
# Uninstalling Prime Central for HCS 9.1.1 and Backing Up and Restoring Data

This chapter explains the procedure to uninstall Prime Central for HCS 9.1.1 and the procedure to back up and restore data. This chapter covers the following topics:


- Uninstalling Prime Central for HCS 9.1.1, page 7-1
- Backing Up and Restoring Data, page 7-2


## Uninstalling Prime Central for HCS 9.1.1

You can uninstall the components by running the following command. Do not specify the name of the individual component for uninstallation, unless the script cannot determine. The system automatically detects and uninstalls the component that was installed. If you need to uninstall one particular component, connect to the virtual machine through SSH, and run the script by the following the steps below. The scripts have to be run *only* on the local machine—ensure that you run the script on the virtual machine that has the component installed.

**Note** After you complete the uninstallation procedure, to install Prime Central for HCS, you must perform a fresh installation. You must not perform the upgrade procedure.

The **`remove-install-logs`** clears the logs from the previous installation.

**Step 1** Log in as **root** user.

**Step 2** **`cd /opt/hcm_installer/scripts/hcm_install_scripts`**

**Step 3** Run the clean command

```
./clean.py [ --remove-primecentral ]
           [ --remove-ec ]
           [ --remove-sv ]
           [ --remove-ce ]
           [ --remove-im ]
           [ --remove-install-logs]
```

# Backing Up and Restoring Data

You have to manually run the backup and restore commands from the command line interface. The script is based on Python. All the components are backed up in online mode and there will be minimal impact to the running system. We recommend that you perform this procedure at a time you anticipate fewer events. However, restoration of data must be done during maintenance period as the components have to be brought down for a brief period. The backup and restore scripts are available in the product DVD. This section contains the following topics:


- Before Backing Up Data, page 7-2
- Backing Up Data, page 7-4
- Before Restoring Data, page 7-5
- Restoring the Backed Up Data, page 7-7
- Performing Additional Restore Processes, page 7-7


**Note** The Service Visualizer process will be restarted during the backup process. This can prevent you from accessing the Prime Central AEL and Service Availability portlet for a brief period during the backup procedure.

When you run the backup and restore script, the following components (along with the built-in utilities mentioned) will be backed up and restored. This list is in the order in which the components are backed up and restored.

1. Prime Central—Prime Central with Oracle EE databases with built-in utilities.
2. Event Collector—
   - The Event Collector Object Server database with the nco_sql and ALTER SYSTEM BACKUP commands.
   - The SNMP Gateway configuration files.
   - The NCOMS property file.
3. Service Visualizer—
   - The Service Visualizer database with the rad_db command.
   - The Service Visualizer WebGUI configuration with the ws_ant.sh command.

   The Service Visualizer processes will be restarted as part of the backup process. This will impact the Alarm Browser and Service Availability views.
4. Correlation Engine—The Correlation Engine configuration with the nci_export and nci_import commands.
5. Infrastructure Monitoring—The Infrastructure Monitoring configuration with the migrate-export.sh and migrate-import.sh scripts. The DB2 database on Infrastructure Monitoring with the "db2 backup database ..." and "db2 restore database ..." commands.

## Before Backing Up Data

Before performing a backup procedure, ensure the following are satisfied:

- The script should be executed on a running Prime Central for HCS system.

- The script must be run on a central machine that has access to SSH to the 5 components of Prime Central for HCS.
- The backup python script has the following six command line arguments, for which you need to input data:
  - IP Address of Prime Central VM
  - IP Address of Event Collector VM
  - IP Address of Service Visualizer VM
  - IP Address of Correlation Engine VM
  - IP Address of Infrastructure Monitoring VM
  - Backup directory on local machine where the backup file will be placed. A directory will be created if it does not exist. The directory can either be a full path or a local path.

#### Netrc File

A netrc file contains the username and password for each VM. You have to create and maintain the netrc file. The netrc file is a usual file that you create with .netrc (with the dot before the name to make it a hidden file). Any text editor can be used to create the file and insert the proper machine names and credentials. Example text editors on Linux machines are vi, emacs, and gedit.

Be sure to follow the guidelines mentioned below:

- Make sure the netrc file has the proper permissions. The required permission for a netrc file is read and write access only for the owner. This translates to permission 600 or rw in Linux.
- The netrc file must contain the IP address or the hostname of the machine and the credentials of the user that has the permission to execute the backup commands for each component. The IP address or the hostname of the netrc must match with the entry in the backup command line option (for example, IP and IP or hostname and hostname).

**Caution** The default username and password in the netrc file is optional. However, if you choose to provide the default credentials, and the IP addresses in the command line option and the netrc file do not match, the scripts, by default, use the default user credentials. While the procedure might appear to be progressing properly, it might create issues later, since the machine to which it logs on to will be with a different username.

- Each IP address of the machine must be appended with a specific identifier to distinguish the machine. For example, machine *IP Address*-pc, to indicate Prime Central component.
- This is because the components could be installed on the same machine which would cause issues when looking up the username and password in the netrc file.

Here is an example of a netrc file:

```
machine IP-address-pc
login root
password cisco123

machine IP-address-ec-os
login root
password se032c

machine IP-address-ec-sql
login root
password cisco123
```

```
machine IP-address-sv-os
login root
password smartway

machine IP-address-sv-tip
login tipadmin
password cisco123

machine IP-address-ce
login netcool
password smartway

machine IP-address-im
login root
password se032c

default
login netcool
password smartway
```

To complete the backup process, provide the following inputs in the netrc file:

***Table 7-1 Inputs for Backup Script***

| Component | User | Description |
|---|---|---|
| Prime Central | root | Needs root OS access to SSH into the Prime Central VM and to set up for Oracle EE backup. |
| Event Collector-OS | root | Needs root OS access to SSH into the VM and to set up for Event Collector backup. |
| Event Collector-SQL | root | Needs root Event Collector Database user for access to the nco_sql command. |
| Service Visualizer-OS | root | Needs root OS access to SSH into the VM and run the restore script. |
| Service Visualizer-tip | tipadmin | Needs a user (example, tipadmin) that has access to Service Visualizer Server. |
| Correlation Engine | netcool | Needs a user (example, netcool) that has access to Correlation Engine nci_import command. |
| Infrastructure Monitoring | root | Needs root OS access to SSH into the VM and run backup script. |

# Backing Up Data

The backup script is located in your product DVD. By default, the backup script will look for the netrc file in the same directory as the backup script with the name pc.netrc. If you prefer to override the default name and location, you can use the environment variable PC_NETRC_FILE. An example:

```
export PC_NETRC_FILE=/home/netcool/.netrc
```

In the following script, replace the IP addresses with the IP address you provided in the netrc file:

**./backup.py** *Prime-Central-IP Event-Collector-Engine-IP Service-Visualizer-IP Correlation-Engine-IP Infrastructure-Monitoring-IP Backup-Directory*

After you run the backup script, all the five components are backed up, one at a time. After a successful backup procedure, a tar file will be created and placed in the backup directory that you specified in the command line argument. The naming convention of the backup file is *backup-<timestamp>.tar*. If the backup procedure was successful, the return code upon exit will be zero (indicating that zero components were unsuccessfully backed up).

If a component fails in the backup process, a message indicates so on the console. However, the backup script will continue to backup the rest of the components. When the script finishes running, the return code upon exit will be a non-zero value. This indicates the number of components that were not backed up. In such a scenario of partial execution, the naming convention of a tar file is *partial-backup-<timestamp>.tar*.

# Before Restoring Data

Before performing a restore procedure, ensure the following are satisfied:

- The script should be executed on a running Prime Central for HCS system.
- The script must be run on a central machine that has access to SSH to the 5 components of Prime Central for HCS.
- The restore python script has the following six command line arguments, for which you need to input data:
  - IP Address of Prime Central VM
  - IP Address of Event Collector VM
  - IP Address of Service Visualizer VM
  - IP Address of Correlation Engine VM
  - IP Address of Infrastructure Monitoring VM
  - The backup file name from a previous backup. The location of the backup file can be a full path or local path.

### Netrc File

A netrc file contains the username and password for each VM. You have to create and maintain the netrc file. The netrc file is a usual file that you create with .netrc (with the dot before the name to make it a hidden file). Any text editor can be used to create the file and insert the proper machine names and credentials. Example text editors on Linux machines are vi, emacs, and gedit.

Be sure to follow the guidelines mentioned below:

- Make sure the netrc file has the proper permissions. The required permission for a netrc file is read and write access only for the owner. This translates to permission 600 or rw in Linux.
- The netrc file must contain the IP address or the hostname of the machine and the credentials of the user that has the permission to execute the restore commands for each component. The IP address or the hostname of the netrc must match with the entry in the restore command line option (for example, IP and IP or hostname and hostname).

**Caution** The default username and password in the netrc file is optional. However, if you choose to provide the default credentials, and the IP addresses in the command line option and the netrc file do not match, the scripts, by default, use the default user credentials. While the procedure might appear to be progressing properly, it might create issues later, since the machine to which it logs on to will be with a different username.

- Each IP address of the machine must be appended with a specific identifier to distinguish the machine. For example, machine *IP address-pc*, to indicate Prime Central component.

This is because the components could be installed on the same machine which would cause issues when looking up the username and password in the netrc file.

Here is an example of a netrc file:

```
machine IP-address-pc
login root
password cisco123

machine IP-address-ec-os
login root
password se032c

machine IP-address-ec-sql
login root
password cisco123

machine IP-address-sv-os
login root
password smartway

machine IP-address-sv-tip
login tipadmin
password cisco123

machine IP-address-ce
login netcool
password smartway

machine IP-address-im
login root
password se032c

default
login netcool
password smartway
```

To complete the restore process, provide the following inputs in the netrc file:

***Table 7-2 Inputs for Restore Script***

| Component | User | Description |
|---|---|---|
| Prime Central | root | Needs root OS access to SSH into the Prime Central VM and to set up for Oracle EE restore. |
| Event Collector-OS | root | Needs root OS access to SSH into the VM and to set up for Event Collector restore. |

*Table 7-2 Inputs for Restore Script*

| Component | User | Description |
|---|---|---|
| Event Collector-SQL | root | Needs root Event Collector Database user for access to the nco_sql command. |
| Service Visualizer-OS | root | Needs root OS access to SSH into the VM and run the restore script. |
| Service Visualizer-tip | tipadmin | Needs a user (example, tipadmin) that has access to Service Visualizer Server. |
| Correlation Engine | netcool | Needs a user (example, netcool) that has access to Correlation Engine nci_import command. |
| Infrastructure Monitoring | root | Needs root OS access to SSH into the VM and run restore script. |

# Restoring the Backed Up Data

The restore scripts are available in your product DVD. After you complete backing up your data, wait for at least an hour before you run the restore scripts. When you select a particular backup to be restored, all other backups available at that point in time are no longer available for restoration. However, you can continue to restore new backups. By default, the restore script will look for the netrc file in the same directory as the backup script with the name "pc.netrc". If you prefer to override the default name and location, you can use the environment variable PC_NETRC_FILE.

An example:

```
export PC_NETRC_FILE=/home/netcool/.netrc
```

In the following script, replace the IP addresses with the IP address you provided in the netrc file:

**./restore.py** *<Prime-Central-IP> <Event-Collector-Engine-IP> <Service-Visualizer-IP> <Correlation-Engine-IP> <Infrastructure-Monitoring-IP> Backup-file-location*

The *Backup-file-location* argument must include the path and file name of the backup file. For example, `/home/user/backup-location-dir/backup-1313781159.527971.tar`.

The restore script restores the five components, one at a time. If a component fails in the restore process, a message appears on the console. If you attempt to restore data after a partial backup (a backup in which one or more components failed), the restore script will only restore the components which were successful during the backup.

# Performing Additional Restore Processes

This section is applicable only if you require a full restoration following a successful backup procedure. You must perform the following procedures after you finish the initial restore procedure. This section contains the following topics:


- Restoring Oracle DB on Prime Central, page 7-8
- Retrieving a new Certificate, page 7-13
- Log Files, page 7-14

## Restoring Oracle DB on Prime Central

This is the first procedure of this two-stage process. Follow the steps outlined below:

**Step 1** On the Prime Central VM, log in as root user.

**Step 2** Stop the portal; run the following command:

```
[root@pc ~]# su - primeusr
[root@pc ~]# portalctl stop
```

**Step 3** Stop the integration layer components; run the following command:

```
[primeusr@pc ~]# itgctl stop
```

**Step 4** Exit the session:

```
[primeusr@pc ~]# exit
```

**Step 5** Change to the Oracle user and capture the ORACLE_BASE for your use, later.

```
[root@pc ~]# su - oracle
oracle@pc [~]# echo $ORACLE_BASE
/opt/oracle
```

**Step 6** Connect to the Oracle database. As a Oracle user, run the following command:

```
oracle@pc [~]# rman target /
Recovery Manager: Release 11.2.0.1.0 - Production on Tue Jan 8 14:45:33 2013
Copyright (c) 1982, 2009, Oracle and/or its affiliates.  All rights reserved.
connected to target database: PRIMEDB (DBID=2843161957)
RMAN>
```

**Step 7** Verify the DBID from connecting to the database with **rman target/** matches the control file name (cfc-xxxxxxxxxx-xxxxxxxx-xx).

In the following example, the DBID 2843161957 in tested:

```
RMAN> list backup;

using target database control file instead of recovery catalog

List of Backup Sets
===================


BS Key  Type LV Size       Device Type Elapsed Time Completion Time
------- ---- -- ---------- ----------- ------------ ---------------
1       Incr 0  268.05M    DISK        00:00:53     08-JAN-13
        BP Key: 1   Status: AVAILABLE  Compressed: YES  Tag: TAG20130108T091947
        Piece Name: /opt/oracle/backup/PRIMEDB_t804158387_s1_p1
  List of Datafiles in backup set 1
  File LV Type Ckp SCN    Ckp Time  Name
  ---- -- ---- ---------- --------- ----
  1    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/system01.dbf
  2    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/sysaux01.dbf
  3    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/undotbs01.dbf
  4    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/users01.dbf
  5    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/undotbs02.dbf
  6    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/PRIMEDBA_TS_DATA.dbf
  7    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/PRIMEADMIN_TS_DATA.dbf

BS Key  Type LV Size       Device Type Elapsed Time Completion Time
------- ---- -- ---------- ----------- ------------ ---------------
```

```
2       Full    9.36M      DISK        00:00:01     08-JAN-13
        BP Key: 2   Status: AVAILABLE  Compressed: NO  Tag: TAG20130108T092042
        Piece Name: /opt/oracle/backup/cfc-2843161957-20130108-00
  SPFILE Included: Modification time: 08-JAN-13
  SPFILE db_unique_name: PRIMEDB
  Control File Included: Ckp SCN: 1018769      Ckp time: 08-JAN-13

RMAN>
```

**Step 8** Shutdown and restart the database:

```
RMAN> shutdown abort;

Oracle instance shut down

RMAN> startup force nomount;

Oracle instance started

Total System Global Area    4409401344 bytes

Fixed Size                     2212576 bytes
Variable Size               2751466784 bytes
Database Buffers            1610612736 bytes
Redo Buffers                  45109248 bytes

RMAN>
```

**Step 9** Set the database ID with the DBID verified in step 7:

```
RMAN> set DBID=2843161957

executing command: SET DBID

RMAN>
```

**Step 10** Run the following command and make sure to enter '/opt/oracle' for ORACLE_HOME. The 'backup/cf%F' will always be the same:

```
RMAN> run {
2> set controlfile autobackup format for device type disk to '/opt/oracle/backup/cf%F';
3> restore controlfile from autobackup;
4> }

executing command: SET CONTROLFILE AUTOBACKUP FORMAT

Starting restore at 08-JAN-13
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=771 device type=DISK

channel ORA_DISK_1: looking for AUTOBACKUP on day: 20130108
channel ORA_DISK_1: AUTOBACKUP found: /opt/oracle/backup/cfc-2843161957-20130108-00
channel ORA_DISK_1: restoring control file from AUTOBACKUP
/opt/oracle/backup/cfc-2843161957-20130108-00
channel ORA_DISK_1: control file restore from AUTOBACKUP complete
output file name=/opt/oracle/oradata/primedb/control01.ctl
output file name=/opt/oracle/oradata/primedb/control02.ctl
Finished restore at 08-JAN-13

RMAN>
```

**Step 11** Shutdown the database and start it up again:

```
RMAN> shutdown abort;

Oracle instance shut down

RMAN> startup mount;

connected to target database (not started)
Oracle instance started
database mounted

Total System Global Area    4409401344 bytes

Fixed Size                     2212576 bytes
Variable Size               2751466784 bytes
Database Buffers            1610612736 bytes
Redo Buffers                  45109248 bytes

RMAN>
```

**Step 12** Identify the largest checkpoint sequence number (Ckp SCN). In this example, the Ckp SCN is 1018730. Run the following command:

```
RMAN> list backup;


List of Backup Sets
===================


BS Key  Type LV Size       Device Type Elapsed Time Completion Time
------- ---- -- ---------- ----------- ------------ ---------------
1       Incr 0  268.05M    DISK        00:00:53     08-JAN-13
        BP Key: 1   Status: AVAILABLE  Compressed: YES  Tag: TAG20130108T091947
        Piece Name: /opt/oracle/backup/PRIMEDB_t804158387_s1_p1
  List of Datafiles in backup set 1
  File LV Type Ckp SCN    Ckp Time  Name
  ---- -- ---- ---------- --------- ----
  1    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/system01.dbf
  2    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/sysaux01.dbf
  3    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/undotbs01.dbf
  4    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/users01.dbf
  5    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/undotbs02.dbf
  6    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/PRIMEDBA_TS_DATA.dbf
  7    0  Incr 1018730    08-JAN-13 /opt/oracle/oradata/primedb/PRIMEADMIN_TS_DATA.dbf

RMAN>
```

**Step 13** Run the following command and remember to change 1018730 with the sequence number from the previous command:

```
RMAN> run {
2> CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT '$1/%d_t%t_s%s_p%p';
3> SET UNTIL SEQUENCE 1018730 THREAD 1;
4> restore database;
5> recover database;
6> }

old RMAN configuration parameters:
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT   '/opt/oracle/backup/%d_t%t_s%s_p%p';
new RMAN configuration parameters:
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT   '$1/%d_t%t_s%s_p%p';
new RMAN configuration parameters are successfully stored
```

```
executing command: SET until clause

Starting restore at 08-JAN-13
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=770 device type=DISK

channel ORA_DISK_1: starting datafile backup set restore
channel ORA_DISK_1: specifying datafile(s) to restore from backup set
channel ORA_DISK_1: restoring datafile 00001 to /opt/oracle/oradata/primedb/system01.dbf
channel ORA_DISK_1: restoring datafile 00002 to /opt/oracle/oradata/primedb/sysaux01.dbf
channel ORA_DISK_1: restoring datafile 00003 to /opt/oracle/oradata/primedb/undotbs01.dbf
channel ORA_DISK_1: restoring datafile 00004 to /opt/oracle/oradata/primedb/users01.dbf
channel ORA_DISK_1: restoring datafile 00005 to /opt/oracle/oradata/primedb/undotbs02.dbf
channel ORA_DISK_1: restoring datafile 00006 to
/opt/oracle/oradata/primedb/PRIMEDBA_TS_DATA.dbf
channel ORA_DISK_1: restoring datafile 00007 to
/opt/oracle/oradata/primedb/PRIMEADMIN_TS_DATA.dbf
channel ORA_DISK_1: reading from backup piece /opt/oracle/backup/PRIMEDB_t804158387_s1_p1
channel ORA_DISK_1: piece handle=/opt/oracle/backup/PRIMEDB_t804158387_s1_p1
tag=TAG20130108T091947
channel ORA_DISK_1: restored backup piece 1
channel ORA_DISK_1: restore complete, elapsed time: 00:01:35
Finished restore at 08-JAN-13

Starting recover at 08-JAN-13
using channel ORA_DISK_1

starting media recovery

archived log for thread 1 with sequence 1 is already on disk as file
/opt/oracle/redo/redo1.log
archived log for thread 1 with sequence 2 is already on disk as file
/opt/oracle/redo/redo2.log
archived log file name=/opt/oracle/redo/redo1.log thread=1 sequence=1
archived log file name=/opt/oracle/redo/redo2.log thread=1 sequence=2
media recovery complete, elapsed time: 00:00:04
Finished recover at 08-JAN-13

RMAN>
```

**Step 14** Shutdown the database and start it up again:

```
RMAN> shutdown abort;

Oracle instance shut down

RMAN> startup mount;

connected to target database (not started)
Oracle instance started
database mounted

Total System Global Area    4409401344 bytes

Fixed Size                     2212576 bytes
Variable Size               2751466784 bytes
Database Buffers            1610612736 bytes
Redo Buffers                  45109248 bytes
```

**Step 15** Run the alter database command and exit:

```
RMAN> ALTER DATABASE OPEN RESETLOGS;

database opened

RMAN> exit
Recovery Manager complete.
oracle@pc [~]#
```

**Step 16** Check the status of the Oracle DB:

```
oracle@pc [~]# lsnrctl status

LSNRCTL for Linux: Version 11.2.0.1.0 - Production on 17-JAN-2013 16:33:40

Copyright (c) 1991, 2009, Oracle.  All rights reserved.

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=pc-02.hcslab.com)(PORT=1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 11.2.0.1.0 - Production
Start Date                17-JAN-2013 09:01:40
Uptime                    0 days 7 hr. 32 min. 0 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File   /opt/oracle/product/11.2.0/db_1/network/admin/listener.ora
Listener Log File         /opt/oracle/diag/tnslsnr/pc-02/listener/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=pc-02.hcslab.com)(PORT=1521)))
Services Summary...
Service "primedb" has 1 instance(s).
  Instance "primedb", status READY, has 1 handler(s) for this service...
Service "primedbXDB" has 1 instance(s).
  Instance "primedb", status READY, has 1 handler(s) for this service...
The command completed successfully
```

The command must display the status as READY for you to proceed.

**Step 17** Restart the Oracle DB, if the status is not READY for primedb instance. Use the sqlplus to connect and and run the shutdown and startup commands:

```
oracle@pc [~]# sqlplus '/ as sysdba'

SQL*Plus: Release 11.2.0.1.0 Production on Thu Jan 17 16:40:18 2013

Copyright (c) 1982, 2009, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit Production
With the Partitioning, OLAP and Real Application Testing options

SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup
ORACLE instance started.

Total System Global Area 4409401344 bytes
Fixed Size                  2212576 bytes
Variable Size            2751466784 bytes
```

```
Database Buffers         1610612736 bytes
Redo Buffers               45109248 bytes
Database mounted.
Database opened.
SQL> quit
Disconnected from Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit
Production
With the Partitioning, OLAP and Real Application Testing options
oracle@pc [~]# exit
logout
[root@pc ~]#
```

**Step 18** Start the portal and integration layer components:

```
[root@pc ~]# su - primeusr
[primeusr@pc ~]# portalctl start
[primeusr@pc ~]# itgctl start
[primeusr@pc ~]# exit
[root@pc ~]#
```

## Retrieving a new Certificate

This is the second step of the two-stage process for a full restoration of data after the backup process.

**Step 1** Log on to Service Visualizer.

**Note** Service Visualizer URL is *https:[SV_HOSTNAME]:16316/ibm/console*. Enter *tipadmin* and *--admin-password* as the user name and password.

**Step 2** From the left pane, go to **Security > SSL Certificate and Key Management > Key Stores and Certificates** (from the Related Links pane).

The **SSL Certificate and Key Management** page appears.

**Step 3** Click **NodeDefaultTrustStore.**

The general properties of NodeDefaultTrustStore appears.

**Step 4** From the Additional Properties listed on the right pane, **Signer Certificate.**

**Step 5** Check the Prime Central alias (*PC_hostname*-8443), and click **Delete.**

**Step 6** Click **Save.**

**Step 7** To obtain a new certificate, select the **Retrieve from Port.**

**Step 8** Enter Prime Central, 8443 and PC_hostname-8443 as the host name, port and alias.

**Step 9** Click **Retrieve Signer Information** button.

The retrieved signed information appears.

**Step 10** Click **Apply.**

**Step 11** Click **Save**. (Available at the top of the page, in the Messages pane.)

**Step 12** Log in to **Service Visualizer CLI.** Run the following commands:

```
[root@sv ~]# /etc/init.d/tbsm stop
waiting for TIP to stop...
```

```
stopped.
[root@sv ~]# /etc/init.d/tbsm start
ADMU3000I: Server server1 open for e-business; process id is 23203
started
```

**Step 13** Log out of Prime Central GUI and log back in.

## Log Files

- A backup log file appears in the directory at the location which contains the backup script. The naming convention is backup-log-<*timestamp*>.txt.
- A restore log file appears in the directory at the location which contains the restore script. The naming convention is restore-log-<*timestamp*>.txt