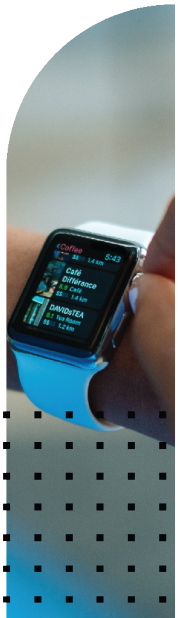
Sizing Guide

FortiSOAR 7.0.2



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

NSE 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

October, 2021
FortiSOAR 7.0.2 Sizing Guide
00-400-000000-20210112

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-10-21	Initial release of 7.0.2

FortiSOAR Sizing Calculator

The sizing calculator utility associated with this document helps you define your sizing requirements for FortiSOAR. This document explains how to use the sizing calculator and defines parameters such as ingestion rate, number of workflows run per day, workflow and audit purging policies, etc, required to be added in the utility. The sizing calculator utility uses specified parameter values and outputs a recommended configuration for your FortiSOAR instance.

You can download the sizing calculator from: https://help.fortinet.com/fortisoar/sizing_calculator.xlsx.

Inputs for the sizing calculator

You need to specify the following details in the sizing calculator to calculate your FortiSOAR configuration:

1. Average number of alerts/day
2. Average number of playbooks run/day
3. Playbook logs retention policy in weeks (recommended 52 weeks)
4. Audit logs retention policy in weeks (recommended 52 weeks)

Other defaults in the sizing calculator

Following additional default details need to be specified You need to specify the following details in the sizing calculator to calculate your FortiSOAR configuration:

1. **Disk size computation**:
   a. **Primary Data**: For **every alert**, the calculator considers **0.5 MB** of primary data to be generated. This is an approximate number considering:
      i. 8 indicators extracted
      ii. 10 comments added, including one attached file of approximately 500 KB.
      Note: If your investigation relies on heavier attachments or screenshots, or primarily relies on email ingestion with large images, you might consider doubling the disk size projections. Refer to the "Test Run" section which considers an - additional large attachment approximately ~500KB in size that is uploaded as a comment, such that ~1 MB of primary data gets generated in the environment for every alert ingested
   b. **Audit Logs**: The calculator considers around **7 GB** of audit data to be generated weekly.
   c. **Workflow Logs**: The calculator considers log size of **5KB** generated **per playbook**.
   You can run the following command on your FortiSOAR instance (6.4.3 and above) to confirm the database consumptions for your current data and change the inputs to your sizing calculator accordingly:
   `csadm db -getsize`

The above command gives the total database sizes. Size per playbook log could be obtained by dividing the total 'Workflow Logs' size from the above output by the total 'Executed Playbook Logs' in the UI. To get the size per alert/incident, divide the total 'Primary Data' size by total number of alerts in the UI.

2. CPU and Memory based on playbooks run/day used by the Calculator:

Playbooks run/day	Configuration
Up to 10,000	16GB RAM, 4 core CPU
10,000 – 50,000	32GB RAM, 8 core CPU
50,000 – 150,000	64GB RAM, 16 core CPU
150,000 – 250,000	Active/Active HA cluster with 32GB RAM 8 core CPU

These sizes are recommended keeping in mind long term sustenance and average workflow execution times of 15 seconds/workflow. Your environment might also have higher or lower scale limits based on the workflows runs.

Playbook runs involve frequent disk I/O. Having SSD disks with a higher guaranteed IOPS (2000 or higher) are strongly recommended in the production environment for the best performance.

Test Run

Refer to the following sections to further understand the sizing calculation logic with the help of results from a sustenance run. The tests were run on the default recommended hardware configurations and using a common daily ingestion volume seen in customer environments. It shows details of the system utilization over the period of the run. The test results can be used as a reference for deciding on the CPU, memory and disk for your FortiSOAR instance.

Test Configuration 1

For each of these tests the load varies in terms of the number of alerts ingested per day. The following parameters are common for each of the runs:

Instance Configuration:

- 32GB RAM, 8 cores, 2400 IOPS

Load:

- ~5040 alerts/day (2 schedules are run: one creates 1 alerts every minute, and the second creates bursts of 150 alerts every hour)

Default use-cases run per alert (7):

- SLA Calculation (All applicable SLA Playbooks)
- Alert Assignment Notification
- Indicator Extraction
- Enrichment

- Triage
- User Assignment
- Computing Alert Priority

Record sizes:

- 8 Indicators are created per alert
- Each alert has 10 small text comment, 2 comments with a screenshot and a large 500 MB File Attachment as a comment. Around 1 MB or primary data gets generated per alert ingested.
- Sample alert data: You can download this sample alert data from: https://help.fortinet.com/fortisoar/Sizing_Alert.zip.

Audit log and Work log retention

- Audit log retention: 7 days
- Workflow log retention: 7 days

Other FortiSOAR Tunables

Following configurations were updated as recommended for the production instance:

- Workflow workers: 16
  `/etc/celery/celeryd.conf: CELERYD_OPTS="--concurrency=16"`
- Postgres shared buffer: 2GB
  `/var/lib/pgsql/12/data/postgresql.conf: shared_buffers = 2048MB`
- ElasticSearch Xmx and Xmx 8GB:
  `/etc/elasticsearch/jvm.options:`
  `-Xms8g`
  `-Xmx8g`

Results

Data Disk Consumption:

1. Postgres partition consumption: `/var/lib/pgsql`
2. Elasticsearch disk consumption: `/var/lib/elasticsearch`

Time Span	Primary Data Size	Audit Logs Size	Workflow Logs Size	Elasticsearch Size	Total Disk Size
After 1 week	29GB	7.08GB	7.35GB	7GB	50.43GB
After 2 weeks	62GB	15.17GB	15.75GB	15GB	107.92GB
After 4 weeks	125GB	30.34GB	31.5GB	30GB	216.84GB
After 1 year (projected)	1512GB	369.17GB	383.25GB	365GB	2629GB

Note: Total Disk Consumption is calculated as Primary Data size + Audit log size + Workflow logs size + Elasticsearch size.

Test Configuration 2

The configuration for this test is the same as Test Configuration 1, apart from the record sizes of the alert ingested.

Record sizes:

- 8 Indicators are created per alert
- Each alert has 10 small text comment, 2 comments with a screenshot. Around 0.5 MB or primary data gets generated per alert ingested.
- Sample alert data: You can download this sample alert data from: https://help.fortinet.com/fortisoar/Sizing_Alet_Without_Attachment.zip.

Results

Data Disk Consumption:

Time Span	Primary Data Size	Audit Logs Size	Workflow Logs Size	Elasticsearch Size	Total Disk Size
After 1 week	7.77GB	7.49GB	52.5GB	6.50GB	74.26GB
After 2 weeks	15.54GB	14.98GB	52.5GB	14.60GB	97.62GB
After 4 weeks	31.08GB	14.98GB	52.5GB	29.20GB	127.76GB
After 1 year (projected)	405.15GB	14.98GB	52.5GB	403.10GB	875.73GB

Note: Total Disk Consumption is calculated as Primary Data size + Audit log size + Workflow logs size + Elasticsearch size.

Test Configuration 3

Apart from the instance configuration and load, all the other configuration for this test is the same as Test Configuration 1.

Instance Configuration:

- 32GB RAM, 8 cores, 2400 IOPS
- Two Node Active/Active HA

Load:

- ~9360 alerts/day (2 schedules are run: one creates 4 alerts every minute, and the second creates bursts of 150 alerts every hour)

Results

Data Disk Consumption:

Time Span	Primary Data Size	Audit Logs Size	Workflow Logs Size	Elasticsearch Size	Total Disk Size
After 1 week	47GB	11GB	16GB	7GB	81GB
After 2 weeks	101GB	23.57GB	34.28GB	15GB	173.85GB
After 4 weeks	201.42GB	47.14GB	68.57GB	30GB	347.13GB
After 1 year (projected)	2450GB	573.57GB	834.28GB	365GB	4222.85GB

Note: Total Disk Consumption is calculated as Primary Data size + Audit log size + Workflow logs size + Elasticsearch size.

www.fortinet.com