enter the following commands to stop and restart them:

./prime.sh stopall

./prime.sh start

3. If the problem persists, check the log file in *Prime-Provisioning-installation-directory*/tmp.

Troubleshooting Prime Fault Management

Problem The Alarm Browser portlet displays the error "The application failed to run."

Solution To open the Alarm Browser portlet, you must accept the self-signed, untrusted security certificates. In the Warning - Security dialog box, if you click **No** to the following message, the security certificate is denied, and the Alarm Browser displays the error "The application failed to run":

```
This web site's certificate cannot be verified. Do you want to continue?
```

Depending on your browser, do one of the following to resolve the error:

Mozilla Firefox

1. Log out of the Prime Central portal.
2. Clear your browser cache.
3. Choose **Tools** > **Options** and click the **Advanced** panel.
4. Click the **Encryption** tab.
5. Click **View Certificates**. The Certificate Manager dialog box opens.
6. Click the **Servers** tab and delete the certificate for the Fault Management server (with port 16311).
7. At the confirmation prompt, click **OK**.
8. Click **OK** to close the Certificate Manager dialog box.

Microsoft Internet Explorer

1. Log out of the Prime Central portal.
2. Log back in to the Prime Central portal and accept the self-signed, untrusted security certificates.

Problem The Alarm Browser does not show alarms for a supported application, even though the application is shown as Up in the Suite Monitoring portlet > Applications tab.

Solution If an application is registered with Prime Central but is not up and running when Prime Central Fault Management is installed, you must manually register with the application if you want to receive alarms immediately. (Within 10 minutes of the Prime Central Fault Management installation, an automatic cron job starts alarm retrieval.)

To bypass the 10-minute waiting period and begin receiving alarms immediately, do the following:

1. As the primeusr user, log in to the Prime Central Fault Management server.
2. After the application is registered with Prime Central, go to the *installation-directory*/prime_integrator/scripts folder and enter:

   ./DMRegistration.sh

Problem The Alarm Browser does not show alarms for Prime Performance Manager, even though the application is shown as Up in the Suite Monitoring portlet > Applications tab.

Solution If Prime Performance Manager is supposed to send alarms directly to Prime Central Fault Management, make sure an upstream OSS host is configured correctly in the Prime Performance Manager System Event Editor. The OSS host must be a fully qualified hostname or an IP address.

Problem The Alarm Report portlet generates an error when you open the following predefined reports:

- Events Details
- Performance Details

Solution By default, Prime Central Fault Management is configured to support detailed alarm reports for 50,000 alarms. For reports with more than 50,000 alarms, you can reduce the elapsed period and run multiple reports on a smaller subset of alarms. Alternately, you can increase the Java heap size of the reporting server to 3 GB and run detailed alarm reports for up to 100,000 alarms.

To increase the Java heap size on the reporting server:

1. As the primeusr user, log in to the Prime Central Fault Management server.
2. Enter the following command to stop the Fault Management server:

   $NCHOME/fmctl stop
3. Change directories to $NCHOME/tipv2/profiles/TIPProfile/config/cells/TIPCell/nodes/TIPNode/servers/server1.
4. Use a standard text editor such as vi to open the server.xml file and change the maximumHeapSize value to **3072**.

Note If you have set up disaster recovery on another device, you must also make this change on that device.

5. Save and close the server.xml file.
6. Enter the following commands to start the Fault Management server:

   su - primeusr

   fmctl start

Problem After generating a report while using the Alarm Report portlet and either logging out of Prime Central or closing the portlet, you may receive the following Authentication Required prompt:

`A username and password are being requested by https://`*server-name*`:`*port-number*`. The site says: "Cognos 8."`

You are prompted to enter a username and password.

Solution At the Authentication Required prompt, click **Cancel**.

Problem In the Suite Monitoring portlet > Prime Central tab, the Prime Central Fault Management state is Down.

This problem occurs when Prime Central and the Fault Management component are installed on the same server with an embedded Oracle database, and the server is rebooted. The Oracle database takes longer to

restart automatically than does Fault Management. Because Fault Management cannot connect to the Oracle database, its state is shown as Down.

Solution As the primeusr user, restart Prime Central Fault Management:

fmctl stop

fmctl start

Problem After performing any of the following alarm management operations, the Alarm Browser does not display the result:

- Acknowledging or deacknowledging an alarm
- Clearing an alarm
- Retiring an alarm
- Adding notes to an alarm

Solution In the Alarm Browser portlet, click the **Refresh** icon. If the result is still not displayed after a manual refresh, do the following:

1. Open the Message Center.
2. Find the alarm action and click the **Memo** field to view any error information. (Errors reported by the applications prevent Prime Central Fault Management from completing the alarm action.)
3. If you see any timeout errors, verify that the Prime Central server and the application are synchronized.
4. If an error indicates that the alarm no longer exists on the application, do the following:
   - If the alarm state is Cleared, wait up to one hour for the alarm to be removed automatically.
   - If the alarm state is not Cleared, resynchronize the alarms by opening an SSH session on the Prime Central Fault Management server and entering:

     su – primeusr

     fmctl resync

Problem Notes added via the NBI Alarm Management API for Prime Network appear twice in the Prime Central Fault Management Alarm Browser.

Solution Make sure that the *username* element in the NBI call specifies a valid Prime Central Fault Management user. If an invalid user is specified, or the *username* element is left empty, a duplicate note is created for the alarm.

Problem `centraladmin` is indicated as the relevant user for notes added via the NBI Alarm Management API, even though a different username was specified.

Solution Make sure that the *username* element in the NBI call specifies a valid Prime Central Fault Management user. If an invalid user is specified, `centraladmin` is used instead.

Problem Suite Monitoring portlet indicates that Fault Management's status is `Down` (applicable to Fault Management 1.2 and later).

Solution If the Suite Monitoring portlet indicates that the integration layer is also down, begin by troubleshooting why. As soon as the integration layer becomes operational, Fault Management should as well.

If Fault Management continues to be down, even after the integration layer comes up, first check the integration layer's log file to determine if there are any network connection issues between the integration layer and the Fault Management server. If there are no connection issues, you then need to determine which Fault Management components are not running. The Suite Monitoring portlet sends a status request to Fault Management. At this point, Fault Management checks if all of its components are running. If they are, then the portlet indicates that the integration layer's status is `Up`.

The Suite Monitoring portlet's status check is equivalent to running the `fmctl status` command as *primeusr* on the Fault Management server. If you run this command on the Fault Management server and it returns:

- `SUCCESS: Prime Central Fault Management is fully started`, then Fault Management is up and running. Recheck the integration layer log files for more troubleshooting hints.
- `WARNING: Prime Central Fault Management is in an indeterminate state`, then Fault Management is still down. You will need to determine which components are down and then review the appropriate log files for more details:
  - ObjectServer: ~/faultmgmt/omnibus/log/NCOMS.log
  - Oracle Gateway: ~/faultmgmt/omnibus/log/nco_g_oracle.log
  - SNMP Probe: ~/faultmgmt/omnibus/log/mttrapd.log
  - CORBA Probe: ~/faultmgmt/omnibus/log/cisco_ctm_corba_v9_idXX.log
  - TIP/TCR: ~/faultmgmt/tipv2/profiles/TIPProfile/logs/server1/SystemOut.log
  - Impact: ~/faultmgmt/log/netcool-errors.log
  - DMRegistration: ~/faultmgmt/log/dmregistration.log

To restart Fault Management, run the **fmctl restart** command.

To view more detailed information, run the **fmctl** command.

Problem The Fault Management Oracle gateway is down and does not come up after restart.

Solution The problem is caused by one of two things:

Prime Central is installed on the same server as Fault Management and the Oracle database came up after the Oracle gateway. Restart the gateway by entering the following commands:

- **su - primeusr**
- **nco_g_oracle &**

The gateway database may have become corrupt. Do the following:

- Stop the gateway:

  kill -9 <nco_g_oracle pid>

- Move the contents of the ~/$OMNIHOME/var/nco_g_oracle directory to the /tmp/nco_g_oracle directory.
- Restart the gateway:
  - **su - primeusr**
  - **nco_g_oracle &**

Appendix A: Troubleshooting

Problem You see `mbind: Invalid Argument` errors in the Fault Management log files.

Solution Do the following:

1. Remove the numactl-devel Red Hat RPM package:
   1. Log in as the root user.
   2. Enter:

      rpm -ev numactl-devel
2. Remove all instances of the `mbind: Invalid Argument` error in the following files:
   - ~/faultmgmt/impact/etc/NCI_ReportsHSQLDB.ds
   - ~/faultmgmt/impact/etc/NCI_defaultobjectserver.ds
   - ~/faultmgmt/impact/etc/NCI_wsadmin.props

Problem Retired alarms are not deleted from the Oracle database after 14 days.

Solution Do one of the following:

If the /tmp/fm_backups-date.tar file exists:

1. Log in as the root user.
2. Enter the following commands:

   # **mkdir /tmp/fm**

   # **cp /tmp/fm_backups*.tar /tmp/fm**

   # **cd /tmp/fm**

   # **tar -xvf fm_backups*.tar**

   # **cp tmp/FaultMgmtCron.csh /etc/cron.hourly**

   # **chmod 777 /etc/cron.hourly/FaultMgmtCron.csh**

   # **rm –rf /tmp/fm**

If the /tmp/fm_backups-date.tar file does not exist:

1. Log in as the root user.
2. Enter:

   vi /etc/cron.hourly/FaultMgmtCron.csh
3. Copy and paste the following text into the FaultMgmtCron.csh file. If your primeusr home folder is not /opt/primecentral, make the appropriate changes.

```
#!/usr/bin/env tcsh

echo Current directory is 'pwd'
set PRIMEHOME=/opt/primecentral
set PRIMEFMHOME=/opt/primecentral/faultmgmt
source /opt/primecentral/.cshrc

cd /opt/primecentral/faultmgmt/prime_integrator/scripts
./AlarmPartitioning.sh
```

Appendix A: Troubleshooting

4. Save the file.
5. Enter:

   chmod 777 /etc/cron.hourly/FaultMgmtCron.csh

Appendix A: Troubleshooting