FortiAnalyzer - Best Practices

Version 6.0

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/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

July 02, 2019
FortiAnalyzer 6.0 Best Practices
05-000-424272-20190702

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-07-24	Initial release.
2017-10-05	Updated sections: • Replace managed device. • ADOM Design. • Installation: use a dedicated Super_User account on the FortiGate for FortiAnalyzer access.
2017-11-22	Updated sections: • Back up the configuration: compare checksum to verify backup. • Installation: the dedicated Super_User account on the FortiGate only needs *Read Only* access to *System Configuration*.
2018-10-10	Updated sections: • Moved the information about the dedicated Super_User account to its own *General Maintenance > Add managed device* section. • Added recommendation to use High Availability (HA) for FortiAnalyzer 6.0.0 and higher in *Business Continuity* section.
2019-05-29	Added information about decommissioning FortiAnalyzer.
2019-07-02	Updated information in Set disk size and RAID level on page 11.

Overview

This guide is a collection of best practices guidelines for using FortiAnalyzer. Use these best practices to help you get the most out of your FortiAnalyzer products, maximize performance, and avoid potential problems.

Additional information

For product and feature guides, go to the Fortinet Document Library at https://docs.fortinet.com.

For procedures on how to implement these best practices, see the *FortiAnalyzer Administration Guide* in the Fortinet Document Library.

For customer service and support, go to https://support.fortinet.com.

For technical notes, how-to articles, FAQs, and links to the technical forum and technical documentation, go to the Fortinet Knowledge Base at http://kb.fortinet.com/kb.

Installation

Plan your installation carefully and select the FortiAnalyzer model(s) that meet your requirements.

- Plan the size of your installation appropriately. Ensure you plan for future management and logging requirements, including consideration for:
  - The number of connected devices.
  - If applicable, log rates and analytic and archive retention periods.
- Ensure you have remote serial console or virtual console access.
- Ensure a local TFTP server is available on a network local to the FortiAnalyzer.

Business Continuity

- Set up and use High Availability (HA). HA is available in FortiAnalyzer 6.0.0 and higher.
- Ensure there is no power interruption. A power loss could cause the loss of a FortiAnalyzer device's database integrity. See Maintain database integrity on page 8.
  - Always shut down or reboot the FortiAnalyzer gracefully. Removing power without a graceful shutdown might damage FortiAnalyzer databases.
  - Ensure the FortiAnalyzer environment has a stable and uninterruptible power supply.
- If an unexpected power loss occurs, revert to a known good backup of the configuration.
- Ensure there are spare parts on site, such as fans, power supplies, and hard disk drives.

General Maintenance

Perform general maintenance tasks such as backup and restore so you can revert to a previous configuration if necessary.

Back up the configuration

- Perform regular backups to ensure you have a recent copy of your FortiAnalyzer configuration.
- Verify the backup by comparing the checksum in the log entry with that of the backed up file.
- Set up a backup schedule so you always have a recent backup of the configuration. See the *FortiAnalyzer CLI Reference*.
- If your FortiAnalyzer is a virtual machine, you can also use VM snapshots.

If you use ADOMs, a large number of ADOMs can significantly increase the size of configuration files which increases backup and restore time. See ADOM considerations on page 10.

Schedule maintenance tasks for off-peak hours

Fortinet recommends scheduling maintenance tasks for off-peak hours whenever possible, including tasks such as:

- Configuration backup.
- Log deletion.
- Log rolling and related log upload.
- For FortiAnalyzer devices in Collector mode, log aggregation. Schedule this task after daily log rolling so that analyzer has the latest rolled logs for that day.

Maintain database integrity

To maintain database integrity, never power off a FortiAnalyzer unit without a graceful shutdown. Removing power without a proper shutdown can damage FortiAnalyzer databases.

Always use the following CLI command to shutdown the device before removing power:

```
execute shutdown
```

Fortinet highly recommends connecting FortiAnalyzer units to an uninterruptible power supply (UPS) to prevent unexpected power issues that might damage internal databases.

Replace managed device

When you need to replace a standalone FortiGate device or a cluster member, the best practice is to add the new device as a new member so as to preserve existing logs. Consider adding the old and new FortiGate devices into a group for reporting purposes.

For information on replacing FortiGate units in a high-availability pair, see the cookbook recipe Replacing FortiGate HA Pairs with Logging Enabled.

Add managed device

When Security Fabric is enabled on FortiGate, FortiAnalyzer requires using an administrator account on the FortiGate to query the FortiGate for Security Fabric-related information.

Fortinet recommends using a dedicated Super_User administrator account on the FortiGate for FortiAnalyzer access. This ensures that associated log messages are identified as originating from FortiAnalyzer activity. This dedicated Super_User administrator account only needs *Read Only* access to *System Configuration*; all other access can be set to *None*.

Replace the FortiAnalyzer device

When you need to move logs to a new FortiAnalyzer device, use one of the following methods:

- Use log forwarding in aggregation mode. See *Log Forwarding* in the *FortiAnalyzer Administration Guide*.
- Use log fetching (Fetcher Management). See *Fetcher Management* in the *FortiAnalyzer Administration Guide*.

ADOM Design

Enable ADOMs to support logs other than FortiGate logs (including Syslog and FortiClient EMS). You do not need to separate ADOMs by FortiOS versions.

In version 5.4.x, the following applies to version 5.4.4 and higher. In version 5.6.x, it applies to version 5.6.1 and higher:

When creating, editing, or viewing ADOMs, the version is displayed only if FortiManager features are enabled.

If your devices have a mix of high-volume and low-volume log rates, put high-volume log rate devices in one ADOM and low-volume log rate devices in another ADOM. This helps prevent quota enforcement from adversely affecting the low-volume log devices. For best practices about setting quotas for ADOMs, see Allocate quota and set log retention policy on page 12.

For more information, see the *FortiAnalyzer Administration Guide*.

ADOM considerations

A large number of ADOMs can significantly increase the size of configuration files which increases backup and restore time. Do not create more ADOMs than your business needs.

Log Management

Set up a log management strategy that gives a good balance of redundancy and performance. Retain logs log enough for business requirements and archive older logs for better performance.

Set up a log backup strategy

- Set up a backup strategy for logs.
- Set up a schedule to roll and upload logs. You can use the GUI or CLI to set this up. For details, see the *System Settings* > *Device logs* section in the *FortiAnalyzer Administration Guide*.
  - You can also back up logs using the `execute backup logs` command. For details, see the *FortiAnalyzer CLI Reference*.

Set up redundancy

- For log storage redundancy, you can set this up at the disk level by selecting an appropriate RAID level.
- For log delivery redundancy, you can set this up in the following ways:
  - Set FortiGates to send logs to multiple devices, provided the FortiGate models support this function.
  - Use a hierarchical approach in your network design which includes using FortiAnalyzer devices in Collector mode and one or more FortiAnalyzer devices in Analyzer mode.

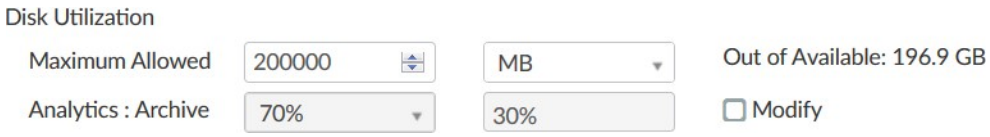
Set disk size and RAID level

Fortinet recommends using the default RAID level specified in the FortiAnalyzer data sheet, that is, RAID 50. If your configuration does not meet RAID 50 requirements, consider upgrading your hardware.

When planning for disk space requirements, consider future storage needs. Adding disks to an existing RAID array requires rebuilding the RAID array and restoring backed up logs.

The disk space available for you to set log quotas depends on the RAID level and the reserved space for temporary files. Temporary files are needed for indexing, reporting, and file management. In your planning, include both the disk space for the original logs FortiAnalyzer receives (Archive) and the space required to index the logs (Analytics).

Fortinet recommends using the default ratio of *Analytics : Archive* for most deployments. If you plan to retain archive logs for a much longer period than your analytical data, you might allocate a higher percentage to Archive.



If you need more disk space for a VM, you can add a virtual disk.

In FortiAnalyzer 6.0.3 and later, you can also increase the size of an existing virtual disk. No format is required.

Use the `execute lvm extend` command to add or expand virtual disks. See the *FortiAnalyzer CLI Reference*.

Set log retention and storage

Determine the logs needed to meet business requirements

Consider carefully which types of logs to store on FortiAnalyzer. In some cases, you can be more selective about the type and volume of logs sent from FortiGate to FortiAnalyzer. Reducing the type and volume of logs gives FortiAnalyzer more resources to process the logs that meet your log storage, forensic, and reporting needs.

Allocate quota and set log retention policy

Ensure your quota settings is sufficient to fulfill your log retention policy. You must keep enough log data to meet your organization's reporting requirements. Configure quota settings and the log retention policy to ensure there is enough time to generate all scheduled reports.

Log View > *Storage Statistics* shows graphs with trends to help you with this planning.

If you are using ADOMs, ensure the quota is sufficient for every ADOM. Allocating insufficient quota to an ADOM might cause the following issues:

- Prevent you from meeting your log retention objective.
- Waste CPU resources enforcing quotas with log deletion and database trims.
- Adversely affect reporting when quota enforcement acts on analytical data before a report is complete.

For analytics, ensure the quota is sufficient and the retention period is long enough to complete all scheduled reports. When reports are generated and the log retention period is past, there is no need to keep analytical data since it can be regenerated from the original archived log data.

Use Fetcher Management for log fetching

To generate a report for a time period not covered by current analytical data:

- Use log fetching (*Fetcher Management*) to fetch archived logs to generate reports.
- Import log data from an external backup to generate reports.

Log fetching simplifies generating reports from log data for the following reasons:

- Log fetching allows you to specify the devices and time periods to be indexed.
- You can pull indexed logs into an ADOM with quota and log retention settings specifically set up to generate report on older logs.
- Log fetching helps to avoid duplications that might occur with importing data from an external backup.

For information on *Fetcher Management* (log fetching) and importing a log file, see the *FortiAnalyzer Administration Guide*.

Rebuild SQL database

Some firmware upgrades might change the SQL schema that indexes logs (analytics). If so, FortiAnalyzer automatically rebuilds the SQL database. During the rebuild, searching and reporting functions are limited.

You rarely need to manually rebuild an SQL database. If you think there might be problems with the SQL database, contact Customer Service & Support before considering a manual rebuild.

You might consider rebuilding the SQL database in the following situations:

- After moving a device to a new ADOM, you might need to rebuild the SQL database in the new ADOM.
- If disk space is running low, you might rebuild the SQL database to try free up disk space.

Report Performance

For reports that you run regularly, set up the following:

- Put those reports into a group.
- Schedule those reports. If possible, schedule reports to run at off-peak hours and do not schedule reports to run at the same time as log maintenance tasks.
- Enable auto-cache for those reports.

Grouping reports has these advantages:

- Reduce the number of *hcache* tables.
- Improve *auto-cache* completion time.
- Improve report performance and reduce report completion time.

Consider grouping reports in these conditions:

- If you use the same or a similar report template for different FortiGates in the same ADOM.
- If you regularly use different filters on your reports.

Other ways to improve report performance include:

- Avoid running reports at the same time as log aggregation or log transfer.
- Avoid queries to external sources such as DNS (for name resolution) or LDAP (for obtaining a user list).

For more information, see the *FortiAnalyzer Administration Guide* and the *FortiAnalyzer Report Performance Troubleshooting Guide*.

Security Best Practices

For stronger security, implement the following security best practices.

Administrator access best practices

- Enable password policy and set requirements for the administrator password. The password policy lets you specify the administrator's password minimum length, type of characters it must contain, and the number of days to password expiry.
- Use CLI commands to configure the administrator's password lockout and retry attempts.
  For example, to set the lockout duration to two attempts and set a two minute duration before the administrator can log in again, enter the following CLI commands:

```
config system global
   set admin-lockout-threshold 2
   set admin-lockout-duration 120
end
```

- Set a lower idle timeout so that unattended workstations are logged out.
- Use two-factor authentication and RADIUS authentication for administrators. For more information, see the *Two-Factor Authenticator Interoperability Guide* and *FortiAuthenticator Administration Guide* in the Fortinet Document Library.
- Limit administrator access. For example, configure trusted hosts and allowaccess.

Encryption best practices

Set a strong encryption level. Use the SSL protocol version (TLS version) that meets PCI compliance or your organization's security requirements. For example:

```
config system global
   set fgfm-ssl-protocol tlsv1.2
   set oftp-ssl-protocol tlsv1.2
   set ssl-protocol tlsv1.2
   set webservice-proto tlsv1.2
   set ssl-low-encryption disable
end

config fmupdate fds-setting
   set fds-ssl-protocol tlsv1.2
end
```

For more information, see the applicable knowledge base article: Setting SSL Protocol Version on FortiManager and Setting SSL Protocol Version on FortiAnalyzer.

Other security best practices

- Disable unused interfaces.
- Upgrade firmware to the latest version.
- Install physical devices in a restricted area.
- Set up NTP. For example:

```
config system ntp
   set status enable
   set sync_interval 60
   config ntpserver
      edit 1
         set server {<address_ipv4> | <fqdn_str>}
      end
   end
end
```

- For audit purposes:
  - Use named accounts wherever possible.
  - Send logs to a central log destination.

Do not lose the administrator log in information as there is no password recovery mechanism in FortiAnalyzer 5.4.0 and later.

VM Size and License

When using VMs, implement the following:

- Allocate sufficient CPU and memory resources to all VMs.
- Ensure the VM license meets your requirements for daily log rate (GB/day) and log storage capacity.

For details, see the *FortiAnalyzer VM Install Guide*.