Troubleshooting Cisco Prime Collaboration Provisioning 12.6SU2

The following tables list the maximum capacity of Prime Collaboration Provisioning when it is installed on a system that meets the virtual machine requirements. Prime Collaboration may not function as expected if the load exceeds the specified system capacity, for an OVA.

Installation and Upgrade

How to verify the Cisco Prime Collaboration Provisioning installation (for advanced/standard mode)?

After you install Prime Collaboration Provisioning, verify if it has been properly installed.

1. In a browser, specify the IP address of the server on which Prime Collaboration Provisioning (standard/advanced) has been installed.

   The login page is displayed. Log in with globaladmin credentials.
2. Log in to the Provisioning server using the SSH service and with the CLI admin that you created during OVA configuration. By default, this username is admin.
3. Enter the following command to display the processes that are running:

   show application status cpcm

   bash: no job control in this shell

   httpd denotes httpd service.

   nice.sh denotes Nice service.

   startcupm.sh denotes Jboss service.

   postmaster/su denotes Postgres service.

   STAT PID USER COMMAND ELAPSED

   ==========

   Ss 629 root httpd 02:11:38

   S 613 root nice.sh 02:11:38

   S 610 root startcupm.sh 02:11:38

   S 608 root su 02:11:38

The parameters in the COMMAND column are the processes that are running on the Prime Collaboration Provisioning server (standard/advanced). If you do not see the processes running, enter the following commands to restart the Prime Collaboration Provisioning services:

admin#application stop cpcm

admin#application start cpcm

The above commands take one or two minutes to stop or start the Prime Collaboration Provisioning services.

You can verify if the installation is complete and successful, by checking if the JBoss service is running.

In the SSH terminal, run the following command as a root user to know if the JBoss service is running :

ps - aef|grep startcupm

You can also check at what time the JBoss service was started, in the following location (in the last line of the log file) :

/opt/cupm/sep/logs/jboss.log

If the JBoss service is running, see the Getting Started chapter, of the Cisco Prime Collaboration Provisioning Guide - Standard and Advanced to get started with the Prime Collaboration Provisioning application.

How to upgrade Cisco Prime Collaboration Provisioning from small to medium deployment model?

After you manually upgrade the system requirements (vRAM, vCPU, vDISK and such), you must run the following scripts as a root user:

1. Execute the memorymodel.sh file under /opt/cupm:
   ./memorymodel.sh medium "-Xms512m -Xmx1024m -XX:MaxPermSize=256m -server" "-Xms512m -Xmx1024m -XX:MaxPermSize=256m" simple all
2. Execute cpcmdiskutil.sh under /opt/cupm:
   . /cpcmdiskutil.sh /dev/sda
3. Restart the server(vmware instance)

How to upgrade Cisco Prime Collaboration Provisioning server from small/medium to large deployment model?

1. Backup the database from the Prime Collaboration Provisioning application by following the procedures provided in Cisco Prime Collaboration Provisioning Guide.
2. Deploy large OVA as a database server (say, “server1”) by following the procedure provided in the Cisco Prime Collaboration Provisioning Install and Upgrade Guide. During the deployment, ensure that the globaladmin password is same as the password provided during deployment.

3. Deploy large OVA as an application server (say, “server2”) by following the procedure provided in the Cisco Prime Collaboration Provisioning Install and Upgrade Guide. During the deployment, ensure that the globaladmin password is same as the password provided during deployment.

    a. Copy the licenses from the old server to the new server2.
    b. If you make use of the MAC address of the existing Prime Collaboration Provisioning server, then you must update the MAC address using the VMware client for this VMWare instance.
    c. If you make use of a new MAC address for server2, then the licenses in the /opt/cupm/license directory must be rehosted to match the new server2 VM.

4. Stop provisioning services in the application server (“server2”).
    a. Go to /opt/cupm folder.
        Execute ./cupm-app-service.sh stop
    b. Ensure that Apache, JBoss and NICE Services are stopped using the following commands:
        ps -aef | grep startcupm
        ps -aef | grep nice
    c. If there are any process running, use the following commands to stop their execution:
        kill -9 <startcupm process id>
        kill -9 <nice process id>
    d. To check whether the nice process is still holding on the postgres connection, enter the following command: ps -aef
        Look for the process: /opt/cupm/jvm/bin/java -server −classpath /opt/cupm/sep/lib/dom.jar:
        If the process is running, enter the following command:
        kill -9 <Process-Id found earlier>.
    e. Wait for a minute to make the resources, such as ports, to become free.
5. Restore database in the database server (“server1”) using the backed up database file taken from step 1.
   For details, see the section “Restoring Database in the database server” in the Cisco Prime Collaboration Provisioning Guide - Standard and Advanced.
6. Stop and then start the provisioning services in database server (“server1”).
    a. cd /opt/cupm folder.
        ./cupm-db-service.sh stop.
    b. Wait for 30 seconds before starting the db services
    c. To start the db services: cd /opt/cupm
        ./cupm-db-service.sh start.
7. Copy the following files from the original Prime Collaboration Provisioning server to the newly deployed application server (“server2”)

a. /opt/cupm/sep/dfc.properties

b. /opt/cupm/sep/dfc.keystore

c. /opt/cupm/jboss/server/cupm/conf/login-config.xml

8. Change directory to /opt/cupm/sep and edit the dfc.properties file using the “vi” editor

a. cd /opt/cupm/sep

b. vi dfc.properties

c. Change the property dfc.memory.model=medium to dfc.memory.model=large

d. Change the property dfc.postgres.host=localhost to dfc.postgres.host=<IP of server Database>

e. Save changes and exit the editor

9. Start application services in the application server (“server2”).

a. Change directory to /opt/cupm folder to start the application services

b. cd /opt/cupm.

./cupm-app-service.sh start.

The system is now ready to be used.

How to downgrade Cisco Prime Collaboration deployment model?

Prime Collaboration does not support downgrade of deployment model; that is you cannot downgrade from Prime Collaboration Large deployment to Small.

How to configure a second NIC for Prime Collaboration?

A second NIC can be added to the Prime Collaboration as follows:

- Use vSphere Client (Edit virtual machine settings option) to add a second virtual Network Adapter to the virtual machine
- Login to the Prime Collaboration admin CLI to configure the IP address for the second interface
- Configure the ip route gateways for the two interfaces (with the same CLI access)

Login as admin user and execute the following CLI commands:

```
admin# configure
admin (config)# interface GigabitEthernet 1 (Note that the first interface is Giga-
bitEthernet 0)
admin (config-GigabitEthernet)# ip address <ip address> <net mask>
admin (config-GigabitEthernet)# exit
```

To configure the ip routes to the two different gateways:

```
admin (config)# ip route <network addr> <net mask> <route-specific gateway1>
admin (config)# ip route <network addr> <net mask> <route-specific gateway2>
……
```

Change the default route (0.0.0.0 0.0.0.0) to the appropriate gateway if needed.

How to change the IP Address on the Provisioning Server (for a Distributed Setup)?

The following procedure is applicable for Cisco Prime Collaboration Provisioning 10.0 and 10.5. For Provisioning 9.0 and 9.5, see the Setting Up the Server chapter in *Cisco Prime Collaboration Provisioning Guide*.

1. Stop the application services using the following command:
    - execute ./cupm-full-service.sh stop
2. Login to the database server as admin through SSH and execute the following commands:
    - admin# conf t
    - admin(config)# interface GigabitEthernet 0
    - admin(config-GigabitEthernet)# ip address <ipaddress> <subnet mask>
3. Specify "y" when the following message is displayed: Changing the IP may result in undesired side effects on any installed application(s). Are you sure you want to proceed? [y/n] y
4. Login to the database server as admin with the new IP address and execute the following configuration commands:
    - admin(config)# ip default-gateway <a.b.c.d>
    - admin(config)# ip domain-name <new_domain>
    - admin(config)# ip name-server <a.b.c.d>
    - admin(config)# hostname <new_name>
    - admin(config)# exit
    - admin# write memory
5. Login to the database server as root with the new IP address.
6. Update the Nice system record in postgres:
    - Login to postgres
    - cd /opt/postgres/9.0/bin
    - ./psql -Upmadmin -d cupm
    - Select * from nicesyseng;

- Check if there are any entries that contain your old IP address (in the "host" column). If there are any entries, delete them by executing the following query: delete from nicesyseng where host='<old_ip_address>';

7. In the /opt/postgres/9.0/data/pg_hba.conf file, replace the line: host all all <ip>/32 trust with host all all <changed app-server ip>/32 trust
8. Login to the application server as admin through SSH and execute the following commands:
   - admin# conf t
   - admin(config)# interface GigabitEthernet 0
   - admin(config-GigabitEthernet)# ip address <ipaddress> <subnet mask>
9. Specify "y" when the following message is displayed: Changing the IP may result in undesired side effects on any installed application(s). Are you sure you want to proceed? [y/n] y
10. Login to the application server as admin with the new IP address and execute the following configuration commands:
    - admin(config)# ip default-gateway <a.b.c.d>
    - admin(config)# ip domain-name <new_domain>
    - admin(config)# ip name-server <a.b.c.d>
    - admin(config)# hostname <new_name>
    - admin(config)# exit
    - admin# write memory
11. Login to the application server as root with the new IP address.
12. Update the following line in the /opt/cupm/sep/dfc.properties file:
    - dfc.postgres.host=<database-server-new-ip-address>
13. Update the following line in the /opt/cupm/jboss/server/cupm/deploy/dfc-ds.xml:
    - <connection-url>jdbc:postgresql://<database-server-new-ip-address>:5432/cupm</connection-url>
14. Reboot the database server. After this is completed, reboot the application server.

How to change IP address on the Provisioning Server (Single Setup)?

The following procedure is applicable for Cisco Prime Collaboration Provisioning 10.0 and 10.5. For Provisioning 9.0 and 9.5, see the Setting Up the Server chapter in *Cisco Prime Collaboration Provisioning Guide*.

1. Log in to the server as admin through SSH and execute the following commands:

- admin# conf t
- admin(config)# interface GigabitEthernet 0
- admin(config-GigabitEthernet)# ip address <ipaddress> <subnet mask>

2. Specify "y" when the following message is displayed: Changing the IP may result in undesired side effects on any installed application(s). Are you sure you want to proceed? [y/n] y
3. Login as admin with the new IP address and execute the following configuration commands:

    - admin(config)# ip default-gateway <a.b.c.d>
    - admin(config)# ip domain-name <new_domain>
    - admin(config)# ip name-server <a.b.c.d>
    - admin(config)# hostname <new_name>
    - admin(config)# exit
    - admin# write memory

4. Login as root with the new IP address.
5. Update the Nice system record in postgres:

- Login to postgres
- cd /opt/postgres/9.0/bin
- ./psql -Upmadmin -d cupm
- Select * from nicesyseng;
- In the console output, check if there are any entries that contain your old IP address (in the "host" column). If there are any entries, delete them by executing the following query: delete from nicesyseng where host='<old_ip_address>';

6. Reboot the server.

Licensing

How to find the MAC address of Prime Collaboration Provisioning servers?

To find the MAC address of Prime Collaboration Provisioning 10.0,

1. Click the About icon at the top right corner of the user interface.
2. In the About page, click the Provisioning information link to launch the system information details for both Prime Collaboration Provisioning.

For all the other versions of Prime Collaboration, you can check the MAC address through the vSphere client. You can also log in as root to the Prime Collaboration Provisioning server and run the command ifconfig.

Provisioning

How to configure Prime Collaboration Provisioning to synchronize a subset of subscribers from Cisco Unified Communications Manager?

The option to synchronize a subset of subscribers from Cisco Unified Communications Manager is disabled by default. To enable this feature, add the properties mentioned below in $CUPM\sep\ipt.properties file.

- dfc.ipt.sync.users.filter.attribute.name: department
- dfc.ipt.sync.users.filter.attribute.value: *

Names and Values to be set in the ipt.properties file:

1. Specify the following parameters for the property dfc.ipt.sync.users.filter.attribute.name:

```
a.  department
b.  userid
c.  firstname
d.  lastname
```

2. Specify the following values for the property dfc.ipt.sync.users.filter.attribute.value

```
a.  (this will sync only those users that have the above specified property (ex:
   department) value as not empty)
b.  test* (this will sync those users that have the above specified property (ex:
   department) value that starts with 'test')
c.  *test* (this will sync those users that have the above specified property (ex:
   department) value that contains 'test')
```

How to set Throttling Values for Cisco Unified Communications Managers?

The throttling values set in Provisioning must be equal to or less than the values set in Cisco Unified Communications Manager. If you change the throttling settings in Cisco Unified Communications Manager, you must also change the same settings in Provisioning.

The throttling settings in Provisioning are set in the ipt.properties file (located at /opt/cupm/sep folder).

Note: The default location for the installation directory is /opt/cupm.

The following properties (in the ipt.properties file) are used to control the write request sent to Cisco Unified Communications Manager:

```
•dfc.ipt.axl.soap.MaxAXLWritesPerMinute: 20
```

This property specifies the default number of write requests per minute. Its value is used if there is no version or device specific value specified.

```
•dfc.ipt.axl.soap.MaxAXLWritesPerMinute.ccm501: 50
```

This property specifies the number of write requests per minute for Cisco Unified Communications Manager version 5.0(1). Its value is used if there is no device specific value specified.

```
•dfc.ipt.axl.soap.MaxAXLWritesPerMinute.<IP address>: 20
```

This property specifies the number of write requests per minute for a specific Cisco Unified Communications Manager indicated by the IP address.

For example, dfc.ipt.axl.soap.MaxAXLWritesPerMinute.1.2.3.4: 20 sets the value to 20 for Cisco Unified Communications Manager with the IP address of 1.2.3.4.

Video Diagnostics

While performing the troubleshooting workflow between endpoints, I am seeing these issues:

- Troubleshooting status shows Errored and log tab shows Pathtrace Discovery could not be completed because of an internal error.
- Some network nodes are missing in the path topology

If you are seeing any one of the above issues, you can check whether:

- "utils network mtr" runs successfully between the source endpoint and destination device; where the source endpoint is a Cisco TelePresence System (CTS 500, 1000 and or 3000).
- "systemtools network traceroute" runs successfully between the source endpoint and destination device; where the source endpoint is a Cisco C and/or EX series system.
  traceroute runs successfully between the first hop router or layer 3 switch and destination device. The first hop router or layer 3 switch is connected to either a Cisco Video Phone (89xx/99xx) Cisco Cius, Cisco Jabber video, Polycom, and/or E20.
  In addition, you must ensure that traceroute command from Prime Collaboration server to the source device works successfully where the source device is Cisco Jabber Video, Polycom, E20.

- "systemtools network traceroute" runs successfully between the source endpoint and destination device; where the source endpoint is a Cisco MXP.

The first hop router or layer 3 switch must have the CLI Access Level RW (Prime Collaboration server > Operate > Device Work Center > Current Inventory table).

The troubleshooting status shows No CLI Access and does not allow troubleshooting.

Check whether the source device has CLI Access Level as RW (Prime Collaboration server > Operate > Device Work Center > Current Inventory table).

Why the mediatrace or IP SLA statistics is not displayed in the troubleshooting result page?

In the troubleshooting workflow, if both the endpoints do not support five-tuple configuration, the mediatrace statistics is not displayed. In the troubleshooting workflow, if one of the endpoints support five-tuple, the mediatrace statistics is displayed.

The E20, MXP, Cisco Jabber Video, and Polycom devices does not support five-tuple configuration.

For running IPSLA VO diagnostics, you must ensure that traceroute command from source switch or router to destination switch or router runs successfully.

General

How to remove the SSL certificate warning?

- Windows Internet Explorer–You can permanently remove the SSL certificate warning by installing the Prime Collaboration self-signed certificate.
- Mozilla Firefox–You can remove the SSL certificate warning only by adding an exception.

In Windows Internet Explorer, to remove the SSL certificate warning:

1. Choose Continue to this website (not recommended).
2. Choose Tools > Internet Options.
3. In the Internet Options dialog box, click the Security tab, choose Trusted sites, and then click Sites.
4. Confirm that the URL that appears in the field and matches the application URL, and then click Add.
5. Close all dialog boxes and refresh the browser.
6. Choose Certificate Error to the right of the address bar, and then click View certificates.
7. In the Certificate dialog box, click Install Certificate.
8. In the Certificate Import Wizard dialog box, click Next.

9. Click the Place all certificates in the following store radio button, and then click Browse.
10. In the Select Certificate Store dialog box, choose Trusted Root Certification Authorities, and then click OK.
11. Click Next > Finish.
12. In the Security Warning message box, click Yes.
13. In the Certificate Import Wizard message box, click OK.
14. In the Certificate dialog box, click OK.
15. Repeat Step 2 and Step 3.
16. Select the URL in the Websites section, and then click Remove.
17. Close all dialog boxes, restart the browser, and invoke Prime Collaboration. See the "Getting Started" chapter of Cisco Prime Collaboration Provisioning Guide - Standard and Advanced for information about invoking Prime Collaboration.

If you have a safe URL implemented, do the following:

1. Choose Tools > Internet Options.
2. In the Internet Options dialog box, click the Advanced tab.
3. In the Security section, uncheck the Warn about certificate address mismatch check box.

In Mozilla Firefox, to remove the SSL certificate warning:\

1. Click I Understand the Risks >Add Exception.
2. In the the Add Security Exception dialog box, click Confirm Security Exception.

UC Performance Monitor goes blank due to customized layout settings change

1. Launch Home -> UC Performance Monitor
2. Select some clusters and view the dashboards.
3. Now change the Dashlet layout or do any such customization.
4. Again, launch the UC performance monitor. It shows blank page.

   Workaround: Reset the customized settings and the launch the UC Performance Monitor.