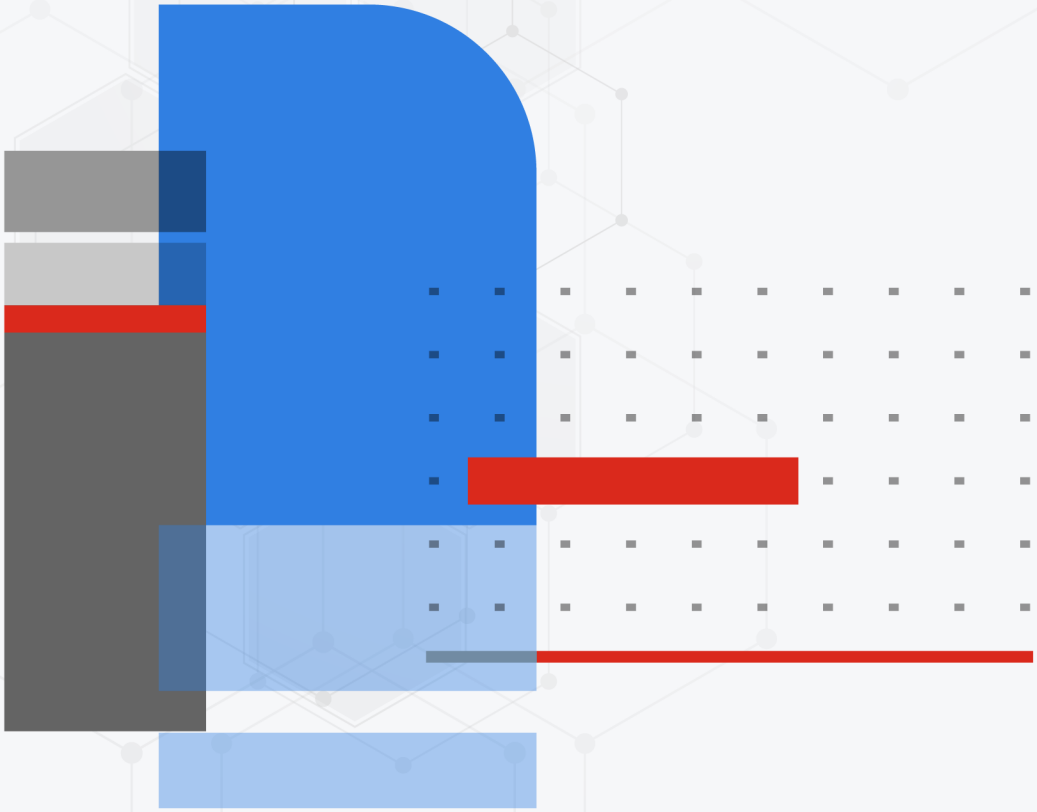
Sizing Guide - EventDB

FortiSIEM 6.7.0



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/training-certification

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

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

10/02/2023
FortiSIEM 6.7.0 Sizing Guide - EventDB

TABLE OF CONTENTS

Change Log

Date	Change Description
03/30/2018	Initial release of FortiSIEM Sizing Guide.
04/12/2018	Revision 2 with updates to Storage Requirements for FortiSIEM EventDB and Elasticsearch Data Nodes sections.
11/20/2019	Sizing Guide released for 5.2.6.
03/30/2020	Sizing Guide release for 5.3.0.
09/08/2020	Sizing Guide release for 6.1.0.
03/23/2021	Sizing Guide release for 6.2.0.
04/12/2021	Sizing Guide updated with Sizing Online Deployments and Sizing Archive Deployments for 6.2.0.
05/06/2021	Sizing Guide release for 6.2.1.
06/15/2021	FSM-3500G information added for 6.2.x.
07/06/2021	Sizing Guide release for 6.3.0.
08/26/2021	Sizing Guide release for 6.3.1.
10/15/2021	Sizing Guide release for 6.3.2.
12/22/2021	Sizing Guide release for 6.3.3.
01/04/2022	Minimum Requirements Hardware section updated for 6.x Sizing guides.
01/05/2022	Spark / HDFS Resource Allocation Considerations added to HDFS Based Deployments section for 6.4.0.
01/18/2022	Sizing Guide release for 6.4.0.
03/09/2022	Spark / HDFS Resource Allocation Considerations section updated for 6.4.0 Sizing Guide.
05/09/2022	Sizing Guide release for 6.5.0.
05/31/2022	Added: Hardware Appliance EPS Test with ClickHouse, Cluster Wide Shard Count Limit (Elasticsearch), ClickHouse Based Deployment
07/26/2022	Sizing Guide release for 6.6.0. Virtual Appliance EPS Test with ClickHouse Database section added. Sizing Online Deployments - ClickHouse Based Deployment section updated.
08/23/2022	Added: Shard Count column for ClickHouse Software Based Deployments (Minimum Requirement) and ClickHouse Software Based Deployments (Recommended Requirement).

Date	Change Description
08/24/2022	Update to ClickHouse Software Based Deployments (Minimum Requirement) and ClickHouse Software Based Deployments (Recommended Requirement) tables.
09/12/2022	Sizing Guide release for 6.5.1.
09/14/2022	Sizing Guide release for 6.6.1.
09/19/2022	Sizing Guide release for 6.6.2.
02/07/2023	Sizing Guide - EventDB release for 6.7.0.
02/13/2023	Sizing Guide - EventDB release for 6.7.1.
03/07/2023	Sizing Guide - EventDB release for 6.7.2.
03/28/2023	Sizing Guide - EventDB release for 6.7.3.
04/11/2023	Sizing Guide - EventDB release for 6.7.4.
05/22/2023	Sizing Guide - EventDB release for 6.7.5.
06/16/2023	Sizing Guide - EventDB release for 6.7.6.
07/13/2023	Sizing Guide - EventDB release for 6.7.7.
09/12/2023	Sizing Guide - EventDB release for 6.7.8.
10/02/2023	Added OPT information under Minimum Requirements - Hardware.

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:

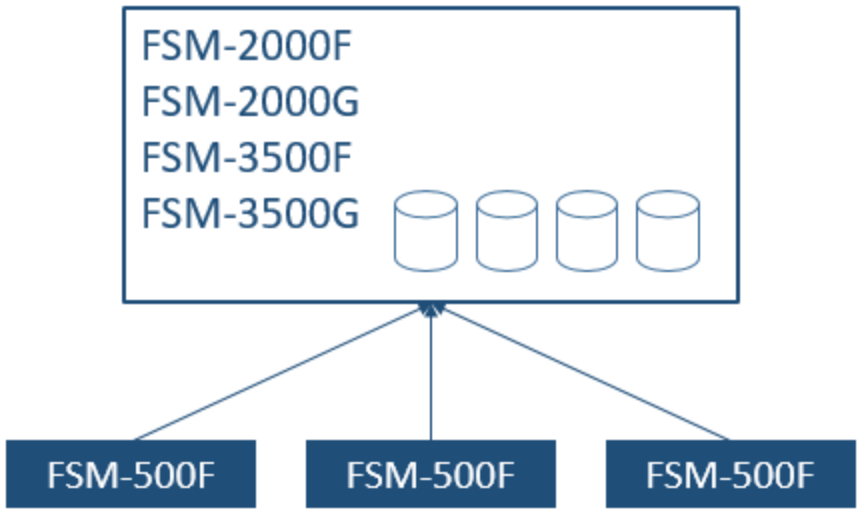
- Incoming EPS must be sustained without any event loss.
- Summary dashboards should be up to date and not fall behind.
- Widget dashboards should show data indicating that inline reporting is keeping up.
- Incidents should be up to date.
- Real-time search should show current data and trend chart should 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:

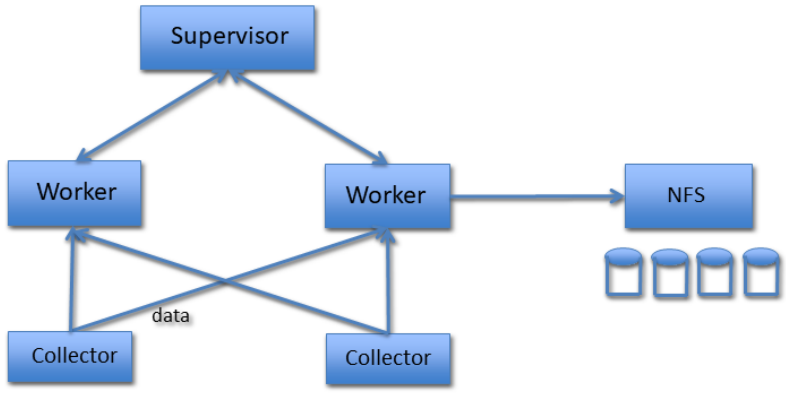
	Event Sender				
FortiSIEM HW Appliance	**Hardware Spec**	**Collector Model**	**Count**	**EPS/Collector**	**Sustained EPS without Loss**
FSM-2000F	2000F - 12vCPU (1x6C2T), 32GB RAM, 12x3TB SATA (3 RAID Groups)	FSM-500F	3	5K	15K
FSM-2000G	2000G - 40vCPU (2x10C2T), 128GB RAM, 4x1TB SSD (RAID5), 8x4TB SAS (2 RAID50 Groups)	FSM-500F	3	6K	20K
FSM-3500G	3500G,48vCPU (2x12C2T),128GB RAM,24x4TBSATA (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 (4:1)

You are likely licensed for Peak EPS. Typically, EPS peaks during morning hours on weekdays and goes down dramatically after 2 pm on weekdays and also remains low on weekends. So the average EPS should be used to calculate storage needs.

For calculating Bytes/log, consider the following aspects:

- Network devices and Linux servers tend to send shorter logs (150-200 bytes/log) while Windows Security logs tend to be much larger (500-1000 bytes/log).
- Busy corporate firewalls and domain controllers tend to send much higher log volumes (higher EPS) than other systems, assuming they are sending all logs.
- Database indices built on logs for efficient searching consumes significant storage as well.
- ASCII text (syslog) compresses much better than binary (for example, Netflow)

Therefore, it is difficult to properly assume a specific bytes/log mix in your environment without measurement. Our experience from sampling of 5 large customers has shown that Bytes/log is between 100-150 including all factors – device mix, log mix, indexing cost and compression. Fortinet calculated this by dividing the total FortiSIEM event file size (in `\data`) over one day by the total number of events on that day, and then averaging over a few days.

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 two scenarios – Worst case and average case for NFS storage. In worst case, Peak EPS and 150 Bytes/log is used. In the average case, 0.5 Peak EPS and 100 Bytes/log is used.

Peak EPS	Storage (Months)	NFS Storage (TB) (Rounded to the nearest 0.5TB)	
		Worst Case	Average Case
1000	12	1.5	0.5
1000	24	2.5	1
1000	36	3.5	1.5
2000	12	2.5	1
2000	24	4.5	1.5
2000	36	6.5	2.5
5000	12	5.5	2
5000	24	11	4
5000	36	16	5.5
10000	12	11	4
10000	24	21.5	7.5
10000	36	32	11

NFS Storage (GB):

- Worst case = (Peak EPS*150*86400*30*Storage(Months))/(4 * 1024 * 1024 * 1024)
- Average case = (0.5*Peak EPS*100*86400*30*Storage(Months))/(4 * 1024 * 1024 * 1024)

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	
		Worst Case (100 Bytes/log)	Average Case (66 Bytes/log)
5K	6 months	7.5 TB	2.5 TB
	1 year	15 TB	5 TB
	3 years	45 TB	15 TB
10K	6 months	15 TB	5 TB
	1 year	30 TB	10 TB
	3 years	90 TB	30 TB
20K	6 months	30 TB	10 TB
	1 year	60 TB	20 TB
	3 years	180 TB	60 TB
50K	6 months	75 TB	25 TB
	1 year	150 TB	50 TB
	3 years	450 TB	150 TB
100K	6 months	150 TB	50 TB
	1 year	300 TB	100 TB
	3 years	900 TB	100 TB

Worst Case Storage = EPS * 86400 * worst case bytes/log * retention

Average Case Storage = 0.5* EPS * 86400 * average case bytes/log * retention

Used 1024 for B -> KB etc.

www.fortinet.com