PowerKEY CAS Gateway 4.0
Installation and Configuration Guide

Please Read

Important

Read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

Contents

About This Guide v

Chapter 1 System Requirements 1

Hardware Requirements 2
Software Requirements 3

Chapter 2 Install the Software on the EC/DTACS Server 5

Installing the PCG Package on the EC 8.0 or DTACS 5.0 Server 6
Installing the PCG Package on an EC 7.x or DTACS 4.1 Server 8

Chapter 3 Deploy the PCG Virtual Machine 11

Deploying the PCG Virtual Machine from the vSphere Web UI 12
Reconfiguring the PCG Virtual Hardware 14
Power On and Login to the New PCG Virtual Machine 15
Configuring the PCG Network 16
Installing VMware Tools (Optional) 17

Chapter 4 Provision the PCG on the EC/DTACS Web UI 19

Provisioning the PCG on the EC Web UI 20
Provisioning the PCG on the DTACS Web UI 24

Chapter 5 Verify PCG Versions 29

Verifying PCG Package Versions on the EC/DTACS 30
Verifying the PCG Version on the PCG Server 31

Chapter 6 Configure SNMPv2 33

Configuring SNMPv2 34
Configuring SNMPv3 35

Appendix A Hardware Configuration Procedures for the Cisco UCS C220 Server 37

Cisco UCS C220 Server Diagram 38
Cisco UCS C220 Server CIMC Configuration 40
RAID Configuration 42

Appendix B Deploy the PCG Virtual Machine from an ESXi Client 47

Deploying a PCG Virtual Machine from an ESXi Client 48
Mounting an ISO from an ESXi Client 50

Appendix C Backup and Restore Keyfiles 51

Backing Up Keyfiles 52
Restoring Keyfiles to a Recovered System 53

Appendix D Upgrade the PCG Server 55

Upgrading the PCG Package on an EC 8.0 or DTACS 5.0 Server 56
Upgrading the PCG Package from an EC 7.x or DTACS 4.1 Server 58
Upgrading the PCG Package on the PCG Server 61

Appendix E Manually Configure the PCG Network 63

Manually Configuring the PCG Network 64

Appendix F Deliver ECMs to DHCTs 67

Delivering ECMs 68

Appendix G Troubleshoot the pcgmon Process 71

Removing the pcgmon Lock File 72

Index 73

About This Guide

Purpose

This ***PowerKEY CAS Gateway 4.0 Installation and Configuration Guide*** provides an overview of the PowerKEY® Conditional Access System (CAS) and describes the PowerKEY CAS Gateway (PCG) server. The PCG is a DVB SimulCrypt-compliant Entitlement Control Message (ECM) generator (ECMG) that performs real-time PowerKEY ECM generation. Visit ***www.cisco.com*** (***http://www.cisco.com***) for data sheets and white papers describing the benefits and features of the PCG server and its role in the Cisco PowerKEY CAS.

Audience

This document is written for system operators. Field service engineers and Cisco Services engineers may also find the information in this document helpful.

Required Skills and Expertise

System operators or engineers who upgrade the PCG software need the following skills:

- Advanced knowledge of Linux.
  - Experience with the Linux vi editor. Several times throughout the system upgrade process, system files are edited using the Linux vi editor. The Linux vi editor is not intuitive. The instructions provided in this guide are no substitute for an advanced working knowledge of vi.
  - The ability to review and edit cron files.
- Knowledge of VMware.
- Extensive EC, DTACS, PCG and DBDS system expertise.

Migration Paths

There is no supported upgrade path from PCG 3.x to PCG 4.x due to the new operating system on PCG 4.x. All sites running PCG 3.x must build a new PCG virtual machine using the current PCG OVA (i.e. PCG-4.0.3-2.ova).

Tested Reference Configuration

Note: Refer to the UCS HW and SW Interoperability form at ***http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html*** for further details concerning server compatibility.

The following is the list of tested reference configuration details.

Configuration	Specifications
Server Series	C Series Standalone Servers
UCS Release	2.0.13d
Server Model	C220-M4(SFF)
OS Vendor	VMware
OS	VMware vSphere ESXi 5.5 U3
Component	RAID Adapter
Adapter	UCSC-MRAID12G-2GB - Cisco 12Gbps SAS Modular Raid Controller
Adapter Driver	4.620.00-7194

1

System Requirements

Before you deploy the PCG VM, make sure your system environment meets the hardware and software requirements defined in this chapter.

In This Chapter

- Hardware Requirements 2
- Software Requirements..... 3

Hardware Requirements

- Cisco UCS C220 M3 or C220 M4 servers with the latest ESXi software installed.

  Important: If you are using a new UCS C220 server, refer to ***Hardware Configuration Procedures for the Cisco UCS C220 Server*** (on page 37) for details about configuring the server. This must be completed prior to deploying the OVA.

- Supported PCG Server Platform:

Platform	Hard Drive (GB)	Memory (GB minimum)
Cisco UCS C220 M3	16 x 300	128
Cisco UCS C220 M4	16 x 300	128

- Cisco UCS hardware should have adequate CPU, Memory and hard disk capacities:

CPU	Hard Disk (GB)	Memory (GB)	Network Interfaces
2	4	1 x 32 (root)	1 Public

- **Network Mapping**:
  - NET0 — vSwitch0 — Controller Network
  - NET1 — vSwitch1 — Simulcrypt Synchronizer (SCS) Network

Software Requirements

The following software is required for the PCG 4.0 installation.

- Requires a vCenter Web UI login or a vSphere client to connect and perform management tasks.
  - A vCenter login must have admin privileges to deploy VMs.
- Reserve two static IP addresses:
  - One for the network interface to the client (EC or DTACS server).
  - One for the Simulcrypt Synchronizer (SCS).
- Obtain the associated domain name server, default gateway and network mask values from your system administrator.
- Download the following software from your customer-specific forum on Cisco's File Exchange Server and save it to a local directory that is accessible to the vSphere or the ESXi host.
  - PCG Linux VMware OVA (i.e. PCG-[VERSION].ova)
  - PCG Application Package
    - **EC 8.0/DTACS 5.0**: CSCOec-pcg-[VERSION].x86_64.rpm
    - **EC 7.x/DTACS 4.1**: PCG-[VERSION].iso

2

Install the Software on the EC/DTACS Server

This chapter provides the procedure to install or upgrade the PCG package to your EC/DTACS system.

Notes:

- Make sure the RPM or ISO version you plan to install matches the OVA version that will be deployed to build the PCG VM.
- If you did not yet download the PCG ISO file to your local system, refer to ***Software Requirements*** (on page 3) to do so now.

In This Chapter

- Installing the PCG Package on the EC 8.0 or DTACS 5.0 Server 6
- Installing the PCG Package on an EC 7.x or DTACS 4.1 Server 8

Installing the PCG Package on the EC 8.0 or DTACS 5.0 Server

Complete the following steps to install the PCG package on an EC 8.0 or DTACS 5.0 server.

1. Copy the **PCG-[VERSION].iso** (i.e. PCG-4.0.3-2.iso) to the **/var/tmp/** directory on your EC or DTACS server.
2. Log into the EC or DTACS controller as **admin** user.
3. Enter the following command to create a temporary directory in **/var/tmp**.

   Command Syntax:

   ```
   sudo mkdir -p /var/tmp/[directory_name]
   ```

   Example:

   ```
   [admin@EC/DTACS ~]$ sudo mkdir -p /var/tmp/pcg-mnt
   ```

4. Enter the following command to mount the lofi device on the temporary directory you created in the previous step.

   Command Syntax:

   ```
   sudo mount -t iso9660 -o loop /var/tmp/PCG-[VERSION].iso
   /var/tmp/[directory_name]
   ```

   Example:

   ```
   [admin@EC/DTACS ~]$ sudo mount -t iso9660 -o loop
   /var/tmp/PCG-4.0.3-2.iso /var/tmp/pcg-mnt
   ```

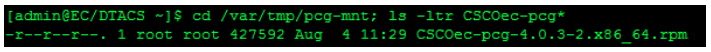
5. Change to the new directory and then enter the following command to verify that the **CSCOec-pcg** rpm is present in the directory.

   Command Syntax:

   ```
   cd /var/tmp/[directory_name]; ls -ltr CSCOec-pcg*
   ```

   Example:

   ```
   [admin@EC/DTACS ~]$ cd /var/tmp/pcg-mnt; ls -ltr CSCOec-pcg*
   ```

6. Enter the following command to install the **CSCOec-pcg** package on the EC or DTACS server. An **Is this ok [y/N]** prompt appears.

   Command Syntax:

   ```
   sudo yum install CSCOec-pcg-[VERSION].x86_64.rpm
   ```

   Example:

   ```
   [admin@EC/DTACS ~]$ sudo yum install
   CSCOec-pcg-4.0.3-2.x86_64.rpm
   ```

```
Marking CSCOec-pcg-4.0.3-2.x86_64.rpm to be installed
solution-base                                                | 3.0 kB     00:00
solution-base/primary_db                                     | 311 kB     00:00
upstream-base                                                | 3.0 kB     00:00
upstream-updates                                             | 3.0 kB     00:00
Resolving Dependencies
--> Running transaction check
---> Package CSCOec-pcg.x86_64 0:4.0.3-2 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package            Arch           Version           Repository              Size
================================================================================
Installing:
 CSCOec-pcg         x86_64         4.0.3-2           /CSCOec-pcg-4.0.3-2.x86_64  1.3 M

Transaction Summary
================================================================================
Install       1 Package(s)

Total size: 1.3 M
Installed size: 1.3 M
Is this ok [y/N]:
```

7 When prompted to confirm the installation, type **y** and press **Enter**. The package is downloaded and installed.

```
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : CSCOec-pcg-4.0.3-2.x86_64                                   1/1
Modifying pcg.cfg....
  Verifying  : CSCOec-pcg-4.0.3-2.x86_64                                   1/1

Installed:
  CSCOec-pcg.x86_64 0:4.0.3-2

Complete!
```

8 Enter the following command to verify that the PCG package is installed.

```
[admin@EC/DTACS ~]$ rpm -qa CSCOec-pcg
```

```
[admin@EC/DTACS pcg-mnt]$ rpm -qa CSCOec-pcg
CSCOec-pcg-4.0.3-2.x86_64
```

9 Enter the following commands to unmount and delete the temporary directory.

Command Syntax:

```
cd
sudo umount /var/tmp/[directory_name]
sudo rm -rf /var/tmp/[directory_name]
```

Example:

```
[admin@EC/DTACS ~]$ cd
[admin@EC/DTACS ~]$ sudo umount /var/tmp/pcg-mnt
[admin@EC/DTACS ~]$ sudo /var/tmp/pcg-mnt
```

Installing the PCG Package on an EC 7.x or DTACS 4.1 Server

Complete the following steps to install the PCG package on an EC 7.x or a DTACS 4.1 server.

1 Copy the **PCG-[VERSION].iso** (i.e. PCG-4.0.3-2.iso) to the **/var/tmp/** directory on your EC or DTACS controller.

2 Log into the EC or DTACS server as an Administrative user and then change to **root** user.

3 Enter the following command to change to the **/var/tmp** directory.

```
# cd /var/tmp
```

4 Enter the following commands to prepare the ISO to be mounted as a loopback device.

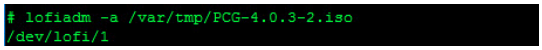
Note: Document the device name that is created as you will need it later in this procedure.

Command Syntax:

```
lofiadm -a /var/tmp/PCG-[VERSION].iso
```

Example:

```
# lofiadm -a /var/tmp/PCG-4.0.3-2.iso
```



Result: The device name is /dev/lofi/1.

5 Enter the following command to create a temporary directory in /var/tmp.

Command Syntax:

```
mkdir /var/tmp/[directory_name]
```

Example:

```
# mkdir -p /var/tmp/pcg-mnt
```

6 Using the device name from the output of Step 4, enter the following command to mount the lofi device on the temporary directory.

Command Syntax:

```
mount -o ro -F hsfs [device_name] /var/tmp/[directory_name]
```

Example:

```
# mount -o ro -F hsfs /dev/lofi/1 /var/tmp/pcg-mnt
```

7 Enter the following command to verify the mount point.

```
# df -k | tail
```

```
# df -h | tail
rpool/disk1            125G   2.9G    93G     4%    /disk1
dpool/backups          125G    27M   123G     1%    /disk1/dvs/backups
dpool/corefiles        125G    31K   123G     1%    /disk1/dvs/corefiles
dpool/tmp              125G   1.9G   123G     2%    /disk1/dvs/dncs/tmp
dpool/disk2            125G    25M   123G     1%    /disk2
dpool                  125G    36K   123G     1%    /dpool
rpool/export           125G    32K    93G     1%    /export
rpool/export/home      125G   822M    93G     1%    /export/home
rpool                  125G    45K    93G     1%    /rpool
/dev/lofi/1            2.6M   2.6M     0K   100%    /var/tmp/pcg-mnt
```

Mount point

8 Enter the following command change to the temporary directory.

Command Syntax:

```
cd /var/tmp/[directory_name]
```

Example:

```
# cd /var/tmp/pcg-mnt
```

9 Enter the following command to convert the SAIpcg package to the standard package format. You are prompted to select the package you want to process.

Command Syntax:

```
pkgtrans SAIpcg-[VERSION].pkg /var/tmp
```

Example:

```
# pkgtrans SAIpcg-4.0.3-2.pkg /var/tmp
```

```
# pkgtrans SAIpcg-4.0.2.pkg /var/tmp

The following packages are available:
  1  SAIpcg     PowerKEY CAS Gateway
                (SunOS_all) 4.0.2

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

10 Enter the value next to the SAIpcg package and press **Enter**. The package conversion completes.

Note: If the SAIpcg is the only package listed, you can simply press **Enter**.

```
Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]: 1
Transferring <SAIpcg> package instance
```

11 Enter the following command to go back one directory level.

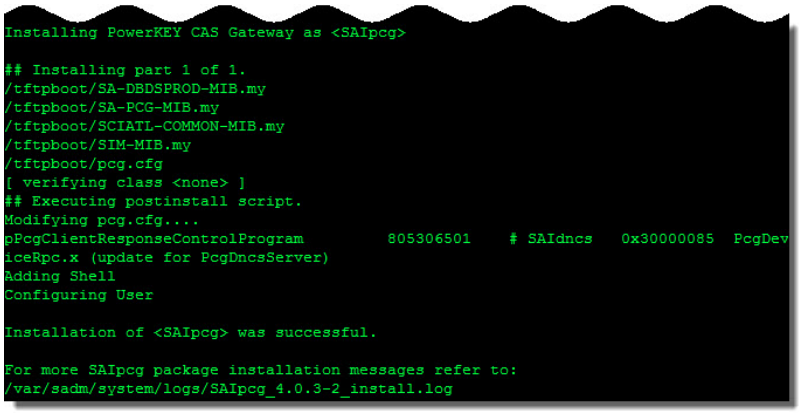
```
# cd ../
```

12 Enter the following command to install or upgrade the **SAIpcg** package. You are prompted to confirm the installation.

```
# install_pkg
```

```
# install_pkg

Checking the system, please wait...

*******************************************************************************

This script will install the following packages on "vodwater":

SAIpcg          PowerKEY CAS Gateway
                4.0.3-2

*******************************************************************************

Are you SURE you want to continue?  [y,n,?,q] y
```

13 Enter **y** and press **Enter**. The SAIpcg package is installed.



14 Enter the following commands to clean up the temporary files and unmount the temporary directory.

Command Syntax:

```
umount /var/tmp/[temporary_directory]
lofiadm -d [device_name]
rm -rf /var/tmp/SAIpcg /var/tmp/SAIpcg-[VERSION]
/var/tmp/[temporary_directory]
```

Example:

```
# umount /var/tmp/pcg-mnt
# lofiadm -d /dev/lofi/1
# rm -rf /var/tmp/SAIpcg /var/tmp/SAIpcg-4.0.3-2
/var/tmp/pcg-mnt
```

3

Deploy the PCG Virtual Machine

This chapter describes how to deploy the PCG virtual machine using the PCG Linux platform OVA that you downloaded to your local PC.

Note: If you did not yet downloaded the PCG OVA to your local system, refer to ***Software Requirements*** (on page 3) to do so now.

In This Chapter

- Deploying the PCG Virtual Machine from the vSphere Web UI 12
- Reconfiguring the PCG Virtual Hardware 14
- Power On and Login to the New PCG Virtual Machine 15
- Configuring the PCG Network 16
- Installing VMware Tools (Optional) 17

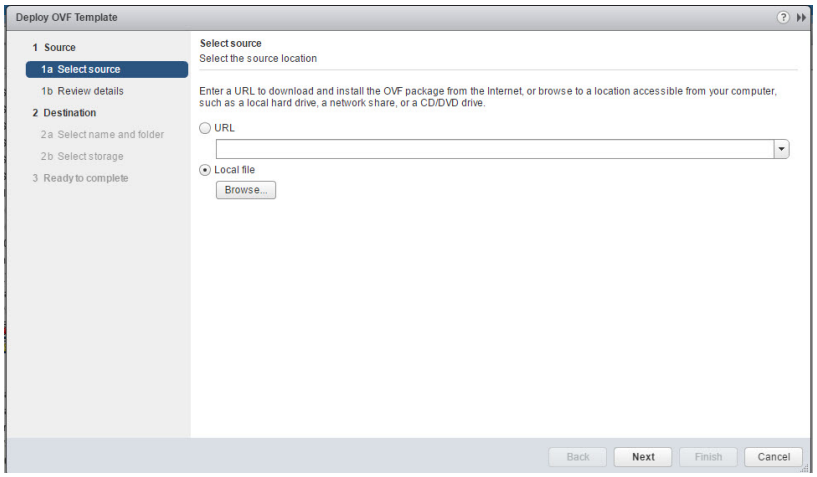
Deploying the PCG Virtual Machine from the vSphere Web UI

Complete the following procedure to deploy the PCG VM using the PCG OVA.

Important: This procedure is written using the vSphere Web UI. If you are not using vSphere, go to *Appendix B, Deploy the PCG Virtual Machine from an ESXi Client* (on page 47).

1 Login to the vSphere Web UI and go to the **Hosts and Clusters** view.

2 Right-click the ESXi host where you want to deploy the VM and then select **Deploy OVF Template**. The Select source window displays.



3 Click the **Local file** radio button and then click **Browse**.

4 Navigate to the directory location where you saved the PCG OVA. Select the PCG OVA and click **Open**. The absolute path of the PCG OVA is displayed next to the Browse button.

5 Click **Next**. The Review details window displays.

6 Review the details and click **Next**. The Accept EULAs window displays.

7 Review the license agreement and click **Accept**. Then click **Next**. The Select name and folder window display.

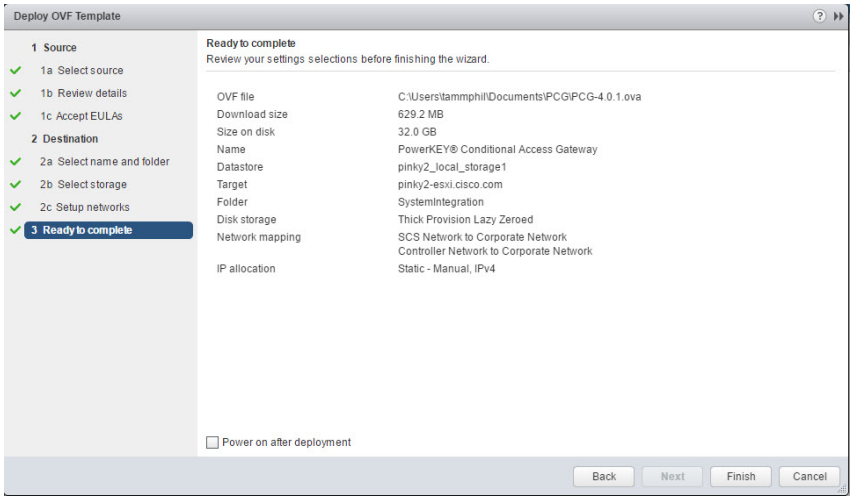
8 In the **Name** box, type a name that describes the PCG VM (i.e. PCG_4.0).

9 Select the folder (datastore) where you want to build the PCG VM. The Select storage window displays.

10 From the **Select virtual disk format** dropdown menu, select **Thick Provision Lazy Zeroed**.

11 Verify that the correct datastore is listed and highlighted. Then click **next**. The Setup networks window displays.

12 Select the appropriate **Destination Network** for each Source Network. Then click **Next**. The Ready to Complete window displays.



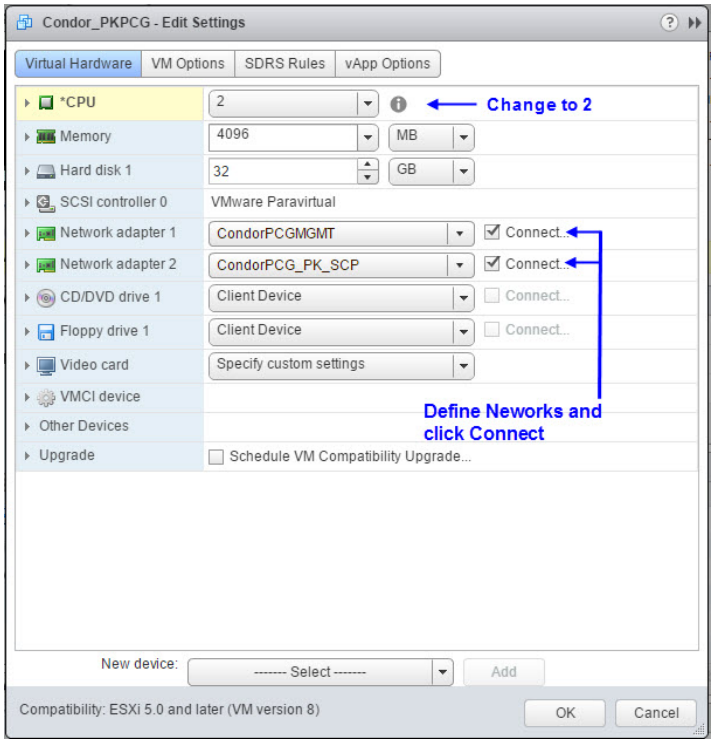
13 Review the details and click **Finish**.

14 Monitor the deployment of the VM from the **Recent Tasks** area to verify that the VM successfully deployed.

Reconfiguring the PCG Virtual Hardware

Complete the following procedure to reconfigure the virtual hardware for the PCG VM.

1. Right-click the VM and select **Edit Settings**. The Virtual Machine Properties window displays.
2. From the **CPU** dropdown menu, select **2**.
3. From the **Network adapter 1** dropdown, select the management/controller interface for your network. Then click **Connect**.
4. From the **Network adapter 2** dropdown, select the SCS interface for your network. Then click **Connect**.



5. Click **OK** to reconfigure the VM.
6. Monitor the **Recent Tasks** area to confirm that the VM virtual hardware is successfully reconfigured.

Power On and Login to the New PCG Virtual Machine

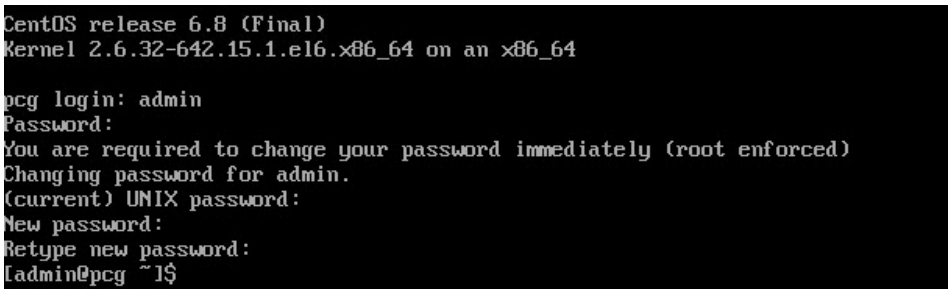
Complete the following steps to power on and login to the new PCG VM.

1. Select and right-click the PCG VM and select **Power On**.
2. Right-click the VM again and select **Open Console**.
3. Log into the VMware console with the following credentials:

   User Name: admin

   Password: password

   Important: The admin user has full root privileges via the sudo command. Direct root access is not permitted.
4. Press **Enter**. You are prompted to change the password. Please change it to something appropriate for your environment.
5. At the **(current) UNIX password** prompt, re-enter the default password which is **password**.
6. At the **New password** prompt, enter a new password.
7. At the **Retype new password** prompt, re-enter the new password. The admin prompt displays.



Configuring the PCG Network

Complete the following steps to configure the PCG network.

Note: You should be logged into the PCG VM from a Console window.

1 Type the following command to configure the network interfaces and to set the hostname for the PCG server.

Notes:

- Substitute the hostname for your system for [hostname]. In this example, the hostname is set to pcg1_lab.
- The network interfaces will be set to loopback interfaces.

Command Syntax:

```
sudo /usr/local/bin/pcgifcfg [hostname] commit
```

Example:

```
[admin@pcg ~]$ sudo /usr/local/bin/pcgifcfg pcg1_lab commit
```

```
[admin@pcg ~]$ sudo /usr/local/bin/pcgifcfg pcg1_lab commit


All network interfaces have been set to loopback (unreachable) IP addresses as
required by the PCG software. You must reboot to activate these changes. Please
verify these before rebooting. You will lose all network connectivity. The
files in question are /etc/sysconfig/network-scripts/ifcfg-eth*.
```

2 Enter the following command to reboot the PCG server and activate the changes.'

```
[admin@pcg ~]$ sudo reboot
```

3 Log back into the PCG server as **admin** user.

4 Enter the following command to display the mapping of the network interfaces to MAC addresses.

Important: The MAC addresses shown in this output are examples. The output for your system will be different.

```
[admin@pcg ~]$ sudo /usr/local/bin/pcgifmap
```

```
[admin@pcg1-lab ~]$ sudo /usr/local/bin/pcgifmap
eth0: 00:50:56:8b:5c:e2
eth1: 00:50:56:8b:00:ca
```

5 Record the eth0 MAC address from your output as it is required to configure the PCG via the EC/DTACS Web interface in a later procedure.

eth0: _____

Installing VMware Tools (Optional)

The installation of VMware Tools is optional. If you wish to install VMware Tools on the PCG machine, follow the instructions provided by VMware.

- ***Installing and Configuring VMware Tools*** (***http//:www.vmware.com/pdf/vmware-tools-installation-configuration.pdf***)
- ***VMware KB 1018414*** (***http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1018414***)

Abbreviated Procedure

Complete the following steps to install VMware Tools.

1. Click the link in vCenter to make the VMware Tools CD available to the PCG VM.
2. As **admin** user, enter the following command to change to **root** user.
   ```
   [admin@pcg1_lab]$ sudo -i
   ```
3. Enter the following command to mount the virtual cdrom.
   ```
   [admin@pcg1_lab]# mount -o ro /dev/cdrom /mnt
   ```
4. Enter the following command to change to the **/root** directory.
   ```
   [admin@pcg1_lab]# cd /root
   ```
5. Enter the following command to extract the VMware Tools tar file.
   ```
   [admin@pcg1_lab]# tar xzpf /mnt/VMwareTools-*.tar.gz
   ```
6. Enter the following command to install the VMware Tools using the default options.
   ```
   [admin@pcg1_lab]# ./vmware-tools-distrib/vmware-install.pl -d
   ```

4

Provision the PCG on the EC/DTACS Web UI

This chapter includes the procedures to provision the PCG VM on the EC/DTACS Web UI. Once the PCG is configured in the Web UI, the PCG is reset. During the reset, the EC/DTACS server responds by provisioning the PCG according to the new settings.

Note: Ethernet settings can be used to communicate with the SCS, which can provision the PCG with scrambler or SCS device IP addresses and parameters (i.e. maximum number of scrambling control groups (SCGs)).

In This Chapter

- Provisioning the PCG on the EC Web UI 20
- Provisioning the PCG on the DTACS Web UI 24

Provisioning the PCG on the EC Web UI

Complete the following procedure to provision the PCG on the EC Web UI.

Important: This procedure is written for both EC 8.0 and EC 7.x.

1 Enter the appropriate values in the following table as they are required to provision the PCG on the EC.

Notes:

- The Controller IP address, subnet mask and default gateway, as well as the SCS IP address and subnet mask should be obtained from your System Administrator.
- Obtain the PCG eth0 MAC address that you recorded in ***Configuring the PCG Network*** (on page 16).

Parameter	Value
Control IP Address	
Control Subnet Mask	
Control Default Gateway	
SCS IP Address	
SCS Subnet Mask	
Control MAC Address (eth0)	

2 Login to the EC Web UI as an administrative user (i.e. ecadmin).

3 Depending on your EC version, use one of the following methods to navigate to the Powerkey CAS Gateway List Web UI.

Important: The PCG feature must be enabled as a licensed feature. If PCG is not yet enabled, contact Cisco Services.

- **SR 8.0**: Click the **Navigation** button,  , and then select **Network Element Provisioning > PCG**.
- **SR 7.x**: Click the **EC** dropdown menu and then select **Network Element Provisioning > PCG**.

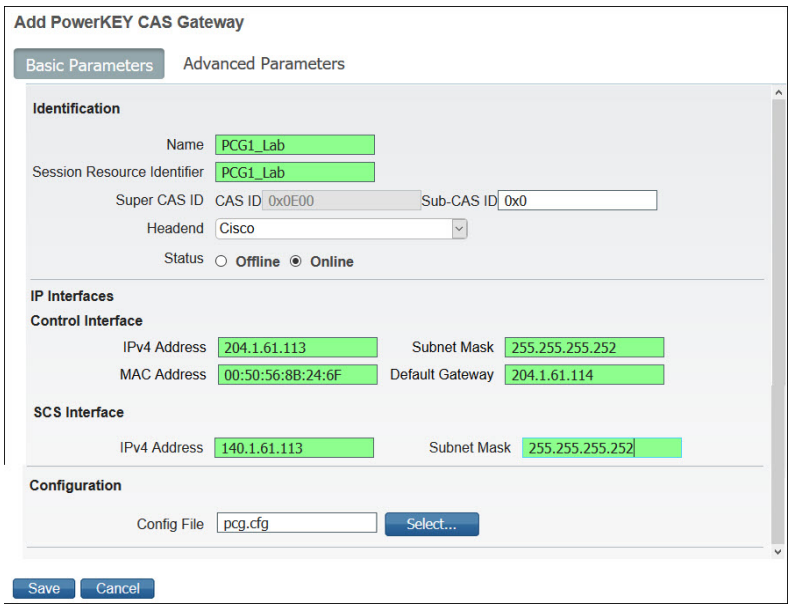
4 Click **Add**. The Add PowerKEY CAS Gateway window displays and the Basic Parameters display by default.

5 Enter the values you recorded in Step 1 in the appropriate fields.

Note: The values for the fields appended with an asterisk (*) were recorded in Step 1 of this procedure.

Field	Description
Name	A unique name for the PCG
Session Resource Identifier	A unique identifier for the PCG. It can be the same as the Name
Sub-CAS ID	Default is 0x0
Headend	Select the appropriate headend
Status	Set the status to Offline or Online
Control Interface IPv4 Address*	The IP address of the Control interface on the PCG
Control Interface Subnet Mask*	The subnet mask of the Control interface on the PCG
Control Interface MAC Address*	The MAC address of the Control interface (e.g. eth0) on the PCG
Control Interface Default Gateway*	The default gateway of the Control interface on the PCG
SCS Interface IPv4 Address*	The IP address of the SCS interface (e.g. eth1) on the PCG
SCS Interface Subnet Mask*	The subnet mask of the SCS interface on the PCG
Config File	The name of the PCG application configuration file. This file is installed, when the PCG application is installed on the EC. The default is pcg.cfg

Example:

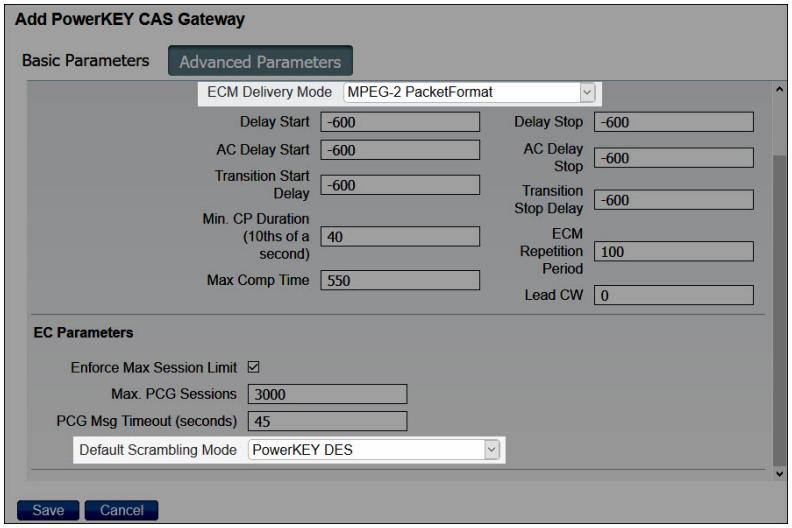


6 Click the **Advanced Parameters** tab. The Advanced Parameters window displays.

7 Define the following values for the fields shown below.

Field	Description
ECM Delivery Mode	Select MPEG2 PacketFormat
Default Scrambling Mode	Select PowerKEY DES

Example:



8 Click **Save**. You are returned to the PowerKEY CAS Gateway List window. The PCG you provisioned and saved appears in the list.

9 Select the radio button next to the new PCG and click **Reset Device**. The EC provisions the PCG according to the new settngs.

10 As **dncs** user in an EC terminal window, type the following command to monitor the bootp log and verify that the PCG is successfully provisioned.

```
[dncs@vodwater root]$ qtail bootp
```

```
.
.
Aug 17 12:02:47 bootpd: info(6):   recvd pkt from IP addr 204.1.61.114
Aug 17 12:02:47 bootpd: info(6):   request from Ethernet address 00:50:56:8B:24:6F
Aug 17 12:02:47 bootpd: info(6):   unknown client Ethernet address 00:50:56:8B:24:6F, lookin
g into DNCS.
Aug 17 12:02:47 bootpd: info(6):   DNCS PCG[pcg_204.1.61.113:ht=ethernet:sm=255.255.255.252:
ip=204.1.61.113:ha=0x0050568B246F:vm=rfc1048:gw=204.1.61.114:sa=dncsatm:bf=pcg.cfg:vm=rfc104
8:]
Aug 17 12:02:47 bootpd: info(6):   DNCS found info for client Ethernet address 00:50:56:8B:2
4:6F.
Aug 17 12:02:47 bootpd: info(6):   found 204.1.61.113 (pcg_204.1.61.113)
Aug 17 12:02:47 bootpd: info(6):   bootfile="/pcg.cfg"
Aug 17 12:02:47 bootpd: info(6):   vendor magic field is 99.130.83.99
Aug 17 12:02:47 bootpd: info(6):   sending reply (with RFC1048 options)
Aug 17 12:02:47 bootpd: info(6):   sending reply to gateway 204.1.61.114
Aug 17 12:02:47 bootpd: info(6):   sendto port is: 67
```

11 When you have verified the bootp for the PCG device, enter **Ctrl+C** to exit the qtail session.

12 As **admin** user on the EC, enter the following command to verify that you can successfully SSH into the PCG server.

Command Syntax:

```
ssh admin@[Control IP Address]
```

Example:

```
[admin@vodwater ~]$ ssh admin@204.1.61.113
```

13 When prompted to continue with the connection, type **yes** and press **Enter**.

14 When prompted, enter the password for the **admin** user on the PCG server. You are successfully logged into the PCG server.

Provisioning the PCG on the DTACS Web UI

Complete the following procedure to provision the PCG on the DTACS Web UI.

Note: This procedure is written for both DTACS 5.0 and DTACS 4.1.

1 Enter the appropriate values in the following table as they are required to provision the PCG on the DTACS.

Important:

- The Controller IP address, subnet mask and default gateway, as well as the SCS IP address and subnet mask should be obtained from your System Administrator.
- Obtain the PCG eth0 MAC address that you recorded in ***Configuring the PCG Network*** (on page 16).

Parameter	Value
Control IP Address	
Control Subnet Mask	
Control Default Gateway	
SCS IP Address	
SCS Subnet Mask	
Control MAC Address (eth0)	

2 Login to the DTACS Web UI as an administrative user (i.e. dtacsadmin).

3 Depending on your DTACS version, use one of the following methods to navigate to the PCG Web UI.

- **SR 5.0**: Click the **Navigation** button,  , and then select **Network Elements > PCG**.
- **SR 4.1**: Click the **DTACS** dropdown menu and then select **Network Elements > PCG**.

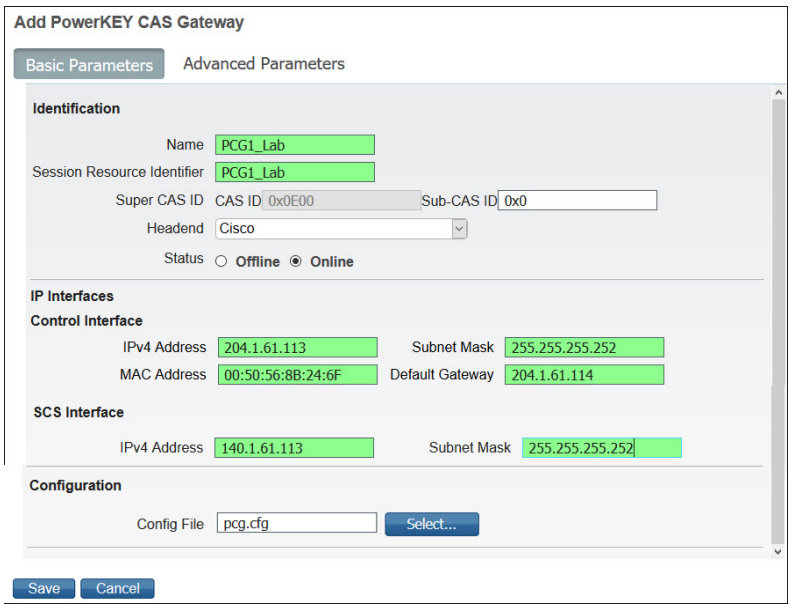
4 Click **Add**. The SCC CAS Gateway List window display and the Basic Parameters display by default.

5 Enter the values you recorded in Step 1 in the appropriate fields.

Note: The values for the fields appended with an asterisk (*) were recorded in Step 1 of this procedure.

Field	Description
Name	A unique name for the PCG
Session Resource Identifier	A unique identifier for the PCG. It can be the same as the Name.
Sub-CAS ID	Default is 0x0
Control Interface IPv4 Address	The IP address of the Control interface on the PCG
Control Interface Subnet Mask	The subnet mask of the Control interface on the PCG
Control Interface MAC Address	The MAC address of the Control interface (eth0) on the PCG
Control Interface Default Gateway	The default gateway for the of the Control interface on the PCG
SCS Interface IPv4 Address	The IP address of the SCS interface on the PCG
SCS Interface Subnet Mask	The subnet mask of the SCS interface on the PCG
Config File	The name of the PCG application configuration file. This file is installed, when the PCG application is installed on the DTACS. The default is pcg.cfg

Example:

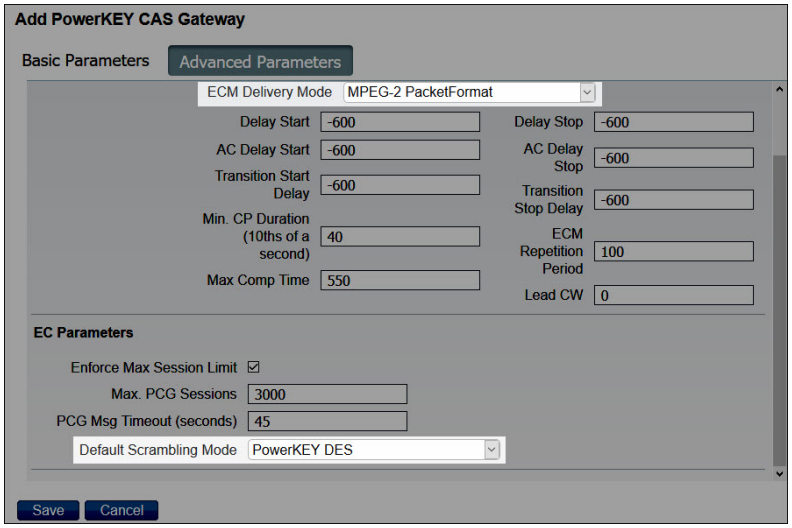


6 Click the **Advanced Parameters** tab. The Advanced Parameters window displays.

7 Define the following values for the fields shown below.

Field	Description
ECM Delivery Mode	Select MPEG2 PacketFormat
Default Scrambling Mode	Select PowerKEY DES

Example:

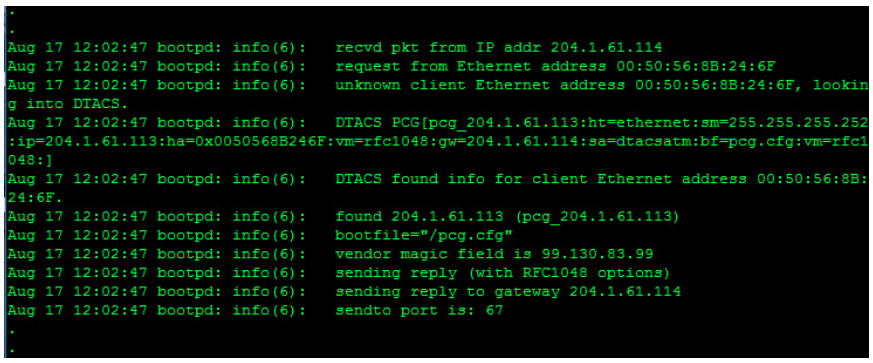


8 Click **Save**. You are returned to the SCC CAS Gateway List window. The PCG you provisioned and saved appears in the list.

9 Select the radio button next to the new PCG and click **Reset Device**. The DTACS provisions the PCG according to the new settings.

10 As **dncs** user in a DTACS terminal window, type the following command to monitor the bootp log and verify that the PCG is successfully provisioned.

```
[dncs@dtacs_50 root]$ qtail bootp
```



11 When you have verified the bootp for the PCG device, enter **Ctrl+C** to exit the qtail session.

12 As **admin** user, enter the following command to verify that you can successfully SSH into the PCG server.

Command Syntax:

```
ssh [Control IP Address]
```

Example:

```
[admin@dtacs_50 ~]$ ssh 204.1.61.113
```

13 When prompted to continue with the connection, type **yes** and press **Enter**.

14 When prompted, enter the password for the **admin** user on the PCG server. You are successfully logged into the PCG server.

5

Verify PCG Versions

This chapter describes the procedures to verify the PCG version from the EC and the DTACS servers, as well as from the PCG server.

In This Chapter

- Verifying PCG Package Versions on the EC/DTACS..... 30
- Verifying the PCG Version on the PCG Server..... 31

Verifying PCG Package Versions on the EC/DTACS

Important: The EC/DTACS dictates what PCG version should be loaded on the PCG servers.

Complete the following steps to verify the PCG version installed on the EC or DTACS server.

1 From the EC or DTACS terminal window, enter the following command to verify the version of the PCG package currently installed.

EC 8.0/DTACS 5.0:

```
[admin@EC/DTACS ~]$ rpm -qa | grep i pcg
```

```
[admin@EC/DTACS ~]$ rpm -qa | grep -i pcg
CSCOec-pcg-4.0.3-2.x86_64
```

EC 7.x/DTACS 4.x:

```
$ pkginfo -l SAIpcg
```

```
   PKGINST:  SAIpcg
      NAME:  PowerKEY CAS Gateway
  CATEGORY:  application
      ARCH:  SunOS_all
   VERSION:  4.0.3-2
   BASEDIR:  /
    VENDOR:  Cisco Inc.
      DESC:  PCG 4.0.3-2
    PSTAMP:  lwr-dbds-lxplat3-dev1.cisco.com20170804112859
 INSTDATE:  Aug 17 2017 15:20
    STATUS:  completely installed
     FILES:        9 installed pathnames
                   3 executables
                2793 blocks used (approx)
```

2 To determine the PCG version on the PCG server, go to ***Verifying the PCG Version on the PCG Server*** (on page 31).

Verifying the PCG Version on the PCG Server

Important: Do ***NOT*** use the rpm command to verify the version of the PCG package as the output of the rpm command only reflects the PCG version loaded during initial installation. Therefore, it may not match the actual version of the PCG code that is running.

Complete the following steps to determine the current version of the PCG application installed on the PCG server.

1 From the EC/DTACS terminal window, SSH into the PCG server as **admin** user.

Command Syntax:

```
ssh admin@[PCG_IP]
```

Example:

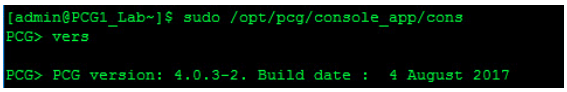
```
[admin@EC/DTACS ~]$ ssh admin@204.1.61.113
```

2 Enter the following command to access the PCG console application.

```
[admin@pcg1_lab ~]$ sudo /opt/pcg/console_app/cons
```

3 At the **PCG>** prompt, enter the following command to verify the version of the PCG package currently installed.

```
PCG> vers
```



Result: The PCG version on the EC/DTACS and the PCG server should match.

4 Does the PCG version match the PCG version on the EC/DTACS server?

- If **yes**, you have completed this procedure.
- If **no**, go to ***Upgrade the PCG Server*** (on page 55).

6

Configure SNMPv2

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks.

This chapter describe how to configure SNMPv2 and SNMPv3 for the PCG device.

In This Chapter

- Configuring SNMPv2 34
- Configuring SNMPv3 35

Configuring SNMPv2

Complete the following procedure to configure SNMPv2 on the PCG.

1. If you are not logged into the PCG, login as **admin** user.
2. Enter the following command to edit the **/etc/snmp/snmpd.conf** file.

   ```
   [admin@pcg1_lab ~]$ sudo vi /etc/snmp/snmpd.conf
   ```

3. Move to the end of the file and add the following three lines.

   Line Syntax:

   ```
   agentaddress [PCG eth0 IP]:161
   rocommunity [community_name]
   trapsess -v2c -c [community_name][destination_host]:[port]
   ```

   Example:

   ```
   agentaddress 204.1.61.105:161
   rocommunity public
   trapsess -v2c -c public 204.123.1.33:162
   ```

   Notes:

   - Replace [PCG eth0 IP] with the IP address of the eth0 network interface.
   - Replace [community_name] with the desired SNMP community name.
   - Replace [destination_host]:[port] with the IP address and port of the SNMP trap listener.

4. Save and close the file.
5. Enter the following command to stop the SNMP service.

   ```
   [admin@pcg1_lab ~]$ sudo service snmpd stop
   ```

6. Enter the following command to start the SNMP service.

   ```
   [admin@pcg1_lab ~]$ sudo service snmpd start
   ```

7. Enter the following command to verify that the SNMP service is running.

   ```
   [admin@pcg1_lab ~]$ sudo service snmpd status
   ```

Configuring SNMPv3

Creating the SNMPv3 User

Complete the following steps to create an SNMPv3 user.

Note: Refer to the SNMP RFCs for SNMPv3 username and passphrase constraints.

1 Enter the following command to stop the SNMP service.

```
[admin@pcg1_lab ~]$ sudo service snmpd stop
```

2 Enter the following command to create the SNMPv3 user.

```
[admin@pcg1_lab ~]$ sudo /usr/bin/net-snmp-create-v3-user
```

3 When prompted for SNMPv3 user name, enter a user name and press **Enter**.

4 When prompted for an authentication password, enter a password and press **Enter**.

5 When prompted for an encryption pass-phrase, either type a password and press **Enter** or press **Enter** to use the same password as the authentication password.

Result: The /var/lib/net-snmp/snmpd.conf is updated and the SNMPv3 user is created.

```
[admin@pcg1_lab ~]$ /usr/bin/net-snmp-create-v3-user
Enter a SNMPv3 user name to create:
snmp
Enter authentication pass-phrase:
snmp
Enter encryption pass-phrase:
  [press return to reuse the authentication pass-phrase]

adding the following line to /var/lib/net-snmp/snmpd.conf:
   createUser snmp MD5 "snmp" DES
adding the following line to /etc/snmp/snmpd.conf:
   rwuser snmp
```

Changing the SNMPv3 User Options

1 Open the **/etc/snmp/snmpd.conf** file and go to the end of the file to the rwuser line.

Note: The SNMPv3 user name you created will be at the end of the rwuser line.

2 Go to the end of the line and add **authPriv** after the new username entry.

Example:

```
rwuser snmp authPriv
```

3 Next, change rwuser to **rouser**. This allows read-only SNMP operations.

Example:

```
rouser snmp authPriv
```

4 Save and close the **snmpd.conf** file.

Restart the SNMP Service

1. Enter the following command to stop the SNMP service.

```
[admin@pcg1_lab ~]$ sudo service snmpd stop
```

2. Enter the following command to start the SNMP service.

```
[admin@pcg1_lab ~]$ sudo service snmpd start
```

3. Enter the following command to verify that the SNMP service is running.

```
[admin@pcg1_lab ~]$ sudo service snmpd status
```

Defining the SNMPv3 Trap Destination

Complete the following steps to define the SNMPv3 trap destination.

1. Enter the following command to stop the SNMP service.

```
[admin@pcg1_lab ~]$ sudo service snmpd stop
```

2. Add the following line to the **/etc/snmpd/snmpd.conf** file.

   Line Syntax:

```
trapsess -v3 -u [username] -l authPriv -a [authProt] -x
[privProt] [trapDestIP]:[trapDestPort
```

   Example:

```
[admin@pcg1_lab ~]$ sudo trapsess -v3 -u snmp -l authPriv -a
SHA -x DES 204.123.1.33:162
```

   Notes:

   - Replace <username> with the SNMPv3 username.
   - Replace <trapDestIP> with the IP address of the SNMP trap receiver.
   - Replace <trapDestPort> with the port number of the SNMP trap receiver (typically 162). The -l option can be set to noAuthNoPriv, authNoPriv, or authPriv but is recommended to be authPriv.
   - Replace <authProt> with the authentication protocol defined for the SNMPv3 user: MD5 or SHA.
   - Replace <privProt> with the encryption (privacy) protocol defined for the SNMPv3 user: DES or AES.

3. Enter the following command to start the SNMP service.

```
[admin@pcg1_lab ~]$ sudo service snmpd start
```

A

Hardware Configuration Procedures for the Cisco UCS C220 Server

This appendix describes the server hardware and explains how to configure it for initial use with the PCG system.

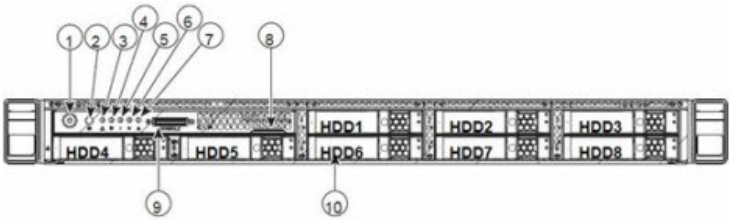
In This Appendix

- Cisco UCS C220 Server Diagram 38
- Cisco UCS C220 Server CIMC Configuration 40
- RAID Configuration 42

Cisco UCS C220 Server Diagram

Chassis Front View

The following diagram displays the chassis front view of the Cisco UCS C220 Server.

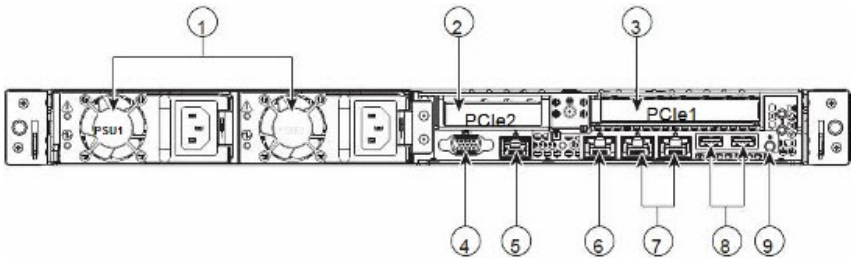


Field	Description
1	Power button or power status LED
2	Identification button or LED
3	System status LED
4	Fan status LED
5	Temperature status LED
6	Power supply status LED
7	Network link activity LED
8	Pull-out asset tag
9	KVM connector (used with KVM cable that provides two USBs, one VGA, and one serial connector)
10	Drives hot-swappable (up to eight 2.5-inch drives)

Chassis Rear View

The following diagram displays the chassis rear view of the Cisco UCS C220 server.

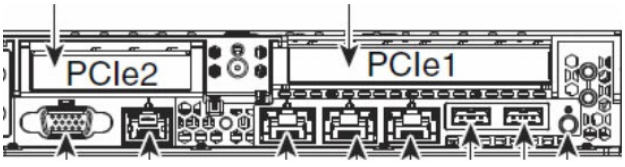
Note: Only the essential features of the rear panel are shown in this image. Also, be certain that the network cards are installed in the slots as shown in this diagram.



Field	Description
1	Power supplies
2	Low-profile PCIe slot 2 on riser (half-height, half-length, x8 lane)
3	Standard-profile PCIe slot on riser (full-height, half-length, x16 lane)
4	VGA video connector
5	Serial port (RJ-45 connector)
6	1-Gb Ethernet dedicated management port
7	Dual 1-Gb Ethernet ports (LAN1 and LAN2)
8	USB ports
9	Rear identification button or LED

Detailed View of PCI Ports

The following diagram shows the detailed view of the PCI Ports.



Note: For the PCIe1 card, the top row contains ports 2, 3, 4, and 5. The bottom row contains ports 0 and 1.

Cisco UCS C220 Server CIMC Configuration

Notes:

- The CIMC firmware and BIOS version should be at or higher than the minimum required version shown in ***Tested Reference Configuration*** section located in the ***Preface*** (on page v). If it does not meet these requirements, contact Cisco Services for assistance in upgrading the firmware and the BIOS.
- You have to perform this procedure only once, that is, when you initially install the UCS C220.
- Be sure that you use configuration data that pertains to the system that you are migrating.

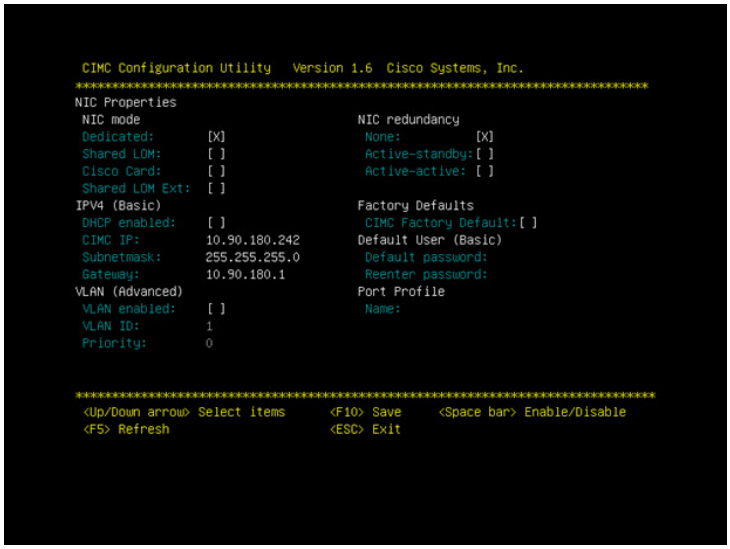
Complete the following steps to configure the Cisco UCS C220 server.

1. Follow the instructions in the ***UCS Server Installation and Service Guide***. This guide is shipped with the server.
2. Press the **Power** button to power on the UCS C220 server.
3. Press **F8** at the Cisco splash screen. The server boots to the CIMC Configuration Utility window.

   Important: Note the BIOS version on the Cisco splash screen as the system is booting.
4. Use the information in the CIMC Configuration Utility window to complete the configuration.

   Note: In addition to the information in the CIMC Configuration Utility window, be sure to obtain the network IP address for the CIMC interface.

   Important: The following image is an example only. Do not use the IP address, netmask, or gateway in the image.



5 Enter a default password and re-enter it at the prompt.
Note: Store this password in a safe place for future use.

6 Press **F10** to save changes.

7 Press **Esc** to exit. The EFI shell prompt may appear.

RAID Configuration

Important: This procedure only needs to be performed once — when you initially install the UCS C220 server.

Go to the appropriate section to configure RAID on your UCS hardware.

- *Configuring RAID for UCS C220 M3 Servers* (on page 42)
- *Configuring RAID for UCS C220 M4 Servers* (on page 44)

Configuring RAID for UCS C220 M3 Servers

The UCS hardware RAID configuration for this system release consists of a RAID 1 for the OS disk and one global hot spare (3x300GB).

Complete the following steps to create these volumes and hot spares.

1. Press **Ctrl-Alt-Del** to reboot the server.
2. Monitor the reboot process closely. After the disks are displayed, observe the boot messages and **press Ctrl-H** when prompted to access the WebBIOS (RAID Configuration Utility). After a few minutes, a **Start** button appears.
3. Click **Start** to configure RAID. The MegaRAID BIOS Config Utility main menu appears.
4. Click the **Configuration Wizard** link in the left area of the utility menu.
5. Click **New Configuration** and then click **Next**. The utility prompts you to clear the existing configuration.
6. Click **Yes**.
7. Click **Manual Configuration** and then click **Next**. The Drive Group Definition screen appears.

   Note: In the drives panel, there is a list of all three hard drives. Create two drive groups, the first consisting of two disks (1 and 2) and the second consisting of one global hot spare drive.
8. Select the **Slot 0** disk and while pressing the **Ctrl** key, click the **Slot 1** disk to highlight both disks.
9. Click **Add to Array** to form Drive Group (0).
10. Click **Accept DG**.
11. Click **Next** and select **Drive Group 0**.
12. Click **Add to SPAN to Drive Group 0** to the span list.
13. Click **Next**. The Virtual Drive Definition window appears.
14. Select **RAID 1** from the **RAID Level** dropdown menu.

15 Click **Update Size**. The maximum allowed size for the selected RAID level populates the Select Size field and records the size.

16 Click **Accept**. The **Write Policy** window appears.

17 Click **Yes** to confirm the default write policy.

18 Click **Back** and then select **Drive Group 0**.

19 Click **Add to SPAN to Drive Group 1** to the span list.

20 Click **Next**. The Virtual Drive Definition window appears.

21 Select **RAID 1** from the RAID Level drop-down menu.

22 Click **Update Size**. The maximum allowed size for the selected RAID level populates the Select Size field and records the size.

23 Click **Accept**. The Write Policy window appears.

24 Click **Yes** to confirm the default write policy. The total list of Vdisks created from Drive Groups 0 to 1 appears.

25 Click **Next**.

26 Examine the configuration preview to verify that the virtual drives match the previous list and select **Accept**. The system prompts to confirm that you want to save the configuration.

27 Click **Yes**. A warning message appears and indicates that you may lose data.

Note: If you cancel the previous screen, you will be prompted to initialize the new virtual drives.

28 Click **Yes** to initialize. The Virtual Drive VD0 is displayed.

29 Click **Home**. The Raid Configuration utility main menu appears.

30 Click the **Physical View** from the left pane if it is not currently displayed.

31 Click **Back** and then repeat Steps 21 through 22 for the drive in Slot 16.

32 Click **Home** and select the **Physical View** (if it is not displayed by default).

33 From the Main Menu, click **Exit** to exit the RAID Configuration Utility.

34 Click **Yes** to confirm that you want to exit the utility.

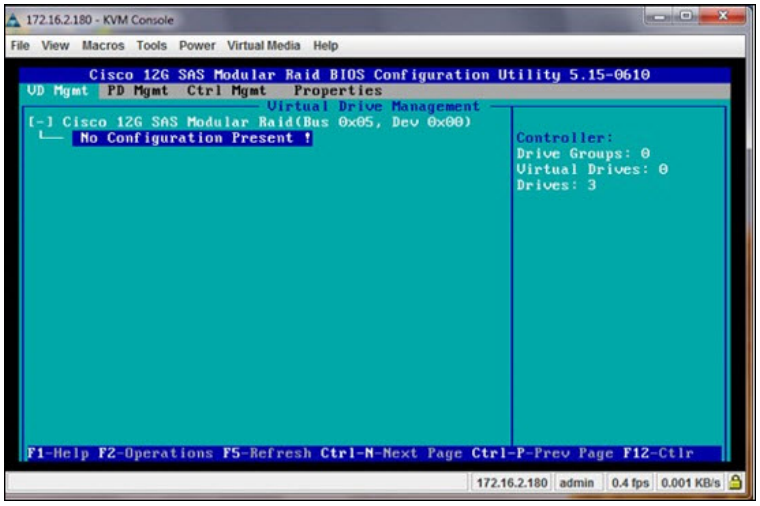
Configuring RAID for UCS C220 M4 Servers

Complete the following steps to configure RAID for a C220 M4 UCS server.

1 Power on the Cisco UCS C220 M4 server.

Note: If the server is already powered on, reboot the server.

2 On boot up, press **CTRL+R** to enter the Cisco 12G SAS Modular Raid Controller BIOS Configuration Utility.



3 Press **CTRL+N** and then click the **PD Mgmt** tab.

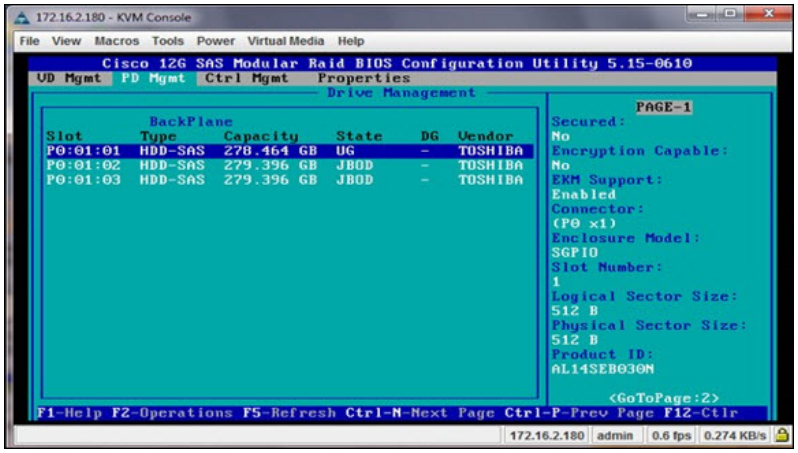
4 Use the **UP** or **DOWN** arrow keys to move between the disks.

5 Complete the following steps to change the disks from Just a Bunch Of Disks (JBOD) to **Unconfigured Good (UG)**.

a Select the first disk and press **F2**.

b Select **Make unconfigured good**.

c When prompted to confirm the change, click **Yes** and press **Enter**. The state of the drive will change from JBOD to UG.



d Repeat Steps 4a through 4c for remaining drives.

6 Go back to the **VD Mgmt** tab and press **CTRL+P**.

7 Select **No Configuration Present** and press **Enter**.

8 Configure the following:

a From the RAID Level area, select **RAID-1**.

b From the Secure VD area, select **No**.

c From PD per Span area, enter **2**.

d From the Drives area, use the UP or DOWN arrow to highlight the appropriate drive and press **Enter**. An **X** displays next to the drive to indicate that it is selected.

e Repeat Step 8d to select the next drive that will make up this drive pair.

9 Go to the **Advanced** option and highlight the **Initialize** option.

10 Press **Enter**. An **X** is inserted next to Initialize to indicate that it is selected.

11 Click **Ok**.

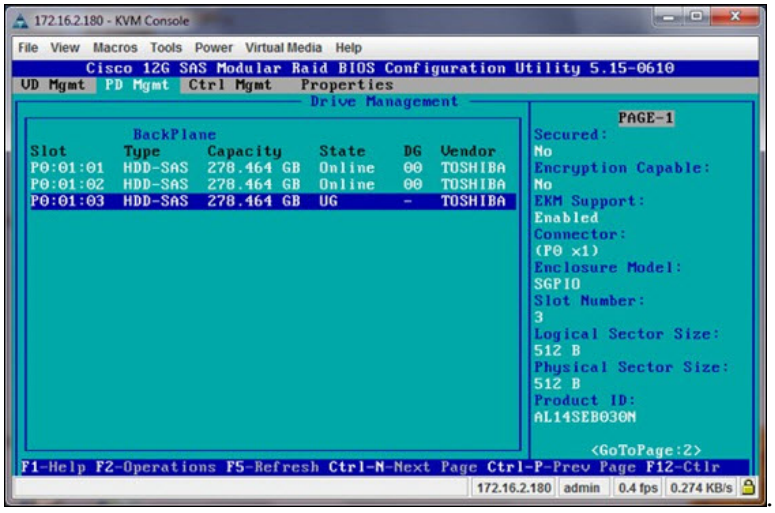
12 Click **Ok** to close the Advanced option window. The Configuration window is displayed.

13 Click **Ok** and system will now initialize the RAID-1 array. Wait for the initialization to complete.

14 Click **Ok** after the Confirmation window indicates that the initialization is complete.

15 Click **CTRL+N** to return to the **PD Mgmt** window.

16 From the PD Mgmt window, use the **UP** or **DOWN** arrows to highlight the **UG drive**.



17 Press **F2** and then select **Make Global HS**.

Note: The state of the drive changes from **UG** to **Hotspare**.

18 Press **ESC** and click **Ok** to exit the utility.

19 Click the **Macros** tab and select **Static Macros > CTRL+ALT+DEL** to reboot the server.

Note: The server must be rebooted for the changes to go into effect.

B

Deploy the PCG Virtual Machine from an ESXi Client

This appendix describes how to deploy the PCG virtual machine using an ESXi client.

In This Appendix

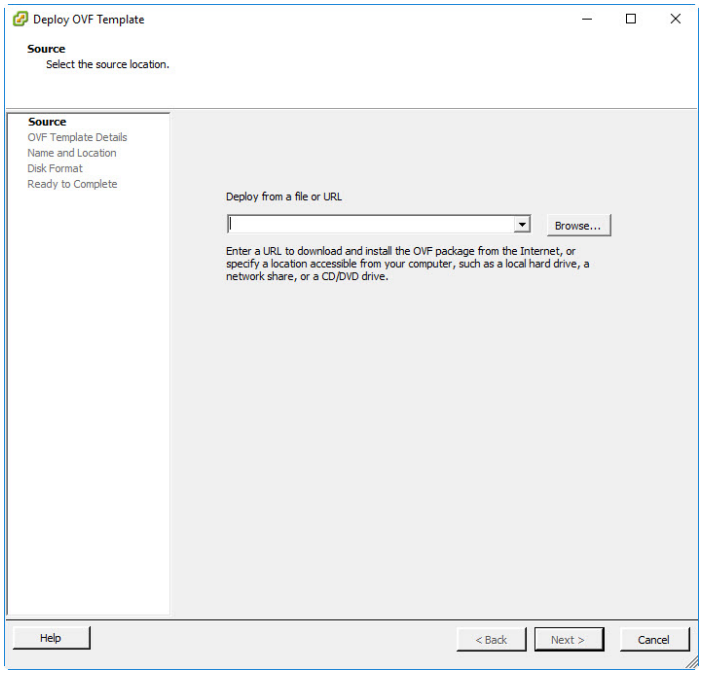
- Deploying a PCG Virtual Machine from an ESXi Client..... 48
- Mounting an ISO from an ESXi Client..... 50

Deploying a PCG Virtual Machine from an ESXi Client

Complete the following steps to deploy the PCG VM from an ESXi client.

1 Log on to the ESXi client.

2 From the File menu, select **Deploy OVF Template**. The Source window displays.



3 Click **Browse** and navigate to the directory where the PCG platform OVA (i.e. PCG-4.0.3-2.ova) resides.

4 Select the OVA and click **Open**. The absolute path to the OVA is added to the text box in the Source Window.

5 Click **Next**. The OVF Template Details window displays.

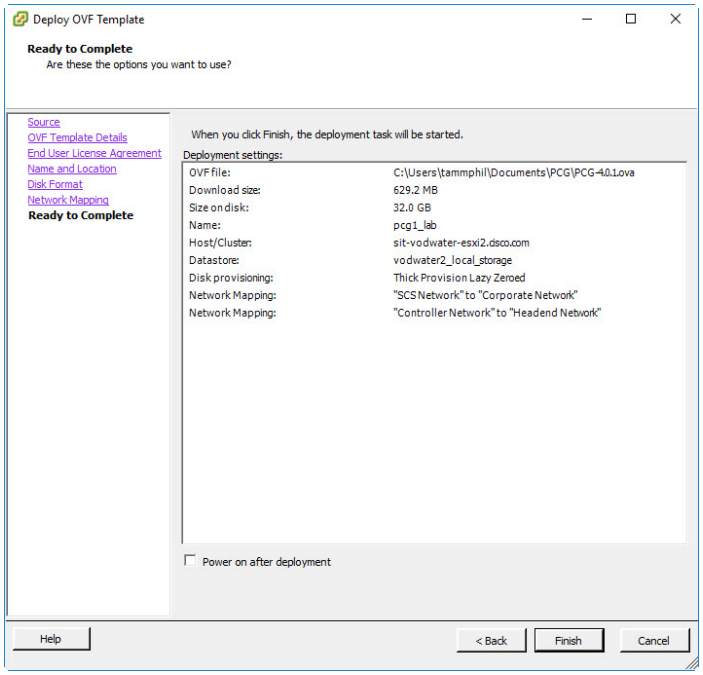
6 Review the details and click **Next**. The End User License Agreement displays.

7 Review the license agreement and click **Accept**. Then click **Next**. The Name and Location window display.

8 In the **Name** text box, enter a name to describe the PCG server. Then click **Next**. The Disk Format window displays.

9 Click the **Thick Provision Lazy Zeroed** radio button and then click **Next**. The Network Mapping window displays.

10 Select the appropriate **Destination Network** for each Source Network. Then click **Next**. The Ready to Complete window displays.



11 Review the configuration and then click **Finish**. A Deploying window appears and remains open until the new virtual machine is deployed.

12 When the VM completes, select it from the vSphere Client window.

13 Right-click the VM and select **Edit Settings**. The Edit Settings window displays.

14 Click **Hard disk 2** and in the **Disk Provisioning** area, change the Provisioned Size to **32** GB

15 Click **OK**. The VM is reconfigured.

16 Return to ***Power On and Login to the New PCG Virtual Machine*** (on page 15).

Mounting an ISO from an ESXi Client

Complete the following steps to mount the SAIpcg ISO using an ESXi client.

1 Login to vSphere client using ESXi host IP address where the PCG VM resides.

2 Select and right-click the PCG VM and then select **Edit Settings**.

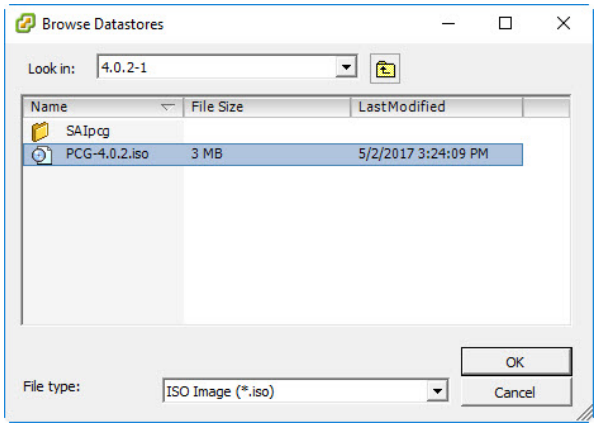
3 Click **CD/DVD drive 1**. Configuration options for the CD/DVD drive display in the right area of the window.

4 From the **Device Status** area, click the **Connected** check box.

5 From the **Device Type** section, click the Datastore ISO File radio button.

6 Click **Browse**. The Browse Datastores window opens.

7 Navigate to the location of the SAIpcg ISO.



8 Select the ISO file and click **OK**. The path to the ISO is shown in the Datastore ISO File text box.

9 Click **OK**.

10 Monitor the **Recent Tasks** area to verify that the task completed successfully.

11 From the EC/DTACS terminal window, type `df -k` to verify that the ISO successfully mounted.

Note: If the ISO did not mount, type `svcs volfs restart` and repeat Step 10.

12 Return to Step 11 of ***Upgrading the PCG Package from an EC 7.x or DTACS 4.1 Server*** (on page 58).

C

Backup and Restore Keyfiles

Due to the possibility of a catastrophic event (i.e. hardware failure), it is important to create backups of the keyfiles on your PCG server. This will enable you to restore them in the event they are lost, damaged or inaccessible.

This chapter provides the procedures to backup and restore keyfiles. It is recommended that you back up and restore the following files:

- /opt/pcg/mon_app/mon.cfg
- /etc/snmp/snmpd.conf

In This Appendix

- Backing Up Keyfiles 52
- Restoring Keyfiles to a Recovered System 53

Backing Up Keyfiles

Complete the following steps to backup the keyfiles.

1. From the EC/DTACS terminal window. SSH into the PCG server as **admin** user.
2. As **root** user, enter the following command to change to the **/opt** directory.

   ```
   [root@pcg1_lab ~]# cd /opt
   ```

3. Enter the following command to create a **pcgbkup-[PCG_IP]** directory.

   Command Syntax:

   ```
   mkdir /pcgbkup-[PCG_IP]
   ```

   Example:

   ```
   [root@pcg1_lab opt]# mkdir /pcgbkup-204.1.61.113
   ```

4. Copy the recommended key files to the **pcgbkup-[PCG_IP]** directory.
5. Execute the following command to create a tar ball.

   Command Syntax:

   ```
   tar cvf pcgbkup-[PCG_IP].tar pcgbkup-[PCG_IP]
   ```

   Example:

   ```
   [root@pcg1_lab opt]# tar cvf pcgbkup-204.1.61.113.tar
   pcgbkup-204.1.61.113
   ```

6. Using scp, copy the tar file to a different server or NAS device.

   Command Syntax:

   ```
   scp pcgbkup-[PCG_IP].tar
   admin:[NAS_IP]:[directory_on_EC/DTACS]
   ```

   Example:

   ```
   [root@pcg1_lab opt]# scp pcgbkup-140.1.61.21.tar
   admin:10.90.46.181:/var/tmp
   ```

Restoring Keyfiles to a Recovered System

Complete the following steps to restore the keyfiles to a recovered PCG system.

1 Refer to the ***Deploy the PCG Virtual Machine*** (on page 11) to deploy a new PCG server.

2 Complete the following steps to restore the keyfiles from the server where you backed the files up to the PCG server.

a From the EC/DTACS terminal window, SSH into the newly installed PCG server as **admin** user.

b As **root** user, copy the **pcgbkup-[PCG_IP].tar** file from the backup server to the PCG server.

Command Syntax:

```
scp admin:[NAS_IP]:[directory_on_NAS]/pcgbkup-[PCG_IP].tar
[directory_on_PCG]
```

Example:

```
[root@pcg1_lab1 opt]# scp
admin:10.90.46.181:/var/tmp/pcgbkup-140.1.61.21.tar
/var/tmp
```

c Enter the following command to untar the **/opt/pcgbkup-[PCG_IP].tar** file.

Command Syntax:

```
tar -xvf /var/tmp/pcgbkup-[PCG_IP].tar
```

Example:

```
[root@pcg1_lab1 ~]# tar -xvf
/var/tmp/pcgbkup-204.1.61.113.tar
```

d Type `ls -ltr /var/tmp` to view the list of keyfiles.

e Copy the keyfiles to the appropriate locations.

Command Syntax:

```
cp [directory_location]/mon.cfg /opt/pcg/mon_app
cp [directory_location]/snmpd.conf /etc/snmp
```

Example:

```
[root@pcg1_lab1 ~]# cp /var/tmp/mon.cfg /opt/pcg/mon_app
[root@pcg1_lab1 ~]# cp /var/tmp/snmpd.conf /etc/snmp
```

3 Login to the EC/DTACS Web UI and access the PCG Web UI by selecting the appropriate option. The PCG List window displays.

- **EC**: Network Element Provisioning > PCG
- **DTACS**: Network Elements > PCG

4 From the PCG List Web UI, select the **PCG** and click **Edit**.

5 Update the **Control MAC Address** and then click **Save**.

6 Return to the PCG List window and select the **PCG** again; then click **Reset**.

7 Verify the PCG version on the EC/DTACS server, as well as on the PCG server. Refer to ***Verifying PCG Package Versions on the EC/DTACS*** (on page 30) for details.

D

Upgrade the PCG Server

This appendix describes the procedures to upgrade the PCG application. The PCG package *is only* upgraded on the EC/DTACS server by updating the CSCOec-pcg rpm.

Important: The PCG application ***cannot*** be upgraded from the PCG server. You must upgrade the EC/DTACS server and then reboot the PCG to obtain the current PCG code.

In This Appendix

- Upgrading the PCG Package on an EC 8.0 or DTACS 5.0 Server 56
- Upgrading the PCG Package from an EC 7.x or DTACS 4.1 Server 58
- Upgrading the PCG Package on the PCG Server 61

Upgrading the PCG Package on an EC 8.0 or DTACS 5.0 Server

Complete the following steps to upgrade the PCG package (e.g. CSCOec-pcg) on an EC 8.0 or DTACS 5.0 system.

1 Refer to **Appendix C** in the ***Admin Node User's Guide*** for procedures to upgrade the software repo with the PCG application.

Important: The software repo must be updated before continuing with the next step.

2 Login to the EC/DTACS server as **admin** user.

3 Enter the following command to upgrade the PCG application.

```
[admin@EC/DTACS ~]$ sudo yum update CSCOec-pcg
```

Result: The upgrade process starts and after running various checks, displays a "Transaction Summary".

```
Loaded plugins: security
Setting up Update Process
base                                                     | 3.7 kB     00:00
epel                                                     | 4.3 kB     00:00
updates                                                  | 3.4 kB     00:00
vcs-releases                                             | 1.5 kB     00:00
vcs-releases/primary                                     | 424 kB     00:00
vcs-releases                                                        1985/1985
vcs-snapshots                                            | 1.5 kB     00:00
vcs-snapshots/primary                                    | 129 kB     00:00
vcs-snapshots                                                         710/710
Resolving Dependencies
--> Running transaction check
---> Package CSCOec-pcg.x86_64 0:4.0.0-2 will be updated
---> Package CSCOec-pcg.x86_64 0:4.0.2-1 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package            Arch           Version           Repository            Size
================================================================================
Updating:
 CSCOec-pcg         x86_64         4.0.2-1           vcs-releases         418 k

Transaction Summary
================================================================================
Upgrade       1 Package(s)

Total download size: 418 k
Is this ok [y/N]: y
```

4 When prompted to confirm the upgrade, type **y** and press **Enter**. The PCG package is upgraded and a **Complete!** message displays.

```
Downloading Packages:
CSCOec-pcg-4.0.2-1.rpm                                   | 418 kB     00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
Warning: RPMDB altered outside of yum.
  Updating   : CSCOec-pcg-4.0.2-1.x86_64                                  1/2
Modifying pcg.cfg....
  Cleanup    : CSCOec-pcg-4.0.0-2.x86_64                                  2/2
  Verifying  : CSCOec-pcg-4.0.2-1.x86_64                                  1/2
  Verifying  : CSCOec-pcg-4.0.0-2.x86_64                                  2/2

Updated:
  CSCOec-pcg.x86_64 0:4.0.2-1

Complete!
```

5 Enter the following command to verify that the installed PCG package is the upgraded version.

```
[admin@EC/DTACS ~]$ rpm -qa CSCOec-pcg
```

Upgrading the PCG Package from an EC 7.x or DTACS 4.1 Server

Complete the following steps to upgrade the PCG package on an EC 7.x or a DTACS 4.1 server.

Note: This procedure assumes an upgrade from PCG-4.0.3-1 or earlier.

1. Copy the **PCG-[VERSION].iso** (i.e. PCG-4.0.3-2.iso) to the **/var/tmp/** directory on your EC or DTACS controller.
2. Log into the EC or DTACS server as an Administrative user and then change to **root** user.
3. Enter the following command to change to the **/var/tmp** directory.

   ```
   # cd /var/tmp
   ```
4. Enter the following commands to prepare the ISO to be mounted as a loopback device.

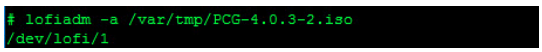
   Note: Document the device name that is created as you will need it later in this procedure.

   Command Syntax:

   ```
   lofiadm -a /var/tmp/PCG-[VERSION].iso
   ```

   Example:

   ```
   # lofiadm -a /var/tmp/PCG-4.0.3-2.iso
   ```

   Result: The device name is /dev/lofi/1.
5. Enter the following command to create a temporary directory in **/var/tmp**.

   Command Syntax:

   ```
   mkdir /var/tmp/[directory_name]
   ```

   Example:

   ```
   # mkdir -p /var/tmp/pcg-mnt
   ```
6. Using the device name from the output of Step 4, enter the following command to mount the lofi device on the temporary directory.

   Command Syntax:

   ```
   mount -o ro -F hsfs [device_name] /var/tmp/[directory_name]
   ```

   Example:

   ```
   # mount -o ro -F hsfs /dev/lofi/1 /var/tmp/pcg-mnt
   ```

7 Enter the following command to verify the mount point.

```
# df -k | tail
```

```
# df -h | tail
rpool/disk1            125G   2.9G    93G     4%    /disk1
dpool/backups          125G    27M   123G     1%    /disk1/dvs/backups
dpool/corefiles        125G    31K   123G     1%    /disk1/dvs/corefiles
dpool/tmp              125G   1.9G   123G     2%    /disk1/dvs/dncs/tmp
dpool/disk2            125G    25M   123G     1%    /disk2
dpool                  125G    36K   123G     1%    /dpool
rpool/export           125G    32K    93G     1%    /export
rpool/export/home      125G   822M    93G     1%    /export/home
rpool                  125G    45K    93G     1%    /rpool
/dev/lofi/1            2.6M   2.6M     0K   100%    /var/tmp/pcg-mnt
```

Mount point

8 Enter the following command to change to the temporary directory.

Command Syntax:

```
cd /var/tmp/[directory_name]
```

Example:

```
# cd /var/tmp/pcg-mnt
```

9 Enter the following command to convert the SAIpcg package to the standard package format. You are prompted to select the package you want to process.

Command Syntax:

```
pkgtrans SAIpcg-[VERSION].pkg /var/tmp
```

Example:

```
# pkgtrans SAIpcg-4.0.3-2.pkg /var/tmp
```

```
# pkgtrans SAIpcg-4.0.2.pkg /var/tmp

The following packages are available:
  1  SAIpcg     PowerKEY CAS Gateway
                (SunOS_all) 4.0.2

Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]:
```

10 Enter the value next to the SAIpcg package and press **Enter**. The package conversion completes.

Note: If the SAIpcg is the only package listed, you can simply press **Enter**.

```
Select package(s) you wish to process (or 'all' to process
all packages). (default: all) [?,??,q]: 1
Transferring <SAIpcg> package instance
```

11 Enter the following command to go back one directory level.

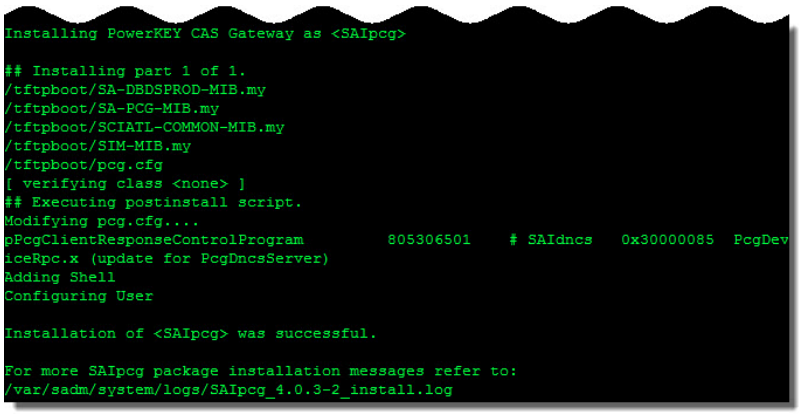
```
# cd ../
```

12 Enter the following command to upgrade the **SAIpcg** package. You are prompted to confirm the installation.

```
# install_pkg
```

```
# install_pkg

Checking the system, please wait...

*******************************************************************************

This script will install the following packages on "vodwater":

SAIpcg          PowerKEY CAS Gateway
                4.0.3-2

*******************************************************************************

Are you SURE you want to continue?  [y,n,?,q] y
```

13 Enter **y** and press **Enter**. The SAIpcg package is installed.



14 Enter the following commands to clean up the temporary files and unmount the temporary directory.

Command Syntax:

```
umount /var/tmp/[temporary_directory]
lofiadm -d [device_name]
rm -rf /var/tmp/SAIpcg /var/tmp/SAIpcg-[VERSION]
/var/tmp/[temporary_directory]
```

Example:

```
# umount /var/tmp/pcg-mnt
# lofiadm -d /dev/lofi/1
# rm -rf /var/tmp/SAIpcg /var/tmp/SAIpcg-4.0.3-2
/var/tmp/pcg-mnt
```

15 Enter the following command to SSH into the PCG server as **admin** user and then access the PCG console application. The PCG prompt displays.

Command Syntax:

```
ssh admin@[Control IP Address]
```

Example:

```
[admin@vodwater ~]$ ssh admin@204.1.61.113
[admin@pcg1_lab ~]$ sudo /opt/pcg/console_app/cons
```

16 At the PCG> prompt, enter the following command to verify the version of the PCG package currently installed.

```
PCG> vers
```

17 Does the PCG package version match the PCG package version you upgraded to the EC/DTACS?

- If **yes**, you have completed the upgrade.
- If **no**, and the version of the PCG application on the EC/DTACS is newer than the version on the PCG, go to ***Upgrading the PCG Package on the PCG Server*** (on page 61).

Upgrading the PCG Package on the PCG Server

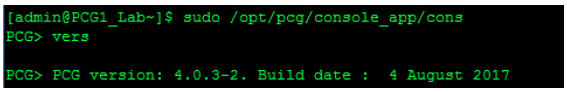
Important: Once the PCG server is initially installed, you can not upgrade the PCG application directly from the PCG. You must upgrade the PCG package on the EC/DTACS and then reboot the PCG server to pull the new code.

Complete the following steps to upgrade the PCG package on the PCG 4.0 server.

1. If you have not yet upgraded the PCG package on the EC/DTACS, go to one of the following sections to do so now.
   - ***Upgrading the PCG Package on an EC 8.0 or DTACS 5.0 Server*** (on page 56)
   - ***Upgrading the PCG Package from an EC 7.x or DTACS 4.1 Server*** (on page 58)
2. After upgrading the EC/DTACS server, SSH into the PCG server as **admin** user.
3. Enter the following command to reboot the PCG server. The PCG SSH session closes and you are returned to the EC/DTACS session.

   ```
   [admin@pcg1_lab ~]$ reboot
   ```
4. After a few minutes, SSH back into the PCG server as **admin** user from the EC/DTACS.
5. Enter the following command to verify that the new version of PCG is now running on the PCG server.

   ```
   [admin@pcg1_lab ~]$ sudo /opt/pcg/console_app/cons
   PCG> vers
   ```



E

Manually Configure the PCG Network

This appendix explains how to manually configure the PCG network.

In This Appendix

- Manually Configuring the PCG Network..... 64

Manually Configuring the PCG Network

Complete the following steps to manually configure the PCG network.

1 From a terminal window on the EC or DTACS server, type the following two commands.

```
[admin@EC/DTACS ~]$ ping -a dncsatm
[admin@EC/DTACS ~]$ ping -a dtacsatm
```

2 Record the IP addresses from Step 1 below:

dncsatm: _____

dtacsatm: _____

3 Enter the following command on the EC/DTACS to change to the **tftpboot** directory.

EC 8.0/DTACS 5.0:

```
[admin@EC/DTACS ~]$ cd /var/lib/tftpboot
```

EC 7.x/DTACS 4.1:

```
# cd /tftpboot
```

4 Enter the following command to secure copy the **pcg** file to the PCG server.

Command Syntax:

```
scp pcg admin@[PCG_IP]:/opt/pcg/pcg_app/app
```

Example:

```
[admin@EC/DTACS ~]$ scp pcg
admin@204.3.1.33:/opt/pcg/pcg_app/app
```

5 Enter the following command to secure copy the **pcg.cfg** file to the PCG server.

Command Syntax:

```
scp pcg.cfg admin@[PCG_IP]:/opt/pcg/pcg_app/app
```

Example:

```
[admin@EC/DTACS ~]# scp pcg.cfg
admin@204.3.1.33:/opt/pcg/pcg_app/app
```

6 From the EC/DTACS terminal window, SSH to the PCG server as **admin** user.

7 Enter the following command to change the access rights of the **pcg** and the **pcg.cfg** files to **755**.

```
[admin@pcg1_lab ~]$ sudo chmod 755 /opt/pcg/pcg_app/app/pcg
/opt/pcg/pcg_app/app/pcg.cfg
```

8 Enter the following command to change the ownership of the **pcg** and the **pcg.cfg** files to **root:root**.

```
[admin@pcg1_lab ~]$ sudo chown root:root
/opt/pcg/pcg_app/app/pcg /opt/pcg/pcg_app/app/pcg.cfg
```

9 Open the **mon.cfg** file in a text editor.

```
[admin@pcg1_lab ~]$ sudo vi /opt/pcg/mon_app/mon.cfg
```

10 Go to the **skip-bootp** line and change the value from no to **yes**.

11 Save and close the **mon.cfg** file.

12 Open the **pcg.cfg** file in a text editor.

```
[admin@pcg1_lab ~]$ sudo vi /opt/pcg/pcg_app/app/pcg.cfg
```

13 Make the following changes in the pcg.cfg file.

- **RpcServerIPAddr**: enter the appropriate IP address recorded in Step 2
- **AlarmServerIPAddr**: enter the appropriate IP address recorded in Step 2
- **ForceDownload**: change the value to **no**
- Add the following lines to the end of the file:
  - **PcgScsInterface = eth1**
  - **PcgtoDncsIfIPAddr**: append the IP address for the PCG interface that communicates to the EC or DTACS

14 Save and close the **pcg.cfg** file.

15 Open the **ifcfg-eth0** file in a text editor and edit the following fields.

```
[admin@pcg1_lab ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- **BOOTPROTO**: set to **Static**
- **IPADDR**: append the IP address of the PCG interface that communicates with the EC or DTACS
- **NETMASK**: append the subnet mask of the PCG interface that communicates with the EC or DTACS
- **ONBOOT**: set to **yes**

16 Save and close the **ifcfg-eth0** file.

17 Open the **ifcfg-eth1** file in a text editor and edit the following fields.

```
[admin@pcg1_lab ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-eth1
```

- **BOOTPROTO**: set to **Static**
- **IPADDR**: append the IP address of the PCG interface that communicates with the SCS on private network
- **NETMASK**: append the subnet mask of the PCG interface that communicates with the SCS on private network
- **ONBOOT**: set to **yes**

18 Save and close the **ifcfg-eth1** file.

19 Enter the following command to edit the **/etc/sysconfig/network-scripts/route-eth0** file.

Note: Substitute the IP address of the gateway that the PCG uses to communicate with the EC or DTACS for [PCG_IP_gw].

Command Syntax:

```
sudo default via [PCG_IP_gw] dev eth0
```

Example:

```
[admin@pcg1_lab ~]$ sudo default via 204.1.61.0 dev eth0
```

20 Enter the following command to edit the **/etc/sysconfig/network-scripts/route-eth1** file.

Note: Substitute the gateway that the PCG uses to communicate with the SCS on a private network.

Command Syntax:

```
sudo [network/subnet_mask] via [PCG_IP_gw] dev eth1
```

Example:

```
[admin@pcg1_lab ~]$ sudo 204.1.61.0/24 via 172.10.3.206 dev
eth0
```

21 Enter the following command to restart the network.

```
[admin@pcg1_lab ~]$ sudo service network restart
```

F

Deliver ECMs to DHCTs

This appendix describes how the PowerKEY ECMs are delivered to the DHCTs. The process begins with system initialization and proceeds to the EC or DTACS server. The SCS or scrambler interactions are outlined below.

- The PCG is fully configured and provisioned
- The EC or DTACS server creates sessions on the PCG
- The SCS establishes a TCP connection, channel and valid streams on the PCG
- The PCG responds with ECM streams for existing sessions/services setup by the EC or DTACS server on the PCG

In This Appendix

- Delivering ECMs 68

Delivering ECMs

Complete the following steps to deliver ECMs to DHCTs.

1 When the PCG powers up, configure it manually or using BOOTP. The SCS-facing port receives its network address and the PCG application is launched.

Result: The PCG sends a provision request to the EC or DTACS server. When the EC or DTACS server receives the request, it sends the PCG a provision response. The response contains data that sets the EC-facing network address for communication with the scrambler device(s).

Optional: The response may inform the PCG about how many devices can communicate with the PCG, provide their IP addresses, and indicate how many programs can be serviced on each device.

Note: The PCG can support a maximum of 3000 sessions.

2 Create a session from the EC or DTACS Web UI. This provides the access criteria for the PCG service.

Note: If you are using ROSA for access criteria management, then configure the EIS or Access Criteria Manager Component (ACMC) through the ROSA element manager. Ensure the access criteria specified here match the access criteria explicitly administered on the EC or DTACS source definition Web UI for the associated service or program. Access criteria can be configured through the ACMC.

- A single channel over a TCP connection serves multiple programs. When a program is scheduled for scrambling, the SCS sets up a stream for the program. The scrambler issues access criteria and control words to the PCG for the session, and the PCG responds with the ECMs.
- The SCS then sends the ECMs and the scrambled program (with the corresponding control word) to the built-in modulator. From there it goes to the RF and then to the set-top.

Note: If the PCG communicates with an SCS device that does not have a built-in modulator, then a separate modulator is needed to provide RF.

Notes:

- PCG scrambling modes are changed in the EC and DTACS to support the new modes added for AES-128 scrambling.
- EC and DTACS support configuring PCG scramble mode for the following AES modes:
  - AES-ECB-CTS
  - ATIS-IIF-DSA
  - AES-NSA (or AES-DVB-LSA-CBC-MDI)

G

Troubleshoot the pcgmon Process

This appendix describes a common issue that can occur when the PCG server is rebooted without properly shutting down the PCG processes. The issue is that a pcgmon lock file is created and prevents the pcgmon process from starting.

In This Appendix

- Removing the pcgmon Lock File 72

Removing the pcgmon Lock File

Complete the following steps to remove the PCG application lock file from the PCG.

1. Enter the following command in a PCG terminal window to manually start the pcgmon service.

   ```
   [admin@pcg1_lab ~]$ sudo service pcgmon start
   ```

   ```
   PCG monitor appears to be running.  Not starting.
   Remove /var/lock/subsys/pcgmon if this is in error.
   ```

2. Enter the following command to remove the **/var/lock/subsys/pcgmon** file.

   ```
   [admin@pcg1_lab ~]$ sudo rm /var/lock/subsys/pcgmon
   ```

3. When prompted to remove the file, enter **y**.
4. Repeat Step 1 to start the pcgmon service.
5. Enter the following command to verify that the pcgmon service is now running.

   ```
   [admin@pcg1_lab ~]$ sudo service pcgmon status
   ```

Index

A

Abbreviated Procedure • 17

B

Backing Up Keyfiles • 52

C

Changing the SNMPv3 User Options • 35
Chassis Front View • 38
Chassis Rear View • 39
Cisco UCS C220 Server CIMC Configuration • 40
Cisco UCS C220 Server Diagram • 38
Configure SNMPv2 • 33
Configuring RAID for UCS C220 M3 Servers • 42
Configuring RAID for UCS C220 M4 Servers • 44
Configuring SNMPv2 • 34
Configuring SNMPv3 • 35
Configuring the PCG Network • 16
Creating the SNMPv3 User • 35

D

Defining the SNMPv3 Trap Destination • 36
Delivering ECMs • 68
Deploy the PCG Virtual Machine • 11
Deploying a PCG Virtual Machine from an ESXi Client • 48
Deploying the PCG Virtual Machine from the vSphere Web UI • 12
Detailed View of PCI Ports • 39

H

Hardware Requirements • 2

I

Install the Software on the EC/DTACS Server • 5
Installing the PCG Package on an EC 7.x or DTACS 4.1 Server • 8
Installing the PCG Package on the EC 8.0 or DTACS 5.0 Server • 6
Installing VMware Tools (Optional) • 17

M

Manually Configuring the PCG Network • 64
Mounting an ISO from an ESXi Client • 50

P

Power On and Login to the New PCG Virtual Machine • 15
Provision the PCG on the EC/DTACS Web UI • 19
Provisioning the PCG on the DTACS Web UI • 24
Provisioning the PCG on the EC Web UI • 20

R

RAID Configuration • 42
Reconfiguring the PCG Virtual Hardware • 14
Removing the pcgmon Lock File • 72
Restart the SNMP Service • 36
Restoring Keyfiles to a Recovered System • 53

S

Software Requirements • 3
System Requirements • 1

U

Upgrading the PCG Package from an EC 7.x or DTACS 4.1 Server • 58
Upgrading the PCG Package on an EC 8.0 or DTACS 5.0 Server • 56
Upgrading the PCG Package on the PCG Server • 61

V

Verify PCG Versions • 29
Verifying PCG Package Versions on the EC/DTACS • 30
Verifying the PCG Version on the PCG Server • 31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883

August 2017

Part Number TP-00109