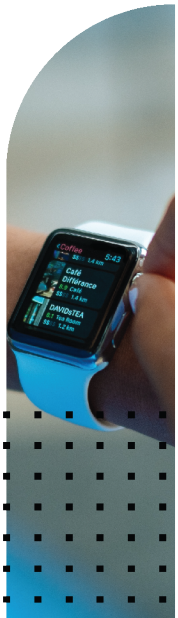
Deployment Guide

FortiAnalyzer Federation 7.0.0



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://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

April 22, 2021
FortiAnalyzer Federation 7.0.0 Deployment Guide
05-700-711439-20210422

TABLE OF CONTENTS

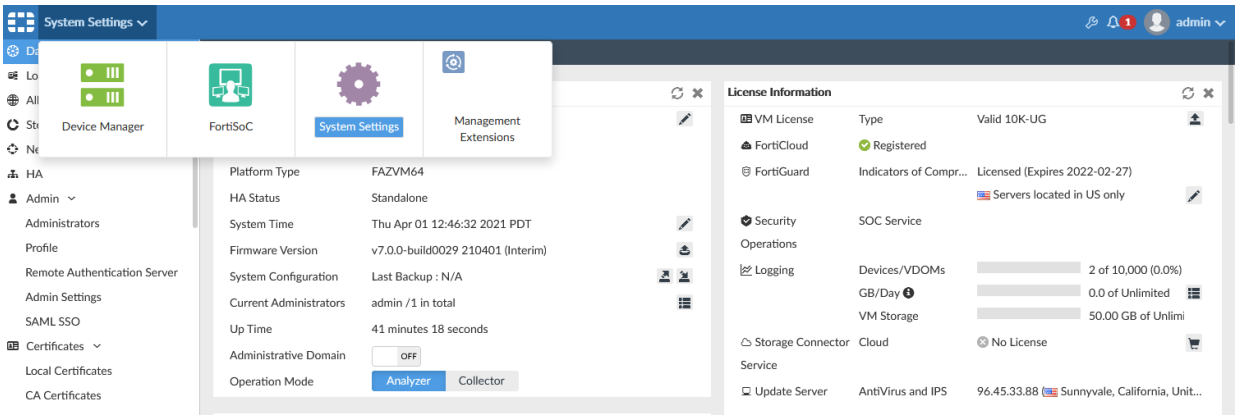
Change Log

Date	Change Description
2021-06-22	Initial release.

Introduction

The FortiAnalyzer Federation enables centralized viewing of devices, incidents, and events across multiple FortiAnalyzers acting as members. In this mode, FortiAnalyzer Federation members form a Fabric with one device operating in supervisor mode as the root device. Incident and event information is synced from members to the supervisor using the API.

The FortiAnalyzer Federation device operating as the supervisor includes the following modules:



Device Manager	Displays FortiAnalyzer Federation members with their ADOMs and authorized logging devices.
FortiSoC	Displays the *Event Monitor* and *Incidents* panes. Administrators can view incidents and events created on member FortiAnalyzer Federation.
System Settings	Configure the settings for the FortiAnalyzer supervisor. See the FortiAnalyzer Administration Guide.
Management Extensions	Enables supported management extension applications. See the FortiAnalyzer Administration Guide.

For information on the modules available as a FortiAnalyzer Federation member, see the FortiAnalyzer Federation Administration Guide.

FortiAnalyzer Federation roles

FortiAnalyzer Federation includes two operation modes, including supervisor and member.

- Supervisors acts as the root device in the FortiAnalyzer Federation. SOC administrators can use the supervisor to view member devices and their ADOMs and authorized logging devices, as well as incidents and events created on members.
- Members are devices in the FortiAnalyzer Federation that send information to the supervisor for centralized viewing. When configured as a member, FortiAnalyzer devices continue to have access to the

FortiAnalyzer features identified in the FortiAnalyzer Administration Guide. Incidents and events are created or raised from each member.

Deployment

This section includes the following topics:

Configuring the FortiAnalyzer Federation

To configure a FortiAnalyzer Federation, you must configure a supervisor, one or more members, and enable soc-fabric communication on the interfaces being used.

All FortiAnalyzer Federation members must be configured with the same timezone settings as the supervisor.

Configuring a supervisor

To configure a supervisor:

1. In the FortiAnalyzer Federation supervisor CLI, enter the following commands to enable soc-fabric communication:
```
config system interface
  edit <interface used for soc-fabric communication>
    set allowaccess soc-fabric (enable other types of interface access as
        needed, for example https)
```
2. Enter the following commands to configure the supervisor:
```
config system soc-fabric
  set status enable
  set role supervisor
  set name <create the FortiAnalyzer Federation name>
  set psk <create the FortiAnalyzer Federation password>
  set port 6443 <set the communication port if not using the default one>
  set secure-connection {enable | disable}
  next
end
```

Configuring a member

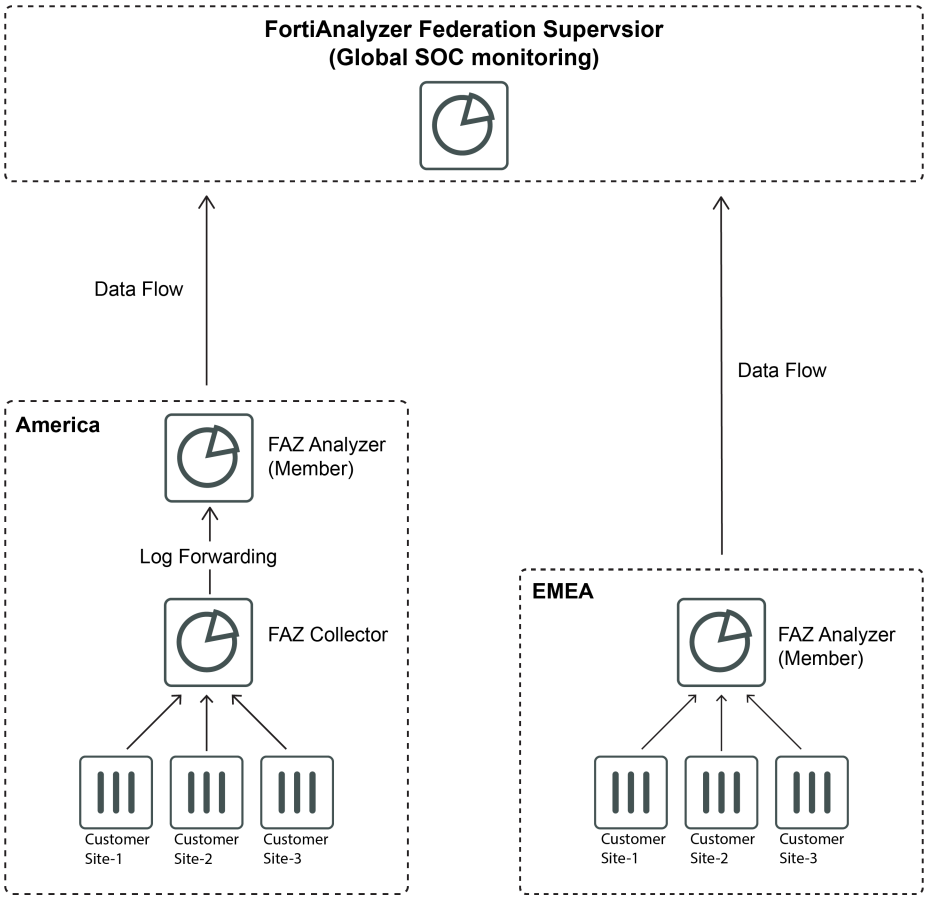
FortiAnalyzer Federation allows multiple FortiAnalyzers to act as fabric members. Each FortiAnalyzer in Analyzer mode must be individually configured as a member to participate in the FortiAnalyzer Federation.

To configure a member:

1. In the FortiAnalyzer Federation member CLI, enter the following commands to enable soc-fabric communication:
```
config system interface
   edit <interface used for soc-fabric communication>
      set allowaccess soc-fabric (enable other types of interface access as
           needed, for example https)
```
2. Enter the following commands to configure the member:
```
config system soc-fabric
   set status enable
   set role member
   set name <enter the FortiAnalyzer Federation Name>
   set psk <enter the FortiAnalyzer Federation auth password>
   set supervisor <enter the IP/FNDN of the supervisor>
   set port 6443 <set the communication port if not using the default one>
   set secure-connection {enable | disable}
   next
end
```

Deployment architecture

The following is an example of the topology that can make up the FortiAnalyzer Federation, with the supervisor acting as the root device, and multiple FortiAnalyzer Federation members sending information to the supervisor through the API. Information can be sent from a FortiAnalyzer operating as a Collector to an Analyzer before being synced to the supervisor. The FortiAnalyzer Federation is ideal for use in high volume environments with many FortiAnalyzers.



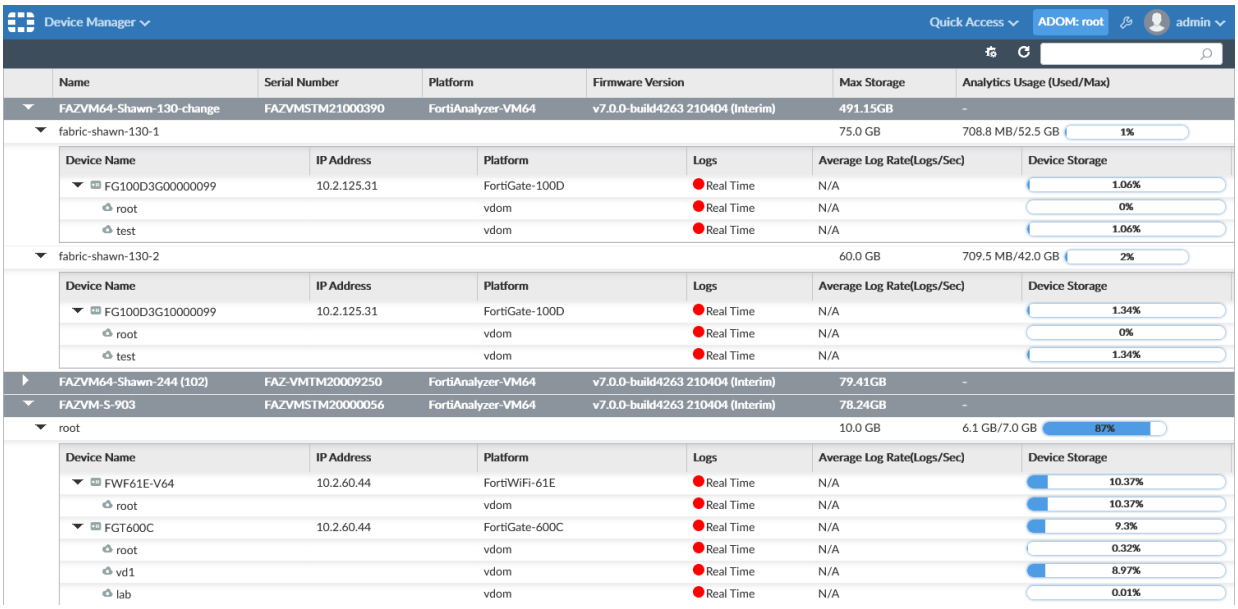
Using the FortiAnalyzer Federation supervisor

The FortiAnalyzer Federation supervisor includes the following features:

Device Manager

In the FortiAnalyzer Federation supervisor, the *Device Manager* is used to collect and display information from members. You can expand each member to view its ADOMs and authorized logging devices. The *Device Manager* displays information about device storage, logging rates, and the current real time log status of devices.

Device filtering can be performed by searching for device information using the search field. For example, you can search "FortiGate" to view all FortiGate devices, or "100D" to view only FortiGate 100D models.



Device Manager includes the following information for each FortiAnalyzer Federation member:

Name	The name of the FortiAnalyzer Federation member.
Serial Number	The device's serial number.
Platform	The device's platform.
Firmware Version	The device's firmware version.
Max Storage	The total maximum storage.

Analytics Usage (Used/Max)	The analytics for log storage usage, displaying the total amount used against the maximum available.

FortiAnalyzer Federation member ADOMs are displayed below each member. Each ADOM includes their authorized logging devices. The following information is displayed for each device and VDOM:

Device Name	The name of the device.
IP Address	The IP address of the device.
Platform	The platform of the device.
Logs	The real time log status. A green circle indicates that logs are being sent. A red circle indicates that logs are not being sent. The status indicator will turn from green to red when logs have not been sent for 15 minute or longer.
Average Log Rate (Logs/Sec)	The average log rate per second. This information is only available when the device is sending logs in real time.
Device Storage	The amount of storage used by the device or VDOM.

Event Monitor

On the FortiAnalyzer Federation supervisor, the event monitor includes *All Events* and *Supervisor Local Events panes*.

- All Events on page 11
- Supervisor Local Events on page 12

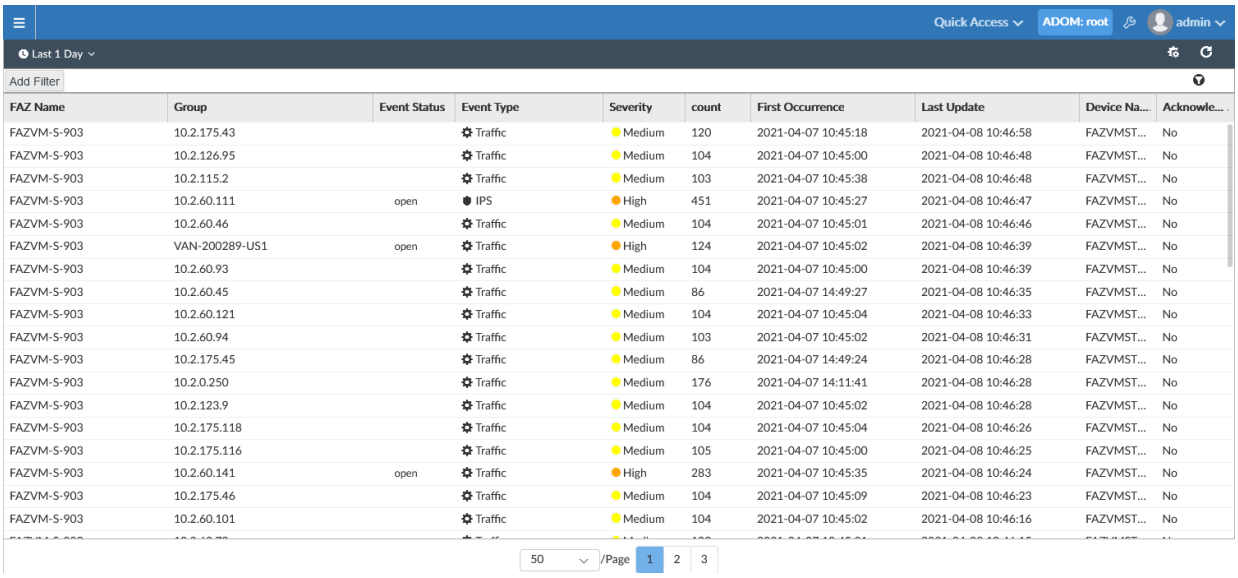
All Events

The *All Events* pane displays events created on each FortiAnalyzer Federation member.

Event handlers must be configured on members for events to be viewable on the supervisor.

On the supervisor, events are organized into pages. You can configure the number of events that are displayed per page and navigate between the pages by using the page navigation buttons at the bottom of the pane.

Apply filters by clicking *Add Filter* or by right-clicking within a column in the events table and selecting your search parameters.



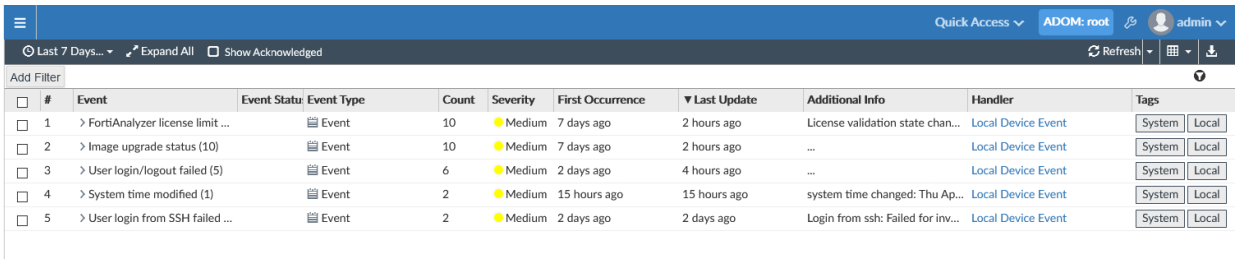
Double-click an event line to view the event group details. Event group details displays events from members in the FortiAnalyzer Federation. The member name and ADOM is displayed in the table.

To view log details, select an event in the event group and click *View Log*. You can drilldown further on each result to view event details.

Click *Search in Log View* to perform a log view search using the selected event.

Supervisor Local Events

Supervisor Local Events shows local events from the FortiAnalyzer acting as supervisor in the FortiAnalyzer Federation. Local events include events such as license validation, system time changes, reboots, and other events that have occurred on the supervisor in the FortiAnalyzer Federation.

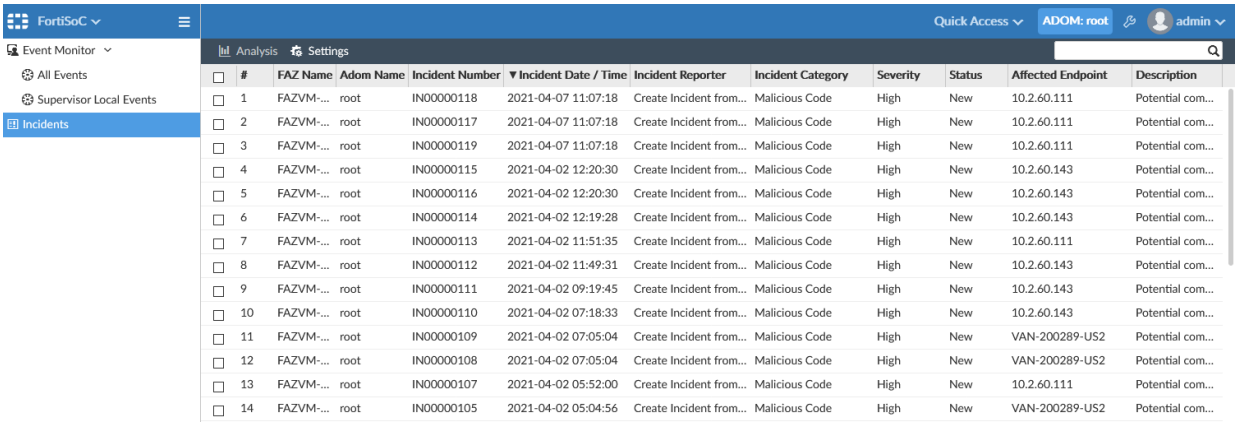


Incidents

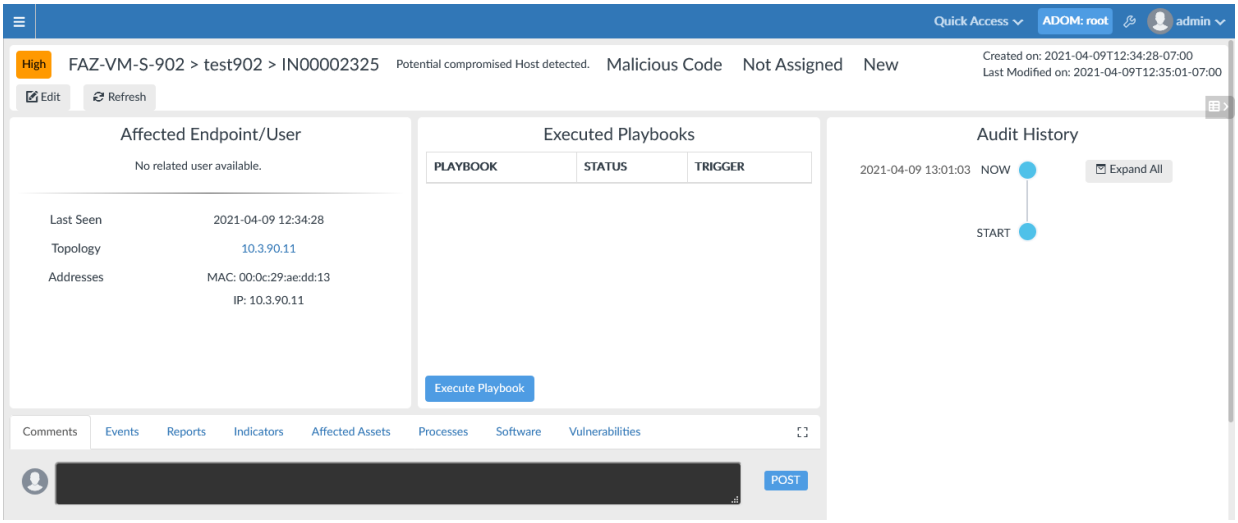
On the supervisor, *Incidents* displays all incidents created on FortiAnalyzer Federation members.

Incidents contain event details, as well as information helpful for administrator analysis. From the incident's analysis page, administrators can view incidents, audit history, and attached reports, events, and comments.

Incident information syncs from members to the supervisor. New incidents can only be raised on FortiAnalyzer Federation members.



Double-click on an incident to view the incident analysis page. The incident analysis page indicates the FortiAnalyzer and ADOM that the incident was created on. For more information on the options available to SOC analysts, see the FortiAnalyzer Administration Guide.



Appendix A - FortiAnalyzer Federation limitations

FortiAnalyzer Federation includes the following limitations in 7.0.0:

- FortiAnalyzer Federation supports the creation of incidents, event handlers, and events on members with centralizing viewing from the supervisor.
- FortiAnalyzer Federation supports log analysis, including *LogView* and *Reports*, on FortiAnalyzer Federation members.
- Incidents on the FortiAnalyzer Federation supervisor are available in read-only mode.
- FortiAnalyzers configured in high availability (HA) mode can join the FortiAnalyzer Federation as members. HA is not supported for FortiAnalyzer Federation supervisors.

Appendix B - Troubleshooting

Confirming a member has joined the Fabric

When adding a new member, check that the member has joined the Fabric.

To confirm that a member has joined the Fabric:

1. In the FortiAnalyzer Federation supervisor CLI, enter the following command:

```
diagnose test application fazsvcd 36 nodes
FAZ-S-901 # diagnose test application fazsvcd 36 nodes
Supervisor:
3632041446 (Self)
   Status: up
Members:
209855595
   Status : up
   Node Ping Time : 19 Apr 2021 18:41:22 (1618882882)
   Last Ping Time : 19 Apr 2021 18:41:34 (1618882894)
   Fabric Serial Number : FAZVMSTM21000123
   Platform : v7.0.0-build0037 210411 (Interim)
   Platform Type : FAZVM64
   Platform Full Name : FortiAnalyzer-VM64
   Version : v7.0.0-build0037 210411 (Interim)
   Serial Number : FAZVMSTM21000123
   Hostname : FAZVM64-Shawn-130-change
   FIPS Mode : Disabled
   HA Mode : Stand Alone
   Branch Point : 0037
   Release Version Information : Interim
   Current Time : Mon Apr 19 11:56:36 PDT 2021
   Daylight Time Saving : Yes
   Timezone : (GMT-8:00) Pacific Time (US & Canada).
   Disk Usage (free) : 442.98GB
   Disk Usage (total) : 491.15GB
   License Status : Valid
2024759224
   Status : up
   Node Ping Time : 19 Apr 2021 18:42:30 (1618882950)
   Last Ping Time : 19 Apr 2021 18:41:34 (1618882894)
   Fabric Serial Number : FAZVMSTM20000234
   Platform : v7.0.0-build0043 210416 (Interim)
   Platform Type : FAZVM64
   Platform Full Name : FortiAnalyzer-VM64
   Version : v7.0.0-build0043 210416 (Interim)
   Serial Number : FAZVMSTM20000234
   Hostname : FAZVM-S-903
   FIPS Mode : Disabled
   HA Mode : Stand Alone
   Branch Point : 0043
   Release Version Information : Interim
```

```
    Current Time : Mon Apr 19 11:57:50 PDT 2021
    Daylight Time Saving : Yes
    Timezone : (GMT-8:00) Pacific Time (US & Canada).
    Disk Usage (free) : 57.41GB
    Disk Usage (total) : 78.24GB
    License Status : Valid
  2462459651
    Status : up
    Node Ping Time : 19 Apr 2021 18:42:30 (1618882950)
    Last Ping Time : 19 Apr 2021 18:41:34 (1618882894)
    Fabric Serial Number : FAZVMSTM21000345
    Platform : v7.0.0-build0043 210416 (Interim)
    Platform Type : FAZVM64
    Platform Full Name : FortiAnalyzer-VM64
    Version : v7.0.0-build0043 210416 (Interim)
    Serial Number : FAZVMSTM21000345
    Hostname : FAZ-VM-S-902
    FIPS Mode : Disabled
    HA Mode : Stand Alone
    Branch Point : 0043
    Release Version Information : Interim
    Current Time : Mon Apr 19 11:59:24 PDT 2021
    Daylight Time Saving : Yes
    Timezone : (GMT-8:00) Pacific Time (US & Canada).
    Disk Usage (free) : 406.06GB
    Disk Usage (total) : 491.15GB
    License Status : Valid
```

This diagnostic shows all of the current members on the supervisor or on the member. Ensure that the status for each member is *up*.

Member unable to join the Fabric

If the member does not join the Fabric, possible issues include:

- Incorrect supervisor IP
- Incorrect PSK
- Encryption setting mismatch between supervisor/member
- Incorrect Fabric name
- The supervisor allowaccess setting described above does not include the soc-fabric setting
- The supervisor is not reachable by the member, use ping to confirm.
- The supervisor/member is not running.

The supervisor uses a mixture of synchronized data and data retrieved directly from the member. This data is retrieved through the Fabric from the JSONAPI service running on the member, so it is possible to view cached alert information while the member is not actually running.

Server error: Fabric member not available

Problem: When selecting an alert, the supervisor displays Server Error: Fabric member xxx is not available.

Description: The supervisor is not able to contact the member through the Fabric.

To troubleshoot a server error:

1. Ensure that the member has booted and is running.
2. Ensure that the member has connected to the Fabric using the following CLI command:
   ```
   diagnose test application fazsvcd 36 nodes
   ```

JSONAPI service reports error

Problem: When selecting an alert, the supervisor displays: JSONAPI Service reports: <error message>.

Description: The member has joined the Fabric, but the JSONAPI service of the member cannot service the request.

To troubleshoot a JSON API service reports error:

1. Ensure that the member has completely booted up.
2. Determine if the member is performing some type of database rebuild which may prevent service availability.
3. Access the members' GUI to determine if it can use its own JSONAPI service.
   More detailed connectivity information is available using the following diagnostics, which can be run on the supervisor and member:
   ```
   diagnose test application fazsvcd 56
   diagnose test application fazsvcd 53
   diagnose test application fazsvcd 36 members
   ```

www.fortinet.com