QUANTUM

14 November 2024

QUANTUM SCALABLE CHASSIS

R81

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 R81 for Scalable Platforms

For more about this release, see the 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
14 November 2024	Improved explanations in procedures
17 June 2024	Removed: ■ Serial Over LAN (sol) - this feature is not supported in R81 and higher versions
01 May 2023	Removed: ■ "Working with Session Control (asg_session_control)" - this command is not supported.
07 April 2023	Updated: ■ *"Security Group" on page 16* - Best Practice about enabling the SMO Image Cloning
04 April 2023	Updated: ■ *"Multi-blade Traffic Capture (tcpdump)" on page 150*
08 March 2023	Removed information about the "`asg_bond -v`" command because it is not supported.
02 Match 2023	Removed the chapter "IP Block and URL Block Features" because these features are not supported.
18 December 2022	Updated: ■ *"General Diagnostic in Security Groups" on page 339*
15 December 2022	Updated: ■ *"General Diagnostic in Security Groups" on page 339* ■ *"Packet Drop Monitoring (drop_monitor)" on page 190*
10 July 2022	Updated: ■ *"Introduction" on page 15*

Date	Description
17 October 2021	Added: ■ *"Configuring Services to Synchronize After a Delay" on page 279* ■ *"Forwarding specific inbound-connections to the SMO (asg_excp_conf)" on page 283* Updated: ■ *"Configuring Alerts for SGM and Security Group Events (asg alert)" on page 216*
28 February 2019	First release of this document

Table of Contents

Introduction

Introducing the Check Point Chassis, the world's fastest Threat Prevention platforms.

The carrier-class next generation Threat Prevention and Firewall solutions, provide the security you need today and into the future.

Already supporting fast networking connectivity such as 40 GbE and 100 GbE, the 64000 and 44000 can be integrated with new and advanced solutions, both on premises or in the cloud.

These Chassis let you continue to grow your business, so when traffic volume or security requirements increase, you can easily scale up the system capacity.

Welcome to the future of Cyber Security!

Licensing

For information on how to monitor and administer licenses, see the *License* section in the *R81 Scalable Platforms Gaia Administration Guide*.

Run all licensing commands in Gaia gClish on the applicable Security Group.

Important Links

For more information and the software, see the R81 Home Page for Scalable Platforms: sk169954.

- Read the Scalable Platforms Known Limitations in sk148074.
- Read the R81 Known Limitations in sk166717.
- To learn about the differences between R81 and R81 for Scalable Platforms versions, see sk170425.

  To learn about the differences between different Scalable Platform versions, see sk173183.

Visit the *Check Point CheckMates Community*:

- Start discussions.
- Get answers from experts.
- Join the API community to get code samples and share yours.

Security Group Concepts

This section describes some of the Security Group concepts.

Security Group

In This Section:

To be part of a Security Gateway, a Security Gateway Module (SGM) must belong to a Security Group.

Note - You must run the applicable commands in Gaia gClish of the applicable Security Group.

Viewing SGMs in a Security Group

Syntax

```
show smo security-group
```

Adding SGMs to a Security Group

Best Practice - To add new SGMs to an existing Security Group:

1. Enable the SMO Image Cloning feature in the Security Group.
   This feature automatically clones all the required software packages to the new SGMs.
   Run in Gaia gClish on the Security Group:

   ```
   set smo image auto-clone state on
   ```

   ```
   show smo image auto-clone state
   ```

2. Add the new SGMs to the existing Security Group:

   ```
   add smo security-group <SGM IDs>
   ```

3. Make sure the Security Group is configured correctly (run the command exactly as it appears below):

   ```
   show smo verifiers print name Security_Group
   ```

4. To optimize connection distribution among the SGMs, update the Security Group with the correct number of the SGMs.
   See *"Configuring the SGM Range" on page 59*.
5. Disable the SMO Image Cloning feature in the Security Group.
   Run in Gaia gClish on the Security Group:

   ```
   set smo image auto-clone state off
   ```

   ```
   show smo image auto-clone state
   ```

Syntax

```
add smo security-group <SGM IDs>
```

Parameters

Parameter	Description
<SGM IDs>	Applies to Security Group Members as specified by the *<SGM IDs>*. *<SGM IDs>* can be: ■ No *<SGM IDs>* specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)

Example

```
[Global] MyChassis-ch01-01 > add smo security-group 1_1-1_3,2_1-2_
3
```

Deleting SGMs from a Security Group

Syntax

Important - Before you remove an SGM from the Security Gateway, make sure that is it in the DOWN state.
All SGMs that are assigned to the current Security Group and are not part of the new Security Group, must be in the DOWN state.
Otherwise, the command fails.

```
delete smo security-group <SGM IDs>
```

Best Practice - After you delete SGMs from an existing Security Group:

1. Make sure the Security Group is configured correctly (run the command exactly as it appears below):
   ```
   show smo verifiers print name Security_Group
   ```
2. To optimize connection distribution among the SGMs, update the Security Group with the correct number of the SGMs.
   See *"Configuring the SGM Range" on page 59*.

Parameters

Parameter	Description
<SGM IDs>	Applies to Security Group Members as specified by the *<SGM IDs>*. *<SGM IDs>* can be: ■ No *<SGM IDs>* specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)

Example

```
[Global] MyChassis-ch01-01 > delete smo security-group 1_1-1_3,2_
1-2_3
```

Single Management Object 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.

One Security Group Member, the SMO Master, handles all management tasks, such as Security Gateway configuration, policy installation, remote connections, and logging

are handled. The SMO Master updates all other Security Group Members.

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

Use the "`asg stat -i tasks`" command to identify the SMO and see how tasks are distributed on the Security Group Members (see *"Showing Hardware State (asg stat)" on page 196*).

Example output in a Single Chassis configuration

The SMO task runs on the Security Group Member #1, on which you ran this command (see the string "`(local)`").

```
[Expert@MyChassis-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@MyChassis-ch0x-0x:0]#
```

Example output in a Dual Chassis configuration

The SMO task runs on Chassis #2 - on the Security Group Member #3, on which you ran this command (see the string "`(local)`").

```
[Expert@MyChassis-ch0x-0x:0]# asg stat -i tasks
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |                            |         3(local)           |
| General (1)        |         2                  |         3(local)           |
| LACP (2)           |         2                  |         3(local)           |
| CH Monitor (3)     |         2                  |         3(local)           |
| DR Manager (4)     |                            |         3(local)           |
| UIPC (5)           |         2                  |         3(local)           |
| Alert (6)          |                            |         3(local)           |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
[Expert@MyChassis-ch0x-0x:0]# member 2_4
Moving to member 2_4
... ...
[Expert@MyChassis-ch0x-0x:0]# asg stat -i tasks
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |                            |         3                  |
| General (1)        |         2                  |         3                  |
| LACP (2)           |         2                  |         3                  |
| CH Monitor (3)     |         2                  |         3                  |
| DR Manager (4)     |                            |         3                  |
| UIPC (5)           |         2                  |         3                  |
| Alert (6)          |                            |         3                  |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Example output from all Security Group Members (in our example, there are two on each Chassis):

```
[Expert@MyChassis-ch0x-0x:0]# g_all asg stat -i tasks
1_01:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1(local)           |                            |
| General (1)        |         1(local)           |         1                  |
| LACP (2)           |         1(local)           |         1                  |
| CH Monitor (3)     |         1(local)           |         1                  |
| DR Manager (4)     |         1(local)           |                            |
| UIPC (5)           |         1(local)           |         1                  |
| Alert (6)          |         1(local)           |                            |
-------------------------------------------------------------------------------

1_02:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1                  |                            |
| General (1)        |         1                  |         1                  |
| LACP (2)           |         1                  |         1                  |
| CH Monitor (3)     |         1                  |         1                  |
| DR Manager (4)     |         1                  |                            |
| UIPC (5)           |         1                  |         1                  |
| Alert (6)          |         1                  |                            |
-------------------------------------------------------------------------------

2_01:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1                  |                            |
| General (1)        |         1                  |         1(local)           |
| LACP (2)           |         1                  |         1(local)           |
| CH Monitor (3)     |         1                  |         1(local)           |
| DR Manager (4)     |         1                  |                            |
| UIPC (5)           |         1                  |         1(local)           |
| Alert (6)          |         1                  |                            |
-------------------------------------------------------------------------------

2_02:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1                  |                            |
| General (1)        |         1                  |         1                  |
| LACP (2)           |         1                  |         1                  |
| CH Monitor (3)     |         1                  |         1                  |
| DR Manager (4)     |         1                  |                            |
| UIPC (5)           |         1                  |         1                  |
| Alert (6)          |         1                  |                            |
-------------------------------------------------------------------------------
[Expert@MyChassis-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 you create a Security Group, its Security Group Members enforce an initial policy that allows only the implied rules necessary for management.

Uninstalling a Policy

Note - You cannot uninstall policies from a Security Group in SmartConsole.

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` See *"Working with Policies (asg policy)" on the next page*.

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 all Security Group Members in the Security Group.
`-vs <VS IDs>`	Applies to Virtual Systems as specified by the `<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 This parameter is only applicable in a VSX environment.
`-v`	Shows detailed verification results for Security Group Members.
`-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.

Examples

Example 1 - Detailed verification results for Security Group Members

```
[Expert@MyChassis-ch0x-0x:0]# asg policy verify -v
+-------------------------------------------------------------------------+
|Policy Verification                                                      |
+-------+------------------+--------------+-----------------+--------+---+
|SGM    |Policy Name       |Policy Date   |Policy Signature |Status  |
+-------+------------------+--------------+-----------------+--------+---+
|1_01   |Standard          |27Feb19 08:56 |e17c177f7        |Success |
+-------+------------------+--------------+-----------------+--------+---+
|1_02   |Standard          |27Feb19 08:56 |e17c177f7        |Success |
+-------+------------------+--------------+-----------------+--------+---+

+-------------------------------------------------------------------------+
|Summary                                                                  |
+-------------------------------------------------------------------------+
|Policy Verification completed successfully                               |
+-------------------------------------------------------------------------+
[Expert@MyChassis-ch0x-0x:0]#
```

Example 2 - Detailed verification results for for each Virtual System on Security Group Members

```
[Expert@MyChassis-ch0x-0x:0]# asg policy verify -vs all -v
+-------------------------------------------------------------------------+
|Policy Verification                                      |               |
+-------+-------+------------------+--------------+-----------------+--------+---+
|VS     |SGM    |Policy Name       |Policy Date   |Policy Signature |Status  |
+-------+-------+------------------+--------------+-----------------+--------+---+
|0      |1_01   |Standard          |27Feb19 08:56 |996eee5e6        |Success |
|       |1_03   |Standard          |27Feb19 08:56 |996eee5e6        |Success |
|       |1_04   |Standard          |27Feb19 08:56 |996eee5e6        |Success |
|       |1_05   |Standard          |27Feb19 08:56 |996eee5e6        |Success |
|       |1_06   |Standard          |27Feb19 08:56 |996eee5e6        |Success |
|       |1_11   |Standard          |27Feb19 08:56 |996eee5e6        |Success |
|       |1_12   |Standard          |27Feb19 08:56 |996eee5e6        |Success |
+-------+-------+------------------+--------------+-----------------+--------+---+
|1      |1_01   |Standard          |27Nov12 13:03 |836fa2ec1        |Success |
|       |1_03   |Standard          |27Nov12 13:03 |836fa2ec1        |Success |
|       |1_04   |Standard          |27Nov12 13:03 |836fa2ec1        |Success |
|       |1_05   |Standard          |27Nov12 13:03 |836fa2ec1        |Success |
|       |1_06   |Standard          |27Nov12 13:03 |836fa2ec1        |Success |
|       |1_11   |Standard          |27Nov12 13:03 |836fa2ec1        |Success |
|       |1_12   |Standard          |27Nov12 13:03 |836fa2ec1        |Success |
+-------+-------+------------------+--------------+-----------------+--------+---+
|2      |1_01   |Standard          |27Feb19 08:56 |10eef9ced        |Success |
|       |1_03   |Standard          |27Feb19 08:56 |10eef9ced        |Success |
|       |1_04   |Standard          |27Feb19 08:56 |10eef9ced        |Success |
|       |1_05   |Standard          |27Feb19 08:56 |10eef9ced        |Success |
|       |1_06   |Standard          |27Feb19 08:56 |10eef9ced        |Success |
|       |1_11   |Standard          |27Feb19 08:56 |10eef9ced        |Success |
|       |1_12   |Standard          |27Feb19 08:56 |10eef9ced        |Success |
+-------+-------+------------------+--------------+-----------------+--------+---+

+-------------------------------------------------------------------------+
|Summary                                                                  |
+-------------------------------------------------------------------------+
|Policy Verification completed successfully                               |
+-------------------------------------------------------------------------+
[Expert@MyChassis-ch0x-0x:0]#
```

Example 3 - Uninstall of a Policy

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x: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 Management Server, it first installs the policy on the SMO Security Group Member.

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 the 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	Do **one** of these:
	■ Reboot the **target** Security Group Member:
	`reboot -b <Security Group Member ID>`
	■ Start the Check Point services and remove the ClusterXL Critical Device "`admin_down`":
	`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-ch0x-0x:0]# g_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-ch0x-0x:0]#
```

MAC Addresses and Bit Conventions

MAC addresses on the system are divided into these types - BMAC, VMAC, and SMAC:

BMAC

A MAC address assigned to all interfaces with the naming convention "`BPEthX`".

This is unique for each Security Group Member.

It does not rely on the interface index number.

Bit convention for the BMAC type:

Bit range	Instructions
1	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
2-8	Security Group Member ID (starting from 1). This is limited to 127.
9-13	Always zero.
14	Distinguishes between BMAC and SMAC addresses. This is used to prevent possible collisions with SMAC space. Possible values: ■ `0` - BMAC ■ `1` - SMAC
15-16	Absolute interface number. This is taken from the interface name. When the `BPEthX` format is used, `X` is the interface number. This is limited to four interfaces.

VMAC

A MAC address assigned to all interfaces with the naming convention "`eth`*`X`*`-`*`YZ`*".

This is unique for each Chassis.

It does not rely on the interface index number.

Bit convention for the VMAC type:

Bit range	Instructions
1	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
2-3	Chassis ID. Limited to 4 Chassis.
4-8	Switch number. Limited to 32 switches.
9-16	Port number. Limited to 256 for each switch.

SMAC

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 the SMAC type:

Bit range	Instructions
1	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
2-8	Security Group Member ID (starting from 1). This is limited to 127.
9-13	Always zero.
14	Distinguishes between BMAC and SMAC addresses. This is used to prevent possible collisions with SMAC space. Possible values: ■ `0` - BMAC ■ `1` - SMAC
15	Always zero.
16	Sync interface. Possible values are: ■ `0` - Sync1 ■ `1` - Sync2

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
- Chassis ID
- Security Group Member ID
- Assigned interface

Syntax

```
asg_mac_resolver <MAC address>
```

Example

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x:0]#
```

Notes:

- The specified MAC Address comes from BPEth0 on Security Group Member #1 on the Chassis #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.

Managing Security Groups

This section provides basic information about managing Security Groups.

Connecting to a Specific Security Group Member (member)

When you connect to the Security Group, you are actually connected to one of the Security Group Members (SGMs) in that Security Group.

You can open a connection to a different Security Group Member (SGM).

You must run the applicable command in the Expert mode, which establishes a new SSH connection over the Sync interface.

#	Syntax	Example
1	`member [<Chassis ID>_]<SGM ID>`	`[Expert@MyChassis-ch0x-0x:0]# member 1_03` `Moving to blade 1_3`
2	`m[<Chassis ID>_]<SGM ID>`	`[Expert@MyChassis-ch0x-0x:0]# m 1_03` `Moving to blade 1_3`

Notes:

- When you only enter the SGM ID, the command assumes the default Chassis.
- To go back to the previous SGM, run: `exit`
- You open many SSH sessions to SGMs.

Global Commands

In This Section:

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

Working with Global Commands

Background

- Gaia gClish commands apply globally to all Security Group Members, by default.
- Gaia gClish commands do not apply to Security Group Members that are in the DOWN state in the Security Group.

  If you run a "`set`" command while a Security Group Member is in the DOWN state, 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.

  For these commands, see the *R81 Scalable Platforms Gaia Administration Guide*.

Global Commands

Command	Instructions
`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 one lock. ■ To set Gaia gClish operations for an Security Group Member, the Security Group Member must hold the "`config-lock`". ■ To set the "`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.

General Global Commands

Global commands apply to more than one Security Group Member.

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

Use the "`global help`" command in Gaia gClish to show the list of global commands you can use in Gaia gClish.

Syntax

```
global help
```

Examples

Example output in Gateway mode

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x: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 these commands to add, update, and remove parameters in configuration files.

Important - After you change the configuration files, you must reboot the Security Group with the "`reboot -b all`" command.

Syntax

Shell	Syntax
Gaia gClish	`update_conf_file <File Name> <Parameter Name>=<Parameter Value>`
Expert mode	`g_update_conf_file <File Name> <Parameter Name>=<Parameter Value>`

Important:

- There must not be a space in front of the equal sign (=).
- There must not be a space after the equal sign (=).

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`
<Parameter Name>	Name of the parameter to configure.
<Parameter Value>	New value for the parameter to configure.

Notes:

- These commands work with configuration files in a specified format.
  It is composed of lines, where each line defines one parameter:
  <Parameter Name>=<Parameter Value>
  The `$FWDIR/boot/modules/fwkern.conf` and `$PPKDIR/conf/simkern.conf` files use this format.
- If the specified configuration file does not exist, these commands create it.
- These commansd make the required changes on all Security Group Members.

Examples

```
[Expert@MyChassis-ch0x-0x: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>
```

Setting Firewall Kernel Parameters (g_fw ctl set)

Description

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

Syntax for viewing the current value of a kernel parameter

```
g_fw ctl get <Parameter Type> <Parameter Name>
```

Syntax for setting a value of a kernel parameter

```
g_fw ctl set <Parameter Type> <Parameter Name> <Parameter Value>
```

Parameters

Parameter	Description
`get`	Shows the specified parameter and its value.
`set`	Change the parameter value to the specified value.
<Parameter Type>	Type of the parameter: ▪ `int` - Accepts integer values ▪ `str` - Accepts string values **Note** - You must enter the correct parameter type.
<Parameter Name>	Parameter name to configure.
<Parameter Value>	Parameter value to configure.

Note - To make changes persistent, you must manually add the applicable kernel parameters and their values in the `$FWDIR/boot/modules/fwkern.conf` file.
Use the "`g_update_conf_file`" command in the Expert mode.
See *"Updating Configuration Files (update_conf_file)" on page 40*.

For more information, see the *R81 Scalable Platforms 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 another Security Group Member.

Syntax (for Gaia gClish and the Expert mode)

```
asg_cp2blades [-b <SGM IDs>] [-s] <Source Path> [<Destination Path>]
```

Parameters

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`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.
`<Destination Path>`	Full path of the destination. If not specified, the command copies the file to the relative source file location.

Example

```
[Expert@MyChassis-ch0x-0x: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

Use the "`asg_clear_table`" command in Gaia gClish or the Expert mode to delete connections from the Connections table on the Security Group Members.

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

Important - If you are connected to the Security Group over SSH, your connection is disconnected.

Syntax (for Gaia gClish and the Expert mode)

```
asg_clear_table [-b <SGM IDs>]
```

Parameters

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`) **Note** - With this option, you can only select Security Group Members from one Chassis.

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 *R81 Scalable Platforms Gaia Administration Guide* > Chapter *Network Management* > Section *Network Interfaces*.

Syntax

`show interfaces all`
`show interface <Options>`

Example

```
[Expert@MyChassis-ch0x-0x: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 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`
`ifconfig`	`asg_ifconfig`
`ls`	`g_ls`
`md5sum`	`g_md5sum`
`mv`	`g_mv`
`netstat`	`g_netstat`
`reboot`	`g_reboot`
`tail`	`g_tail`
`tcpdump`	`g_tcpdump`
`top`	`g_top`

Notes:

- The parameters and options for the standard Linux command are available for the global command.
- You can use one or more flags.
- Do **not** use these two flags together in the same command:
  - The "`-l`" flag - to execute the command only on the local Security Group Member
  - The "`-r`" flag - to execute the command only on the remote Security Group Member

Syntax

- In Gaia Clish:

```
<Gaia gClish Command> [-b <SGM IDs>] <Command Options>]
```

- In the Expert mode:

```
<Global Expert mode Command> [-b <SGM IDs>] <Command Options>]
```

Parameters

Parameter	Description
<Gaia gClish Command>	Standard command in Gaia gClish as appears in the table above.
<Global Expert mode Command>	Global command in the Expert mode as appears in the table above.

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`) **Note** - You can only select Security Group Members from one Chassis with this option.
`<Command Options>`	Standard command options for the specified command.

Below are explanations about some of the global commands.

Global 'ls'

Description

The global `ls` command shows the file in the specified directory on all Security Group Members.

Syntax

- In Gaia Clish:

```
ls [-b <SGM IDs>] <Command Options>]
```

- In the Expert mode:

```
g_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-ch0x-0x: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-ch0x-0x:0]#
```

Global 'reboot'

Description

The global `reboot` command reboots all Security Group Members.

Syntax

- In Gaia Clish:

  ```
  reboot [-a]
  ```

- In the Expert mode:

  ```
  g_reboot [-a]
  ```

Parameters

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

Global 'top'

Description

The global `top` command:

- Shows CPU utilization in real time on Security Group Members.
- Uses the local Security Group Member configuration file (`~/.toprc`) to format the output on the remote Security Group Members.

  The command copies this file to the remote Security Group Members.

Syntax

- In Gaia Clish:

```
top -h
```

```
top [local] [-f [-o <Output File>] [-n <Number of Iterations>]] -b <SGM IDs> [<Command Options>]
```

```
top [local] [s <Output File>] -b <SGM IDs> [<Command Options>]
```

- In the Expert mode:

```
g_top -h
```

```
g_top [local] [-f [-o <Output File>] [-n <Number of Iterations>]] -b <SGM IDs> [<Command Options>]
```

```
g_top [local] [s <Output File>] -b <SGM IDs> [<Command Options>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`local`	Uses the '`top`' configuration file (`~/.toprc`) on the local Security Group Member.
`-f`	Exports the output to a file. Default: `/vat/log/gtop.<Time>`
`-o <Output File>`	Specifies the path and name of the output file. Must use with the "`-f`" parameter.
`-n <Number of Iterations>`	The command saves the output the specified number of times. Default: 1 Must use with the "`-f`" parameter.
`-s <Output File>`	Shows the content of the output file `<Output File>`, in which the command saved its output earlier.
`<Command Options>`	Parameters of the standard `top` command. For more information, see the `top` command documentation.

Configuring the 'g_top' output

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Run: `top`
4	Set the desired view (press **h** to see the built-in help).
5	Press **Shift+W** to save the '`top`' configuration.
6	Run: `g_top`

Global 'arp'

Description

The global `arp` command shows the ARP cache table on all Security Group Members.

Syntax

- In Gaia Clish:

```
arp [-b <SGM IDs>] <Command Options>]
```

- In the Expert mode:

```
g_arp [-b <SGM IDs>] <Command Options>]
```

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

```
[Expert@MyChassis-ch0x-0x: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 >
```

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.

Syntax

Shell	Syntax
Gaia Clish Gaia gClish	`fw` `fw6`
Expert mode	`g_fw` `g_fw6`

Examples

Example 1

```
[Expert@MyChassis-ch0x-0x: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
[Global] MyChassis-ch01-01 >
```

Example 2

```
[Expert@MyChassis-ch0x-0x: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
[Global] MyChassis-ch01-01 >
```

fw dbgfile

Description

Use the "`fw dbgfile`" commands in Gaia gClish to debug how the Security Group inspect traffic.

Syntax to collect the debug

```
fw dbgfile collect -f <Debug Output File> [-buf <Buffer 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 Output File>] [-o <Debug Output File>]
```

Parameters

Parameter	Description
`collect`	Collects the Security Gateway debug information.
`view`	Shows the collected debug information.
<Debug Output File>	Specifies the full path and the name of the debug output file.
`-buf` *<Buffer 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` *<Debug Output File>*	Specifies the full path and the name of the debug output file to read.

Examples

Example - Collect debug information

```
[Global] MyChassis-ch01-01 > fw dbgfile collect -f /var/log/debug.txt -buf 8200 -m fw + conn -m kiss + pmdump
```

Example - Show the collected debug information

```
[Global] MyChassis-ch01-01 > fw dbgfile view /var/log/debug.txt
```

Important - For complete debug procedure, see the *R81 Scalable Platforms 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.

Syntax

Shell	Syntax for IPv4	Syntax for IPv6
Gaia Clish Gaia gClish	`fwaccel help`	`fwaccel6 help`
Expert mode	`g_fwaccel help`	`g_fwaccel6 help`

Parameters and Options

For more information, see the *R81 Scalable Platforms Performance Tuning Administration Guide* > Chapter *SecureXL* > Section *SecureXL Commands and Debug* - Subsection *'fwaccel' and 'fwaccel6'*.

Global Commands Generated by CMM

The CMM monitors and controls the Chassis components, activates, and shuts down SGMs and SSMs.

Users can activate and shut down SGMs in serious situations.

For example, when the Sync Interface cannot access the SGM. In that case, the `reboot` command does not work.

Commands that control SGM power from the CMM:

Command	Description	Comments
`asg_reboot <global_command_flags>`	Restarts SGMs	This command performs a software reboot only.
`asg_hard_reboot <global_command_flags>`	Reboots SGMs	This command performs a hardware reboot.
`asg_hard_shutdown <global_command_flags>`	Turns off SGMs	
`asg_hard_start <global_command_flags>`	Turns on SGMs	

You can run global commands from Gaia gClish and the Expert mode.

Notes:

- At least one SGM must be UP and running on the remote Chassis to run these commands.
- To learn how to restart an SSM from the CMM, see *"Chassis Control (asg_chassis_ctrl)" on page 227*.

Example for the 'asg_reboot' command

```
[Expert@MyChassis-ch0x-0x:0]# asg_reboot -b 1_03,2_05
You are about to perform hard reboot on SGMs: 1_03,2_05
It might cause performance hit for a period of time

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

Hard reboot requires auditing
Enter your full name: User1
Enter reason for hard reboot [Maintenance]:
WARNING: Hard reboot on SGMs: 1_03,2_05, User: User1, Reason: Maintenance

Rebooting SGMs: 1_03,2_05
```

Configuring the Chassis State (set chassis id ... admin-state, asg chassis_admin)

Description

Use these commands in *Gaia gClish* to change the Chassis administrative state to UP or DOWN.

Note - You must have administrator permission to do this.

When a Chassis is in the Administrative DOWN state:

- Backup connections for SGMs are lost.
- New connections are not synchronized with the Chassis in the DOWN state.

Syntax

```
set chassis id <Chassis ID> admin-state {up | down}
```

```
asg chassis_admin -c <Chassis ID> {up | down}
```

Parameters

Parameter	Description
`<Chassis ID>`	Chassis identification number - 1 or 2
`{up | down}`	Chassis state

Notes:

- The "`set chassis`" and "`asg chassis_admin`" commands are audited in the "`asg log audit`".
- Run one of these commands in Gaia gClish to see the Chassis state:

  ```
  asg stat
  ```

  ```
  asg monitor
  ```

- In a Dual Chassis environment, a Chassis in the administrative DOWN state causes degradation in the system performance.

Example 1 - Setting the state of Chassis 2 to DOWN

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > asg chassis_admin -c 2 down
```

Example 2 - Setting the state of Chassis 2 to UP

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > asg chassis_admin -c 2 up
```

Example Output

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > set chassis id 1 admin-state down
You are about to perform Chassis admin-state down on chassis: 1
Are you sure? (Y - yes, any other key - no) y
Chassis admin-state down requires auditing
Enter your full name: John
Enter reason for Chassis admin-state down [Maintenance]: Test
WARNING: Chassis admin-state down on Chassis: 2, User: John, Reason: Test
Chassis 2 is going DOWN...
Chassis 2 state is DOWN
[Global] MyChassis-ch01-01 >
```

Configuring the SGM Range

Description

Use the "`set blade-range`" command in Gaia gClish to configure which SGMs are part of the SGM range.

The SGM range determines on which SGMs in a Security Group to apply the Gaia gClish embedded commands you run.

Syntax

```
set blade-range <Chassis ID>_<SGM ID> - <Chassis ID>_<SGM ID>
```

Parameters

Parameter	Description
<Chassis ID>	Specifies the Chassis. Valid values: ■ `1` ■ `2`
<SGM ID>	Specifies the SGM. Valid values: ■ from `1` to `12` ■ `all` This value does not work in VSX mode

Backing Up and Restoring Gaia Configuration

For more information, see the *R81 Scalable Platforms Gaia Administration Guide*:

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

Working with Security Group Gaia gClish Configuration (asg_config)

Description

Use the "`asg_config`" command in Gaia gClish or Expert mode to:

- Show the current Gaia gClish configuration on all SGMs.
- Save the current Gaia gClish configuration of all SGMs to a file.

Use cases:

- Copy the Gaia gClish configuration to a different Security Group.

  For example, you can use the saved configuration from an existing Security Group to configure up a new Security Group.

- Quickly re-configure a Security Group that was reverted to factory defaults.

  Before you revert to the factory default image, save the existing Gaia gClish configuration. Then use it to override the factory default settings.

Syntax

```
asg_config show
asg_config save [-t] [<Output File>]
```

Parameters

Parameter	Description
`show`	Show the existing Gaia gClish configuration.
`save`	Save the current Gaia gClish configuration to a file. If you do not include a path, the output file is saved to this directory: `/home/admin/`

Parameter	Description
`-t`	Adds a timestamp in Unix Epoch format to the file name.
<Output File>	Specifies the path and name of the output file. If you do not include a path, the output file is saved to this directory: `/home/admin/`

Example - Save the current Gaia gClish configuration to the `/home/admin/myconfig` file

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > asg_config save -t mycongfig
[Global] MyChassis-ch01-01 > exit
[Expert@MyChassis-ch0x-0x:0]# ls -l ~/mycongfig*
-rw-rw---- 1 admin root 75891 Feb 28 04:38 mycongfig.1551346686
[Expert@MyChassis-ch0x-0x:0]# date -d @1551346686
Thu Feb 28 04:38:06 EST 2019
[Expert@MyChassis-ch0x-0x:0]#
```

Configuring Security Group Members (asg_blade_config)

Description

Use the "`asg_blade_config`" command in the Expert mode to manage Security Group Members:

- Copy the Security Group Member configuration from the local Security Group Member to other Security Group Members in the Security Group
- Change the synchronization start IP address
- Reset the system uptime value
- Get a policy from the Management Server

Syntax

```
asg_blade_config
      fetch_smc
      full_sync <IP Address>
      get_smo_ip
      is_in_pull_conf_group
      is_in_security_group
      pull_config
      reset_sic -reboot_all <Activation Key>
      set_sync_start_ip <Start IP Address>
      upgrade_cu
      upgrade_start <New Version> [cu]
      upgrade_stat
      upgrade_stop
```

Parameters

Parameter	Description
`fetch_smc`	Fetches policy from Management Server and distributes it to all Security Group Members.
`full_sync <IP Address>`	Runs Full Sync with the remote Security Group Member, whose IP address is `<IP Address>`.
`get_smo_ip`	Gets the SMO IP address from the Cluster Control Protocol (CCP) packets sent in the Security Group.
`is_in_pull_conf_group`	Checks whether the Security Group Member is in the Pulling Configuration Group.
`is_in_security_group`	Checks whether the Security Group Member is in the Security Group.
`pull_config`	Pulls configuration from other Security Group Members.
`reset_sic -reboot_all <Activation Key>`	Starts a Secure Internal Communication (SIC) cleanup. You must enter the `<Activation Key>`. You use this key later in SmartConsole to establish Secure Internal Communication.
`set_sync_start_ip <Start IP Address>`	Changes the Sync start IP address of local Security Group Member to `<Start IP Address>`.
`upgrade_cu`	Enables the Connectivity Upgrade mode (runs an iteration).
`upgrade_start <New Version> [cu]`	Starts an upgrade procedure from the current version to the `<New Version>`. The "`cu`" parameter uses the Connectivity Upgrade mode.
`upgrade_stat`	Shows the upgrade procedure information.
`upgrade_stop`	Stops the upgrade procedure.

Troubleshooting the `asg_blade_config` command

To troubleshoot problems associated with the "`asg_blade_config`" command, examine the logs listed in the `$FWDIR/log/blade_config` file.

For example, if a Security Group Member unexpectedly reboots, you can search the log file for the word reboot to learn why.

Changing the Gaia Management Interface

Use this command to change the Gaia management interface for the SGMs.

Important - In VSX mode, you must use the "`vsx_util change_interfaces`" command on the Management Server.

To change the Management Interface on a chassis in the Gateway mode:

Step	Instructions
1	Make sure the management interface cable is connected to the network.
2	Connect to the Security Group over a serial console. This makes sure you do not lose connectivity when you change the management interface.
3	Go to Gaia gClish: enter `gclish` and press Enter.

4	Run these commands in Gaia gClish in the order they are listed:
	`set management interface <New Mgmt Interface>`
	`delete interface <Current Mgmt Interface> ipv4-address`
	`set interface <New Mgmt Interface> ipv4-address <IP Address> mask-length <Length>`
	`set interface <New Mgmt Interface> state on`
	
	Parameters:
	■ *<New Mgmt Interface>*
	Interface name of the new management interface. For example: `eth1-Mgmt3`
	■ *<Current Mgmt Interface>*
	Interface name of the existing management interface that is to be changed or deleted. For example: `eth1-Mgmt2`
	■ *<IP Address>*
	Interface IPv4 address.
	■ *<Length>*
	Interface IPv4 net mask.
	
	For more information, see the *R81 Scalable Platforms Gaia Administration Guide* > Chapter *Network Management*.

Step	Instructions
5	In SmartConsole: a. Open the Security Gateway object. b. From the left tree, click **Network Management**. c. Click **Get Interfaces** > **Get Interfaces Without Topology**. d. Click **OK**. e. Install the Access Control Policy the Security Gateway object.

Working with the Distribution Mode

In This Section:

Background

The SSMs use the Distribution Mode to assign incoming traffic to Security Group Members in each Security Group.

By default, the SSMs automatically configure the Distribution Mode.

Supported Distribution Modes

Mode	Instructions	Applies To
User (Internal)	Packets are assigned to a Security Group Member based on the packet's Destination IP address. If Layer 4 distribution is enabled, SSM assigns packets to a Security Group Member based on the packet's Source Port and the Destination IP address.	One SSM

Mode	Instructions	Applies To
Network (External)	Packets are assigned to a Security Group Member based on the packet's Source IP address. If Layer 4 distribution is enabled, SSM assigns packets to a Security Group Member based on the packet's Source IP address and Destination Port.	One SSM
General	SSMs assign packets to a Security Group Member based on the packet's Source IP address and the Destination IP address. If Layer 4 distribution is enabled, SSMs assign packets to a Security Group Member based on the packet's Source IP address, Source Port, Destination IP address, and Destination Port.	All SSMs in the Chassis
Auto-Topology (Per-Port)	Each port for a Security Group Member is configured separately in the User Mode or Network Mode.	SSM data interface

Notes:

- The default mode is **Auto-Topology** (**(Per-Port)**) and the Layer 4 distribution is disabled.
- The **User** (**(Internal)**) Mode and **Network** (**(External)**) Mode can work together.
  The supported combinations are:
  - User Mode and User Mode
  - User Mode and Network Mode
  - Network Mode and Network Mode

  In many scenarios, it is possible to optimize the combination of the User Mode and Network Mode to pass traffic through same Security Group Member from the two sides.

Automatic Distribution Configuration (Auto-Topology)

By default, Security Groups work in the **Auto-Topology** (**Per Port**) Mode.

The best Distribution Mode is selected based on the Security Group topology as defined in SmartConsole in the Security Gateway object.

The Distribution Mode is automatically based on these interface types:

- Physical interfaces, except for management and synchronization interfaces
- VLAN
- Bond
- VLAN on top of Bond

The examples below show how the Distribution Mode can be configured automatically for each interface.

Example 1 - All ports on each SSM are Internal or External

The Distribution Mode for the two SSMs is automatically configured as the **User** (**Internal**) Mode or the **Network** (**External**)Mode.

Physical Interface	Topology	SSM	Distribution Mode
eth1-01	Internal	1	**User** (**Internal**)
eth1-02	Internal		
eth2-01	External	2	**Network** (**External**)
eth2-02	External		

Example 2 - On at least one of the SSMs, some ports are Internal and others are External

The Distribution Mode for the SSMs is automatically configured as **Auto-Topology** (**Per Port**).

Interface	Topology	SSM	Port	Distribution Mode
eth1-01	Internal	1	1	**User** (**Internal**)
eth1-02	External	1	2	**Network** (**External**)
eth2-01	External	2	1	**Network** (**External**)
eth2-02	External	2	2	**Network** (**External**)

Example 3 - Physical and VLAN Interfaces

Three VLANs are defined on one SSM port.

On at least one of the SSMs, some VLANs are Internal and others are External.

Therefore, the SSM Distribution Mode is automatically configured as **Auto-Topology** (**Per Port**).

Interface	Topology	SSM	Port	VLAN ID	Distribution Mode
`eth1-01`	External	1	1	NA	**Network** (**External**)
`eth1-01.100`	Internal	1	1	100	**User** (**Internal**)
`eth1-01.200`	External	1	1	200	**Network** (**External**)
`eth1-01.300`	Internal	1	1	300	**User** (**Internal**)

Example 4 - VSX Virtual Systems

A Virtual Switch does not have topology.

Therefore, the Distribution Mode is calculated based on the topologies of the `wrp` interfaces that belong to Virtual Systems, as shown.

In this example, the Distribution Mode is calculated as **Network** (**External**).

Interface	Topology	Distribution Mode
`eth1-01`	External	Not Available
`wrp64`	Internal	**Network** (**External**)
`wrp128`	Internal	**Network** (**External**)
`wrp192`	Internal	**User** (**Internal**)

Example 5 - Bond Interfaces

In this example, the interfaces on each Bond are configured with the same Distribution Mode.

The two Bond interfaces are configured with one port for SSM #1 and one port for SSM #2.

On the two SSMs, one port is Internal and the other is External.

The SSM Distribution Mode is automatically configured as **Auto-Topology** (**Per Port**).

Interface	Topology	Slaves	SSM	Port	VLAN ID
`bond1`	Internal	`eth1-01`	1	1	**User** (**Internal**)
`eth2-01`	2	1	User		
`bond2`	External	`eth1-02`	1	2	**Network** (**External**)
`eth2-02`	2	2	Network		

Example 6 - VLAN Over Bond Interfaces

The automatic Distribution Mode configuration is based on the VLAN topology.

In this example, the interfaces on each VLAN are configured with the same Distribution Mode.

The two Bond interfaces are configured on port 1 for each SSM.

The SSM Distribution Mode is automatically configured as **Auto-Topology** (**Per Port**).

Interface	Topology	Slaves	SSM	Port	VLAN ID	Distribution Mode
`bond1.100`	Internal	`eth1-01`	1	1	100	**User** (**Internal**)
`eth2-01`	2	1	100	User		
`bond1.200`	External	`eth1-01`	1	1	200	**Network** (**External**)
`eth2-01`	2	1	200	Network		

Manual Distribution Configuration (Manual-General)

In some deployments, you must manually configure a Distribution Mode to the **General**.

In other cases, it may be necessary to force the system to work in the **General** Mode.

When the Distribution Mode is manually configured (**Manual-General** Mode), the Distribution Mode of each SSM is **General**.

In this configuration, the topology of the interfaces is irrelevant.

Best Practice - Do **not** manually change 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 on a Security Group to set and show the distribution configuration.

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.

Parameter	Notes

`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-ch0x-0x:0]# printf '%x\n' 512 200 [Expert@MyChassis-ch0x-0x: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 Gaia gClish commands on a Security Group 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

Note - 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 <Name of Interface> configuration {user
| network | policy}
```

Syntax to show the interface Distribution Mode

```
show distribution interface <Name of Interface> configuration
```

Parameters

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

Examples

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

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

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

```
[Global] MyChassis-ch01-01 > 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 Gaia gClish command on a Security Group to show the status report of the Distribution Mode.

Syntax

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

Examples

Example 1 - Regular output

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show distribution status
Topic:                                  Configuration:
distribution mode                       per-port
policy mode                             on
ssm 1 mode                              per-port
ssm 2 mode                              per-port
ipv6 mode                               off
L4 mode                                 off
40g mode                                off
matrix size                             1024
[Global] MyChassis-ch01-01 >
```

Example 2 - Verbose output

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show distribution status verbose
Topic:                                  Configuration:
distribution mode                       per-port
policy mode                             on
ssm 1 mode                              per-port
ssm 2 mode                              per-port
ipv6 mode                               off
L4 mode                                 off
40g mode                                off
matrix size                             1024
interface bond1.300 mode                policy-internal
interface bond2.33 mode                 policy-external
interface bond1 slaves                  eth1-01,eth2-01
interface bond2 slaves                  eth1-02,eth2-02
mask ipv4 general destination           0000001f
mask ipv4 general source                0000001f
mask ipv4 l4 ip                         000003ff
mask ipv4 l4 port                       00000000
mask ipv4 user-network destination      000003ff
mask ipv4 user-network source           000003ff
mask ipv6 general destination           0000000000000000000000000000001f
mask ipv6 general source                0000000000000000000000000000001f
mask ipv6 user-network destination      000000000000000000000000000003ff
mask ipv6 user-network source           000000000000000000000000000003ff

Total GW topology interfaces            2
Total GW topology VLANs                 2
Total SSM 1 interfaces                  17
Total SSM 2 interfaces                  17

Per interface distribution legend:
         Internal (User)        - Destination IP based
         External (Network)     - Source IP based
         General                - Source and Destination IP based

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

Explanation about the output

Field	Instructions
`distribution mode`	Shows the currently configured Distribution Mode: ■ `per-port` - Auto-Topology ■ `user` - User (Internal) ■ `network` - Network (External) ■ `general` - General
`policy mode`	Auto-Topology assignment: ■ `on` - Auto-topology, or Manual override ■ `off` - Manual-General
`ssm 1 mode` `ssm 2 mode`	Distribution Mode assignment for SSM.
`ipv6 mode`	Shows the IPv6 status: ■ `on`- enabled ■ `off`- disabled
`l4_mode`	Shows the Layer 4 distribution status: ■ `on`- enabled ■ `off`- disabled
`40g mode`	Shows the QSFP port speed: ■ `on` - 1 x 40GbE ■ `off` - 4 x 10GbE
`matrix size`	Shows the size of the distribution matrix. The distribution matrix is a table that contains SGM IDs for traffic assignment.
`interface`	Shows the Distribution Mode assignment for each interface.

Running a Verification Test (show distribution verification)

Description

Use this Gaia gClish command on a Security Group to run a verification test of the Distribution Mode configuration.

This test compares the SGM and SSM configurations with the actual results.

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

Verbose mode shows detailed reports for all SGMs and SSMs.

Syntax

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

Example

Example - Verbose output of successful tests

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show distribution verification verbose
Test:                                          Configuration:
Verification:                    Result:
chassis 1 blade 1 dxl-general-mode             off                                 off
                         Passed
chassis 1 blade 1 dxl-md5sum                   a5a0317b8cc0de2a8518396e61593d2b
a5a0317b8cc0de2a8518396e61593d2b  Passed
chassis 1 blade 1 dxl-size                     1024                                1024
                         Passed
chassis 1 blade 2 dxl-general-mode             off                                 off
                         Passed
chassis 1 blade 2 dxl-md5sum                   a5a0317b8cc0de2a8518396e61593d2b
a5a0317b8cc0de2a8518396e61593d2b  Passed
chassis 1 blade 2 dxl-size                     1024                                1024
                         Passed
chassis 1 blade 3 dxl-general-mode             off                                 off
                         Passed
chassis 1 blade 3 dxl-md5sum                   a5a0317b8cc0de2a8518396e61593d2b
a5a0317b8cc0de2a8518396e61593d2b  Passed
chassis 1 blade 3 dxl-size                     1024                                1024
                         Passed
chassis 1 blade 4 dxl-general-mode             off                                 off
                         Passed
chassis 1 blade 4 dxl-md5sum                   a5a0317b8cc0de2a8518396e61593d2b
a5a0317b8cc0de2a8518396e61593d2b  Passed
chassis 1 blade 4 dxl-size                     1024                                1024
                         Passed
chassis 1 blade 5 dxl-general-mode             off                                 off
                         Passed
chassis 1 blade 5 dxl-md5sum                   a5a0317b8cc0de2a8518396e61593d2b
a5a0317b8cc0de2a8518396e61593d2b  Passed
chassis 1 blade 5 dxl-size                     1024                                1024
                         Passed
chassis 1 ssm 1 ipv6-mode                      on                                  on
                         Passed
chassis 1 ssm 1 l4-mode                        off                                 off
                         Passed
chassis 1 ssm 1 mask ipv4 general destination  0000001f
0000001f                         Passed
chassis 1 ssm 1 mask ipv4 general source       0000001f
0000001f                         Passed
chassis 1 ssm 1 mask ipv4 l4 ip                000000ff
000000ff                         Passed
chassis 1 ssm 1 mask ipv4 l4 port              00000003
00000003                         Passed
chassis 1 ssm 1 mask ipv4 user-network destination  000003ff
000003ff                         Passed
chassis 1 ssm 1 mask ipv4 user-network source  000003ff
000003ff                         Passed
chassis 1 ssm 1 mask ipv6 general destination  00000000000000000000000000001f
00000000000000000000000000001f  Passed
chassis 1 ssm 1 mask ipv6 general source       00000000000000000000000000001f
00000000000000000000000000001f  Passed
chassis 1 ssm 1 mask ipv6 user-network destination  00000000000000000000000000003ff
00000000000000000000000000003ff  Passed
chassis 1 ssm 1 mask ipv6 user-network source  00000000000000000000000000003ff
00000000000000000000000000003ff  Passed
chassis 1 ssm 1 matrix-max_size                2k                                  2k
                         Passed
chassis 1 ssm 1 matrix-size                    1024                                1024
                         Passed
chassis 1 ssm 1 mode                           user                                user
                         Passed
chassis 1 ssm 1 signature                      d9195da1c6de046ab3581836c911f98f
d9195da1c6de046ab3581836c911f98f  Passed
chassis 1 ssm 2 ipv6-mode                      on                                  on
                         Passed
```

```
chassis 1 ssm 2 l4-mode                              off                                  off
                         Passed
chassis 1 ssm 2 mask ipv4 general destination        0000001f
0000001f                         Passed
chassis 1 ssm 2 mask ipv4 general source             0000001f
0000001f                         Passed
chassis 1 ssm 2 mask ipv4 l4 ip                      000000ff
000000ff                         Passed
chassis 1 ssm 2 mask ipv4 l4 port                    00000003
00000003                         Passed
chassis 1 ssm 2 mask ipv4 user-network destination   000003ff
000003ff                         Passed
chassis 1 ssm 2 mask ipv4 user-network source        000003ff
000003ff                         Passed
chassis 1 ssm 2 mask ipv6 general destination        0000000000000000000000000000001f
0000000000000000000000000000001f  Passed
chassis 1 ssm 2 mask ipv6 general source             0000000000000000000000000000001f
0000000000000000000000000000001f  Passed
chassis 1 ssm 2 mask ipv6 user-network destination   0000000000000000000000000000003ff
0000000000000000000000000000003ff  Passed
chassis 1 ssm 2 mask ipv6 user-network source        0000000000000000000000000000003ff
0000000000000000000000000000003ff  Passed
chassis 1 ssm 2 matrix-max_size                      2k                                   2k
                         Passed
chassis 1 ssm 2 matrix-size                          1024                                 1024
                         Passed
chassis 1 ssm 2 mode                                 user                                 user
                         Passed
chassis 1 ssm 2 signature                            d9195da1c6de046ab3581836c911f98f
d9195da1c6de046ab3581836c911f98f  Passed
chassis 2 blade 1 dxl-general-mode                   off                                  off
                         Passed
chassis 2 blade 1 dxl-md5sum                         a5a0317b8cc0de2a8518396e61593d2b
a5a0317b8cc0de2a8518396e61593d2b  Passed
chassis 2 blade 1 dxl-size                           1024                                 1024
                         Passed
chassis 2 blade 2 dxl-general-mode                   off                                  off
                         Passed
chassis 2 blade 2 dxl-md5sum                         a5a0317b8cc0de2a8518396e61593d2b
a5a0317b8cc0de2a8518396e61593d2b  Passed
chassis 2 blade 2 dxl-size                           1024                                 1024
                         Passed
chassis 2 blade 3 dxl-general-mode                   off                                  off
                         Passed
chassis 2 blade 3 dxl-md5sum                         a5a0317b8cc0de2a8518396e61593d2b
a5a0317b8cc0de2a8518396e61593d2b  Passed
chassis 2 blade 3 dxl-size                           1024                                 1024
                         Passed
chassis 2 blade 4 dxl-general-mode                   off                                  off
                         Passed
chassis 2 blade 4 dxl-md5sum                         a5a0317b8cc0de2a8518396e61593d2b
a5a0317b8cc0de2a8518396e61593d2b  Passed
chassis 2 blade 4 dxl-size                           1024                                 1024
                         Passed
chassis 2 blade 5 dxl-general-mode                   off                                  off
                         Passed
chassis 2 blade 5 dxl-md5sum                         a5a0317b8cc0de2a8518396e61593d2b
a5a0317b8cc0de2a8518396e61593d2b  Passed
chassis 2 blade 5 dxl-size                           1024                                 1024
                         Passed
chassis 2 ssm 1 ipv6-mode                            on                                   on
                         Passed
chassis 2 ssm 1 l4-mode                              off                                  off
                         Passed
chassis 2 ssm 1 mask ipv4 general destination        0000001f
0000001f                         Passed
chassis 2 ssm 1 mask ipv4 general source             0000001f
0000001f                         Passed
```

```
chassis 2 ssm 1 mask ipv4 l4 ip                      000000ff
000000ff                          Passed
chassis 2 ssm 1 mask ipv4 l4 port                    00000003
00000003                          Passed
chassis 2 ssm 1 mask ipv4 user-network destination   000003ff
000003ff                          Passed
chassis 2 ssm 1 mask ipv4 user-network source        000003ff
000003ff                          Passed
chassis 2 ssm 1 mask ipv6 general destination        0000000000000000000000000000001f
0000000000000000000000000000001f  Passed
chassis 2 ssm 1 mask ipv6 general source             0000000000000000000000000000001f
0000000000000000000000000000001f  Passed
chassis 2 ssm 1 mask ipv6 user-network destination   0000000000000000000000000000003ff
0000000000000000000000000000003ff  Passed
chassis 2 ssm 1 mask ipv6 user-network source        0000000000000000000000000000003ff
0000000000000000000000000000003ff  Passed
chassis 2 ssm 1 matrix-max_size                      2k                                2k
                          Passed
chassis 2 ssm 1 matrix-size                          1024                              1024
                          Passed
chassis 2 ssm 1 mode                                 user                              user
                          Passed
chassis 2 ssm 1 signature                            d9195da1c6de046ab3581836c911f98f
d9195da1c6de046ab3581836c911f98f  Passed
chassis 2 ssm 2 ipv6-mode                            on                                on
                          Passed
chassis 2 ssm 2 l4-mode                              off                               off
                          Passed
chassis 2 ssm 2 mask ipv4 general destination        0000001f
0000001f                          Passed
chassis 2 ssm 2 mask ipv4 general source             0000001f
0000001f                          Passed
chassis 2 ssm 2 mask ipv4 l4 ip                      000000ff
000000ff                          Passed
chassis 2 ssm 2 mask ipv4 l4 port                    00000003
00000003                          Passed
chassis 2 ssm 2 mask ipv4 user-network destination   000003ff
000003ff                          Passed
chassis 2 ssm 2 mask ipv4 user-network source        000003ff
000003ff                          Passed
chassis 2 ssm 2 mask ipv6 general destination        0000000000000000000000000000001f
0000000000000000000000000000001f  Passed
chassis 2 ssm 2 mask ipv6 general source             0000000000000000000000000000001f
0000000000000000000000000000001f  Passed
chassis 2 ssm 2 mask ipv6 user-network destination   0000000000000000000000000000003ff
0000000000000000000000000000003ff  Passed
chassis 2 ssm 2 mask ipv6 user-network source        0000000000000000000000000000003ff
0000000000000000000000000000003ff  Passed
chassis 2 ssm 2 matrix-max_size                      2k                                2k
                          Passed
chassis 2 ssm 2 matrix-size                          1024                              1024
                          Passed
chassis 2 ssm 2 mode                                 user                              user
                          Passed
chassis 2 ssm 2 signature                            d9195da1c6de046ab3581836c911f98f
d9195da1c6de046ab3581836c911f98f  Passed

Summary:
all active SSMs are configured as: user
all active SSMs are configured as: user
[Global] MyChassis-ch01-01 >
```

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

Description

Use these commands in Gaia gClish on a Security Group 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

Syntax

`set distribution l4-mode enabled [ip-mask <IP Mask> [port-mask <Port Mask>]]`
`set distribution l4-mode disabled`
`show distribution l4-mode`

Note - The "`ip-mask`" and "`port-mask`" configuration applies to SSM160.

Examples

Example 1 - Configure the Layer 4 Distribution Mode

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > set distribution l4-mode enabled
ip-mask 7F port-mask 3
2_01:
masks update completed successfully
[Global] MyChassis-ch01-01 >
```

Example 2 - Disable the Layer 4 Distribution Mode

```
[Expert@MyChassis-ch0x-0x: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

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show distribution l4-mode
2_01:
L4 Distribution: Enabled
L4 Distribution IP mask: 0x0000007f
L4 Distribution port mask: 0x00000003
[Global] MyChassis-ch01-01 >
```

Port Forwarding on the Management Interface

Initiating traffic from an SGM (that is not the SMO) through the Security Group's management interface, such as `eth1-mgmt4`, only works with UDP and TCP:

Protocol	Allowed Traffic
TCP	■ SSH ■ DNS (port 53) ■ Remote Threat Emulation (port 18194) ■ LDAP ■ TACACS ■ SMTP ■ Certificate Revocation List (CRL) ■ Check Point Daemon (CPD) ■ URL Filtering with a proxy ■ URL Filtering without a proxy
UDP	■ DNS ■ RADIUS ■ TACACS ■ SYSLOG ■ NTP

To add new allowed ports to the list:

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.

Step	Instructions
3	Edit the `$FWDIR/conf/fw_global_params.conf` file: `vi $FWDIR/conf/fw_global_params.conf`

4	Add this line:
	■ For TCP ports:
	`mgmt_forwarding_tcp_ports_list_string="<Port1>,<Port2>,....,<PortN>"`
	■ For UDP ports:
	`mgmt_forwarding_udp_ports_list_string="<Port1>,<Port2>,....,<PortN>"`
	Example for TCP ports:
	`mgmt_forwarding_tcp_ports_list_string="55010,55011,55012"`

5	Save the changes in the file and exit the editor.
6	Copy the modified file to all SGMs in the Security Group: `g_cp2blades $FWDIR/conf/fw_global_params.conf`
7	Apply the new configuration: `g_all cpha_blade_config fw_global_params_changed`

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 the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`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 Member.

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 cannot change the state of a Security Group Member to **UP** if it is in the **DOWN** state because of a software or hardware problem.
- The "`g_clusterXL_admin`" command generates log entries.
  To see these log entries, run:

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

Example

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x:0]#
```

Configuring a Unique MAC Identifier (asg_unique_mac_utility)

In This Section:

Background

When there are more than one Security Group on a Layer 2 segment, the Unique MAC Identifier must be different for each Security Group.

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 "`ethX-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.

Use the "`asg_unique_mac_utility`" command in Gaia gClish or the Expert mode to set:

- Data interface Unique MAC Identifier
- Host name

Configuring the Unique MAC Identifier Manually

Step	Instructions
1	Connect to the command line on the Security Group.
2	Run this command in Gaia gClish or the Expert mode: `asg_unique_mac_utility`

3	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`

4	Reboot the Security Group to apply the new Unique MAC Identifier: `reboot -b all`

Options of the Unique MAC Identifier Utility

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.

This command shows summary or verbose information.

Syntax

```
asg_arp -h
```

```
asg_arp [-b <SGM IDs>] [-v] [--verify] [-i <Name of Interface>] [-m <MAC Address>] [<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 the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)
`-i <Name of Interface>`	Shows the ARP cache for the specified interface.
`-m <MAC Address>`	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 all Chassis 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-ch0x-0x: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-ch0x-0x:0]#
```

Example Verbose Output

This example shows the ARP cash in the Verbose Mode:

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x:0]#
```

Example Output for Verifying MAC Addresses

This example shows the output of the MAC address verification (on a Single Chassis):

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x: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-ch0x-0x: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 for interfaces of the type `eth`*X*`-`*YZ* with the "`ifconfig`" command in the Expert mode.

Example:

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x:0]#
```

Example Legacy Output

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

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x:0]#
```

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) - the 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	Instructions
`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 in the Expert mode:

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

To apply the intervals, run in the Expert mode:

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

Verification

To send GARP Requests manually, on the SMO, run in the Expert mode:

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

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

To debug, run in the Expert mode:

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

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	Guidelines
Not using NAT rules	Set the Distribution Mode to **General**.

NAT Rules	Guidelines
Using NAT rule	■ Set the Distribution Mode to **User** for the networks hidden behind NAT. ■ Set the Distribution Mode to **Network** for the destination networks.

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 a specified Virtual System on the same Security Group Member.

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 checks the distribution again according to the Distribution Mode configured on the WRP interface. It can decide to forward the packet to a different Security Group Member.

In addition, on each Virtual System, the stateful Correction Layer 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	Guidelines
Not using NAT rules on any Virtual System	Set the Distribution Mode to **General**.
Using NAT rule on at least one Virtual System	■ On the Virtual Systems that use NAT rules: • Set the Distribution Mode to **User** for the networks hidden behind NAT. • Set the Distribution Mode to **Network** for the destination networks. ■ On the remaining Virtual Systems that do not use NAT rules: • Set the Distribution Mode to **User** for the internal networks. • Set the Distribution Mode to **Network** for the external networks.

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 provide High Availability.

You must run this command in the Expert mode.

Syntax to configure the IPS behavior during a cluster failover

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

Parameters

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

Syntax to view the configured IPS behavior during a cluster failover

```
fw ctl get int fwha_ips_reject_on_failover
```

Explanation:

Output	Current Configuration
`fwha_ips_reject_on_failover = 0`	Prefers connectivity
`fwha_ips_reject_on_failover = 1`	Prefers security

Dual Chassis in Active/Standby High Availability Mode

This chapter describes how to deploy Dual Chassis in Active/Standby High Availability.

How Active/Standby Mode Works

Background

The Dual Chassis High Availability mechanism is based on two identical Chassis.

One Chassis handles traffic (Active state), while the other Chassis is in the Standby state.

The Standby Chassis synchronizes with the Active Chassis, so that traffic continues uninterrupted when there is a Chassis failover.

- Chassis High Availability works on the principle that the Chassis with the highest **quality grade** becomes the Active Chassis.

  To make sure that the most reliable Chassis is Active, each Chassis is assigned a quality grade.

  The quality grade is based on a continuous monitoring of Chassis critical components and traffic characteristics.

  Automatic failover occurs only when the quality grade of the Standby Chassis is greater than the quality grade of the Active Chassis, plus the minimum differential.

  A configurable minimum grade differential prevents unnecessary failover, which can cause performance degradation.

  See:

  - *"Configuring Chassis High Availability" on page 103*
  - *"Setting the Quality Grade Differential" on page 107*
  - *"Setting Chassis Weights (Chassis High Availability Factors)" on page 103*
- Each Chassis port has its own unique MAC address.

  The MAC addresses for SGMs are the same on the same Chassis.

  The MAC addresses are different for the ports on the two Chassis.

  A Chassis failover event sends GARP / ICMPv6 packets for each interface. This informs the network to use the other interfaces.

  See *"Working with the GARP Chunk Mechanism" on page 95*.

With the applicable Gaia gClish commands, you configure these High Availability parameters:

- Chassis High Availability - "Active Up" Mode or "Primary Up" Mode.
- Chassis quality grade factors
- Failover grade difference for failover
- Failover freeze interval
- Port priority

Configuring Active/Standby Mode

Syntax

```
set chassis high-availability mode <Mode ID>
```

Available Modes

Mode ID	Mode Title	Mode Description
0	**Active/Standby - Active Up**	No primary Chassis. The currently Active Chassis stays Active unless it goes DOWN, or the Standby Chassis has a higher Chassis quality grade.
1	**Active/Standby - Primary Up**	Active Chassis always stays Active unless it goes DOWN, or the Standby Chassis has a higher Chassis quality grade. See *"Setting the Chassis Priority" on page 109*.
2	Not available	Not supported.
3	**Standby Chassis VSLS Mode**	In VSX, provides Virtual System Load Sharing.

Synchronizing Dual Chassis on a Wide Area Network

You can install your Chassis at two different remote sites as a geographically distributed cluster.

There are two limitations to this capability:

1. The synchronization network must guarantee no more than 100ms latency and no more than 5% packet loss.
2. The synchronization network can include switches and hubs.

   Routers cannot be installed on the synchronization network because they drop Cluster Control Protocol packets.

Configuring Chassis High Availability

In This Section:

Use these settings to configure Active/Standby Chassis.

Setting Chassis Weights (Chassis High Availability Factors)

Each hardware component in a Chassis has a quality weight factor, which sets its relative importance to overall Chassis health.

For example, ports are more important than fans and are typically assigned a higher weight value.

The Chassis grade is the sum of all component weight values.

In a High Availability environment, the Chassis with the higher grade becomes Active and handles traffic.

The grade for each component is calculated based on this formula:

```
(Unit Weight) x (Number of UP components)
```

To see the weight of each component, run in Gaia gClish:

```
asg stat -v
```

Description

Use the "`set chassis high-availability factors`" command to configure a hardware component's weight.

Syntax in Gaia gClish of the Security Group

`set chassis high-availability factors sgm <`*`SGM Factor`*`>`
`set chassis high-availability factors port {other <`*`Other Port Factor`*`> | standard <`*`Standard Port Factor`*`> | mgmt <`*`Management Port Factor`*`> | bond <`*`Bond Port Factor`*`>}`
`set chassis high-availability factors sensor {cmm <`*`CMM Factor`*`> | fans <`*`Fans Factor`*`> | power_supplies <`*`PSU Factor`*`> | ssm <`*`SSM Factor`*`>}`

Parameters

Parameter	Description
<SGM Factor>	Weight factor for a Security Group Member. Valid range: integer between 0 and 1000.
<Other Port Factor>	High grade port factor. Valid range: integer between 0 and 1000.
<Standard Port Factor>	Standard grade port factor. Valid range: integer between 0 and 1000.
<Management Port Factor>	Management port factor. Valid range: integer between 0 and 1000.
<Bond Port Factor>	Bond interface factor. Valid range: integer between 0 and 1000.
<CMM Factor>	Weight factor for a CMM. Valid range: integer between 0 and 1000.
<Fans Factor>	Weight factor for a fan unit. Valid range: integer between 0 and 1000.
<PSU Factor>	Weight factor for a Power Supply Unit. Valid range: integer between 0 and 1000.
<SSM Factor>	Weight factor for a SSM. This factor applies to all SSMs. Valid range: integer between 0 and 1000.

Examples

```
[Global] MyChassis-ch01-01 > set chassis high-availability factors sgm 100
[Global] MyChassis-ch01-01 > set chassis high-availability factors port other 70
[Global] MyChassis-ch01-01 > set chassis high-availability factors port standard 50
[Global] MyChassis-ch01-01 > set chassis high-availability factors sensor cmm 40
[Global] MyChassis-ch01-01 > set chassis high-availability factors sensor fans 30
[Global] MyChassis-ch01-01 > set chassis high-availability factors sensor power_supplies 20
[Global] MyChassis-ch01-01 > set chassis high-availability factors sensor ssm 45
```

Setting the Chassis ID

You must make sure that the Chassis IDs are **different** before you start to configure the software.

Chassis IDs are configured on the CMM and should be **1** for the first Chassis and **2** for the second Chassis.

Important - If the Chassis is up and running, change the Chassis ID on the Standby Chassis. You must perform a Chassis failover.

Step	Instructions
1	Pull out the first CMM from the Chassis.
2	Connect to the remaining CMM with a serial cable (baud rate - 9600).
3	Log in with these user name and password: `admin` / `admin`
4	Edit the `/etc/shmm.cfg` file: `vi /etc/shmm.cfg`
5	Search for: `SHMM_CHASSIS=`

6	Set the correct Chassis ID:
	■ For Chassis 1:
	`SHMM_CHASSID="1"`
	■ For Chassis 2:
	`SHMM_CHASSID="2"`

7	Save the changes in the file and exit the editor.
8	Remove the current CMM and insert the second CMM.
9	Repeat Steps 2 - 6 for the second CMM.
10	Insert both CMMs into the Chassis.
11	Attach the correct identification labels to the Chassis and CMMs. This step is required if the Chassis has already been configured (after the First Time Configuration Wizard).

Step	Instructions
12	Pull out all SGMs from the Chassis. Insert all SGMs into the Chassis. **Important** - This step causes a hard reboot of the Chassis.

Setting the Quality Grade Differential

Description

Use the "`set chassis high-availability failover`" command in Gaia gClish to set the minimum quality grade differential that causes a failover.

Syntax in Gaia gClish of the Security Group

```
set chassis high-availability failover <Trigger>
```

Parameters

Parameter	Description
<Trigger>	Minimum difference in Chassis quality grade to trigger a failover. Valid range: Integer between 1 and 1000.

Setting the Failover Freeze Interval

Description

A Standby Chassis cannot failover a second time until the specified failover freeze interval expires.

The default failover freeze interval is:

- For the "Active Up" chassis configuration - 30 seconds
- For the "Primary Up" chassis configuration - 150 seconds
- For VSX Virtual System Load Sharing (VSLS) configuration - 150 seconds

If the Standby Chassis grade changes to a value greater than the minimum quality grade gap for a failover, the Standby Chassis fails over and becomes a new Active.

The failover does not start until the freeze interval expires. This confirms that the Standby Chassis quality grade is stable, before it becomes a new Active.

For example, a Standby Chassis quality grade can become unstable if a fan speed increases and decreases frequently.

Syntax in Gaia gClish of the Security Group

```
set chassis high-availability freeze_interval <Freeze Interval>
```

Parameters

Parameter	Description
<Freeze Interval>	Minimum time in seconds to wait until the next Standby Chassis failover. Valid range: integer between 1 and 1000.

Notes:

- When you run the "`asg stat`" command after Standby Chassis failover, the output shows the freeze time.
- The *<Freeze Interval>* value is 5 fold greater, if the setup is configured to work in VSLS or "Primary Up" mode.
  Example: If the freeze time must be 250 seconds, you must enter the value 50.

Setting the Chassis Priority

After you configure the High Availability with the "`set chassis high-availability mode 1`" command (see *"How Active/Standby Mode Works" on page 101*), you must configure the chassis priority:

```
set chassis high-availability vs chassis_priority "<ID of Primary Chassis> <ID of Secondary Chassis>"
```

Example - set Chassis 2 to be the Primary over Chassis 1:

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > set chassis high-availability vs chassis_priority "2 1"
[Global] MyChassis-ch01-01 >
```

Advanced Features

In This Section:

The Interface Link Preemption Mechanism

The Interface Link Preemption Mechanism prevents constant Chassis failover and fallback when the interface link state changes frequently.

When you enable this feature, an interface state that changes from DOWN to UP is included in the Chassis grade only if the link state is UP for at least "N" seconds.

The Interface Link Preemption Mechanism is enabled by default with the preemption time of 5 seconds.

Syntax to show the current configured link preemption time

Shell	Syntax
Gaia Clish	`fw ctl get int fwha_ch_if_preempt_time`
Expert mode	`g_fw ctl get int fwha_ch_if_preempt_time`

Syntax to configure the link preemption time on-the-fly (does not survive reboot)

Shell	Syntax
Gaia Clish	`fw ctl set int fwha_ch_if_preempt_time <Preemption Time>`
Expert mode	`g_fw ctl set int fwha_ch_if_preempt_time <Preemption Time>`

Syntax to configure the link preemption time permanently (survives reboot)

Shell	Syntax
Gaia Clish	`update_conf_file fwkern.conf fwha_ch_if_preempt_time=<Preemption Time>`
Expert mode	`g_update_conf_file fwkern.conf fwha_ch_if_preempt_time=<Preemption Time>`

Syntax to disable the link preemption mechanism on-the-fly (does not survive reboot)

Shell	Instructions
Gaia Clish	`fw ctl set int fwha_ch_if_preempt_time 0`
Expert mode	`g_fw ctl set int fwha_ch_if_preempt_time 0`

Syntax to disable the link preemption mechanism permanently (survives reboot)

Shell	Syntax
Gaia Clish	`update_conf_file fwkern.conf fwha_ch_if_preempt_time=0`
Expert mode	`g_update_conf_file fwkern.conf fwha_ch_if_preempt_time=0`

Parameters

Parameter	Description
<Preemption Time>	The interface link preemption time. An interface state that changes from DOWN to UP is included in the Chassis grade only if the link state is UP for at least this specified number of seconds. Default: 5 seconds

Example

```
[Expert@MyChassis-ch0x-0x:0]# g_fw ctl set int fwha_ch_if_preempt_
time 20
[Expert@MyChassis-ch0x-0x:0]# g_update_conf_file fwkern.conf fwha_
ch_if_preempt_time=20
```

The Sync Lost Mechanism in High Availability

The Chassis uses the Check Point proprietary Cluster Control Protocol (CCP) to send control packets between two High Availability Chassis.

When a Sync interface fails on one Chassis, it is necessary to update the other Standby Chassis.

The Sync Lost Mechanism handles the loss of connectivity between the two Chassis on the Sync network.

The Sync Lost Mechanism is enabled by default.

To prevent the two Chassis from changing their states to Active, the Chassis on which the Sync interface failed, sends the CCP packets "`sync_lost`" over the non-sync interface (the Data Ports and Management interfaces) to the other Chassis. This causes the two Chassis to freeze their current states until connectivity between the two Chassis is restored. During the Sync Loss, the Standby Chassis does not change its state to Active until it stops receiving the CCP packets "`sync_lost`" from the other Chassis.

The Chassis sends the CCP packets "`sync_lost`" in this manner:

- In a non-VSX environment - All Chassis interfaces send these CCP packets
- In a VSX environment - All interfaces of the VS0 context only send these CCP packets

Syntax to show current state of the Sync Lost Mechanism

Shell	Syntax
Gaia Clish	`fw ctl get int fwha_ch_sync_lost_mechanism_enabled`
Expert mode	`g_fw ctl get int fwha_ch_sync_lost_mechanism_enabled`

Explanation for the returned values:

- 0 - disabled
- 1 - enabled

Syntax to enable the Sync Lost Mechanism on-the-fly (does not survive reboot)

Shell	Syntax
Gaia Clish	`fw ctl set int fwha_ch_sync_lost_mechanism_enabled 1`
Expert mode	`g_fw ctl set int fwha_ch_sync_lost_mechanism_enabled 1`

Syntax to enable the Sync Lost Mechanism permanently (survives reboot)

Shell	Syntax
Gaia Clish	`update_conf_file fwkern.conf fwha_ch_sync_lost_mechanism_enabled=1`
Expert mode	`g_update_conf_file fwkern.conf fwha_ch_sync_lost_mechanism_enabled=1`

Syntax to disable the Sync Lost Mechanism on-the-fly (does not survive reboot)

Shell	Instructions
Gaia Clish	`fw ctl set int fwha_ch_sync_lost_mechanism_enabled 0`
Expert mode	`g_fw ctl set int fwha_ch_sync_lost_mechanism_enabled 0`

Syntax to disable the Sync Lost Mechanism permanently (survives reboot)

Shell	Syntax
Gaia Clish	`update_conf_file fwkern.conf fwha_ch_sync_lost_mechanism_enabled=0`
Expert mode	`g_update_conf_file fwkern.conf fwha_ch_sync_lost_mechanism_enabled=0`

Managing the Connection Synchronization

You can manage connection synchronization for High Availability.

Syntax to configure the connection synchronization mode on-the-fly (does not survive reboot):

Shell	Syntax
Gaia Clish	`fw ctl set int fwha_sync_excp_mask <Mode>`
Expert mode	`g_fw ctl set int fwha_ch_sync_lost_mechanism_enabled <Mode>`

Syntax to configure the connection synchronization mode permanently (survives reboot):

Shell	Syntax
Gaia Clish	`update_conf_file fwkern.conf fwha_sync_excp_mask=<Mode>` `reboot -b all`
Expert mode	`g_update_conf_file fwkern.conf fwha_sync_excp_mask=<Mode>` `g_reboot -b all`

Syntax to show the configured connection synchronization mode

```
asg stat -v
```

Parameters

Parameter	Description
<Mode>	Specifies the Connection Synchronization Mode: ■ `0` - Disables the backup synchronization on the Active Chassis and the Standby Chassis ■ `1` - Synchronizes only the backup member on the Active Chassis ■ `2` - Synchronizes only the backup member on the Standby Chassis ■ `3` - Synchronizes the backup member on the Active Chassis and the Standby Chassis

Working with SyncXL

SyncXL™ is a Check Point technology that makes sure that active connections are only synchronized to one Security Group Member (SGM) on the Active Chassis and the Standby Chassis.

When the state of an SGM or Standby Chassis changes, all SGMs update their counterpart SGMs.

These events automatically trigger the synchronization:

Event	Description
SGM Failure	Connections with a backup connection on an SGM are synchronized to a backup SGM
SGM Recovery	The newly recovered SGM can be: ■ A backup for connections that are active on other SGMs ■ Active for connections before the SGM failure
Standby Chassis High Availability Failover	When the Active Chassis fails over to the Standby Chassis, a backup entry is defined for each connection the Active Chassis handles.

Ratio between SGMs on the Standby Chassis and the Active Chassis

- To handle load and capacity, the Standby Chassis must have at least 50% of its SGMs in the UP state, compared with the Active Chassis.

  For example, if there are 10 SGMs in the UP state on the Active Chassis, there must be at least 5 SGMs in the UP state on the Standby Chassis.

  SyncXL is automatically disabled if this condition is not met.

  The kernel parameter "`fwha_sync_between_chassis_blades_ratio`" controls the ratio threshold (default is 50%):

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.

Step	Instructions
3	Configure the required value for the kernel parameter in the current session (does not survive reboot): `g_fw ctl set int fwha_sync_between_chassis_blades_ratio <Value>`
4	Configure the required value for the kernel parameter permanently (survives reboot): `g_update_conf_file fwkern.conf fwha_sync_between_chassis_blades_ratio=<Value>`

- Make sure that each active connection has backups on both Standby Chassis in a Dual Chassis:

  Set the value of the kernel parameter "`fwha_sync_excp_mask`" to `3` as described in *"Managing the Connection Synchronization" on page 114*.

Notes:

- VoIP connections are synchronized to all SGMs.
- Local connections (to and from the Standby Chassis's pseudo IP address) are not synchronized.
- SyncXL does not work on the Sync interface, or the Management interface.

Setting the Administratively DOWN State on First Join

Description

You can configure the Chassis to set a newly installed SGM in a Security Group to be in the administratively DOWN state automatically.

The administrator can confirm that the SGM is configured correctly before changing its state to UP.

Syntax

```
set chassis high-availability down_on_first_join {0 | 1}
```

- 0 - Do **not** enable the administratively DOWN state automatically on an SGM on first join
- 1 - Enable the administratively DOWN state automatically on an SGM first join

To add a new SGM to a Security Group in the administratively DOWN state

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to Gaia Clish.
3	Go to Gaia gClish: enter `gclish` and press Enter.
4	Enable the administratively DOWN state automatically on an SGM first join: `set chassis high-availability down_on_first_join 1`
5	Install a new SGM into the Chassis. See *"Adding or Replacing an SGM" on page 351*.
6	Add the new SGM to the Security Group: `add smo security-group <SGM ID>` See *"Security Group" on page 16*.
7	Make sure the SGM configuration is correct.
8	Change the SGM state to UP: `g_clusterXL_admin -b <SGM IDs> up` See *"Configuring the Cluster State (g_clusterXL_admin)" on page 86*.

Configuring a Unique IP Address for Each Standby Chassis (UIPC)

In a Dual Chassis deployment:

- A heavy load on the Active Chassis can prevent you from creating a network connection to the SMO and working with management tasks.
- It can be necessary to have a direct access to the Standby Chassis to troubleshoot a problem, such as an SGM in the DOWN state.

  You cannot use the SMO to connect to the Standby Chassis.

You can assign a unique IP address to each Standby Chassis to help resolve these issues.

This adds an extra alias IP alias addres to the management interfaces on all SGMs.

When there is a high load on the SMO, connect to the Standby Chassis using the unique IP address you assigned to the Standby Chassis.

The SGMs on the Standby Chassis are always in the UP state and available to run Gaia gClish commands.

Notes:

- The UIPC feature is disabled by default.
- Only one SGM "owns" the UIPC task.
- If the Standby Chassis is not managed through a management port, you can add the unique IP address to one of the data ports.
  The connection to the unique IP address reaches a specific SGM based on the distribution configuration.

Description

Use the "`set chassis id`" command in Gaia gClish to assign a unique IP address to a Standby Chassis.

Important:

- The UIPC feature is enabled automatically after you run the "`set chassis id`" command.
- After you assign a unique IP address to a Standby Chassis, you must make sure the Access Control policy of the Security Group allows the connection to the alias IP address.

Syntax

```
set chassis id <Standby Chassis ID> general unique_ip <IP Address>
delete chassis id <Standby Chassis ID> general unique_ip
show chassis id <Standby Chassis ID> general unique_ip
```

Parameters

Parameter	Description
<Standby Chassis ID>	Specifies the Standby Chassis ID. Valid values: ■ 1 ■ 2
<IP Address>	Specifies the alias IP address on the same network as one of the SGMs interfaces.

Example 1 - Adding a UIPC

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > set chassis id 1 general unique_ip 172.16.6.186
1_01:
Adding alias IP: 172.16.6.186 mask 255.255.255.0 on chassis 1 to interface eth1-Mgmt4
1_02:
Adding alias IP: 172.16.6.186 mask 255.255.255.0 on chassis 1 to interface eth1-Mgmt4
2_01:
2_02:
Alias IP was added successfully
Alias IP address should be added to the policy rulebase in SmartDashBoard
[Global] MyChassis-ch01-01 >
```

Example 2 - Deleting a UIPC

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > delete chassis id 1 general unique_ip
1_01:
Deleting alias IP 172.16.6.186 of chassis 1
1_02:
Deleting alias IP 172.16.6.186 of chassis 1
2_01:
2_02:
Alias IP was deleted successfully
Alias IP address should be removed from the policy rulebase in SmartDashBoard
[Global] MyChassis-ch01-01 >
```

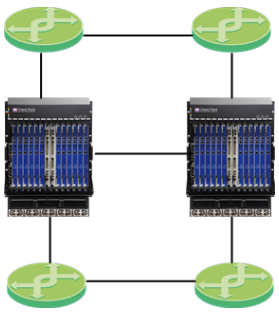
Dual Chassis in Bridge Mode

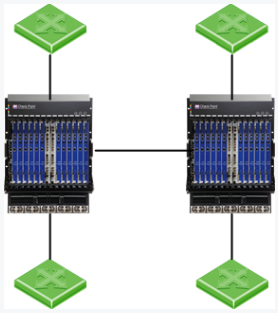
In This Section:

This chapter describes how to deploy Dual Chassis in Layer 2 Bridge mode.

Bridge Mode Topologies

Active/Active Bridge Mode supports these topologies:

Topology	Description	Diagram
Layer 2 connectivity between Chassis	This topology requires Spanning Tree Protocol (STP) on the Layer 2 switches. STP is a network protocol that confirms a loop-free topology for Ethernet networks. STP sends special data frames called Bridge Protocol Data Units (BPDUs). These BPDUs help the switches select which port to block, if there is a loop detection. The BPDUs get to the switch from a different interface when they pass through the bridge interface of the chassis. This results in a successful blockage.	

Topology	Description	Diagram
No Layer 2 connectivity between Chassis	This topology does not require STP on the Layer 2 switches. It is usually a router-based topology, where a dynamic routing protocol selects through which segment to route the traffic.	

BPDU

The BDPU maximum age timer controls the maximum length of time that passes before a bridge port saves its configuration BPDU information.

The default time it takes to reach a chassis failover is 20 seconds. It is possible to configure be configure this time to a value from 6 to 40 seconds.

Example for Cisco switches:

Use the "`spanning-tree vlan`" command on each VLAN to configure the BDPU maximum age timer. For more information, see Cisco documentation.

Configuring Bridge Interfaces in Gateway Mode

Description

Use the applicable commands in Gaia gClish to work with Bridge interfaces.

For more information, see the *R81 Scalable Platforms Gaia Administration Guide* > Chapter *Network Management* > Section *Network Interfaces* - Subsection *Bridge Interfaces*.

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > add bridging group 2
[Global] MyChassis-ch01-01 >
[Global] MyChassis-ch01-01 > add bridging group 2 interface eth2
[Global] MyChassis-ch01-01 >
[Global] MyChassis-ch01-01 > add bridging group 2 interface eth3
[Global] MyChassis-ch01-01 >
[Global] MyChassis-ch01-01 > show bridging group 2
Bridge Configuration
    Bridge Interfaces
        eth2
        eth3
[Global] MyChassis-ch01-01 >
```

Configuring Bridge Interfaces in VSX Mode

Configure a Virtual System in Bridge Mode when you first create its object.

For more information, see the *R81 Scalable Platforms VSX Administration Guide*.

To configure an existing Virtual System in Active/Standby Bridge Mode:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server, or the *Target* Domain Management Server that manages this Virtual System.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the Virtual System object.
4	In **Virtual System General Properties**, select **Bridge Mode**.
5	Click **Next**. The **Virtual System Network Configuration** window opens.
6	Configure the external and internal interfaces for the Virtual System.
7	Click **Next**.
8	Click **Finish**.
9	Connect to the command line on the Security Group.
10	Log in to Gaia Clish.
11	Go to Gaia gClish: enter `gclish` and press Enter.
12	Switch to the context of the applicable Virtual System: `set virtual-system <VS ID>`
13	Examine the interfaces: `show interfaces all`

Configuring Virtual Systems in Bridge Mode to Forward Non-IP Protocols

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Create the required empty file on all Security Group Members: `g_all touch $FWDIR/conf/enable_non_ip_protocols`
4	Follow *"Configuring Bridge Interfaces in VSX Mode" on the previous page*.

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:

Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
IPv6 Neighbor Discovery	Network object that represents the Bridged Network	Network object that represents the Bridged Network	Any	neighbor-advertisement neighbor-solicitation router-advertisement router-solicitation redirect6	Accept	Log	Policy Targets

Logging and Monitoring

CPView

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 Group).

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

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

For more information, see sk101878.

Syntax

```
cpview --help
```

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.

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_<ID of the cpview process>.cap<Number of the capture>`
H	Shows a tooltip with CPView options.
Space bar	Immediately refreshes the statistics.

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 Address>`

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Shows information about all interfaces.
`-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 Address>`	Shows information only about one 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-ch0x-0x: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-ch0x-0x: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-ch0x-0x: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>"
  ```

Monitoring Traffic (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	Instructions
Native	This is the default setting. When you do not specify the "analyze" or "banalyze" option in the syntax, the command behaves almost in 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 parameters "analyze" and "banalyze" are mutually exclusive.
  You cannot specify them in the same command.
- If you run this command in the context of a Virtual System, you can only see the output that applies to that context.

Syntax

```
asg_ifconfig -h
```

```
asg_ifconfig [-b <SGM IDs>] [<Name of Interface>] [analyze [-d
<Delay>] [-a] [-v]]
```

```
asg_ifconfig [-b <SGM IDs>] [<Name of Interface>] [banalyze [-d
<Delay>] [-a] [-v] [-rb] [-rd] [-rp] [-tb] [-td] [-tp]]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)
`<Name of Interface>`	Specifies the name of the interface.
`analyze`	Shows accumulated traffic information and traffic distribution between the Security Group Members. Use the "`-a`", "`-v`", and "`-d <Delay>`" parameters to show traffic distribution between interfaces.

Parameter	Description

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

`-d <Delay>`	Delay, in seconds, between data samples. Default: 5 seconds.
`-a`	Shows total traffic volume. By default (without "`-a`"), the output shows the average traffic volume per second.
`-v`	Verbose mode. Shows detailed information of each interface and the accumulated traffic information

Examples

Example 1 - Default output

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

By default, the output shows the average traffic volume per second.

```
[Expert@MyChassis-ch0x-0x: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>
```

Example 2 - The 'analyze' mode

This example shows:

- The accumulated and detailed traffic volume statistics for the interface `eth2-Sync` for each Security Group Member.
- The total for all Security Group Members.
- The traffic distribution for each Security Group Member.
- The "`-a`" option shows the total traffic volume instead of the average volume per second.

```
[Expert@MyChassis-ch0x-0x: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>
```

Example 2 - The 'banalyze' mode

This example shows:

- The accumulated and detailed traffic volume statistics for the interface `eth2-Sync` on each Security Group Member.
- The total on each Security Group Member.
- The traffic distribution on each Security Group Member.
- The "`-a`" option shows the total traffic volume instead of the average volume per second.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> asg_ifconfig eth2-Sync banalyze -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

=*= Accumulative =*=
            RX: packets:225018 bytes:36970520 (37.0 MiB)  dropped:0
            TX: packets:3522445 bytes:1381032583 (1.4 GiB)  dropped:0

=*= Traffic Distribution =*=

------------------------------------------------------------------------------
  Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
------------------------------------------------------------------------------
 eth2-Sync  100.0%     100.0%     0.0%     100.0%     100.0%   0.0%
------------------------------------------------------------------------------

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

=*= Accumulative =*=
            RX: packets:221395 bytes:35947248 (35.9 MiB)  dropped:0
            TX: packets:4674143 bytes:1850315554 (1.9 GiB)  dropped:0

=*= Traffic Distribution =*=

------------------------------------------------------------------------------
  Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
------------------------------------------------------------------------------
 eth2-Sync  100.0%     100.0%     0.0%     100.0%     100.0%   0.0%
------------------------------------------------------------------------------

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

=*= Accumulative =*=
            RX: packets:10 bytes:644 (644.0 b)  dropped:0
            TX: packets:67826313 bytes:7345458105 (7.3 GiB)  dropped:0

=*= Traffic Distribution =*=

------------------------------------------------------------------------------
  Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
------------------------------------------------------------------------------
 eth2-Sync  100.0%     100.0%     0.0%     100.0%     100.0%   0.0%
------------------------------------------------------------------------------

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

=*= Accumulative =*=
            RX: packets:13 bytes:860 (860.0 b)  dropped:0
            TX: packets:68489217 bytes:7487476060 (7.5 GiB)  dropped:0

=*= Traffic Distribution =*=

------------------------------------------------------------------------------
```

```
  Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
------------------------------------------------------------------------------
 eth2-Sync  100.0%     100.0%     0.0%     100.0%     100.0%   0.0%
------------------------------------------------------------------------------

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 =*=
            RX: packets:203386 bytes:19214238 (19.2 MiB)  dropped:0
            TX: packets:7164109 bytes:2740761091 (2.7 GiB)  dropped:0

=*= Traffic Distribution =*=

------------------------------------------------------------------------------
  Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
------------------------------------------------------------------------------
 eth2-Sync  100.0%     100.0%     0.0%     100.0%     100.0%   0.0%
------------------------------------------------------------------------------

=*= All Blades =*=
      RX: packets:649822 bytes:92133510 (92.1 MiB)  dropped:0
      TX: packets:148153782 bytes:20805043393(20.8 GiB)  dropped:0

=*= Traffic Distribution =*= (all blades)

------------------------------------------------------------------------------
  Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
------------------------------------------------------------------------------
 eth2-Sync  100.0%     100.0%     0.0%     100.0%     100.0%   0.0%
------------------------------------------------------------------------------
[Global] MyChassis-ch01-01>
```

Monitoring Multicast Traffic

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 <Destination Route>] [-s <Source Route>] [-i
<Source Interface>][-b <SGM IDs>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
No Parameters	Shows all routes, interfaces and Security Group Members.
`-d <Destination Route>`	Specifies the destination multicast group IP address.
`-s <Source Route>`	Specifies the source IP address.
`-i <Source Interface>`	Specifies the source interface name.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)

Examples

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

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x: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-ch0x-0x: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 as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`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`.

Examples

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

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x: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-ch0x-0x:0]#
```

Example 3 - Shows PIM neighbors

```
[Expert@MyChassis-ch0x-0x: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 the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)

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-ch0x-0x: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-ch0x-0x: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-ch0x-0x: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 Gateway (Security Group) object.

You can still see VPN tunnel status and details information in SmartConsole.

SNMP

- You can use the OID sub-tree **tunnelTable** (.1.3.6.1.4.1.2620.500.9002) in the Check Point MIB to see the VPN status.
- For VSX environments, search for the *SNMP Monitoring* section in the *R81 Scalable Platforms VSX Administration Guide* for VSX-related SNMP information.

CLI Tools

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

Use these commands:

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

  ```
  cpstat -f all vpn
  ```

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

  ```
  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, run in Gaia gClish:

  ```
  vpn shell tunnels
  ```

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 the "`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 Address> [<tracert Options>]
```

Parameters

Parameter	Description
<IP Address>	Specifies the destination IP address.
<tracert Options>	Specifies the native `tracert` command options.

Example

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x:0]#
```

Multi-blade Traffic Capture (tcpdump)

Description

Use the "`tcpdump`" commands in Gaia gClish to capture and show traffic that is sent and received by Security Group Members in the Security Group.

These commands are enhancements to the standard `tcpdump` utility:

Command	Description
`tcpdump -mcap`	Saves packets from specified Security Group Members to a capture file.
`tcpdump -view`	Shows packets from the specified capture file, including the Security Group Member ID.

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

Syntax

```
tcpdump [-b <SGM IDs>] -mcap -w <Output File> [<tcpdump Options>]
tcpdump -view -r <Input File> [<tcpdump Options>]
```

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 the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)

`-w <Output File>`	Saves the captured packets at the specified path in a file with the specified the name.
	This output file contains captured packets from all specified Security Group Members.
	In the same directory, the command saves additional output files for each Security Group Member.
	The names of these additional files are: `<SGM ID>_<Specified Name of Output File>`
	Example:
	■ The specified full path is:
	`/tmp/capture.cap`
	■ The additional capture files are:
	`/tmp/1_1_capture.cap`
	`/tmp/1_2_capture.cap`
	`/tmp/1_3_capture.cap`
	and so on

`-r <Input File>`	Reads the captured packets (in the `tcpdump` format) from the specified path from a file with the specified the name.
`<tcpdump Options>`	Standard `tcpdump` parameters. See the `tcpdump` manual page - https://linux.die.net/man/8/tcpdump.

Examples

Example 1 - Capture packets on all Security Group Members

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > tcpdump -mcap -w /tmp/capture.cap
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

Clarification about this output:
At this moment, an administrator pressed the CTRL+C keys

stop
Received user request to stop the packets capture process.

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

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

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > tcpdump -b 1_1,1_3,2_1 -mcap -w /tmp/capture.cap -nnni eth1-Mgmt4
... ...
[Global] MyChassis-ch01-01 >
```

Example 3 - Show captured packets from a file

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> tcpdump -view -r /tmp/capture.cap
Reading from file /tmp/capture.cap, 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, Standby Chassis monitors the link state only on data ports `(eth<X>-<YZ>)`.

The Management Monitor feature uses SNMP to monitor management ports for the SSM160 and SSM440 hardware components.

The link state is sent to all SGMs and is integrated with the Standby Chassis High Availability mechanism.

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 on the Security Group.

When the Management Monitor feature is enabled:

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

See the "`Standby Chassis Parameters > Ports > Mgmt`" line in the output example below.

- The "`show interfaces`" command in Gaia gClish shows the link state of management interfaces based on this feature mechanism.

Important:
In a Dual Chassis deployment, if the number of SGMs differs between Standby Chassis 1 and Standby Chassis 2, after you activate the monitoring of management interfaces, you must manually adjust the gap in the chassis grade that is required for chassis failover.
The grade is calculated from all healthy modules in the system: SGM, SSM, Fans, PSU, and so on.
For example:

- Standby Chassis 1 has the grade of X
- Standby Chassis 2 has the grade of Y
- If the difference between these grades is greater than 11, chassis failover occurs

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish

[Global] MyChassis-ch-01-01 > show chassis high-availability mgmt-monitoring
1_01:
off

1_02:
off

1_03:
off

1_04:
off

1_05:
off

2_01:
off

2_02:
off

2_03:
off

2_04:
off

2_05:
off

[Global] MyChassis-ch-01-01 > set chassis high-availability mgmt-monitoring on
1_01:
success

1_02:
success

1_03:
success

1_04:
success

1_05:
success

2_01:
success

2_02:
success

2_03:
success

2_04:
success

2_05:
success

[Global] MyChassis-ch-01-01 > asg stat -v

-------------------------------------------------------------------------------
| System Status - 61000                                                       |
-------------------------------------------------------------------------------
| Standby Chassis Mode                | Active Up                             |
| Up time                       | 2 days, 02:26:01 hours                      |
```

```
| SGMs                        | 10/10                                                |
| Version                     | R80.20SP (Build Number 2)                            |
-------------------------------------------------------------------------------
| SGM ID             Standby Chassis 1                          Standby Chassis 2
 |
|                     STANDBY                                ACTIVE                |
-------------------------------------------------------------------------------
|  1                    ACTIVE                                 ACTIVE               |
|  2                    ACTIVE                                 ACTIVE               |
|  3                    ACTIVE                                 ACTIVE               |
|  4                    ACTIVE                                 ACTIVE               |
|  5                    ACTIVE                                 ACTIVE               |
-------------------------------------------------------------------------------
| Standby Chassis Parameters                                                        |
-------------------------------------------------------------------------------
| Unit         |        Standby Chassis 1          |        Standby Chassis 2          |
Weight |
-------------------------------------------------------------------------------
| SGMs         |          5 / 5            |          5 / 5            |   6    |
| Ports        |                           |                           |        |
|   Standard   |          1 / 1            |          1 / 1            |  11    |
|   Bond       |          2 / 2            |          2 / 2            |  11    |
|   Mgmt       |          1 / 1            |          1 / 1            |  11    |
|   Mgmt Bond  |          0 / 0            |          0 / 0            |  11    |
|   Other      |          0 / 0            |          0 / 0            |   6    |
| Sensors      |                           |                           |        |
|   Fans       |          6 / 6            |          6 / 6            |   5    |
|   SSMs       |          2 / 2            |          2 / 2            |  11    |
|   CMMs       |          2 / 2            |          2 / 2            |   6    |
|   PSUs       |          5 / 5            |          5 / 5            |   6    |
|              |                           |                           |        |
| Grade        |        168 / 168          |        168 / 168          |   -    |
-------------------------------------------------------------------------------
| Minimum grade gap for chassis failover:                                 11     |
| Synchronization                                                                |
|     Sync to Active chassis:    Enabled                                         |
|     Sync to Standby chassis:   Enabled                                         |
-------------------------------------------------------------------------------
| Standby Chassis HA mode:              Active Up                                |
| Standby Chassis HA in Freeze           (9 seconds left)                        |
-------------------------------------------------------------------------------
[Global] MyChassis-ch-01-01 >

[Global] MyChassis-ch-01-01 > show interfaces
+-------------------------------------------------------------------------------------------------------
--------------+
|Interfaces Data
            |
+-------------------------------------------------------------------------------------------------------
--------------+
|Interface      |IPv4 Address                          |Info        |Link State
|Speed|MTU  |Duplex|
|               |MAC  Address                          |            |(ch1)/(ch2)         |
|     |      |
|               |IPv6 Address (global)                 |            |                    |
|     |      |
|               |IPv6 Address (local)                  |            |                    |
|     |      |
+---------------+--------------------------------------+------------+--------------------+----
-+-----+------+
... ... ...
+---------------+--------------------------------------+------------+--------------------+----
-+-----+------+
|eth1-Mgmt1     |192.168.15.234/25                     |Ethernet    |(Up)/(Up)           |10G
|1500 |Full  |
|               |xx:xx:xx:xx:xx:xx                     |            |                    |
|     |      |
|               |-                                     |            |                    |
|     |      |
|               |xxxx::xxxx:xxxx:xxxx:xxxx/64          |            |                    |
```

```
|     |      |
+---------------+-------------------------------------+------------+--------------------+----
-+-----+------+
... ... ...
[Global] MyChassis-ch-01-01 >
```

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 traffic.

You can show the performance statistics for IPv4 traffic, IPv6 traffic, or for all traffic.

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

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

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}]]]`
`asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-v] [-vv [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 the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)
`-vs <VS IDs>`	Applies to Virtual Systems as specified by the `<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 This parameter is only applicable in a VSX environment.
`-v`	Shows statistics for each Security Group Member. Adds a performance summary for each Security Group Member.
`-vv`	Shows statistics for each Virtual System. **Note** - This parameter is only relevant in a VSX environment.

Parameter	Description
`mem [{fwk | cpd | fwd | all_daemons}]`	Shows memory usage for each daemon. Use this with the "`-vv`" parameter. Valid values: ■ `fwk` (default) ■ `fwd` ■ `cpd` ■ `all_daemons`
`cpu [{1m | 1h | 24h}]`	Shows CPU usage for a specified period of time. Use this with the "`-vv`" parameter. Valid values: ■ `1m` - The last 60 seconds (default) ■ `1h` - The last hour ■ `24h` - The last 24 hours
`-p`	Shows detailed statistics and traffic distribution between these paths on the Active Chassis: ■ 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 the 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. The default delay is 10 seconds.

Notes:

- The "`-b <SGM IDs>`" and "`-vs <VS IDs>`" parameters must be at the beginning of the command syntax.
  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 appear when you run the "`asg perf -h`" command.

Examples

Example 1 - Summary without Parameters (asg perf)

```
[Expert@MyChassis-ch0x-0x: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)

```
[Expert@MyChassis-ch0x-0x: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 to enable the resource control monitoring on all Security Group Members.

Run in the Expert mode on the Security Group:

```
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 - Detailed Statistics and Traffic Distribution (asg perf -p)

This example the output for the Virtual Systems 0 and 1.

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x: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-ch0x-0x: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`)

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 traffic.

You can show the performance statistics for IPv4 traffic, IPv6 traffic, or for all traffic.

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

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

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}]]]
```

```
asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-v] [-vv [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 the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)
`-vs <VS IDs>`	Applies to Virtual Systems as specified by the `<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 This parameter is only applicable in a VSX environment.
`-v`	Shows statistics for each Security Group Member. Adds a performance summary for each Security Group Member.
`-vv`	Shows statistics for each Virtual System. **Note** - This parameter is only relevant in a VSX environment.

Parameter	Description
`mem [{fwk | cpd | fwd | all_daemons}]`	Shows memory usage for each daemon. Use this with the "`-vv`" parameter. Valid values: ■ `fwk` (default) ■ `fwd` ■ `cpd` ■ `all_daemons`
`cpu [{1m | 1h | 24h}]`	Shows CPU usage for a specified period of time. Use this with the "`-vv`" parameter. Valid values: ■ `1m` - The last 60 seconds (default) ■ `1h` - The last hour ■ `24h` - The last 24 hours
`-p`	Shows detailed statistics and traffic distribution between these paths on the Active Chassis: ■ 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 the 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. The default delay is 10 seconds.

Notes:

- The "`-b <SGM IDs>`" and "`-vs <VS IDs>`" parameters must be at the beginning of the command syntax.
  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 appear when you run the "`asg perf -h`" command.

Examples

Example 1 - Summary without Parameters (asg perf)

```
[Expert@MyChassis-ch0x-0x: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)

```
[Expert@MyChassis-ch0x-0x: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 to enable the resource control monitoring on all Security Group Members.

Run in the Expert mode on the Security Group:

```
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-ch0x-0x: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-ch0x-0x: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-ch0x-0x: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

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 (!)**.

Syntax

```
asg_perf_hogs
```

Example

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x:0]#
```

Configuration

Configure the "`asg_perf_hogs`" behavior in 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

In the **[tests]** section of the `$SMODIR/conf/performance_hogs.conf` file you enable and disable 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:

- To enable the test:

  ```
  <Test Name>=1
  ```

- To disable the test:

  ```
  <Test Name>=0
  ```

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 seconds.

`processes_to_check`	List of processes to check:
	You must enclose each process in double quotes.
	You must enter a space before another 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: 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: 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 seconds.
- Recommended range: 300 - 86400 seconds.

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 on the Security Group.

Syntax

```
set chassis high-availability port <Name of Interface> priority
<Priority>
```

Parameters

Parameter	Description
<Name of Interface>	Specifies the interface name.
<Priority>	Specifies the 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 Chassis.

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 in the Non-Interactive Mode

Syntax

```
asg search -help
```

```
asg search [-v] [-vs <VS IDs>] [<Source IP Address> <Source Port> <Destination IP Address> <Destination Port> <Protocol>]
```

Parameters

Parameter	Description
No Parameters	Runs in the interactive mode.
`-help`	Shows the built-in help.
`-vs <VS IDs>`	Applies to Virtual Systems as specified by the `<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 This parameter is only applicable in a VSX environment.
<Source IP Address>	Specifies the source IPv4 or IPv6 address.
<Source Port>	Specifies the source port number. See *IANA Service Name and Port Number Registry*.
<Destination IP Address>	Specifies the destination IPv4 or IPv6 address.
<Destination Port>	Specifies the destination port number. See *IANA Service Name and Port Number Registry*.
<Protocol>	Specifies the IP Protocol name or number. See *IANA Protocol Numbers*.

Parameter	Description
`-v`	Shows connection indicators for: ■ **A** - Active Security Group Member ■ **B** - Backup Security Group Member ■ **F** - Firewall Connections table ■ **S** - SecureXL Connections table ■ **C** - Correction Layer table This is in addition to the indicators for Active and Backup Security Group Members.

Notes:

- You must enter the all parameters in the sequence as appears in the above syntax.
- You can enter "`\*`" as a wildcard parameter (meaning, any value).
- The "`-vs`" parameter is only available for a Security Group in VSX mode.

Examples

Example 1 - Search for one IPv4 source address, one IPv4 destination address, all ports, and the TCP protocol

```
[Expert@MyChassis-ch0x-0x: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 address, all destination IP addresses, destination port 8080, and TCP protocol

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x: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 in the Interactive Mode

In the Interactive Mode, you enter the connection search parameters in the required sequence.

Step	Instructions
1	Connect to the command line on the Security Group.
2	Go to Gaia gClish: enter `gclish` and press Enter.
3	Run the command: `> asg search [-vs <VS IDs>] [-v]`
4	Enter these parameters in the order below: 1. Source IPv4 or IPv6 address. 2. Destination IPv4 or IPv6 address. 3. Destination port number. See *IANA Service Name and Port Number Registry*. 4. IP protocol. See *IANA Protocol Numbers*. 5. Source port number. See *IANA Service Name and Port Number Registry*. **Note** - Press the **Enter** key to enter a wildcard value (meaning, any value).

Example - Search for one IPv4 source and destination

```
[Expert@MyChassis-ch0x-0x: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

[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>] [-6]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)
`-6`	Shows only IPv6 connections.

Example

```
[Expert@MyChassis-ch0x-0x: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 (drop_monitor)

In This Section:

Description

Use the "`drop_monitor`" command in the Expert mode to monitor dropped packets on interfaces in real time.

Drop statistics arrive from these modules:

- NICs
- CoreXL
- PSL
- SecureXL

Notes:

- This command opens a monitor session and shows aggregated data from Security Group Members (and optionally SSMs).
  To stop an open session, press **CTRL+C**.
- By default, this utility shows drop statistics for IPv4 traffic.

Syntax

```
drop_monitor -h
```

```
drop_monitor [-d] [-v] [-m <SGM IDs>] [-i <List of Interfaces>]
[-f <Refresh Rate>] [-sf <Query Timeout>] [-le] [-e] [-dm] [-ds]
[-r] [-s] [-v6]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-d` `--debug`	Runs the command in the debug mode.
`-v` `--verbose`	Shows detailed drop statistics - for each Security Group Member and all SecureXL statistics.

Parameter	Description
`-m <SGM IDs>` `--members <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)
`-i <List of Interfaces>` `--interfaces <List of Interfaces>`	Shows drop statistics for the specified network interfaces. Enter the names of applicable interfaces separated a comma. By default, this utility shows drop statistics only for the backplane interfaces.
`-f <Refresh Rate>` `--refresh-rate <Refresh Rate>`	Specifies the output refresh rate in seconds. The default is 3 seconds.
`-sf <Query Timeout>` `--ssms-refresh-rate <Query Timeout>`	Specifies the SSM query timeout in seconds. The default is 60 seconds.
`-le` `--local-export`	Exports drop statistics from the local Security Group Member in the JSON format.
`-e` `--global-export`	Exports drop statistics from all Security Group Members in the JSON format.
`-dm` `--detailed-members`	Shows drop statistics for each Security Group Member, in addition to the total drop statistics.
`-ds` `--detailed-securexl`	Shows detailed drop statistics for SecureXL.

Parameter	Description
`-r` `--reset`	Resets the statistics counters to 0 before it collects the data. **Notes:** ■ Drop statistics are reset for CoreXL, PSL, SecureXL, and backplane interfaces. ■ Drop statistics are not reset for SSMs.
`-s` `--include-ssms-stats`	Shows drop statistics for local SSMs only. Only data links, management links, and downlinks are supported.
`-v6` `--ipv6`	Shows drop statistics for IPv6 traffic.

Example 1 - Default output

```
[Expert@MyChassis-ch0x-0x:0]# drop_monitor

Dropped packets statistics of network interfaces, CoreXL, SecureXL and PSL
+----------+------------------+-------+
| Category | Statistics       | Total |
+----------+------------------+-------+
+----------+------------------+-------+
|          | RX Dropped       |   0   |
|   NIC    | TX Dropped       |   0   |
|          | Qdisc Dropped    |   0   |
+----------+------------------+-------+
|          | Outbound Dropped |   0   |
|  CoreXL  | Inbound Dropped  |   0   |
|          | F2P Dropped      |   0   |
+----------+------------------+-------+
|   PSL    | Total Dropped    |   0   |
|          | Rejected         |   0   |
+----------+------------------+-------+
| SecureXL | Total drops      |   0   |
+----------+------------------+-------+
 * Network drop values presented are for BPEth1,BPEth0 interfaces.
[Expert@MyChassis-ch0x-0x:0]#
```

Example 2 - Verbose output

```
[Expert@MyChassis-ch0x-0x:0]# drop_monitor -v

Dropped packets statistics of network interfaces, CoreXL, SecureXL and PSL
+----------+----------------------+------+------+-------+
| Category | Statistics           | 1_01 | 1_02 | Total |
+----------+----------------------+------+------+-------+
+----------+----------------------+------+------+-------+
|          | RX Dropped           |  0   |  0   |   0   |
|   NIC    | TX Dropped           |  0   |  0   |   0   |
|          | Qdisc Dropped        |  0   |  0   |   0   |
+----------+----------------------+------+------+-------+
|          | Outbound Dropped     |  0   |  0   |   0   |
|  CoreXL  | Inbound Dropped      |  0   |  0   |   0   |
|          | F2P Dropped          |  0   |  0   |   0   |
+----------+----------------------+------+------+-------+
|   PSL    | Total Dropped        |  0   |  0   |   0   |
|          | Rejected             |  0   |  0   |   0   |
+----------+----------------------+------+------+-------+
|          | XMT error            |  0   |  0   |   0   |
|          | general reason       |  0   |  0   |   0   |
|          | Syn Defender         |  0   |  0   |   0   |
|          | Attack mitigation    |  0   |  0   |   0   |
|          | VPN forwarding       |  0   |  0   |   0   |
|          | corrupted packet     |  0   |  0   |   0   |
|          | hl - spoof viol      |  0   |  0   |   0   |
|          | encrypt failed       |  0   |  0   |   0   |
|          | cluster error        |  0   |  0   |   0   |
|          | anti spoofing        |  0   |  0   |   0   |
|          | monitored spoofed    |  0   |  0   |   0   |
|          | hl - new conn        |  0   |  0   |   0   |
|          | hl - TCP viol        |  0   |  0   |   0   |
|          | F2F not allowed      |  0   |  0   |   0   |
| SecureXL | fragment error       |  0   |  0   |   0   |
|          | Session rate exceed  |  0   |  0   |   0   |
|          | PXL decision         |  0   |  0   |   0   |
|          | template quota       |  0   |  0   |   0   |
|          | drop template        |  0   |  0   |   0   |
|          | sanity error         |  0   |  0   |   0   |
|          | outb - no conn       |  0   |  0   |   0   |
|          | clr pkt on vpn       |  0   |  0   |   0   |
|          | partial conn         |  0   |  0   |   0   |
|          | decrypt failed       |  0   |  0   |   0   |
|          | Connections Limit by |  0   |  0   |   0   |
|          | Source IP exceed its |  0   |  0   |   0   |
|          | local spoofing       |  0   |  0   |   0   |
|          | interface down       |  0   |  0   |   0   |
+----------+----------------------+------+------+-------+
 * Network drop values presented are for BPEth1,BPEth0 interfaces.
[Expert@MyChassis-ch0x-0x:0]#
```

Example 3 - Drop statistics for specific Security Group Members and SSMs

```
[Expert@MyChassis-ch0x-0x:0]# drop_monitor -m 1_01,1_02 -dm -s

Dropped packets statistics of network interfaces, CoreXL, SecureXL and PSL
+----------+------------------+------+------+-------+
| Category | Statistics       | 1_01 | 1_02 | Total |
+----------+------------------+------+------+-------+
+----------+------------------+------+------+-------+
|          | RX Dropped       |  0   |  0   |   0   |
|   NIC    | TX Dropped       |  0   |  0   |   0   |
|          | Qdisc Dropped    |  0   |  0   |   0   |
+----------+------------------+------+------+-------+
|          | Outbound Dropped |  0   |  0   |   0   |
|  CoreXL  | Inbound Dropped  |  0   |  0   |   0   |
|          | F2P Dropped      |  0   |  0   |   0   |
+----------+------------------+------+------+-------+
|   PSL    | Total Dropped    |  0   |  0   |   0   |
|          | Rejected         |  0   |  0   |   0   |
+----------+------------------+------+------+-------+
| SecureXL | Total drops      |  0   |  0   |   0   |
+----------+------------------+------+------+-------+
 * Network drop values presented are for BPEth1,BPEth0 interfaces.

SSMs drop statistics
+---------+-----+-----------------+----------------+---------------+---------------+
| Chassis | SSM | Output Discards | Input Discards |  Input Errors | Output Errors |
+---------+-----+-----------------+----------------+---------------+---------------+
+---------+-----+-----------------+----------------+---------------+---------------+
|    1    |  1  |        0        |    1003268     |      1081     |       0       |
|         |  2  |        0        |      9617      |       4       |       0       |
+---------+-----+-----------------+----------------+---------------+---------------+
 * SSMs network drop values presented are for data interfaces.
[Expert@MyChassis-ch0x-0x: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 Gateway Mode (Gateway or VSX)
- Number of members in the Security Group
- Number of Virtual Systems
- Information related to VSX configuration
- Uptime
- Software Version

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 applies only to that Virtual System.

Parameters

Parameter	Description
No Parameters	Shows the Chassis 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** - Chassis state monitor ■ **DR Manager** - Dynamic Routing manager ■ **UIPC** - Unique IP Address for each Chassis (see *"Configuring a Unique IP Address for Each Standby Chassis (UIPC)" on page 117*) ■ **Alert** - Alerts
`-v [-amw]`	Shows the detailed Chassis status (verbose output). The "`-amw`" parameter shows the update status for the applicable Software Blades.
`vs [all [-p]]`	Shows the VSX information: ■ `vs` Shows general output for a Virtual System. Run this command in the context of the applicable 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 in the context of the Virtual System.

Examples

Example 1 - Default Output (asg stat)

Syntax

```
asg stat
```

Example output from a Security Group in a Dual Chassis configuration

```
[Expert@MyChassis-ch0x-0x:0]# asg stat
-------------------------------------------------------------------------------
| System Status - 61000                                                       |
-------------------------------------------------------------------------------
| Chassis Mode                | Active Up                                     |
| Up time                     | 21:29:56 hours                                |
| SGMs                        | 12/12                                         |
| Version                     | R81 (Build Number XXX)                    |
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit         |          Chassis 1            |          Chassis 2           |
-------------------------------------------------------------------------------
| SGMs         |            6 / 6              |            6 / 6             |
| Ports        |            5 / 5              |            5 / 5             |
| Fans         |            6 / 6              |            6 / 6             |
| SSMs         |            2 / 2              |            2 / 2             |
| CMMs         |            2 / 2              |            2 / 2             |
| PSUs         |            5 / 5              |            5 / 5             |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Example output from a Security Group in a Single Chassis configuration

```
[Expert@MyChassis-ch0x-0x:0]# asg stat
-------------------------------------------------------------------------------
| System Status - 61000                                                       |
-------------------------------------------------------------------------------
| Up time                     | 02:10:27 hours                                |
| SGMs                        | 30/30                                         |
| Version                     | R81 (Build Number XXX)                    |
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit         |                          Chassis 1                          |
-------------------------------------------------------------------------------
| SGMs         |                           30 / 30                           |
| Ports        |                            4 / 4                            |
| Fans         |                            6 / 6                            |
| SSMs         |                            2 / 2                            |
| CMMs         |                            2 / 2                            |
| PSUs         |                            5 / 5                            |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Example 2 - Detailed Output (asg stat -v)

Syntax

```
asg stat -v
```

Example output from a Security Group in a Dual Chassis configuration - top section

This output shows a Security Group with 12 Security Group Members in the Active (UP) state (out of total 12).

The Chassis #1 is Active.

The Chassis #2 is Standby.

```
[Expert@MyChassis-ch0x-0x:0]# asg stat -v
-------------------------------------------------------------------------------
| System Status - 61000                                                       |
-------------------------------------------------------------------------------
| Chassis Mode                | Active Up                                     |
| Up time                     | 21:30:50 hours                                |
| SGMs                        | 12/12                                         |
| Version                     | R81 (Build Number XXX)                    |
-------------------------------------------------------------------------------
| SGM ID             Chassis 1                          Chassis 2             |
|                    ACTIVE                             STANDBY               |
-------------------------------------------------------------------------------
|  1                   ACTIVE                             ACTIVE               |
|  2                   ACTIVE                             ACTIVE               |
|  3                   ACTIVE                             ACTIVE               |
|  4                   ACTIVE                             ACTIVE               |
|  5                   ACTIVE                             ACTIVE               |
|  6                   ACTIVE                             ACTIVE               |
-------------------------------------------------------------------------------
... output was truncated for brevity - the example continues below ...
```

Example output from a Security Group in a Single Chassis configuration - top section

This output shows a Security Group with 30 Security Group Members in the Active (UP) state (out of total 30).

```
[Expert@MyChassis-ch0x-0x:0]# asg stat -v
-------------------------------------------------------------------------------
| System Status - 61000                                                       |
-------------------------------------------------------------------------------
| Up time                     | 02:10:39 hours                                |
| SGMs                        | 30/30                                         |
| Version                     | R81 (Build Number XXX)                    |
-------------------------------------------------------------------------------
| SGM ID                              Chassis 1                               |
|                                     ACTIVE                                  |
-------------------------------------------------------------------------------
|  1                                    ACTIVE                                |
|  2                                    ACTIVE                                |
|  3                                    ACTIVE                                |
... output was truncated for brevity ...
|  30                                   ACTIVE                                |
-------------------------------------------------------------------------------
... output was truncated for brevity - the example continues below ...
```

Explanation about the output:

Field	Instructions
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 **Note** - To change manually the state of the Security Group Member, use the "`g_clusterXL_admin`" command (see *"Configuring the Cluster State (g_clusterXL_admin)" on page 86*).

Example output from a Security Group in a Dual Chassis configuration - bottom section

```
... output was truncated for brevity - the example starts above ...
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit         |        Chassis 1          |        Chassis 2          | Weight |
-------------------------------------------------------------------------------
| SGMs         |          6 / 6            |          6 / 6            |   6    |
| Ports        |                           |                           |        |
|   Standard   |          5 / 5            |          5 / 5            |  11    |
|   Bond       |          0 / 0            |          0 / 0            |  11    |
|   Other      |          0 / 0            |          0 / 0            |   6    |
| Sensors      |                           |                           |        |
|   Fans       |          6 / 6            |          6 / 6            |   5    |
|   SSMs       |          2 / 2            |          2 / 2            |  11    |
|   CMMs       |          2 / 2            |          2 / 2            |   6    |
|   PSUs       |          5 / 5            |          5 / 5            |   6    |
|              |                           |                           |        |
| Grade        |        185 / 185          |        185 / 185          |   -    |
-------------------------------------------------------------------------------
| Minimum grade gap for chassis failover:                                 11  |
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
|     Sync to Standby chassis:   Enabled                                      |
-------------------------------------------------------------------------------
| Chassis HA mode:              Active Up                                     |
-------------------------------------------------------------------------------
```

Example output from a Security Group in a Single Chassis configuration - bottom section

```
... output was truncated for brevity - the example starts above ...
-------------------------------------------------------------------------------
| Chassis Parameters                                                          |
-------------------------------------------------------------------------------
| Unit         |                      Chassis 1                       | Weight |
-------------------------------------------------------------------------------
| SGMs         |                       30 / 30                        |   6    |
| Ports        |                                                      |        |
|   Standard   |                        4 / 4                         |  11    |
|   Bond       |                        0 / 0                         |  11    |
|   Other      |                        0 / 0                         |   6    |
| Sensors      |                                                      |        |
|   Fans       |                        6 / 6                         |   5    |
|   SSMs       |                        2 / 2                         |  11    |
|   CMMs       |                        2 / 2                         |   6    |
|   PSUs       |                        5 / 5                         |   6    |
|              |                                                      |        |
| Grade        |                      318 / 318                       |   -    |
-------------------------------------------------------------------------------
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
-------------------------------------------------------------------------------
```

Note - In the notation "*<Number> / <Number>*", the left number shows the number of components that in the UP state, and the right number shows the number the components that must be in the UP state.
For example, on the **SGMs** line, "30 / 30" means that there are currently 30 Security Group Members in the UP state out of the 30 that must be in the UP state.

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 in the UP state.
	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 in Gaia gClish:
	`set chassis high-availability factors <Hardware Component>`
	For example, to change the weight of the Security Group Member to 12, run in Gaia Clish on that Security Group Member:
	`set chassis high-availability factors sgm 12`
	See *"Configuring Chassis High Availability" on page 103*.
	If you run the "`asg stat -v`" command, the output shows a greater unit weight and system grade.

Field	Description
Minimum grade gap for chassis failover	Chassis failover occurs to the Chassis with the higher grade only if its grade is greater than the other Chassis by more than the minimum gap. Minimum threshold for traffic processing - the minimum grade required for the Chassis to become Active.
Synchronization	Status of synchronization between Security Group Members: ■ Within a Chassis - between Security Group Members located in the same Security Group ■ Between two Chassis - between Security Group Members located in different Chassis ■ Exception Rules - exception rules configured by an administrator with the "`g_sync_exception`" command.

Example 3 - List of Tasks (asg stat -i tasks)

Syntax

```
asg stat -i tasks
```

Example output from a Security Group in a Dual Chassis configuration

The SMO task runs on Chassis #2 - on the Security Group Member #3, on which you ran this command (see the string "`(local)`").

```
[Expert@MyChassis-ch0x-0x:0]# asg stat -i tasks
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |                            |         3(local)           |
| General (1)        |         2                  |         3(local)           |
| LACP (2)           |         2                  |         3(local)           |
| CH Monitor (3)     |         2                  |         3(local)           |
| DR Manager (4)     |                            |         3(local)           |
| UIPC (5)           |         2                  |         3(local)           |
| Alert (6)          |                            |         3(local)           |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
[Expert@MyChassis-ch0x-0x:0]# member 2_4
Moving to member 2_4
... ...
[Expert@MyChassis-ch0x-0x:0]# asg stat -i tasks
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |                            |         3                  |
| General (1)        |         2                  |         3                  |
| LACP (2)           |         2                  |         3                  |
| CH Monitor (3)     |         2                  |         3                  |
| DR Manager (4)     |                            |         3                  |
| UIPC (5)           |         2                  |         3                  |
| Alert (6)          |                            |         3                  |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Example output from all Security Group Members (in our example, there are two on each Chassis):

```
[Expert@MyChassis-ch0x-0x:0]# g_all asg stat -i tasks
1_01:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1(local)           |                            |
| General (1)        |         1(local)           |         1                  |
| LACP (2)           |         1(local)           |         1                  |
| CH Monitor (3)     |         1(local)           |         1                  |
| DR Manager (4)     |         1(local)           |                            |
| UIPC (5)           |         1(local)           |         1                  |
| Alert (6)          |         1(local)           |                            |
-------------------------------------------------------------------------------

1_02:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1                  |                            |
| General (1)        |         1                  |         1                  |
| LACP (2)           |         1                  |         1                  |
| CH Monitor (3)     |         1                  |         1                  |
| DR Manager (4)     |         1                  |                            |
| UIPC (5)           |         1                  |         1                  |
| Alert (6)          |         1                  |                            |
-------------------------------------------------------------------------------

2_01:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1                  |                            |
| General (1)        |         1                  |         1(local)           |
| LACP (2)           |         1                  |         1(local)           |
| CH Monitor (3)     |         1                  |         1(local)           |
| DR Manager (4)     |         1                  |                            |
| UIPC (5)           |         1                  |         1(local)           |
| Alert (6)          |         1                  |                            |
-------------------------------------------------------------------------------

2_02:
-------------------------------------------------------------------------------
| Task (Task ID)     |        Chassis 1           |        Chassis 2           |
-------------------------------------------------------------------------------
| SMO (0)            |         1                  |                            |
| General (1)        |         1                  |         1                  |
| LACP (2)           |         1                  |         1                  |
| CH Monitor (3)     |         1                  |         1                  |
| DR Manager (4)     |         1                  |                            |
| UIPC (5)           |         1                  |         1                  |
| Alert (6)          |         1                  |                            |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Example output from a Security Group in a Single Chassis configuration

The SMO task runs on the Security Group Member #1, on which you ran this command (see the string "`(local)`").

```
[Expert@MyChassis-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@MyChassis-ch0x-0x:0]#
```

Monitoring System and Component Status (asg monitor)

Description

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

This command shows the same information as the *"Showing Hardware State (asg stat)" on page 196*, 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`
`asg monitor -h`
`asg monitor [-v | -all] [-amw] <Interval>`
`asg monitor -l`

Parameters

Parameter	Description
No Parameters	Shows the Security Group Member status.
`-h`	Shows the built-in help.
`-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.

Examples

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

```
[Expert@MyChassis-ch0x-0x:0]# asg monitor -amw

-------------------------------------------------------------------------------
| System Status - 61000                                                       |
-------------------------------------------------------------------------------
| Up time                     | 12:03:48 hours                                |
| SGMs                        | 2 / 2                                         |
| Version                     | R81 (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 Chassis component status

```
[Expert@MyChassis-ch0x-0x: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     |                                                       |        |
|   Fans      |                        6 / 6                          |   5    |
|   SSMs      |                        2 / 2                          |  11    |
|   CMMs      |                        2 / 2                          |   6    |
|   PSUs      |                        5 / 5                          |   6    |
|             |                                                       |        |
| Grade       |                      205 / 205                        |   -    |
-------------------------------------------------------------------------------
| Synchronization                                                             |
|     Sync to Active chassis:    Enabled                                      |
-------------------------------------------------------------------------------
```

Configuring Alert Thresholds (set chassis alert_threshold)

Description

Use the "`set chassis alert_threshold`" command in Gaia gClish to configure thresholds for performance and hardware alerts.

Syntax to configure alert threshold

```
set chassis alert_threshold <Threshold Name> <Value>
```

Syntax to view an alert threshold configuration

```
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 specified threshold

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 the High limit)
concurr_conn_total_threshold_high	Security Group	Concurrent connections - High limit
concurr_conn_total_threshold_low_ratio	Security Group	Concurrent connections - Low limit (% of the 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 the High limit)
conn_rate_total_threshold_high	Security Group	Connection rate per second - High limit

Threshold Name	Scope	Description
conn_rate_total_threshold_low_ratio	Security Group	Connection rate per second - Low limit (% of the 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 the 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 the 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 the 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 the High limit)
packet_rate_total_threshold_high	Security Group	Packet rate per second - High limit
packet_rate_total_threshold_low_ratio	Security Group	Packet rate per second - Low limit (% of the High limit)
throughput_threshold_high	Security Group Member	Throughput (bps) - High limit
throughput_threshold_low_ratio	Security Group Member	Throughput (bps) - Low limit (% of the High limit)
throughput_total_threshold_high	Security Group	Throughput (bps) - High limit

Threshold Name	Scope	Description
`throughput_total_threshold_low_ratio`	Security Group	Throughput (bps) - Low limit (% of the High limit)

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

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01> set chassis alert_threshold mem_util_threshold_perc_high 70
[Global] MyChassis-ch01-01>
```

Monitoring SGM 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
No Parameters	Shows both the Resource (RAM and Storage) and SSD Health information.
`-h`	Shows the built-in help.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`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)

Examples

Example 1 - Default output

```
[Expert@MyChassis-ch0x-0x: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 a specific Security Group Member

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x:0]#
```

Example 3 - Verbose SSD Health information

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x:0]#
```

Description for the Resource Table section

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%.

Description for the SMART Attributes section

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 SGM and Security Group Events (asg alert)

The "`asg alert`" command is an interactive wizard that configures alerts for Security Group Member and Chassis 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 Chassis ID, SGM 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.

Option	Description
Show Configuration	Shows existing alert configuration.
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** ■ **Log**

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.

Log Alert Configuration

There are no parameters to configure.

You can configure the **Log Mode** to:

- **Enabled**
- **Disabled**
- **Monitor**

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)
```

You can select one or more event types:

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

Monitoring Hardware Components (asg hw_monitor)

Description

Use the "`asg hw_monitor`" command in Gaia gClish or Expert mode to show and monitor hardware information and thresholds for the monitored components:

- SGM - CPU temperature for each socket
- Chassis fan speeds
- SSM - Throughput rates
- Power consumption for each Chassis
- Power Supply Unit - Installed or not installed, and the PSU fan speed
- CMM - Installed, Active, or Standby

Syntax

```
asg hw_monitor [-v] [-f <Filter>]
```

Parameters

Parameter	Description
`-v`	Shows detailed component status report (verbose)
`-f`	Show status of one or more specified (filtered) components
<Filter>	One or more of these component types, in a comma separated list: ■ `CMM` ■ `CPUtemp` ■ `Fan` ■ `PowerConsumption` ■ `PowerUnit` ■ `SSM`

Examples

Example output on a 61000 N+N chassis

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > asg hw_monitor -v
-------------------------------------------------------------------------------
| Hardware Monitor                                                            |
-------------------------------------------------------------------------------
| Sensor           | Location       | Value | Threshold | Units       | State|
-------------------------------------------------------------------------------
| Chassis 1                                                                   |
-------------------------------------------------------------------------------
| CMM              | bay 1          | 1     | 0         | <S,D>/<A>   | 1    |
| CMM              | bay 2          | 0     | 0         | <S,D>/<A>   | 1    |
| CPUtemp          | blade 1, CPU0  | 45    | 65        | Celsius     | 1    |
| CPUtemp          | blade 1, CPU1  | 39    | 65        | Celsius     | 1    |
| CPUtemp          | blade 2, CPU0  | 44    | 65        | Celsius     | 1    |
| CPUtemp          | blade 2, CPU1  | 39    | 65        | Celsius     | 1    |
| CPUtemp          | blade 3, CPU0  | 44    | 65        | Celsius     | 1    |
| CPUtemp          | blade 3, CPU1  | 38    | 65        | Celsius     | 1    |
| CPUtemp          | blade 4, CPU0  | 47    | 65        | Celsius     | 1    |
| CPUtemp          | blade 4, CPU1  | 42    | 65        | Celsius     | 1    |
| CPUtemp          | blade 5, CPU0  | 0     | 65        | Celsius     | 1    |
| CPUtemp          | blade 5, CPU1  | 0     | 65        | Celsius     | 1    |
| CPUtemp          | blade 6, CPU0  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 6, CPU1  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 7, CPU0  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 7, CPU1  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 8, CPU0  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 8, CPU1  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 9, CPU0  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 9, CPU1  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 10, CPU0 | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 10, CPU1 | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 11, CPU0 | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 11, CPU1 | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 12, CPU0 | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 12, CPU1 | 0     | 65        | Celsius     | 0    |
| Fan              | bay 1, fan 1   | 3     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 2   | 3     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 1   | 3     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 2   | 3     | 11        | Speed Level | 1    |
| Fan              | bay 3, fan 1   | 3     | 11        | Speed Level | 1    |
| Fan              | bay 3, fan 2   | 3     | 11        | Speed Level | 1    |
| PowerConsumption | N/A            | 2711  | 4050      | Watts       | 1    |
| PowerUnit(AC)    | bay 1          | 0     | 0         | NA          | 1    |
| PowerUnit(AC)    | bay 2          | 0     | 0         | NA          | 1    |
| PowerUnit(AC)    | bay 3          | 0     | 0         | NA          | 1    |
| PowerUnit(AC)    | bay 4          | 0     | 0         | NA          | 0    |
| PowerUnit(AC)    | bay 5          | 0     | 0         | NA          | 0    |
| PowerUnitFan     | bay 1, fan 1   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 1, fan 2   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 2, fan 1   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 2, fan 2   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 3, fan 1   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 3, fan 2   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 4, fan 1   | 0     | 0         | NA          | 0    |
| PowerUnitFan     | bay 4, fan 2   | 0     | 0         | NA          | 0    |
| PowerUnitFan     | bay 5, fan 1   | 0     | 0         | NA          | 0    |
| PowerUnitFan     | bay 5, fan 2   | 0     | 0         | NA          | 0    |
| SSM              | bay 1          | 0     | 0         | Mbps        | 1    |
| SSM              | bay 2          | 0     | 0         | Mbps        | 1    |
-------------------------------------------------------------------------------
| Chassis 2                                                                   |
-------------------------------------------------------------------------------
| CMM              | bay 1          | 1     | 0         | <S,D>/<A>   | 1    |
| CMM              | bay 2          | 0     | 0         | <S,D>/<A>   | 1    |
| CPUtemp          | blade 1, CPU0  | 46    | 65        | Celsius     | 1    |
| CPUtemp          | blade 1, CPU1  | 46    | 65        | Celsius     | 1    |
| CPUtemp          | blade 2, CPU0  | 48    | 65        | Celsius     | 1    |
| CPUtemp          | blade 2, CPU1  | 49    | 65        | Celsius     | 1    |
| CPUtemp          | blade 3, CPU0  | 46    | 65        | Celsius     | 1    |
| CPUtemp          | blade 3, CPU1  | 47    | 65        | Celsius     | 1    |
| CPUtemp          | blade 4, CPU0  | 46    | 65        | Celsius     | 1    |
```

```
| CPUtemp          | blade 4, CPU1  | 50    | 65        | Celsius     | 1    |
| CPUtemp          | blade 5, CPU0  |       | 65        | Celsius     | 1    |
| CPUtemp          | blade 5, CPU1  |       | 65        | Celsius     | 1    |
| CPUtemp          | blade 6, CPU0  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 6, CPU1  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 7, CPU0  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 7, CPU1  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 8, CPU0  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 8, CPU1  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 9, CPU0  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 9, CPU1  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 10, CPU0 | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 10, CPU1 | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 11, CPU0 | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 11, CPU1 | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 12, CPU0 | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 12, CPU1 | 0     | 65        | Celsius     | 0    |
| Fan              | bay 1, fan 1   | 5     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 2   | 5     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 1   | 5     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 2   | 5     | 11        | Speed Level | 1    |
| Fan              | bay 3, fan 1   | 5     | 11        | Speed Level | 1    |
| Fan              | bay 3, fan 2   | 5     | 11        | Speed Level | 1    |
| PowerConsumption | N/A            | 2711  | 4050      | Watts       | 1    |
| PowerUnit(AC)    | bay 1          | 0     | 0         | NA          | 1    |
| PowerUnit(AC)    | bay 2          | 0     | 0         | NA          | 1    |
| PowerUnit(AC)    | bay 3          | 0     | 0         | NA          | 1    |
| PowerUnit(AC)    | bay 4          | 0     | 0         | NA          | 0    |
| PowerUnit(AC)    | bay 5          | 0     | 0         | NA          | 0    |
| PowerUnitFan     | bay 1, fan 1   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 1, fan 2   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 2, fan 1   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 2, fan 2   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 3, fan 1   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 3, fan 2   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 4, fan 1   | 0     | 0         | NA          | 0    |
| PowerUnitFan     | bay 4, fan 2   | 0     | 0         | NA          | 0    |
| PowerUnitFan     | bay 5, fan 1   | 0     | 0         | NA          | 0    |
| PowerUnitFan     | bay 5, fan 2   | 0     | 0         | NA          | 0    |
| SSM              | bay 1          | 0     | 0         | Mbps        | 1    |
| SSM              | bay 2          | 0     | 0         | Mbps        | 1    |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

Example output on a 61000 or 41000 chassis

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > asg hw_monitor -v
-------------------------------------------------------------------------------
| Hardware Monitor                                                            |
-------------------------------------------------------------------------------
| Sensor           | Location       | Value | Threshold | Units       | State|
-------------------------------------------------------------------------------
| Chassis 1                                                                   |
-------------------------------------------------------------------------------
| CMM              | bay 1          | 0     | 0         | <S,D>/<A>   | 1    |
| CMM              | bay 2          | 1     | 0         | <S,D>/<A>   | 1    |
| CPUtemp          | blade 1, CPU0  | 47    | 65        | Celsius     | 1    |
| CPUtemp          | blade 1, CPU1  | 46    | 65        | Celsius     | 1    |
| CPUtemp          | blade 2, CPU0  | 46    | 65        | Celsius     | 1    |
| CPUtemp          | blade 2, CPU1  | 44    | 65        | Celsius     | 1    |
| CPUtemp          | blade 3, CPU0  | 46    | 65        | Celsius     | 1    |
| CPUtemp          | blade 3, CPU1  | 45    | 65        | Celsius     | 1    |
| CPUtemp          | blade 4, CPU0  | 45    | 65        | Celsius     | 1    |
| CPUtemp          | blade 4, CPU1  | 46    | 65        | Celsius     | 1    |
| Fan              | bay 1, fan 1   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 2   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 3   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 4   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 5   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 6   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 7   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 8   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 9   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 10  | 4     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 1   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 2   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 3   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 4   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 5   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 6   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 7   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 8   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 9   | 4     | 11        | Speed Level | 1    |
| Fan              | bay 2, fan 10  | 4     | 11        | Speed Level | 1    |
| PowerConsumption | N/A            | 1894  | 4050      | Watts       | 1    |
| PowerUnit(AC)    | bay 1          | 0     | 0         | NA          | 1    |
| PowerUnit(AC)    | bay 2          | 0     | 0         | NA          | 1    |
| PowerUnit(AC)    | bay 3          | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 1, fan 1   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 1, fan 2   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 2, fan 1   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 2, fan 2   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 3, fan 1   | 0     | 0         | NA          | 1    |
| PowerUnitFan     | bay 3, fan 2   | 0     | 0         | NA          | 1    |
| SSM              | bay 1          | 40    | 0         | Mbps        | 1    |
| SSM              | bay 2          | 0     | 0         | Mbps        | 1    |
-------------------------------------------------------------------------------
| Chassis 2                                                                   |
-------------------------------------------------------------------------------
| CMM              | bay 1          | 1     | 0         | <S,D>/<A>   | 1    |
| CMM              | bay 2          | 0     | 0         | <S,D>/<A>   | 1    |
| CPUtemp          | blade 1, CPU0  | 47    | 65        | Celsius     | 0    |
| CPUtemp          | blade 1, CPU1  | 51    | 65        | Celsius     | 0    |
| CPUtemp          | blade 2, CPU0  | 46    | 65        | Celsius     | 1    |
| CPUtemp          | blade 2, CPU1  | 56    | 65        | Celsius     | 1    |
| CPUtemp          | blade 3, CPU0  | 49    | 65        | Celsius     | 1    |
| CPUtemp          | blade 3, CPU1  | 51    | 65        | Celsius     | 1    |
| CPUtemp          | blade 4, CPU0  | 0     | 65        | Celsius     | 0    |
| CPUtemp          | blade 4, CPU1  | 0     | 65        | Celsius     | 0    |
| Fan              | bay 1, fan 1   | 3     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 2   | 3     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 3   | 3     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 4   | 3     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 5   | 3     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 6   | 3     | 11        | Speed Level | 1    |
| Fan              | bay 1, fan 7   | 3     | 11        | Speed Level | 1    |
```

```
| Fan              | bay 1, fan 8    | 3      | 11         | Speed Level | 1     |
| Fan              | bay 1, fan 9    | 3      | 11         | Speed Level | 1     |
| Fan              | bay 1, fan 10   | 3      | 11         | Speed Level | 1     |
| Fan              | bay 2, fan 1    | 3      | 11         | Speed Level | 1     |
| Fan              | bay 2, fan 2    | 3      | 11         | Speed Level | 1     |
| Fan              | bay 2, fan 3    | 3      | 11         | Speed Level | 1     |
| Fan              | bay 2, fan 4    | 3      | 11         | Speed Level | 1     |
| Fan              | bay 2, fan 5    | 3      | 11         | Speed Level | 1     |
| Fan              | bay 2, fan 6    | 3      | 11         | Speed Level | 1     |
| Fan              | bay 2, fan 7    | 3      | 11         | Speed Level | 1     |
| Fan              | bay 2, fan 8    | 3      | 11         | Speed Level | 1     |
| Fan              | bay 2, fan 9    | 3      | 11         | Speed Level | 1     |
| Fan              | bay 2, fan 10   | 3      | 11         | Speed Level | 1     |
| PowerConsumption | N/A             | 1624   | 4050       | Watts       | 1     |
| PowerUnit(AC)    | bay 1           | 0      | 0          | NA          | 1     |
| PowerUnit(AC)    | bay 2           | 0      | 0          | NA          | 1     |
| PowerUnit(AC)    | bay 3           | 0      | 0          | NA          | 0     |
| PowerUnitFan     | bay 1, fan 1    | 0      | 0          | NA          | 1     |
| PowerUnitFan     | bay 1, fan 2    | 0      | 0          | NA          | 1     |
| PowerUnitFan     | bay 2, fan 1    | 0      | 0          | NA          | 1     |
| PowerUnitFan     | bay 2, fan 2    | 0      | 0          | NA          | 1     |
| PowerUnitFan     | bay 3, fan 1    | 0      | 0          | NA          | 0     |
| PowerUnitFan     | bay 3, fan 2    | 0      | 0          | NA          | 0     |
| SSM              | bay 1           | 2      | 0          | Mbps        | 1     |
| SSM              | bay 2           | 0      | 0          | Mbps        | 1     |
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Output description

Column	Description
Location	Front panel location.
Value **Threshold** **Units**	Most components have a defined threshold value. The threshold gives an indication of the health and functionality of the component. When the value of the resource is greater than the threshold, the chassis sends an alert (see *"Configuring Alerts for SGM and Security Group Events (asg alert)" on page 216*).
State	Valid values: ■ **0** = Component is not installed ■ **1** = Component is installed

Chassis Control (asg_chassis_ctrl)

Description

Use the Chassis Control utility to monitor and configure SSMs and CMMs with different commands and parameters.

Chassis Control is based on SNMP communication between the Chassis and its components.

Syntax

```
asg_chassis_ctrl <Option> <Parameters>
```

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

Options and Parameters

Options and Parameters	Description
`help [-v]`	Shows help messages in Verbose Mode.
`active_sgms`	Shows all installed SGMs.
`active_ssm`	Shows active SSMs. An SSM that is not installed or is in the DOWN state, does not appear as Active.
`get_fans_status`	Shows the health status of the Chassis fans.
`get_lb_dist {<SSM ID> | all}`	Shows the current distribution matrix from the specified SSM or all SSMs. The matrix is a table containing SGM IDs and used to determine to which other SGMs a packet should be forwarded.
`get_ssm_firmware {<SSM ID> | all}`	Shows the firmware version of the specified SSM or all SSMs.
`get_ssm_type {<SSM ID> | all}`	Shows the model of the specified SSM or all SSMs.
`get_psu_status`	Shows the current status of the AC PSUs.
`get_pems_status`	Shows the current status of the DC PEMs.
`get_cmm_status`	Shows the current status of the CMMs.
`get_cpus_temp <SGM ID>`	Shows temperatures of the specified SGM CPUs.
`get_dist_md5sum`	Shows the MD5 of the distribution matrix for the given SSM. Comparing this checksum against the checksum on other SSMs and verifies that they are synchronized.
`get_ports_stat <SSM ID>`	Prints the port status for the specified SSM.

Options and Parameters	Description
`get_dist_mode <SSM ID>`	Shows the port Distribution Mode for the specified SSM.
`get_dist_mask <SSM ID>`	Shows a summary of the distribution masks in the different modes.
`get_matrix_size <SSM ID>`	Shows the size, in bytes, of the SSM distribution matrix.
`get_sel_info <CMM ID>`	Shows data from the specified CMM event. This information is useful for troubleshooting and system forensics.
`restart_ssm <SSM IDgt;`	Restarts the specified SSM.
`restart_cmm <CMM ID>`	Restarts the specified CMM.
`start_ssm <SSM ID>`	Starts the specified SSM.
`shutdown_ssm <smm_id>`	Shuts down the specified SSM.
`mib2_stats <SSM ID> <Port ID> [<Error Type>]`	Shows MIB2 statistics for the specified SSM and port.
`get_bmac <SSM ID>`	Shows SGM MAC addresses from the SSM.
`get_power_type`	Shows the Chassis input power type (AC or DC).
`get_ac_power_type`	Shows the AC power type.
`jumbo_frames {enable | disable | show} <SSM ID>`	Enables, disables or shows Jumbo Frames on an SSM160/SSM440.
`set_port_mtu <SSM ID> <Port ID> <MTU Size>`	Sets the port MTU size for the specified SSM and port. ■ *<SSM ID>* - SSM identifier (from `1` to `4`, or `all`) ■ *<Port ID>* - Port number ■ *<MTU Size>* - This MTU size can be one of these values: • An integer value up to 12,288 • `max` - Maximum supported MTU size • `default` - System default MTU size (typically, 1544)

Options and Parameters	Description
`get_port_mtu <SSM ID> <Port ID>`	Shows the MTU for the specified SSM and port.
`get_port_media_details <SSM ID>`	Shows port information.
`get_pem_cb_status`	Shows DC PEM status.
`enable_port`	Enables the port.
`disable_port`	Disables the port.

Notes:

- To see the full syntax for an option, enter the command and option without parameters.
- To make sure the Chassis Control commands work correctly in a Dual Chassis configuration, run this command on each Chassis.

Example

```
[Expert@MyChassis-ch0x-0x:0]# asg_chassis_ctrl get_cmm_status
Getting CMM(s) status
CMM #1 -> Health: 1, Active: 1
CMM #2 -> Health: 1, Active: 0
Active CMM firmware version: 2.83
[Expert@MyChassis-ch0x-0x:0]#
```

Collecting System Diagnostics (smo verifiers)

In This Section:

Diagnostic Tests

Description

Use the "`smo verifiers`" commands in Gaia gClish to run a specific set of diagnostic tests.

The full set of tests run by default, but you can manually select the tests 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.
`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.

Parameter	Description
`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

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo verifiers list
-------------------------------------------------------------------------------
| ID | Title              | Command                                          |
-------------------------------------------------------------------------------
| System Components                                                          |
-------------------------------------------------------------------------------
|  1 | System Health      | asg stat -v                                      |
|  2 | Hardware           | asg hw_monitor -v                                |
|  3 | Resources          | asg resource                                     |
|  4 | Software Versions  | asg_version verify -v                            |
|  5 | Software Provision | asg_provision                                    |
|  6 | CPU Type           | cpu_socket_verifier -v                           |
|  7 | Media Details      | transceiver_verifier -v                          |
|  8 | Chassis ID         | verify_chassis_id                                |
|  9 | SSD Health         | asg resource --ssd                               |
-------------------------------------------------------------------------------
| Policy and Configuration                                                   |
-------------------------------------------------------------------------------
| 10 | Distribution Mode  | distutil verify -v                               |
| 11 | DXL Balance        | dxl stat                                         |
| 12 | Policy             | asg policy verify -a                             |
| 13 | AMW Policy         | asg policy verify_amw -a                         |
| 14 | SWB Updates        | asg_swb_update_verifier -v                       |
| 15 | Installation       | installation_verify                              |
| 16 | Security Group     | security_group_util diag                         |
| 17 | Cores Distribution | cores_verifier                                   |
| 18 | Clock              | clock_verifier -v                                |
| 19 | Licenses           | asg_license_verifier -v                          |
| 20 | IPS Enhancement    | asg_ips_enhance status                           |
| 21 | Configuration File | config_verify -v                                 |
-------------------------------------------------------------------------------
| Networking                                                                 |
-------------------------------------------------------------------------------
| 22 | MAC Setting        | mac_verifier -v                                  |
| 23 | ARP Consistency    | asg_arp -v                                       |
| 24 | Interfaces         | interface_verifier -v                            |
| 25 | Bond               | asg_bond -v                                      |
| 26 | IPv4 Route         | asg_route                                        |
| 27 | IPv6 Route         | asg_route -6                                     |
| 28 | Dynamic Routing    | asg_dr_verifier                                  |
| 29 | Local ARP          | asg_local_arp_verifier -v                        |
| 30 | Port Speed         | asg_port_speed verify                            |
| 31 | IGMP Consistency   | asg_igmp                                         |
| 32 | PIM Neighbors      | asg_pim_neighbors                                |
-------------------------------------------------------------------------------
| Misc                                                                       |
-------------------------------------------------------------------------------
| 33 | Core Dumps         | core_dump_verifier -v                            |
| 34 | Processes          | asg_process_verifier -v                          |
| 35 | Performance hogs   | asg_perf_hogs                                    |
-------------------------------------------------------------------------------
| Run "show smo verifiers print id <TestNum>" to display test output         |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

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

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo verifiers last-run report
2019-01-28, 10:32:18
-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                              |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Passed     |                                     |
|  2 | Hardware           | Passed     |                                     |
|  3 | Resources          | Passed     |                                     |
|  4 | Software Versions  | Passed     |                                     |
|  5 | Software Provision | Passed     |                                     |
|  6 | CPU Type           | Passed     |                                     |
|  7 | Media Details      | Failed (!) | (1)SSM 2 on chassis 2               |
|  8 | Chassis ID         | Passed     |                                     |
|  9 | SSD Health         | Passed     |                                     |
-------------------------------------------------------------------------------
| Policy and Configuration                                                    |
-------------------------------------------------------------------------------
| 10 | Distribution Mode  | Passed     | (1)Warning: Mismatch in number of   |
|    |                    |            | load balancing interfaces between SGM |
|    |                    |            |  and SSM                            |
| 11 | DXL Balance        | Passed     |                                     |
| 12 | Policy             | Passed     |                                     |
| 13 | AMW Policy         | Passed     | (1)Not configured                   |
| 14 | SWB Updates        | Passed     | (1)Not configured                   |
| 15 | Installation       | Passed     |                                     |
| 16 | Security Group     | Passed     |                                     |
| 17 | Cores Distribution | Passed     |                                     |
| 18 | Clock              | Passed     |                                     |
| 19 | Licenses           | Passed     |                                     |
| 20 | IPS Enhancement    | Passed     |                                     |
| 21 | Configuration File | Failed (!) | (1)Configuration files inconsistent |
-------------------------------------------------------------------------------
| Networking                                                                  |
-------------------------------------------------------------------------------
| 22 | MAC Setting        | Passed     |                                     |
| 23 | ARP Consistency    | Passed     |                                     |
| 24 | Interfaces         | Passed     |                                     |
| 25 | Bond               | Passed     |                                     |
| 26 | IPv4 Route         | Passed     |                                     |
| 27 | IPv6 Route         | Passed     | (1)Not configured                   |
| 28 | Dynamic Routing    | Passed     |                                     |
| 29 | Local ARP          | Passed     | (1)Not configured                   |
| 30 | Port Speed         | Passed     |                                     |
| 31 | IGMP Consistency   | Passed     |                                     |
| 32 | PIM Neighbors      | Passed     |                                     |
-------------------------------------------------------------------------------
| Misc                                                                        |
-------------------------------------------------------------------------------
| 33 | Core Dumps         | Passed     |                                     |
| 34 | Processes          | Passed     |                                     |
| 35 | Performance hogs   | Passed     |                                     |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 33/35 tests                                                         |
| Run: "show smo verifiers list id 7,21" to view a complete list of failed tes |
| ts                                                                          |
| Output file: /var/log/verifier_sum.1-35.2019-01-28_10-32-18.txt             |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

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

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > 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      | Passed     |                                     |
|  2 | Hardware           | Passed     |                                     |
|  3 | Resources          | Passed     |                                     |
|  4 | Software Versions  | Passed     |                                     |
|  5 | Software Provision | Passed     |                                     |
|  6 | CPU Type           | Passed     |                                     |
|  7 | Media Details      | Failed (!) | (1)SSM 2 on chassis 2               |
|  8 | Chassis ID         | Passed     |                                     |
|  9 | SSD Health         | Passed     |                                     |
-------------------------------------------------------------------------------
| Policy and Configuration                                                    |
-------------------------------------------------------------------------------
| 10 | Distribution Mode  | Passed     | (1)Warning: Mismatch in number of   |
|    |                    |            | load balancing interfaces between SGM |
|    |                    |            |  and SSM                            |
| 11 | DXL Balance        | Passed     |                                     |
| 12 | Policy             | Passed     |                                     |
| 13 | AMW Policy         | Passed     | (1)Not configured                   |
| 14 | SWB Updates        | Passed     | (1)Not configured                   |
| 15 | Installation       | Passed     |                                     |
| 16 | Security Group     | Passed     |                                     |
| 17 | Cores Distribution | Passed     |                                     |
| 18 | Clock              | Passed     |                                     |
| 19 | Licenses           | Passed     |                                     |
| 20 | IPS Enhancement    | Passed     |                                     |
| 21 | Configuration File | Failed (!) | (1)Configuration files inconsistent |
-------------------------------------------------------------------------------
| Networking                                                                  |
-------------------------------------------------------------------------------
| 22 | MAC Setting        | Passed     |                                     |
| 23 | ARP Consistency    | Passed     |                                     |
| 24 | Interfaces         | Passed     |                                     |
| 25 | Bond               | Passed     |                                     |
| 26 | IPv4 Route         | Passed     |                                     |
| 27 | IPv6 Route         | Passed     | (1)Not configured                   |
| 28 | Dynamic Routing    | Passed     |                                     |
| 29 | Local ARP          | Passed     | (1)Not configured                   |
| 30 | Port Speed         | Passed     |                                     |
| 31 | IGMP Consistency   | Passed     |                                     |
| 32 | PIM Neighbors      | Passed     |                                     |
-------------------------------------------------------------------------------
| Misc                                                                        |
-------------------------------------------------------------------------------
| 33 | Core Dumps         | Passed     |                                     |
| 34 | Processes          | Passed     |                                     |
| 35 | Performance hogs   | Passed     |                                     |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 33/35 tests                                                         |
| Run: "show smo verifiers list id 7,21" to view a complete list of failed tes |
| ts                                                                          |
| Output file: /var/log/verifier_sum.1-35.2019-01-28_10-32-18.txt             |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

Running Specific Diagnostic Tests

These commands run the specified diagnostic tests only:

```
show smo verifiers report name
show smo verifiers report id
```

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

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > 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           |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

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

This example collects diagnostic information for specified tests 1, 2, 3, 4, 5, and 26.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo verifiers report id 1,2,3,4,5,26
Duration of tests vary and may take a few minutes to complete

-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                              |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  1 | System Health      | Passed     |                                     |
|  2 | Hardware           | Failed (!) | (1)Chassis fan is down              |
|    |                    |            | (2)Chassis fan exceeds threshold    |
|  3 | Resources          | Failed (!) | (1)Memory capacity                  |
|    |                    |            | (2)Memory capacity mismatch         |
|    |                    |            | (3)Primary HD capacity mismatch     |
|  4 | Software Versions  | Failed (!) |                                     |
|  5 | Software Provision | Passed     |                                     |
-------------------------------------------------------------------------------
| Networking                                                                  |
-------------------------------------------------------------------------------
| 26 | IPv4 Route         | Passed     |                                     |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 3/6 tests                                                           |
| Run: "show smo verifiers list id 2,3,4" to view a complete list of failed te |
| sts                                                                         |
| Output file: /var/log/verifier_sum.1-5.30.2018-12-10_12-17-20.txt           |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

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

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > 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      | Passed     |                                     |
|  2 | Hardware           | Failed (!) | (1)Chassis fan is down              |
|    |                    |            | (2)Chassis fan exceeds threshold    |
|  3 | Resources          | Failed (!) | (1)Memory capacity                  |
|    |                    |            | (2)Memory capacity mismatch         |
|    |                    |            | (3)Primary HD capacity mismatch     |
|  4 | Software Versions  | Failed (!) |                                     |
|  5 | Software Provision | Passed     |                                     |
|  6 | CPU Type           | Passed     |                                     |
|  7 | Media Details      | Failed (!) | (1)SSM 2 on chassis 1               |
|    |                    |            | (2)SSM 1 on chassis 2               |
|    |                    |            | (3)SSM 2 on chassis 2               |
|  8 | Chassis ID         | Passed     |                                     |
|  9 | SSD Health         | Passed     |                                     |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 5/9 tests                                                           |
| Run: "show smo verifiers list id 2,3,4,7" to view a complete list of failed |
| tests                                                                       |
| Output file: /var/log/verifier_sum.1-9.2018-12-10_12-20-35.txt              |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

Error Types

The "`smo verifiers`" command detects these errors:

Error Type	Error	Description
`System health`	`Chassis <X> error`	The Chassis 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`	CPU type is not configured in the list of compliant CPUs on at least one Security Group Member. 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.

Change the threshold values in the `$SMODIR/conf/asg_diag_config` file.

These are the supported resources you can control:

Resource	Instructions
`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.
`Skew`	The maximum permissible clock difference, in seconds, between the SGMs and CMMs. **Note** - This resource applies only to 60000 / 40000 Appliances.
`Certified cpu`	Each line represents one compliant CPU type. **Note** - This resource applies only to 60000 / 40000 Appliances

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	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the `$SMODIR/conf/asg_diag_config` file: `vi $SMODIR/conf/asg_diag_config`
4	Search for this parameter: `MismatchSeverity`

Step	Instructions
5	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
6	Save the changes in the file and exit the editor.
7	Copy the modified file to all Security Group Members: `asg_cp2blades $SMODIR/conf/asg_diag_config`

Troubleshooting Failures

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

Example

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

In the example below, the test shows that two fans are down and the CPU temperature exceeds its threshold.

The output identifies the failed components.

1. The **Hardware** test failed:

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo verifiers report id 2
Duration of tests vary and may take a few minutes to complete

-------------------------------------------------------------------------------
| Tests Status                                                                |
-------------------------------------------------------------------------------
| ID | Title              | Result     | Reason                              |
-------------------------------------------------------------------------------
| System Components                                                           |
-------------------------------------------------------------------------------
|  2 | Hardware           | Failed (!) | (1)Chassis fan is down              |
|    |                    |            | (2)Chassis fan exceeds threshold    |
|    |                    |            | (3)CPU exceeds threshold            |
-------------------------------------------------------------------------------
| Tests Summary                                                               |
-------------------------------------------------------------------------------
| Passed: 0/1 test                                                            |
| Run: "show smo verifiers list id 2" to view a complete list of failed tests |
| Output file: /var/log/verifier_sum.2.2017-01-29_15-46-58.txt                |
| Run "show smo verifiers last-run print" to display verbose output           |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

2. Print the full report for this failed test:

```
[Global] MyChassis-ch01-01 > show smo verifiers print id 2
-------------------------------------------------------------------------------
| Hardware Monitor                                                            |
-------------------------------------------------------------------------------
| Sensor           | Location       | Value | Threshold | Units     | State |
-------------------------------------------------------------------------------
| Chassis 1                                                                   |
-------------------------------------------------------------------------------
| CMM              | bay 1          | 1     | 0         | <S,D>/<A>   | 1   |
| CMM              | bay 2          | 0     | 0         | <S,D>/<A>   | 1   |
| CPUtemp          | blade 1, CPU0  | 0     | 65        | Celsius     | 1   |
| CPUtemp          | blade 1, CPU1  | 0     | 65        | Celsius     | 1   |
| CPUtemp          | blade 2, CPU0  | 44    | 65        | Celsius     | 1   |
| CPUtemp          | blade 2, CPU1  | 41    | 65        | Celsius     | 1   |
| CPUtemp          | blade 3, CPU0  | 44    | 65        | Celsius     | 1   |
| CPUtemp          | blade 3, CPU1  | 40    | 65        | Celsius     | 1   |
| CPUtemp          | blade 4, CPU0  | 47    | 65        | Celsius     | 1   |
| CPUtemp          | blade 4, CPU1  | 43    | 65        | Celsius     | 1   |
| CPUtemp          | blade 5, CPU0  | 46    | 65        | Celsius     | 1   |
| CPUtemp          | blade 5, CPU1  | 42    | 65        | Celsius     | 1   |
| Fan              | bay 1, fan 1   | 0     | 11        | Speed Level | 0   |
| Fan              | bay 1, fan 2   | 0     | 11        | Speed Level | 0   |
| Fan              | bay 2, fan 1   | 15    | 11        | Speed Level | 1   |
| Fan              | bay 2, fan 2   | 15    | 11        | Speed Level | 1   |
| Fan              | bay 3, fan 1   | 15    | 11        | Speed Level | 1   |
| Fan              | bay 3, fan 2   | 15    | 11        | Speed Level | 1   |
| PowerConsumption | N/A            | 2471  | 4050      | Watts       | 1   |
| PowerUnit(AC)    | bay 1          | 0     | 0         | NA          | 1   |
| PowerUnit(AC)    | bay 2          | 0     | 0         | NA          | 1   |
| PowerUnit(AC)    | bay 3          | 0     | 0         | NA          | 1   |
| PowerUnit(AC)    | bay 4          | 0     | 0         | NA          | 0   |
| PowerUnit(AC)    | bay 5          | 0     | 0         | NA          | 0   |
| PowerUnitFan     | bay 1, fan 1   | 0     | 0         | NA          | 1   |
| PowerUnitFan     | bay 1, fan 2   | 0     | 0         | NA          | 1   |
| PowerUnitFan     | bay 2, fan 1   | 0     | 0         | NA          | 1   |
| PowerUnitFan     | bay 2, fan 2   | 0     | 0         | NA          | 1   |
| PowerUnitFan     | bay 3, fan 1   | 0     | 0         | NA          | 1   |
| PowerUnitFan     | bay 3, fan 2   | 0     | 0         | NA          | 1   |
| PowerUnitFan     | bay 4, fan 1   | 0     | 0         | NA          | 0   |
| PowerUnitFan     | bay 4, fan 2   | 0     | 0         | NA          | 0   |
| PowerUnitFan     | bay 5, fan 1   | 0     | 0         | NA          | 0   |
| PowerUnitFan     | bay 5, fan 2   | 0     | 0         | NA          | 0   |
| SSM              | bay 1          | 136   | 0         | Mbps        | 1   |
| SSM              | bay 2          | 128   | 0         | Mbps        | 1   |
-------------------------------------------------------------------------------
| Chassis 2                                                                   |
-------------------------------------------------------------------------------
| CMM              | bay 1          | 1     | 0         | <S,D>/<A>   | 1   |
| CMM              | bay 2          | 0     | 0         | <S,D>/<A>   | 1   |
| CPUtemp          | blade 1, CPU0  | 50    | 65        | Celsius     | 1   |
| CPUtemp          | blade 1, CPU1  | 64    | 65        | Celsius     | 1   |
| CPUtemp          | blade 2, CPU0  | 48    | 65        | Celsius     | 1   |
| CPUtemp          | blade 2, CPU1  | 64    | 65        | Celsius     | 1   |
| CPUtemp          | blade 3, CPU0  | 48    | 65        | Celsius     | 1   |
| CPUtemp          | blade 3, CPU1  | 64    | 65        | Celsius     | 1   |
| CPUtemp          | blade 4, CPU0  | 47    | 65        | Celsius     | 1   |
| CPUtemp          | blade 4, CPU1  | 74    | 65        | Celsius     | 1   |
| CPUtemp          | blade 5, CPU0  | 84    | 65        | Celsius     | 1   |
| CPUtemp          | blade 5, CPU1  | 71    | 65        | Celsius     | 1   |
| Fan              | bay 1, fan 1   | 4     | 11        | Speed Level | 1   |
| Fan              | bay 1, fan 2   | 4     | 11        | Speed Level | 1   |
| Fan              | bay 2, fan 1   | 4     | 11        | Speed Level | 1   |
| Fan              | bay 2, fan 2   | 4     | 11        | Speed Level | 1   |
| Fan              | bay 3, fan 1   | 4     | 11        | Speed Level | 1   |
| Fan              | bay 3, fan 2   | 4     | 11        | Speed Level | 1   |
|    .                                                                        |
|    .                                                                        |
-------------------------------------------------------------------------------
[Global] MyChassis-ch01-01 >
```

Alert Modes

In This Section:

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`" command (or the "`show smo verifiers report`" command) on a regular basis.

If the test fails, an alert appears. The alerts continue to appear in the **Message of the Day** (MOTD) until the issues are resolved.

When the issues are resolved, a **Clear Alert** message appears the next time the test runs.

You can manually run the "`smo verifiers`" command (the "`show smo verifiers report`" command) to confirm the issue is resolved.

Important Notes

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

  Changing the default time

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the `$SMODIR/conf/asgsnmp.conf` file: `vi $SMODIR/conf/asgsnmp.conf`
4	Change the value in this line: `asg_diag_alert_wrapper`
5	Save the changes in the file and exit the editor.
6	Copy this file to all other Security Group Members: `asg_cp2blades $SMODIR/conf/asgsnmp.conf`

- By default, all tests run.

  Excluding the tests

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

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Run: `$SMODIR/conf/asg_diag_config`

4	Add this line to the file:
	`excluded_tests=[<Test1>]`
	`[,<Test2>,...]`

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

6	Copy this file to all other Security Group Members:
	`asg_cp2blades`
	`$SMODIR/conf/asgsnmp.conf`

- All failed tests show in the MOTD.

Excluding failed test notifications from the MOTD

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Run: `# $SMODIR/conf/asg_diag_config`
4	Set the `failed_tests_motd` parameter to `off`
5	Copy this file to all other Security Group Members: `asg_cp2blades $SMODIR/conf/asg_diag_config`
6	Go to Gaia gClish: enter `gclish` and press Enter.
7	Enforce the change: `show smo verifiers report` You can also wait for the next time the "`smo verifiers`" run automatically.

Disabling the MOTD feature

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the `$SMODIR/conf/asg_diag_config` file: `vi $SMODIR/conf/asg_diag_config`
4	Set the value of the `motd` parameter to `off`.
5	Save the changes in the file and exit the editor.
6	Copy this file to all other Security Group Members: `asg_cp2blades $SMODIR/conf/asg_diag_config`
7	Go to Gaia gClish: enter `gclish` and press Enter.
8	Enforce the change: `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`" command only shows a warning about resource mismatches between Security Group Members.

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

Changing the default behavior

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the `$SMODIR/conf/asg_diag_config` file: `vi $SMODIR/conf/asg_diag_config`
4	Search for this parameter: `MismatchSeverity`
5	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
6	Save the changes in the file and exit the editor.
7	Copy this file to all other Security Group Members: `asg_cp2blades $SMODIR/conf/asg_diag_config`

System Monitoring

Use these features to monitor your system status.

Showing System Serial Numbers (asg_sgm_serial, asg_serial_info)

Description

These commands in Gaia gClish or Expert mode show and save serial numbers for Chassis hardware components:

- `asg_sgm_serial` - Shows serial numbers for SGMs in the UP state that belong to the Security Group only.
- `asg_serial_info` - Shows CMM, SSM, and Chassis serial numbers.

The information is saved in the `gasginfo` archive file.

Syntax

```
asg_sgm_serial [-a]
asg_serial_info [-a]
```

Parameters

Parameter	Description
`-a`	Apply command on all SGMs in the Security Group

Example 1

```
[Expert@MyChassis-ch0x-0x:0]# asg_sgm_serial
1_01:
 Board Serial          : AKO0769153
1_02:
 Board Serial          : AKO0585533
2_01:
 Board Serial          : AKO0462069
2_02:
 Board Serial          : AKO0447878
[Expert@MyChassis-ch0x-0x:0]#
```

Example 2

```
[Expert@MyChassis-ch0x-0x:0]# asg_serial_info
chassis 1 CMM1 serial: 1163978/005
chassis 1 CMM2 serial: 1157482/001
chassis 1 SSM1 serial: 0011140011
chassis 1 SSM2 serial: 0011140012
chassis 1 serial: 1159584/016
chassis 2 CMM1 serial: 1163090/041
chassis 2 CMM2 serial: 1155519/014
chassis 2 SSM1 serial: 0311310621
chassis 2 SSM2 serial: 0311310626
chassis 2 serial: 0831232/001
[Expert@MyChassis-ch0x-0x:0]#
```

Note - To show CMM, SSM and Chassis serial numbers, one of the SGMs on each Chassis must be UP. For example, if no SGM in the UP position is found on Chassis-2, the serial numbers for components in the Chassis are not shown or saved.

Showing System Serial Numbers (asg_sgm_serial, asg_serial_info)

Description

Use these commands in Gaia gClish or Expert mode to show and save serial numbers for chassis hardware components:

Command	Description
`asg_sgm_serial`	Shows serial numbers for SGMs that are in the UP state that belong to the Security Group only.
`asg_serial_info`	Shows serial numbers for CMMs, SSMs, and Chassis.

Notes:

- The information is saved in the `gasginfo` archive file.
- To show the serial numbers for CMMs, SSMs and Chassis, one of the SGMs on each Chassis must be in the UP state.
  For example, if no SGMs in the UP state are found on Chassis 2, the serial numbers for components in the Chassis are not shown or saved.

Syntax

```
asg_sgm_serial [-a]
```

```
asg_serial_info [-a]
```

Parameters

Parameter	Description
-a	Applies command to all SGMs in the Security Group.

Example 1

```
[Expert@MyChassis-ch0x-0x:0]# asg_sgm_serial
1_01:
 Board Serial          : AKO0769153
1_02:
 Board Serial          : AKO0585533
2_01:
 Board Serial          : AKO0462069
2_02:
 Board Serial          : AKO0447878
[Expert@MyChassis-ch0x-0x:0]#
```

Example 2

```
[Expert@MyChassis-ch0x-0x:0]# asg_serial_info
chassis 1 CMM1 serial: 1163978/005
chassis 1 CMM2 serial: 1157482/001
chassis 1 SSM1 serial: 0011140011
chassis 1 SSM2 serial: 0011140012
chassis 1 serial: 1159584/016
chassis 2 CMM1 serial: 1163090/041
chassis 2 CMM2 serial: 1155519/014
chassis 2 SSM1 serial: 0311310621
chassis 2 SSM2 serial: 0311310626
chassis 2 serial: 0831232/001
[Expert@MyChassis-ch0x-0x: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 R81
OS build xxx
OS kernel version 3.10.0-693cpx86_64
OS edition 64-bit

1_02:
Product version Check Point Gaia R81
OS build xxx
OS kernel version 3.10.0-693cpx86_64
OS edition 64-bit

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

Showing Software and Firmware Versions (asg_version)

Description

Use the "`asg_version`" command in Gaia gClish or Expert mode:

- To retrieve system configuration
- To retrieve software versions:
  - Check Point software (Firewall and SecureXL versions)
  - Firmware versions for SGMs, SSMs, and CMMs
  - Make sure that system hardware components are running approved software and firmware versions

Syntax

```
asg_version -h
asg_version [verify] [-v] [-i] [-b <SGM IDs>]
```

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`verify`	Makes sure that system hardware components run approved software and firmware versions.
`-i`	Shows Active and Standby SGMs.

Parameter	Description
`-b<SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)
`-v`	Shows verbose version information.

Examples

Example 1 - Showing a list of two SGMs

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > asg_version -b 1_01,1_03
SGMs
======

----------
-*- 2 SGMs: 1_01 1_03 -*-
OS build 42, OS kernel version 2.6.18-92cpx86_64, OS edition 64-bit

Hardware
--------
-*- 1 blade: 1_01 -*-
BIOS: 1.30 BL: 1.52 IPMC: 1.52 FPGA: 2.40 FPGARE: 2.40
-*- 1 blade: 1_03 -*-
BIOS: 0.54 BL: 1.42 IPMC: 1.42 FPGA: 2.38 FPGARE: 2.38
OS version
----------
BIOS: 0.54 BL: 1.42 IPMC: 1.42 FPGA: 2.38 FPGARE: 2.
[Global] MyChassis-ch01-01 >
```

Examples 2 - Showing verbose output

```
[Expert@MyChassis-ch0x-0x:0]# asg_version -v

+-------------------------------------------------------------------------------+
| Hardware Versions                                                             |
+-------------------------------------------------------------------------------+
| Component       | Type            | Configuration      | Firmware           |
+-------------------------------------------------------------------------------+
| Chassis 1                                                                     |
+-------------------------------------------------------------------------------+
| SSM1            | SSM160          | N/A                | 5.5.R1.4.CP404     |
| SSM2            | SSM160          | N/A                | 5.5.R1.4.CP404     |
| CMM             | N/A             | N/A                | 2.83               |
+-------------------------------------------------------------------------------+

+-------------------------------------------------------------------------------+
| Hardware Versions                                                             |
+-------------------------------------------------------------------------------+
| Component       | Type            | Configuration      | Firmware           |
+-------------------------------------------------------------------------------+
| Chassis 2                                                                     |
+-------------------------------------------------------------------------------+
| SSM1            | SSM160          | N/A                | 5.5.R1.4.CP404     |
| SSM2            | SSM160          | N/A                | 5.5.R1.4.CP404     |
| CMM             | N/A             | N/A                | 2.83               |
+-------------------------------------------------------------------------------+

blades
======
Type
----------
10 blades: 1_01 1_02 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 *
SGM260

OS version
----------
10 blades: 1_01 1_02 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 *
OS build 64, OS kernel version 2.6.18-92cpx86_64, OS edition 64-bit

FireWall-1 version
------------------
10 blades: 1_01 1_02 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 *
This is Check Point's software version R80.20SP - Build 062
kernel: R80.20SP - Build 057

Performance Pack version
------------------------
10 blades: 1_01 1_02 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 *
This is Check Point Performance Pack version: R80.20SP - Build 054
Kernel version: R80.20SP - Build 054

Installed Bundles
-----------------
10 blades: 1_01 1_02 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 *
N/A

Hardware
--------
10 blades: 1_01 1_02 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 *
BIOS: 2.10 BL: 1.40 IPMC: 1.40 FPGA: 2.66 NVRAM: 21.00

SSD
-
1 blade: 1_01 *
Firmware Version: D2010370
7 blades: 1_02 1_04 2_01 2_02 2_03 2_04 2_05 *
Firmware Version: 400i
2 blades: 1_03 1_05 *
Firmware Version: D2010355

Number of cores
---------------
```

```
10 blades: 1_01 1_02 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 *
40

Number of CoreXL instances
--------------------------
10 blades: 1_01 1_02 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 *
36

CPUs frequency
--------------
10 blades: 1_01 1_02 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 *
2.4GHz
[Expert@MyChassis-ch0x-0x:0]#
```

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 log files in a 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 Chassis 1 that contain the word "`Restarted`":

```
[Expert@MyChassis-ch0x-0x: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-R81/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-R81/fw1/bin/cmd[11379], count=2
[Global] MyChassis-ch01-01 >
```

Configuring a Dedicated Logging Port

The Chassis logging mechanism lets each SGM forward logs directly to a dedicated Log Server over the SSM's management ports.

However, the SSM's management ports can experience a high load when SGMs generate a large number of logs.

To reduce the load on the SSM management ports:

1. Configure a dedicated SSM port for logging
2. Configure the Chassis to send the logs to the dedicated Log Server

Topology:

`[Management Server](some interface) <===> (SSM port 1)[Chassis]`

`[Management Server](some interface) <===> (interface 1) [Log Server] (interface 2) <===> (SSM port 2)[Chassis]`

Procedure:

Step	Instructions
1	Install a dedicated Log Server: a. Install a dedicated Log Server with two physical interfaces. See the applicable *Installation and Upgrade Guide* > 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 SSM port. **Important** - Do **not** use the same SSM port, which connects to the Management Server. d. In SmartConsole, create the required object that represents the dedicated Log Server. See the applicable *Installation and Upgrade Guide* > Chapter *Installing a Dedicated Log Server or SmartEvent Server.*

2	In the Gaia OS of the Security Group, configure in Gaia gClish the dedicated management port on the SSM.
	Syntax:
	`[Expert@MyChassis-ch0x-0x:0]# gclish`
	`[Global] MyChassis-ch01-01> set interface ethX-MgmtY ipv4-address <IPv4 Address> mask-length <Mask Length>`
	Example:
	`[Global] MyChassis-ch01-01 > set interface eth1-Mgmt2 ipv4-address 2.2.2.10 mask-length 24`
	Note - You must assign an IPv4 address from the same subnet as assigned to the dedicated interface on the Log Server, which connects to the SSM.

3	In SmartConsole, configure the Security Group object to send its logs to the dedicated Log Server. See the applicable *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

Run this command in Gaia gClish or the Expert mode.

```
asg_log_servers
```

Example

```
[Expert@MyChassis-ch0x-0x: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 the CLI 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 (Pnote), a second confirmation can be required.

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

```
[Expert@MyChassis-ch0x-0x:0]# 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
```

Description

Use the "`asg log audit`" command to see the audit logs.

Syntax

```
asg log audit
```

Example

```
[Expert@MyChassis-ch0x-0x:0]# 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
[Expert@MyChassis-ch0x-0x:0]#
```

Viewing the Audit Log File (show smo log auditlog)

Description

Use the "`show smo auditlog filter`" command in Gaia gClish to see the contents of the `auditlog` file.

This log file contains an entry for each change made to the SGM configuration database with Gaia gClish or other commands.

The `auditlog` file for each SGM is located in the `/var/log/` directory.

The log contains two types of activities:

Activity	Description
Permanent	The activity permanently changes the configuration database on the SGM hard disk.
Transient	The activity changes the configuration database in SGM memory, which does not survive reboot.

Syntax

```
show smo log auditlog [filter <String>] [from [<N>]] [to [<N>]]
[tail [<X>]]
```

Parameters

Parameter	Description
`filter <String>`	Specifies a word or phrase , by which to filter the output.
`from <N>`	Shows logs filtered by the time range (number of seconds).
`to <N>`	Shows logs filtered by the time range (number of seconds).
`tail <X>`	Shows only the last *X* lines of the log file for each SGM. For example, "`-tail 3`" shows only the last 3 lines of the specified log file. Default: 10 lines.

Note - Each entry contains one of these characters:

- **p +**
  Means a permanent action that added or changed an item in the configuration database.
- **p -**
  Means a permanent action that deleted an item in the configuration database.
- **t +**
  Means a transient action that added or changed an item in the configuration database in memory only.
- **t -**
  Means a transient action that deleted an item in the configuration database in memory only.

Example filter

This example shows only permanent actions to save the configuration.

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo log auditlog filter update_status
Oct 19 03:19:30 1_02  admin localhost p +installer:update_status -1
Oct 19 03:19:32 1_02  admin localhost p -installer:update_status -1
Oct 19 03:19:32 1_02  admin localhost p +installer:update_status 0
Oct 19 03:19:45 1_06  admin localhost p +installer:update_status -1
Oct 19 03:19:46 1_06  admin localhost p -installer:update_status -1
Oct 19 03:19:46 1_06  admin localhost p +installer:update_status 0
Oct 19 03:20:00 1_07  admin localhost p +installer:update_status -1
Oct 19 03:20:01 1_07  admin localhost p -installer:update_status -1
[Global] MyChassis-ch01-01 >
```

Viewing a Log File (asg log)

Description

Use the "`asg log`" command in the Expert mode to see the contents of a specified log file.

Syntax

```
asg log [-b <SGM IDs>] --file <Log File> [--from "<Timestamp>"] [--to "<Timestamp>"] [--tail <N>] [--filter <String>]
```

Parameters

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)
`<Log File>`	Specifies the log file by its type or full path: ■ `audit` If you specify the log type, the output shows all audit logs in the `/var/log/` directory. To specify a log file, enter its full path and name. For example: `/var/log/asgaudit.log.1` ■ `ports` If you specify the log type, the output shows all ports logs in the `/var/log/` directory. To specify a log file, enter its full path and name. For example: `/var/log/ports` ■ `dist_mode` If you specify the log type, the output shows all logs for the Distribution Mode activity. To specify a log file, enter its full path and name. For example: `/var/log/dist_mode` See *"Working with the Distribution Mode" on page 65*.
`--from "<Timestamp>"`	Shows only the log entries from the specified timestamp and above. You must use the timestamp as it appears in the log file.

Parameter	Description
`--to "<Timestamp>"`	Shows only the log entries until the specified timestamp. You must use the timestamp as it appears in the log file.
`--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 3 lines of the specified log file. Default: 10 lines.
`--filter <String>`	Specifies a text string to use as a filter for the log entries. For example: `--filter debug`

Examples

Example 1 - Audit logs (specified by the log type)

```
[Expert@MyChassis-ch0x-0x:0]# 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
[Expert@MyChassis-ch0x-0x:0]#
```

Example 2 - Port logs (specified by the log type), last 12 lines

```
[Expert@MyChassis-ch0x-0x:0]# 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
[Expert@MyChassis-ch0x-0x:0]#
```

Example 3 - Port logs (specified by the full path), filtered by timestamps

```
Expert@MyChassis-ch01-01:0]# asg log --file /var/log/ports --from "Jan 28 14:52:30"
Jan 28 14:52:30 2019 1_01  MyChassis-ch01-01 sgm_pmd: update_firewall_with_ssm_amount:461:
Updating SSMs amount to 2 out of 2, mask: 3
Jan 28 14:52:30 2019 1_01  MyChassis-ch01-01 cphaconf: Setting available_ssm_mask: 3, num_of_
available: 2, num_of_required to: 2
Jan 28 14:53:02 2019 1_01  MyChassis-ch01-01 sgm_pmd: update_firewall_with_ssm_amount:461:
Updating SSMs amount to 2 out of 2, mask: 3
Jan 28 14:53:02 2019 1_01  MyChassis-ch01-01 cphaconf: Setting available_ssm_mask: 3, num_of_
available: 2, num_of_required to: 2
Jan 28 14:53:34 2019 1_01  MyChassis-ch01-01 sgm_pmd: update_firewall_with_ssm_amount:461:
Updating SSMs amount to 2 out of 2, mask: 3
Jan 28 14:53:34 2019 1_01  MyChassis-ch01-01 cphaconf: Setting available_ssm_mask: 3, num_of_
available: 2, num_of_required to: 2
Jan 28 14:54:06 2019 1_01  MyChassis-ch01-01 sgm_pmd: update_firewall_with_ssm_amount:461:
Updating SSMs amount to 2 out of 2, mask: 3
Jan 28 14:54:06 2019 1_01  MyChassis-ch01-01 cphaconf: Setting available_ssm_mask: 3, num_of_
available: 2, num_of_required to: 2
Jan 28 14:54:38 2019 1_01  MyChassis-ch01-01 sgm_pmd: update_firewall_with_ssm_amount:461:
Updating SSMs amount to 2 out of 2, mask: 3
Jan 28 14:54:38 2019 1_01  MyChassis-ch01-01 cphaconf: Setting available_ssm_mask: 3, num_of_
available: 2, num_of_required to: 2
Jan 28 14:55:10 2019 1_01  MyChassis-ch01-01 sgm_pmd: update_firewall_with_ssm_amount:461:
Updating SSMs amount to 2 out of 2, mask: 3
Jan 28 14:55:10 2019 1_01  MyChassis-ch01-01 cphaconf: Setting available_ssm_mask: 3, num_of_
available: 2, num_of_required to: 2
Jan 28 14:55:42 2019 1_01  MyChassis-ch01-01 sgm_pmd: update_firewall_with_ssm_amount:461:
Updating SSMs amount to 2 out of 2, mask: 3
Jan 28 14:55:42 2019 1_01  MyChassis-ch01-01 cphaconf: Setting available_ssm_mask: 3, num_of_
available: 2, num_of_required to: 2
Jan 28 14:56:14 2019 1_01  MyChassis-ch01-01 sgm_pmd: update_firewall_with_ssm_amount:461:
Updating SSMs amount to 2 out of 2, mask: 3
Jan 28 14:56:14 2019 1_01  MyChassis-ch01-01 cphaconf: Setting available_ssm_mask: 3, num_of_
available: 2, num_of_required to: 2
Jan 28 14:56:46 2019 1_01  MyChassis-ch01-01 sgm_pmd: update_firewall_with_ssm_amount:461:
Updating SSMs amount to 2 out of 2, mask: 3
Jan 28 14:56:46 2019 1_01  MyChassis-ch01-01 cphaconf: Setting available_ssm_mask: 3, num_of_
available: 2, num_of_required to: 2
[Expert@MyChassis-ch01-01:0]#
```

Example 4 - Distribution Mode logs (specified by the log type), filtered by the string "bridge"

```
[Expert@MyChassis-ch0x-0x:0]# 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
[Expert@MyChassis-ch0x-0x:0]#
```

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 a Security Group Member is **not** affected by non-monitored Virtual Systems. For example, a non-monitored Virtual System in a problem state is ignored - the Security Group Member state does **not** change to DOWN.

Use Case

A Virtual System that is not monitored is useful, if it is necessary for the Security Group Member to be in the UP state, even if a specific Virtual System is DOWN or does not have a Security 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`	Shows all non-monitored Virtual Systems.
`stop`	Stops the monitoring of the specified Virtual Systems. **Important** - When you stop the monitoring of a Virtual System, you must run the "`cpha_vsx_util monitor start <VS IDs>`" command to start it again. Monitoring does not start automatically after a reboot.
`start`	Starts the monitoring of the specified Virtual Systems.
`<VS IDs>`	Applies to Virtual Systems as specified by the `<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 This parameter is only applicable in a VSX environment.

Software Blades Update Verification (asg_swb_update_verifier)

Description

Use the "`asg_swb_update_verifier`" command in Gaia gClish or Expert mode to make sure that the signatures are up-to-date for these Software Blades:

- Anti-Virus
- Anti-Bot
- Application Control
- URL Filtering

Syntax

```
asg_swb_update_verifier [-v] [-b <SGM IDs> [-m <Product>] [-n [-p
<IP Address>:<Port>]] ] [-u <Product>]
```

Parameters

Parameter	Description
`-v`	Shows verbose output.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`)
`-m <Product>`	Forces a manual update for the specified Software Blades on the Security Group Members specified with the "`-b <SGM IDs>`" parameter. Valid values: ■ `all` All applicable Software Blades ■ `Anti-Bot` The Anti-Bot Software Blade ■ `Anti-Virus` The Anti-Virus Software Blade ■ `APPI` The Application Control Software Blade ■ `URLF` The URL Filtering Software Blade

Parameter	Description
`-n`	Forces an update download from the Internet. Use with the "`-m`" parameter.
`-p <IP Address>:<Port>`	Forces an update download from the Internet and uses the specified HTTP proxy. Use with the "`-m`" parameter. ■ *<IP Address>* - IP address of the HTTP proxy server ■ *<Port>* - TCP port to use on the HTTP proxy server
`-u <Product>`	Forces a database update for the specified Software Blades. Valid values: ■ `all` All applicable Software Blades ■ `Anti-Bot` The Anti-Bot Software Blade ■ `Anti-Virus` The Anti-Virus Software Blade ■ `APPI` The Application Control Software Blade ■ `URLF` The URL Filtering Software Blade

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > asg_swb_update_verifier
+-------------------------------------------------------------------------------+
| product    | sgm  | status           | DB version | next update check        |
+-------------------------------------------------------------------------------+
| APPI       | 2_01 | failed           | 14061202   | Thu Jun 12 10:32:55 2014 |
| APPI       | 2_02 | failed           | 14061202   | Thu Jun 12 10:32:41 2014 |
| Anti-Bot   | 2_01 | up-to-date       | 1405220911 | Thu Jun 12 09:28:34 2014 |
| Anti-Bot   | 2_02 | up-to-date       | 1405220911 | Thu Jun 12 09:28:45 2014 |
| Anti-Virus | 2_01 | up-to-date       | 1406121233 | Thu Jun 12 09:28:12 2014 |
| Anti-Virus | 2_02 | new              | 1406121234 | Thu Jun 12 09:28:10 2014 |
| URLF       | 2_01 | not-installed    | N/A        | N/A                      |
| URLF       | 2_02 | not-installed    | N/A        | N/A                      |
+-------------------------------------------------------------------------------+

Report:
------------------------------ APPI ----------------------------------------
DB versions verification                                          [   OK   ]
statuses verification                                            [ FAILED ]

------------------------------ URLF ----------------------------------------
DB versions verification                                          [   OK   ]
statuses verification                                            [   OK   ]

------------------------------ Anti-Bot ------------------------------------
DB versions verification                                          [   OK   ]
statuses verification                                            [   OK   ]

------------------------------ Anti-Virus ----------------------------------
DB versions verification                                          [   OK   ]
statuses verification                                            [   OK   ]
[Global] MyChassis-ch01-01 >
```

Output description

Field	Description
product	Name of the Software Blade.
sgm	Security Group Member ID.
status	Update status.
DB version	Database version for a Software Blade.
next update check	Date and time for the next automatic update.
DB versions verification	■ **OK** - The database version is correct. ■ **FAILED** - The database version is incorrect.
statuses verification	■ **OK** - The update installed correctly or no update is needed. ■ **FAILED** - The update did not install correctly.

Working with 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 the Chassis 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 Clish.
4	Go to Gaia gClish: enter `gclish` and press Enter.

5	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 SGM and Security Group Events (asg alert)" on page 216*.

SNMP Monitoring of Security Groups in VSX Mode

For more information, see the:

- *R81 Scalable Platforms Gaia Administration Guide*
- *R81 Scalable Platforms 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 Connections	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	
Sensors on every Chassis	Table	1.3.6.1.4.1.2620.1.48.22.1.1	Status details of: ■ Fans ■ SSMs ■ CPU temperature ■ CMM ■ PSUs ■ PSU Fans
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 Hyper-Threading

Hyper-Threading mechanism runs more than one process at the same time on a CPU core.

A physical CPU that supports Hyper-Threading, adds one or more logical CPUs, which the operating system sees as independent CPUs.

To enable Hyper-Threading:

Step	Instructions
1	Connect to the command line on the chassis.
2	Log in to Gaia Clish or the Expert mode.
3	Start the Check Point Configuration Tool: `cpconfig`
4	Select **Configure HyperThreading**.
5	Follow the on-screen instructions.

Note - Hyper-Threading is enabled by default on the SGM260.

Important - You must reboot all SGMs after all changes in the Hyper-Threading configuration.

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 Chassis, 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 *R81 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	In the **Calculate the maximum limit for concurrent connections** section, select **Manually**.
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]
```

Working with Jumbo Frames

In This Section:

The 40000 / 60000 chassis support Jumbo Frames with a total size of:

- For the SSM440 - up to 9,416 bytes
- For the SSM160 - Up to 12,200 bytes
- For the SGM400 - Up to 9,702 bytes

Note - Carefully calculate the MTU. For example: IPsec or GRE traffic adds bytes to the header and this leaves fewer bytes for the data payload.

Configuring Support for Jumbo Frames on Security Gateway

Description

You can configure support for Jumbo Frames for each applicable interface on an SGM.

Notes:

- This command can take several seconds to work.
- In a Dual Chassis environment, this command configures support for Jumbo Frames on both Chassis.

Syntax in Gaia gClish

```
set interface <Name of Interface> mtu <MTU Size>
```

Parameters

Parameter	Description
<Name of Interface>	Interface name as defined in the Gaia operating system.
<MTU Size>	Valid values to enable the support for Jumbo Frames: ■ For SSM440: 1501 - 9,416 bytes ■ For SSM160: 1501 - 12,200 bytes ■ For SGM400: 1501 - 9,702 bytes Valid values to disable the support for Jumbo Frames on all SSM and SGM models: ■ 68 - 1500 bytes

Example 1 - Enabling Jumbo Frames on eth1-01

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > set interface eth1-01 mtu 9000
1_02:
Note: MTU changes are propagated to the SSMs. Use "asg_jumbo_
conf show" to validate changes
[Global] MyChassis-ch01-01 >
```

Example 2 - Disabling Jumbo Frames on eth1-01

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > set interface eth1-01 mtu 1500
1_02:
Note: MTU changes are propagated to the SSMs. Use "asg_jumbo_
conf show" to validate changes
[Global] MyChassis-ch01-01 >
```

Configuring Support for Jumbo Frames on VSX Gateway

To enable the support for Jumbo Frames on a VSX Gateway:

Step	Instructions
1	Connect with SmartConsole to the Management Server that manages the VSX Gateway, or the applicable Virtual Device.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the VSX Gateway object, or the applicable Virtual Device object.
4	From the left tree, click **Topology**.
5	Edit the applicable interface.
6	On the **General** tab, set the **MTU** to 1501 or a greater value. Valid values to enable the support for Jumbo Frames: ■ For SSM440: 1501 - 9,416 bytes ■ For SSM160: 1501 - 12,200 bytes ■ For SGM400: 1501 - 9,702 bytes
7	Click **OK**.
8	Install Access Control Policy on the VSX Gateway object, or the applicable Virtual Device object.

To disable the support for Jumbo Frames on a VSX Gateway:

Step	Instructions
1	Connect with SmartConsole to the Management Server that manages the VSX Gateway, or the applicable Virtual Device.
2	From the left navigation panel, click **Gateways & Servers**.
3	Open the VSX Gateway object, or the applicable Virtual Device object.
4	From the left tree, click **Topology**.
5	Edit the applicable interface.

Step	Instructions
6	On the **General** tab, set the **MTU** to a value between 68 and 1500 bytes.
7	Click **OK**.
8	Install Access Control Policy on the VSX Gateway object, or the applicable Virtual Device object.

Confirming Jumbo Frames Configuration on SSM160/SSM440 (asg_chassis_ctrl)

To run the validation test on the SSM:

Step	Instructions
1	Show the Jumbo Frames configuration on the specified SSM: `asg_chassis_ctrl jumbo_frames show <SSM ID>`
2	Show the configured MTU on the specified SSM port: `asg_chassis_ctrl get_port_mtu <SSM ID> <Port ID>`

Example

```
[Expert@MyChassis-ch0x-0x:0]# asg_chassis_ctrl jumbo_frames show
1
Jumbo frames are enabled on SSM1
[Expert@MyChassis-ch0x-0x:0]#
```

```
[Expert@MyChassis-ch0x-0x:0]# asg_chassis_ctrl get_port_mtu 1 1
MTU of port 1 on SSM1 is 1544
[Expert@MyChassis-ch0x-0x:0]#
```

Confirming Jumbo Frames on SGMs and SGM Interfaces (asg_jumbo_conf show)

Description

You can confirm configuration of Jumbo Frames on SGMs and SGM interfaces.

Use the "`asg_jumbo_conf show`" command in the Expert mode to:

- Make sure that Jumbo Frames are enabled on the SGMs.
- See the configured MTU values on SGM interfaces configured for Jumbo Frames.

Syntax

```
asg_jumbo_conf show [-v]
```

Parameters

Parameter	Description
`-v`	Detailed report (verbose)

Example

```
[Expert@MyChassis-ch0x-0x:0]# asg_jumbo_conf show -v
Jumbo frames are enabled on SGMs (SSM1 max MTU: 12288 SSM2 max
MTU: 12288 )
Retrieving SSMs Jumbo frames configuration
Chassis1
SSMs:
Jumbo frames are enabled on SSM1
Jumbo frames are enabled on SSM2
Interfaces MTU configuration:
interface:BPEth0:mtu 12288
interface:BPEth1:mtu 12288
The MTU of all the interfaces which are not in the list is 1500
[Expert@MyChassis-ch0x-0x:0]#
```

Working with Rx and Tx Ring Parameters

Use the `ethtool` command in the Expert mode to change in the size of Rx (receive) and Tx (transmit) ring parameters.

The ring parameters are also called interface buffers.

This change is supported only for the `BPEth0` and `BPEth1` interfaces.

Viewing the current configuration

```
ethtool -g {BPEth0 | BPEth1}
```

Example:

```
[Expert@MyChassis-ch0x-0x:0]# ethtool -g BPEth0
Ring parameters for BPEth0:
Pre-set maximums:
RX: 4096
RX Mini: 0
RX Jumbo: 0
TX: 4096
Current hardware settings:
RX: 256
RX Mini: 0
RX Jumbo: 0
TX: 1024
[Expert@MyChassis-ch0x-0x:0]#
```

Configuring the Rx (Receive) Ring Parameter

```
ethtool -G {BPEth0 | BPEth1} rx <Rx Size>
```

Example:

```
[Expert@MyChassis-ch01-01:0]# ethtool -G BPEth0 rx 4096
```

Configuring the Tx (Rransmit) Ring Parameter

```
ethtool -G {BPEth0 | BPEth1} tx <Tx Size>
```

Example:

```
[Expert@MyChassis-ch01-01:0]# ethtool -G BPEth0 tx 4096
```

Configuring the Rx (Receive) and Tx (Transmit) Ring Parameters

```
ethtool -G {BPEth0 | BPEth1} rx <Rx Size> tx <Tx Size>
```

Example:

```
[Expert@MyChassis-ch01-01:0]# ethtool -G BPEth0 rx 4096 tx 4096
```

Advanced Hardware Configuration

This chapter describes advanced hardware configuration for CMMs, SSMs, and SGMs.

Configuring Port Speed

In This Section:

SSM Port Speed

SSM Ports	Port Speed
1 - 7	The port speed is can be: Auto, 1G, or 10G
8	The port speed is always 10G. This is the Sync port for Dual Chassis.
9 - 16 on SSM160	These are the QSFP ports. The port speed is according to the SSM QSFP port mode.
9 - 40 on SSM440	These are the QSFP ports. The port speed is according to the SSM QSFP port mode. **Note** - A license is required to use the 100GB ports on SSM440.

Supported Fanouts on SSM440:

Option	Ports 01-08	Ports 09-24	Ports 25-40
1	8 x 10G	4 x 40G	2 x 100G
2	8 x 10G	16 x 10G	2 x 100G
3	8 x 10G	4 x 40G	2 x 40G
4	8 x 10G	16 x 10G	8 x 10G

Configuring the Speed of SSM Ports 1-7

Description

Use these commands in Gaia gClish to configure and show the speed of the SSM data ports 1-7.

Configuration is saved to the database on all SGMs.

Syntax to configure the speed

```
set interface <Name of Port> link-speed <Speed>
```

Syntax to show the configured speed

```
show interface <Name of Port> speed
```

For more information, see the *R81 Scalable Platforms Gaia Administration Guide* > Chapter *Network Management* > Section *Network Interfaces*.

Parameters

Parameter	Description
<Name of Port>	Interface name in the "`eth<X>-<YZ>`" format. Example: `eth1-01`
<Speed>	Interface speed: ■ `auto` - Automatically selected based on the hardware detected ■ `1G` - 1 Gbit/second ■ `10G` - 10 Gbit/second

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > set interface eth1-01 link-speed 1G
1_01:
success

[Global] MyChassis-ch01-01 > show interface eth1-01 speed
1_01:
speed 1G
[Global] MyChassis-ch01-01 >
```

Configuring the QSFP Port Mode on SSMs

Description

Use these commands in Gaia gClish to configure and show the QSFP port mode on the SSM.

Configuration is saved to the database on all SGMs.

Important - Changing the QSFP port mode causes the SSM to reboot. This can cause traffic outage.

Syntax

```
set ssm id <SSM ID> qsfp-ports-mode <QSFP Port Mode>
```

Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><SSM ID></td><td>SSM identification number: 1 or 2.</td></tr>
<tr><td><QSFP Port Mode></td><td>Specifies the QSFP port mode and speeds.
<table>
<tr><th>SSM Model</th><th>QSFP Port Mode</th><th>Port Speeds</th></tr>
<tr><td>SSM160</td><td>4x10G</td><td>Ports from 9 to 16 - work in 10G mode</td></tr>
<tr><td>SSM160</td><td>40G</td><td>Ports 9 and 13 - work in 40G mode</td></tr>
<tr><td>SSM440</td><td>2x100G_
4x40G</td><td>Ports 9, 13, 17, and 21 - work in 40G mode
Ports 25 and 33 - work in 100G mode</td></tr>
<tr><td>SSM440</td><td>6x40G</td><td>Ports 9, 13, 17, 21, 25, and 33 - work in 40G mode</td></tr>
<tr><td>SSM440</td><td>32x10G</td><td>Ports from 9 to 40 - work in 10G mode</td></tr>
<tr><td>SSM440</td><td>2x100G_
16x10G</td><td>Ports from 9 to 24 - work in 10G mode
Ports 25 and 33 - work in 100G mode</td></tr>
</table></td></tr>
</table>

Example for SSM440

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > set ssm id 2 qsfp-ports-mode 2x100G_
16x10G
You are about to perform SSM QSFP ports mode configuration on SSM:
2 on blades: all

After this action SSM will be rebooted automatically.
It might cause performance hit or outage for a period of time.


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

SSM QSFP ports mode configuration on SSM: 2 requires auditing
Enter your full name: admin
Enter reason for SSM QSFP ports mode configuration on SSM: 2
[Maintenance]: Maintenance
WARNING: SSM QSFP ports mode configuration on SSM: 2 on blades:
all, User: admin, Reason: Maintenance
Please wait...
1_01:
success
[Global] MyChassis-ch01-01 >
```

Viewing the SSM Port Speed

Description

Use this command in Gaia gClish to make sure that:

- The SSM port speed is configured as defined in the database.
- The SSM QSFP port mode is configured as defined in the database.

Syntax

```
show smo verifiers print name Port_Speed
```

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish
[Global] MyChassis-ch01-01 > show smo verifiers print name Port_Speed
==============================
Port Speed:
==============================

+-------------------------------------------------------------------+
|Port speed verifier                                                |
+---------------+-------------+-------------+-------------+----------+
|Interface      |DB           |Chassis1     |Chassis2     |Result    |
+---------------+-------------+-------------+-------------+----------+
|eth1-01        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-02        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-03        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-04        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-05        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-06        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-07        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-09        |40G          |40G          |40G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-10        |auto         |auto         |auto         |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-11        |auto         |auto         |auto         |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-12        |auto         |auto         |auto         |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-13        |40G          |40G          |40G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-14        |auto         |auto         |auto         |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-15        |auto         |auto         |auto         |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth1-16        |auto         |auto         |auto         |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth2-01        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth2-02        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth2-03        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth2-04        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth2-05        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth2-06        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth2-07        |10G          |10G          |10G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth2-09        |40G          |40G          |40G          |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth2-10        |auto         |auto         |auto         |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth2-11        |auto         |auto         |auto         |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth2-12        |auto         |auto         |auto         |OK        |
+---------------+-------------+-------------+-------------+----------+
|eth2-13        |40G          |40G          |40G          |OK        |
+---------------+-------------+-------------+-------------+----------+
```

```
|eth2-14        |auto          |auto          |auto          |OK         |
+---------------+--------------+--------------+--------------+-----------+
|eth2-15        |auto          |auto          |auto          |OK         |
+---------------+--------------+--------------+--------------+-----------+
|eth2-16        |auto          |auto          |auto          |OK         |
+---------------+--------------+--------------+--------------+-----------+
|SSM1 QSFP mode |40G           |40G           |40G           |OK         |
|---------------+--------------+--------------+--------------+-----------+
|SSM2 QSFP mode |40G           |40G           |40G           |OK         |
+---------------+--------------+--------------+--------------+-----------+
Comparing SSMs configuration with DB...                      [   OK   ]

------------------------------------------------------------------------------
| Tests Status                                                               |
------------------------------------------------------------------------------
| ID | Title               | Result     | Reason                           |
------------------------------------------------------------------------------
| Networking                                                                 |
------------------------------------------------------------------------------
| 39 | Port Speed          | Passed     |                                  |
------------------------------------------------------------------------------
| Tests Summary                                                              |
------------------------------------------------------------------------------
| Passed: 1/1 test                                                           |
| Setting MOTD...                                                            |
| Output file: /var/log/alert_verifier_sum.1-39.2018-12-09_18-55-43.txt      |
[Global] MyChassis-ch01-01 >
```

Configuring the Management Port Speed

Procedure

Step	Instructions
1	Connect to the command line on the SSM.

2	Run these commands in the order they are listed:
	`config`
	`port <Port Name>`
	`speed <Port Speed>`
	`commit`
	`end`

3	Make sure the port speed is correct: `show port <Port Name>`
4	Exit from the command line on the SSM: `exit`

Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><Port Name></td><td>Enter the applicable values:
<table>
<tr><th>Interface Name</th><th>Enter on SSM160</th><th>Enter on SSM440</th></tr>
<tr><td>eth<<i>X</i>>-Mgmt3</td><td>1/5/3</td><td>1/6/1</td></tr>
<tr><td>eth<<i>X</i>>-Mgmt4</td><td>1/5/4</td><td>1/6/2</td></tr>
</table></td></tr>
<tr><td><Port Speed></td><td>Speed in Mbps (megabit per second).
Valid values:
10000 (only on SSM440)
1000
100</td></tr>
</table>

Example for `eth<X>-Mgmt4` on SSM160

```
> T-HUB4# config
Entering configuration mode terminal
---T-HUB4(config)# port 1/5/4
T-HUB4(config-port-1/5/4)# speed 100
T-HUB4(config-port-1/5/4)# commit
Commit complete.
T-HUB4(config-port-1/5/4)# end

T-HUB4# show port 1/5/4

================================================================================
Ethernet Interface
================================================================================
Interface          : 1/5/4
Description        :
Admin State        : up              Port State              : up
Config Duplex      : auto            Operational Duplex      : full
Config Speed       : 100             Operational Speed(Mbps) : 100
--------------------------------------------------------------------------------
Flow Control       : disabled
Dual Port          : No              Active Link        : RJ45
--------------------------------------------------------------------------------
Default VLAN       : 1               MTU[Bytes]         : 1544
MAC Learning       :
LAG ID             : N/A
================================================================================
T-HUB4# exit
```

Chassis Management Modules (CMMs)

In This Section:

Background

The Chassis Management Module (CMM) monitors and controls all hardware components in the Chassis.

The CMM communicates with a dedicated SGM using SNMP.

If a hardware sensor reports a problem, the CMM automatically takes action or sends a report.

CMMs have a Command Line Interface.

For more information, see the *Quantum Scalable Chassis Getting Started Guide* and sk93332.

Connecting to the Active CMM

Method	Instructions
Telnet, or SSH	1. Open a Telnet or SSH session from one of the SGMs. 2. Log in to the Expert mode. 3. Connect to the CMM with this command: `member CMM` 4. Enter `admin` for the user name and password.
Serial port	1. Connect to the serial port on the front panel of the CMM. 2. Open a console window in your terminal emulation program (for example, PuTTY, SecureCRT). Use the default serial connection parameters: 9600, 8, N, 1 3. Enter `admin` for the user name and password.

Connecting to the Standby CMM

Step	Instructions
1	Connect to the command line on the Active CMM (see *"Connecting to the Active CMM" on the previous page*).
2	At the command prompt, run: `ifconfig`
3	Record the IP Address for the USB interface.
4	Open a Telnet or SSH session from the Active CMM to the Standby CMM with the IP address from the table below:

IP address of Active CMM	IP address of Standby CMM
192.168.1.130	192.168.1.131
192.168.1.131	192.168.1.130
192.168.1.2	192.168.1.3
192.168.1.3	192.168.1.2

Collecting the CMM Diagnostic Information (clia fruinfo)

Step	Instructions
1	Connect to the command line on the Active CMM (see *"Connecting to the Active CMM" on the previous page*).
2	Configure your terminal emulation program (for example, PuTTY, SecureCRT) to save the log file for the current session.
3	Get the contents of the `/etc/summary` file: `cat /etc/summary` **Note** - This command can take several minutes to run.
4	Get the contents of the `/tmp/debug.log` file: `cat /tmp/debug.log`

Step	Instructions
5	Get the contents of the `/etc/shmm.cfg` file: `cat /etc/shmm.cfg`

6	Run these commands to collect the hardware information:
	`clia fruinfo 20 0`
	`clia fruinfo 20 1`
	`clia fruinfo 20 2`
	`clia fruinfo 20 3`
	`clia fruinfo 20 4`
	`clia fruinfo 20 5`
	`clia fruinfo 20 6`
	`clia fruinfo 20 7`
	`clia fruinfo 20 8`
	`clia fruinfo 20 9`

Step	Instructions

7	Run these commands to collect the hardware information:
	`clia fruinfo y 10`
	`clia fruinfo y 12`
	`clia fruinfo y 82`
	`clia fruinfo y 84`
	`clia fruinfo y 86`
	`clia fruinfo y 88`
	`clia fruinfo y 8a`
	`clia fruinfo y 8c`
	`clia fruinfo y 8e`
	`clia fruinfo y 90`
	`clia fruinfo y 92`
	`clia fruinfo y 94`
	`clia fruinfo y 96`
	`clia fruinfo y 98`
	`clia fruinfo y 9a`
	`clia fruinfo y 9c`

8	On 61000 N+N chassis model:
	Run these additional commands to collect the hardware information:
	`clia fruinfo 20 10`
	`clia fruinfo 20 11`
	`clia fruinfo 20 12`
	`clia fruinfo 20 13`
	`clia fruinfo 20 14`
	`clia fruinfo 20 15`
	`clia fruinfo 20 16`

9	Get the contents of the `/tmp/debug.log` file again: `cat /tmp/debug.log`

Changing the CMM Administrator Password

Step	Instructions
1	Connect to the command line on the CMM.
2	Log in to the Expert mode.
3	Change the password: `passwd admin`
4	Enter and confirm the new password.

Changing the Chassis Configuration

To change the Chassis configuration, edit this file:

```
/etc/shmm.cfg
```

CMM Commands

Command	Syntax	Description
`clia help`	`clia help`	Shows a list of available commands.
`clia alarm`	`clia alarm [0]`	Shows and resets the current alarms on the CMM.
`clia board`	`clia board`	Confirms the boards are recognized.
`clia fru`	`clia fru <SGM ID>` `clia fru <SSM ID>`	Shows information about an SGM or SSM.
`clia reboot`	`clia reboot`	Reboots the CMM. The Chassis fails over to the Standby CMM.
`clia sel`	`clia sel`	Retrieves event logs.
`clia shelf pd`	`clia shelf pd`	Shows power consumption information for all boards.
`ic2 test`	`ic2_test`	■ Tests the I2C connection ■ Detects all devices connected to the CMM using I2C

Security Switch Modules (SSMs)

In This Section:

The Security Switch Module (SSM):

- Distributes network traffic to the Security Gateway Modules (SGMs)
- Transmits traffic to and from the SGMs
- Shares the load between the SGMs

The SSMs and SGMs communicate automatically through SNMP requests. You can also connect directly to the SSM and run CLI commands.

The SSM contains two modules:

- **Fabric switch** - Includes the data ports
- **Base switch** - Includes the management ports

For more information, see the *Quantum Scalable Chassis Getting Started Guide* and sk93332.

SSM CLI

The SSM communicates with the SGMs through SNMP.

Sometimes, it is necessary to connect directly to the SSM and run CLI commands.

Connecting to the SSM CLI

You can connect to the SSM CLI in one of these ways:

Connection	Description
Through a serial console port on the SSM front panel	Use the default serial connection parameters: 9600, 8, N, 1

From the CLI of one of the SGMs	1. Connect to the command line on the SGM.
	2. Log in to the Expert mode.
	3. Go to the CLI on the applicable SSM:
	`member ssm1`
	`member ssm2`

Important - The default administrator password for the SSM CLI is: `admin`

Available SSM CLI Commands

Command	Description
`show running-config [<Feature Name>]`	Shows the current SSM configuration. **Best Practice** - Because the full configuration is very long, we recommended that you show a configuration only for one specified feature. To see a full list of the available features, enter "`show running-config`" and press the **Tab** key. For example, run the "`show running-config load-balance`" command to see the load balancing configuration.
`show port`	Shows the current status of SSM ports.
`show port <Port ID>`	Shows detailed port information such as speed, administrative state, link state and so on for the specified SSM port.
`show port <Port ID> statistics`	Shows interface statistics for the specified SSM port.
`show version`	Shows the firmware version.

Example

```
# show port 1/3/1 statistics
================================================================================
 Port Statistics
================================================================================
                                                 Input                 Output
--------------------------------------------------------------------------------
Unicast Packets                                   5003                   7106
Multicast Packets                               568409                   1880
Broadcast Packets                               122151                   1972
Flow Control                                         0                      0
Discards                                            16                      0
Errors                                               0                      0
--------------------------------------------------------------------------------
Total                                           695563                  10958
================================================================================

================================================================================
 Ethernet Statistics in Packets
================================================================================
RX CRC Errors                     0         TX Collisions                     0
RX Undersize                      0
--------------------------------------------------------------------------------
                                                 Input                 Output
--------------------------------------------------------------------------------
Fragments                                            0                      0
Oversize                                             0                      0
Jabbers                                              0                      0
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Packets                                                        Input and Output
--------------------------------------------------------------------------------
Octets                                                                71085491
Packets                                                                 706521
Packets of 64 Octets                                                      2290
Packets of 65 to 127 Octets                                             689951
Packets of 128 to 255 Octets                                              4122
Packets of 256 to 511 Octets                                              6009
Packets of 512 to 1023 Octets                                              258
Packets of 1024 to 1518 Octets                                             994
Packets of 1519 or more Octets                                               0
--------------------------------------------------------------------------------
Total                                           695563                  10958
================================================================================

================================================================================
 Rates in Bytes per Second
================================================================================
                                                 Input                 Output
Rate for last 10 sec                              1477                     25
Rate for last 60 sec                              1435                     50
================================================================================
```

Note - In the output of this specific command, pay special intention to the **Discards** and **Errors** fields. If the values in these fields constantly increase, this can indicate a problem.

Viewing the SSM Logs

Step	Instructions
1	Connect to the command line on the SSM. See *"Connecting to the SSM CLI" on page 316*.
2	Enable the private shell: `unhide private` The default password is: `private`
3	Open the private shell: `show private shell`
4	Run: `tail /var/log/messages`

Changing the Load Distribution on SGM Groups

Step	Instructions
1	Connect to the command line on the SSM. See *"Connecting to the SSM CLI" on page 316*.
2	Connect to the configuration terminal: `configure terminal`
3	Configure the load distribution on SGM Groups: `(config)# load-balance mtx-bucket 1 buckets [<SGM ID1><SGM ID2>:<SGM ID3><SGM ID4> ...]` **Important** - You must provide a full list of the SGMs. Otherwise, SSM might drop the traffic.
4	Save the changes: `(config)# commit`
5	Exit the configuration terminal: `(config)# exit`
6	Apply the new load distribution configuration: `load-balance apply`
7	Log out from current session: `logout`

Changing the SSM Administrator Password

Note - You must perform this procedure on each SSM separately. This procedure does not cause any traffic interruption.

Step	Instructions
1	Connect to an SGM over SSH or serial console.
2	Log in to the Expert mode.

3	Go to one of the SSMs:
	`member ssm1`
	`member ssm2`

4	Enter the administrator password. The default administrator password for the SSM CLI is: `admin`
5	Connect to the configuration terminal: `configure terminal`
6	Configure the administrator user: `system security user admin`
7	Configure the password: `password`
8	Enter the new password.
9	Save the changes: `(config)# commit`
10	End the current session: `end`
11	Log out from current session: `logout`

Example

```
[Expert@MyChassis-ch0x-0x:0]# member ssm2
Moving to ssm2
T-ATCA404
admin@ssm2's password: *****
BATM T-ATCA404
admin connected from 198.51.100.204 using ssh on T-ATCA404
--- WARNING ---------------------------------------------------------
Running db may be inconsistent. Enter private configuration mode and
install a saved configuration.
---------------------------------------------------------------------
T-ATCA404#
T-ATCA404# conf t
Entering configuration mode terminal
T-ATCA404 (config)# system security user admin
T-ATCA404 (config-user-admin)# password
(<MD5 digest string>): *****
T-ATCA404 (config-user-admin)# commit
Commit complete.
T-ATCA404 (config-user-admin)# end
T-ATCA404# logout
Connection to ssm2 closed
```

Mapping of SSM Port IDs to SGM Port IDs

Each port ID on the SGM maps to a port on the SSM.

SGM Port Mapped to SSM #1	SGM Port Mapped to SSM #2	SSM160 Port	SSM440 Port
eth1-01	eth2-01	1/3/1	1/1/1
eth1-02	eth2-02	1/3/2	1/1/2
eth1-03	eth2-03	1/3/3	1/1/3
eth1-04	eth2-04	1/3/4	1/1/4
eth1-05	eth2-05	1/3/5	1/1/5
eth1-06	eth2-06	1/3/6	1/1/6
eth1-07	eth2-07	1/3/7	1/1/7
eth1-Sync	eth2-Sync	1/3/8	1/1/8
eth1-09	eth2-09	1/1/1	1/4/1
eth1-10	eth2-10	1/1/2	1/4/2
eth1-11	eth2-11	1/1/3	1/4/3
eth1-12	eth2-12	1/1/4	1/4/4
eth1-13	eth2-13	1/2/1	1/4/5
eth1-14	eth2-14	1/2/2	1/4/6
eth1-15	eth2-15	1/2/3	1/4/7
eth1-16	eth2-16	1/2/4	1/4/8
eth1-17	eth2-17	N/A	1/4/9
eth1-18	eth2-18	N/A	1/4/10
eth1-19	eth2-19	N/A	1/4/11
eth1-20	eth2-20	N/A	1/4/12
eth1-21	eth2-21	N/A	1/4/13

SGM Port Mapped to SSM #1	SGM Port Mapped to SSM #2	SSM160 Port	SSM440 Port
eth1-22	eth2-22	N/A	1/4/14
eth1-23	eth2-23	N/A	1/4/15
eth1-24	eth2-24	N/A	1/4/16
eth1-25	eth2-25	N/A	1/2/1
eth1-26	eth2-26	N/A	1/2/2
eth1-27	eth2-27	N/A	1/2/3
eth1-28	eth2-28	N/A	1/2/4
eth1-29	eth2-29	N/A	1/2/5
eth1-30	eth2-30	N/A	1/2/6
eth1-31	eth2-31	N/A	1/2/7
eth1-32	eth2-32	N/A	1/2/8
eth1-33	eth2-33	N/A	1/3/1
eth1-34	eth2-34	N/A	1/3/2
eth1-35	eth2-35	N/A	1/3/3
eth1-36	eth2-36	N/A	1/3/4
eth1-37	eth2-37	N/A	1/3/5
eth1-38	eth2-38	N/A	1/3/6
eth1-39	eth2-39	N/A	1/3/7
eth1-40	eth2-40	N/A	1/3/8
eth1-Mgmt1	eth2-Mgmt1	1/5/1	N/A
eth1-Mgmt2	eth2-Mgmt2	1/5/2	N/A
eth1-Mgmt3	eth2-Mgmt3	1/5/3	1/6/1
eth1-Mgmt4	eth2-Mgmt4	1/5/4	1/6/2

Checking the Connectivity from the SGMs to the SSMs

Step	Instructions
1	Connect to the command line on an SGM.
2	Log in to the Expert mode.
3	Send ping from SGMs to IP addresses of all the SSMs.
4	Get the firmware version of all SSMs: `asg_chassis_ctrl get_ssm_firmware all`

Adding or Removing SSMs After Initial Setup

Description

If you add or remove SSMs after the initial chassis installation, the chassis can show an incorrect number of installed SSMs or an SSM in the DOWN state.

Use the "`asg_ssm_amount`" command to define the correct number of SSMs in the chassis.

Important:

- When you change the number of SSMs, it is necessary to reboot the chassis. This interrupts the traffic.
- You must run this command if you add or remove SSMs on the Standby Chassis.
- Make sure that only one SGM is turned on when you run this command.
- When you change the number of SSMs from 2 to 1, make sure that the remaining SSM is installed in the SSM Slot 1.

Syntax

```
asg_ssm_amount <Number of SSMs in Standby Chassis>
```

Parameters

Parameter	Description
<Number of SSMs in Standby Chassis>	Total number of SSMs in the Standby Chassis. For more information, see the *Quantum Scalable Chassis Getting Started Guide* > Chapter *Hardware Components*.

Changing the number of SSMs

You can change the number of SSMs with one of these procedures.

Procedure 1 - Requires a long down time

This procedure is for changing the number of SSMs from 1 to 2.

This procedure is simple, but requires a longer down time, because you reboot all SGMs at the same time.

Step	Instructions
1	Make sure all SGMs are in the UP state.
2	Connect to the SMO Security Group Member over a serial console. Using a console connection, in the Expert mode, run on the SMO:
3	Log in to the Expert mode.
4	Set the number of SSMs in the Standby Chassis to two: `asg_ssm_amount 2`
5	Reboot all SGMs: `reboot -b all`
6	Wait for all the SGMs to be in the UP state. **Note** - An additional reboot is expected. The utility prompts you for auto-reboot.
7	Insert the new SSM. Use a console connection to monitor the booting process. **Note** - In a Dual Chassis configuration, make sure to connect the new sync slave.
8	On the SMO Security Group Member, run: `asg_port_speed create_conf`
9	Verify the configuration integrity: `asg diag verify`

Procedure 2 - Requires a minimal down time, but requires to disconnect the Sync and Data ports

This procedure is for changing the number of SSMs from 1 to 2, and from 2 to 1.

This procedure requires a minimal down time, because the Standby Chassis are rebooted one at a time.

However, this procedure requires to disconnect the Sync and Data ports, which causes a traffic outage.

Part 1 - On the Standby Chassis

Step	Operation	Command	Notes
1	Disconnect the cables from the Sync and Data ports on the Standby Chassis.		
2	Physically pull out all the SGMs except the SMO.		
3	Physically install or remove the additional SSMs. **Important** - When you change the number of SSMs from 2 to 1, make sure that the remaining SSM is installed in the SSM Slot 1.		
4	Using a console cable, connect to the remaining SGM (SMO).		

5	Configure the required number of SSMs.	▪ To set the number of SSMs to one:
		`asg_ssm_amount 1`
		▪ To set the number of SSMs to two:
		`asg_ssm_amount 2`	

6	Reboot the remaining SGM (SMO).	`reboot`	

Step	Operation	Command	Notes

7	When the SGM is in the UP state on the Standby Chassis, make sure the configuration matches the configured number of SSMs.	a. Examine the list of active SSMs:
		`ccutil active_ssm`
		Example output:
		`SSM1 ACTIVE`
		`SSM2 ACTIVE`
		`SSM3 ACTIVE`
		`SSM4 ACTIVE`
		b. Examine the chassis status:
		`asg stat -v`
		c. Examine the interfaces:
		`ifconfig`
			For verification, see *"Setting the Chassis ID" on page 106*.
			Make sure the chassis has the `eth3-<XX>` and `eth4-<XX>` ports.

8	Insert all other SGMs.		
9	When the SGMs are in the UP state on the Standby Chassis, disconnect the cables from the Sync and Data ports on the Active Chassis.		This causes a traffic outage.
10	Connect the cables to the Sync and Data ports on the Standby Chassis.		The Standby Chassis is now the Active Chassis and inspects the traffic.

Part 2 - On the former Active Chassis

Step	Operation	Command	Notes
11	Repeat steps 2 - 8 on the former Active Chassis, which is now disconnected.		
12	Connect the cables to the Sync and Data ports on the former Active Chassis.		

13	When the SGM is in the UP state on the former Active Chassis, make sure the configuration matches the configured number of SSMs.	a. Examine the list of active SSMs:
		`ccutil active_ssm`
		Example output:
		`SSM1 ACTIVE`
		`SSM2 ACTIVE`
		`SSM3 ACTIVE`
		`SSM4 ACTIVE`
		b. Examine the chassis status:
		`asg stat -v`
		c. Examine the interfaces:
		`ifconfig`	

Security Gateway Modules (SGMs)

Background

The Security Gateway Modules (SGMs) in the Chassis work together as one, high performance Security Gateway or VSX Gateway. You can add SGMs and it scales the performance of the system. An SGM can be added and removed without losing connections. If an SGM is removed or fails, traffic is distributed to the other active SGMs.

These SGM models are available:

- SGM400
- SGM260
- SGM220

For more information, see the *Quantum Scalable Chassis Getting Started Guide* and sk93332.

Identifying SGMs in the Chassis (asg_detection)

Description

Use this command in the Expert mode to flash the LEDs of an SGM.

Use Case

This lets you identify the specified SGM.

Syntax

```
asg_detection [ -b <SGM IDs> ] [ -t <time> | off ]
```

Parameters

Parameter	Description
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`) The default is the local SGM, on which you run this command.
`-t <Time>`	Specifies for how long (in seconds) the LEDs flash. Default is 60 seconds.
`-t off`	Stops LED flashes if they continue after the time specified with the "`-t <Time>`" parameter.

Slot IDs for SGMs and SSMs

Some commands use SGM IDs and SSM IDs, or Slot IPMB Addresses.

Use these tables to find the correct SGM ID and SSM ID, or Slot IPMB Address.

For additional information, see the *Quantum Scalable Chassis Getting Started Guide* > Chapter *Hardware Components*.

64000 and 61000 Chassis

Physical Slot Number	Slot IPMB Address	SGM Number	SSM Number
1	0x9A	SGM1	
2	0x96	SGM2	
3	0x92	SGM3	
4	0x8E	SGM4	
5	0x8A	SGM5	
6	0x86	SGM6	
7	0x82		SSM1
8	0x84		SSM2
9	0x88	SGM7	
10	0x8C	SGM8	
11	0x90	SGM9	
12	0x94	SGM10	
13	0x98	SGM11	
14	0x9C	SGM12	

44000 Chassis

Physical Slot Number	Slot IPMB Address	SGM Number	SSM Number
1	0x82		SSM1
2	0x84	SGM6 (or SSM2)	SSM2 (or SGM6)

Physical Slot Number	Slot IPMB Address	SGM Number	SSM Number
3	0x86	SGM5	
4	0x88	SGM4	
5	0x8A	SGM3	
6	0x8C	SGM2	
7	0x8E	SGM1	

41000 Chassis

Physical Slot Number	Slot IPMB Address	SGM Number	SSM Number
1	0x82		SSM1
2	0x84		SSM2
3	0x86	SGM4	
4	0x88	SGM3	
5	0x8A	SGM2	
6	0x8C	SGM1	

Troubleshooting

This section provides troubleshooting commands.

Collecting System Information (asg_info)

In This Section:

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 .

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 this file:

```
/var/log/asg_info.<Hostname>.<Date>.tar
```

By default, this command collects the information from all Security Group Members and Virtual Systems (in VSX mode).

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	■ VS0 only (VSX Gateway itself) ■ For each Virtual System ■ 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:

File	How the File is Collected and File Location
`latest_policy.policy.tgz`	■ Collected as a global file ■ Located in `\global\VS0\var\CPbackup\asg_backup\`
`dist_mode.log`	■ Collected from the Security Group Member and Virtual Systems folders ■ Located in `\SGM_1_01\VS1\var\log\`
`start_mbs.log`	■ Collected from the Security Group Member folder and not from the Virtual Systems folders ■ Located in `\SGM_1_01\VS0\var\log\`

Syntax and Parameters

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 <Path to XML Configuration File>] [Options]`

Parameters

Parameter	Description
`-h`	Shows the built-in help.
`-b <SGM IDs>`	Applies to Security Group Members as specified by the `<SGM IDs>`. `<SGM IDs>` can be: ■ No `<SGM IDs>` specified, or `all` Applies to all Security Group Members and all Chassis ■ 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 Chassis, one Chassis (`chassis1`, or `chassis2`) ■ In Dual Chassis, the Active Chassis (`chassis_active`) Default - Runs on all Security Group Members that are in the UP state.
`-vs <VS IDs>`	Applies to Virtual Systems as specified by the `<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 This parameter is only applicable in a VSX environment.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td><Collect Flags></td><td>The collect flags are:
<table>
<tr><th>Flag</th><th>Instructions</th></tr>
<tr><td>--all</td><td>Collects all log files and command outputs.</td></tr>
<tr><td>-a</td><td>Collects archive files.</td></tr>
<tr><td>-c</td><td>Collects information about core dump files.</td></tr>
<tr><td>-f</td><td>Collects comprehensive log files and command outputs.</td></tr>
<tr><td>-i</td><td>Collects the "cpinfo" output.</td></tr>
<tr><td>-m | --cmm</td><td>Collects CMM log files.</td></tr>
<tr><td>-q</td><td>Collects major log files and command outputs.</td></tr>
<tr><td>--user_conf <Path to XML Configuration File></td><td>Collects the specified XML configuration file.
See "Configuration Files" on page 338 below.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Options</td><td>The options are:
<table>
<tr><th>Option</th><th>Instructions</th></tr>
<tr><td>-h</td><td>Shows the built-in help.</td></tr>
<tr><td>-e <Email_1;...;Email_N></td><td>Semicolon separated list of email addresses for upload notifications.</td></tr>
<tr><td>schedule</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 "cplic print" command).
To see and delete the configured periodic jobs, run:
asg_info schedule</td></tr>
<tr><td>-u</td><td>Interactive upload of the "asg_info" output file to the Check Point User Center.</td></tr>
<tr><td>-uk</td><td>Non-interactive upload of the "asg_info" output file to the Check Point User Center.
This option requires a valid CK (see the output of the "cplic print" command).</td></tr>
<tr><td>-v</td><td>Shows verbose output.</td></tr>
<tr><td>--list</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	Instructions
Default	`$FWDIR/conf/asg_info_config.xml` Files and commands are defined automatically.
User defined	You 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 the two files at the same.

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 (drop_monitor)" on page 190*.
		■ 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 230*.
		■ Examine the Security Gateway logs on the Management Server or Log Server

Layer Number	Layer Name	Recommended Diagnostic Commands

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 157*.
		■ For information about the VSX mode, run this command:
		`asg perf -vs all -v --vvxxx`
		See *"Monitoring Performance (asg perf)" on page 157*.

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)" on page 150*. ■ 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 *"Monitoring Traffic (asg_ifconfig)" on page 131*.
		• For information about the routes:
		`asg_route`
		See *"Collecting System Diagnostics (smo verifiers)" on page 230*.
		• For information about the routes:
		`asg_dr_verifier`
		See *"Collecting System Diagnostics (smo verifiers)" on page 230*.
		• 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 *"Monitoring Traffic (asg_ifconfig)" on page 131*.
		• For information about the routes:
		`asg_route`
		See *"Collecting System Diagnostics (smo verifiers)" on page 230*.
		• For information about the routes:
		`show route ...`

2	Data Link	■ 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 345*.

Layer Number	Layer Name	Recommended Diagnostic Commands

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

In This Section:

MAC Verification (mac_verifier)

You can run verifiers to make sure the configuration is correct and consistent.

Description

Each MAC address contains information about the Chassis ID, SGM IDs, 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 Chassis.
-v	Shows information for each interface MAC Address.

Examples

Example 1

```
[Expert@MyChassis-ch0x-0x:0]# 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
-------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

Example 2

```
[Expert@MyChassis-ch0x-0x:0]# 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
------------------------------------------------------------------------------
[Expert@MyChassis-ch0x-0x:0]#
```

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 Virtual Systems in the Bridge Mode.

Notes:

- You must run the "`asg_br_verifier`" command in the context of the specific Virtual System in the Bridge Mode.
- 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 Virtual Systems in the Bridge Mode.

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.

Examples

Example 1 - Output in a normal state

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x:0]#
```

Example 2 - Output in a state of wrong configuration

```
[Expert@MyChassis-ch0x-0x: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-ch0x-0x:0]#
```

Verifying VSX Gateway Configuration (asg vsx_verify)

Important - Use the HCP Tool (see sk171436) instead of this command.

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 the `/config/active` file).

  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 the "`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-R81/fw1/conf/fwha_vsx_conf_id.conf
+b21dfa3feab817c3640bbb984346cdf1  /opt/CPsuite-R81/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

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 Files

Below are the log files on the Chassis:

Feature	Debug File
Alerts	`/var/log/send_alert.*`
Command auditing	`/var/log/asgaudit.log*`
CPD	`$CPDIR/log/cpd.elg`
Distribution	`/var/log/dist_mode.log*`
Dynamic Routing	`/var/log/routed.log`
Expert mode shell auditing	`/var/log/command_logger.log*`
FWD	`$FWDIR/log/fwd.elg`
FWK	`$FWDIR/log/fwk.elg.*`
Gaia Clish auditing	`/var/log/auditlog*`
Gaia First Time Configuration Wizard	`/var/log/ftw_install.log`
General	`/var/log/messages*`
SMO Image Cloning	`/var/log/image_clone.log.dbg*`
Installation	`/var/log/start_mbs.log`
Installation - OS	`/var/log/anaconda.log`
Log Servers	`/var/log/log_servers*`
Policy	`$FWDIR/log/cpha_policy.log.*`
Reboot logs	`/var/log/reboot.log`
SGM Configuration Pull Configuration	`$FWDIR/log/blade_config.*`
VPND	`$FWDIR/log/vpnd.elg*`

Replacing Hardware Components

This chapter provides instructions for replacing hardware components:

- Chassis Management Module (CMM)
- Security Gateway Module (SGM)

Adding or Replacing an SGM

In This Section:

You can perform an operating system upgrade on a new or replacement SGM.

There are two methods to update operating system versions:

- Create a snapshot image from one of the SGMs on the Standby Chassis and revert the new SGM to this snapshot.
- Install from a distribution media (a CD/DVD, or a USB device).

Using Snapshot Image to Add a New or a Replacement SGM

Use snapshot as a backup. Confirm that the latest hotfixes are installed on a new or replacement SGM (or if an SGM is sent for service as an RMA).

Part 1- Required steps on the working SGM

Best Practice - In a Dual Chassis configuration, create a snapshot on one of the SGMs on the Standby Chassis.

Step	Procedure	Instructions	Notes
1	Connect to the command line on the Standby Chassis, over an SSH or console connection.		
2	Log in to the Expert mode.	`gHostName> expert`	
3	Go to one of the SGMs on the Standby Chassis.	`[Expert@MyChassis-ch0X-0X:0]# member <Standby Chassis ID>_<SGM ID>`	Example: `[Expert@MyChassis-ch0x-0x:0]# member 2_3`
4	Disable the global mode.	`gHostName> set global-mode off`	This makes sure that the new snapshot image is created only on this SGM.
5	Create a new snapshot image.	`HostName> add snapshot <Snapshot_Name> desc "<Snapshot Description>"`	Example: `[Global] MyChassis-ch01-01 > add snapshot <Snapshot_Working_SGM> desc "Snapshot of a working SGM #3 on the Standby Chassis"`

Step	Procedure	Instructions	Notes
6	Monitor the progress of the snapshot image creation.	`HostName> show snapshots`	Run this command repeatedly. The process can take 15 - 20 minutes.

Step	Procedure	Instructions	Notes

7	Insert a USB removable disk in the USB port of the SGM, and mount it to the `/mnt/usb` directory.	a. Find the device name for the USB removable disk in one of these ways:
		■ In the `/var/log/messages` file:
		`[Expert@MyChassis-ch0X-0X:0]# tail /var/log/messages`
		Example:
		`:SCSI device sdb: 7827392 512-byte hdwr sectors (4008 MB)`
		`sdb: Write Protect is off`
		`sdb: assuming drive cache: write through`
		`SCSI device sdb: 7827392 512-byte hdwr sectors (4008 MB)`
		`sdb: Write Protect is off`
		`sdb: assuming drive cache: write through`
		`sdb: **sdb1**`
		`sd 9:0:0:0: Attached scsi removable disk sdb`
		`sd 9:0:0:0: Attached scsi generic sg1`
		■ With the "`fdisk -l`" command:
		`[Expert@MyChassis-ch0X-0X:0]# fdisk -l`
		b. Create the `/mnt/usb` directory:
		`[Expert@MyChassis-ch0X-0X:0]# mkdir -p /mnt/usb`
		c. Mount the USB removable disk (for example: `/dev/sdb1`) to your `/mnt/usb` directory:
		`[Expert@MyChassis-ch0X-0X:0]# mount /dev/sdb1 /mnt/usb`	

Step	Procedure	Instructions	Notes
8	When the image creation is complete, export the snapshot image file to a TAR file on the local SGM.	`HostName> set snapshot export <Name of Snapshot Image File Without the .TAR Extension> path /home/admin`	Later, you copy this file to the USB device.
9	Monitor the progress of the snapshot image creation.	`HostName> show snapshots`	Run this command repeatedly. The process can take 15 - 20 minutes.
10	Copy the snapshot file to the USB removable disk.	`[Expert@MyChassis-ch0X-0X:0]# cp -v /home/admin/<Name of Snapshot Image File Without the .TAR Extension>.tar /mnt/usb/`	
11	Check the snapshot image TAR file on the USB removable disk.	`[Expert@MyChassis-ch0X-0X:0]# ls -l /mnt/usb/`	
12	Unmount the USB removable disk from the `/usb/mnt` directory.	`[Expert@MyChassis-ch0X-0X:0]# umount /mnt/usb`	

Step	Procedure	Instructions	Notes
13	Remove the USB removable disk from the SGM.		

Part 2- Required steps on the replacement SGM

Step	Procedure	Instructions	Notes
14	Insert the replacement SGM into a slot that is not part of any Security Group.		If all the slots are used, reconfigure the Security Group to remove one of the SGMs from it: `HostName> delete smo security-group <SGM ID>`
15	Connect to the command line on the replacement SGM.		
16	Disable the global mode.	`gHostName> set global-mode off`	This makes sure that the new snapshot image applies only to this SGM.
17	Connect to the replacement SGM over a console connection.		

Step	Procedure	Instructions	Notes

18	Insert a USB removable disk in the USB port of the replacement SGM, and mount it to the `/mnt/usb` directory.	a. Find the device name for the USB removable disk in one of these ways:
		■ In the `/var/log/messages` file:
		`[Expert@MyChassis-ch0X-0X:0]# tail /var/log/messages`
		Example:
		`:SCSI device sdb: 7827392 512-byte hdwr sectors (4008 MB)`
		`sdb: Write Protect is off`
		`sdb: assuming drive cache: write through`
		`SCSI device sdb: 7827392 512-byte hdwr sectors (4008 MB)`
		`sdb: Write Protect is off`
		`sdb: assuming drive cache: write through`
		`sdb: sdb1`
		`sd 9:0:0:0: Attached scsi removable disk sdb`
		`sd 9:0:0:0: Attached scsi generic sg1`
		■ With the "`fdisk -l`" command:
		`[Expert@MyChassis-ch0X-0X:0]# fdisk -l`
		b. Create the `/mnt/usb` directory:
		`[Expert@MyChassis-ch0X-0X:0]# mkdir -p /mnt/usb`
		c. Mount the USB removable disk (for example: `/dev/sdb1`) to your `/mnt/usb` directory:
		`[Expert@MyChassis-ch0X-0X:0]# mount /dev/sdb1 /mnt/usb`	

19	Copy the snapshot file from the USB removable disk to the replacement SGM.	`[Expert@MyChassis-ch0X-0X:0]# cp -v /mnt/usb/<Name of Snapshot Image>.tar /home/admin/`	

Step	Procedure	Instructions	Notes
20	Import the snapshot image file.	`HostName> set snapshot import <Name of Snapshot Image File Without the .TAR Extension> path /home/admin/`	
21	Monitor the progress of the snapshot image import.	`HostName> show snapshots`	Run this command repeatedly. The process can take 15 - 20 minutes.
22	Unmount the USB removable disk from the `/mnt/usb` directory.	`[Expert@MyChassis-ch0X-0X:0]# umount /mnt/usb`	
23	Remove the USB removable disk from the replacement SGM.		
24	Revert the snapshot image.	`HostName> set snapshot revert <Snapshot_Name>`	Revert can take 15 - 20 minutes. During the revert, the SGM can reboot several times. Proceed to the next step after the revert is complete.

Step	Procedure	Instructions	Notes
25	Connect to the command line on the chassis, over an SSH or console connection.		
26	Log in to the Expert mode.	`gHostName> expert`	
27	Update the Security Group to include the replacement SGM.	`HostName> add smo security-group <SGM ID>`	You can run this command: `HostName> add smo security_group {$NEW_SGM_ID}`
28	Confirm that the replacement SGM is in the UP state and enforces the latest policy.	`[Expert@MyChassis-ch0X-0X:0]# asg monitor`	
29	Confirm that all SGMs on the chassis have the same OS version.	`[Expert@MyChassis-ch0X-0X:0]# asg_version`	

Example

```
[Expert@MyChassis-ch0x-0x:0]# gclish

[Global] MyChassis-ch01-01 > set global-mode off

MyChassis-ch01-01 > add snapshot rma_62 desc rma
Taking snapshot. You can continue working normally.
You can use the command 'show snapshots' to monitor creation progress,

MyChassis-ch01-01 > show snapshots
Restore points:
---------------
armdilo62_2
Restore point now under creation:
riua_62 (19%)

Creation of an additional restore point will need 2.624G
Amount of space available for restore points is il.41G

MyChassis-ch01-01 > show snapshots
Restore points:
----------------
rma_62
armdi 1062_2

Creation of an additional restore point will need 2.624G
Amount of space available for restore points is 41.53G

MyChassis-ch01-01 > set snapshot export rma_62 path /mnt/usb/
Exporting snapshot. You can continue working normally.
You can use the command 'show snapshots' to monitor exporting progress.

MyChassis-ch01-01 > set global-mode on

[Global] MyChassis-ch01-01 > exit

[Expert@MyChassis-ch0x-0x:0]# member 2_3
Moving to blade 2_3
This system is for authorized use only.
Last login: Wed Jun 20 08:43:28 2012 from MyChassis-ch02-03

[Expert@MyChassis-ch0x-0x:0]# cd /mnt/usb

[Expert@MyChassis-ch0x-0x:0]# ls
rzna_62.tar

[Expert@MyChassis-ch0x-0x:0]# umount /uint/usb
```

Installing a New SGM Using a CD/DVD Device

Step	Instructions
1	Burn the required image onto a CD/DVD. See the R81 Home Page: sk169954..
2	Install the new SGM into an unoccupied slot in the Standby Chassis.
3	If necessary, reconfigure the Security Group to include the new SGM.
4	Connect to the new SGM with a console connection.
5	Remove the SGM boot sector: `eraseboot`
6	Connect the CD/DVD device to the SGM.
7	Reboot the SGM: a. Pull it out b. Insert it
8	The installation starts. Follow the instructions in the console connection to the new SGM.

Replacing the CMM

Install the replacement CMM that you received in the Return Merchandise Authorization (RMA).

These steps are for CMM installation on a Standby Chassis in a Dual Chassis environment.

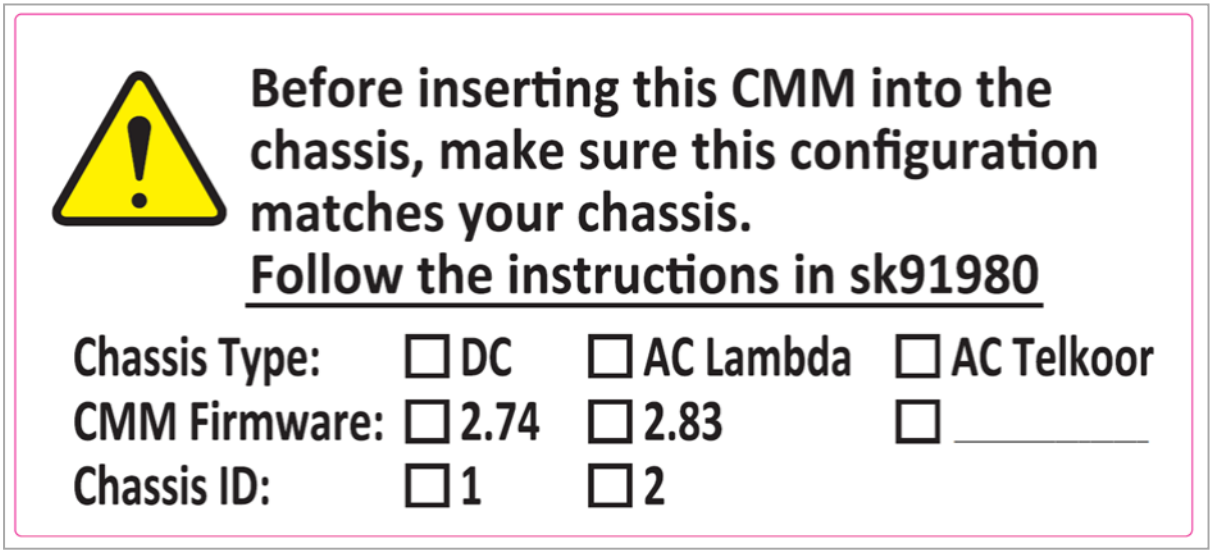
Prerequisites

1. Make sure you have a supported Standby Chassis type.

Standby Chassis Model	Supported Standby Chassis Type
61000	■ DC Standby Chassis ■ AC Telkoor - The AC Standby Chassis has two rows with three Telkoor power supplies in each row ■ AC Lambda - The AC Standby Chassis has one row with five Lambda power supplies
61000 N+N	■ DC Standby Chassis ■ AC Lambda - The AC Standby Chassis has one row with four Lambda power supplies
41000 44000	■ AC Telkoor - Three Telkoor power supplies ■ DC Standby Chassis

2. Get the label from the CMM box.

   Example:



3. Make sure that the Standby Chassis ID on the label on the outside of the CMM packaging box is the same as the label on the Standby Chassis.

   If the Chassis ID is different from the Chassis ID of the RMA CMM, change the RMA CMM Chassis ID. See *"Setting the Chassis ID" on page 106*.

Replacing the CMM

Step	Instructions
1	Install the replacement CMM in the Standby Chassis.

2	Make sure that all CMMs in the environment have the same CMM firmware version:
	`asg_version -i`
	Example:
	`[Expert@MyChassis-ch0x-0x:0]# asg_version -i`
	`+-----------------------------------------------------------------------+`
	`| Hardware Versions |`
	`+-----------------------------------------------------------------------+`
	`| Component | Type | Configuration | Firmware |`
	`+-----------------------------------------------------------------------+`
	`| **Standby Chassis 1** |`
	`+-----------------------------------------------------------------------+`
	`| SSM1 | SSM160 | N/A | 5.5.x |`
	`| SSM2 | SSM160 | N/A | 5.5.x |`
	`| CMM(active) | N/A | N/A | **2.83** |`
	`| CMM(standby) | N/A | N/A | **2.83** |`
	`+-----------------------------------------------------------------------+`
	`+-----------------------------------------------------------------------+`
	`| Hardware Versions |`
	`+-----------------------------------------------------------------------+`
	`| Component | Type | Configuration | Firmware |`
	`+-----------------------------------------------------------------------+`
	`| **Standby Chassis 2** |`
	`+-----------------------------------------------------------------------+`
	`| SSM1 | SSM160 | N/A | 5.5.x |`
	`| SSM2 | SSM160 | N/A | 5.5.x |`
	`| CMM(active) | N/A | N/A | **2.83** |`
	`| CMM(standby) | N/A | N/A | **2.83** |`
	`+-----------------------------------------------------------------------+`
	`[Expert@MyChassis-ch0x-0x:0]#`

The output must be the same as the box label.

- If the CMM firmware versions are **not** the same, upgrade the CMM Firmware.

  See the *R81 Quantum Scalable Chassis Installation and Upgrade Guide* > Chapter *Upgrading Hardware Components*.

- If the Standby Chassis IDs are **not** the same, change the Standby Chassis ID on the RMA CMM.

  See *"Setting the Chassis ID" on page 106*.

- If the Standby Chassis Types are **not** the same, follow the procedure *"Correcting an Incorrect Chassis Type" on the next page*.

Correcting an Incorrect Chassis Type

Step	Instructions
1	Connect to the command line on the Standby Chassis.
2	Log in to Gaia Clish.
3	Go to Gaia gClish: enter `gclish` and press Enter.
4	Change the state of the Standby Chassis to "Down": `set chassis id <Standby Chassis ID> admin-state down`
5	Remove all CMMs from the Standby Chassis.
6	Insert only the replacement CMM in the Standby Chassis.
7	Open a console connection to the CMM: a. Connect one end of a serial cable to the serial port on the CMM front panel. b. Connect the other end of the serial cable to a computer. c. Open a console window in your terminal emulation program (for example, PuTTY, SecureCRT). Use the default serial connection parameters: 9600, 8, N, 1
8	Start the installation: `install.sh`

9	On the 61000 N+N chassis model, select the applicable Standby Chassis type.
	The menu can be different based on the CMM firmware.
	Example of this menu appears for the CMM firmware version 2.74:
	`----------`
	`| Select one of following options. |`
	`| 1: Press 1 for 13U chassis (Telkoor PSU). |`
	`| 2: Press 2 for 14U chassis (Telkoor PSU). |`
	`| 3: Press 3 for 14U chassis (Lambda PSU). |`
	`| Q: Press Q for to skip. |`
	`----------`
	■ If the Standby Chassis type is "AC Telkoor" or "DC Standby Chassis", enter `2`.
	■ If the Standby Chassis type is "AC Lambda", enter `3`.

10	Insert the second CMM.

Step	Instructions

11	On the 41000 and 44000 chassis models:
	When the option to upgrade `EEprom` appears, select option `1`.
	`----------`
	`| EEprom upgrading |`
	`| 1: Press 1 for EEProm upgrading. |`
	`| 2. Press 2 to skip. |`
	`----------`
	Note - On the 60000 chassis models, there is no need to upgrade the EEprom.

12	Change the state of the Standby state to "Up": `set chassis id <Standby Chassis ID> admin-state up`

Deploying a Security Group in Monitor Mode

In This Section:

Introduction to Monitor Mode

You can configure Monitor Mode on one of the Security Group's interfaces.

The Security Group listens to traffic from a Mirror Port (or Span Port) on a connected switch.

Use the Monitor Mode to analyze network traffic without changing the production environment.

The mirror port on a switch duplicates the network traffic and sends it to the Security Group with an interface configured in Monitor Mode to record the activity logs.

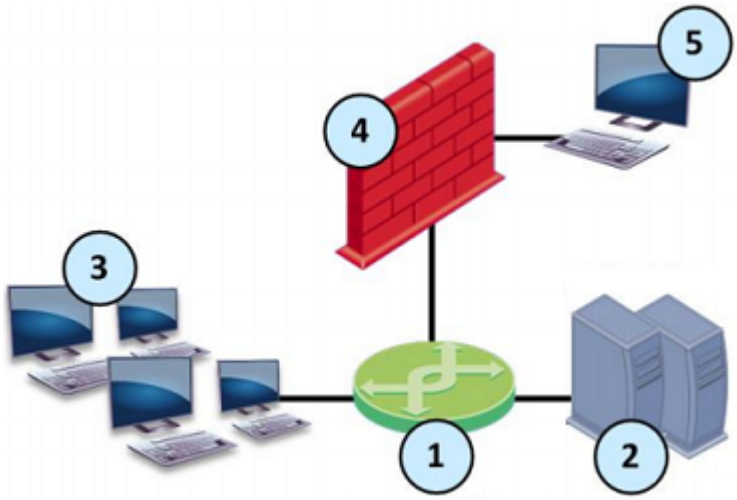
You can use the Monitor Mode:

- To monitor the use of applications as a permanent part of your deployment
- To evaluate the capabilities of the Software Blades:
  - The Security Group neither enforces any security policy, nor performs any active operations (prevent / drop / reject) on the interface in the Monitor Mode.
  - The Security Group terminates and does not forward all packets that arrive at the interface in the Monitor Mode.
  - The Security Group does not send any traffic through the interface in the Monitor Mode.

Benefits of the Monitor Mode include:

- There is no risk to your production environment.
- It requires minimal set-up configuration.
- It does not require TAP equipment, which is expensive.

Example Topology for Monitor Mode



Item	Description
1	Switch with a mirror or SPAN port that duplicates all incoming and outgoing packets. The Security Group connects to a mirror or SPAN port on the switch.
2	Servers.
3	Clients.
4	Security Group with an interface in Monitor Mode.
5	Security Management Server that manages the Security Group.

Supported Software Blades in Monitor Mode

This table lists Software Blades and their support for the Monitor Mode.

Software Blade	Support for the Monitor Mode
Firewall	Fully supports the Monitor Mode.
IPS	These protections and features do **not** work: ■ The **SYN Attack** protection (SYNDefender). ■ The **Initial Sequence Number (ISN) Spoofing** protection. ■ The **Send error page** action in Web Intelligence protections. ■ Client and Server notifications about connection termination.
Application Control	Does **not** support UserCheck.
URL Filtering	Does **not** support UserCheck.
Data Loss Prevention	Does **not** support these: ■ UserCheck. ■ The "**Prevent**" and "**Ask User**" actions - these are automatically demoted to the "**Inform User**" action. ■ FTP inspection.
Identity Awareness	Does **not** support these: ■ Captive Portal. ■ Identity Agent.
Threat Emulation	Does **not** support these: ■ The Emulation Connection Prevent Handling Modes "**Background**" and "**Hold**". See sk106119. ■ FTP inspection.
Content Awareness	Does **not** support the FTP inspection.
Anti-Bot	Fully supports the Monitor Mode.
Anti-Virus	Does **not** support the FTP inspection.
IPsec VPN	Does **not** support the Monitor Mode.
Mobile Access	Does **not** support the Monitor Mode.

Software Blade	Support for the Monitor Mode
Anti-Spam & Email Security	Does **not** support the Monitor Mode.
QoS	Does **not** support the Monitor Mode.

Limitations in Monitor Mode

These features and deployments are **not** supported in Monitor Mode:

- Passing production traffic through a Security Gateway, on which you configured Monitor Mode interface(s).
- If you configure more than one Monitor Mode interface on a Security Gateway, you must make sure the Security Gateway does not receive the same traffic on the different Monitor Mode interfaces.
- HTTPS Inspection
- NAT rules.
- HTTP / HTTPS proxy.
- Anti-Virus in Traditional Mode.
- User Authentication.
- Client Authentication.
- Check Point Active Streaming (CPAS).
- Cluster deployment.
- CloudGuard Gateways.
- CoreXL Dynamic Dispatcher (sk105261).
- Setting the value of the kernel parameters "`psl_tap_enable`" and "`fw_tap_enable`" to 1 (one) on-the-fly with the "`fw ctl set int`" command (Issue ID 02386641).

For more information, see sk101670: Monitor Mode on Gaia OS and SecurePlatform OS.

Configuring a Security Group in Gateway mode in Monitor Mode

Important:

- For Cloud-based services (for example, Social Network widgets and URL Filtering), you must connect the Security Group in Monitor Mode to the Internet.
- You must install valid license and contracts file on the Security Group in Monitor Mode.

Procedure:

1. **Install the environment**

   For more information, see the *Quantum Scalable Chassis Getting Started Guide* and *R81 Quantum Scalable Chassis Installation and Upgrade Guide*.

Step	Instructions
1	Install the Chassis environment.
2	Configure the applicable Security Group and assign the applicable interface(s).
3	If you did not configure the **First Time Wizard settings** when you created a Security Group, you must run the Gaia First Time Configuration Wizard for the Security Group.
4	During the First Time Configuration Wizard, you must configure these settings: ■ In the **Management Connection** window, select the interface, through which you connect to Gaia operating system. ■ In the **Internet Connection** window, do not configure IP addresses. ■ In the **Installation Type** window, select **Security Gateway and/or Security Management**. ■ In the **Products** window: a. In the **Products** section, select **Security Gateway** only. b. In the **Clustering** section, clear **Unit is a part of a cluster, type**. ■ In the **Dynamically Assigned IP** window, select **No**. ■ In the **Secure Internal Communication** window, enter the applicable **Activation Key** (between 4 and 127 characters long).

2. **Configure the Monitor Mode on the applicable interface**

You can configure the Monitor Mode on an interface either in Gaia Portal, or Gaia gClish of the Security Group.

Configuring the Monitor Mode in Gaia Portal

Step	Instructions
1	With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
2	In the left navigation tree, click **Network Management** > **Network Interfaces**.
3	Select the applicable physical interface from the list and click **Edit**.
4	Select the **Enable** option to set the interface status to UP.
5	In the **Comment** field, enter the applicable comment text (up to 100 characters).
6	On the **IPv4** tab, select **Use the following IPv4 address**, but do **not** enter an IPv4 address.
7	On the **IPv6** tab, select **Use the following IPv6 address**, but do **not** enter an IPv6 address. **Important** - This setting is available only after you enable the IPv6 Support in Gaia and reboot.
8	On the **Ethernet** tab: ■ Select **Auto Negotiation**, or select a link speed and duplex setting from the list. ■ In the **Hardware Address** field, enter the Hardware MAC address (if not automatically received from the NIC). **Caution** - Do **not** manually change the MAC address unless you are sure that it is incorrect or has changed. An incorrect MAC address can lead to a communication failure. ■ In the **MTU** field, enter the applicable Maximum Transmission Unit (MTU) value (minimal value is 68, maximal value is 16000, and default value is 1500). ■ Select **Monitor Mode**.
9	Click **OK**.

Configuring the Monitor Mode in Gaia gClish

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to Gaia Clish.
3	Go to Gaia gClish: enter `gclish` and press Enter.
4	Examine the configuration and state of the applicable physical interface: `show interface <Name of Physical Interface>`

5	If the applicable physical interface has an IP address assigned to it, remove that IP address.
	■ To remove an IPv4 address:
	`delete interface <Name of Physical Interface> ipv4-address`
	■ To remove an IPv6 address:
	`delete interface <Name of Physical Interface> ipv6-address`

6	Enable the Monitor Mode on the physical interface: `set interface <Name of Physical Interface> monitor-mode on`
7	Configure other applicable settings on the interface in the Monitor Mode: `set interface <Name of Physical Interface> ...`
8	Examine the configuration and state of the Monitor Mode interface: `show interface <Name of Physical Interface>`
9	Save the configuration: `save config`

3. **Configure the Security Gateway object in SmartConsole**

   You can configure the applicable Security Gateway object in SmartConsole either in Wizard Mode, or in Classic Mode.

Configuring the Security Gateway object in Wizard Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click **Gateways & Servers**.
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✳) > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **Gateway**
4	In the **Check Point Security Gateway Creation** window, click **Wizard Mode**.
5	On the **General Properties** page: a. In the **Gateway name** field, enter the applicable name for this Security Gateway object. b. In the **Gateway platform** field, select the correct model - **41000 Appliances**, **44000 Appliances**, **61000 Appliances**, or **64000 Appliances**. c. In the **Gateway IP address** section, select **Static IP address** and configure the same IPv4 and IPv6 addresses that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses. d. Click **Next**.
6	On the **Trusted Communication** page: a. Select the applicable option: ■ If you selected **Initiate trusted communication now**, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard. ■ If you selected **Skip and initiate trusted communication later**, make sure to follow **Step 7**. b. Click **Next**.

Step	Instructions
7	On the **End** page: a. Examine the **Configuration Summary**. b. Select **Edit Gateway properties for further configuration**. c. Click **Finish**. **Check Point Gateway** properties window opens on the **General Properties** page.
8	If during the Wizard Mode, you selected **Skip and initiate trusted communication later**: a. The **Secure Internal Communication** field shows **Uninitialized**. b. Click **Communication**. c. In the **Platform** field select the correct model - **41000 Appliances**, **44000 Appliances**, **61000 Appliances**, or **64000 Appliances**. d. Enter the same **Activation Key** you entered during the Security Group's First Time Configuration Wizard. e. Click **Initialize**. Make sure the **Certificate state** field shows **Established**. f. Click **OK**.
9	On the **Network Security** tab, make sure to enable only the Firewall Software Blade.
10	On the **Network Management** page: a. Click **Get Interfaces** > **Get Interfaces with Topology**. b. Confirm the interfaces information.
11	Select the interface in the Monitor Mode and click **Edit**. Configure these settings: a. Click the **General** page. b. In the **General** section, enter a *random* IPv4 address. **Important** - This random IPv4 address must not conflict with existing IPv4 addresses on your network. c. In the **Topology** section: Click **Modify**. In the **Leads To** section, select **Not defined (Internal)**. In the **Security Zone** section, select **According to topology: Internal Zone**. Click **OK** to close the **Topology Settings** window. d. Click **OK** to close the **Interface** window.

Step	Instructions
12	Click **OK**.
13	Publish the SmartConsole session.
14	This Security Gateway object is now ready to receive the Security Policy.

Configuring the Security Gateway in Classic Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click **Gateways & Servers**.
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✳) > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **Gateway**
4	In the **Check Point Security Gateway Creation** window, click **Classic Mode**. **Check Point Gateway** properties window opens on the **General Properties** page.
5	In the **Name** field, enter the applicable name for this Security Gateway object.
6	In the **IPv4 address** and **IPv6 address** fields, configure the same IPv4 and IPv6 addresses that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.

Step	Instructions
7	Establish the Secure Internal Communication (SIC) between the Management Server and this Security Group: a. Near the **Secure Internal Communication** field, click **Communication**. b. In the **Platform** field select the correct model - **41000 Appliances**, **44000 Appliances**, **61000 Appliances**, or **64000 Appliances**. c. Enter the same **Activation Key** you entered during the Security Group's First Time Configuration Wizard. d. Click **Initialize**. e. Click **OK**.

	If the **Certificate state** field does not show `Established`, perform these steps:
	a. Connect to the command line on the Security Group.
	b. Make sure there is a physical connectivity between the Security Group and the Management Server (for example, pings can pass).
	c. Run:
	`cpconfig`
	d. Enter the number of this option:
	`Secure Internal Communication`
	e. Follow the instructions on the screen to change the Activation Key.
	f. In SmartConsole, click **Reset**.
	g. Enter the same Activation Key you entered in the `cpconfig` menu.
	h. In SmartConsole, click **Initialize**.

8	In the **Platform** section, select the correct options: a. In the **Hardware** field, select the correct model - **41000 Appliances**, **44000 Appliances**, **61000 Appliances**, or **64000 Appliances**. b. In the **Version** field, select **R81**. c. In the **OS** field, select **Gaia**.

Step	Instructions
9	On the **Network Security** tab, make sure to enable only the Firewall Software Blade. **Important** - Do **not** select anything on the **Management** tab.
10	On the **Network Management** page: a. Click **Get Interfaces** > **Get Interfaces with Topology**. b. Confirm the interfaces information.
11	Select the interface in the Monitor Mode and click **Edit**. Configure these settings: a. Click the **General** page. b. In the **General** section, enter a *random* IPv4 address. **Important** - This random IPv4 address must not conflict with existing IPv4 addresses on your network. c. In the **Topology** section: Click **Modify**. In the **Leads To** section, select **Not defined (Internal)**. In the **Security Zone** section, select **According to topology: Internal Zone**. Click **OK** to close the **Topology Settings** window. d. Click **OK** to close the **Interface** window.
12	Click **OK**.
13	Publish the SmartConsole session.
14	This Security Gateway object is now ready to receive the Security Policy.

4. **Configure the Security Group to process packets that arrive in the wrong order**

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Set the value of the kernel parameter **psl_tap_enable** to 1 in the `$FWDIR/boot/modules/fwkern.conf` file to enable the Passive Streaming Layer (PSL) Tap Mode:: `g_update_conf_file fwkern.conf psl_tap_enable=1`

Step	Instructions
4	Set the value of the kernel parameter **fw_tap_enable** to 1 in the `$FWDIR/boot/modules/fwkern.conf` file to enable the Firewall Tap Mode: `g_update_conf_file fwkern.conf fw_tap_enable=1`
5	Set the value of the kernel parameter **fw_tap_enable** to 1 in the `$PPKDIR/conf/simkern.conf` file to enable the Firewall Tap Mode: `g_update_conf_file $PPKDIR/conf/simkern.conf fw_tap_enable=1`
6	Reboot the Security Group.
7	Connect to the command line on the Security Group.
8	Log in to the Expert mode.

9	Make sure the Security Group loaded the new configuration:
	`g_fw ctl get int psl_tap_enable`
	`g_fw ctl get int fw_tap_enable`

Notes:

- This configuration helps the Security Group process packets that arrive in the wrong or abnormal order (for example, TCP [SYN-ACK] arrives before TCP [SYN]).
- This configuration helps the Security Group work better for the first 10-30 minutes when it processes connections, in which the TCP [SYN] packets did not arrive.
- This configuration is also required when you use a TAP device or Mirror / Span ports with separated TX/RX queues.
- This configuration will make the Mirror Port on Security Group work better for the first 10-30 minutes when processing connections, in which the TCP-SYN packet did not arrive.
- It is not possible to set the value of the kernel parameters "`psl_tap_enable`" and "`fw_tap_enable`" on-the-fly with the "`g_fw ctl set int <parameter>`" command (Known Limitation 02386641).

5. **Configure the required Global Properties for the Security Group in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or *Target* Domain Management Server that manages this Security Group.
2	In the top left corner, click **Menu > Global properties**.
3	From the left tree, click the **Stateful Inspection** pane and configure: a. In the **Default Session Timeouts** section: i. Change the value of the **TCP session timeout** from the default **3600** to **60** seconds. ii. Change the value of the **TCP end timeout** from the default **20** to **5** seconds. b. In the **Out of state packets** section, you must clear all the boxes. Otherwise, the Security Group drops the traffic as out of state (because the traffic does not pass through the Security Group, it does not record the state information for the traffic).
4	From the left tree, click the **Advanced** page > click the **Configure** button, and configure: a. Click **FireWall-1** > **Stateful Inspection**. b. Clear **reject_x11_in_any**. c. Click **OK** to close the **Advanced Configuration** window.
5	Click **OK** to close the **Global Properties** window.
6	Publish the SmartConsole session.

6. **Configure the required Access Control Policy for the Security Group in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.
2	From the left navigation panel, click **Security Policies**.
3	Create a new policy and configure the applicable layers: a. At the top, click the **+** tab (or press **CTRL T**). b. On the **Manage Policies** tab, click **Manage policies and layers**. c. In the **Manage policies and layers** window, create a new policy and configure the applicable layers. d. Click **Close**. e. On the **Manage Policies** tab, click the new policy you created.

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>4</td><td>Create the Access Control rule that accepts all traffic:
<table>
<tr><th>No</th><th>Name</th><th>Source</th><th>Destination</th><th>VPN</th><th>Services & Applications</th><th>Action</th><th>Track</th><th>Install On</th></tr>
<tr><td>1</td><td>Accept All</td><td>*Any</td><td>*Any</td><td>Any</td><td>*Any</td><td>Accept</td><td>Log</td><td>Object of Security Gateway in Monitor Mode</td></tr>
</table></td></tr>
<tr><td>5</td><td>Best Practice
We recommend these Aggressive Aging settings for the most common TCP connections:
a. In the SmartConsole, click Objects menu > Object Explorer.
b. Open Services and select TCP.
c. Search for the most common TCP connections in this network.
d. Double-click the applicable TCP service.
e. From the left tree, click Advanced.
f. At the top, select Override default settings.
On Domain Management Server, select Override global domain settings.
g. Select Match for 'Any'.
h. In the Aggressive aging section:
Select Enable aggressive aging.
Select Specific and enter 60.
i. Click OK.
j. Close the Object Explorer.</td></tr>
<tr><td>6</td><td>Publish the SmartConsole session.</td></tr>
<tr><td>7</td><td>Install the Access Control Policy on the Security Gateway object.</td></tr>
</table>

7. **Make sure the Security Group enabled the Monitor Mode for Software Blades**

Step	Instructions
1	Connect to the command line on the Security Group.

Step	Instructions
2	Log in to the Expert mode.

3	Install the default policy on the VSX Gateway object:
	Make sure the parameter **fw_span_port_mode** is part of the installed policy:
	`grep -A 3 -r fw_span_port_mode $FWDIR/state/local/*`
	The returned output must show:
	`:val (true)`

8. **Connect the Security Group to the switch**

   Connect the interface in the Monitor Mode to the mirror or SPAN port on the switch.

For more information, see the:

- *Quantum Scalable Chassis Getting Started Guide* and *R81 Quantum Scalable Chassis Installation and Upgrade Guide*.
- *R81 Scalable Platforms Gaia Administration Guide*.
- *R81 Security Management Administration Guide*.

Configuring a Security Group in VSX mode in Monitor Mode

Important:

- For Cloud-based services (for example, Social Network widgets and URL Filtering), you must connect the Security Group in Monitor Mode to the Internet (also, see sk79700 and sk106496).
- You must install valid license and contracts file on the Security Group in Monitor Mode.

Procedure:

1. **Install the environment**

   For more information, see the *Quantum Scalable Chassis Getting Started Guide* and *R81 Quantum Scalable Chassis Installation and Upgrade Guide*.

Step	Instructions
1	Install the Chassis environment.
2	Configure the applicable Security Group.
3	If you did not configure the **First Time Wizard settings** when you created a Security Group, you must run the Gaia First Time Configuration Wizard for the Security Group.
4	During the First Time Configuration Wizard, you must configure these settings: ■ In the **Management Connection** window, select the interface, through which you connect to Gaia operating system. ■ In the **Internet Connection** window, do not configure IP addresses. ■ In the **Installation Type** window, select **Security Gateway and/or Security Management**. ■ In the **Products** window: a. In the **Products** section, select **Security Gateway** only. b. In the **Clustering** section, clear **Unit is a part of a cluster, type**. ■ In the **Dynamically Assigned IP** window, select **No**. ■ In the **Secure Internal Communication** window, enter the applicable **Activation Key** (between 4 and 127 characters long).

2. **Configure the Monitor Mode on the applicable interface**

You can configure the Monitor Mode on an interface either in Gaia Portal, or Gaia gClish of the Security Group.

Configuring the Monitor Mode in Gaia Portal

Step	Instructions
1	With a web browser, connect to Gaia Portal at: `https://<IP address of Gaia Management Interface>`
2	In the left navigation tree, click **Network Management** > **Network Interfaces**.
3	Select the applicable physical interface from the list and click **Edit**.
4	Select the **Enable** option to set the interface status to UP.
5	In the **Comment** field, enter the applicable comment text (up to 100 characters).
6	On the **IPv4** tab, select **Use the following IPv4 address**, but do **not** enter an IPv4 address.
7	On the **IPv6** tab, select **Use the following IPv6 address**, but do **not** enter an IPv6 address. **Important** - This setting is available only after you enable the IPv6 Support in Gaia and reboot.
8	On the **Ethernet** tab: ■ Select **Auto Negotiation**, or select a link speed and duplex setting from the list. ■ In the **Hardware Address** field, enter the Hardware MAC address (if not automatically received from the NIC). **Caution** - Do **not** manually change the MAC address unless you are sure that it is incorrect or has changed. An incorrect MAC address can lead to a communication failure. ■ In the **MTU** field, enter the applicable Maximum Transmission Unit (MTU) value (minimal value is 68, maximal value is 16000, and default value is 1500). ■ Select **Monitor Mode**.
9	Click **OK**.

Configuring the Monitor Mode in Gaia gClish

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to Gaia Clish.
3	Go to Gaia gClish: enter `gclish` and press Enter.
4	Examine the configuration and state of the applicable physical interface: `show interface <Name of Physical Interface>`

5	If the applicable physical interface has an IP address assigned to it, remove that IP address.
	■ To remove an IPv4 address:
	`delete interface <Name of Physical Interface> ipv4-address`
	■ To remove an IPv6 address:
	`delete interface <Name of Physical Interface> ipv6-address`

6	Enable the Monitor Mode on the physical interface: `set interface <Name of Physical Interface> monitor-mode on`
7	Configure other applicable settings on the interface in the Monitor Mode: `set interface <Name of Physical Interface> ...`
8	Examine the configuration and state of the Monitor Mode interface: `show interface <Name of Physical Interface>`
9	Save the configuration: `save config`

3. **Configure the Security Group to process packets that arrive in the wrong order**

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Set the value of the kernel parameter **psl_tap_enable** to 1 in the `$FWDIR/boot/modules/fwkern.conf` file to enable the Passive Streaming Layer (PSL) Tap Mode:: `g_update_conf_file fwkern.conf psl_tap_enable=1`
4	Set the value of the kernel parameter **fw_tap_enable** to 1 in the `$FWDIR/boot/modules/fwkern.conf` file to enable the Firewall Tap Mode: `g_update_conf_file fwkern.conf fw_tap_enable=1`
5	Set the value of the kernel parameter **fw_tap_enable** to 1 in the `$PPKDIR/conf/simkern.conf` file to enable the Firewall Tap Mode: `g_update_conf_file $PPKDIR/conf/simkern.conf fw_tap_enable=1`
6	Reboot the Security Group.
7	Connect to the command line on the Security Group.
8	Log in to the Expert mode.

9	Make sure the Security Group loaded the new configuration:
	`g_fw ctl get int psl_tap_enable`
	`g_fw ctl get int fw_tap_enable`

Notes:

- This configuration helps the Security Group process packets that arrive in the wrong or abnormal order (for example, TCP [SYN-ACK] arrives before TCP [SYN]).
- This configuration helps the Security Group work better for the first 10-30 minutes when it processes connections, in which the TCP [SYN] packets did not arrive.
- This configuration is also required when you use a TAP device or Mirror / Span ports with separated TX/RX queues.
- This configuration will make the Mirror Port on Security Group work better for the first 10-30 minutes when processing connections, in which the TCP-SYN packet did not arrive.
- It is not possible to set the value of the kernel parameters "`psl_tap_enable`" and "`fw_tap_enable`" on-the-fly with the "`g_fw ctl set int <parameter>`" command (Known Limitation 02386641).

4. **Configure the VSX Gateway object in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or *Main* Domain Management Server that should manage this VSX Gateway.
2	From the left navigation panel, click **Gateways & Servers**.
3	Create a new VSX Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✶) > **VSX** > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **VSX** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **VSX** > **Gateway** The **VSX Gateway Wizard** opens.
4	On the **VSX Gateway General Properties (Specify the object's basic settings)** page: a. In the **Enter the VSX Gateway Name** field, enter the applicable name for this VSX Gateway object. b. In the **Enter the VSX Gateway IPv4** field, enter the same IPv4 address that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. c. In the **Enter the VSX Gateway IPv6** field, enter the same IPv6 address that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. d. In the **Select the VSX Gateway Version** field, select **R81**. e. Click **Next**.

Step	Instructions
5	On the **VSX Gateway General Properties (Secure Internal Communication)** page: a. In the **Activation Key** field, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard. b. In the **Confirm Activation Key** field, enter the same Activation Key again. c. Click **Initialize**. d. Click **Next**.

	If the **Trust State** field does not show **Trust established**, perform these steps:
	a. Connect to the command line on the Security Group.
	b. Make sure there is a physical connectivity between the Security Group and the Management Server (for example, pings can pass).
	c. Run:
	`cpconfig`
	d. Enter the number of this option:
	`Secure Internal Communication`
	e. Follow the instructions on the screen to change the Activation Key.
	f. In SmartConsole, on the **VSX Gateway General Properties** page, click **Reset**.
	g. Enter the same Activation Key you entered in the `cpconfig` menu.
	h. In SmartConsole, click **Initialize**.

6	On the **VSX Gateway Interfaces (Physical Interfaces Usage)** page: a. Examine the list of the interfaces - it must show all the physical interfaces on the Security Group. b. If you plan to connect more than one Virtual System directly to the same physical interface, you must select **VLAN Trunk** for that physical interface. c. Click **Next**.
7	On the **Virtual Network Device Configuration (Specify the object's basic settings)** page: a. You can select **Create a Virtual Network Device** and configure the first applicable Virtual Device at this time (we recommend to do this later) - Virtual Switch or Virtual Router. b. Click **Next**.

Step	Instructions
8	On the **VSX Gateway Management (Specify the management access rules)** page: a. Examine the default access rules. b. Select the applicable default access rules. c. Configure the applicable source objects, if needed. d. Click **Next**. **Important** - These access rules apply only to the VSX Gateway (context of VS0), which is not intended to pass any "production" traffic.
9	On the **VSX Gateway Creation Finalization** page: a. Click **Finish** and wait for the operation to finish. b. Click **View Report** for more information. c. Click **Close**.
10	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`
11	Install the default policy on the VSX Gateway object: a. Click **Install Policy**. b. In the **Policy** field, select the default policy for this VSX Gateway object. This policy is called: `<Name of VSX Gateway object>_VSX` c. Click **Install**.
12	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`

5. **Configure the Virtual System object (and other Virtual Devices) in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server, or each *Target* Domain Management Server that should manage each Virtual Device.
2	Configure the applicable Virtual System (and other Virtual Devices) on this VSX Gateway. When you configure this Virtual System, for the Monitor Mode interface, add a regular interface. In the **IPv4 Configuration** section, enter a *random* IPv4 address. **Important** - This random IPv4 address must not conflict with existing IPv4 addresses on your network.
3	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`
4	Disable the Anti-Spoofing on the interface that is configured in the Monitor Mode: a. In SmartConsole, open the Virtual System object. b. Click the **Topology** page. c. Select the Monitor Mode interface and click **Edit**. The **Interface Properties** window opens. d. Click the **General** tab. e. In the **Security Zone** field, select **None**. f. Click the **Topology** tab. g. In the **Topology** section, make sure the settings are **Internal (leads to the local network)** and **Not Defined**. h. In the **Anti-Spoofing** section, clear **Perform Anti-Spoofing based on interface topology**. i. Click **OK** to close the **Interface Properties** window. j. Click **OK** to close the **Virtual System Properties** window. k. The Management Server pushes the VSX Configuration.

6. **Configure the required Global Properties for the Virtual System in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or *Target*Domain Management Server that manages this Virtual System.

Step	Instructions
2	In the top left corner, click **Menu > Global properties**.
3	From the left tree, click the **Stateful Inspection** pane and configure: a. In the **Default Session Timeouts** section: i. Change the value of the **TCP session timeout** from the default **3600** to **60** seconds. ii. Change the value of the **TCP end timeout** from the default **20** to **5** seconds. b. In the **Out of state packets** section, you must clear all the boxes. Otherwise, the Security Group drops the traffic as out of state (because the traffic does not pass through the Security Group, it does not record the state information for the traffic).
4	From the left tree, click the **Advanced** page > click the **Configure** button, and configure: a. Click **FireWall-1** > **Stateful Inspection**. b. Clear **reject_x11_in_any**. c. Click **OK** to close the **Advanced Configuration** window.
5	Click **OK** to close the **Global Properties** window.
6	Publish the SmartConsole session.

7. **Configure the required Access Control Policy for the Virtual System in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or *Target* Domain Management Server that manages this Virtual System.
2	From the left navigation panel, click **Security Policies**.
3	Create a new policy and configure the applicable layers: a. At the top, click the **+** tab (or press **CTRL T**). b. On the **Manage Policies** tab, click **Manage policies and layers**. c. In the **Manage policies and layers** window, create a new policy and configure the applicable layers. d. Click **Close**. e. On the **Manage Policies** tab, click the new policy you created.

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>4</td><td>Create the Access Control rule that accepts all traffic:
<table>
<tr><th>No</th><th>Name</th><th>Source</th><th>Destination</th><th>VPN</th><th>Services & Applications</th><th>Action</th><th>Track</th><th>Install On</th></tr>
<tr><td>1</td><td>Accept All</td><td>*Any</td><td>*Any</td><td>Any</td><td>*Any</td><td>Accept</td><td>Log</td><td>Object of Security Gateway in Monitor Mode</td></tr>
</table></td></tr>
<tr><td>5</td><td>Best Practice
We recommend these Aggressive Aging settings for the most common TCP connections:
a. In the SmartConsole, click Objects menu > Object Explorer.
b. Open Services and select TCP.
c. Search for the most common TCP connections in this network.
d. Double-click the applicable TCP service.
e. From the left tree, click Advanced.
f. At the top, select Override default settings.
On Domain Management Server, select Override global domain settings.
g. Select Match for 'Any'.
h. In the Aggressive aging section:
Select Enable aggressive aging.
Select Specific and enter 60.
i. Click OK.
j. Close the Object Explorer.</td></tr>
<tr><td>6</td><td>Publish the SmartConsole session.</td></tr>
<tr><td>7</td><td>Install the Access Control Policy on the Virtual System object.
a. Click Install Policy.
b. In the Policy field, select the applicable policy for this Virtual System object.
c. Click Install</td></tr>
</table>

Step	Instructions
8	Examine the VSX configuration: a. Connect to the command line on the Security Group. b. Log in to the Expert mode. c. Run: `vsx stat -v`

8. **Make sure the Security Group enabled the Monitor Mode for Software Blades**

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.

3	Install the default policy on the VSX Gateway object:
	Make sure the parameter **fw_span_port_mode** is part of the installed policy:
	`grep -A 3 -r fw_span_port_mode $FWDIR/state/local/*`
	The returned output must show:
	`:val (true)`

9. **Connect the Security Group to the switch**

   Connect the interface in the Monitor Mode to the mirror or SPAN port on the switch.

For more information, see the:

- *Quantum Scalable Chassis Getting Started Guide* and *R81 Quantum Scalable Chassis Installation and Upgrade Guide*.
- *R81 Scalable Platforms Gaia Administration Guide*.
- *R81 Scalable Platforms VSX Administration Guide*.
- *R81 Security Management Administration Guide*.

Configuring Specific Software Blades for Monitor Mode

This section shows how to configure specific Software Blades for Monitor Mode.

Note - For VSX, see:

- sk79700: VSX supported features on R75.40VS and above
- sk106496: Software Blades updates on VSX R75.40VS and above - FAQ

Configuring the Threat Prevention Software Blades for Monitor Mode

Configure the settings below, if you enabled one of the Threat Prevention Software Blades (IPS, Anti-Bot, Anti-Virus, Threat Emulation or Threat Extraction) on the Security Group in Monitor Mode:

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>1</td><td>Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.</td></tr>
<tr><td>2</td><td>From the left navigation panel, click Security Policies > Threat Prevention.</td></tr>
<tr><td>3</td><td>Create the Threat Prevention rule that accepts all traffic:
<table>
<tr><th>Protected Scope</th><th>Protection/Site/File/Blade</th><th>Action</th><th>Track</th></tr>
<tr><td>*Any</td><td>-- N/A</td><td>Applicable Threat Prevention Profile</td><td>Log
Packet Capture</td></tr>
</table>
Notes:

We recommend the Optimized profile.
The Track setting Packet Capture is optional.
</td></tr>
<tr><td>4</td><td>Right-click the selected Threat Prevention profile and click Edit.</td></tr>
<tr><td>5</td><td>From the left tree, click the General Policy page and configure:
<ol type="a">
In the Blades Activation section, select the applicable Software Blades.
In the Activation Mode section:

In the High Confidence field, select Detect.
In the Medium Confidence field, select Detect.
In the Low Confidence field, select Detect.

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

Step	Instructions
6	From the left tree, click the **Anti-Virus** page and configure: a. In the **Protected Scope** section, select **Inspect incoming and outgoing files**. b. In the **File Types** section: ■ Select **Process all file types**. ■ **Optional:** Select **Enable deep inspection scanning (impacts performance)**. c. **Optional:** In the **Archives** section, select **Enable Archive scanning (impacts performance)**.
7	From the left tree, click the **Threat Emulation** page > click **General** and configure: ■ In the **Protected Scope** section, select **Inspect incoming files from the following interfaces** and from the menu, select **All**.
8	Configure other applicable settings for the Software Blades.
9	Click **OK**.
10	Install the Threat Prevention Policy on the Security Gateway object.

For more information:

See the *R81 Threat Prevention Administration Guide*.

Configuring the Application Control and URL Filtering Software Blades for Monitor Mode

Configure the settings below, if you enabled Application Control or URL Filtering Software Blade on the Security Group in Monitor Mode:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.
2	From the left navigation panel, click **Manage & Settings > Blades**.
3	In the **Application Control & URL Filtering** section, click **Advanced Settings**. The **Application Control & URL Filtering Settings** window opens.
4	On the **General** page: ■ In the **Fail mode** section, select **Allow all requests (fail-open)**. ■ In the **URL Filtering** section, select **Categorize HTTPS websites**.
5	On the **Check Point online web service** page: ■ In the **Website categorization mode** section, select **Background**. ■ Select **Categorize social networking** widgets.
6	Click **OK** to close the **Application Control & URL Filtering Settings** window.
7	Install the Access Control Policy on the Security Gateway object.

For more information:

See the *R81 Security Management Administration Guide*.

Configuring the Data Loss Prevention Software Blade for Monitor Mode

Configure the settings below, if you enabled the Data Loss Prevention Software Blade on the Security Group in Monitor Mode:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.
2	From the left navigation panel, click **Manage & Settings > Blades**.
3	In the **Data Loss Prevention** section, click **Configure in SmartDashboard**. The SmartDashboard window opens.
4	In SmartDashboard: a. Click the **My Organization** page. b. In the **Email Addresses or Domains** section, configure with full list of company's domains. There is no need to include subdomains (for example, `mydomain.com`, `mydomain.uk`). c. In the **Networks** section, select **Anything behind the internal interfaces of my DLP gateways**. d. In the **Users** section, select **All users**.
5	Click the **Policy** page. Configure the applicable rules: ■ In the **Data** column, right-click the pre-defined data types and select **Edit**. • On the **General Properties** page, in the **Flag** field, select **Improve Accuracy**. • In the **Customer Names** data type, we recommend to add the company's real customer names. ■ In the **Action** column, you must select **Detect**. ■ In the **Severity** column, select **Critical** or **High** in all applicable rules. ■ You may choose to disable or delete rules that are not applicable to the company or reduce the Severity of these rules. **Note** - Before you can configure the DLP rules, you must configure the applicable objects in SmartConsole.

Step	Instructions
6	Click the **Additional Settings > Protocols** page. Configure these settings: ■ In the **Email** section, select **SMTP (Outgoing Emails)**. ■ In the **Web** section, select **HTTP**. Do **not** configure the **HTTPS**. ■ In the **File Transfer** section, do **not** select **FTP**.
7	Click **Launch Menu > File > Update** (or press the **CTRL S** keys).
8	Close the SmartDashboard.
9	Install the Access Control Policy on the Security Gateway object.

10	Make sure the Security Group enabled the SMTP Mirror Port Mode:
	a. Connect to the command line on the Security Group.
	b. Log in to the Expert mode.
	c. Run this command:
	`dlp_smtp_mirror_port status`
	d. Make sure the value of the kernel parameter `dlp_force_smtp_kernel_inspection` is set to 1 (one).
	Run these two commands:
	`g_fw ctl get int dlp_force_smtp_kernel_inspection`
	`g_all grep dlp_force_smtp_kernel_inspection $FWDIR/boot/modules/fwkern.conf`

For more information:

See the *R81 Data Loss Prevention Administration Guide*.

Configuring the Security Group in Monitor Mode Behind a Proxy Server

If you connect a Proxy Server between the Security Group in Monitor Mode and the switch, then configure these settings to see Source IP addresses and Source Users in the Security Gateway logs:

Step	Instructions
1	On the Proxy Server, configure the "**X Forward-For header**". See the applicable documentation for your Proxy Server.
2	On the Security Group in Monitor Mode, enable the stripping of the X-Forward-For (XFF) field. Follow the sk100223: How to enable stripping of X-Forward-For (XFF) field.

Deploying a Security Group in Bridge Mode

In This Section:

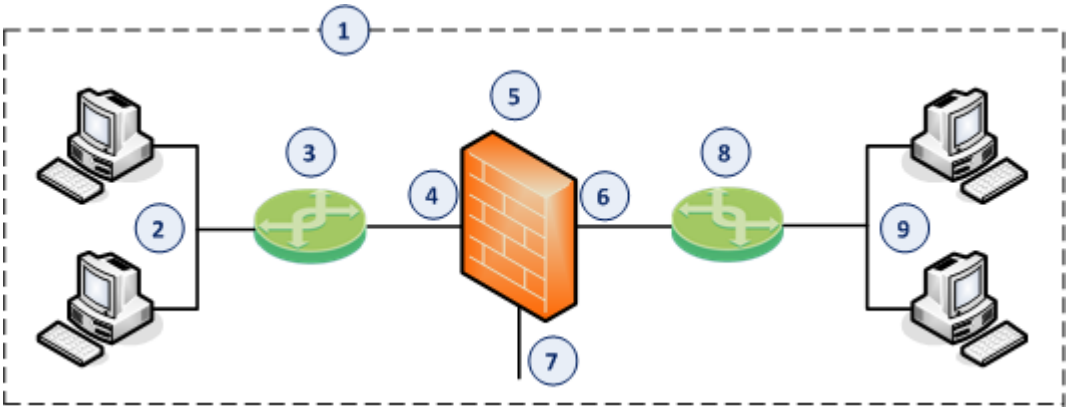
Introduction to Bridge Mode

If it is not possible divide the existing network into several networks with different IP addresses, you can configure a Security Group in the Bridge Mode.

A Security Group in Bridge Mode is invisible to Layer 3 traffic.

When traffic arrives at one of the bridge slave interfaces, the Security Group inspects it and passes it to the second bridge slave interface.

Example Topology for Bridge Mode



Item	Description
1	Network, which an administrator needs to divide into two Layer 2 segments. The Security Group in Bridge Mode connects between these segments.
2	First network segment.
3	Switch that connects the first network segment to one bridged slave interface **(4)** on the Security Group in Bridge Mode.
4	One bridged slave interface (for example, `eth1-05`) on the Security Group in Bridge Mode.
5	Security Group in Bridge Mode.
6	Another bridged slave interface (for example, `eth1-07`) on the Security Group in Bridge Mode.
7	Dedicated Gaia Management Interface (for example, `eth1-Mgmt1`) on the Security Group.
8	Switch that connects the second network segment to the other bridged slave interface **(6)** on the Security Group in Bridge Mode.
9	Second network segment.

Supported Software Blades in Monitor Mode

This table lists Software Blades, features, and their support for the Bridge Mode.

Software Blade or Feature	Support of a Security Gateway in Bridge Mode	Support of VSX Virtual Systems in Bridge Mode
Firewall	Yes	Yes
IPsec VPN	*No*	*No*
IPS	Yes	Yes
URL Filtering	Yes	Yes
DLP	Yes	No
Anti-Bot	Yes	Yes
Anti-Virus	Yes (1)	Yes (1)
Application Control	Yes	Yes
HTTPS Inspection	Yes (2)	*No*
Identity Awareness	Yes (3)	*No*
Threat Emulation - ThreatCloud emulation	Yes	Yes in Active/Active Bridge Mode *No* in Active/Standby Bridge Mode
Threat Emulation - Local emulation	Yes	*No* in all Bridge Modes

Software Blade or Feature	Support of a Security Gateway in Bridge Mode	Support of VSX Virtual Systems in Bridge Mode
Threat Emulation - Remote emulation	Yes	Yes in Active/Active Bridge Mode *No* in Active/Standby Bridge Mode
Mobile Access	*No*	*No*
UserCheck	Yes	*No*
Multi-Portal (Mobile Access Portal, Identity Awareness Captive Portal, Data Loss Prevention Portal, and so on)	Yes	*No*
QoS	Yes (see sk89581)	*No* (see sk79700)
HTTP / HTTPS proxy	Yes	*No*
Security Servers - SMTP, HTTP, FTP, POP3	Yes	*No*
Client Authentication	Yes	*No*
User Authentication	Yes	*No*

Notes:

1. Does not support the Anti-Virus in Traditional Mode.
2. HTTPS Inspection in Layer 2 works as Man-in-the-Middle, based on MAC addresses:
   - Client sends a TCP [SYN] packet to the MAC address X.
   - Security Gateway creates a TCP [SYN-ACK] packet and sends it to the MAC address X.
   - Security Gateway in Bridge Mode does not need IP addresses, because CPAS takes the routing and the MAC address from the original packet.

   Note - To be able to perform certificate validation (CRL/OCSP download), Security Gateway needs at least one interface to be assigned with an IP address. Probe bypass can have issues with Bridge Mode. Therefore, we do not recommend Probe bypass in Bridge Mode configuration.
3. Identity Awareness in Bridge Mode supports only the AD Query authentication.

Limitations in Bridge Mode

You can configure only **two** slave interfaces in one Bridge interface. You can think of this Bridge interface as a two-port Layer 2 switch. Each port can be a Physical interface, a VLAN interface, or a Bond interface.

These features and deployments are **not** supported in Bridge Mode:

- NAT rules (specifically, Firewall kernel in logs shows the traffic as accepted, but Security Gateway does not actually forward it). For more information, see sk106146.
- Access to Multi-Portal (Mobile Access Portal, Identity Awareness Captive Portal, Data Loss Prevention Portal, and so on) from bridged networks, if the bridge does not have an assigned IP address.

For more information, see sk101371: Bridge Mode on Gaia OS and SecurePlatform OS.

Configuring a Security Group in Bridge Mode

Procedure:

1. **Install the environment**

   For more information, see the *Quantum Scalable Chassis Getting Started Guide* and *R81 Quantum Scalable Chassis Installation and Upgrade Guide*.

Step	Instructions
1	Install the Chassis environment.
2	Configure the applicable Security Group and assign the applicable interfaces.
3	Run the Gaia First Time Configuration Wizard for the Security Group.
4	During the First Time Configuration Wizard, you must configure these settings: ■ In the **Management Connection** window, select the interface, through which you connect to Gaia operating system. ■ In the **Internet Connection** window, do not configure IP addresses. ■ In the **Installation Type** window, select **Security Gateway and/or Security Management**. ■ In the **Products** window: a. In the **Products** section, select **Security Gateway** only. b. In the **Clustering** section, clear **Unit is a part of a cluster, type**. ■ In the **Dynamically Assigned IP** window, select **No**. ■ In the **Secure Internal Communication** window, enter the applicable **Activation Key** (between 4 and 127 characters long).

2. **Configure the Bridge interface on the Security Group**

   You configure the Bridge interface in either in Gaia Portal, or Gaia gClish of the Security Group.

   Configuring the Bridge interface in Gaia Portal

   Note - You must connect to the Gaia Portal of the applicable Security Group.

Step	Instructions
1	In the navigation tree, click **Network Management** > **Network Interfaces**.
2	Make sure that the slave interfaces, which you wish to add to the Bridge interface, do not have IP addresses.
3	Click **Add** > **Bridge**. To configure an existing Bridge interface, select the Bridge interface and click **Edit**.
4	On the **Bridge** tab, enter or select a **Bridge Group** ID (unique integer between 1 and 1024).
5	Select the interfaces from the **Available Interfaces** list and then click **Add**. **Notes:** ■ Make sure that the slave interfaces do not have any IP addresses or aliases configured. ■ Do **not** select the interface that you configured as Gaia Management Interface. ■ A Bridge interface in Gaia can contain only two slave interfaces.
6	On the **IPv4** tab, enter the IPv4 address and subnet mask. **Important** - R81 does **not** support the option **Obtain IPv4 address automatically** (Known Limitation MBS-3246).
7	**Optional:** On the **IPv6** tab, enter the IPv6 address and mask length. **Important:** ■ First, you must enable the IPv6 Support and reboot . ■ R81 does **not** support IPv6 Address on Gaia Management Interface (Known Limitation 01622840). ■ R81 does **not** support the option **Obtain IPv6 address automatically** (Known Limitation MBS-3246).
8	Click **OK**.

Configuring the Bridge interface in Gaia gClish

Step	Instructions
1	Connect to the command line on the applicable Security Group.

Step	Instructions
2	Log in to Gaia Clish. Go to Gaia gClish: enter `gclish` and press Enter.

3	Make sure that the slave interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned:
	`show interface <Name of Slave Interface> ipv4-address`
	`show interface <Name of Slave Interface> ipv6-address`

4	Add a new bridging group: `add bridging group <Bridge Group ID 0 - 1024>` **Note** - Do **not** change the state of bond interface manually using the "`set interface <Bridge Group ID> state`" command. This is done automatically by the bridging driver.

5	Add slave interfaces to the new bridging group:
	`add bridging group <Bridge Group ID> interface <Name of First Slave Interface>`
	`add bridging group <Bridge Group ID> interface <Name of Second Slave Interface>`
	Notes:
	■ Do **not** select the interface that you configured as Gaia Management Interface.
	■ Only Ethernet, VLAN, and Bond interfaces can be added to a bridge group.
	■ A Bridge interface in Gaia can contain only two slave interfaces.

Step	Instructions

6	Assign an IP address to the bridging group.
	Note - You configure an IP address on a Bridging Group in the same way as you do on a physical interface .
	■ To assign an IPv4 address, run:
	`set interface <Name of Bridging Group> ipv4-address <IPv4 Address> {subnet-mask <Mask> | mask-length <Mask Length>}`
	You can optionally configure the bridging group to obtain an IPv4 Address automatically.
	■ To assign an IPv6 address, run:
	`set interface <Name of Bridging Group> ipv6-address <IPv6 Address> mask-length <Mask Length>`
	You can optionally configure the bridging group to obtain an IPv6 Address automatically.
	Important - First, you must enable the IPv6 Support and reboot .

7	Save the configuration: `save config`

3. **Configure the Security Gateway object in SmartConsole**

   You can configure the Security Gateway object in either Wizard Mode, or Classic Mode.

   Configuring the Security Gateway object in Wizard Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click **Gateways & Servers**.
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✳) > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **Gateway**

Step	Instructions
4	In the **Check Point Security Gateway Creation** window, click **Wizard Mode**.
5	On the **General Properties** page: a. In the **Gateway name** field, enter the applicable name for this Security Gateway object. b. In the **Gateway platform** field, select the correct model - **41000 Appliances**, **44000 Appliances**, **61000 Appliances**, or **64000 Appliances**. c. In the **Gateway IP address** section, select **Static IP address** and configure the same IPv4 and IPv6 addresses that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses. d. Click **Next**.
6	On the **Trusted Communication** page: a. Select the applicable option: ▪ If you selected **Initiate trusted communication now**, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard. ▪ If you selected **Skip and initiate trusted communication later**, make sure to follow **Step 7**. b. Click **Next**.
7	On the **End** page: a. Examine the **Configuration Summary**. b. Select **Edit Gateway properties for further configuration**. c. Click **Finish**. **Check Point Gateway** properties window opens on the **General Properties** page.

Step	Instructions
8	If during the Wizard Mode, you selected **Skip and initiate trusted communication later**: a. The **Secure Internal Communication** field shows **Uninitialized**. b. Click **Communication**. c. In the **Platform** field select the correct model - **41000 Appliances**, **44000 Appliances**, **61000 Appliances**, or **64000 Appliances**. d. Enter the same **Activation Key** you entered during the Security Group's First Time Configuration Wizard. e. Click **Initialize**. Make sure the **Certificate state** field shows **Established**. f. Click **OK**.
9	On the **General Properties** page, on the **Network Security** tab, enable the applicable Software Blades. **Important** - See the *Supported Software Blades in Bridge Mode* and *Limitations in Bridge Mode* sections in *"Deploying a Security Group in Bridge Mode" on page 401*.
10	On the **Network Management** page, configure the **Topology** of the Bridge interface. **Notes:** ■ If a Bridge interface connects to the Internet, then set the **Topology** to **External**. ■ If you use this Bridge Security Gateway object in Access Control Policy rules with **Internet** objects, then set the **Topology** to **External**.
11	Click **OK**.
12	Publish the SmartConsole session.
13	This Security Gateway object is now ready to receive the Security Policy.

Configuring the Security Gateway object in Classic Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click **Gateways & Servers**.

Step	Instructions
3	Create a new Security Gateway object in one of these ways: ■ From the top toolbar, click the **New** (✳) > **Gateway**. ■ In the top left corner, click **Objects** menu > **More object types** > **Network Object** > **Gateways and Servers** > **New Gateway**. ■ In the top right corner, click **Objects Pane** > **New** > **More** > **Network Object** > **Gateways and Servers** > **Gateway**
4	In the **Check Point Security Gateway Creation** window, click **Classic Mode**. **Check Point Gateway** properties window opens on the **General Properties** page.
5	In the **Name** field, enter the applicable name for this Security Gateway object.
6	In the **IPv4 address** and **IPv6 address** fields, configure the same IPv4 and IPv6 addresses that you configured on the **Management Connection** page of the Security Group's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.
7	Establish the Secure Internal Communication (SIC) between the Management Server and this Security Group: a. Near the **Secure Internal Communication** field, click **Communication**. b. In the **Platform** field select the correct model - **41000 Appliances**, **44000 Appliances**, **61000 Appliances**, or **64000 Appliances**. c. Enter the same **Activation Key** you entered during the Security Group's First Time Configuration Wizard. d. Click **Initialize**. e. Click **OK**.

Step	Instructions

	If the **Certificate state** field does not show `Established`, perform these steps:
	a. Connect to the command line on the Security Group.
	b. Make sure there is a physical connectivity between the Security Group and the Management Server (for example, pings can pass).
	c. Run:
	`cpconfig`
	d. Enter the number of this option:
	`Secure Internal Communication`
	e. Follow the instructions on the screen to change the Activation Key.
	f. In SmartConsole, click **Reset**.
	g. Enter the same Activation Key you entered in the `cpconfig` menu.
	h. In SmartConsole, click **Initialize**.

8	In the **Platform** section, select the correct options: a. In the **Hardware** field, select the correct model - **41000 Appliances**, **44000 Appliances**, **61000 Appliances**, or **64000 Appliances**. b. In the **Version** field, select **R81**. c. In the **OS** field, select **Gaia**.
9	On the **General Properties** page, on the **Network Security** tab, enable the applicable Software Blades. **Important** - See the *Supported Software Blades in Bridge Mode* and *Limitations in Bridge Mode* sections in *"Deploying a Security Group in Bridge Mode" on page 401*.
10	On the **Network Management** page, configure the **Topology** of the Bridge interface. **Notes:** ■ If a Bridge interface connects to the Internet, then set the **Topology** to **External**. ■ If you use this Bridge Security Gateway object in Access Control Policy rules with **Internet** objects, then set the **Topology** to **External**.

Step	Instructions
11	Click **OK**.
12	Publish the SmartConsole session.
13	This Security Gateway object is now ready to receive the Security Policy.

4. **Configure the applicable Security Policies for the Security Gateway in SmartConsole**

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.
2	From the left navigation panel, click **Security Policies**.
3	Create a new policy and configure the applicable layers: a. At the top, click the **+** tab (or press **CTRL T**). b. On the **Manage Policies** tab, click **Manage policies and layers**. c. In the **Manage policies and layers** window, create a new policy and configure the applicable layers. d. Click **Close**. e. On the **Manage Policies** tab, click the new policy you created.
4	Create the applicable rules in the Access Control and Threat Prevention policies. **Important** - See the *Supported Software Blades in Bridge Mode* and *Limitations in Bridge Mode* sections in *"Deploying a Security Group in Bridge Mode" on page 401*.
5	Install the Access Control Policy on the Security Gateway object.
5	Install the Threat Prevention Policy on the Security Gateway object.

For more information, see the:

- *Quantum Scalable Chassis Getting Started Guide* and *R81 Quantum Scalable Chassis Installation and Upgrade Guide*.
- *R81 Scalable Platforms Gaia Administration Guide*.
- *R81 Security Management Administration Guide*.
- Applicable *Administration Guides* on the R81 Home Page for Scalable Platforms.
- Applicable *Administration Guides* on the R81 Home Page.

Accept, or Drop Ethernet Frames with Specific Protocols

By default, Security Gateway in the Bridge mode *allows* Ethernet frames that carry protocols other than IPv4 (0x0800), IPv6 (0x86DD), or ARP (0x0806) protocols.

You can configure a Security Group in the Bridge Mode to either accept, or drop Ethernet frames that carry specific protocols.

When Access Mode VLAN (VLAN translation) is configured, BPDU frames can arrive with the wrong VLAN number to the switch ports through the Bridge interface. This mismatch can cause the switch ports to enter blocking mode.

In Active/Standby Bridge Mode only, you can disable BPDU forwarding to avoid such blocking mode:

Step	Instructions
1	Connect to the command line on the applicable Security Group.
2	Log in to the Expert mode.
3	Back up the current `/etc/rc.d/init.d/network` file: `cp -v /etc/rc.d/init.d/network{,_BKP}`
4	Edit the current `/etc/rc.d/init.d/network` file: `vi /etc/rc.d/init.d/network`

5	After the line:
	`./etc/init.d/functions`
	Add this line:
	`/sbin/sysctl -w net.bridge.bpdu_forwarding=0`

6	Save the changes in the file and exit the editor.
7	Reboot the Security Group: `reboot -b all`
8	Connect to the command line on the applicable Security Group.
9	Log in to the Expert mode.

Step	Instructions

10	Make sure the new configuration is loaded:
	`sysctl net.bridge.bpdu_forwarding`
	The expected output:
	`net.bridge.bpdu_forwarding = 0`

Routing and Bridge Interfaces

Security Gateways with a Bridge interface can support Layer 3 routing over non-bridged interfaces.

If you configure a Bridge interface with an IP address on a Security Group, the Bridge interface functions as a regular Layer 3 interface.

The Bridge interface participates in IP routing decisions on the Security Group and supports Layer 3 routing.

- Cluster deployments do not support this configuration.
- You cannot configure the Bridge interface to be the nexthop gateway for a route.
- A Security Group can support multiple Bridge interfaces, but only one Bridge interface can have an IP address.
- A Security Group cannot filter or transmit packets that it inspected before on a Bridge interface (to avoid double-inspection).

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:

Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On

IPv6 Neighbor Discovery	Network object that represents the Bridged Network	Network object that represents the Bridged Network	`Any`	`neighbor-advertisement`
				`neighbor-solicitation`
				`router-advertisement`
				`router-solicitation`
				`redirect6`
					`Accept`	`Log`	`Policy Targets`

Managing Ethernet Protocols

It is possible to configure a Security Gateway with bridge interface to allow or drop protocols that are not based on IP that pass through the bridge interface. For example, protocols that are not IPv4, IPv6, or ARP.

By default, these protocols are allowed by the Security Gateway.

Frames for protocols that are not IPv4, IPv6, or ARP are allowed if:

- On the Security Gateway, the value of the kernel parameter `fwaccept_unknown_protocol` is 1 (all frames are accepted)
- OR in the applicable `user.def` file on the Management Server, the protocol IS defined in the `allowed_ethernet_protocols` table.
- AND in the applicable `user.def` file on the Management Server, the protocol is NOT defined in the `dropped_ethernet_protocols` table.

To configure the Security Group to accept only specific protocols that are not IPv4, IPv6, or ARP:

Step	Instructions

1	On the Security Group, configure the value of the kernel parameter `fwaccept_unknown_protocol` to 0.
	a. Connect to the command line on the Security Group.
	b. Log in to the Expert mode.
	c. Configure the value of the kernel parameter `fwaccept_unknown_protocol` to 0:
	`g_update_conf_file fwkern.conf fwaccept_unknown_protocol=0`
	d. Reboot the Security Group.
	If the reboot is not possible at this time, then:
	■ Run this command to make the required change:
	`g_fw ctl set int fwaccept_unknown_protocol 0`
	■ Run this command to make sure the required change was accepted:
	`g_fw ctl get int fwaccept_unknown_protocol`

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>2</td><td>On the Management Server, edit the applicable <code>user.def</code> file.

Note - For the list of <code>user.def</code> files, see sk98239.

a. Back up the current applicable <code>user.def</code> file.
b. Edit the current applicable <code>user.def</code> file.
c. Add these directives:
■ <code>allowed_ethernet_protocols</code> - contains the EtherType numbers (in Hex) of protocols to accept
■ <code>dropped_ethernet_protocols</code> - contains the EtherType numbers (in Hex) of protocols to drop

Example
<pre>$ifndef __user_def__
$define __user_def__

\\
\\ User defined INSPECT code
\\

allowed_ethernet_protocols={
<0x0800,0x86DD,0x0806>);
dropped_ethernet_protocols={ <0x8137,0x8847,0x9100>
);

endif /*__user_def__*/</pre>For the list of EtherType numbers, see http://standards-oui.ieee.org/ethertype/eth.csv.
d. Save the changes in the file and exit the editor.</td></tr>
<tr><td>3</td><td>In SmartConsole, install the Access Control Policy on the Security Gateway object.</td></tr>
</table>

Configuring Link State Propagation (LSP)

Background

You can use the Link State Propagation (LSP) to bind physical interfaces together on an SSM. This causes all bound interfaces in an LSP Port Group to go DOWN when one of the bound interfaces goes DOWN.

After a predefined period time (default is 190 seconds), all interfaces go back to the UP state.

This feature makes sure that third party devices connected to Chassis fail over quickly, when using dynamic routing.

The Link State Propagation is disabled by default.

Configuring LSP Port Groups

Define LSP Port Groups in the `/etc/lsp_groups.conf` file.

Each line in this file defines one LSP Port Group with one or more interface groups, delimited by a comma.

An interface group has one or more interfaces, delimited by a plus sign (+).

Syntax of the configuration file

Item	Description
1	LSP Port Group (full syntax)
2	Interface Group
<*if*>	Physical Interface

Example 1

```
eth1-01+eth2-01,eth3-01+eth4-01
```

In this example, the LSP Port Group has two interface groups with two interfaces:

- Interface Group 1 contains `eth1-01` and `eth2-01`
- Interface Group 2 contains `eth3-01` and `eth4-01`

Example 2

```
eth1-02+eth1-03+eth1-04+eth1-05,eth3-02+eth4-02,eth3-03+eth4-03
```

In this example, the LSP port Group has three interface groups.

One group with four interfaces and two other groups with two interfaces each.

Adding an LSP Port Group

Step	Instructions
1	Connect to the command line on an SGM.
2	Log in to the Expert mode.
3	Edit the `/etc/lsp_groups.conf` file: `vi /etc/lsp_groups.conf`
4	Add one line for each LSP Port Group in the file.
5	Save the changes in the file and exit the editor.
6	Copy the file to all SGMs: `asg_cp2blades /etc/lsp_groups.conf`

7	Restart the LSP mechanism with these two commands:
	`asg_lsp_util disable`
	`asg_lsp_util enable`
	This step in necessary for the system to detect the change.

Deleting an LSP Port Group

Important - If you do not use the LSP, disable it (with the "`asg_lsp_util disable`" command). Do **not** delete the configuration file, or the only LSP port group line in the file.

Step	Instructions
1	Connect to the command line on an SGM.
2	Log in to the Expert mode.
3	Edit the `/etc/lsp_groups.conf` file: `vi /etc/lsp_groups.conf`
4	Delete the applicable LSP Port Group line from the file.
5	Save the changes in the file and exit the editor.
6	Copy the file to all SGMs: `asg_cp2blades /etc/lsp_groups.conf`

7	Restart the LSP mechanism with these two commands:
	`asg_lsp_util disable`
	`asg_lsp_util enable`
	This step in necessary for the system to detect the change.

What is the Next Step?

See the Administration Guides for the applicable Software Blades on the R81 Home Page.

Glossary

A

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Breakout Cable
An optical fiber cable that contains several jacketed simplex optical fibers that are packaged together inside an outer jacket. Synonyms: Fanout cable, Fan-Out cable, Splitter cable.

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Chassis Monitoring Module
A hardware component that controls and monitors 60000 / 40000 Appliance (Chassis) operation such as, fan speed, Chassis and module temperature, and component hot-swapping. Acronym: CMM.

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Security Gateway that is part of a cluster.

Compliance
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. See sk119715. Acronym: CTNT.

CoreXL
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself. For details, see sk92449.

D

DAC Cable
Direct Attach Copper cable. A form of the high-speed shielded twinax copper cable with pluggable transceivers on both ends. Used to connect to network devices (switches, routers, or servers).

DAIP Gateway
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia gClish
The name of the global command line shell in Check Point Gaia operating system for Security Gateway Modules. Commands you run in this shell apply to all Security Gateway Module in the Security Group.

Gaia Portal
Web interface for the Check Point Gaia operating system.

H

Hotfix
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Awareness
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Logging
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPS
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mobile Access
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

Network Object
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

Power Entry Module
Hardware component that supplies DC power with EMC filtering and over-current protection. Acronym: PEM.

Power Supply Unit
Hardware component that supplies AC power with filtering and over-current protection. Acronym: PSU.

Provisioning
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Q

QoS
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Rule
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base
All rules configured in a given Security Policy. Synonym: Rulebase.

S

SecureXL
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Gateway Module
A hardware component on a 60000 / 40000 Appliance (Chassis) that operates as a physical Security Gateway. A Chassis contains many Security Gateway Modules that work together as a single, high performance Security Gateway or VSX Gateway. Acronym: SGM.

Security Group
A logical group of Security Gateway Modules that provides Active/Active cluster functionality. A Security Group can contain one or more Security Gateway Modules. Security Groups work separately and independently from each other. To the production networks, a Security Group appears a single Security Gateway.

Security Management Server
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

Security Switch Module
A hardware component on a 60000 / 40000 Appliance (Chassis) that manages the flow of network traffic to and from the Security Gateway Module in the Chassis. Acronym: SSM.

Shared Management
Feature that allows to assign the same Management Port (interface ethX-MgmtY) on a Quantum Maestro Orchestrator to different Security Groups. The assigned Management Port has a different IP address and a different MAC address in each Security Group, to which this port is assigned.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

Single Management Object
Single Security Gateway object in SmartConsole that represents a Security Group configured on Scalable Chassis. Acronym: SMO.

SmartConsole
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

SMO
See "SMO".

SMO Master
The Security Gateway Module in a Security Group that handles management tasks for all Security Gateway Modules in the Security Group. By default, this role is assigned to the Security Gateway Module with the lowest Member ID in the Security Group. See "SMO".

Software Blade
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

T

Threat Emulation
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.