QUANTUM

22 April 2024

QUANTUM MAESTRO

R80.30SP

Administration Guide

Check Point Copyright Notice

Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications
For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point R80.30SP Quantum Maestro Administration Guide
For more about this release, see the R80.30SP home page.

Latest Version of this Document in English
Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
26 November 2023	Updated: ■ *"Installing a Hotfix Package on Orchestrators" on page 201* - CPUSE online installation is not supported ■ *"Clean Install of the Gaia Image on an Orchestrator with a Bootable USB Device" on page 241* Removed: ■ "Working with Session Control (asg_session_control)" - this command is not supported
07 April 2023	Updated: ■ *"Installing and Uninstalling a Hotfix on Security Group Members" on page 204*
04 April 2023	Updated: ■ *"Multi-blade Traffic Capture (tcpdump -mcap, tcpdump -view)" on page 95*
02 February 2023	Updated: ■ *"Policy Management on Security Group Members" on page 17*
18 December 2022	Updated: ■ *"General Diagnostic in Security Groups" on page 226*
15 December 2022	Updated: ■ *"General Diagnostic in Security Groups" on page 226*
01 February 2022	Improved the layout of the HTML output
20 December 2021	Updated: ■ *"Working with the Distribution Mode" on page 24*

Date	Description
17 October 2021	Added: ■ *"Backing Up and Restoring Gaia Configuration" on page 58* ■ *"Configuring Services to Synchronize After a Delay" on page 186* ■ *"Forwarding specific inbound-connections to the SMO (asg_excp_conf)" on page 190* Updated: ■ *"Installing and Uninstalling a Hotfix on Security Group Members" on page 204*
28 June 2021	Updated: ■ *"Replacing a Quantum Maestro Orchestrator" on page 242*
13 June 2021	Removed (temporarily): ■ *"Replacing a Quantum Maestro Orchestrator" on page 242*
19 February 2020	Updated: ■ *"Installing and Uninstalling a Hotfix on Security Group Members" on page 204* - removed the steps for "Online CPUSE packages"
06 October 2019	First release of this document

Table of Contents

Introduction

Quantum Maestro Orchestrator is a scalable Network Security System built to secure the largest networks in the world by orchestrating multiple Check Point Security Group Members into a unified system.

The Quantum Maestro Orchestrator provides:

- Security of infinite scale
- Redundancy - Quantum Maestro Orchestrator automatically distributes traffic between the Security Group Members assigned to Security Groups
- Ability to connect more Security Group Members and use their resources easily in the existing Security Groups

Security Group Concepts

This section describes some of the Security Group concepts.

Single Management Object (SMO) and Policies

In This Section:

Single Management Object

Single Management Object (SMO) is a Check Point technology that manages the Security Group as one large Security Gateway with one management IP address.

All management tasks are handled by one Security Group Member (the SMO Master), which updates all other Security Group Members.

All management tasks, such as Security Gateway configuration, policy installation, remote connections and logging are handled by the SMO master.

The Active Security Group Member with the lowest ID number is automatically assigned to be the SMO.

Use this command to identify the SMO and see how tasks are distributed on the Security Group Members (see *"Showing Hardware State (asg stat)" on page 126*).

Example output in a Single Site configuration:

```
[Expert@HostName-ch0x-0x:0]# asg stat -i tasks
-------------------------------------------------------------------------------
| Task (Task ID)     |                        Chassis 1                         |
-------------------------------------------------------------------------------
| SMO (0)            |                         1(local)                         |
| General (1)        |                         1(local)                         |
| LACP (2)           |                         1(local)                         |
| CH Monitor (3)     |                         1(local)                         |
| DR Manager (4)     |                         1(local)                         |
| UIPC (5)           |                         1(local)                         |
| Alert (6)          |                         1(local)                         |
-------------------------------------------------------------------------------
[Expert@HostName-ch0x-0x:0]#
```

Installing and Uninstalling Policies

Installing a Policy

To install a policy on the Security Group, click **Install Policy** in SmartConsole. The policy installation process includes these steps:

1. The Management Server installs the policy on the SMO Master.
2. The SMO Master copies the policy to all Security Group Members in the Security Group.
3. Each Security Group Member in the Security Group installs the policy locally.

During the policy installation, each Security Group Member sends and receives policy status updates to and from the other Security Group Members in the Security Group. This is because the Security Group Members must install their policies in a synchronized manner.

Note - When creating a Security Group, its Security Group Members enforce an initial policy which allows only the implied rules necessary for management.

Uninstalling a Policy

Step	Instructions
1	Connect over a serial port to the SMO in the Security Group.
2	Log in to the Gaia gClish.

3	Uninstall the policy:
	`> asg policy unload`
	Example:
	`> asg policy unload`
	`You are about to perform unload policy on blades: all`
	`Unloading policy from a virtual system will stop its monitoring by VS monitor (except VS 0).`
	`To re-enable VS monitoring on the specified VS(s) you must run the following command on a single SGM: 'cpha_vsx_util monitor start <vs_ids>'. For example: 'cpha_vsx_util monitor start 1,3'`
	`Must be executed via serial connection`
	`Are you sure? (Y - yes, any other key - no) y`

Note - You cannot uninstall policies from SmartConsole.

Working with Policies (asg policy)

Description

Use the `asg policy` command in Gaia gClish or the Expert mode to perform policy-related actions.

Syntax

`asg policy -h`
`asg policy {verify | verify_amw} [-vs <VS_IDs>] [-a] [-v]`
`asg policy unload [--disable_pnotes] [-a]`
`asg policy unload --ip_forward`

Best Practice - Run these commands over a serial connection to Security Group Members in the Security Group.

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`verify`	Confirms that the correct policies are installed on all Security Group Members in the Security Group.
`verify_amw`	Confirms that the correct Anti-Malware policies are installed on all Security Group Members in the Security Group.
`unload`	Uninstalls the policy from the Security Group Members in the Security Group.
`-vs <VS_IDs>`	Shows verification results for each Virtual System. *<VS_IDs>* can be: ■ No `<VS_IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems **Note** - This parameter is only applicable in a VSX environment.
`-v`	Shows detailed verification results for Security Group Members in each Virtual System.
`-a`	Runs the verification on Security Group Members in both UP and DOWN states.
`--disable_pnotes`	Security Group Members stay in the UP state without an installed policy. **Important** - If you omit this option, Security Group Members go into the DOWN state until the policy is installed again!
`--ip_forward`	Enables IP forwarding.

Below are some examples:

Example 1 - Detailed Virtual System Output

```
[Expert@MyChassis-ch01-01:0]# asg policy verify -v
+-------------------------------------------------------------------------+
|Policy Verification                                                      |
+-------+------------------+---------------+-----------------+---------+
|SGM    |Policy Name       |Policy Date    |Policy Signature |Status   |
+-------+------------------+---------------+-----------------+---------+
|1_01   |Standard          |27Feb19 08:56  |e17c177f7        |Success  |
+-------+------------------+---------------+-----------------+---------+

+-------------------------------------------------------------------------------+
|Summary                                                                        |
+-------------------------------------------------------------------------------+
|Policy Verification completed successfully                                     |
+-------------------------------------------------------------------------------+
[Expert@MyChassis-ch01-01:0]#
```

Example 2 - Uninstall Policy

```
[Expert@MyChassis-ch01-01:0]# asg policy unload
You are about to perform unload policy on blades: all
All SGMs will be in DOWN state, beside local SGM. It is recommended to run the procedure
via serial connection

Are you sure? (Y - yes, any other key - no) y

Unload policy requires auditing
Enter your full name: John Doe
Enter reason for unload policy [Maintenance]:
WARNING: Unload policy on blades: all, User: John Doe, Reason: Maintenance
+--------------------------------+
|Unload policy                   |
+---------------+----------------+
|SGM            |Status          |
+---------------+----------------+
|1_3            |Success         |
+---------------+----------------+
|1_2            |Success         |
+---------------+----------------+
|1_1            |Success         |
+---------------+----------------+
|2_3            |Success         |
+---------------+----------------+
|2_2            |Success         |
+---------------+----------------+
|2_1            |Success         |
+---------------+----------------+

+-------------------------------------------------------------------------------+
|Summary                                                                        |
+-------------------------------------------------------------------------------+
|Unload policy completed successfully                                           |
+-------------------------------------------------------------------------------+
[Expert@MyChassis-ch01-01:0]#
```

Policy Management on Security Group Members

In This Section:

Because the Security Group works as one large Security Gateway, all Security Group Members are configured with the same policy. When you install a policy from the Security Management Server, it first installs the policy on the SMO. The SMO copies the policy and Security Group Member configuration to all Security Group Members in the UP state. When the Security Group Member enters the UP state, it automatically gets the installed policy and configurations that are installed, from the SMO. When there is only one Security Group Member in the UP state, it is possible there is no SMO. Then, that Security Group Member uses its local policy and configuration.

If there are problems with the policy or configuration on the Security Group Member, you can manually copy the information from a different Security Group Member.

The Security Group Member configuration has these components:

- Firewall policy, which includes the Rule Base
- Set of configuration files defined in the `/etc/xfer_file_list` file. This file contains the location of all related configuration files. It also defines the action to take if the copied file is different from the one on the local Security Group Member.

Synchronizing Policy and Configuration Between Security Group Members

Use the `asg_blade_config pull_config` command in Gaia gClish to synchronize policies manually.

Optionally it can configure files from a specified source Security Group Member to the target Security Group Member.

The target Security Group Member is the Security Group Member you use to run this command.

To synchronize Security Group Members manually:

Step	Instructions
1	Run: `> asg_blade_config pull_config`

2	Reboot the target Security Group Member, or run these two commands:
	`cpstart`
	`clusterXL_admin up`

Note - You can run the `asg stat -i all_sync_ips` command in Gaia gClish to get a list of all synchronization IP addresses on the Security Group Member.

Understanding the Configuration File List

The `/etc/xfer_file_list` file contains pointers to the related configuration files on the Security Group Member. Each record defines the path to a configuration file, followed by the action to take if the imported file is different from the local file. This table shows an example of the record structure.

Context	File name and path	Action
`global_context`	`$FWDIR/boot/modules/fwkern.conf`	`/bin/false`

The context field defines the type of configuration file:

- `global_context` - Security Gateway configuration file
- `all_vs_context` - Virtual Systems configuration file

The action field defines the action to take when the imported (copied) file is different than the local file:

- `/bin/true` - Reboot is **not** required
- `/bin/false` - Reboot **is** required
- String enclosed in double quotes - Name of a "callback script" that selects the applicable action.

Example - Configuration file list:

```
[Expert@MyChassis-ch01-01:0]# cat /etc/xfer_file_list
#The Columns are:
#1) global_context or all_vs_context - VSX support.
#       It separates the files relevant to all VSs (all_vs_context) from those which are only relevant for VS0 (global_context)
#       In a security gateway mode, there is no difference between the two values
#2) File location in the SMO - where to pull the files from
#3) Action to perform after the file is copied, if it's different.
#       The result of the operation determines if a reboot is needed after the operation - 1 for reboot, 0 for no reboot
#       Please Notice - /bin/false => reboot, /bin/true => don't reboot
#4) [Optional] A local path to copy the file to, needed if different from the source

global_context /opt/CPda/bin/policy.xml /bin/true
global_context /etc/upgrade_pkg-0.1-cp989000001.i386.rpm "rpm -U --force --nodeps /etc/upgrade_pkg-0.1-cp989000001.i386.rpm"
global_context /etc/sysconfig/image.md5 "/usr/lib/smo/libclone.tcl --clone --rsip --xfer --reboot"
global_context $PPKDIR/boot/modules/sim_aff.conf "sim affinityload"
global_context $PPKDIR/boot/modules/simkern.conf /bin/false
global_context $FWDIR/boot/boot.conf /bin/false
global_context $FWDIR/boot/modules/fwkern.conf /bin/false
all_vs_context $FWDIR/conf/fwauthd.conf /bin/false
all_vs_context $FWDIR/conf/discntd.if /bin/false
#global_context /var/opt/fw.boot/ha_boot.conf /bin/false
global_context /config/active /usr/bin/confd_clone /config/db/cloned_db
global_context /tmp/sms_rate_limit.tmp /bin/true
global_context /tmp/sms_history.tmp /bin/true
global_context /home/admin/.ssh/known_hosts /bin/true
global_context /etc/passwd /bin/true
global_context /etc/shadow /bin/true
... output is cut for brevity ...
global_context /etc/smodb.json  "/usr/lib/smo/libclone_smodb.tcl clone_smodb_apply"     /tmp/smo_smodb.json
global_context $FWDIR/conf/prioq.conf   /bin/false
global_context /web/templates/httpd-ssl.conf.templ /usr/scripts/generate_httpd-ssl_conf.sh
all_vs_context $FWDIR/conf/fwaccel_dos_rate_on_install /bin/false
all_vs_context $FWDIR/conf/fwaccel6_dos_rate_on_install /bin/false
global_context $FWDIR/database/sam_policy.db $SMODIR/scripts/compare_samp_db.tcl /tmp/sam_policy.db.new
global_context $FWDIR/database/sam_policy.mng /bin/false
all_vs_context $FWDIR/conf/icap_client_blade_configuration.C /bin/true
global_context $CPDIR/conf/chassis_priority_db.C /bin/true
[Expert@MyChassis-ch01-01:0]#
```

MAC Addresses and Bit Conventions

MAC addresses on the system are divided into these types:

<table>
<tr><th>Type</th><th>Description</th></tr>
<tr><td>BMAC</td><td>A MAC address assigned to all interfaces with the <code>BPEthX</code> naming convention.
This is unique for each Security Group Member.
It does not rely on the interface index number.

Bit convention for BMAC
<table>
<tr><th>Bit range</th><th>Description</th></tr>
<tr><td>1</td><td>Distinguishes between VMAC and other MAC addresses.
This is used to prevent possible collisions with VMAC space.
Possible values are:
■ <code>0</code> - BMAC or SMAC
■ <code>1</code> - VMAC</td></tr>
<tr><td>2-8</td><td>Security Group Member ID (starting from 1).
This is limited to 127.</td></tr>
<tr><td>9-13</td><td>Always zero.</td></tr>
<tr><td>14</td><td>Distinguishes between BMAC and SMAC addresses.
This is used to prevent possible collisions with SMAC space.
Possible values:
■ <code>0</code> - BMAC
■ <code>1</code> - SMAC</td></tr>
<tr><td>15-16</td><td>Absolute interface number. This is taken from the interface name.
When the <code>BPEthX</code> format is used, <code>X</code> is the interface number.
This is limited to four interfaces.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Type</th><th>Description</th></tr>
<tr><td>VMAC</td><td>A MAC address assigned to all interfaces with the <code>ethX-YZ</code> naming convention.
This is unique for each Site.
It does not rely on the interface index number.

Bit convention for VMAC
<table>
<tr><th>Bit range</th><th>Description</th></tr>
<tr><td>1</td><td>Distinguishes between VMAC and other MAC addresses.
This is used to prevent possible collisions with VMAC space.
Possible values are:
<code>0</code> - BMAC or SMAC
<code>1</code> - VMAC</td></tr>
<tr><td>2-3</td><td>Site ID.
Limited to 2 Sites.</td></tr>
<tr><td>4-8</td><td>Switch number.
Limited to 32 switches.</td></tr>
<tr><td>9-16</td><td>Port number.
Limited to 256 for each switch.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Type</th><th>Description</th></tr>
<tr><td>SMAC</td><td>A MAC address assigned to Sync interfaces.
This is unique for each Security Group Member.
It does not rely on the interface index number.

Bit convention for SMAC
<table>
<tr><th>Bit range</th><th>Description</th></tr>
<tr><td>1</td><td>Distinguishes between VMAC and other MAC addresses.
This is used to prevent possible collisions with VMAC space.
Possible values are:

■ 0 - BMAC or SMAC
■ 1 - VMAC</td></tr>
<tr><td>2-8</td><td>Security Group Member ID (starting from 1).
This is limited to 127.</td></tr>
<tr><td>9-13</td><td>Always zero.</td></tr>
<tr><td>14</td><td>Distinguishes between BMAC and SMAC addresses.
This is used to prevent possible collisions with SMAC space.
Possible values:

■ 0 - BMAC
■ 1 - SMAC</td></tr>
<tr><td>15</td><td>Always zero.</td></tr>
<tr><td>16</td><td>Sync interface.
Possible values are:

■ 0 - Sync1
■ 1 - Sync2</td></tr>
</table></td></tr>
</table>

MAC Address Resolver (asg_mac_resolver)

Description

Use the `asg_mac_resolver` command in Gaia gClish or the Expert mode to make sure that all types of MAC addresses, BMAC, VMAC, and SMAC, are correct.

From the MAC address you provide, the `asg_mac_resolver` command determines the:

- MAC type
- Site ID
- Security Group Member ID
- Assigned interface

Syntax

```
asg_mac_resolver <MAC address>
```

Example

```
[Expert@MyChassis-ch01-01:0]# asg_mac_resolver 00:1C:7F:01:00:FE
[00:1C:7F:01:00:FE, BMAC] [Chassis ID: 1] [SGM ID: 1] [Interface: BPEth0]
[Expert@MyChassis-ch01-01:0]#
```

Notes:

- The specified MAC Address comes from BPEth0 on Security Group Member #1 on Site #1.
- `00:1C:7F:01:00:FE` is the Magic MAC attribute, which is identified by `FE`.
- The index length is 16 bits (2 Bytes) identified by 01:00 x x x x x x x x x x x x x x x x.

Working with the Distribution Mode

In This Section:

The Quantum Maestro Orchestrator uses the Distribution Mode to assign incoming traffic to Security Group Members in each Security Group.

By default, the Quantum Maestro Orchestrator automatically configures the Distribution Mode.

Supported Distribution Modes

Mode	Description
User (Internal)	Packets are assigned to a Security Group Member based on the packet's Destination IP address. If Layer 4 distribution is enabled, packets are assigned to a Security Group Member based on the packet's Source port and the Destination IP address.
Network (External)	Packets are assigned to a Security Group Member based on the packet's Source IP address. If Layer 4 distribution is enabled, packets are assigned to a Security Group Member based on the packet's Source IP address and Destination port.
General	Packets are assigned to a Security Group Member based on both the packet's Source IP address and the Destination IP address. If Layer 4 distribution is enabled, packets are assigned to a Security Group Member based on the packet's Source IP address, Source port, Destination IP address, and Destination port.
Auto-Topology (Per-Port)	Each port for a Security Group Member is configured separately in the User Mode or Network Mode.

Notes:

- The default distribution mode is **Auto-Topology** with Layer 4 distribution enabled.
- The **User Mode** and **Network Mode** can work together. These combinations are supported:
  - User Mode and User Mode
  - User Mode and Network Mode
  - Network Mode and Network Mode

  In many scenarios, the User Mode and Network Mode combination could be optimized to pass traffic on same Security Group Member from both sides.

Automatic Distribution Configuration (Auto-Topology)

By default, Security Groups work in **General Mode**. The best Distribution Mode is selected based on the Security Group topology as defined in SmartConsole.

The Distribution Mode is automatically based on these interface types:

- Physical interfaces, except for management and synchronization interfaces
- VLAN
- Bond
- VLAN over Bond

Manual Distribution Configuration (Manual-General)

In some deployments, you must manually configure a Distribution Mode on the Security Group to the **General**. In other cases, it may be necessary to force the Security Group to work in **General Mode**.

When the Distribution Mode is manually configured (**Manual-General Mode**), the Distribution Mode of the Security Group is **General**. In this configuration, the topology of the interfaces is irrelevant.

Best Practice - Do *not* change manually the Distribution Mode of a Virtual System. This can cause performance degradation.

Setting and Showing the Distribution Configuration (set distribution configuration)

Use these Gaia gClish commands to set and show the distribution configuration on the Security Group.

Important - If the Security Group runs in a VSX mode, run the commands in the context of VS0 only. The commands apply immediately across all Virtual Systems.

Syntax to show the Distribution Configuration

```
> show distribution configuration
```

Syntax to set the Distribution Configuration

```
> set distribution configuration {auto-topology | manual-general}
ip-version {ipv4 | ipv6 | all} ip-mask <mask>
```

Parameters

Parameter	Notes
`auto-topology`	Configures the distribution mode to Auto-Topology (Per-Port).
`manual-general`	Configures the distribution mode to Manual General.
`ipv4`	Configures the distribution mode for IPv4 traffic only.
`ipv6`	Configures the distribution mode for IPv6 traffic only.
`all`	Configures the distribution mode for IPv4 and IPv6 traffic.

`ip-mask <`*`mask`*`>`	Must be the same as the distribution matrix size.
	Must be specified in the Hex format.
	Follow these steps:
	1. Examine the distribution matrix size:
	`> show distribution verification verbose`
	Examine the `Matrix Size` line.
	Example:
	`... Matrix Size 512 ...`
	2. Exit from the Gaia gClish to the Expert mode.
	3. Convert the matrix size from the decimal to the hexadecimal format:
	`# printf '%x\n' <`*`Matrix Size`*`>`
	Example:
	`[Expert@MyChassis-ch01-01:0]# printf '%x\n' 512 200 [Expert@MyChassis-ch01-01:0]#`
	4. Go to the Gaia gClish:
	`# gclish`
	5. Configure the distribution mode with the required mask:
	`> set distribution ... ip-mask <`*`Matrix Size in HEX`*`>`
	Example:
	`> set distribution ... ip-mask 200`

Configuring the Interface Distribution Mode (set distribution interface)

Description

Use these commands to:

- Set the interface Distribution Mode - For an interface when the system is not working in the General Mode
- Show the interface Distribution Mode - If it is assigned by Auto-Topology, or is manually configured

Notes:

- You must run these commands in the Gaia gClish of the Security Group.
- In VSX mode, you must go to the context of the applicable Virtual System before you can change the interface Distribution Mode. Run the `set virtual-system <VS_ID>` command.

Syntax to set the interface Distribution Mode

```
> set distribution interface <if_name> configuration {user |
network | policy}
```

Syntax to show the interface Distribution Mode

```
> show distribution interface <if_name> configuration
```

Parameters

Parameter	Description
`<if_name>`	Interface name as assigned by the operating system.
`user`	Manually assign the User (Internal) Distribution Mode - based on Destination IP address.
`network`	Manually assign the Network (External) Distribution Mode - based on Source IP address.
`policy`	Use Auto-Topology to automatically assign the Distribution Mode according to the policy.

Below are some examples:

Example 1 - Set the Distribution Mode to Network (External)

```
> set distribution interface eth1-01 configuration network
/bin/distutil set_ifn_dist_mode eth1-01 external
```

Example 2 - Set the Distribution Mode to use the Auto-Topology to assign traffic according to the policy

```
> set distribution interface eth1-01 configuration policy
/bin/distutil set_ifn_dist_mode eth1-01 policy
```

Example 3 - Set the Distribution Mode to User (Internal)

```
> set distribution interface eth1-01 configuration user
/bin/distutil set_ifn_dist_mode eth1-01 internal
```

Showing Distribution Status (show distribution status)

Description

Use this command to show the status report of the Distribution Mode.

Syntax

```
> show distribution status [verbose]
```

Below are some examples:

Example 1 - Regular output

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> show distribution status
Verification passed successfully
[Global] MyChassis-ch01-01>
```

Example 2 - Verbose output

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> show distribution verification verbose
Test:               Configuration:      Verification:       Result:
Mode                per-port            per-port            Passed
L4 Mode             on                  on                  Passed
Matrix Size         512                 512                 Passed
eth2-08             policy-external     policy-external     Passed
eth1-08             policy-internal     policy-internal     Passed
eth2-07             policy-internal     policy-internal     Passed
eth2-06             policy-internal     policy-internal     Passed
eth1-05             manual-internal     manual-internal     Passed
eth1-06             policy-internal     policy-internal     Passed
eth1-07             policy-internal     policy-internal     Passed

Verification passed successfully
[Global] MyChassis-ch01-01>
```

Explanation about the output:

Field	Description
`L4 Mode`	Shows if Layer 4 distribution is enabled.
`Mode`	Shows the distribution mode.
`Matrix Size`	Shows the size of the Distribution Mode matrix.
`Ports`	Shows the Distribution Mode assignment for each interface.

Running a Verification Test (show distribution verification)

Description

Use the `show distribution verification` command to run a verification test of the Distribution Mode configuration.

This test compares the Security Group Member and SSM configurations with the actual results.

You can see a summary or a verbose report of the test results.

Syntax

```
> show distribution verification [verbose]
```

Below are some examples:

Example 1 - Verbose output of successful tests

```
> show distribution verification verbose
Test:               Configuration:      Verification:       Result:
Mode                per-port            per-port            Passed
L4 Mode             off                 off                 Passed
Matrix Size         512                 512                 Passed
eth2-16             policy-internal     policy-internal     Passed
eth1-16             policy-internal     policy-internal     Passed
eth1-15             policy-external     policy-external     Passed
>
```

Example 2 - Verbose output of failed tests

```
> show distribution verification verbose
Test:               Configuration:      Verification:       Result:
Mode                per-port            per-port            Passed
L4 Mode             on                  off                 Failed
Matrix Size         512                 0                   Failed
eth1-05             policy-internal     policy-internal     Passed
eth1-06             policy-internal     policy-internal     Passed
eth2-05             policy-external     policy-external     Passed
eth2-06             manual-internal     policy-external     Failed

Verification failed with above errors
>
```

Configuring the Layer 4 Distribution Mode and Masks (set distribution l4-mode)

Description

Use these commands in Gaia gClish to:

- Enable Layer 4 distribution and set new masks for the IP address and the port
- Disable Layer 4 distribution
- Show Layer 4 Distribution Mode and masks

Note - When working with a Virtual System, you must go to the context of the applicable Virtual System context before you can change the Distribution Mode. Run the `set virtual-system <VS_ID>` command.

Syntax

```
> set distribution l4-mode enabled
```

```
> set distribution l4-mode disabled
```

```
> show distribution l4-mode
```

Below are some examples:

Example 1 - Configure the Layer 4 Distribution Mode

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> set distribution l4-mode enabled
1_01:
success

1_02:
success
[Global] MyChassis-ch01-01>
```

Example 2 - Disable the Layer 4 Distribution Mode

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> set distribution l4-mode disabled
1_01:
success

1_02:
success
[Global] MyChassis-ch01-01>
```

Example 3 - Show the current Layer 4 Distribution Mode and Masks

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> show distribution l4-mode
1_01:
L4 Distribution: Enabled

1_02:
L4 Distribution: Enabled
[Global] MyChassis-ch01-01>
```

NAT and the Correction Layer on a Security Gateway

For optimal system performance, one Security Group Member handles all traffic for a session. With NAT, packets sent from the client to the server can be distributed to a different Security Group Member than packets from the same session sent from the server to the client. The system correction layer must then forward the packet to the correct Security Group Member.

Configuring the Distribution Mode correctly keeps correction situations to a minimum and optimizes system performance.

To achieve optimal distribution between Security Group Members in a Security Group in Gateway mode:

NAT Rules	Instructions
Not using NAT rules	Set the General Distribution Mode.
Using NAT rule	Set the hidden networks to the User Mode Set the destination networks to the Network Mode

NAT and the Correction Layer on a VSX Gateway

In a VSX Gateway, the guidelines in NAT and the correction layer on a Security Gateway apply to each Virtual System individually. For best results, manage an entire session by the same Security Group Member by a specified Virtual System. When a Virtual Switch (junction) connects several Virtual Systems, the same session can be handled by one Virtual System on one Security Group Member, and by another Virtual System on a different Security Group Member.

When a packet reaches a Virtual System from a junction, the system VSX Stateless Correction Layer rechecks the distribution according to the WRP interface's Distribution Mode. It can decide to forward the packet to a different Security Group Member.

In addition, on each Virtual System, the system's correction layer, which is stateful, can forward session packets, similar to the Security Gateway.

All forwarding operations have a performance impact. Therefore, the Distribution Mode configuration should minimize forwarding operations.

To achieve optimal distribution between Security Group Members in a Security Group in VSX mode:

NAT Rules	Instructions
Not using NAT rules on any Virtual System	Set the General Distribution Mode.
Using NAT rule on at least one Virtual System	■ On the Virtual Systems that use NAT rules: • Set the hidden networks to the User Mode • Set the destination networks to the Network Mode ■ On the remaining Virtual Systems that do not use NAT rules: • Set internal networks to the User Mode • Set the external networks to the Network Mode

Working with the GARP Chunk Mechanism

In This Section:

Description

When Proxy ARP is enabled, the Firewall responds to ARP requests for hosts other than itself. When failover occurs between Security Group Members, the new Active Security Group Member sends Gratuitous ARP (GARP) Requests with its own (new) MAC address to update the network ARP tables.

To prevent network congestion during failover, GARP Requests are sent in user defined groups called chunks. Each chunk contains a predefined number of GARP Requests based on these parameters:

- The number of GARP Requests in each chunk (default is 1000 in each HTU).
- High Availability Time Unit (HTU) - Time interval (1 HTU = 0.1 sec), after which a chunk is sent.
- The chunk mechanism iterates on the proxy ARP IP addresses, and each time sends GARP Requests only for some of them until it completes the full list.

When the iteration sends the full list, it waits *N* HTUs and sends the list again.

Configuration

Important - To make the configuration permanent (to survive reboot), add the applicable kernel parameters to the `$FWDIR/boot/modules/fwkern.conf` file with this command:

```
g_update_conf_file fwkern.conf <Parameter>=<Value>
```

For example, to send 10 GARP Requests each second, set the value of the kernel parameter `fwha_refresh_arps_chunk` to 1:

```
g_fw ctl set int fwha_refresh_arps_chunk 1
```

To send 50 GARP Requests each second, set the value of the kernel parameter `fwha_refresh_arps_chunk` to 5:

```
g_fw ctl set int fwha_refresh_arps_chunk 5
```

Whenever the iteration is finished sending GARP Requests for the entire list, it waits *N* HTUs and sends the GARP Requests again.

The time between the iterations can be configured with these kernel parameters:

Kernel Parameter	Description
`fwha_periodic_send_garps_interval1`	The default value is 1 HTU (0.1 second). The Security Group sends the GARP immediately after failover. **Important** - Do not change this value.
`fwha_periodic_send_garps_interval2`	The default value is 10 HTUs (1 second). After the iteration sends the GARP list, it waits for this period of time and sends it again.
`fwha_periodic_send_garps_interval3`	The default value is 20 HTUs (2 seconds). After the iteration sends the GARP list, it waits for this period of time and sends it again.
`fwha_periodic_send_garps_interval4`	The default value is 50 HTUs (5 seconds). After the iteration sends the GARP list, it waits for this period of time and sends it again.
`fwha_periodic_send_garps_interval5`	The default value is 100 HTUs (10 seconds). After the iteration sends the GARP list, it waits for this period of time and sends it again.

To change an interval, run:

```
g_fw ctl set int fwha_periodic_send_garps_interval<N> <Value>
```

To apply the intervals, run:

```
g_fw ctl set int fwha_periodic_send_garps_apply_intervals 1
```

Verification

To send GARP Requests manually, on the SMO, run:

```
g_fw ctl set int test_arp_refresh 1
```

This causes GARP Requests to be sent (same as was failover).

To debug:

```
g_fw ctl zdebug -m cluster + ch_conf | grep fw_refresh_arp_proxy_
on_failover
```

IPS Management During a Cluster Failover

You can configure how IPS is managed during a cluster failover.

This occurs when one Cluster Member takes over for a different Cluster Member to supply High Availability.

You must run this command in the Expert mode.

Syntax to configure the IPS cluster failover behavior

```
# asg_ips_failover_behavior {connectivity | security}
```

Parameters

Parameter	Description
`connectivity`	Prefer connectivity (default). Keeps connections alive, even if IPS inspection cannot be guaranteed.
`security`	Prefer security. Closes connections, for which IPS inspection cannot be guaranteed.

Syntax to view the configured IPS cluster failover behavior

```
fw ctl get int fwha_ips_reject_on_failover
```

- If the output shows `fwha_ips_reject_on_failover = 0`, it means the connectivity is preferred.
- If the output shows `fwha_ips_reject_on_failover = 1`, it means the security is preferred.

Managing Security Groups

This section provides basic information about managing Security Groups.

Global Commands

In This Section:

The Gaia operating system includes a set of global commands that apply to all or specified Security Group Members in a Security Group.

Working with Global Commands

Background

- Gaia gClish commands apply globally to all Security Group Members in the Security Group, by default.
- Gaia gClish commands do not apply to Security Group Members that are DOWN in the Security Group. If you run a `set` command while a Security Group Member is DOWN, the command does not update that Security Group Member. The Security Group Member synchronizes its database during startup and applies the changes after reboot.
- Gaia Clish commands apply only to the specific Security Group Member. They are documented in the *R80.30SP Quantum Maestro Gaia Administration Guide*.

Global Commands

Command	Description
`auditlog`	■ Enabled by default. ■ All commands are recorded in the audit log. ■ To learn more about the audit log, see *Looking at the Audit Log*.
`config-lock`	■ Protects the Gaia gClish database by locking it. Each Security Group Member has a single lock. ■ To set Gaia gClish operations for an Security Group Member, the Security Group Member must hold the `config-lock`. ■ To set `config-lock`, run: `# set config-lock on override` ■ Gaia gClish traffic runs on the Sync interface, TCP port 1129.
`blade-range`	■ Runs commands on specified Security Group Members. ■ Runs Gaia gClish embedded commands only on this subset of Security Group Members. ■ We do not recommend that you use the `blade-range` command, because all Security Group Members must have identical configurations.

Check Point Global Commands

These global commands apply to more than one Security Group Member. These global commands let you work with Security Gateway and SecureXL.

fw, fw6

Description

The `fw` and `fw6` commands are global scripts that run the `fw` and `fw6` commands on each Security Group Member.

Below are some examples:

Example 1

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> fw ctl
-*- 2 blades: 1_01 1_02 -*-
 Usage: fw ctl command args...
 Commands: install, uninstall, pstat, iflist, arp, debug, kdebug, bench
    chain, conn, multik, conntab, fwghtab_bl_stats
>
```

Example 2

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> fw ctl iflist
-*- 6 blades: 1_01 1_02 1_03 2_01 2_02 2_03 -*-
0 : BPEth0
1 : BPEth1
2 : eth1-Mgmt4
3 : eth2-Mgmt4
4 : eth1-01
5 : eth1-CIN
6 : eth2-CIN
8 : eth2-01
16 : Sync
17 : eth1-Mgmt1
18 : eth2-Mgmt1
>
```

fw dbgfile

Description

Use the `fw dbgfile` commands in Gaia gClish to debug the system.

Syntax to collect the debug

```
> fw dbgfile collect -f <debug_file_path> [-buf <buf_size>] [-m
<debug_module_1> <debug_flags_1> [-m <debug_module_2> <debug_
flags_2>] ... [-m <debug_module_N> <debug_flags_N>]]
```

Syntax to show the collected debug

```
> fw dbgfile view [<debug_file_path>] [-o <agg_file_path>]
```

Parameters

Parameter	Description
`collect`	Collects the Security Gateway debug information.
`view`	Shows the collected debug information.
`<debug_file_path>`	Specifies the full path of the debug file.
`-buf <buf_size>`	Specifies the debug buffer size. Always set the maximal size 8200.
`-m <debug_module_1> <debug_flags_1> [-m <debug_module_2> <debug_flags_2>] ... [-m <debug_module_N> <debug_flags_N>]`	Specifies Security Gateway debug modules and debug flags in those modules. You can specify more than one debug module.
`-o <agg_file_path>`	Uses an aggregate debug file. `<agg_file_path>` - Full path of the aggregate debug file.

Below are some examples:

Example - Collect debug information

```
> fw dbgfile collect -f /var/log/debug.txt -buf 8200 -m fw + conn -m kiss + pmdump
```

Example - Show the collected debug information

```
> fw dbgfile view /var/log/debug.txt
```

Important - For complete debug procedure, see the *R80.30SP Quantum Maestro Security Gateway Guide* - Chapter *Kernel Debug on Security Groups*.

fwaccel, fwaccel6

Description

The `fwaccel` commands control the acceleration for IPv4 traffic.

The `fwaccel6` commands control the acceleration for IPv6 traffic.

When you run the `fwaccel` and `fwaccel6` commands in Gaia gClish, they show combined information from all Security Group Members, for most parameters.

Syntax for IPv4

```
fwaccel help
```

Syntax for IPv6

```
fwaccel6 help
```

Parameters and Options

For more information, see the *R80.30SP Quantum Maestro Performance Tuning Administration Guide* - Chapter *SecureXL* - Section *SecureXL Commands* - Subsection *'fwaccel' and 'fwaccel6'*.

General Global Commands

Global commands apply to more than one Security Group Member.

See the syntax of the global commands in *"Global Operating System Commands" on page 52*.

These commands are available in Gaia Clish and Gaia gClish:

In Gaia Clish and Gaia gClish	In the Expert mode
`update_conf_file`	`g_update_conf_file`
`global`	`global_help`
`asg_cp2blades`	`asg_cp2blades`
`asg_clear_table`	`asg_clear_table`

Below are some global commands

Viewing the List of Global Commands (global help)

Description

The `global help` command in Gaia gClish shows the list of global commands you can use in Gaia gClish and how they are generally used.

Syntax

```
> global help
```

Below are some examples:

Example output in Gateway mode

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> global help
Usage: <command_name> [-b SGMs] [-a -l -r --] <native command arguments>
Executes the specified command on specified blades.

Optional Arguments:
  -b   blades: in one of the following formats
               1_1,1_4 or 1_1-1_4 or 1_01,1_03-1_08,1_10
               all (default)
               chassis1
               chassis2
               chassis_active
  -a         : Force execution on all SGMs (incl. down SGMs).
  -l         : Execute only on local blade.
  -r         : Execute only on remote SGMs.

Command list:
snapshot_show_current snapshot_recover fwaccel6_m fwaccel6 fw6 unlock update_conf_file mv fwaccel_m ethtool md5sum dmesg cp
tcpdump cat tail clusterXL_admin reboot ls fwaccel vpn fw netstat cpstop cpstart cplic asg
[Global] MyChassis-ch01-01>
```

Example output in VSX mode

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> global help
Usage: <command_name> [-b SGMs] [-a -l -r --] <native command arguments>
Executes the specified command on specified blades.

Optional Arguments:
  -b   blades: in one of the following formats
               1_1,1_4 or 1_1-1_4 or 1_01,1_03-1_08,1_10
               all (default)
               chassis1
               chassis2
               chassis_active
  -a         : Force execution on all SGMs (incl. down SGMs).
  -l         : Execute only on local blade.
  -r         : Execute only on remote SGMs.

Command list:
cplic cpstart cpstop netstat fw vpn fwaccel ls reboot clusterXL_admin tail cat tcpdump cp dmesg md5sum ethtool fwaccel_m mv
update_conf_file unlock fwaccel6_m snapshot_recover snapshot_show_current asg
[Global] MyChassis-ch01-01>
```

Updating Configuration Files (update_conf_file)

Description

Use the `update_conf_file` command in Gaia gClish or the `g_update_conf_file` command in the Expert mode to add, update, and remove variables from configuration files.

Important - After you change the configuration files, you must reboot all Security Group Members..

Syntax

`update_conf_file <file_name> <variable>=<value>`
`g_update_conf_file <file_name> <variable>=<value>`

Parameters

Parameter	Description
<file_name>	Full path and name of the configuration file to update You do not need to specify the full path for these files (only specify the file name): ■ `$FWDIR/boot/modules/fwkern.conf` ■ `$PPKDIR/conf/simkern.conf`
<variable>	Name of the variable to update
<value>	New value for the variable

Examples

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> update_conf_file /home/admin/MyConfFile.txt var1=hello
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var1=hello

[Global] MyChassis-ch01-01> update_conf_file /home/admin/MyConfFile.txt var2=24h
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var2=24h
var1=hello

[Global] MyChassis-ch01-01> update_conf_file /home/admin/MyConfFile.txt var1=goodbye
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var2=24h
var1=goodbye

[Global] MyChassis-ch01-01> update_conf_file /home/admin/MyConfFile.txt var2=
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var1=goodbye
[Global] MyChassis-ch01-01>
```

Notes:

- This command works with configuration files in a specified format. It is composed of lines where each line defines one variable:

  `<variable>=<value>`

  The `$FWDIR/boot/modules/fwkern.conf` and `$PPKDIR/conf/simkern.conf` files use this format.

- Variable name must not include an equal sign (=).
- If the specified configuration file does not exist, this command creates it.
- This command makes the required changes on all Security Group Members.

  It is not necessary to copy the updated file to other Security Group Members with the "`asg_cp2blades`" command.

Setting Firewall Kernel Parameters (g_fw ctl set)

Description

Use these commands in the Expert mode to set or show specified Firewall kernel parameters.

Syntax for viewing the current value of a variable

```
# g_fw ctl get <type> <parameter_name>
```

Syntax for setting a value of a variable

```
# g_fw ctl set <type> <parameter_name> <value>
```

Parameters

Parameter	Description
`get`	Shows the specified parameter and its value.
`set`	Change the parameter value to the specified value.
<type>	Type of parameter value: ▪ `int` - Integer value ▪ `str` - String value **Note** - You must enter the correct parameter type.
<parameter_name>	Parameter name.
<value>	Parameter value.

Note - To make changes persistent, you must manually add the applicable kernel parameters and their values in the `$FWDIR/boot/modules/fwkern.conf`. Use the `g_update_conf_file` command in the Expert mode. See *"Updating Configuration Files (update_conf_file)" on page 46*.

For more information, see the *R80.30SP Quantum Maestro Security Gateway Guide* - Chapter *Working with Kernel Parameters on Security Groups*.

Copying Files Between Security Group Members (asg_cp2blades)

Description

Use the `asg_cp2blades` command in Gaia gClish or the Expert mode to copy files from the current Security Group Member to other Security Group Members.

Syntax

```
asg_cp2blades [-b <SGM_IDs>] [-s] <source_path> [<dest_path>]
```

Parameters

Parameter	Description
`-b <SGM_IDs>`	Applies to Security Group Members as specified by `<SGM_IDs>`. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`)
`-r`	Copy folders and directories that contain files.
`-s`	Save a local copy of the old file on each Security Group Member The copy is saved in the same directory as the new file. The old file has the same name with this at the end: `*.bak.<date>.<time>`
<source_path>	Full path and name of the file to copy
<dest_path>	Full path of the destination If not specified, the command copies the file to the relative source file location.

Example

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01 > asg_cp2blades /home/admin/note.txt
Operation completed successfully
[Global] MyChassis-ch01-01 >
[Global] MyChassis-ch01-01 > cat /home/admin/note.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
hello world
[Global] MyChassis-ch01-01>
```

Deleting Connections from the Connections Table (asg_clear_table)

Description

Deleting Connections from the Connections Table (asg_clear_table)

Description

Use the `asg_clear_table` command in Gaia gClish or the Expert mode to delete connections from the Security Gateway Connections table.

The command runs up to 15 times, or until there are less than 50 connections left.

Note - If you are connected to the machine with SSH, your connection is disconnected.

Syntax

```
asg_clear_table [-b <SGM_IDs>]
```

Parameters

Parameter	Description
`-b <SGM_IDs>`	Applies to Security Group Members as specified by `<SGM_IDs>`. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`) **Note** - With this option, you can only select Security Group Members from one Site.

Viewing Information about Interfaces on Security Group Members (show interface)

Description

Use the `show interface` command in Gaia gClish to view information about the interfaces on the Security Group Members.

For more information, see the *R80.30SP Quantum Maestro Gaia Administration Guide* - Chapter *Network Management* - Section *Network Interfaces*.

Syntax

```
> show interfaces all
```

```
> show interface <options>
```

Example

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> show interface eth1-01 ipv4-address
1_01:
ipv4-address 4.4.4.10/24

1_02:
ipv4-address 4.4.4.10/24

1_03:
ipv4-address 4.4.4.10/24

1_04:
ipv4-address 4.4.4.10/24

1_05:
Blade 1_05 is down. See "/var/log/messages".

2_01:
ipv4-address 4.4.4.10/24

2_02:
ipv4-address 4.4.4.10/24

2_03:
ipv4-address 4.4.4.10/24

2_04:
ipv4-address 4.4.4.10/24

2_05:
ipv4-address 4.4.4.10/24
[Global] MyChassis-ch01-01>
```

Global Operating System Commands

Global operating system commands are standard Linux commands that run on all or specified Security Group Members. When you run a global command in the Gaia gClish, the operating system runs a global script that is the standard Linux command on the Security Group Members. When you run a command in the Expert mode, it works as a standard Linux command. To use the global command in the Expert mode, run the global command script version as shown in this table:

Gaia gClish Command	Global Command in the Expert Mode
`arp`	`g_arp`
`cat`	`g_cat`
`cp`	`g_cp`
`dmesg`	`g_dmesg`
`ethtool`	`g_ethtool`
`ls`	`g_ls`
`md5sum`	`g_md5sum`
`mv`	`g_mv`
`netstat`	`g_netstat`
`reboot`	`g_reboot`
`tail`	`g_tail`
`tcpdump`	`g_tcpdump`
`ifconfig`	`asg_ifconfig`
`top`	`g_top`

Note - The parameters and options for the standard Linux command are available for the global command. You can use one or more flags. However, do not use the `-l` and `-r` flags together.

Syntax

```
{<Gaia gClish Command> | <Global Command>} [-b <SGM_IDs>]
[<Command Options>]
```

Parameters

Parameter	Description
`-b <SGM_IDs>`	Applies to Security Group Members as specified by `<SGM_IDs>`. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`) **Note** - With this option you can only select Security Group Members from one Site.
<Gaia gClish Command>	Standard command in Gaia gClish.
<Global Command>	Global command in the Expert mode as shown in the table above.
<Command Options>	Standard command options for the specified command.

Below is the syntax for some of the global commands

Global 'ls'

Description

This command shows the file in the specified directory on all Security Group Members.

Syntax

```
# g_ls [-b <SGM_IDs>] <command_options>]
> ls [-b <SGM_IDs>] <command_options>]
```

Example

This example runs the '`g_ls`' command in the Expert mode on Security Group Members `1_1`, `1_2`, and `1_3`.

The example output shows the combined results for these Security Group Members.

```
[Expert@MyChassis-ch01-01:0]# g_ls -b 1_1-1_3,2_1 /var/
-*- 4 blades: 1_01 1_02 1_03 -*-
CPbackup    ace    crash  lib   log   opt       run    suroot
CPsnapshot  cache  empty  lock  mail  preserve  spool  tmp
[Expert@MyChassis-ch01-01:0]#
```

Global 'reboot'

Description

This command reboots all Security Group Members.

Syntax

```
# g_reboot [-a]
```

```
> reboot [-a]
```

Parameters

Parameter	Description
No Parameter	Reboots all Security Group Members that are in the UP state only.
`-a`	Reboots all Security Group Members in both the DOWN and UP states.

Global 'top'

Description

The global `top` command shows activity of Security Group Member processors in real time.

The default output also shows a list of the most processor-intensive processes.

The global `top` command relies on the user configuration for the local `top` utility.

The command uses the local Security Group Member configuration file for configuring the output on the remote Security Group Members.

With the standard functionality of the Linux `top` command, the global `top` command adds these features for the Security Group.

Syntax for Gaia gClish

```
> top -h
```

```
> top [local] [{-f [-o <filename>] [-n <iter>] | -s <filename>}]
-b <SGM_IDs> [<top_params>]
```

Syntax for the Expert mode

```
# g_top -h
```

```
# g_top [local] [{-f [-o <filename>] [-n <iter>] | -s
<filename>}] -b <SGM_IDs> [<top_params>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`local`	Use the local configuration file.
`-f`	Export the output to a file.
`-o <filename>`	File and path of the output file. Default = `/var/log/gtop.<time>` Use with `-f`
`-n <iter>`	Number of iterations. Default = 1 Use with `-f`
`-b <SGM_IDs>`	Applies to Security Group Members as specified by `<SGM_IDs>`. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`)
`<top_params>`	Parameters of the standard `top` command. For more information, see the `top` command documentation.
-s <*filename*>	Shows the content of the output file <*filename*>.

The `top` command uses a configuration file to manage output display. By default, it copies and uses this configuration file from the local blade (usually located in the `~/.toprc`). This file is copied to all Security Group Members and is used when the `top` command is run.

To manage the 'g_top' display:

1. Run:

   ```
   # top
   ```

2. Set the desired display view (press **h** to see the built-in help).
3. Press **Shift+W** to save the configuration.
4. Run:

   ```
   # g_top
   ```

To send output to a file

At times, it is more convenient to send the `g_top` output to a file. For example, when there are more Security Group Members than the screen can handle.

To enable the File Mode, run:

```
# g_top -f
```

Global 'arp'

Description

This command shows the ARP cache table on all Security Group Members.

Syntax

```
# g_arp [-b <SGM_IDs>] [<command_options>]
> arp [-b <SGM_IDs>] [<command_options>]
```

Example - ARP table on all interfaces of all Security Group Members

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> arp
1_01:
Address     HWtype  HWaddress           Flags Mask   Iface
192.0.2.2   ether   00:1C:7F:02:04:FE   C            Sync
172.23.9.28 ether   00:14:22:09:D2:22   C            eth1-Mgmt4
192.0.2.3   ether   00:1C:7F:03:04:FE   C            Sync
1_02:
Address     HWtype  HWaddress           Flags Mask   Iface
192.0.2.3   ether   00:1C:7F:03:04:FE   C            Sync
172.23.9.28 ether   00:14:22:09:D2:22   C            eth1-Mgmt4
192.0.2.1   ether   00:1C:7F:01:04:FE   C            Sync
1_03:
Address     HWtype  HWaddress           Flags Mask   Iface
192.0.2.1   ether   00:1C:7F:01:04:FE   C            Sync
172.23.9.28 ether   00:14:22:09:D2:22   C            eth1-Mgmt4
192.0.2.2   ether   00:1C:7F:02:04:FE   C            Sync
[Global] MyChassis-ch01-01>
```

Backing Up and Restoring Gaia Configuration

For more information, see the *R80.30SP Quantum Maestro Gaia Administration Guide*:

- Chapter *Maintenance* > Section *System Backup*.
- Chapter *Maintenance* > Section *Snapshot Management*.

Configuring the Cluster State (g_clusterXL_admin)

Description

Use the `g_clusterXL_admin` command in the Expert mode to change the cluster state manually, to UP or DOWN, for one or more Security Group Members.

Use Case

This command is useful for tests and debug.

Best Practice - Do **not** use this command in production environments, because it can cause performance degradation.

Syntax

```
g_clusterXL_admin -h
```

```
g_clusterXL_admin -b <SGM_IDs> {up | down [-a]} [-r]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-b <SGM_IDs>`	Applies to Security Group Members as specified by `<SGM_IDs>`. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`)
`up`	Changes the cluster state to UP.
`down`	Changes the cluster state to DOWN.
`-a`	Synchronizes accelerated connections to other Security Group Members.
`-r`	Runs this command on all *<SGM_IDs>*, except the local Security Group Members.

Example

```
[Expert@MyChassis-ch01-01:0]# g_clusterXL_admin -b 2_03 up
You are about to perform blade_admin up on blades: 2_03
This action will change members state

Are you sure? (Y - yes, any other key - no) y

Blade_admin up requires auditing
Enter your full name: John Doe
Enter reason for blade_admin up [Maintenance]: test
WARNING: Blade_admin up on blades: 2_03, User: John Doe, Reason: test

Members outputs:
-*- 1 blade: 2_03 -*-
Setting member to normal operation ...
Member current state is ACTIVE
[Expert@MyChassis-ch01-01:0]#
```

Notes:

- When the Security Group Member is in the Administrative **DOWN** state:
  - Gaia gClish commands do not run on this Security Group Member.
  - Traffic is not sent to this Security Group Member.
  - The `asg stat` command shows this Security Group Member as **DOWN (admin)**.
- When the cluster state of the Security Group Member is changed to Administrative **UP**, it automatically synchronizes the configuration from a different Security Group Member that is in the UP state.
- This command generates log entries.

  Run:

  ```
  asg log --file audit
  ```

Configuring a Unique MAC Identifier (asg_unique_mac_utility)

When there are more than one Security Group on a Layer 2 segment, the Unique MAC Identifier must be different for each system. The Unique MAC Identifier is assigned by default during the initial setup. The last octet of the management interface MAC address is the Unique MAC Identifier.

The last octet of the management interface MAC address is set for these data interface types:

- Interfaces with names in the `eth`*`X`*`-`*`YZ`* format
- Bond interfaces
- VSX `wrp` interfaces
- VLAN interfaces

If there is no configured management interface, the Unique MAC Identifier is assigned the default value 254.

You can use the `asg_unique_mac_utility` command in Gaia gClish or the Expert mode to set:

- Data interface Unique MAC Identifier
- Host name

To set the Unique MAC Identifier manually:

Step	Instructions
1	Run this command in Gaia gClish or the Expert mode: `asg_unique_mac_utility`

2	Select an option from the menu and follow the instructions on the screen.
	Example:
	`----------------------------------------------`
	`| Unique MAC Utility                          |`
	`----------------------------------------------`
	`| HOSTNAME [MySecurityGroup]                  |`
	`| Unique MAC [192]                            |`
	`----------------------------------------------`
	
	`Choose one of the following options:`
	`-----------------------------------`
	`1) Set Hostname with Unique MAC wizard`
	`2) Apply Unique MAC from current HOSTNAME`
	`3) Manual set Unique MAC`
	`4) Exit`
	`>`

3	Reboot the system to apply the new Unique MAC Identifier.

Unique MAC Identifier Utility Options

The options for setting the Unique MAC Identifier are:

- **"Set Hostname with Unique MAC wizard"**

  The `_asg` suffix and the setup number, between 1 and 254, are added to the setup name.

  Example:

Setup Name	Suffix	Setup number
`My_SG`	`_asg`	`22`

  This creates a new host name with a Unique MAC Identifier of 22. The setup number replaces the Unique MAC Identifier default value of 254.

New Host Name	Unique MAC Identifier
`My_SG_asg22`	`22`

After reboot, all data interface MAC addresses have the new Unique MAC Identifier value 16.

Example:
`eth1-01 00:1C:7F:XY:ZW:`**16**

Note - The last octet for `eth1-01` (shown in bold) is 16 hex (22 decimal).

- **"Apply Unique MAC from current Hostname"**

  Assign a new Unique MAC Identifier to the interfaces.

  The new Unique MAC Identifier is created from the setup number in the host name.

  The current host name must first comply with the setup name number convention:

  ```
  /asg suffix/setup
  ```

- **"Manual set Unique MAC"**

  Set the Unique MAC Identifier to the default value of `254`.

Working with the ARP Table (asg_arp)

In This Section:

The `asg_arp` Command

Description

The `asg_arp` command in the Expert mode shows the ARP cache for the whole Security Group or for the specified Security Group Member, interface, MAC address, and Host name. You can show summary or verbose information.

Syntax

```
# asg_arp -h
```

```
# asg_arp [-b <SGM_IDs>] [-v] [--verify] [-i <if>] [-m <mac>] [<hostname>]
```

```
# asg_arp --legacy
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-v`	Verbose mode that shows detailed Security Group Member cache information.
`-b <SGM_IDs>`	Applies to Security Group Members as specified by `<SGM_IDs>`. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`)
`-i <if>`	Shows the ARP cache for the specified interface.
`-m <mac>`	Shows the ARP cache for the specified MAC address.
`<hostname>`	Shows the ARP cache for the specified host name.
`--verify`	Runs MAC address verification on both Sites and shows the results.
`--legacy`	Shows the ARP cache for each Security Group Member in the legacy format.

Example Default Output

This example shows the ARP cash in the Default Mode:

```
[Expert@MyChassis-ch01-01:0]# asg_arp
Address              HWaddress           Iface
172.23.19.4          54:7F:EE:6A:D0:BC   eth1-Mgmt2
1_01                 00:1C:7F:01:04:FE   Sync
1_2                  00:1C:7F:02:04:FE   Sync
ssm1                 02:02:03:04:05:40   eth1-CIN
ssm2                 04:02:03:04:05:40   eth2-CIN
[Expert@MyChassis-ch01-01:0]#
```

Example Verbose Output

This example shows the ARP cash in the Verbose Mode:

```
[Expert@MyChassis-ch01-01:0]# asg_arp -v
Address              HWtype   HWaddress           Flags Mask  Iface               SGMs
172.23.19.4          ether    54:7F:EE:6A:D0:BC   C           eth1-Mgmt2          1_01
1_01                 ether    00:1C:7F:01:04:FE   C           Sync                1_02
1_2                  ether    00:1C:7F:02:04:FE   C           Sync                1_01
ssm1                 ether    02:02:03:04:05:40   C           eth1-CIN            1_01,1_02
ssm2                 ether    04:02:03:04:05:40   C           eth2-CIN            1_01
[Expert@MyChassis-ch01-01:0]#
```

Example Output for Verifying MAC Addresses

This example shows the output of the MAC address verification.

```
[Expert@MyChassis-ch01-01:0]# asg_arp --verify
Address              HWtype   HWaddress           Flags Mask  Iface               SGMs
172.23.19.4          ether    54:7F:EE:6A:D0:BC   C           eth1-Mgmt2          1_01
1_01                 ether    00:1C:7F:01:04:FE   C           Sync                1_02
1_2                  ether    00:1C:7F:02:04:FE   C           Sync                1_01
ssm1                 ether    02:02:03:04:05:40   C           eth1-CIN            1_01,1_02
ssm2                 ether    04:02:03:04:05:40   C           eth2-CIN            1_01

MAC address for IP 172.23.19.4 is inconsistent across the SGMs

------------------------------------------------------------------------------
Collecting information from SGMs...
------------------------------------------------------------------------------
Verifying FW1 mac magic value on all SGMs...
Success
------------------------------------------------------------------------------
Verifying IPV4 and IPV6 kernel values...
Success
------------------------------------------------------------------------------
Verifying FW1 mac magic value in /etc/smodb.json...
Success
------------------------------------------------------------------------------
Verifying MAC address on local chassis (Chassis 1)...
Success
------------------------------------------------------------------------------
[Expert@MyChassis-ch01-01:0]#
```

Verifying ARP Entries

Use these commands to confirm that the Unique MAC value has changed.

For the Unique MAC database value, run this command in the Expert mode:

```
# g_allc dbget chassis:private:magic_mac
```

Example:

```
[Expert@MyChassis-ch01-01:0]# g_allc dbget chassis:private:magic_mac
-*- 4 sgms: 1_01 1_02 2_02 2_03 -*-
22
```

For the Unique MAC Kernel value, run this command in Gaia gClish:

```
> fw ctl get int fwha_mac_magic
```

Example:

```
[Global] MyChassis-ch01-01> fw ctl get int fwha_mac_magic
-*- 4 sgms: 1_01 1_02 2_02 2_03 -*-
fwha_mac_magic = 22
[Global] MyChassis-ch01-01>
```

You can display the magic attribute within type `eth`*X*`-`*YZ* interfaces with the `ifconfig` command.

Example:

```
[Expert@MyChassis-ch01-01:0]# ifconfig eth1-01
eth1-01 Link encap:Ethernet HWaddr 00:1C:7F:81:01:16
          inet6 addr: fe80::21c:7fff:fe81:116/64 Scope:Link
          UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
          RX packets:154820 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0 RX bytes:15965660 (15.2 MiB)
          TX bytes:2003398 (1.9 MiB)
[Expert@MyChassis-ch01-01:0]#
```

Example Legacy Output

This example shows ARP cache for each Security Group Member in the Legacy Mode output:

```
[Expert@MyChassis-ch01-01:0]# asg_arp --legacy
1_01:
Address                  HWtype  HWaddress           Flags Mask            Iface
ssm2                     ether   04:02:03:04:05:40   C                     eth2-CIN
ssm1                     ether   02:02:03:04:05:40   C                     eth1-CIN
1_2                      ether   00:1C:7F:02:04:FE   C                     Sync
172.23.19.4              ether   54:7F:EE:6A:D0:BC   C                     eth1-Mgmt2
1_02:
Address                  HWtype  HWaddress           Flags Mask            Iface
1_01                     ether   00:1C:7F:01:04:FE   C                     Sync
ssm1                     ether   02:02:03:04:05:40   C                     eth1-CIN
[Expert@MyChassis-ch01-01:0]#
```

IPv6 Neighbor Discovery

Neighbor discovery works over the ICMPv6 Neighbor Discovery protocol, which is the functional equivalent of the IPv4 ARP protocol. ICMPv6 Neighbor Discovery Protocol must be explicitly permitted in the Access Control Rule Base for all bridged networks. This is different from ARP. ARP traffic is Layer 2 only, therefore it permitted regardless of the Rule Base.

This is an example of an explicit Rule Base that permits ICMPv6 Neighbor Discovery protocol:

Source	Destination	Services and Applications	Action

Network object that represents the Bridged Network	Network object that represents the Bridged Network	`neighbor-advertisement`
		`neighbor-solicitation`
		`router-advertisement`
		`router-solicitation`
		`redirect6`
			`Accept`

Logging and Monitoring

This section provides instructions for monitoring the environment.

CPView

In This Section:

Overview of CPView

Description

CPView is a text based built-in utility on a Check Point computer. CPView Utility shows statistical data that contain both general system information (CPU, Memory, Disk space) and information for different Software Blades (only on Security Gateway).

The CPView continuously updates the data in easy to access views.

On Security Gateway, you can use this statistical data to monitor the performance.

For more information, see sk101878.

Syntax

```
cpview --help
```

Using CPView

Use these keys to navigate the CPView:

Key	Description
Arrow keys	Moves between menus and views. Scrolls in a view.
Home	Returns to the **Overview** view.
Enter	Changes to the **View Mode**. On a menu with sub-menus, the **Enter** key moves you to the lowest level sub-menu.
Esc	Returns to the **Menu Mode**.
Q	Quits CPView.

Use these keys to change CPView interface options:

Key	Description
R	Opens a window where you can change the refresh rate. The default refresh rate is 2 seconds.
W	Changes between wide and normal display modes. In wide mode, CPView fits the screen horizontally.
S	Manually sets the number of rows or columns.
M	Switches on/off the mouse.
P	Pauses and resumes the collection of statistics.

Use these keys to save statistics, show help, and refresh statistics:

Key	Description
C	Saves the current page to a file. The file name format is: `cpview_<cpview process ID>.cap<number of captures>`
H	Shows a tooltip with CPView options.
Space bar	Immediately refreshes the statistics.

CPView User Interface

The CPView user interface has three sections:

Section	Description
Header	This view shows the time the statistics in the third view are collected. It updates when you refresh the statistics.
Navigation	This menu bar is interactive. Move between menus with the arrow keys and mouse. A menu can have sub-menus and they show under the menu bar.
View	This view shows the statistics collected in that view. These statistics update at the refresh rate.

Network Monitoring

You can monitor and log traffic.

Working with Interface Status (asg if)

Description

Use the `asg if` command in Gaia gClish or the Expert mode to:

- Enable and disable the interfaces
- Show information about interfaces:
  - IPv4, IPv6, and MAC address
  - Interface type
  - Link State
  - Speed
  - MTU
  - Duplex

Syntax

`asg if -h`
`asg if -i <interface1>[,<interface2>,...,<interfaceN>] [-v] [{enable | disable}]`
`asg if -ip <IP>`

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Shows information about all interfaces.

Parameter	Description
`-i <interface1> [,<interface2>,...,<interfaceN>]`	Shows information only about the interfaces specified by their names. ■ You can specify one or more interfaces. ■ If you specify more than interface, you must separate their names by a comma without spaces. Example: `asg if -i Sync,eth1-Mgmt1`
`-v`	Shows verbose output. **Note** - This view is not supported for logical interfaces (for example, Bond, VLAN, and `ethX-MgmtY` interfaces).
`enable`	Enables the specified interfaces.
`disable`	Disables the specified interfaces.
`-ip <IP>`	Shows information only about the single interface specified by its IPv4 or IPv6 address.

Verbose Mode (asg if -v)

The Verbose Mode shows extended information, including information retrieved from the switch.

You can use the Verbose Mode for one interface or a comma-separated list of interfaces (without spaces).

This operation can take a few seconds for each interface.

Example output

```
[Expert@MyChassis-ch01-01:0]# asg if -i eth1-01 -v
Collecting information, may take few seconds
+-----------------------------------------------------------------------------------------------+
|Interfaces Data                                                                                |
+-----------------------------------------------------------------------------------------------+
|Interface|IPv4 Address         |Info        |State          |Speed   |MTU       |Duplex  |
|         |MAC  Address         |            |(ch1)/(ch2)    |        |          |        |
|         |IPv6 Address (global)|            |               |        |          |        |
|         |IPv6 Address (local) |            |               |        |          |        |
+---------+---------------------+------------+---------------+--------+----------+--------+
|eth1-01  |-                    |Bond slave  |(up)/(up)      |10G     |1500      |Full    |
|         |00:1c:7f:a1:01:0     |            |master:        |        |          |        |
|         |-                    |            |bond1(up)/(up)|        |          |        |
|         |-                    |            |               |        |          |        |
+---------+---------------------+------------+---------------+--------+----------+--------+
|Comment                                                                                        |
+-----------------------------------------------------------------------------------------------+
|internal interface                                                                             |
+-----------------------------------------------------------------------------------------------+
|Traffic                                                                                        |
+-----------------------------------------------------------------------------------------------+
|media            |In traffic |In pkt(uni/mul/brd)|Out traffic    |Out pkt(uni/mul/brd)   |
+-----------------+-----------+-------------------+---------------+-----------------------+
|FTLF8528P2BNV-EM |28.8Kbps   |0pps/38pps/5pps    |4.1Mbps        |0pps/355pps/0pps       |
+-----------------------------------------------------------------------------------------------+
|Errors (total/pps)                                                                             |
+-----------------------------------------------------------------------------------------------+
|OutDiscards                  |InDiscards         |InErrors       |OutErrors              |
+-----------------------------+-------------------+---------------+-----------------------+
|0/0                          |0/0                |0/0            |0/0                    |
+-----------------------------+-------------------+---------------+-----------------------+
[Expert@MyChassis-ch01-01:0]#
```

Global View of All Interfaces (show interfaces)

Use the `show interfaces` command in Gaia gClish to show the current status of all defined interfaces on the system.

Example

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> show interfaces
+-------------------------------------------------------------------------------------------+
|Interfaces Data                                                                            |
+-------------------------------------------------------------------------------------------+
|Interface  |IPv4 Address      |Info         |State         |Speed    |MTU       |Duplex   |
|           |MAC  Address      |             |(ch1)         |         |          |         |
+-----------+------------------+-------------+--------------+---------+----------+---------+
|bond1      |17.17.17.10       |Bond Master  |(down)        |NA       |NA        |NA       |
|           |00:1c:7f:81:05:fe |             |slaves:       |         |          |         |
|           |                  |             |eth1-05(down)|         |          |         |
|           |                  |             |eth2-05(down)|         |          |         |
+-----------+------------------+-------------+--------------+---------+----------+---------+
|  eth1-05  |-                 |Bond slave   |(down)        |10G      |1500      |Full     |
|           |00:1c:7f:81:05:fe |             |master:       |         |          |         |
|           |                  |             |bond1(down)   |         |          |         |
+-----------+------------------+-------------+--------------+---------+----------+---------+
|  eth2-05  |-                 |Bond slave   |(down)        |10G      |1500      |Full     |
|           |00:1c:7f:81:05:fe |             |master:       |         |          |         |
|           |                  |             |bond1(down)   |         |          |         |
+-----------+------------------+-------------+--------------+---------+----------+---------+
|bond1.201  |18.18.18.10       |Vlan         |(down)        |NA       |NA        |NA       |
|           |00:1c:7f:81:05:fe |             |              |         |          |         |
+-----------+------------------+-------------+--------------+---------+----------+---------+
|br0        |-                 |Bridge Mast  |(up)          |NA       |NA        |NA       |
|           |00:1c:7f:81:07:fe |             |ports:        |         |          |         |
|           |                  |             |eth2-07(down)|         |          |         |
|           |                  |             |eth1-07(down)|         |          |         |
+-----------+------------------+-------------+--------------+---------+----------+---------+
|  eth1-07  |-                 |Bridge port  |(down)        |10G      |1500      |Full     |
|           |00:1c:7f:81:07:fe |             |master:       |         |          |         |
|           |                  |             |br0(up)       |         |          |         |
+-----------+------------------+-------------+--------------+---------+----------+---------+
|  eth2-07  |-                 |Bridge port  |(down)        |10G      |1500      |Full     |
|           |00:1c:7f:82:07:fe |             |master:       |         |          |         |
|           |                  |             |br0(up)       |         |          |         |
+-----------+------------------+-------------+--------------+---------+----------+---------+
|eth1-01    |15.15.15.10       |Ethernet     |(up)          |10G      |1500      |Full     |
|           |00:1c:7f:81:01:fe |             |              |         |          |         |
+-----------+------------------+-------------+--------------+---------+----------+---------+
|eth1-Mgmt4 |172.23.9.67       |Ethernet     |(up)          |10G      |1500      |Full     |
|           |00:d0:c9:ca:c7:fa |             |              |         |          |         |
+-----------+------------------+-------------+--------------+---------+----------+---------+
|eth2-01    |25.25.25.10       |Ethernet     |(up)          |10G      |1500      |Full     |
|           |00:1c:7f:82:01:fe |             |              |         |          |         |
+-----------+------------------+-------------+--------------+---------+----------+---------+
|Sync       |192.0.2.1         |Ethernet     |(up)          |10G      |1500      |Full     |
|           |00:1c:7f:01:04:fe |             |              |         |          |         |
+-----------+------------------+-------------+--------------+---------+----------+---------+
[Global] MyChassis-ch01-01>
```

Notes:

- This sample output shows that this Sync interface is a Bond-Master and if the interfaces are UP or DOWN.
- To add a comment to an interface, run in Gaia gClish:

  ```
  > set interface <Name of Interface> comment "<Comment Text>"
  ```

Showing Bond Interfaces (asg_bond)

In This Section:

Description

The `asg_bond` command in Gaia gClish or the Expert mode shows bond interfaces and runs LACP packet tests:

- MAC address consistency for each Security Group Member
- Slave state consistency for all Security Group Members
- Database consistency for all Security Group Members
- Confirms the LACP aggregator ID between bond and slaves are compatible
- Verifies that the LACP packet between neighbors and key comparison

You can run this command for specified bonds or for all bonds.

Syntax

```
asg_bond {-h | --help}
asg_bond [-v] [ -i <filter>]
```

Parameters

Parameter	Description
`-h | --help`	Shows the built-in help.
`-i <filter>`	Filters the output for the specified bond name or text string. The output shows all bonds that match the bond name, or those names that contain the text string.
`-v`	Runs LACP packet test for the specified interfaces.

Viewing a Global List of All Bonds (asg_bond)

Use the `asg_bond` command in Gaia gClish or the Expert mode without parameters to show all currently defined bonds.

Example

```
[Expert@MyChassis-ch01-01:0]# asg_bond
+------+-----------------------------------------+---------+--------+------------------+
|Name  |Address                  |Mode               |Slaves   |Result  |Comments          |
+------+-------------------------+-------------------+---------+--------+------------------+
|bond1 |(MAC)  00:1c:7f:81:02:fe|LACP 802.3ad       |eth1-02  |OK      |                  |
|      |(IPv4) 13.13.1.10       |Load Sharing       |eth1-03  |        |                  |
|      |                        |                   |eth2-03  |        |                  |
|      |                        |                   |eth2-02  |        |                  |
+------+-------------------------+-------------------+---------+--------+------------------+
|bond3 |(MAC)  00:1c:7f:82:04:fe|XOR                |eth2-04  |OK      |                  |
|      |(IPv4) 23.23.1.10       |Load Sharing       |eth1-04  |        |                  |
+------+-------------------------+-------------------+---------+--------+------------------+
|bond5 |(MAC)  00:1c:7f:81:07:fe|Round-Rubin        |eth1-07  |OK      |                  |
|      |(IPv4) 33.33.1.10       |Load Sharing       |eth2-07  |        |                  |
+------+-------------------------+-------------------+---------+--------+------------------+
|bond7 |(MAC)  00:00:00:00:00:fe|Active-Backup      |         |OK      |- No slaves exist |
|      |                        |High Availability  |         |        |                  |
+------+-------------------------+-------------------+---------+--------+------------------+
[Expert@MyChassis-ch01-01:0]#
```

Viewing a Specific Bond Interface (asg_bond -i)

Use the `asg_bond -i <bond`*X*`>` command in Gaia gClish or the Expert mode to show specific defined bonds.

Example

```
[Expert@MyChassis-ch01-01:0]# asg_bond -i bond5
+--------+-------------------------------+--------------+---------+--------+---------+
|Name    |Address                        |Mode          |Slaves   |Result  |Comments |
+--------+-------------------------------+--------------+---------+--------+---------+
|bond5   |(MAC)  00:1c:7f:81:07:fe       |Round-Rubin   |eth1-07  |OK      |         |
|        |(IPv4) 33.33.1.10              |Load Sharing  |eth2-07  |        |         |
+--------+-------------------------------+--------------+---------+--------+---------+
[Expert@MyChassis-ch01-01:0]#
```

Note - You can also specify a substring that is part of a bond name to show all bonds that contain the substring.

Bond Verification Test (asg_bond -v)

Use the `asg_bond -v` command in Gaia gClish or the Expert mode to run a bond verification test on all currently defined bonds.

Example

This example shows the verification test results for all bonds, including one with an error.

Notes:

- The comments column shows a description of problems detected by the verification tests.
- `Bond7` shows an incomplete definition with no slaves configured.

```
[Expert@MyChassis-ch01-01:0]# asg_bond -v
Listening for LACP packets [.............................]   [ OK ]

+-----+----------------------+----------------+-------+------+-------------------------+
|Name |Address               |Mode            |Slaves |Result|Comments                 |
+-----+----------------------+----------------+-------+------+-------------------------+
|bond1|(MAC) 00:1c:7f:81:02:fe |LACP 802.3ad    |eth1-02|Failed|eth1-02 missing LACP pkts|
|     |(IPv4)13.13.1.10      |Load Sharing    |eth1-03|      |eth1-03 missing LACP pkts|
|     |                      |                |eth2-03|      |eth2-03 missing LACP pkts|
|     |                      |                |eth2-02|      |eth2-02 missing LACP pkts|
+-----+----------------------+----------------+-------+------+-------------------------+
|bond3|(MAC)  00:1c:7f:82:04:fe|XOR             |eth2-04|OK    |                         |
|     |(IPv4) 23.23.1.10     |Load Sharing    |eth1-04|      |                         |
+-----+----------------------+----------------+-------+------+-------------------------+
|bond5|(MAC)  00:1c:7f:81:07:fe|Round-Rubin     |eth1-07|OK    |                         |
|     |(IPv4) 33.33.1.10     |Load Sharing    |eth2-07|      |                         |
+-----+----------------------+----------------+-------+------+-------------------------+
|bond7|(MAC)  00:00:00:00:00:fe|Active-Backup   |       |OK    | - No slaves exist       |
|     |                      |High Availability|       |      |                         |
+-----+----------------------+----------------+-------+------+-------------------------+
[Expert@MyChassis-ch01-01:0]#
```

Showing Traffic Information (asg_ifconfig)

In This Section:

Description

The `asg_ifconfig` command in Gaia gClish or the Expert mode collects traffic statistics from all or a specified range of Security Group Members.

The combined output shows the traffic distribution between Security Group Members and their interfaces (calculated during a certain period).

The `asg_ifconfig` command has these modes:

Mode	Description
Native	This is the default setting. When the `analyze` or `banalyze` option is not specified the command behaves almost the same as the native Linux `ifconfig` command. However, the output shows statistics for all interfaces on all Security Group Members, and for interfaces on the local Security Group Member.
Analyze	Shows accumulated traffic information and traffic distribution between Security Group Members.
Banalyze	Shows accumulated traffic information and traffic distribution between interfaces.

Notes:

- The `analyze` and `banalyze` parameters cannot be used together.
- If you run this command in a Virtual System context, you can only see the output that applies to that context.

Syntax

```
asg_ifconfig -h
```

```
asg_ifconfig [-b <SGM_IDs>] [<interface>] [analyze | banalyze] [-d <delay>] [-a] [-v]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-b <SGM_IDs>`	Applies to Security Group Members as specified by `<SGM_IDs>`. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`)
`<interface>`	The name of the interface.
`analyze`	Shows accumulated traffic information. Use the `-a`, `-v`, and `-d <delay>` parameters to show traffic distribution between interfaces.

`banalyze`	Shows accumulated traffic information.
	Use the `-a`, `-v`, and `-d <delay>` parameters to show traffic distribution between interfaces.
	You can use these parameters to sort the traffic distribution table:
	■ `-rp` X packets
	■ `-rb` X bytes
	■ `-rd` X dropped packets
	■ `-tp` X packets
	■ `-tb` X bytes
	■ `-td` X dropped packet
	For example, if you sort with the `-rb` option, the higher values appear at the top of the `RX bytes` column in the traffic distribution table:
	`SGM ID  RX packets  RX bytes  RX dropped`
	`1_03  70%`
	`1_02  20%`
	`1_01  10%`
	By default, the traffic distribution table is not sorted.

`-d <delay>`	Delay, in seconds, between data samples. Default = 5.

Parameter	Description
`-a`	Shows total traffic volume. By default (without `-a`), the average traffic volume per second shows.
`-v`	Verbose mode - shows traffic distribution between interfaces.

Native Usage

This example shows the total traffic sent and received by `eth2-01` for all Security Group Members on Site 1 (Active Site).

By default, the average traffic volume per second shows.

Example

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg_ifconfig -b chassis1 eth2-01

as1_02:
eth2-01     Link encap:Ethernet  HWaddr 00:1C:7F:81:01:EA
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX packets:94 errors:0 dropped:0 overruns:0 frame:0
            TX packets:63447 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:5305 (5.1 KiB)  TX bytes:5688078 (5.4 MiB)

1_03:
eth2-01     Link encap:Ethernet  HWaddr 00:1C:7F:81:01:EA
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX packets:137 errors:0 dropped:0 overruns:0 frame:0
            TX packets:26336 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:7591 (7.4 KiB)  TX bytes:2355386 (2.2 MiB)

1_04:
eth2-01     Link encap:Ethernet  HWaddr 00:1C:7F:81:01:EA
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX packets:124 errors:0 dropped:0 overruns:0 frame:0
            TX packets:3098 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:6897 (6.7 KiB)  TX bytes:378990 (370.1 KiB)

1_05:
eth2-01     Link encap:Ethernet  HWaddr 00:1C:7F:81:01:EA
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500 Metric:1
            RX packets:79 errors:0 dropped:0 overruns:0 frame:0
            TX packets:26370 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:4507 (4.4 KiB)  TX bytes:2216546 (2.1 MiB)
[Global] MyChassis-ch01-01>
```

Using the Analyze Option

This example shows accumulated traffic volume statistics for `eth2-Sync` for each Security Group Member and the total for all Security Group Members.

The traffic distribution for each Security Group Member also shows.

The `-a` option shows the total traffic volume instead of the average volume per second.

Example

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg_ifconfig eth2-Sync analyze -v -a
Command is executed on SGMs: chassis_active

1_01:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:01:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:225018 bytes:36970520 (37.0 MiB)  dropped:0
            TX: packets:3522445 bytes:1381032583 (1.4 GiB)  dropped:0

1_02:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:02:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:221395 bytes:35947248 (35.9 MiB)  dropped:0
            TX: packets:4674143 bytes:1850315554 (1.9 GiB)  dropped:0

1_03:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:03:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:10 bytes:644 (644.0 b)  dropped:0
            TX: packets:67826313 bytes:7345458105 (7.3 GiB)  dropped:0

1_04:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:04:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:13 bytes:860 (860.0 b)  dropped:0
            TX: packets:68489217 bytes:7487476060 (7.5 GiB)  dropped:0

1_05:
eth2-Sync   Link encap:Ethernet  HWaddr 00:1C:7F:05:04:FE
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:203386 bytes:19214238 (19.2 MiB)  dropped:0
            TX: packets:7164109 bytes:2740761091 (2.7 GiB)  dropped:0

=*= Accumulative =*=
eth2-Sync   Link encap:Ethernet
            UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
            RX: packets:649822 bytes:92133510 (92.1 MiB)  dropped:0
            TX: packets:151676227 bytes:20805043393 (20.8 GiB)  dropped:0

=*= Traffic Distribution =*=

-------------------------------------------------------------------------------
     SGM ID RX packets   RX bytes RX dropped TX packets   TX bytes TX dropped
-------------------------------------------------------------------------------
       1_01      34.6%      40.1%       0.0%       2.3%       6.6%       0.0%
       1_02      34.1%      39.0%       0.0%       3.1%       8.9%       0.0%
       1_03       0.0%       0.0%       0.0%      44.7%      35.3%       0.0%
       1_04       0.0%       0.0%       0.0%      45.2%      36.0%       0.0%
       1_05      31.3%      20.9%       0.0%       4.7%      13.2%       0.0%
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01>
```

Showing Multicast Traffic Information

In This Section:

Use these commands to show information about multicast traffic.

Showing Multicast Routing (asg_mroute)

Description

The `asg_mroute` command in Gaia gClish or the Expert mode shows this multicast routing information in a tabular format:

- **Source** - Source IP address
- **Dest** - Destination address
- **Iif** - Source interface
- **Oif** - Outbound interface

You can filter the output for specified interfaces and Security Group Members.

Syntax

```
asg_mroute -h
```

```
asg_mroute [-d <dest_route>] [-s <src_route>] [-i <src_if>][-b <SGM_IDs>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Shows all routes, interfaces and Security Group Members.
`-d <dest_route>`	Destination multicast group IP address.
`-s <src_route>`	Source IP address.
`-i <src_if>`	Source interface name.

Parameter	Description
`-b <SGM_IDs>`	Applies to the Security Group Members specified by <*SGM_IDs*>. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`)

Below are some examples:

Example 1 - Shows all multicast routes for all interfaces and Security Group Members

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg_mroute
+-------------------------------------------------------------------------------------+
|Multicast Routing (All SGMs)                                                         |
+-------------------------------------------------------------------------------------+
|Source                    |Dest                      |Iif            |Oif            |
+--------------------------+--------------------------+---------------+---------------+
|12.12.12.1                |225.0.90.90               |eth1-01        |eth1-02        |
+--------------------------+--------------------------+---------------+---------------+
|22.22.22.1                |225.0.90.90               |eth1-02        |eth1-01        |
+--------------------------+--------------------------+---------------+---------------+
|22.22.22.1                |225.0.90.91               |eth1-02        |eth1-01        |
+--------------------------+--------------------------+---------------+---------------+
[Global] MyChassis-ch01-01>
```

Example 2 - Shows only specific IP address, interfaces, destination IP address, or Security Group Members

```
[Expert@MyChassis-ch01-01:0]# asg_mroute -s 22.22.22.1 -i eth1-02 -d 225.0.90.91
+-------------------------------------------------------------------------------------+
|Multicast Routing (All SGMs)                                                         |
+-------------------------------------------------------------------------------------+
|Source                    |Dest                      |Iif            |Oif            |
+--------------------------+--------------------------+---------------+---------------+
|22.22.22.1                |225.0.90.91               |eth1-02        |eth2-01        |
+--------------------------+--------------------------+---------------+---------------+
[Expert@MyChassis-ch01-01:0]#
```

Showing PIM Information (asg_pim)

Description

The `asg_pim` command in Gaia gClish or the Expert mode shows this PIM information in a tabular format:

- **Source** - Source IP address
- **Dest** - Destination IP address
- **Mode** - Both Dense Mode and Sparse Mode are supported
- **Flags** - Local source and MFC state indicators
- **In. intf** - Source interface
- **RPF** - Reverse Path Forwarding indicator
- **Out int** - Outbound interface
- **State** - Outbound interface state

You can filter the output for specified interfaces and Security Group Members.

Syntax

```
asg_pim -h
asg_pim [-b <SGM_IDs>] [-i <if>]
asg_pim neighbors [-n <neighbor>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Shows all routes, interfaces and Security Group Members.

Parameter	Description
`-b <SGM_IDs>`	Applies to Security Group Members specified by <*SGM_IDs*>. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`)
`-i <if>`	Shows only the specified source interface.
`neighbors`	Runs verification tests to make sure that PIM `neighbors` are the same on all Security Group Members and shows this information: ■ **Verification** - Results of verification test ■ **Neighbor** - PIM neighbor ■ **Interface** - Interface name ■ **Holdtime** - Time in seconds to hold a connection open during peer negotiation ■ **Expires** - Minimum and Maximum expiration values for all Security Group Members
`-n <neighbor>`	Shows only the specified PIM `neighbor`.

Below are some examples:

Example 1 - Shows PIM information and multicast routes for all interfaces and Security Group Members

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg_pim
+-------------------------------------------------------------------------------------+
|PIM (All SGMs)                                                                       |
+-------------------------------------------------------------------------------------+
|source     |dest        |Mode      |Flags|In. intf |RPF       |Out. intf   |State     |
+-----------+------------+----------+-----+---------+----------+------------+----------+
|12.12.12.1 |225.0.90.90 |Dense-Mode|L|M  |eth1-01  |none      |            |          |
+-----------+------------+----------+-----+---------+----------+------------+----------+
|22.22.22.1 |225.0.90.90 |Dense-Mode|L|M  |eth1-02  |none      |eth1-01     |Forwarding|
+-----------+------------+----------+-----+---------+----------+------------+----------+
|22.22.22.1 |225.0.90.91 |Dense-Mode|L|M  |eth1-02  |none      |eth1-01     |Forwarding|
|           |            |          |     |         |          |eth2-01     |Forwarding|
+-----------+------------+----------+-----+---------+----------+------------+----------+
Flags: L - Local source, M - MFC State
[Global] MyChassis-ch01-01>
```

Example 2 - Shows PIM Information for the specific interface on all Security Group Members

```
[Expert@MyChassis-ch01-01:0]# asg_pim -i eth1-02 -b all
+-------------------------------------------------------------------------------------+
|PIM (All SGMs)                                                                       |
+-------------------------------------------------------------------------------------+
|SGM 1_01                                                                             |
+-------------------------------------------------------------------------------------+
|source     |dest        |Mode      |Flags|In. intf |RPF       |Out. intf   |State     |
+-----------+------------+----------+-----+---------+----------+------------+----------+
|22.22.22.1 |225.0.90.90 |Dense-Mode|L|M  |eth1-02  |none      |eth1-01     |Forwarding|
+-----------+------------+----------+-----+---------+----------+------------+----------+
|22.22.22.1 |225.0.90.91 |Dense-Mode|L    |eth1-02  |none      |eth1-01     |Forwarding|
|           |            |          |     |         |          |eth2-01     |Forwarding|
+-----------+------------+----------+-----+---------+----------+------------+----------+
|SGM 1_02                                                                             |
+-------------------------------------------------------------------------------------+
|source     |dest        |Mode      |Flags|In. intf |RPF       |Out. intf   |State     |
+-----------+------------+----------+-----+---------+----------+------------+----------+
|22.22.22.1 |225.0.90.90 |Dense-Mode|L|M  |eth1-02  |none      |eth1-01     |Forwarding|
+-----------+------------+----------+-----+---------+----------+------------+----------+
|22.22.22.1 |225.0.90.91 |Dense-Mode|L|M  |eth1-02  |none      |eth1-01     |Forwarding|
|           |            |          |     |         |          |eth2-01     |Forwarding|
+-----------+------------+----------+-----+---------+----------+------------+----------+
[Expert@MyChassis-ch01-01:0]#
```

Example 3 - Shows PIM neighbors

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg_pim neighbors
+-------------------------------------------------------------------------------------+
|PIM Neighbors (All SGMs)                                                             |
+-------------------------------------------------------------------------------------+
|Verification:                                                                        |
|Neighbors Verification: Passed - Neighbors are identical on all blades               |
+--------------------+--------------------+--------------------+----------------------+
|Neighbor            |Interface           |Holdtime            |Expires(min-max)      |
+--------------------+--------------------+--------------------+----------------------+
|11.1.1.1            |bond1               |105                 |11:36:45-11:37:59     |
+--------------------+--------------------+--------------------+----------------------+
[Global] MyChassis-ch01-01>
```

Showing IGMP Information (asg_igmp)

Description

Use the `asg_igmp` command in Gaia gClish or the Expert mode to show IGMP information in a tabular format.

You can filter the output for specified interfaces and Security Group Members. If no Security Group Member is specified, the command runs a verification to make sure that IGMP data is the same on all Security Group Members:

- Group verification - Confirms the groups exist on all Security Group Members. If a group is missing on some Security Group Members, a message shows which group is missing on which blade.
- Global properties - Confirms the flags, address and other information are the same on all Security Group Members.
- Interfaces - Confirms that all blades have the same interfaces and that they are in the same state (UP or DOWN). If inconsistencies are detected, a warning message shows.

Syntax

```
asg_igmp -h
```

```
asg_igmp [-i <interface>] [-b <SGM_IDs>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-i <interface>`	Source interface name.
`-b <SGM_IDs>`	Applies to Security Group Members as specified by `<SGM_IDs>`. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`)

Below are some examples:

Example 1 - Shows IGMP information and multicast routes for all interfaces and Security Group Members

Note - In this example, the verification detected an interface inconsistency.

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg_igmp

Collecting IGMP information, may take few seconds...
+-------------------------------------------------------------------------------------------+
|IGMP (All SGMs)                                                                            |
+-------------------------------------------------------------------------------------------+
|Interface: eth1-01
+-------------------------------------------------------------------------------------------+
|Verification:                                                                              |
|Group Verification: Passed - Information is identical on all blades                        |
|Global Properties Verification: Passed - Information is identical on all blades            |
+-------------------------------------------------------------------------------------------+
|Group               |Age       |Expire                                                     |
+--------------------+----------+-----------------------------------------------------------+
|225.0.90.91         |2m        |4m                                                         |
+--------------------+----------+-----------------------------------------------------------+
|Flags     |IGMP Ver |Query Interval |Query Response Interval  |protocol |Advertise Address|
+----------+---------+---------------+-------------------------+---------+-----------------+
|Querier   |2        |125            |10                       |PIM      |12.12.12.10      |
+-------------------------------------------------------------------------------------------+

+-------------------------------------------------------------------------------------------+
|Interface: eth1-02                                                                         |
+-------------------------------------------------------------------------------------------+
|Verification:                                                                              |
|Group Verification: Failed - Found inconsistency between blades                            |
| -Group 225.0.90.92: missing in blades 1_02                                                |
|Global Properties Verification: Passed - Information is identical on all blades            |
+-------------------------------------------------------------------------------------------+
|Group               |Age       |Expire                                                     |
+--------------------+----------+-----------------------------------------------------------+
|225.0.90.92         |2m        |3m                                                         |
+--------------------+----------+-----------------------------------------------------------+
|Flags     |IGMP Ver |Query Interval |Query Response Interval  |protocol |Advertise Address|
+----------+---------+---------------+-------------------------+---------+-----------------+
|Querier   |2        |125            |10                       |PIM      |22.22.22.10      |
+-------------------------------------------------------------------------------------------+

+-------------------------------------------------------------------------------------------+
|Interface: eth2-01                                                                         |
+-------------------------------------------------------------------------------------------+
|Verification:                                                                              |
|Group Verification: Passed - Information is identical on all blades                        |
|Global Properties Verification: Passed - Information is identical on all blades            |
+-------------------------------------------------------------------------------------------+
|Group               |Age       |Expire                                                     |
+--------------------+----------+-----------------------------------------------------------+
|225.0.90.90         |2m        |3m                                                         |
+--------------------+----------+-----------------------------------------------------------+
|Flags     |IGMP Ver |Query Interval |Query Response Interval  |protocol |Advertise Address|
+----------+---------+---------------+-------------------------+---------+-----------------+
|Querier   |2        |125            |10                       |PIM      |2.2.2.10         |
+-------------------------------------------------------------------------------------------

NOTE: Inconsistency found in interfaces configuration between blades
Inconsistent interfaces: eth1-02
[Global] MyChassis-ch01-01>
```

Example 2 - Shows IGMP Information for a specified interface

```
[Expert@MyChassis-ch01-01:0]# asg_igmp -i bond1.3
Collecting IGMP information, may take few seconds...
+-------------------------------------------------------------------------------------------------+
|IGMP (All SGMs)                                                                                  |
+-------------------------------------------------------------------------------------------------+
|Interface: bond1.3                                                                               |
+-------------------------------------------------------------------------------------------------+
|Verification                                                                                     |
|Group Verification: Passed - Information is identical on all blades                              |
|Global Properties Verification: Passed - Information is identical on all blades                  |
+-------------------------------------------------------------------------------------------------+
|Group               |Age       |Expire                                                           |
--------------------+----------+-----------------------------------------------------------------+
|225.0.90.90         |46m       |3m                                                               |
+--------------------+----------+-----------------------------------------------------------------+
|Flags     |IGMP Ver |Query Interval |Query Response Interval  |protocol |Advertise Address|
+----------+---------+---------------+-------------------------+---------+-----------------+
|Querier   |2        |125            |10                       |PIM      |12.12.12.11      |
+-------------------------------------------------------------------------------------------------+
[Expert@MyChassis-ch01-01:0]#
```

Monitoring VPN Tunnels

Because VPN tunnels synchronize between all Security Group Members, use traditional tools to monitor tunnels.

SmartConsole

You must not activate the **Monitoring** Software Blade in the Security Group object. But, you can still use the tunnels information in SmartConsole to see VPN tunnel status and details.

SNMP

- You can use the **tunnelTable** sub-tree in Check Point MIB .1.3.6.1.4.1.2620.500.9002 to see VPN status with SNMP.
- For VSX environments, search for the *SNMP Monitoring* section in the *R80.30SP Quantum Maestro VSX Administration Guide* for VSX-related SNMP information.

CLI Tools

Use these commands:

- To see VPN statistics for each Security Group Member, in the Expert mode run:

  ```
  # cpstat -f all vpn
  ```

- To monitor VPN tunnels for each Security Group Member, in the Expert mode run:

  ```
  # vpn tu
  ```

  VPN tunnels are synchronized to all Security Group Members, therefore you can run this command from the scope of one Security Group Member.

- To monitor VPN tunnels in the non-interactive mode, in Gaia gClish run:

  ```
  > vpn shell t
  ```

Note - In a VSX environment, you must run these commands from the context of the applicable Virtual System.

Traceroute (asg_tracert)

Description

Use the `asg_tracert` command in Gaia gClish or the Expert mode to show correct `tracert` results on the Security Group.

The native `tracert` cannot handle `tracert` pings correctly because of the stickiness mechanism used in the Security Group Firewall.

The `asg_tracert` command supports all native options and parameters of the `tracert` command.

Syntax

```
asg_tracert <ip> [<tracert_options>]
```

Parameters

Parameter	Description
<ip>	IP address
<tracert_options>	Native `tracert`command options

Example

```
[Expert@MyChassis-ch01-01:0]#asg_tracert 100.100.100.99
  traceroute to 100.100.100.99 (100.100.100.99), 30 hops max, 40 byte packets
   1   (20.20.20.20)  0.722 ms  0.286 ms  0.231 ms
   2   (100.100.100.99)  1.441 ms  0.428 ms  0.395 ms
[Expert@MyChassis-ch01-01:0]#
```

Multi-blade Traffic Capture (tcpdump -mcap, tcpdump -view)

Description

Use this command in Gaia gClish to see TCP/IP and other packets sent and received by all Security Group Members in the Security Group.

This release includes these Security Group-specific enhancements to the standard `tcpdump` utility:

- `tcpdump -mcap` - Gets packets from specified Security Group Members and saves them to a capture file.
- `tcpdump -view` - Shows packets in the specified capture file, including the Security Group Member ID from the packet captured packet.

Note - Use the "`g_tcpdump`" command in the Expert mode.

Syntax

```
> tcpdump [-b <SGM_IDs>] -mcap -w <capture_path> [<tcpdump_ops>]
> tcpdump -view -r <capture_path> [<tcpdump_ops>]
```

Note - To stop the capture and save the data to the capture file, press **CTRL+C** at the prompt.

Parameters

Parameter	Description
`-b <SGM_IDs>`	Applies to Security Group Members as specified by `<SGM_IDs>`. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`)

Parameter	Description
`-w <capture_path>`	Saves full file path. In addition to the merged capture file, for each Security Group Member capture files are created in the same directory, suffixed by their Security Group Member ID.
`-r <capture_path>`	Reads the specified traffic capture file. Regular `tcpdump` output, prefixed by Security Group Member ID of the processing Security Group Member ID.
<tcpdump_ops>	Standard *tcpdump* parameters (see the `tcpdump` manual page).

Below are some examples:

Example 1 - Capture all Security Group Members

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01 > tcpdump -mcap -w /tmp/capture
Capturing packets...
Write "stop" and press enter to stop the packets capture process.
1_01:
tcpdump: listening on eth1-Mgmt4, link-type EN10MB (Ethernet), capture size 96 bytes
stop
Received user request to stop the packets capture process.

Copying captured packets from all SGMs...
Merging captured packets from SGMs to /tmp/capture...
Done.
[Global] MyChassis-ch01-01>
```

Example 2 - Capture packets from specified Security Group Members and interfaces

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01 > tcpdump -b 1_1,1_3,2_1 -mcap -w /tmp/capture -nnni eth1-Mgmt4
... ...
[Global] MyChassis-ch01-01 >
```

Example 3 - Show captured packets from file

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> tcpdump -view -r /tmp/capture
Reading from file /tmp/capture, link-type EN10MB (Ethernet)
 [1_3] 14:11:57.971587 IP 0.0.0.0.cp-cluster > 172.16.6.0.cp-cluster: UDP, length 45
 [2_3] 14:12:07.625171 IP 0.0.0.0.cp-cluster > 172.16.6.0.cp-cluster: UDP, length 45
 [2_3] 14:12:09.974195 IP 0.0.0.0.cp-cluster > 172.16.6.0.cp-cluster: UDP, length 37
 [2_1] 14:12:09.989745 IP 0.0.0.0.cp-cluster > 172.16.6.0.cp-cluster: UDP, length 45
 [2_3] 14:12:10.022995 IP 0.0.0.0.cp-cluster > 172.23.9.0.cp-cluster: UDP, length 32
... ...
[Global] MyChassis-ch01-01>
```

Monitoring Management Interfaces Link State

By default, Security Group monitors the link state only on data ports `(ethX-YZ)`. The Management Monitor feature lets SNMP monitor management ports on the Quantum Maestro Orchestrators. The link state is sent to all Security Group Members.

The Management Monitor feature is disabled by default.

To enable this feature, run the "`set chassis high-availability mgmt-monitoring on`" command in Gaia gClish of the Security Group.

When the Management Monitor feature is enabled:

- The monitored management ports are included in the Security Group grade mechanism, according to predefined factors (default is 11).
- The output of the "`asg stat -v`" command shows the Management ports.

  See the "`Chassis Parameters > Ports > Mgmt`" line in the output example below.
- The "`show interfaces`" command shows the link state of management interfaces based on this feature mechanism.

Example

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> show chassis high-availability mgmt-monitoring
off
[Global] MyChassis-ch01-01> set chassis high-availability mgmt-monitoring on
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> show chassis high-availability mgmt-monitoring
on
[Global] MyChassis-ch01-01> asg stat -v
-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Up time                     | 13:10:04 hours                                |
| SGMs                        | 2 / 2                                         |
| Version                     | R80.30SP (Build Number XXX)                   |
-------------------------------------------------------------------------------
| SGM ID                              Chassis 1                               |
|                                     ACTIVE                                  |
-------------------------------------------------------------------------------
|  1                                    ACTIVE                                |
|  2                                    ACTIVE                                |
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit        |                       Chassis 1                       | Weight |
-------------------------------------------------------------------------------
| SGMs        |                         2 / 2                         |   6    |
| Ports       |                                                       |        |
|   Standard  |                         8 / 8                         |  11    |
|   Bond      |                         0 / 0                         |  11    |
|   Mgmt      |                         1 / 1                         |  11    |
|   Other     |                         0 / 0                         |   6    |
| Sensors     |                                                       |        |
|   SSMs      |                         2 / 2                         |  11    |
|             |                                                       |        |
| Grade       |                        73 / 73                        |   -    |
-------------------------------------------------------------------------------
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01>
[Global] MyChassis-ch01-01> show interfaces
+-------------------------------------------------------------------------------------------------------
--------------+
|Interfaces Data
             |
+-------------------------------------------------------------------------------------------------------
--------------+
|Interface      |IPv4 Address                          |Info        |Link State
|Speed|MTU  |Duplex|
|               |MAC  Address                          |            |(ch1)               |
|     |      |
+---------------+--------------------------------------+------------+--------------------+----
-+-----+------+
|eth1-Mgmt1     |172.23.19.53/24                       |Ethernet    |(Up)                |10G
|1500 |Full  |
|               |00:1c:7f:62:91:94                     |            |                    |
|     |      |
+---------------+--------------------------------------+------------+--------------------+----
-+-----+------+
|Sync           |192.0.2.1/24                          |Ethernet    |(up)                |10G
|1500 |Full  |
|               |00:1c:7f:01:04:fe                     |            |                    |
|     |      |
+---------------+--------------------------------------+------------+--------------------+----
-+-----+------+
... ... output was truncated for brevity ... ...
```

Performance Monitoring and Control

This section provides commands to monitor and control the performance of Security Group Members.

Monitoring Performance (asg perf)

Description

Use the `asg perf` command in Gaia gClish or the Expert mode to monitor continuously the key performance indicators and load statistics.

There are different commands for IPv4 and IPv6. You can show the performance statistics for IPv4 traffic, IPv6 traffic or for all traffic.

When you run this command, the statistics shows on the screen.

The output automatically updates after a predefined interval (default = 10 seconds).

To stop the command and return to the command line, press `e`.

Syntax

```
asg perf -h
```

```
asg perf [-b <SGM_IDs>] [-vs <VS_IDs>] [-k] [-v] [-vv] [-p] [-4 | -6] [-c]
```

```
asg perf [-b <SGM_IDs>] [-vs <VS_IDs>] [-k] [-e] [--delay <seconds>]
```

```
asg perf [-b <SGM_IDs>] [-vs <VS_IDs>] [-v] [-vv [ mem [{fwk | cpd | fwd | all_daemons}] | cpu [1m | 1h | 24h]]]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.

Parameter	Description
`-b <SGM_IDs>`	Applies to Security Group Members as specified by `<SGM_IDs>`. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`)
`-vs <VS_IDs>`	Shows the status of Virtual Systems. *<VS_IDs>* can be: ■ No `<VS_IDs>` specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems Note - This parameter is only applicable in a VSX environment.
`-v`	Shows statistics for each Security Group Member.
`-vv`	Shows statistics for each Virtual System. Note - This parameter is only relevant in a VSX environment.
`mem`	Shows memory usage for each daemon. Use this with `-vv`. Possible values: ■ `fwk` (Default) ■ `fwd` ■ `cpd` ■ `all_daemons`
`cpu`	Shows CPU usage for a specified period of time. Use this with `-vv`. Possible values are: ■ `1m` (default) - The last 60 seconds ■ `1h` - The last hour ■ `24h` - The last 24 hours

Parameter	Description
`-p`	Show detailed statistics and traffic distribution between these paths on the Active Site: ■ Acceleration path (SecureXL) ■ Medium path (PXL) ■ Slow path (Firewall)
`-4 | -6`	■ `-4` - Shows IPv4 information only. ■ `-6` - Shows IPv6 information only. If no value is specified, the combined performance information shows for both IPv4 and IPv6.
`-c`	Shows percentages instead of absolute values.
`-k`	Shows peak (maximum) system performance values.
`-e`	Resets peak values and deletes all peaks files and system history files.
`--delay <`*`seconds`*`>`	Temporarily changes the update interval for the current `asg perf` session. Enter a delay value in seconds.Default delays is 10 seconds.

Notes:

- The `-b <`*`SGM_IDs`*`>` and `-vs <`*`VS_IDs`*`>` parameters must be at the start of the command.

  If both parameters are used, `-b <`*`SGM_IDs`*`>` must be first.

- If your Security Group is not configured in VSX mode, the VSX related commands are not available.

  They do not show when you run the `asg perf -h` command.

Below are some examples:

Example 1 - Summary without Parameters (asg perf)

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg perf
Thu May 21 08:17:24 IDT 2015
Aggregated statistics (IPv4 Only) of SGMs: chassis_active VSs: 0
+-------------------------------------------------------------+
|Performance Summary                                          |
+---------------------------------------------+---------------+
|Name                                         |Value          |
+---------------------------------------------+---------------+
|Throughput                                   |751.6 K        |
|Packet rate                                  |733            |
|Connection rate                              |3              |
|Concurrent connections                       |142            |
|Load average                                 |2%             |
|Acceleration load (avg/min/max)              |1%/0%/4%       |
|Instances load (avg/min/max)                 |2%/0%/8%       |
|Memory usage                                 |10%            |
+---------------------------------------------+---------------+
 * Instances / Acceleration Cores: 8 / 4
 * Activated SWB: FW,IPS
[Global] MyChassis-ch01-01>
```

Notes:

- By default, absolute values are shown.
- Unless otherwise specified, the combined statistics for IPv4 and IPv6 are shown.
- When no Security Group Members are specified, performance statistics are shown for the Active Security Group Member only.

Example 2 - Performance Summary (asg perf -v)

The `-v` parameter adds a performance summary for each Security Group Member.

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg perf -vs all -v -vv cpu 24h
Tue Oct 22 07:23:37 IST 2013
Aggregated statistics (IPv4 and IPv6) of SGMs: chassis_active Virtual Systems: 0
+-------------------------------------------------------------------------+
|Performance Summary                                                      |
+-------------------------------------------+-------------+-------------+
|Name                                       |Value        |IPv4%        |
+-------------------------------------------+-------------+-------------+
|Throughput                                 |10.2 K       |100%         |
|Packet rate                                |11           |100%         |
|Connection rate                            |0            |N/A          |
|Concurrent connections                     |22           |100%         |
|Load average                               |7%           |             |
|Acceleration load (avg/min/max)            |6%/6%/6%     |             |
|Instances load (avg/min/max)               |5%/4%/9%     |             |
|Memory usage                               |55%          |             |
+-------------------------------------------+-------------+-------------+

+-------------------------------------------------------------------------+
|Per SGM Distribution Summary                                             |
+-----+-----------+--------+--------+--------+----------+----------+------+
|SGM  |Throughput |Packet  |Conn.   |Concu.  |Accel.    |Instances |Mem.  |
|ID   |           |Rate    |Rate    |Conn    |Cores%    |Cores%    |Usage%|
+-----+-----------+--------+--------+--------+----------+----------+------+
|1_01 |10.2 K     |11      |0       |22      |6/6/6     |5/4/9     |55%   |
+-----+-----------+--------+--------+--------+----------+----------+------+
|Total|10.2 K     |11      |0       |22      |6/6/6     |5/4/9     |55%   |
+-----+-----------+--------+--------+--------+----------+----------+------+

+-----------------------------------+
|Per VS CPU Usage Summary           |
+-----+---------+---------+---------+
|VS ID|Avg. Cpu%|Min. Cpu%|Max. Cpu%|
|     |         |(SGM id) |(SGM id) |
+-----+---------+---------+---------+
| 0   |2        |1  (1_02)|2  (1_01)|
| 1   |0        |0  (1_01)|0  (1_04)|
+-----+---------+---------+---------+
* CPU stats is aggregated over the last 24hrs
[Global] MyChassis-ch01-01>
```

Make sure that resource control monitoring is enabled on all Security Group Members.

To enable resource control monitoring, in the Expert mode run:

```
# g_fw vsx resctrl monitor enable
```

By default, absolute values are shown.

Notes:

- Average, minimum and maximum values are calculated across all active Security Group Members.
- The Security Group Member ID with the minimum and maximum value shows in brackets for each Security Group Member.

- Unless otherwise specified, the combined statistics for both IPv4 and IPv6 are shown.
- When no Security Group Members are specified, performance statistics are shown for the active Security Group Member only.

Example 3 - Peak Values (asg perf -p)

This example shows peak values for one Virtual System.

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg perf -vs 0-1 -p
Aggregated statistics (IPv4 and IPv6) of SGMs: all Virtual Systems: 0-1
+-------------------------------------------------------------------------+
|Performance Summary                                                      |
+-----------------------------------------+---------------+-------------+
|Name                                     |Value          |IPv4%        |
+-----------------------------------------+---------------+-------------+
|Throughput                               |1.7 K          |100%         |
|Packet rate                              |2              |100%         |
|Connection rate                          |0              |N/A          |
|Concurrent connections                   |20             |100%         |
|Load average                             |6%             |             |
|Acceleration load (avg/min/max)          |5%/5%/5%       |             |
|Instances load (avg/min/max)             |5%/3%/10%      |             |
|Memory usage                             |57%            |             |
+-----------------------------------------+---------------+-------------+
=+-----------------------------------------------------------------------+
|Per Path Distribution Summary                                            |
+------------------+------------+--------------+--------------+-----------+
|                  |Acceleration|Medium        |Firewall      |Dropped    |
+------------------+------------+--------------+--------------+-----------+
|Throughput        |0           |0             |1.7 K         |0          |
|Packet rate       |0           |0             |2             |0          |
|Connection rate   |0           |0             |0             |           |
|Concurrent conn.  |10          |0             |10            |           |
+------------------+------------+--------------+--------------+-----------+
[Global] MyChassis-ch01-01>
```

Example 4 - Per Path Statistics (asg perf -p -v)

This example shows detailed performance information for each Security Group Member and traffic distribution between different paths. It also shows VPN throughput and connections.

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg perf -p -v
Tue Oct 22 07:31:31 IST 2013
Aggregated statistics (IPv4 and IPv6) of SGMs: chassis_active Virtual Systems: 0
+-------------------------------------------------------------+
|Performance Summary                                          |
+-------------------------------------+-----------------------+
|Name                                 |Value                  |
+-------------------------------------+-----------------------+
|Throughput                           |3.3 G                  |
|Packet rate                          |6.2 M                  |
|Connection rate                      |0                      |
|Concurrent connections               |3.4 K                  |
|Load average                         |54%                    |
|Acceleration load (avg/min/max)      |58%/48%/68%            |
|Instances load (avg/min/max)         |3%/1%/5%               |
|Memory usage                         |18%                    |
+-------------------------------------+-----------------------+

+-------------------------------------------------------------------------------------------+
|Per SGM Distribution Summary                                                               |
+-------+------------+------------+-----+-----------+-------------+--------------+------+
|SGM ID |Throughput  |Packet rate |Conn.|Concurrent |Core usage   |Core Instances|Memory|
|       |            |            |Rate |Connections|avg/min/max %|avg/min/max % |Usage |
+-------+------------+------------+-----+-----------+-------------+--------------+------+
|1_01   |644.3 M     |1.2 M       |0    |520        |52/44/62     |6/3/10        |18%   |
|1_02   |526.7 M     |997.1 K     |0    |512        |61/51/68     |2/0/5         |18%   |
|1_03   |526.6 M     |997.0 K     |0    |512        |62/53/73     |2/1/3         |18%   |
|1_04   |526.7 M     |997.0 K     |0    |804        |54/48/60     |2/1/3         |18%   |
|1_05   |526.7 M     |997.1 K     |0    |512        |59/45/76     |3/1/5         |18%   |
|1_06   |526.7 M     |997.1 K     |0    |512        |61/52/70     |4/4/5         |18%   |
+-------+------------+------------+-----+-----------+-------------+--------------+------+
|Total  |3.3 G       |6.2 M       |0    |3.4 K      |58/48/68     |3/1/5         |18%   |
+-------+------------+------------+-----+-----------+-------------+--------------+------+

+-------------------------------------------------------------------------------+
|Per Path Distribution Summary                                                  |
+-------------------------+------------+------------+------------+-------------+
|                         |Acceleration|Medium      |Firewall    |Dropped      |
+-------------------------+------------+------------+------------+-------------+
|Throughput               |3.2 G       |0           |2.1 M       |117.6 M      |
|Packet rate              |6.0 M       |0           |1.4 K       |222.8 K      |
|Connection rate          |0           |0           |0           |             |
|Concurrent connections   |3.2 K       |0           |156         |             |
+-------------------------+------------+------------+------------+-------------+

+-------------------------------------+-----------------------+
|VPN Performance                      |                       |
+-------------------------------------+-----------------------+
|VPN throughput                       |2.9 G                  |
|VPN connections                      |3.1 K                  |
+-------------------------------------+-----------------------+
[Global] MyChassis-ch01-01>
```

Example 5 - Virtual System Memory Summary with Performance Summary (asg perf -vs all -vv mem)

The `-vv mem` parameter shows memory usage for each Virtual System across all Active Security Group Members.

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg perf -vs all -vv mem
Tue Jul 29 16:05:44 IDT 2014
Aggregated statistics (IPv4 Only) of SGMs: chassis_active VSs: all
+-------------------------------------------------------------+
|Performance Summary                                          |
+---------------------------------------------+---------------+
|Name                                         |Value          |
+---------------------------------------------+---------------+
|Throughput                                   |684.5 K        |
|Packet rate                                  |700            |
|Connection rate                              |3              |
|Concurrent connections                       |144            |
|Load average                                 |2%             |
|Acceleration load (avg/min/max)              |0%/0%/1%       |
|Instances load (avg/min/max)                 |2%/0%/12%      |
|Memory usage                                 |10%            |
+---------------------------------------------+---------------+
 * Instances / Acceleration Cores: 8 / 4
+-------------------------------------------------------------------------------+
|Per VS Memory Summary                                                          |
+--------+-------------+-------------+-------------+-------------+---------+
| VS ID  | User Space  | Memory in   | FWK memory  | Total memory| CPU     |
|        | memory      | Kernel      |             |             | Usage % |
+--------+-------------+-------------+-------------+-------------+---------+
|   0 max|222.3M (1_01)|1.658G (1_04)|47.11M (1_04)|1.880G (1_04)|   N/A   |
|     min|215.8M (1_03)|1.213G (1_01)|45.55M (1_03)|1.249G (1_01)|   N/A   |
+--------+-------------+-------------+-------------+-------------+---------+
|   1 max|56.34M (1_02)|   0K (1_04) |31.16M (1_02)|56.34M (1_02)|   N/A   |
|     min|54.24M (1_01)|   0K (1_04) |29.52M (1_03)|54.24M (1_01)|   N/A   |
+--------+-------------+-------------+-------------+-------------+---------+
* Maximum and minimum values are calculated across all active SGMs
[Global] MyChassis-ch01-01>
```

Notes:

- The Security Group Member that uses the most user space memory on Virtual System 1 is Security Group Member `1_01`
- The Security Group Member that uses the least `fwk` daemon memory on Virtual System 3 is Security Group Member `1_02`
- This information shows only if `vsxmstat` is enabled for `perfanalyze` use
- Make sure that the `vsxmstat` feature is enabled (`vsxmstat status_raw`)

Performance Hogs (asg_perf_hogs)

In This Section:

You can run tests to check for software components that decrease (hog) performance.

Syntax

Description

You can run:

- The `asg_perf_hogs` command in the Expert mode
- The `show smo verifiers report name Performance_hogs` command in Gaia gClish

Syntax

```
# asg_perf_hogs
```

Example

```
[Expert@MyChassis-01:0]# asg_perf_hogs
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [PASSED] | PPACK debug flags                                  |
| [PASSED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [FAILED] | routed trace options                               |
-----------------------------------------------------------------

Found the following issues:
-----------------------------------------------------------------
[ All] routed trace options are set: Cluster; igmp:All; pim:All
[Expert@MyChassis-01:0]#
```

Notes:

- When you run the `asg_perf_hogs` command by itself, you can get the full details of all the tests it runs.
- When you run the `show smo verifiers report name Performance_hogs` command, it shows a general result of `asg_perf_hogs` test output.
- If all of the `asg_perf_hogs` tests pass, the `show smo verifiers report name Performance_hogs` command shows **Passed**.
- If even one of the `asg_perf_hogs` tests fails, the `show smo verifiers report name Performance_hogs` command shows **Failed (!)**.

Configuration

You can configure `asg_perf_hogs` with the `$SMODIR/conf/performance_hogs.conf` file.

```
[tests]
long_running_procs=1
accel_off=1
sim_debug_flags=1
fw1_debug_flags=1
local_logging=1
disabled_templates=1
correction_table_entries=1
routing_cache_entries=1
swap_saturation=1
delayed_notifications=1
neighbour_table_overflow=1
soft_lockups=1
standby_chassis_load=1
routed_trace_options=1
peak_connections=1
[correction_table_entries]
threshold=10
[long_running_procs]
elapsed_time=60
processes_to_check=("fw ctl zdebug" "fw ctl debug" "fw ctl kdebug" "fw monitor" "tcpdump")
[routing_cache_entries]
threshold=90
[swap_saturation]
threshold=50
[neighbour_table_overflow]
timeout=3600
[soft_lockups]
timeout=3600
[standby_chassis_load]
threshold=50
[peak_connections]
threshold=90
[disabled_templates]
#max_rule_num=999
```

The [tests] Section

The **[tests]** section in the `$SMODIR/conf/performance_hogs.conf` file lets you enable and disable which tests to run.

Note - Not all the tests can be configured.

To enable or disable a test:

In the `[tests]` section, set the applicable value for the applicable test:

- `1` = To enable the test
- `0` = To disable the test

To configure a test:

Step	Instructions
1	Find the configuration section for the test in the `$SMODIR/conf/performance_hogs.conf` file. If it does not exist, add the section with this format: `[<test_name>]`
2	Change or add the parameters for the test. See the tables below for allowed parameters.

Below are the descriptions of some of the tests in the `[tests]` section in the `$SMODIR/conf/performance_hogs.conf` file.

long_running_procs

The `long_running_procs` test confirms that certain processes do not run longer than the configured time.

Note - This test runs in contexts of all Virtual Systems.

Parameters:

Parameter	Description
`elapsed_time`	Longest time in seconds a process should run Default = 60 seconds Minimum recommended value = 30

Parameter	Description
`processes_to_check`	List of processes to check: Each process must be in quotes. Put a space between each test. Default: `"fw ctl zdebug" "fw ctl debug" "fw ctl kdebug" "fw monitor" "tcpdump"` Example: `processes_to_check=("fw ctl zdebug" "fw ctl debug" "fw ctl kdebug" "fw monitor" "tcpdump")`

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [FAILED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [PASSED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------

Found potential CPU hogging processes:
-----------------------------------------------------------------
Blade    PID     ELAPSED     TIME CMD
[1_01]  1484       03:48 00:00:00 tcpdump -nnni eth1-01

Found the following issues:
-----------------------------------------------------------------
[ All] The process 'tcpdump' is running for more than 60 seconds
```

accel_off

The `accel_off` test confirms that SecureXL is working.

Notes:

- This test has no configuration options.
- The test runs in the context of the current Virtual System only.

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [PASSED] | Routing cache entries                              |
| [FAILED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------
 Found the following issues:
-----------------------------------------------------------------
[ All] SecureXL acceleration is disabled!
```

fw1_debug_flags

The `fw1_debug_flags` test confirms that Firewall debug flags that are not enabled by default, stay in the disabled position.

Notes:

- This test has no configuration options.
- This test runs in contexts of all Virtual Systems.

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [FAILED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [PASSED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------
 Found the following issues:
-----------------------------------------------------------------
[ All] FW1 debug flags are set:; Module: fw; ; Flags: error warning packet
```

local_logging

The `local_logging` test confirms that logs are written to a Log Server and not locally.

Notes:

- This test has no configuration options.
- This test runs in the context of the current Virtual System only.

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [FAILED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [PASSED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------
 Found the following issues:
-----------------------------------------------------------------
[ All] Local logging is active: No connection with log server!
```

routing_cache_entries

The `routing_cache_entries` test confirms that the IPv4 route cache capacity is not above a certain threshold.

Threshold is the percent capacity of the IPv4 route cache that should not be exceeded:

- Default = 90
- Recommended range = 75 - 95

Note - This test runs in the context of the current Virtual System only.

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [FAILED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------
 Found the following issues:
-----------------------------------------------------------------
[ All] Routing cache is 93% full (983731 out of 1048576 entries).
```

swap_saturation

The `swap_saturation` test confirms that swap file usage is not above the threshold.

Threshold is the percent use of the swap file allowed. Recommended range is 75 - 99.

Note - This test runs regardless of the Virtual System context.

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [PASSED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [FAILED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------
 Found the following issues:
-----------------------------------------------------------------
[ All] Swap saturation is 90%. Total swap space: 1044216 bytes, used: 950000 bytes.
```

neighbour_table_overflow

The `neighbour_table_overflow` test confirms that the ARP cache did not overflow.

Timeout is the number of seconds the specifies for how long to look in the `/var/log/messages` file for ARP cache overloaded messages. Recommended range is 300 - 86400.

Notes:

- To learn how to adjust the ARP cache, see sk43772.
- This test runs regardless of the Virtual System context.

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [PASSED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [FAILED] | Neighbour table overflow                           |
| [PASSED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------
Found the following issues:
-----------------------------------------------------------------
[ All] Neighbour table overflow occurred during the last 3600 seconds.
Please see solution SK43772 for information how to configure arp cache size.
```

soft_lockups

The `soft_lockups` test confirms there are no kernel soft lockups during the timeout period.

Timeout is the number of seconds to look back in the `/var/log/messages` file for kernel soft lockup messages:

- Default = 3600
- Recommended range = 300 - 86400

Note - This test runs regardless of the Virtual System context.

Example output

```
-----------------------------------------------------------------
|  Status  |  Test performed                                    |
-----------------------------------------------------------------
| [PASSED] | Disabled Accept Templates                          |
| [PASSED] | Disabled NAT Templates                             |
| [PASSED] | FW1 debug flags                                    |
| [FAILED] | Kernel soft lockups                                |
| [PASSED] | Local logging                                      |
| [PASSED] | Long running processes                             |
| [PASSED] | Neighbour table overflow                           |
| [PASSED] | Routing cache entries                              |
| [PASSED] | SecureXL status                                    |
| [PASSED] | Swap saturation                                    |
| [PASSED] | routed trace options                               |
-----------------------------------------------------------------
 Found the following issues:
-----------------------------------------------------------------
[1_01] Soft lockup occurred during the last 3600 seconds.
```

Setting Port Priority

Description

For each Security Group port, you can set a port priority (high or standard).

Use the `set chassis high-availability port ... priority ...` command in Gaia gClish.

Syntax

```
> set chassis high-availability port <if_name> priority <priority>
```

Parameters

Parameter	Description
<if_name>	Interface name
<priority>	Port grade Valid values: ■ `1` - Standard priority ■ `2` - Other priority

Use the `set chassis high-availability port ... priority ...` command together with the `set chassis high-availability factors port ...` command:

- Set the port grade as standard or high.

  For example, to set the standard grade at 50, run:

  ```
  > set chassis high-availability factors port standard 50
  ```

- Set the port to high grade or standard grade.

  For example, to assign the standard port grade to `eth1-01`, run:

  ```
  > set chassis high-availability port eth1-01 priority 1
  ```

Searching for a Connection (asg search)

In This Section:

This section describes how to search for a connection in the Connections Table.

Description

Use the `asg search` command in Gaia gClish or the Expert mode to:

- Search for a connection or a filtered list of connections.
- See which Security Group Member handles the connection, actively or as backup, and on which Site.

You can run this command directly or in Interactive Mode. In the Interactive Mode, you can enter the parameters in the correct sequence.

The `asg search` command also runs a consistency test between Security Group Members.

This command supports both IPv4 and IPv6 connections.

Searching with the Command Line

Syntax

```
> asg search -help
```

```
> asg search [-v] [-vs <VS_IDs>] [<source_ip> <dest_ip> <dest_port> <protocol>]
```

Parameters

Parameter	Description
`-help`	Shows the built-in help.
Without parameters	Runs in the interactive mode.

Parameter	Description
`-vs <VS_IDs>`	Shows connections for the specified Virtual System. *<VS_IDs>* can be: ■ No *<VS_IDs>* specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems
<source_ip>	Source IPv4 or IPv6 address.
<dest_ip>	Destination IPv4 or IPv6 address.
<dest_port>	Destination port number.
<protocol>	IP Protocol.
<source_port>	Source port number.
`-v`	Shows connection indicators for: ■ **A** - Active Security Group Member ■ **B** - Backup Security Group Member ■ **F** - Firewall connection table ■ **S** - SecureXL connection table ■ **C** - Correction Layer table This is in addition to the indicators for Active and Backup Security Group Member.

Notes:

- You must enter the all parameters in the sequence shown in the above syntax.
- You can enter `\*` as a parameter to show all values for that parameter.
- The `-vs` parameter is only available for a Security Group in VSX mode.

Below are some examples:

Example 1 - Search for one IPv4 source and destination for the TCP protocol

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg search -v 192.0.2.4 192.0.2.15 \* tcp
Lookup for conn: <192.0.2.4, 192.0.2.15, *, tcp>, may take few seconds...

<192.0.2.4, 1130,  192.0.2.15, 49829, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36323, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130,  192.0.2.15, 49851, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36308, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36299, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130,  192.0.2.15, 49835, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130,  192.0.2.15, 49856, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36331, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130,  192.0.2.15, 49857, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130,  192.0.2.15, 49841, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36315, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130,  192.0.2.15, 49859, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36300, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36301, 192.0.2.15, 1130,  tcp> -> [2_01 A, 1_04 A]

Legend:
A - Active SGM
B - Backup SGM
C - Correction Layer table
F - Firewall connection table
S - SecureXL connection table
[Global] MyChassis-ch01-01>
```

Example 2 - Search for one IPv6 source, all destinations, source port 8080, and TCP protocol

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg search 2620:0:2a03:16:2:33:0:1 \* 8080 tcp

<2620:0:2a03:16:2:33:0:1, 52117, 951::69cb:e42d:eac0:652f, 8080, tcp> -> [1_01 A, 2_01 B]
<2620:0:2a03:16:2:33:0:1, 62775, 951::69cb:e42d:eac0:652f, 8080, tcp> -> [1_01 A, 2_01 B]
<2620:0:2a03:16:2:33:0:1, 54378, 951::69cb:e42d:eac0:652f, 8080, tcp> -> [1_01 A, 2_01 B]
Legend:
A - Active SGM
B - Backup SGM
[Global] MyChassis-ch01-01>
```

Example 3 - Search for all sources, destinations, ports and protocols for VS0

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg search -vs 0 \* \* \* \* \*.
Lookup for conn: <*, *, *, *, *>, may take few seconds...

<172.23.9.130, 18192, 172.23.9.138, 43563, tcp> -> [1_01 A]
<172.23.9.130, 32888, 172.23.9.138, 257, tcp> -> [1_01 A]
<172.23.9.130, 22, 194.29.47.14, 52120, tcp> -> [1_01 A]
<172.23.9.138, 257, 172.23.9.130, 32963, tcp> -> [1_01 A]
<172.23.9.130, 22, 194.29.47.14, 52104, tcp> -> [1_01 A]
<255.255.255.255, 67, 0.0.0.0, 68, udp> -> [1_01 A]
<172.23.9.138, 257, 172.23.9.130, 32864, tcp> -> [1_01 A]
<172.23.9.138, 257, 172.23.9.130, 32888, tcp> -> [1_01 A]
<172.23.9.138, 257, 172.23.9.130, 33465, tcp> -> [1_01 A]
<172.23.9.130, 22, 194.29.40.23, 65515, tcp> -> [1_01 A]
<172.23.9.130, 22, 194.29.47.14, 52493, tcp> -> [1_01 A]
<172.23.9.130, 18192, 172.23.9.138, 49059, tcp> -> [1_01 A]
<172.23.9.130, 18192, 172.23.9.138, 33356, tcp> -> [1_01 A]
<172.23.9.138, 33356, 172.23.9.130, 18192, tcp> -> [1_01 A]
<172.23.9.138, 43563, 172.23.9.130, 18192, tcp> -> [1_01 A]
<172.23.9.130, 32864, 172.23.9.138, 257, tcp> -> [1_01 A]
<0.0.0.0, 68, 255.255.255.255, 67, udp> -> [1_01 A]
<172.23.9.130, 32963, 172.23.9.138, 257, tcp> -> [1_01 A]
<172.23.9.130, 33465, 172.23.9.138, 257, tcp> -> [1_01 A]
<194.29.47.14, 52120, 172.23.9.130, 22, tcp> -> [1_01 A]
<194.29.47.14, 52104, 172.23.9.130, 22, tcp> -> [1_01 A]
<fe80::d840:5de7:8dbe:2345, 546, ff02::1:2, 547, udp> -> [1_01 A]
<194.29.47.14, 52493, 172.23.9.130, 22, tcp> -> [1_01 A]
<172.23.9.138, 49059, 172.23.9.130, 18192, tcp> -> [1_01 A]
<194.29.40.23, 65515, 172.23.9.130, 22, tcp> -> [1_01 A]
Legend:
A - Active SGM
B - Backup SGM
[Global] MyChassis-ch01-01>
```

Searching with Interactive Mode

With Interactive Mode, you can enter connection search parameters interactively in the required sequence.

You can use this as an alternative to the command line syntax.

To run 'asg search' in Interactive Mode:

Step	Instructions
1	Run in Gaia gClish: `> asg search [-vs <VS_IDs>] [-v]`
2	Enter these parameters in the order below: 1. Source IPv4 or IPv6 address 2. Destination IPv4 or IPv6 address 3. Destination port number 4. IP protocol 5. Source port number **Note** - You can enter `*` to show all values for any parameter.

Example - Search for one IPv4 source and destination

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> asg search -v

Please enter conn's 5 tuple:
----------------------------
Enter source IP (press enter for wildcard):
 >192.0.2.4
Enter destination IP (press enter for wildcard):
 >192.0.2.15
Enter destination port (press enter for wildcard):
 >
Enter IP protocol ('tcp', 'udp', 'icmp' or enter for wildcard):
 >tcp
Enter source port (press enter for wildcard):
 >
Lookup for conn: <192.0.2.4, *, 192.0.2.15, *, tcp>, may take few seconds...
<192.0.2.4, 37408, 192.0.2.15, 1130, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 1130, 192.0.2.15, 49670, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 1130, 192.0.2.15, 49653, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 37406, 192.0.2.15, 1130, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 1130, 192.0.2.15, 49663, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 1130, 192.0.2.15, 49658, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 37407, 192.0.2.15, 1130, tcp> -> [2_01 AF, 1_04 AF]

Legend:
A - Active SGM
B - Backup SGM
C - Correction Layer table
F - Firewall connection table
S - SecureXL connection table

Example 2 - One IPv6 source with any Destination on port 8080 and TCP:
[Global] MyChassis-ch01-01 >

[Global] MyChassis-ch01-01 > asg search 2620:0:2a03:16:2:33:0:1 \* 8080 tcp
Enter source IP (press enter for wildcard):
 > 2620:0:2a03:16:2:33:0:1
Enter destination IP (press enter for wildcard):
 >
Enter destination port (press enter for wildcard):
 >8080
Enter IP protocol ('tcp', 'udp', 'icmp' or enter for wildcard):
 >tcp
Enter source port (press enter for wildcard):
 >

Lookup for conn: <2620:0:2a03:16:2:33:0:1, *, *, 8080, tcp>, may take few seconds...
<2620:0:2a03:16:2:33:0:1, 52117, 951::69cb:e42d:eac0:652f, 8080, tcp> -> [1_01 A, 2_01 B]
<2620:0:2a03:16:2:33:0:1, 62775, 951::69cb:e42d:eac0:652f, 8080, tcp> -> [1_01 A, 2_01 B]
<2620:0:2a03:16:2:33:0:1, 54378, 951::69cb:e42d:eac0:652f, 8080, tcp> -> [1_01 A, 2_01 B]

A - Active SGM
B - Backup SGM
[Global] MyChassis-ch01-01>
```

Showing the Number of Firewall and SecureXL Connections (asg_conns)

Description

Use the `asg_conns` command in Gaia gClish or the Expert mode to show the number of Firewall and SecureXL connections on each Security Group Member.

Syntax

```
asg_conns -h
asg_conns [-b <SGM_IDs>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-b <SGM_IDs>`	Applies to Security Group Members as specified by `<SGM_IDs>`. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`)
`-6`	Shows only IPv6 connections.

Example

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01 > asg_conns
1_01:
     #VALS     #PEAK   #SLINKS
       246      1143       246
1_02:
     #VALS     #PEAK   #SLINKS
        45       172        45
1_03:
     #VALS     #PEAK   #SLINKS
        45       212        45
1_04:
     #VALS     #PEAK   #SLINKS
       223       624       223
1_05:
     #VALS     #PEAK   #SLINKS
        45       246        45

Total (fw1 connections table): 604 connections

1_01:
There are 60 conn entries in SecureXL connections table
Total conn entries @ DB 0:  4
Total conn entries @ DB 3:  2
.
.
Total conn entries @ DB 26:  4
Total conn entries @ DB 30:  2
1_02:
There are 16 conn entries in SecureXL connections table
Total conn entries @ DB 0:  2
Total conn entries @ DB 1:  2
.
.
Total conn entries @ DB 26:  2
1_03:
There are 16 conn entries in SecureXL connections table
Total conn entries @ DB 0:  2
Total conn entries @ DB 5:  2
.
.
Total conn entries @ DB 30:  2
1_04:
There are 260 conn entries in SecureXL connections table
Total conn entries @ DB 0:  10
Total conn entries @ DB 1:  6
.
.
Total conn entries @ DB 31:  94
1_05:
There are 16 conn entries in SecureXL connections table
Total conn entries @ DB 2:  2
.
.
Total conn entries @ DB 26:  2

Total (SecureXL connections table): 368 connections
[Global] MyChassis-ch01-01>
```

Packet Drop Monitoring (asg_drop_monitor)

Description

Use the `asg_drop_monitor` command in the Expert mode to monitor dropped packets in real time.

Drop statistics arrive from these modules:

- NICs
- Operating System
- CoreXL
- PSL
- SecureXL

This command opens a monitor session and shows aggregated data from all Security Appliances in this Security Group. To stop an open session, press **CTRL+C**.

Syntax

```
# asg_drop_monitor -h
# asg_drop_monitor [-r] [-6]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-r`	Reset statistics to 0.
`-6`	Shows only IPv6 results.
`-ssm [-t <timeout>]`	This parameter is not supported (see MBS-5478).

Example

```
# asg_drop_monitor

(IPv4 Drop Statistics - All Blades)
Wed Feb 27 11:04:51 EST 2019
NICs drops (Rx):
18415

IP Stack qdisc drops (Tx):
0

CoreXL queue drops (F2F):
14781348

CoreXL queue drops (PXL F2P)
0

PSL drops(total):
0

PSL rejects:
0

Ppak drops:
Displaying aggregated data from blades: all

Reason                Value              Reason                Value
--------------------  ---------------    --------------------  ---------------
general reason                8881796    CPASXL decision                     0
PSLXL decision                      0    clr pkt on vpn                      0
encrypt failed                      0    drop template                       0
decrypt failed                      0    interface down                      0
cluster error                       0    XMT error                           0
anti spoofing                       0    local spoofing                      0
sanity error                        0    monitored spoofed                   0
QOS decision                        0    C2S violation                       0
S2C violation                       0    Loop prevention                     0
DOS Fragments                       0    DOS IP Options                      0
DOS Blacklists                      0    DOS Penalty Box                     0
DOS Rate Limiting                   0    Syn Attack                          0
Reorder                             0    Expired Fragments                   0
#
```

Hardware Monitoring and Control

You can monitor the hardware components of your system.

Showing Hardware State (asg stat)

Description

Use the `asg stat` command in Gaia gClish or the Expert mode to show the state of the system and hardware components.

The command output shows:

- Security GatewayMode (Gateway or VSX)
- Uptime
- Number of members in the Security Group
- Number of Virtual Systems
- Software Version
- Information related to VSX configuration

Syntax

```
asg stat
      -h
      -i list_all
      -i sgm_info
      -i tasks
      -v [-amw]
      vs [all [-p]]
```

Note - If you run this command in the context of a Virtual System, the output is for the applicable Virtual System.

Parameters

Parameter	Description
No Parameter	Shows the Security Group status (short output).
`-h`	Shows the built-in help.

Parameter	Description
`-i list_all`	Shows: ■ The IDs of the Security Group members, their state and IP addresses ■ Tasks and on which Security Group member they run
`-i sgm_info`	Shows the IDs of the Security Group members, their state and IP addresses
`-i tasks`	Shows the list of Tasks and on which Security Group member they run: ■ **SMO** - Single Management Object ■ **General** - General ■ **LACP** - Interface Bonding ■ **CH Monitor** - Site state monitor ■ **DR Manager** - Dynamic Routing manager ■ **UIPC** - Unique IP Address for each Site ■ **Alert** - Alerts
`-v [-amw]`	Shows the detailed Security Group status (verbose output).
`vs [all [-p]]`	Shows the VSX information: ■ `vs` Shows general output for a Virtual System. Run this command in the context of the Virtual System. ■ `vs all` Output also shows all Virtual Systems. ■ `vs all -p` Output shows a summary health status for all Virtual Systems. For more information on a specific Virtual System, run the "`asg stat vs`" command from the context of the Virtual System.

Below are some example

Example 1 - Default Output (asg stat)

Syntax

```
asg stat
```

Example

```
[Expert@MyChassis-ch01-01:0]# asg stat
-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Up time                     | 02:10:27 hours                                |
| SGMs                        | 30/30                                         |
| Version                     | R80.30SP (Build Number XXX)                   |
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit          |                          Chassis 1                        |
-------------------------------------------------------------------------------
| SGMs          |                           30 / 30                         |
| Ports         |                            4 / 4                          |
| SSMs          |                            2 / 2                          |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch01-01:0]#
```

Example 2 - Detailed Output (asg stat -v)

Syntax

```
asg stat -v
```

Example output (top section)

```
[Expert@MyChassis-ch01-01:0]# asg stat -v
-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Up time                     | 02:10:39 hours                                |
| SGMs                        | 30/30                                         |
| Version                     | R80.30SP (Build Number XXX)                   |
-------------------------------------------------------------------------------
| SGM ID                              Chassis 1                               |
|                                     ACTIVE                                  |
-------------------------------------------------------------------------------
|  1                                    ACTIVE                                |
|  2                                    ACTIVE                                |
|  3                                    ACTIVE                                |
... ... ... ...
|  30                                   ACTIVE                                |
-------------------------------------------------------------------------------
... ... ...
```

This output shows that `Chassis1` is Active with 30 Security Group Members in the Active (UP) state.

Explanation about the output:

Field	Description
SGM ID	Identifier of the Security Group Member. The `(local)` is the Security Group Member, on which you ran the command.
State	State of the Security Group Member: ■ `ACTIVE` - The Security Group Member is processing traffic ■ `DOWN` - The Security Group Member is not processing traffic ■ `Detached` - No Security Group Member is detected in a slot To change manually the state of the Security Group Member, use the `g_clusterXL_admin` command. This command administratively changes the state to ACTIVE or DOWN. The Security Group Member that is DOWN because of a software or hardware problem cannot be changed to ACTIVE with this command.

Example output (bottom section)

```
... ... ...
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit         |                      Chassis 1                       | Weight |
-------------------------------------------------------------------------------
| SGMs         |                        30 / 30                       |   6    |
| Ports        |                                                      |        |
|   Standard   |                         4 / 4                        |  11    |
|   Bond       |                         0 / 0                        |  11    |
|   Other      |                         0 / 0                        |   6    |
| Sensors      |                                                      |        |
|   SSMs       |                         2 / 2                        |  11    |
|              |                                                      |        |
| Grade        |                      246 / 246                       |   -    |
-------------------------------------------------------------------------------
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
-------------------------------------------------------------------------------
```

Note - The `X/X` notation shows the number of components that are UP and the components must be UP. For example, on the SGMs line, 30/30 means that 30 Security Group Members are currently UP and 30 must be UP.

Field	Description

Grade	The sum of the grades of all components. The grade of each component is the unit weight multiplied by the number of components that are UP.
	You can configure the unit weight of each component to show the importance of the component in the system.
	To configure the unit weight run:
	`> set chassis high-availability factors <sensor_name>`
	For example, to change the weight of the Security Group Member to 12, run:
	`> set chassis high-availability factors sgm 12`
	If you run the `asg stat -v` command, the output shows a higher unit weight and system grade.

Synchronization	Status of synchronization between Security Group Members located in the same Security Group.

Monitoring System and Component Status (asg monitor)

Description

Use the `asg monitor` command in Gaia gClish or the Expert mode to continuously monitor the status of the system and its components.

This command shows the same information as the *"Showing Hardware State (asg stat)" on page 126*, but the information stays on the screen and refreshes at intervals specified by the user. Default = 1 second). To stop the monitor session, press **CTRL+C**.

Note - If you run this command in a Virtual System context, you only see the output for that Virtual System. You can also specify the Virtual System context as a command parameter.

Syntax

```
asg monitor -h
asg monitor
asg monitor [-v | -all] [-amw] <Interval>
asg monitor -l
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Shows the Security Group Member status.
`-amw`	Shows the Anti-Malware policy date instead of the Firewall policy date.
`-v`	Shows only the System component status.
`-all`	Shows both Security Group Member and System component status.
<Interval>	Configures the data refresh interval (in seconds) for this session. Default is 10 seconds.
`-l`	Shows legend of column title abbreviations.

Below are some examples:

Example 1 - Shows the Security Group Member status with the Anti-Malware policy date

```
[Expert@MyChassis-ch01-01:0]# asg monitor -amw

-------------------------------------------------------------------------------
| System Status - Maestro                                                     |
-------------------------------------------------------------------------------
| Up time                     | 12:03:48 hours                                |
| SGMs                        | 2 / 2                                         |
| Version                     | R80.30SP (Build Number XX)                    |
| FW Policy Date              | 21Feb19 14:37                                 |
| AMW Policy Date             | 21Feb19 14:37                                 |
-------------------------------------------------------------------------------
| SGM ID                              Chassis 1                               |
|                                     ACTIVE                                  |
-------------------------------------------------------------------------------
|  1                                    ACTIVE                                |
|  2                                    ACTIVE                                |
-------------------------------------------------------------------------------
```

Example 2 - Shows the Security Group component status

```
[Expert@MyChassis-ch01-01:0]# asg monitor -v
Thu Feb 21 21:07:11 IST 2019

-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit         |                      Chassis 1                       | Weight |
-------------------------------------------------------------------------------
| SGMs         |                        2 / 2                         |   6    |
| Ports        |                                                      |        |
|   Standard   |                        8 / 8                         |  11    |
|   Bond       |                        0 / 0                         |  11    |
|   Mgmt       |                        1 / 1                         |  11    |
|   Mgmt Bond  |                        0 / 0                         |  11    |
|   Other      |                        0 / 0                         |   6    |
| Sensors      |                                                      |        |
|   SSMs       |                        2 / 2                         |  11    |
|              |                                                      |        |
| Grade        |                      133 / 133                       |   -    |
-------------------------------------------------------------------------------
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
-------------------------------------------------------------------------------
```

Configuring Alert Thresholds (set chassis alert_threshold)

Description

You can configure alert thresholds for performance and hardware monitoring alerts.

Run these commands in Gaia gClish to:

- Set the hardware and performance alert thresholds.
- Show the alert configuration

Syntax

```
> set chassis alert_threshold <threshold_name> <value>
> show chassis alert_threshold <threshold_name>
```

Parameters

Parameter	Description
<threshold_name>	Threshold name as specified in the table below
<value>	High or low value for the applicable threshold

Example - Set the memory utilization high limit to 70% of installed memory:

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> set chassis alert_threshold mem_util_threshold_perc_high 70
[Global] MyChassis-ch01-01>
```

Performance Alert Thresholds:

Threshold Name	Scope	Description
concurr_conn_threshold_high	Security Group Member	Concurrent connections - High limit
concurr_conn_threshold_low_ratio	Security Group Member	Concurrent connections - Low limit (% of high limit)
concurr_conn_total_threshold_high	System	Concurrent connections - High limit

Threshold Name	Scope	Description
concurr_conn_total_threshold_low_ratio	System	Concurrent connections - Low limit (% of high limit)
conn_rate_threshold_high	Security Group Member	Connection rate per second - High limit
conn_rate_threshold_low_ratio	Security Group Member	Connection rate per second - Low limit (% of high limit)
conn_rate_total_threshold_high	System	Connection rate per second - High limit
conn_rate_total_threshold_low_ratio	System	Connection rate per second - Low limit (% of high limit)
cpu_load_threshold_perc_high	Security Group Member	CPU load (%) - High limit
cpu_load_threshold_perc_low_ratio	Security Group Member	CPU load (%) - Low limit (% of high limit)
hd_util_threshold_perc_high	Security Group Member	Disk utilization (%) - High limit
hd_util_threshold_perc_low_ratio	Security Group Member	Disk utilization (%) - Low limit (% of high limit)
mem_util_threshold_perc_high	Security Group Member	Memory utilization (%) - High limit
mem_util_threshold_perc_low_ratio	Security Group Member	Memory utilization (%) - Low limit (% of high limit)
packet_rate_threshold_high	Security Group Member	Packet rate per second - High limit
packet_rate_threshold_low_ratio	Security Group Member	Packet rate per second - Low limit (% of high limit)
packet_rate_total_threshold_high	System	Packet rate per second - High limit

Threshold Name	Scope	Description
`packet_rate_total_threshold_low_ratio`	System	Packet rate per second - Low limit (% of high limit)
`throughput_threshold_high`	Security Group Member	Throughput (bps) - High limit
`throughput_threshold_low_ratio`	Security Group Member	Throughput (bps) - Low limit (% of high limit)
`throughput_total_threshold_high`	System	Throughput (bps) - High limit
`throughput_total_threshold_low_ratio`	System	Throughput (bps) - Low limit (% of high limit)

Monitoring System Resources (asg resource)

Description

Use the `asg resource` command in Gaia gClish or the Expert mode to show this information for Security Group Members:

- RAM and Storage usage and thresholds
- SSD Health

Syntax

```
> asg resource -h
> asg resource [-b <SGM_IDs>]
> asg resource --ssd [-v]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Shows both the Resource (RAM and Storage) and SSD Health information.
`-b <SGM_IDs>`	Applies to Security Group Members as specified by `<SGM_IDs>`. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`)
`--ssd [-v]`	Shows only the SSD Health information for all Security Group Members: ■ `--ssd` - Shows summary information only (whether it passed the SMART test) ■ `--ssd -v` - Shows the summary and verbose information (SSD SMART Attributes)

Below are some examples:

Example 1 - Default output

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01 > asg resource
+-------------------------------------------------------------------------------------+
|Resource Table                                                                       |
+------------+-------------------------+------------+------------+------------------+
|Member ID   |Resource Name            |Usage       |Threshold   |Total             |
+------------+-------------------------+------------+------------+------------------+
|1_01        |Memory                   |21%         |50%         |62.8G             |
|            |HD: /                    |16%         |80%         |33.9G             |
|            |HD: /var/log             |2%          |80%         |48.4G             |
|            |HD: /boot                |14%         |80%         |288.6M            |
+------------+-------------------------+------------+------------+------------------+
|1_02        |Memory                   |21%         |50%         |62.8G             |
|            |HD: /                    |16%         |80%         |33.9G             |
|            |HD: /var/log             |2%          |80%         |48.4G             |
|            |HD: /boot                |14%         |80%         |288.6M            |
+------------+-------------------------+------------+------------+------------------+
... output is cut for brevity ...
+------------+-------------------------+------------+------------+------------------+
|2_01        |Memory                   |21%         |50%         |62.8G             |
|            |HD: /                    |16%         |80%         |33.9G             |
|            |HD: /var/log             |2%          |80%         |48.4G             |
|            |HD: /boot                |14%         |80%         |288.6M            |
+------------+-------------------------+------------+------------+------------------+
|2_02        |Memory                   |21%         |50%         |62.8G             |
|            |HD: /                    |16%         |80%         |33.9G             |
|            |HD: /var/log             |2%          |80%         |48.4G             |
|            |HD: /boot                |14%         |80%         |288.6M            |
+------------+-------------------------+------------+------------+------------------+
... output is cut for brevity ...
+-----------------------------------------+
|SSD Health                               |
+---------------+-------------------------+
|Member ID      |SMART overall-health     |
+---------------+-------------------------+
|1_01           |PASSED                   |
+---------------+-------------------------+
|1_02           |PASSED                   |
+---------------+-------------------------+
... output is cut for brevity ...
+---------------+-------------------------+
|2_01           |PASSED                   |
+---------------+-------------------------+
|2_02           |PASSED                   |
+---------------+-------------------------+
... output is cut for brevity ...

SSD attributes verifier ended successfully.
[Global] MyChassis-ch01-01>
```

Example 2 - Resource Table for specific Security Group Member

```
[Expert@MyChassis-01:0]# asg resource -b 1_01
+-------------------------------------------------------------------------------+
|Resource Table                                                                 |
+-----------+-----------------------+-----------+-----------+-----------------+
|Member ID  |Resource Name          |Usage      |Threshold  |Total            |
+-----------+-----------------------+-----------+-----------+-----------------+
|1_01       |Memory                 |21%        |50%        |62.8G            |
|           |HD: /                  |16%        |80%        |33.9G            |
|           |HD: /var/log           |2%         |80%        |48.4G            |
|           |HD: /boot              |14%        |80%        |288.6M           |
+-----------+-----------------------+-----------+-----------+-----------------+
+---------------------------------------+
|SSD Health                             |
+---------------+-----------------------+
|Member ID      |SMART overall-health   |
+---------------+-----------------------+
|1_01           |PASSED                 |
+---------------+-----------------------+
|1_02           |PASSED                 |
+---------------+-----------------------+
|1_03           |PASSED                 |
+---------------+-----------------------+
|1_04           |PASSED                 |
+---------------+-----------------------+
|1_05           |PASSED                 |
+---------------+-----------------------+
|2_01           |PASSED                 |
+---------------+-----------------------+
|2_02           |PASSED                 |
+---------------+-----------------------+
|2_03           |PASSED                 |
+---------------+-----------------------+
|2_04           |PASSED                 |
+---------------+-----------------------+
|2_05           |PASSED                 |
+---------------+-----------------------+

SSD attributes verifier ended successfully.
[Expert@MyChassis-01:0]#
```

Example 3 - Verbose SSD Health information

```
[Expert@MyChassis-01:0]# asg resource --ssd -v
+----------------------------------------+
|SSD Health                              |
+---------------+------------------------+
|Member ID      |SMART overall-health    |
+---------------+------------------------+
|1_01           |PASSED                  |
+---------------+------------------------+
|1_02           |PASSED                  |
+---------------+------------------------+
... output is cut for brevity ...
+---------------+------------------------+
|2_01           |PASSED                  |
+---------------+------------------------+
|2_02           |PASSED                  |
+---------------+------------------------+
... output is cut for brevity ...
+-------------------------------------------------------------------------+
|SSD Attributes                                                           |
+------+----------------------------+--------+--------+----------------+
Member 1_01
+------+----------------------------+--------+--------+----------------+
|ID    |Attribute name              |Value   |Trhesh  |Last_failed     |
+------+----------------------------+--------+--------+----------------+
|5     |Reallocated_Sector_Ct       |100     |0       |-               |
+------+----------------------------+--------+--------+----------------+
|9     |Power_On_Hours              |100     |0       |-               |
+------+----------------------------+--------+--------+----------------+
|12    |Power_Cycle_Count           |100     |0       |-               |
+------+----------------------------+--------+--------+----------------+
... output is cut for brevity ...
+------+----------------------------+--------+--------+----------------+
|194   |Temperature_Celsius         |100     |0       |-               |
+------+----------------------------+--------+--------+----------------+
... output is cut for brevity ...
+------+----------------------------+--------+--------+----------------+
Member 1_02
+------+----------------------------+--------+--------+----------------+
|ID    |Attribute name              |Value   |Trhesh  |Last_failed     |
+------+----------------------------+--------+--------+----------------+
|5     |Reallocated_Sector_Ct       |100     |0       |-               |
+------+----------------------------+--------+--------+----------------+
... output is cut for brevity ...
[Expert@MyChassis-ch01-01:0]#
```

Resource Table section description

Column	Description
Member ID	Shows the Security Group Member ID.
Resource Name	Identifies the resource. There are four types of resources: ■ **Memory** ■ **HD** - Hard drive space (/) ■ **HD: /var/log** - Space on hard drive committed to log files ■ **HD: /boot** - Location of the kernel
Usage	Shows the percentage of the resource in use.
Threshold	Indicates the health and functionality of the component. When the value of the resource is greater than the threshold, an alert is sent. You can modify the threshold in Gaia gClish.
Total	Total absolute value in units. For example, the first row shows that `Security Appliance1` on `Chassis1` has 62.8 GB of RAM, and 21% of it are used. An alert is sent, if the usage is greater than 50%.

SMART Attributes section description

Column	Description
SMART overall-health	Shows the state of the SMART test - passed, or failed.
ID	Shows the attribute ID in the decimal format.
Attribute name	Shows the attribute name.
Value	Shows the current value as returned by the SSD. This is a most universal measurement, on the scale from 0 (bad) to some maximum (good) value. Maximum values are typically 100, 200 or 253. The higher the value, the better the SSD health is.
Trhesh	Shows the current threshold. This is the minimum value limit for the attribute. If the value falls below this threshold, the SSD should be checked for errors, and possibly replaced.
Last_failed	Shows when a failure was last reported for this attribute.

Configuring Alerts for Security Group Member and Security Group Events (asg alert)

The `asg alert` command is an interactive wizard you can use to configure alerts for Security Group Member and Site events.

These events include hardware failure, recovery, and performance-related events. You can create other general events.

An alert is sent when an event occurs, for example, when the value of a hardware resource is greater than the threshold.

The alert message includes the Site ID, Security Group Member ID, and/or unit ID.

The wizard has these options:

Option	Description
Full Configuration Wizard	Creates a new alert.
Edit Configuration	Changes an existing alert.
Show Configuration	Shows existing alert configurations.
Run Test	Runs a test simulation to make sure that the alert works correctly.

To create or change an alert:

Step	Instructions
1	Run in Gaia gClish of a Security Group: `asg alert`
2	Select **Full Configuration Wizard** or **Edit Configuration**.
3	Select and configure these parameters as prompted by the wizard: ■ **SMS** ■ **Email** ■ **SNMP**

SMS Alert Configuration

Parameter	Description
SMS provider URL	Fully qualified URL to your SMS provider.
HTTP proxy and port	Optional. Configure only if the Security Gateway requires a proxy server to reach the SMS provider.
SMS rate limit	Maximum number of SMS messages sent per hour. If there are too many messages, they can be combined together.
SMS user text	Custom prefix for SMS messages.

Email Alert Configuration

Parameter	Description
SMTP server IP	One or more SMTP servers to which the email alerts are sent.
Email recipient addresses	One or more recipient email address for each SMTP server.
Periodic connectivity checks	Tests run periodically to confirm connectivity with the SNMP servers. If there is no connectivity, alert messages are saved and sent in one email when connectivity is restored.
Interval	Interval, in minutes, between connectivity tests.
Sender email address	Email address of the sender for alerts.
Subject	Subject header text for the email alert.
Body text	User defined text for the alert message.

SNMP Alert Configuration

Define one or more SNMP managers to get SNMP traps sent from the Security Gateway.

For each manager, configure these parameters:

SNMP Alert Parameters	Description
SNMP manager name	Unique name for the SNMP manager
SNMP manager IP	IP address of the SNMP Manager (trap receiver)
SNMP version	SNMP version (v2c, v3)
SNMP v3 user name	User name for SNMP v3 authentication
SNMP v3 security level	Security level for SNMP v3 authentication
SNMP v3 engine ID	Unique SNMP v3 engine ID used by your system The default is `0x80000000010203EA`
SNMP v3 authentication protocol	Authentication protocol (MD5 or SHA) for SNMP v3 authentication
SNMP v3 authentication password	Authentication password for SNMP v3 authentication
SNMP v3 privacy protocol	Privacy protocol (DES or AES) for SNMP v3 authentication
SNMP v3 privacy password	Privacy password for SNMP v3 authentication
SNMP user text	Custom text for SNMP trap messages
SNMP community string	Community name

Notes:

- Based on the settings, some parameters do not show.
- There are no configurable parameters for log alerts.

System Event Types

```
System event types are:
-----------------------------------
1       | SGM State
2       | Chassis State
3       | Port State
4       | Diagnostics
5       | Memory Leak Detection
6       | LSP Monitor Port State Change
7       | VS Monitor State Change
Hardware Monitor events:
8       | Fans
9       | SSM
10      | CMM
11      | Power Supplies
12      | CPU Temperature
Performance events:
13      | Concurrent Connections
14      | Connection Rate
15      | Packet Rate
16      | Throughput
17      | CPU Load
18      | Hard Drive Utilization
19      | Memory Utilization

Please choose event types for which to send alerts: [all]
(format: all or 1,4 or 1,3-7,10)n
```

You can select one or more event types:

- One event type.
- A comma-delimited list of more than one event type.
- All event types.

Collecting System Diagnostics (smo verifiers)

Diagnostic Tests

Description

The `smo verifiers` commands in Gaia gClish run a specific set of diagnostic tests.

The full set of tests run by default. but you can manually select the tests you want to run.

The output shows the result of the test, `Passed` or `Failed`, and the location of the output log file.

Syntax

```
> show smo verifiers list
      [id <TestId1>,<TestId2>,...]
      [section <SectionName>]
```

```
> show smo verifiers report [except]
      [id <TestId1>,<TestId2>,...]
      [name <TestName>]
      [section <SectionName>]
```

```
> show smo verifiers print [except]
      [id <TestId1>,<TestId2>,...]
      [name <TestName>]
      [section <SectionName>]
```

```
> show smo verifiers
      periodic
      last-run report
      print
```

```
> delete smo verifiers purge [save <Num_Logs>]
```

Parameters

Parameter	Description
`list`	Shows the list of tests to run.
`report`	Runs tests and shows a summary of the test results.
`print`	Runs tests and shows the full output and summary of the test results.

Parameter	Description
`except`	Runs all tests except the specified tests. Shows the requested results.
`id <TestId1>,<TestId2>,...`	Specifies the tests by their IDs (comma separated list). To see a list of test IDs, run: `> show smo verifiers list`
`name <TestName>`	Specifies the tests by their names. Press the **Tab** key to see a full list of verifiers names.
`section <SectionName>`	Specifies the verifiers section by its name. Press the **Tab** key to see a full list of the existing sections.
`purge`	Deletes the old `smo verifiers` logs. Keeps the newest log.
`save <Num_Logs>`	Number of logs to save from the `smo verifiers` log files. Default = 5.
`periodic`	Shows the latest `periodic` run results.
`last-run`	Shows the latest run results.

Showing the Tests

The `show smo verifiers list` command shows the full list of diagnostic tests.

The list shows the test `ID`, test `Title` (name), and the `Command` the `smo verifiers` command runs.

Example

```
> show smo verifiers list
-------------------------------------------------------------------------
| ID | Title              | Command                                     |
-------------------------------------------------------------------------
| System Components                                                     |
-------------------------------------------------------------------------
|  1 | System Health      | asg stat -v                                 |
|  2 | Resources          | asg resource                                |
|  3 | Software Provision | asg_provision                               |
|  4 | Media Details      | transceiver_verifier -v                     |
|  5 | SSD Health         | asg resource --ssd                          |
-------------------------------------------------------------------------
| Policy and Configuration                                              |
-------------------------------------------------------------------------
|  6 | Distribution Mode  | distutil verify -v                          |
|  7 | DXL Balance        | dxl stat                                    |
|  8 | Policy             | asg policy verify -a                        |
|  9 | AMW Policy         | asg policy verify_amw -a                    |
| 10 | SWB Updates        | asg_swb_update_verifier -v                  |
| 11 | Installation       | installation_verify                         |
| 12 | Security Group     | security_group_util diag                    |
| 13 | Cores Distribution | cores_verifier                              |
| 14 | Clock              | clock_verifier -v                           |
| 15 | Licenses           | asg_license_verifier -v                     |
| 16 | IPS Enhancement    | asg_ips_enhance status                      |
| 17 | Configuration File | config_verify -v                            |
-------------------------------------------------------------------------
| VSX Configuration                                                     |
-------------------------------------------------------------------------
| 18 | USER KERNEL Dist   | distutil verify_vsx_dist                    |
| 19 | HW Utilization     | hw_utilization -d                           |
| 20 | BMAC VMAC verify   | mac_verifier -x                             |
-------------------------------------------------------------------------
| Networking                                                            |
-------------------------------------------------------------------------
| 21 | MAC Setting        | mac_verifier -v                             |
| 22 | ARP Consistency    | asg_arp -v                                  |
| 23 | Bond               | asg_bond -v                                 |
| 24 | IPv4 Route         | asg_route                                   |
| 25 | IPv6 Route         | asg_route -6                                |
| 26 | Dynamic Routing    | asg_dr_verifier                             |
| 27 | Local ARP          | asg_local_arp_verifier -v                   |
| 28 | IGMP Consistency   | asg_igmp                                    |
| 29 | PIM Neighbors      | asg_pim_neighbors                           |
-------------------------------------------------------------------------
| Misc                                                                  |
-------------------------------------------------------------------------
| 30 | Core Dumps         | core_dump_verifier -v                       |
| 31 | Performance hogs   | asg_perf_hogs                               |
-------------------------------------------------------------------------
| Run "show smo verifiers print id <TestNum>" to display test output    |
-------------------------------------------------------------------------
```

Showing the Last Run Diagnostic Tests

The `show smo verifiers last-run report` command shows the default output for the last run diagnostic tests.

The `show smo verifiers last-run print` command shows verbose output for the last run diagnostic tests.

Example

```
> show smo verifiers last-run report
2019-02-07, 01:00:02
-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                               |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Failed (!) | (1)Chassis 1 error                   |
|  2 | Resources          | Passed     |                                      |
|  3 | Software Provision | Passed     |                                      |
|  4 | Media Details      | Passed     |                                      |
|  5 | SSD Health         | Passed     | (1)Failed to get SSD overall-health t |
|    |                    |            | est result from Member               |
-------------------------------------------------------------------------------
| Policy and Configuration                                                    |
-------------------------------------------------------------------------------
|  6 | Distribution Mode  | Failed (!) | (1)Verifier error - Check raw output  |
|  7 | DXL Balance        | Passed     |                                      |
|  8 | Policy             | Passed     |                                      |
|  9 | AMW Policy         | Passed     | (1)Not configured                    |
| 10 | SWB Updates        | Passed     | (1)Not configured                    |
| 11 | Installation       | Passed     |                                      |
| 12 | Security Group     | Passed     |                                      |
| 13 | Cores Distribution | Passed     |                                      |
| 14 | Clock              | Passed     |                                      |
| 15 | Licenses           | Failed (!) | (1)Trial license will expire within 2 |
|    |                    |            |  weeks                               |
|    |                    |            | (2)Execution error                   |
| 16 | IPS Enhancement    | Passed     |                                      |
| 17 | Configuration File | Passed     |                                      |
-------------------------------------------------------------------------------
| VSX Configuration                                                           |
-------------------------------------------------------------------------------
| 18 | USER KERNEL Dist   | Failed (!) |                                      |
| 19 | HW Utilization     | Failed (!) | (1)Execution error                   |
| 20 | BMAC VMAC verify   | Passed     |                                      |
-------------------------------------------------------------------------------
| Networking                                                                  |
-------------------------------------------------------------------------------
| 21 | MAC Setting        | Passed     |                                      |
... output was truncated for brevity ...
-------------------------------------------------------------------------------
| Misc                                                                        |
-------------------------------------------------------------------------------
| 30 | Core Dumps         | Failed (!) |                                      |
| 31 | Performance hogs   | Failed (!) |                                      |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 24/31 tests                                                         |
| Run: "show smo verifiers list id 1,6,15,18,19,30,31" to view a complete list |
|  of failed tests                                                            |
| Output file: /var/log/alert_verifier_sum.1-31.2019-02-07_01-00-02.txt       |
-------------------------------------------------------------------------------
```

Running all Diagnostic Tests

The `show smo verifiers report` command runs all diagnostic tests and shows their summary output.

When a test fails, the reasons for failure show in the **Reason** column.

Example

```
> show smo verifiers report
Duration of tests vary and may take a few minutes to complete

-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                               |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Failed (!) | (1)Chassis 1 error                   |
|  2 | Resources          | Passed     |                                      |
|  3 | Software Provision | Passed     |                                      |
|  4 | Media Details      | Passed     |                                      |
|  5 | SSD Health         | Passed     | (1)Failed to get SSD overall-health t |
|    |                    |            | est result from Member               |
-------------------------------------------------------------------------------
| Policy and Configuration                                                    |
-------------------------------------------------------------------------------
|  6 | Distribution Mode  | Failed (!) | (1)Verifier error - Check raw output  |
|  7 | DXL Balance        | Passed     |                                      |
|  8 | Policy             | Passed     |                                      |
|  9 | AMW Policy         | Passed     | (1)Not configured                    |
| 10 | SWB Updates        | Passed     | (1)Not configured                    |
| 11 | Installation       | Passed     |                                      |
| 12 | Security Group     | Passed     |                                      |
| 13 | Cores Distribution | Passed     |                                      |
| 14 | Clock              | Passed     |                                      |
| 15 | Licenses           | Failed (!) | (1)Trial license will expire within 2 |
|    |                    |            |  weeks                               |
|    |                    |            | (2)Execution error                   |
| 16 | IPS Enhancement    | Passed     |                                      |
| 17 | Configuration File | Passed     |                                      |
-------------------------------------------------------------------------------
| VSX Configuration                                                           |
-------------------------------------------------------------------------------
| 18 | USER KERNEL Dist   | Failed (!) |                                      |
| 19 | HW Utilization     | Failed (!) | (1)Execution error                   |
| 20 | BMAC VMAC verify   | Passed     |                                      |
-------------------------------------------------------------------------------
| Networking                                                                  |
-------------------------------------------------------------------------------
| 21 | MAC Setting        | Passed     |                                      |
... output was truncated for brevity ...
-------------------------------------------------------------------------------
| Misc                                                                        |
-------------------------------------------------------------------------------
| 30 | Core Dumps         | Failed (!) |                                      |
| 31 | Performance hogs   | Failed (!) |                                      |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 24/31 tests                                                         |
| Run: "show smo verifiers list id 1,6,15,18,19,30,31" to view a complete list |
|  of failed tests                                                            |
| Output file: /var/log/verifier_sum.1-31.2019-02-07_18-35-22.txt             |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
```

Running Specific Diagnostic Tests

The `show smo verifiers report name` and the `show smo verifiers report id` commands run the specified diagnostic tests only.

Syntax to run a test by its name

```
> show smo verifiers report name <Test Name>
```

Note - Press the **Tab** key after the `name` parameter to see a full list of verifier names.

Example

```
> show smo verifiers report name System_Health
Duration of tests vary and may take a few minutes to complete

-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                              |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Passed     |                                     |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 1/1 test                                                            |
| Output file: /var/log/verifier_sum.1.2018-12-10_12-16-51.txt                |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
```

Syntax to run a test by its ID

```
> show smo verifiers report id <TestID1>,<TestID2>,...,<TestIDn>
```

Note - To see a list of test IDs, run the `show smo verifiers list` command.

Example

```
> show smo verifiers report id 1,2,5
Duration of tests vary and may take a few minutes to complete

-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                               |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Failed (!) | (1)Chassis 1 error                   |
|  2 | Resources          | Passed     |                                      |
|  5 | SSD Health         | Passed     | (1)Failed to get SSD overall-health t |
|    |                    |            | est result from Member               |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 2/3 tests                                                           |
| Run: "show smo verifiers list id 1" to view a complete list of failed tests  |
| Output file: /var/log/verifier_sum.1-2.5.2019-02-07_18-37-22.txt            |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
```

Collecting Diagnostic Information for a Report Specified Section

The `show smo verifiers report section` command runs all diagnostic tests in the specified section.

Syntax

```
> show smo verifiers report section <Test Name>
```

Note - Press the **Tab** key after the `section` parameter to see a full list of verifier sections.

Example

```
> show smo verifiers report section System_Components
Duration of tests vary and may take a few minutes to complete

-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                               |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Failed (!) | (1)Chassis 1 error                   |
|  2 | Resources          | Passed     |                                      |
|  3 | Software Provision | Passed     |                                      |
|  4 | Media Details      | Passed     |                                      |
|  5 | SSD Health         | Passed     | (1)Failed to get SSD overall-health t |
|    |                    |            | est result from Member               |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 4/5 tests                                                           |
| Run: "show smo verifiers list id 1" to view a complete list of failed tests  |
| Output file: /var/log/verifier_sum.1-5.2019-02-07_18-38-56.txt              |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
```

Error Types

The `smo verifiers` detects these errors:

Error Type	Error	Description
`System health`	`Chassis <X> error`	The Security Group quality grade is less than the defined threshold. We recommend that you correct this issue immediately.
`Hardware`	`<Component> is missing`	The component is not installed in the Chassis. **Note** - This applies only to 60000 / 40000 Appliances.
	`<Component> is down`	The component is installed in the Chassis, but is inactive. **Note** - This applies only to 60000 / 40000 Appliances.
`Resources`	`<Resource> capacity`	The specified resource capacity is not sufficient. You can change the defined resource capacity.
	`<Resource> exceed threshold`	The resource usage is greater than the defined threshold.
`CPU type`	`Non compliant CPU type`	At least one Security Group Member CPU type is not configured in the list of compliant CPUs. You can define the compliant CPU types.
`Security group`	`<Source> error`	The information collected from this source is different between the Security Group Members.
	`<Sources> differ`	The information collected from many sources is different.

Changing Compliance Thresholds

You can change some compliance thresholds that define a healthy, working system.

In the `$SMODIR/conf/asg_diag_config` file, change the threshold values.

These are the supported resources you can control:

Resource	Description
`Memory`	RAM memory capacity in GB
`HD: /`	Disk capacity in GB for *<disk>* - the root (`/`) partition
`HD:/var/log`	Disk capacity in GB for the `/var/log` partition
`HD: /boot`	Disk capacity in GB for the `/boot` partition

Changing the Default Test Behavior of the 'asg diag resource verifier'

By default, the `asg diag resource verifier` command only shows a warning about resource mismatches between Security Group Members.

The verification test results show as "`Passed`" in the output and no further action is taken.

You can change the default test behavior:

Step	Instructions
1	Edit the `$FWDIR/conf/asg_diag_config` file: `# g_all vi $FWDIR/conf/asg_diag_config`
2	Search for the parameter `MismatchSeverity`.
3	Set the value of this parameter to one of these values: ■ `fail` - Verification test result is set to "`Failed`" ■ `warn` - Verification test result is set to "`Passed`", and a warning is shown ■ `ignore` - Verification test result is set to "`Ignore`", and no errors are shown
4	Save the changes in the file and exit the Vi editor.

Troubleshooting Failures

Use the `smo verifiers` command to troubleshoot a failed diagnostic test.

Below is the example procedure based on the **System Health** test that failed.

Example

1. The **System Health** test failed:

```
> show smo verifiers report id 1
Duration of tests vary and may take a few minutes to complete

-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                              |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Failed (!) | (1)Chassis 1 error                  |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 0/1 test                                                            |
| Run: "show smo verifiers list id 1" to view a complete list of failed tests |
| Output file: /var/log/verifier_sum.1.2019-02-07_20-12-07.txt                |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
>
```

2. Print the full report for this failed test:

```
> show smo verifiers print id 1
==============================
System Health:
==============================


-------------------------------------------------------------------------------
| VSX System Status - Maestro                                                 |
-------------------------------------------------------------------------------
| Up time                     | 06:44:48 hours                                |
| SGMs                        | 3 / 3                                         |
| Virtual Systems             | 1                                             |
| Version                     | R80.30SP (Build Number xxx)                   |
-------------------------------------------------------------------------------
| VS ID:  0                     VS Name:  MyVSname                            |
-------------------------------------------------------------------------------
| SGM ID                               Chassis 1                              |
|                                      ACTIVE                                 |
-------------------------------------------------------------------------------
|  2                                     ACTIVE                               |
|  3                                     ACTIVE                               |
|  4                                     ACTIVE                               |
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit         |                            Chassis 1                       |
-------------------------------------------------------------------------------
| SGMs         |                              3 / 3                         |
| Ports        |                              0 / 0                         |
| SSMs         |                              1 / 2   !                     |
-------------------------------------------------------------------------------
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
-------------------------------------------------------------------------------


-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                              |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Failed (!) | (1)Chassis 1 error                  |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 0/1 test                                                            |
| Run: "show smo verifiers list id 1" to view a complete list of failed tests |
| Output file: /var/log/verifier_sum.1.2019-02-07_20-12-14.txt                |
-------------------------------------------------------------------------------
```

3. Examine which command produced the failed test:

```
> show smo verifiers list id 1
-------------------------------------------------------------------------
| ID | Title              | Command                                     |
-------------------------------------------------------------------------
| System Components                                                     |
-------------------------------------------------------------------------
|  1 | System Health      | asg stat -v                                 |
-------------------------------------------------------------------------
| Run "show smo verifiers print id <TestNum>" to display test output    |
-------------------------------------------------------------------------
>
```

4. Run the applicable command to understand what fails:

```
> asg stat -v

-------------------------------------------------------------------------------
| VSX System Status - Maestro                                                 |
-------------------------------------------------------------------------------
| Up time                     | 06:45:06 hours                                |
| SGMs                        | 3 / 3                                         |
| Virtual Systems             | 1                                             |
| Version                     | R80.30SP (Build Number xxx)                   |
-------------------------------------------------------------------------------
| VS ID:  0                     VS Name:  MyVSname                            |
-------------------------------------------------------------------------------
| SGM ID                              Chassis 1                               |
|                                     ACTIVE                                  |
-------------------------------------------------------------------------------
|  2                                    ACTIVE                                |
|  3                                    ACTIVE                                |
|  4                                    ACTIVE                                |
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit        |                      Chassis 1                        | Weight |
-------------------------------------------------------------------------------
| SGMs        |                        3 / 3                          |   6    |
| Ports       |                                                       |        |
|   Standard  |                        0 / 0                          |  11    |
|   Bond      |                        0 / 0                          |  11    |
|   Other     |                        0 / 0                          |   6    |
| Sensors     |                                                       |        |
|   SSMs      |                        1 / 2   !                      |  11    |
|             |                                                       |        |
| Grade       |                       29 / 40  !                      |   -    |
-------------------------------------------------------------------------------
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
-------------------------------------------------------------------------------
>
```

Alert Modes

The Alert Modes are:

- **Enabled** - The system sends an alert for the selected events.
- **Disabled** - The system does not send alerts for the selected events.
- **Monitor** - The system generates a log entry instead of an alert.

Diagnostic Events

Best Practice - Run the `smo verifiers` (or the `show smo verifiers report`) command on a regular basis.

If the test fails, an alert shows. The alerts continue to show on Message of the Day (MOTD) until the issues resolve. When the issues resolve, a **Clear Alert** message shows the next time the test runs. You can manually run the `smo verifiers` (the `show smo verifiers report`) command to confirm the issue is resolved.

Important Notes

- By default, the tests run at 01h:00m each day.

  You can change the default time.

Step	Instructions
1	Edit the `$FWDIR/conf/asgsnmp.conf` file: `# vi $FWDIR/conf/asgsnmp.conf`
2	Change the value in this line: `asg_diag_alert_wrapper`
3	Copy this file to all other Security Group Members: `# asg_cp2blades $FWDIR/conf/asgsnmp.conf`

- By default, all tests run.

  You can exclude the tests you do not want.

  Note - When you manually run the `show smo verifiers report` command, the complete set of tests runs, even those you excluded.

Step	Instructions
1	Run: `# $FWDIR/conf/asg_diag_config`
2	Add this line to the file: `excluded_tests=[<Test1>] [,<Test2>,...]`
3	Copy this file to all other Security Group Members: `# asg_cp2blades $FWDIR/conf/asgsnmp.conf`

- All failed tests show in the MOTD.

  You can exclude failed test notifications from the MOTD

Step	Instructions
1	Run: `# $FWDIR/conf/asg_diag_config`
2	Set the `failed_tests_motd` parameter to `off`
3	Copy this file to all other Security Group Members: `# asg_cp2blades $FWDIR/conf/asg_diag_config`
4	Enforce the change. Run in Gaia gClish: `> show smo verifiers report` You can also wait for the next time the `smo verifiers` run automatically.

You can disable the MOTD feature

Step	Instructions
1	Edit the `$FWDIR/conf/asg_diag_config` file: `# vi $FWDIR/conf/asg_diag_config`
2	Set the value of the `motd` parameter to `off`.
3	Copy this file to all other Security Group Members: `# asg_cp2blades $FWDIR/conf/asg_diag_config`
4	Enforce the change. Run in Gaia gClish: `> show smo verifiers report` You can also wait for the next time the `smo verifiers` run automatically.

Known Limitations of the SMO Verifiers Test

By default, the `smo verifiers` only show a warning about resource mismatches between Security Group Members.

If the verification test results show as **Passed** in the output, no more steps are necessary.

You can change the default behavior

Step	Instructions
1	Edit the `$FWDIR/conf/asg_diag_config` file: `# vi $FWDIR/conf/asg_diag_config`
2	Search for **MismatchSeverity**.
3	Change the parameter to one of these values: ■ `fail` - Verification test result is set to **Failed** ■ `warn` - Verification test result is set to **Passed** and a warning shows ■ `ignore` - Verification test result is set to **Ignore** and no errors show

System Monitoring

This section describes features to monitor your system status.

Showing System Serial Numbers (asg_serial_info)

Description

The `asg_serial_info` command in Gaia gClish or the Expert mode shows the serial numbers of all the Security Group Members in the Security Group.

Syntax

```
asg_serial_info
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.

Example

```
[Expert@MyChassis-ch01-03:0]# asg_serial_info
Collecting SGMs information...
+-------------------------+
|     Serial numbers      |
+------------+------------+
| Chassis ID |     1      |
| SGM2       | 11xxxxxxxx |
| SGM3       | 12xxxxxxxx |
| SGM4       | 13xxxxxxxx |
+------------+------------+

[Expert@MyChassis-ch01-03:0]#
```

Showing the Security Group Version (ver)

Description

Use the `ver` command in Gaia gClish to show the Security Group software version.

Syntax

```
> ver
```

Example

```
[Global] MyChassis-ch01-01> ver
1_01:
Product version Check Point Gaia R80.30SP
OS build xxx
OS kernel version 3.10.0-693cpx86_64
OS edition 64-bit

1_02:
Product version Check Point Gaia R80.30SP
OS build xxx
OS kernel version 3.10.0-693cpx86_64
OS edition 64-bit

[Global] MyChassis-ch01-01>
```

Showing System Messages (show smo log)

Description

Use the `show smo log` command in Gaia gClish to show the output of log files aggregated from all Security Group Members.

The output shows in chronological sequence. Each line shows the Security Group Member that created the log entry.

Syntax

```
> show smo log <log file> [from <date>] [to <date>] [tail <n>]
[filter <string>]
```

Parameters

Parameter	Description
`tail <n>`	Show only the last `n` lines of the log file for each Security Group Member. For example, `tail 3` shows only the last three lines of the specified log file.
<log file>	Enter the name of the common log file or the full path of the file.
`from <date>`	Shows only the log from a given date and above.
`to <date>`	Shows only the log until the given date.
`filter <string>`	Word or phrase to use as an output filter. For example, `filter ospf` shows only OSPF messages.

Example

This example shows messages on Site 1 that contain the word `Restarted`:

```
[Expert@MyChassis-ch01-01:0]# gclish
[Global] MyChassis-ch01-01> show smo log messages filter Restarted
Feb  5 12:40:07 1_03 MyChassis-ch01-03 pm[8465]: Restarted /bin/routed[8489], count=1
Feb  5 12:40:09 1_04 MyChassis-ch01-04 pm[8449]: Restarted /bin/routed[9995], count=1
Feb  5 12:40:09 1_04 MyChassis-ch01-04 pm[8449]: Restarted /opt/CPsuite-R80.30/fw1/bin/cmd
[11291], count=1
Feb  5 12:40:09 1_04 MyChassis-ch01-04 pm[8449]: Restarted /usr/libexec/gexecd[11292],
count=1
Feb  5 12:40:10 1_03 MyChassis-ch01-03 pm[8465]: Restarted /usr/libexec/gexecd[9701], count=1
Feb  5 12:40:10 1_03 MyChassis-ch01-03 pm[8465]: Restarted /bin/routed[11328], count=2
Feb  5 12:40:10 1_05 MyChassis-ch01-05 pm[8458]: Restarted /bin/routed[9734], count=1
Feb  5 12:40:10 1_05 MyChassis-ch01-05 pm[8458]: Restarted /usr/libexec/gexecd[11331],
count=1
Feb  5 12:40:11 1_01 MyChassis-ch01-01 pm[8463]: Restarted /bin/routed[12253], count=3
Feb  5 12:40:11 1_04 MyChassis-ch01-04 pm[8449]: Restarted /bin/routed[11378], count=2
Feb  5 12:40:11 1_04 MyChassis-ch01-04 pm[8449]: Restarted /opt/CPsuite-R80.30/fw1/bin/cmd
[11379], count=2
[Global] MyChassis-ch01-01>
```

Configuring a Dedicated Logging Port

The logging mechanism lets each Security Group Member in Security Groups forward logs directly to a dedicated Log Server over the Quantum Maestro Orchestrator's management port assigned to this Security Group. However, the Quantum Maestro Orchestrator's management ports can experience a high load when Security Group Members generate a large number of logs.

To reduce the load on the Quantum Maestro Orchestrator's management ports:

1. Assign a dedicated Quantum Maestro Orchestrator port of type `management` to a Security Group for logging
2. Configure the Security Group to send the logs to the dedicated Log Server

Topology:

```
[Management Server](some interface) <===> (management port 1 on Quantum Maestro Orchestrator)[Security Group]
```

```
[Management Server](some interface) <===> (interface 1) [Log Server] (interface 2) <===> (management port 2 on Quantum Maestro Orchestrator)[Security Group]
```

Procedure:

Step	Instructions
1	Install a dedicated Log Server: a. Install a dedicated Log Server with two physical interfaces. See *Installation and Upgrade Guide* for your version - Chapter *Installing a Dedicated Log Server or SmartEvent Server.* b. Connect one physical interface on the dedicated Log Server to the Management Server. c. Connect another physical interface on the dedicated Log Server directly to an available management port on the Quantum Maestro Orchestrator. **Important** - Do *not* use the same port, which connects to the Management Server. d. In SmartConsole, create the required object that represents the dedicated Log Server. See *Installation and Upgrade Guide* for your version - Chapter *Installing a Dedicated Log Server or SmartEvent Server.*
2	On the Quantum Maestro Orchestrator, assign the dedicated port of type `management` to a Security Group and apply the changes.

Step	Instructions

3	In the Gaia OS of the Security Group, configure in Gaia gClish the dedicated management port.
	Syntax:
	`[Expert@MyChassis-ch01-01:0]# gclish`
	`[Global] MyChassis-ch01-01> set interface ethX-MgmtY ipv4-address <IPv4 Address> mask-length <Mask Length>`
	Example:
	`> set interface eth1-Mgmt2 ipv4-address 2.2.2.10 mask-length 24`
	Note - You muse assign an IPv4 address from the same subnet as assigned to the dedicated interface on the Log Server, which connects to the Quantum Maestro Orchestrator.

4	In SmartConsole, configure the Security Group object to send its logs to the dedicated Log Server. See *R80.30 Logging and Monitoring Administration Guide* - Chapter *Getting Started* - Section *Deploying Logging Section* - Subsection *Configuring the Security Gateways for Logging*.

Note - The SMO makes sure that return traffic from the Log Server reaches the correct Security Group Member in the Security Group.

Log Server Distribution (asg_log_servers)

Description

In SmartConsole, you can configure multiple Log Servers for each Security Gateway object.

In this environment, the Security Gateway sends its logs to all of its configured Log Servers.

Each Security Group Member sends its logs to all Log Servers in the configuration.

To reduce the load on the Log Servers, enable the distribution of different Log Servers to different Security Groups.

When enabled, each Security Group Member sends its logs to one Log Server only.

Note - You cannot configure the Security Group Member to send its logs to a specific Log Server. Distribution is automatic.
The Security Group automatically decides which Log Server is assigned to which Security Group Member.

Syntax

You can run this command in Gaia gClish or the Expert mode.

```
asg_log_servers
```

Example

```
[Expert@MyChassis-ch01-01:0]# asg_log_servers

+------------------------------------------------+
|             Log Servers Distribution           |
+------------------------------------------------+
Log Servers Distribution Mode: Disabled

Available Log Servers:
* logServer
* Gaia
* LogServer2

Logs will be sent to all available servers.

Choose one of the following options:
-----------------------------------
1) Configure Log Servers Distribution mode
2) Exit

 >1
+------------------------------------------------+
|             Log Servers Distribution           |
+------------------------------------------------+

Log Servers Distribution Mode: Disabled

Choose the desired option:
--------------------------
1) Enable Log Servers Distribution mode
2) Disable Log Servers Distribution mode
3) Back
```

If Log Servers Distribution is already enabled, the command shows which Log Servers are assigned to each Security Group Member:

```
+-----------------------------------------------+
|             Log Servers Distribution          |
+-----------------------------------------------+

Log Servers Distribution Mode: Enabled

Available Log Servers:
* LogServer
* Gaia
* LogServer2

Log Servers Distribution:

+-----------------------------------+
| Blade id |        Chassis 1       |
|-----------------------------------|
|    1     |  Gaia                  |
|    2     |  LogServer2            |
|    3     |  LogServer             |
|    4     |  Gaia                  |
|    5     |  -                     |
|    6     |  LogServer             |
|    7     |  -                     |
|    8     |  -                     |
|    9     |  LogServer             |
|    10    |  Gaia                  |
|    11    |  LogServer2            |
|    12    |  -                     |
+-----------------------------------+

("-" - Blade is not in Security Group)

Choose one of the following options:
-----------------------------------
1) Configure Log Servers Distribution mode
2) Exit
```

Command Auditing (asg log audit)

Use command auditing to:

- Notify users about critical actions they are about to do
- Obtain confirmation for critical actions
- Create forensic logs

If users confirm the action, it is necessary to supply their names and provide a reason for running the command.

If the command affects a critical device or a process (pnote) a second confirmation can be required.

For example, if you use administrative privileges to change the state of the Security Group Member to DOWN, the output looks like this:

```
# asg_sgm_admin -b 2_01 down
You are about to perform sgm_admin down on blades: 2_01

Are you sure? (y - yes, any other key - no) y

sgm_admin down requires auditing
Enter your full name: John Smith
Enter reason for sgm_admin down [Maintenance]: Maintenance
WARNING: sgm_admin down on SGM: 2_01, User: John Smith, Reason: Maintenance
```

To see the audit logs, run: `# asg log audit`

Example

```
# asg log audit
Aug 11 14:14:21 2_01 WARNING: Chassis admin-state up on chassis: 1, User: johnsmith, Reason:
Maintenance
Aug 11 16:45:15 2_01 WARNING: Reboot on blades: 1_01,1_02,1_03,1_04,1_05,2_02,2_03,2_04,2_05,
User: johnsmith, Reason: Maintenance
Aug 18 14:28:57 2_01 WARNING: Chassis admin-state down on chassis: 2, User: johnsmith,
Reason: Maintenance
Aug 18 14:31:08 2_01 WARNING: Chassis admin-state up on chassis: 1, User: Peter, Reason:
Maintenance
Aug 18 14:32:32 2_01 WARNING: Chassis admin-state down on chassis: 2, User: O, Reason:
Maintenance
Aug 20 15:38:58 2_01 WARNING: Blade_admin down on blades: 2_02,2_03,2_04,2_05, User: Paul,
Reason: Maintenance
Aug 21 10:00:05 2_01 CRITICAL: Reboot on blades: all, user: ms, Reason: Maintenance
#
```

Viewing a Log File (asg log)

Description

Use the `asg log` command to see the contents of a specified log file.

Syntax

```
# asg log [-b <SGM_IDs>] --file <log_name> [--from "<timestamp>"]
[--to "<timestamp>"] [--tail <n>] [--filter <string>]
```

Parameters

Parameter	Description
`-b <SGM_IDs>`	Applies to Security Group Members as specified by `<SGM_IDs>`. `<SGM_IDs>` can be: ■ No `<SGM_IDs>` specified, or `all` - Applies to all Security Group Members and Sites ■ One Security Group Member (for example, `1_1`) ■ A comma-separated list of Security Group Members (for example, `1_1,1_4`) ■ A range of Security Group Members (for example, `1_1-1_4`) ■ In Dual Site, one Site (`chassis1`, or `chassis2`) ■ In Dual Site, the Active Site (`chassis_active`)
`<log_name>`	Enter the log file: ■ `audit` - Shows the audit logs in `/var/log/` For example: `/var/log/asgaudit.log.1` ■ `ports` - Shows the ports logs in `/var/log/` For example: `/var/log/ports` ■ `dist_mode` - Shows the logs for Distribution Mode activity.
`--from "<timestamp>"`	Shows only the log from a given timestamp and above. You must use the timestamp as it appears in the log file.
`--to "<timestamp>"`	Shows only the log until the given timestamp. You must use the timestamp as it appears in the log file.

Parameter	Description
`--tail <n>`	Show only the last *n* lines of the log file for each Security Group Member. For example, `-tail 3` shows only the last three lines of the specified log file. Default = 10 lines.
`--filter <string>`	Word or phrase use as a filter. For example: `--filter debug`

Below are some examples:

Example 1 - Audit logs

```
# asg log --file audit
Feb 02 17:36:12 1_01  WARNING: Blade_admin up on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_
03,2_04,2_05, User: y, Reason: y
Feb 03 08:16:17 1_01  WARNING: Blade_admin down on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_
03,2_04,2_05, User: y, Reason: y
Feb 03 08:17:40 1_01  WARNING: Blade_admin up on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_
03,2_04,2_05, User: y, Reason: y
Feb 03 08:19:53 1_01  WARNING: Blade_admin down on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_
03,2_04,2_05, User: y, Reason: y
Feb 03 08:22:33 1_01  WARNING: Blade_admin up on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_
03,2_04,2_05, User: y, Reason: y
Feb 03 08:23:30 1_01  WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04_05,
User: y, Reason: y
Feb 03 08:38:16 1_01  WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_
05, User: y, Reason: y
Feb 03 09:21:09 1_01  WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_
05, User: y, Reason: y
Feb 03 11:07:08 1_01  WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_
05, User: y, Reason: y
Feb 03 11:16:56 1_01  WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 11:33:10 1_01  WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 11:50:08 1_01  WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 13:32:32 1_01  WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 14:30:26 1_01  WARNING: Reset sic on blades: all, User: johndoe, Reason: test
Feb 03 14:48:03 1_01  WARNING: Reset sic on blades: all, User: johndoe, Reason: test
Feb 03 15:34:11 1_01  WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 17:55:23 1_01  WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_
05, User: y, Reason: y
```

Example 2 - Port logs (last 12 lines)

```
# asg log --file ports -tail 12
Feb  3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-09 link is down
Feb  3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-10 link is down
Feb  3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-11 link is down
Feb  3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-12 link is down
Feb  3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-13 link is down
Feb  3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-14 link is down
Feb  3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-15 link is down
Feb  3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-16 link is down
Feb  3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-Mgmt1 link is down
Feb  3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-Mgmt2 link is down
Feb  3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-Mgmt3 link is down
Feb  3 18:01:40 2_05 MyChassis-ch02-05 cmd: Chassis 1 eth2-Mgmt4 link is down
```

Example 3 - Using a filter

```
# asg log -b 1_01,1_04 --file dist_mode -f bridge
Feb  2 18:10:30 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb  2 18:10:30 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-vsbridges =
4
Feb  2 18:12:31 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb  2 18:12:31 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-vsbridges =
4
Feb  2 18:14:14 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb  2 18:14:14 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-vsbridges =
4
Feb  2 18:14:30 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb  2 18:14:30 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-vsbridges =
4
Feb  2 18:16:19 1_01 MyChassis-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
```

Example 4 - Using a timestamp

```
# asg log --file /var/log/ports --from "Feb 21 17:28:41 2019" --to "Feb 21 17:28:41 2019"
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1,
interface: eth1-Mgmt1, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1,
interface: eth1-57, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1,
interface: eth1-59, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1,
interface: eth1-61, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1,
interface: eth1-63, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1,
interface: eth2-57, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1,
interface: eth2-59, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1,
interface: eth2-61, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Setting link state: chassis: 1,
interface: eth2-63, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02  MyChassis-ch01-02 cphaprob: Link state command ended successfully
```

Monitoring Virtual Systems (cpha_vsx_util monitor)

Description

Use the `cpha_vsx_util monitor` command in the Expert mode to stop or start monitoring of Virtual Systems.

The state of the Security Group Member is not affected by an unmonitored Virtual Systems. For example, an unmonitored Virtual System in problem state (pnote) is ignored. The Security Group Member state does change to DOWN.

A Virtual Systemthat is not monitored is useful, if you want the Security Group Member to be UP, even if a specific Virtual System is DOWN or does not have a Policy (for example, after you unload the local policy).

Syntax

```
# cpha_vsx_util monitor show
# cpha_vsx_util monitor {start | stop} <VS_IDs>
```

Parameters

Parameter	Description
`show`	Show all unmonitored Virtual Systems.
`stop`	Stop monitoring the Virtual Systemss.
`start`	Start monitoring the Virtual Systems.
<VS_IDs>	*<VS_IDs>* can be: ■ No *<VS_IDs>* specified (default) - Applies to the context of the current Virtual System ■ One Virtual System ■ A comma-separated list of Virtual Systems (for example, `1,2,4,5`) ■ A range of Virtual Systems (for example, `3-5`) ■ `all` - Shows all Virtual Systems

Important - When you stop Virtual System monitoring, you must run the `cpha_vsx_util monitor start` command to start it again. Monitoring does not start automatically after reboot.

Working with SNMP

You can use SNMP to monitor different aspects of Quantum Maestro Orchestrators and Security Groups.

Monitoring Quantum Maestro Orchestrators over SNMP

In This Section:

You can use SNMP to monitor different aspects of the Quantum Maestro Orchestrator:

- Software versions
- Key performance indicators

Note - Hardware monitoring is not supported..

Enabling SNMP Monitoring on Quantum Maestro Orchestrators

Step	Instructions
1	Upload these Check Point MIB files from the Quantum Maestro Orchestrator to your third-party SNMP monitoring software: ■ The SNMP MIB file: `$CPDIR/lib/snmp/chkpnt.mib` ■ The SNMP Trap MIB file: `$CPDIR/lib/snmp/chkpnt-trap.mib`
2	Connect to the command line on the Quantum Maestro Orchestrator.
3	Log in to Gaia Clish.

4	Enable the Gaia SNMP Agent:
	`> set snmp agent on`
	`> save config`

Supported SNMP OIDs for Quantum Maestro Orchestrators

Only these branches are supported:

Branch	OID	
svn	Numerical	.1.3.6.1.4.1.2620.1.6
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.svn
mngmt	Numerical	.1.3.6.1.4.1.2620.1.7
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.mngmt

Supported SNMP Trap OIDs for Quantum Maestro Orchestrators

Only these branches are supported:

Branch	OID	
chkpntTrapInfo	Numerical	.1.3.6.1.4.1.2620.1.2000.0
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapInfo
chkpntTrapNet	Numerical	.1.3.6.1.4.1.2620.1.2000.1
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapNet
chkpntTrapDisk	Numerical	.1.3.6.1.4.1.2620.1.2000.2
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapDisk

Branch	OID	
`chkpntTrapCPU`	Numerical	`.1.3.6.1.4.1.2620.1.2000.3`
	Full Text	`.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapCPU`
`chkpntTrapMemory`	Numerical	`.1.3.6.1.4.1.2620.1.2000.4`
	Full Text	`.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapMemory`

Notes:

- The `/etc/snmp/GaiaTrapsMIB.mib` file is not supported.
- The `set snmp traps` command is not supported.

Monitoring Security Groups over SNMP

In This Section:

You can use SNMP to monitor different aspects of the Security Group, including:

- Software versions
- Hardware status
- Key performance indicators
- High Availability status

Enabling SNMP Monitoring of Security Groups

Step	Instructions
1	Upload these Check Point MIB files from a Security Group Member in the applicable Security Group to your third-party SNMP monitoring software: ■ The SNMP MIB file: `$CPDIR/lib/snmp/chkpnt.mib` ■ The SNMP Trap MIB file: `$CPDIR/lib/snmp/chkpnt-trap.mib`
2	Connect to the command line on the Security Group.
3	Log in to Gaia gClish.

4	Enable the Gaia SNMP Agent:
	`> set snmp agent on`
	`> save config`

Supported SNMP OIDs for Security Groups

Only this branches is supported:

Branch	OID	
`asg`	Numerical	`1.3.6.1.4.1.2620.1.48`
	Full Text	`.iso.org.dod.internet.private.enterprise.checkpoint.products.asg`

Supported SNMP Trap OIDs for Security Groups

Only this SNMP Trap is supported:

Branch	OID	
`asgTrap`	Numerical	`1.3.6.1.4.1.2620.1.2001`
	Full Text	`.iso.org.dod.internet.private.enterprise.checkpoint.products.asgTrap`

Notes:

- The `/etc/snmp/GaiaTrapsMIB.mib` file is not supported.
- The `set snmp traps` command is not supported. You must use the `asg alert` configuration wizard for this purpose. See *"Configuring Alerts for Security Group Member and Security Group Events (asg alert)" on page 142*.

SNMP Monitoring of Security Groups in VSX Mode

For more information, see the:

- *R80.30SP Quantum Maestro Gaia Administration Guide*
- *R80.30SP Quantum Maestro VSX Administration Guide*
- sk90860: How to configure SNMP on Gaia OS

Common SNMP OIDs for Security Groups

This table shows frequently used SNMP OIDs that are applicable to Security Groups:

Name	Type	Numerical OID	Comments
System Throughput	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.1 IPv6: .1.3.6.1.4.1.2620.1.48.21.1	
System Connection Rate (connections per second)	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.2 IPv6: .1.3.6.1.4.1.2620.1.48.21.2	
System Packet Rate (packet per second)	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.3 IPv6: .1.3.6.1.4.1.2620.1.48.21.3	
System Concurrent Connections	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.4 IPv6: .1.3.6.1.4.1.2620.1.48.21.4	
System Accelerated Connections Per Second	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.6 IPv6: .1.3.6.1.4.1.2620.1.48.21.6	
System non-accelerated Connections Per Second	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.7 IPv6: .1.3.6.1.4.1.2620.1.48.21.7	
System Accelerated Concurrent Connections	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.8 IPv6: .1.3.6.1.4.1.2620.1.48.21.8	
System Non-accelerated concurrent conn.	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.9 IPv6: .1.3.6.1.4.1.2620.1.48.21.9	

Name	Type	Numerical OID	Comments
System CPU load - average	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.10 IPv6: .1.3.6.1.4.1.2620.1.48.21.10	
System Acceleration CPU load - average	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.11 IPv6: .1.3.6.1.4.1.2620.1.48.21.11	
System FW instances load - average	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.14 IPv6: .1.3.6.1.4.1.2620.1.48.21.14	
System VPN Throughput	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.17 IPv6: .1.3.6.1.4.1.2620.1.48.21.17	
System Path distribution (fast, medium, slow, drops)	Table	IPv4: .1.3.6.1.4.1.2620.1.48.20.24 IPv6: .1.3.6.1.4.1.2620.1.48.21.24	Path distribution of: ■ throughput ■ pps ■ cps ■ concurrent connections
Per-Security Group Member counters	Table	IPv4: .1.3.6.1.4.1.2620.1.48.20.25 IPv6: .1.3.6.1.4.1.2620.1.48.21.25	Counters of: ■ throughput ■ cps ■ pps ■ concurrent connections ■ SecureXL CPU usage (avg / min / max) ■ Firewall CPU usage (avg / min / max)

Name	Type	Numerical OID	Comments
Performance peaks	Table	IPv4: .1.3.6.1.4.1.2620.1.48.20.26 IPv6: .1.3.6.1.4.1.2620.1.48.21.26	
Resources on every Security Group Member	Table	1.3.6.1.4.1.2620.1.48.23	Memory and Hard Disk utilization
CPU Utilization on every Security Group Member	Table	1.3.6.1.4.1.2620.1.48.29	

System Optimization

This section describes some optimization steps you can take.

Configuring Services to Synchronize After a Delay

Some TCP services (for example, HTTP) are characterized by connections with a very short duration. There is no point to synchronize these connections, because every synchronized connection consumes resources on the Security Group, and the connection is likely to have finished by the time an internal failover occurs.

For short-lived services, you can use the *Delayed Notifications* feature to delay telling the Security Group about a connection, so that the connection is only synchronized, if it still exists X seconds (by default, 3 seconds) after the connection was initiated. The Delayed Notifications feature requires SecureXL to be enabled on the Security Group (this is the default).

Notes:

- By default, a connection is synchronized to backup Security Group Members only if it exists for more than 3 seconds.
- Asymmetric connections are synchronized to backup Security Group Members on the Active Site, if according to the DXL calculation, the Client-to-Server connection and the Server-to-Client connection are passing through different Security Group Members.

To control the "Delayed Notifications" feature:

- To **enable** this feature (this is the default):
  1. Connect to the command line on the Security Group.
  2. Log in to the Expert mode.
  3. Run:
     - To enable temporarily in the current session, if you disabled it earlier (does not survive reboot):

       ```
       g_fw ctl set int fw_cluster_use_delay_sync 1
       ```

     - To enable permanently, if you disabled it earlier (survives reboot):

       ```
       g_update_conf_file fwkern.conf fw_cluster_use_delay_
       sync=1
       ```

- To **disable** this feature (this increases the CPU load):
  1. Connect to the command line on the Security Group.
  2. Log in to the Expert mode.
  3. Run:
     - To disable temporarily in the current session (does not survive reboot):

       ```
       g_fw ctl set int fw_cluster_use_delay_sync 0
       ```

     - To disable permanently (survives reboot):

       ```
       g_update_conf_file fw_cluster_use_delay_sync=0
       ```

To configure an applicable delay:

1. In SmartConsole, click **Objects > Object Explorer**.
2. In the left tree, click the small arrow on the left of the **Services** to expand this category.
3. In the left tree, select **TCP**.
4. Search for the applicable TCP service.
5. Double-click the applicable TCP service.
6. In the TCP service properties window, click **Advanced** page.
7. At the top, select **Override default settings**.

   On Domain Management Server, select **Override global domain settings**.
8. At the bottom, in the **Cluster and synchronization** section:
   a. Select **Synchronize connections on cluster if State Synchronization is enabled on the cluster**.
   b. Select **Start synchronizing**.
   c. Enter the applicable value.

   Important - This change applies to all policies that use this service.
9. Click **OK**.
10. Close the **Object Explorer**.
11. Publish the SmartConsole session.
12. Install the Access Control Policy on the Scalable Platform Security Gateway object.

Note - The Delayed Notifications setting in the service object is ignored, if Connection Templates are not offloaded by the Firewall to SecureXL. For additional information about the Connection Templates, see the *R80.30SP Quantum Maestro Performance Tuning Administration Guide*.

Firewall Connections Table Size for VSX Gateway

You can configure the limit for the Firewall Connections table on Virtual Systems:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Virtual System.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the Virtual System object.
4	From the left tree, click **Optimizations**.
5	On the **Optimizations** page, select **Manually** in the **Calculate the maximum limit for concurrent connections**.
6	Enter or select a value.
7	Click **OK**.
8	Install the Access Control Policy on the Virtual System object.

Forwarding specific inbound-connections to the SMO (asg_excp_conf)

You can configure the Security Group to forward specific inbound connections to the SMO Security Group Member.

Important:

- This command supports only IPv4 connections.
- This command does not support local outgoing connections that the Security Group initiates.
- In VSX mode, you must run this command in the context of the applicable Virtual System.
- This command supports a maximum of 15 exceptions (in VSX mode, this limit is global for all Virtual Systems).
- These exceptions are saved in the `$FWDIR/tmp/tmp_exception_entries.txt` file (IPv4 addresses are converted to a special format).

Syntax

```
asg_excp_conf
      clear
      del <ID>
      get
      set <type> <src_ip> <sport> <dst_ip> <dport>
```

Parameters

Parameter	Description
`clear`	Clears the table with all exception entries.
`del <ID>`	Deletes a specific exception entry by its ID. Use the "`get`" parameter to see the IDs. ID numbers start from 0 (zero).
`get`	Shows the table with all exception entries.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><code>set <type> <src_ip> <sport> <dst_ip> <dport></code></td><td>
Configures a new exception entry.
Notes:

This command does not support wildcard characters (<code>*</code> or <code>?</code>) or the word "<code>any</code>".
You must always configure the exact values of the connection 4-tuple.
The order of these arguments is predefined (for example, "<code><src_ip></code>" is always the second argument).

Arguments:

<code><type></code>
Configures the match condition - which connection parameters the Security Group must consider.
Although you configure all connection parameters, the Security Group uses only specific parameters determined by the <code><type></code> value.
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>1</td><td>Match the inbound connection by the source IPv4 address only</td></tr>
<tr><td>2</td><td>Match the inbound connection by the destination IPv4 address only</td></tr>
<tr><td>3</td><td>Match the inbound connection by the source port only</td></tr>
<tr><td>4</td><td>Match the inbound connection by the destination port only</td></tr>
<tr><td>5</td><td>Match the inbound connection by all these parameters:
source IPv4 address
destination IPv4 address</td></tr>
<tr><td>6</td><td>Match the inbound connection by all these parameters:
source IPv4 address
source port</td></tr>
</table>

</td></tr>
</table>

Parameter	Description
	<table><tr><th>Value</th><th>Description</th></tr><tr><td>7</td><td>Match the inbound connection by all these parameters: - source IPv4 address - destination port </td></tr><tr><td>8</td><td>Match the inbound connection by all these parameters: - source port - destination IPv4 address </td></tr><tr><td>9</td><td>Match the inbound connection by all these parameters: - destination IPv4 address - destination port </td></tr><tr><td>10</td><td>Match the inbound connection by all these parameters: - source port - destination port </td></tr><tr><td>11</td><td>Match the inbound connection by all these parameters: - source IPv4 address - source port - destination IPv4 address </td></tr><tr><td>12</td><td>Match the inbound connection by all these parameters: - source IPv4 address - destination IPv4 address - destination port </td></tr><tr><td>13</td><td>Match the inbound connection by all these parameters: - source IPv4 address - source port - destination port </td></tr></table>

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>14</td><td>Match the inbound connection by by all these parameters:
source port
destination IPv4 address
destination port</td></tr>
<tr><td>15</td><td>Match the inbound connection by all these parameters:
source IPv4 address
source port
destination IPv4 address
destination port</td></tr>
</table>

<src_ip>
Configures the Source IPv4 address
<sport>
Configures the Source port
<dst_ip>
Configures the Destination IPv4 address
<dport>
Configures the Destination port

</td></tr>
</table>

Examples

asg_excp_conf set

```
[Expert@HostName-ch0x-0x:0] asg_excp_conf set 2 192.168.20.30
40000 172.16.40.50 80
1_01:
Exception entry added successfuly.
1_02:
Exception entry added successfuly.
1_03:
Exception entry added successfuly.
1_04:
Exception entry added successfuly.
2_01:
Exception entry added successfuly.
2_02:
Exception entry added successfuly.
2_03:
Exception entry added successfuly.
2_04:
Exception entry added successfuly.
[Expert@HostName-ch0x-0x:0]
```

asg_excp_conf get

```
[Expert@HostName-ch0x-0x:0] asg_excp_conf get
1_01:
-------------------------------------------------
Exceptions table: ---------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
-------------------------------------------------------------
-------------------------------------------------------------
1_02:
-------------------------------------------------
Exceptions table: ---------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
-------------------------------------------------------------
-------------------------------------------------------------
1_03:
-------------------------------------------------
Exceptions table: ---------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
-------------------------------------------------------------
-------------------------------------------------------------
1_04:
-------------------------------------------------
Exceptions table: ---------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
-------------------------------------------------------------
-------------------------------------------------------------
2_01:
-------------------------------------------------
Exceptions table: ---------------------------------------------
```

```
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
------------------------------------------------------------------
------------------------------------------------------------------
2_02:
--------------------------------------------------
Exceptions table: ------------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
------------------------------------------------------------------
------------------------------------------------------------------
2_03:
--------------------------------------------------
Exceptions table: ------------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
------------------------------------------------------------------
------------------------------------------------------------------
2_04:
--------------------------------------------------
Exceptions table: ------------------------------------------------
--------
0 : Exception Type 2 , Source IP: 192.168.20.30  , Source Port:
40000 , Destination IP: 172.16.40.50    Destination Port     80
1 : Exception Type 4 , Source IP: 192.168.20.30  , Source Port:
50000 , Destination IP: 172.16.40.50    Destination Port   8080
------------------------------------------------------------------
------------------------------------------------------------------
[Expert@HostName-ch0x-0x:0]
```

asg_excp_conf del

```
[Expert@HostName-ch0x-0x:0]# asg_excp_conf del 0
1_01:
Exception ID 0 deleted
1_02:
Exception ID 0 deleted
1_03:
Exception ID 0 deleted
1_04:
Exception ID 0 deleted
2_01:
Exception ID 0 deleted
2_02:
Exception ID 0 deleted
2_03:
Exception ID 0 deleted
2_04:
Exception ID 0 deleted
[Expert@HostName-ch0x-0x:0]
```

asg_excp_conf clear

```
[Expert@HostName-ch0x-0x:0] asg_excp_conf clear
1_01:
Exception table cleared
1_02:
Exception table cleared
1_03:
Exception table cleared
1_04:
Exception table cleared
2_01:
Exception table cleared
2_02:
Exception table cleared
2_03:
Exception table cleared
2_04:
Exception table cleared
[Expert@HostName-ch0x-0x:0]
```

Installing and Uninstalling a Hotfix

This section provides instructions for installing and uninstalling a Hotfix:

- On Quantum Maestro Orchestrators

  See *"Installing and Uninstalling a Hotfix on Quantum Maestro Orchestrators" below*

- On Security Group Members

  See *"Installing and Uninstalling a Hotfix on Security Group Members" on page 204*

Installing and Uninstalling a Hotfix on Quantum Maestro Orchestrators

In This Section:

You use the **CPUSE** on each Quantum Maestro Orchestrator to install the applicable hotfixes.

Important:

- **It is *not* supported to upgrade the CPUSE Agent on Quantum Maestro Orchestrators.**
- For the **CPUSE** instructions, see sk92449.
- Jumbo Hotfix Accumulator reboots Quantum Maestro Orchestrator after installation or uninstall.
- Quantum Maestro Orchestrator stops processing traffic from the start of Jumbo Hotfix Accumulator installation or uninstall and until Quantum Maestro Orchestrator comes up from the reboot.
- You must install the same Take of Jumbo Hotfix Accumulator on all Quantum Maestro Orchestrators.

Installing a Hotfix Package on Orchestrators

Internet Connection	Installation Methods	Action Plan
Quantum Maestro Orchestrator **is** connected to the Internet	You can perform only an offline installation.	See the instructions for a Quantum Maestro Orchestrator that is **not** connected to the Internet.

Internet Connection	Installation Methods	Action Plan
Quantum Maestro Orchestrator is **not** connected to the Internet	You can perform only an offline installation.	**To install CPUSE packages in Gaia Portal** 1. Use the computer, from which you connect to Gaia Portal on Quantum Maestro Orchestrator. 2. Download the applicable CPUSE Software Packages from the *Check Point Support Center*. 3. Connect to Gaia Portal on each Quantum Maestro Orchestrator. 4. Import the applicable CPUSE Software Packages. 5. Verify the applicable CPUSE Software Packages. 6. Install the applicable CPUSE Software Packages. **To install CPUSE packages in Gaia Clish** 1. Use the computer, from which you connect to Gaia Clish on Quantum Maestro Orchestrator. 2. Download the applicable CPUSE Software Packages from the *Check Point Support Center*. 3. Transfer the applicable CPUSE Offline Software Packages to each Quantum Maestro Orchestrator to some directory (for example, `/var/log/path_to_CPUSE_packages/`). Make sure to transfer the CPUSE packages in the binary mode. 4. Connect to the command line on each Quantum Maestro Orchestrator and log in to Gaia Clish. 5. Import the applicable CPUSE Software Packages. 6. Verify the applicable CPUSE Software Packages. 7. Install the applicable CPUSE Software Packages.

Uninstalling a Hotfix Package on Orchestrators

To uninstall CPUSE packages in Gaia Portal

1. Connect to Gaia Portal on each Quantum Maestro Orchestrator.
2. Select and uninstall the applicable CPUSE Software Packages.

To uninstall CPUSE packages in Gaia Clish

1. Connect to the command line on each Quantum Maestro Orchestrator and log in to Gaia Clish.
2. Uninstall the applicable CPUSE Software Packages.

Deleting a Hotfix Package on Orchestrators

This section applies to a hotfix package that exists on the Quantum Maestro Orchestrator, but is not installed.

To delete CPUSE packages in Gaia Portal

1. Connect to Gaia Portal on each Quantum Maestro Orchestrator.
2. Select and delete the applicable CPUSE Software Packages.

To delete CPUSE packages in Gaia Clish

1. Connect to the command line on each Quantum Maestro Orchestrator and log in to Gaia Clish.
2. Delete the applicable CPUSE Software Packages.

Installing and Uninstalling a Hotfix on Security Group Members

In This Section:

This section describes the Full Connectivity installation and uninstall of an Offline CPUSE package.

Installing a Hotfix Package

Important:

- **It is not supported to upgrade the CPUSE Agent on Security Group Members.**
- This procedure keeps the current connections in a Security Group.
- This procedure applies to Security Groups in both Security Gateway and VSX mode.
  In VSX mode, you must run all the commands in the context of VS0.
- **Do not install the hotfix on all the Security Group Members in a specific Security Group at the same time.**
- In this procedure, you divide all Security Group Members in a specific Security Group into two or more logical groups.
  In the procedure below, we use **two** logical groups denoted below as "**A**" and "**B**".
  You install the hotfix on one logical group of the Security Group Members at one time.
  The other logical group(s) of the Security Group Members continues to handle traffic.
  Each logical group should contain the same number of Security Group Members - as close as possible.

  Examples

Environment	Description
Single Site	• There are 8 Security Group Members in the Security Group. • The Logical Group "A" contains Security Group Members from 1_1 to 1_4. • The Logical Group "B" contains Security Group Members from 1_5 to 1_8.
Single Site	• There are 5 Security Group Members in the Security Group. • The Logical Group "A" contains Security Group Members from 1_1 to 1_3. • The Logical Group "B" contains Security Group Members from 1_4 to 1_5.
Dual Site	• There are 4 Security Group Members in the Security Group (on each Site). • The Logical Group "A" contains Security Group Members on Site 1 from 1_1 to 1_4. • The Logical Group "B" contains Security Group Members on Site 2 from 2_1 to 2_4.

Installation Procedure

Step 1 - Perform the preliminary steps

For Offline CPUSE packages

Follow these steps if Security Group Members are **not** connected to the Internet or cannot reach Check Point Cloud.

Step	Instructions
A	Make sure you have the applicable CPUSE Offline package (TGZ file) / exported package (TAR file).
B	Transfer the CPUSE Offline package to the Security Group (into some directory, for example `/var/log/`).
C	Connect to the command line on the Security Group.
D	Go to the Gaia gClish: `gclish`

E	Import the CPUSE Offline package from the hard disk:
	`installer import local /<Full Path>/<Name of the CPUSE Offline Package>`
	Example:
	`[Global] MyChassis-ch01-01 > installer import local /var/log/Check_Point_R80.30SP_Hotfix_Bundle_FULL.tgz`

F	Show the imported CPUSE packages: `show installer packages imported`

Step	Instructions

G	Make sure the imported CPUSE package can be installed on this Security Group:
	`installer verify`*`[Press Tab]`*
	`installer verify <`*`Number of CPUSE Package`*`> member_ids all`
	Example:
	`[Global] MyChassis-ch01-01 > installer verify 2 member_ids all`
	`... ...`
	`Update Service Engine`
	`+-----------------------------------------------------------+`
	`|Member ID  |Status                                                 |`
	`+-----------------------------------------------------------+`
	`|1_01 (local) |Installation is allowed.                        |`
	`|1_02         |Installation is allowed.                        |`
	`|1_03         |Installation is allowed.                        |`
	`|1_04         |Installation is allowed.                        |`
	`|1_05         |Installation is allowed.                        |`
	`|1_06         |Installation is allowed.                        |`
	`|1_07         |Installation is allowed.                        |`
	`|1_08         |Installation is allowed.                        |`
	`+-----------------------------------------------------------+`
	`[Global] MyChassis-ch01-01 >`

Step 2 - On the Security Group, make sure to disable the SMO Image Cloning feature

Note - The SMO Image Cloning feature automatically clones all the required software packages to the Security Group Members during their boot. When you install or remove software packages gradually on Security Group Members, it is necessary to disable this feature, so that after a reboot the updated Security Group Members do not clone the software packages from the existing non-updated Security Group Members.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is `/bin/bash` (Expert mode), then go to Gaia gClish: `gclish`
C	Examine the state of the SMO Image Cloning feature: `show smo image auto-clone state`
D	Disable the SMO Image Cloning feature, if it is enabled: `set smo image auto-clone state off`
E	Examine the state of the SMO Image Cloning feature: `show smo image auto-clone state`

Step 3 - Install the Hotfix on the Security Group Members in the Logical Group "A"

Note - You are still connected to the command line on the Security Group.

Step	Instructions
A	Go to the Expert mode.

B	Set Security Group Members in the Logical Group "A" to the "down" state:
	`g_clusterXL_admin -b <SGM IDs in Group "A"> down`
	Example:
	`[Expert@MyChassis-ch0x-0x:0]# g_clusterXL_admin -b 1_1-1_4 down`

C	Connect to one of the Security Group Members in the Logical Group "A": `member <Member ID>`
D	Go to the Gaia gClish: `gclish`

E	Install the CPUSE hotfix package on the Security Group Members in the Logical Group "A":
	`installer install[Press Tab]`
	`installer install <Number of CPUSE Package> member_ids <SGM IDs in Group "A">`
	Example:
	`[Global] MyChassis-ch01-01 > installer install 2 member_ids 1_1-1_4`
	`... ...`
	`Update Service Engine`
	`+-----------------------------------------------------------+`
	`|Member ID  |Status  |`
	`+-----------------------------------------------------------+`
	`|1_01 (local) |Package is ready for installation  |`
	`|1_02  |Package is ready for installation  |`
	`|1_03  |Package is ready for installation  |`
	`|1_04  |Package is ready for installation  |`
	`+-----------------------------------------------------------+`
	`The machines (1_02,1_02,1_03,1_04) will automatically reboot after install.`
	`Do you want to continue? ([y]es / [n]o) y`
	`[Global] MyChassis-ch01-01 >`

F	Go to the Expert mode.
G	Monitor the system until the Security Group Members in the Logical Group "A" are in the UP state and enforce the Security Policy again: `asg monitor`

Step 4 - Install the Hotfix on the Security Group Members in the Logical Group "B"

Note - You are still connected to the command line on the Security Group.

Step	Instructions
A	Go to the Expert mode.

B	Set Security Group Members in the Logical Group "B" to the "down" state:
	`g_clusterXL_admin -b <SGM IDs in Group "B"> down`
	Example:
	`[Expert@MyChassis-ch0x-0x:0]# g_clusterXL_admin -b 1_5-1_8 down`

C	Connect to one of the Security Group Members in the Logical Group "B": `member <Member ID>`
D	Go to the Gaia gClish: `gclish`

E	Install the CPUSE hotfix package on the Security Group Members in the Logical Group "B":
	`installer install[Press Tab]`
	`installer install <Number of CPUSE Package> member_ids <SGM IDs in Group "B">`
	Example:
	`[Global] MyChassis-ch01-01 > installer install 2 member_ids 1_5-1_8`
	`... ...`
	`Update Service Engine`
	`+-----------------------------------------------------------+`
	`|Member ID  |Status  |`
	`+-----------------------------------------------------------+`
	`|1_05 (local) |Package is ready for installation  |`
	`|1_06  |Package is ready for installation  |`
	`|1_07  |Package is ready for installation  |`
	`|1_08  |Package is ready for installation  |`
	`+-----------------------------------------------------------+`
	`The machines (1_05,1_06,1_07,1_08) will automatically reboot after install.`
	`Do you want to continue? ([y]es / [n]o) y`
	`[Global] MyChassis-ch01-01 >`

F	Go to the Expert mode.
G	Monitor the system until the Security Group Members in the Logical Group "A" are in the UP state and enforce the security policy again: `asg monitor`

Step 5 - Make sure the Hotfix is installed on all Security Group Members

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is `/etc/cli.sh` (Gaia Clish), then go to the Expert mode: `expert`
C	Run: `asg diag verify`

Uninstalling a Hotfix Package on Security Group Members

Important:

- **It is not supported to upgrade the CPUSE Agent on Security Group Members.**
- This procedure keeps the current connections in a Security Group.
- This procedure applies to Security Groups in both Security Gateway and VSX mode.
  In VSX mode, you must run all the commands in the context of VS0.
- **Do not uninstall the hotfix from all the Security Group Members in a specific Security Group at the same time.**
- You uninstall the hotfix from one logical group of the Security Group Members at one time.
  The other logical group of the Security Group Members continues to handle traffic.
  You divide all Security Group Members in a specific Security Group into two logical groups - denoted below as "**A**" and "**B**".
  1. You uninstall the hotfix from the Security Group Members in the Logical Group "A"
  2. You uninstall the hotfix from the Security Group Members in the Logical Group "B"

  Each logical group should contain the same number of Security Group Members - as close as possible.

  Examples

Environment	Description
Single Site	• There are 8 Security Group Members in the Security Group. • The Logical Group "A" contains Security Group Members from 1_1 to 1_4. • The Logical Group "B" contains Security Group Members from 1_5 to 1_8.
Single Site	• There are 5 Security Group Members in the Security Group. • The Logical Group "A" contains Security Group Members from 1_1 to 1_3. • The Logical Group "B" contains Security Group Members from 1_4 to 1_5.
Dual Site	• There are 4 Security Group Members in the Security Group (on each Site). • The Logical Group "A" contains Security Group Members on Site 1 from 1_1 to 1_4. • The Logical Group "B" contains Security Group Members on Site 2 from 2_1 to 2_4.

Uninstall Procedure

Step 1 - On the Security Group, make sure to disable the SMO Image Cloning feature

Note - The SMO Image Cloning feature automatically clones all the required software packages to the Security Group Members during their boot. When you install or remove software packages gradually on Security Group Members, it is necessary to disable this feature, so that after a reboot the updated Security Group Members do not clone the software packages from the existing non-updated Security Group Members.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is `/bin/bash` (Expert mode), then go to Gaia gClish: `gclish`
C	Examine the state of the SMO Image Cloning feature: `show smo image auto-clone state`
D	Disable the SMO Image Cloning feature, if it is enabled: `set smo image auto-clone state off`
E	Examine the state of the SMO Image Cloning feature: `show smo image auto-clone state`

Step 2 - Uninstall the Hotfix from the Security Group Members in the Logical Group "A"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group "**A**" **through the console**. ■ Connect to one of the Security Group Members in the Logical Group "**B**" **over SSH**.
B	Go to the Expert mode.

C	Set Security Group Members in the Logical Group "A" to the state "`DOWN`":
	`g_clusterXL_admin -b <SGM IDs in Group "A"> down`
	Example:
	`[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_1-1_4 down`

D	Connect to one of the Security Group Members in the Logical Group "A": `member <Member ID>`

E	Go from the Expert mode to Gaia gClish:
	■ If your default shell is `/bin/bash` (the Expert mode), then run:
	`gclish`
	■ If your default shell is `/etc/cli.sh` (Gaia Clish), then run:
	`exit`

Step	Instructions

F	Uninstall the CPUSE hotfix package on the Security Group Members in the Logical Group "A":
	`installer uninstall [Press the Tab key]`
	`installer uninstall <Number of CPUSE Package> member_ids <SGM IDs in Group "A">`
	Example:
	`[Global] HostName-ch01-01 > installer uninstall 2 member_ids 1_1-1_4`
	`... ...`
	`Update Service Engine`
	`+-----------------------------------------------------------+`
	`|Member ID  |Status                                          |`
	`+-------------+-----------------------------------------------+`
	`|1_01 (local) |Package is ready for uninstallation          |`
	`|1_02         |Package is ready for uninstallation          |`
	`|1_03         |Package is ready for uninstallation          |`
	`|1_04         |Package is ready for uninstallation          |`
	`+-------------+-----------------------------------------------+`
	`The machines (1_02,1_02,1_03,1_04) will automatically reboot after uninstall.`
	`Do you want to continue? ([y]es / [n]o) y`
	`[Global] HostName-ch01-01 >`

G	Go from Gaia gClish to the Expert mode:
	■ If your default shell is `/bin/bash` (the Expert mode), then run:
	`exit`
	■ If your default shell is `/etc/cli.sh` (Gaia Clish), then run:
	`expert`

H	Monitor the system until the Security Group Members in the Logical Group "A" are in the state "`UP`" and enforce the Security Policy again: `asg monitor`

Step 3 - Uninstall the Hotfix from the Security Group Members in the Logical Group "B"

Step	Instructions
A	Connect in one of these ways: ■ Connect to one of the Security Group Members in the Logical Group "**B**" **through the console**. ■ Connect to one of the Security Group Members in the Logical Group "**A**" **over SSH**.
B	Go to the Expert mode: `expert`

C	Set Security Group Members in the Logical Group "B" to the state "`DOWN`":
	`g_clusterXL_admin -b <SGM IDs in Group "B"> down`
	Example:
	`[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_5-1_8 down`

D	Connect to one of the Security Group Members in the Logical Group "A": `member <Member ID>`

E	Go from the Expert mode to Gaia gClish:
	■ If your default shell is `/bin/bash` (the Expert mode), then run:
	`gclish`
	■ If your default shell is `/etc/cli.sh` (Gaia Clish), then run:
	`exit`

Step	Instructions

F	Uninstall the CPUSE hotfix package on the Security Group Members in the Logical Group "B":
	`installer uninstall [Press the Tab key]`
	`installer uninstall <Number of CPUSE Package> member_ids <SGM IDs in Group "B">`
	Example:
	`[Global] HostName-ch01-01 > installer uninstall 2 member_ids 1_5-1_8`
	`... ...`
	`Update Service Engine`
	`+-----------------------------------------------------------+`
	`|Member ID |Status |`
	`+-----------------------------------------------------------+`
	`|1_05 (local) |Package is ready for uninstallation |`
	`|1_06 |Package is ready for uninstallation |`
	`|1_07 |Package is ready for uninstallation |`
	`|1_08 |Package is ready for uninstallation |`
	`+-----------------------------------------------------------+`
	`The machines (1_05,1_06,1_07,1_08) will automatically reboot after uninstall.`
	`Do you want to continue? ([y]es / [n]o) y`
	`[Global] HostName-ch01-01 >`

G	Go from Gaia gClish to the Expert mode:
	■ If your default shell is `/bin/bash` (the Expert mode), then run:
	`exit`
	■ If your default shell is `/etc/cli.sh` (Gaia Clish), then run:
	`expert`

H	Monitor the system until the Security Group Members in the Logical Group "A" are in the state "`UP`" and enforce the Security Policy again: `asg monitor`

Step 4 - Make sure the Hotfix is uninstalled from all Security Group Members

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is `/etc/cli.sh` (Gaia Clish), then go to the Expert mode: `expert`
C	Run: `asg diag verify`

Troubleshooting

This section provides troubleshooting commands.

Collecting System Information (asg_info)

Best Practice - Use the more advanced tool Check Point Support Data Collector (CPSDC) as described in sk164414.

Description

Use the `asg_info` command in Gaia gClish or the Expert mode to collect information from the systems that generate data files and command line output.

The `asg_info` command collects the information from these areas:

- Log files
- Configuration files
- System status
- System diagnostics

The `asg_info` command saves the collected information in the `/var/log/asg_info.<hostname>.<date>.tar` file.

By default, this command collects the information from all Security Group Members and Virtual Systems.

Granularity of Commands

The `asg_info` command in Gaia gClish or the Expert mode executes the applicable commands with this granularity:

Source	Granularity
Security Group Members	■ All Security Group Members ■ Single Security Group Member ■ Specified Security Group Members
VSX	■ For each Virtual System ■ VS0 only ■ Specified Virtual Systems

Collected Files

The `asg_info` command collects a predefined list of files from the Security Group Member and Virtual Systems. A global file is located in the global folder.

Examples:

1. The `latest_policy.policy.tgz` file:
   - Collected as a global file
   - Located in `\global\VS0\var\CPbackup\asg_backup\`
2. The `dist_mode.log` file:
   - Collected from the Security Group Member and Virtual Systems folders
   - Located in `\SGM_1_01\VS1\var\log\`
3. The `start_mbs.log` file:
   - Collected from the Security Group Member folder and not from the Virtual Systems folders
   - Located in `\SGM_1_01\VS0\var\log\`

Syntax

```
asg_info -h
```

```
asg_info [-b <SGM_IDs>] [--vs <VS_IDs>] <collect_flags> [options]
```

```
asg_info [-b <SGM_IDs>] [--vs <VS_IDs>] [--user_conf <xml_filename>] [options]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><code>-b <<i>SGM_IDs</i>></code></td><td>Applies to Security Group Members as specified by <code><<i>SGM_IDs</i>></code>.
<code><<i>SGM_IDs</i>></code> can be:
No <code><<i>SGM_IDs</i></code> > specified, or <code>all</code> - Applies to all Security Group Members and Sites
One Security Group Member (for example, <code>1_1</code>)
A comma-separated list of Security Group Members (for example, <code>1_1,1_4</code>)
A range of Security Group Members (for example, <code>1_1-1_4</code>)
In Dual Site, one Site (<code>chassis1</code>, or <code>chassis2</code>)
In Dual Site, the Active Site (<code>chassis_active</code>)
Default - Runs on all Security Group Members that are in the UP state.</td></tr>
<tr><td><code>-vs <<i>VS_IDs</i>></code></td><td><i><VS_IDs></i> can be:
No <code><<i>VS_IDs</i>></code> specified (default) - Applies to the context of the current Virtual System
One Virtual System
A comma-separated list of Virtual Systems (for example, <code>1,2,4,5</code>)
A range of Virtual Systems (for example, <code>3-5</code>)
<code>all</code> - Shows all Virtual Systems
Note - This parameter is only applicable in a VSX environment.</td></tr>
<tr><td><code><<i>collect_flags</i>></code></td><td>The collect flags are:<table><tr><th>Flag</th><th>Description</th></tr><tr><td><code>--all</code></td><td>Collects all log files and command outputs.</td></tr><tr><td><code>-a</code></td><td>Collects archive files.</td></tr><tr><td><code>-c</code></td><td>Collects information about core dump files.</td></tr><tr><td><code>-f</code></td><td>Collects comprehensive log files and command outputs.</td></tr><tr><td><code>-i</code></td><td>Collects the <code>cpinfo</code> output.</td></tr><tr><td><code>-m | --cmm</code></td><td>Not supported.</td></tr><tr><td><code>-q</code></td><td>Collects major log files and command outputs.</td></tr><tr><td><code>--user_conf</code></td><td>Adds the specified XML configuration file.</td></tr></table></td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><code>options</code></td><td>The options are:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><code>-h</code></td><td>Shows the built-in help.</td></tr>
<tr><td><code>-e <<i>Email_1;...;Email_N</i>></code></td><td>Semicolon separated list of email addresses for upload notifications.</td></tr>
<tr><td><code>schedule</code></td><td>Specifies the periodic schedule to upload report to the Check Point User Center.
Notes:
This option must be the first or the last in the list of options.
This option asks to select the schedule (Daily, Weekly, or Monthly).
This option requires a valid CK (see the output of the <code>cplic print</code> command).
To see and delete the configured periodic jobs, run:
<code>asg_info schedule</code></td></tr>
<tr><td><code>-u</code></td><td>Interactive upload of the <code>asg_info</code> output file to the Check Point User Center.</td></tr>
<tr><td><code>-uk</code></td><td>Non-interactive upload of the <code>asg_info</code> output file to the Check Point User Center.
This option requires a valid CK (see the output of the <code>cplic print</code> command).</td></tr>
<tr><td><code>-v</code></td><td>Shows verbose output.</td></tr>
<tr><td><code>--list</code></td><td>Dry run - shows all the files and command outputs to be collected without actually collecting them.</td></tr>
</table></td></tr>
</table>

Configuration Files

File	Description
Default	`$FWDIR/conf/asg_info_config.xml` Files and commands are defined automatically.
User defined	The user can define files and commands based on the same standard as appears in the default file.

Note - You can run the `asg_info` command either with the default file, or with the user-defined file. Not both files.

Example of a user-defined XML configuration file:

```
<configurations>
      <collect_file_list>
            <upgrade_wizard>
                  <collect_mode>-f</collect_mode>
                  <path>/var/log/upgrade_wizard.log*</path>
                  <per_vs>0</per_vs>
                  <per_sgm>1</per_sgm>
                  <delete_after_collect>0</delete_after_collect>
            </upgrade_wizard>
            <active_cmm_debug>
                  <collect_mode>-m</collect_mode>
                  <path>/var/log/active_cmm_debug.log</path>
                  <per_vs>0</per_vs>
                  <per_sgm>1</per_sgm>
                  <delete_after_collect>1</delete_after_collect>
            </active_cmm_debug>
      </collect_file_list>
<cmd_list>
            <asg_if>
                  <mode>-f</mode>
                  <pre_command>g_all</pre_command>
                  <command>asg if</command>
                  <ipv6>0</ipv6>
                  <esx>1</esx>
                  <per_chassis>0</per_chassis>
                  <per_vs>1</per_vs>
                  <per_sgm>0</per_sgm>
                  <vsx_only>0</vsx_only>
                  <dest_file_name>asg_info</dest_file_name>
            </asg_if>
</cmd_list>
</configurations>
```

General Diagnostic in Security Groups

Based on the OSI model, you can run these commands:

Layer Number	Layer Name	Recommended Diagnostic Commands
7	Application	N / A

6	Presentation	■ For information about the Firewall drops, run this command in the Expert mode:
		`drop_monitor`
		See *"Packet Drop Monitoring (asg_drop_monitor)" on page 124*
		■ For information about the Firewall drops, run this command in the Expert mode:
		`g_fw ctl zdebug + drop`
		■ For information about the Software Blade Updates, run this command in the Expert mode:
		`asg_swb_update_verifier`
		See *"Collecting System Diagnostics (smo verifiers)" on page 146*
		■ Examine the Security Gateway logs on the Management Server or Log Server

5	Session	■ For information about the Connections table, run this command in the Expert mode:
		`g_fw tab -t connections -s`
		■ For information about the Firewall drops, run this command in the Expert mode:
		`g_fw ctl zdebug + drop`
		■ For information about the performance, run this command in Gaia gClish or the Expert mode:
		`asg perf -v -p`
		See *"Monitoring Performance (asg perf)" on page 99*
		■ For information about the VSX mode, run this command:
		`asg perf -vs all -v --vvxxx`
		See *"Monitoring Performance (asg perf)" on page 99*

Layer Number	Layer Name	Recommended Diagnostic Commands
4	Transport	■ For information about the Correction Layer and traffic flow, use the `g_tcpdump` command in the Expert mode See *"Multi-blade Traffic Capture (tcpdump -mcap, tcpdump -view)" on page 95* ■ For information about the VPN, examine the Security Gateway logs on the Management Server or Log Server

Layer Number	Layer Name	Recommended Diagnostic Commands

3	Network	■ In the Expert mode, run these commands:
		• For information about the traffic:
		`asg_ifconfig`
		See *"Showing Traffic Information (asg_ifconfig)" on page 80*
		• For information about the routes:
		`asg_route`
		See *"Collecting System Diagnostics (smo verifiers)" on page 146*
		• For information about the routes:
		`asg_dr_verifier`
		See *"Collecting System Diagnostics (smo verifiers)" on page 146*
		• For information about the routes:
		`netstat -rn`
		• For information about the routes:
		`route`
		■ In Gaia gClish, run these commands:
		• For information about the traffic:
		`asg_ifconfig`
		See *"Showing Traffic Information (asg_ifconfig)" on page 80*
		• For information about the routes:
		`asg_route`
		See *"Collecting System Diagnostics (smo verifiers)" on page 146*
		• For information about the routes:
		`show route ...`

Layer Number	Layer Name	Recommended Diagnostic Commands

2	Data Link	■ For information about the Bond interfaces, run this command in Gaia gClish or the Expert mode:
		`asg_bond -v`
		See *"Showing Bond Interfaces (asg_bond)" on page 77*
		■ For information about the Bridge interfaces, run this command in Gaia gClish or the Expert mode:
		`asg_br_verifier`
		See *"Layer 2 Bridge Verifier (asg_br_verifier, asg_brs_verifier)" on page 232*

1	Physical	■ Run this command in Gaia gClish:
		`show maestro port <Port>`
		■ For information about the Bond interfaces, run this command in the Expert mode:
		`cat /proc/net/bonding/<Name of Bond Interface>`
		■ For information about the Port Link, run this command in the Expert mode:
		`ethtool ethsBP<X>-<XX>`
		■ For information about the interface statistics, run this command in the Expert mode:
		`ethtool -S ethsBP<X>-<XX>`

Configuration Verifiers

You can run verifiers to make sure the configuration is correct and consistent.

MAC Verification (mac_verifier)

Description

Each MAC address contains information about the Site ID, Security Group Member ID, and interfaces.

Use this command to make sure that the virtual MAC addresses on physical and bond interfaces are the same for all Security Group Members.

You must run this command in the Expert mode.

Syntax

```
# mac_verifier -h
# mac_verifier [-l] [-v]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-l`	Shows MAC address consistency on the Active Site.
`-v`	Shows information for each interface MAC Address.

Below are some examples:

Example 1

```
# mac_verifier
-------------------------------------------------------------------------------
Collecting information from SGMs...
-------------------------------------------------------------------------------
Verifying FW1 mac magic value on all SGMs...
Success
-------------------------------------------------------------------------------
Verifying IPV4 and IPV6 kernel values...
Success
-------------------------------------------------------------------------------
Verifying FW1 mac magic value in /etc/smodb.json...
Success
-------------------------------------------------------------------------------
Verifying MAC address on local chassis (Chassis 1)...
Success
-------------------------------------------------------------------------------
```

Example 2

```
# mac_verifier -v
-------------------------------------------------------------------------------
Collecting information from SGMs...
-------------------------------------------------------------------------------
Verifying FW1 mac magic value on all SGMs...
FW1 mac magic value on all SGMs:
Command completed successfully

Success
-------------------------------------------------------------------------------
Verifying IPV4 and IPV6 kernel values...
IPV6 is not enabled
Success
-------------------------------------------------------------------------------
Verifying FW1 mac magic value in /etc/smodb.json...
FW1 mac magic value and /etc/smodb.json value are the same (160)
Success
-------------------------------------------------------------------------------
Verifying MAC address on local chassis (Chassis 1)...
-*- 2 blades: 1_01 1_02 -*-
BPEth0      MAC address of BPEth0 is correct

-*- 2 blades: 1_01 1_02 -*-
BPEth1      MAC address of BPEth1 is correct

-*- 2 blades: 1_01 1_02 -*-
eth1-05 00:1c:7f:81:05:a0

-*- 2 blades: 1_01 1_02 -*-
eth1-06 00:1c:7f:81:06:a0

-*- 2 blades: 1_01 1_02 -*-
eth1-07 00:1c:7f:81:07:a0

... output was truncated for brevity ...

-*- 2 blades: 1_01 1_02 -*-
eth2-64 00:1c:7f:82:40:a0

Success
-------------------------------------------------------------------------------
```

Layer 2 Bridge Verifier (asg_br_verifier, asg_brs_verifier)

Description

Use the `asg_br_verifier` command in Gaia gClish or the Expert mode to confirm that there are no bridge configuration problems in a Bridge mode Virtual System.

Notes:

- You must run the `asg_br_verifier` command in the context of the specific Bridge mode Virtual System.
- This command also confirms that the `fdb_shadow` tables are the same for the Virtual System on different Security Group Members.
- You can run the `asg_brs_verifier` command in the Expert mode from the context of any Virtual System to get the output for all Bridge mode Virtual Systems.

Syntax for the `asg_br_verifier` command

```
asg_br_verifier -h
asg_br_verifier [-c] [-d] [-s] [-t] [-v]
```

Syntax for the `asg_brs_verifier` command

```
# asg_brs_verifier -h
# asg_brs_verifier [-d] [-s] [-t] [-v]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Runs bridge verification on all Virtual Systems.
`-c`	Also shows the table entries (unformatted output).
`-d`	Shows verbose unformatted output. The `-d` and `-v` options are mutually exclusive.
`-s`	Also shows the table summary.
`-t`	Also shows the table entries (formatted output).

Parameter	Description
`-v`	Shows verbose formatted output. The `-v` and `-d` options are mutually exclusive.

Below are some examples:

Example 1 - Output in a normal state

```
[Expert@MyChassis-ch01-01:0]# asg_br_verifier
================================================================================
vs #3
================================================================================

Number of entries in fdb_shadow table:

-*- 10 blades: 1_01 1_02 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 -*-
11

Status: OK

================================================================================
[Expert@MyChassis-ch01-01:0]#
```

Example 2 - Output in a state of wrong configuration

```
[Expert@MyChassis-ch01-01:0]# asg_br_verifier -v
================================================================================
vs #3
================================================================================

Number of entries in fdb_shadow table:

-*- 9 blades: 1_01 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 -*-
11
-*- 1 blade: 1_02 -*-
0


Status: number of entries is different

================================================================================

Collecting table info from all SGMs. This may take a while.

Table entries in fdb_shadow table:

-*- 9 blades: 1_01 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 -*-
address="00:00:00:00:00:00" Interface="eth1-07"
address="00:10:AA:7D:08:81" Interface="eth2-07"
address="00:1E:9B:56:08:81" Interface="eth1-07"
address="00:23:FA:4E:08:81" Interface="eth1-07"
address="00:49:DC:58:08:81" Interface="eth2-07"
address="00:7E:60:77:08:81" Interface="eth1-07"
address="00:80:EA:55:08:81" Interface="eth1-07"
address="00:8D:86:52:08:81" Interface="eth2-07"
address="00:9E:8C:7F:08:81" Interface="eth1-07"
address="00:E5:DB:78:08:81" Interface="eth2-07"
address="00:E5:F7:78:08:81" Interface="eth2-07"
-*- 1 blade: 1_02 -*-
fdb_shadow table is empty
Status: Table entries in fdb_shadow table is different between SGMs

================================================================================
[Expert@MyChassis-ch01-01:0]#
```

Verifying VSX Gateway Configuration (asg vsx_verify)

Description

The `asg vsx_verify` command replaces the old verifier in the `smo verifiers` command and runs on a VSX system only.

Use this command to confirm that all Security Group Members have the same VSX configuration - Interfaces, Routes, and Virtual Systems.

- The same MD5 of configuration files that must be identical between Security Group Members.
- Similarity in configuration files that must be identical, but not necessarily written that way (like `/config/active`).

  The command uses the `db_cleanup` report to do this.
- The same VSX configuration on Security Group Members.
- Similarity of VMAC and BMAC addresses.

Use output when there is an inconsistency in the configuration.

The differences are compared in two ways:

- The return value of the command run on the Security Group Members with `gexec_inner_command`
- The output of the commands

Example of a difference in the command output:

```
Difference between blade: 1_01 and blade: 2_01 found.
=====================================================
--- 1_01
+++ 2_01
-73b4c20e598d6b495de7515ad4ea2fdc  /opt/CPsuite-R80.30/fw1/conf/fwha_vsx_conf_id.conf
+b21dfa3feab817c3640bbb984346cdf1  /opt/CPsuite-R80.30/fw1/conf/fwha_vsx_conf_id.conf
```

When a command fails, the output contains:

```
Command "asg xxx" failed to run on blade "2_01"
```

Syntax

```
> asg vsx_verify [{-a | -c | -v}]
```

Parameters

Parameter	Description
`-a`	Includes Security Group Members in the Administrative DOWN state
`-c`	Compares: ■ Database configuration between Security Group Members ■ Operating system and database configuration on each Security Group Member
`-v`	Includes Virtual Systems configuration verification table

Below are some examples:

Example 1 - 'asg vsx_verify -v'

```
> asg vsx_verify -v
+-------------------------------------------------------------------------------+
|Chassis 1 SGMs:                                                                |
|1_01 1_02 1_03                                                                 |
+-------------------------------------------------------------------------------+

+-------------------------------------------------------------------+
|VSX Global Configuration Verification                              |
+------+----------------------------------+------------------+-------+
|SGM   |VSX Configuration Signature       |Virtual Systems   |State  |
|      |VSX Configuration ID              |Installed\Allowed |       |
+------+----------------------------------+------------------+-------+
|all   |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                 |                  |       |
+------+----------------------------------+------------------+-------+

+-------------------------------------------------------------------------------+
|Virtual Systems Configuration Verification                                     |
+----+-----+-----------+---------------+----------------+---------+---------+
|VS  |SGM  |VS Name    |VS Type        |Policy Name     |SIC State|Status   |
+----+-----+-----------+---------------+----------------+---------+---------+
|0   |all  |VSX_OBJ    |VSX Gateway    |Standard        |Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
|1   |all  |VSW-INT    |Virtual Switch |<Default Policy>|Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
|2   |all  |VSW-INT    |Virtual Switch |<Not Applicable>|Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
|3   |all  |VS-1       |Virtual System |Standard        |Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
|4   |all  |VS-2       |Virtual System |Standard        |Trust    |Success  |
+----+-----+-----------+---------------+----------------+---------+---------+
Comparing Routes DB & OS. This procedure may take some time...
Press 'y' to skip this procedure...
Comparing..

+-------------------------------------------------------------------------------+
|Summary                                                                        |
+-------------------------------------------------------------------------------+
|VSX Configuration Verification completed successfully                          |
+-------------------------------------------------------------------------------+

All logs collected to /var/log/vsx_verify.1360846320.log
>
```

Example 2 - 'asg vsx_verify -a -v'

```
> asg vsx_verify -v -a
Output
+------------------------------------------------------------------------------+
|Chassis 1 SGMs:                                                               |
|1_01* 1_02 1_03 1_04                                                          |
+------------------------------------------------------------------------------+

+-------------------------------------------------------------------+
|VSX Global Configuration Verification                              |
+------+-----------------------------------+------------------+-------+
|SGM   |VSX Configuration Signature        |Virtual Systems   |State  |
|      |VSX Configuration ID               |Installed\Allowed |       |
+------+-----------------------------------+------------------+-------+
|1_01  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|1_02  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|1_03  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|1_04  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |DOWN   |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|2_01  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|2_02  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|2_03  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+
|2_04  |8ef02b3e73386afd6e044c78e466ea82 |5\25              |UP     |
|      |9                                  |                  |       |
+------+-----------------------------------+------------------+-------+

+------------------------------------------------------------------------------+
|Virtual Systems Configuration Verification                                    |
+----+-----+-----------+---------------+----------------+---------+--------+
|VS  |SGM  |VS Name    |VS Type        |Policy Name     |SIC State|Status  |
+----+-----+-----------+---------------+----------------+---------+--------+
|0   |all  |VSX_OBJ    |VSX Gateway    |Standard        |Trust    |Success |
+----+-----+-----------+---------------+----------------+---------+--------+
|1   |all  |VSW-INT    |Virtual Switch |<Default Policy>|Trust    |Success |
+----+-----+-----------+---------------+----------------+---------+--------+
|2   |all  |VSW-INT    |Virtual Switch |<Not Applicable>|Trust    |Success |
+----+-----+-----------+---------------+----------------+---------+--------+
|3   |all  |VS-1       |Virtual System |Standard        |Trust    |Success |
+----+-----+-----------+---------------+----------------+---------+--------+
|4   |all  |VS-2       |Virtual System |Standard        |Trust    |Success |
+----+-----+-----------+---------------+----------------+---------+--------+
Comparing Routes DB & OS. This procedure may take some time...
Press 'y' to skip this procedure...
Comparing..

+------------------------------------------------------------------------------+
|Summary                                                                       |
+------------------------------------------------------------------------------+
|VSX Configuration Verification completed with the following errors:           |
|1. [1_02:1] eth1-06 operating system   address doesn't match                  |
|2. [1_02:1] eth1-06 DB address doesn't match                                  |
|3. [1_01:1] Found inconsistency between addresses in operating system  ,DB and NCS ofeth1-06
|
|                                                                              |
+------------------------------------------------------------------------------+
All logs collected to /var/log/vsx_verify.1360886320.log
>
```

Log and Configuration Files

This section describes some log and configuration files you can examine during the troubleshooting.

Files on Security Group Members in Security Groups

Feature	File
Dividing physical interfaces to slave BackPlane interfaces and assembling the bond (BPEth) interfaces	`/var/log/start_tor_sgm.log.dbg` `/var/log/start_bfm.log.dbg`
Discovering the hardware components	`/var/log/start_linker.log.dbg`
Information about the dedicated Sync interfaces	`/var/log/start_smo.log.dbg`
Early boot configuration cloning	`/var/log/image_clone.log.dbg`
Synchronization of the new configuration to the Gaia database	`/var/log/start_smo_1.log.dbg`
Silent install when adding a new Security Group Member to an existing Security Group	`/var/log/silent_install.log.dbg`
LLDP updates	`/var/log/smartd.log.dbg` Also, run the `lldpctl` command
Pulling the Security Group configuration, rebooting, cluster configuration	`$FWDIR/log/blade_config.*`
Additional cluster information	`$FWDIR/log/cpha_policy.log.*`
Security Group installation	`/var/log/start_mbs.log`
Distribution	`/var/log/dist_mode.log*`
General log file	`/var/log/messages*`
Gaia Alerts	`/var/log/send_alert.*`
Gaia OS installation	`/var/log/anaconda.log`

Feature	File
Gaia First Time Configuration Wizard	`/var/log/ftw_install.log`
Dynamic Routing	`/var/log/routed.log`
CPD daemon	`$CPDIR/log/cpd.elg`
FWD daemon	`$FWDIR/log/fwd.elg`
VPND daemon	`$FWDIR/log/vpnd.elg*`
FWK daemon (VSX information)	`$FWDIR/log/fwk.elg.*` (in the context of each Virtual System)
Log Servers	`/var/log/log_servers*`
Gaia Clish auditing	`/var/log/auditlog*`
Expert shell auditing	`/var/log/command_logger.log*`
Command auditing	`/var/log/asgaudit.log*`
Reboot logs	`/var/log/reboot.log`
All logs that do not have a dedicated log file	`/var/log/junk.log.dbg`

Files on Quantum Maestro Orchestrators

Feature	File
Information about Security Groups	`/etc/sgdb.json`
Information about detected Security Group Members	`/etc/rsrcdb.json`
Applying Security Group configuration	`/var/log/ssm_sg.log.dbg`
Starting of the SDK	`/var/log/start_tor_ssm.log.dbg`
Configuring the SDK	`/var/log/messages`
LLDP updates	`/var/log/smartd.log.dbg` Also, run the `lldpctl` command
All logs that do not have a dedicated log file	`/var/log/junk.log.dbg`

Installing the Gaia Operating System on a Quantum Maestro Orchestrator

To perform a clean installation of the Gaia Operating System on a Quantum Maestro Orchestrator, you can:

- Restore your Quantum Maestro Orchestrator to Factory Defaults.

  Note - This removes all existing configurations.

- Perform a clean install of the supported Gaia image with a bootable USB device.

Reset an Orchestrator to Factory Defaults

Important - This operation reverts the Quantum Maestro Orchestrator to the last Gaia that was installed using the Clean Install method.

Step	Instructions
1	Connect to the Quantum Maestro Orchestrator using the serial console.
2	Log in to the Gaia Clish.
3	Restart the Quantum Maestro Orchestrator. Run: `reboot`

4	During boot, press any key within 4 seconds to enter the Boot menu when you see this prompt at the top of the screen:
	`Loading the system`
	`Press any key to see the boot menu [Booting in 5 seconds]`

5	In the menu, select **Reset to factory defaults** and press Enter.
6	Type **yes** and press Enter.
7	Wait for the Quantum Maestro Orchestrator to boot.
8	With a web browser, connect to the Gaia Portal on the Quantum Maestro Orchestrator: `https://<IP Address of MGMT Port>`
9	Run the Gaia First Time Configuration Wizard.

Clean Install of the Gaia Image on an Orchestrator with a Bootable USB Device

Step	Instructions
1	Contact *Check Point Support* to configure the Quantum Maestro Orchestrator to boot from the USB device by default.
2	Download the required Clean Install package (ISO) for Maestro Orchestrators from sk162552.
3	Follow sk65205 to create a bootable USB device. **Important:** ■ Always use the latest available build of the ISOmorphic Tool. If you use an outdated build, the installation can fail. ■ Select the option **Open Server with console**.
4	Insert the bootable USB device into the Quantum Maestro Orchestrator.
5	Connect to the Quantum Maestro Orchestrator through the console port.
6	Restart the Quantum Maestro Orchestrator. Run: `reboot`
7	Wait for the Quantum Maestro Orchestrator to boot from the USB device.
8	Select the boot option **Open Server with console**.
9	Install the Gaia Operating System.
10	**Before the reboot, remove the USB device.**
11	Confirm the reboot.
12	With a web browser, connect to the Gaia Portal on the Quantum Maestro Orchestrator: `https://<IP Address of MGMT Port>`
13	Run the Gaia First Time Configuration Wizard.

Replacing a Quantum Maestro Orchestrator

Follow the steps in sk174202.

Glossary