

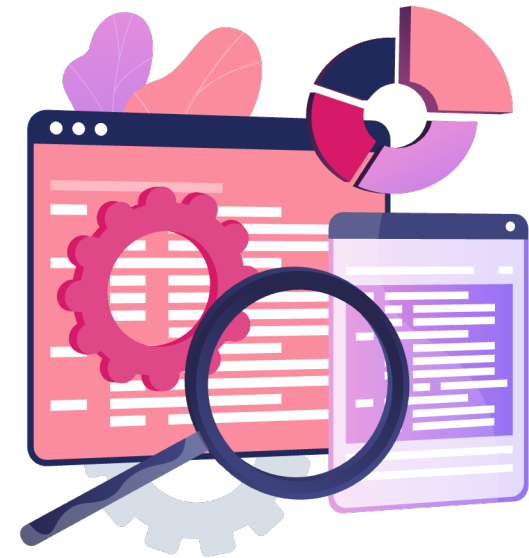
CHAPTER 11

SECURITY MAINTENANCE

YOU DESERVE THE BEST SECURITY

Learning Objectives

- Describe the different methods for backing up Check Point system information and discuss best practices and recommendations for each method.
- Identify how to monitor the health of supported Check Point hardware using the Gaia Portal and the command line.
- Identify ways to update Check Point solution software.
- Define and distinguish between different Check Point software release types.



Snapshot Overview

- Creates a binary image of the entire root (lv_current) disk partition.
- Includes:
 - File system, with customized files
 - System configuration (interfaces, routing, hostname, and similar)
 - Software Blades configuration
 - Management database



- Gaia Snapshots are like ISO images. They are stored on the system in Logical Volume Manager (LVM) volumes.
- With R77.30 and higher, volumes are managed using the Check Point LVM Manager, a command line tool included with Gaia. For example, if there is not enough available disk space, you can increase the size of the log partition.
- For additional information about Snapshots, refer to the *Gaia Administration Guide*. In addition, see sk95566 - Managing partition sizes via LVM manager on Gaia OS.

Best Practices

- Create a snapshot:
 - After a fresh (new) installation of Gaia.
 - Before making a major configuration.
 - Before an upgrade or hotfix installation.



Snapshot Management

- Snapshots are managed using the Gaia Portal on the Management Server and the command line (Gaia Clish and Export mode).
- Snapshot management activities include:
 - Creating a snapshot.
 - Exporting a snapshot.
 - Importing a snapshot.
 - Deleting a snapshot.



- You can also schedule a snapshot; however, a snapshot is very large. For this reason, its scheduling procedure is different than the scheduling procedure for backups.
- For additional information about scheduling a snapshot, refer to the *Gaia Administration Guide*.

Creating a Snapshot Using the Gaia Portal

Gaia Portal on the Management Server → Maintenance → Snapshot Management

Open Server
A-SMS

Maintenance ▶ Snapshot Management

My snapshot

Name	Description	Created	Size	Version	State
A_SMS_17Feb2023	Snapshot of A-SMS collected on 17 Feb 2023	17-Feb-2023 08:24:32	13.43G	R81.20	✓

New Image

Create an image of the current running system. You can revert to this image at a later time.

Name:

Description:

OK Cancel

Scheduled Snapshot

Name:

Description:

Destination:

Recurrence:

Retention Policy:

Scheduled Snapshot Settings

This schedule is currently disabled. No snapshot will be created.

Statistics

Creation of an additional image will require 12.072G
Amount of space available for images is 44.97G

Free Used

Snapshot Management - Gaia Portal

From the Snapshot Management page:

1. Click **New**.
2. In the Name field, enter a name for the image.

Optional: In the Description field, enter a description for the image.

3. Click **OK**.



- Before creating a snapshot, make sure the appliance or storage destination has sufficient disk space.
- The required free disk space is the size of the system root partition multiplied by 1.15.

Export, Import, and Delete Snapshots

Open Server
A-SMS

Maintenance > Snapshot Management

View mode: Advanced

OSPF
Route Aggregation
Inbound Route Filters
Route Redistribution
Routing Options
Routing Event Trigger
Router Discovery
Policy Based Routing
NAT Pools
Routing Monitor
User Management
Change My Password
Users
Roles
Password Policy
Authentication Servers
System Groups
GUI Clients
High Availability
VRRP
Advanced VRRP
Maintenance
License Status
Snapshot Management
System Backup
Download SmartConsole
Shut Down
Upgrades (CPUSE)
Status and Actions
Software Updates Policy

My Snapshot

New Revert Delete Import Export

Name	Description	Created	Size	Version	State
A_SMS_17Feb2023	Snapshot of A-SMS collected on 17 Feb 2023	17-Feb-2023 08:24:32	13.43G	R81.20	✓

Scheduled Snapshot

Name:
Description:
Destination:
Recurrence:
Retention Policy:
Scheduled Snapshot Settings

This schedule is currently disabled. No snapshot will be created.

Statistics

Creation of an additional image will require 12.072G
Amount of space available for images is 44.97G

Free Used

Exporting a Snapshot Using the Gaia Portal

From the Snapshot Management page:

1. Select a snapshot.
2. Check the snapshot size.
3. Make sure there is enough free disk space in the /var/log/ partition. (See the Student Guide for details.)
4. Click **Export**.
5. Click **Start Export**.



- Do not rename the exported image.
- If you rename a snapshot image, it is not possible to revert to it.

Importing a Snapshot Using the Gaia Portal

From the Snapshot Management page:

1. Select a snapshot.

Pay close attention to the warnings about overwriting settings, the credentials, and the reboot and the image details.

2. Click **OK**.
3. If you reverted a snapshot on a Security Gateway, install the Security Policy.

Deleting a Snapshot Using the Gaia Portal

From the Snapshot Management page:

1. Select a snapshot.
2. Click **Delete**.
3. Click **OK**.

Snapshot Management - Gaia Clish

You can use the Gaia Clish for most snapshot management tasks.

- Creating a snapshot.
- Exporting a snapshot.
- Importing a snapshot.
- Reverting a snapshot.
- Deleting a snapshot.

Creating a Snapshot Using Gaia Clish

- Create a snapshot as a local LVM volume:

```
add snapshot-onetime name <Name of Snapshot> [description  
"<Description of Snapshot>"]
```

- Create a snapshot and export it to a local file:

```
add snapshot-onetime name <Name of Snapshot> [description  
"<Description of Snapshot>"] target local path <Local  
Path>
```

Creating a Snapshot Using Gaia Clish (Continued)

- Create a snapshot and upload it to an FTP server.

```
add snapshot-onetime name <Name of Snapshot> [description  
"<Description of Snapshot>"] target ftp ip <IPv4 Address  
of FTP Server> path <Path on FTP Server> username <User  
Name on FTP Server> password <Password in Plain Text>
```

- Create a snapshot image and upload it to an SCP server.

```
add snapshot-onetime name <Name of Snapshot> [description  
"<Description of Snapshot>"] target scp ip <IPv4 Address  
of SCP Server> path <Path on SCP Server> username <User  
Name on SCP Server> password <Password in Plain Text>
```


Exporting a Snapshot Using Gaia Clish

- Export an existing snapshot and save it as a local file:

```
set snapshot-onetime export <Name of Exported Snapshot>  
target local path <Local Path>
```



These commands only export an existing snapshot image from a local LVM volume.

Exporting a Snapshot Using Gaia Clish (Continued)

- Export an existing snapshot and upload it to an FTP server:

```
set snapshot-onetime export <Name of Exported Snapshot>  
target ftp path <Path on FTP Server> ip <IPv4 Address of  
FTP Server> username <User Name on FTP Server> password  
<Password in Plain Text>
```

- Export an existing snapshot and upload it to an SCP server:

```
set snapshot-onetime export <Name of Exported Snapshot>  
target scp path <Path on SCP Server> ip <IPv4 Address of  
SCP Server> username <User Name on SCP Server> password  
<Password in Plain Text>
```

Importing a Snapshot Using Gaia Clish

- Import an existing snapshot from a local file:

```
set snapshot-onetime import <Name of Imported Snapshot>  
target local path <Local Path>
```



These commands only export an existing snapshot image from a local LVM volume.

Importing a Snapshot (Continued)

- Import an existing snapshot from an FTP server:

```
set snapshot-onetime import <Name of Imported Snapshot>  
target ftp ip <IPv4 Address of FTP Server> path <Path on  
FTP Server> username <User Name on FTP Server> password  
<Password in Plain Text>
```

- Import an existing snapshot from an SCP server:

```
set snapshot-onetime import <Name of Imported Snapshot>  
target scp ip <IPv4 Address of SCP Server> path <Path on  
SCP Server> username <User Name on SCP Server> password  
<Password in Plain Text>
```

Reverting a Snapshot Using Gaia Clish



- When Gaia reverts to a snapshot, it overwrites the existing running configuration and settings. Make sure you know credentials of the snapshot to which you revert.
- Before reverting to a snapshot on a new appliance or after resetting to factory defaults, run the Gaia First Time Configuration Wizard and configure the same settings used when you created the snapshot.
- If you revert a snapshot on a Security Gateway, install the Security Policy.

Reverting a Snapshot Using Gaia Clish (Continued)

- Import and revert an existing snapshot image from a local LVM volume:

```
set snapshot-onetime revert target lvm name <External Name of Snapshot>
```

- Importing and reverting an existing snapshot image from a local file:

```
set snapshot-onetime revert target local name <Imported Name of Snapshot> path <Local Path>
```

Reverting a Snapshot Using Gaia Clish (Continued)

- Import and revert an existing snapshot image from an FTP server:

```
set snapshot-onetime revert target ftp name <Imported Name  
of Snapshot> path <Path on FTP Server> ip <IPv4 Address of  
FTP Server> username <User Name on FTP Server> password  
<Password in Plain Text>
```

- Import and revert an existing snapshot image from an SCP server:

```
set snapshot-onetime revert target scp name <Imported Name  
of Snapshot> path <Path on SCP Server> ip <IPv4 Address of  
SCP Server> username <User Name on SCP Server> password  
<Password in Plain Text>
```

Deleting a Snapshot Using Gaia Clish

- Delete a local snapshot:

```
delete snapshot <Name of Snapshot>
```

```
lvs
```



The Gaia Clish does not support deletion of multiple snapshots at the same time.

Factory Default Images

- Factory default images on Check Point appliances are created automatically when you install or upgrade an appliance to another release.
- You can restore your Check Point appliance to the factory default image for a specified release.



This procedure overwrites all existing configuration settings.

Factory Default Images (Continued)



- Create a snapshot image before you restore a factory default image.
- Export all existing snapshots from the appliance before you restore a factory default image.

Factory Default Image Management

Restoring a Factory Default Image Using Gaia Portal

From the navigation tree:

1. Click **Maintenance** and then **Snapshot Management**.
2. Select the **Revert** option.
3. Follow the instructions on the screen.
4. In the navigation tree, click **Maintenance** and then **Shut Down**.
5. Click **Reboot**.

Restoring a Factory Default Image Using Gaia Clish

1. Connect to the command line on your appliance.
2. Log into the Gaia Clish.
3. Run the following commands:
`set fcd revert<SPACE><TAB>`
`set fcd revert <Name of Default Image>`
4. Follow the instructions on the screen.
5. Run the following command: `reboot`

System Backup Overview

Creates a compressed file that includes:

- ✓ Gaia operating system
- ✓ Security Management Server database

File location: **/var/log/CPbackup/backups/**

File type: ***tgz**

Backup and Restore



- Backup and Restore is the preferred method of recovery.
- Save your Gaia system configuration settings as a ready-to-run CLI shell script. This lets you quickly restore your system configuration after a system failure or migration.
- Schedule regular system backups to preserve the Gaia operating system configuration and Firewall database. The schedule (daily, weekly, monthly) depends how frequently you change your configuration and policies.

**PLEASE
NOTE...**

You can only migrate using the same Gaia version on the source and target computers.



- You can only do a migration using the same Gaia version on the source and target computers.



- To change the name of a backup file, you must use the command line (Expert mode). You cannot use the Gaia Portal. Do not use special characters.
- After you add, configure, or delete features, run the save config command to save the settings permanently.
- You can save your Gaia configuration settings as a ready-to-run CLI shell script. This lets you quickly restore your system configuration after a system failure or migration.

Excluding Files from a Backup

Background

- The Gaia operating system contains backup configuration files (schema files) that control which files to collect during the backup.
- Optionally, you can delete selected Software Blade or features from the backup; for example:
 - Data Loss Prevention
 - Gaia OS
 - Network Management
 - Firewall or Firewall logs
 - Mobile Access
 - QoS

Refer to the *Gaia Administration Guide* for a complete list.

Excluding Files from a Backup - Procedure

Connect to the command line on the Gaia Server:

1. Log into the Expert mode.
2. Back up the current configuration file:

```
cp -v /var/CPbackup/schemes/<Name-of-File>.cpbak{ ,_BKP}
```

3. Edit the current configuration file:

```
vi /var/CPbackup/schemes/<Name-of-File>.cpbak
```

Excluding Files from a Backup (Continued)

4. Make the required changes in the applicable section:

The section **<INCLUDE_FILES>** controls which files to include during the backup.

The section **<EXCLUDE_FILES>** controls which files not to include during the backup.

5. Save the changes in the file and exit the editor.

System Backup - Gaia Portal

- Backups are managed using the Gaia Portal and the command line (Gaia Clish and Expert Mode).
- Restore operations are performed from the Gaia Clish.

The screenshot shows the Gaia Portal interface for System Backup configuration. The left sidebar contains a navigation menu with 'System Backup' highlighted. The main content area is titled 'Maintenance > System Backup' and includes a 'Configuration' button. Below the title, there are buttons for 'Backup', 'Delete', 'Restore', 'Restore Remote Backup', 'Import', 'Export', 'View Logs', and 'View Last Backups'. A table for 'Local Backup' is currently empty. Below this, a blue bar indicates the 'Backup location: /var/log/CPbackup/backups'. The 'Scheduled Backup' section has buttons for 'Add Scheduled Backup', 'Edit', and 'Delete', followed by an empty table with columns for 'Backup Schedule Name', 'Recurrence', 'Destination', and 'Retention Policy'.

Creating a Backup Using the Gaia Portal

From the System Backup page:

1. Click **Backup**.
2. Select the destination of the backup file:
 - This appliance (locally)
 - Security Management Server
 - SCP, FTP, or TFTP server

Restoring from a Locally Saved Backup

From the System Backup page:

1. Select the backup file.
2. Click **Restore**.

Restoring from a Remotely Saved Backup

From the System Backup page:

1. Click **Restore Remote Backup**.
2. Enter the full name of the backup file on a remote server.
3. Select the destination of the backup file.
4. Click **Restore**.

Exporting a Backup Using the Gaia Portal

From the System Backup page:

1. Select the backup file.
2. Click **Export**.
3. Click **OK** to confirm.
4. Make sure you have enough free disk space on your computer.

Importing a Backup Using the Gaia Portal

From the System Backup page:

1. Select the backup file.
2. Click **Import**.
3. Browse to and select the backup file.
4. Click **Import**.

Deleting a Backup Using the Gaia Portal

From the System Backup page:

1. Select the backup file.
2. Click **Delete**.
3. Click **OK** to confirm.

System Backup - Gaia Clish

- Collect a backup and store it locally:

```
add backup local [interactive]
```

- Collect a backup and upload it to an SCP server:

```
add backup scp ip <IPv4 Address of SCP Server> path <Path  
on SCP Server> username <User Name on SCP Server>  
[password <Password in Plain Text>] [interactive]
```

System Backup - Gaia Clish (Continued)

- Collect a backup and upload it to an FTP server:

```
add backup ftp ip <IPv4 Address of FTP Server> path  
<Path on FTP Server> username <User Name on FTP  
Server> [password <Password in Plain Text>]  
[interactive]
```

- Collect a backup and upload it to a TFTP server:

```
add backup tftp ip <IPv4 Address of TFTP Server>  
[interactive]
```

- View the status of the latest backup:

```
show backup {last-successful | logs | status}
```

System Backup - Gaia Clish (Continued)

- View the status of the latest backup:

```
show backup {last-successful | logs | status}
```

- View the list of local backups and their location:

```
show backups
```

System Restore - Gaia Clish

- Restore a backup from a local hard disk:

```
set backup restore local<SPACE><TAB>
```

- Restore a backup from an SCP Server:

```
set backup restore scp ip <IPv4 Address of SCP Server>  
path <Path on SCP Server> file <Name of Backup File>  
username <User Name on SCP Server> [password <Password in  
Plain Text>] [interactive]
```

System Restore - Gaia Clish (Continued)

- Restore a backup from an FTP Server:

```
set backup restore local<SPACE><TAB>
```

- Restore a backup from a TFTP Server:

```
set backup restore tftp ip <IPv4 Address of TFTP Server>  
file <Name of Backup File> [interactive
```

Hardware Health Overview

- To ensure hardware operation, it is important to monitor the health of your Check Point appliances and servers on a regular basis.
- Depending on the hardware type, you must monitor these **hardware elements**:
 - Fan sensors - Shows the fan number, status, and speed.
 - System Temperature sensors
 - Voltage sensors
 - Power Supplies (on servers that support it)


Methods to Monitor Hardware Health

- You can monitor hardware health of Check Point appliances different ways.
- Two common methods are:
 - Gaia Portal
 - Gaia Clish















See:


- *Gaia Administration Guide*
- sk119232 - Hardware sensors thresholds on Check Point appliances

Monitoring Hardware Health Using the Gaia Portal

Maintenance ▶ Hardware Health 

Hardware Health

Sensor	Value	Status
 CPU1 DDR4-1	1.19 Volt	 Ok
 CPU1 DDR4-2	1.19 Volt	 Ok
 VCC 12V Voltage	12.07 Volt	 Ok
 VCC 3V Voltage	3.30 Volt	 Ok
 VCC 5V Voltage	5.03 Volt	 Ok
 3V Standby Voltage	3.31 Volt	 Ok
 5V Standby Voltage	5.04 Volt	 Ok

 Click any row to see its history...

1. Connect to the Gaia Portal from the appliance.
2. In the navigation tree, select **Maintenance** and then click **Hardware Health**.

The page displays the hardware status (OK, Low, or High).

3. Click on any row to view details

Monitoring Hardware Health Using the Gaia Clish

1. Access the Gaia Clish.
2. Use **show sysenv all** to display the hardware status:

```
gaia> show sysenv all
```

```
Hardware Information
```

Name	Value	unit	type	status	Maximum	Minimum
+12V	29.44	Volt	Voltage	0	12.6	11.4
+5V	6.02	Volt	Voltage	0	5.3	4.75
VBat	3.23	Volt	Voltage	0	3.47	2.7

```
gaia>
```

Monitoring Hardware Health Using the Gaia Clish (Continued)

3. To view a specific component, use the following syntax:

```
show sysenv [component]
```

Where component is:

```
bios
```

```
fans
```

```
ps
```

```
temp
```

```
volt
```

Showing RAID Information Using Gaia Portal

From the navigation tree:

1. Click **Maintenance**.
2. Click **RAID Monitoring**.
3. You can see the information about RAID Volumes and RAID Volume Disks.

Monitor the RAID status of the disks to see when the hard disks are synchronized.

Showing RAID Information Using Command Line

Run one of these commands in Gaia Clish or Expert mode:

```
raid_diagnostic
```

```
cpstat os -f raidInfo
```

If you reboot the appliance before the hard disks are synchronized, the synchronization starts again at the next boot.

Software Release Overview

- Major and minor releases
- Management Feature release
- Special release
- Jumbo Hotfix Accumulator

sk95746 - Check Point Recommended Version and Release Terminology

Check Point recommends that you install the most recent recommended software to stay up-to-date with the functional improvements, stability fixes, security enhancements, and protection against new and evolving attacks.

Major and Minor Releases

Major release

- Introduces new functionality and innovative technologies.

Minor release

- Provides new features and stability fixes.

Phases:

- Early Availability
- Latest Version
- Recommended Version

Management Feature release

- Introduces new features and stability fixes between Major and Minor releases.

Special Release

- Specific to a feature or scenario.

Jumbo Hotfix Accumulator

Accumulation of fixes and enhancements.

Released in two phases:

- Latest Jumbo:
 - Latest version for early adopters.
- Recommended Jumbo:
 - Recommended version for all deployments.

Check Point recommends you install the most recent Recommended Jumbo Hotfix Accumulator.

Check Point Upgrade Service Engine

- Lets you automatically update Check Point products for the Gaia operating system and the Gaia operating system itself.
- The software update packages and full images are for major releases, minor releases, and Hotfixes.
- CPUSE processes are handled by the Deployment Agent daemon (DA).
- Gaia automatically locates and shows the available software update packages and full images that are applicable.

Review Questions

1. Give at least two situations in which a snapshot is recommended.
2. Why is it recommended to schedule regular backups?
3. What is the preferred method of recovery?
4. In what compressed file format is a backup saved?

Lab 11A

Maintaining the Security Environment



Student Satisfaction Survey

Thank you for participating in this course!!

Please take a few minutes to complete the **Student Satisfaction Survey**. The survey measures your satisfaction with the training course delivery, the instructor, training materials, and ATC facilities.

<https://www.surveymonkey.com/r/CheckPointATC>