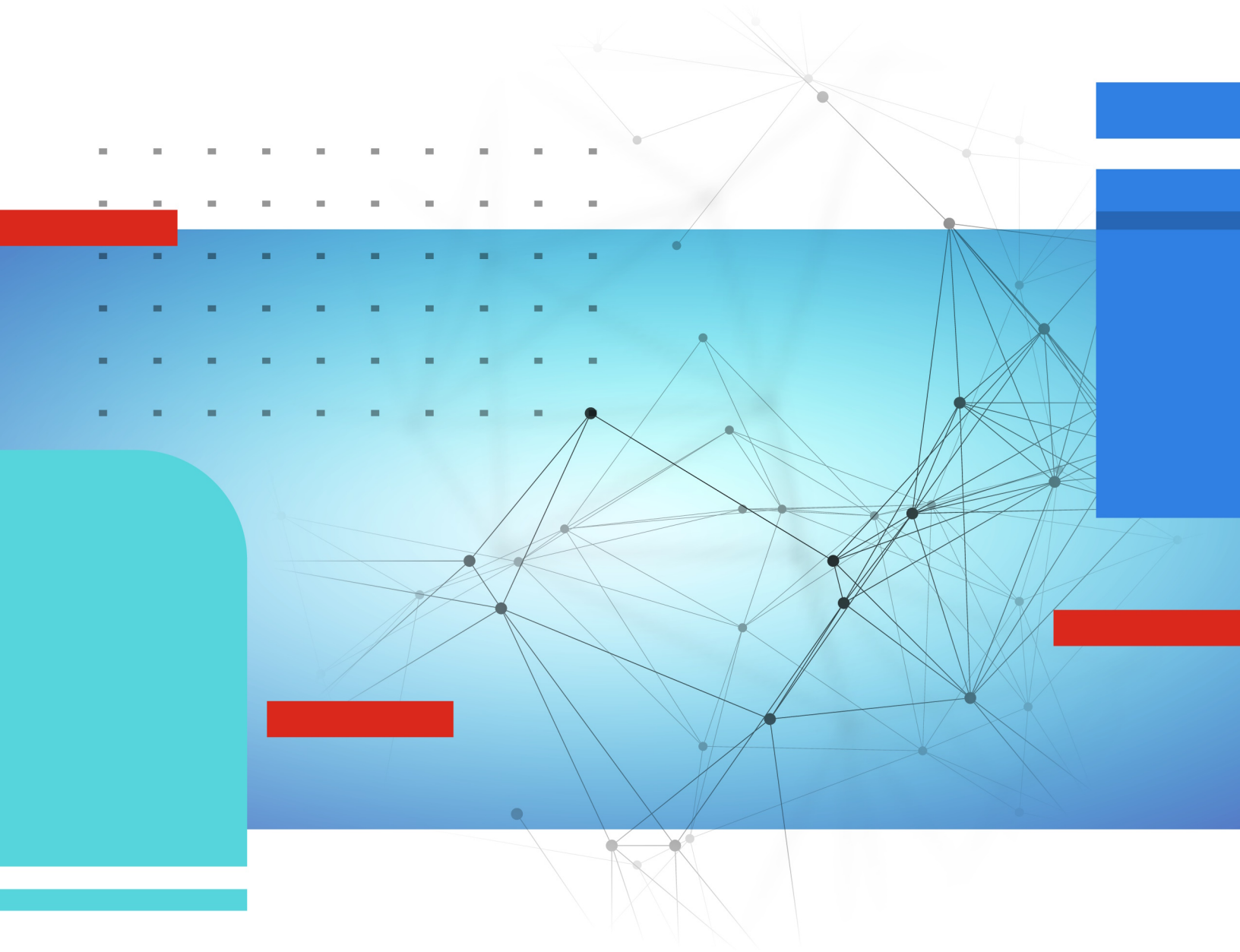
Sizing Guide - EventDB

FortiSIEM 7.3.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

12/16/2024
FortiSIEM 7.3.0 Sizing Guide - EventDB

TABLE OF CONTENTS

Change Log

Date	Change Description
12/16/2024	Sizing Guide - EventDB release for 7.3.0.

FortiSIEM Sizing Guide - EventDB

This document provides information about the following topics:

Minimum Requirements

Hardware

Minimum hardware requirements for FortiSIEM nodes are as follows.

Node	vCPU	RAM	Local Disks
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum • without UEBA – 24GB • with UEBA - 32GB Recommended • without UEBA – 32GB • with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB Local Event database – based on need
Supervisor (Cluster)	Minimum – 12 Recommended - 32	Minimum • without UEBA – 24GB • with UEBA - 32GB Recommended • without UEBA – 32GB • with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB
Workers	Minimum – 8 Recommended - 16	Minimum – 16GB Recommended • without UEBA – 24GB • with UEBA - 32GB	OS – 25GB OPT – 100GB
Collector	Minimum – 4	Minimum – 4GB	OS – 25GB

Node	vCPU	RAM	Local Disks
	Recommended – 8 (based on load)	Recommended – 8GB	OPT – 100GB

- Supervisor VA needs more memory since it hosts many heavy-duty components such as Application Server (Java), PostGreSQL Database Server and Rule Master.
- For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when `configFSM.sh` runs.

Note that these are only the minimum requirements. The performance may improve by increasing vCPUs and RAM in certain situations. External storage depends on your EPS mix and the number of days of log storage needs. To provide more meaningful guidance, scalability tests were conducted as described below.

Internal Scalability Tests

FortiSIEM team performed several scalability tests described below.

Test Setup

- A specific set of events were sent repeatedly to achieve the target EPS.
- The target EPS was constant over time.
- A set of Linux servers were monitored via SNMP and performance monitoring data was collected.
- Events triggered many incidents.

Test Success Criteria

The following success criteria should be met on testing:

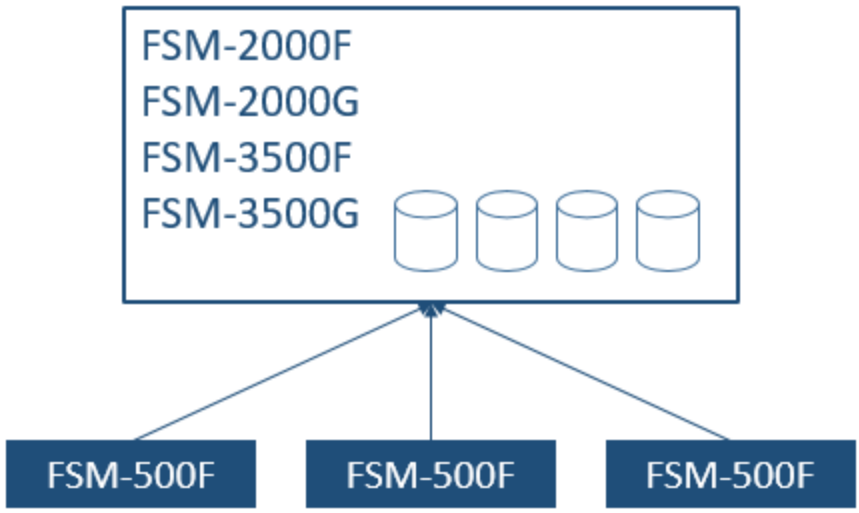
- Incoming EPS must be sustained without any event loss.
- Summary dashboards should be up to date and not fall behind.
- Widget dashboards should show data indicating that inline reporting is keeping up.
- Incidents should be up to date.
- Real-time search should show current data and trend chart should reflect incoming EPS.
- GUI navigation should be smooth.
- CPU, memory and IOPS are not maxed out. Load average must be less than the number of cores.

The tests were run for the following cases:

- All-in-one FSM Hardware Appliance: FSM-2000F and FSM-3500F with collectors FSM-500F sending events.
- FSM Virtual Appliance with FortiSIEM EventDB as the data store.

Hardware Appliance EPS Test with FortiSIEM Event Database

The test beds is shown below. Scripts generated events on FSM-500F Collectors, which parsed those events and sent them to the appliances.



The results are shown below:

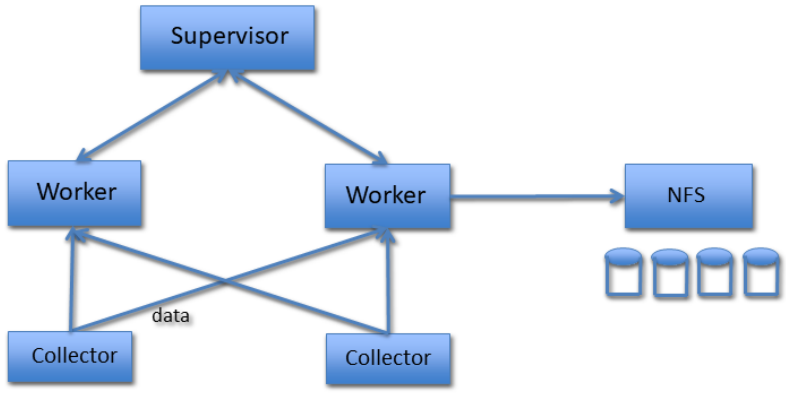
		Event Sender			
Appliance	**Hardware Spec**	**Collector Model**	**Count**	**EPS/Collector**	**Sustained EPS without Loss**
FSM-2000F	• 12vCPU (1x6C2T) • 32GB RAM • 12x3TB SATA (3 RAID Groups)	FSM-500F	3	5K	15K
FSM-2000G	• 40vCPU (2x10C2T) • 128GB RAM • 4x1TB SSD (RAID5) • 8x4TB SAS (2 RAID50 Groups)	FSM-500F	3	6K	20K
FSM-3500G	• 48vCPU (2x12C2T) • 128GB RAM • 24x4TB SATA (3 RAID50 Groups)	FSM-500F	6	8K	40K

Virtual Appliance EPS Test with FortiSIEM Event Database

All tests were done in AWS. The following hardware was used.

Type	AWS Instance Type	Hardware Spec
Collector	c4.xlarge	4vCPU, 7 GB RAM
Worker	c4.2xlarge	8vCPU, 15 GB RAM
Super	m4.4xlarge	16vCPU, 64 GB RAM, CMDB Disk 10K IOPS
NFS Server	c4.2xlarge	8vCPU, 16 GB RAM, 10K IOPS

The test bed is as follows:



The following result shows 10K EPS sustained per Worker with over 20K CMDB Devices.

Event Sender			Event Handler				
Collector Count	EPS/Collector	Monitored Device/Collector	Super	Workers	Orgs	CMDB Device	Sustained EPS without Loss
150	200	150	1	3	150	22,500	30K

Sizing Online Deployment

Processing Requirement

Requirement		Recommendation			
EPS	Deployment	HW Model	SW Configuration		
			Nodes	HW Per Node (vCPU, RAM)	NFS IOPS
Up to 5K	Hardware	FSM-2000F			
Up to 5K	Software		All-in-one	16, 24GB	

Requirement		Recommendation			
EPS	Deployment	HW Model	SW Configuration		
			Nodes	HW Per Node (vCPU, RAM)	NFS IOPS
5K – 10K	Hardware	FSM-2000F			
5K – 10K	Software		Supervisor	16, 24GB	
			1 Worker	8, 16GB	2000
10K – 15K	Hardware	FSM-3500F			
10K – 15K	Software		Supervisor	16, 24GB	
			2 Workers	8, 16GB	3000
15K – 25K	Hardware	FSM-3500F			
15K – 25K	Software		Supervisor	16, 24GB	
			3 Workers	16,16GB	5000
25K – 35K	Software		Supervisor	16, 24GB	
			4 Workers	16, 16GB	7000
Add 10K EPS	**Software**		**Add 1 Worker**	**16, 16GB**	**Add 2000 IOPS**
10K – 15K	Hardware	FSM-3500G			
10K – 15K	Software		Supervisor	16, 24GB	
			2 Workers	8, 16GB	3000
15K – 25K	Hardware	FSM-3500G			
15K – 25K	Software		Supervisor	16, 24GB	
			3 Workers	16, 16GB	5000
25K – 35K	Software		Supervisor	16, 24GB	
			4 Workers	16, 16GB	7000
Add 10K EPS	**Software**		**Add 1 Worker**	**16, 16GB**	**Add 2000 IOPS**

Storage Requirement

FortiSIEM storage requirement depends on three factors:

- EPS
- Bytes/log mix in your environment
- Compression ratio (typically 4:1)

Calculating the average event size and average event rate in your environment is important to estimate the likely storage requirements more accurately. Considerations include:

1. The EPS variance over time. In many environments the event rate peaks during morning hours on weekdays and goes down dramatically after 2 pm on weekdays, and also remains low on weekends.
2. The log size and log mix. Unix and Router logs tend to be in the 200-300 Bytes range, Firewall logs (e.g. Fortinet, Palo Alto) tend to be in the 700-1,500 Bytes range, Windows Security logs tend to be a little larger (1,500 – 2,000 Bytes), and Cloud logs tend to be much larger (2,000 Bytes -10K Bytes sometimes).

It is important to provision the NFS server with enough IOPS and network bandwidth for read and write of event data and where possible cater for peaks in EPS. It is recommended that NFS is provisioned with 10Gbit interfaces or higher and the FortiSIEM Supervisor and Worker nodes to also be provisioned with 10Gbit interfaces to the NFS storage network.

The table below shows storage estimates for two EventDB based scenarios. The worst case is calculated at 100% of the peak EPS. The average case is 50% of the peak EPS. Both scenarios assume 500 byte average event size and 4:1 compression. 1kb = 1024b. 1 month = 30 days.

Peak EPS	Storage (Months)	NFS Storage (TB)*	
		Worst Case	Average Case
1000	12	3.6	1.8
1000	24	7.1	3.6
1000	36	10.7	5.4
2000	12	7.1	3.6
2000	24	14.2	7.1
2000	36	21.3	10.7
5000	12	17.7	8.9
5000	24	35.4	17.7
5000	36	53.1	26.6
10000	12	35.4	17.7
10000	24	70.8	35.4
10000	36	106.1	53.1

NFS Storage (TB):

- Worst case = (Peak EPS*500*86400*30*Storage(Months))/(4*10^12)
- Average case = (0.5*Peak EPS*500*86400*30*Storage(Months))/(4*10^12)

Sizing Archive Deployment

In this situation, online workers are used to query the Archived EventDB database, so only a NFS infrastructure is required. Since Archived data is not indexed, our experiments have shown that Archived EventDB needs about 60% storage compared to Online EventDB. This information can be used to estimate the amount of NFS storage required for Archive.

EPS	Retention	NFS Storage	
	Months	Worst Case (500 Bytes/log)	Average Case (50% EPS, 500 Bytes/log)
1000	12	2.2	1.1
1000	24	4.3	2.2
1000	36	6.4	3.2
2000	12	4.3	2.2
2000	24	8.5	4.3
2000	36	12.8	6.4
5000	12	10.6	5.3
5000	24	21.2	10.6
5000	36	31.9	16.0
10000	12	21.2	10.6
10000	24	42.5	21.2
10000	36	63.7	31.9

www.fortinet.com