



FortiController - Session-Aware Load Balancing (SLBC) Guide

Version 5.2.10

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



April 12, 2021

FortiController 5.2.10 Session-Aware Load Balancing (SLBC) Guide

01-5210-247862-20210412

TABLE OF CONTENTS

Change log	8
About Session-Aware Load Balanced Clusters (SLBCs)	10
SLBC FortiController models	14
FortiController-5103B	15
FortiController-5903C	16
FortiController-5913C	18
Getting started and SLBC Basics	20
SLBC licensing	22
FortiOS Carrier licensing	22
Certificates	22
Changing FortiController interface configurations	22
Changing FortiController-5103B interface speeds	22
Changing FortiController interface speeds	23
Splitting front panel network interfaces	23
Quick SLBC cluster setup	24
Connecting to the FortiController GUI	25
Connecting to the FortiController command line interface (CLI)	25
Factory default settings	26
Managing the cluster	26
Default VDOM configuration	26
Replacing the default management certificate	27
Managing the workers (including SNMP, FortiManager)	27
Managing the FortiControllers (including SNMP and FortiManager)	28
Managing the devices in an SLBC cluster with the External Management IP	29
Single chassis or chassis 1 special management port numbers	30
Chassis 2 special management port numbers	31
Example single chassis management IP addresses and port numbers	31
Example management IP addresses and port numbers for two chassis and two or four FortiControllers	32
Monitoring the cluster	32
Worker communication with FortiGuard	33
Basic cluster NAT/Route mode configuration	34
Using the GUI to configure NAT/Route mode	34
Using the CLI to configure NAT/Route mode	35
Primary unit (master) selection	36
Selecting the primary FortiController (and the primary chassis)	36
Selecting the primary worker	37
Adding and removing workers	37
Adding one or more new workers	38
Removing a worker from a cluster	38
Adding link aggregation (LACP) to an SLBC cluster (FortiController trunks)	39
Adding an aggregated interface	39
Individual FortiAnalyzer settings on each worker	40
Configuring different FortiAnalyzer settings for each SLBC worker	40

Configuring different FortiAnalyzer settings for each worker and for the root VDOM of each worker	40
Adding VLANs	41
Adding a VLAN to a FortiController interface	41
VRRP support	41
FGCP to SLBC migration	42
Assumptions	42
Conversion steps	42
Updating SLBC firmware	43
Upgrading a single-chassis cluster	44
Upgrading a two-chassis cluster	44
Verifying the configuration and the status of the units in the cluster	45
Configuring communication between FortiControllers	47
Changing the base control subnet and VLAN	48
Changing the base management subnet and VLAN	48
Changing the heartbeat VLAN	48
Using the FortiController-5103B mgmt interface as a heartbeat interface	49
Changing the heartbeat interface mode	49
Enabling session sync and configuring the session sync interface	49
Changing load balancing settings	50
Tuning TCP load balancing performance (TCP local ingress)	50
Tuning UDP load balancing (UDP local ingress and UDP remote/local session setup)	50
Changing the load distribution method	51
TCP and UDP local ingress session setup and round robin load balancing	52
Changing how UDP sessions are processed by the cluster	52
Tuning load balancing performance: fragmented sessions	53
Changing session timers	53
Life of a TCP packet	55
Life of a TCP packet (default configuration: TCP local ingress disabled)	55
Life of a TCP packet (TCP local ingress enabled)	55
Life of a UDP packet	57
Life of a UDP packet (default configuration: UDP local ingress disabled and UDP remote session setup)	57
Life of a UDP packet (UDP local ingress disabled and UDP local session setup)	57
Life of a UDP packet (UDP local ingress enabled and UDP remote session setup)	58
Life of a UDP packet (UDP local ingress enabled and UDP local session setup)	59
SLBC with one FortiController-5103B	60
Setting up the hardware	60
Configuring the FortiController	60
Adding the workers to the cluster	62
Operating and managing the cluster	63
Active-Passive SLBC with two FortiController-5103Bs	65
Setting up the hardware	65
Configuring the FortiControllers	66

Adding the workers to the cluster	70
Operating and managing the cluster	71
Dual mode SLBC with two FortiController-5103Bs	73
Setting up the Hardware	74
Configuring the FortiControllers	74
Adding the workers to the cluster	80
Operating and managing the cluster	81
Active-passive SLBC with two FortiController-5103Bs and two chassis	83
Setting up the hardware	84
Configuring the FortiController in chassis 1	84
Configuring the FortiController in chassis 2	86
Adding the workers to the cluster	87
Operating and managing the cluster	89
Checking the cluster status	90
Active-passive SLBC with four FortiController-5103Bs and two chassis	94
Setting up the hardware	95
Configuring the FortiController in chassis 1 slot 1	96
Configuring the FortiController in chassis 1 slot 2	98
Configuring the FortiController in chassis 2 slot 1	98
Configuring the FortiController in chassis 2 slot 2	99
Configuring the cluster	100
Adding the workers to the cluster	103
Operating and managing the cluster	105
Checking the cluster status	106
Dual mode SLBC with four FortiController-5103Bs and two chassis	113
Setting up the hardware	114
Configuring the FortiController in chassis 1 slot 1	115
Configuring the FortiController in chassis 1 slot 2	117
Configuring the FortiController in chassis 2 slot 1	118
Configuring the FortiController in chassis 2 slot 2	118
Configuring the cluster	119
Adding the workers to the cluster	123
Operating and managing the cluster	125
Checking the cluster status	126
Dual mode SLBC with four FortiController-5903Cs and two chassis	133
Setting up the hardware	134
Configuring the FortiController in Chassis 1 Slot 1	135
Configuring the FortiController in chassis 1 slot 2	137
Configuring the FortiController in chassis 2 slot 1	137
Configuring the FortiController in chassis 2 slot 2	138
Configuring the cluster	139
Adding the workers to the cluster	142
Operating and managing the cluster	144

Checking the cluster status	145
Dual mode SLBC HA with LAGs third-party switch example	152
AP mode single chassis SLBC with LAGs third-party switch example	155
AP mode SLBC HA with LAGs third-party switch example	158
FortiController get and diagnose commands	163
get load-balance status	163
diagnose system flash list	163
diagnose system ha showcsum	163
diagnose system ha stats	164
diagnose system ha status	164
diagnose system ha force-slave-state	165
diagnose system load-balance worker-blade status	165
diagnose system load-balance worker-blade session-clear	165
diagnose switch fabric-channel egress list	166
diagnose switch base-channel egress list	166
diagnose switch fabric-channel packet heartbeat-counters list	167
diagnose switch fabric-channel physical-ports	168
diagnose switch fabric-channel mac-address list	169
diagnose switch fabric-channel mac-address filter	170
diagnose switch fabric-channel trunk list	170
FortiController/FortiSwitch MIBs	173
FortiController/FortiSwitch traps	175
Generic Fortinet traps (OID 1.3.6.1.4.1.12356.1.3.0)	175
Common Fortinet traps (OID 1.3.6.1.4.1.12356.100.1.3.0)	176
FortiSwitch/FortiController traps (OID 1.3.6.1.4.1.12356.106.2.0)	176
FortiController/FortiSwitch MIB fields	178
FortiSwitch system information (OID 1.3.6.1.4.1.12356.106.4.1)	178
FortiSwitch software version (OID 1.3.6.1.4.1.12356.106.4.2)	179
FortiSwitch high availability trap objects (OID 1.3.6.1.4.1.12356.106.13.3)	179
Worker blade information (OID 1.3.6.1.4.1.12356.106.14.2.1)	180
Worker blade VDOM (OID 1.3.6.1.4.1.12356.106.14.2.2)	182
Worker blade Antivirus (OID 1.3.6.1.4.1.12356.106.14.2.3)	183
Worker blade IPS (OID 1.3.6.1.4.1.12356.106.14.2.4)	185
Worker blade processor usage (OID 1.3.6.1.4.1.12356.106.14.2.5)	186
Shelf manager traps	188
Notification root (OID 1.3.6.1.4.1.3183.1.1.0)	188
IPMI trap data (OID 1.3.6.1.4.1.3183.1.1.1)	188
IPMI trap text (OID 1.3.6.1.4.1.3183.1.1.2)	188
IPMI PET multi-variable format (OID 1.3.6.1.4.1.3183.1.1.3)	189
Shelf manager MIB fields	190
Shelf manager IPM controller (OID 1.3.6.1.4.1.16394.2.1.1.1)	190
Shelf manager FRU device (OID 1.3.6.1.4.1.16394.2.1.1.2)	191
Shelf manager sensor (OID 1.3.6.1.4.1.16394.2.1.1.3)	193

Shelf manager board (OID 1.3.6.1.4.1.16394.2.1.1.4)	195
Shelf manager system event log (sel) (OID 1.3.6.1.4.1.16394.2.1.1.5)	196
Shelf manager shelf (OID 1.3.6.1.4.1.16394.2.1.1.6)	196
Shelf manager LAN configuration (OID 1.3.6.1.4.1.16394.2.1.1.7)	197
Shelf manager platform event filter (PEF) (OIDs 1.3.6.1.4.1.16394.2.1.1.8 - 19)	198
Shelf manager FRU info table (OID 1.3.6.1.4.1.16394.2.1.1.20)	199
Shelf manager FRU device by site (OID 1.3.6.1.4.1.16394.2.1.1.21)	200
Shelf manager FRU LED state (OID 1.3.6.1.4.1.16394.2.1.1.22)	202
Shelf manager board basic (OID 1.3.6.1.4.1.16394.2.1.1.32)	204
Shelf manager fan tray (OID 1.3.6.1.4.1.16394.2.1.1.33)	205
Shelf manager power supply (OID 1.3.6.1.4.1.16394.2.1.1.34)	208
Shelf manager shelf manager (OID 1.3.6.1.4.1.16394.2.1.1.35)	211
Shelf manager chassis (OID 1.3.6.1.4.1.16394.2.1.1.36)	213
Shelf manager events (OID 1.3.6.1.4.1.16394.2.1.1.37)	215
Shelf manager shelf manager status (OID 1.3.6.1.4.1.16394.2.1.1.38)	216
Shelf manager shelf manager version (OID 1.3.6.1.4.1.16394.2.1.1.39)	216
Shelf manager telco alarm (OID 1.3.6.1.4.1.16394.2.1.1.40)	217
Shelf manager SEL information (OID 1.3.6.1.4.1.16394.2.1.1.41)	217
FortiController/FortiSwitch SNMP links	219

Change log

Date	Change description
April 12, 2021	Added missing <code>f1-only</code> option to Splitting front panel network interfaces on page 23 .
December 22, 2020	New FortiController/FortiSwitch SNMP information: <ul style="list-style-type: none">• FortiController/FortiSwitch MIBs on page 173.• FortiController/FortiSwitch traps on page 175.• FortiController/FortiSwitch MIB fields on page 178.• Shelf manager traps on page 188.• Shelf manager MIB fields on page 190.• FortiController/FortiSwitch SNMP links on page 219.
January 23, 2020	New third-party switch examples: <ul style="list-style-type: none">• Dual mode SLBC HA with LAGs third-party switch example on page 152• AP mode single chassis SLBC with LAGs third-party switch example on page 155• AP mode SLBC HA with LAGs third-party switch example on page 158
January 9, 2020	Information accessibility improvements. Added information about use of attenuators for fabric channel interfaces and other corrections to FortiController-5903C on page 16 and FortiController-5913C on page 18 .
July 26, 2018	FortiOS 6.0.2 document release. New section, VRRP support on page 41 . Added a note about the requirement to reset your system's configuration after splitting the FortiController-5903C and FortiController-5913C front panel interfaces to Changing FortiController interface configurations on page 22 .
30 April, 2018	Added FortiGate-5001E and FortiGate-5001E1 workers. Added the section Individual FortiAnalyzer settings on each worker on page 40 . Added the section Managing the cluster on page 26 . Added a note about not using the worker front panel interfaces to About Session-Aware Load Balanced Clusters (SLBCs) on page 10 . Added the section: Managing the cluster on page 26 . Added a note about 8 being the maximum number of physical interfaces in an LACP interface to Adding link aggregation (LACP) to an SLBC cluster (FortiController trunks) on page 39 .
15 February, 2017	New chapter: FortiController get and diagnose commands on page 163 .
21 November, 2016	Added information about the MTU size of FortiController data interfaces.
19 July, 2016	Corrected information about FortiToken licensing and SLBC throughput.
2 February 2016	Added a note about GTP load balancing not being supported by SLBC to About Session-Aware Load Balanced Clusters (SLBCs) on page 10 . Additional explanation about dual model network connections added to the dual model examples. Clarification of the VLANs used for session sync by FortiController-5903C and FortiController-5913C added to Configuring communication between FortiControllers on page 47 .
6 November, 2015	New section SLBC licensing on page 22 .

Date	Change description
1 November, 2015	Clarification and corrections about how to connect the B1 and B2 interfaces on a FortiController-5903C and FortiController-5913C cluster in the following sections: Dual mode SLBC with four FortiController-5903Cs and two chassis on page 133 and Configuring communication between FortiControllers on page 47 .
30 October 2015	Improved the coverage of the FortiController-5903C and FortiController-5913C throughout the document. New sections: SLBC FortiController models on page 14 , Changing FortiController interface configurations on page 22 , and Dual mode SLBC with four FortiController-5903Cs and two chassis on page 133 . More FortiController-5903C and FortiController-5913C examples to be added to future versions.
12 July 2015	New format, contents re-organized. Configuration examples enhanced with content from http://cookbook.fortinet.com . New section: FGCP to SLBC migration on page 42 . If you notice problems, send comments to techdoc@fortinet.com .

About Session-Aware Load Balanced Clusters (SLBCs)

This FortiController Session-Aware Load Balancing (SLBC) Guide describes connecting and configuring session-aware load balancing (SLBC) clusters consisting of FortiControllers acting as load balancers and FortiGate-5000s and operating as workers all installed in FortiGate-5000 series chassis. All traffic is directed to the FortiController front panel interfaces and then the FortiControllers load balance traffic to the workers.



The worker front panel interfaces are not used for traffic or for management and should not be connected to networks. All communication with the workers occurs over the FortiGate-5000 chassis fiber and base backplane channels.

SLBC clusters load balance TCP and UDP sessions. As a session-aware load balancer, the FortiController includes DP processors that maintain state information for all TCP and UDP sessions. The DP processors are capable of directing any TCP or UDP session to any worker installed in the same chassis. This session-awareness means that all TCP and UDP traffic being processed by a specific worker continues to be processed by the same worker. Session-awareness also means that more complex networking features such as network address translation (NAT), fragmented packets, complex UDP protocols, and complex protocols such as SIP that use pinholes, can be load balanced by the cluster.

In an SLBC, when a worker that is processing SIP traffic creates a pinhole, this information is communicated to the FortiController. The FortiController then knows to distribute the voice and media sessions to this worker.

SLBC things to know:

- The SIP protocol uses known SIP ports for control traffic but dynamically uses a wide range of ports for voice and other media traffic. To successfully pass SIP traffic through a firewall, the firewall must use a session helper or application gateway to look inside the SIP control traffic and determine the ports to open for voice and media. To allow the voice and media traffic, the firewall temporarily opens these ports, creating what's known as a pinhole that temporarily allows traffic on a port as determined by the SIP control traffic. The pinhole is closed when the first voice or media session packet is received. When this happens the pinhole is converted to a normal session and the pinhole itself is deleted.
- Session-aware load balancing does not support traffic shaping.
- IPv4 and IPv6 interface (or route-based) IPsec VPN sessions are not load balanced but are all processed by the primary worker. Policy-based IPsec VPNs, manual key IPsec VPNs and hub and spoke IPsec VPNs are not supported. These IPsec VPN session are dropped. Uni-directional SSL VPN sessions are load balanced to all workers.
- You cannot mix ELBC, FGCP and SLBC clusters in the same chassis.
- GTP sessions are not load balanced by SLBC. All GTP sessions are processed by the primary worker.

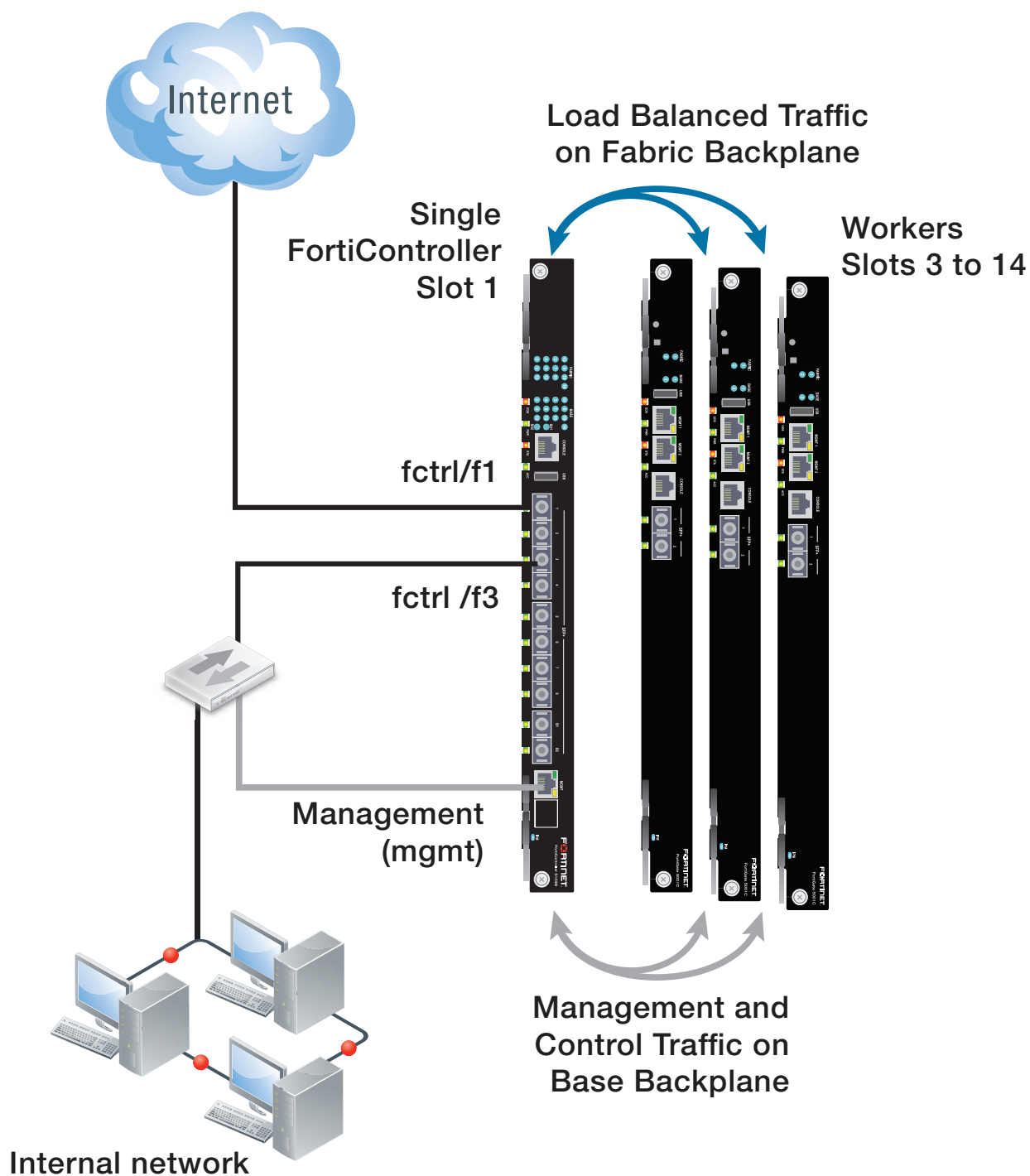
An SLBC consists of one or two FortiControllers installed in chassis slots 1 and 2 and from one to 12 workers installed chassis slots 3 and up. Network traffic is received by the FortiControllers and load balanced to the workers by the DP processors on the FortiControllers. Networks are connected to the FortiController front panel interfaces and communication between the FortiControllers and the workers uses the chassis fabric and base backplanes.

An SLBC with two FortiControllers can operate in active-passive mode or dual mode. In active-passive mode, if the active FortiController fails traffic is transferred to the secondary FortiController. In dual mode both FortiControllers load balance traffic and twice as many network interfaces are available.

You can also install FortiControllers and workers in a second chassis. The second chassis acts as a secondary and will keep operating if the active chassis fails. You can install one or two FortiControllers in each chassis. If you install one

FortiController in each chassis you create an active-passive setup. If the active chassis fails, traffic is processed by the secondary chassis. You can also install two FortiControllers in each chassis. The SLBC cluster in each chassis can operate in active-passive mode or dual mode. If the active chassis fails, traffic is processed by the secondary chassis.

The following picture shows a FortiController cluster consisting of one FortiController and three FortiGate-5001Cs.

Example FortiController Session-Aware Load Balanced Cluster (SLBC)

SLBC does not support session sync between workers in the same chassis. The FortiControllers in a cluster keep track of the status of the workers in their chassis and load balance sessions to the workers. If a worker fails the FortiController

detects the failure and stops load balancing sessions to that worker. The sessions that the worker is processing when it fails are lost.

Most of the examples in this document are based on the FortiController-5103B. However all configurations should be similar with other FortiControllers the only differences being things like the FortiController interface names. Supported FortiControllers include the FortiController-5103B, 5903C, and 5913C. Supported workers include the FortiGate-5001B, 5101C, 5001C, 5001D, 5001E, and the 5001E1.

Before using this document, your chassis should be mounted and connected to your power system. The chassis should be powered up and the front panel LEDs should indicate that it is functioning normally.

SLBC FortiController models

Currently three FortiController models are available for session aware load balancing (SLBC).



The FortiController-5902D and the FortiSwitch-5203B are used for content clustering and are not compatible with SLBC.

Some FortiController hardware and software features that affect SLBC configurations

	FortiController-5103B	FortiController-5903C	FortiController-5913C
Network interfaces	Eight front panel 10Gbps SFP+ FortiGate interfaces (F1 to F8) . Speed can be changed to 1Gbps. MTU size 9000 bytes.	Four front panel 40Gbps QSFP+ fabric channel interfaces (F1 to F4). Can be split into four 4x10G SFP+ interfaces. MTU size 9000 bytes.	Two front panel 100Gbps CFP2 fabric channel interfaces (F1 and F2). Can be split into two 10x10G SFP+ interfaces. MTU size 9000 bytes.
Base channel interfaces	Two front panel base backplane 1Gbps SFP+ interfaces (B1 and B2).	Two front panel 10Gbps SFP+ base channel interfaces (B1 and B2). Speed can be changed to 1Gbps.	Two front panel 10Gbps SFP+ base channel interfaces (B1 and B2). Speed can be changed to 1Gbps.
Fabric backplane interfaces	10Gbps Speed can be changed to 1Gbps.	40Gbps Speed can be changed to 10- or 1Gbps.	40Gbps Speed can be changed to 10- or 1Gbps.
Base backplane interfaces	1Gbps	1Gbps	1Gbps
Chassis supported	FortiGate-5144C (14 slots) FortiGate-5140B (14 slots) FortiGate-5060 (6 slots)	FortiGate-5144C (14 slots)	FortiGate-5144C (14 slots)
Heartbeat between FortiControllers	B1, B2, and Mgmt (optional) Default VLAN 999	B1 and B2 Default VLAN 999	B1 and B2 default VLAN 999
Base control between chassis	B1, B2, and mgmt (optional) Default VLAN 301	B1 and B2 Default VLAN 301	B1 and B2 Default VLAN 301
Base management between chassis	B1, B2, and mgmt (optional) Default VLAN 101	B1 and B2 Default VLAN 101	B1 and B2 Default VLAN 101
Session sync	One of F1 to F8	B1 and B2	B1 and B2

FortiController-5103B	FortiController-5903C	FortiController-5913C
VLAN 2000 (VLAN cannot be changed)	VLAN 1900 and 1901 (cannot be changed)	VLAN 1900 and 1901 (cannot be changed)

The remaining sections of this chapter describe each SLBC FortiController in more detail.



Splitting the FortiController-5903C and FortiController-5913C ports may require you to reset the workers to factory defaults and then completely re-configure your SLBC cluster. Fortinet recommends you split ports before configuring your cluster to save downtime due to the need to re-do your configuration.

FortiController-5103B

The FortiController-5103B distributes IPv4 TCP and UDP sessions to multiple FortiGate-5000-series boards (called workers) over the ATCA chassis fabric backplane. The FortiController-5103B board forms a session-aware load balanced cluster with up to 12 FortiGate-5000 boards operating as workers and uses DP processors to load balance millions of sessions to the cluster, providing 10 Gbps of traffic to each cluster member. Performance of the cluster shows linear improvement if more workers are added.

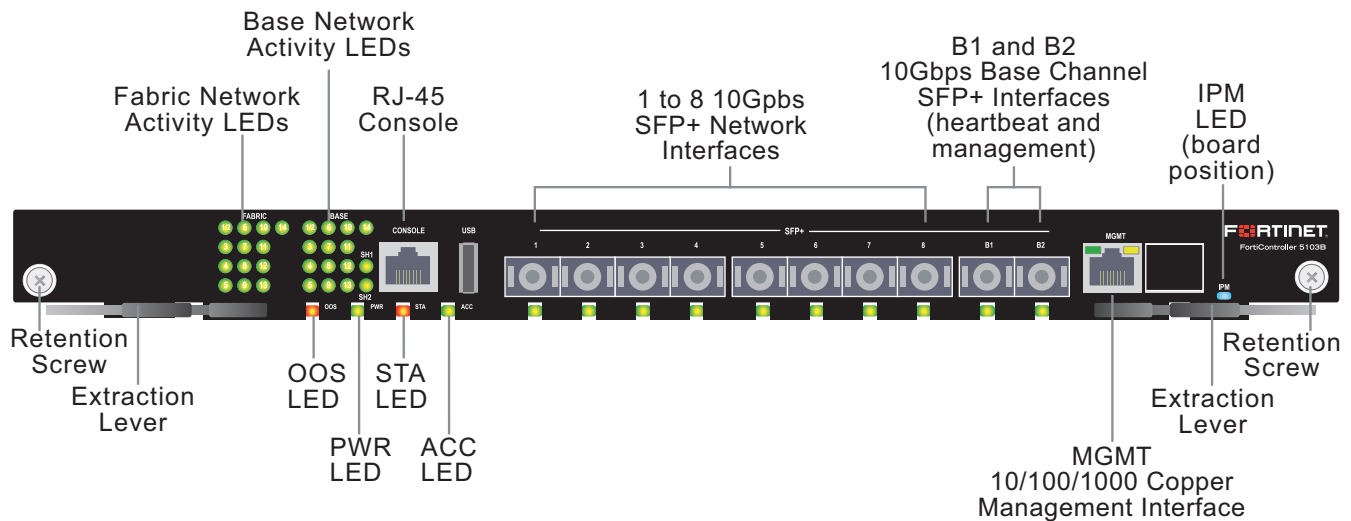
Clusters can be formed with one or two FortiController-5103B boards and up to 12 workers. All of the workers must be the same model. Currently FortiGate-5001B, FortiGate-5001C, FortiGate-5101C, and FortiGate-5001D models are supported.

The FortiController-5103B board can be installed in any ATCA chassis that can provide sufficient power and cooling. Supported FortiGate chassis include the 14-slot FortiGate-5140B and the 6-slot FortiGate-5060 chassis.

You can also install the FortiController-5103B board in a FortiGate-5144C chassis but this is not recommended because the 5144C chassis has a 40Gbit fabric backplane while the FortiController-5103B only supports 10Gbit fabric backplane connections. Older FortiGate-5000 chassis do not supply the power and cooling required for the FortiController-5103B board.

In all ATCA chassis, FortiController-5103B boards are installed in the first and second hub/switch slots (usually slots 1 and 2). A single FortiController-5103B board should be installed in slot 1 (but you can install it in slot 2). If you add a second board it should be installed in slot 2.

FortiController-5103B front panel



The FortiController-5103B board includes the following hardware features:

- One 1Gbps base backplane channel for layer-2 base backplane switching between FortiGate-5000 boards installed in the same chassis as the FortiController-5103B board. This base backplane channel includes 13 1Gbps connections to up to 13 other slots in the chassis (slots 2 to 14).
- One 10Gbps fabric backplane channel for layer-2 fabric backplane switching between FortiGate-5000 boards installed in the same chassis as the FortiController-5103B board. This fabric backplane channel includes 13 10Gbps connections to up to 13 other slots in the chassis (slots 2 to 14). Speed can be changed to 1Gbps.
- Eight front panel 10Gbps SFP+ FortiGate interfaces (1 to 8). In a session-aware load balanced cluster these interfaces are connected to 10Gbps networks to distribute sessions to FortiGate-5000 boards installed in chassis slots 3 to 14. Speed can be changed to 1Gbps. The MTU size of these interfaces is 9000 bytes.
- Two front panel base backplane 10Gbps SFP+ interfaces (B1 and B2) that connect to the base backplane channel. These interfaces are used for heartbeat and management communication between FortiController-5103B boards. Speed can be changed to 1Gbps.
- On-board DP processors to provide high-capacity session-aware load balancing.
- One 1Gbps out of band management ethernet interface (MGMT).
- One RJ-45, RS-232 serial console connection (CONSOLE).

FortiController-5903C

The FortiController-5903C distributes IPv4 TCP and UDP sessions to multiple FortiGate-5000-series boards (called workers) over the FortiGate-5144C chassis fabric backplane. The FortiController-5903C includes four front panel 40Gbps Quad Small form-factor Pluggable + (QSFP+) interfaces (F1 to F4) for connecting to 40Gbps networks. The FortiController-5903C forms a session-aware load balanced cluster and uses DP processors to load balance millions of sessions to the cluster, providing up to 40 Gbps of traffic to each cluster member (each worker). Performance of the cluster shows linear improvement if more workers are added.

Clusters can also be formed with one or two FortiController-5903Cs and up to 12 workers. All of the workers must be the same model. Currently FortiGate-5001B, FortiGate-5001C, FortiGate-5101C, FortiGate-5001D, FortiGate-5001E, and

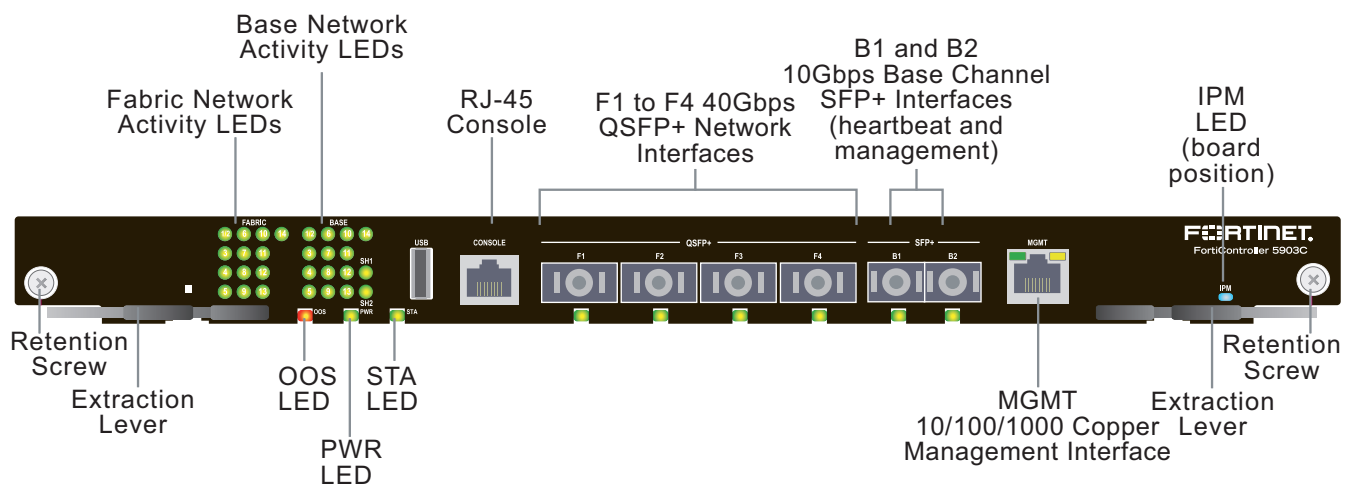
FortiGate-5001E1 workers are supported. FortiGate-5001C, FortiGate-5001D, FortiGate-5001E, and FortiGate-5001E1 workers can handle up to 40 Gbps of traffic. FortiGate-5001B and FortiGate-5101C workers can handle up to 10 Gbps.

The FortiController-5903C can also provide 40Gbps fabric and 1Gbps base backplane channel layer-2 switching in a dual star architecture.

You should install the FortiController-5903C in a FortiGate-5144C chassis to meet FortiController-5903C power requirements, to have access to a 40G fabric backplane, and to have enough slots for the number of workers that the FortiController-5903C can load balance sessions to.

In all ATCA chassis, FortiController-5903Cs are installed in the first and second hub/switch slots (usually slots 1 and 2). A single FortiController-5903C should be installed in slot 1 (but you can install it in slot 2). If you add a second FortiController-5903C it should be installed in slot 2.

FortiController-5903C Front Panel



The FortiController-5903C includes the following hardware features:

- One 1 base backplane channel for layer-2 base backplane switching between workers installed in the same chassis as the FortiController-5903C. This base backplane channel includes 13 1Gbps connections to up to 13 other slots in the chassis (slots 2 to 14).
- One 40Gbps fabric backplane channel for layer-2 fabric backplane switching between workers installed in the same chassis as the FortiController-5903C. This fabric backplane channel includes 13 40Gbps connections to up to 13 other slots in the chassis (slots 2 to 14). Speed can be changed to 10Gbps or 1Gbps.
- Four front panel 40Gbps QSFP+ fabric channel interfaces (F1 to F4). In a session-aware load balanced cluster these interfaces are connected to 40Gbps networks to distribute sessions to workers installed in chassis slots 3 to 14. These interfaces can also be split into 4x10G SFP+ interfaces. The MTU size of these interfaces is 9000 bytes. Splitting the F1 to F4 interfaces may require you to reset the workers to factory defaults and then completely re-configure your SLBC cluster. Fortinet recommends you split interfaces before configuring your cluster to save downtime due to the need to re-do your configuration.
- Two front panel 10Gbps SFP+ base channel interfaces (B1 and B2) that connect to the base backplane channel. These interfaces are used for heartbeat and management communication between FortiController-5903Cs. Speed can be changed to 1Gbps.
- On-board DP processors to provide high-capacity session-aware load balancing.
- One 1Gbps out of band management Ethernet interface (MGMT).

- Internal 64 GByte SSD for storing log messages, DLP archives, SQL log message database, historic reports, IPS packet archiving, file quarantine, WAN Optimization byte caching and web caching. according to the PRD there is no internal storage
- One RJ-45, RS-232 serial console connection (CONSOLE).
- One front panel USB port.



If your attached network equipment is sensitive to optical power, you may need to use attenuators with the F1 to F4 QSFP+ or split SFP+ fabric channel front panel interfaces to reduce the optical power transmitted to attached network equipment.

FortiController-5913C

The FortiController-5913C is an Advanced Telecommunications Computing Architecture (ATCA) compliant session-aware load balancing hub/switch board that distributes IPv4 TCP and UDP sessions to multiple FortiGate-5000-series boards (called workers) over the FortiGate-5144C chassis fabric backplane. The FortiController-5913C includes two front panel 100Gbps C form-factor pluggable 2 (CFP2) interfaces (F1 and F2) for connecting to 100Gbps networks. The FortiController-5913C forms a session-aware load balanced cluster and uses DP processors to load balance millions of sessions to the cluster, providing up to 40 Gbps of traffic to each cluster member (each worker). Performance of the cluster shows linear improvement if more workers are added.

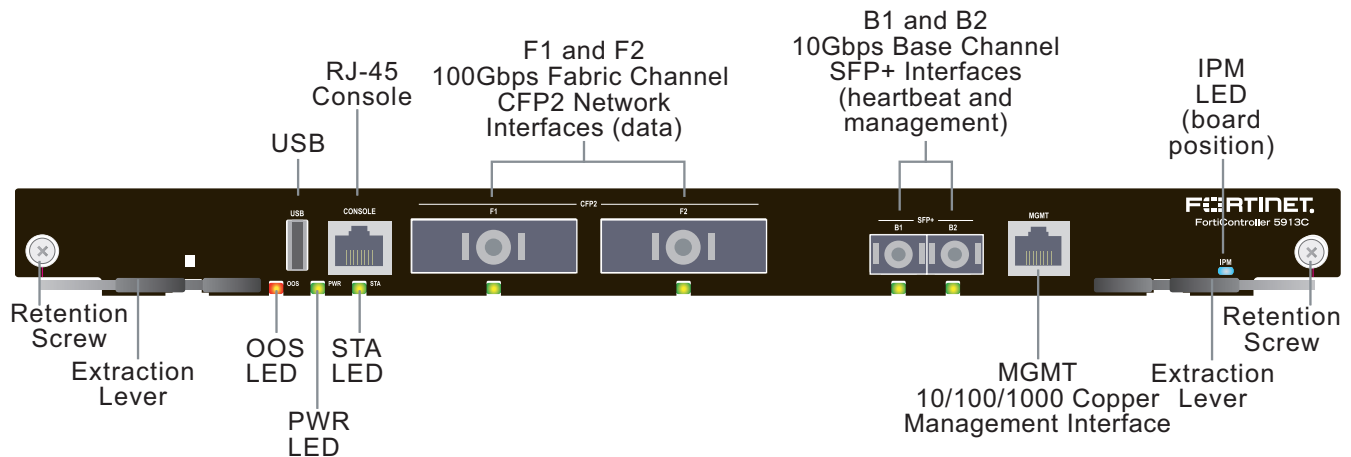
Clusters can also be formed with one or two FortiController-5913Cs and up to 12 workers. All of the FortiGate-5000 workers must be the same model. Currently FortiGate-5001B, FortiGate-5001C, FortiGate-5101C, FortiGate-5001D, FortiGate-5001E, and FortiGate-5001E1 workers are supported. FortiGate-5001C, FortiGate-5001D, FortiGate-5001E and FortiGate-5001E1 workers can handle up to 40 Gbps of traffic. FortiGate-5001B and FortiGate-5101C workers can handle up to 10 Gbps.

The FortiController-5913C can also provide 40Gbps fabric and 1Gbps base backplane channel layer-2 switching in a dual star architecture.

You should install the FortiController-5913C in a FortiGate-5144C chassis to meet FortiController-5913C power requirements, to have access to a 40G fabric backplane, and to have enough slots for the number of workers that the FortiController-5913C can load balance sessions to.

In all ATCA chassis, FortiController-5913Cs are installed in the first and second hub/switch slots (usually slots 1 and 2). A single FortiController-5913C should be installed in slot 1 (but you can install it in slot 2). If you add a second FortiController-5913C it should be installed in slot 2.

FortiController-5913C Front Panel



The FortiController-5913C includes the following hardware features:

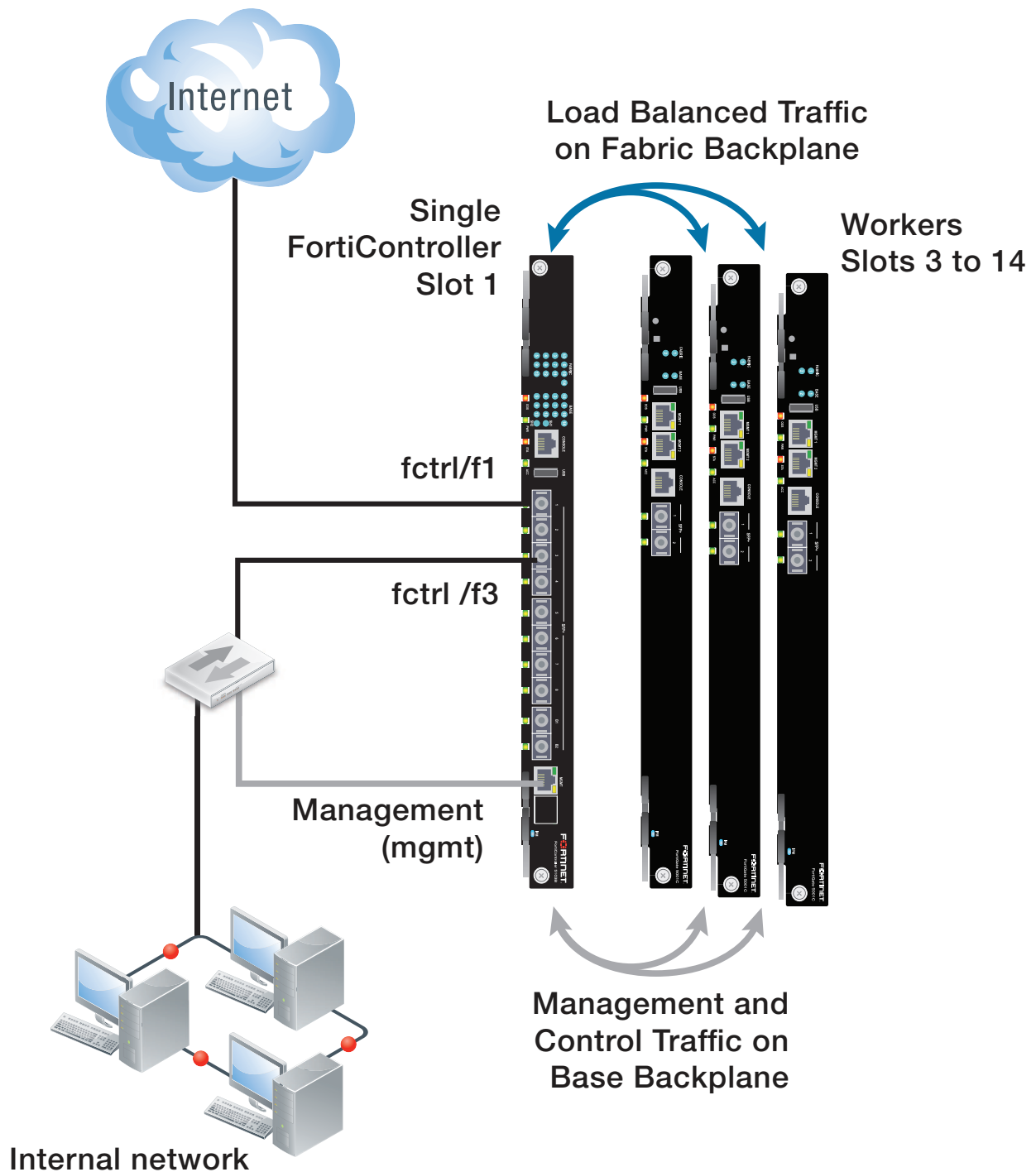
- One 1Gbps base backplane channel for layer-2 base backplane switching between workers installed in the same chassis as the FortiController-5913C. This base backplane channel includes 13 1Gbps connections to up to 13 other slots in the chassis (slots 2 to 14).
- One 40Gbps fabric backplane channel for layer-2 fabric backplane switching between workers installed in the same chassis as the FortiController-5913C. This fabric backplane channel includes 13 40Gbps connections to up to 13 other slots in the chassis (slots 2 to 14). Speed can be changed to 10Gbps or 1Gbps.
- Two front panel 100Gbps CFP2 fabric channel interfaces (F1 and F2). In a session-aware load balanced cluster these interfaces are connected to 100Gbps networks to distribute sessions to workers installed in chassis slots 3 to 14. These interfaces can also be split into 10x10G SFP+ interfaces. The MTU size of these interfaces is 9000 bytes. Splitting the F1 and F2 interfaces may require you to reset the workers to factory defaults and then completely re-configure your SLBC cluster. Fortinet recommends you split interfaces before configuring your cluster to save downtime due to the need to re-do your configuration.
- Two front panel 10Gbps SFP+ base channel interfaces (B1 and B2) that connect to the base backplane channel. These interfaces are used for heartbeat and management communication between FortiController-5913Cs. Speed can be changed to 1Gbps.
- On-board DP processors to provide high-capacity session-aware load balancing.
- One 1Gbps out of band management ethernet interface (MGMT).
- One RJ-45, RS-232 serial console connection (CONSOLE).
- One front panel USB port.



If your attached network equipment is sensitive to optical power, you may need to use attenuators with the F1 and F2 CFP2 or split SFP+ fabric channel front panel interfaces to reduce the optical power transmitted to attached network equipment.

Getting started and SLBC Basics

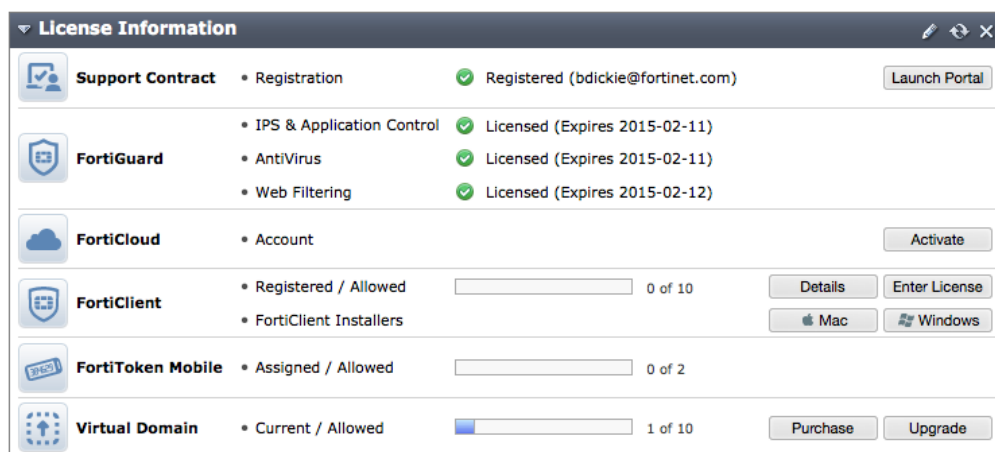
This chapter describes connecting and configuring a basic SLBC cluster consisting of one FortiController installed in chassis slot 1 and three FortiGate workers installed in chassis slots 3, 4, and 5.

Example session-aware load balanced cluster (SLBC)

SLBC licensing

The following sections describe some considerations when licensing an SLBC cluster.

Register and apply licenses to each worker before adding the worker to the SLBC cluster. This includes Technical Support, FortiClient, FortiCloud activation, FortiClient licensing, and entering a license key if you purchased more than 10 Virtual Domains (VDOMS). FortiToken licenses can be added at any time because they are synchronized to all workers.



FortiOS Carrier licensing

If the workers in an SLBC cluster will be running FortiOS Carrier, apply the FortiOS Carrier license before configuring the cluster (and before applying other licenses). Applying the FortiOS Carrier license sets the configuration to factory defaults, requiring you to repeat steps performed before applying the license.

Certificates

You can also install any third-party certificates on the primary worker before forming the SLBC cluster. Once the cluster is formed, third-party certificates are synchronized to all workers.

Changing FortiController interface configurations

This section shows how to change FortiController interface speeds and split FortiController-5903C and FortiController-5913C ports.

Changing FortiController-5103B interface speeds

To change front panel B1 and B2 interface speeds, from the FortiController-5103B GUI go to **Switch > Base Channel** and edit the b1 or b2 interface. Set the Speed to 10Gbps Full-duplex or 1Gbps Full duplex and select OK. From the CLI

enter the following command to change the speed of the B1 port.

```
config switch base-channel physical-port
  edit b1
    set speed {10000full | 1000full}
  end
```

To change front panel F1 to F8 interface speeds, from the FortiController-5103B GUI go to **Switch > Fabric Channel** and edit a f1 to f8 interface. Set the Speed to 10Gbps Full-duplex or 1Gbps Full duplex and select OK. From the CLI enter the following command to change the speed of the F6 port.

```
config switch fabric-channel physical-port
  edit f6
    set speed {10000full | 1000full}
  end
```

To change backplane fabric channel interface speeds, from the FortiController-5103B GUI go to **Switch > Fabric Channel** and edit a slot-1/2 to slot 14 interface. Set the Speed to 10Gbps Full-duplex or 1Gbps Full duplex and select OK. From the CLI enter the following command to change the speed of the slot-4 port.

```
config switch fabric-channel physical-port
  edit slot-4
    set speed {10000full | 1000full}
  end
```

Changing FortiController interface speeds

To change front panel B1 and B2 interface speeds, from the GUI go to **Switch > Base Channel** and edit the b1 or b2 interface. Set the Speed to 10Gbps Full-duplex or 1Gbps Full duplex and select OK. From the CLI enter the following command to change the speed of the B1 port.

```
config switch base-channel physical-port
  edit b1
    set speed {10000full | 1000full}
  end
```

To change backplane fabric channel interface speeds, from the GUI go to **Switch > Fabric Channel** and edit a slot-1/2 to slot 14 interface. Set the Speed to 40Gbps Full-duplex, 10Gbps Full-duplex or 1Gbps Full duplex and select OK. From the CLI enter the following command to change the speed of the slot-4 port.

```
config switch fabric-channel physical-port
  edit slot-4
    set speed {40000full | 10000full | 1000full}
  end
```

Splitting front panel network interfaces

You can use the following command to split the FortiController-5903C F1 to F4 or the FortiController-5913C F1 and F2 front panel data network interfaces into 10G interfaces. You can also use this command to split just the F1 interface into 10G interfaces.

```
config system global
  set fabric-front-port-10g-mode {disable | enable | f1-only}
end
```

Set to `disable` by default and none of the interfaces are split.

Set to enable to split all of the interfaces as follows:

- Each FortiController-5903C 40Gbps interface is split into four 10Gbps interfaces for a total of sixteen 10Gbps interfaces. The interfaces are named fctrl1/f1-1, fctrl1/f1-2, fctrl1/f1-3, fctrl1/f1-4, fctrl1/f2-1, and so on.
- Each FortiController-5913C 100Gbps interface is split into ten 10Gbps interfaces for a total of twenty 10Gbps interfaces. The interfaces are named fctrl1/f1-1, fctrl1/f1-2, fctrl1/f1-3, fctrl1/f1-4, fctrl1/f1-5, ..., fctrl1/f2-1, fctrl1/f2-2 and so on.

Set to `f1-only` to split the F1 interface as follows:

- Each FortiController-5903C 40Gbps F1 interface is split into four 10Gbps interfaces named fctrl1/f1-1, fctrl1/f1-2, fctrl1/f1-3, and fctrl1/f1-4.
- Each FortiController-5913C 100Gbps F1 interface is split into ten 10Gbps interfaces named fctrl1/f1-1, fctrl1/f1-2, fctrl1/f1-3, ..., fctrl1/f1-10.



Splitting the FortiController-5903C and FortiController-5913C front panel interfaces may require you to reset the workers to factory defaults and then completely re-configure your SLBC cluster. Fortinet recommends you split interfaces before configuring your cluster to save downtime due to the need to re-do your configuration.

In addition, you don't have to split all of the interfaces at the same time, but you should split as many as you will need so that you won't have to re-configure everything in the future if you decide to split some more interfaces. You also have to reconfigure the SLBC cluster if you decide to re-combine some interfaces that were previously split.

Quick SLBC cluster setup

This section contains some high-level steps that guide you through the basics of setting up an example SLBC cluster consisting of a single FortiController and 3 workers installed in a FortiGate-5000 chassis.

1. Install the FortiGate-5000 series chassis and connect it to power.
2. Install the FortiController in chassis slot 1.
3. Install the workers in chassis slots 3, 4, and 5.
4. Power on the chassis.
5. Check the chassis, FortiController and worker LEDs to verify that all components are operating normally.
6. Check the FortiSwitch-ATCA release notes and confirm that your FortiController is running the latest supported firmware. You can download the release notes from [the Fortinet Documentation website](https://support.fortinet.com) and the correct firmware from Fortinet's Support site (<https://support.fortinet.com>). Select the FortiSwitch-ATCA product.
7. Log into the CLI of each of the workers and use the following command to set them to FortiController mode:

```
config system elbc
    set mode forticontroller
end
```

8. From the FortiController GUI **Dashboard System Information** widget, beside **HA Status** select **Configure**.
9. Set **Mode** to **Active-Passive**, change the **Group ID**, and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

Or from the CLI enter the following command:

```
config system ha
    set mode a-p
```



```
set groupid 4
set hbdev b1 b2
end
```

10. You can optionally configure other HA settings.



If you have more than one cluster on the same network, each cluster should have a different Group ID. Changing the Group ID changes the cluster interface MAC addresses. Its possible that a group ID setting will cause a MAC address conflict. If this happens select a different Group ID. The default Group ID of 0 is not a good choice and usually should be changed.

11. Go to **Load Balance > Config** add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.
12. Configure the cluster external management interface so that you can manage the worker configuration. From the FortiController GUI go to **Load Balance > Config** and edit the **External Management IP/Netmask** and change it to an IP address and netmask for the network that the mgmt interfaces of the FortiController and the workers are connected to. The **External Management IP/Netmask** must be on the same subnet as the FortiController management IP address.
13. Connect FortiController front panel interface 1 (F1 on some models) to the Internet and front panel interface 3 (F3 on some models) to the internal network.
The workers see these interfaces as **fctrl/f1** and **fctrl/f3**.
Do not use the worker front panel interfaces for data or management connections.
14. Log into the workers using the External Management IP/Netmask and configure the workers to process traffic between fctrl/f1 and fctrl/f3.



If you need to add a default route to connect to the External Management IP/Netmask, log into the FortiController CLI and enter the following command:

```
config route static
edit route 1
set gateway <gateway-ip>
end
```

Connecting to the FortiController GUI

You can connect to the FortiController GUI by browsing to the FortiController mgmt interface IP address. From the FortiController GUI you can add workers to the cluster and configure load balancing settings.

By default, you can connect to the FortiController GUI by connecting the mgmt interface to your network and browsing to <https://192.168.1.99>.

Connecting to the FortiController command line interface (CLI)

You can connect to the FortiController CLI using the serial cable that came packaged with your FortiController or an Ethernet connection to the mgmt interface.

To connect to the CLI over an Ethernet network use SSH to connect to the mgmt port (default IP address 192.168.1.99).

To connect to the CLI using a serial console connection

1. Connect the FortiController unit's Console port to the serial communications (COM) port on your management computer using a serial cable (or using an RS-232 to USB converter).
2. Start the terminal emulation application and configure the following settings.
Bits per second 9600, Data bits 8, Parity None, Stop bits 1, Flow control None
3. Press Enter to connect to the CLI.
4. Type a valid administrator account name (such as admin) and press Enter.
5. Type the password for that administrator account and press Enter. (In its default state, there is no password for the admin account.)

Factory default settings

The FortiController unit ships with a factory default configuration. The default configuration allows you to connect to and use the FortiController GUI or CLI to configure the FortiController.

To configure the FortiController you should add a password for the admin administrator account, change the management interface IP address, and, if required, configure the default route for the management interface.

FortiController factory default settings

Administrator Account User Name	admin
Password	(none)
MGMT IP/Netmask	192.168.1.99/24

At any time during the configuration process, if you run into problems, you can reset the FortiController or the FortiGates to factory default settings and start over. From the CLI enter `execute factory-reset`.

Managing the cluster

This section describes managing the FortiControllers and workers in an SLBC cluster.



Do not disable or change the configuration of the FortiController or worker **base-mgmt** interfaces or the default . These interfaces are used for internal management communication and other related functions. They are visible from the FortiController and worker GUI and CLI but normally you would not need to change them.

Default VDOM configuration

By default when the SLBC cluster first starts up it is operating in multiple VDOM mode. The system has a management VDOM (named **elbc-mgmt**) and the **root** VDOM. All management interfaces are in elbc-mgmt and all other interfaces are in the root VDOM. You can add more VDOMs and add interfaces to them or just use the root VDOM.

Default management VDOM (elbc-mgmt)

The default SLBC cluster configuration includes a management VDOM named **elbc-mgmt**. The mgmt, b1, and b2 interfaces are in this VDOM. You cannot delete or rename this VDOM. You also cannot remove interfaces from it or add interfaces to it. You can however, configure other settings such as routing required for management communication, interface IP addresses, and so on.

You have full control over the configurations of other SLBC cluster VDOMs.

Replacing the default management certificate

The default Fortinet_Factory certificate, used for HTTPS and SSH management connections with the FortiController, has a key strength is 1024 bits. If you want to use your own certificate, which may have a higher key strength, and other advantages, such as being trusted on your network, you can use the `execute user certificate upload` command to install your custom certificate on the FortiController.

Then you can use the following command to replace the default server certificate with your custom certificate.

```
config system global
    set admin-server-cert <certificate-name>
end
```

For security reasons, certificates are not synchronized between FortiControllers. So you need to upload the certificate and repeat the `set admin-server-cert` command on each FortiController in your SLBC cluster.

Managing the workers (including SNMP, FortiManager)

After the workers have been added to a SLBC you can use the SLBC External Management IP to manage the primary worker. This includes access to the primary worker GUI or CLI, SNMP queries to the primary worker, and using FortiManager to manage the primary worker. As well SNMP traps and log messages are sent from the primary worker with the External Management IP as their source address. And finally connections to FortiGuard for updates, web filtering lookups and so on, all originate from the External Management IP.

Connecting to the external management IP address using a web browser or using other methods like SSH or telnet connects you to the primary worker (also called the master or the ELBC master). For example, if the External Management IP address is 10.10.10.1 you can browse to `https://10.10.10.1` to connect to the primary worker GUI. You can connect to the primary worker CLI using `ssh admin@10.10.10.1`, or `telnet 10.10.10.1` and so on as long as allow access settings permit.

Configuration changes made to the primary worker are synchronized to all of the workers in the cluster.

The primary worker SNMP configuration is the same as a any FortiGate SNMP configuration. SNMP queries to the primary worker report on the status of the primary worker only. However, some of the SNMP events (traps) sent by the primary worker can report HA events which can indicate when workers enter and leave the cluster etc.

You can use FortiManager to manage the primary worker and FortiManager does support the primary worker SLBC configuration. Of course, configuration changes made through FortiManager to the primary worker are synchronized to the other workers.

You can also managed individual workers, including the primary worker, using the SLBC External Management IP and a special port number. See [Managing the workers \(including SNMP, FortiManager\) on page 27](#).

You can also manage any individual worker (including the primary worker) by connecting directly to their mgmt1 or mgmt2 interfaces. You can configure these management interfaces when you first configure the worker before adding it to the cluster. The mgmt1 and mgmt2 interface settings are not synchronized so each worker will maintain its own mgmt1 and mgmt2 configuration. You can use the console to configure the mgmt1 and mgmt2 interfaces after the workers are operating in a cluster.

To get SNMP results from all of the workers in the cluster you can send SNMP queries to each one using their individual mgmt1 or mgmt2 IP addresses or using the External Management IP address and special port number.

The primary worker SNMP configuration is synchronized to all workers. SNMP traps sent by the primary worker come from the external management IP address. Individual workers can send traps from their mgmt1 and mgmt2 interfaces.

If you use the External Management IP address for SNMP queries the FortiController performs network address translation on the SNMP packets. So when the worker sees SNMP query packets their source address is set to the internal management IP. The internal management IP is 10.101.10.1 for the FortiController in slot 1 and 10.101.10.16 for the FortiController in slot 2. So you must configure SNMP communities to allow SNMP packets from these source addresses (or from any source address). For example:

```
config system snmp community
  edit 1
    config hosts
      edit 1
        set ip 10.101.10.1
      next
      edit 2
        set ip 10.101.10.16
      end
    end
  end
```

You can manage individual workers using FortiManager, but this is not recommended.

Managing the FortiControllers (including SNMP and FortiManager)

You can manage the primary FortiController using the IP address of its mgmt interface, set up when you first configured the primary FortiController. You can use this address for GUI access, CLI access, SNMP queries and FortiManager access.

The only way to remotely manage a secondary FortiController is by using the SLBC External Management IP and a special port number. See [Managing the FortiControllers \(including SNMP and FortiManager\) on page 28](#). You can also connect to the primary or secondary FortiController's console port.

FortiManager supports managing the primary FortiController. It may take some time after a new FortiController model is released for FortiManager to support it. Managing secondary FortiControllers with FortiManager is not recommended.

To manage a FortiController using SNMP you need to load the FORTINET-CORE-MIB.mib file into your SNMP manager. You can get this MIB file from the Fortinet support site, in the same location as the current FortiController firmware (select the FortiSwitchATCA product). You also need to configure SNMP settings (usually on the primary FortiController. The SNMP configuration is synchronized to the secondary FortiControllers.

First, enable SNMP access on the mgmt interface. Then from the CLI, configure system information. Make sure to set status to enable:

```
config system snmp sysinfo
  set contact-info <string>
  set description <string>
  set location <string>
  set status {enable | disable}
```

```

    set trap-high-cpu-treshold <percentage>
    set trap-lowmemory-treshold <percentage>
end

```

Second add one or more SNMP communities:

```

config system snmp community
    edit <index_integer>
        set events {cpu-high | mem-low | ha-switch | ha-hb-member-up | ha-member-down | hbfail |
            hbrcv | tkmem-down | tkmem-up}
        set name <name_string>
        set query-v1-port <port_number>
        set query-v1-status {enable | disable}
        set query-v2c-port <port_number>
        set query-v2c-status <port_number>
        set status {enable | disable}
        set trap-v1-lport <port_number>
        set trap-v1-rport <port_number>
        set trap-v1-status {enable | disable}
        set trap-v2c-lport <port_number>
        set trap-v2c-rport <port_number>
        set trap-v2c-status {enable | disable}
    end
end

```

FortiControllers can send SNMP traps for the following events:

- **cpu-high**, cpu usage too high
- **mem-low**, available memory too low
- **ha-switch**, cluster status change
- **ha-hb-member-up**, FortiController (cluster member) up
- **ha-member-down**, FortiController (cluster member) down,
- **hbfail**, heartbeat failure
- **hbrcv**, heartbeat received
- **tkmem-down**, worker (trunk member) down
- **tkmem-up**, worker (trunk member) up

Managing the devices in an SLBC cluster with the External Management IP

The External Management IP address is used to manage all of the individual devices in a SLBC by adding a special port number. This special port number begins with the standard port number for the protocol you are using and is followed by two digits that identify the chassis number and slot number. The port number can be calculated using the following formula:

service_port x 100 + (chassis_id - 1) x 20 + slot_id

Where:

- **service_port** is the normal port number for the management service (80 for HTTP, 443 for HTTPS and so on).
- **chassis_id** is the chassis ID specified as part of the FortiController HA configuration and can be 1 or 2.
- **slot_id** is the number of the chassis slot.



By default, chassis 1 is the primary chassis and chassis 2 is the secondary chassis. But the actual primary chassis is the one with the primary FortiController and the primary FortiController can be changed independently of the chassis number. And the chassis_id depends on the chassis number and not on whether the chassis contains the primary FortiController.

Some examples:

- HTTPS, chassis 1 slot 2: $443 \times 100 + (1 - 1) \times 20 + 2 = 44300 + 0 + 2 = 44302$:
browse to: `https://172.20.120.100:44302`
- HTTP, chassis 2, slot 4: $80 \times 100 + (2 - 1) \times 20 + 4 = 8000 + 20 + 4 = 8024$:
browse to `http://172.20.120.100/8024`
- HTTPS, chassis 1, slot 10: $443 \times 100 + (1 - 1) \times 20 + 10 = 44300 + 0 + 10 = 44310$,
browse to `https://172.20.120.100/44310`
- HTTPS, chassis 2, slot 10: $443 \times 100 + (2 - 1) \times 20 + 10 = 44300 + 20 + 10 = 44330$:
browse to `https://172.20.120.100/44330`
- SNMP query port, chassis 1, slot 4: $161 \times 100 + (1 - 1) \times 20 + 4 = 16100 + 0 + 4 = 16104$
- Telnet to connect to the CLI of the worker in chassis 2 slot 4:
`telnet 172.20.120.100 2324`
- To use SSH to connect to the CLI the worker in chassis 1 slot 5:
`ssh admin@172.20.120.100 -p2205`

Single chassis or chassis 1 special management port numbers

Slot number	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 1	8001	44301	2301	2201	16101
Slot 2	8002	44302	2302	2202	16102
Slot 3	8003	44303	2303	2203	16103
Slot 4	8004	44304	2304	2204	16104
Slot 5	8005	44305	2305	2205	16105
Slot 6	8006	44306	2306	2206	16106
Slot 7	8007	44307	2307	2207	16107
Slot 8	8008	44308	2308	2208	16108
Slot 9	8009	44309	2309	2209	16109
Slot 10	8010	44310	2310	2210	16110
Slot 11	8011	44311	2311	2211	16111
Slot 12	8012	44312	2312	2212	16112
Slot 13	8013	44313	2313	2213	16113
Slot 14	8014	44314	2314	2214	16114

Chassis 2 special management port numbers

Slot Number	HTTP (80)	HTTPS (443)	Telnet (23)	SSH (22)	SNMP (161)
Slot 1	8021	44321	2321	2221	16121
Slot 2	8022	44322	2322	2222	16122
Slot 3	8023	44323	2323	2223	16123
Slot 4	8024	44324	2324	2224	16124
Slot 5	8025	44325	2325	2225	16125
Slot 6	8026	44326	2326	2226	16126
Slot 7	8027	44327	2327	2227	16127
Slot 8	8028	44328	2328	2228	16128
Slot 9	8029	44329	2329	2229	16129
Slot 10	8030	44330	2330	2230	16130
Slot 11	8031	44331	2331	2231	16131
Slot 12	8032	44332	2332	2232	16132
Slot 13	8033	44333	2333	2233	16133
Slot 14	8034	44334	2334	2234	16134

Example single chassis management IP addresses and port numbers

Use the special port numbers below to manage the devices in an SLBC that includes one or two FortiControllers and multiple workers installed in one chassis with External Management IP address 10.10.10.1:

- To manage the primary worker using HTTPS browse to:
`https://10.10.10.1`
- To manage the FortiController in slot 1 using HTTPS, browse to the following address. This is usually the primary FortiController.
`https://10.10.10.1:44301`
- To manage the FortiController in slot 2 using HTTPS, browse to the following address. This is usually the secondary FortiController and this is the only way to use HTTPS to manage the secondary FortiController.
`https://10.10.10.1:44302`
- To manage the worker in slot 4 using HTTPS browse to:
`https://10.10.10.1:44304`
- To manage the worker in slot 14 using HTTP browse to:
`http://10.10.10.1:8014`
- To manage the worker in slot 12 using SSH, enter a command similar to:
`ssh admin@10.10.10.1 -p2212`
- To manage the worker in slot 5 using telnet, enter a command similar to:
`telnet 10.10.10.1 2305`

- To use SNMP to query the FortiController in slot 1 use port 16101 in the SNMP query.
- To use SNMP to query the FortiController in slot 2 use port 16102 in the SNMP query.
- To use SNMP to query a worker in slot 7 use port 16107 in the SNMP query.

Example management IP addresses and port numbers for two chassis and two or four FortiControllers

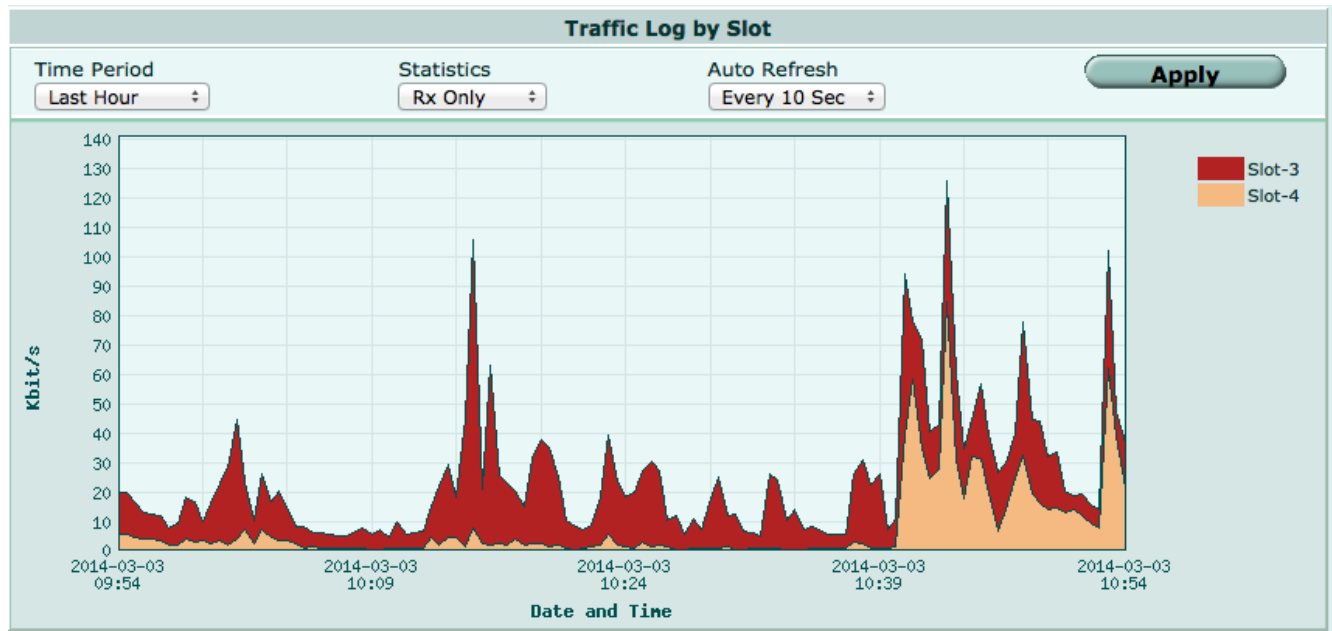
Use the special port numbers below to manage the devices in an SLBC that includes two or four FortiControllers and multiple workers installed in two chassis with External Management IP address 10.10.10.1:

- To manage the primary worker using HTTPS browse to the external management IP address. (This worker may be in chassis 1 or chassis 2.)
`https://10.10.10.1`
- To manage the FortiController in chassis 1 slot 1 using HTTPS, browse to the following address. This is usually the primary FortiController.
`https://10.10.10.1:44301`
- To manage the FortiController in chassis 1 slot 2 using HTTPS, browse to the following address.
`https://10.10.10.1:44302`
- To manage the FortiController in chassis 2 slot 1 using HTTPS, browse to the following address.
`https://10.10.10.1:44321`
- To manage the FortiController in chassis 2 slot 2 using HTTPS, browse to the following address.
`https://10.10.10.1:44322`
- To manage the worker in chassis 1 slot 10 using HTTPS browse to:
`https://10.10.10.1:44310`
- To manage the worker in chassis 2 slot 5 using HTTP browse to:
`http://10.10.10.1:8025`
- To manage the worker in chassis 2 slot 13 using HTTP browse to:
`http://10.10.10.1:8033`
- To manage the worker in chassis 1 slot 8 using SSH, enter a command similar to:
`ssh admin@10.10.10.1 -p2208`
- To manage the worker in chassis 2 slot 5 using telnet, enter a command similar to:
`telnet 10.10.10.1 2325`
- To use SNMP to query the FortiController in chassis 1 slot 1 use port 16101 in the SNMP query.
- To use SNMP to query the FortiController in chassis 2 slot 2 use port 16122 in the SNMP query.
- To use SNMP to query a worker in chassis 1 slot 7 use port 16107 in the SNMP query.
- To use SNMP to query a worker in chassis 2 slot 11 use port 16131 in the SNMP query.

Monitoring the cluster

From the FortiController GUI you can go to **Load Balance > Monitor** to view the amount of traffic processed by each worker according to each worker's slot number. The traffic log displays the amount of data processed by each worker and the Session Count displays the current number of half-sessions being processed by each worker. (The actual

number of sessions is half the number of half-sessions.) You can display the total session count or the pinhole session count.



Worker communication with FortiGuard

Individual workers need to be able to communicate with FortiGuard for anti virus updates, IPS updates, application control updates, FortiGuard web filtering lookups and other FortiGuard services. You can do this by adding a default route to the worker elbc-mgmt VDOM that points at the FortiController internal management interface. This causes each worker to route Internet-bound management traffic over the internal management network. The FortiController then forwards this traffic to the Internet using its default route.

When you add the default route to the primary worker elbc-mgmt VDOM it is synchronized to all of the workers in the cluster.

```
config vdom
  edit elbc-mgmt
    config router static
      set device base-mgmt
      set gateway 10.101.10.1
    end
  end
```

The gateway address is on the same subnet as the FortiController internal management network. If you change the FortiController internal management network you should also change the gateway for this default route. So the default gateway address for this route is 10.101.10.1. If you change the internal management network address to 20.202.20.0, then the gateway for this route would be 20.202.20.1.

Basic cluster NAT/Route mode configuration

When all of the devices have been added to the cluster, configuring the cluster is just like configuring a standalone FortiGate unit operating with multiple VDOMs. When you first log into the primary worker you are logging into a FortiGate unit in multiple VDOM mode.

You can either log into the FortiController GUI and from there go to **Load Balance > Status** and connect to the worker GUI or you can connect directly to the worker primary unit using the **External Management IP/Netmask**.

No additional changes to the FortiController configuration are required. However, you can tune the FortiController configuration, see [Changing load balancing settings on page 50](#)

In the load balanced cluster the workers are configured with two VDOMs:

- **elbc-mgmt** includes the mgmt interface and is used for management traffic. When you connect to the mgmt interface you connect to this VDOM. Normally you do not have to change the configuration of this VDOM.
- **root** includes the fctrl/f1 to fctrl/f8 interfaces. Configure this VDOM to allow traffic through the cluster and to apply UTM and other FortiOS features to the traffic.

By default the root VDOM operates in NAT/Route mode. You can add more VDOMs that operate in NAT/Route or Transparent mode. If you add more VDOMs you must add some of the fctrl/f1 to fctrl/f8 interfaces to each VDOM. You can also add VLAN interfaces and add these interfaces to VDOMs.



FortiController interfaces other than the fctrl/f1 to fctrl/f8 interfaces are visible from the GUI and CLI. In a session-aware load balanced cluster these interfaces are not used for network traffic.

Using the GUI to configure NAT/Route mode

To configure DNS settings

1. Log into the FortiController GUI.
2. Go to **Load Balance > Status** and select the **Config Master** icon beside the primary worker, which is always the top entry in the list.
3. Log into the worker GUI.



You can also connect to the worker GUI by browsing directly to the External Management IP/Netmask.

4. Go to **System > Network > DNS** and configure DNS settings as required.

To configure an interface

1. Go to **Virtual Domains > root**.
2. Go to **System > Network > Interfaces** and Edit an interface (for example, fctrl/f1).
3. Configure the interface as required, for example set the **Addressing Mode** to **Manual** and set the **IP/Netmask** to 172.20.120.10/255.255.255.0.

4. Select **OK**.
5. Repeat for all interfaces connected to networks.

To add a default route

1. Go to **Router > Static** and select Create New and configure the default route:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	fctrl/f1
Gateway	172.20.120.2

2. Select **OK**.

To allow users on the internal network to connect to the Internet

1. Go to **Policy > Policy > Policy** and select Create New to add the following security policy.

Policy Type	Firewall
Policy Subtype	Address
Incoming Interface	fctrl/f2
Source Address	all
Outgoing Interface	fctrl/f1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

2. Select **Enable NAT** and **Use Destination Interface Address**.
3. Select other security policy options as required (for example, add Security Profiles).
4. Select **OK**.

Using the CLI to configure NAT/Route mode

1. Connect to the CLI Using a serial cable to connect the Console port of the primary worker, which would usually be the worker in slot 3.
2. You can also use SSH or Telnet to connect to the External Management IP/Netmask.
3. Configure the primary and secondary DNS server IP addresses.

```
config global
  config system dns
    set primary <dns-server_ip>
    set secondary <dns-server_ip>
  end
end
```

4. Connect to the root VDOM.

```
config vdom
```

```
edit root
```

5. From within the root VDOM, configure the interfaces.

```
config system interface
  edit fctrl/f1
    set ip 172.20.120.10
  next
  edit fctrl/f2
    set ip 10.31.101.40
  end
```

6. Add the default route.

```
config router static
  edit 1
    set device fctrl/f1
    set gateway 172.20.120.2
  end
```

7. Add a security policy.

```
config firewall policy
  edit 1
    set srcintf fctrl/f2
    set scraddr all
    set dstintf fctrl/f1
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
    set nat enable
  end
```

Primary unit (master) selection

SLBC clusters typically consist of multiple FortiControllers and multiple workers. Cluster operation requires the selection of a primary (or master) FortiController and a primary (or master) worker. SLBC primary unit selection is similar to FGCP HA primary unit selection. This section provides some notes about how the primary units are selected.

Selecting the primary FortiController (and the primary chassis)

In a single chassis cluster the FortiController with the longest up time becomes the primary unit (also called the master). If you start configuring the cluster by configuring the FortiController in chassis slot 1 first, this FortiController would typically be the primary unit when the cluster is first up and running. If the FortiController in chassis slot 1 is restarted, its uptime is lower so the FortiController in chassis slot 2 becomes the primary unit.

If the FortiControllers all have the same up time, the FortiController with the lowest serial number becomes the primary unit.

In a two chassis cluster, the FortiController with the highest uptime also becomes the primary FortiController, also making the chassis it is in the primary chassis.

The other factor that contributes to selecting the primary chassis is comparing the number of active workers. The chassis with the most active workers becomes the primary chassis and the primary FortiController in that chassis becomes the primary FortiController for the cluster.

The primary FortiController is the one you log into when you connect to the FortiController management IP address. Configuration changes made to this FortiController are synchronized to the other FortiController(s) in the cluster.

You can change the HA Device Priority of individual FortiControllers. The FortiController with the highest device priority becomes the primary unit. The device priority is not synchronized among all FortiControllers in the cluster so if you want one FortiController to become the primary unit you can set its device priority higher.

Just changing the device priority will not cause the cluster to select a new primary unit. The FortiController with the highest device priority will become the primary unit the next time the cluster negotiates to select a new primary FortiController. You can force the cluster to renegotiate by selecting the Enable Override configuration option. This will cause the cluster to re-negotiate more often. The Enable Override setting is synchronized to all FortiControllers in a cluster.

If it doesn't matter which FortiController becomes the primary unit there is no need to adjust device priorities or select Enable Override. Selecting Enable Override can cause the cluster to negotiate more often, potentially disrupting traffic.

Selecting the primary worker

There are two types of primary worker: the ELBC master and the config master.

- The config master is the worker that you log into using the cluster External Management IP. All configuration changes made to this worker are synchronized to other workers in the cluster. The configuration of this worker is compared to the configurations of the other workers in the cluster by comparing their configuration file checksums. If the checksums are different the configuration of the config master is copied to the worker or workers that are out of synch.
- The ELBC master is the worker that is considered the master by the FortiControllers in the cluster.

You can determine which worker is the ELBC master and which is the config master from the FortiController **Load Balance > Status** GUI page. Usually the same worker will have both primary roles. But not always. The ELBC master is the worker in the lowest slot number that is active. The config master is the in-synch worker with the lowest slot number. If the workers are not in-synch, then the worker with the highest uptime becomes the config master.

Adding and removing workers

You can add a new worker to a functioning cluster at any time. When the worker is added the FortiController starts load balancing sessions to it. The new worker must be running the same firmware build as the workers already in the cluster. However, its configuration does not have to match because when its set to `forticontroller` mode its configuration will be reset to factory defaults. Then when the worker joins the cluster its configuration will be synchronized with the cluster configuration.

You can also remove a worker from a cluster at any time simply by powering down and removing the worker from the chassis. The cluster detects that the worker is removed and will stop sending sessions to it. If a worker fails or is removed the sessions that the worker is processing are lost. However, the cluster load balances new sessions to the remaining workers in the cluster.

If you re-install the missing worker the cluster will detect it and start load balancing sessions to it.



If `nat-source-port` is set to `running-slots` sessions maybe lost or interrupted when you remove or add workers. The full command syntax is:

```
config load-balance settings
    set nat-source-port running-slots
end
```

Adding one or more new workers

1. From the FortiController GUI go to **Load Balance > Config**, edit the membership list and add the slot or slots that you will install the new workers in to the members list.
2. You can also use the following FortiController CLI command (for example, to add workers to slots 8 and 9):

```
config load-balance settings
    config slots
        edit 8
        next
        edit 9
    end
```

3. Insert the new workers into their slots.
4. Connect to each worker's CLI and enter the following command:

```
config system elbc
    set mode forticontroller
end
```

The worker restarts in load balance mode and joins the cluster.

5. To verify that a worker has joined the cluster, from the FortiController GUI go to **Load Balance > Status** and verify that the worker appears in the correct chassis slot.

Removing a worker from a cluster

1. From the FortiController GUI go to **Load Balance > Config**, edit the membership list and move the slot or slots that contain the workers to be removed to the available slots list.

You can also use the following FortiController CLI command (for example, to remove the workers in slots 8 and 9):

```
config load-balance settings
    config slots
        delete 8
        delete 9
    end
```

2. Remove the workers from their slots.
3. To verify that a worker has been removed from the cluster, from the FortiController GUI go to **Load Balance > Status** and verify that the worker does not appear in the chassis and that its chassis slot appears to be empty.

Adding link aggregation (LACP) to an SLBC cluster (FortiController trunks)

Configuring LACP interfaces on an SLBC cluster allows you to increase throughput from a single network by combining two or more physical FortiController interfaces into a single aggregated interface, called a FortiController trunk. You configure LACP interfaces from the FortiController CLI or GUI. LACP interfaces appear on worker GUI and CLI as single FortiController trunk interfaces and you can create routes, firewall policies and so on for them just like a normal physical interface. You can add up to eight FortiController interfaces to an aggregate interface. If you have split an interface, each interface in the split interface is still counted as a single interface.



It is possible to add LACP and other aggregated interfaces from the worker GUI or CLI.

However, you should not do this, because these aggregated interfaces are not recognized by the FortiController and will not function properly.

After combining two FortiController front panel interfaces into an LACP interface, the two front panel interfaces may continue to appear on the worker GUI and CLI. However you should not configure policies or routes or other options for these interfaces.

Adding an aggregated interface

1. Log into the primary FortiController GUI or CLI.
2. Go to **Switch > Fabric Channel** and select **New Trunk**.
3. Enter a Name for the aggregate interface.
4. Set the mode to **LACP Passive** or **LACP Active**.

Do not select **FortiTrunk**. This option is not supported.

Selecting **LACP Passive** creates an 802.3ad passive mode aggregate interface. Selecting LACP Active creates an 802.3ad Active mode aggregate interface. Static mode means the aggregate does not send or receive LACP control messages.

5. Move the FortiController front panel interfaces to add to the aggregate interface to the **Selected** column and select **OK** to add the interface. You can add up to eight interfaces.

From the FortiController CLI:

```
config switch fabric-channel trunk
  edit f1-f2
    set port-select-criteria {dst-ip | src-dst-ip | src-ip}
    set mode {static | lacp-active | lacp-passive}
    set lacp-speed {fast | slow}
    set member-withdrawl-behavior {block | forward}
    set min-links <0-8>
    set members <members>
  end
```

6. Log into the primary worker GUI or CLI.
7. From the GUI go to **Global > Network > Interfaces**.

You should see the LACP interface that you added in the interface list. Its Type as listed on the interface page should be fctrl trunk. When you edit the interface the type is FortiController Trunk. You can configure the interface as required, adding an IP address and so on.

Aggregate interfaces are added the root VDOM by default. You can move them to other VDOMs as required. Once in the correct VDOM, you can create policies and other configuration objects that reference the aggregate interface.

Individual FortiAnalyzer settings on each worker

If the workers are running FortiOS 6.0 or newer, you can use the following command to configure individual workers to send log messages to a different FortiAnalyzer for each worker in your SLBC cluster.

```
config system vdom-exception
  edit 1
    set object {log.fortinalyzer.setting | log.fortianalyzer.override.setting}
    set scope {all | inclusive | exclusive}
    set vdom <vdom-name> [<vdom-name> ...]
  end
```

where:

object is the name of the configuration object that can be configured independently for all VDOMs. Currently you can control the synchronization of FortiAnalyzer settings

scope determines whether the configuration object can be configured separately for all VDOMs or if some VDOMs share the same configuration. Scope can be:

- **all** object configuration is independent for all VDOMs.
- **inclusive** object configuration independent for the listed VDOMs. Other VDOMs use the global configuration.
- **exclusive** use the global object configuration for the listed VDOMs. Other VDOMs can be configured independently.
- **vdom** the name (s) of the VDOMs that are part of the scope.

Configuring different FortiAnalyzer settings for each SLBC worker

Use the following configuration to set different global FortiAnalyzer settings for each SLBC worker. To do this you only have to enter the following command on each worker:

```
config system vdom-exception
  edit 1
    set object log.fortinalyzer.setting
  end
```

Then on each worker use global settings to configure the FortiAnalyzer that the worker sends log messages to. Each worker sends log messages to a different FortiAnalyzer and all VDOMs on each worker send log messages to the globally set FortiAnalyzer.

Configuring different FortiAnalyzer settings for each worker and for the root VDOM of each worker

Use the following configuration to set different global FortiAnalyzer settings for each worker and to also allow the root VDOM of each worker to use a different FortiAnalyzer than the global FortiAnalyzer:

```
config system vdom-exception
  edit 1
```



```
set object log.fortinalyzer.setting
next
edit 2
set object log.fortinalyzer.override.setting
set scope inclusive
set vdom root
end
```

Then on each worker use global settings to configure the FortiAnalyzer that the worker sends log messages to. Also on each worker, edit the root VDOM and configure the FortiAnalyzer that the root VDOM on this worker sends log messages to.

Each worker sends log messages to a different FortiAnalyzer and the root VDOM on each worker sends log messages to a different FortiAnalyzer than the global setting.

Adding VLANs

You can add VLANs to FortiController interfaces from the worker GUI. No FortiController configuration changes are required. Network equipment connected to the physical FortiController interfaces that contain VLANs must be able to pass and handle VLAN traffic.

Adding a VLAN to a FortiController interface

1. Log into the primary worker GUI or CLI.
2. From the GUI go to **System > Network > Interface**.
3. Select **Create New**.
4. Add a **Name** and set the type to **VLAN**.
5. Set **Interface** to one of the FortiController front panel interfaces.
6. Add a **VLAN ID** and configure the rest of the interface settings as required.
7. Select **OK** to save the VLAN interface.

VRRP support

FortiController-5000 SLBC supports the Virtual Router Redundancy Protocol (VRRP), allowing you to configure HA between FortiController-5000 SLBC clusters using VRRP. You can also add a FortiController-5000 SLBC cluster to a VRRP group with other VRRP routers.

You configure VRRP on the FortiController-5000 by creating a VRRP group and adding one or more FortiController front panel interfaces to the group. During normal operation, the primary FortiController sends outgoing VRRP routing advertisements. Both the primary and backup FortiControllers listen for incoming VRRP advertisements from other routers in the VRRP group. If the primary FortiController fails, the new primary FortiController takes over the role of both sending and receiving VRRP advertisements, maintaining the FortiController-5000 cluster within the VRRP group.

FGCP to SLBC migration

This section describes how to convert a FortiGate Clustering Protocol (FGCP) virtual cluster (with VDOMs) to an SLBC cluster. The conversion involves replicating the VDOM, interface and VLAN configuration of the FGCP cluster on the SLBC cluster primary worker then backing up the configuration of each FGCP cluster VDOM. Each of the VDOM configuration files is manually edited to adjust interface names among other things. Then these modified VDOM configuration files are restored to the corresponding SLBC cluster primary worker VDOMs.

Only VDOM configurations are migrated. You have to manually configure primary worker management and global settings.

This section describes general conversion steps and does not include configuration specifics, CLI syntax, or GUI procedures.

Assumptions

- The FGCP cluster and the SLBC workers must be running the same firmware version. If required, you can upgrade the FGCP cluster or SLBC worker firmware before or after the conversion.
- This example assumes that VDOMs are enabled on the FGCP cluster. The FGCP cluster must have VDOMs enabled for this conversion to work because SLBC cluster workers have VDOMs enabled. You can transfer the configuration from one VDOM to another but you can't transfer the configuration of an FGCP cluster without VDOMs enabled to a VDOM in an SLBC cluster worker. (If your FGCP cluster does not have multiple VDOMs enabled you could enable VDOMs on the FGCP cluster and add all configuration elements to the root VDOM but this would essentially mean re-configuring the FGCP cluster in which case it would make more sense to re-configure the SLBC workers.)
- Both clusters are operating, once the SLBC workers are configured you can divert traffic to the SLBC cluster and then take the FGCP cluster out of service.
- The FGCP cluster units do not have to be the same model as the SLBC cluster workers.
- The SLBC workers have been registered and licensed.

Conversion steps

1. Add VDOM(s) to the SLBC primary worker with names that match those of the FGCP cluster.
2. Map FGCP cluster interface names to SLBC primary worker interfaces names. For example you could map the FGCP cluster port1 and port2 interfaces to the SLBC primary worker fctl/f1 and fctl/f2 interfaces. You can also include aggregate interfaces in this mapping and you can also map FGCP cluster interfaces to SLBC trunks.
3. Add interfaces to the SLBC primary worker VDOMs according to your mapping. This includes moving SLBC physical interfaces into the appropriate VDOMs, creating aggregate interfaces, and creating SLBC trunks if required.
4. Add VLANs to the SLBC primary worker that match VLANs in the FGCP cluster. They should have the same names as the FGCP VLANs, be added to the corresponding SLBC VDOMs and interfaces, and have the same VLAN IDs.
5. Add inter-VDOM links to the SLBC primary worker that match the FGCP cluster.
6. Backup the configuration of each FGCP cluster VDOM.
7. Backup the configuration of each SLBC primary worker VDOM.
8. Use a text editor to replace the first 4 lines of each FGCP cluster VDOM configuration file with the first four lines of the corresponding SLBC primary worker VDOM configuration file. Here are example lines from an SLBC primary worker VDOM configuration file:

```
#config-version=FG-5KB-5.02-FW-build670-150318:opmode=0:vdom=1:user=admin
#conf_file_ver=2306222306838080295
#buildno=0670
#global_vdom=0:vd_name=VDM1
```

9. With a text editor edit each FGCP cluster VDOM configuration file and replace all FGCP cluster interface names with the corresponding SLBC worker interfaces names according to the mapping you created in step 2.
10. Set up a console connection to the SLBC primary worker to check for errors during the following steps.
11. From the SLBC primary worker, restore each FGCP cluster VDOM configuration file to each corresponding SLBC primary worker VDOM.
12. Check the following on the SLBC primary worker:
 - Make sure `set type fctrl-trunk` is enabled for SLBC trunk interfaces.
 - Enable the global and management VDOM features that you need including SNMP, logging, connections to FortiManager, FortiAnalyzer, and so on.
 - If there is a FortiController in chassis slot 2, make sure the worker base2 interface status is up.
 - Remove `snmp-index` entries for each interface.
 - Since you can manage the workers from the FortiController you can remove management-related configurations using the worker `mgmt1` and `mgmt2` interfaces (Logging, SNMP, admin access, etc.) if you are not going to use these interfaces for management.

Updating SLBC firmware

After you have registered your FortiControllers and workers you can download the most recent FortiController and FortiOS firmware from the support web site <https://support.fortinet.com>. Select the **FortiSwitchATCA** product.

You can upgrade the worker firmware from the primary worker GUI or CLI. Upgrading the primary worker firmware also upgrades the firmware of all of the FortiControllers in the cluster. In a two chassis configuration the process is a bit more complex. See [Updating SLBC firmware on page 43](#).

You can upgrade the FortiController firmware from the primary FortiController GUI or CLI. Upgrading the primary FortiController firmware also upgrades the firmware of all of the FortiControllers in the cluster in one operation. This also works for a two chassis cluster.

When you upgrade workers or FortiControllers, the cluster upgrades the secondary workers or FortiControllers first. Once the all of the secondary units have been upgraded the primary worker or FortiController is upgraded.

Worker and FortiController firmware can be upgraded independently as long as the firmware running your FortiControllers supports the FortiOS firmware that you are upgrading the workers to. If you need to upgrade both the workers and the FortiControllers you should upgrade the workers first unless stated otherwise in the FortiSwitch ATCA release notes.



Upgrading FortiController and worker firmware may briefly interrupt network traffic so if possible this should be done during a quiet period.

The command output provides the same information as the **Load Balance > Status** page, including the slot that contains the primary unit (slot 3), the number of workers in the cluster, the slots containing all of the workers (3, 4, and 6) and the status of each. Status information includes the status of the connection between the FortiController and the base and fabric backplanes, whether the heartbeat is active, the status of the FortiController and the data processed by it. The status message can also indicate if the FortiController is waiting for a fabric connection or waiting for a base connection.

You can also use the following commands to display detailed session aware load balancing diagnostics:

```
diagnose SLBC {dp | tcam-rules}
```

The `dp` option provides diagnostics for the DP processors and the `tcam-rules` option provides diagnostics for content aware routing rules (TCAM).

Upgrading a single-chassis cluster

To upgrade single-chassis cluster worker firmware

This procedure upgrades the firmware running on all of the workers in a single operation.

1. Log into the primary worker GUI.
2. From the **Global System Information** dashboard widget beside **Firmware Version** select **Update**.
3. Select the new firmware file and select OK.

The firmware image file is uploaded and verified then installed on all of the workers. After a few minutes the cluster continues operating, the workers running the new firmware build.

You can confirm that all of the workers are back in the cluster from the FortiController **Load Balance > Status** page.

To upgrade single-chassis cluster FortiController firmware

This procedure upgrades the firmware running on all of the FortiControllers in a single operation.

1. Log into the FortiController GUI.
2. From the **System Information** dashboard widget beside **Firmware Version** select **Update**.
3. Select the new firmware file and select OK.

The firmware image file is uploaded and verified then installed on all the FortiControllers. After a few minutes the cluster continues operating.

4. You can confirm that all of the FortiControllers and workers are back in the cluster and operating normally from the **Load Balance > Status** page of the FortiController GUI.

Upgrading a two-chassis cluster

Use the following multi-step process to upgrade worker firmware in a two-chassis cluster.

1. Log into the primary worker GUI.
2. From the **Global System Information** dashboard widget beside **Firmware Version** select **Update**.
3. Select the new firmware image file and select **OK**.

The firmware image file is uploaded and verified then installed on all of the workers in the secondary chassis. The primary chassis continues processing traffic.

From console connections to the workers in the primary chassis you can see messages indicating that they are waiting for their chassis to become the secondary chassis so that they can upgrade their firmware.

From console connections to the workers in the secondary chassis you can see them upgrade their firmware and restart.

4. Once all of the workers in the secondary chassis have upgraded their firmware and restarted, log into the primary FortiController CLI and enter the following command to force the primary chassis to become the secondary chassis:

```
diagnose system ha force-slave-state by-chassis <delay> <chassis-number>
```

For example, if chassis 1 is the primary chassis, enter the following command:

```
diagnose system ha force-slave-state by-chassis 10 1
```

This command waits 10 seconds, then forces chassis 1 to become the secondary chassis, resulting in chassis 2 becoming the primary chassis.

The workers in the new primary chassis process all network traffic. And the workers in the new secondary chassis upgrade their firmware.

The workers in the primary chassis can wait up to 20 minutes to become the secondary chassis and upgrade their firmware. If the primary chassis does not become the secondary chassis within 20 minutes, all worker firmware is restored to the original version.

5. After the firmware on all of the workers is upgraded you should clear the force slave state using the following command:

```
diagnose system ha force-slave-state by-chassis clear
```

6. You can confirm that all of the workers are back in the cluster from the FortiController **Load Balance > Status** page.

To upgrade two chassis cluster FortiController firmware

This procedure upgrades the firmware running on the FortiControllers in a single operation.

1. Log into the primary FortiController GUI.
2. From the **System Information** dashboard widget beside **Firmware Version** select **Update**.
3. Select the new firmware file and select **OK**.

The firmware image file is uploaded and verified then installed on all the FortiControllers. After a few minutes the cluster continues operating.

You can confirm that all of the FortiControllers and workers are back in the cluster and operating normally from the FortiController **Load Balance > Status** page.

Verifying the configuration and the status of the units in the cluster

Use the following command from the FortiController CLI to verify that the primary FortiController can communicate with all of the workers and to show the status of each worker. For example, for a cluster that includes 2 workers the command output would be the following if the cluster is operating properly:

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]

Slot  3: Status:Working  Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot  4: Status:Working  Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot  5: Status:Working  Function:Active
```

```
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message: "Running"
```

The command output provides the same information as the **Load Balance > Status** page, including the slot that contains the primary unit (slot 3), the number of workers in the cluster, the slots containing all of the workers (3, 4, and 6) and the status of each. Status information includes the status of the connection between the FortiController and the base and fabric backplanes, whether the heartbeat is active, the status of the FortiController and the data processed by it. The status message can also indicate if the FortiController is waiting for a fabric connection or waiting for a base connection.

You can also use the following commands to display detailed session aware load balancing diagnostics:

```
diagnose SLBC {dp | tcam-rules}
```

The `dp` option provides diagnostics for the DP processors and the `tcam-rules` option provides diagnostics for content aware routing rules (TCAM).

Configuring communication between FortiControllers

SLBC clusters consisting of more than one FortiController use the following types of communication between FortiControllers to operate normally:

- **Heartbeat** communication allows the FortiControllers in the cluster to find each other and share status information. If a FortiController stops sending heartbeat packets it is considered down by other cluster members. By default heartbeat traffic uses VLAN 999.
- **Base control** communication between FortiControllers on subnet 10.101.11.0/255.255.255.0 using VLAN 301.
- **Base management** communication between FortiControllers on subnet 10.101.10.0/255.255.255.0 using VLAN 101.
- **Session synchronization** between FortiControllers in different chassis so that if one FortiController fails another can take its place and maintain active communication sessions. FortiController-5103B session sync traffic uses VLAN 2000. FortiController-5903C and FortiController-5913C session sync traffic between the FortiControllers in slot 1 uses VLAN 1900 and between the FortiControllers in slot 2 uses VLAN 1901. You cannot change these VLANs. Session sync synchronizes sessions between workers that have the same slot-id (e.g. chassis 1 slot 3 to chassis 2 slot 3). As a result of enabling session-sync if a fail-over occurs, the SLBC will use a best effort approach to maintain existing sessions.

If a cluster contains more than one FortiController you must connect their front panel B1 and B2 interfaces together for heartbeat and base control and management communication. You can also use the front panel Mgmt interface for this configuration.

A cluster with two chassis must include session synchronization connections among all of the FortiControllers.

- For the FortiController-5103B you must connect one of the front panel F1 to F8 interfaces of all of the FortiController-5103Bs together. For example, in a FortiController-5103B cluster with two chassis you can connect the F8 interfaces of the FortiControllers in the cluster together.
- For the FortiController-5903C and FortiController-5913C cluster you use the B1 and B2 interfaces for session synchronization connections.

See the two-chassis examples in this document for details. The requirements for these session sync connections depend on the type of cluster.

- In a two chassis A-P mode cluster with two or four FortiController-5103Bs, the session sync ports of all FortiController-5103Bs (for example F8) must be connected to the same broadcast domain by connecting all of the F8 interfaces to the same switch.
- In a FortiController-5103B two chassis dual mode cluster, session sync ports need to be 1-to-1 connected according to chassis slot. So F8 from the FortiController-5103Bs in chassis 1 slot 1 needs to be connected to F8 in chassis 2 slot 1. And, F8 in chassis 1 slot 2 needs to be connected to F8 in chassis 2 slot 2. Because these are 1 to 1 connections you can use patch cables to connect them. You can also make these connections through a switch.
- In a two chassis A-P or dual mode cluster with two or four FortiController-5903Cs or FortiController-5913Cs, all of the B1 interfaces must all be connected to the same 10 Gbps switch. All of the B2 interfaces must all be connected to a different 10 Gbps switch. Connecting the B1 and B2 interfaces to the same switch is not recommended because it requires a double-tagging VLAN configuration.

Network equipment carrying this communication must be able to handle the traffic. This traffic uses VLANs and specific subnets so you may have to configure the network equipment to allow this communication.

Changing the base control subnet and VLAN

You can change the base control subnet and VLAN from the FortiController CLI. For example to change the base control subnet to 10.122.11.0/255.255.255.0 and the VLAN ID to 320:

```
config load-balance setting
  set base-ctrl-network 10.122.11.0 255.255.255.0
  config base-ctrl-interfaces
    edit b1
      set vlan-id 320
    next
    edit b2
      set vlan-id 320
    end
  end
```

If required, you can use different VLAN IDs for the B1 and B2 interface.

Changing this VLAN only changes the VLAN used for base control traffic between chassis. Within a chassis the default VLAN is used.

Changing the base management subnet and VLAN

You can change the base management subnet from the FortiController GUI by going to **Load Balance > Config** and changing the **Internal Management Network**.

You can also change the base management subnet and VLAN ID from the FortiController CLI. For example, use the following command to change the base management subnet to 10.121.10.0 and the VLAN to 131:

```
config load-balance setting
  set base-mgmt-internal-network 10.121.10.0 255.255.255.0
  config base-mgt-interfaces
    edit b1
      set vlan-id 131
    next
    edit b2
      set vlan-id 131
    end
```

If required, you can use different VLAN IDs for the B1 and B2 interface.

Changing this VLAN only changes the VLAN used for base management traffic between chassis. Within a chassis the default VLAN is used.

Changing the heartbeat VLAN

To change the VLAN from the FortiController GUI, from the **System Information** dashboard widget, beside **HA Status**, select **Configure**. Change the **VLAN to use for HA heartbeat traffic(1-4094)** setting.

You can also change the heartbeat VLAN ID from the FortiController CLI. For example, to change the heartbeat VLAN ID to 333:

```
config system ha
    set hbdev-vlan-id 333
end
```

Using the FortiController-5103B mgmt interface as a heartbeat interface

The FortiController-5103B can use the following command to add the mgmt interface to the list of heartbeat interfaces used. This example adds the mgmt interface for heartbeats to the B1 and B2 interfaces. The B1 and B2 ports are recommended because they are 10G ports and the Mgmt interface is a 100Mb interface.

```
config system ha
    set hbdev b1 b2 mgmt
end
```

Changing the heartbeat interface mode

By default, only the first heartbeat interface (usually B1) is used for heartbeat traffic. If this interface fails on any of the FortiControllers in a cluster, then the second heartbeat interface is used (B2).

You can use the following command to simultaneously use all heartbeat interfaces for heartbeat traffic:

```
config load-balance-setting
    set base-mgmt-interface-mode active-active
end
```

Enabling session sync and configuring the session sync interface

In a two chassis configuration you can use the following command to enable session synchronization:

```
config load-balance setting
    set session-sync enable
end
```

Then for the FortiController-5103B you need to use the following command to select the interface to use for session sync traffic. The following example, sets the FortiController-5103B session sync interface to F4:

```
config system ha
    set session-sync-port f4
end
```

The FortiController-5903C and FortiController-5913C use b1 and b2 as the session sync interfaces so no configuration changes are required.

Changing load balancing settings

The default load balance configuration provides optimal performance for most network traffic and most requirements. A number of load balance settings are available to change how packets and sessions are processed by the cluster. These changes may be required for certain traffic types or to optimize performance for your configuration.

Tuning TCP load balancing performance (TCP local ingress)

TCP packets pass through the FortiController twice: first on ingress when the packet is received from the network by the FortiController front panel interface and a second time on egress after the packet leaves a worker and before it exits from a FortiController front panel interface to the network. New TCP sessions can be added to the DP processor session table on ingress or on egress. By default they are added on egress. Adding sessions on egress makes more efficient use of DP processor memory because sessions that are denied by worker firewall policies are not added to the DP processor session table. As a result the SLBC cluster can support more active sessions.

Adding sessions to the session table on egress has a limitation: round-robin load balancing does not work. If you need round-robin load balancing you must configure the cluster to add sessions to the DP processor on ingress by entering the following command:

```
config load-balance session-setup
    set tcp-ingress enable
end
```

Round-robin load balancing is now supported; but, since sessions are added to the DP processor before filtering by worker firewall policies, some of these sessions may subsequently be denied by these firewall policies. These denied sessions remain in session table taking up memory until they time out.

In addition, adding sessions on ingress means that the FortiController is potentially open to DDOS attacks that could be prevented by worker firewall policies.

In most cases, the default configuration of disabling TCP local ingress should be maintained. However, if you need to use round-robin load balancing you can enable TCP local ingress as long as you are aware of the limitations of this configuration.

For details about the life of a TCP packet, see [Life of a TCP packet on page 55](#).

Tuning UDP load balancing (UDP local ingress and UDP remote/local session setup)

Similar to TCP packets, UDP packets also pass through the FortiController twice: first on ingress when the packet is received from the network by the FortiController front panel interface and a second time on egress after the packet leaves a worker and before it exits from a FortiController front panel interface to the network.

Just like TCP sessions, by default new UDP sessions are added to the DP processor session table on egress. You can also enable UDP local ingress to add sessions to the DP processor on ingress using the following command:

```
config load-balance session-setup
  set udp-ingress enable
end
```

or from the FortiController GUI by going to **Load Balance > Session > Setup > UDP Local Ingress**.

On egress, UDP packets are not handled the same way as TCP packets. UDP Packets are transmitted directly from the FortiController fabric backplane interface to the FortiController front panel interface, bypassing the DP processor. The workers update the DP processor UDP session table by sending worker-to-FortiController remote setup session helper packets.

You can change this on egress behavior by adjusting the UDP remote/local session setup. The default setting is remote. If you change the setting to local, both incoming and outgoing UDP sessions are forwarded by the DP processor; effectively doubling the number of UDP sessions that the DP processor handles. Doubling the session load on the DP processor can create a performance bottleneck.

You can switch UDP remote/local session setup to local if you experience errors with UDP traffic. In practice; however, remote mode provides better performance without causing errors.

You can change UDP remote/local session setup with the following command:

```
config load-balance session-setup
  set udp-session local
end
```

or from the FortiController GUI by going to **Load Balance > Session > Setup > UDP Session Setup**.

For details about the life of a UDP packet, see [Life of a UDP packet on page 57](#).

Changing the load distribution method

Go to **Load Balance > Session > Setup > Load Distribution** to change the load distribution method used by the cluster. The default load distribution method is src-dst-ip-sport-dport which means sessions are identified by their source address and port and destination address and port.

You can change the load distribution method using the following CLI command:

```
config load-balance session-setup
  set load-distribution {round-robin | src-ip | dst-ip | src-dst-ip | src-ip-sport | dst-
    ip-dport | src-dst-ip-sport-dport}
end
```

The following load balancing schedules are also available:

round-robin	Directs new requests to the next slot regardless of response time or number of connections. Round robin is only supported if TCP or UDP local ingress is enabled.
src-ip	The traffic load is distributed across all slots according to source IP address.
dst-ip	The traffic load is statically distributed across all slots according to destination IP address.
src-dst-ip	The traffic load is distributed across all slots according to the source and destination IP addresses.
src-ip-sport	The traffic load is distributed across all slots according to the source IP address and

	source port.
dst-ip-dport	The traffic load is distributed across all slots according to the destination IP address and destination port.
src-dst-ip-sport-dport	The traffic load is distributed across all slots according to the source and destination IP address, source port, and destination port. This is the default load balance schedule and represents true session-aware load balancing.

TCP and UDP local ingress session setup and round robin load balancing

By default TCP and UDP local ingress is set to disable and sessions are added to the load balancer memory only after they are accepted by worker firewall policies. This setting results in improved performance because fewer sessions are recorded and managed by the load balancer so the load balancer has more memory available to handle more accepted sessions.

Enabling local ingress session setup also means a cluster is more vulnerable to DDOS attacks because the cluster is processing more sessions and because FortiGate DDOS protection cannot block DDOS attacks before they are recorded by the load balancer.

However, disabling local ingress session setup means that round-robin load distribution is not supported.

So in general, unless you need to use round-robin load distribution you should leave TCP and UDP local ingress set to disable.

Changing how UDP sessions are processed by the cluster

Go to **Load Balance > Session > Setup > Session Setup** to change how the cluster handles UDP sessions. UDP session setup can be set to remote or local.

On the CLI the configuration is:

```
config load-balance session-setup
  set udp-ingress-setup disable
  set udp-session-setup {local | remote}
end
```

- In local mode, UDP sessions are setup locally on the FortiController. All types of UDP traffic are supported by local mode.
- In remote mode, UDP sessions are setup on individual workers in the cluster. Remote mode results in better performance but some types of UDP traffic are not supported by remote mode.

Remote should work in most configurations, but for some configurations you may have to change the setting to local. For example, if the load distribution method is set to round-robin unidirectional UDP packets in a session may be distributed to different chassis slots. For some UDP protocols this will cause problems.

You should also enable local mode if the cluster processes non-symmetric UDP traffic no matter what the distribution method is.

Tuning load balancing performance: fragmented sessions

Go to **Load Balance > Session > Setup > Session Performance** to control how the cluster handles fragmented sessions.

From the CLI the configuration is:

```
config load-balance session-setup
  set fragment-sessions enable
end
```

Changing this setting has no effect. Sending fragmented packets to the DP processors is disabled in the current release.

Changing session timers

Go to **Load Balance > Session > Timer** to view and change load balancing session timers. These timers control how long the FortiController waits before closing a session or performing a similar activity. In most cases you do not have to adjust these timers, but they are available for performance tuning. The range for each timer is 1 to 15,300 seconds.

Use the following command to change these timers from the CLI:

```
config load-balance session-age
  set fragment 120
  set pin-hole 120
  set rsync 300
  set tcp-half-close 125
  set tcp-half-open 125
  set tcp-normal 3605
  set tcp-timewait 2
  set udp 185
end
```

Four of these FortiController timers have corresponding timers in the FortiGate-5000 configuration. The FortiController timers must be set to values greater than or equal to the corresponding FortiGate-5000 timers.

The worker timers are (default values shown):

```
config global
  config system global
    set tcp-halfclose-timer 120
    set tcp-halfopen-timer 120
    set tcp-timewait-timer 1
    set udp-idle-timer 180
  end
```

The following timers are supported:

age-interval tcp normal	The time to wait without receiving a packet before the session is considered closed. Default 3605 seconds.
age-interval tcp timewait	The amount of time that the FortiController keeps normal TCP sessions in the TIME_WAIT state. Default is 2 seconds.
age-interval tcp half-open	The amount of time that the FortiController keeps normal TCP sessions

	in the HALF_OPEN state. Default is 125 seconds.
age-interval tcp half-close	The amount of time that the FortiController keeps normal TCP sessions in the HALF_CLOSE state. Default is 125 seconds.
age-interval udp	The amount of time that the FortiController keeps normal UDP sessions open after a packet is received. Default is 185 seconds.
age-interval pin-hole	The amount of time that the FortiController keeps pinhole sessions open. Default is 120 second.
age-interval rsync	When two FortiControllers are operating in HA mode, this timer controls how long a synced session can remain on the subordinate unit due to inactivity. If the session is active on the primary unit, rsync updates the session on the subordinate unit. So a long delay means the session is no longer active and should be removed from the subordinate unit. Default is 300 seconds.
age-interval fragment	To track fragmented frames, the FortiController creates fragmented sessions to track the individual fragments. Idle fragmented sessions are removed when this timer expires. Default is 120 seconds.

Life of a TCP packet

This section describes the life of a TCP packet and related sessions as it passes through a SLBC cluster. The life of a packet is affected by TCP load balancing settings (see [Tuning TCP load balancing performance \(TCP local ingress\)](#) on page 50).

Life of a TCP packet (default configuration: TCP local ingress disabled)

Here is what can happen when a TCP packet enters a SLBC cluster with the default load balancing configuration (TCP local ingress disabled):

1. A TCP packet is received by a FortiController front panel interface.
2. The DP processor looks up the packet in its session table and one of the following happens:
 - If the packet is part of an established session it is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of the worker that is processing the session. The packet is then processed by the worker and exits the worker's fabric backplane interface.
 - If the packet is starting a new session it is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of a worker. The worker is selected by the DP processor based on the load distribution method. The worker applies FortiGate firewall policies and accepts the packet. The packet is processed by the worker and exits the worker's fabric backplane interface.
 - If the packet is starting a new session it is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of a worker. The worker is selected by the DP processor based on the load distribution method. The worker applies FortiGate firewall policies and denies the session. The packet is dropped.
3. Accepted packets are received by the FortiController backplane interface.
 - If the packet is part of an established session the DP processor records the packet as part of an established session.
 - If the packet is starting a new session, the DP processor adds the new session to its session table.
4. The packets exit the cluster through a FortiController front panel interface.
 - The DP processor session table contains sessions accepted by worker firewall policies. These sessions expire and are removed from the table when no new packets have been received for that session by the TCP session timeout.

Life of a TCP packet (TCP local ingress enabled)

With TCP local ingress enabled the life of a TCP packet looks like this:

1. A TCP packet is received by a FortiController front panel interface.
2. The DP processor looks up the packet in its session table and one of the following happens:
 - If the packet is part of an established session it is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of the worker that is processing the session. The packet is then

processed by the worker and exits the worker's fabric backplane interface.

If the packet is starting a new session the new session is added to the DP processor session table. The packet is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of a worker. The worker is selected by the DP processor based on the load distribution method. The worker applies FortiGate firewall policies and accepts the packet. The packet is processed by the worker and exits the worker's fabric backplane interface.

If the packet is starting a new session the new session is added to the DP processor session table. The packet is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of a worker. The worker is selected by the DP processor based on the load distribution method. The worker applies FortiGate firewall policies and denies the packet. The packet is blocked by the worker.

3. Accepted packets are received by the FortiController backplane interface and recorded by DP processor as part of an established session.
4. The packets exit the cluster through a FortiController front panel interface.

The DP processor session table contains sessions accepted by and denied by worker firewall policies. These sessions expire and are removed from the table when no new packets have been received for that session by the TCP session timeout.

Life of a UDP packet

This section describes four variations on the life of a UDP packet and related sessions as it passes through a SLBC cluster. The life of a packet is affected by UDP load balancing settings (see [Tuning UDP load balancing \(UDP local ingress and UDP remote/local session setup\)](#) on page 50).

Life of a UDP packet (default configuration: UDP local ingress disabled and UDP remote session setup)

Here is what can happen when a UDP packet enters a SLBC cluster with the default load balancing configuration (UDP local ingress disabled and UDP remote/local session setup set to remote):

1. A UDP packet is received by a FortiController front panel interface.
2. The DP processor looks up the packet in its session table and one of the following happens:
 - If the packet is part of an established session it is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of the worker that is processing the session. The packet is then processed by the worker and exits the worker's fabric backplane interface. The packet is received by the FortiController fabric backplane interface and then exits the cluster from a FortiController front panel interface.
 - If the packet is starting a new session it is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of a worker. The worker is selected by the DP processor based on the load distribution method. The worker applies FortiGate firewall policies and accepts the packet. The packet is processed by the worker and exits the worker's fabric backplane interface. The packet is received by the FortiController fabric backplane interface and then exits the cluster from a FortiController front panel interface
 - If the packet is starting a new session it is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of a worker. The worker is selected by the DP processor based on the load distribution method. The worker applies FortiGate firewall policies and denies the session. The packet is blocked by the worker.
3. Accepted packets are received by the FortiController backplane interface.
4. Using worker-to-FortiController session setup helper packets, the workers send session updates for established sessions and new sessions to the DP processor.
5. The packets exit the cluster through a FortiController front panel interface.
 - The DP processor session table contains sessions accepted by worker firewall policies. These sessions expire and are removed from the table when no new packets have been received for that session by the UDP session timeout.

Life of a UDP packet (UDP local ingress disabled and UDP local session setup)

Here is what can happen when a UDP packet enters a SLBC cluster with UDP local ingress disabled and UDP remote/local session setup set to local:

A UDP packet is received by a FortiController front panel interface.

The DP processor looks up the packet in its session table and one of the following happens:

If the packet is part of an established session it is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of the worker that is processing the session. The packet is then processed by the worker and exits the worker's fabric backplane interface.

If the packet is starting a new session it is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of a worker. The worker is selected by the DP processor based on the load distribution method. The worker applies FortiGate firewall policies and accepts the packet. The packet is processed by the worker and exits the worker's fabric backplane interface.

If the packet is starting a new session it is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of a worker. The worker is selected by the DP processor based on the load distribution method. The worker applies FortiGate firewall policies and denies the session. The packet is blocked by the worker.

Accepted packets are received by the FortiController backplane interface.

If the packet is part of an established session the DP processor records the packet as part of an established session.

If the packet is starting a new session, the DP processor adds the new session to its session table.

The packets exit the cluster through a FortiController front panel interface.

The DP processor session table contains sessions accepted by worker firewall policies. These sessions expire and are removed from the table when no new packets have been received for that session by the UDP session timeout.

Life of a UDP packet (UDP local ingress enabled and UDP remote session setup)

With UDP local ingress enabled and UDP session setup set to remote, the life of a UDP packet looks like this:

1. A UDP packet is received by a FortiController front panel interface.
2. The DP processor looks up the packet in its session table and one of the following happens:
 - If the packet is part of an established session it is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of the worker that is processing the session. The packet is then processed by the worker and exits the worker's fabric backplane interface.
 - If the packet is starting a new session the new session is added to the DP processor session table. The packet is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of a worker. The worker is selected by the DP processor based on the load distribution method. The worker applies FortiGate firewall policies and accepts the packet. The packet is processed by the worker and exits the worker's fabric backplane interface.
 - If the packet is starting a new session the new session is added to the DP processor session table. The packet is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of a worker. The worker is selected by the DP processor based on the load distribution method. The worker applies FortiGate firewall policies and denies the packet. The packet is blocked by the worker.
3. Accepted packets are received by the FortiController backplane interface.
4. Using worker-to-FortiController heartbeats, the workers send session updates for established sessions and new sessions to the DP processor.
5. The packets exit the cluster through a FortiController front panel interface.
 - The DP processor session table contains sessions accepted by and denied by worker firewall policies. These sessions expire and are removed from the table when no new packets have been received for that session by the UDP session timeout.

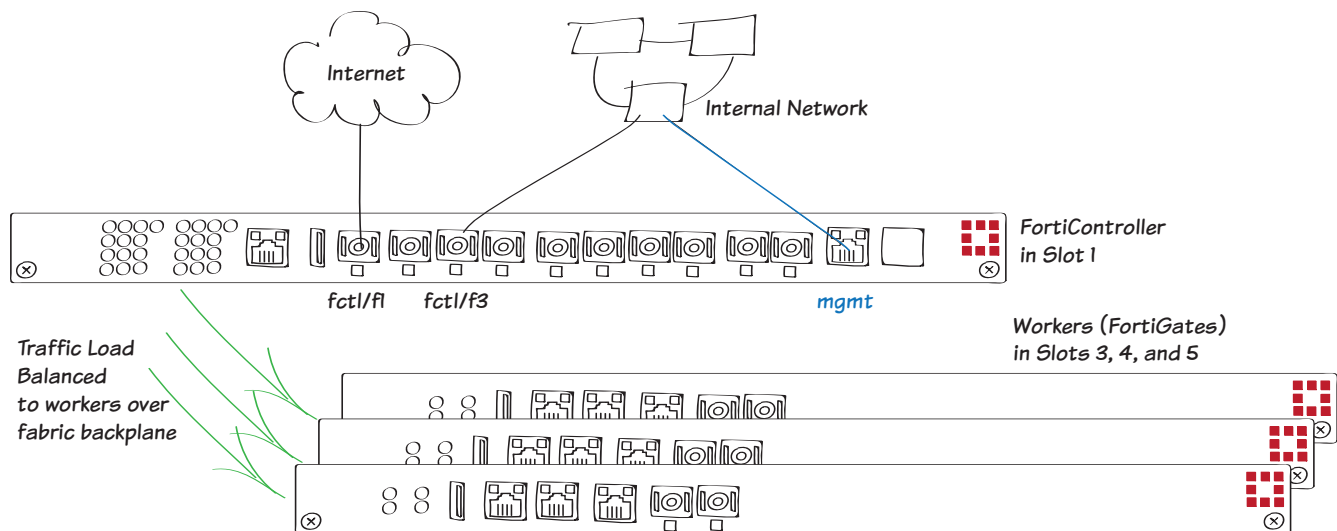
Life of a UDP packet (UDP local ingress enabled and UDP local session setup)

With UDP local ingress enabled and UDP session setup set to local, the life of a UDP packet looks like this:

1. A UDP packet is received by a FortiController front panel interface.
2. The DP processor looks up the packet in its session table and one of the following happens:
 - If the packet is part of an established session it is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of the worker that is processing the session. The packet is then processed by the worker and exits the worker's fabric backplane interface.
 - If the packet is starting a new session the new session is added to the DP processor session table. The packet is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of a worker. The worker is selected by the DP processor based on the load distribution method. The worker applies FortiGate firewall policies and accepts the packet. The packet is processed by the worker and exits the worker's fabric backplane interface.
 - If the packet is starting a new session the new session is added to the DP processor session table. The packet is forwarded to the FortiController fabric backplane interface and from there to the fabric backplane interface of a worker. The worker is selected by the DP processor based on the load distribution method. The worker applies FortiGate firewall policies and denies the packet. The packet is blocked by the worker.
3. Accepted packets are received by the FortiController backplane interface and recorded by DP processor as part of an established session.
4. The packets exit the cluster through a FortiController front panel interface.
 - The DP processor session table contains sessions accepted by and denied by worker firewall policies. These sessions expire and are removed from the table when no new packets have been received for that session by the UDP session timeout.

SLBC with one FortiController-5103B

This example describes the basics of setting up a Session-aware Load Balancing Cluster (SLBC) that consists of one FortiController-5103B, installed in chassis slot 1, and three FortiGate-5001C workers, installed in chassis slots 3, 4, and 5. This SLBC configuration can have up to eight 10Gbit network connections.



Setting up the hardware

1. Install a FortiGate-5000 series chassis and connect it to power.
2. Install the FortiController in slot 1.
3. Install the workers in slots 3, 4, and 5.
4. Power on the chassis.
5. Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally.
To check normal operation LED status see the [FortiGate-5000 hardware guides](#) and [FortiController hardware guides](#).
6. Check the [FortiController release notes](#) for the latest supported FortiController and FortiGate firmware.
7. Get FortiController and FortiOS firmware from the [Fortinet Support site](#).
For FortiController firmware, select the **FortiSwitchATCA** product.

Configuring the FortiController

1. Connect to the FortiController GUI (using HTTPS) or CLI (using SSH) using the default IP address 192.168.1.99.
Or connect to the FortiController CLI through the console port (Baud Rate 9600bps, Data bits 8, Parity None, Stop bits 1, and Flow Control None).

2. Login using the admin administrator account and no password.
3. Add a password for the admin administrator account. From the GUI use the **Administrators** widget or from the CLI enter this command.

```
config admin user
  edit admin
    set password <password>
  end
```

4. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
  edit mgmt
    set ip 172.20.120.151/24
  end
```

5. If you need to add a default route for the management IP address, enter this command.

```
config route static
  edit route 1
    set gateway 172.20.120.2
  end
```

6. Set the chassis type that you are using, for example:

```
config system global
  set chassis-type fortigate-5140
end
```

7. From the GUI, go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. Since the workers have not been configured yet their status is **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.

Worker Blade	Role	Weight	Status	
Slot #3	Active	5	Down	[Delete] [Edit] [Add]
Slot #4	Active	5	Down	[Delete] [Edit] [Add]
Slot #5	Active	5	Down	[Delete] [Edit] [Add]

You can also enter the following CLI command to add slots 3, 4, and 5 to the cluster:

```
config load-balance setting
  config slots
    edit 3
  next
```

```

edit 4
next
edit 5
end
end

```

You can also use the following CLI command to configure the external management IP/Netmask and management access to this address:

```

config load-balance setting
    set base-mgmt-external-ip 172.20.120.100 255.255.255.0
    set base-mgmt-allowaccess https ssh ping
end

```

Adding the workers to the cluster

1. Log into the CLI of each worker and enter the following command to reset the worker to its factory default settings.

```
execute factoryreset
```

If the workers are going to run FortiOS Carrier, add the FortiOS Carrier license instead. Adding the license also resets the worker to factory default settings.

2. Register each worker and apply licenses to each worker before adding them to the cluster.

This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMs). You should also install any third-party certificates on each worker before forming the cluster. FortiToken licenses can be added at any time because they are synchronized to all workers.

3. Optionally give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network.

These IP addresses are not synchronized, so you can connect to and manage each worker separately.

```

config system interface
    edit mgmt1
        set ip 172.20.120.120
    end

```

4. Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

```

config system global
    set hostname worker-slot-3
end

```

5. Enter the following command on each worker to enable FortiController mode.

```

config system elbc
    set mode forticontroller
end

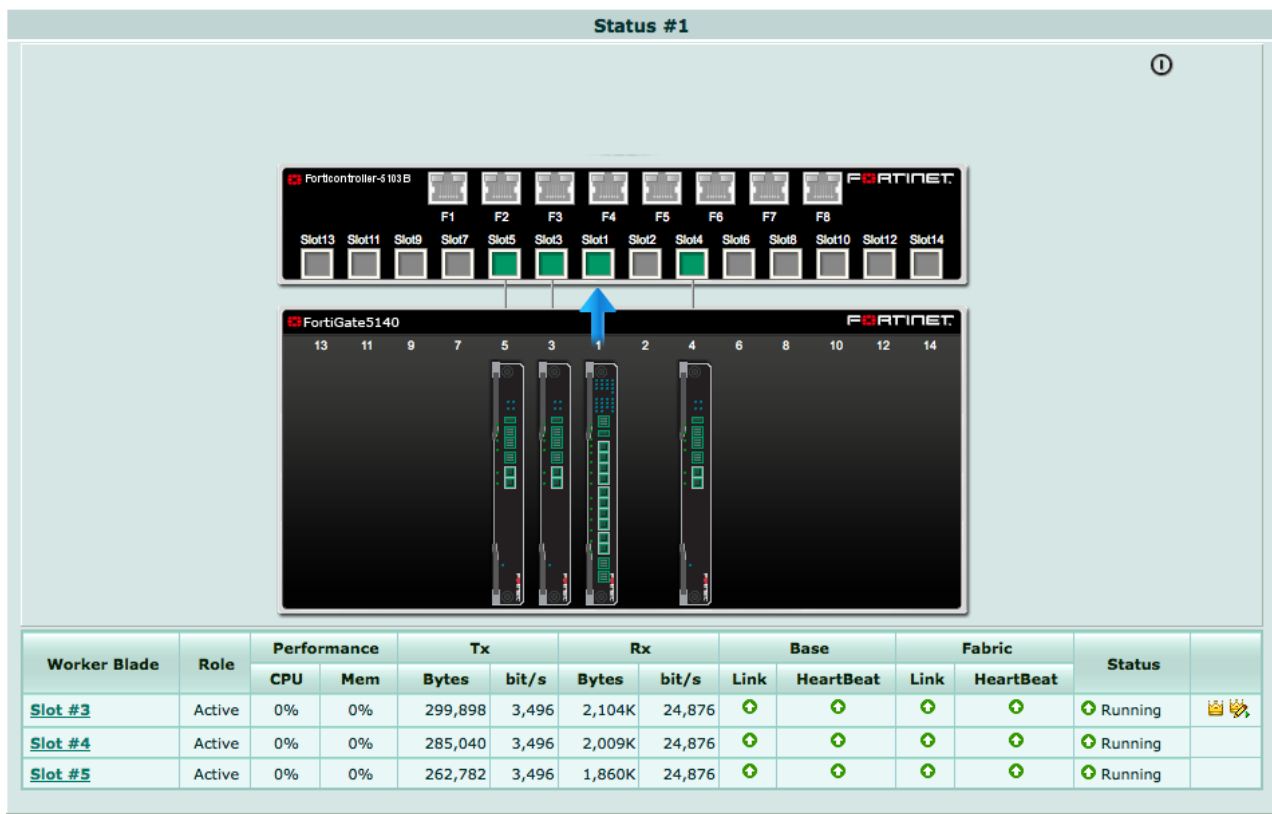
```

The worker restarts and joins the cluster.

6. On the FortiController GUI go to **Load Balance > Status**.

As the workers restart they should appear in their appropriate slots.

The primary worker should be the worker in slot 3. The primary FortiController status display includes a **Config Master** link that you can use to connect to the primary worker.



Operating and managing the cluster

You can now manage the workers in the same way as you would manage a standalone FortiGate. You can connect to the worker GUI or CLI using the **External Management IP**. If you had configured the worker mgmt1 or mgmt2 interfaces you can also connect to one of these addresses to manage the cluster.

To operate the cluster, connect networks to the FortiController front panel interfaces and connect to a worker GUI or CLI to configure the workers to process the traffic they receive. When you connect to the External Management IP, you connect to the primary worker. When you make configuration changes they are synchronized to all workers in the cluster.

You can use the external management IP followed by a special port number to manage individual devices in the cluster. For details, see [Managing the devices in an SLBC cluster with the External Management IP on page 29](#).

By default on the workers, all FortiController front panel interfaces are in the root VDOM. You can configure the root VDOM or create additional VDOMs and move interfaces into them.

For example, you could connect the internet to FortiController front panel interface 4 (fctrl/f4 on the worker GUI and CLI) and an internal network to FortiController front panel interface 2 (fctrl/f2 on the worker GUI and CLI). Then enter the root VDOM and add a policy to allow users on the internal network to access the internet.

Incoming Interface	fctrl/f3	+
Source Address	Internal-net	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	fctrl/f1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	✓ ACCEPT	

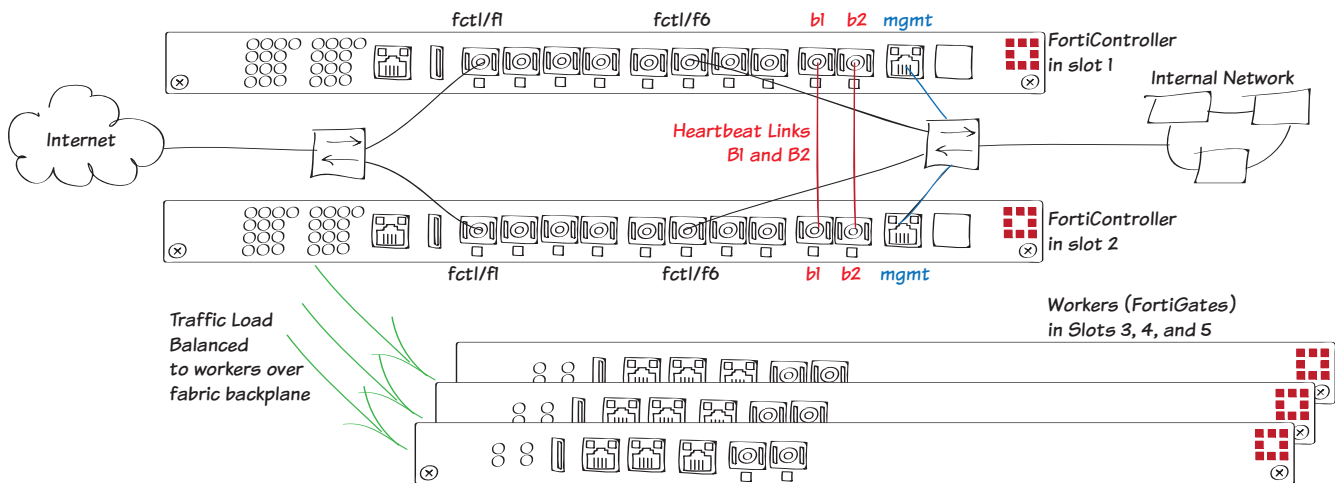
Firewall / Network Options**ON** NAT

- ☒ Use Outgoing Interface Address ☐ Fixed Port
- ☐ Use Dynamic IP Pool

Click to add...

Active-Passive SLBC with two FortiController-5103Bs

This example describes the basics of setting up an active-passive SLBC cluster that consists of two FortiController-5103Bs, installed in chassis slots 1 and 2, and three FortiGate-5001C workers, installed in chassis slots 3, 4, and 5. This SLBC configuration can have up to eight redundant 10Gbit network connections.



The FortiControllers in the same chassis to operate in active-passive HA mode for redundancy. The FortiController in slot 1 becomes the primary unit actively processing sessions. The FortiController in slot 2 becomes the secondary unit, sharing the primary unit's session table. If the primary unit fails the secondary unit resumes all active sessions.

All networks have redundant connections to both FortiControllers. You also create heartbeat links between the FortiControllers and management links from the FortiControllers to an internal network.

Setting up the hardware

1. Install a FortiGate-5000 series chassis and connect it to power.
2. Install the FortiController in slots 1 and 2.
3. Install the workers in slots 3, 4, and 5.
4. Power on the chassis.
5. Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally.
To check normal operation LED status see the [FortiGate-5000 hardware guides](#) and [FortiController hardware guides](#).
6. Create duplicate connections from the FortiController front panel interfaces to the internet and to the internal network.
7. Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a secondary heartbeat link by connecting the FortiController B2 interfaces together.
You can directly connect the heartbeat interfaces with a patch cable or connect them through a switch. If you use a switch, it must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301

and 101). These connections establish heartbeat, base control, and base management communication between the FortiControllers.

Only one heartbeat connection is required but redundant connections are recommended.

8. Connect the mgmt interfaces of both FortiControllers to the internal network or any network to manage the cluster from.
9. Check the [FortiController release notes](#) for the latest supported FortiController and FortiGate firmware.
10. Get FortiController and FortiOS firmware from the [Fortinet Support site](#).
For FortiController firmware, select the **FortiSwitchATCA** product.

Configuring the FortiControllers

1. Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in slot 1 using the default IP address 192.168.1.99.

Or connect to the FortiController CLI through the console port (Baud Rate 9600bps, Data bits 8, Parity None, Stop bits 1, and Flow Control None).

2. Login using the admin administrator account and no password.
3. Add a password for the admin administrator account. From the GUI use the **Administrators** widget or from the CLI enter this command.

```
config admin user
  edit admin
    set password <password>
  end
```

4. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
  edit mgmt
    set ip 172.20.120.151/24
  end
```

5. If you need to add a default route for the management IP address, enter this command.

```
config route static
  edit route 1
    set gateway 172.20.120.2
  end
```

6. Set the chassis type that you are using, for example:

```
config system global
  set chassis-type fortigate-5140
end
```

7. Configure active-passive HA on the FortiController in slot 1. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.
8. Set **Mode** to **Active-Passive**, change the **Group ID**, and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync

Configure

Mode: Active-Passive

Device Priority (0-255):

Group ID(0-31):

Enable Override: ☐

Heartbeat interval(200-1000ms):

Number of heartbeats lost(2-255):

VLAN to use for HA heartbeat traffic(1-4094):

Enable Chassis Redundancy: ☐

Available

mgmt

Selected

b1
b2

Heartbeat Device

OK
Cancel

You can also enter the following from the CL:

```
config system ha
  set mode a-p>
  set groupid 23
  set hbdev b1 b2
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the Group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

You can also adjust other HA settings. For example, you could increase the **Device Priority** of the FortiController that you want to become the primary unit, enable **Override** to make sure the FortiController with the highest device priority becomes the primary unit, and change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on your network.

You would only select **Enable chassis redundancy** if your cluster has more than one chassis.

9. Log into the GUI of the FortiController in slot 2 and duplicate the HA configuration of the FortiController in slot 1, except for the Device Priority and override setting, which can be different on each FortiController.

After a short time, the FortiControllers restart in HA mode and form an active-passive cluster. Both FortiControllers must have the same HA configuration and at least one heartbeat link must be connected.

Normally the FortiController in slot 1 is the primary unit, and you can log into the cluster using the management IP address you assigned to this FortiController.

10. Confirm that cluster has been formed by viewing the HA configuration from the FortiController GUI. The display should show both FortiControllers in the cluster.

Since the configuration of all FortiControllers is synchronized, you can complete the configuration of the cluster from the primary FortiController.

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
FTS13B3912000029	FTS13B3912000029	Master	169.254.128.81	545.32	0	0/0	1	1
FTS13B3912000051	FTS13B3912000051	Slave	169.254.128.82	405.77	0	0/0	1	1

Configure

Mode: Active-Passive

Device Priority (0-255):

Group ID(0-31):

Enable Override: ☐

Heartbeat interval(200-1000ms):

Number of heartbeats lost(2-255):

VLAN to use for HA heartbeat traffic(1-4094):

Enable Chassis Redundancy: ☐

Heartbeat Device

Available

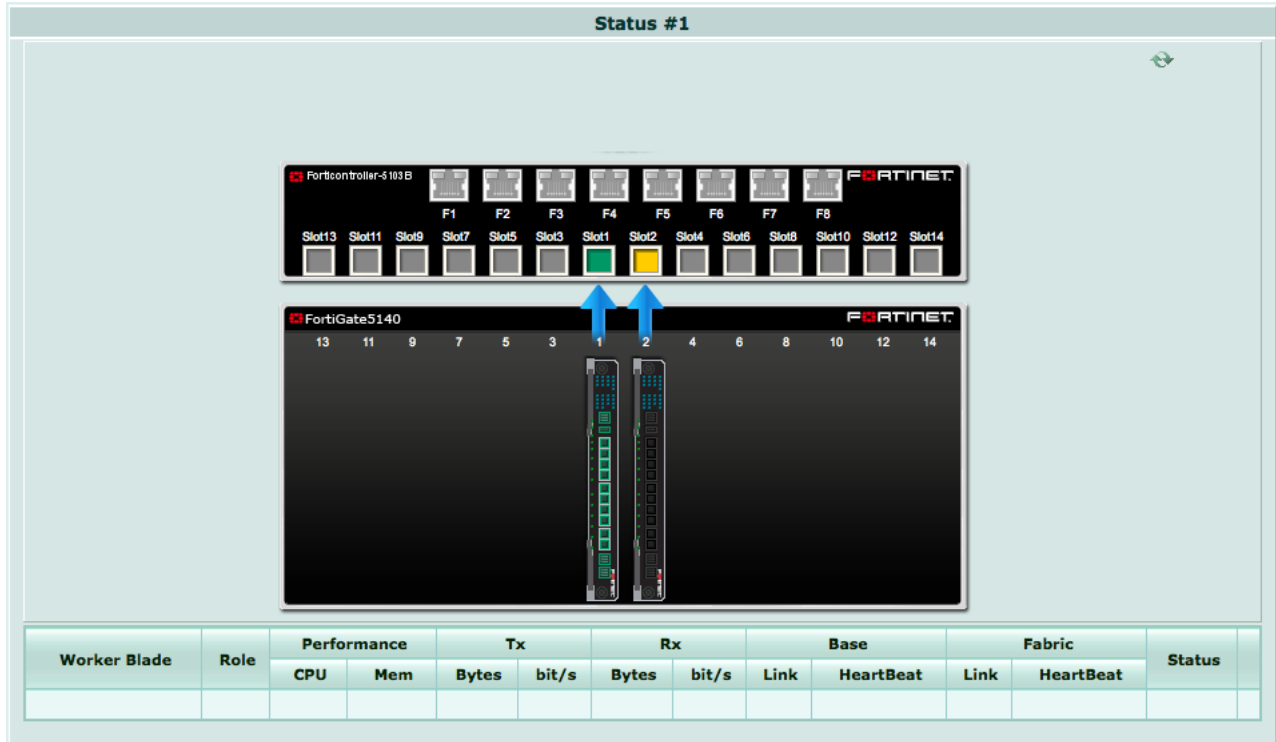
- mgmt

Selected

- b1
- b2

11. Go to **Load Balance > Status** see the status of the cluster.

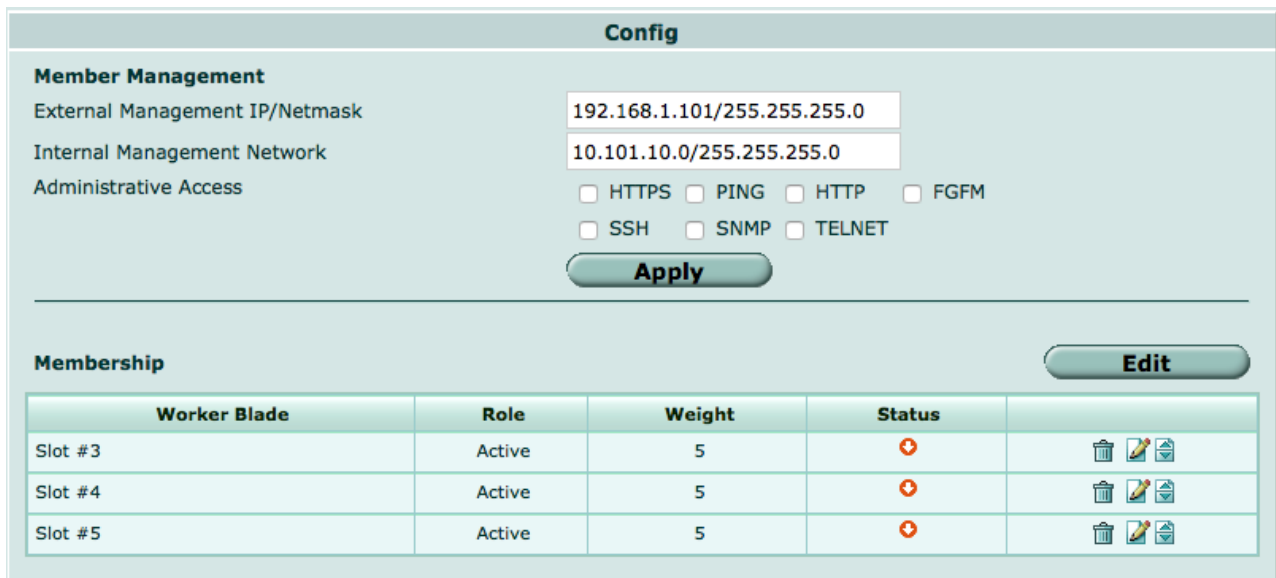
This page should show both FortiControllers in the cluster. The FortiController in slot 1 is the primary unit (slot icon colored green) and the FortiController in slot 2 is the secondary unit (slot icon colored yellow).



12. Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured yet their status will be **Down**.

13. Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.



You can also enter the following CLI command to add slots 3, 4, and 5 to the cluster:

```
config load-balance setting
  config slots
    edit 3
```

```

    next
    edit 4
    next
    edit 5
    end
end

```

You can also use the following CLI command to configure the external management IP/Netmask and management access to this address:

```

config load-balance setting
    set base-mgmt-external-ip 172.20.120.100 255.255.255.0
    set base-mgmt-allowaccess https ssh ping
end

```

- 14. Enable base **management** traffic between FortiControllers.** The CLI syntax shows setting the default base management VLAN (101). You can also use this command to change the base management VLAN.

```

config load-balance setting
    config base-mgmt-interfaces
        edit b1
            set vlan-id 101
        next
        edit b2
            set vlan-id 101
        end
    end
end

```

- 15. Enable base **control** traffic between FortiControllers.** The CLI syntax shows setting the default base control VLAN (301). You can also use this command to change the base management VLAN.

```

config load-balance setting
    config base-ctrl-interfaces
        edit b1
            set vlan-id 301
        next
        edit b2
            set vlan-id 301
        end
    end
end

```

Adding the workers to the cluster

1. Log into the CLI of each worker and enter the following command to reset the worker to its factory default settings.

```
execute factoryreset
```

If the workers are going to run FortiOS Carrier, add the FortiOS Carrier license instead. Adding the license also resets the worker to factory default settings.

2. Register each worker and apply licenses to each worker before adding them to the cluster.

This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMs). You should also install any third-party certificates on each worker before forming the cluster. FortiToken licenses can be added at any time because they are synchronized to all workers.

3. Optionally give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network.

These IP addresses are not synchronized, so you can connect to and manage each worker separately.

```
config system interface
```

```
edit mgmt1
  set ip 172.20.120.120
end
```

4. Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

```
config system global
  set hostname worker-slot-3
end
```

5. Enter the following command on each worker to enable FortiController mode.

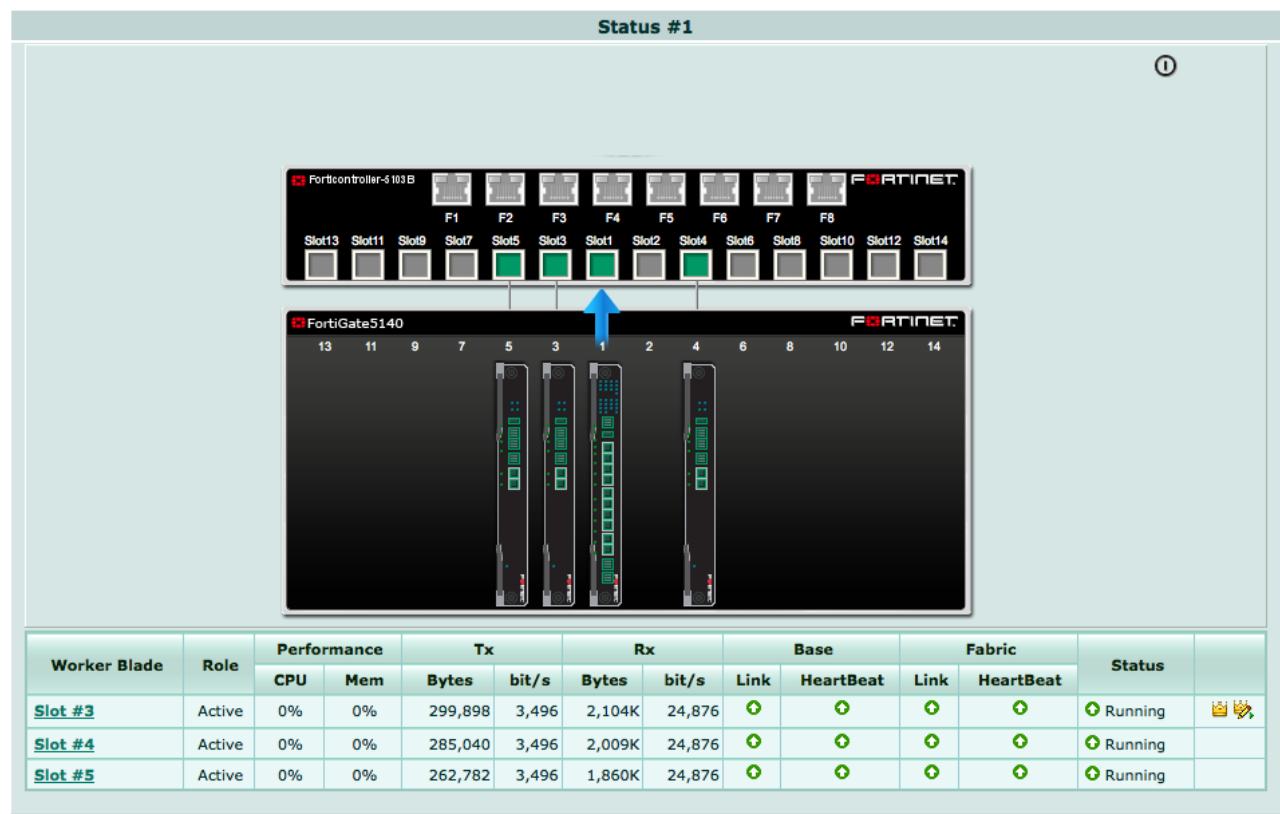
```
config system elbc
  set mode forticontroller
end
```

The worker restarts and joins the cluster.

6. On the FortiController GUI go to **Load Balance > Status**.

As the workers restart they should appear in their appropriate slots.

The primary worker should be the worker in slot 3. The primary FortiController status display includes a **Config Master** link that you can use to connect to the primary worker.



Operating and managing the cluster

You can now manage the workers in the same way as you would manage a standalone FortiGate. You can connect to the worker GUI or CLI using the **External Management IP**. If you had configured the worker mgmt1 or mgmt2 interfaces you can also connect to one of these addresses to manage the cluster.

To operate the cluster, connect networks to the FortiController front panel interfaces and connect to a worker GUI or CLI to configure the workers to process the traffic they receive. When you connect to the External Management IP, you connect to the primary worker. When you make configuration changes they are synchronized to all workers in the cluster.

You can use the external management IP followed by a special port number to manage individual devices in the cluster. For details, see [Managing the devices in an SLBC cluster with the External Management IP on page 29](#).

By default on the workers, all FortiController front panel interfaces are in the root VDOM. You can configure the root VDOM or create additional VDOMs and move interfaces into them.

For example, you could connect the internet to FortiController front panel interface 1 (fctrl/f1 on the worker GUI and CLI) and an internal network to FortiController front panel interface 6 (fctrl/f6 on the worker GUI and CLI) . Then enter the root VDOM and add a policy to allow users on the internal network to access the internet.

Incoming Interface	fctrl/f6	+
Source Address	Internal-net	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	fctrl/f1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	✓ ACCEPT	

Firewall / Network Options

ON NAT

☒ Use Outgoing Interface Address

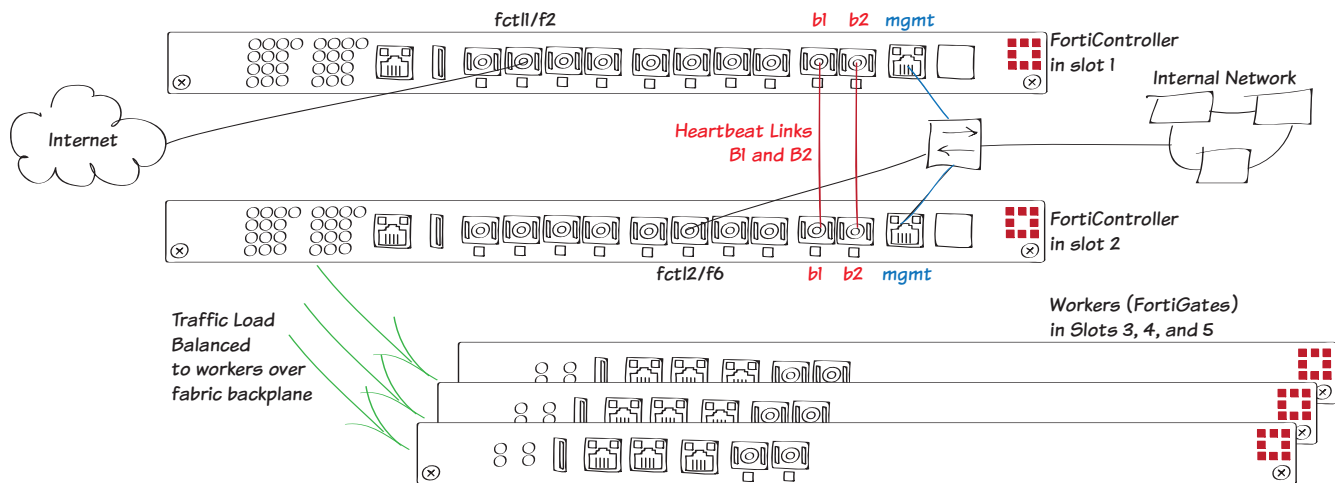
☐ Use Dynamic IP Pool

☐ Fixed Port

Click to add...

Dual mode SLBC with two FortiController-5103Bs

This example describes the basics of setting up a dual mode SLBC cluster that consists of two FortiController-5103Bs, installed in chassis slots 1 and 2, and three FortiGate-5001C workers, installed in chassis slots 3, 4, and 5. This SLBC configuration can have up to 16 10Gbit network connections.



The two FortiControllers in the same chassis to operate in dual mode to double the number of network interfaces available. In dual mode, two FortiControllers load balance traffic to multiple workers. Traffic can be received by both FortiControllers and load balanced to all of the workers in the chassis. In a dual mode configuration the front panel interfaces of both FortiControllers are active.

In a dual mode FortiController-5103B cluster, up to 16 10Gbyte network interfaces are available. The interfaces of the FortiController in slot 1 are named fctrl/f1 to fctrl/f8 and the interfaces of the FortiController in slot 2 are named fctrl2/f1 to fctrl2/f8.

All networks have single connections to the first or second FortiController. It is a best practice in a dual-mode configuration to distribute traffic evenly between the FortiControllers. So in this example, ingress traffic from the internet is processed by the FortiController in slot 1 and egress traffic for the internal network is processed by the FortiController in slot 2.



Redundant connections to a single network from two dual-mode FortiControllers in same chassis is only supported if you configure link aggregation.

One or more heartbeat links are created between the FortiControllers. Redundant heartbeat links are recommended. The heartbeat links use the FortiController front panel B1 and B2 interfaces.

If one of the FortiControllers fails, the remaining FortiController keeps processing traffic received by its front panel interfaces. Traffic to and from the failed FortiController is lost.

Setting up the Hardware

1. Install a FortiGate-5000 series chassis and connect it to power.
2. Install the FortiController in slots 1 and 2.
3. Install the workers in slots 3, 4, and 5.
4. Power on the chassis.
5. Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally.
To check normal operation LED status see the [FortiGate-5000 hardware guides](#) and [FortiController hardware guides](#).
6. Create duplicate connections from the FortiController front panel interfaces to the internet and to the internal network.
7. Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a secondary heartbeat link by connecting the FortiController B2 interfaces together.
You can directly connect the heartbeat interfaces with a patch cable or connect them through a switch. If you use a switch, it must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). These connections establish heartbeat, base control, and base management communication between the FortiControllers.
Only one heartbeat connection is required but redundant connections are recommended.
8. Connect the mgmt interfaces of both FortiControllers to the internal network or any network to manage the cluster from.
9. Check the [FortiController release notes](#) for the latest supported FortiController and FortiGate firmware.
10. Get FortiController and FortiOS firmware from the [Fortinet Support site](#).
For FortiController firmware, select the **FortiSwitchATCA** product.

Configuring the FortiControllers

1. Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in slot 1 using the default IP address 192.168.1.99.
Or connect to the FortiController CLI through the console port (Baud Rate 9600bps, Data bits 8, Parity None, Stop bits 1, and Flow Control None).
2. Login using the admin administrator account and no password.
3. Add a password for the admin administrator account. From the GUI use the **Administrators** widget or from the CLI enter this command.

```
config admin user
  edit admin
    set password <password>
  end
```
4. Change the FortiController mgmt interface IP address.
From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
  edit mgmt
    set ip 172.20.120.151/24
  end
```
5. If you need to add a default route for the management IP address, enter this command.

```
config route static
edit route 1
set gateway 172.20.120.2
end
```

6. Set the chassis type that you are using, for example:

```
config system global
set chassis-type fortigate-5140
end
```

7. Configure dual Mode HA on the FortiController in slot 1. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.
8. Set **Mode** to **Dual Mode**, change the **Group ID**, and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
-----------	----	------	----	---------	----------------------------	----------------	---------	-----------

Configure

Mode: Dual Mode

Device Priority (0-255): 128

Group ID(0-31): 4

Enable Override: ☐

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy: ☐

Available

mgmt

Selected

b1
b2

OK
Cancel

You can also enter this CLI command:

```
config system ha
```

```
set mode dual
set groupid 4
set hbdev b1 b2
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the Group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

You can also adjust other HA settings. For example, you could increase the **Device Priority** of the FortiController that you want to become the primary unit, or enable **Override** to make sure the FortiController with the highest device priority becomes the primary unit.

If the heartbeat interfaces are connected using a switch, you can change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on the switch.

You would only select **Enable chassis redundancy** if you are configuring HA between two chassis.

9. Log into the GUI of the FortiController in slot 2 and duplicate the HA configuration of the FortiController in slot 1, except for the Device Priority and override setting, which can be different on each FortiController.

After a short time, the FortiControllers restart in HA mode and form a dual mode cluster. Both FortiControllers must have the same HA configuration (aside from device priority and override) and at least one heartbeat link must be connected.

Normally the FortiController in slot 1 is the primary unit, and you can log into the cluster using the management IP address you assigned to this FortiController.

If the FortiControllers are unable to form a cluster, check to make sure that they both have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

10. Confirm that cluster has been formed by viewing HA configuration from the FortiController GUI. The display should show both FortiControllers in the cluster.

Since the configuration of the FortiControllers is synchronized, you can complete the configuration of the cluster from the primary FortiController.

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
FT513B3912000029	FT513B3912000029	Master	169.254.128.33	1894.42	0	0/0	1	1
FT513B3912000051	FT513B3912000051	Slave	169.254.128.34	827.73	0	0/0	1	1

Configure

Mode: Dual Mode

Device Priority (0-255): 128

Group ID(0-31): 4

Enable Override: ☐

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy: ☐

Heartbeat Device

Available

mgmt

Selected

b1
b2

OK
Cancel

11. Go to **Load Balance > Status** to see the status of the cluster. This page should show both FortiControllers in the cluster.

Since both FortiControllers are active, their slot icons both appear green on the GUI.

Status #1

Worker Blade	Role	Performance		Tx		Rx		Base		Fabric		Status
		CPU	Mem	Bytes	bit/s	Bytes	bit/s	Link	HeartBeat	Link	HeartBeat	

12. Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured yet their status will be **Down**.

13. Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.

Config

Member Management

External Management IP/Netmask: 192.168.1.101/255.255.255.0

Internal Management Network: 10.101.10.0/255.255.255.0

Administrative Access:

☐ HTTPS ☐ PING ☐ HTTP ☐ FGFM

☐ SSH ☐ SNMP ☐ TELNET

Apply

Membership **Edit**

Worker Blade	Role	Weight	Status	
Slot #3	Active	5	Down	
Slot #4	Active	5	Down	
Slot #5	Active	5	Down	

14. You can also enter the following CLI command to add slots 3, 4, and 5 to the cluster:

```
config load-balance setting
  config slots
    edit 3
    next
    edit 4
    next
    edit 5
    end
  end
```

You can also use the following CLI command to configure the external management IP/Netmask and management access to this address:

```
config load-balance setting
  set base-mgmt-external-ip 172.20.120.100 255.255.255.0
  set base-mgmt-allowaccess https ssh ping
end
```

15. Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.
16. Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.

Config

Member Management
 External Management IP/Netmask
 Internal Management Network
 Administrative Access

192.168.1.101/255.255.255.0

10.101.10.0/255.255.255.0

☐ HTTPS
☐ SSH

☐ PING
☐ SNMP

☐ HTTP
☐ TELNET

☐ FGFM

Apply

Membership

Edit

Worker Blade	Role	Weight	Status	
Slot #3	Active	5	+	
Slot #4	Active	5	+	
Slot #5	Active	5	+	

You can also enter the following CLI command to add slots 3, 4, and 5 to the cluster:

```
config load-balance setting
  config slots
    edit 3
    next
    edit 4
    next
    edit 5
    end
  end
```

You can also use the following CLI command to configure the external management IP/Netmask and management access to this address:

```
config load-balance setting
  set base-mgmt-external-ip 172.20.120.100 255.255.255.0
  set base-mgmt-allowaccess https ssh ping
end
```

17. Enable base **management traffic between FortiControllers.** The CLI syntax shows setting the default base management VLAN (101). You can also use this command to change the base management VLAN.

```
config load-balance setting
  config base-mgmt-interfaces
    edit b1
      set vlan-id 101
    next
    edit b2
      set vlan-id 101
    end
  end
```

18. Enable base **control traffic between FortiControllers.** The CLI syntax shows setting the default base control VLAN (301). You can also use this command to change the base management VLAN.

```
config load-balance setting
  config base-ctrl-interfaces
    edit b1
      set vlan-id 301
    next
    edit b2
```

FortiController 5.2.10 Session-Aware Load Balancing (SLBC) Guide

79

```
        set vlan-id 301
    end
end
```

Adding the workers to the cluster

1. Log into the CLI of each worker and enter the following command to reset the worker to its factory default settings.

```
execute factoryreset
```

If the workers are going to run FortiOS Carrier, add the FortiOS Carrier license instead. Adding the license also resets the worker to factory default settings.

2. Register each worker and apply licenses to each worker before adding them to the cluster.

This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMs). You should also install any third-party certificates on each worker before forming the cluster. FortiToken licenses can be added at any time because they are synchronized to all workers.

3. Optionally give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network.

These IP addresses are not synchronized, so you can connect to and manage each worker separately.

```
config system interface
    edit mgmt1
        set ip 172.20.120.120
    end
```

4. Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

```
config system global
    set hostname worker-slot-3
end
```

5. Enter the following command on each worker to enable dual FortiController mode.

```
config system elbc
    set mode dual-forticontroller
end
```

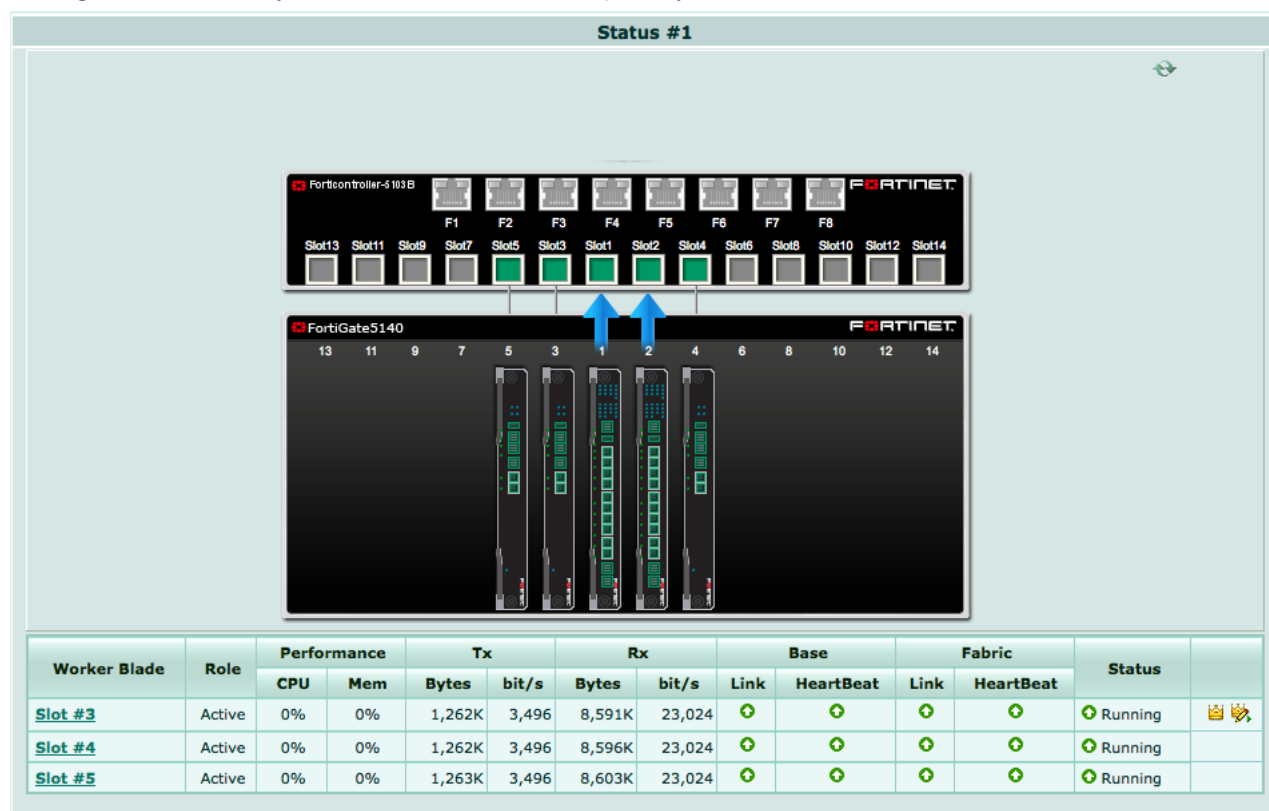
The worker restarts and joins the cluster.

6. On the FortiController GUI go to **Load Balance > Status**.

As the workers restart they should appear in their appropriate slots.

The primary worker should be the worker in chassis 1 slot 3. The primary FortiController status display includes a

Config Master link that you can use to connect to the primary worker.



Operating and managing the cluster

You can now manage the workers in the same way as you would manage a standalone FortiGate. You can connect to the worker GUI or CLI using the **External Management IP**. If you had configured the worker mgmt1 or mgmt2 interfaces you can also connect to one of these addresses to manage the cluster.

To operate the cluster, connect networks to the FortiController front panel interfaces and connect to a worker GUI or CLI to configure the workers to process the traffic they receive. When you connect to the External Management IP, you connect to the primary worker. When you make configuration changes they are synchronized to all workers in the cluster.

You can use the external management IP followed by a special port number to manage individual devices in the cluster. For details, see [Managing the devices in an SLBC cluster with the External Management IP on page 29](#).

To manage a FortiController using SNMP you need to load the FORTINET-CORE-MIB.mib file into your SNMP manager. You can get this MIB file from the Fortinet support site, in the same location as the current FortiController firmware (select the FortiSwitchATCA product).

By default on the workers, all FortiController front panel interfaces are in the root VDOM. You can configure the root VDOM or create additional VDOMs and move interfaces into them.

For example, you could connect the internet to FortiController front panel interface 1 (fctrl/f1 on the worker GUI and CLI) and an internal network to FortiController front panel interface 6 (fctrl/f6 on the worker GUI and CLI). Then enter the root VDOM and add a policy to allow users on the internal network to access the internet.

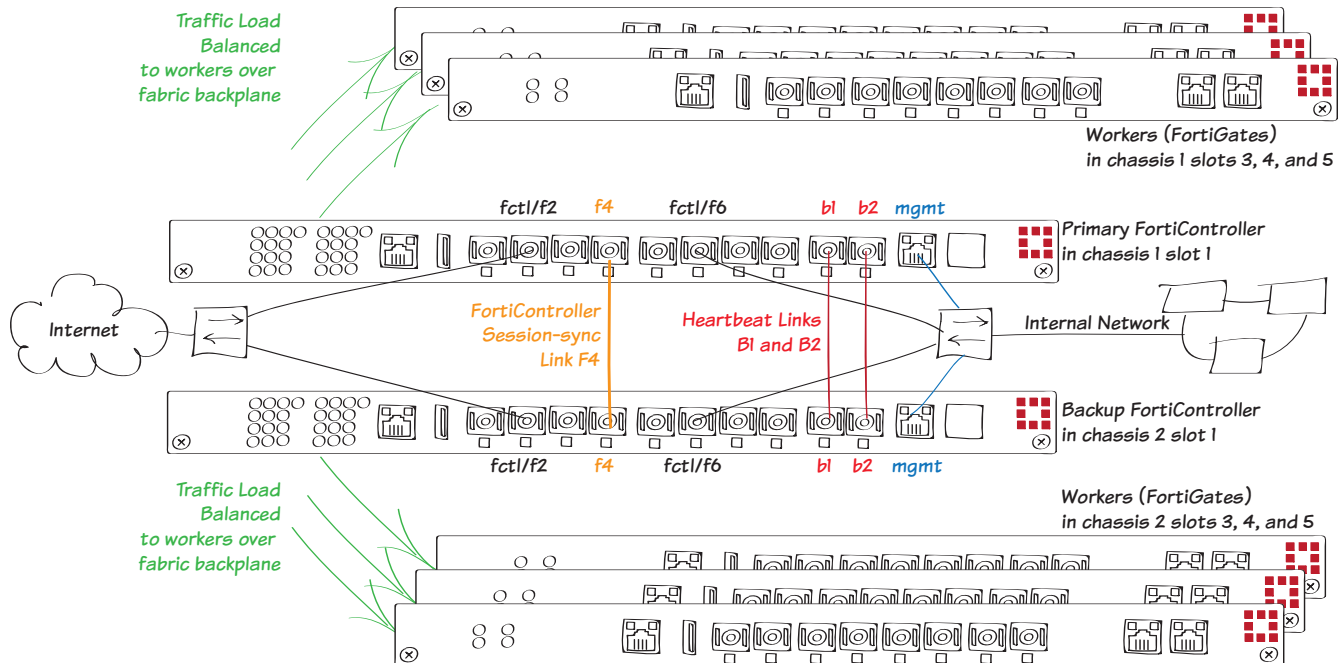
Incoming Interface	fctrl/f6	+
Source Address	Internal-net	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	fctrl/f1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	✓ ACCEPT	

Firewall / Network Options☒ NAT☒ Use Outgoing Interface Address☐ Use Dynamic IP Pool☐ Fixed Port

Click to add...

Active-passive SLBC with two FortiController-5103Bs and two chassis

This example describes how to setup an active-passive SLBC cluster consisting of two FortiGate-5000 chassis, two FortiController-5103Bs, and six FortiGate-5001Bs acting as workers, three in each chassis. This SLBC configuration can have up to seven redundant 10Gbit network connections.



The FortiControllers operate in active-passive HA mode for redundancy. The FortiController in chassis 1 slot 1 will be configured to be the primary unit, actively processing sessions. The FortiController in chassis 2 slot 1 becomes the secondary unit. If the primary unit fails the secondary unit resumes all active sessions.

All networks in this example have redundant connections to both FortiControllers and redundant heartbeat and base control and management links are created between the FortiControllers using their front panel B1 and B2 interfaces.

This example also includes a FortiController session sync connection between the FortiControllers using the FortiController F4 front panel interface (resulting in the SLBC having a total of seven redundant 10Gbit network connections). (You can use any fabric front panel interface.)

Heartbeat and base control and management traffic uses VLANs and specific subnets. So the switches and network components used must be configured to allow traffic on these VLANs and you should be aware of the subnets used in case they conflict with any connected networks.

This example sets the device priority of the FortiController in chassis 1 higher than the device priority of the FortiController in chassis 2 to make sure that the FortiController in chassis 1 becomes the primary FortiController for the cluster

Setting up the hardware

1. Install two FortiGate-5000 series chassis and connect them to power. Ideally each chassis should be connected to a separate power circuit.
2. Install a FortiController in slot 1 of each chassis.
3. Install the workers in slots 3, 4, and 5 of each chassis.
4. Power on both chassis.
5. Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally.
To check normal operation LED status see the [FortiGate-5000 hardware guides](#) and [FortiController hardware guides](#).
6. Create duplicate connections from both FortiController front panel interfaces to the internet and to the internal network.
7. Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a secondary heartbeat link by connecting the FortiController B2 interfaces together.
You can directly connect the heartbeat interfaces with a patch cable or connect them through a switch. If you use a switch, it must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). These connections establish heartbeat, base control, and base management communication between the FortiControllers.
Only one heartbeat connection is required but redundant connections are recommended.
8. Create a FortiController session sync connection between the chassis by connecting the FortiController F4 interfaces together. If you use a switch it must allow traffic on the FortiController session sync VLAN (2000). You can use any of the F1 to F8 interfaces. We chose F4 in this example to make the diagram easier to understand.
9. Connect the mgmt interfaces of both FortiControllers to the internal network or any network to manage the cluster from.
10. Check the [FortiController release notes](#) for the latest supported FortiController and FortiGate firmware.
11. Get FortiController and FortiOS firmware from the [Fortinet Support site](#).
For FortiController firmware, select the **FortiSwitchATCA** product.

Configuring the FortiController in chassis 1

1. Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in chassis 1 using the default IP address 192.168.1.99.
Or connect to the FortiController CLI through the console port (Baud Rate 9600bps, Data bits 8, Parity None, Stop bits 1, and Flow Control None).
2. Login using the admin administrator account and no password.
3. From the Dashboard System Information widget, set the **Host Name** to ch1-slot1. Or enter this command.

```
config system global
  set hostname ch1-slot1
end
```
4. Add a password for the admin administrator account. From the GUI use the **Administrators** widget or from the CLI enter this command.

```
config admin user
  edit admin
    set password <password>
  end
```

5. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
  edit mgmt
    set ip 172.20.120.151/24
  end
```

6. If you need to add a default route for the management IP address, enter this command.

```
config route static
  edit route 1
    set gateway 172.20.120.2
  end
```

7. Set the chassis type that you are using, for example:

```
config system global
  set chassis-type fortigate-5140
end
```

8. Enable FortiController session sync.

```
config load-balance setting
  set session-sync enable
end
```

9. Configure Active-Passive HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

10. Set **Mode** to **Active-Passive**, set the **Device Priority** to 250, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
5103-slot1	FT513B3912000051	Master	169.254.128.33	247020.05	0	0/1	1	1

Configure

Mode: Active-Passive

Device Priority (0-255): 250

Group ID(0-31): 5

Enable Override: ☒

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy: ☒

Chassis ID(1 - 2): 1

Heartbeat Device

Available: mgmt

Selected: b1, b2

OK Cancel

11. Enter the following command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
    set session-sync-port f4
end
```

You can also enter the complete HA configuration with this command:

```
config system ha
    set mode active-passive
    set groupid 5
    set priority 250
    set override enable
    set chassis-redundancy enable
    set chassis-id 1
    set hbdev b1 b2
    set session-sync-port f4
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different group ID. The default group ID of 0 is not a good choice and normally should be changed.

Enable Override is selected to make sure the FortiController in chassis 1 always becomes the primary unit. Enabling override could lead to the cluster renegotiating more often, so once the chassis is operating you can disable this setting.

You can also adjust other HA settings. For example, if the heartbeat interfaces are connected using a switch, you can change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on the switch. You can also adjust the **Heartbeat Interval** and **Number of Heartbeats** lost to adjust how quickly the cluster determines if one of the FortiControllers has failed.

Configuring the FortiController in chassis 2

1. Log into the FortiController in chassis 2.
2. From the Dashboard System Information widget, set the **Host Name** to ch2-slot1. Or enter this command.

```
config system global
    set hostname ch1-slot1
end
```

3. Enter the following command to duplicate the HA configuration of the FortiController in chassis 1.

Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10), and set the **Chassis ID** to 2.

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

You can also enter the complete HA configuration with this command:

```
config system ha
    set mode active-passive
    set groupid 5
    set priority 10
    set chassis-redundancy enable
    set chassis-id 2
    set hbdev b1 b2
    set session-sync-port f4
end
```

Adding the workers to the cluster

1. Log into the CLI of each worker and enter the following command to reset the worker to its factory default settings.

```
execute factoryreset
```

If the workers are going to run FortiOS Carrier, add the FortiOS Carrier license instead. Adding the license also resets the worker to factory default settings.

2. Register each worker and apply licenses to each worker before adding them to the cluster.

This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMs). You should also install any third-party certificates on each worker before forming the cluster. FortiToken licenses can be added at any time because they are synchronized to all workers.

3. Optionally give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network.

These IP addresses are not synchronized, so you can connect to and manage each worker separately.

```
config system interface
  edit mgmt1
    set ip 172.20.120.120
  end
```

4. Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

```
config system global
  set hostname worker-chassis-1-slot-3
end
```

5. Enter the following command on each worker to enable FortiController mode.

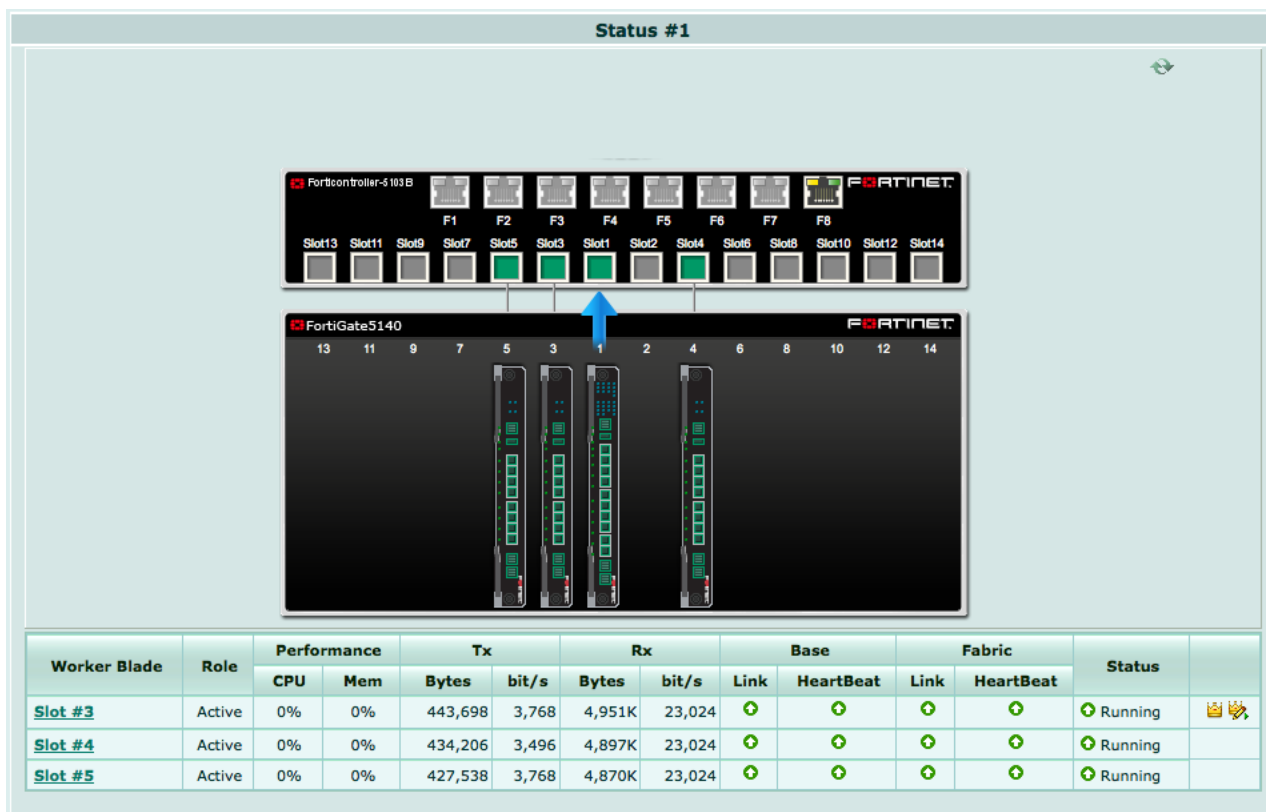
```
config system elbc
  set mode forticontroller
end
```

The worker restarts and joins the cluster.

6. On the primary FortiController GUI go to **Load Balance > Status**.

As the workers in chassis 1 restart they should appear in their appropriate slots.

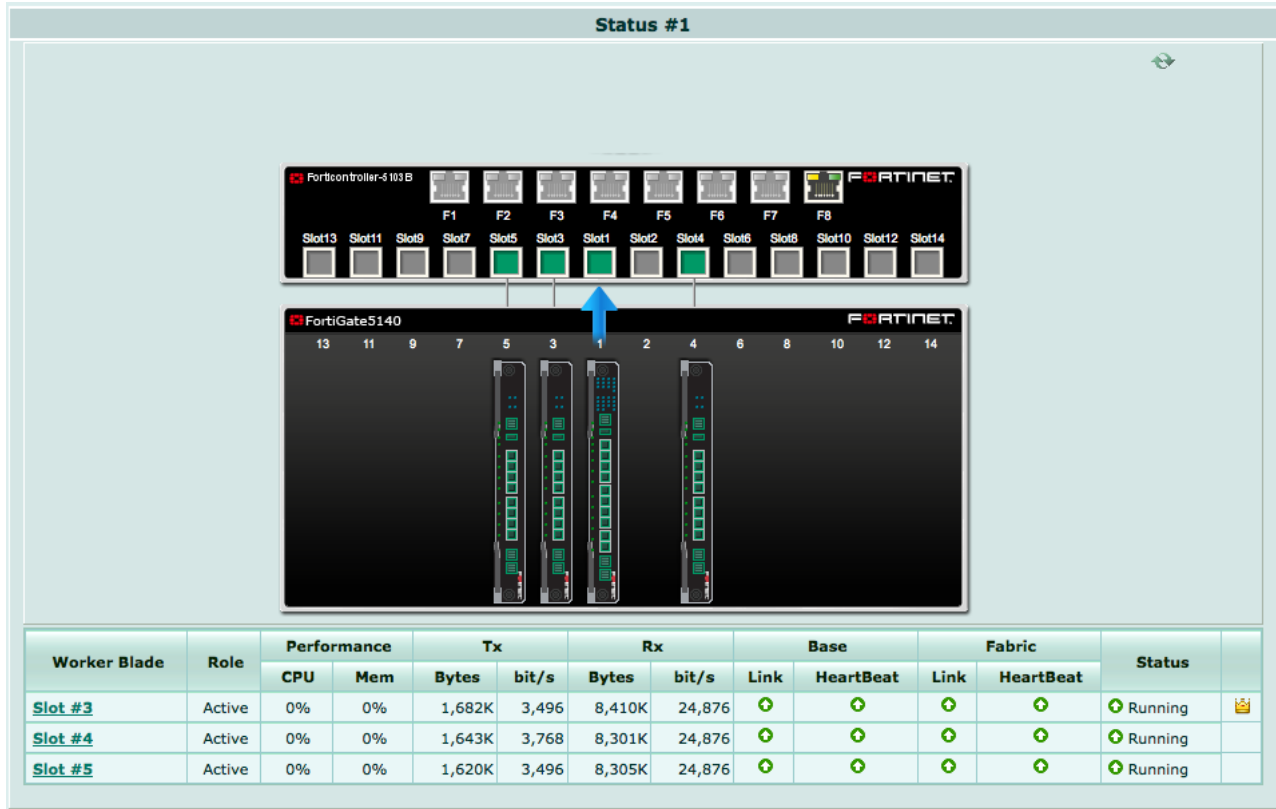
The primary worker should be the worker in chassis 1 slot 3. The primary FortiController status display includes a **Config Master** link that you can use to connect to the primary worker.



- Log into the secondary FortiController GUI (for example by browsing to <https://172.20.120.100:44321>) and go to **Load Balance > Status**.

As the workers in chassis 2 restart they should appear in their appropriate slots.

The secondary FortiController Status page shows the status of the workers in chassis 2 and does not include the **Config Master** link.



Operating and managing the cluster

You can now manage the workers in the same way as you would manage a standalone FortiGate. You can connect to the worker GUI or CLI using the **External Management IP**. If you had configured the worker mgmt1 or mgmt2 interfaces you can also connect to one of these addresses to manage the cluster.

To operate the cluster, connect networks to the FortiController front panel interfaces and connect to a worker GUI or CLI to configure the workers to process the traffic they receive. When you connect to the External Management IP, you connect to the primary worker. When you make configuration changes they are synchronized to all workers in the cluster.

You can use the external management IP followed by a special port number to manage individual devices in the cluster. For details, see [Managing the devices in an SLBC cluster with the External Management IP on page 29](#).

To manage a FortiController using SNMP you need to load the FORTINET-CORE-MIB.mib file into your SNMP manager. You can get this MIB file from the Fortinet support site, in the same location as the current FortiController firmware (select the FortiSwitchATCA product).

By default on the workers, all FortiController front panel interfaces are in the root VDOM. You can configure the root VDOM or create additional VDOMs and move interfaces into them.

For example, you could connect the internet to FortiController front panel interface 1 (fctrl/f1 on the worker GUI and CLI) and an internal network to FortiController front panel interface 6 (fctrl/f6 on the worker GUI and CLI). Then enter the root VDOM and add a policy to allow users on the internal network to access the internet.

Incoming Interface	fctrl/f6	+
Source Address	Internal-net	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	fctrl/f1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	✓ ACCEPT	

Firewall / Network Options

ON NAT

☒ Use Outgoing Interface Address

☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

Checking the cluster status

You can use the following get and diagnose commands to show the status of the cluster and all of the devices in it.

1. Log into the primary FortiController CLI and enter the following command to view the system status of the primary FortiController.

```
get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000029
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: chl-slot1
Current HA mode: a-p, master
System time: Sat Sep 13 06:51:53 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

2. Enter the following command to view the load balance status of the primary FortiController and its workers. The command output shows the workers in slots 3, 4, and 5, and status information about each one.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
  Working: 3 [ 3 Active 0 Standby]
  Ready: 0 [ 0 Active 0 Standby]
```

```

Dead:      0 [ 0 Active 0 Standby]
Total:     3 [ 3 Active 0 Standby]

Slot 3: Status:Working  Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot 4: Status:Working  Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot 5: Status:Working  Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"

```

3. Enter this command from the primary FortiController to show the HA status of the primary and secondary FortiControllers.

The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (this case 0 for each FortiController) the number of failed workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (`status=alive`) and the B2 interfaces are not (`status=dead`). The cluster can still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```

diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch1-slot1(FT513B3912000029), Master(priority=0),
  ip=169.254.128.41, uptime=62581.81, chassis=1(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=2
  force-state(0:none) hbdevs: local_interface=      b1 best=yes
                           local_interface=      b2 best=no

ch2-slot1(FT513B3912000051), Slave(priority=1),
  ip=169.254.128.42, uptime=1644.71, chassis=2(1)
  slot: 1
  sync: conf_sync=0, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=2
  force-state(0:none) hbdevs: local_interface=      b1 last_hb_time=66430.35 status=alive
                           local_interface=      b2 last_hb_time= 0.00  status=dead

```

4. Log into the secondary FortiController CLI and enter this command to view the status of the secondary FortiController.

```

get system status
Version: FortiController-5103B v5.0,build0020,131118 (Patch 3)
Branch Point: 0020
Serial-Number: FT513B3912000051
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: ch2-slot1

```

```

Current HA mode: a-p, backup
System time: Sat Sep 13 07:29:04 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00) Pacific Time (US&Canada)

```

5. Enter the following command to view the status of the secondary FortiController and its workers.

```

get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: N/A
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]
  Slot 3: Status:Working  Function:Active
    Link:      Base: Up      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"
  Slot 4: Status:Working  Function:Active
    Link:      Base: Up      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"
  Slot 5: Status:Working  Function:Active
    Link:      Base: Up      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"

```

6. Enter the following command from the secondary FortiController to show the HA status of the secondary and primary FortiControllers.

Notice that the secondary FortiController is shown first. The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (this case 0 for each FortiController) the number of failed workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (`status=alive`) and the B2 interfaces are not (`status=dead`). The cluster can still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```

diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch2-slot1(FT513B3912000051), Slave(priority=1),
  ip=169.254.128.42, uptime=3795.92, chassis=2(1)
  slot: 1
  sync: conf_sync=0, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)  hbdevs: local_interface=      b1 best=yes
  local_interface=      b2 best=no

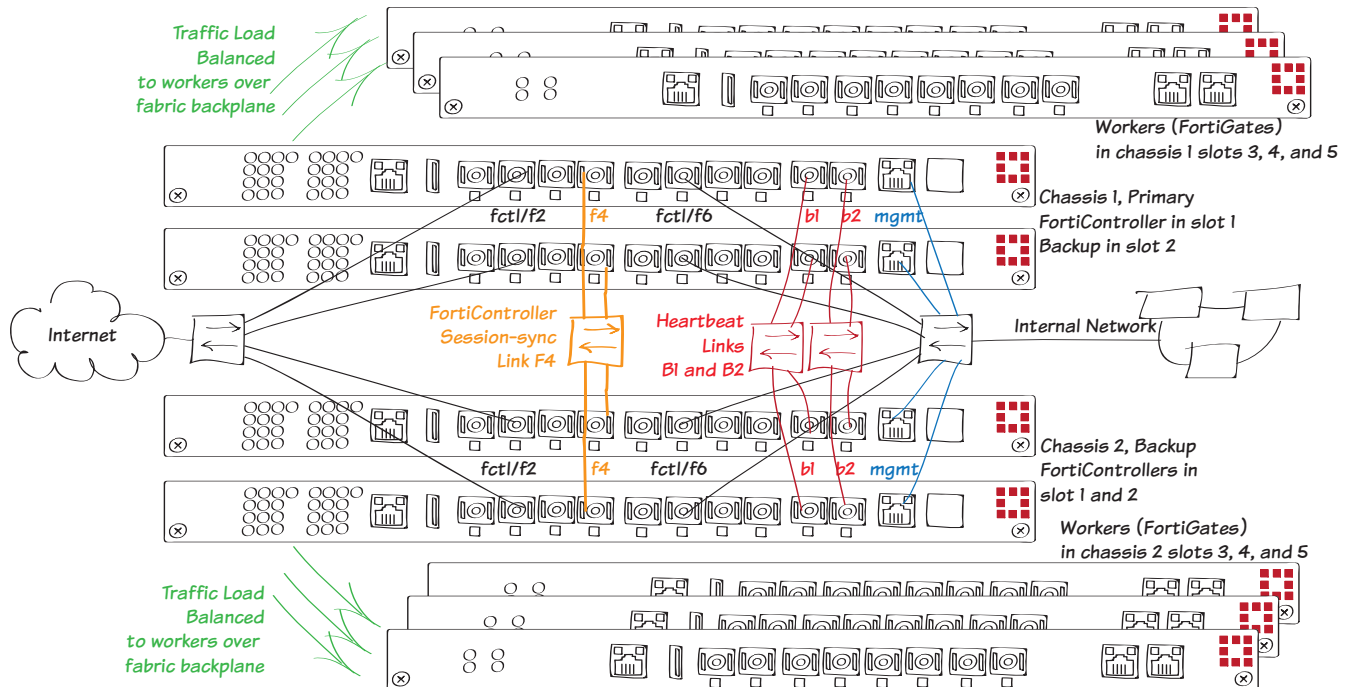
ch1-slot1(FT513B3912000029), Master(priority=0),
  ip=169.254.128.41, uptime=64732.98, chassis=1(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0

```

```
force-state(0:none)  hbdevs: local_interface=      b1 last_hb_  
time=68534.90  status=alive  
    local_interface=      b2 last_hb_time=    0.00  status=dead
```

Active-passive SLBC with four FortiController-5103Bs and two chassis

This example describes how to setup an active-passive session-aware load balancing cluster (SLBC) consisting of two FortiGate-5000 chassis, four FortiController-5103Bs, two in each chassis, and six FortiGate-5001Bs acting as workers, three in each chassis. This SLBC configuration can have up to seven redundant 10Gbit network connections.



The FortiControllers operate in active-passive HA mode for redundancy. The FortiController in chassis 1 slot 1 will be configured to be the primary unit, actively processing sessions. The other FortiControllers become the subordinate units.

In active-passive HA with two chassis and four FortiControllers, both chassis have two FortiControllers in active-passive HA mode and the same number of workers. Network connections are duplicated to the redundant FortiControllers in each chassis and between chassis for a total of four redundant data connections to each network.

All traffic is processed by the primary unit. If the primary unit fails, all traffic fails over to the chassis with two functioning FortiControllers and one of these FortiControllers becomes the new primary unit and processes all traffic. If the primary unit in the second chassis fails as well, one of the remaining FortiControllers becomes the primary unit and processes all traffic.

Heartbeat and base control and management communication is established between the chassis using the FortiController B1 and B2 interfaces. Only one heartbeat connection is required but redundant connections are recommended. Connect all of the B1 and all of the B2 interfaces together using switches. This example shows using one switch for the B1 connections and another for the B2 connections. You could also use one switch for both the B1 and B2 connections but using separate switches provides more redundancy.

The following VLAN tags and subnets are used by traffic on the B1 and B2 interfaces:

- Heartbeat traffic uses VLAN 999.
- Base control traffic on the 10.101.11.0/255.255.255.0 subnet uses VLAN 301.
- Base management on the 10.101.10.0/255.255.255.0 subnet uses VLAN 101.

This example also includes a FortiController session sync connection between the FortiControllers using the FortiController F4 front panel interface (resulting in the SLBC having a total of seven redundant 10Gbit network connections). (You can use any fabric front panel interface, F4 is used in this example to make the diagram clearer.) In a two chassis A-P mode cluster with two or four FortiControllers, the session sync ports of all FortiControllers must be connected to the same broadcast domain. You can do this by connecting all of the F4 interfaces to the same switch.

FortiController-5103B session sync traffic uses VLAN 2000.

This example sets the device priority of the FortiController in chassis 1 slot 1 higher than the device priority of the other FortiControllers to make sure that the FortiController in chassis 1 slot 1 becomes the primary FortiController for the cluster. Override is also enabled on the FortiController in chassis 1 slot 1. Override may cause the cluster to negotiate more often to select the primary unit. This makes it more likely that the unit that you select to be the primary unit will actually be the primary unit; but enabling override can also cause the cluster to negotiate more often.

Setting up the hardware

1. Install two FortiGate-5000 series chassis and connect them to power. Ideally each chassis should be connected to a separate power circuit.
2. Install the FortiControllers in slot 1 and slot 2 of each chassis.
3. Install the workers in slots 3, 4, and 5 of each chassis.
4. Power on both chassis.
5. Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally.
To check normal operation LED status see the [FortiGate-5000 hardware guides](#) and [FortiController hardware guides](#).
6. Create redundant connections from all four FortiController F1 front panel interfaces to the internet,
7. Create redundant connections from all four FortiController F6 interfaces to the internal network.
8. Create redundant connections from all four FortiController mgmt interfaces to a management network (in the example the mgmt interfaces are connected to the internal network).
9. Create a heartbeat link by connecting the four FortiController B1 interfaces together.
Create a secondary heartbeat link by connecting the four FortiController B2 interfaces together.
The switches used to connect the heartbeat interfaces must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). The heartbeat interfaces provide HA heartbeat, base control, and base management communication between the FortiControllers.
Only one heartbeat connection is required but redundant connections are recommended.
10. Create a FortiController session sync link between the chassis by connecting the four FortiController F4 interfaces together. If you use a switch it must allow traffic on the FortiController session sync VLAN (2000). You can use any of the F1 to F8 interfaces. We chose F4 in this example to make the diagram easier to understand.
11. Check the [FortiController release notes](#) for the latest supported FortiController and FortiGate firmware.
12. Get FortiController and FortiOS firmware from the [Fortinet Support site](#).
For FortiController firmware, select the **FortiSwitchATCA** product.

Configuring the FortiController in chassis 1 slot 1

This will become the primary FortiController. To make sure this is the primary FortiController it will be assigned the highest device priority and override will be enabled.

1. Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in chassis 1 slot 1 using the default IP address 192.168.1.99.
Or connect to the FortiController CLI through the console port (Baud Rate 9600bps, Data bits 8, Parity None, Stop bits 1, and Flow Control None).
2. Login using the admin administrator account and no password.
3. From the Dashboard System Information widget, set the **Host Name** to ch1-slot1. Or enter this command.

```
config system global
  set hostname ch1-slot1
end
```
4. Add a password for the admin administrator account. From the GUI use the **Administrators** widget or from the CLI enter this command.

```
config admin user
  edit admin
    set password <password>
  end
```
5. Change the FortiController mgmt interface IP address.
From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
  edit mgmt
    set ip 172.20.120.151/24
  end
```
6. If you need to add a default route for the management IP address, enter this command.

```
config route static
  edit route 1
    set gateway 172.20.120.2
  end
```
7. Set the chassis type that you are using, for example:

```
config system global
  set chassis-type fortigate-5140
end
```
8. Enable FortiController session sync.

```
config load-balance setting
  set session-sync enable
end
```
9. Configure Active-Passive HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.
10. Set **Mode** to **Active-Passive**, set the **Device Priority** to 250, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
5103-slot1	FT513B3912000051	Master	169.254.128.33	247020.05	0	0/1	1	1

Configure

Mode: Active-Passive

Device Priority (0-255):

Group ID(0-31):

Enable Override: ☒

Heartbeat interval(200-1000ms):

Number of heartbeats lost(2-255):

VLAN to use for HA heartbeat traffic(1-4094):

Enable Chassis Redundancy: ☒

Chassis ID(1 - 2):

Heartbeat Device

Available

mgmt

➔

➜

Selected

b1
b2

11. Enter the following command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
  set session-sync-port f4
end
```

You can also enter the complete HA configuration with this command:

```
config system ha
  set mode active-passive
  set groupid 5
  set priority 250
  set override enable
  set chassis-redundancy enable
  set chassis-id 1
  set hbdev b1 b2
  set session-sync-port f4
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different group ID. The default group ID of 0 is not a good choice and normally should be changed.

Enable Override is selected to make sure the FortiController in chassis 1 always becomes the primary unit. Enabling override could lead to the cluster renegotiating more often, so once the chassis is operating you can disable this setting.

You can also adjust other HA settings. For example, if the heartbeat interfaces are connected using a switch, you can change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on the switch. You can also adjust the **Heartbeat Interval** and **Number of Heartbeats** lost to adjust how quickly the cluster determines if one of the FortiControllers has failed.

Configuring the FortiController in chassis 1 slot 2

1. Log into the GUI or CLI of the FortiController in chassis 1 slot 2.
2. From the Dashboard System Information widget, set the **Host Name** to ch1-slot2. Or enter this command.

```
config system global
    set hostname ch1-slot2
end
```

3. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
    edit mgmt
        set ip 172.20.120.152/24
    end
```

4. Configure Active-Passive HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.
5. Set **Mode** to **Active-Passive**, set the **Device Priority** to 250, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.
6. Enter the following command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
    set session-sync-port f4
end
```

You can also enter the complete HA configuration with this command:

```
config system ha
    set mode active-passive
    set groupid 5
    set priority 250
    set override enable
    set chassis-redundancy enable
    set chassis-id 1
    set hbdev b1 b2
    set session-sync-port f4
end
```

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

Configuring the FortiController in chassis 2 slot 1

1. Log into the GUI or CLI of the FortiController in chassis 2 slot 1.
2. From the Dashboard System Information widget, set the **Host Name** to ch2-slot1. Or enter this command.

```
config system global
```

```
set hostname ch2-slot1
end
```

3. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
edit mgmt
set ip 172.20.120.251/24
end
```

4. Configure Active-Passive HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.
5. Set **Mode** to **Active-Passive**, set the **Device Priority** to 10, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 2 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.
6. Enter the following command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
set session-sync-port f4
end
```

You can also enter the complete HA configuration with this command:

```
config system ha
set mode active-passive
set groupid 5
set priority 10
set override enable
set chassis-redundancy enable
set chassis-id 2
set hbdev b1 b2
set session-sync-port f4
end
```

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

Configuring the FortiController in chassis 2 slot 2

1. Log into the GUI or CLI of the FortiController in chassis 2 slot 2.
2. From the Dashboard System Information widget, set the **Host Name** to ch2-slot2. Or enter this command.

```
config system global
set hostname ch2-slot2
end
```

3. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
edit mgmt
set ip 172.20.120.252/24
end
```

4. Configure Active-Passive HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.
5. Set **Mode** to **Active-Passive**, set the **Device Priority** to 10, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 2 and move the **b1** and **b2** interfaces to the **Selected** column and select

OK.

6. Enter the following command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
    set session-sync-port f4
end
```

You can also enter the complete HA configuration with this command:

```
config system ha
    set mode active-passive
    set groupid 5
    set priority 10
    set override enable
    set chassis-redundancy enable
    set chassis-id 2
    set hbdev b1 b2
    set session-sync-port f4
end
```

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

Configuring the cluster

After a short time the FortiControllers restart in HA mode and form an active-passive SLBC HA cluster. All of the FortiControllers must have the same HA configuration and at least one heartbeat link (the B1 and B2 interfaces) must be connected. If the FortiControllers are unable to form a cluster, check to make sure that they all have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

With the configuration described in the previous steps, the FortiController in chassis 1 slot 1 should become the primary unit and you can log into the cluster using the management IP address that you assigned to this FortiController.

The other FortiControllers become secondary FortiControllers. You cannot log into or manage the secondary FortiControllers until you configure the cluster External Management IP and add workers to the cluster. Once you do this, you can use the External Management IP address and a special port number to manage the secondary FortiControllers. You can also connect to any secondary FortiController CLI using their console port.

1. Confirm that the cluster has been formed. From the primary FortiController GUI **System Information** widget, beside **HA Status**, select **Configure**.

The display should show all four of the FortiControllers in the cluster. (The host names shown on some of the screen images in this example may not match the host names used in the example configuration.)

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
ch1-slot1	FT513B3912000029	Master	169.254.128.121	1075.00	0	0/3	1	1
ch2-slot1	FT513B3912000051	Slave	169.254.128.124	423.61	0	0/0	0	0
ch2-slot2	FT513B3913000168	Slave	169.254.128.123	273.87	0	0/3	0	1
ch1-slot2	FT513B3914000006	Slave	169.254.128.122	703.38	0	0/3	1	1

Configure

Mode: Active-Passive

Device Priority (0-255):

Group ID(0-31):

Enable Override: ☒

Heartbeat interval(200-1000ms):

Number of heartbeats lost(2-255):

VLAN to use for HA heartbeat traffic(1-4094):

Enable Chassis Redundancy: ☒

Chassis ID(1 - 2):

Heartbeat Device

Available

mgmt

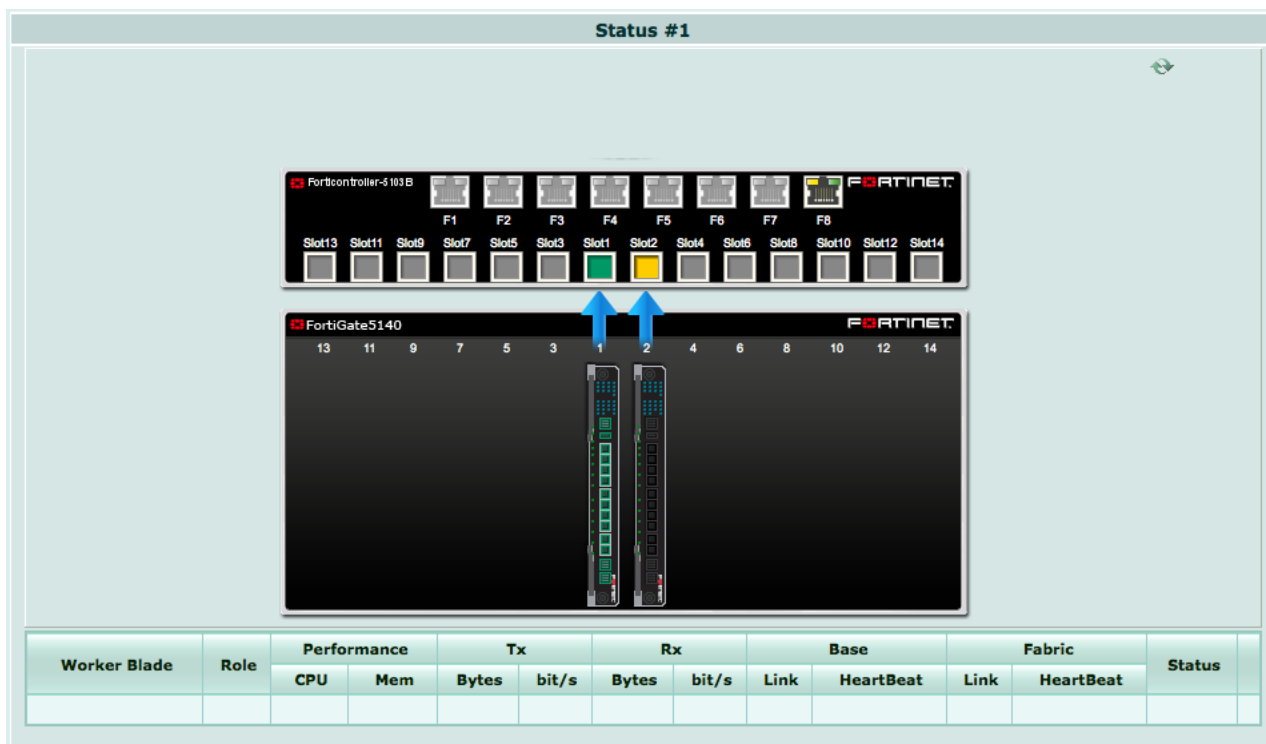
Selected

b1
b2

OK
Cancel

- Go to **Load Balance > Status** to see the status of the both FortiControllers.

The primary FortiController slot icon should be colored green. The secondary FortiController in the same chassis should also be visible, but with a yellow slot icon.



- Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured their status will be **Down**.

- Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure all of the devices in the cluster.

Config

Member Management

External Management IP/Netmask: 192.168.1.101/255.255.255.0

Internal Management Network: 10.101.10.0/255.255.255.0

Administrative Access:

☐ HTTPS ☐ PING ☐ HTTP ☐ FGFM

☐ SSH ☐ SNMP ☐ TELNET

Apply

Membership **Edit**

Worker Blade	Role	Weight	Status	
Slot #3	Active	5	⬇	🗑️ ✎️ 📄
Slot #4	Active	5	⬇	🗑️ ✎️ 📄
Slot #5	Active	5	⬇	🗑️ ✎️ 📄

You can also enter the following command to add slots 3, 4, and 5 to the cluster.

```
config load-balance setting
config slots
```

```

edit 3
next
edit 4
next
edit 5
end
end

```

You can also use the following CLI command to configure the external management IP/Netmask and management access to this address:

```

config load-balance setting
set base-mgmt-external-ip 172.20.120.100 255.255.255.0
set base-mgmt-allowaccess https ssh ping
end

```

5. Enable base **management** traffic between FortiControllers. The CLI syntax shows setting the default base management VLAN (101). You can also use this command to change the base management VLAN.

```

config load-balance setting
config base-mgmt-interfaces
edit b1
set vlan-id 101
next
edit b2
set vlan-id 101
end
end

```

6. Enable base **control** traffic between FortiControllers. The CLI syntax shows setting the default base control VLAN (301). You can also use this command to change the base management VLAN.

```

config load-balance setting
config base-ctrl-interfaces
edit b1
set vlan-id 301
next
edit b2
set vlan-id 301
end
end

```

Adding the workers to the cluster

1. Log into the CLI of each worker and enter the following command to reset the worker to its factory default settings.

```
execute factoryreset
```

If the workers are going to run FortiOS Carrier, add the FortiOS Carrier license instead. Adding the license also resets the worker to factory default settings.

2. Register each worker and apply licenses to each worker before adding them to the cluster.

This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMs). You should also install any third-party certificates on each worker before forming the cluster. FortiToken licenses can be added at any time because they are synchronized to all workers.

3. Optionally give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network.

These IP addresses are not synchronized, so you can connect to and manage each worker separately.

```
config system interface
    edit mgmt1
        set ip 172.20.120.120
    end
```

4. Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

```
config system global
    set hostname worker-chassis-1-slot-3
end
```

5. Enter the following command on each worker to enable FortiController mode.

```
config system elbc
    set mode forticontroller
end
```

The worker restarts and joins the cluster.

6. On the primary FortiController GUI go to **Load Balance > Status**.

As the workers in chassis 1 restart they should appear in their appropriate slots.

The primary worker should be the worker in chassis 1 slot 3. The primary FortiController status display includes a **Config Master** link that you can use to connect to the primary worker.

Status #1

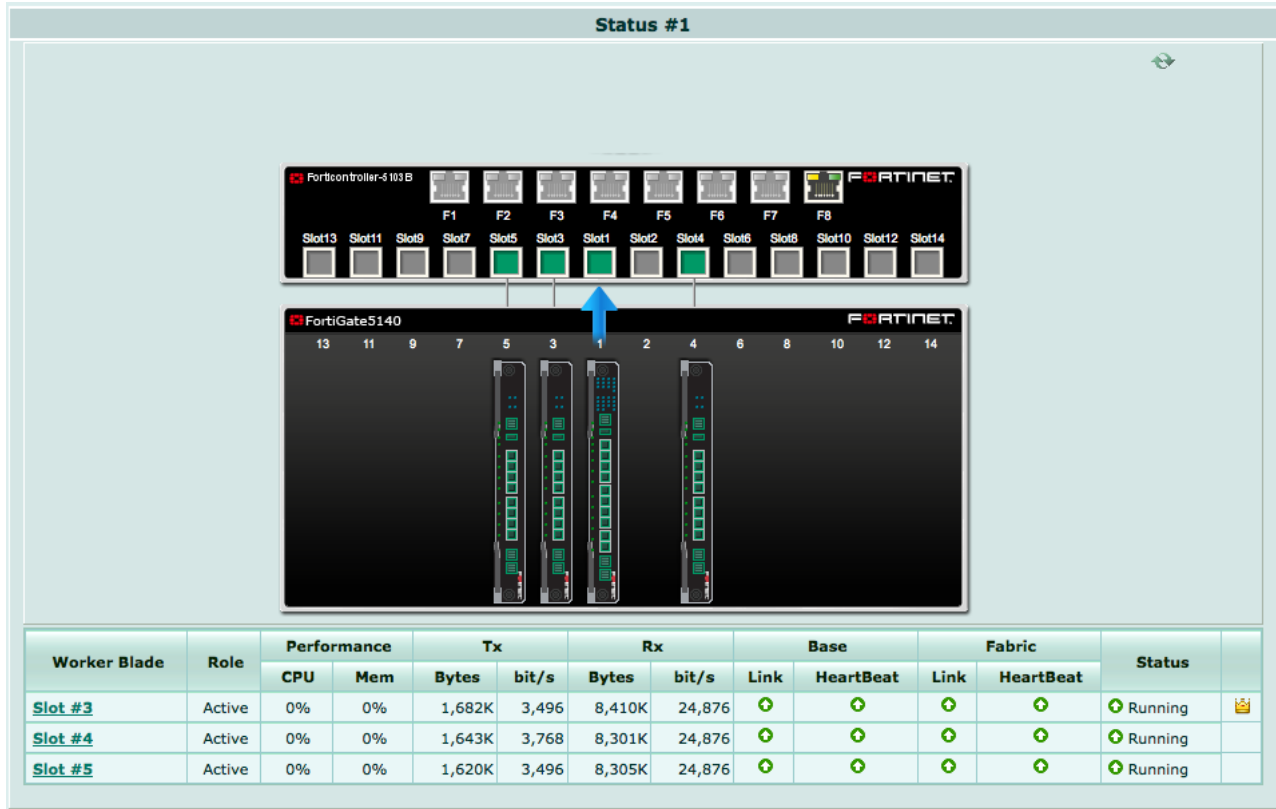
The diagram shows two chassis. The top chassis is a FortiController-5103B with 14 slots (Slot13 to Slot14). The bottom chassis is a FortiGate5140 with 14 slots (Slot13 to Slot14). A blue arrow points to Slot 1 in the FortiGate5140 chassis.

Worker Blade	Role	Performance		Tx		Rx		Base		Fabric		Status	
		CPU	Mem	Bytes	bit/s	Bytes	bit/s	Link	HeartBeat	Link	HeartBeat		
Slot #3	Active	0%	0%	443,698	3,768	4,951K	23,024	+	+	+	+	Running	👑🔧
Slot #4	Active	0%	0%	434,206	3,496	4,897K	23,024	+	+	+	+	Running	
Slot #5	Active	0%	0%	427,538	3,768	4,870K	23,024	+	+	+	+	Running	

7. Log into the secondary FortiController GUI (for example by browsing to <https://172.20.120.100:44321>) and go to **Load Balance > Status**.

As the workers in chassis 2 restart they should appear in their appropriate slots.

The secondary FortiController Status page shows the status of the workers in chassis 2 and does not include the **Config Master** link.



Operating and managing the cluster

You can now manage the workers in the same way as you would manage a standalone FortiGate. You can connect to the worker GUI or CLI using the **External Management IP**. If you had configured the worker mgmt1 or mgmt2 interfaces you can also connect to one of these addresses to manage the cluster.

To operate the cluster, connect networks to the FortiController front panel interfaces and connect to a worker GUI or CLI to configure the workers to process the traffic they receive. When you connect to the External Management IP, you connect to the primary worker. When you make configuration changes they are synchronized to all workers in the cluster.

You can use the external management IP followed by a special port number to manage individual devices in the cluster. For details, see [Managing the devices in an SLBC cluster with the External Management IP on page 29](#).

To manage a FortiController using SNMP you need to load the FORTINET-CORE-MIB.mib file into your SNMP manager. You can get this MIB file from the Fortinet support site, in the same location as the current FortiController firmware (select the FortiSwitchATCA product).

By default on the workers, all FortiController front panel interfaces are in the root VDOM. You can configure the root VDOM or create additional VDOMs and move interfaces into them.

For example, you could connect the internet to FortiController front panel interface 2 (fctrl/f2 on the worker GUI and CLI) and an internal network to FortiController front panel interface 6 (fctrl/f6 on the worker GUI and CLI). Then enter the root VDOM and add a policy to allow users on the internal network to access the internet.

Incoming Interface	fctrl/f6	+
Source Address	Internal_NET	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	fctrl/f2	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	✓ ACCEPT	

Firewall / Network Options

ON NAT

☒ Use Outgoing Interface Address

☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

Checking the cluster status

You can use the following get and diagnose commands to show the status of the cluster and all of the devices in it.

1. Log into the **primary FortiController** CLI and enter the following command to view the system status of the primary FortiController.

```
get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000029
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: chl-slot1
Current HA mode: a-p, master
System time: Sun Sep 14 08:16:25 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

2. Enter the following command to view the load balance status of the primary FortiController and its workers. The command output shows the workers in slots 3, 4, and 5, and status information about each one.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
Working: 3 [ 3 Active 0 Standby]
Ready: 0 [ 0 Active 0 Standby]
```

```
Dead:    0 [ 0 Active 0 Standby]
Total:   3 [ 3 Active 0 Standby]
```

```
Slot 3: Status:Working   Function:Active
Link:    Base: Up        Fabric: Up
Heartbeat: Management: Good Data: Good
Status Message:"Running"
Slot 4: Status:Working   Function:Active
Link:    Base: Up        Fabric: Up
Heartbeat: Management: Good Data: Good
Status Message:"Running"
Slot 5: Status:Working   Function:Active
Link:    Base: Up        Fabric: Up
Heartbeat: Management: Good Data: Good
Status Message:"Running"
```

3. Enter the following command from the primary FortiController to show the HA status of the FortiControllers.

The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (in this case 0 for each FortiController) the number of failed workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (`status=alive`) and the B2 interfaces are not (`status=dead`). The cluster can still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=4416.18,
chassis=1(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=          b1 best=yes
                           local_interface=          b2 best=no

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=1181.62,
chassis=2(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=          b1 last_hb_time=
4739.97 status=alive
                           local_interface=          b2 last_hb_time=    0.00 status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=335.79,
chassis=2(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=          b1 last_hb_time=
4739.93 status=alive
                           local_interface=          b2 last_hb_time=    0.00 status=dead
```

```

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4044.46,
chassis=1(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=          b1 last_hb_time=
4740.03    status=alive
          local_interface=          b2 last_hb_time=    0.00    status=dead

```

4. Log into the chassis 1 slot 2 FortiController CLI and enter this command to view the status of this secondary FortiController.

To log in with SSH: `ssh admin@172.20.120.100 -p2202`

```

get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3914000006
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: ch1-slot2
Current HA mode: a-p, backup
System time: Sun Sep 14 12:44:58 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)

```

5. Enter the following command to view the status of this secondary FortiController and its workers.

```

get load-balance status
ELBC Master Blade: slot-3
  Confsync Master Blade: slot-3
  Blades:
    Working:  3 [  3 Active  0 Standby]
    Ready:    0 [  0 Active  0 Standby]
    Dead:     0 [  0 Active  0 Standby]
    Total:    3 [  3 Active  0 Standby]

    Slot 3: Status:Working  Function:Active
      Link:      Base: Up      Fabric: Up
      Heartbeat: Management: Good  Data: Good
      Status Message:"Running"
    Slot 4: Status:Working  Function:Active
      Link:      Base: Up      Fabric: Up
      Heartbeat: Management: Good  Data: Good
      Status Message:"Running"
    Slot 5: Status:Working  Function:Active
      Link:      Base: Up      Fabric: Up
      Heartbeat: Management: Good  Data: Good
      Status Message:"Running"

```

6. Enter the following command from the FortiController in chassis 1 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 1 slot 2 is shown first.

```

diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4292.69,

```

```

chassis=1(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=      b1 best=yes
                        local_interface=            b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=4664.49,
chassis=1(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time= 4958.88
status=alive
                        local_interface=            b2 last_hb_time=  0.00    status=dead

                        ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123,
uptime=1429.99, chassis=2(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time= 4958.88
status=alive
                        local_interface=            b2 last_hb_time=  0.00    status=dead

                        ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=584.20,
chassis=2(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time= 4958.88
status=alive
                        local_interface=            b2 last_hb_time=  0.00    status=dead

```

7. Log into the **chassis 2 slot 1 FortiController CLI** and enter the following command to view the status of this secondary FortiController.

To log in with SSH: `ssh admin@172.20.120.100 -p2221`

```

get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000051
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: ch2-slot1
Current HA mode: a-p, backup
System time: Sun Sep 14 12:53:09 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)

```

8. Enter the following command to view the status of this secondary FortiController and its workers.

```

get load-balance status
  ELBC Master Blade: slot-3
  Confsync Master Blade: N/A
  Blades:
    Working:  3 [  3 Active  0 Standby]
    Ready:    0 [  0 Active  0 Standby]
    Dead:     0 [  0 Active  0 Standby]
    Total:    3 [  3 Active  0 Standby]

    Slot  3: Status:Working  Function:Active
    Link:      Base: Up      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"

    Slot  4: Status:Working  Function:Active
    Link:      Base: Up      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"

    Slot  5: Status:Working  Function:Active
    Link:      Base: Up      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"

```

9. Enter the following command from the FortiController in chassis 2 slot 1 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 2 slot 1 is shown first.

```

diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch2-slot1(FT513B3912000051), Slave
(priority=2), ip=169.254.128.123, uptime=1858.71, chassis=2(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none) hbdevs: local_interface= b1 best=yes
      local_interface= b2 best=no

ch1-slot1(FT513B3912000029), Master
(priority=0), ip=169.254.128.121, uptime=5093.30, chassis=1(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none) hbdevs: local_interface= b1 last_hb_
time= 2074.15 status=alive
      local_interface= b2 last_hb_time= 0.00 status=dead

ch2-slot2(FT513B3913000168), Slave
(priority=3), ip=169.254.128.124, uptime=1013.01, chassis=2(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none) hbdevs: local_interface= b1 last_hb_

```

```

time= 2074.15    status=alive
                local_interface=          b2 last_hb_time=    0.00    status=dead

ch1-slot2(FT513B3914000006), Slave
(priority=1), ip=169.254.128.122, uptime=4721.60, chassis=1(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)    hbdevs: local_interface=          b1 last_hb_
time= 2074.17    status=alive
                local_interface=          b2 last_hb_time=    0.00    status=dead

```

- 10. Log into the chassis 2 slot 2 FortiController CLI and enter the following command to view the status of this secondary FortiController.**

To log in with SSH: `ssh admin@172.20.120.100 -p2222`

```

get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3913000168
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: ch2-slot2
Current HA mode: a-p, secondary
System time: Sun Sep 14 12:56:45 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)

```

- 11. Enter the following command to view the status of the secondary FortiController and its workers.**

```

get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: N/A
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]

Slot  3: Status:Working  Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"

Slot  4: Status:Working  Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"

Slot  5: Status:Working  Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"

```

- 12. Enter the following command from the FortiController in chassis 2 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 2 slot 2 is shown first.**

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=1276.77, chassis=2(1)
slot: 2
sync: conf_sync=1, elbc_sync=1
session: total=0, session_sync=in sync
state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none) hbdevs: local_interface= b1 best=yes
local_interface= b2 best=no

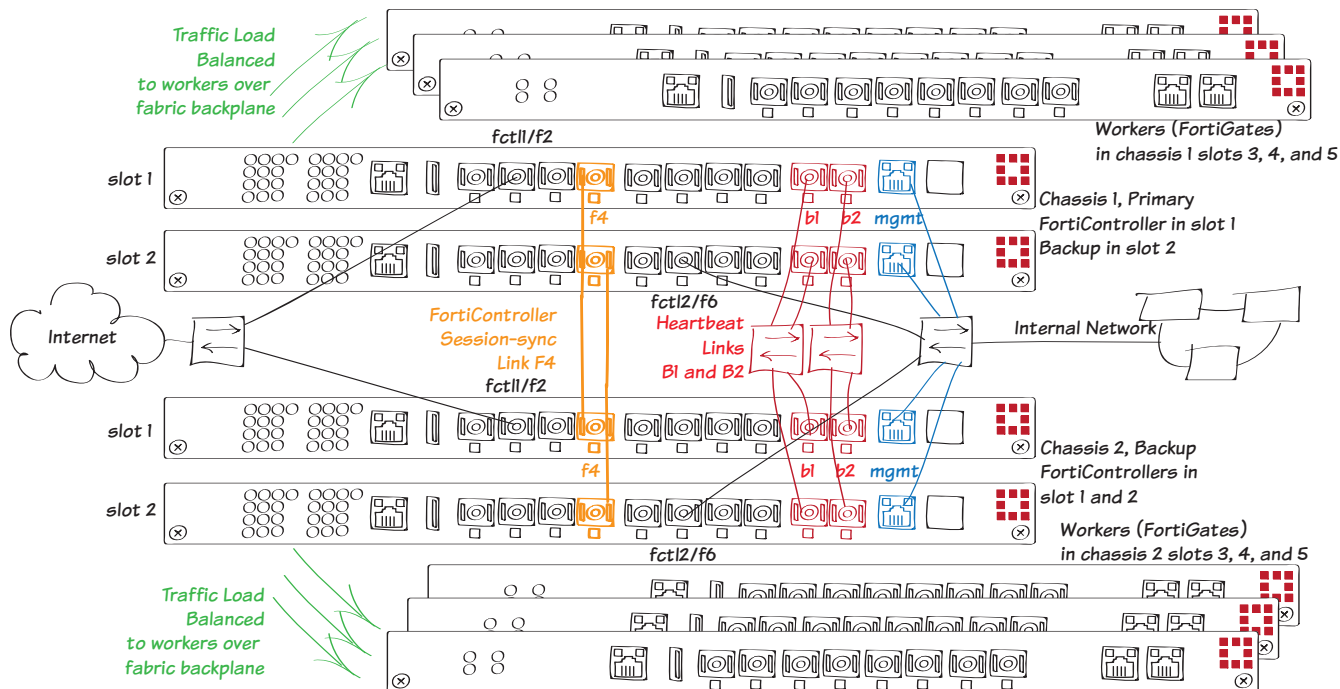
ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=5356.98, chassis=1(1)
slot: 1
sync: conf_sync=1, elbc_sync=1, conn=3(connected)
session: total=0, session_sync=in sync
state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none) hbdevs: local_interface= b1 last_hb_time= 1363.89 status=alive
local_interface= b2 last_hb_time= 0.00 status=dead

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=2122.58, chassis=2(1)
slot:
sync: conf_sync=1, elbc_sync=1, conn=3(connected)
session: total=0, session_sync=in sync
state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none) hbdevs: local_interface= b1 last_hb_time= 1363.97 status=alive
local_interface= b2 last_hb_time= 0.00 status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4985.27, chassis=1(1)
slot: 2
sync: conf_sync=1, elbc_sync=1, conn=3(connected)
session: total=0, session_sync=in sync
state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none) hbdevs: local_interface= b1 last_hb_time= 1363.89 status=alive
local_interface= b2 last_hb_time= 0.00 status=dead
```


Dual mode SLBC with four FortiController-5103Bs and two chassis

This example describes how to setup a dual-mode session-aware load balancing cluster (SLBC) consisting of two FortiGate-5000 chassis, four FortiController-5103Bs two in each chassis, and six FortiGate-5001Bs acting as workers, three in each chassis. This SLBC configuration can have up to 14 redundant 10Gbit network connections.



In this dual mode configuration, the FortiController in chassis 1 slot 1 is configured to become the primary unit. Both of the FortiControllers in chassis 1 receive traffic and load balance it to the workers in chassis 1. In dual mode configuration the front panel interfaces of both FortiControllers are active. All networks have single connections to the FortiController in slot 1 or the FortiController in slot 2. It is a best practice in a dual-mode configuration to distribute traffic evenly between the FortiControllers. So in this example, ingress traffic from the Internet is processed by the FortiController in slot 1 and egress traffic for the internal network is processed by the FortiController in slot 2.



Redundant connections to a network from the FortiControllers in the same chassis is not supported (unless you configure link aggregation).

The front panel F1 to F8 interfaces of the FortiController in slot 1 are named fctr1/f1 to fctr1/f8 and the front panel F1 to F8 interfaces of the FortiController in slot 2 are named fctr2/f1 to fctr2/f8.

The network connections to the FortiControllers in chassis 1 are duplicated with the FortiControllers in chassis 2. If one of the FortiControllers in chassis 1 fails, the FortiController in chassis 2 slot 1 becomes the primary FortiController and all traffic fails over to the FortiControllers in chassis 2. If one of the FortiControllers in chassis 2 fails, the remaining

FortiController in chassis 2 keeps processing traffic received by its front panel interfaces. Traffic to and from the failed FortiController is lost.

Heartbeat and base control and management communication is established between the chassis using the FortiController B1 and B2 interfaces. Only one heartbeat connection is required but redundant connections are recommended. Connect all of the B1 and all of the B2 interfaces together using switches. This example shows using one switch for the B1 connections and another for the B2 connections. You could also use one switch for both the B1 and B2 connections but using separate switches provides more redundancy.

The following VLAN tags and subnets are used by traffic on the B1 and B2 interfaces:

- Heartbeat traffic uses VLAN 999.
- Base control traffic on the 10.101.11.0/255.255.255.0 subnet uses VLAN 301.
- Base management on the 10.101.10.0/255.255.255.0 subnet uses VLAN 101.

This example also includes a FortiController session sync connection between the FortiControllers using the FortiController F4 front panel interface (resulting in the SLBC having a total of 14 redundant 10Gbit network connections). (You can use any fabric front panel interface, F4 is used in this example to make the diagram clearer.)

In a two chassis dual mode cluster, session sync ports need to be 1-to-1 connected according to chassis slot. So F4 from the FortiController in chassis 1 slot 1 needs to be connected to F4 in chassis 2 slot 1. And, F4 in chassis 1 slot 2 needs to be connected to F4 in chassis 2 slot 2. Because these are 1 to 1 connections you can use patch cables to connect them. You can also make these connections through a switch.

FortiController-5103B session sync traffic uses VLAN 2000.

This example sets the device priority of the FortiController in chassis 1 slot 1 higher than the device priority of the other FortiControllers to make sure that the FortiController in chassis 1 slot 1 becomes the primary FortiController for the cluster. Override is also enabled on the FortiController in chassis 1 slot 1. Override may cause the cluster to negotiate more often to select the primary unit. This makes it more likely that the unit that you select to be the primary unit will actually be the primary unit; but enabling override can also cause the cluster to negotiate more often.

Setting up the hardware

1. Install two FortiGate-5000 series chassis and connect them to power. Ideally each chassis should be connected to a separate power circuit.
2. Install the FortiControllers in slot 1 and slot 2 of each chassis.
3. Install the workers in slots 3, 4, and 5 of each chassis.
4. Power on both chassis.
5. Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally.
To check normal operation LED status see the [FortiGate-5000 hardware guides](#) and [FortiController hardware guides](#).
6. Create redundant connections from the F2 interfaces of the FortiControllers in slot 1 of both chassis to the internet.
In the FortiOS GUI or CLI, this is the fct1/f2 interface.
7. Create redundant connections from the F6 interfaces of the FortiControllers in slot 2 of both chassis to the internal network.
In the FortiOS GUI or CLI, this is the fct2/f6 interface.
8. Create redundant connections from all four FortiController mgmt interfaces to a management network (in the example the mgmt interfaces are connected to the internal network).
9. Create a heartbeat link by connecting the four FortiController B1 interfaces together.

Create a secondary heartbeat link by connecting the four FortiController B2 interfaces together.

The switches used to connect the heartbeat interfaces must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). The heartbeat interfaces provide HA heartbeat, base control, and base management communication between the FortiControllers.

Only one heartbeat connection is required but redundant connections are recommended.

10. Create a FortiController session sync link between the chassis by connecting the four FortiController F4 interfaces together. If you use a switch it must allow traffic on the FortiController session sync VLAN (2000). You can use any of the F1 to F8 interfaces. We chose F4 in this example to make the diagram easier to understand.
11. Check the [FortiController release notes](#) for the latest supported FortiController and FortiGate firmware.
12. Get FortiController and FortiOS firmware from the [Fortinet Support site](#).
For FortiController firmware, select the **FortiSwitchATCA** product.

Configuring the FortiController in chassis 1 slot 1

This will become the primary FortiController. To make sure this is the primary FortiController it will be assigned the highest device priority and override will be enabled.

1. Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in chassis 1 slot 1 using the default IP address 192.168.1.99.
Or connect to the FortiController CLI through the console port (Baud Rate 9600bps, Data bits 8, Parity None, Stop bits 1, and Flow Control None).
2. Login using the admin administrator account and no password.
3. From the Dashboard System Information widget, set the **Host Name** to ch1-slot1. Or enter this command.

```
config system global
    set hostname ch1-slot1
end
```

4. Add a password for the admin administrator account. From the GUI use the **Administrators** widget or from the CLI enter this command.

```
config admin user
    edit admin
        set password <password>
    end
```

5. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
    edit mgmt
        set ip 172.20.120.151/24
    end
```

6. If you need to add a default route for the management IP address, enter this command.

```
config route static
    edit route 1
        set gateway 172.20.120.2
    end
```

7. Set the chassis type that you are using, for example:

```
config system global
    set chassis-type fortigate-5140
end
```

8. Enable FortiController session sync.

```
config load-balance setting
    set session-sync enable
end
```

9. Configure Dual mode HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

10. Set **Mode** to **Dual Mode**, set the **Device Priority** to 250, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
ch1-slot1	FT513B3912000051	Master	169.254.128.89	4772.75	0	1/1	0	1

Configure

Mode: Dual Mode

Device Priority (0-255): 250

Group ID(0-31): 25

Enable Override: ☒

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy: ☒

Chassis ID(1 - 2): 1

Heartbeat Device

Available: mgmt

Selected: b1, b2

OK Cancel

11. Enter the following command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
    set session-sync-port f4
end
```

You can also enter the complete HA configuration with this command:

```
config system ha
    set mode dual
    set groupid 25
    set priority 250
    set chassis-redundancy enable
    set chassis-id 1
    set hbdev b1 b2
    set session-sync-port f4
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different group ID. The default group ID of 0 is not a good choice and normally should be changed.

Enable Override is selected to make sure the FortiController in chassis 1 always becomes the primary unit. Enabling override could lead to the cluster renegotiating more often, so once the chassis is operating you can disable this setting.

You can also adjust other HA settings. For example, if the heartbeat interfaces are connected using a switch, you can change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on the switch. You can also adjust the **Heartbeat Interval** and **Number of Heartbeats** lost to adjust how quickly the cluster determines if one of the FortiControllers has failed.

Configuring the FortiController in chassis 1 slot 2

1. Log into the GUI or CLI of the FortiController in chassis 1 slot 2.
2. From the Dashboard System Information widget, set the **Host Name** to ch1-slot2. Or enter this command.

```
config system global
    set hostname ch1-slot2
end
```

3. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
    edit mgmt
        set ip 172.20.120.152/24
    end
```

4. Configure Dual Mode HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.
5. Set **Mode** to **Dual Mode**, set the **Device Priority** to 10, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.
6. Enter the following command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
    set session-sync-port f4
end
```

You can also enter the complete HA configuration with this command:

```
config system ha
    set mode dual
    set groupid 25
    set priority 10
    set override enable
    set chassis-redundancy enable
    set chassis-id 1
    set hbdev b1 b2
    set session-sync-port f4
end
```

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

Configuring the FortiController in chassis 2 slot 1

1. Log into the GUI or CLI of the FortiController in chassis 2 slot 1.
2. From the Dashboard System Information widget, set the **Host Name** to ch2-slot1. Or enter this command.

```
config system global
    set hostname ch2-slot1
end
```

3. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
    edit mgmt
        set ip 172.20.120.251/24
    end
```

4. Configure Dual Mode HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.
5. Set **Mode** to **Dual Mode**, set the **Device Priority** to 10, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 2 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.
6. Enter the following command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
    set session-sync-port f4
end
```

You can also enter the complete HA configuration with this command:

```
config system ha
    set mode dual
    set groupid 25
    set priority 10
    set override enable
    set chassis-redundancy enable
    set chassis-id 2
    set hbdev b1 b2
    set session-sync-port f4
end
```

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

Configuring the FortiController in chassis 2 slot 2

1. Log into the GUI or CLI of the FortiController in chassis 2 slot 2.
2. From the Dashboard System Information widget, set the **Host Name** to ch2-slot2. Or enter this command.

```
config system global
    set hostname ch2-slot2
end
```

3. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
    edit mgmt
```

```
set ip 172.20.120.252/24
end
```

4. Configure Dual Mode HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.
5. Set **Mode** to **Dual Mode**, set the **Device Priority** to 10, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 2 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.
6. Enter the following command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
set session-sync-port f4
end
```

You can also enter the complete HA configuration with this command:

```
config system ha
set mode dual
set groupid 25
set priority 10
set override enable
set chassis-redundancy enable
set chassis-id 2
set hbdev b1 b2
set session-sync-port f4
end
```

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

Configuring the cluster

After a short time, the FortiControllers restart in HA mode and form a dual mode active-passive SLBC HA cluster. All of the FortiControllers must have the same HA configuration and at least one heartbeat link (the B1 and B2 interfaces) must be connected. If the FortiControllers are unable to form a cluster, check to make sure that they all have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

With the configuration described in the previous steps, the FortiController in chassis 1 slot 1 should become the primary FortiController and you can log into the cluster using the management IP address that you assigned to this FortiController.

The other FortiControllers become secondary FortiControllers. You cannot log into or manage the secondary FortiControllers until you configure the cluster External Management IP and add workers to the cluster. Once you do this, you can use the External Management IP address and a special port number to manage the secondary FortiControllers. You can also connect to any backup FortiController CLI using their console port.

1. Confirm that the cluster has been formed. From the primary FortiController GUI **System Information** widget, beside **HA Status**, select **Configure**.

The display should show all four of the FortiControllers in the cluster. (The host names shown on some of the screen images in this example may not match the host names used in the example configuration.)

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
ch1-slot1	FT513B3912000029	Master	169.254.128.201	1095.42	0	0/3	1	1
ch2-slot1	FT513B3912000051	Slave	169.254.128.203	843.96	0	0/3	1	1
ch2-slot2	FT513B3913000168	Slave	169.254.128.204	829.83	0	0/3	1	1
ch1-slot2	FT513B3914000006	Slave	169.254.128.202	861.79	0	0/3	1	1

Configure

Mode: Dual Mode

Device Priority (0-255): 128

Group ID(0-31): 25

Enable Override: ☐

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy: ☒

Chassis ID(1 - 2): 1

Heartbeat Device

Available

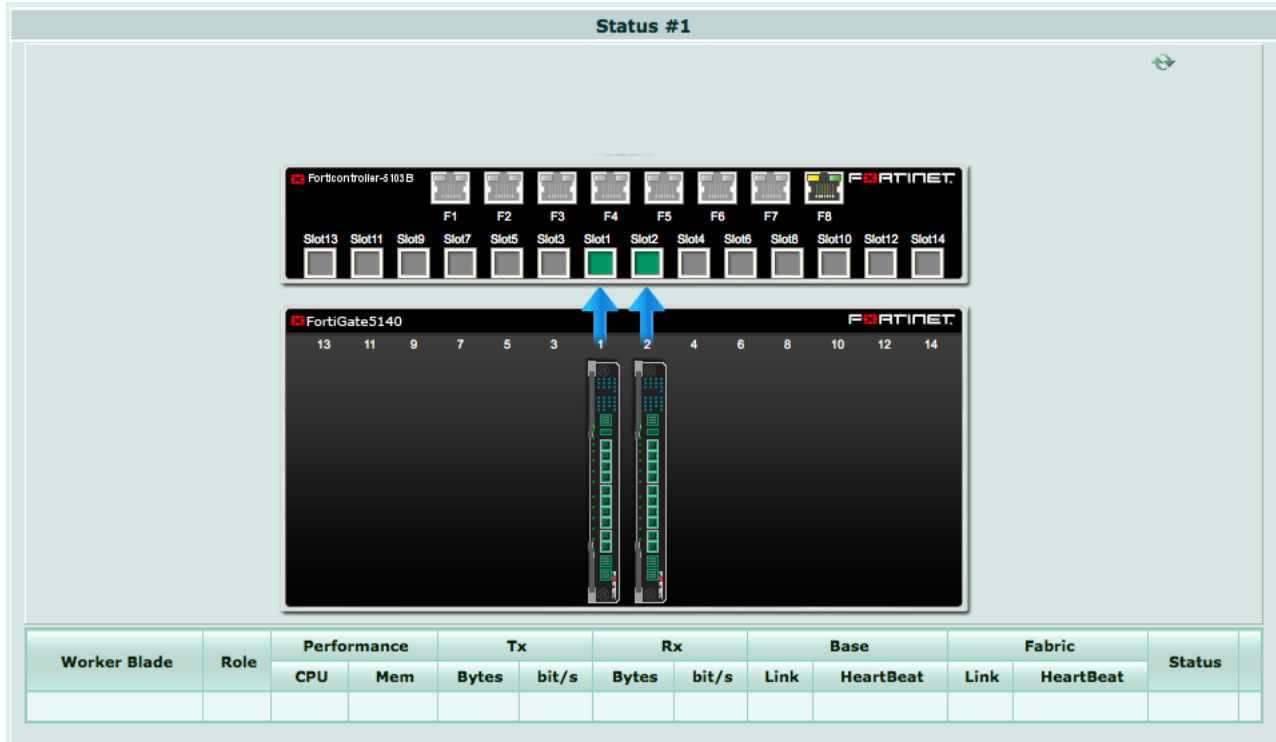
mgmt

Selected

b1
b2

OK
Cancel

2. Go to **Load Balance > Status** to see the status of the FortiControllers in chassis 1.
Both FortiController slot icons should be green because both FortiControllers can process traffic.



- Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.
- The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured for SLBC operation their status will be **Down**.
- Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure all of the devices in the cluster.

Config

Member Management

External Management IP/Netmask: 192.168.1.101/255.255.255.0

Internal Management Network: 10.101.10.0/255.255.255.0

Administrative Access:

☐ HTTPS ☐ PING ☐ HTTP ☐ FGFM

☐ SSH ☐ SNMP ☐ TELNET

Apply

Membership **Edit**

Worker Blade	Role	Weight	Status	
Slot #3	Active	5	⬇	🗑️ ✎️ ↕️
Slot #4	Active	5	⬇	🗑️ ✎️ ↕️
Slot #5	Active	5	⬇	🗑️ ✎️ ↕️

- Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure all of the devices in the cluster.

Config

Member Management
 External Management IP/Netmask
 Internal Management Network
 Administrative Access

192.168.1.101/255.255.255.0

10.101.10.0/255.255.255.0

☐ HTTPS

☐ PING

☐ HTTP

☐ FGFM

☐ SSH

☐ SNMP

☐ TELNET

Apply

Membership

Edit

Worker Blade	Role	Weight	Status	
Slot #3	Active	5	+	
Slot #4	Active	5	+	
Slot #5	Active	5	+	

You can also enter the following command to add slots 3, 4, and 5 to the cluster.

```
config load-balance setting
  config slots
    edit 3
    next
    edit 4
    next
    edit 5
    end
  end
```

You can also use the following CLI command to configure the external management IP/Netmask and management access to this address:

```
config load-balance setting
  set base-mgmt-external-ip 172.20.120.100 255.255.255.0
  set base-mgmt-allowaccess https ssh ping
end
```

6. Enable base **management** traffic between FortiControllers. The CLI syntax shows setting the default base management VLAN (101). You can also use this command to change the base management VLAN.

```
config load-balance setting
  config base-mgmt-interfaces
    edit b1
      set vlan-id 101
    next
    edit b2
      set vlan-id 101
    end
  end
```

7. Enable base **control** traffic between FortiControllers. The CLI syntax shows setting the default base control VLAN (301). You can also use this command to change the base management VLAN.

```
config load-balance setting
  config base-ctrl-interfaces
    edit b1
      set vlan-id 301
    next
    edit b2
```

FortiController 5.2.10 Session-Aware Load Balancing (SLBC) Guide

122

```
        set vlan-id 301
    end
end
```

Adding the workers to the cluster

1. Log into the CLI of each worker and enter the following command to reset the worker to its factory default settings.

```
execute factoryreset
```

If the workers are going to run FortiOS Carrier, add the FortiOS Carrier license instead. Adding the license also resets the worker to factory default settings.

2. Register each worker and apply licenses to each worker before adding them to the cluster.

This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMs). You should also install any third-party certificates on each worker before forming the cluster. FortiToken licenses can be added at any time because they are synchronized to all workers.

3. Optionally give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network.

These IP addresses are not synchronized, so you can connect to and manage each worker separately.

```
config system interface
    edit mgmt1
        set ip 172.20.120.120
    end
```

4. Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

```
config system global
    set hostname worker-chassis-1-slot-3
end
```

5. Enter the following command on each worker to enable dual FortiController mode.

```
config system elbc
    set mode dual-forticontroller
end
```

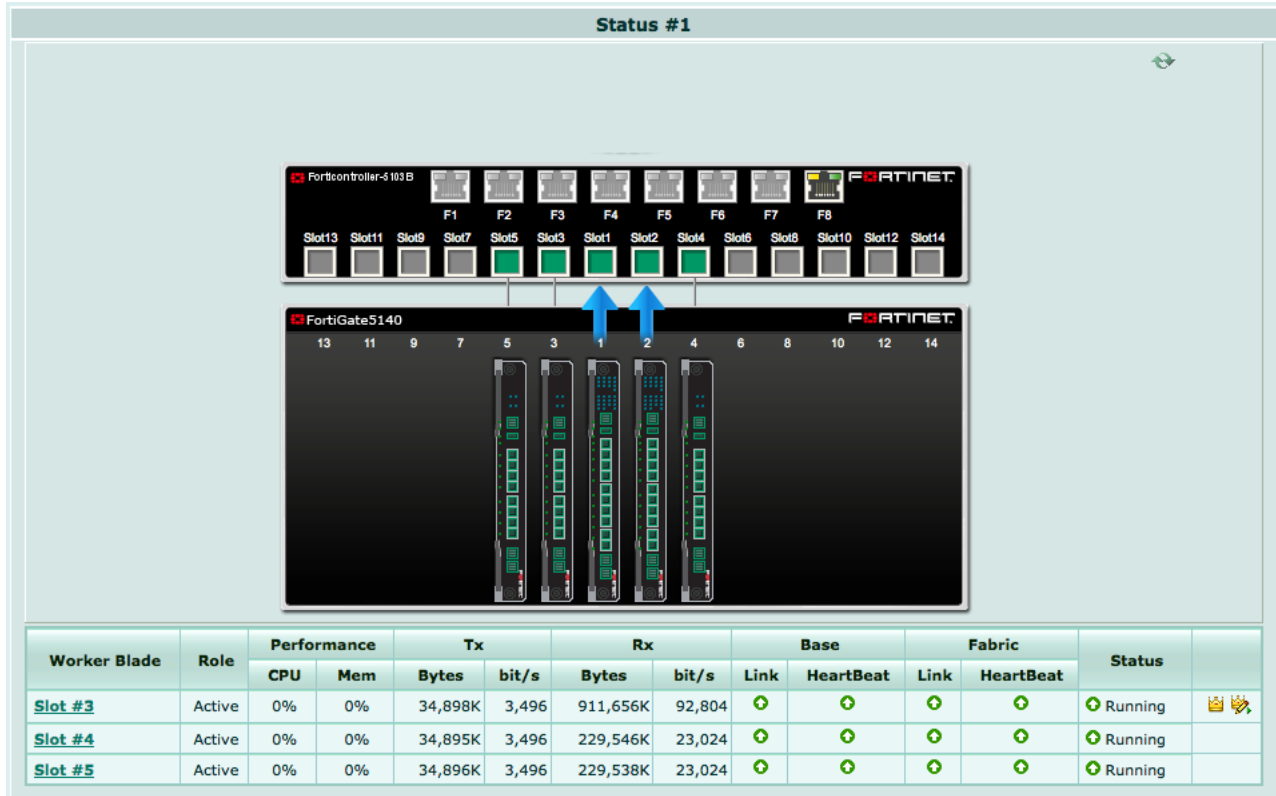
The worker restarts and joins the cluster.

6. Repeat these steps for each worker in both chassis.

7. On the primary FortiController GUI go to **Load Balance > Status**.

As the workers in chassis 1 restart they should appear in their appropriate slots.

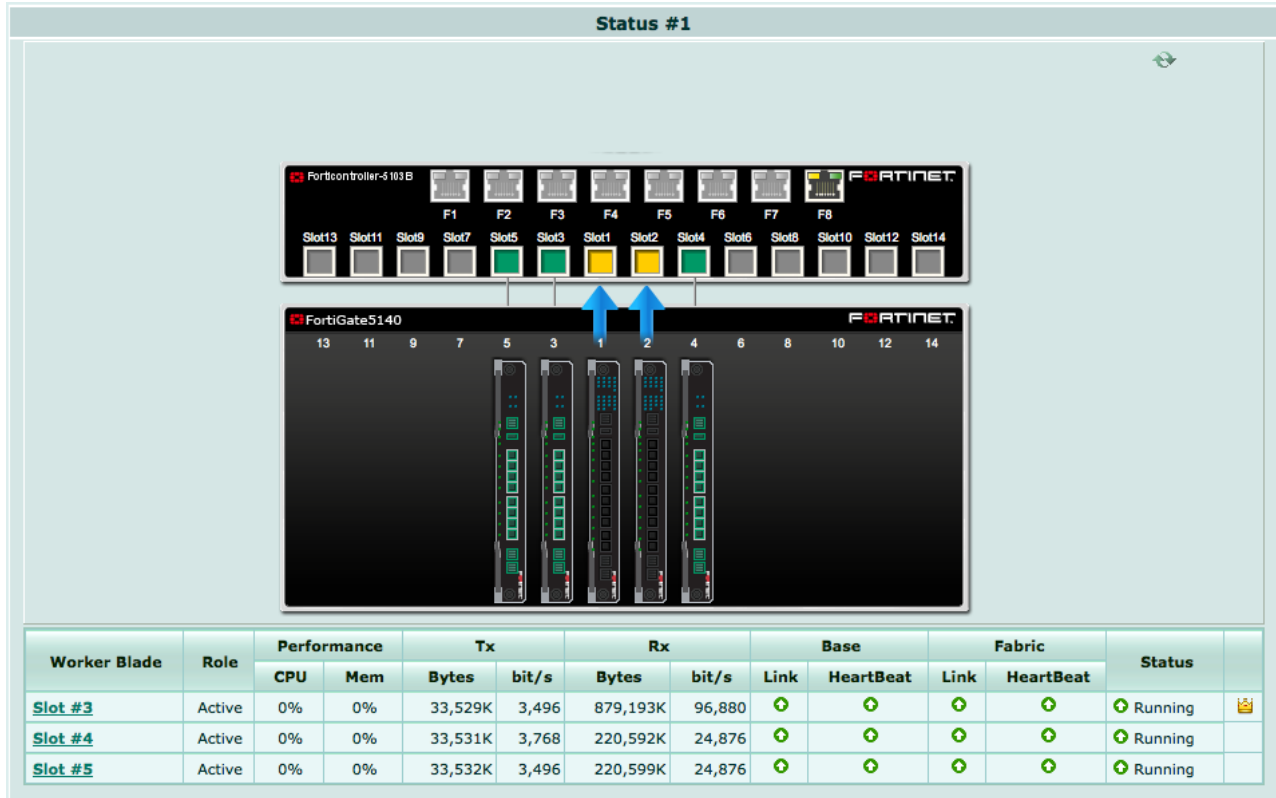
The primary worker should be the worker in chassis 1 slot 3. The primary FortiController status display includes a **Config Master** link that you can use to connect to the primary worker.



8. Log into the secondary FortiController GUI (for example by browsing to <https://172.20.120.100:44321>) and go to **Load Balance > Status**.

As the workers in chassis 2 restart they should appear in their appropriate slots.

The secondary FortiController Status page shows the status of the workers in chassis 2 and does not include the **Config Master** link.



Operating and managing the cluster

You can now manage the workers in the same way as you would manage a standalone FortiGate. You can connect to the worker GUI or CLI using the **External Management IP**. If you had configured the worker mgmt1 or mgmt2 interfaces you can also connect to one of these addresses to manage the cluster.

To operate the cluster, connect networks to the FortiController front panel interfaces and connect to a worker GUI or CLI to configure the workers to process the traffic they receive. When you connect to the External Management IP, you connect to the primary worker. When you make configuration changes they are synchronized to all workers in the cluster.

You can use the external management IP followed by a special port number to manage individual devices in the cluster. For details, see [Managing the devices in an SLBC cluster with the External Management IP on page 29](#).

To manage a FortiController using SNMP you need to load the FORTINET-CORE-MIB.mib file into your SNMP manager. You can get this MIB file from the Fortinet support site, in the same location as the current FortiController firmware (select the FortiSwitchATCA product).

By default on the workers, all FortiController front panel interfaces are in the root VDOM. You can configure the root VDOM or create additional VDOMs and move interfaces into them.

For example, you could connect the internet to FortiController front panel interface 2 (fctrl/f2 on the worker GUI and CLI) and an internal network to FortiController front panel interface 6 (fctrl/f6 on the worker GUI and CLI). Then enter the root VDOM and add a policy to allow users on the internal network to access the internet.

Incoming Interface	fctrl/f6	+
Source Address	Internal_NET	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	fctrl/f2	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	

Firewall / Network Options

ON NAT

☒ Use Outgoing Interface Address
 ☐ Fixed Port

☐ Use Dynamic IP Pool

Checking the cluster status

1. Log into the **primary FortiController** CLI and enter the following command to view the system status of the primary FortiController.

```
get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000029
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: chl-slot1
Current HA mode: dual, master
System time: Mon Sep 15 10:11:48 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time (US&Canada)
```

2. Enter the following command to view the load balance status of the primary FortiController and its workers. The command output shows the workers in slots 3, 4, and 5, and status information about each one.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
  Working: 3 [ 3 Active 0 Standby]
  Ready:   0 [ 0 Active 0 Standby]
  Dead:    0 [ 0 Active 0 Standby]
  Total:   3 [ 3 Active 0 Standby]
```

```

Slot 3: Status:Working   Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good   Data: Good
Status Message:"Running"
Slot 4: Status:Working   Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good   Data: Good
Status Message:"Running"
Slot 5: Status:Working   Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good   Data: Good
Status Message:"Running"
Heartbeat: Management: Good   Data: Good
Status Message:"Running"

```

3. Enter the following command from the primary FortiController to show the HA status of the FortiControllers.

The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (in this case 0 for each FortiController) the number of failed workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (status=alive) and the B2 interfaces are not (status=dead). The cluster can still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```

diagnose system ha status
mode: dual
minimize chassis failover: 1
ch1-slot1 (FT513B3912000029), Master (priority=0), ip=169.254.128.201, uptime=1517.38,
chassis=1 (1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)   hbdevs: local_interface=      b1 best=yes
                           local_interface=      b2 best=no

ch2-slot1 (FT513B3912000051), Slave (priority=2), ip=169.254.128.203, uptime=1490.50,
chassis=2 (1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3 (connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)   hbdevs: local_interface=      b1 last_hb_time=82192.16
    status=alive
                           local_interface=      b2 last_hb_time=      0.00   status=dead

ch2-slot2 (FT513B3913000168), Slave (priority=3), ip=169.254.128.204, uptime=1476.37,
chassis=2 (1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3 (connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)   hbdevs: local_interface=      b1 last_hb_time=82192.27
    status=alive
                           local_interface=      b2 last_hb_time=      0.00   status=dead

ch1-slot2 (FT513B3914000006), Slave (priority=1), ip=169.254.128.202, uptime=1504.58,

```

```

chassis=1(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=    b1 last_hb_time=82192.16
status=alive
      local_interface=    b2 last_hb_time=    0.00    status=dead

```

4. Log into the **chassis 1 slot 2 FortiController** CLI and enter this command to view the status of this secondary FortiController.

```

get system status
Version: FortiController-5103B
v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3914000006
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: ch1-slot2
Current HA mode: dual, backup
System time: Mon Sep 15 10:14:53 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)

```

5. Enter the following command to view the status of this secondary FortiController and its workers.

```

get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]
Slot  3: Status:Working  Function:Active
  Link:      Base: Down   Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot  4: Status:Working  Function:Active
  Link:      Base: Down   Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot  5: Status:Working  Function:Active
  Link:      Base: Down   Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"

```

6. Enter the following command from the FortiController in chassis 1 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 1 slot 2 is shown first.

```

diagnose system ha status
mode: dual
minimize chassis failover: 1
ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.202, uptime=1647.44,
chassis=1(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1

```



```

    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=    b1 best=yes
    local_interface=    b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.201, uptime=1660.17,
chassis=1(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=    b1 last_hb_time=82305.93
status=alive
    local_interface=    b2 last_hb_time=    0.00    status=dead

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.203, uptime=1633.27,
chassis=2(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=    b1 last_hb_time=82305.83
status=alive
    local_interface=    b2 last_hb_time=    0.00    status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.204, uptime=1619.12,
chassis=2(1)
    slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=    b1 last_hb_time=82305.93
status=alive
    local_interface=    b2 last_hb_time=    0.00    status=dead

```

- 7. Log into the chassis 2 slot 1 FortiController CLI and enter the following command to view the status of this secondary FortiController.**

```

get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000051
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: ch2-slot1
Current HA mode: dual, backup
System time: Mon Sep 15 10:17:10 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)

```

- 8. Enter the following command to view the status of this secondary FortiController and its workers.**

```

get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: N/A
Blades:

```

```

Working:  3 [  3 Active  0 Standby]
Ready:    0 [  0 Active  0 Standby]
Dead:     0 [  0 Active  0 Standby]
Total:    3 [  3 Active  0 Standby]
Slot  3: Status:Working   Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"
Slot  4: Status:Working   Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"
Slot  5: Status:Working   Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"

```

9. Enter the following command from the FortiController in chassis 2 slot 1 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 2 slot 1 is shown first.

```

diagnose system ha status
mode: dual
minimize chassis failover: 1
ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.203, uptime=1785.61,
chassis=2(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=      b1 best=yes
                           local_interface=      b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.201, uptime=1812.38,
chassis=1(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time=79145.95
status=alive
                           local_interface=      b2 last_hb_time=      0.00    status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.204, uptime=1771.36,
chassis=2(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time=79145.99
status=alive
                           local_interface=      b2 last_hb_time=      0.00    status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.202, uptime=1799.56,
chassis=1(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)

```

```

    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=    b1 last_hb_time=79145.86
status=alive
        local_interface=    b2 last_hb_time=    0.00    status=dead

```

- 10. Log into the chassis 2 slot 2 FortiController CLI and enter the following command to view the status of this secondary FortiController.**

```

get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3913000168
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: ch2-slot2
Current HA mode: dual, backup
System time: Mon Sep 15 10:20:00 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)

```

- 11. Enter this command to view the status of this secondary FortiController and its workers.**

```

get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: N/A
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]
  Slot  3: Status:Working  Function:Active
    Link:      Base: Down      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"
  Slot  4: Status:Working  Function:Active
    Link:      Base: Down      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"
  Slot  5: Status:Working  Function:Active
    Link:      Base: Down      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"

```

- 12. Enter the following command from the FortiController in chassis 2 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 2 slot 2 is shown first.**

```

diagnose system ha status
mode: dual
minimize chassis failover: 1
ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.204, uptime=1874.39,
chassis=2(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=    b1 best=yes
        local_interface=    b2 best=no

```

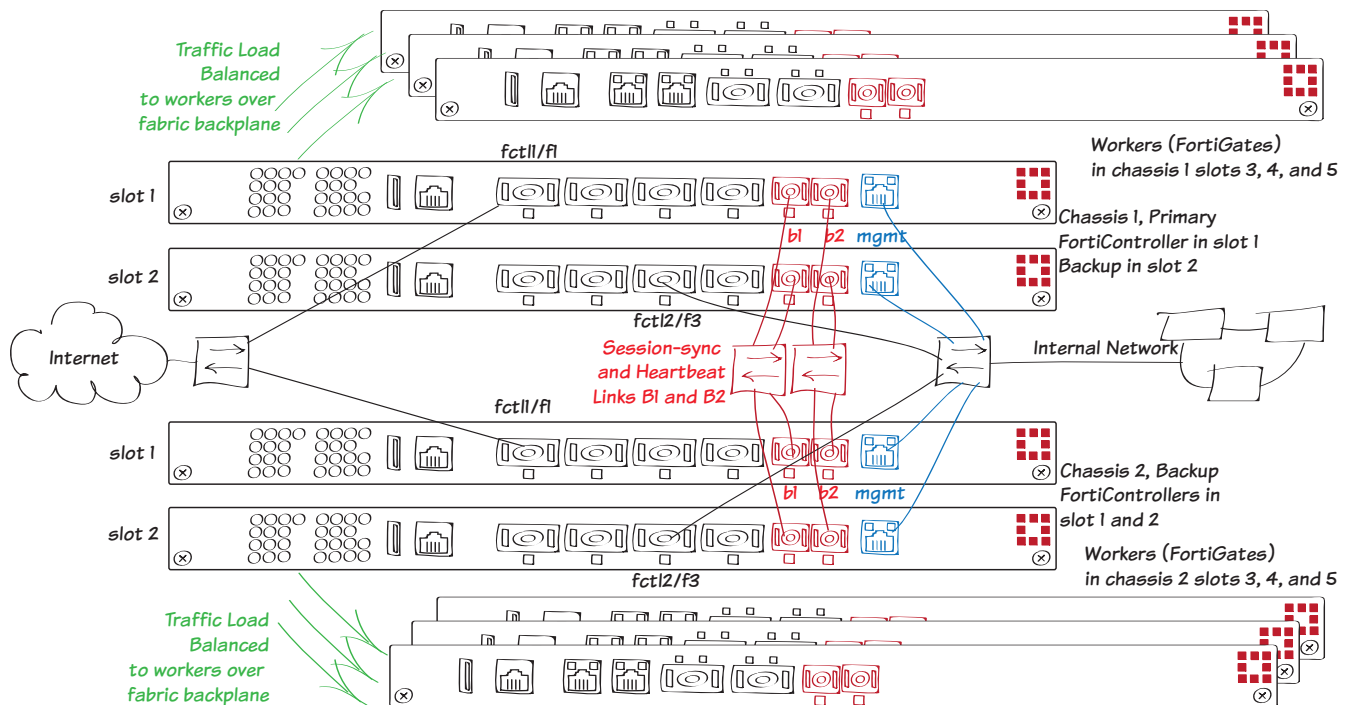
```
ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.201, uptime=1915.59,
chassis=1(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time=78273.86
status=alive
      local_interface=      b2 last_hb_time=      0.00    status=dead

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.203, uptime=1888.78,
chassis=2(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time=78273.85
status=alive
      local_interface=      b2 last_hb_time=      0.00    status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.202, uptime=1902.72,
chassis=1(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time=78273.72
status=alive
      local_interface=      b2 last_hb_time=      0.00    status=dead
```

Dual mode SLBC with four FortiController-5903Cs and two chassis

This example describes how to setup a dual-mode SLBC cluster consisting of two FortiGate-5144C chassis, four FortiController-5903Cs, two in each chassis, and six FortiGate-5001Ds acting as workers, three in each chassis. This SLBC configuration can have up to 8 redundant 40Gbps network connections. The FortiGate-5144C is required to supply enough power for the FortiController-5903Cs and provide 40Gbps fabric backplane communication.



In this dual mode configuration, the FortiController in chassis 1 slot 1 is configured to become the primary FortiController. Both of the FortiControllers in chassis 1 receive traffic and load balance it to the workers in chassis 1. In dual mode configuration the front panel interfaces of both FortiControllers are active. All networks have single connections to the FortiController in slot 1 or the FortiController in slot 2. It is a best practice in a dual-mode configuration to distribute traffic evenly between the FortiControllers. So in this example, ingress traffic from the Internet is processed by the FortiController in slot 1 and egress traffic for the internal network is processed by the FortiController in slot 2.



Redundant connections to a network from the FortiControllers in same chassis is not supported (unless you configure link aggregation).

The front panel F1 to F4 interfaces of the FortiController in slot 1 are named fctrl1/f1 to fctrl1/f4 and the front panel F1 to F4 interfaces of the FortiController in slot 2 are named fctrl2/f1 to fctrl2/f4.

The network connections to the FortiControllers in chassis 1 are duplicated with the FortiControllers in chassis 2. If one of the FortiControllers in chassis 1 fails, the FortiController in chassis 2 slot 1 becomes the primary FortiController and all traffic fails over to the FortiControllers in chassis 2. If one of the FortiControllers in chassis 2 fails, the remaining

FortiController in chassis 2 keeps processing traffic received by its front panel interfaces. Traffic to and from the failed FortiController is lost.

Heartbeat, base control, base management, and session sync communication is established between the chassis using the FortiController B1 and B2 interfaces. Connect all of the B1 interfaces together using a 10 Gbps switch. Collect all of the B2 interfaces together using another 10 Gbps switch. Using the same switch for the B1 and B2 interfaces is not recommended and requires a double VLAN tagging configuration.

The switches must be configured to support the following VLAN tags and subnets used by the traffic on the B1 and B2 interfaces:

- Heartbeat traffic uses VLAN 999.
- Base control traffic on the 10.101.11.0/255.255.255.0 subnet uses VLAN 301.
- Base management on the 10.101.10.0/255.255.255.0 subnet uses VLAN 101.
- Session sync traffic between the FortiControllers in slot 1 uses VLAN 1900.
- Session sync traffic between the FortiControllers in slot 2 uses VLAN 1901.

This example sets the device priority of the FortiController in chassis 1 slot 1 higher than the device priority of the other FortiControllers to make sure that the FortiController in chassis 1 slot 1 becomes the primary FortiController for the cluster. Override is also enabled on the FortiController in chassis 1 slot 1. Override may cause the cluster to negotiate more often to select the primary unit. This makes it more likely that the unit that you select to be the primary unit will actually be the primary unit; but enabling override can also cause the cluster to negotiate more often.

Setting up the hardware

1. Install two FortiGate-5144C chassis and connect them to power. Ideally each chassis should be connected to a separate power circuit.
2. Install the FortiControllers in slot 1 and slot 2 of each chassis.
3. Install the workers in slots 3, 4, and 5 of each chassis.
4. Power on both chassis.
5. Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally.
To check normal operation LED status see the [FortiGate-5000 hardware guides](#) and [FortiController hardware guides](#).
6. Create redundant connections from the F1 interfaces of the FortiControllers in slot 1 of both chassis to the internet.
In the FortiOS GUI or CLI, this is the fct1/f2 interface.
7. Create redundant connections from the F3 interfaces of the FortiControllers in slot 2 of both chassis to the internal network.
In the FortiOS GUI or CLI, this is the fct2/f3 interface.
8. Create redundant connections from all four FortiController mgmt interfaces to a management network (in the example the mgmt interfaces are connected to the internal network).
9. Create a heartbeat and session-sync link by connecting the four FortiController B1 interfaces together.
Create a secondary heartbeat and session-sync link by connecting the four FortiController B2 interfaces together.
Using the same switch for the B1 and B2 interfaces is not recommended and requires a double VLAN tagging configuration.
The switches used to connect the heartbeat interfaces must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). The switches must also allow traffic on the session-sync

VLANs (1900 for B2 and 1901 for B2). The heartbeat interfaces provide HA heartbeat, base control, base management, and session-sync communication between the FortiControllers.

Only one heartbeat connection is required but redundant connections are recommended.

10. Check the [FortiController release notes](#) for the latest supported FortiController and FortiGate firmware.

11. Get FortiController and FortiOS firmware from the [Fortinet Support site](#).

For FortiController firmware, select the **FortiSwitchATCA** product.

Configuring the FortiController in Chassis 1 Slot 1

This will become the primary FortiController. To make sure this is the primary FortiController it will be assigned the highest device priority and override will be enabled.

1. Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in chassis 1 slot 1 using the default IP address 192.168.1.99.

Or connect to the FortiController CLI through the console port (Baud Rate 9600bps, Data bits 8, Parity None, Stop bits 1, and Flow Control None).

2. Login using the admin administrator account and no password.

3. From the Dashboard System Information widget, set the **Host Name** to ch1-slot1. Or enter this command.

```
config system global
    set hostname ch1-slot1
end
```

4. Add a password for the admin administrator account. From the GUI use the **Administrators** widget or from the CLI enter this command.

```
config admin user
    edit admin
        set password <password>
    end
```

5. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
    edit mgmt
        set ip 172.20.120.151/24
    end
```

6. If you need to add a default route for the management IP address, enter this command.

```
config route static
    edit route 1
        set gateway 172.20.120.2
    end
```

7. Set the chassis type that you are using, for example:

```
config system global
    set chassis-type fortigate-5144
end
```

8. Enable FortiController session sync.

```
config load-balance setting
    set session-sync enable
end
```

The FortiController-5903C uses b1 and b2 as the session sync interfaces so you don't have to set the `session-sync-port`.

9. Configure Dual mode HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.
10. Set **Mode** to **Dual Mode**, set the **Device Priority** to 250, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
ch1-slot1	FT513B3912000051	Master	169.254.128.89	4772.75	0	1/1	0	1

Configure

Mode: Dual Mode

Device Priority (0-255): 250

Group ID(0-31): 25

Enable Override: ☒

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy: ☒

Chassis ID(1 - 2): 1

Available: mgmt

Selected: b1, b2

Heartbeat Device

OK Cancel

You can also enter the complete HA configuration with this command:

```
config system ha
  set mode dual
  set groupid 25
  set priority 250
  set chassis-redundancy enable
  set chassis-id 1
  set hbdev b1 b2
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different group ID. The default group ID of 0 is not a good choice and normally should be changed.

Enable Override is selected to make sure the FortiController in chassis 1 always becomes the primary unit. Enabling override could lead to the cluster renegotiating more often, so once the chassis is operating you can disable this setting.

You can also adjust other HA settings. For example, if the heartbeat interfaces are connected using a switch, you can change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on the switch. You can also adjust the **Heartbeat Interval** and **Number of Heartbeats** lost to adjust how quickly the cluster determines if one of the FortiControllers has failed.

Configuring the FortiController in chassis 1 slot 2

1. Log into the GUI or CLI of the FortiController in chassis 1 slot 2.
2. From the Dashboard System Information widget, set the **Host Name** to ch1-slot2. Or enter this command.

```
config system global
    set hostname ch1-slot2
end
```

3. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
    edit mgmt
        set ip 172.20.120.152/24
    end
```

4. Configure Dual Mode HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.
5. Set **Mode** to **Dual Mode**, set the **Device Priority** to 10, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

You can also enter the complete HA configuration with this command:

```
config system ha
    set mode dual
    set groupid 25
    set priority 10
    set override enable
    set chassis-redundancy enable
    set chassis-id 1
    set hbdev b1 b2
end
```

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

Configuring the FortiController in chassis 2 slot 1

1. Log into the GUI or CLI of the FortiController in chassis 2 slot 1.
2. From the Dashboard System Information widget, set the **Host Name** to ch2-slot1. Or enter this command.

```
config system global
    set hostname ch2-slot1
end
```

3. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
```

```
edit mgmt
  set ip 172.20.120.251/24
end
```

4. Configure Dual Mode HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.
5. Set **Mode** to **Dual Mode**, set the **Device Priority** to 10, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 2 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

You can also enter the complete HA configuration with this command:

```
config system ha
  set mode dual
  set groupid 25
  set priority 10
  set override enable
  set chassis-redundancy enable
  set chassis-id 2
  set hbdev b1 b2
end
```

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

Configuring the FortiController in chassis 2 slot 2

1. Log into the GUI or CLI of the FortiController in chassis 2 slot 2.
2. From the Dashboard System Information widget, set the **Host Name** to ch2-slot2. Or enter this command.

```
config system global
  set hostname ch2-slot2
end
```

3. Change the FortiController mgmt interface IP address.

From the GUI use the **Management Port** widget or from the CLI enter this command:

```
config system interface
  edit mgmt
    set ip 172.20.120.252/24
  end
```

4. Configure Dual Mode HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.
5. Set **Mode** to **Dual Mode**, set the **Device Priority** to 10, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 2 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

You can also enter the complete HA configuration with this command:

```
config system ha
  set mode dual
  set groupid 25
  set priority 10
  set override enable
  set chassis-redundancy enable
  set chassis-id 2
  set hbdev b1 b2
end
```

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

Configuring the cluster

After a short time, the FortiControllers restart in HA mode and form a dual mode active-passive SLBC HA cluster. All of the FortiControllers must have the same HA configuration and at least one heartbeat link (the B1 and B2 interfaces) must be connected. If the FortiControllers are unable to form a cluster, check to make sure that they all have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

With the configuration described in the previous steps, the FortiController in chassis 1 slot 1 should become the primary FortiController and you can log into the cluster using the management IP address that you assigned to this FortiController.

The other FortiControllers become secondary FortiControllers. You cannot log into or manage the secondary FortiControllers until you configure the cluster External Management IP and add workers to the cluster. Once you do this, you can use the External Management IP address and a special port number to manage the secondary FortiControllers. You can also connect to any backup FortiController CLI using their console port.

1. Confirm that the cluster has been formed. From the primary FortiController GUI **System Information** widget, beside **HA Status**, select **Configure**.

The display should show all four of the FortiControllers in the cluster. (The host names shown on some of the screen images in this example may not match the host names used in the example configuration.)

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
ch1-slot1	FT513B3912000029	Master	169.254.128.201	1095.42	0	0/3	1	1
ch2-slot1	FT513B3912000051	Slave	169.254.128.203	843.96	0	0/3	1	1
ch2-slot2	FT513B3913000168	Slave	169.254.128.204	829.83	0	0/3	1	1
ch1-slot2	FT513B3914000006	Slave	169.254.128.202	861.79	0	0/3	1	1

Configure

Mode: Dual Mode

Device Priority (0-255): 128

Group ID(0-31): 25

Enable Override: ☐

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy: ☒

Chassis ID(1 - 2): 1

Available: mgmt

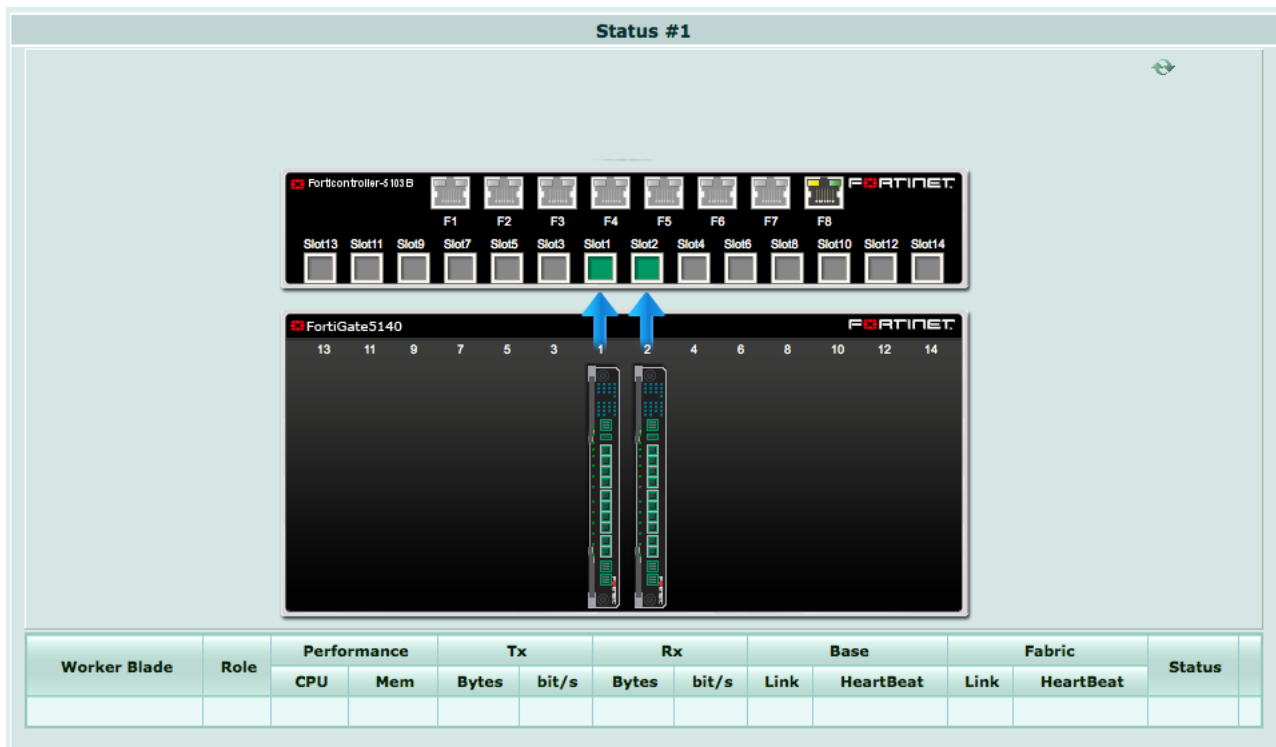
Selected: b1, b2

Heartbeat Device

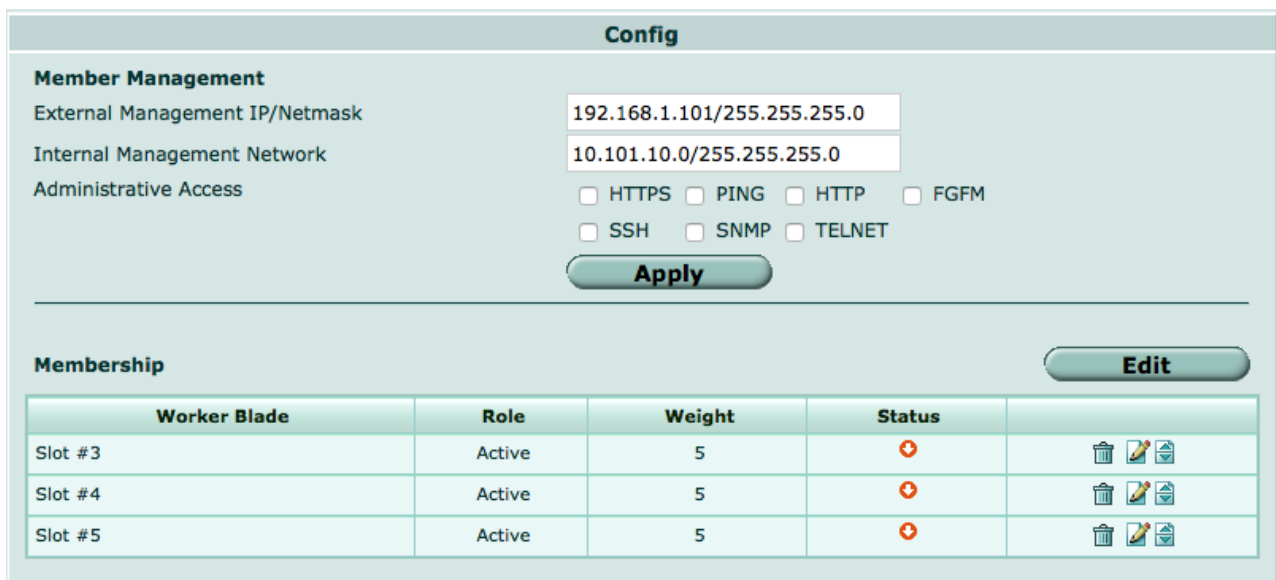
OK Cancel

2. Go to **Load Balance > Status** to see the status of the FortiControllers in chassis 1.

Both FortiController slot icons should be green because both FortiControllers can process traffic.



- Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.
- The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured for SLBC operation their status will be **Down**.
- Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure all of the devices in the cluster.



- Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure all of the devices in the cluster.

Config

Member Management
 External Management IP/Netmask
 Internal Management Network
 Administrative Access

192.168.1.101/255.255.255.0

10.101.10.0/255.255.255.0

☐ HTTPS
☐ SSH

☐ PING
☐ SNMP

☐ HTTP
☐ TELNET

☐ FGFM

Apply

Membership

Edit

Worker Blade	Role	Weight	Status	
Slot #3	Active	5	+	
Slot #4	Active	5	+	
Slot #5	Active	5	+	

You can also enter the following command to add slots 3, 4, and 5 to the cluster.

```
config load-balance setting
  config slots
    edit 3
    next
    edit 4
    next
    edit 5
    end
  end
```

You can also use the following CLI command to configure the external management IP/Netmask and management access to this address:

```
config load-balance setting
  set base-mgmt-external-ip 172.20.120.100 255.255.255.0
  set base-mgmt-allowaccess https ssh ping
end
```

6. Make sure the FortiController fabric backplane ports are set to the correct speed. Since the workers are FortiGate-5001Ds and the cluster is using FortiGate-5144C chassis, the FortiController fabric backplane interface speed should be set to 40Gbps full duplex.

To change backplane fabric channel interface speeds, from the GUI go to **Switch > Fabric Channel** and edit the slot-3, slot-4, and slot-5 interfaces. For each one, set the Speed to **40Gbps Full-duplex** and select **OK**.

From the CLI enter the following to change the speed of the slot-3, slot-4 and slot-5 interfaces.

```
config switch fabric-channel physical-port
  edit slot-3
    set speed 40000full
  next
  edit slot-4
    set speed 40000full
  next
  edit slot-5
    set speed 40000full
  end
end
```

FortiController 5.2.10 Session-Aware Load Balancing (SLBC) Guide

141

7. Enable base **management** traffic between FortiControllers. The CLI syntax shows setting the default base management VLAN (101). You can also use the following command to change the base management VLAN.

```
config load-balance setting
  config base-mgmt-interfaces
    edit b1
      set vlan-id 101
    next
    edit b2
      set vlan-id 101
    end
  end
```

8. Enable base **control** traffic between FortiControllers. The CLI syntax shows setting the default base control VLAN (301). You can also use the following command to change the base management VLAN.

```
config load-balance setting
  config base-ctrl-interfaces
    edit b1
      set vlan-id 301
    next
    edit b2
      set vlan-id 301
    end
  end
```

Adding the workers to the cluster

1. Log into the CLI of each worker and enter the following command to reset the worker to its factory default settings.

```
execute factoryreset
```

If the workers are going to run FortiOS Carrier, add the FortiOS Carrier license instead. Adding the license also resets the worker to factory default settings.

2. Register each worker and apply licenses to each worker before adding them to the cluster.

This includes **FortiCloud** activation and **FortiClient** licensing, and entering a license key if you purchased more than 10 **Virtual Domains** (VDOMs). You should also install any third-party certificates on each worker before forming the cluster. FortiToken licenses can be added at any time because they are synchronized to all workers.

3. Optionally give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network.

These IP addresses are not synchronized, so you can connect to and manage each worker separately.

```
config system interface
  edit mgmt1
    set ip 172.20.120.120
  end
```

4. Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

```
config system global
  set hostname worker-chassis-1-slot-3
end
```

5. Set the backplane communication speed of each worker to 40Gbps to match the FortiController-5903C.

```
config system interface
  edit elbc-ctrl/1
    set speed 40000full
```

```

next
edit elbc-ctrl/2
    set speed 40000full
end

```

6. Enter the following command on each worker to enable dual FortiController mode.

```

config system elbc
    set mode dual-forticontroller
end

```

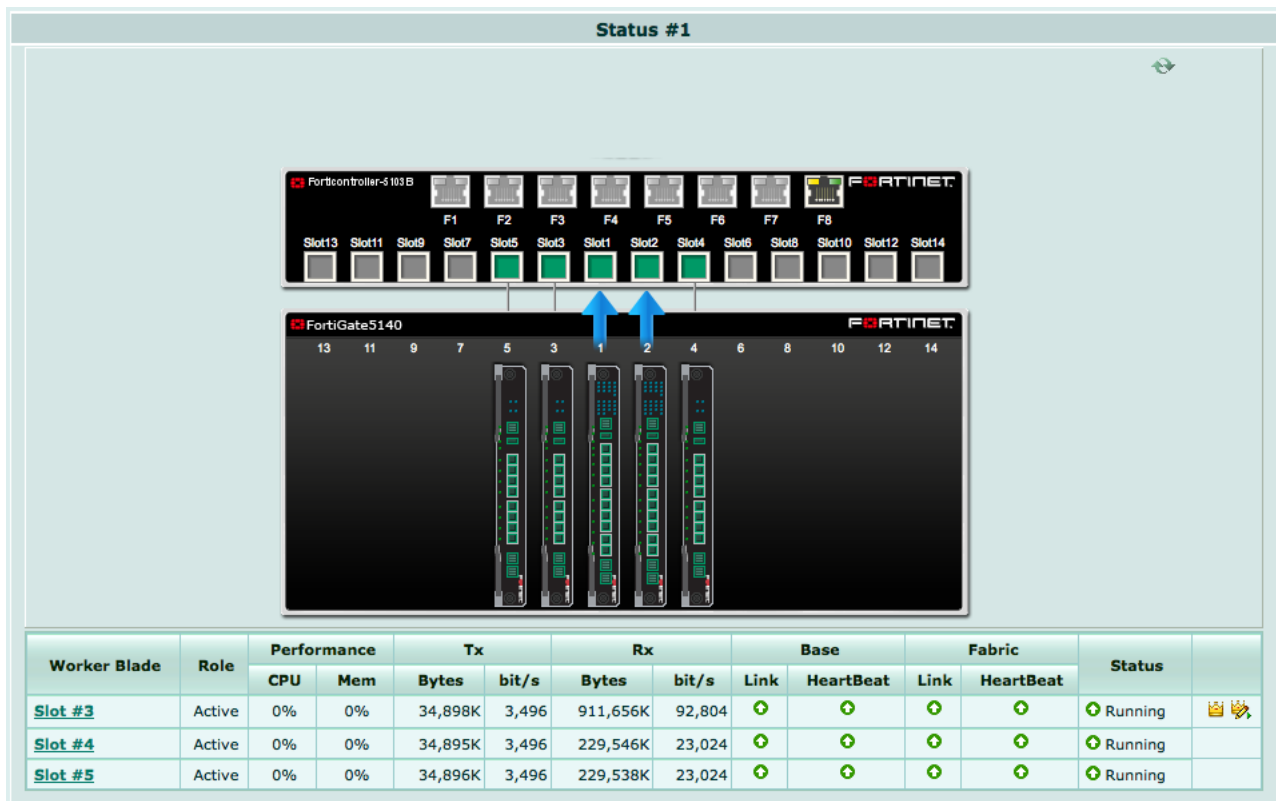
The worker restarts and joins the cluster.

7. Repeat these steps for each worker in both chassis.

8. On the primary FortiController GUI go to **Load Balance > Status**.

As the workers in chassis 1 restart they should appear in their appropriate slots. If the workers don't appear, check the elbc-ctrl/1 and elbc-ctrl/2 interfaces speeds (they should be set to 40000full).

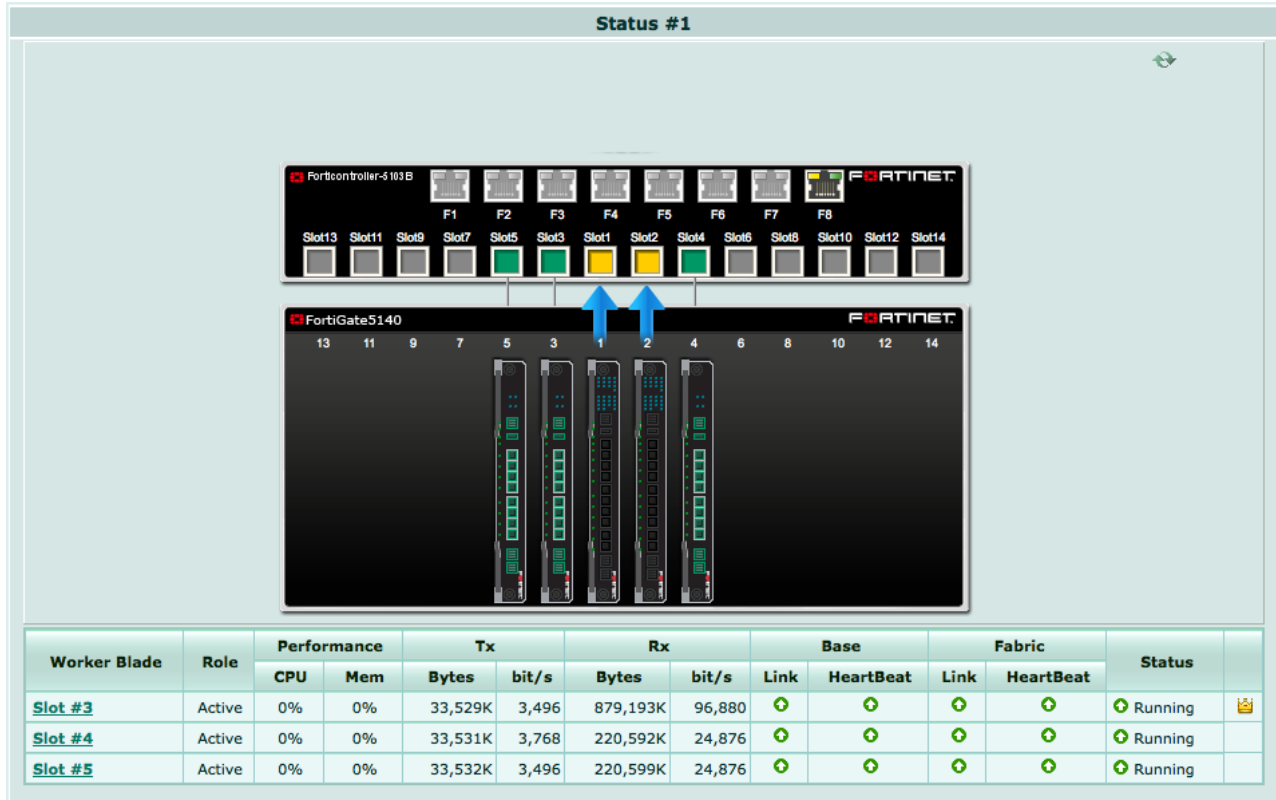
The primary worker should be the worker in chassis 1 slot 3. The primary FortiController status display includes a **Config Master** link that you can use to connect to the primary worker.



9. Log into the secondary FortiController GUI (for example by browsing to <https://172.20.120.100:44321>) and go to **Load Balance > Status**.

As the workers in chassis 2 restart they should appear in their appropriate slots.

The secondary FortiController Status page shows the status of the workers in chassis 2 and does not include the **Config Master** link.



Operating and managing the cluster

You can now manage the workers in the same way as you would manage a standalone FortiGate. You can connect to the worker GUI or CLI using the **External Management IP**. If you had configured the worker mgmt1 or mgmt2 interfaces you can also connect to one of these addresses to manage the cluster.






To operate the cluster, connect networks to the FortiController front panel interfaces and connect to a worker GUI or CLI to configure the workers to process the traffic they receive. When you connect to the External Management IP, you connect to the primary worker. When you make configuration changes they are synchronized to all workers in the cluster.

You can use the external management IP followed by a special port number to manage individual devices in the cluster. For details, see [Managing the devices in an SLBC cluster with the External Management IP on page 29](#).

To manage a FortiController using SNMP you need to load the FORTINET-CORE-MIB.mib file into your SNMP manager. You can get this MIB file from the Fortinet support site, in the same location as the current FortiController firmware (select the FortiSwitchATCA product).

By default on the workers, all FortiController front panel interfaces are in the root VDOM. You can configure the root VDOM or create additional VDOMs and move interfaces into them.

For example, you could connect the internet to FortiController front panel interface 2 (fctrl/f2 on the worker GUI and CLI) and an internal network to FortiController front panel interface 6 (fctrl/f6 on the worker GUI and CLI). Then enter the root VDOM and add a policy to allow users on the internal network to access the internet.

Incoming Interface	fctrl2/f3 
Source Address	Internal_Net 
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	fctrl1/f1 
Destination Address	all 
Schedule	always
Service	ALL 
Action	✓ ACCEPT

Firewall / Network Options**ON** NAT

- ☒ Use Outgoing Interface Address ☐ Fixed Port
☐ Use Dynamic IP Pool

Checking the cluster status

1. Log into the **primary FortiController** CLI and enter the following command to view the system status of the primary FortiController.

```
ssh admin@172.20.120.100 -p2201
get system status
Version: FortiController-5903C v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000029
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: chl-slot1
Current HA mode: dual, master
System time: Mon Sep 15 10:11:48 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

2. Enter the following command to view the load balance status of the primary FortiController and its workers. The command output shows the workers in slots 3, 4, and 5, and status information about each one.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]
```

```

Slot 3: Status:Working   Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good   Data: Good
Status Message:"Running"
Slot 4: Status:Working   Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good   Data: Good
Status Message:"Running"
Slot 5: Status:Working   Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good   Data: Good
Status Message:"Running"
Heartbeat: Management: Good   Data: Good
Status Message:"Running"

```

3. Enter the following command from the primary FortiController to show the HA status of the FortiControllers.

The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (in this case 0 for each FortiController) the number of failed workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (status=alive) and the B2 interfaces are not (status=dead). The cluster can still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```

diagnose system ha status
mode: dual
minimize chassis failover: 1
ch1-slot1 (FT513B3912000029), Master (priority=0), ip=169.254.128.201, uptime=1517.38,
chassis=1 (1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)   hbdevs: local_interface=      b1 best=yes
                           local_interface=      b2 best=no

ch2-slot1 (FT513B3912000051), Slave (priority=2), ip=169.254.128.203, uptime=1490.50,
chassis=2 (1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3 (connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)   hbdevs: local_interface=      b1 last_hb_time=82192.16
    status=alive
                           local_interface=      b2 last_hb_time=      0.00   status=dead

ch2-slot2 (FT513B3913000168), Slave (priority=3), ip=169.254.128.204, uptime=1476.37,
chassis=2 (1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3 (connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)   hbdevs: local_interface=      b1 last_hb_time=82192.27
    status=alive
                           local_interface=      b2 last_hb_time=      0.00   status=dead

ch1-slot2 (FT513B3914000006), Slave (priority=1), ip=169.254.128.202, uptime=1504.58,

```

```

chassis=1(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=    b1 last_hb_time=82192.16
status=alive
      local_interface=    b2 last_hb_time=    0.00    status=dead

```

4. Log into the **chassis 1 slot 2 FortiController** CLI and enter the following command to view the status of this secondary FortiController.

```

get system status
Version: FortiController-5903C
v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3914000006
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: ch1-slot2
Current HA mode: dual, backup
System time: Mon Sep 15 10:14:53 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)

```

5. Enter the following command to view the status of this secondary FortiController and its workers.

```

get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]
Slot  3: Status:Working  Function:Active
  Link:      Base: Down    Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot  4: Status:Working  Function:Active
  Link:      Base: Down    Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot  5: Status:Working  Function:Active
  Link:      Base: Down    Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"

```

6. Enter the following command from the FortiController in chassis 1 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 1 slot 2 is shown first.

```

diagnose system ha status
mode: dual
minimize chassis failover: 1
ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.202, uptime=1647.44,
chassis=1(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1

```

```

    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=    b1 best=yes
        local_interface=    b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.201, uptime=1660.17,
chassis=1(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=    b1 last_hb_time=82305.93
status=alive
        local_interface=    b2 last_hb_time=    0.00    status=dead

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.203, uptime=1633.27,
chassis=2(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=    b1 last_hb_time=82305.83
status=alive
        local_interface=    b2 last_hb_time=    0.00    status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.204, uptime=1619.12,
chassis=2(1)
    slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=    b1 last_hb_time=82305.93
status=alive
        local_interface=    b2 last_hb_time=    0.00    status=dead

```

7. Log into the chassis 2 slot 1 FortiController CLI and enter this command to view the status of this secondary FortiController.

```

get system status
Version: FortiController-5903C v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000051
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: ch2-slot1
Current HA mode: dual, backup
System time: Mon Sep 15 10:17:10 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)

```

8. Enter the following command to view the status of this secondary FortiController and its workers.

```

get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: N/A
Blades:

```

```

Working:  3 [  3 Active  0 Standby]
Ready:    0 [  0 Active  0 Standby]
Dead:     0 [  0 Active  0 Standby]
Total:    3 [  3 Active  0 Standby]
Slot  3: Status:Working   Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"
Slot  4: Status:Working   Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"
Slot  5: Status:Working   Function:Active
  Link:      Base: Up      Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"

```

9. Enter the following command from the FortiController in chassis 2 slot 1 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 2 slot 1 is shown first.

```

diagnose system ha status
mode: dual
minimize chassis failover: 1
ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.203, uptime=1785.61,
chassis=2(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=      b1 best=yes
                           local_interface=      b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.201, uptime=1812.38,
chassis=1(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time=79145.95
status=alive
                           local_interface=      b2 last_hb_time=      0.00    status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.204, uptime=1771.36,
chassis=2(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time=79145.99
status=alive
                           local_interface=      b2 last_hb_time=      0.00    status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.202, uptime=1799.56,
chassis=1(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)

```

```

    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none) hbdevs: local_interface= b1 last_hb_time=79145.86
    status=alive
           local_interface= b2 last_hb_time= 0.00 status=dead

```

- 10. Log into the chassis 2 slot 2 FortiController CLI and enter the following command to view the status of this secondary FortiController.**

```

get system status
Version: FortiController-5903C v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3913000168
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: ch2-slot2
Current HA mode: dual, backup
System time: Mon Sep 15 10:20:00 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)

```

- 11. Enter the following command to view the status of the secondary FortiController and its workers.**

```

get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: N/A
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]
  Slot  3: Status:Working  Function:Active
    Link:      Base: Down      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"
  Slot  4: Status:Working  Function:Active
    Link:      Base: Down      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"
  Slot  5: Status:Working  Function:Active
    Link:      Base: Down      Fabric: Up
    Heartbeat: Management: Good  Data: Good
    Status Message:"Running"

```

- 12. Enter the following command from the FortiController in chassis 2 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 2 slot 2 is shown first.**

```

diagnose system ha status
mode: dual
minimize chassis failover: 1
ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.204, uptime=1874.39,
chassis=2(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none) hbdevs: local_interface= b1 best=yes
           local_interface= b2 best=no

```

```
ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.201, uptime=1915.59,
chassis=1(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time=78273.86
status=alive
      local_interface=      b2 last_hb_time=      0.00    status=dead

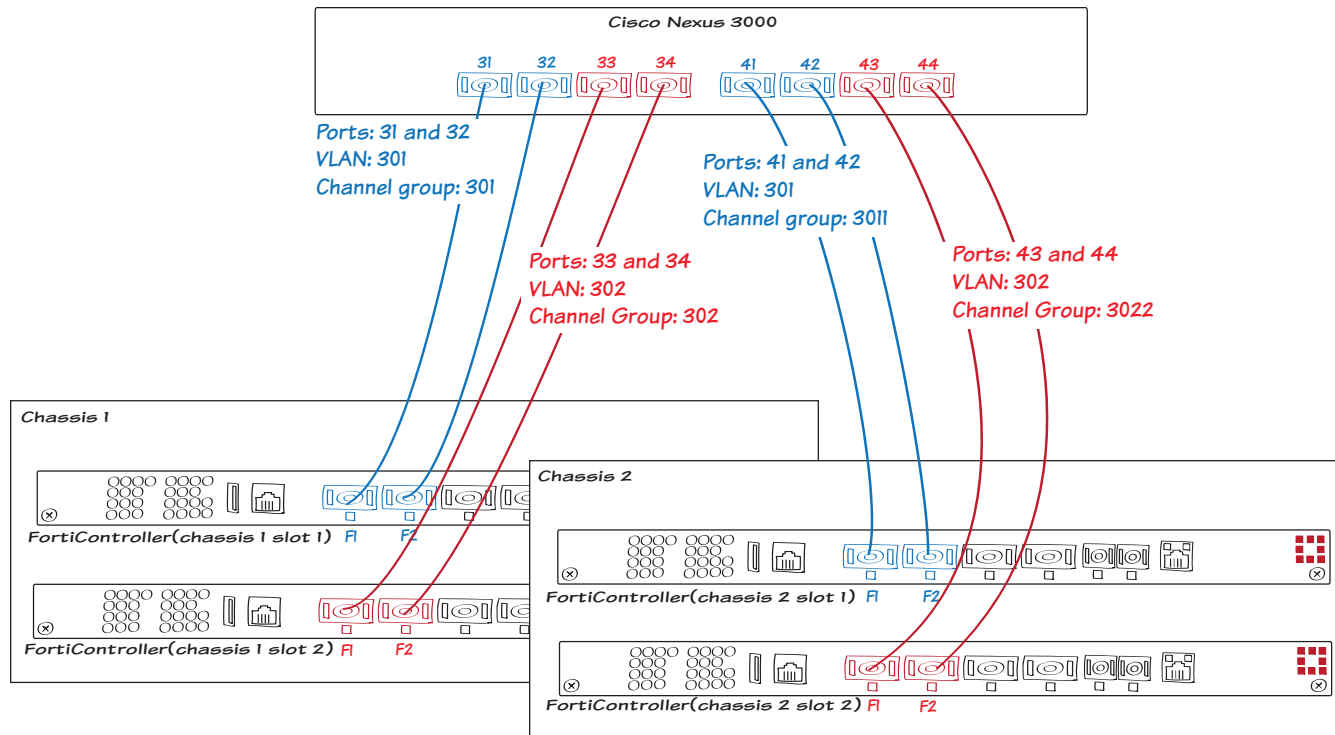
ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.203, uptime=1888.78,
chassis=2(1)
  slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time=78273.85
status=alive
      local_interface=      b2 last_hb_time=      0.00    status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.202, uptime=1902.72,
chassis=1(1)
  slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
    force-state(0:none)    hbdevs: local_interface=      b1 last_hb_time=78273.72
status=alive
      local_interface=      b2 last_hb_time=      0.00    status=dead
```

Dual mode SLBC HA with LAGs third-party switch example

This example shows how to configure a single Cisco Nexus 3000 switch to provide redundant connections for the LACP LAGs in a dual mode SLBC HA cluster.

The cluster includes two FortiGate-5000 chassis. Each chassis has two FortiController-5903Cs in slots 1 and 2 operating in dual FortiController mode and two FortiGate-5000 workers in slots 3 and 4. Each dual mode FortiController-5903C is configured with an LACP group that includes the F1 and F2 interfaces. So each chassis has two LACP groups.



The Cisco Nexus 3000 switch requires four LACP groups, one for each of the FortiController LACP groups. To support redundancy, the LACP groups on the switch for the FortiControllers in chassis 1 slot 1 and chassis 3 slot 1 are on one VLAN (in the example, 301) and the LACP groups on the switch for the FortiControllers in chassis 1 slot 2 and chassis 2 slot 2 are on another VLAN (in the example, 302).

To set up the configuration:

1. Log in to the CLI of each FortiController and enter the following command to create a trunk that includes the F1 and F2 interfaces. In this example, each FortiController has the same trunk configuration.

```
config switch fabric-channel trunk
edit "trunk01"
set mode lacp-active
set members f1-1 f1-2
end
```

2. Log into the CLI of the primary worker and enter the following command to add two FortiController trunk interfaces. These match the trunks added to the FortiControllers:

```
config system interface
edit "fctrl1/trunk01"
```



```
set vdom "root"
set ip 11.0.0.1 255.0.0.0
set type fctrl-trunk
set member fctrl1/f1 fctrl1/f2
next
edit "fctrl2/trunk01"
set vdom "root"
set ip 12.0.0.1 255.0.0.0
set type fctrl-trunk
set member fctrl2/f1 fctrl2/f2
end
```

3. Log into the Cisco nexus 3000 switch CLI.

4. Configure four port channels, one for each FortiController LAG:

```
interface port-channel301
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301

interface port-channel302
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302

interface port-channel3011
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301

interface port-channel3022
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
```

5. Configure the switch interfaces (31 to 34) for the chassis 1 trunks.

```
interface Ethernet1/31
description cls1 f1-1
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 301 mode active

interface Ethernet1/32
description cls1 f1-2
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 301 mode active

interface Ethernet1/33
description cls2 f1-1
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 302 mode active

interface Ethernet1/34
description cls2 f1-2
```

```
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 302 mode active
```

6. Configure the switch interfaces (41 to 44) for the chassis 2 trunks.

```
interface Ethernet1/41
description c2s1 f1-1
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 3011 mode active
```

```
interface Ethernet1/42
description c2s1 f1-2
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 3011 mode active
```

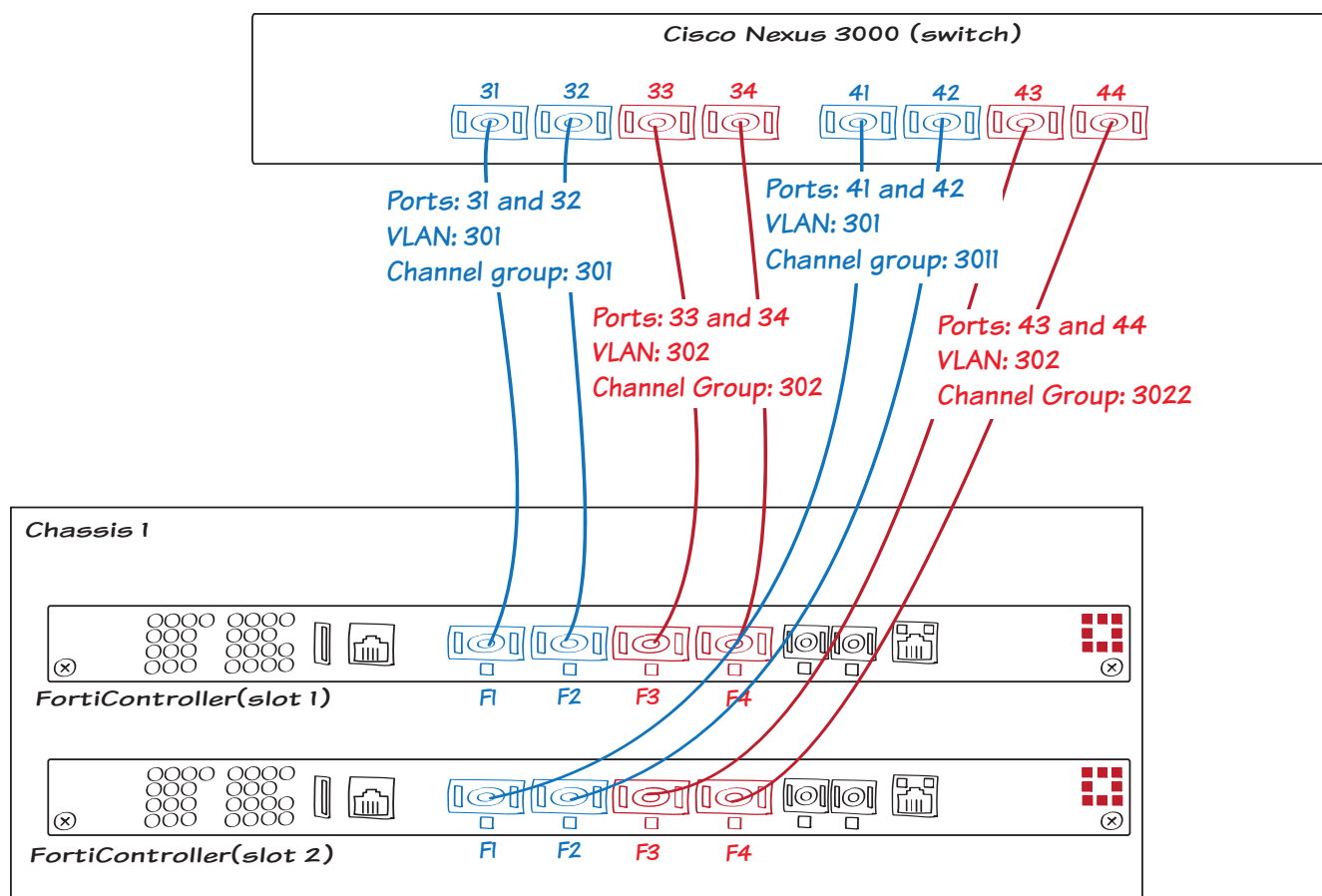
```
interface Ethernet1/43
description c2s2 f1-1
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 3022 mode active
```

```
interface Ethernet1/44
description c2s2 f1-2
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 3022 mode active
```

AP mode single chassis SLBC with LAGs third-party switch example

This example shows how to configure a single Cisco Nexus 3000 switch to provide redundant connections for the LACP LAGs in an AP mode single-chassis SLBC configuration.

The FortiGate-5000 chassis has two FortiController-5903Cs in slots 1 and 2 operating in AP FortiController mode and two FortiGate-5000 workers in slots 3 and 4. The primary FortiController-5903C in slot 1 is configured with two LACP groups. One LACP group includes the F1 and F2 interfaces. The other LACP group includes the F3 and F4 interfaces. These LACP groups are synchronized to the secondary FortiController-5903C in slot 2.



The Cisco Nexus 3000 switch requires four LACP groups, two for the LAGs in the FortiController in slot 1 and two for the two redundant LAGs on the FortiController in slot 2. To support redundancy, the switch interfaces for the two F1/F2 LACP groups are assigned one VLAN (in the example, 301) and the switch interfaces for the two F3/F4 LACP groups are assigned another VLAN (in the example, 302).

To set up the configuration:

1. Log in to the CLI of the primary FortiController and enter the following command to create two trunks.

```
config switch fabric-channel trunk
```

```

edit "trunk01"
    set mode lacp-active
    set members f1-1 f1-2
next
edit "trunk02"
    set mode lacp-active
    set members f1-3 f1-4
end

```

The trunks are synchronized to the FortiController in slot 2.

2. Log into the CLI of the primary worker and enter the following command to add two FortiController trunk interfaces. These match the trunks added to the FortiControllers:

```

config system interface
    edit "fctrl/trunk01"
        set vdom "root"
        set ip 11.0.0.1 255.0.0.0
        set type fctrl-trunk
        set member fctrl/f1 fctrl/f2
    next
    edit "fctrl/trunk02"
        set vdom "root"
        set ip 12.0.0.1 255.0.0.0
        set type fctrl-trunk
        set member fctrl/f3 fctrl/f4
    end
end

```

3. Log into the Cisco nexus 3000 switch CLI.
4. Configure four port channels, one for each FortiController LAG:

```

interface port-channel301
    switchport mode trunk
    switchport trunk native vlan 301
    switchport trunk allowed vlan 301

interface port-channel302
    switchport mode trunk
    switchport trunk native vlan 302
    switchport trunk allowed vlan 302

interface port-channel3011
    switchport mode trunk
    switchport trunk native vlan 301
    switchport trunk allowed vlan 301

interface port-channel3022
    switchport mode trunk
    switchport trunk native vlan 302
    switchport trunk allowed vlan 302

```

5. Configure the switch interfaces (31 to 34) for the slot 1 trunks.

```

interface Ethernet1/31
    description slot1 f1
    switchport mode trunk
    switchport trunk native vlan 301
    switchport trunk allowed vlan 301
    channel-group 301 mode active

interface Ethernet1/32
    description slot1 f2

```

```
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 301 mode active

interface Ethernet1/33
description slot1 f3
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 302 mode active

interface Ethernet1/34
description slot1 f4
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 302 mode active
```

6. Configure the switch interfaces (41 to 44) for the slot 2 trunks.

```
interface Ethernet1/41
description slot2 f1
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 3011 mode active

interface Ethernet1/42
description slot2 f2
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 3011 mode active

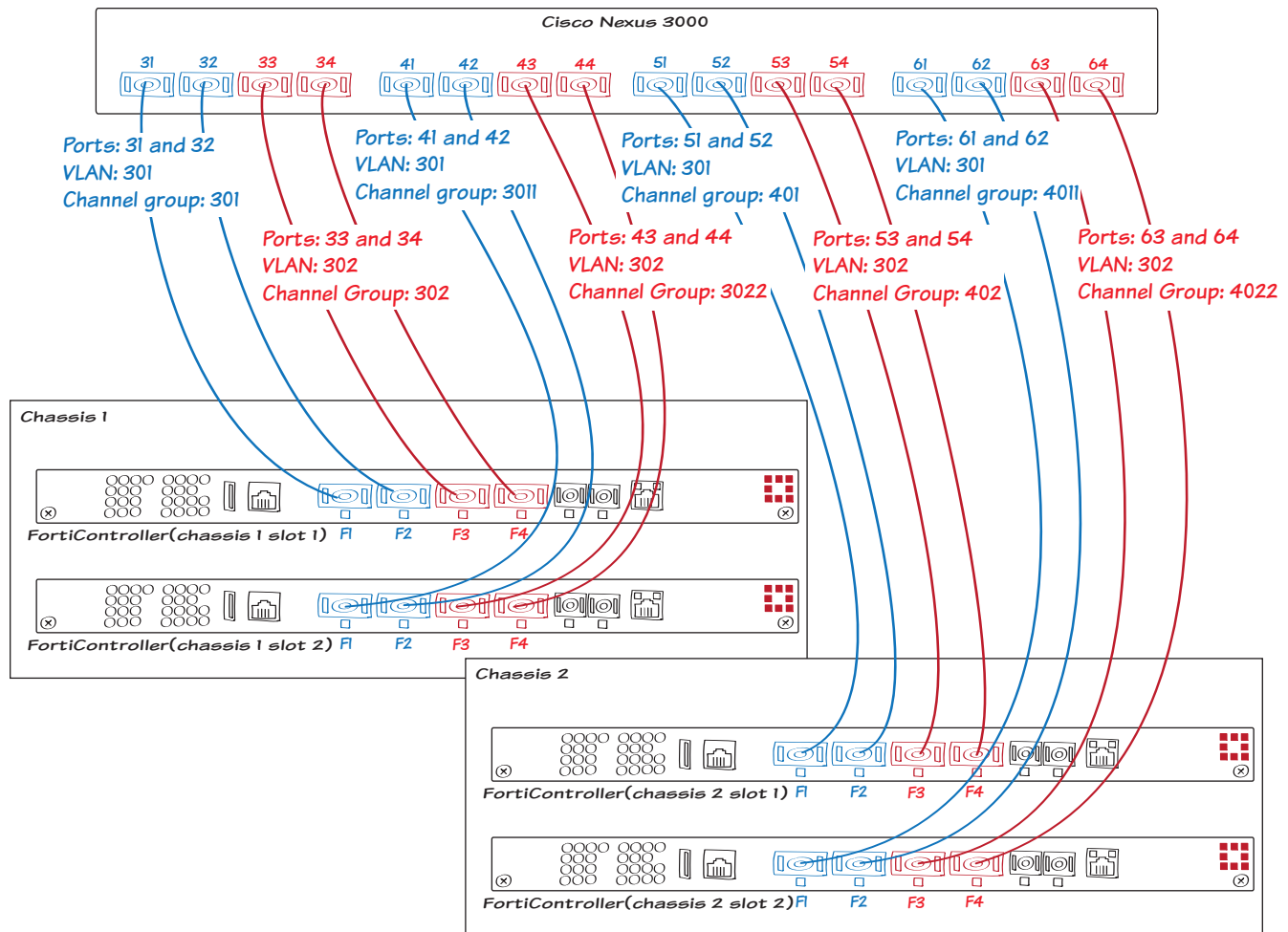
interface Ethernet1/43
description slot2 f3
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 3022 mode active

interface Ethernet1/44
description slot2 f4
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 3022 mode active
```

AP mode SLBC HA with LAGs third-party switch example

This example shows how to configure a single Cisco Nexus 3000 switch to provide redundant connections for LACP LAGs in an AP mode SLBC HA cluster.

The cluster includes two FortiGate-5000 chassis. Each chassis has two FortiController-5903Cs in slots 1 and 2 operating in AP FortiController mode and two FortiGate-5000 workers in slots 3 and 4. The primary FortiController-5903C in chassis 1 slot 1 is configured with two LACP groups. One LACP group contains the F1 and F2 interfaces, the other LACP group contains the F3 and F4 interfaces. These LACP groups are synchronized to the secondary FortiController-5903C in slot 2 and to the primary and secondary FortiController-5903Cs in chassis 2.



The Cisco Nexus 3000 switch requires two LACP groups for each FortiController, for a total of 8 LACP groups. To support redundancy, the LACP groups that connect the F1 and F2 interfaces of all the FortiControllers are on one VLAN (in the example, 301) and the LACP groups that include the F3 and F4 interfaces are on another VLAN (in the example, 302).

To set up the configuration:

1. Log in to the CLI of the primary FortiController (in chassis 1 slot 1) and enter the following command to create two trunks.

```

config switch fabric-channel trunk
  edit "trunk01"
    set mode lacp-active
    set members f1-1 f1-2
  next
  edit "trunk02"
    set mode lacp-active
    set members f1-3 f1-4
  end

```

The trunks are synchronized to all of the FortiControllers in the cluster.

2. Log into the CLI of the primary worker and enter the following command to add two FortiController trunk interfaces. These match the trunks added to the FortiControllers:

```

config system interface
  edit "fctrl1/trunk01"
    set vdom "root"
    set ip 11.0.0.1 255.0.0.0
    set type fctrl-trunk
    set member fctrl1/f1 fctrl1/f2
  next
  edit "fctrl1/trunk02"
    set vdom "root"
    set ip 12.0.0.1 255.0.0.0
    set type fctrl-trunk
    set member fctrl1/f3 fctrl1/f4
  end

```

The trunk interfaces are synchronized to all of the workers in the cluster.

3. Log into the Cisco nexus 3000 switch CLI.
4. Configure eight port channels, one for each FortiController LACP group:

```

interface port-channel301
  switchport mode trunk
  switchport trunk native vlan 301
  switchport trunk allowed vlan 301

interface port-channel302
  switchport mode trunk
  switchport trunk native vlan 302
  switchport trunk allowed vlan 302

interface port-channel3011
  switchport mode trunk
  switchport trunk native vlan 301
  switchport trunk allowed vlan 301

interface port-channel3022
  switchport mode trunk
  switchport trunk native vlan 302
  switchport trunk allowed vlan 302

interface port-channel401
  switchport mode trunk
  switchport trunk native vlan 301
  switchport trunk allowed vlan 301

interface port-channel402
  switchport mode trunk

```

```
switchport trunk native vlan 302
switchport trunk allowed vlan 302

interface port-channel4011
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301

interface port-channel4022
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
```

5. Configure the switch interfaces (31 to 34) for the chassis 1 slot 1 trunks.

```
interface Ethernet1/31
description cls1 f1
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 301 mode active

interface Ethernet1/32
description cls1 f2
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 301 mode active

interface Ethernet1/33
description cls1 f3
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 302 mode active

interface Ethernet1/34
description cls1 f4
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 302 mode active
```

6. Configure the switch interfaces (41 to 44) for the chassis 1 slot 2 trunks.

```
interface Ethernet1/41
description cls2 f1
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 3011 mode active

interface Ethernet1/42
description cls2 f2
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 3011 mode active

interface Ethernet1/43
```



```
description cls2 f3
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 3022 mode active
```

```
interface Ethernet1/44
description cls2 f4
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 3022 mode active
```

7. Configure the switch interfaces (51 to 54) for the chassis 2 slot 1 trunks.

```
interface Ethernet1/51
description c2s1 f1
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 401 mode active
```

```
channel-group 301 mode active
interface Ethernet1/52
description c2s1 f2
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 401 mode active
```

```
interface Ethernet1/53
description c2s1 f3
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 402 mode active
```

```
interface Ethernet1/54
description c2s2 f4
switchport mode trunk
switchport trunk native vlan 302
switchport trunk allowed vlan 302
channel-group 402 mode active
```

8. Configure the switch interfaces (61 to 64) for the chassis 2 slot 2 trunks.

```
interface Ethernet1/61
description c2s2 f1
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 4011 mode active
```

```
interface Ethernet1/62
description c2s2 f2
switchport mode trunk
switchport trunk native vlan 301
switchport trunk allowed vlan 301
channel-group 4011 mode active
```

```
interface Ethernet1/63
  description c2s2 f3
  switchport mode trunk
  switchport trunk native vlan 302
  switchport trunk allowed vlan 302
  channel-group 4022 mode active

interface Ethernet1/64
  description c2s2 f4
  switchport mode trunk
  switchport trunk native vlan 302
  switchport trunk allowed vlan 302
  channel-group 4022 mode active
```

FortiController get and diagnose commands

This chapter introduces some useful FortiController get and diagnose commands.

get load-balance status

Display information about the status of the workers in the cluster. In the example below the cluster includes the primary worker in slot 5 and one other worker in slot 6. You can also see that both workers are active and operating correctly.

```
get load-balance status
  ELBC Master Blade: slot-5
  Confsync Master Blade: slot-5
  Blades:
    Working:  2 [  2 Active  0 Standby]
    Ready:    0 [  0 Active  0 Standby]
    Dead:     0 [  0 Active  0 Standby]
    Total:    2 [  2 Active  0 Standby]

    Slot  5: Status:Working  Function:Active
      Link:      Base: Up      Fabric: Up
      Heartbeat: Management: Good  Data: Good
      Status Message:"Running"
    Slot  6: Status:Working  Function:Active
      Link:      Base: Up      Fabric: Up
      Heartbeat: Management: Good  Data: Good
      Status Message:"Running"
```

diagnose system flash list

Displays information about the FortiController flash partitions including the firmware version on each partition.

```
diagnose system flash list
```

ImageName	Version	TotalSize(KB)	Used(KB)	Use%	BootImage	RunningImage
primary	FT513B-5MR0-b0024-140815-P0	253871	27438	11%	Yes	Yes
secondary	FT513B-5MR0-b0024-140827-int	253871	27640	11%	No	No

diagnose system ha showcsum

Check the HA checksums for the cluster.

```
diagnose system ha showcsum [<level>] [<object>]

diagnose system ha showcsum
debugzone checksum:
```

```
06 d3 98 d4 ed 3f 08 1d 39 b3 0e 94 e9 57 98 41
checksum:
06 d3 98 d4 ed 3f 08 1d 39 b3 0e 94 e9 57 98 41
```

diagnose system ha stats

Display FortiController statistics for the cluster including the number of heartbeats transmitted and received for each heartbeat device and the number of status changes. Normally the receive and transmitted numbers should match or be similar and there shouldn't be any status changes.

```
diagnose system ha stats
hbdev: b1
    Hearbeat RX          : 13676
    Hearbeat TX          : 13676
hbdev: b2
    Hearbeat RX          : 12385
    Hearbeat TX          : 13385
HA failover Master->Slave : 0
HA failover Slave->Master : 1
```

diagnose system ha status

Display HA status information for the FortiController HA cluster including the HA mode. As well the command displays status information for each of the FortiControllers in the cluster including the uptime, heartbeat IP address, and synchronization status.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
FT513B3913000068(FT513B3913000068), Slave(priority=1), ip=169.254.128.2,
uptime=3535.28, chassis=1(1)
    slot: 2
    sync: conf_sync=1, elbc_sync=1
    session: total=0, session_sync=in sync
    state: worker_failure=0/2, intf_state=(port up:)=5
    force-state(0:none)    hbdevs: local_interface=    b1 best=yes

FT513B3913000082(FT513B3913000082), Master(priority=0),
ip=169.254.128.1, uptime=3704.54, chassis=1(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0, session_sync=in sync
    state: worker_failure=0/2, intf_state=(port up:)=5
    force-state(0:none)    hbdevs: local_interface=    b1
last_hb_time= 3622.36    status=alive
```

diagnose system ha force-slave-state

Set an individual FortiController unit or chassis to switch to secondary mode (slave state). You can set devices to operate in secondary mode, view which devices have been forced into this mode, and clear the force mode settings. You must enter this command from the primary FortiController's CLI.

```
diagnose system ha force-slave-state {by-chassis | by-serial-number | clear | show}
```

- **by-chassis** force a chassis to be slave
- **by-serial-number** force up to 3 devices to be slave by serial number
- **clear** clear force settings from the cluster
- **show** show current force state

The following example shows how to force chassis 1 to operate in passive mode (slave state). The command delays applying the passive mode state by 20 seconds.

```
diagnose system ha force-slave-state by-chassis 20 1
```

diagnose system load-balance worker-blade status

Display the status of the workers in the cluster. You can use this command to see the relative load being placed on individual workers (CPU and memory usage).

```
diagnose system load-balance worker-blade status
```

```
load balance worker blade in slot 5 (service group 1, chassis 1, snmp  
blade index 1)
```

```
  cpu usage 0 %    mem usage 0 %    uptime 0 seconds  
  sessions  0      setup rate 0  
  last successful update was NEVER, last attempt was less than 10  
seconds ago  
  last update error count 1, total 685
```

```
load balance worker blade in slot 6 (service group 1, chassis 1, snmp  
blade index 2)
```

```
  cpu usage 0 %    mem usage 0 %    uptime 0 seconds  
  sessions  0      setup rate 0  
  last successful update was NEVER, last attempt was less than 10  
seconds ago  
  last update error count 1, total 685
```

diagnose system load-balance worker-blade session-clear

Clear worker sessions.

```
diagnose system load-balance worker-blade session-clear
```

diagnose switch fabric-channel egress list

Display the egress port map for the cluster fabric channel.

```
diagnose switch fabric-channel egress list
```

Switch Interface Egress Map, fabric-Channel
Port Map: Name(Id):

f1(1)	f2(2)	f3(3)	
f4(4)	f5(5)	f6(6)	
f7(7)	f8(8)	slot-1/2(15)	
slot-3(16)	slot-4(17)	slot-5(18)	
slot-6(19)	slot-7(20)	slot-8(21)	
slot-9(22)	slot-10(23)	slot-11(24)	
slot-12(25)	slot-13(26)	slot-14(27)	CPU(0)

Source Interface Destination Ports

f5	0-27
f6	0-27
f7	0-27
f8	0-27
slot-1/2	0-27
slot-3	0-27
slot-4	0-27
slot-5	0-27
slot-6	0-27
slot-7	0-27
slot-8	0-27
slot-9	0-27
slot-10	0-27
slot-11	0-27
slot-12	0-27
slot-13	0-27
slot-14	0-27
trunk	

diagnose switch base-channel egress list

Display the egress port map for the cluster base channel.

```
diagnose switch base-channel egress list
```

Switch Interface Egress Map, base-Channel
Port Map: Name(Id):

sh1(10)	sh2(11)	slot-1/2(12)
slot-3(13)	slot-4(14)	slot-5(15)
slot-6(16)	slot-7(2)	slot-8(3)
slot-9(4)	slot-10(5)	slot-11(6)
slot-12(7)	slot-13(8)	slot-14(9)

base-mgmt (25)		b1 (29) b2 (28)	CPU (0)
Source Interface	Destination Ports		
sh1	0,2-29		
sh2	0,2-29		
slot-1/2	0,2-29		
slot-3	0,2-29		
slot-4	0,2-29		
slot-5	0,2-29		
slot-6	0,2-29		
slot-7	0,2-29		
slot-8	0,2-29		
slot-9	0,2-29		
slot-10	0,2-29		
slot-11	0,2-29		
slot-12	0,2-29		
slot-13	0,2-29		
slot-14	0,2-29		
base-mgmt	0,2-29		
b1	0,2-16,25-26		
b2	0,2-16,25-26		

diagnose switch fabric-channel packet heartbeat-counters list

Display details about heartbeat packets in different ports.

```
diagnose switch fabric-channel packet heartbeat-counters list
```

```
fabric-channel CPU counters:
packet receive error :      0
Non-zero port counters:
f1:
  LACP packet           :      167
  STP packet            :     2292
  unknown bridge packet:      153
f2:
  LACP packet           :      168
  unknown bridge packet:      153
f3:
  LACP packet           :      167
  unknown bridge packet:      153
f4:
  LACP packet           :      168
  unknown bridge packet:      153
slot-5:
  elbcv3 heartbeat      :     25210
slot-6:
  elbcv3 heartbeat      :     25209
```

diagnose switch fabric-channel physical-ports

Display information about fabric channel physical ports.

```
diagnose switch fabric-channel physical-ports {clear-stats | list <port-name> | summary}
```

- **clear-stats** reset counters on one or all ports
- **list <port-name>** list details of a physical port's statistics
- **summary** list summary information of all physical ports

The following example shows how to list all fabric channel ports, list details for slot-5, clear the counters for slot-5 and list the details for slot-5 again.

```
diagnose switch fabric-channel physical-ports summary
```

Portname	Status	Vlan	Duplex	Speed	Flags
f1	up	100	full	10G	QE,TL,
f2	up	100	full	10G	QE,TL,
f3	up	100	full	10G	QE,TL,
f4	up	100	full	10G	QE,TL,
f5	down	104	full	10G	QE, ,
f6	down	105	full	10G	QE, ,
f7	down	106	full	10G	QE, ,
f8	up	107	full	10G	QE, ,
slot-1/2	down	1	full	10G	QI, ,
slot-3	down	1	full	10G	QI, ,
slot-4	down	1	full	10G	QI, ,
slot-5	up	400	full	10G	QI, ,
slot-6	up	400	full	10G	QI, ,
slot-7	down	1	full	10G	QI, ,
slot-8	down	1	full	10G	QI, ,
slot-9	down	1	full	10G	QI, ,
slot-10	down	1	full	10G	QI, ,
slot-11	down	1	full	10G	QI, ,
slot-12	down	1	full	10G	QI, ,
slot-13	down	1	full	10G	QI, ,
slot-14	down	1	full	10G	QI, ,

Flags: QS(802.1Q) QE(802.1Q-in-Q,external) QI(802.1Q-in-Q,internal)
 TS(static trunk) TF(forti trunk) TL(lacp trunk); MD(mirror dst)
 MI(mirror ingress) ME(mirror egress) MB(mirror ingress and egress)

```
diagnose switch fabric-channel physical-ports list slot-5
```

```
Port(slot-5) is up, line protocol is up
Interface Type is 10 Gigabit Media Independent Interface (XGMII)
Address is 00:09:0F:62:11:12, loopback is not set
MTU 16356 bytes, Encapsulation IEEE 802.3/Ethernet-II
full-duplex, 10000 b/s, link type is manual
25994 packets input, 2065330 bytes(unicasts 0, multicasts and broadcasts
25994)
33025 packets output, 14442754 bytes(unicasts 2, multicasts and
```



```
broadcasts 33023)
input: good 25994, drop 0, unknown protocols 0
      error 0 (crc 0, undersize 0, frame 0, oversize 0, jabbers 0,
collisions 0)
output: good 33025, drop 0, error 0

diagnose switch fabric-channel physical-ports clear-stats

diagnose switch fabric-channel physical-ports list slot-5

Port(slot-5) is up, line protocol is up
Interface Type is 10 Gigabit Media Independent Interface (XGMII)
Address is 00:09:0F:62:11:12, loopback is not set
MTU 16356 bytes, Encapsulation IEEE 802.3/Ethernet-II
full-duplex, 10000 b/s, link type is manual
4 packets input, 272 bytes(unicasts 0, multicasts and broadcasts 4)
5 packets output, 2415 bytes(unicasts 0, multicasts and broadcasts 5)
input: good 4, drop 0, unknown protocols 0
      error 0 (crc 0, undersize 0, frame 0, oversize 0, jabbers 0,
collisions 0)
output: good 5, drop 0, error 0
```

diagnose switch fabric-channel mac-address list

List the MAC addresses of interfaces connected to the fabric channel.

```
diagnose switch fabric-channel mac-address list

MAC: 64:00:f1:d2:89:78      VLAN: 100 Trunk: trunk(trunk-id 1)
  Flags: 0x000004c0 [ used trunk ]

MAC: 64:00:f1:d2:89:7b      VLAN: 100 Trunk: trunk(trunk-id 1)
  Flags: 0x000004c0 [ used trunk ]

MAC: 00:09:0f:74:eb:ed      VLAN: 1002 Port: slot-5(port-id 18)
  Flags: 0x00000440 [ used ]

MAC: 08:5b:0e:08:94:cc      VLAN: 100 Trunk: trunk(trunk-id 1)
  Flags: 0x000004c0 [ used trunk ]

MAC: 00:1d:09:f1:14:6b      VLAN: 100 Trunk: trunk(trunk-id 1)
  Flags: 0x000004c0 [ used trunk ]

MAC: 64:00:f1:d2:89:79      VLAN: 100 Trunk: trunk(trunk-id 1)
  Flags: 0x000004c0 [ used trunk ]

MAC: 64:00:f1:d2:89:7a      VLAN: 100 Trunk: trunk(trunk-id 1)
  Flags: 0x000004c0 [ used trunk ]

MAC: 00:1d:09:f1:14:6b      VLAN: 2005 Trunk: unknown(trunk-id 0)
  Flags: 0x000004c0 [ used trunk ]
```

```
MAC: 00:09:0f:74:ec:6b    VLAN: 1002 Port: slot-6(port-id 19)
Flags: 0x00000440 [ used ]
```

diagnose switch fabric-channel mac-address filter

Filter fabric-channel MAC address data to diagnose behavior for link aggregation trunks.

```
diagnose switch fabric-channel mac-address filter {clear | flags | port-id-map | show |
    trunk-id-map | vlan-map}
```

- **clear** clear the MAC address display filter
- **flags** enter a bit pattern to match and mask bits that are displayed
- **port-id-map** set the port-id's to display
- **show** show the current filter settings
- **trunk-id-map** set the trunk-id's to display
- **vlan-map** set the VLANs to display

The following commands show how to display the MAC address list for link aggregation trunk 1.

```
diagnose switch fabric-channel mac-address filter trunk-id-map 1
```

```
diagnose switch fabric-channel mac-address list
```

```
MAC: 64:00:f1:d2:89:78    VLAN: 100 Trunk: trunk(trunk-id 1)
Flags: 0x000004c0 [ used trunk ]
```

```
MAC: 64:00:f1:d2:89:7b    VLAN: 100 Trunk: trunk(trunk-id 1)
Flags: 0x000004c0 [ used trunk ]
```

```
MAC: 08:5b:0e:08:94:cc    VLAN: 100 Trunk: trunk(trunk-id 1)
Flags: 0x000004c0 [ used trunk ]
```

```
MAC: 00:1d:09:f1:14:6b    VLAN: 100 Trunk: trunk(trunk-id 1)
Flags: 0x000004c0 [ used trunk ]
```

```
MAC: 64:00:f1:d2:89:79    VLAN: 100 Trunk: trunk(trunk-id 1)
Flags: 0x000004c0 [ used trunk ]
```

```
MAC: 64:00:f1:d2:89:7a    VLAN: 100 Trunk: trunk(trunk-id 1)
Flags: 0x000004c0 [ used trunk ]
```

diagnose switch fabric-channel trunk list

List the fabric channel trunks and display status information for each link aggregation and LACP trunk. Information displayed includes the port in each link aggregation group and LACP flags.

```
diagnose switch fabric-channel trunk list
```

```
Switch Trunk Information, fabric-Channel
```

```
Trunk Name: trunk
Port Selection Algorithm: src-dst-ip
Minimum Links: 0
```

```
Active Port    Update Time
```

Active Port	Update Time
f1	14:52:36 Aug-27-2014
f2	14:52:38 Aug-27-2014
f3	14:52:38 Aug-27-2014
f4	14:52:38 Aug-27-2014

```
Non-Active Port  Status
```

```
LACP flags: (A|P) (S|F) (A|I) (I|O) (E|D) (E|D)
(A|P) - LACP mode is Active or Passive
(S|F) - LACP speed is Slow or Fast
(A|I) - Aggregatable or Individual
(I|O) - Port In sync or Out of sync
(E|D) - Frame collection is Enabled or Disabled
(E|D) - Frame distribution is Enabled or Disabled
```

```
status: up
Live links: 4
ports: 4
LACP mode: active
LACP speed: slow
aggregator ID: 1
actor key: 1
actor MAC address: 00:09:0f:62:11:01
partner key: 2
partner MAC address: 00:22:56:ba:5d:00
```

```
slave: f1
  status: up
  link failure count: 0
  permanent MAC addr: 00:09:0f:62:11:01
  actor state: ASAIEE
  partner state: ASAIEE
  aggregator ID: 1
```

```
slave: f2
  status: up
  link failure count: 0
  permanent MAC addr: 00:09:0f:62:11:02
  actor state: ASAIEE
  partner state: ASAIEE
  aggregator ID: 1
```

```
slave: f3
  status: up
  link failure count: 0
  permanent MAC addr: 00:09:0f:62:11:03
  actor state: ASAIEE
```

```
partner state: ASAIEE
aggregator ID: 1

slave: f4
status: up
link failure count: 0
permanent MAC addr: 00:09:0f:62:11:04
actor state: ASAIEE
partner state: ASAIEE
aggregator ID: 1
```

FortiController/FortiSwitch MIBs

The FortiController SNMP agent supports Fortinet proprietary MIBs as well as RFCs 1213 and 2665. The support for these RFCs includes parts of RFC 2665 (Ethernet-like MIB) and those elements of RFC 1213 (MIB II) that apply to the FortiController configuration.

There are two MIB files for FortiController boards:

- The Fortinet CORE MIB (FORTINET-CORE-MIB.mib) contains traps, fields and information that are common to all Fortinet products.
- The Fortinet FortiSwitch MIB (FORTINET-FORTISWITCH-MIB.mib) contains traps, fields and information that are specific to FortiController.

You can download these two MIB files from the Fortinet Support site (<https://support.fortinet.com>).

To find the MIBs, after logging into the Support site, select **Download > Firmware Images**. Then select the FortiSwitchATCA product. Select the Download tab and find the FORTINET-CORE-MIB.mib and FORTINET-FORTISWITCH-MIB.mib for your FortiController firmware version.



The functionality described in this document is supported by the following products:

- FortiController 5913C
- FortiController 5903C
- FortiController 5103B

The information is also compatible with most recent versions of the firmware running on these products.

While these hardware products are named FortiController, the FORTINET-FORTISWITCH-MIB.mib file refers to the products as FortiSwitch.

The FORTINET-FORTISWITCH-MIB.mib file includes FortiSwitch/FortiController traps as well as MIB fields that provide information about FortiSwitch/FortiController operating status as well as the operating status of the worker blades in a FortiController SLBC cluster.

Your SNMP manager may already include standard and private MIBs in a compiled database. If this is not the case, you need to download and compile the standard MIB2 files. Then you will need to add the Fortinet Core and FortiController MIBs to this database to view Fortinet specific information.

SNMPv3 with authentication and security level defined will assure encryption of the SNMP queries and replies.

MIB file name or RCF	Description
FORTINET-CORE-MIB.mib	The proprietary Fortinet MIB includes all system configuration and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor FortiController configuration settings and receive traps from the FortiController SNMP agent.
FORTINET-FORTISWITCH-MIB.mib	The FortiController SNMP agent supports MIB II groups with the following exceptions: <ul style="list-style-type: none">• No support for the EGP group from MIB II (RFC 1213, section 3.11 and 6.10).• Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not

MIB file name or RCF	Description
	accurately capture all FortiController traffic activity.
RFC-1213(MIB2)	The FortiController SNMP agent supports MIB2 with these exceptions: <ul style="list-style-type: none">• No support for the EGP group from MIB II (RFC1213, section 3.11 and 6.10).• Protocol statistics returned for MIB II groups (IP/ICMP/TCP/UDP/etc.) do not accurately capture all FortiController traffic activity.
RFC-2665 (Ethernet-like MIB)	The FortiController SNMP agent supports Ethernet-like MIB information with the following exception. <ul style="list-style-type: none">• No support for the dot3Tests and dot3Errors groups.

FortiController/FortiSwitch traps

An SNMP manager can request information from the FortiController/FortiSwitch SNMP agent, or the SNMP agent can send traps when certain pre-defined events occur. To receive FortiController/FortiSwitch SNMP traps, you must load and compile the FORTINETCORE-MIB and FORTINET-FORTISWITCH-MIB into your SNMP manager and configure your FortiController to send traps to your SNMP manager and accept queries from your SNMP manager. All traps sent include the trap message as well as the FortiController serial number (fnSysSerial) and hostname (sysName).

The tables in this section include information about SNMP traps and variables. These tables have been included to help you locate the object identifier number (OID), trap message, and trap description of the FortiController/FortiSwitch trap or variable you require. The name of the table indicates if the trap is located in the Fortinet MIB or the FortiSwitch MIB. The trap message column includes the message included with the trap as well as the SNMP MIB field name to help locate information concerning the trap.

Traps starting with fn such as fnTrapCpuThreshold are defined in the Fortinet MIB. Traps starting with fs such as fsTrapHaSwitch are defined in the FortiSwitch MIB.

The object identifier (OID) is made up of the number at the top of the table with the index then added at the end. For example:

If the OID is 1.3.6.1.4.1.12356.1.3.0 and the index is 4, the full OID is 1.3.6.1.4.1.12356.1.3.0.4

The OID and the name of the object allow SNMP managers to refer to the specific fields and traps from the Fortinet and FortiSwitch MIBs.

Generic Fortinet traps (OID 1.3.6.1.4.1.12356.1.3.0)

Index	Trap message	Description
.1	ColdStart	Standard traps as described in RFC 1215.
.2	WarmStart	
.3	LinkUp	
.3	LinkDown	

Common Fortinet traps (OID 1.3.6.1.4.1.12356.100.1.3.0)

Path: `fnCoreMib.fnCommon.fnTraps`

Index	Trap	Description
.101	<code>fnTrapCpuThreshold</code>	Indicates that the CPU usage has exceeded the configured threshold.
.102	<code>fnTrapMemThreshold</code>	Indicates memory usage has exceeded the configured threshold.
.104	<code>fnTrapTempHigh</code>	A temperature sensor on the device has exceeded its threshold.
.105	<code>fnTrapVoltageOutOfRange</code>	Power levels have fluctuated outside of normal levels.
.106	<code>fnTrapPowerSupplyFailure</code>	Power supply failure detected.
.108	<code>fnTrapFanFailure</code>	A fan failure has been detected.
.201	<code>fnTrapIpChange</code>	The IP address for an interface has changed. The trap message includes the name of the interface, the new IP address and the serial number of the FortiController.

FortiSwitch/FortiController traps (OID 1.3.6.1.4.1.12356.106.2.0)

Path: `fortinet.fnFortiSwitchMib.fsTraps.fsTrapPrefix`

Index	Trap	Description
.401	<code>FsTrapHaSwitch</code>	The specified cluster member has transitioned from a secondary role to a primary role.

Index	Trap	Description
.403	fsTrapHaHBFail	The specified heartbeat device has failed due to link down or heartbeat loss.
.404	fsTrapHaMemberDown	The specified device (by serial number) is moving to a down state.
.405	fsTrapHaMemberUp	A new cluster member has joined the cluster.
.701	fsTrapHBFail	Indicates no heart beat packets received.
.702	fsTrapHBReceived	Indicates heart beat packets have been received.
.703	fsTrapMemberDown	A trunk member has left this trunk.
.704	fsTrapMemberUp	A trunk member has joined this trunk.

FortiController/FortiSwitch MIB fields

FORTINET-FORTISWITCH-MIB.mib contains fields that give access to FortiController/FortiSwitch status information and worker blade status information. The tables in this section list the names of the MIB fields and describe the information available for each one.

To help locate a field, the object identifier (OID) number for each table of fields has been included.

You can view more details about the information available for all FortiGate MIB fields by compiling the FORTINET-CORE-MIB.mib and FORTINET-FORTISWITCH-MIB files into your SNMP manager and browsing the MIB fields.

The fields in the FORTINET-FORTISWITCH-MIB.mib have the following structure:

- FortiSwitch System 1.3.6.1.4.1.12356.106.4
 - FortiSwitch system information 1.3.6.1.4.1.12356.106.4.1
 - FortiSwitch software 1.3.6.1.4.1.12356.106.4.2
- FortiSwitch high availability 1.3.6.1.4.1.12356.106.13
 - FortiSwitch high availability trap objects 1.3.6.1.4.1.12356.106.13.3
- Worker blades 1.3.6.1.4.1.12356.106.14
 - Worker blade information 1.3.6.1.4.1.12356.106.14.1
 - Worker blade tables 1.3.6.1.4.1.12356.106.14.2
 - Individual worker blade information 1.3.6.1.4.1.12356.106.14.2.1
 - Worker blade VDOMs 1.3.6.1.4.1.12356.106.14.2.2
 - Worker blade Antivirus 1.3.6.1.4.1.12356.106.14.2.3
 - Worker blade IPS 1.3.6.1.4.1.12356.106.14.2.4
 - Worker blade processor usage 1.3.6.1.4.1.12356.106.14.2.5

FortiSwitch system information (OID 1.3.6.1.4.1.12356.106.4.1)

Path: `fortinet.fnFortiSwitchMib.fsSystemInfo`

Index	MIB field	Description
	fsSystemInfo	FortiController system information.
.1	fsSysVersion	Current version of the firmware running on the FortiController.
.2	fsSysCpuUsage	Current percent CPU usage.
.3	fsSysMemUsage	Current memory usage in KB.

Index	MIB field	Description
.4	fsSysMemCapacity	The total physical memory (RAM) installed in KB.
.5	fsSysDiskUsage	Current log disk usage in KB.
.6	fsSysDiskCapacity	Log disk capacity in KB.

FortiSwitch software version (OID 1.3.6.1.4.1.12356.106.4.2)

Path: **fortinet.fnFortiSwitchMib.fsSoftware**

Index	MIB field	Description
	fsSoftware	FortiSwitch software (firmware) version information.
.1	fsDirverVersion	FortiSwitch software (firmware) version.

FortiSwitch high availability trap objects (OID 1.3.6.1.4.1.12356.106.13.3)

Path: **fortinet.fnFortiSwitchMib.FsHighAvailabilty.FsHATrapObjects**

Index	MIB field	Description
	FsHATrapObjects	High availability trap objects.
.1	fsHaTrapMemberSerial	Serial number of an HA cluster member. Used to identify the origin of a trap when a cluster is configured.
.2	fsHaTrapHeartbeatDevice	Name of an HA Heartbeat device. Used to identify which device a trap refers to.

Worker blade information (OID 1.3.6.1.4.1.12356.106.14.2.1)

Path:

fortinet.fnFortiSwitchMib.fsServiceGroupWorkerBlades.fsSgWbTables.fsSgWorkerBladeTable

Index	MIB field	Description
.1	fsSgWorkerBladeEntry	System info for a particular worker blade
.1.1	fsSgWbEntIndex	Index that uniquely identifies a worker blade in the fsSgWorkerBladeTable.
.1.2	fsSgWbServiceGroupID	Service group identifier that this worker blade belongs to.
.1.3	fsSgWbChassisID	Chassis identifier of the chassis this worker blade is installed in.
.1.4	fsSgWbSlotID	Slot identifier of the slot this worker blade is installed in.
.1.5	fsSgWbState	State of this worker blade.
.1.6	fsSgWbStatusMsg	Status message for this worker blade.
.1.7	fsSgWbMaster	Indicates if this worker blade is the service group master.
.1.8	fsSgWbConfsyncMaster	Indicates if this worker blade is the confsync master.
.1.9	fsSgWbSysVersion	Firmware version of this worker blade.
.1.10	fsSgWbSysObjectID	MIB-2 system object id of this worker blade.
.1.11	fsSgWbSysName	MIB-2 system name of this worker blade.
.1.12	fsSgWbSysSerial	Serial number of this worker blade.
.1.13	fsSgWbSysUpTime	MIB-2 system up time of this worker blade. The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

Index	MIB field	Description
.1.14	fsSgWbSysDescr	MIB-2 system description of this worker blade.
.1.15	fsSgWbSysContact	MIB-2 system contact for this worker blade.
.1.16	fsSgWbSysLocation	MIB-2 system location of this worker blade.
.1.17	fsSgWbSysMgmtVdom	Index that identifies the management virtual domain.
.1.18	fsSgWbSysCpuUsage	Current CPU usage (percentage).
.1.19	fsSgWbSysMemUsage	Current memory utilization (percentage).
.1.20	fsSgWbSysMemCapacity	Total physical memory (RAM) installed (KB).
.1.21	fsSgWbSysLowMemUsage	Current lowmem utilization (percentage). Lowmem is memory available for the kernel's own data structures and kernel specific tables. The system can get into a bad state if it runs out of lowmem.
.1.22	fsSgWbSysLowMemCapacity	Total lowmem capacity (KB).
.1.23	fsSgWbSysDiskUsage	Current hard disk usage (MB), if disk is present.
.1.24	fsSgWbSysDiskCapacity	Total hard disk capacity (MB), if disk is present.
.1.25	fsSgWbSysSesCount	Number of active sessions on the worker blade.
.1.26	fsSgWbSysSesRate1	The average session setup rate (sessions per second) over the past minute.
.1.27	fsSgWbSysSesRate10	The average session setup rate (sessions per second) over the past 10 minutes.
.1.28	fsSgWbSysSesRate30	The average session setup rate (sessions per second) over the past 30 minutes.

Index	MIB field	Description
.1.29	fsSgWbSysSesRate60	The average session setup rate (sessions per second) over the past 60 minutes.
.1.30	fsSgWbCpuCounts	The number of CPU cores inside working blade.

Worker blade VDOM (OID 1.3.6.1.4.1.12356.106.14.2.2)

Path: fortinet.fnFortiSwitchMib.fsServiceGroupWorkerBlades.fsSgWbTables.fsSgWbVdTable

Index	MIB field	Description
.1	fsSgWbVdEntry	An entry containing information applicable to a particular virtual domain on particular worker blade.
.1.1	fsSgWbVdBladeIndex	Internal worker blade index. Used to uniquely identify rows in this table. These indices are also used by other tables referencing a virtual domain on a worker blade.
.1.2	fsSgWbVdEntIndex	Internal virtual domain index. Used to uniquely identify rows in this table. These indices are also used by other tables referencing a virtual domain on a worker blade.
.1.3	fsSgWbVdEntName	The name of the virtual domain.
.1.4	fsSgWbVdEntOpMode	Operation mode of the virtual domain (NAT or Transparent).

Worker blade Antivirus (OID 1.3.6.1.4.1.12356.106.14.2.3)

Path:

fortinet.fnFortiSwitchMib.fsServiceGroupWorkerBlades.fsSgWbTables.fsSgWbAvStatsTable

Index	MIB field	Description
.1	FsSgWbAvStatsEntry	Antivirus statistics for a particular virtual domain on this worker blade.
.1.1	fsSgWbAvVirusDetected	Number of virus transmissions detected in the virtual domain on this worker blade since start-up.
.1.2	fsSgWbAvVirusBlocked	Number of virus transmissions blocked in the virtual domain on this worker blade since start-up.
.1.3	fsSgWbAvHTTPVirusDetected	Number of virus transmissions over HTTP detected in the virtual domain on this worker blade since start-up.
.1.4	fsSgWbAvHTTPVirusBlocked	Number of virus transmissions over HTTP blocked in the virtual domain on this worker blade since start-up.
.1.5	fsSgWbAvSMTPVirusDetected	Number of virus transmissions over SMTP detected in the virtual domain on this worker blade since start-up.
.1.6	fsSgWbAvSMTPVirusBlocked	Number of virus transmissions over SMTP blocked in the virtual domain on this worker blade since start-up.
.1.7	fsSgWbAvPOP3VirusDetected	Number of virus transmissions over POP3 detected in the virtual domain on this worker blade since start-up.

Index	MIB field	Description
.1.8	fsSgWbAvPOP3VirusBlocked	Number of virus transmissions over POP3 blocked in the virtual domain on this worker blade since start-up.
.1.9	fsSgWbAvIMAPVirusDetected	Number of virus transmissions over IMAP detected in the virtual domain on this worker blade since start-up.
.1.10	fsSgWbAvIMAPVirusBlocked	Number of virus transmissions over IMAP blocked in the virtual domain on this worker blade since start-up.
.1.11	fsSgWbAvFTPVirusDetected	Number of virus transmissions over FTP detected in the virtual domain on this worker blade since start-up.
.1.12	fsSgWbAvFTPVirusBlocked	Number of virus transmissions over FTP blocked in the virtual domain on this worker blade since start-up.
.1.13	fsSgWbAvIMVirusDetected	Number of virus transmissions over IM protocols detected in the virtual domain on this worker blade since start-up.
.1.14	fsSgWbAvIMVirusBlocked	Number of virus transmissions over IM protocols blocked in the virtual domain on this worker blade since start-up.
.1.15	fsSgWbAvNNTPVirusDetected	Number of virus transmissions over NNTP detected in the virtual domain on this worker blade since start-up.

Index	MIB field	Description
.1.16	fsSgWbAvNNTPVirusBlocked	Number of virus transmissions over NNTP blocked in the virtual domain on this worker blade since start-up.
.1.17	fsSgWbAvOversizedDetected	Number of over-sized file transmissions detected in the virtual domain on this worker blade since start-up.
.1.18	fsSgWbAvOversizedBlocked	Number of over-sized file transmissions blocked in the virtual domain on this worker blade since start-up.

Worker blade IPS (OID 1.3.6.1.4.1.12356.106.14.2.4)

Path:

fortinet.fnFortiSwitchMib.fsServiceGroupWorkerBlades.fsSgWbTables.fsSgWbIpsStatsTable

Index	MIB field	Description
.1	fsSgWbIpsStatsEntry	IPS/IDS statistics for a particular virtual domain on each worker blade.
.1.1	fsSgWbIpsIntrusionsDetected	Number of intrusions detected since start-up in this virtual domain on this worker blade.
.1.2	fsSgWbIpsIntrusionsBlocked	Number of intrusions blocked since start-up in this virtual domain on this worker blade.
.1.3	fsSgWbIpsCritSevDetections	Number of critical severity intrusions detected since start-up in this virtual domain on this worker blade.
.1.4	fsSgWbIpsHighSevDetections	Number of high severity intrusions detected since start-up in this virtual domain on this worker blade.

Index	MIB field	Description
.1.5	fsSgWblpsMedSevDetections	Number of medium severity intrusions detected since start-up in this virtual domain on this worker blade.
.1.6	fsSgWblpsLowSevDetections	Number of low severity intrusions detected since start-up in this virtual domain on this worker blade.
.1.7	fsSgWblpsInfoSevDetections	Number of informational severity intrusions detected since start-up in this virtual domain on this worker blade.
.1.8	fsSgWblpsSignatureDetections	Number of intrusions detected by signature since start-up in this virtual domain on this worker blade.
.1.9	fsSgWblpsAnomalyDetections	Number of intrusions DECed as anomalies since start-up in this virtual domain on this worker blade.

Worker blade processor usage (OID 1.3.6.1.4.1.12356.106.14.2.5)

Path:

fortinet.fnFortiSwitchMib.fsServiceGroupWorkerBlades.fsSgWbTables.fsSgWbProcessorTable

Index	MIB field	Description
.1	fsSgWbProcessorEntry	System info for a particular worker blade.
.1.1	fsSgWbProcessorBladeIndex	Internal FortiGate Blade index. Along with fsSgWbVdEntIndex, used to uniquely identify rows in this table. These indices are also used by other table referencing a virtual domain on a worker blade.

Index	MIB field	Description
.1.2	fsSgWbProcessorEntIndex	Index that uniquely identifies a Process in the fsSgWorkerBladeTable.
.1.3	fsSgWbProcessorCpuUsage	Current CPU usage (percentage) on this processor/core.

Shelf manager traps

The following shelf manager traps are available from the PPS-PETv2-MIB.txt MIB file. Shelf manager traps follow the IPMI Platform Event Trap (PET) format.

The path is SNMPv2-SMI::enterprises.wiredForManagement.pet.version OID 1.3.6.1.4.1.3183.1.1

- Notification root 1.3.6.1.4.1.3183.1.1.0
- IPMI trap data 1.3.6.1.4.1.3183.1.1.1
- IPMI trap text 1.3.6.1.4.1.3183.1.1.2
- IPMI PET multi-variable format 1.3.6.1.4.1.3183.1.1.3

Notification root (OID 1.3.6.1.4.1.3183.1.1.0)

Path: SNMPv2-SMI::enterprises.wiredForManagement.pet.version.notificationRoot

Index	Trap	Description
.1	ipmiNotification	IPMI PET format v1.0.
.2	ipmiNotification2	IPMI PET in text format.
.3	ipmiNotification3	IPMI PET in multi-variable format.

IPMI trap data (OID 1.3.6.1.4.1.3183.1.1.1)

Path: SNMPv2-SMI::enterprises.wiredForManagement.pet.version.ipmi-trap-data

PET information in standard form.

IPMI trap text (OID 1.3.6.1.4.1.3183.1.1.2)

Path: SNMPv2-SMI::enterprises.wiredForManagement.pet.version.ipmi-trap-text

PET information in plain text form.

IPMI PET multi-variable format (OID 1.3.6.1.4.1.3183.1.1.3)

Path: `SNMPv2-SMI::enterprises.wiredForManagement.pet.version.ipmiTrapMultivar`

IPMI PET in multi-variable format.

Index	Trap	Description
.1	ipmi-trap-record-id	System Event Log (SEL) record ID in 0..0xFFFF range.
.2	ipmi-trap-record-type	SEL record type.
.3	ipmi-trap-timestamp	SEL timestamp in seconds from 1/1/1970.
.4	ipmi-trap-manufacturer	Manufacturer ID for timestamped OEM events.
.5	ipmi-trap-generator-address	IPMB address of the event generator.
.6	ipmi-trap-generator-lun	LUN of the event generator.
.7	ipmi-trap-generator-channel	Channel number of the event source.
.8	ipmi-trap-sensor-type	Sensor Type.
.9	ipmi-trap-sensor-number	Sensor number.
.10	ipmi-trap-event-type	Event reading type.
.11	ipmi-trap-event-direction	Event direction.
.12	ipmi-trap-event-data	Event data.
.13	ipmi-trap-entire-record	The entire SEL record.
.14	ipmi-trap-severity	Optional event severity.
.15	ipmi-trap-string	Optional alert string.

Shelf manager MIB fields

To run SNMP queries with the FortiGate-5000 shelf manager you need to import the PPS-SENTRY-MIB.txt file into your SNMP manager. Use SNMP version 2c and the community string `public`.

To help locate a field, the object identifier (OID) number for each table of fields has been included. The OID number for a field is that field's position within the table, starting at 0.

The path is `SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm` and the OID for this path is `.1.3.6.1.4.1.16394.2.1.1`

This section describes the following fields in this path.

- IPM sentry SHMM 1.3.6.1.4.1.16394.2.1.1
 - IPM controller 1.3.6.1.4.1.16394.2.1.1.1
 - FRU device 1.3.6.1.4.1.16394.2.1.1.2
 - Sensor 1.3.6.1.4.1.16394.2.1.1.3
 - Board 1.3.6.1.4.1.16394.2.1.1.4
 - System event log (Sel) 1.3.6.1.4.1.16394.2.1.1.5
 - Shelf 1.3.6.1.4.1.16394.2.1.1.6
 - LAN configuration 1.3.6.1.4.1.16394.2.1.1.7
 - Shelf manager platform event filter (PEF) 1.3.6.1.4.1.16394.2.1.1.8 - 19
 - FRU information table 1.3.6.1.4.1.16394.2.1.1.20
 - Shelf manager FRU device by site 1.3.6.1.4.1.16394.2.1.1.21
 - FRU LED state 1.3.6.1.4.1.16394.2.1.1.22
 - Board basic information 1.3.6.1.4.1.16394.2.1.1.32
 - Fan trays 1.3.6.1.4.1.16394.2.1.1.33
 - Power supply 1.3.6.1.4.1.16394.2.1.1.34
 - Shelf manager 1.3.6.1.4.1.16394.2.1.1.35
 - Chassis 1.3.6.1.4.1.16394.2.1.1.36
 - Shelf manager event 1.3.6.1.4.1.16394.2.1.1.37
 - Shelf manager shelf manager status 1.3.6.1.4.1.16394.2.1.1.38
 - Shelf manager shelf manager version 1.3.6.1.4.1.16394.2.1.1.39
 - Shelf manager telco alarm 1.3.6.1.4.1.16394.2.1.1.40
 - Shelf manager sel information 1.3.6.1.4.1.16394.2.1.1.41

Shelf manager IPM controller (OID 1.3.6.1.4.1.16394.2.1.1.1)

Path: `SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.ipm-controller`

A list of IPM controllers.

Index	MIB field	Description
.1	ipm-controller-entry	An IPM controller entry.
.1.1	ipm-controller-index	The IPM controller index.
.1.2	ipm-controller-sdr-version	The IPM controller SDR version
.1.3	ipm-controller-picmg-version	The IPM controller PICMG version.
.1.4	ipm-controller-slave-address	Address of the backup IPM controller.
.1.5	ipm-controller-channel-number	The IPM controller channel number.
.1.6	ipm-controller-power-state-notification	Information about the state of the IPM controller power.
.1.7	ipm-controller-global-initialization	IPM controller global initialization.
.1.8	ipm-controller-capabilities	IPM controller capabilities.
.1.9	ipm-controller-id-string	IPM controller ID.
.1.10	ipm-controller-maximum-fru	The maximum number of FRUs that the IPM controller can manage.
.1.11	ipm-controller-own-fru-id	The FRU ID of the IPM controller.

Shelf manager FRU device (OID 1.3.6.1.4.1.16394.2.1.1.2)

Path: `SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.fru-device`

List of FRU Devices.

Index	MIB field	Description
.1	fru-device-entry	A FRU device list entry.
.1.1	fru-device-index	Returns FRU device index in (SA<<16 + FruID) form.
.1.2	fru-device-sdr-version	Returns SDR Version from corresponding device locator record in SDR repository or -1 if record is absent.

Index	MIB field	Description
.1.3	fru-device-slave-address	Returns device slave address.
.1.4	fru-device-fru-device-id	Returns FRU device ID.
.1.5	fru-device-channel-number	Returns channel number from corresponding device locator record in SDR Repository or -1 if record is absent.
.1.6	fru-device-device-type	Returns device type from corresponding Device Locator Record in SDR Repository for non-zero FRUs, 10h for FRU#0 or -1 if record is absent.
.1.7	fru-device-device-type-modifier	Returns device type Modifier from corresponding device locator record in SDR Repository for non-zero FRUs, FFh for FRU#0 or -1 if record is absent.
.1.8	fru-device-fru-entity-id	Returns entity ID from corresponding device locator record in SDR repository or -1 if record is absent.
.1.9	fru-device-fru-entity-instance	Returns entity instance from corresponding device locator record in SDR repository or -1 if record is absent.
.1.10	fru-device-id-string	Returns device ID string from corresponding device locator record in SDR repository or N/A if record is absent.
.1.11	fru-device-hot-swap-state	Returns the current HotSwap State of a FRU device.
.1.12	fru-device-activated	Returns 1 if FRU is in M4 hot swap state and 0 otherwise. Setting this to 1 is equivalent to FRU activation request and setting to 0 leads to deactivation.

Shelf manager sensor (OID 1.3.6.1.4.1.16394.2.1.1.3)

Path: SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.sensor

The following example shows how to extract the current state mask information from a TELCO alarm sensor. This value returns the current state of the alarm of the SAP module (corresponding to the LED indicator state located on the chassis front panel).

In the following shelf manager message example, the last line indicates that this is a major alarm.

```
20: LUN: 0, Sensor # 131 ("TELCO Alarms")
    Type: Discrete (0x6f), "OEM reserved" (0xdf)
    Belongs to entity (0xf0, 0x01): FRU # 0
    Status: 0xc0
        All event messages enabled from this sensor
        Sensor scanning enabled
        Initial update completed
    Sensor reading: 0x00
    Current State Mask 0x0002
```

1. The sensor object entry point for the OID is .1.3.6.1.4.1.16394.2.1.1.3.1 corresponding to SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.sensor.sensor-entry
2. The SNMP query extracts the value of the sensor-processed-reading MIB field, which has the OID of .1.3.6.1.4.1.16394.2.1.1.3.1.29.
3. The query should also include the IPMB slave address in decimal format:
For the TELCO Alarms : 0x20 is 32 in decimal so the OID is .1.3.6.1.4.1.16394.2.1.1.3.1.29.32.
4. You can get the sensor ID from the shelf manager command `cli sensordata`, where the sensor name and ID is explicit, the OID is .1.3.6.1.4.1.16394.2.1.1.3.1.29.32.131.
5. Finally, poll the Telco alarm state with the OID .1.3.6.1.4.1.16394.2.1.1.3.1.29.32.131.
6. To obtain the status of the alarm with `snmpget`:

```
snmpget -c public -v 2c 192.168.181.98 1.3.6.1.4.1.16394.2.1.1.3.1.29.32.131
SNMPv2-SMI::enterprises.16394.2.1.1.3.1.29.32.131 = STRING: "Current State Mask 0x0002"
```

The returned value is a binary mask where 1=minor, 2=major, 4=critical. So for example, 0x0003, would mean a minor and a critical alarm were raised.

Index	MIB field	Description
.1	sensor-entry	A FRU device list entry.
.1.1	sensor-index	
.1.2	sensor-sdr-version	
.1.3	sensor-record-type	
.1.4	sensor-owner-id	
.1.5	sensor-owner-lun	
.1.6	sensor-number	
.1.7	sensor-entity-instance	

Index	MIB field	Description
.1.8	sensor-entity-id	
.1.9	sensor-initialization	
.1.10	sensor-capabilities	
.1.11	sensor-type	
.1.12	sensor-event	
.1.13	sensor-assertion-event-mask	
.1.14	sensor-deassertion-event-mask	
.1.15	sensor-mask	
.1.16	sensor-unit1	
.1.17	sensor-unit2	
.1.18	sensor-unit3	
.1.19	sensor-linearization	
.1.20	sensor-M	
.1.21	sensor-tolerance	
.1.22	sensor-B	
.1.23	sensor-accuracy	
.1.24	sensor-accuracy-exp	
.1.25	sensor-R-exp	
.1.26	sensor-B-exp	
.1.27	sensor-characteristic-flags	
.1.28	sensor-reading	
.1.29	sensor-processed-reading	
.1.20	sensor-nominal-reading	
.1.31	sensor-nominal-maximum	
.1.32	sensor-nominal-minimum	
.1.33	sensor-maximum-reading	
.1.34	sensor-minimum-reading	
.1.35	sensor-upper-non-recoverable-threshold	
.1.36	sensor-upper-critical-threshold	
.1.37	sensor-upper-non-critical-threshold	

Index	MIB field	Description
.1.38	sensor-lower-non-recoverable-threshold	
.1.39	sensor-lower-critical-threshold	
.1.40	sensor-lower-non-critical-threshold	
.1.41	sensor-positive-going-threshold-hysteresis	
.1.42	sensor-negative-going-threshold-hysteresis	
.1.43	sensor-id-string	
.1.44	sensor-entire-sensor-data	
.1.45	sensor-processed-unr-threshold	Processed upper non-recoverable threshold value.
.1.46	sensor-processed-uc-threshold	Processed upper critical threshold value.
.1.47	sensor-processed-unc-threshold	Processed upper non-critical threshold value.
.1.48	sensor-processed-lnr-threshold	Processed lower non-recoverable threshold value.
.1.49	sensor-processed-lc-threshold	Processed lower critical threshold value.
.1.50	sensor-processed-lnc-threshold	Processed lower non-critical threshold value.

Shelf manager board (OID 1.3.6.1.4.1.16394.2.1.1.4)

Path: `SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.board`

A list of IPM Controllers.

Index	MIB field	Description
.1	board-entry	An IPM controller entry.
.1.1	board-index	Index.
.1.2	board-present	
.1.3	board-healthy	
.1.4	board-reset	
.1.5	board-slave-address	
.1.6	board-fru-device-id	

Shelf manager system event log (sel) (OID 1.3.6.1.4.1.16394.2.1.1.5)

Path: SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.sel

A list of IPM Controllers.

Index	MIB field	Description
.1	sel-entry	An IPM controller entry.
.1.1	sel-index	Index.
.1.2	sel-contents	

Shelf manager shelf (OID 1.3.6.1.4.1.16394.2.1.1.6)

Path: SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.shelf

A list of IPM Controllers.

Index	MIB field	Description
.1	shelf-entry	An IPM Controller entry.
.1.1	shelf-index	Index.
.1.2	shelf-healthy	

Shelf manager LAN configuration (OID 1.3.6.1.4.1.16394.2.1.1.7)

Path: SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.lan-configuration

Index	MIB field	Description
.1	lan-configuration-entry	An IPM entry.
.1.1	lan-configuration-index	Index.
.1.2	lan-configuration-set-in-progress	
.1.3	lan-configuration-authentication-type-support	
.1.4	lan-configuration-authentication-type-enable	
.1.5	lan-configuration-ip-address	
.1.6	lan-configuration-ip-address-source	
.1.7	lan-configuration-mac-address	
.1.8	lan-configuration-subnet-mask	
.1.9	lan-configuration-ipv4-header-parameters	
.1.10	lan-configuration-primary-rmcp-port-number	
.1.11	lan-configuration-secondary-rmcp-port-number	
.1.12	lan-configuration-bmc-generated-arp-control	
.1.13	lan-configuration-gratuitous-arp-interval	
.1.14	lan-configuration-default-gateway-address	
.1.15	lan-configuration-default-gateway-mac-address	
.1.16	lan-configuration-backup-gateway-address	
.1.17	lan-configuration-backup-gateway-mac-address	
.1.18	lan-configuration-community-string	
.1.19	lan-configuration-number-of-destinations	
.1.20 - 35	lan-configuration-destination-type-0 - 15	Sixteen destination type fields.
.1.36 - 51	lan-configuration-destination-address-0 - 15	Sixteen destination addresses.
.1.52	lan-configuration-vlan-id	802.1q VLAN ID (12-bit)
.1.53	lan-configuration-vlan-priority	802.1q VLAN Priority (3-bit)

Index	MIB field	Description
.1.54	lan-configuration-cipher-suite-entry-support	This parameter provides a count of the number (16 max.) of cipher suites available to be enabled for use with IPMI messaging on the given channel.
.1.55	lan-configuration-cipher-suite-entries	This parameter contains zero to sixteen (16) bytes of cipher suite IDs for cipher suites that can be used for establishing an IPMI messaging session with the BMC. The number of cipher suites that are supported is given in the preceding parameter.
.1.56	lan-configuration-cipher-suite-priv-level	This parameter allows the configuration of which privilege levels are associated with each cipher suite. The total number of nibble supported (zero to sixteen) matches the number of fixed cipher suite IDs
.1.57 - 72	lan-configuration-destination-address-vlan-tag-0 - 15	Gets the VLAN IDs (if any) addresses that a LAN alert can be sent to with destination selector 0 to 15.

Shelf manager platform event filter (PEF) (OIDs 1.3.6.1.4.1.16394.2.1.1.8 - 19)

Path: **SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.pef-***

Index	MIB field	Description
8	pef-configuration-set-in-progress	
9	pef-configuration-control	
10	pef-configuration-action-global-control	
11	pef-configuration-startup-delay	

Index	MIB field	Description
12	pef-configuration-alert-startup-delay	
13	pef-configuration-number-of-event-filters	
14	pef-configuration-event-filter-table	Platform event filter table.
14.1	pef-configuration-event-filter-table-entry	Platform event filter entry.
14.1.1	pef-configuration-event-filter-index	Index.
14.1.2	pef-configuration-event-filter-data	
15	pef-configuration-number-of-alert-policy-entries	
16	pef-configuration-alert-policy-table	Platform event alert policy table.
16.1	pef-configuration-alert-policy-table-entry	Platform event alert policy entry.
16.1.1	pef-configuration-alert-policy-index	Index.
16.1.2	pef-configuration-alert-policy-data	
17	pef-configuration-system-guid	
18	pef-configuration-number-of-alert-strings	
19	pef-configuration-alert-string-table	Platform event alert string table.
19.1	pef-configuration-alert-string-table-entry	Platform event alert string entry.
19.1.1	pef-configuration-alert-string-index	Index
19.1.2	pef-configuration-alert-string-key	
19.1.3	pef-configuration-alert-string	

Shelf manager FRU info table (OID 1.3.6.1.4.1.16394.2.1.1.20)

Path: [SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.fru-info-table](#)

FRU contents table.

Index	MIB field	Description
.1	fru-info-table-entry	FRU contents entry.

Index	MIB field	Description
.1.1	fru-info-index	<p>Index: <ipmb_addr>. <fru_id>.<32-bytes block number></p> <p>Where:</p> <p>ipmb_addr << 24 fru_id << 16</p>
.1.2	fru-info-data	
.1.3	fru-info-data-wo	<p>As index use should use the following sequence <ipmb_addr>.<fru_id>.<offset></p> <p>Due to specific of implementation:</p> <p><ipmb_addr> should be u8 <fru_id> should be u8 <offset> should be u16 - offset in bytes.</p> <p>As a result _WRITEABLE_ FRU Info size is reduced to 65535 bytes.</p>

Shelf manager FRU device by site (OID 1.3.6.1.4.1.16394.2.1.1.21)

Path: SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.fru-device-by-site

List of FRU Devices indexed by sites.

Index	MIB field	Description
.1	fru-device-by-site-entry	FRU device list entry indexed by sites.
.1.1	fru-device-by-site-index	<p>Returns FRU device index in the following format:</p> <p>SiteType<<16 + SiteNumber</p>
.1.2	fru-device-by-site-sdr-version	<p>Returns SDR version from corresponding device locator record in SDR repository or -1 if record is absent.</p>

Index	MIB field	Description
.1.3	fru-device-by-site-slave-address	Returns device slave address.
.1.4	fru-device-by-site-fru-device-by-site-id	Returns FRU device ID.
.1.5	fru-device-by-site-channel-number	Returns channel number from corresponding device locator record in SDR repository or -1 if record is absent.
.1.6	fru-device-by-site-device-type	Returns device type from corresponding device locator record in SDR repository for non-zero FRUs, 10h for FRU#0 or -1 if record is absent.
.1.7	fru-device-by-site-device-type-modifier	Returns device type modifier from corresponding device locator record in SDR repository for non-zero FRUs, FFh for FRU#0 or -1 if record is absent.
.1.8	fru-device-by-site-fru-entity-id	Returns entity ID from corresponding device locator record in SDR repository or -1 if record is absent.
.1.9	fru-device-by-site-fru-entity-instance	Returns entity Instance from corresponding device locator record in SDR repository or -1 if record is absent.
.1.10	fru-device-by-site-id-string	Returns device ID string from corresponding device locator record in SDR repository or N/A if record is absent.
.1.11	fru-device-by-site-hot-swap-state	Returns the current HotSwap state of a FRU device.
.1.12	fru-device-by-site-activated	Returns 1 if FRU is in M4 hot swap state and 0 otherwise. Setting this to 1 is equivalent to FRU activation request and setting to 0 leads to deactivation.

Shelf manager FRU LED state (OID 1.3.6.1.4.1.16394.2.1.1.22)

Path: SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.fru-led-state

List of FRU LEDs.

Index	MIB field	Description
.1	fru-led-state-entry	FRU LEDs list entry.
.1.1	led-index	Table entry index, equal to: <ipmb_addr> << 24 <fru_id> << 16 <led_number>
.1.2	led-color-capabilities	The bit mask of colors supported by the LED, defined as follows: [0] - reserved, set to 0 [1] - LED supports BLUE [2] - LED supports RED [3] - LED supports GREEN [4] - LED supports AMBER [5] - LED supports ORANGE [6] - LED supports WHITE
.1.3	led-state-capabilities	The bit mask of special LED flags, defined as follows: [0] - LED is powered from Payload power [1] - LED has another hardware restriction
.1.4	led-default-local-color	The default LED color in local control state, in the range 0 to 6, defined as follows: 0 - local control not supported 1 - BLUE 2 - RED 3 - GREEN 4 - AMBER 5 - ORANGE 6 - WHITE

Index	MIB field	Description
.1.5	led-default-override-color	The default LED color in override state, in the range 1 to 6, defined as follows: 1 - BLUE 2 - RED 3 - GREEN 4 - AMBER 5 - ORANGE 6 - WHITE
.1.6	led-current-state-flags	The bit mask of current LED state flags, defined as follows: [0] - the LED has local control state [1] - the override state has been enabled [2] - the lamp test has been enabled [3] - LED has a hardware restriction that is not currently met
.1.7	led-local-state	The current LED local control state and color. Reported as 0 if the LED does not support local control state, otherwise defined as follows: Bits 0-7:local control LED function (byte 4 of the Get FRU LED state command response) Bits 8-15:local control on-duration (byte 5 of the Get FRU LED state command response) Bits 16-24:local control color (byte 6 of the Get FRU LED State command response)
.1.8	led-override-state	The current LED local control state and color.

Index	MIB field	Description
		<p>On read, reported as 0 if the command response to get FRU LED state does not include bytes 7 to 9.</p> <p>Otherwise, and for write access, the value is defined as follows:</p> <p>Bits 0-7:override state LED function (byte 7 of the get FRU LED state command response, byte 4 of the set FRU LED state command request).</p> <p>Bits 8-15:override state on-duration (byte 8 of the get FRU LED state command response, byte 5 of the set FRU LED state command request).</p> <p>Bits 16-24:override state color (byte 9 of the get FRU LED state command response, byte 6 of the set FRU LED state command request).</p> <p>On write, return to local control state can be requested by placing FCh in bits 0-7;lamp test can be requested by placing FBh in bits 0-7 and lamp test duration, in hundreds of milliseconds, in bits 8-15.</p>
.1.9	lamp-test-duration	Current lamp test duration, in hundreds of milliseconds. Reported as 0 if the LED is not in a lamp test state..

Shelf manager board basic (OID 1.3.6.1.4.1.16394.2.1.1.32)

Path: `SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.board-basic`

A list of boards.

Index	MIB field	Description
.1	board-basic-entry	A board entry.
.1.1	board-basic-slot-number	
.1.2	board-basic-present	
.1.3	board-basic-healthy	
.1.4	board-basic-reset	
.1.5	board-basic-powered	
.1.6	board-basic-slave-address	
.1.7	board-basic-fru-device-id	
.1.8	board-basic-fruinfo-product-area-present	
.1.9	board-basic-fruinfo-product-manufacturer	
.1.10	board-basic-fruinfo-product-name	
.1.11	board-basic-fruinfo-product-part-model-number	
.1.12	board-basic-fruinfo-product-version-number	
.1.13	board-basic-fruinfo-product-serial-number	
.1.14	board-basic-fruinfo-board-area-present	
.1.15	board-basic-fruinfo-board-manufacturer	
.1.16	board-basic-fruinfo-board-product-name	
.1.17	board-basic-fruinfo-board-serial-number	
.1.18	board-basic-fruinfo-board-part-number	
.1.19	board-basic-fruinfo-board-manufacture-time	
.1.20	board-basic-fruinfo-product-asset-tag	
.1.21	board-basic-fruinfo-product-fru-file-id	
.1.22	board-basic-fruinfo-board-fru-file-id	

Shelf manager fan tray (OID 1.3.6.1.4.1.16394.2.1.1.33)

Path: `SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.fantray`

The table contains information about the Fan Trays in the system.

Index	MIB field	Description
.1	fantry-entry	An entry provides information about a single fan tray. Entries are indexed by a physical fan tray number which is equal to fan tray site number.
.1.1	fantray-slot-number	Table entry index, equal to the physical fan tray number.
.1.2	fantray-present	Returns (1) if fan tray is present in the slot, (0) otherwise.
.1.3	fantray-healthy	Returns (0) if the fan tray is unhealthy (i.e. it is in M1, M7 or the latest state change cause for this fan tray was unexpected), (1) otherwise.
.1.4	fantray-health-led	Returns the led state (0 =off, 1 =on) on reading. Writing to this variable turns the led on (value=1) or off (value=0). This variable is available in 2.x systems only. In ATCA systems it always is equal to -1
.1.5	fantray-slave-address	Returns the 8-bit slave address of the IPM controller representing this fan tray on IPMB.
.1.6	fantray-fru-device-id	The FRU device ID of the fan tray.
.1.7	fantray-fruinfo-product-area-present	Returns (1) if the product area is present within the fan tray FRU information, (0) otherwise.
.1.8	fantray-fruinfo-product-manufacturer	Returns the product manufacturer from the fan tray FRU information, or N/A.

Index	MIB field	Description
.1.9	fantray-fruinfo-product-name	Returns the product name from the fan tray FRU information, or N/A.
.1.10	fantray-fruinfo-product-part-model-number	Returns the product part model number from the fan tray FRU information, or N/A.
.1.11	fantray-fruinfo-product-version-number	Returns the product version from the fan tray FRU information, or N/A.
.1.12	fantray-fruinfo-product-serial-number	Returns the product serial number from the fan tray FRU information, or N/A.
.1.13	fantray-fruinfo-board-area-present	Returns (1) if the board area is present within the fan tray FRU information, (0) otherwise.
.1.14	fantray-fruinfo-board-manufacturer	Returns the board manufacturer from the fan tray FRU information, or N/A.
.1.15	fantray-fruinfo-board-product-name	Returns the board product name from the fan tray FRU information, or N/A.
.1.16	fantray-fruinfo-board-serial-number	Returns the board serial number from the fan tray FRU information, or N/A.
.1.17	fantray-fruinfo-board-part-number	Returns the board part number from the fan tray FRU information, or N/A.
.1.18	fantray-fruinfo-board-manufacture-time	Returns the board manufacturing time:the number of seconds since 00:00:00, January 1, 1970, (UTC) Returns -1 if the corresponding field is not present in the fan tray FRU information.

Index	MIB field	Description
.1.19	fantray-fan-level	This variable allows getting/setting a current fan level.
.1.20	fantray-fruinfo-product-asset-tag	Returns the product asset tag from the fan tray FRU information, or N/A.
.1.21	fantray-fruinfo-product-fru-file-id	Returns the product FRU File ID from the fan tray FRU information, or N/A.
.1.22	fantray-fruinfo-board-fru-file-id	Returns the board FRU File ID from the fan tray FRU information, or N/A.

Shelf manager power supply (OID 1.3.6.1.4.1.16394.2.1.1.34)

Path: `SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.powersupply`

The table contains information about the Power Supplies in the system.

Index	MIB field	Description
.1	powersupply-entry	An entry provides information about a single power supply. Entries are indexed by a physical power supply number which is equal to site number.
.1.1	powersupply-slot-number	Table entry index, equal to the physical power supply number.
.1.2	powersupply-degrade	Returns (1) if the power supply is in the degraded state, (0) otherwise. This variable is available in 2.x systems only.
.1.3	powersupply-fail	Returns (1) if the power supply is in the Failed state, (0) otherwise. This variable is available in 2.x systems only.

Index	MIB field	Description
.1.4	powersupply-inhibit	Returns (1) if the power supply is in the Inhibited state, (0) otherwise. Writing a value to this field inhibits the power supply (if value=1) or re-enables it (if value=0). This variable is available in 2.x systems only.
.1.5	powersupply-healthy	Returns (0) if the power supply is unhealthy (i.e. it is in M1, M7 or the latest state change cause for this power supply was unexpected), (1) otherwise.
.1.6	powersupply-slave-address	Returns the 8-bit slave address of the IPM controller representing this power supply on IPMB.
.1.7	powersupply-fru-device-id	Returns the FRU device ID of the power supply.
.1.8	powersupply-fruinfo-product-area-present	Returns (1) if the product area is present within the power supply FRU information, (0) otherwise.
.1.9	powersupply-fruinfo-product-manufacturer	Returns the product manufacturer from the power supply FRU information, or N/A.
.1.10	powersupply-fruinfo-product-name	Returns the product name from the power supply FRU information, or N/A.
.1.11	powersupply-fruinfo-product-part-model-number	Returns the product part model number from the power supply FRU information, or N/A.
.1.12	powersupply-fruinfo-product-version-number	Returns the product version from the power supply FRU information, or N/A.

Index	MIB field	Description
.1.13	powersupply-fruinfo-product-serial-number	Returns the product serial number from the power supply FRU information, or N/A.
.1.14	powersupply-fruinfo-board-area-present	Returns (1) if the board area is present within the power supply FRU information, (0) otherwise.
.1.15	powersupply-fruinfo-board-manufacturer	Returns the board manufacturer from the power supply FRU information, or N/A.
.1.16	powersupply-fruinfo-board-product-name	Returns the board product name from the power supply FRU information, or N/A.
.1.17	powersupply-fruinfo-board-serial-number	Returns the board serial number from the power supply FRU information, or N/A.
.1.18	powersupply-fruinfo-board-part-number	Returns the board part number from the power supply FRU information, or N/A.
.1.19	powersupply-fruinfo-board-manufacture-time	Returns the board manufacturing time:the number of seconds since 00:00:00, January 1, 1970, (UTC). -1 if the corresponding field is not present in the power supply FRU information
.1.20	powersupply-fruinfo-product-asset-tag	Returns the product asset tag from the power supply FRU information, or N/A.
.1.21	powersupply-fruinfo-product-fru-file-id	Returns the product FRU file ID from the power supply FRU information, or N/A.
.1.22	powersupply-fruinfo-board-fru-file-id	Returns the board FRU file ID from the power supply FRU information, or N/A.

Shelf manager shelf manager (OID 1.3.6.1.4.1.16394.2.1.1.35)

Path: SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.shelf-manager

This table contains information about the shelf managers in the system.

Index	MIB field	Description
.1	shelf-manager-entry	An entry provides information about a single shelf manager. Entries are indexed by a physical shelf manager number, which is equal to the site number.
.1.1	shelf-manager-instance	Table entry index, equal to the physical shelf manager number.
.1.2	shelf-manager-ipmc-slave-address	The 8-bit slave address of the IPM controller representing this shelf manager on IPMB.
.1.3	shelf-manager-present	Reports (1) if the shelf manager is present in the slot, (0) otherwise.
.1.4	shelf-manager-healthy	Reports (1) if the shelf manager is healthy (i.e. it is in M4 state), (0) otherwise.
.1.5	shelf-manager-active	Returns (1) if the shelf manager is active, (0) otherwise. Writing 0 to this field triggers a reboot of the shelf manager, causing a switchover to the other shelf manager.
.1.6	shelf-manager-reset	Returns (1) if shelf manager is in the reset state, (0) otherwise. Writing 1 to this field triggers a reset of the target shelf manager if the other shelf manager is present.

Index	MIB field	Description
.1.7	shelf-manager-fruinfo-product-area-present	Returns (1) if the product area is present within the shelf manager FRU Information, (0) otherwise.
.1.8	shelf-manager-fruinfo-product-manufacturer	Returns the product manufacturer from the shelf manager FRU information, or N/A.
.1.9	shelf-manager-fruinfo-product-name	Returns the product name from the shelf manager FRU information, or N/A.
.1.10	shelf-manager-fruinfo-product-part-model-number	Returns the product part model number from the shelf manager FRU information, or N/A.
.1.11	shelf-manager-fruinfo-product-version-number	Returns the product version from the shelf manager FRU information, or N/A.
.1.12	shelf-manager-fruinfo-product-serial-number	Returns the product serial number from the Shelf Manager FRU Information, or N/A.
.1.13	shelf-manager-fruinfo-board-area-present	Returns (1) if the board area is present within the shelf manager FRU information, (0) otherwise.
.1.14	shelf-manager-fruinfo-board-manufacturer	Returns the board manufacturer from the shelf manager FRU Information, or N/A.
.1.15	shelf-manager-fruinfo-board-product-name	Returns the board product name from the shelf manager FRU information, or N/A.
.1.16	shelf-manager-fruinfo-board-serial-number	Returns the board serial number from the shelf manager FRU information, or N/A.

Index	MIB field	Description
.1.17	shelf-manager-fruinfo-board-part-number	Returns the board part number from the shelf manager FRU information, or N/A.
.1.18	shelf-manager-fruinfo-board-manufacture-time	Returns the board manufacturing time:the number of seconds since 00:00:00, January 1, 1970, UTC;-1if the corresponding field is not present in the shelf manager FRU information.
.1.19	shelf-manager-fruinfo-product-asset-tag	Returns the product asset tag from the shelf manager FRU Information, or N/A.
.1.20	shelf-manager-fruinfo-product-fru-file-id	Returns the product FRU file ID from the shelf manager FRU information, or N/A.
.1.21	shelf-manager-fruinfo-board-fru-file-id	Returns the board FRU file ID from the shelf manager FRU information, or N/A

Shelf manager chassis (OID 1.3.6.1.4.1.16394.2.1.1.36)

Path: SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.chassis

Index	MIB field	Description
.1	chassis-id	Read/write shelf address record from the shelf FRU information.
.2	chassis-type	The 8-bit chassis type from the shelf FRU information
.3	chassis-part-number	Returns (1) if fan tray is present in the slot, (0) otherwise.
.4	chassis-serial-number	Chassis serial number from the shelf FRU information.

Index	MIB field	Description
.5	chassis-product-area-present	Reports (1) if the product area is present within the shelf FRU information or (0) if it is absent.
.6	chassis-product-manufacturer	Returns the product manufacturer from the shelf FRU information or N/A.
.7	chassis-product-name	Returns the product name from the shelf FRU information or N/A.
.8	chassis-product-part-model-number	Returns the product part model number from the shelf FRU information or N/A.
.9	chassis-product-version-number	Returns the product version from the shelf FRU information or N/A.
.10	chassis-product-serial-number	Returns the product serial number from the shelf FRU information or N/A.
.11	chassis-board-area-present	Reports (1) if the board area is present within the shelf FRU information or (0) if it is absent.
.12	chassis-board-manufacturer	Returns the board manufacturer from the shelf FRU information or N/A.
.13	chassis-board-product-name	Returns the board product name from the shelf FRU information or N/A.
.14	chassis-board-serial-number	Returns the board serial number from the shelf FRU information or N/A.
.15	chassis-board-part-number	Returns the board part number from the shelf FRU information or N/A.

Index	MIB field	Description
.16	chassis-board-manufacture-time	Returns the board manufacturing time: the number of seconds since 00:00:00, January 1, 1970, (UTC); -1 if the corresponding field is not present in the shelf FRU information.
.17	chassis-product-asset-tag	Returns the product asset tag from the shelf FRU information or N/A.
.18	chassis-product-fru-file-id	Returns the product FRU file ID from the shelf FRU information or N/A.
.19	chassis-board-fru-file-id	Returns the board FRU file ID from the shelf FRU information or N/A.

Shelf manager events (OID 1.3.6.1.4.1.16394.2.1.1.37)

Path: `SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.events`

This table contains information about the System Event Log (SEL) entries in the system.

Index	MIB field	Description
.1	event-entry	The entry provides information about a single SEL entry.
.1.1	event-index	Table entry index.
.1.2	event-delete	Returns (0) on reading, Writing 1 causes the current SEL entry to be deleted.
.1.3	event-timestamp	Timestamp of the SEL entry in seconds since 1/1/1970.
.1.4	event-class	Event class.
.1.5	event-type	Event type.
.1.6	event-asserted	Event assertion state.
.1.7	event-origin-site-type	Origin site type.

Index	MIB field	Description
.1.8	event-origin-site-number	Origin site number.
.1.9	event-origin-slave-address	Origin IPMB address.
.1.10	event-origin-fru-id	Origin FRU device ID.
.1.11	event-origin-sensor-number	Origin sensor number.
.1.12	event-format	SEL record type.
.1.13	event-reading-type	Event/Reading type code.
.1.14	event-data	Event data.
.1.15	event-sel-id	Event entry ID in SEL i.e. index in the SEL branch.

Shelf manager shelf manager status (OID 1.3.6.1.4.1.16394.2.1.1.38)

Path: SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.shelf-manager-status

Index	MIB field	Description
.1	rmcp-interface-status	Returns status of the RMCP interface.
.2	shelf-fru-found-status	Show if the shelf FRU information was found or not.
.3	active-status	Show if the current shelf manager is active or backup.

Shelf manager shelf manager version (OID 1.3.6.1.4.1.16394.2.1.1.39)

Path: SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.shelf-manager-version

Index	MIB field	Description
.1	major-version	Returns shelf manager major version.
.2	minor-version	Returns shelf manager minor version.
.3	carrier-type	Returns carrier type.

Index	MIB field	Description
.4	carrier-subtype	Returns carrier subtype.
.5	carrier-subversion	Returns carrier subversion.
.6	functional-level	Returns functional level: 0 - Normal shelf manager. 1 - Entry-level shelf manager.

Shelf manager telco alarm (OID 1.3.6.1.4.1.16394.2.1.1.40)

Path: **SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.telco-alarm**

Index	MIB field	Description
.1	minor-alarm	Returns or changes minor TELCO alarm state.
.2	major-alarm	Returns or changes major TELCO alarm state.
.3	critical-alarm	Returns or changes critical TELCO alarm state.
.4	alarm-cutoff	Returns TELCO alarm cutoff state.

Shelf manager SEL information (OID 1.3.6.1.4.1.16394.2.1.1.41)

Path: **SNMPv2-SMI::enterprises.pps.products.chassis-management.ipm-sentry-shmm.sel-info**

Index	MIB field	Description
.1	sel-version	Returns SEL version.
.2	sel-entry-count	Returns the current number of SEL entries.
.3	sel-capacity	Returns SEL capacity in events.
.4	sel-add-timestamp	Returns timestamp for the most recent SEL entry addition in seconds since 1/1/1970.

Index	MIB field	Description
.5	sel-del-timestamp	Returns timestamp for the most recent SEL entry deletion in seconds since 1/1/1970.
.6	sel-overflow-state	Returns the value of the SEL overflow status flag.

FortiController/FortiSwitch SNMP links

This section includes links to Fortinet Knowledge base articles that contain configuration examples and other information that you can use to configure and troubleshoot SNMP with a FortiGate-5000 SLBC chassis.

Technical Note : FortiGate Chassis - Shelf manager management overview

This article provides an overview of the capabilities of the shelf manager card which is used to monitor and manage a FortiGate 5140 chassis.

Technical Note: How to configure SNMP polling on FortiController and worker blades with SLBC

How to configure SLBC to poll FortiController, FortiGate directly or through FortiController.

Technical Note : Advanced SNMP trap configuration for a FortiGate 5140 shelf manager

This document provides an overview of functionality, as well as example SNMP traps, that can be generated by the FortiGate 5140 shelf manager.

Technical Note : How to modify the community strings on the shelf manager - FortiGate chassis

This article describes how to modify the community strings on the shelf manager for SNMP polling.

Technical Note: How to configure shelf manager to send SNMP trap V2 and not V1

This article describes how to change the configuration of the shelf manager to send SNMP traps with SNMP v2.

Technical Note: No response for SNMP queries directed to secondary FortiController on chassis slot #2

When FortiController high availability is configured, SNMP queries meant for the secondary FortiController on slot #2 have to be relayed by the primary FortiController via the base management channel. If the primary FortiController's internal base interface's IP is not added to the SNMP community's hosts list on the secondary FortiController, the SNMP queries will be dropped and not processed.



FORTINET®



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.