

**DO NOT REPRINT**  
**© FORTINET**



# FortiAnalyzer Study Guide

for FortiAnalyzer 7.0

# **DO NOT REPRINT**

## **© FORTINET**

### **Fortinet Training**

<https://training.fortinet.com>

### **Fortinet Document Library**

<https://docs.fortinet.com>

### **Fortinet Knowledge Base**

<https://kb.fortinet.com>

### **Fortinet Fuse User Community**

<https://fusecommunity.fortinet.com/home>

### **Fortinet Forums**

<https://forum.fortinet.com>

### **Fortinet Support**

<https://support.fortinet.com>

### **FortiGuard Labs**

<https://www.fortiguard.com>

### **Fortinet Network Security Expert Program (NSE)**

<https://training.fortinet.com/local/staticpage/view.php?page=certifications>

### **Fortinet | Pearson VUE**

<https://home.pearsonvue.com/fortinet>

### **Feedback**

Email: [askcourseware@fortinet.com](mailto:askcourseware@fortinet.com)



12/1/2021

## TABLE OF CONTENTS

<b>01 Introduction and Initial Configuration.....</b>	<b>4</b>
<b>02 Administration and Management.....</b>	<b>38</b>
<b>03 Device Registration and Communication.....</b>	<b>88</b>
<b>04 Logging.....</b>	<b>133</b>
<b>05 FortiSoC—Incidents and Events.....</b>	<b>183</b>
<b>06 FortiSoC—Playbooks.....</b>	<b>225</b>
<b>07 Reports.....</b>	<b>253</b>
<b>SQL and Datasets (supplementary material).....</b>	<b>312</b>

**DO NOT REPRINT****© FORTINET**

## FortiAnalyzer

### Introduction and Initial Configuration



FortiAnalyzer 7.0

Last Modified: 1 December 2021

In this lesson, you will learn about the key features and concepts of FortiAnalyzer, and how to initially configure FortiAnalyzer.

FortiAnalyzer integrates logging, analytics, and reporting into one system so you can quickly identify and react to network security threats.

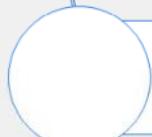
**DO NOT REPRINT**

**© FORTINET**

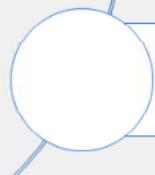
## Lesson Overview



**Key Features and Concepts**



**Initial Configuration**



**External Storage**

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will explore the topics shown on this slide.

**DO NOT REPRINT**  
**© FORTINET**

## Key Features and Concepts

### Objectives

- Describe the purpose of FortiAnalyzer
- Describe the purpose of administrative domains and when you might use them
- Describe the differences between FortiAnalyzer operating modes
- Identify where log data is stored

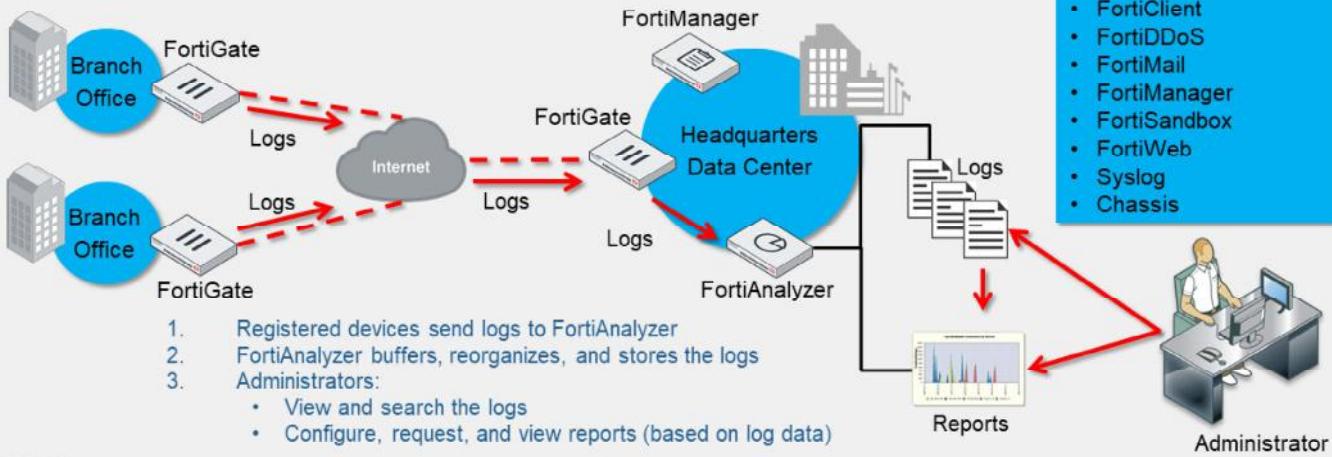
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiAnalyzer key features and concepts, you will be able to use the device effectively in your own network.

**DO NOT REPRINT**  
**© FORTINET**

## Centralized Log Repository

- Aggregates log data from one or more Fortinet devices
- Creates a single view of security events taking place on a range of devices



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

FortiAnalyzer aggregates log data from one or more Fortinet devices, thereby acting as a centralized log repository. Log aggregation provides a single channel for accessing your complete network data, so you don't need to access multiple devices several times a day.

The logging and reporting workflow operates as follows:

1. Registered devices send logs to FortiAnalyzer.
2. FortiAnalyzer collates and stores those logs in a way that makes it easy to search and run reports.
3. Administrators can connect to FortiAnalyzer using the GUI to view the logs manually, or generate reports to look at the data. You can also use the CLI to perform administrative tasks.

**DO NOT REPRINT****© FORTINET**

## Reports, Alerts, and Content Archiving

- **Reports**

- Network-wide reporting of events, activities, and trends occurring on supported devices
- Archived, filtered, and mined for compliance or historical analysis purposes

- **Alerts**

- Identify and react to network security threats quickly, when specific conditions in the logs (which you have configured) are met
- View alerts through **Event Monitor** (in the GUI), email, SNMP, or syslog

- **Content archiving**

- Simultaneously logs and archives full or summary copies of content transmitted over the network (email, FTP, NNTP, and web traffic)
- Typically used to prevent sensitive information from getting out of your network

Some key features of FortiAnalyzer include reporting, alert generation, and content archiving.

Reports provide a clear picture of network events, activities, and trends occurring on supported devices. FortiAnalyzer reports collate the information in the logs so that you can interpret the information and, if necessary, take the required actions. You can archive and filter the network knowledge you glean from these reports, as well as mine it for compliance or historical analysis purposes.

FortiAnalyzer alerts allow you to react quickly to threats, because it's not realistic to physically monitor your network around the clock. The system can generate alerts when specific conditions in the logs are met—conditions you have configured FortiAnalyzer to monitor for registered devices. You can see your alerts on the GUI, and you can also send them to multiple recipients by email, SNMP, or syslog.

Content archiving provides a way to simultaneously log and archive full or summary copies of the content transmitted over the network. You typically use content archiving to prevent sensitive information from getting out of your organization's network. You can also use it to record network use. The data loss prevention (DLP) engine can examine email, FTP, NNTP, and web traffic, but you must configure the archive setting for each rule in a DLP sensor on FortiGate, so you can specify what you want to archive.

**DO NOT REPRINT**  
**© FORTINET**

## Administrative Domains (ADOMs)

- ADOMs group devices for administrators to monitor and manage
  - One or more devices are assigned to ADOMs and administrators are assigned to administer one or more ADOMs
- Purpose:
  - To divide administration of devices and control (restrict) access
    - Virtual domain (VDOM), a feature of FortiGate, further restricts access
  - To more efficiently manage data policies and disk space allocation
    - Set for each ADOM (not for each device)

ADOMs are not enabled by default!

### System Settings > Dashboard

System Information	
Host Name	FortiAnalyzer
Serial Number	FAZ-VM0000065040
Platform Type	FAZVM64-KVM
HA Status	Standalone
System Time	Fri Oct 22 14:26:48 2021 PDT
Firmware Version	v7.0.2-build0180 211019 (GA)
System Configuration	Last Backup : Thu Oct 21 10:45:46 2021
Current Administrators	admin / 1 in total
Up Time	1 day 2 hours 57 minutes 54 seconds
Administrative Domain	<input checked="" type="checkbox"/>
Operation Mode	Analyzer <input type="radio"/> Collector <input type="radio"/>

```
#config system global
set adom-status {enable | disable}
end
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

ADOMs allow you to group devices to monitor and manage. For example, administrators can manage devices that are grouped based on their geographical location or business division.

The purpose of ADOMs is to:

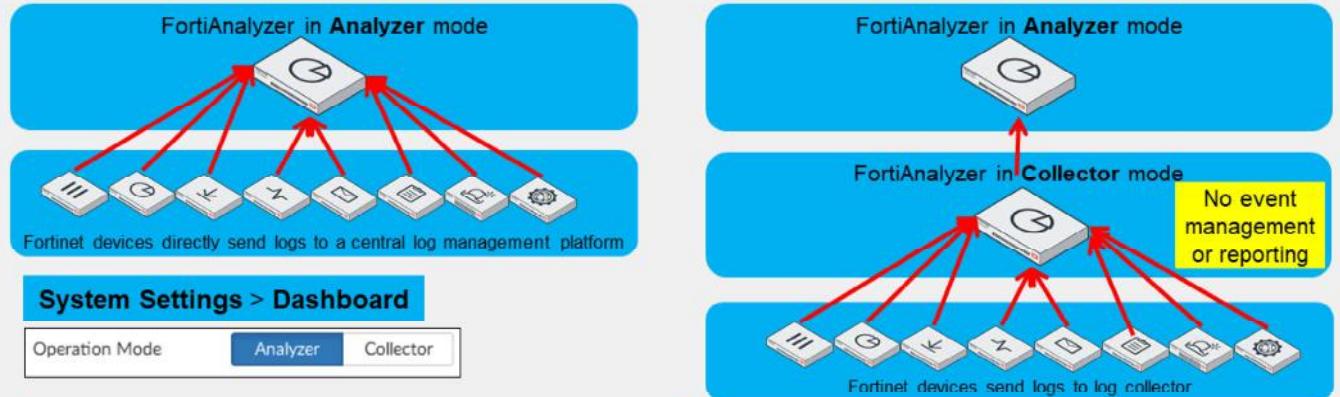
- Divide administration of devices by ADOM and to control (restrict) administrator access. If your network uses virtual domains (VDOMs), ADOMs can further restrict access to data that comes from the VDOM of a specific device.
- More efficiently manage data policies and disk space allocation, which are set per ADOM

ADOMs are not enabled by default and can be configured only by the default **admin** administrator (or an administrator who has the **super user** profile).

You will learn more about ADOMs later in this course.

**DO NOT REPRINT**  
**© FORTINET**

## FortiAnalyzer Operating Modes



- System Settings > Dashboard**
- |                |                 |           |
|----------------|-----------------|-----------|
| Operation Mode | <b>Analyzer</b> | Collector |
|----------------|-----------------|-----------|
- Central log aggregator for one or more logging devices or FortiAnalyzer in collector mode
    - Can still forward logs to another FortiAnalyzer (or syslog/CEF server)
  - Default mode

- Collects logs from multiple devices and forwards to FortiAnalyzer in analyzer mode
  - Can forward to syslog/CEF server in real-time forwarding mode only

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

7

FortiAnalyzer has two modes of operation: analyzer and collector. The mode of operation you choose depends on your network topology and individual requirements.

When operating in analyzer mode, the device acts as a central log aggregator for one or more log collectors, such as a FortiAnalyzer device operating in collector mode, or any other supported device sending logs. Analyzer is the default operating mode.

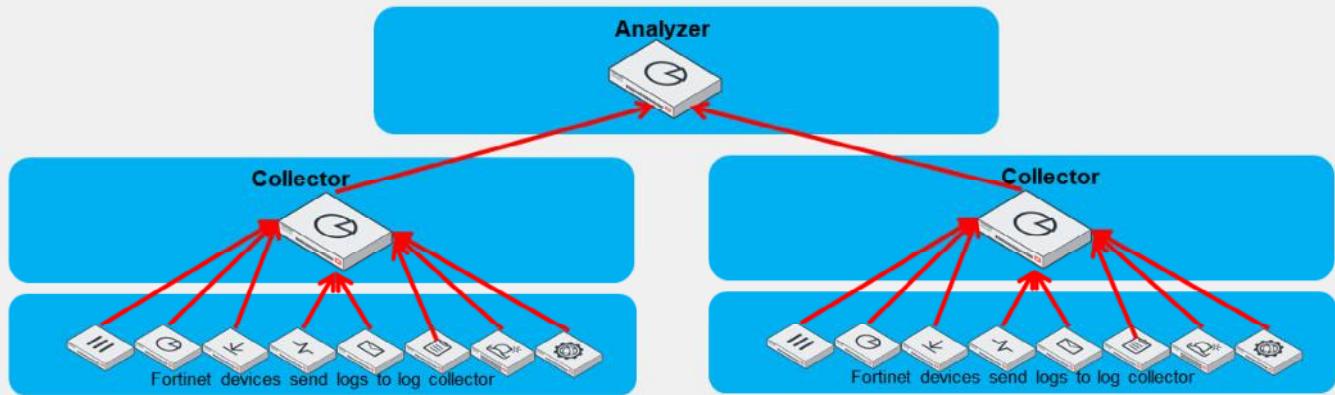
When operating in collector mode, the device collects logs from multiple devices and then forwards those logs, in their original binary format, to another device, such as a FortiAnalyzer operating in analyzer mode. It can also send them to a syslog server or a common event format (CEF) server, depending on the forwarding mode. A collector does not have the same feature-rich options as an analyzer, because its only purpose is to collect and forward logs. It does not allow event management or reporting.

You can change the operating mode in the **System Information** widget on the dashboard.

Note that FortiAnalyzer can also be part of a FortiAnalyzer Federation, but that is outside of the scope of this course. For more details see the *FortiAnalyzer Federation Deployment Guide* in the Fortinet Documentation Library.

**DO NOT REPRINT**  
**© FORTINET**

## Analyzer—Collector Collaboration



- Increase FortiAnalyzer performance by using analyzer and collector modes
- Analyzer offloads the log receiving task to the collector so it can focus on data analysis and reporting
- Collector log receiving rate is maximized
- Collector can help with slow or unreliable links by storing logs and forwarding them on schedule
- For the collector, you should allocate most of the disk space for archive logs

By using both analyzer and collector modes, you increase FortiAnalyzer performance: Collectors offload the task of receiving logs from multiple devices from the analyzer. This allows the analyzer to focus on data analysis and reporting tasks.

Furthermore, because a collector is strictly dedicated to log collection, its log receiving rate and speed are maximized. If bandwidth is an issue, like in the case of slow WAN links, you can use the store and upload option to send logs only during low-bandwidth periods.

Since the collector does not perform any analytics tasks, it should have most of the disk space allocated for archive logs.

**DO NOT REPRINT**  
© FORTINET

## Database Language Support

- FortiAnalyzer supports Structured Query Language (SQL) for logging and reporting
- FortiAnalyzer inserts log data into the SQL database for log view and report generation
- FortiAnalyzer uses a PostgreSQL database
- *Advanced reporting capabilities require some knowledge of SQL and databases*



SQL is the database language that FortiAnalyzer uses for logging and reporting.

Advanced reporting capabilities require some knowledge of SQL and databases. For example, you may need to compose custom SQL queries, known as datasets, to extract the data you require from the database.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Which FortiAnalyzer feature allows you to group devices that administrators can monitor and manage?  
 A. Administrative domains (ADOMs)  
 B. Reports
  
2. Which operating mode on FortiAnalyzer is used to collect logs from multiple devices and then forward those logs to another device?  
 A. Analyzer  
 B. Collector

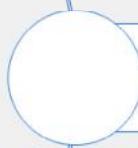
**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



### Key Features and Concepts



### Initial Configuration



### External Storage

Good job! You now understand FortiAnalyzer key features and concepts.

Now, you will learn how to initially configure FortiAnalyzer.

**DO NOT REPRINT**  
© FORTINET

## Initial Configuration

### Objectives

- Access FortiAnalyzer
- Identify the tools you can use to configure FortiAnalyzer
- Change the default administrator password
- Add FortiAnalyzer to your network
- Perform a system backup

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in the initial configuration of FortiAnalyzer, you will be able to add FortiAnalyzer to your network, and perform basic administrative tasks.

**DO NOT REPRINT****© FORTINET**

## Factory Default Settings

- Use factory default settings to initially log in to FortiAnalyzer and begin your network configuration
  - You can find default settings in your FortiAnalyzer *QuickStart* guide ([docs.fortinet.com](https://docs.fortinet.com))
  - Always use port1 to connect FortiAnalyzer with the management computer
- If you are deploying the FortiAnalyzer VM, the management IP address depends on the virtualization platform or the cloud provider you are using

User name	Password
admin	<none>

Port	IP address	Netmask	Management access
port1	192.168.1.99	255.255.255.0	https, ssh

It is important to know the factory default settings, such as the default username and password, the port1 IP address, the netmask, and the default supported management access protocols, so you can initially connect to the management interface and configure FortiAnalyzer for your network.

You can find the default settings in your model-specific *QuickStart Guide*. Different FortiAnalyzer models have different numbers of ports, but port1 is the management port and always has the same default IP address.

If you are deploying the FortiAnalyzer VM, the management IP address and its assignment depend on the virtualization platform you are using. Visit visit <https://docs.fortinet.com/product/fortianalyzer-public-cloud/7.0> for more details.

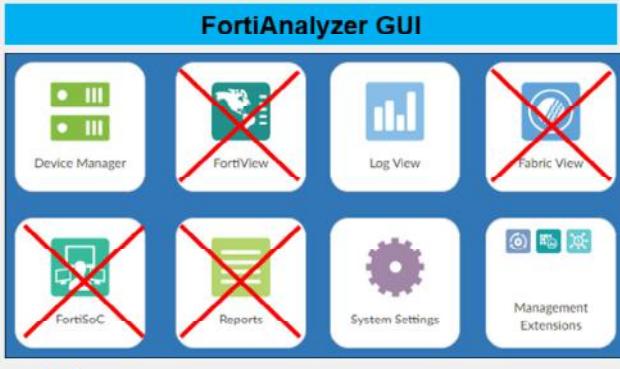
You can also configure your management IP on the CLI with the commands:

```
config system interface
  edit port1
    set ip <IP address> <netmask>
end
```

See the next slide for information about the CLI.

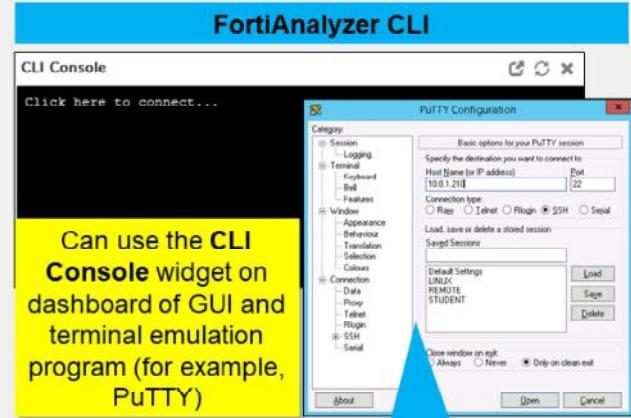
**DO NOT REPRINT**  
**© FORTINET**

## Available Tools to Configure FortiAnalyzer



**X** = Not available in Collector mode

- Can use both tools locally and remotely
- Features depend on the profile of the administrator logged in and the operation mode of FortiAnalyzer (analyzer or collector)
- Configuration changes take effect immediately



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

14

Just like with FortiGate, the GUI and CLI are the two configuration tools you can use to manage FortiAnalyzer. You can use both tools locally, by connecting directly to FortiAnalyzer, and remotely, based on your configured settings. You can deny or permit access based on IP address.

When you use the CLI, you can run commands through the **CLI Console** widget, available on the GUI dashboard, and through a terminal emulation application, such as PuTTY. Using PuTTY requires a separate Telnet, SSH, or local console (DB-9) connection.

The FortiAnalyzer features available on the GUI and CLI depend on the profile of the administrator logged in and the operation mode of FortiAnalyzer. For example, when operating in collector mode, the GUI doesn't include **FortiView**, **Fabric View**, **Report**, or **FortiSOC**. Also, if you are logged in with the **Standard\_User** or **Restricted\_User** administrator profiles, full access privileges, like those granted to the **Super\_User** profile, are not available. The CLI also includes some settings that are not available through the GUI.

Any configuration changes you make using the GUI and CLI take effect immediately, without resetting the FortiAnalyzer system or interrupting services.

Note that the SQL database is disabled by default when FortiAnalyzer is in collector mode, so logs that require the SQL database are not available in collector mode unless the SQL database is enabled on the CLI.

**DO NOT REPRINT**  
**© FORTINET**

## Logging in for the First Time

**FortiAnalyzer GUI**

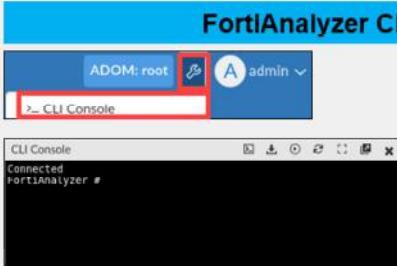
- In a supported browser, use the factory default information to log in:
  - o <https://192.168.1.99>

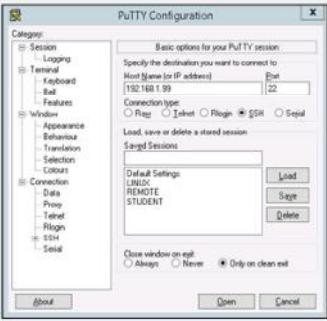


**FortiAnalyzer CLI**

Log in to the GUI and click **System Settings > Dashboard**

Click inside **CLI Console** widget (automatically logged in)





Log in with default FortiAnalyzer port1 IP address with supported protocol

Leave the password blank

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

To log in to the FortiAnalyzer GUI for the first time, open a browser and enter the URL `https://` followed by <the management IP address>. After the login screen opens, use the factory default administrator credentials to log in. Type the username **admin** (in lower case) and leave the password field empty.

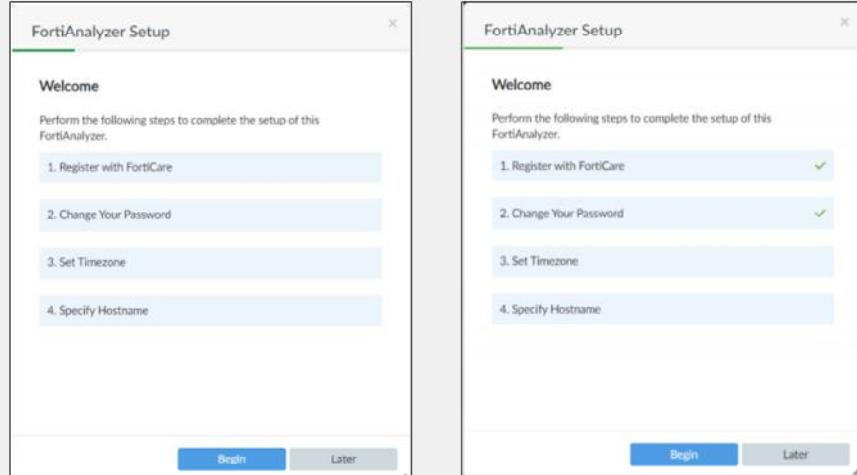
To log in to the CLI for the first time, you can use one of two methods:

- Integrated CLI Console: Log in to the GUI and click on the **Tools** icon located on the upper-right corner. Then click **>\_CLI Console**. You are automatically logged in to the console.
- Terminal emulation application (such as PuTTY): Enter the FortiAnalyzer port1 IP address and select a supported management access protocol, such as SSH. When connected and prompted to log in, use the factory default administrator credentials.

**DO NOT REPRINT**  
© FORTINET

## FortiAnalyzer Setup Wizard

- The wizard appears after you log in for the first time
- You can choose to complete all or some of the steps now or later
- Completed steps display a green check mark beside them



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

16

The FortiAnalyzer Setup Wizard appears after you log in for the first time.

You can use it to register your FortiAnalyzer device with FortiCare, change the default password, set the correct time zone, and set the device hostname.

You can choose to complete all or some of the steps now or at a later time.

Completed steps display a green check mark beside them.

**DO NOT REPRINT**  
**© FORTINET**

## Changing the Default Admin Password

- Change the default `admin` password
- Must change for security reasons!
  - Select secure password
- No password recovery!

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

For security reasons, one of the first tasks you should perform is to change the default `admin` password. It is recommended that you do this during the Setup Wizard. You can also change it at any time on the **Administrators** page by right-clicking the administrator user, and then selecting **Change Password**. Make sure you enter a secure, strong password.

Be aware that there is no password recovery option for FortiAnalyzer!

If you forget your password and lose access to FortiAnalyzer, one option is to use the `execute migrate` command that allows you to load a backup of the configuration.

Follow these steps:

1. Perform a factory reset on the VM or device.
2. Run the `execute migrate` command.
3. Use the default `admin` account and password (system settings are not restored).

The other option is to format the flash and reload the image (from the BIOS configuration menu). This erases the system settings, including the administrative accounts.

So, make sure you remember your password or store it in a secure location.

**DO NOT REPRINT**  
© FORTINET

## Increasing Account Security Through Password Policy

- Increase administrator account security by configuring a password policy (disabled by default)
  - Global administration setting

**System Settings > Admin > Admin Settings**

Password Policy	<input checked="" type="checkbox"/>
Minimum Length	<input type="text" value="8"/> (8-32 characters)
Must Contain	<input type="checkbox"/> Uppercase Letters <input type="checkbox"/> Lowercase Letters <input type="checkbox"/> Numbers (0-9) <input type="checkbox"/> Special Characters
Admin Password Expires after	<input type="text" value="0"/> (days)

You can increase the security of your administrator accounts by configuring a global password policy for all administrators on the **Admin Settings** page. By default, the password policy is disabled.

The policy allows you to set a minimum password length, specify if characters or numbers must be included in the password, and specify the number of days for which a password remains valid.

If you do set a password expiry, ensure you adhere to the policy and change the password before it expires because there is no password recovery option.

**DO NOT REPRINT****© FORTINET**

## Security Recommendations

- Deploy FortiAnalyzer in a protected and trusted private network
- Use secure communication methods (HTTPS or SSH), even in a private network
- Configure trusted hosts
- If access from the outside is required, open only the ports necessary for correct communications
- If access from the outside is required, set up special users and use only secure protocols (HTTPS/SSH)
- Always use secure passwords
- Keep your password in a secure place because FortiAnalyzer does not support password recovery

Before reviewing the configuration settings, it is necessary to discuss the importance of security. FortiAnalyzer stores your network log information, so it is *vital* that you protect your data correctly.

Here are some security recommendations:

- Deploy FortiAnalyzer in a protected and trusted private network. You should never deploy it outside the network.
- Always use secure connection methods for administration: HTTPS for the GUI, or SSH for the CLI. Methods like HTTP and Telnet use plain text, and are not secure, so an attacker can use packet-sniffing tools to obtain information useful for breaching your network.
- Use trusted hosts on your users to allow logins only from specific locations. If you do need to open outside access to the device so that remote FortiGate devices can connect, open only the ports necessary for this. Additional open ports increase your security risk. If you need to open direct login access from the outside, be sure to set up special user accounts for this and open only protocols that are secure. Use a secure password because they are important if you start transmitting traffic over connections that anyone (that is, the internet) could be listening to.
- Make sure you store your administrator password in a secure place because FortiAnalyzer does not support password recovery.

**DO NOT REPRINT**  
**© FORTINET**

## Configuring FortiAnalyzer for Your Own Network

The screenshot shows the FortiAnalyzer configuration interface under the 'Network' tab. It includes three main sections:

- Physical Interfaces:** A table listing 12 ports (port1 to port12) as Physical Interfaces. The 'IP/Netmask' column shows various IP addresses and netmasks. A blue callout labeled 'Set IPs' points to this section.
- DNS:** A section for configuring DNS servers. It shows 'Primary DNS Server' set to 208.91.112.52 and 'Secondary DNS Server' set to 208.91.112.53. A blue callout labeled 'Set DNS' points to this section.
- Routing Table:** A table with one entry (ID 1) showing an IPv4 route. The 'IP/Netmask' is 10.200.3.0/255.255.255.0 and the 'Gateway' is 10.200.1.254, both pointing to 'Interface port3'. A blue callout labeled 'Set gateway' points to this section.

At the bottom left is the NSE Training Institute logo, and at the bottom right is the page number 20.

The initial configuration of FortiAnalyzer is very similar to FortiGate.

In order to configure FortiAnalyzer for your network, you must set the IP address and netmask, select supported administrative access protocols, and specify a default gateway for routing packets. You can do all this on the **Network** page.

**DO NOT REPRINT**  
**© FORTINET**

## Configuring FortiAnalyzer for Your Own Network (Contd)

The screenshot shows the 'Edit Network Interface' screen under 'System Settings > Network'. The interface is named 'port1'. The IP address is set to '10.0.1.210/255.255.255.0'. Under 'Administrative Access', 'HTTPS', 'HTTP', 'PING', and 'SSH' are checked, while 'SNMP', 'Web Service', and 'FortiManager' are unchecked. A callout bubble points to the management address with the text 'Configure management address'. Another callout bubble points to the protocol checkboxes with the text 'Enable protocols to support (default = HTTPS and SSH)'.

Setting your own IP address and netmask provides more security than using the default address and, if more than one FortiAnalyzer is in the same network, different network settings are mandatory. The management interface must have a dedicated (unique) address.

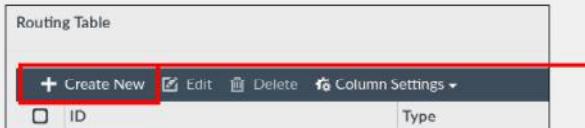
There are a few *non-standard* administrative access protocols that are worth mentioning as well:

- Web service: Allows access to FortiAnalyzer from a web service such as SOAP, a messaging protocol that allows programs that run on disparate operating systems (such as Windows and Linux). The FortiAnalyzer server runs on Linux.
- FortiManager: Allows FortiAnalyzer to be managed by a FortiManager.

**DO NOT REPRINT**  
**© FORTINET**

## Other Network Setting Options

- Assign IPv4/IPv6 static routes to a different gateway so that packets are delivered by a different route



Create New Network Route

IP Type	IPv4
Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	None
Interface	port1 port2 port3

- Include a DNS server in order to resolve hostnames in the logs
  - Recommended to have both a primary and secondary

DNS

Primary DNS Server	208.91.112.52
Secondary DNS Server	208.91.112.53

Default = FortiGuard DNS servers

If you want to configure another port on FortiAnalyzer, you can assign specific IPv4 or IPv6 static routes to a different gateway, so that packets are delivered by a different route.

If you want to be able to resolve hostnames in the logs, you need a DNS server. The default primary and secondary DNS server addresses are the FortiGuard DNS servers. You can use these addresses, or change them to some other servers of your preference. It is a best practice to have both a primary and secondary servers. Furthermore, response times are a consideration for DNS, so choose DNS servers as close as possible to your network, such as your internet provider's DNS.

**DO NOT REPRINT****© FORTINET**

## Resetting the Configuration

- To reset to factory default settings:

```
# execute reset all-settings
```

- To reset all settings except current IP addresses and routes:

```
# execute reset all-except-ip
```

- To erase all device settings and images, databases, and log data from disk, but preserve IP and routing info:

```
# execute format disk
```

- You should always format the disk after resetting the configuration
- A low-level disk format option, deep-erase, is available

- You should connect directly using the console port

If you need to reset your configuration, you can use these commands:

- The `execute reset all-settings` command erases the show configuration on flash, which contains the IP addresses and routes, while the `execute reset all-except-ip` command leaves the settings for IP addresses and routes.
- The `execute format disk` command erases all device settings, images, databases, and log data on disk, while preserving the IP addresses and routing info. You should always run this command after resetting the configuration.
- If your environment requires it, you can use the `execute format disk deep-erase <1-35>` command to perform a low-level format of the disk one or more times. Keep in mind that this process can take a very long time, even days, depending on the size of the disk being formatted and the number of rounds you specify.

It is a best practice to run these commands while connected directly using the console port to avoid losing access after the configuration is reset.

**DO NOT REPRINT**  
**© FORTINET**

## Basic CLI Commands for System and Network Settings

- Use the following FortiAnalyzer CLI commands to examine or troubleshoot system and network settings:

Command	Information
# get system status	Displays the status of your FortiAnalyzer device
# show system interface	Displays the network interface configuration on your FortiAnalyzer device, such as configured ports and associated IP addresses as well as enabled administrative access protocols
# show system DNS	Displays DNS server addresses
# show system ntp	Displays automatic time setting using a network time protocol (NTP) server
# get system ntp	Displays how often FortiAnalyzer synchronizes its time with the NTP server
# show system route	Displays static routing table entries on your FortiAnalyzer device
# execute ping	Tests the network connection between FortiAnalyzer and another network device

You can use the CLI commands shown on this slide to examine or troubleshoot system and network settings on FortiAnalyzer.

**DO NOT REPRINT**  
© FORTINET

## Viewing Server Information

- Use these commands to view server information:

Command	Information
# diagnose system print cpuinfo	Print the CPU information. This command includes the following: processor, vendor ID, CPU family, model, model name, stepping, CPU MHz, cache size, physical ID, and sibling
# diagnose system print df	Print the file system disk space usage. This command displays the following information: file system, 1K-blocks, used, available, percent used, mounted on
# diagnose system print hosts	Print the static table lookup for host names
# diagnose system print loadavg	Print the average load of the system
# diagnose system print netstat	Print the network statistics for active internet connections (servers and established). This command displays the following information: protocol, local address, foreign address, and state
# diagnose system print partitions	Print the partition information of the system
# diagnose system print route	Print the main route list. This command displays the following information: destination, gateway, gateway mask, flags, metric, reference, use, and interface

To access and view server-related information, use the `diagnose system print` commands. For a complete list of commands, refer to the *FortiAnalyzer CLI Reference*, which you can obtain from <https://docs.fortinet.com>.

**DO NOT REPRINT**  
**© FORTINET**

## Performing a System Configuration Backup

- System Configuration Backups contain:
  - System information
  - Device list
  - Report information
- Do not include actual logs and generated reports!
- Backups can be restored only to the same model and firmware version
- Can encrypt backup file
  - Encrypted backups not recommended when dealing with Fortinet Support
- Restore configuration from any previous backup
- If your FortiAnalyzer is a VM, you may also use VM snapshots

### System Settings > Dashboard

System Information	
Host Name	FortiAnalyzer
Serial Number	FAZ-VM0000065040
Platform Type	FAZVM64-KVM
HA Status	Standalone
System Time	Fri Oct 22 14:26:48 2021 PDT
Firmware Version	v7.0.2-build0180 211019 (GA)
System Configuration	Last Backup : Thu Oct 21 10:45:46 2021
Current Administrators	admin / 1 in total
Up Time	1 day 2 hours 57 minutes 54 seconds
Administrative Domain	(Switched)
Operation Mode	Analyzer (Collector)

After you have completed your initial configuration, you should back it up as a best practice. You can perform a backup directly on the GUI using the **System Information** widget.

The **System Configuration** backups contain everything *except the actual logs and generated reports*. You can backup logs and reports using the GUI (**Log View, Reports**) or using the CLI with the command `execute backup`.

What does the **System Configuration** backup include?

- System information, such as the device IP address and administrative user information
- Device list, such as any devices you configured to allow log access
- Report information, such as any configured report settings, as well as all your custom report details. These are not the actual reports.

You can save the backup file as an encrypted file for additional security. Be aware that you can restore a backup only to the same model and firmware version. Furthermore, if you require assistance from Fortinet Support and your configuration is required to assist with troubleshooting, your backup should not be encrypted.

If changes are made to FortiAnalyzer that affect your network negatively, you can restore the configuration from any of your backups.

If your FortiAnalyzer is a VM, you can also use VM snapshots.

**DO NOT REPRINT**  
© FORTINET

## Best Practices

- Always turn off FortiAnalyzer gracefully, because not doing so can damage the databases  

```
# execute shutdown
```
- Have FortiAnalyzer running on an uninterruptable power supply (UPS) to prevent unexpected power-off events. Also ensure your UPS is stable and has sufficient current to ensure expected behavior
- For ease of use, save an unencrypted backup to a secure location
  - Allows for offline access to database configuration file
  - Recommended when dealing with Fortinet Support
- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server for correct log correlation
- Implement a comprehensive backup plan that includes the configuration and the logs
- Increase reliability by configuring high availability (HA) and link aggregation (available in models 2000E or higher, and VMs)

The following are some best practices for operating FortiAnalyzer:

- Always turn off FortiAnalyzer *gracefully* because not doing so can damage the databases.
- Have FortiAnalyzer running on an uninterruptable power supply (UPS) to prevent unexpected power-off events. Also ensure your UPS is stable and has sufficient current to ensure expected behavior.
- For ease of use, save an unencrypted backup to a secure location. You should use an unencrypted backup when dealing with Fortinet Support because it allows for offline access to the database configuration file.
- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server for correct log correlation.
- Implement a comprehensive backup plan that includes the configuration and the logs.
- Increase reliability by configuring high availability (HA) and link aggregation (available on models 2000E and higher, and VMs).

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. You want to permit administrator logins on FortiAnalyzer from specific locations only. How can you configure this on FortiAnalyzer?
  - A. Use administrative profiles.
  - B. Use trusted hosts.
  
2. What should you always do after erasing the configuration from flash memory?
  - A. Run the execute format disk command.
  - B. Run the execute reset all-settings command.

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



**Key Features and Concepts**



**Initial Configuration**



**External Storage**

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

29

Good job! You now understand how to initially configure FortiAnalyzer.

Now, you will learn how to configure external log storage.

DO NOT REPRINT  
© FORTINET

## External Storage

### Objectives

- Understand fabric connectors

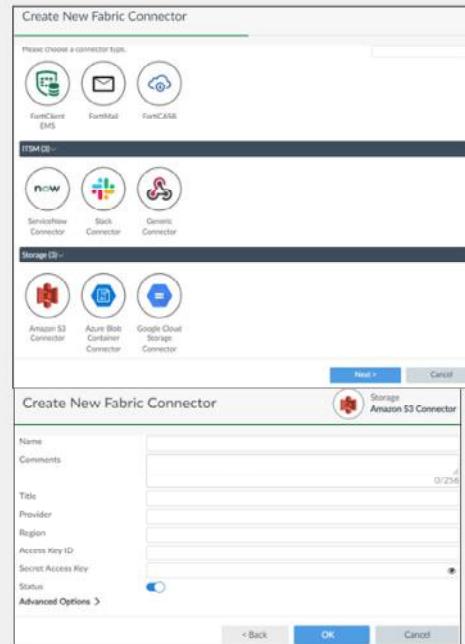
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiAnalyzer fabric connectors, you will be able to configure FortiAnalyzer to send logs and interact with other platforms.

**DO NOT REPRINT**  
**© FORTINET**

## Fabric Connectors

- You can configure FortiAnalyzer to send logs or notification events to:
  - External cloud platforms: AWS, Azure, Google
  - ITSM: ServiceNow, Slack, Webhook
  - Security Fabric: FortiClient EMS, FortiMail, FortiCASB
- Improves data redundancy
- Reduces performance degradation
- Enriches actions available on FortiSOC



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

31

Storage connectors allow you to back up data (rolled logs) to public cloud accounts in Amazon S3, Microsoft Azure, and Google Cloud.

Support for this feature requires you to configure the following components on FortiAnalyzer:

- Create a fabric connector for Amazon S3, Microsoft Azure, or Google Cloud.
- Configure cloud storage.

Fabric connectors also enable FortiAnalyzer to send notifications to ITSM platforms when a new incident is created or for any subsequent updates. This approach is more efficient than third-party platforms polling information from the FortiAnalyzer API at predefined intervals, which could result in FortiAnalyzer performance degradation.

Security Fabric connectors enrich incident response-related actions available on FortiSOC.

**DO NOT REPRINT**  
**© FORTINET**

## Storage Connector Service

- Requires separate license for storage connector
- License includes storage limitation and expiration date

The screenshot shows the 'License Information' section of the FortiAnalyzer interface. It displays various license metrics and settings. A red box highlights the 'Storage Connector Service' row, which shows a Cloud type with a limit of 10.0 TB, currently using 39.5 GB (0.4% licensed). Other sections include VM License, Logging, FortiGuard, and Update Server.

License Information	
VM License	Type: Valid
Logging	Devices/VDOMs: 6 of 10,000
	GB/Day: 2.5 of Unlimited
	VM Storage: 101.72 GB of Unlimited
Storage Connector Service	Type: Cloud Status: (0.4%) Licensed (Expires on 2022-03-13)
FortiGuard	Indicators of Compromise Service: Licensed (Expires 2022-01-18)
Update Server	Server Location: Global Servers AntiVirus and IPS: 192.168.100.105 FortiClient Update: 192.168.100.105

**Device Log Settings**

Registered Device Logs

- Roll log file when size exceeds: 10 (10-1000) MB
- Roll log files at scheduled time
- Upload logs using a standard file transfer protocol
- Upload logs to cloud storage

**Create New**

Name	Cloud Storage Connector	Upload Option	Remote Path
AWSStorage	AWSConnector	On Rolling	/awsbucket
AzureStorage	AzureConnector	On Rolling	/azurescontainer
GoogleStorage	GoogleConnector	On Rolling	/googlebucket

```
# diagnose fmupdate dbcontract fds
FAZ-VM0000160617 [SERIAL_NO]
AccountID: *****@fortinet.com
Industry:
Company: Fortinet
Contract: 8
AVDB-1-99-20220722
AVEN-1-99-20220722
ENHN-1-10-20220727
FMWR-1-06-20220727
FRVS-1-06-20220727
NIDS-1-99-20220722
PBDS-1-06-20220727
SCPC-1-06-20220313
SPRT-1-10-20220727
```

```
#ZVM64 # diagnose test application uploadd 63
loud Storage Usage:
Status: Expire in: 353 days 12 hours 57 minutes
Usage:
Total Gigabytes Uploaded: 39 GB
Number of Files Uploaded: 10446 Files
Quota: 10 TB
Number of Upload Requests Dropped: 0 Requests
```

In order to send logs to cloud platforms, you must buy a separate license for the **Storage Connector Service**. This license includes:

- Storage limitation: amount of data that can be uploaded to the cloud platform.
- Expiry date: the date up to which the storage data can be sent. Normally valid for one year.

This license *does not* include the storage used on the cloud provider. It includes only the amount of data that you can transfer. To configure this feature, you must have an account with permissions to access the cloud storage. Refer to the *FortiAnalyzer Administration Guide* for more details.

Note that if uploaded logs reach data storage limitations before the license expires, you must renew the license in order to continue to use this service.

After the license is uploaded, you can enable the **Upload logs to cloud storage** feature under **System Settings > Device Log Settings**, and then select the cloud storage platforms that the data will be sent to.

You can use the `diagnose fmupdate dbcontract fds` command to find out about the license validity and expiry details.

The `diagnose test application uploadd 63` command gives details, such as usage quota, total data upload in GB, total number of files uploaded, number of days remaining until license expiry, and number of uploaded requests that were dropped.

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



**Key Features and Concepts**



**Initial Configuration**



**External Storage**

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

33

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in the lesson.

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Describe the purpose of FortiAnalyzer
- ✓ Describe the purpose of administrative domains and when you might use them
- ✓ Describe the difference between FortiAnalyzer operating modes
- ✓ Identify where log data is stored
- ✓ Access FortiAnalyzer
- ✓ Identify the tools you can use to configure FortiAnalyzer
- ✓ Change the default administrator password
- ✓ Add FortiAnalyzer to your network
- ✓ Perform a system backup
- ✓ Understanding Fabric connectors

This slide shows the objectives that you covered in this lesson.

DO NOT REPRINT  
© FORTINET



## FortiAnalyzer

Administration and Management



FortiAnalyzer 7.0

Last Modified: 1 December 2021

In this lesson, you will learn some administration and management functions you can use to better defend FortiAnalyzer—and the sensitive log data it stores—against external or internal threats.

**DO NOT REPRINT****© FORTINET**

## Lesson Overview



Administrative Access Controls

Monitoring Administrative Events and Tasks

High Availability

Administrative Domains (ADOMs)

RAID

In this lesson, you will learn about the topics shown on this slide.

DO NOT REPRINT  
© FORTINET

## Administrative Access Controls

### Objectives

- Control or restrict administrative access using admin profiles, trusted hosts, and ADOMs
- Validate administrators using external servers
- Configure two-factor authentication

After completing this section, you should be able to achieve the objectives shown on this slide. By demonstrating competence in using administrative access controls, you will be able to better safeguard the administration and management of your FortiAnalyzer device and the sensitive data it collects.

# DO NOT REPRINT

## © FORTINET

## Multiple Administrators and Security

- Divide administrative tasks among multiple employees by creating additional administrative accounts
- Every additional administrator causes linear-to-exponential growth in risk
- To better protect your network, control or restrict administrator access using:
  - Administrative profiles
  - Trusted hosts
  - ADOMs

Admin profile type

Assign one or more ADOMs to administrator account

### System Settings > Admin > Administrators

Depending on your deployment, you may want to divide FortiAnalyzer administrative tasks among multiple employees by creating additional administrative accounts. However, every additional individual to which you give administrator access causes linear-to-exponential growth in risk.

In order to protect your network, you can control and restrict administrative access using the following methods:

- Administrative profiles: Determines the level of access, or privileges, granted
- Trusted hosts: Determine from where a connection can be established
- ADOMs: Determines to which devices the admin will have access to view and manage its logs

By giving administrative access to multiple people, and employing methods of control, you can better protect your network.

# DO NOT REPRINT

## © FORTINET

### Administrative Profiles

- Never give an administrator more privileges than they need
- Assign the appropriate profile—you can modify and create profiles as required
  - Access profiles define administrator privileges

Profile name	Administrator privileges
Super_User	<ul style="list-style-type: none"> <li>All system privileges enabled</li> <li>All device privileges enabled</li> </ul>
Standard_User	<ul style="list-style-type: none"> <li>No system privileges enabled</li> <li>Read-write access for all device privileges</li> </ul>
Restricted_User	<ul style="list-style-type: none"> <li>No system privileges enabled</li> <li>Read-only access for all device privileges</li> </ul>

**System Settings > Admin > Profile**

+ Create New Edit Clone Delete

#	Name
1	Restricted_User
2	Standard_User
3	Super_User

**NSE Training Institute**

Standard and restricted users can't access system settings, and restricted users can't access management extensions

Can create custom profiles

Can modify individual privileges in profiles

© Fortinet Inc. All Rights Reserved.

5

You should never give administrators more privileges than they need to fulfill their role. FortiAnalyzer comes with four preinstalled default profiles that you can assign to other administrative users. Administrator profiles define administrator privileges and are required for each administrative account. The four default profiles are:

- Super\_User**, which, like in FortiGate, provides access to all device and system privileges.
- Standard\_User**, which provides read and write access to device privileges, but not system privileges.
- Restricted\_User**, which provides read access only to device privileges, but not system privileges. Access to the Management extensions is also removed.
- No\_Permissions\_User**, which provides no system or device privileges. Can be used, for example, to temporarily remove access granted to existing admins.

You can assign the default profiles to administrative accounts, or you can modify the individual privileges associated with each default profile. Alternatively, you can create your own custom profiles.

# DO NOT REPRINT

## © FORTINET

### Trusted Hosts

- Trusted hosts restrict login access to specific IPs or subnets
- Configure up to 10 IPv4 and IPv6 trusted hosts
- Applies to both GUI and CLI (when accessed through SSH)

#### System Settings > Admin > Administrators

Trusted Hosts	<input checked="" type="checkbox"/>
Trusted IPv4 Host 1	0.0.0.0/0.0.0.0
Trusted IPv4 Host 2	255.255.255.255/255.255.255.255
Trusted IPv4 Host 3	255.255.255.255/255.255.255.255
Trusted IPv6 Host 1	::/0
Trusted IPv6 Host 2	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128
Trusted IPv6 Host 3	ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128

Can configure up to 10 IPv4 and IPv6 trusted hosts

In addition to controlling administrative access through administrator profiles, you can further control access by setting up trusted hosts for each administrative user. This restricts administrators to logins from only specific IPs or subnets. You can even restrict an administrator to a single IP address, if you define only one trusted host IP.

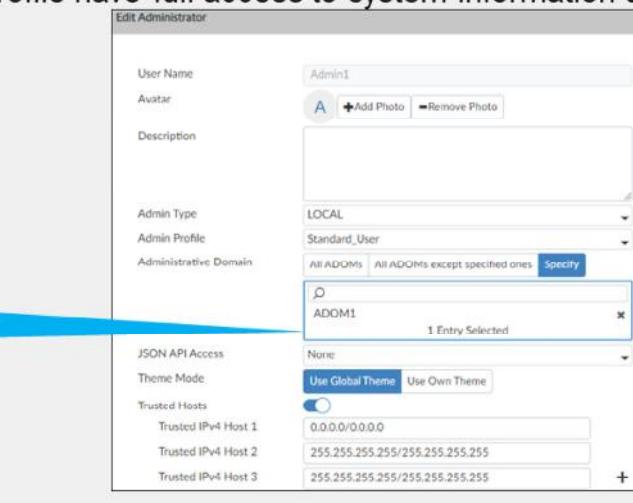
The trusted hosts you define apply to both the GUI and the CLI when accessed through SSH.

**DO NOT REPRINT**  
**© FORTINET**

## Controlling Access Through ADOMs

- Monitor and manage devices in only the assigned ADOM
- Increases security of network and makes device management more effective
- Administrators with `Super_User` profile have full access to system information and to all ADOMs

NSE Training Institute



© Fortinet Inc. All Rights Reserved.

7

Another way you can control administrative access is through ADOMs. Using ADOMs makes device management more effective, because administrators need only to monitor and manage devices in their assigned ADOMs. It also makes the network more secure, because administrators are restricted to only those devices to which they should have access.

Administrators who have the `Super_User` profile have full access to all ADOMs. Administrators with any other profile have access to only those ADOMs to which they are assigned—this can be one or more.

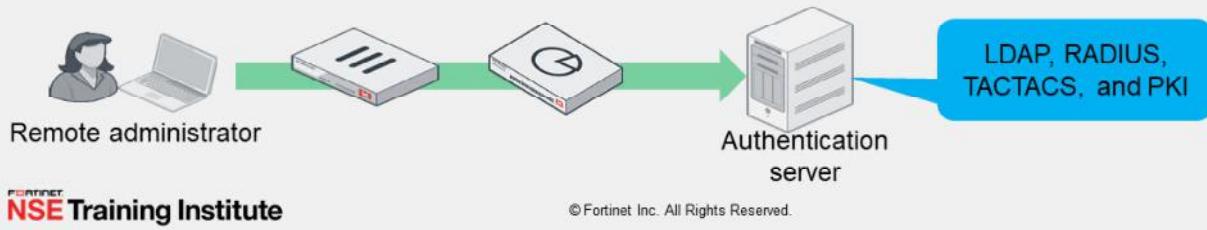
**DO NOT REPRINT**  
**© FORTINET**

## External Authentication of Administrators

- Configure external servers to validate your administrator logins (non-local users)
  - LDAP, RADIUS, TACACS+, and PKI can be used to authenticate administrators
  - Must configure server entries for each authentication server in your network

### System Settings > Admin > Remote Authentication Server

Edit LDAP Server	
Name	External_Server
Server Name/IP	10.0.1.150
Port	389
Common Name Identifier	uid
Distinguished Name	ou=Training,dc=trainingAD,dc=training,dc=lab
Bind Type	Regular
User DN	uid=fazadmin,ou=Training,dc=trainingAD,dc=training,dc=lab
Password	*****
Secure Connection	<input type="checkbox"/>
Administrative Domain	All ADOMS <input type="button" value="Specify"/>



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

8

Instead of creating local administrators, where logins are validated by FortiAnalyzer, you can configure external servers to validate your administrator logins. RADIUS, LDAP, TACACS+, and PKI can all be used to authenticate administrators.

The image on this slide shows an example of an LDAP server configuration.

# DO NOT REPRINT

## © FORTINET

## External Authentication of Administrators (Contd)

- The **Wildcard** feature allows you to authenticate users from one or more groups configured on remote servers
  - Single administrative user on FortiAnalyzer that points to a remote authentication server (no local authentication credentials)
  - Supported using LDAP, RADIUS, TACACS+, GROUP (in **Admin Type** drop-down list)
  - The **Admin Type GROUP** supports multiple authentication server types
    - You can group authentication servers using the CLI

The screenshot shows the 'Edit Administrator' form. The 'User Name' field contains 'Admin1'. Below it is an 'Avatar' section with a placeholder 'A' and buttons for '+Add Photo' and '-Remove Photo'. The 'Description' field is empty. The 'Admin Type' dropdown is set to 'GROUP'. Under 'AuthServers', there is a list containing 'AuthServers' with a checked checkbox labeled 'Match all users on remote server'.

### System Settings > Admin > Remote Authentication Server

Name	Type	ADOM	Details
External_Server	LDAP	All ADOMs	10.0.1.150:389/uid: ou=Training,dc=trainingAD,dc=training,dc=lab
LDAP2	LDAP	All ADOMs	10.0.1.155:389/uid: ou=training,dc=trainad,dc=fnt,dc=lab

In this example, two external authentication servers have been added

You can use the **Match all users on remote server** option to enable administrators to log in to FortiAnalyzer using their credentials on a remote authentication server, such as RADIUS, TACACS+, and LDAP. This option is useful for creating wildcard administrators and removes the need for FortiAnalyzer to store local credentials, because a remote authentication server is being used. This simplifies administration. For example, if an employee leaves the company, their account does not exist on FortiAnalyzer—they exist only as a user on a remote authentication server. If you do not select this option, you must provide a password that is used only if FortiAnalyzer is unable to connect to the authentication server.

You can set remote authentication server groups, which are listed as **GROUP** in the **Admin Type** drop-down list, to extend administrator access. Usually, you create a wildcard administrator only for a single server. However, if you group multiple servers, you can apply a wildcard administrator to all the servers in the group. If you added an LDAP and RADIUS server to your authentication group and the administrator had login credentials on both servers, then the administrator could authenticate on FortiAnalyzer using either their LDAP or RADIUS credentials.

You can group multiple servers of the same type to act as backup—if one server fails, the administrator can still be authenticated by another server in the group. You can add remote authentication server groups using the CLI only. In the example shown on the slide, two existing LDAP servers were added. On the CLI (not shown in the slide), an authentication server group was added and named **AuthServers** and the servers were added to this group.

**DO NOT REPRINT**  
**© FORTINET**

## Two-Factor Authentication

- Configure two-factor authentication
  - Something you know (password) and something you have (token)
  - You need: FortiAuthenticator and FortiToken
- FortiAnalyzer configuration:
  - Create a RADIUS server that points to FortiAuthenticator
  - Create an administrator account that points to the RADIUS server

### System Settings > Admin > Remote Authentication Server

Name	RADIUS
Server Name/IP	10.0.1.11
Port	1812
Server Secret	*****
Secondary Server Name/IP	
Secondary Server Secret	*****
Authentication Type	ANY
Advanced Options >	

### System Settings > Admin > Administrators

User Name	2FA-Admin
Avatar	2 <input type="button" value="Add Photo"/> <input type="button" value="Remove Photo"/>
Description	
Admin Type	RADIUS
RADIUS Server	RADIUS
<input type="checkbox"/> Match all users on remote server	
New Password	*****
Confirm Password	*****
Admin Profile	Restricted_User
Administrative Domain	All ADOMs All ADOMs except specified ones Specify

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

10

To add additional security to external administrators, you can configure two-factor authentication. To do this, you need to use FortiAuthenticator and FortiToken.

On the FortiAnalyzer side, you need to create a RADIUS server that points to FortiAuthenticator and then create an administrator account that points to the RADIUS server.

For more information about configuring external servers and two-factor authentication, see the *FortiAnalyzer Administration Guide*.

**DO NOT REPRINT**  
**© FORTINET**

## SAML Admin Authentication

- FortiAnalyzer supports SAML
- SAML can be enabled across all Security Fabric devices
- Allows smooth movement between devices for administrator (SSO)
- FortiAnalyzer can be the identity provider (IdP) or the service provider (SP)

**System Settings > Admin > SAML SSO**

**Single Sign-On Settings**

Server Address: 10.0.1.210  
Allow admins to login with FortiCloud: Disabled  
Identity Provider (IdP) | Service Provider (SP) | Fabric SP  
Download

SP Settings

Name	Entity ID	URL
FGT	https://10.0.1.120/metadata/	

**NSE Training Institute** © Fortinet Inc. All Rights Reserved. 11

In FortiAnalyzer, SAML can be enabled across all Security Fabric devices, enabling smooth movement between devices for the administrator by means of single sign-on (SSO).

FortiAnalyzer can play the role of the identity provider (IdP), the service provider (SP), or Fabric SP, when an external identity provider is available.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

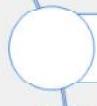
1. How do you restrict an administrator's access to a subset of your organization's ADOMs?  
 A. Assign the ADOMs to the administrator's account  
 B. Configure trusted hosts
  
2. What is a wildcard administrator?  
 A. Allows administrators to log in with credentials stored locally on FortiAnalyzer  
 B. Allows administrators to log in with credentials stored on a remote authentication server

**DO NOT REPRINT****© FORTINET**

## Lesson Progress



Administrative Access Controls



Monitoring Administrative Events and Tasks



High Availability



Administrative Domains (ADOMs)



RAID



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

13

Good job! You now understand administrative access controls.

Now, you will learn how to monitor events.

DO NOT REPRINT  
© FORTINET

## Monitoring Administrative Events and Tasks

### Objectives

- Monitor FortiAnalyzer administrators, events, and tasks
- Monitor FortiGate administrator logins and activity

After completing this section, you should be able to achieve the objectives shown on this slide. By demonstrating competence in monitoring administrative events and tasks, you will be able to ensure administrators are operating within their assigned role, thereby mitigating risk to your organization.

DO NOT REPRINT  
© FORTINET

## Monitoring Administrator Login Status

- Monitor current logged in administrator accounts
  - Identify logged in user by the green checkmark next to their name
- By default, the list is available only to administrators with Super\_User access

### System Settings > Admin > Administrators

	Name	Type	Profile	JSON API Access	ADOMs	Trusted IPv4 Hosts
<input type="checkbox"/>	A  admin	LOCAL	Super_User	<input checked="" type="checkbox"/> <input type="checkbox"/>	None	All ADOMs 0.0.0.0/0.0.0.0
<input type="checkbox"/>	A Admin1	LOCAL	Standard_User	<input checked="" type="checkbox"/> <input type="checkbox"/>	None	All ADOMs 0.0.0.0/0.0.0.0

You can track administrator user sessions, including who is currently logged in and on what trusted host, through the **Administrators** page. By default, only administrators with Super\_User access can see the complete administrator's list.

Administrators who are logged in are indicated by a green check mark.

**DO NOT REPRINT**  
**© FORTINET**

## Viewing Administrator Event Logs

- View FortiAnalyzer event logs, including administrator activity
  - By default, only available to administrators with Super\_User access

### System Settings > Event Log

Last 1 Hour ▾ 14:08:37 to 15:08:36								
Add Filter								
#	Date/Time	Device ID	Sub Type	User	Message	Operation	Performed On	
1	15:08:13	FAZ-VM0000065040	system	admin	User 'admin' with profile 'Super_User' lo...	login	GUI(10.0.1.10)	
2	15:07:46	FAZ-VM0000065040	system	adamin	User 'adamin' login failed from GUI(10.0...	login failed	GUI(10.0.1.10)	
3	15:07:35	FAZ-VM0000065040	system	aduser2	User 'aduser2' with profile 'Standard_Us...	logout	GUI(10.0.1.10)	
4	15:07:22	FAZ-VM0000065040	system	aduser2	User 'aduser2' with profile 'Standard_Us...	login	GUI(10.0.1.10)	
5	15:07:11	FAZ-VM0000065040	system	aduser1	User 'aduser1' with profile 'Standard_Us...	logout	GUI(10.0.1.10)	
6	15:05:30	FAZ-VM0000065040	system	aduser1	User 'aduser1' with profile 'Standard_Us...	login	GUI(10.0.1.10)	

FortiAnalyzer audits administrator activity, so you can source changes to an individual.

You can view the local event log messages, such as configuration changes and logins, on the **Event Log** page. To fine-tune the results, you can add filters. For example, to view local events performed by a specific administrative user, filter by user name.

**DO NOT REPRINT**  
© FORTINET

## Monitoring Tasks

- View the tasks FortiAnalyzer administrators have performed, including progress and status
  - By default, available only to administrators with Super\_User access

System Settings > Task Monitor

	ID	Source	Description	User	Status	Time Used	ADOM	Start Time
<input type="checkbox"/>	25	Device Manager	dvmdb adom ADOM1 object member	 admin	 Success: 1	2s	ADOM1	Wed Aug 18 2021 1:46:52 PM
<input type="checkbox"/>	24	Device Manager	dvmdb adom ADOM1	 admin	 Success: 1	3s	N/A	Wed Aug 18 2021 10:50:58 AM
<input type="checkbox"/>	23	Device Manager	Delete Device	 admin	 Success: 1	1s	N/A	Wed Aug 18 2021 10:50:39 AM
<input type="checkbox"/>	22	Device Manager	Delete Device	 admin	 Success: 1	<1s	N/A	Wed Aug 18 2021 10:50:31 AM
<input type="checkbox"/>	21	Device Manager	dvmdb adom NEW object member	 admin	 Success: 1	3s	N/A	Wed Jun 16 2021 10:18:20 PM
<input type="checkbox"/>	20	Device Manager	dvmdb adom ADOM1 object member	 admin	 Success: 1	2s	N/A	Wed Jun 16 2021 10:12:50 PM

The **Task Monitor** page allows you to view administrator tasks, as well as the progress and status of those tasks.

**DO NOT REPRINT**  
**© FORTINET**

## Monitoring FortiGate Administrator Logins

- Monitor FortiGate administrator logins, system activity, and failed authentications

FortiView > System > Failed Authentication Attempts

FortiGate logging settings must be configured to log events and to send them to FortiAnalyzer!



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

18

FortiAnalyzer also allows you to monitor FortiGate administrative login activity through FortiView.

The **Failed Authentication Attempts** page shows failed login attempts, and includes the source IP of the login, the login type, the interface, and the number of failed login attempts.

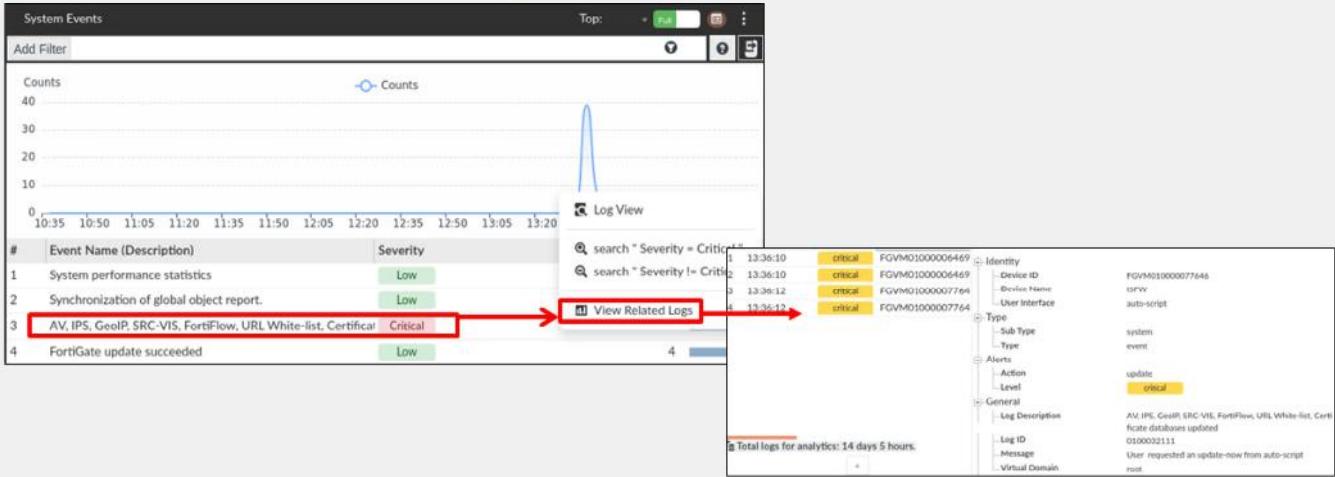
The **FortiView > System > Admin Logins** page (not shown on this slide) shows logins, failed logins, login duration, and configuration changes.

**DO NOT REPRINT**  
**© FORTINET**

## Monitoring FortiGate Administrator Activity

- Monitor FortiGate system activity

FortiView > System > System Events



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

19

Finally, FortiAnalyzer allows you to monitor FortiGate administrative activity using FortiView.

The **System Events** page shows all system and administrator-invoked events. To see more details about an event type, right click on it and select **View Related Logs** to go to the corresponding section in **LogView** where more information is available.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. In order to view FortiGate event logs on FortiAnalyzer, what configuration is required?
  - A. FortiGate must be registered to the root ADOM
  - B. FortiGate logging settings must have event logging enabled
  
2. If an administrative user's job description requires them to manage devices but not system settings, what is the most appropriate default administrator profile to assign?
  - A. Super\_User
  - B. Standard\_User

**DO NOT REPRINT****© FORTINET**

## Lesson Progress



Administrative Access Controls



Monitoring Administrative Events and Tasks



High Availability



Administrative Domains (ADOMs)



RAID

Good job! You now understand how to monitor administrative events and tasks.

Next, you will learn about how to configure high availability (HA) on FortiAnalyzer devices.

**DO NOT REPRINT****© FORTINET**

## High Availability (HA)

### Objectives

- Understand FortiAnalyzer HA
- Configure high availability
- Understand HA synchronization and load balancing
- Upgrade an HA cluster's firmware
- Verify the normal operation of an HA cluster

After completing this section, you should be able to achieve objectives shown in the slide.

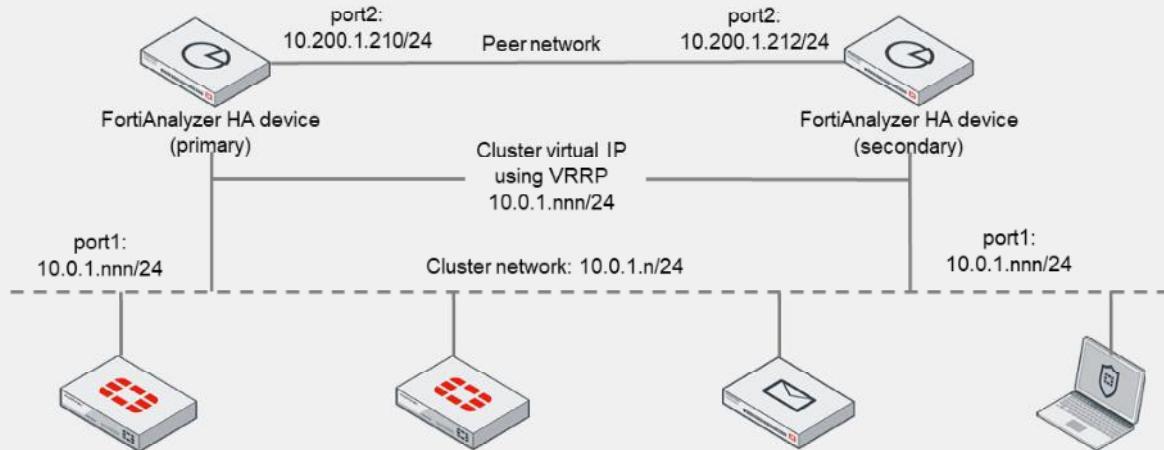
By demonstrating competence in the configuration and troubleshooting of HA, you will be able to increase the availability of your FortiAnalyzer implementation.

# DO NOT REPRINT

## © FORTINET

## High Availability (HA)

- FortiAnalyzer supports HA which provides the following:
  - Real-time redundancy in case of primary device failure
  - Synchronizes logs and data between members of the HA cluster
  - Alleviates the load on the primary device by load balancing some processes on secondary devices



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

23

FortiAnalyzer HA cluster provides the following:

- Provides real-time redundancy when the FortiAnalyzer primary device fails. If the primary device fails, another device in the cluster is selected as the primary device.
- Synchronizes logs and data securely among multiple FortiAnalyzer devices. System and configuration settings applicable to HA are also synchronized.
- Alleviates the load on the primary device by using secondary devices for processes such as running reports.

FortiAnalyzer HA cluster can have a maximum of four devices: one primary device with up to three secondary devices. All devices in the cluster must be of the same FortiAnalyzer series and firmware and be visible to each other on the network. All devices must run in the same operation mode: analyzer or collector.

Although the available disk space doesn't need to match, it is important to ensure all cluster members have enough storage for the expected logs. It's recommended that all members have the same available storage.

When using FortiAnalyzer VMs as cluster members, all VMs must be running in the same platform. For example, a VM running on VMware can't form a cluster with a VM running in KVM.

FortiAnalyzer HA implementation works only in networks where Virtual Router Redundancy Protocol (VRRP) is permitted. Therefore it may not be supported by some public cloud infrastructures.

When FortiAnalyzer devices with different licenses are used to create an HA cluster, the license that allows for the smallest number of managed devices is used.

# DO NOT REPRINT

## © FORTINET

### HA Options

- FortiAnalyzer has two HA operation modes:
  - High Availability (a-p mode)
  - Standalone
- You can configure high availability in FortiAnalyzer **System Settings**

**System Settings > HA**

Cluster Settings	
Operation Mode	<input checked="" type="radio"/> High Availability
Preferred Role	<input checked="" type="radio"/> Primary
Cluster Virtual IP	port1
Interface	port1
IP Address	10.0.1.211
Cluster Settings	
Peer IP and Peer SN	10.0.1.212 FAZ-VMTM19008187
Group Name	FAZHA
Group ID	1 (1-255)
Password	*****
Heart Beat Interval	1 Seconds
Failover Threshold	
Priority	100 (80-120)
Log Data Sync	<input checked="" type="checkbox"/>

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

In **System Settings > HA**, use the **Cluster Settings** section to create or change the HA configuration. To configure a cluster, set the **Operation Mode** of the primary device to **High Availability**. Select the preferred role for the device when it joins the HA cluster.

In the **Cluster Virtual IP** section, you need to select the interface, and type the IP address for which the FortiAnalyzer device is to provide redundancy. This is the IP that other devices need to point to send their logs once the cluster is up.

Next, you add the IP addresses and serial numbers of each secondary device to the primary device peer list. The IP address and serial number of the primary device and all secondary devices must be added to each secondary device. Cluster members need to be reachable at these IP addresses for the heartbeat packets. As shown on the previous slide, these IP addresses don't have to be on the same subnet as the cluster virtual IP.

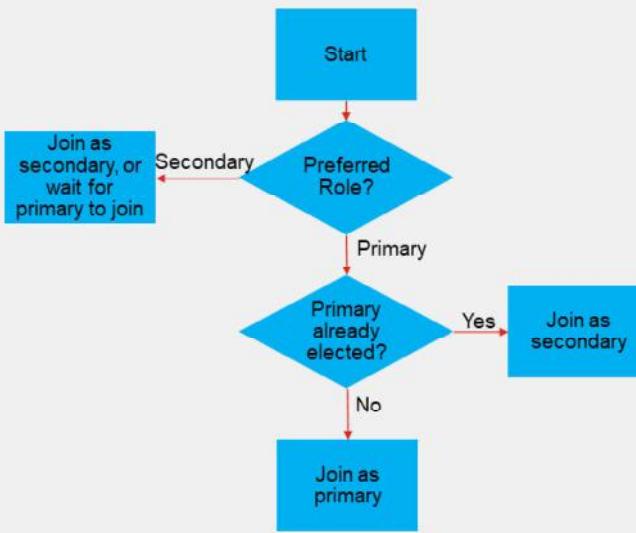
The primary device and all secondary devices must have the same **Group Name**, **Group ID**, and **Password**. The **Priority** setting determines the selection of primary devices. You can assign from 80 to 120, where a higher number has higher priority. The **Log Data Sync** option is enabled by default. It provides real-time log synchronization among cluster members, after the initial log synchronization.

# DO NOT REPRINT

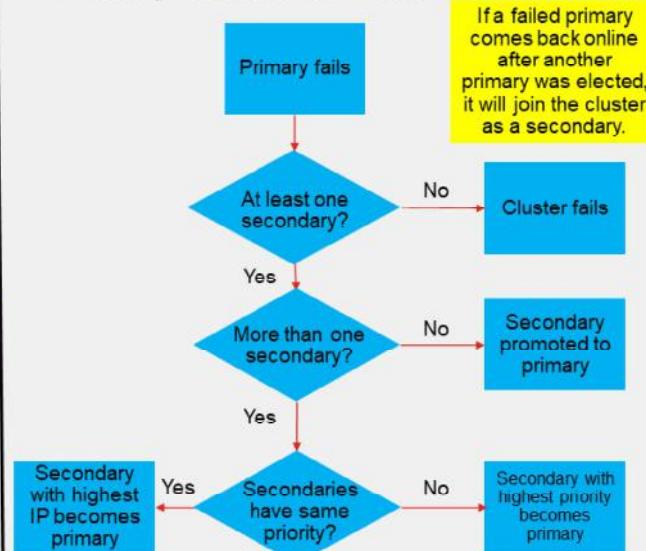
## © FORTINET

## HA Primary Election Process

- Initial primary election



- Primary election after failure



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

25

The initial selection of the primary device is based on the preferred role configured. If the preferred role is **Primary**, then this device becomes the primary device if it is configured first in a new HA cluster. If there is an existing primary device, then this device becomes a secondary device. The default role is **Secondary**, so that the device can synchronize with the primary device. A secondary device cannot become a primary device until it is synchronized with the current primary device.

In the case of a primary device failure, FortiAnalyzer HA uses the following rules to select a new primary:

- All cluster devices are assigned a priority from 80 to 120. The default priority is 100. If the primary device becomes unavailable, the device with the highest priority is selected as the new primary device. For example, a device with a priority of 110 is selected over a device with a priority of 100.
- If multiple devices have the same priority, the device whose primary IP address has the greatest value is selected as the new primary device. For example, 123.45.67.124 is selected over 123.45.67.123.
- If a new device with a higher priority or a greater value IP address joins the cluster, the new device does not replace (or pre-empt) the current primary device automatically.

By default, the only parameter checked to trigger an automatic failover is the network reachability among the cluster members. You can optionally configure HA to check the status of the Postgres database process to initiate a failover if that process stops working. This is done with the commands:

```
FAZ#configure system ha
(ha)#set healthcheck DB
(ha)#end
```

**DO NOT REPRINT****© FORTINET**

## HA Synchronization

- FortiAnalyzer HA synchronizes logs in two states:
  - Initial synchronization (Initial Sync)
  - Real-time synchronization (Log Data Sync)
- FortiAnalyzer HA synchronizes the configuration of the following modules:
  - Device Manager, Incidents and Events, Reports, and most System Settings

System Settings	Configuration synchronized
Dashboard > System Information	Only ADOM widget is synchronized
All ADOMs	Yes
Admin	Yes
Certificates > CA Certificates	Yes
Certificates > CRL	Yes
Log Forwarding	Yes
Task Monitor	Yes
Advanced > Mail Server	Yes
Advanced > Syslog Server	Yes

To ensure logs are synchronized among all HA devices, FortiAnalyzer HA synchronizes logs in two states: initial synchronization and real-time synchronization.

**Initial synchronization:** The primary device synchronizes its logs with new devices added to the cluster. After initial synchronization is complete, the secondary device automatically reboots and rebuilds its log database with the synchronized logs. You can see the status in the Cluster Status pane **Initial Logs Sync** column

**Real-time synchronization:** After the initial log synchronization, the HA cluster goes into the real-time log synchronization state. **Log Data Sync** is enabled by default for all devices in the HA cluster. When **Log Data Sync** is enabled in the primary device, the primary device forwards logs in real time to all secondary devices. This ensures that the logs in the primary and secondary devices are synchronized. If the primary device fails, the secondary device selected to be the new primary device continues to synchronize logs with secondary devices. If you want to use a FortiAnalyzer device as a standby device (not as a secondary), then you don't need real-time log synchronization, so you can disable **Log Data Sync**.

Configuration synchronization provides redundancy and load balancing among the cluster devices. A FortiAnalyzer HA cluster synchronizes the configuration of the following modules to all cluster devices:

- Device Manager
- Incidents and Events
- Reports
- Most System Settings

FortiAnalyzer HA synchronizes most system settings in the HA cluster. The table on this slide shows some of the settings that are synchronized. Refer to the *FortiAnalyzer Administration Guide* for the complete list.

**DO NOT REPRINT****© FORTINET**

## HA Load Balancing and Firmware Upgrade

- FortiAnalyzer supports load balancing
- Improves performance of following modules:
  - Reports
  - FortiView
- To upgrade FortiAnalyzer HA cluster firmware:
  1. Log in to each secondary device.
  2. Upgrade the firmware of all secondary devices.
  3. Wait for the upgrades to complete and verify that all secondary devices joined the cluster.
  4. Verify that logs on all secondary devices are synchronized with the primary device.
  5. Upgrade the primary device.

When the primary device is upgraded, it automatically becomes a secondary device. One of the secondary devices is automatically selected to be the new primary device. This allows the HA cluster to continue operating during the upgrade process.

The FortiAnalyzer HA cluster can also balance the load and improve overall performance. Load balancing enhances the following modules:

- Reports
- FortiView

When generating multiple reports, the loads are distributed to all HA cluster devices in a round-robin fashion. When a report is generated, the report is synchronized with other devices so that the report is visible on all HA device members. Similarly, for FortiView, cluster devices share some of the load when these modules generate output for their widgets.

Like upgrading the firmware of a standalone FortiAnalyzer device, normal FortiAnalyzer operations may cause temporary interruptions while the cluster firmware upgrades. Because of these interruptions, you should upgrade the cluster firmware during a maintenance period. The steps to upgrade HA cluster firmware are shown on this slide.

Note that you might not be able to connect to the FortiAnalyzer GUI until the upgrade synchronization process is complete. During the upgrade, using SSH or telnet to connect to the CLI might be slow. If necessary, use the console to connect to the CLI.

**DO NOT REPRINT**  
**© FORTINET**

## HA Monitoring and Troubleshooting

- **Cluster Status** monitors the status of the FortiAnalyzer devices in an HA cluster
- Displays information about each cluster device

### System Settings > HA

Cluster Status								Search
	Role	Serial Number	IP	Host Name	Uptime/Downtime	Initial Logs Sync	Configuration Sync	Message
<input type="checkbox"/>	Primary	FAZ-VM0000065040	10.0.1.210	FortiAnalyzer	▲ 29s ▼ 04h 10m 08s	- Down	<span style="color: green;">✓</span> Config will be synced to secondaries <span style="color: orange;">✗</span> Down	
<input type="checkbox"/>	Secondary	FAZ-VMTM19008187	10.0.1.212					connect failed

- You can use the following CLI commands to diagnose HA:

```

diagnose ha status (Shows HA status)
diagnose ha stats (Shows HA statistics)
diagnose ha dump-datalog (Dump HA data log)
diagnose ha failover (Run on master, force HA failover)
diagnose ha force-cfg-resync (Force HA to re-sync configuration)
diagnose ha load-balance (Shows HA load balance status)
diagnose ha restart-init-sync (Run on master, restart HA initial sync)

```

The **Cluster Status** pane monitors the status of FortiAnalyzer devices in an HA cluster. This pane displays information about the role of each cluster device, the HA status of the cluster, and the HA configuration of the cluster. The following information is displayed:

- **Role**
- **Serial Number**
- **IP**
- **Host Name**
- **Uptime/Downtime**
- **Initial Logs Sync**
- **Configuration Sync**
- **Message**

You can use the CLI command `diagnose ha status` to display the same HA status information. This slide also shows other useful CLI diagnosis commands to monitor and troubleshoot HA.

The image on the slide is only for demonstration purposes. It was intentionally taken on a misconfigured HA cluster to illustrate some errors you might experience in a similar case.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Which value is checked first when selecting a new primary device in the event of a FortiAnalyzer HA failure?  
 A. Device IP address  
 B. Device priority
  
2. Which of these modules does a FortiAnalyzer HA cluster synchronize during configuration synchronization?  
 A. Reports  
 B. Network

**DO NOT REPRINT****© FORTINET**

## Lesson Progress



Administrative Access Controls



Monitoring Administrative Events and Tasks



High Availability



Administrative Domains (ADOMs)



RAID

Good job! You now understand how to configure HA on FortiAnalyzer.

Next, you will learn about administrative domains, known as ADOMs.

DO NOT REPRINT  
© FORTINET

## Administrative Domains (ADOMs)

### Objectives

- Enable and create administrative domains (ADOMs)

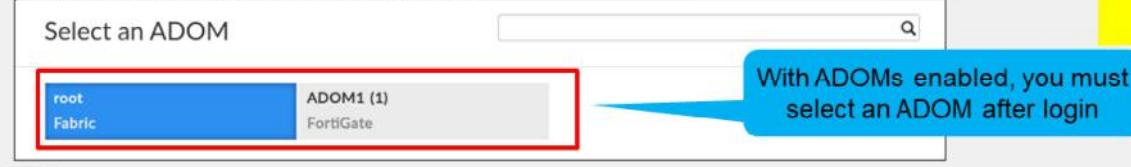
After completing this section, you should be able to achieve objective shown in the slide.

By demonstrating competence in ADOMs, you will be able to group devices for administrators to monitor and manage. You will also be able to manage data policies and disk space allocation more efficiently.

**DO NOT REPRINT**  
**© FORTINET**

## Enabling ADOMs

- Enabled or disabled in CLI or GUI
  - Required if you want to register a non-FortiGate device on FortiAnalyzer
- # config system global  
    set adom status {enable | disable }  
End
- Maximum number of ADOMs depends on the FortiAnalyzer model
- Once enabled, must select an ADOM from all your configured ADOMs



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

32

ADOMs are not enabled by default. By default, only administrators with **Super\_User** access can enable and configure ADOMs. ADOMs are required if you want to register a non-FortiGate device on FortiAnalyzer.

You can enable or disable ADOMs in the GUI through **System Settings** or the CLI with the command config system global.

After you enable ADOMs, the system logs you out so it can reinitialize with the new settings. The maximum number of ADOMs you can enable varies by FortiAnalyzer model.

After you log in with ADOMs enabled, you must select the ADOM you want to view from the list of configured ADOMs.

DO NOT REPRINT  
© FORTINET

## How ADOMs Operate with FortiGate VDOMs

- Global ADOM configuration can operate in Normal mode (default) and Advanced mode
- **Normal:** Cannot assign VDOMs from the same FortiGate device to multiple FortiAnalyzer ADOMs. All VDOMs must be assigned to a single ADOM.
  - Must assign the FortiGate device and all of its VDOMs to a single ADOM
- **Advanced:** Can assign VDOMs from the same FortiGate device to multiple FortiAnalyzer ADOMs
  - Allows you to use the **FortiView**, **Event Management**, and **Reports** functions to analyze data for individual VDOMs

### System Settings > Advanced > Advanced Settings



```
# config system global
    set adom-mode {advanced | normal}
end
```

A global ADOM configuration can operate in either Normal mode, which is the default mode, or Advanced mode.

In Normal mode, you *cannot* assign virtual domains (VDOMs) from the same FortiGate device to multiple FortiAnalyzer ADOMs. You must assign the FortiGate device, and all of its VDOMs, to a single ADOM.

In Advanced mode, you can assign VDOMs from the same FortiGate device to multiple FortiAnalyzer ADOMs. This mode allows you to use the **FortiView**, **Event Management**, and **Reports** functions to analyze data for individual VDOMs. Advanced mode results in more complicated management scenarios.

# DO NOT REPRINT

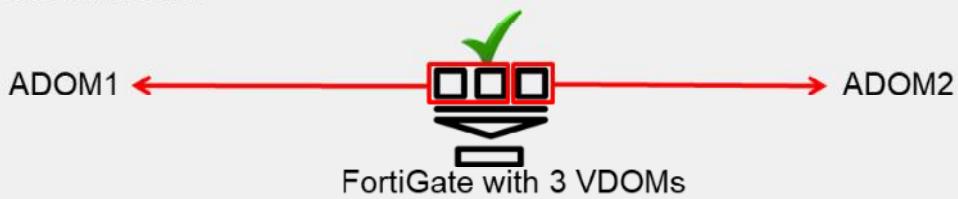
## © FORTINET

### How ADOMs Operate with FortiGate VDOMs (Contd)

- **Normal Mode:**



- **Advanced Mode:**



The image on this slide shows two scenarios, each consisting of a FortiGate unit with three VDOMs configured.

On the top, when using normal mode, is not possible to assign different VDOMs to different ADOMs.

On the bottom, when using advanced mode, each VDOM can be assigned to different ADOMs.

# DO NOT REPRINT

# © FORTINET

## Creating an ADOM

- Create new ADOMs if default ADOMs do not fit requirements
  - Devices can be registered to their *device-specific* ADOMs only
- Disk quota configured per ADOM (not per device)
- You cannot delete a custom ADOM if a device is still assigned to it

The screenshot shows two windows side-by-side. On the left is the 'System Settings > All ADOMs' page, which lists various ADOMs including 'root' (Fabric type, 4.9 GB allocated storage) and several 'FortiGate' entries under 'FortiGate (3)'. A blue callout points to this list with the text 'View configured ADOMs'. On the right is the 'Create ADOM' dialog box. It has fields for 'Name' (set to 'ADOM1') and 'Type' (set to 'FortiGate'). Below these are sections for 'Description', 'Devices' (with a sub-section for 'Select Device'), 'Data Policy' (with fields for 'Keep Logs for Analytics' and 'Keep Logs for Archive'), and 'Disk Utilization' (with fields for 'Allocated' storage, 'Analytics: Archive' usage, and 'Alert and Delete When Usage Reaches'). A red arrow points from the 'Create New' button on the left to the 'Name' field on the right. A blue callout points to the 'Configure disk quota' section on the right with the text 'Configure disk quota'.

# diagnose dvm admom list

NSE Training Institute © Fortinet Inc. All Rights Reserved. 35

On the **All ADOMs** page, you can see all configured ADOMs, as well as the default ADOMs for all non-FortiGate devices. If the default ADOMs do not fit your requirements, you can create your own.

The ADOM type you create must match the device type you are planning to add. For example, if you want to create an ADOM for a FortiGate, you must select FortiGate as the ADOM type. By default, the ADOM type is set to Fabric for the root ADOM or when creating new ADOM.

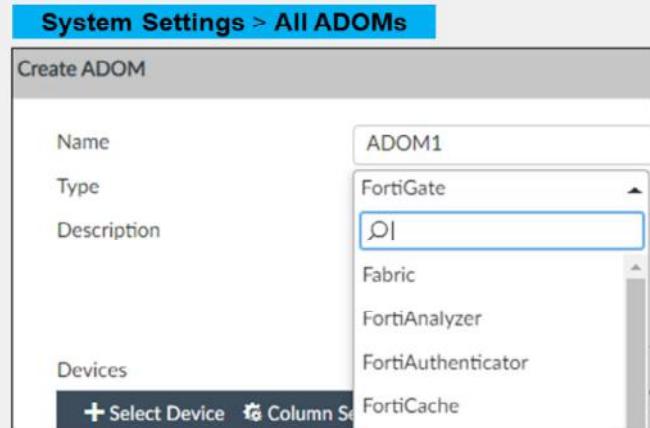
During the creation of a new ADOM, you can set the disk quota. This quota is assigned to the ADOM, and **not** the individual devices added to it. By default, the **Maximum Allowed** disk quota is set to 50 GB.

Note that you cannot delete default ADOMs. You also cannot delete custom ADOMs with assigned devices until you remove all devices from that ADOM.

**DO NOT REPRINT****© FORTINET**

## Security Fabric ADOM

- FortiAnalyzer supports Fabric ADOMs
- Can contain all devices in a security fabric in the same ADOM
- Security Fabric ADOM allows for:
  - Fast data processing
  - Log correlation
- Combines results to be presented in:
  - Reports
  - FortiView
  - Incidents & Events/ FortiSoC
  - Device Manager
  - LogView



In FortiAnalyzer, all Fortinet devices in a Security Fabric can be placed in the same ADOM.

This allows for fast data processing, log correlation and enables combined results to be presented in **Device Manager**, **LogView**, **Incidents & Events/FortiSoC**, and **Reports** panes.

After a Fabric ADOM is created, it is listed under the **Security Fabric** section of **All ADOMs**.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. Disk quota is assigned to the <fill in the blank>.  
 A. ADOM  
 B. Device
2. Which statement about ADOM Advanced mode is true?  
 A. You must assign FortiGate and all its VDOMs to a single ADOM.  
 B. You can assign FortiGate VDOMs from a single device to multiple FortiAnalyzer ADOMs.

**DO NOT REPRINT****© FORTINET**

## Lesson Progress



Administrative Access Controls



Monitoring Administrative Events and Tasks



High Availability



Administrative Domains (ADOMs)



RAID

Good job! You now understand ADOMs.

Next, you will learn about redundant array of independent disks (RAID) and how it applies to FortiAnalyzer.

# DO NOT REPRINT

## © FORTINET

### RAID

#### Objectives

- Configure RAID
- Troubleshoot RAID

After completing this section, you should be able to achieve objectives shown in the slide. By demonstrating competence in RAID, you will be able to better safeguard your logs while they are stored locally on FortiAnalyzer.

**DO NOT REPRINT****© FORTINET**

## Protecting Log Information Through RAID

- RAID is a high-performance storage solution
  - Stands for redundant array of independent disks
- Provides redundancy (a copy) of *log data* (depending on RAID level used)
  - Different from a log backup
- Not supported on all models (check device specifications)
- Combines multiple equal-sized disk drives into a logical unit
  - Data is distributed in different ways—determined by RAID level
- Requires multiple identical drives
- RAID is not a replacement for backing up your logs
  - You should still make log backups even if you employ RAID

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

40

Administering and managing your system also includes protecting your log information. This can include introducing redundancy for your log data by making a copy of your logs should your system stop running. The most commonly used method for high performance storage is RAID. RAID is not supported by all FortiAnalyzer models.

RAID combines two or more physical drives into a single logical drive.

RAID enables you to distribute your data among multiple hard drives. RAID distributes data across drives in different ways, referred to as RAID *levels*. The level you select depends on your goal. Each level provides a different balance of reliability, availability, performance, and capacity.

You can configure most devices in many types of RAID arrays. To set up a RAID array, you must have multiple (at least two) drives that are the same size.

Note that RAID is not a replacement for backing up your logs. You should still back up your logs, even if you employ RAID.

**DO NOT REPRINT****© FORTINET**

## RAID Operation Types

- Basic RAID has two types of operation:
  - Mirroring: Makes identical copies of the data on two (or more) separate physical drives
  - Striping: Combines two or more drives into a single logical drive and stores data in chunks across all drives
- Minimum RAID is a mirror or stripe of two drives
- Not all RAID levels behave the same way:
  - Some do mirror only, others stripe only, others do both, and some include parity (distributed)
  - Some can handle one failed drive, others two
  - *Too many failed drives results in the loss of all data*
- RAID can be hardware-based, or software-based:
  - Hardware RAID is recommended. Dedicated controller card handles all storage operations. Best performance
  - Software RAID is not recommended. The OS handles all operations, which affects its performance

Basic RAID has two types of operation: mirroring and striping.

With mirroring, instead of writing the files to a single hard drive, it writes them to another hard drive as well. This way you have a real-time copy of the data.

With striping, two or more drives are combined into a single logical drive. When data is stored on the logical drive, it gets split into pieces and distributed across all the physical drives in the array.

It is important to note that not all RAID levels operate the same way. Some do only mirroring, others do only striping, and some do both.

There are also versions that include distributed parity, which is a way to achieve data redundancy. With distributed parity, parity data is distributed among multiple drives and requires three or more disks (RAID 5 and above). Also, the number of drives that can fail depends on the RAID level. Regardless of the level, too many failed drives results in the loss of data.

Depending on the device model, you can build hardware RAID and/or software RAID.

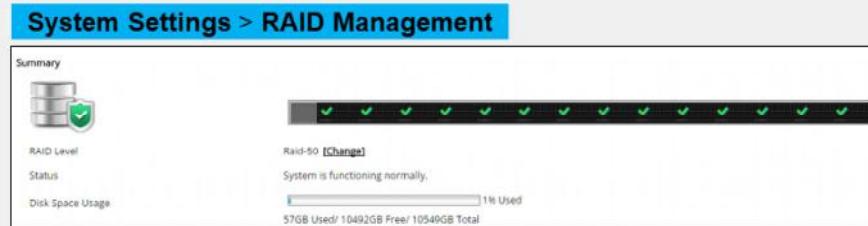
Hardware RAID is always recommended because a dedicated controller card handles all the RAID operations faster and more efficiently.

Software RAID means that the OS needs to handle all RAID operations on top of all its regular functions. This affects performance; therefore it is not recommended unless it is the only option.

**DO NOT REPRINT**  
**© FORTINET**

## Configuring RAID Levels

- Not all FortiAnalyzer models support RAID
  - Check the model specifications
- Supported RAID levels (depends on model):
  - Linear
  - RAID 0
  - RAID 1
  - RAID 1 + spare
  - RAID 5
  - RAID 5 + spare
  - RAID 6
  - RAID 6 + spare
  - RAID 10
  - RAID 50
  - RAID 60



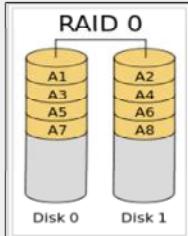
Not all FortiAnalyzer models support RAID, so the menu option to configure RAID may not appear on the GUI. Be sure to check the model specifications to see if RAID is supported, and to what level.

If RAID is supported, you can configure RAID on the **RAID Management** page. Supported levels include Linear, RAID 0, RAID 1, RAID 1 + spare, RAID 5, RAID 5 + spare, RAID 6, RAID 6 + spare, RAID 10, RAID 50, and RAID 60.

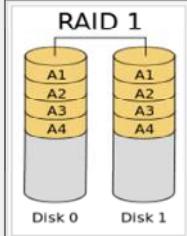
# DO NOT REPRINT

## © FORTINET

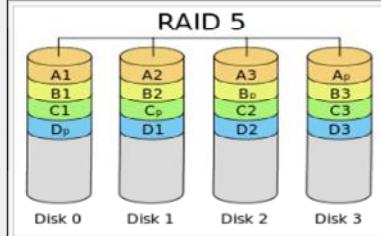
## RAID Levels 0, 1, 5, and 6



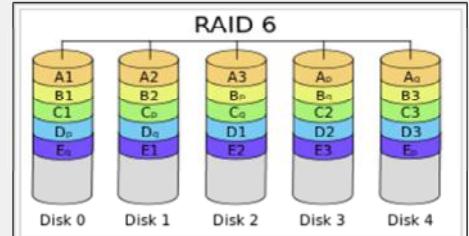
Striping  
Example: RAID 0 with two 1-TB disks provides 2 TB of space



Mirroring  
Example: RAID 1 with two 1-TB disks provides 1 TB of space



Distributed parity  
Example: RAID 5 with four 1-TB disks provides 3 TB of space



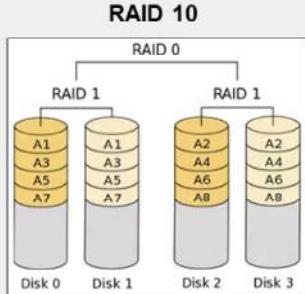
Dual parity  
Example: RAID 6 with five 1-TB disks provides 3 TB of space

Some common RAID levels are: RAID 0 (striping), RAID 1 (mirroring) and its variants, RAID 5 (distributed parity), RAID 6 (double parity), RAID 50 (striping and distributed parity), and RAID 60 (striping and distributed double parity):

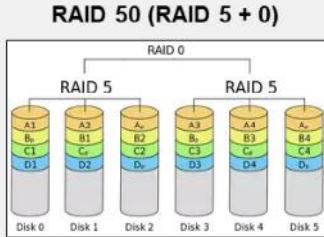
- RAID 0 consists of data split evenly across two or more disks. Speed and performance are the main goals. There is no parity information or data redundancy. This means that there is no fault tolerance; if one disk fails, it affects the entire array and the data is lost.
- RAID 1 consists of an exact copy of a set of data on two (most common) or more disks. Read performance and reliability are the main goals. RAID 1 includes fault tolerance, so if one disk fails the other one can keep working since it contains a complete copy of the data.
- RAID 5 consists of block-level striping with distributed parity. Data and parity are striped across three or more disks. This RAID level provides better performance than mirroring as well as fault tolerance. It can withstand the failure of a single drive, as subsequent reads can be calculated from the distributed parity, so that no data is lost.
- RAID 6 extends RAID 5 by adding another parity block. Accordingly, it consists of block-level striping with two parity blocks distributed across all member disks. It's more robust than RAID 5, as the system can remain operational even if two disks fail.

**DO NOT REPRINT**  
**© FORTINET**

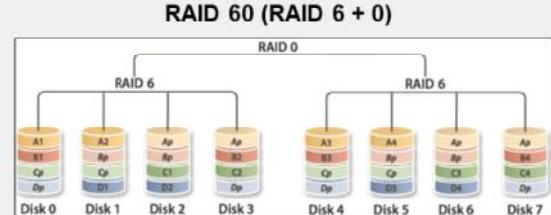
## RAID Levels 10, 50, and 60



Mirroring + striping  
Example: RAID 10 with four 1-TB disks provides 2 TB of space



Striping + distributed parity  
Example: RAID 50 with six 1-TB disks provides 4 TB of space



Striping + distributed double parity  
Example: RAID 60 with eight 1-TB disks provides 4 TB of space

- RAID 10 combines the features of RAID 1 and RAID 0, making sure data is mirrored and spread across multiple disks. RAID 10 balances performance and data security. It's possible to recover data if two drives in a RAID 10 configuration fail, but it's dependent upon which two drives fail.
- RAID 50 combines block-level striping of RAID 0 with the distributed parity of RAID 5. Write performance is improved over RAID 5 and it provides better fault tolerance than a single RAID 5 level. With this level, one drive from each of the RAID 5 sets can fail.
- RAID 60 combines block-level striping of RAID 0 with the distributed double parity of RAID 6. Write performance is affected, but the enhanced redundancy provides peace of mind. Dual parity allows the failure of two disks in each RAID 6 array.

For more information about RAID levels, see the *FortiAnalyzer Administration Guide*.

Source: Wikipedia, standard RAID levels, and nested RAID levels

**DO NOT REPRINT**  
**© FORTINET**

## Viewing RAID Status

- View RAID disk status and disk usage
- Disk status can be one of the following:
  - **Ready:** Functioning normally
  - **Rebuilding:** Writing data to a newly added hard drive to restore logical drive to an optimal state. Not fully fault tolerant until rebuilding is complete!
  - **Initializing:** Writing to all the hard drives in the device in order to make the array fault tolerant
  - **Verifying:** Ensuring the parity data of a redundant drive is valid
  - **Degraded:** Hard drive is no longer being used by the RAID controller
  - **Inoperable:** One or more drives are missing —the drive is no longer available to the operating system  
*Data in an inoperable state cannot be accessed!*

System Settings > RAID Management

Disk Number	Disk Status	Size(GB)	Disk Model
0	✓	894	SAMSUNG MZTNV800HAGP-000000
1	✓	894	SAMSUNG MZTNV800HAGP-000003
2	✓	894	SAMSUNG MZTNV800HAGP-000003
3	✓	894	SAMSUNG MZTNV800HAGP-000003
4	✓	894	SAMSUNG MZTNV800HAGP-000003
5	✓	894	SAMSUNG MZTNV800HAGP-000003
6	✓	894	SAMSUNG MZTNV800HAGP-000003
7	✓	894	SAMSUNG MZTNV800HAGP-000003
8	✓	894	SAMSUNG MZTNV800HAGP-000003
9	✓	894	SAMSUNG MZTNV800HAGP-000003
10	✓	894	SAMSUNG MZTNV800HAGP-000003
11	✓	894	SAMSUNG MZTNV800HAGP-000003
12	✓	894	SAMSUNG MZTNV800HAGP-000003
13	✓	894	SAMSUNG MZTNV800HAGP-000003
14	✓	894	SAMSUNG MZTNV800HAGP-000003

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

45

On the **RAID Management** page, you can also view the status of each disk in the RAID array and disk space usage.

Disk status can be one of the following:

- Ready
- Rebuilding
- Initializing
- Verifying
- Degraded
- Inoperable

**DO NOT REPRINT**  
© FORTINET

## Viewing RAID Failures and Hot Swapping

- View RAID failures

**System Settings > Dashboard > Alert Message Console**

- Failed disks must be replaced to keep availability and performance
- If FortiAnalyzer device supports:
  - Hardware RAID: You can replace the disk while the FortiAnalyzer is still running (*hot swapping*)
  - Software RAID: You must shut down the FortiAnalyzer prior to exchanging the hard disk (hot swapping is supported with hardware RAID only)

You can view any RAID failures on the **Alert Message Console** widget on the dashboard. A log message appears in this widget if there are any failures.

If a hard disk on a FortiAnalyzer fails, you must replace it. On FortiAnalyzer models that support *hardware* RAID, you can replace the disk while FortiAnalyzer is still running. This is known as *hot swapping*. Fortinet supports hot swapping on hardware RAID only. On FortiAnalyzer devices with *software* RAID you must shut down FortiAnalyzer prior to exchanging the hard disk.

**DO NOT REPRINT****© FORTINET**

## Diagnosing RAID

- You can check the RAID and disk status using the following commands
- These commands are available only on the hardware-based FortiAnalyzer

What to investigate...	CLI command to use...
RAID status, including RAID level, RAID status, RAID size, and hard disk information	# diagnose system raid status
RAID controller hardware information	# diagnose system raid hwinfo
SMART information	# diagnose system disk info
SMART health status	# diagnose system disk health
SMART error logs	# diagnose system disk errors
Vendor specific SMART attributes	# diagnose system disk attributes

- On FortiAnalyzer-VM, only the `diagnose system usage` command is available

Use the CLI command `diagnose system raid status` to view the health of the RAID array as well as the health of the individual disks.

Use the command `diagnose system raid hwinfo` to view detailed information about the hardware for the individual disks on FortiAnalyzer.

On FortiAnalyzer-VM, only the `diagnose system disk usage` is available.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. The RAID 10 level comprises what data format?  
A. Dual parity  
 B. Mirroring and striping
  
2. What must you do if a hard disk on a FortiAnalyzer that supports software RAID fails?  
A. Hot swap the disk  
 B. Shut down FortiAnalyzer and replace the disk

**DO NOT REPRINT****© FORTINET**

## Lesson Progress



Administrative Access Controls



Monitoring Administrative Events and Tasks



High Availability



Administrative Domains (ADOMs)



RAID

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Control or restrict administrative access using admin profiles, trusted hosts, and ADOMs
- ✓ Validate administrators using external servers
- ✓ Configure two-factor authentication
- ✓ Monitor FortiAnalyzer administrators, events, and tasks
- ✓ Monitor FortiGate administrator logins and activity
- ✓ Understand FortiAnalyzer HA configuration, synchronization, load balancing and firmware upgrade
- ✓ Enable and create ADOMs
- ✓ Configure and troubleshoot RAID

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use administration and management functions to better defend FortiAnalyzer—and the sensitive log data it stores—against external or internal threats.

**DO NOT REPRINT**  
© FORTINET



## FortiAnalyzer

### Device Registration and Communication



FortiAnalyzer 7.0

Last Modified: 1 December 2021

In this lesson, you will learn how to register devices on FortiAnalyzer for log collection, as well as how to troubleshoot communication between FortiAnalyzer and its registered devices. You will also examine FortiAnalyzer disk quota—an important condition for ensuring all logs are collected—and how to manage registered devices.

**DO NOT REPRINT****© FORTINET**

## Lesson Overview



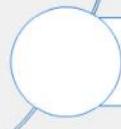
### Registering Devices



### Communication Troubleshooting



### Disk Quota



### Managing Registered Devices

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will explore the topics shown on this slide.

**DO NOT REPRINT****© FORTINET**

## Registering Devices

### Objectives

- Identify the different ways you can register a device
- Describe how device registration works with ADOMs
- View device status

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in device registration, you will be able to configure FortiAnalyzer to collect logs from registered devices.

DO NOT REPRINT  
© FORTINET

## Methods of Device Registration

- Two types of devices:
  - Registered: devices *authorized* to store logs on FortiAnalyzer
  - Unregistered: devices *requesting* to store logs on FortiAnalyzer

### Method 1: Request from a supported device

1. The administrator of the supported device requests registration
2. The FortiAnalyzer administrator accepts (or denies) the request

### Method 2: Using the Add Device wizard with serial number

1. The FortiAnalyzer administrator uses the **Add Device** wizard to add the device based on its serial number
2. If the device is supported and the details are correct, the device is added and automatically registered after the request is sent from the device

For FortiAnalyzer to start collecting logs from a device, that device must become a registered on FortiAnalyzer.

To FortiAnalyzer, there are only two types of devices: those that are registered and those that are unregistered.

A registered device is one that has been *authorized* to store logs on FortiAnalyzer, whereas an unregistered device is one that is *requesting* to store logs on FortiAnalyzer.

There are three ways you can register a device with FortiAnalyzer.

The first method involves a request for registration from a supported device. When the FortiAnalyzer administrator receives that request, the request is accepted (though it can be denied).

The second method involves the FortiAnalyzer **Add Device** wizard. The device can be added based on its serial number. If the device is supported, and all the details of the device are correct, the device becomes registered.

**DO NOT REPRINT**  
© FORTINET

## Methods of Device Registration (Contd)

### Method 3: Using the Add Device wizard with pre-shared key

1. The FortiAnalyzer administrator uses the **Add Device** wizard to add the device based on a pre-shared key
2. After the correct pre-shared key is configured on the device using the CLI, the device is added and automatically registered
3. Only FortiGate devices can be added using this method



```
config log fortianalyzer setting
set status enable
set server "10.0.1.210"
set serial "FAZ-VM0000065040"
set preshared-key "password"
end
```

The third method also involves the FortiAnalyzer **Add Device** wizard. The device is added using a pre-shared key. After the device is configured and the correct pre-shared key is added, it is automatically registered. The pre-shared key needs to be added from the device CLI.

Note that at the time of this writing, only FortiGate devices can be added using this method.

**DO NOT REPRINT**  
**© FORTINET**

## Methods of Device Registration (Contd)

### Method 4: Security Fabric Authorization

1. FortiAnalyzer is configured for Fabric Authorization
2. Configure the FortiAnalyzer connector in FortiGate
3. Request authorization from FortiGate on the Fortinet Security Fabric authorization window
  - The FortiGate administrator needs valid credentials in FortiAnalyzer

This method is only available when both FortiAnalyzer and FortiGate are on version 7.0.1 or higher.



The fourth method uses the Fortinet Security Fabric authorization process.

This method requires that both FortiGate and FortiAnalyzer are running version 7.0.1 or higher. It is also required that the FortiGate administrator has valid credentials to log in on FortiAnalyzer and complete the registration.

DO NOT REPRINT  
© FORTINET

## Device Registration and ADOMs

- Each device can be registered with an administrative domain (ADOM)
- Devices can be registered only with their *device-specific* ADOM type
  - For example: FortiMail device → FortiMail ADOM type
    - Administrators can register a device with the default ADOM for that device
    - Administrators can register a device with a custom ADOM they create (the custom ADOM must still be associated with the ADOM type for the specific device)
    - Cannot add different device types to the same ADOM!
- By default, ADOMs aren't enabled
  - FortiGate devices are automatically assigned to the *root* ADOM
  - Non-FortiGate devices cannot be added to FortiAnalyzer without first enabling ADOMs

Typical use case: multiple FortiGate devices assigned to a custom ADOM

Administrators can register each device with an administrative domain, known as an ADOM. However, devices can only be added to their *device-specific* ADOM type. For example, a FortiMail device can be registered only with the FortiMail ADOM type.

FortiAnalyzer includes default ADOMs for each device it supports. You can use these ADOMs or you can create your own custom ones. When you create a custom ADOM, it still must be associated with the ADOM type of the device you are planning to add to it. Note that you can't add different device types to the same ADOM, whether a default or custom ADOM.

By default, ADOMs are not enabled. Only one *root* ADOM exists, which is based on the Fabric ADOM type. As such, with ADOMs disabled, you are unable to register any non-FortiGate stand-alone device on FortiAnalyzer.

# DO NOT REPRINT

## © FORTINET

### Method 1: Request from a Supported Device - I

1. The FortiGate administrator enables remote logging to FortiAnalyzer

The screenshot shows the 'Log & Report > Log Settings' page. Under 'Remote Logging and Archiving', the 'Send logs to FortiAnalyzer/FortiManager' option is set to 'Enabled'. The 'Source Interface' dropdown is set to '10.0.1.210'. The 'IP address' field contains '10.0.1.210'. The 'Upload option' dropdown is set to 'Real Time'. The 'Allow access to FortiGate REST API' checkbox is checked. The 'Verify FortiAnalyzer certificate' checkbox is unchecked. At the bottom, the 'Connection status' is shown as 'Unauthorized' with a red exclamation mark.

2. The FortiAnalyzer administrator accepts (or denies) the registration request
  - ADOMs → Can add FortiGate to the root ADOM or a custom FortiGate ADOM

The screenshot shows the 'Device Manager (root ADOM)' page. It lists one unauthorized device: 'Local-Fortigate' (FortiGate-VM64, FGVM010000064692, 10.0.1.210). A red arrow points to the 'Authorize' button in the top navigation bar. Another red arrow points to the 'Authorize Device' dialog box below, which shows the device details and an 'OK' button.

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

8

There are two ways to initiate a request from a FortiGate device.

In the first method, FortiGate requests registration on FortiAnalyzer by enabling remote logging and specifying the FortiAnalyzer IP. This is done from the **Log & Report** section as shown on this slide.

After clicking **Apply**, and if the request reaches the FortiAnalyzer successfully, you receive a warning asking you to confirm the serial number of the FortiAnalyzer to verify it is the correct one.

Note that if you click **Test Connectivity**, you see the connection status as **Unauthorized**. This is because the FortiAnalyzer administrator has not yet accepted the *request to register*. At this stage, FortiGate is still an unregistered device.

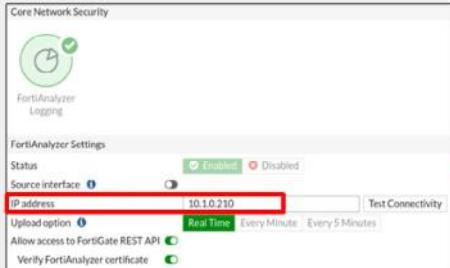
After the request is made by the supported device, it automatically appears under the root ADOM in **Device Manager**. The FortiAnalyzer administrator should review the details of the unauthorized device and, if satisfied, authorize the device.

During acceptance of the registration request, if ADOMs are enabled, you have the option of keeping FortiGate in the root ADOM, or adding it to any custom FortiGate ADOMs you may have configured as illustrated on this slide.

**DO NOT REPRINT**  
**© FORTINET**

## Method 1: Request from a Supported Device - II

1. The FortiGate administrator enables Security Fabric and FortiAnalyzer



2. The FortiAnalyzer administrator accepts (or denies) registration request

- ADOMs → Can add FortiGate(s) to the root ADOM or a custom FortiGate ADOM



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

9

Using this method, the FortiGate administrator enables the Security Fabric. By enabling the Security Fabric, **FortiAnalyzer Logging** is enabled by default. By configuring the FortiAnalyzer IP on the upstream FortiGate, all the FortiGate devices connected to the upstream FortiGate through the Security Fabric receive the configuration for FortiAnalyzer, and all the FortiGate devices connected through the Security Fabric request registration on FortiAnalyzer.

Like in the previous method, after clicking **Apply** you receive a warning asking you to confirm the serial number of the FortiAnalyzer to verify it is the correct one.

Note that if you click **Test Connectivity**, you see the connection status as **Unauthorized**. This is because the FortiAnalyzer administrator has not yet accepted the *request to register*. At this stage, FortiGate is still an unregistered device.

After the request is made by the supported device, it automatically appears under the root ADOM in **Device Manager**. The FortiAnalyzer administrator should review the details of the unauthorized device and, if satisfied, authorize the device.

During acceptance of the registration request, if ADOMs are enabled, you have the option of keeping FortiGate in the root ADOM or adding it to any custom FortiGate ADOMs you may have configured. This was illustrated on the previous slide.

Note that it is recommended to add all the FortiGate devices connected through the Security Fabric under one ADOM. However, it is possible to separate the FortiGate devices and assign them to different ADOMs.

# DO NOT REPRINT

## © FORTINET

### Method 2: Add Device Wizard Using a Serial Number

1. Add a device using **Device Manager**
  
2. Type the required device information in the wizard

- If ADOMs are enabled, the device is automatically registered to its device-specific, prebuilt ADOM
  - If you've already created a custom ADOM based on the device type you are registering, switch to the ADOM *before* adding a device using the wizard

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

10

With this method, you use the device registration wizard in the FortiAnalyzer **Device Manager**. The FortiAnalyzer administrator proactively initiates, and ultimately performs, the registration. The administrator must have the specific serial number of the device that is to be registered. If the device information is verified, the status reads “Device is added successfully”, and the device appears under **Device Manager**.

If ADOMs are enabled, the device is automatically registered to its device-specific ADOM. However, if you've already created a custom ADOM and want to add the device directly to that ADOM instead, switch to the ADOM *before* adding a device using the wizard.

# DO NOT REPRINT

## © FORTINET

### Method 3: Add Device Wizard Using a Pre-Shared Key

- Add a device using **Device Manager**

- Select **Pre-shared Key** and fill the rest of the fields as needed

- If ADOMs are enabled, the device is automatically registered to its device-specific, prebuilt ADOM
  - If you've already created a custom ADOM based on the device type you are registering, switch to the ADOM *before* adding a device using the wizard

The screenshot shows the FortiAnalyzer Device Manager interface. At the top is a header bar with 'Device Manager', 'Edit', 'Delete', 'More', 'Column Settings', and user information ('admin'). Below is a table with columns 'Device Name', 'IP Address', 'Platform', 'Logs', and 'Average Log Rate(Logs/Sec)'. A red box highlights the 'Add Device' button. The main area is titled 'Add Device' with a sub-instruction 'Please input the following information to add a device.' It has fields for 'Name' (set to 'FGT-VM'), 'Link Device By' (radio buttons for 'Serial Number' and 'Pre-shared Key' (selected)), 'Pre-shared Key' (redacted), 'Device Model' (set to 'FortiGate-VM64'), and 'Description' (empty). A 'Next' button is at the bottom right. To the right is a summary window titled 'Add Device' showing the device was added successfully with a list of status messages:

- Device is added successfully
- Creating device database
- Retrieving high availability status
- Initializing configuration database
- Updating group membership
- Successfully add device

A 'Finish' button is at the bottom right of the summary window.

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

11

With this method, you also use the **Add Device** wizard in the FortiAnalyzer **Device Manager**. The FortiAnalyzer administrator proactively initiates, and ultimately performs, the registration. The administrator must set a pre-shared key and fill in the other details about the device that is to be registered, such as the device model. If the device information is verified, the status reads “Device is added successfully”, and the device appears under **Device Manager**.

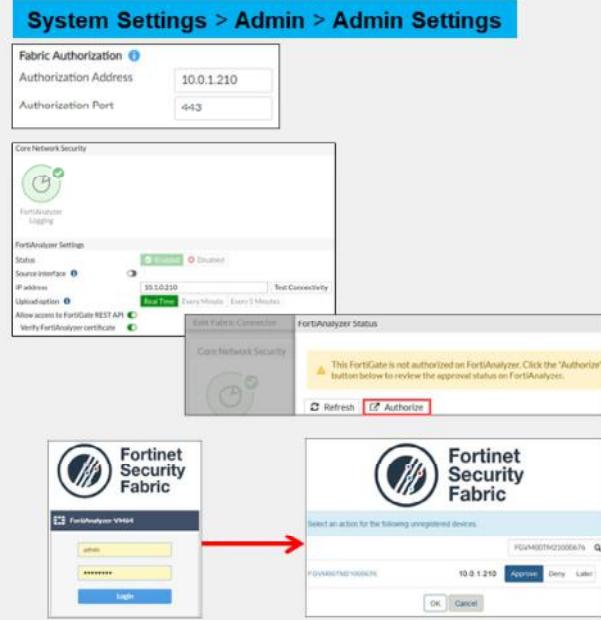
If ADOMs are enabled, the device is automatically registered to its device-specific ADOM. However, if you've already created a custom ADOM and want to add the device directly to that ADOM instead, switch to the ADOM *before* adding a device using the wizard.

The pre-shared key needs to be added from the device CLI to finish the process.

**DO NOT REPRINT**  
**© FORTINET**

## Method 4: Using Fortinet Security Fabric Authorization

1. Configure FortiAnalyzer IP and port that will accept authorizations through Fabric connectors
2. The FortiGate administrator enables Security Fabric and FortiAnalyzer
3. The Fortinet administrator initiates the authorization process using valid FortiAnalyzer credentials
4. The Fortinet administrator approves the registration from the Fortinet Security Fabric window



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

12

To use this method, you first configure FortiAnalyzer to accept authorizations through Fabric connectors. You must type which IP and port is to be used to receive the requests. By default, port 443 is used.

Next, the FortiGate administrator enables the Security Fabric to use FortiAnalyzer for logging, and then initiates the authorization process from the **FortiAnalyzer Status** window.

The FortiGate administrator must have valid credentials in FortiAnalyzer to complete the registration process. This is done by clicking **Approve** in the **Fortinet Security Fabric** window.

**DO NOT REPRINT**  
**© FORTINET**

## Viewing Device Status

- **Device Manager** lists all registered devices for that ADOM
  - Also shows log status (up or down)
  - Storage used

The screenshot shows the FortiAnalyzer Device Manager interface. At the top right, it says "ADOM: NEW" and "admin". Below the header is a toolbar with "Add Device", "Edit", "Delete", "More", and "Column Settings". The main area is a table titled "Device Manager" with columns: Device Name, IP Address, Platform, Logs, Average Log Rate(Logs/Sec), Device Storage, and Description. There are three entries:

Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage	Description
ISFW	10.0.1.200	FortiGate-VM64	Real Time	0	(0.15%)	
Local-FortiGate	10.0.1.254	FortiGate-VM64	Real Time	0	(0.52%)	

Annotations with callouts point to the following areas:

- "Log status" points to the "Logs" column.
- "Storage used" points to the "Device Storage" column.
- "Registered devices" points to the first two rows of the table.
- A yellow box contains the text: "Unregistered devices appear in the root ADOM until registered and assigned to an ADOM".

After you register various Fortinet devices, they appear on the **Device Manager** tab for that ADOM. You can also view details about the log status and used storage for that ADOM.

Unregistered devices appear under the **root ADOM** only until they are registered and assigned to an ADOM.

# DO NOT REPRINT

## © FORTINET

### Which Logs Are Collected?

Logs	DLP Archive	Quarantine	IPS Packet Log
Supported device log types: <ul style="list-style-type: none"><li>• Traffic</li><li>• Event</li><li>• Security</li></ul>	Logs information about sensitive data trying to get in or out of your network: <ul style="list-style-type: none"><li>• Email</li><li>• IM</li><li>• Web traffic</li><li>• FTP</li><li>• NNTP</li></ul>	Logs files quarantined by the device	Logs the network packets containing the traffic matching IPS signatures

FortiAnalyzer has permission to automatically collect these logs (but they must be enabled on FortiGate)

When a FortiGate device is registered, FortiAnalyzer automatically has permission to collect the following types of logs, if they are enabled on FortiGate:

- Logs: This log type details information about traffic, events, and security.
- DLP archive: This log type details information about any sensitive data trying to get in or out of your network.
- Quarantine: This log type details files that have been placed into quarantine by the device sending the logs.
- IPS Packet log: This log type details information about network packets containing the traffic matching IPS signatures.

**DO NOT REPRINT****© FORTINET**

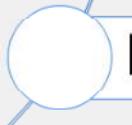
## Knowledge Check

1. Under which situation must ADOMs be enabled on FortiAnalyzer?

- A. When a FortiGate device wants to register with FortiAnalyzer
- B. When a FortiMail device wants to register with FortiAnalyzer

**DO NOT REPRINT****© FORTINET**

## Lesson Progress

**Registration Methods****Communication Troubleshooting****Disk Quota****Managing Registered Devices****NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

16

Good job! You now understand how to register a device.

Now, you will learn about ways to troubleshoot communication issues between FortiAnalyzer and your registered devices.

**DO NOT REPRINT**  
© FORTINET

## Communication Troubleshooting

### Objectives

- Troubleshoot device communication issues

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in communication troubleshooting, you will be able to efficiently troubleshoot issues that could prevent log collection.

**DO NOT REPRINT**  
**© FORTINET**

## Basic CLI Commands

- Use the following FortiAnalyzer CLI commands to check system status, performance, and hardware statistics

What to Investigate	CLI Command to Use
What is the current status of FortiAnalyzer?	# get system status
What are the performance statistics on FortiAnalyzer?	# get system performance
What are the hardware statistics for CPU, memory, disk, and RAID?	# diagnose hardware info

This slide shows some basic CLI commands that you can use to check system status, performance, and hardware statistics.

# DO NOT REPRINT

## © FORTINET

# get system status: Helpful Troubleshooting Data

```

FortiAnalyzer # get system status
Platform Type : FAZVM64
Platform Full Name : FortiAnalyzer-VM64
Version : v7.0.1-build0113 210715 (GA)
Serial Number : FAZ-VM0000065040
BIOS version : 04000002
Hostname : FortiAnalyzer
Max Number of Admin Domains : 5
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
HA Mode : Stand Alone
Branch Point : 0113
Release Version Information : GA
Current Time : Thu Aug 19 21:11:37 PDT 2021
Daylight Time Saving : Yes
Time Zone : (GMT-8:00) Pacific Time (US & Canada).
x86-64 Applications : Yes
Disk Usage : Free 486.08GB, Total 491.15GB
File System : Ext4
License Status : Valid

```

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

19

When using the `get system status` command to troubleshoot system issues, the following information can be helpful:

- **Version:** Ensure the FortiAnalyzer firmware version is compatible with the device you are registering (see the *FortiAnalyzer Release Notes* for supported firmware versions).
- **Admin Domain Configuration:** Ensure ADOMs are enabled if attempting to register a non-FortiGate device.
- **Current Time:** Ensure your date and time is set according to your needs. For many features to work, including scheduling, logging, and SSL-dependent features, the FortiAnalyzer system time must be accurate. While you can manually set the date and time, it is recommended that you synchronize with a Network Time Protocol (NTP) server.
- **Disk Usage:** Ensure you have enough free disk space to accept and store logs from registered devices.
- **License Status:** Ensure you have a valid licence. This is for a VM only.

# DO NOT REPRINT

## © FORTINET

### # get system performance: Helpful Troubleshooting Data

```
FortiAnalyzer # get sys performance
CPU:
  Used: 2.03%
  Used(Excluded NICE): 2.03%
    %used   %user   %nice   %sys   %idle   %iowait   %irq   %softirq
  CPU0    2.03    0.18    0.00    0.74    97.97    0.18    0.00    0.92
  CPU1    1.86    0.74    0.00    0.93    98.14    0.00    0.00    0.19

Memory:
  Total: 6,141,848 KB
  Used: 3,592,320 KB 58.5%
  Total (Excluding Swap): 4,044,700 KB
  Used (Excluding Swap): 2,181,380 KB 53.9%

Hard Disk:
  Total: 515,663,256 KB
  Used: 3,816,720 KB 0.7%
  Inode-Total: 32,007,680 KB
  Inode-Used: 16,543 KB 4.1%
  IOStat: tps      r_tps      w_tps      r_kB/s      w_kB/s      queue      wait_ms      svc_ms      %util      sampling_sec
          8.5       1.2       7.2       68.7        218.6       0.0        2.1        0.6        0.5        30163.83

Flash Disk:
  Total: 503,752 KB
  Used: 228,236 KB 45.3%
  Inode-Total: 32,768 KB
  Inode-Used: 38 KB 0.1%
  IOStat: tps      r_tps      w_tps      r_kB/s      w_kB/s      queue      wait_ms      svc_ms      %util      sampling_sec
          0.1       0.1       0.0       6.5        0.1        0.0        2.8        0.9        0.0        30163.83
```

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

20

When using the `get system performance` command to troubleshoot system issues, look at the used space for CPU, memory, hard disk, and flash disk. If any of these are *nearing* capacity, you may experience issues with log collection. The used capacity need not be 100% before you experience problems. For example, the space assigned to a hard disk quota is not fully available for logs, because some of it is reserved for system usage and unexpected quota overflow. Disk quota is discussed later in this lesson.

For FortiAnalyzer VMs, note that a minimum of 8 GB is recommended for the memory.

# DO NOT REPRINT

## © FORTINET

### #diagnose hardware info: Helpful Troubleshooting Data

```

FortiAnalyzer # diagnose hardware info
## CPU info
processor : 0
vendor_id : GenuineIntel
cpu family : 6
model : 142
model name : Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz
stepping : 10
microcode : 0x96
cpu MHz : 2111.999
cache size : 8192 KB
physical id : 0
siblings : 1
core id : 0
cpu cores : 1
apicid : 0
initial apicid : 0
fpu : yes
fpu_exception : yes
cpuid level : 22
wp : yes
flags : fpu vme de pse tsc msr pae mce cx8 a
bugs : cpu_meltdown spec_rte_v1 spec_rte_v2
spec_store_bypass lltf mds swapgs taa itlb_multihit
bogomips : 4223.99
clflush size : 64
cache_alignment : 64
address sizes : 42 bits physical, 48 bits virtual
power management:

```

## Memory info		## Disk info		
		major	minor	#blocks
MemTotal:	4044700 kB			name
MemFree:	397024 kB			
MemAvailable:	1591812 kB	1	0	4096 ram0
Buffers:	120344 kB	1	1	4096 ram1
Cached:	1552340 kB	1	2	4096 ram2
SwapCached:	105044 kB	1	3	4096 ram3
Active:	2299844 kB			
Inactive:	1048456 kB	7	0	10240 loop0
Active(anon):	1525480 kB	8	0	2097152 sda
Inactive(anon):	619120 kB	8	1	524288 sda1
Active(file):	768356 kB	8	16	83886080 sdb
Inactive(file):	420336 kB	8	16	83886080 sdb1
Unevictable:	122052 kB	253	0	83881984 dm-0
Locked:	122052 kB			
SwapTotal:	2097148 kB			
SwapFree:	581168 kB			
Dirty:	92 kB	N/A		
AnonPages:	1687572 kB			
Mapped:	362856 kB			
Shmem:	474968 kB			
Slab:	93180 kB	202		
SReclaimable:	41412 kB			
SUnreclaim:	51768 kB	202		
KernelStack:	6288 kB			
PageTables:	59824 kB			
NFS_Unstable:	0 kB			
CommitLimit:	4119490 kB			
Committed_AS:	22775420 kB			
VmallocTuLal:	3435573837 kB			
VmallocUsed:	0 kB			
VmallocChunk:	0 kB			
DirectMap4k:	18368 kB			
DirectMap2M:	4175872 kB			
DirectMap1G:	2097152 kB			

The `diagnose hardware info` command provides useful details about CPU, memory (RAM), and disks .

The memory and RAID sections can be very useful while troubleshooting system issues.

The `Memory info` section provides a more granular breakdown of the memory than what is provided by the `get system performance` command. For example, the total memory from `get system performance` includes the total memory plus the swap memory. The `diagnose hardware information` command shows a more detailed breakdown of all memory components.

Swap memory refers to the disk space available to use when the physical memory is full, and the system requires more memory. For a temporary period, inactive pages in memory are moved to the swap space.

If RAID is enabled and being used as a high-performance storage solution, the RAID level impacts the determination of disk size and reserved quota level.

**DO NOT REPRINT**  
**© FORTINET**

## Device and ADOM Status Check

- Use the following FortiAnalyzer CLI commands to check device and ADOM status

What to Investigate	CLI Command to Use
What devices and IPs are connecting to FortiAnalyzer?	# diagnose test application oftpd 3
What ADOMs are enabled and configured?	# diagnose dvm adom list
What devices/VDOMs are currently registered and unregistered?	# diagnose dvm device list

This slide shows the FortiAnalyzer CLI commands you can run to discover which devices and IPs are connecting to FortiAnalyzer, which ADOMs are enabled and configured, and which devices are currently registered and unregistered.

# DO NOT REPRINT

## © FORTINET

## Troubleshooting Communication Issues

- Use the following CLI commands to troubleshoot communication issues

What to Investigate	CLI Command to Use
Are the devices able to contact each other?	# execute ping
Are packets leaving FortiGate, but not reaching FortiAnalyzer? Is traffic blocked, or is there a routing issue?	# diagnose sniff packet <interface> <filter> <level> <timestampl>
Is FortiGate configured for remote logging to FortiAnalyzer?	FortiGate: # show log fortianalyzer setting
Is the FortiAnalyzer source IP address set on FortiGate?	
Are the logging filters for logs sent to FortiAnalyzer on FortiGate enabled?	
Is FortiGate capable of generating logs?	FortiGate: # diagnose log test
Is FortiAnalyzer receiving logs?	# diagnose debug application oftpd 8

 NSE Training Institute

© Fortinet Inc. All Rights Reserved.

23

If you are experiencing communication issues between other devices and FortiAnalyzer, first ensure that both devices can reach each other. Use the `execute ping` CLI command on either device to verify reachability (ping must be enabled and allowed by all intermediate firewalls).

You can also run sniffs on both devices to see if packets that leave FortiGate are reaching FortiAnalyzer. If packets are leaving FortiGate, but not reaching FortiAnalyzer, look at other devices in the network, because an intermediate router or firewall may be blocking the traffic or routing it inappropriately.

Other areas to check:

- Is FortiGate configured for remote logging to FortiAnalyzer?
- Is the FortiAnalyzer source IP set on FortiGate? This is important if FortiAnalyzer is accessed over a VPN that only allows a specific subnet.
- Are the logging filters for logs sent to FortiAnalyzer enabled on FortiGate?
- Is FortiGate capable of generating logs and can FortiAnalyzer receive them? If you don't see any logs on FortiGate, you must examine the logging issue on FortiGate before proceeding with troubleshooting the FortiAnalyzer side.

# DO NOT REPRINT

## © FORTINET

### # diagnose debug application oftpd 8

```

FortiAnalyzer # diagnose debug application oftpd 8

[OFTP_destroy_SSL_context:1898 FGVM010000064692] SSL socket[24] pid[988] ssl[0x1e2d260]
destroy_SSL_Context
[OFTP_recv_SSL_packet:1792 FGVM010000064692] SSL socket[27] pid[988] ssl[0x1d60b30] received
[12] bytes:
[oftpd_handle_session:3656 FGVM010000064692] handle KEEPALIVE (11)
[OFTP_send_SSL_packet:1852 FGVM010000064692] SSL socket[27] pid[988] ssl[0x1d60b30] sent [21]
bytes:
[OFTP_recv_SSL_packet:1792 FGVM010000064692] SSL socket[26] pid[988] ssl[0x1d4e0f0] received
[12] bytes:
[oftpd_handle_session:3656 FGVM010000064692] handle KEEPALIVE (11)
[OFTP_send_SSL_packet:1852 FGVM010000064692] SSL socket[26] pid[988] ssl[0x1d4e0f0] sent [21]
bytes:
[OFTP_recv_SSL_packet:1792 FGVM010000064692] SSL socket[26] pid[988] ssl[0x1d4e0f0] received
[12] bytes:
[OFTP_recv_SSL_packet:1792 FGVM010000064692] SSL socket[26] pid[988] ssl[0x1d4e0f0] received
[95] bytes:
[update_etags:990] FGVM010000064692 csf_group_name=Training-Lab
[on_etag_change:936] FGVM010000064692 url=/api/v2/cmdb/system/saml uid=18
etags=8e12bcf95acd7f2f1dc382e426e0e294

Local-FortiGate # diagnose log test
generating a system event message with level - warning
generating an infected virus message with level - warning
generating a blocked virus message with level - warning
generating a URL block message with level - warning
generating a DLP message with level - warning
generating an IPS log message
generating an botnet log message
generating an anomaly log message
generating an application control IM message with level -
information
generating an IPv6 application control IM message with level -
information
generating deep application control logs with level -
information
generating an antispam message with level - notification
generating an allowed traffic message with level - notice
generating a multicast traffic message with level - notice
generating an ipv6 traffic message with level - notice
generating a wanopt traffic log message with level -
notification
generating a HA event message with level - warning
generating a VOIP event message with level - information
generating authentication event messages
generating a Forticlient message with level - information
generating a URL block message with level - warning
generating a DNS message with level - warning
generating an ssh-command pass log with level - notification
generating an ssh-channel block with level - warning
generating an ssl-cert_blacklisted log with level - warning

```

You can use the following commands at the same time to troubleshoot communication issues:

Step one:

Run the following commands on FortiAnalyzer to view current log activity:

```
# diagnose debug enable
# diagnose debug application oftpd 8
```

Run the following command on FortiGate to send some test logs to FortiAnalyzer:

```
# diagnose log test
```

Review the output shown on this slide. If everything is working as expected and logs are being received, you should see some entries on the FortiAnalyzer side.

# DO NOT REPRINT

## © FORTINET

### FortiAnalyzer Temporarily Unavailable to FortiGate?

- The FortiGate *miglogd* process caches logs on FortiGate when FortiAnalyzer is not reachable
- When maximum cached value is reached, *miglogd* drops cached logs (oldest first)
- When FortiAnalyzer connection is back, *miglogd* sends the cached logs
  - FortiGate buffer keeps logs long enough to sustain a reboot of FortiAnalyzer. This is not intended for lengthy outages.
- FortiGate devices with an SSD have a configurable log buffer

#### FortiGate CLI Commands

```
Local-FortiGate # diagnose test application miglogd 6
mem=0, disk=0, alert=0, alarm=0, sys=0, faz=171, faz-cloud=0, webt=0, fds=0
interface-missed=3726
Queues in all miglogds: cur:0 total-so-far:1023
global log dev statistics:
faz 0: sent=170, failed=0, cached=0, dropped=0 , relayed=0
```

Current cache size and total cache size

If there are bursts or the link is overloaded, failed increases

```
Local-FortiGate # diagnose log kernel-stats
fgtlog: 1
fgtlog 0: total-log=2529, failed-log=0 log-in-queue=0
```

If the queue is full, failed-log value increases

If FortiAnalyzer becomes unavailable to a FortiGate device for any reason, the FortiGate uses its *miglogd* process to cache the logs. There is a maximum value to the cache size, and the *miglogd* process drops cached logs starting with the oldest ones first.

When the connection between the two devices is restored, the *miglogd* process begins to send the cached logs to FortiAnalyzer. The FortiGate buffer keeps logs long enough to sustain a reboot of your FortiAnalyzer (if you are upgrading the firmware, for example). This is not intended for a lengthy FortiAnalyzer outage.

On FortiGate, the CLI command `diagnose test application miglogd 6` displays statistics for the *miglogd* process, including the maximum cache size, and current cache size.

The CLI command `diagnose log kernel-stats` shows an increase in `failed-log` if the cache is full and needs to drop logs.

FortiGate devices with an SSD disk have a configurable log buffer. When the connection to FortiAnalyzer is unreachable, FortiGate can buffer logs on disk if the memory log buffer is full. The logs queued on the disk buffer can be sent successfully once the connection to FortiAnalyzer is restored.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Which CLI command can you use to determine if ADOMs are enabled?  
 A. # get system status  
 B. # show system performance
  
2. What can the CLI command # diagnose test application oftpd 3 help you to determine?  
 A. What ADOMs are enabled and configured  
 B. What devices and IP addresses are connecting to FortiAnalyzer

**DO NOT REPRINT****© FORTINET**

## Lesson Progress

**Registration Methods****Communication Troubleshooting****Disk Quota****Managing Registered Devices****NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

27

Good job! You now understand how to troubleshoot communication issues.

Now, you will learn about the FortiAnalyzer disk quota.

**DO NOT REPRINT**  
© FORTINET

## Disk Quota

### Objectives

- Understand what comprises the disk quota
- Understand the disk quota
- Modify the disk quota

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding disk quota and how to modify it, you will be able to use disk quotas more effectively in your network.

**DO NOT REPRINT****© FORTINET**

## Finite Disk Space

- When the allotted log disk space is *full*:
  - An alert message automatically generates on the **Alert Message Console (System Settings > Dashboard)** as an event log with the level *warning*
  - The oldest logs are overwritten (default)
    - You can adjust this behavior to stop logging when disk is full

```
# config system locallog disk setting  
    set diskfull nolog
```

- What you need to know:
  - FortiAnalyzer disk quota and what is included in the quota
  - How the disk quota is enforced
  - What space is reserved and not available for storing logs

FortiAnalyzer devices have finite disk space. When the allotted log disk space is full, the following occurs:

- An alert message automatically generates on the **Alert Message Console** as an event log with the level *warning*.
- The oldest logs are overwritten. This is the default setting, but you can adjust this behavior to stop logging when the disk is full instead.

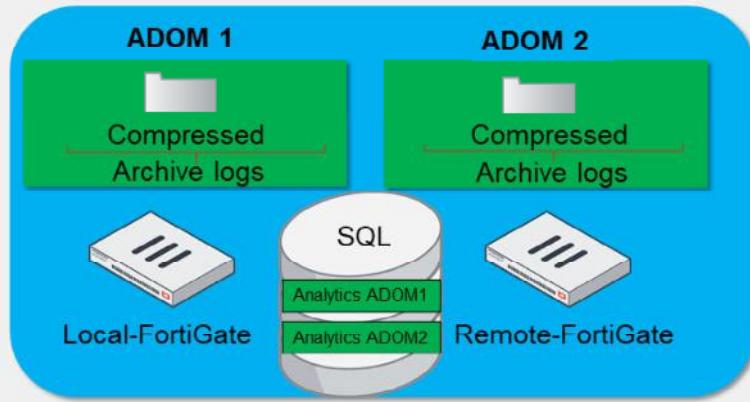
No administrator wants to lose valuable log data and run the risk of noncompliance with regard to data retention. As such, it is vital you know your FortiAnalyzer disk quota, how it is enforced, and what space is reserved and thus not available for storing logs.

# DO NOT REPRINT

## © FORTINET

## Disk Quota

- Disk quota includes:
  - Archive logs
  - Analytics logs



Disk quota includes:

- Archive logs: These are logs compressed on hard disks and offline.
- Analytics Logs: These are the logs stored and indexed in the SQL database and online.

Analytic logs indexed in the SQL database require more disk space than Archive logs. The only exception to this rule is when FortiAnalyzer is working in collector mode because the SQL database is not running.

An average indexed log is 400 bytes in size, and an average compressed log is only 50 bytes in size. Keep this difference in mind when specifying the storage ratio for Analytics and Archive logs. The default ratio is 70%-30%.

# DO NOT REPRINT

## © FORTINET

### Example - Understanding Disk Quota

```
# diagnose log device
```

Total Quota Summary:			
Total Quota	Allocated	Available	Allocate%
64.8GB	64.6GB	142.0MB	99.8%
<b>System Storage Summary:</b>			
Total	Used	Available	Use%
79.8GB	5.6GB	74.2GB	7.0 %
Reserved space: 15.0GB (18.8% of total space)1			

79.8GB (Total System Storage)

- 15.0GB (Reserved Space)

= 64.8 (Total Quota)

64.6GB (Allocated) = Archive + Analytics Quota  
for all ADOMs

5.6GB (Used) = Logs + all system files on mounted  
drive (# diagnose system print df)

Adom name	AdomID	Type	Logs						Database					
			Retention	Quota	UsedSpace	Logs / quarantine / content / IOPS	Used	Used%	Retention	Quota	Used	Used%	Used	Used%
ADOM1	147	FST	365days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
ADOM2	142	FCT	246days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
FortiAnalyzer	121	FAT	365days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
FortiAuthenticator	137	FAC	265days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
FortiCache	125	FCH	365days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
FortiCarrier	117	FCT	365days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
FortiClient	127	FCT	365days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
FortiDDoS	126	FDD	265days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
FortiMail	119	FML	365days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
FortiManager	121	FMG	265days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
FortiNAC	141	FNA	365days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
FortiProxy	129	FPT	265days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
FortiSandbox	122	FSA	265days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
FortiWeb	123	FWW	365days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
Syslog	129	SYS	365days	300.0MB	0.0KB	0.0KB / 0.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	700.0MB	0.0KB	0.0%	0.0B	0.0%
root	3	FST	265days	15.0GB	24.0KB	24.0KB / 24.0KB / 0.0KB / 0.0KB	0.0B	0.0%	60days	25.0GB	5.4MB	0.0%	0.0B	0.0%
Total usage: 16 ADOMs, logs=24.0KB database=900.0MB (ADOMs usage=5.4MB + Internal Usage=924.9MB)														

© Fortinet Inc. All Rights Reserved.

31

You can obtain your disk log usage, including usage for each ADOM, using the CLI command `diagnose log device`.

The total quota value is determined by subtracting the reserved space from the total system storage.

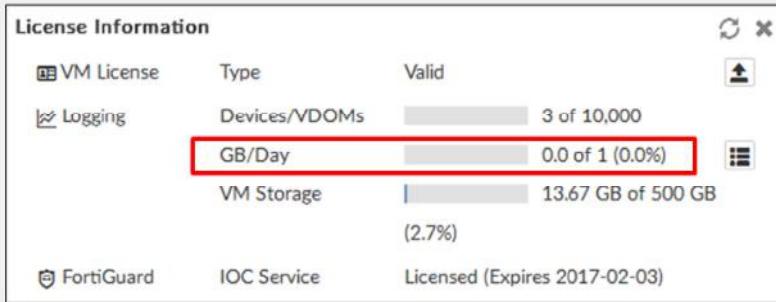
The allocated space is determined by adding the archive and analytics quota for all ADOMs.

The used space is determined by adding the archive and analytics logs and all the system files mounted on the drive. You can receive the system file value by using the CLI command `diagnose system print df`.

**DO NOT REPRINT**  
**© FORTINET**

## Disk Quota on License Information Widget

- The **License Information** widget shows values lower than disk quota
  - Only reports on the number of logs pushed to FortiAnalyzer *on that day*
  - Logs also limited to statistics gathered by *fortilogd* daemon (FortiGate/FortiAnalyzer real-time forwarded logs)
    - Doesn't include log archive, FortiGate store and upload logs, FortiAnalyzer aggregated logs, or FortiClient logs
    - Doesn't include SQL tables



Note that the **License Information** widget shows a lower value than the quota. This is because it reports only on the number of logs pushed to FortiAnalyzer *on that day*. Furthermore, it reports only on the ingress traffic, which is limited to the raw log portion. It doesn't include the log archive, FortiGate store and upload logs, FortiAnalyzer aggregated logs, or FortiClient logs.

The SQL database tables are not included either, because this indexing is done by FortiAnalyzer *after* the log has been received.

# DO NOT REPRINT

## © FORTINET

### Reserved Disk Quota

- The system reserves 5% to 20% disk space for system usage and unexpected quota overflow
- Only 80% to 95% of the disk space is available for allocation to devices

Disk Size	Reserved System Disk Quota
Small (< 500 GB)	20% or 50 GB, whichever is smaller
Medium (500 GB – 1000 GB)	15% or 100 GB, whichever is smaller
Large (1000 GB – 3000 GB)	10% or 200 GB, whichever is smaller
Very large (3000 – 5000 GB)	5% or 500 GB, whichever is smaller

# diagnose log device

Use this command to see amount of reserved space on your FortiAnalyzer

- RAID levels determines the disk size and reserved disk quota level!
  - For example, a FAZ 1000C with 4 x 1 TB hard drives configured in RAID 10 is considered a large disk (2 TB)

By default, each ADOM is allowed 1000 MB (or just under 1 GB) worth of drive space on FortiAnalyzer in order to store log data. However, this number is configurable. You can't set the minimum below 100 MB, and the maximum depends on the disk space allocation of the specific FortiAnalyzer device.

The FortiAnalyzer system reserves between 5% to 25% disk space for compression files, upload files, and temporary report files, leaving about 75% to 95% disk space for allocation to devices.

It is important to note that if using RAID, the RAID level determines the disk size and reserved quota level. See the table on the slide for more details.

**DO NOT REPRINT**  
**© FORTINET**

## Disk Quota Enforcement

- Processes used for disk quota enforcement:

logfiled	sqlplugind	oftpd
Monitors log file size, SQL database size, and archive file size, and sends commands to the other daemons to process  Enforces log file size	Enforces the SQL database size	Enforces the archive file size

- logfiled* checks processes every two minutes (unless system resources are high) and *estimates* space used by SQL database
  - If estimated disk quota use is above 95%, FortiAnalyzer removes older files as needed down to 85%

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

34

Disk quota enforcement is performed by different processes:

- The *logfiled* process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes
- The *sqlplugind* process enforces the SQL database size
- The *oftpd* process enforces the archive file size

**logfiled** checks the processes every two minutes (unless system resources are high) and *estimates* the space used by the SQL database. If the disk quota is estimated to be above 95%, FortiAnalyzer removes files as needed until they are down to 85%.

# DO NOT REPRINT

## © FORTINET

### Modifying ADOM Disk Quota

- Monitor the log rate for each device in the ADOM to determine disk quota requirements
- Adjust the quota based on the requirements

**System Settings > All ADOMs**

OR

**System Settings > Storage Info**

The screenshot shows the 'Storage Info' section of the FortiAnalyzer configuration interface. It includes fields for Data Policy (Keep Logs for Analytics: 60 Days, Keep Logs for Archive: 365 Days) and Disk Utilization (Allocated: 5000 MB, Maximum Available: 375.5 GB). A red box highlights the 'Alert and Delete When Usage Reaches' field, which is set to 90%.

Data Policy	
Keep Logs for Analytics	60 Days
Keep Logs for Archive	365 Days

Disk Utilization	
Allocated	5000 MB
Analytics: Archive	70% 30% <input type="checkbox"/> Modify
Alert and Delete When Usage Reaches	90%

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

35

If ADOMs are enabled, you can adjust your disk quota on the **System Settings > All ADOMs** page.

If ADOMs are not enabled, you can adjust your quota from **System Settings > Storage Info**.

Disk quota calculations are difficult and should be monitored based on the log rate coming from each device. If there is a lot of logging on FortiGate, large devices, or devices with high traffic and UTMs, consider increasing the ADOM disk quota.

**DO NOT REPRINT****© FORTINET**

## Increasing Disk Space

- With FortiAnalyzer VMs, you can dynamically add more disk space:  
# execute lvm info: provides a list of available disks
  - 1. Stop the FortiAnalyzer VM and add a new virtual disk to the VM
  - 2. Reboot FortiAnalyzer and run execute lvm info to identify the added disk
  - 3. Run execute lvm extend <disk number>
  - 4. Reboot FortiAnalyzer (run get system status to see the new disk space)
- With hardware FortiAnalyzer, you have to add another disk
    - If you are using RAID, this requires you to rebuild your RAID array
  - Be sure to account for future growth and size correctly from the outset!

If increasing disk quota is insufficient based on your monitored log rate, you may need to increase your overall disk space. With FortiAnalyzer VMs, you can dynamically add more disk space to your FortiAnalyzer by using the procedure shown on this slide.

With a hardware FortiAnalyzer, you also must add another disk, because disk space is fixed. If you are using RAID, you will also have to rebuild your RAID array if you add another disk. So, it is important to account for further growth and size correctly from the outset.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. By default, what happens when the allotted log disk space is full?

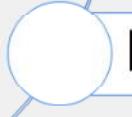
- A. The oldest logs are overwritten.
- B. Logging stops.

2. What is the disk quota composed of?

- A. Archive logs and analytics logs
- B. Raw logs and archive files

**DO NOT REPRINT****© FORTINET**

## Lesson Progress

**Registration Methods****Communication Troubleshooting****Disk Quota****Managing Registered Devices****NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

38

Good job! You now understand the FortiAnalyzer disk quota.

Now, you will learn how to manage registered devices.

**DO NOT REPRINT**  
© FORTINET

## Managing Registered Devices

### Objectives

- Move registered devices between ADOMs
- Add two or more devices to an HA cluster

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in moving devices between ADOMs and adding them to HA clusters, you will be able to manage registered devices effectively in your network.

**DO NOT REPRINT**  
**© FORTINET**

## Moving Registered Devices Between ADOMs

- Do not move devices between ADOMs unless you have to
- Can move devices between ADOMs after registration
  - By default, restricted to administrators with Super\_User access
- You do not need to create a new ADOM if you upgrade your FortiGate firmware
  - Not necessary to separate ADOMs by FortiOS version

Name	Version	From ADOM
ISFW	7.0	ADOM1
Local-FortiGate	7.0	ADOM1
Remote-Fortigate	7.0	ADOM2

NSE Training Institute © Fortinet Inc. All Rights Reserved. 40

You can move devices between ADOMs after registration on the **All ADOMs** page.

While you shouldn't move devices between ADOMs unless you have to, one such use case is if you have a mix of low-volume and high-volume log rates in one ADOM. In this situation, it is recommended that you place low-volume log rate devices in one ADOM and high-volume log rate devices in another ADOM. This prevents quota enforcement from adversely affecting low-volume log devices.

You can move devices between ADOMs by editing the custom ADOM to which you want to add the device, and then selecting the device(s) to add to it.

Note that you do not need to move devices into a new ADOM if you upgrade your FortiGate firmware.

**DO NOT REPRINT****© FORTINET**

## Considerations Before Moving Devices

- What is the disk quota of the new ADOM? Ensure it has enough space for logs.
- Are the device analytics logs required for reports in the *new* ADOM? If so, rebuild the new ADOM database:  
# execute sql-local rebuild-adom <new-ADOM-name>
- Do you want to see the device analytics logs in the *old* ADOM? If not, rebuild the old ADOM database (or they will be removed according to the data policy):  
# execute sql-local rebuild-adom <old-ADOM-name>
- When you move a device, only the archive (compressed) logs are migrated to the new ADOM. The analytics (indexed) logs stay in the old ADOM until you rebuild the database.

There are some important considerations when moving devices between ADOMs, especially if logs are already being collected for the device you are moving:

- What is the disk quota of the new ADOM? Ensure the new ADOM has enough space.
- Are the device analytics logs required for reports in the new ADOM? If so, you must rebuild the new ADOM SQL database. When you move a device, only the archive logs (compressed logs) are migrated to the new ADOM. The analytics logs (indexed logs) stay in the old ADOM until you rebuild the database.
- Do you want to see the device analytics logs in the old ADOM? If no, you need to rebuild the old ADOM SQL database. Otherwise, they are removed according to the data policy.

**DO NOT REPRINT****© FORTINET**

## Adding an HA Cluster

- FortiAnalyzer automatically discovers if a FortiGate device is in a high availability (HA) cluster
  - If you register your device with FortiAnalyzer before adding it to a cluster, you can manually add the cluster within FortiAnalyzer
- With an HA cluster, each device generates its own logs (separate serial number in logs)
  - Primary device responsible for sending all logs from the other devices in the cluster to FortiAnalyzer
- FortiAnalyzer distinguishes different devices by their serial number (SN)
  - SN in logs headers

HA Cluster	
Add Existing Device	<input type="text"/>
Add Other Device	<input type="text"/> Serial Number
HA Cluster List	Action
#	Device Name
1	Local-FortiGate (FGVM010000064692)
2	ISFW (FGVM010000077646)

Edit in Device Manager

FortiAnalyzer automatically discovers if a FortiGate device is in an HA cluster (this is true of some other Fortinet devices too). However, if you register your device with FortiAnalyzer before adding it to a cluster, you can manually add the cluster within FortiAnalyzer.

With an HA cluster, the only device that communicates with FortiAnalyzer is the primary device in the cluster. The other devices send their logs to the primary, which then forwards them to FortiAnalyzer.

To enable a cluster, edit the registered device on FortiAnalyzer in Device Manager and enable the HA Cluster option. You can either add existing devices to the cluster, or manually enter the serial numbers associated with each device.

FortiAnalyzer distinguishes different devices by their serial numbers, which are found in the headers of all the different log messages it receives.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. When you move a FortiGate device from one ADOM to a new ADOM, what is the purpose of rebuilding the new ADOM database?
  - A. To migrate the archived logs to the new ADOM
  - B. To run reports on the device analytics logs in the new ADOM

**DO NOT REPRINT****© FORTINET**

## Lesson Progress

**Registration Methods****Communication Troubleshooting****Disk Quota****Managing Registered Devices****NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

44

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Identify the different ways you can register a device
- ✓ Describe how device registration works with ADOMs
- ✓ View device status
- ✓ Troubleshoot device communication issues
- ✓ Understand what comprises the disk quota
- ✓ Understand the disk quota
- ✓ Modify the disk quota
- ✓ Move registered devices between ADOMs
- ✓ Add two or more devices to an HA cluster

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to add, manage, and maintain devices in your network.

**DO NOT REPRINT**

© FORTINET



## FortiAnalyzer

### Logging



In this lesson, you will learn how to protect, view, and manage logs on FortiAnalyzer.

By understanding logging on FortiAnalyzer, you will be able to use log data to reconstruct and analyze network-based attacks, as well as troubleshoot and investigate network issues.

Last Modified: 1 December 2021

**DO NOT REPRINT**

**© FORTINET**

## Lesson Overview

**Log Overview**

**Protecting Log Information**

**Viewing and Searching Logs**

**Troubleshooting and Managing Logs**

In this lesson, you will explore the topics shown on this slide.

# DO NOT REPRINT

## © FORTINET

### Log Overview

#### Objectives

- Describe the purpose of collecting and storing logs
- Describe the log file workflow (archive and analytics)

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the purpose of log collection, log storage, and the log file workflow, you will have a better understanding of how logs are compiled and collected.

**DO NOT REPRINT****© FORTINET**

## Purpose of Logs

- Log messages record information containing specific details about what is occurring on the network
- Determine load on network devices
- Track service use
- Support incident response and forensic analysis
- Must examine multiple logs to discover the chain of activity that led to a breach

Log messages help paint a picture of what is going on in your network. You can determine the load on your network devices, track service use, and identify any security breaches in your network.

However, it is important to understand that logs are like a puzzle—you must put several pieces together in order to get a complete understanding of what is going on. Multiple log messages are often required to determine the exact chain of activity that leads to a breach—a log in isolation often won't help you to best configure your network to prevent such breaches in the future.

This is why centralized log storage is so important.

**DO NOT REPRINT**  
**© FORTINET**

## Log Storage Regulations

- Regulatory requirements may mandate how logs are managed in an organization
  - Levels and analysis requirements are often defined by legislation
  - Ensure logging is enabled and recording data at correct level to satisfy regulations
- Logs can provide evidence to deal with offending parties when unauthorized activity is detected
  - Logging data must be able to stand up in court
- Monitoring of logs is hampered by extensive amounts of data being captured and the lack of means to manage, correlate, and analyze that data
  - Logging levels should be set high enough to satisfy any regulation and allow you to do your job
    - Too much data is as bad as too little

In certain countries, and in some areas of business, there are regulations that require that companies log specific information and store logs for a minimum amount of time.

The regulations often detail the specific types of logs and data required, as those log entries can be used as evidence in cases of unauthorized or illegal activity. The data must be able to stand up in court, so being able to understand and analyze your logs is very important.

Information overflow, however, is a real issue. You want to make sure that whatever information you are logging is enough to satisfy the regulations while still being able to do your job. Having too much data is just as bad (and in some ways worse) than having too little.

**DO NOT REPRINT****© FORTINET**

## Log Data Management Best Practices

- Document what is being logged and why
- Ensure data for all devices and applications is being captured and not filtered (ongoing!)
- Centralize log storage in common format
- Synchronize time on all devices
- Maintain backups of logs and implement a policy that specifies log retention periods
- Define procedures to preserve data integrity
- Test incident response plan (ongoing)

It is important not only to collect and store logs, but to manage them efficiently. If you don't follow best practices to manage your logs, it can result in loss of data and even loss of revenue. Especially if a network attack results in a legal case, it is essential that you provide the appropriate data in court.

Some best practices include the following:

- Documenting what is being logged and why. If you ever need to investigate a new event based on your log data, you can look at your documentation and see what exactly you're logging so you know if it's even possible to identify.
- Ensuring that data for all your devices and applications is being captured and not filtered. Monitor your devices to ensure they are sending logs.
- Centralizing log storage and storing in a common format. This makes your job easier, since there is no need to check multiple locations in order to look at the log data.
- Synchronizing the time on all logged devices. If your firewall says it's 3 AM, your FortiAnalyzer says it's 12:30 AM, and your computer says it's 8:56 AM, cross-referencing logs can be very difficult.
- Maintaining a backup of logs and implementing a policy that specifies log retention periods.
- Defining procedures to preserve data integrity.
- Testing and retesting your incident response plan to ensure it works and that all administrators know their roles.

**DO NOT REPRINT****© FORTINET**

## Log Types by Device

Device	Log type
FortiGate	<ul style="list-style-type: none"> <li>Traffic [forward, local, sniffer]</li> <li>Event [Endpoint, High Availability, System, User, Router, VPN, WAD, Wireless]</li> <li>Security [Application Control, AntiVirus, Data Leak Prevention (DLP), Anti-Spam, Web Filter, Intrusion Prevention System (IPS), Anomaly (DOS-policy), WAF]</li> </ul>
FortiCarrier	Traffic, Event
FortiCache	Traffic, Event, Antivirus, Web Filter
FortiClient	Traffic, Event
FortiMail	History, Event, Antivirus, Email Filter
FortiManager	Event
FortiSandbox	Malware, Network Alerts
FortiWeb	Event, Intrusion Prevention System (IPS), Traffic
Syslog	Generic (used for compatibility with older FortiGate, or for non-Fortinet devices)

Must enable ADOMs to collect logs from non-FortiGate devices, unless they are part of a Security Fabric

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

7

To be able to analyze and interpret your logs, it is important to understand the different log types and what information they contain, as well as what logs FortiAnalyzer collects from each supported device.

There are three log types: traffic logs, event logs, and security logs. Each log type has corresponding log subtypes.

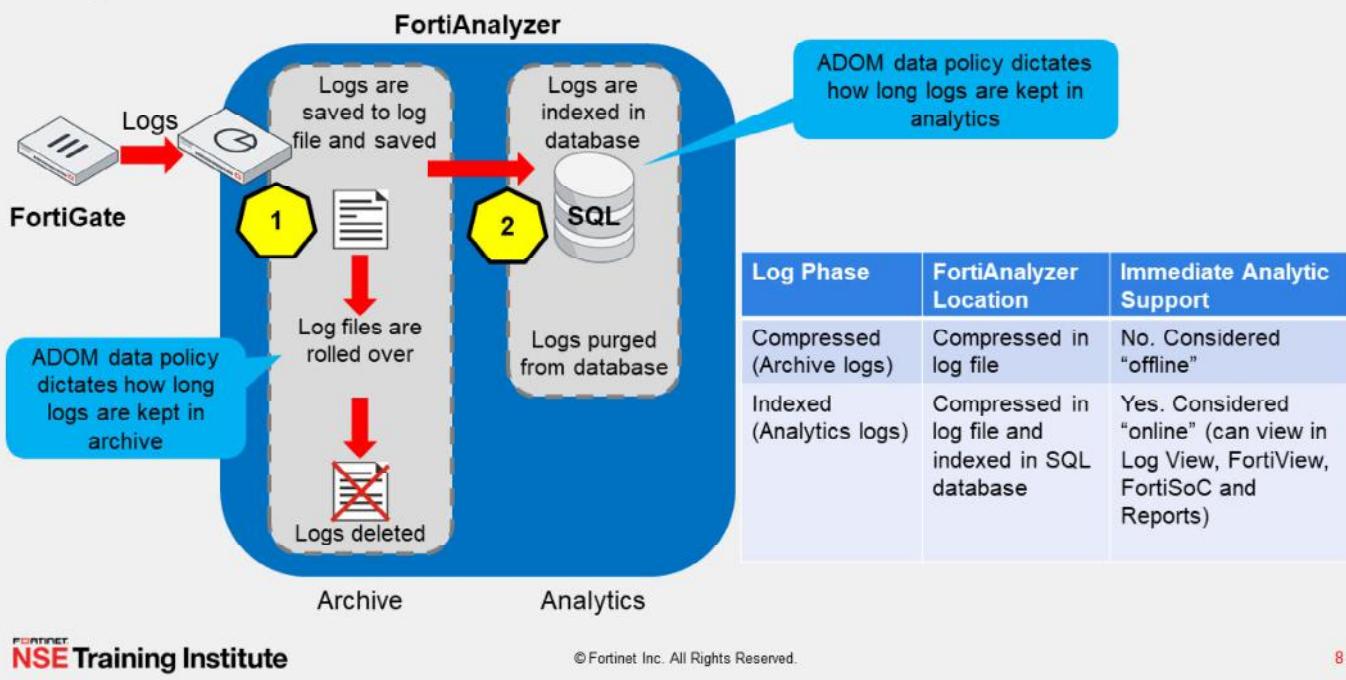
The logs displayed on your FortiAnalyzer are dependent on the device type logging to it and the features enabled. This table illustrates the log types and subtypes FortiAnalyzer collects from various supported devices. Refer to the *FortiAnalyzer Administration Guide* for the complete list.

Remember that you must enable ADOMs in order to support non-FortiGate logging, unless those devices are part of a Security Fabric.

# DO NOT REPRINT

## © FORTINET

### Log File Workflow



When registered devices send logs to FortiAnalyzer, logs enter the following automatic workflow:

1. Logs are received and saved in a log file on the FortiAnalyzer disks. Eventually, when the log file reaches a configured size, or at a set schedule, it is rolled over by being renamed. These files (rolled or otherwise) are known as *archive logs* and are considered offline so they don't offer immediate analytic support. Combined, they count toward the archive quota and retention limits, and they are deleted based on the ADOM data policy.
2. The saved logs are simultaneously indexed in the SQL database to support analysis. The ADOM data policy determines how long these logs are kept in analytics. Logs in the indexed phase are known as *analytics logs*. These logs are considered online and offer immediate analytic support. Analytics logs are purged from the SQL database as specified in the data policy.

**DO NOT REPRINT**

**© FORTINET**

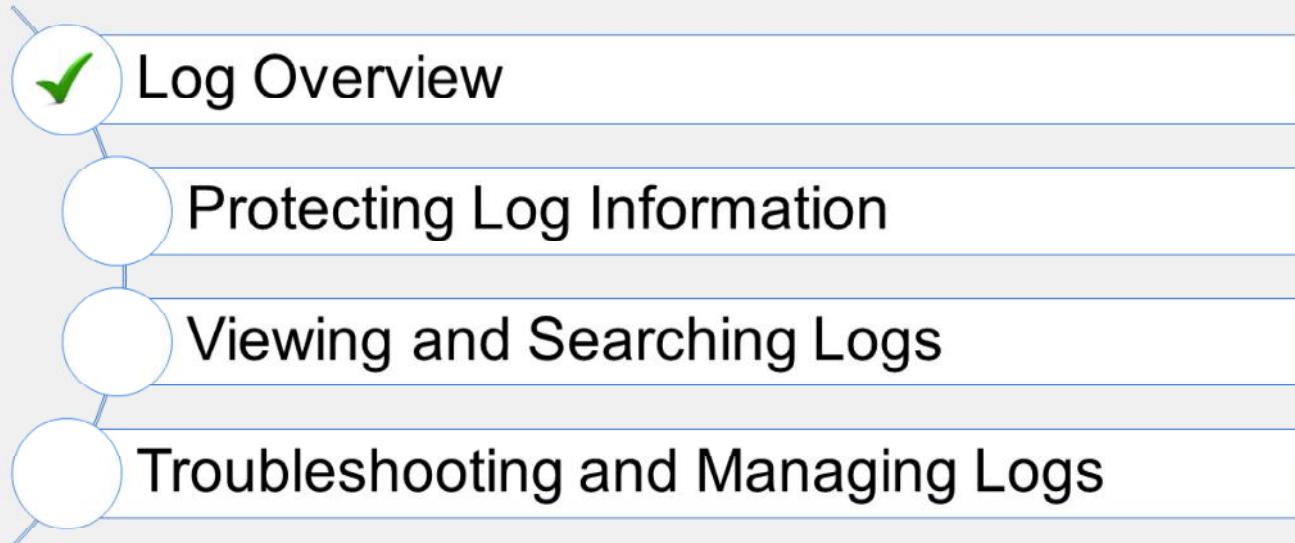
## Knowledge Check

1. Logs in the compressed phase are known as \_\_\_\_\_ logs.  
 A. Archive logs  
 B. Analytics logs
  
2. What happens when a log file saved on FortiAnalyzer disks reaches the size specified in the Device Log settings?  
 A. The log file is rolled over.  
 B. The log file is stored for analytic support.

**DO NOT REPRINT**

**© FORTINET**

## Lesson Overview



Good job! You now understand the purpose of log collection, log storage, and the log file workflow.

Now, you will learn about ways you can protect your log data.

**DO NOT REPRINT**

**© FORTINET**

## Protecting Log Data

### Objectives

- Understand high performance log storage (RAID)
- Perform log backups
- Configure log redundancy
- Configure log encryption

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in the different ways you can protect your logs, you will be able to meet organizational or legal requirements for logs.

**DO NOT REPRINT****© FORTINET**

## Log Storage Using RAID

- The use of RAID allows you to increase the reliability of your data (logs) against critical events
- Different RAID levels will provide different benefits regarding capacity, performance, and availability
- Not all RAID levels provide fault tolerance
- RAID is not supported on all FortiAnalyzer models

You can protect your logs by using a fault tolerant RAID solution. This improves your logs availability should a critical event on your FortiAnalyzer occur.

RAID is not supported on all FortiAnalyzer models.

# DO NOT REPRINT

## © FORTINET

### Log Backup

- Protect log data from disk failure, deletion, or corruption
- Backup mechanisms include:
  - Backing up log files using the GUI or CLI
    - GUI (**Log View**) provides control to download a specific filtered view →
    - GUI (**Log Browse**) provides rolled log download (can also schedule log upload of rolled logs by clicking **System Settings > Advanced > Device Log Settings**)
    - CLI more suitable for bulk data dumps
  - Uploading logs to an FTP, SFTP, or SCP server

The screenshot shows two FortiAnalyzer log management interfaces:

- Log View > Log Browse**: A table listing log entries. One entry is selected, and a context menu is open over it. The menu includes options like "Real-time Log", "Display Raw", "Download" (which is highlighted with a red box), and "Sensitive Search". A blue callout points to the "Download" option with the text "Text or CSV format".
- Log View > Log View**: A table showing a single log entry for a device named FAZ-VM0000065040. The entry details are: File Name: \_self\_locallog\_, Type: Event, From: 2021-06-10 07:35:19, To: 2021-08-21 21:18:03, Size: 579.1k. The "Download" button in the header is also highlighted with a red box.

Below the tables, there are two blue callouts with text:

- "Includes logs, archives, and quarantine (use logs-only if only log files needed)"
- "To restore logs, use execute restore\_logs instead"

At the bottom, a command line is shown: "# execute backup\_logs <device name|all> <ftp|sftp|scp> <IP of server> <user name> <password> <location on server>"

Fortinet NSE Training Institute

© Fortinet Inc. All Rights Reserved.

13

RAID should not be considered a replacement for backing up your logs. You can back up your logs through the GUI or CLI.

- **Log View** allows you to download a specific filtered view.
- **Log Browse** allows you to download rolled logs. FortiAnalyzer also provides the option to upload logs to an FTP, SFTP, or SCP server on a scheduled basis.
- The CLI command `execute backup_logs` sends everything to whatever device or devices you specify. The data is compressed before being sent, so the transfer doesn't begin instantaneously. The device needs to process the logs and store them in an archive, which can take some time. This bulk data dump may include a lot of data, so make sure your server has enough disk space.

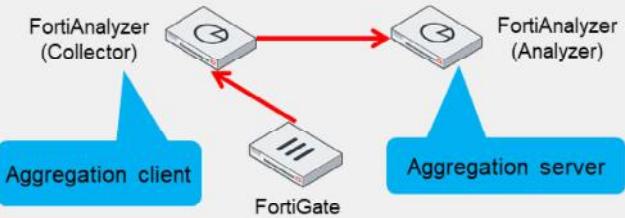
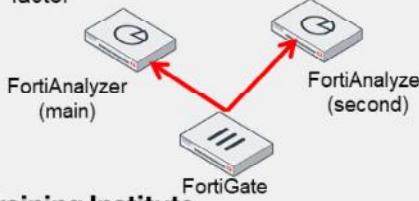
You can restore logs using the GUI and the CLI.

# DO NOT REPRINT

## © FORTINET

## Log Redundancy Options

1. Configure FortiAnalyzer HA cluster
  - Provides real-time redundancy when primary fails
  - Provides log and configuration synchronization
2. Configure FortiGate to send an identical set of logs to a second logging server
  - FortiAnalyzer or syslog
  - CPU, RAM load will be higher on FortiGate (more so if SSL enabled)
  - Log daemon must handle an additional TCP connection to a second log device
  - If system is sized properly, the extra load won't be a factor
3. Set up log forwarding in aggregation mode
  - Collector sends delta (incremental changes) of its logs, quarantined files, and archives to an aggregation server
  - Sends only what the analyzer doesn't have
  - If catastrophic failover of analyzer, collector sends all the data and repopulates the analyzer automatically
  - Aggregation mode only supported between two FortiAnalyzers



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

To protect your logs during log delivery, you can add redundancy to your environment. In a FortiGate-FortiAnalyzer environment, there are a few options.

One option is to configure a FortiAnalyzer HA cluster. FortiAnalyzer HA provides real-time redundancy when a FortiAnalyzer primary device fails. If the primary device fails, another device in the cluster is selected as the primary device. It synchronizes logs and data securely among multiple FortiAnalyzer devices. System and configuration settings applicable to HA are also synchronized. It also provides load balancing for processes, such as running reports.

The second option is to configure FortiGate to send an identical set of logs to a second logging server, such as a second FortiAnalyzer or a syslog. Note that this increases the load on the FortiGate device because the log daemon must handle an additional TCP connection to the second log device. However, with proper system sizing, this additional load is not a factor. This option is not available for smaller FortiGate devices that do not support a second device.

Another option is to set up log forwarding in aggregation mode. Generally, your central (aggregating) device is going to be a larger FortiAnalyzer, but this is not a requirement. The collector sends a delta (incremental changes) of the logs to the aggregation server. The two devices compare what they have stored, and the collector sends only what the analyzer doesn't have. This not only reduces the amount of traffic that is sent, but it also provides a level of redundancy. If there's a catastrophic failure of the analyzer device, the collector sends all the data it has and repopulates the restored analyzer automatically. Aggregation mode is only supported between two FortiAnalyzer devices.

# DO NOT REPRINT

## © FORTINET

## Log Forwarding

- Forward to another FortiAnalyzer, syslog, or common event format (CEF)
  - Supports two forwarding modes: aggregation and forwarding

### 1. Set log forwarding mode

```
# config system log-forward
  edit <log aggregation ID>
    set mode <aggregation, forwarding, disable>
  end
```

- aggregation:** Logs and content files stored and uploaded at scheduled time
- forwarding:** Realtime or near realtime forwarding logs to servers

### 2. Configure the server (FortiAnalyzer or syslog/CEF that receives logs)

- FortiAnalyzer:

```
# config system log-forward-service
  set accept-aggregation enable
  end
```

### 3. Configure the client (FortiAnalyzer forwarding the logs)

- System Settings > Log Forwarding

Can specify which device logs to forward and set log filters to only send logs that match filter criteria

Log forwarding can run in modes other than aggregation mode, which is only applicable between two FortiAnalyzer devices. FortiAnalyzer can also forward logs in real-time mode to a syslog server, a Common Event Format (CEF) server, or another FortiAnalyzer. The FortiAnalyzer that forwards logs to another plays the role of the client, while the recipient plays the role of the server.

To configure log forwarding, you must complete the following:

- Set the log forwarding mode: aggregation or forwarding.
  - Forwarding mode forwards logs as they are received. It does not forward content files (DLP, antivirus quarantine, and IPS).
  - Aggregation mode stores logs and content files and uploads them to the FortiAnalyzer server at a scheduled time.
- Configure the server (the log recipient).
- Configure the client (the FortiAnalyzer forwarding the logs). Here you can also specify which device logs to forward and set log filters to only send logs that match filter criteria.

In addition to forwarding logs, the FortiAnalyzer client retains a local copy of the logs. The local copy of logs are subject to the data policy settings for archive logs on the FortiAnalyzer client.

# DO NOT REPRINT

## © FORTINET

### Encrypted Log Communication: OFTPS

- The Optimized Fabric Transfer Protocol (OFTP) is used over SSL when information is synchronized between FortiAnalyzer and FortiGate
  - OFTP listens on port TCP/514
- Default setting**
  - Auto-negotiated, so the oftp server will use the OFTPS protocol only if being used by the connecting FortiGate

```
#config log fortianalyzer setting
  set reliable enable
```

```
# config log fortianalyzer setting
  set enc-algorithm {high-medium | high* | low}
end
```

FortiGate default encryption level is **high**  
(low encryption models can do only the **low** level)

```
# config system global
  set enc-algorithm {high* | medium | low}
end
```

FortiAnalyzer default encryption level is **high**. This encryption level must be equal to, or less than, the FortiGate device

In the default configuration, there are two communication streams between FortiGate and FortiAnalyzer. One is the OFTP communication, which is encrypted, and the other is the log communication, which is not.

OFTP is used over SSL when information is synchronized between FortiAnalyzer and FortiGate. OFTP listens on port TCP/514. Port UDP/514 is used for unencrypted log communication.

The log communication between devices can be protected by encryption, with the desired encryption level, using the commands shown on the slide.

SSL communications are auto-negotiated between FortiAnalyzer and FortiGate, so the OFTP server uses SSL-encrypted FTP, only if it is being used by the connecting FortiGate. By default, FortiGate uses the *high* encryption level and FortiAnalyzer uses the *high* encryption level. The FortiAnalyzer encryption level must be equal to, or less than, the FortiGate device.

**DO NOT REPRINT**  
© FORTINET

## Preventing Log Modification

- To prevent log modification, you can add a log checksum
- Can configure FortiAnalyzer to record log file hash value, timestamp, and authentication code at transmission or rolling. Options include:
  - md5: Record the log file MD5 hash value only
  - md5-auth: Record the log file MD5 hash value and authentication code
  - none: Do not record the log file checksum

```
# config system global
    set log-checksum md5-auth      {md5 | md5-auth | none}
end
```

- You can also change the OFTP certificate to a custom one

```
# config system certificate oftp
    set custom enable
    set certificate <your PEM format certificate>
    set private-key <your PEM format private key>
end
```

To prevent logs from being tampered with while in storage, you can add a log checksum using the **config system global** command. You can configure FortiAnalyzer to record a log file hash value, timestamp, and authentication code when the log is rolled and archived and when the log is uploaded (if that feature is enabled). This can also help against man-in-the-middle only for the transmission from FortiAnalyzer to an SSH File Transfer Protocol (SFTP) server during log upload.

The following log checksums are available:

- md5: Record log file MD5 hash value only.
- md5-auth: Record log file MD5 hash value and authentication code.
- none: Do not record the log file checksum.

You can also change the OFTP certificate to a custom one using the **config system certificate oftp** command. You require a Privacy-Enhanced Mail (PEM) formatted certificate and associated PEM-formatted private key.

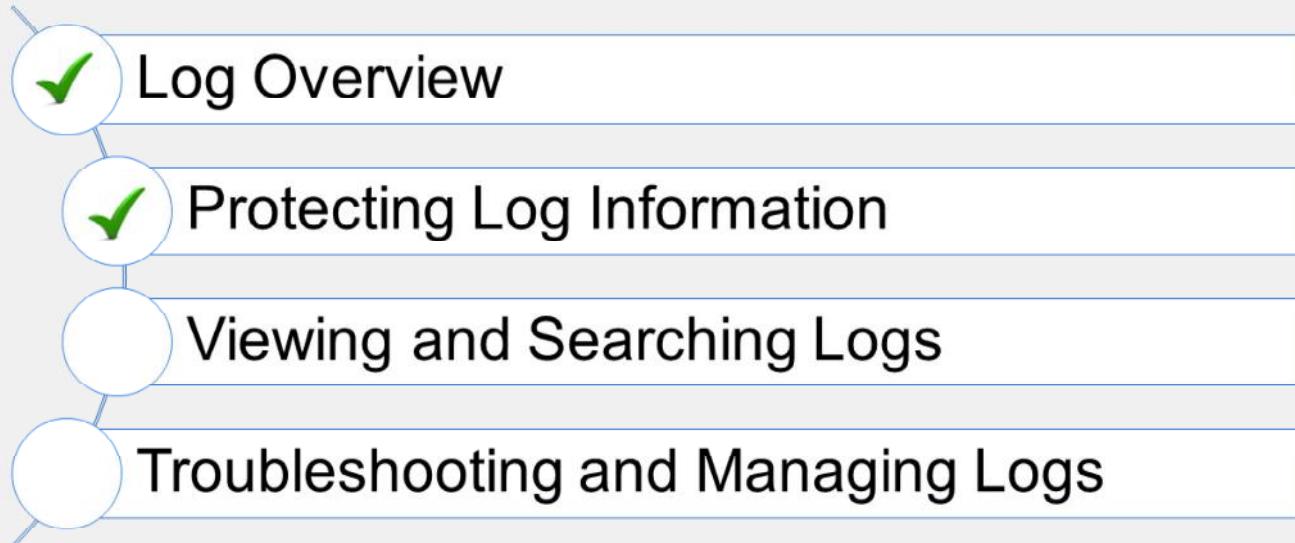
**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. Which log forwarding mode stores logs and content files, and uploads them to another FortiAnalyzer server at a scheduled time?  
 A. Forwarding mode  
 B. Aggregation mode
  
2. FortiAnalyzer uses the OFTP over SSL for which purpose?  
 A. To encrypt log communication between devices  
 B. To prevent log modification

**DO NOT REPRINT****© FORTINET**

## Lesson Overview



Good job! You now understand the different ways you can protect your logs, and how to meet the organizational or legal requirements for logs.

Now, you will learn about ways to view and search your logs on FortiAnalyzer.

**DO NOT REPRINT**

**© FORTINET**

## Viewing and Searching Logs

### Objectives

- View and search for logs in Log View
- View summary data in FortiView
- View dashboards and widgets features

After completing this section, you should be able to achieve the objectives shown on this slide.

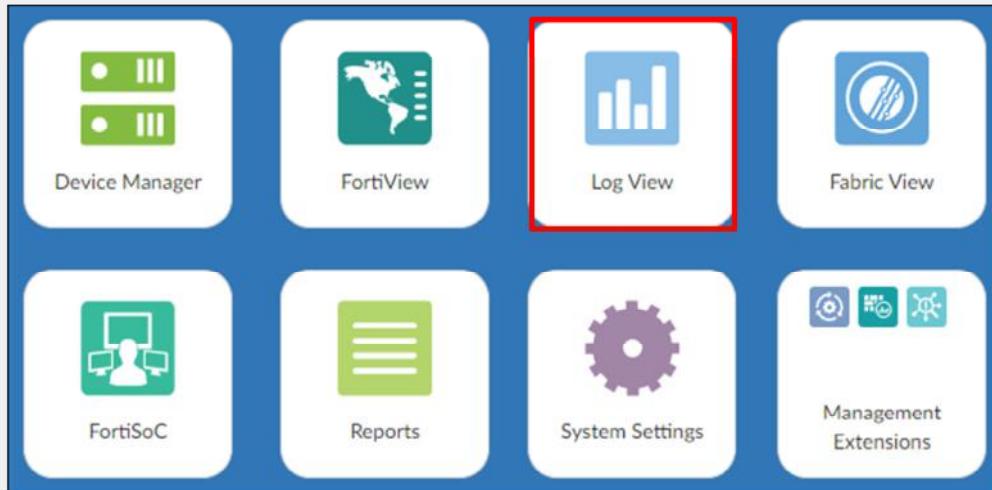
By demonstrating competence in viewing logs, log summaries, and dashboards, you will be able to find and view a variety information related to logs.

# DO NOT REPRINT

## © FORTINET

### Log View

- View traffic logs, event logs, or security logs for each ADOM
  - Can restrict view to one or more devices or a log group (a group of devices that you can place together into a single logical object)



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

21

**Log View** allows you to view traffic logs, event logs, and security logs information for each ADOM. You can restrict the log view to one or more devices in the ADOM or to a log group, which is a group of devices placed together in a single logical object.

Log groups are virtual. They don't have SQL databases or occupy additional disk space.

# DO NOT REPRINT

## © FORTINET

### Searching for Logs

The screenshot shows the FortiAnalyzer Log View interface. On the left, a sidebar lists categories like Fabric, FortiGate, Traffic, Security, Web Filter, Event, System, VPN, User, WAN Opt. & Cache, WiFi, FortiAnalyzer, Log Browse, and Log Group. A red box highlights the 'Web Filter' option under Security. The main area displays a table of log entries with columns: #, Date/Time, Device ID, User, Source, Destination IP, Service, Host Name, and Action. A blue box labeled 'Set filters' points to the 'Add Filter' button at the top of the table. Another blue box labeled 'Select device and log type' points to the sidebar. A third blue box labeled 'Custom View' points to a dropdown menu on the right. A fourth blue box labeled 'Specify columns to display (with associated data) in table' points to the column headers. A fifth blue box labeled 'View in real time or historical View raw or formatted' points to the top right of the table. A sixth blue box labeled 'Log details' points to a detailed view pane on the right side of the screen, which shows expanded information for a selected log entry.

#	Date/Time	Device ID	User	Source	Destination IP	Service	Host Name	Action
1	22:01:21	FGVM010000064692		10.0.1.10	99.83.181.185	HTTP	pokerstars.net	blocked
2	22:01:21	FGVM010000064692		10.0.1.10	99.83.181.185	HTTP	pokerstars.net	blocked
3	22:01:08	FGVM010000064692		10.0.1.10	207.194.175.26	HTTP	r3.ojencr.org	blocked
4	22:01:07	FGVM010000064692		10.0.1.10	207.194.175.26	HTTP	r3.ojencr.org	blocked
5	21:51:54	FGVM010000064692		10.0.1.10	44.240.152.58	HTTPS	dx.mountain.com	blocked
6	21:51:44	FGVM010000064692		10.0.1.10	52.21.152.175	HTTPS	litrck.com	blocked
7	21:51:44	FGVM010000064692		10.0.1.10	97.194.175.26	HTTP	litrck.com	blocked
8	21:51:44	FGVM010000064692		10.0.1.10	44.240.152.58	HTTP	litrck.com	blocked
9	21:51:44	FGVM010000064692		10.0.1.10	44.240.152.58	HTTP	litrck.com	blocked
10	21:51:44	FGVM010000064692		10.0.1.10	44.240.152.58	HTTP	litrck.com	blocked
11	21:51:44	FGVM010000064692		10.0.1.10	44.240.152.58	HTTP	litrck.com	blocked

NSE Training Institute © Fortinet Inc. All Rights Reserved. 22

To search for specific logs in **Log View**, select the device and log type from the left menu and then set appropriate filters.

You can create filters based on any of the available values. For example, a filter for a specific device within the ADOM and a limited time frame.

**Log View** filters supports auto-complete to set the filter value. You can control this feature by using the following CLI command:

```
# config system global
# set default-logview-auto-completion {Enable|Disable}
```

By default, auto-complete is enabled.

You can also change your view by adding or removing columns and viewing logs in real time or historically, or as raw or formatted logs.

To view more information about a log, double-click the log entry. The details pane appears on the right side of the screen.

**DO NOT REPRINT**  
**© FORTINET**

## Saving Frequent Log Searches

- Save frequent searches as a custom view

The screenshot shows the FortiAnalyzer Log View interface. A search results table is displayed, showing log entries for HTTPS traffic over the last hour. A modal dialog box titled "Save as New Custom View" is open in the foreground. The "Name" field contains "HTTPS TRaffic last hour". Other fields in the dialog include "Log Type: Web Filter", "Devices: All\_FortiGate", "Time Period: Last 1 Hour", "Search: service='HTTPS'", and "Privacy: Public". A red arrow points from the "Custom View (1)" button in the toolbar to the "HTTPS TRaffic last hour" entry in the dropdown menu of the modal. Another red arrow points from the "OK" button in the modal back to the main Log View window.

You can save frequent searches as a custom view using the **Custom View** icon on the tool bar. Set your filters, conduct your search, and then save the search under a custom view.

**DO NOT REPRINT**  
**© FORTINET**

## Search—Troubleshooting and Tips

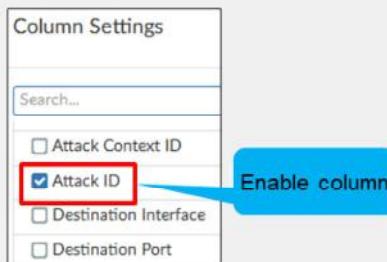
- Confirm if **Case Sensitive Search** is enabled
  - Click **Add Filter** to select the desired filter



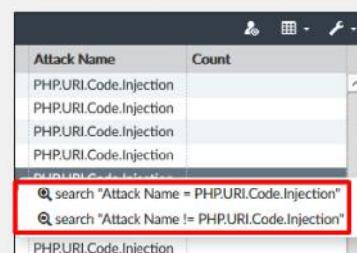
- Click **Add Filter** to select the desired filter



- Add column(s) from **Column Settings > More Columns**



- Right-click the desired column to set a filter based on that data



If your search filters don't return any results when the log data does exist, the filter may be poorly formed. FortiAnalyzer looks for an exact match in the log, so you must form the search string correctly.

Here are some tips for log searches or troubleshooting log searches:

- Verify if **Case Sensitive Search** is enabled in the **Tools** menu. Disable for increased search flexibility.
  - Find a log in the log table that includes data that you want to search for. For example, if you want to search for attacks that include code injections, right-click on that data, and a pop-up appears with the search filters automatically set for you. If you select the search filter, it returns the results based on that filter.
  - When setting a filter, you can select an existing filter option in the drop-down list or type your own filter name.
  - You can add more columns to the view. This can make it easier to find fields available for using with your filters.

# DO NOT REPRINT

## © FORTINET

## FortiAnalyzer Application Logs

- FortiAnalyzer application logs:
  - Include audit logs for SIEM and SOAR applications
  - Each ADOM has its own audit logs
  - Accessible in **Log View**

The screenshot shows the FortiAnalyzer Log View interface. The left sidebar lists 'Fabric' and 'All' devices, with 'FortiAnalyzer' selected. Under 'Log View', 'Log Browse' is highlighted. The main area displays a table of logs from June 5 to June 12, 2018. The columns include Date/Time, Device ID, User, Sub Type, Event Type, Action, Description, Log ID, Level, and Message. A callout bubble points to the 'Log Browse' button with the text 'Use Log Browse to see log details'.

#	Date/Time	Device ID	User	Sub Type	Event Type	Action	Description	Log ID	Level	Message
1	06-09 18:30	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	incident	110269	notice	Task 'Attach Report to Incident...' attached to incident IN...
2	06-09 18:30	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Report Attach...	100005	notice	Report attached to incident IN...
3	06-09 18:30	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Report Sched...	110251	notice	Task 'Run Report' executed via...
4	06-09 18:29	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Incident Atta...	110269	notice	Task 'Attach Report to Incident...' attached to incident IN...
5	06-09 18:29	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Report Attach...	100005	notice	Report attached to incident IN...
6	06-09 18:29	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Report Sched...	110251	notice	Task 'Run Report' executed via...
7	06-09 18:28	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Incident Creat...	110263	notice	Task 'Create Incident' executed...
8	06-09 18:28	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Endpoint Soft...	110105	notice	Task 'Get Endpoint Software In...' failed to exec...
9	06-09 18:28	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Process List R...	110108	notice	Task 'Get Endpoint Process' faile...
10	06-09 18:28	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Endpoint AV ...	110120	notice	Task 'Run AV Scan on Endpoint...' failed to exec...
11	06-09 18:28	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	New Incident...	100001	notice	Incident (N00000002) is created.
12	06-09 18:28	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Locking Up Ev...	110256	notice	Task 'Get Events' failed to exec...
13	06-09 18:28	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Playbook Titl...	110001	notice	Playbook 'Playbook Controller...' created.
14	06-09 18:27	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Incident Atta...	110269	notice	Task 'Attach Report to Incident...' attached to incident IN...
15	06-09 18:27	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Report Attach...	100005	notice	Report attached to incident IN...
16	06-09 18:27	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Report Sched...	110251	notice	Task 'Run Report' executed via...
17	06-09 18:27	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Endpoint AV ...	110120	notice	Task 'Run AV Scan on Endpoint...' failed to exec...
18	04-09 18:27	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Incident Creat...	110243	notice	Task 'Create Incident' executed...
19	04-09 18:27	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Locking Up Ev...	110256	notice	Task 'Get Events' failed to exec...
20	06-09 18:27	FAZ-VMTM19008...	systems	playbook	run-stat	attachment	Endpoint Soft...	110105	notice	Task 'Get Endpoint Software In...' failed to exec...

Below the main table is a smaller table showing log details for the root ADOM:

Local-FortiGate	FGVM01TM19007951	root	Traffic	log.log
2 ISFW	FGVM01TM19007953	root	Event	elog.log
4 ISFW	FGVM01TM19007953	root	Traffic	tlog.log
5 self	FAZ-VMTM19008187	ADOM1	App Events	rlog.log

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

25

FortiAnalyzer applications, such as incident management and automation playbooks, generate local audit logs accessible in **Log View** under each ADOM. In the root ADOM, administrators can view both local event logs and the application logs of the root ADOM. Other ADOMs only show application logs.

To view details about application logs, use **Log Browse** as shown on the slide. Right-click **App Events**, and then select **Display** to see details. You can also download the log file.

# DO NOT REPRINT

## © FORTINET

### FortiView

- FortiView includes two panes:
  - FortiView
  - Monitors
- Each ADOM has its own data analysis in FortiView



FortiView is another way to view log data. FortiView includes the **FortiView** and the **Monitors** panes.

Each ADOM has its own data analysis on the FortiView pane, so ensure you are in the correct ADOM before viewing the contents of FortiView panes.

The FortiAnalyzer **FortiView** module can be disabled for performance tuning through the CLI. When disabled, the GUI hides FortiView and stop background processing for this feature.

To disable **FortiView** using the CLI:

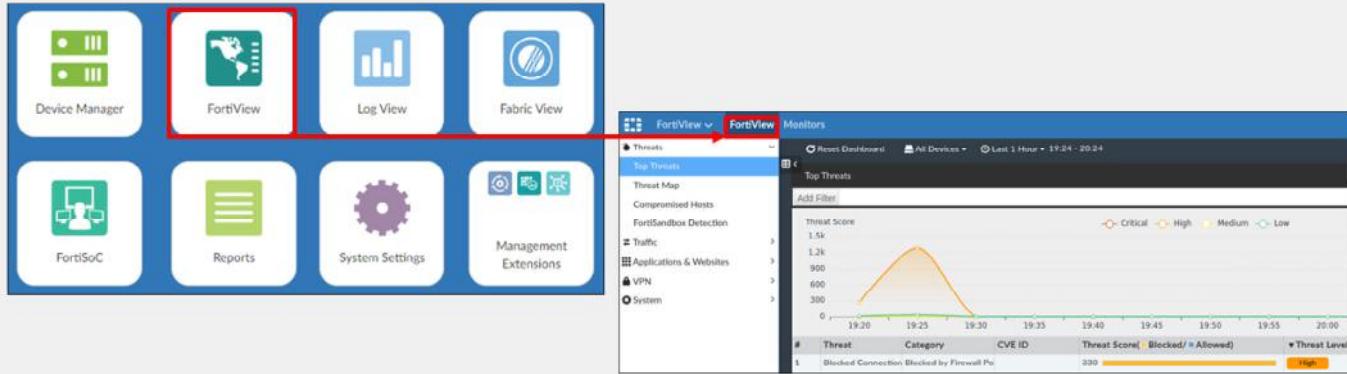
```
config system global
set disable-module fortiview-noc
end
```

# DO NOT REPRINT

## © FORTINET

### FortiView Pane

- Integrates real-time and historical data into single, summary views
- Analytics logs only (archive logs not displayed)



FortiView integrates real-time and historical data into single, summary views. Only data from analytics logs are available. Data from archive logs is not displayed.

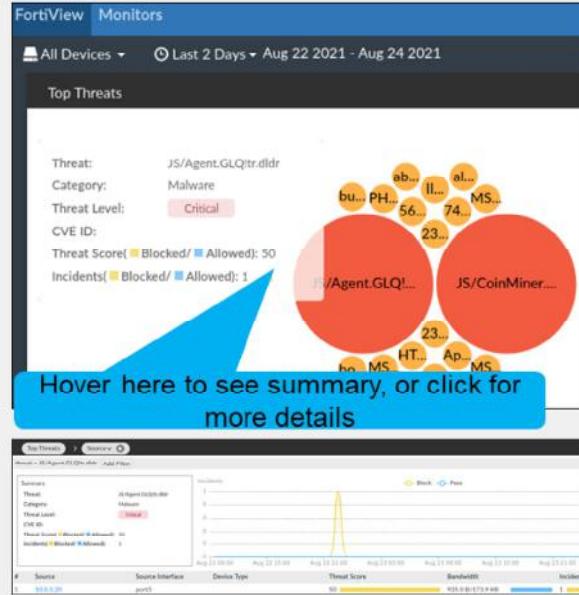
The **FortiView** pane allows you to use multiple filters in the consoles, enabling you to narrow your view to a specific time, by user ID or local IP address, by application, and others. You can use it to investigate traffic activity such as user uploads and downloads or videos watched on YouTube on a network-wide user group or on an individual-user level.

# DO NOT REPRINT

## © FORTINET

### FortiView Summaries for FortiGate, FortiCarrier, and FortiClient EMS

- View summaries of log data in both tabular and graphical formats
  - Threats
    - Top Threats, Threat Map, Compromised Hosts, FortiSandbox Detection
  - Traffic
    - Top Sources/Destinations/Country, Policy Hits, DNS Logs
  - Shadow IT
    - Top Cloud Applications, Top Cloud Users
  - Applications and Websites
    - Top Application/Website Domains/Website Categories/Browsing Users
  - VPN
    - SSL & Dialup VPN, Site-to-Site IPsec
  - System
    - Admin Logins/System Events/Resource Usage /Failed Authentication Attempts



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

28

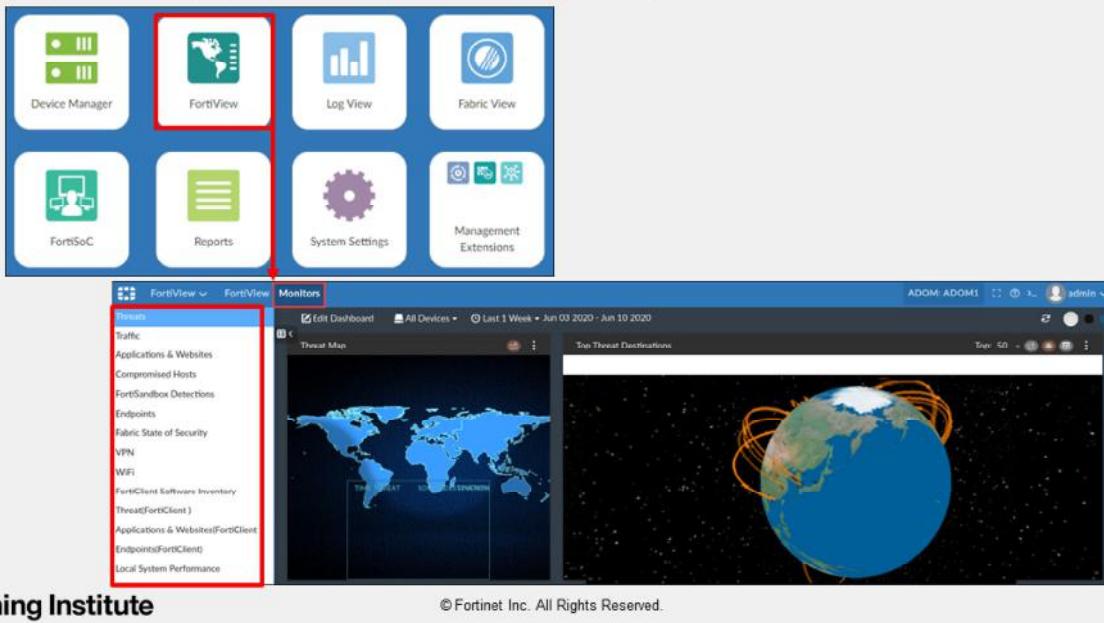
FortiView allows you to view summaries of log data in both tabular and graphical formats for FortiGate, FortiCarrier, and FortiClient EMS devices. For example, you can view top threats to your network, top sources of network traffic, and top destinations of network traffic, to name a few. For each summary view, you can drill down into details as well as set filters to display specific data.

# DO NOT REPRINT

## © FORTINET

### Monitors Pane

- Displays both real-time monitoring and historical trends



The **FortiView Monitors** pane is designed for a network and security operations center where multiple dashboards are displayed in large monitors in a SOC or NOC environment.

**Monitors** display both real-time monitoring and historical trends. This centralized monitoring and awareness helps you to effectively monitor network events, threats, and security alerts.

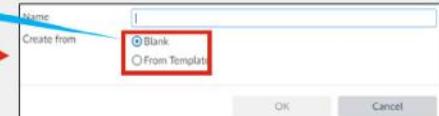
Use **Monitors** dashboards to view multiple panes of network activity, including threats, compromised hosts, applications, Wi-Fi security, system performance, endpoints, global threat research, and FortiClient software inventory, among several others.

**DO NOT REPRINT**  
**© FORTINET**

## Monitors Dashboard and Widgets Features

- Monitors dashboards and widgets features:
  - Add predefined or custom dashboards
  - For both predefined and custom dashboards, you can add, delete, move, or resize widgets
  - You can add the same widget or dashboard multiple times and apply different settings to each widget
  - Each widget monitors one activity
  - You can resize widgets or display a widget in full screen

Use Blank or Template



Change settings

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

30

FortiView **Monitors** dashboards and widgets are very flexible and allow you to do the following:

- Create predefined dashboards using templates or custom dashboards.
- Add, delete, move, or resize widgets for both predefined and custom dashboards.
- You can add the same dashboard multiple times on the same or different monitors.
- Monitor one activity on each widget.
- Add the same widget multiple times and apply different settings to each one. For example, you can add widgets to monitor the same activity using a different chart type, refresh interval, or time period.
- Resize widgets or display a widget in full screen.

For example, if one dashboard has too many widgets, create the same or a different dashboard to display widgets in a bigger size.

# DO NOT REPRINT

## © FORTINET

## Dashboards and Monitors

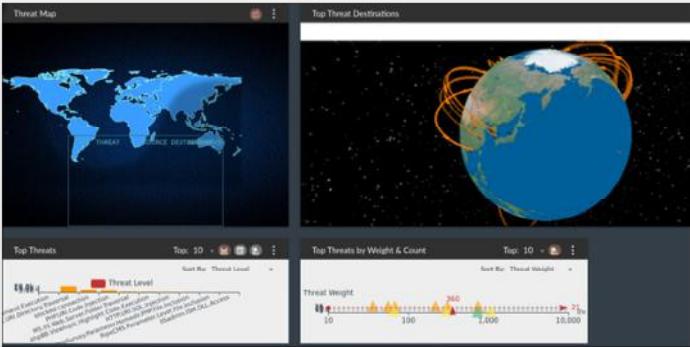
- Compromised Hosts



- Local System Performance



- Threats



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

31

**FortiView Monitors** includes predefined dashboards for Threats, Traffic, Application and Websites, Compromised Hosts, FortiSandbox Detection, Endpoints, VPN, WiFi, FortiClient Software Inventory, FortiClient (Threat, Application and Websites, and Endpoints), Local System Performance, Global Threat Research, and Secure SD-WAN Monitor. Each one of these dashboards can be customized by adding and removing the required widgets.

Here are the details of some dashboards:

- The **Threats** dashboard includes the following widgets:
  - This Top Threat Destinations, Top Threats, Threat Map, Top Threats by Weight & Count, and Top Virus Incidents Over Time.
- Compromised Hosts**
  - This monitor has only one widget showing compromised hosts. By default, this widget includes two panes: Compromised Hosts and Compromised Hosts Incidents (displayed as a world map).
- Local System Performance**
  - This dashboard monitors the system performance of the FortiAnalyzer unit running the FortiView module and not the logging devices. It includes CPU & Memory Usage, Multi-Core CPU Usage, Insert Rate vs Receive Rate, Receive Rate vs Forwarding Rate, Disk I/O, Resource Usage Average, Resource Usage Peak, Failed Authentication Attempts, System Events, and Admin Logins.
- The **Secure SD-WAN Monitor** dashboard includes the following widgets:
  - SD-WAN Performance Status, SD-WAN Rules Utilization, SD-WAN Utilization by Application, Top SD-WAN SLA Issues, Health Check Status, SD-WAN Events.

**DO NOT REPRINT****© FORTINET**

## Indicators of Compromise (Compromised Hosts)

- Indicators of compromise (IOC) engine detects end users with suspicious web usage compromises by checking new and historical logs against IOC signatures (based on a FortiGuard subscription)
- Uses today's FortiGuard threat intelligence to provide visibility of today's threats
- Flow:
  - FortiAnalyzer downloads threat intelligence FortiGuard package (TDS) every day
  - FortiGate sends security logs to FortiAnalyzer
  - FortiAnalyzer runs real-time threat detection when it receives the logs (FortiGate Web Filter logs)
  - Customers can see consolidated view of compromised devices in the FortiAnalyzer FortiView
- Breach detection engine parses logs into two main categories:
  - Infected (real breach)
  - Highly Suspicious (possible breach)

For reporting and a more historical audit of detections of malware, botnet, and intrusions, you can look at the threat report

One FortiView worth mentioning is IOC. The IOC engine detects end users with suspicious web usage compromises by checking new and historical logs against the IOC signatures, which are based on a FortiGuard subscription.

The breach detection engine on FortiAnalyzer uses FortiGuard Threat Detection Service (TDS) intelligence to analyze web filter logs for breach detection. TDS intelligence updates daily to reflect the real-world threat landscape. Note that the logs from AV/IPS, and so on, won't be used since those threats have already been detected or prevented by these services on FortiGate. When a threat match is found, a threat score is given to the end user based on the overall ranking score from TDS. When the check is completed, FortiAnalyzer aggregates all the threat scores of an end user and gives its verdict on the overall IOC of the end user. The verdict can be one of the following:

- **Infected:** indicates a real breach. A match or matches of the blacklisted IPs or domain generation algorithms (DGAs) have been found in the web logs.
- **Highly Suspicious:** indicates a possible breach.

For reporting and a more historical audit of detections of malware, botnet, and intrusions, you can look at the threat report.

**DO NOT REPRINT****© FORTINET**

## IOC Dependencies for Implementation

- One-year subscription to IOC
  - FortiAnalyzer includes an evaluation license, but it is restricted
- Web filter services subscription on FortiGate device(s)
- Web filter policies on FortiGate device(s) that send traffic to FortiAnalyzer
  - Breach detection or analytic engine runs against the FortiGate web filter logs to identify breaches related to web traffic

In order to configure IOC, you require the following:

- A one-year subscription to IOC. Note that FortiAnalyzer does include an evaluation license, but it is restrictive and only meant to give you an idea of how the feature works.
- A web filter services subscription on FortiGate device(s)
- Web filter policies on FortiGate device(s) that send traffic to FortiAnalyzer

# DO NOT REPRINT

## © FORTINET

### IOC/Compromised Host Example

The screenshot shows the FortiView interface. At the top, there's a table titled "Compromised Hosts" with columns: #, End User, Last Detected, Host Name, OS, Verdict, # of Threats, Acknowledge, and Device Name. A single row is selected for host 10.0.3.20, which has an "Infected" verdict, 3 threats, and an "Ack" status. Below this, a modal window titled "Compromised Hosts > Blocklist" is open, showing a dropdown menu with "Blocklist" and "Suspicious" options, where "Suspicious" is highlighted. The main pane displays threat details for host 10.0.3.20, including a summary table and a detailed list of 10 detected threats across various categories like Malware, Spyware, and Installation Traffic.

#	End User	Last Detected	Host Name	OS	Verdict	# of Threats	Acknowledge	Device Name
1	10.0.3.20	2021-08-22 22:34	10.0.3.20		Infected	3	Ack	FGVM01000007764

#	Detect Pattern	Threat Type	Threat Name	Category	Detect Method	# of Events	Security Action	Log Type	Device Name	Scan Time
1	54.83.43.69	Malware	CnC	Freeware Download infected-ip	infected-ip	3	server-rst	traffic	FGVM01000007764	2021-08-22
2	888544.com	Malware	CnC	Adult Materials	infected-domain	1	blocked	webfilter	FGVM01000007764	2021-08-22
3	rightstudent.net	Malware	CnC	Spyware and Malwa	infected-domain	1	blocked	webfilter	FGVM01000007764	2021-08-22
4	tt915.com	Malware	CnC	Pornography	infected-domain	1	blocked	webfilter	FGVM01000007764	2021-08-22
5	wellstart.net	Malware	CnC	Spyware and Malwa	infected-domain	1	blocked	webfilter	FGVM01000007764	2021-08-22
6	56834764387462384.org	Malware	Sinkhole	Not Rated	infected-domain	1	blocked	webfilter	FGVM01000007764	2021-08-22
7	zinomp3.com	Malware	CnC	Pornography	infected-domain	1	blocked	webfilter	FGVM01000007764	2021-08-22
8	ffb07fb6990e3b5da86d6r	Malware	CnC	Spyware and Malwa	infected-domain	1	passthrough	webfilter	FGVM01000007764	2021-08-22
9	http://192.210.173.40/file	Malware	InstallationTraffic	Spyware and Malwa	infected-url	1	passthrough	webfilter	FGVM01000007764	2021-08-22
10	xiv-i3cgc6bw6ctd.com	Malware	CnC	Spyware and Malwa	infected-domain	1	blocked	webfilter	FGVM01000007764	2021-08-22

**NSE Training Institute** © Fortinet Inc. All Rights Reserved. 34

This slide shows an example of an IOC hit in **FortiView**. The breach detection engine has determined a real breach, as indicated by the **Infected** verdict. The **# of Threats** column indicates there are three different threats associated with this hit. For the example shown on this slide they are: CnC, Sinkhole and Installation Traffic

On the IOC FortiView, you can also:

- Filter the entries by specifying devices or a time period.
- Acknowledge the IOC by clicking **Ack** in the **Acknowledge** column (you can still view acknowledged IOCs).
- Double-click an entry to drill-down and view threat details.

By double-clicking the desired entry, more details are displayed and you can filter the view based on two categories:

- Blocklist, which indicates items marked as infected after checking the blocklist included in the IOC database downloaded from FortiGuard.
- Suspicious, which indicates a match was found in the suspicious list included in the IOC database downloaded from FortiGuard, and further analysis is needed.

**DO NOT REPRINT**  
**© FORTINET**

## Resolve IP Address to Hostname

- Configure local DNS servers on FortiAnalyzer:

DNS	
Primary DNS Server	208.91.112.52
Secondary DNS Server	208.91.112.53

- Enter the following CLI command:

```
# config system fortiview settings
    set resolve-ip enable
end
```

May induce delay on FortiView  
while IPs resolve

- Best practice is to resolve IP addresses on FortiGate end
  - Gets both source and destination (FortiAnalyzer resolves destination IPs only)
  - Offloads the work from FortiAnalyzer

In FortiView, if the IP addresses are not resolved to a hostname, you must configure local DNS servers on FortiAnalyzer. Then, enter the CLI command shown on this slide.

This induces a slight delay on every FortiView refresh because it needs to resolve the IP addresses. In very large environments, the delay may be more noticeable, depending on the number of IPs that need to be resolved, as well as the speed of your DNS servers.

As a best practice, it is recommended to resolve IPs on the FortiGate end. This is because you get both source and destination, and it offloads the work from FortiAnalyzer. On FortiAnalyzer, this resolution does destination IPs only.

# DO NOT REPRINT

## © FORTINET

## Searching Archived Logs Through Log Fetching

- Retrieve archive logs from another FortiAnalyzer and then run queries or reports on those archived logs
  - Can select devices and time period to be indexed
  - Customize log retention settings for generating reports on older logs
  - Avoid log duplication
- FortiAnalyzers must run the same firmware version
- FortiAnalyzer fetch client queries the remote FortiAnalyzer fetch server to retrieve data
- Ensure:
  - ADOM has enough space for incoming logs!
  - Data policy supports fetching logs of the specified time period

Fetch Client: System Settings > Fetcher Management

1. On fetch client, create a profile for the fetch server:

Create New Profile	
Name	Fetch-server-profile
Server IP	10.0.1.211
User	fetchadmin
Password	*****
Confirm Password	*****

2. On fetch client, send fetch request:

Profiles	
<input type="button" value="Create New"/>	<input type="button" value="Edit"/>
<input type="button" value="Delete"/>	<input type="button" value="Request Fetch"/>
<input type="button" value="Sync Devices"/>	
<input type="checkbox"/> ▲ Name	Server IP
<input checked="" type="checkbox"/> Fetch-server-profile	10.0.1.211

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

36

Using FortiAnalyzer, you can enable log fetching. This allows FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer, which you can then run queries or reports on for forensic analysis. Log fetching greatly simplifies the generation of reports based upon log data by:

- Allowing the administrative user to select the devices and time period to be indexed
- Allowing customized log retention settings for the indexed logs pulled into the ADOM to suit the purpose of report generation based on older logs
- Avoiding log duplication, which can occur during an import from an external backup source

The FortiAnalyzer device that fetches logs operates as the fetch client, and the other FortiAnalyzer device that sends logs operates as the fetch server. Log fetching can happen only between two FortiAnalyzer devices, and both of them must be running the same firmware version. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end.

You can establish only one log-fetching session at a time between two FortiAnalyzer devices.

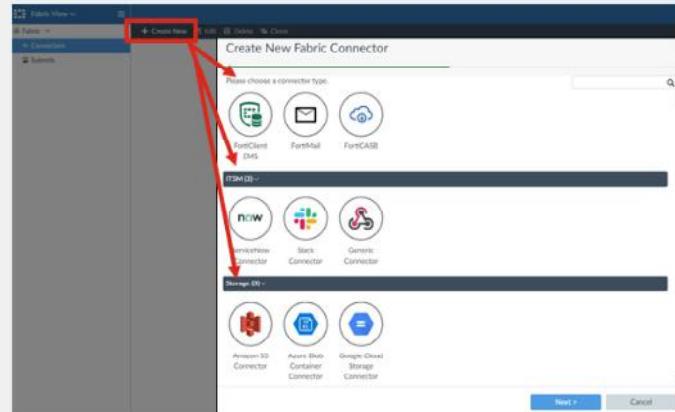
If you only have one FortiAnalyzer, log fetching is not an option. In this case, you would export and import the log file. You may want to delete the exported log file from the FortiAnalyzer prior to reimporting, so you would not have a duplicate copy of those logs in your archive.

# DO NOT REPRINT

## © FORTINET

### Fabric View

- **Fabric View** module enables:
  - To create fabric connectors
  - View the list of endpoints
- You can create the following connectors:
  - ITSM
  - Storage
  - Security Fabric



The **Fabric View** module enables you to create fabric connectors and view the list of endpoints. You can use FortiAnalyzer to create the following types of fabric connectors:

- ITSM connectors include:
  - ServiceNow
  - Webhook, a generic connector
- Storage connectors include:
  - Amazon S3
  - Microsoft Azure
  - Google Cloud
- Security Fabric connectors include:
  - FortiClient EMS to execute EMS operations on endpoints
  - FortiMail
  - FortiCASB

Once configured, Fabric connectors enrich incident response-related actions available on FortiSoC.

# DO NOT REPRINT

## © FORTINET

### Fabric View (Contd)

- **Asset Center** pane:

- To view endpoint and user information to make sure they are compliant
- Useful for incident response and compliance

The screenshot shows the Asset Center pane of the Fabric View interface. It displays a summary of users and endpoints. There are two large green circles: one for 'Total Users' (0) and one for 'Total Endpoints' (3). Below these are sections for 'Endpoint Name', 'User', 'MAC Address', 'IP Address', 'FortiClient (FUD)', 'Malware / O/S Software', and 'Vulnerabilities'. A table lists three endpoints with their details.

Endpoint Name	User	MAC Address	IP Address	FortiClient (FUD)	Malware / O/S Software	Vulnerabilities
192.0.1.10			192.0.1.10			Last User
192.0.3.20			192.0.3.20			Last Update
192.00.1.254			192.00.1.254			2021-04

- **Identity Center** pane:

- Displays a list of users and endpoints
- Correlate them with FortiAnalyzer modules
- Map user and endpoint

The screenshot shows the Identity Center pane of the Fabric View interface. It displays a summary of users and endpoints. There are two large green circles: one for 'Total Users' (6) and one for 'Total Endpoints' (3). Below these are sections for 'User Name', 'User Group', 'Endpoints', 'VPN IP', 'Identification Time', 'Last Seen', and 'Last Update'. A table lists six users with their details.

User Name	User Group	Endpoints	VPN IP	Identification Time	Last Seen	Last Update

The **Fabric View > Identity Center** pane displays a list of users and endpoints in the network from relevant logs, and correlates them with FortiAnalyzer modules. The **Identity Center** is useful for user and endpoint mapping. Some users might use multiple endpoints in the network, endpoints might use different interfaces to connect, network interfaces might have multiple IP addresses, and so on. A map of users and their endpoints gives you better visibility when you analyze logs, events, and incidents. This also helps with your reporting.

The **Fabric View > Asset Center** pane is the central location for security analysts to view endpoint and user information to make sure they are compliant. Endpoints are important assets in a network as they are the main entry points in a cybersecurity breach.

The **Asset Center** pane is useful for the following:

- Incident response: Check assets that are infected or vulnerable as part of your SOC analysis and incident response process.
- Compliance: Identify unknown and non-compliant users and endpoints.

Note that end-user information is limited if there is no FortiClient in your installation:

- Endpoints are detected based on MAC address and displayed by IP address instead of host name.
- User-related information might not be available.
- Detailed information such as OS version, avatar, and social ID information is not available.

**DO NOT REPRINT**

**© FORTINET**

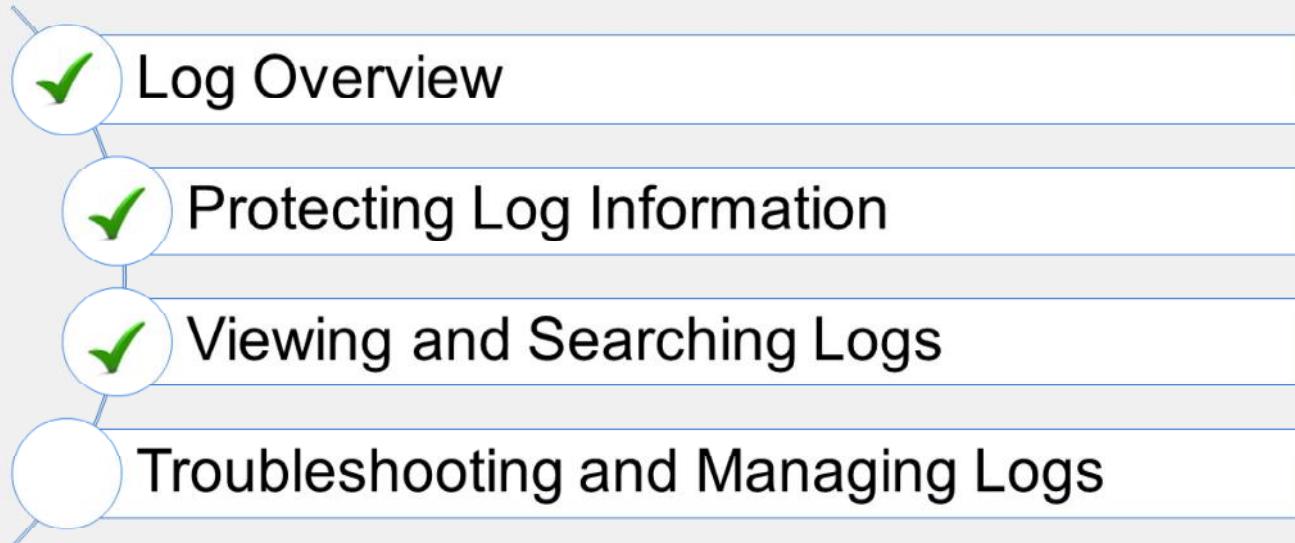
## Knowledge Check

1. Which FortiAnalyzer feature allows you to obtain the archived logs of specified devices from another FortiAnalyzer device?
  - A. Log forwarding in Aggregation mode
  - B. Log fetching
  
2. What is required to use IOC on FortiAnalyzer?
  - A. A valid IPS subscription on the FortiGate device(s)
  - B. A valid web filter subscription on the FortiGate device(s)

**DO NOT REPRINT**

**© FORTINET**

## Lesson Overview



Good job! You now understand how to view and search your logs.

Now you will learn how to troubleshoot and manage your logs.

**DO NOT REPRINT**

**© FORTINET**

## Troubleshooting and Managing Logs

### Objectives

- Gather log volume statistics
- Manage disk quota
- Explore logging best practices

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in troubleshooting and managing your logs, you will be able to ensure you do not lose valuable log data.

**DO NOT REPRINT**  
**© FORTINET**

## Gathering Log Rate and Device Usage Statistics

- Use the following FortiAnalyzer CLI commands to troubleshoot logging issues

Difference between log rate and message rate: one log message can consist of multiple logs in LZ4 format

What to Investigate	CLI Command to Use
What is the log receive rate for each second? What are the log receive rate totals? What is the device log rate? What is the log rate for each log type?	# diagnose fortilogd lograte # diagnose fortilogd lograte-total # diagnose fortilogd lograte-device # diagnose fortilogd lograte-type
What is the message receive rate for each second?	# diagnose fortilogd msgrate
What is the SQL insertion status?	# diagnose sql status sqlplugind
What is the device log usage for all logging devices?	# diagnose log device

In order to understand your log volume and whether your disk quota is configured appropriately, you can use the CLI commands shown on this slide to gather log rate and device usage statistics.

For example, if your log volume is too high, you won't be able to keep your logs in analytics and archive for the amount of time configured in the ADOM.

**DO NOT REPRINT**  
© FORTINET

## Gathering Log Rate and Log Volume per ADOM

- Use the following FortiAnalyzer CLI commands to calculate log rate and log volume per ADOM

What to Investigate	CLI Command to Use
What is the log receive rate for all ADOMs?	# diagnose fortilogd lograte-adom all
What is the log receive rate for a specific ADOM?	# diagnose fortilogd lograte-adom {adom-name}
What is the log volume for all ADOMs?	# diagnose fortilogd logvol-adom all
What is the log volume for a specific ADOM?	# diagnose fortilogd logvol-adom {adom-name}

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

43

In order to understand your log rate and log volume per ADOM, you can use the CLI commands shown on this slide to gather log rate and volume statistics. This is very useful in the environments where the FortiAnalyzer administrator has multiple ADOMs to manage multiple FortiGate devices, like in the case of MSSPs.

The log volume is given in GB/day.

# DO NOT REPRINT

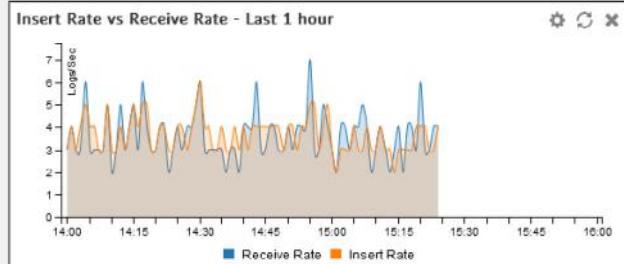
## © FORTINET

### Insert Rate vs. Receive Rate and Log Insert Lag

- **Insert Rate vs. Receive Rate**

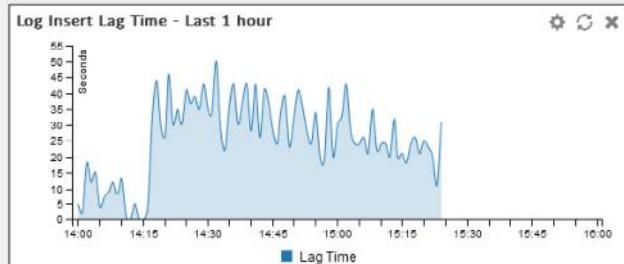
- Insert Rate = SQL Insertion Rate
  - Handled by **sqlplugin**
- Receive Rate = Raw Receiving Rate
  - Handled by **fortilogd**

#### System Settings > Dashboard



- **Log Insert Lag Time**

- Difference between log received and log inserted in the database



 NSE Training Institute

© Fortinet Inc. All Rights Reserved.

44

You can also view log insert rate, receive rate, and log insert lag time using the respective dashboard widgets. If these widgets are not already on the dashboard, you can add them by clicking **Toggle Widgets** on the upper-left and selecting the widgets from the list.

**Insert Rate vs. Receive Rate** is a graph that shows the rate at which raw logs reach the FortiAnalyzer (receive rate) and the rate at which they are indexed (insert rate) by the SQL database and the **sqlplugin** daemon. At minimum, the difference between these parameters should be generally consistent.

**Log Insert Lag Time** shows the amount of time between when a log was received and when it was indexed. Ideally, this parameter should be as small as possible with the occasional spikes according to the network activity being logged. A good baseline should be created to allow for the identification of possible performance issues.

# DO NOT REPRINT

## © FORTINET

### Increase ADOM Disk Quota

- Monitor log rate coming from each device # diagnose log device
- If high volume of logs exists, consider increasing ADOM log quota so the oldest logs are not lost
- Allocating insufficient quota to an ADOM can:
  - Prevent you from reaching your log retention objective
  - Cause unnecessary CPU resources enforcing quota with log deletion and database trims
  - Adversely affect reporting if the quota enforcement acts on analytical data before a report is complete



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

45

Based on your log rate and device usage statistics, you may need to adjust your ADOM disk quota so you don't lose valuable log data.

Always monitor your log rate for each device in the ADOM. If you have a high volume of logs, increase the ADOM quota so the oldest logs are not lost prematurely.

Allocating insufficient quota to an ADOM can cause many problems. It can:

- Prevent you from reaching your log retention objective
- Cause unnecessary CPU resources enforcing quota with log deletion and database trims
- Adversely affect reporting if the quota enforcement acts on analytical data before a report is complete

**DO NOT REPRINT**  
**© FORTINET**

## Rolling Logs and Auto-Deleting Old Logs

- How can you better manage your logs on disk?

- Roll log files when the size exceeds a set threshold

### System Settings > Advanced > Device Log Settings

Registered Device Logs

Roll log file when size exceeds  (10-1000)MB

Roll log files at scheduled time

Upload logs using a standard file transfer protocol

Upload logs to cloud storage

### System Settings > Advanced > File Management

Automatically Delete

<input checked="" type="checkbox"/> Device log files older than <input type="text" value="6"/> Months	Scheduled daily at time <input type="text" value="01:00"/>
<input checked="" type="checkbox"/> Reports older than <input type="text" value="6"/> Weeks	Scheduled daily at time <input type="text" value="01:00"/>
<input checked="" type="checkbox"/> Content archive files older than <input type="text" value="7"/> Days	Scheduled daily at time <input type="text" value="01:00"/>
<input checked="" type="checkbox"/> Quarantined files older than <input type="text" value="12"/> Months	Scheduled daily at time <input type="text" value="01:00"/>

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

46

Aside from increasing your disk log quota, what can you do to better manage your logs on disk?

You can:

- Specify a global log roll policy to roll or upload logs when the size exceeds a set threshold
- Specify a global automatic deletion policy for all log files, quarantined files, reports, and content archive files on FortiAnalyzer

**DO NOT REPRINT****© FORTINET**

## Logging Best Practices

- Upload FortiAnalyzer local logs to a remote server
- Increase local event logging level to debug
- Configure SNMP traps for critical system events
- Configure log upload for rolled logs on a daily basis

Here are some logging best practices:

- Upload FortiAnalyzer local logs to a remote server
- Increase local event logging level to debug
- Configure SNMP traps for critical system events
- Configure log upload for rolled logs on a daily basis

**DO NOT REPRINT****© FORTINET**

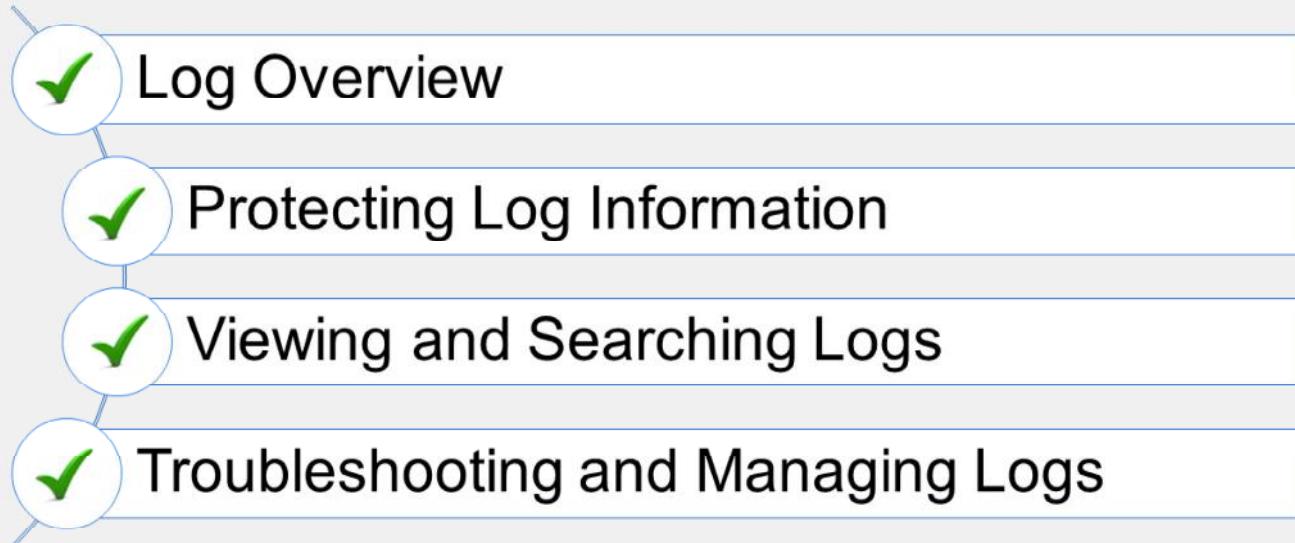
## Knowledge Check

1. Which data does the CLI command # diagnose fortilogd lograte provide?  
 A. The log receive rate per second  
 B. The message receive rate per second
  
2. Your ADOM data policy is set to keep logs in archive for 365 days, but the logs are being deleted prematurely from that ADOM and CPU resources are also high. What is the most likely problem?  
 A. The ADOM disk quota is set too low.  
 B. A global automatic deletion policy is set to delete device logs every six months.

**DO NOT REPRINT**

**© FORTINET**

## Lesson Overview



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Describe the purpose of collecting and storing logs
- ✓ Describe the log file workflow (archive and analytics)
- ✓ Understand high performance log storage (RAID)
- ✓ Perform log backups
- ✓ Configure log redundancy
- ✓ Configure log encryption
- ✓ View and search logs in Log View
- ✓ View summary data in FortiView
- ✓ Gather log volume statistics
- ✓ Manage disk quota

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use logs effectively in your system.

**DO NOT REPRINT**

© FORTINET



## FortiAnalyzer

FortiSoC—Incidents and Events



Last Modified: 1 December 2021

In this lesson, you will learn about the FortiSoC features in FortiAnalyzer, and how to configure them.

**DO NOT REPRINT**

**© FORTINET**

## Lesson Overview



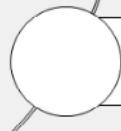
**FortiSoC Dashboards**



**Managing Events**



**Managing Incidents**



**Threat Hunting and Outbreak Alerts**

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will learn about the topics shown on this slide.

**DO NOT REPRINT**

**© FORTINET**

## FortiSoC Dashboards

### Objectives

- Understand FortiSoC features
- Understand Management extension applications
- Summarize FortiSoC dashboards information

After completing this section, you will be able to achieve the objectives shown in this slide. By demonstrating competence in understanding FortiSoC features and the FortiSoC dashboards, you will be able to use them efficiently in your network.

**DO NOT REPRINT****© FORTINET**

## FortiSoC Features



### Incident Management

- Incident / Case Management
- Indicators attachment for incidents
- API to FortiSOAR for Escalation



### SOC Automation

- FortiSOC Module
- Playbook Templates & Automation
- Connectors for Playbooks
- Visual Playbook Editor
- Playbook Execution
- Playbook Monitor



### Fabric Analytics

- SOC Analytics

The legacy SOC operation had many disadvantages that are not manageable in the dynamic world we live today. For example, it required analysts to handle too many alerts, often using separate interfaces, with the predictable loss of efficiency when trying to solve security breaches.

The FortiSoC module in FortiAnalyzer, provides a more complete solution for SOC analysts that include:

- **Incident Management:** Provides complete incident lifecycle management capabilities, including alerts, monitoring and escalation.
- **Automation:** Common tasks can be run without any manual intervention, leading to a much more efficient operation.
- **Fabric Analytics:** Provides visibility throughout the network from a single interface.

**DO NOT REPRINT**  
**© FORTINET**

## FortiSoC Features (Contd)

- FortiSoC provides the following capabilities in FortiAnalyzer:
  - SOAR (Security Orchestration, Automation and Response)
  - SIEM (Security Information and Event Management)
- Requires a subscription to run at full capacity
  - A trial with limited capabilities is included for testing purposes



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

5

FortiSoC is a subscription service that enables Security Orchestration, Automation, and Response (SOAR), and Security Information and Event Management (SIEM) capabilities on FortiAnalyzer.

The FortiAnalyzer SIEM capabilities parse, normalize, and correlate logs from Fortinet products and the security event log of Windows and Linux hosts (with Fabric Agent integration). Parsing is predefined by FortiAnalyzer and does not require manual configuration by administrators.

FortiSoC also provides incident management capabilities.

Additionally, playbook automation is supported to accelerate incident response times.

Fortinet offers two dedicated products, FortiSOAR and FortiSIEM, that expand these capabilities and add many others. FortiSOAR is available as stand-alone product and as a management extension application that can be installed in FortiAnalyzer.

**DO NOT REPRINT**  
**© FORTINET**

## Management Extensions

- Management extensions allow you to enable licensed applications and run them on FortiAnalyzer
- Management extensions are full-fledged running instances of a product in the form of a docker container
  - Allows you to use and monitor different solutions from Fortinet using a single pane of glass.
- Three management extension applications (MEAs) available in FortiAnalyzer:
  - FortiSOAR
  - FortiSIEM
  - Policy Analyzer



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

6

Management extensions allow you to enable licensed applications and run them on FortiAnalyzer.

A management extension application (MEA) is full-fledged running instance of a product in the form of a docker container. Installed MEAs enable you to use and monitor different solutions from Fortinet using a single pane of glass.

Three MEAs available:

- FortiSOAR: Includes a limited trial by default. Full functionality available when licensed.
- FortiSIEM: SIEM collector functionality only. Requires to be registered to a licensed FortiSIEM Supervisor.
- Policy Analyzer: Requires a FortiManager configured to manage FortiGate

**DO NOT REPRINT**  
**© FORTINET**

## Management Extensions (Contd)

- FortiSOAR
  - Allows you to manage your security operations using FortiAnalyzer and without the need of having a separate FortiSOAR instance.
- FortiSIEM
  - Alleviates the need for a separate FortiSIEM Collector node (Virtual machine or appliance), when you already have a FortiAnalyzer deployed
- Policy Analyzer
  - Works in conjunction with FortiManager to automatically install policy packages in managed FortiGate devices, based on the analysis of the logs received



Review the hardware requirements before you enable a management extension application. Some of them require a minimum amount of memory or a minimum number of CPU cores.

The FortiSOAR MEA allows you to manage your security operations using FortiAnalyzer and without the need of having a separate FortiSOAR instance. It is in fact a fully operational FortiSOAR instance.

The FortiSIEM MEA makes FortiAnalyzer a SIEM collector, alleviating the need for a separate FortiSIEM Collector node (Virtual machine or appliance), when you already have a FortiAnalyzer deployed

The Policy Analyzer MEA works in conjunction with FortiManager to automatically install policy packages in managed FortiGate devices, based on the analysis of the received logs.

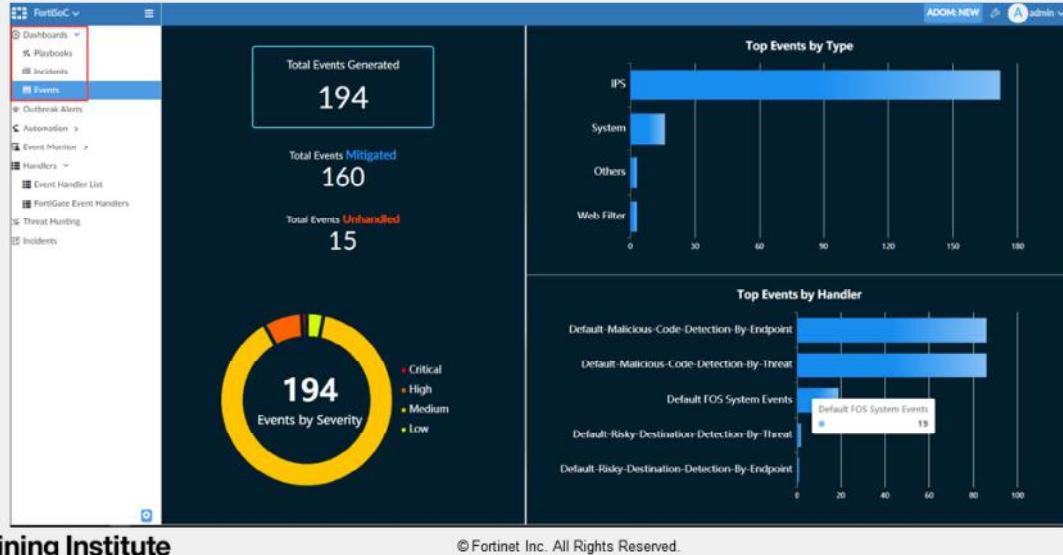
Review the hardware requirements before you enable a management extension application. Some of them require a minimum amount of memory or a minimum number of CPU cores.

For more information about each management extension, refer to the corresponding administrator guide in the *Fortinet Documentation Library*.

**DO NOT REPRINT**  
**© FORTINET**

## FortiSoC—Dashboards

- FortiSoC includes three dashboards
- Each dashboard provides a general overview and statistics for its respective item



8

FortiSoC includes three dashboards that provide a general overview and statistics about events, incidents, and playbooks in your environment. Data is presented in several formats and you can get more details by hovering your mouse over a section of the interest.

These dashboards enable customers to effectively monitor SOC productivity, and identify gaps to improve performance and efficiency.

Combined, these dashboards provide a good overview of how your SOC team is doing and if there are some areas that need to be improved.

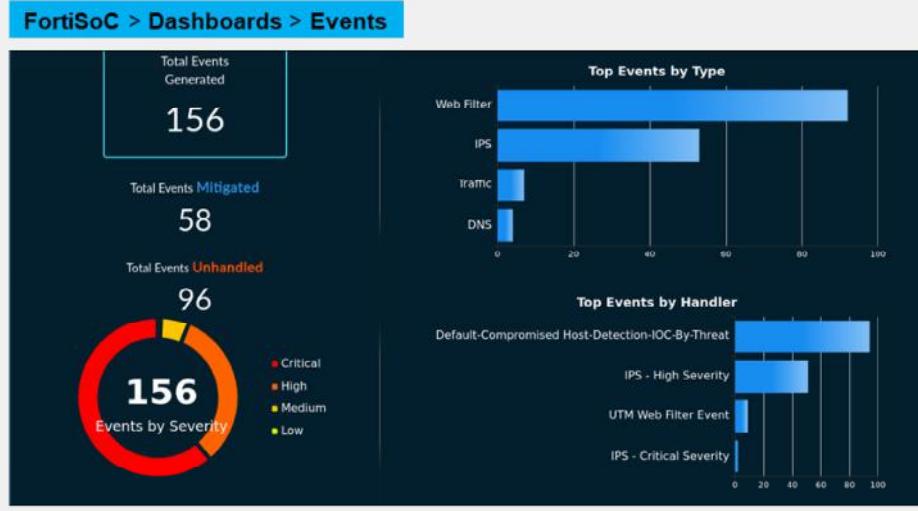
These dashboards are not customizable.

# DO NOT REPRINT

## © FORTINET

## Events Dashboard

- FortiSoC includes dashboards for playbooks, incidents, and events



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

The **Events** dashboard includes **Total Events Generated/Mitigated/Unhandled**, **Events by Severity**, **Top Events by Type**, and **Top Events by Handler**.

With this dashboard the SOC team will be able to easily identify what events will need to be addressed with more urgency based on their severity and status, as well as keep track of the most common event types occurring in the network. The information is provided in several graphic formats and using different colors for each event category.

For example, the slide shows that more than half of the events have been classified as critical and there are 96 events that are still unhandled.

**DO NOT REPRINT****© FORTINET**

## Incidents Dashboard

- FortiSoC includes dashboards for playbooks, incidents, and events

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

10

The **Incidents** dashboard includes **Total Incidents**, **Unsolved Incidents**, and **Incidents Timeline**.

This dashboard offers a clear representation of how many incidents need attention or are still being handled by the analysts. It also offers a color-coded representation of the incidents severity.

DO NOT REPRINT  
© FORTINET

## Playbooks Dashboard

- FortiSoC includes dashboards for playbooks, incidents, and events

FortiSoC > Dashboards > Playbooks



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

11

The **Playbooks** dashboard includes information about **Total Playbooks Executed**, **Total Playbook Actions Executed**, **Playbooks Executed**, and **Total Executed Playbooks and Actions Trend**.

This dashboard shows all the playbooks that have been executed in the last seven days, including their names, and the total number of actions performed. This gives an idea of how much time has been saved by automating tasks that would have been done manually.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. What are the three dashboards included in FortiSoC?  
 A. Threats, SIEM, and SOAR  
 B. Incidents, Events, and Playbooks

**DO NOT REPRINT**

**© FORTINET**

## Lesson Overview



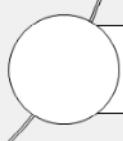
**FortiSoC Dashboards**



**Managing Events**



**Managing Incidents**



**Threat Hunting and Outbreak Alerts**

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

13

Good job! You now understand FortiSoC features and the dashboard.

Now, you will learn how to manage events.

**DO NOT REPRINT**  
**© FORTINET**

## Managing Events

### Objectives

- Understand how events are generated
- Manage event handlers
- Manage events

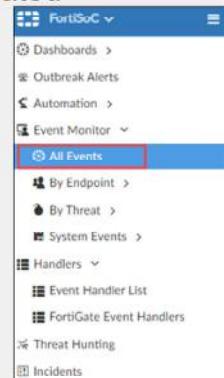
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in managing events and event handlers, you will be able to properly handle the security events taking place in your environment.

**DO NOT REPRINT**  
**© FORTINET**

## How Are Events Generated?

- FortiAnalyzer generates events based on the details included in the logs it receives
- Only logs matching specified criteria will generate events
- Event handlers are responsible of determining if an event needs to be created
  - Look for matches to a set of criteria and/or filters
  - Generate events only from analytics logs
- Many predefined event handlers available
  - Can be cloned and customized
  - Can also be created from scratch
- Generated events can be viewed under **Event Monitor**



After receiving logs from other devices, and based on the details included in them, FortiAnalyzer uses event handlers to determine if new events need to be generated.

Event Handlers look if the information in the logs matches a series of configurable criteria like threat type, device type, log type among many others.

FortiAnalyzer comes with several predefined Event Handlers that can be used out of the box, or can be cloned and customized. You can also create custom ones from scratch.

All generated events can be viewed under **Event Monitor**, where you can see them all combined or further divided by endpoint, threat, and system events.

**DO NOT REPRINT**  
**© FORTINET**

## Managing Event Handlers

- Event handlers look for specific conditions in the logs
- FortiAnalyzer comes with many predefined event handlers
- You can enable or disable them as needed
- You can clone and customize the predefined ones or create your own from scratch

Status	Name	Filters	Devices
<input checked="" type="checkbox"/>	Default-Malicious-Code-Detection-By-Endpoint	> 8 Filters	All Devices
<input checked="" type="checkbox"/>	Default-Risky-Destination-Detection-By-Endpoint	> 14 Filters	All Devices
<input checked="" type="checkbox"/>	Default-Compromised Host-Detection-IOC-By-Endpoint	> 3 Filters	All Devices
<input checked="" type="checkbox"/>	Default-Botnet-Communication-Detection-By-Endpoint	> 9 Filters	All Devices
<input checked="" type="checkbox"/>	Copy of Default-IPS_Signature_On_Hold CRITICAL	> 1 Filter	All Devices
<input checked="" type="checkbox"/>	Copy of Default-IPS_Signature_On_Hold HIGH	> 1 Filter	All Devices
<input type="checkbox"/>	Default FFW System Events	> 8 Filters	All Devices
<input type="checkbox"/>	Default-FFW-Compromised Host-Detection-IOC-By-Threat	> 3 Filters	All Devices

NSE Training Institute

16

An event handler looks for specific conditions in the logs and, if a match exist, will generate an event with details that can also be configured.

FortiAnalyzer includes many predefined event handlers that you can enable to generate events. They are available under **Event Handler List**.

If none of the predefined event handlers meets your requirements, you can clone and customize them or create new ones from scratch.

**DO NOT REPRINT**  
**© FORTINET**

## Event Handlers - Matching Filters

- The matching criteria for each event handler include:
  - Devices (by name)
  - Subnets
  - Pre-filters (exclusion filters)
  - Device type
  - Log Type/subtype (depends on Device type)
  - Log match (all or any)
  - Log field
  - Generic text filter (for more precise filtering)
- More than one filter can be configured to look for more specific matches
  - Individual filters can be enabled or disabled as needed

The screenshot shows the configuration of an event handler named "Sample Handler". It includes sections for Status, Name, Description, Devices (All Devices selected), Subnets (All Subnets selected), and Pre-filters. A single filter is defined, labeled "Filter 1", which specifies a log device type of FortiGate, a log type of Traffic Log (traffic), and a log subtype of Antivirus (virus). The group by condition is set to Destination Endpoint (dstendpoint). The logs match condition is set to "Any of the following conditions". A log field is selected as Level (pri) with a match criteria of Equal To and a value of Emergency. A generic text filter is also present.

To better understand the settings of event handlers, it helps to divide them in two logical sections.

The first section contains the fields that will need to be matched up against logs in order to generate events. The second section consists of what details will be added to the events generated if a match is found.

On the slide, the fields from the first section are shown. By configuring these fields, you can be as granular as needed to get only the relevant matches, hence, the required events.

Note that you can create several filters, each one with its own configuration. This can be used, for example, to look for matches on logs from different devices types.

You can also add a pre-filter, which is a common filter that will be applied before all other ones configured. The conditions on the pre-filter can then be used to limit which logs will be checked for matches by the other filters. Because of that, they are also known as *exclusion filters*.

# DO NOT REPRINT

## © FORTINET

## Event Handlers - Generic Text Filters

- Generic text filters allow more precise and flexible control over which logs will trigger an event
  - Multiple operators and logic are supported
- Supported operators:

Operator	Meaning
<code>==</code>	Equal (Exact match)
<code>!=</code>	Not equal (Not matching)
<code>&lt;</code>	Smaller than
<code>&lt;=</code>	Smaller than or equal
<code>&gt;</code>	Greater than
<code>&gt;=</code>	Greater than or equal
<code>~</code>	Contained (Included somewhere in the string)
<code>!~</code>	Not contained (Not included)

Tokens: '(', ')', '&', '|', 'and', 'or', 'not'

The screenshot shows the 'Generic text format' configuration in the FortiAnalyzer GUI. It includes a list of tokens and operators, and examples of log entries.

**Tokens:** '(', ')', '&', '|', 'and', 'or'  
**Operators:** '==', '!=', '<', '<=', '>', '>='

**Examples:**

```
dstip==192.168.1.168 and hostname ~ "facebook"
dstip==192.168.1.168 and ( dstport == 514 or dstport == 515 )
```

Syntax examples available in the GUI

Tip: Search your logs for the log file on which you want to add an event handler and copy the string you want to match

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

18

When configuring an event handler, the use of generic text filters allows more precise and flexible control over which logs will trigger an event. These filters use operators based on regex and the POSIX standard.

Multiple operators and logic are supported. You can hover your cursor over the question mark next to **Generic Text Filter** to display an example.

**Example:** `dstip==192.168.1.168 & hostname ~ "facebook"` will match all logs with a destination IP field equal to 192.168.1.168 and with the hostname field containing the string facebook in it.

Keep in mind you will need to use the escape character "\\" if you need to include a reserved character in your filter.

As a tip to avoid syntax errors, you can search your raw logs for the log file for which you want to add an event handler and copy/paste the string you want to match.

**DO NOT REPRINT**  
**© FORTINET**

## Events Details and Notifications

- If a match is found, the following settings will be used to generate an event:
  - Generate Alert When (event frequency)
  - Event Message
  - Event Status (Mitigated, contained, and so on)
  - Event Severity (from low to critical)
  - Tags (can be used to filter views )
  - Additional Info (extra relevant details)
  - Notifications (requires back end configuration)

The screenshot shows a configuration form for generating alerts based on event matches. It includes fields for 'Generate Alert When' (set to 'At least 1 Exact matches occurred over a period of 30 minutes'), 'Event Message' (set to '(Blank)'), 'Event Status' (set to 'Medium'), 'Event Severity' (set to 'Medium'), 'Tags' (empty), and 'Additional Info' (radio button selected for 'Use system default'). The 'Notifications' section contains several checkboxes for sending alerts through various methods: Send Alert through Fabric Connectors, Send Alert Email, Send SNMP(v1/v2) Trap, Send SNMP(v3) Trap, Send Alert to Syslog Server, and Send Each Alert Separately.

On the slide, the fields from the “second section” are shown. These refer to details that will be added to the event that will be created.

You can create custom messages in event handlers in the **Additional Info** section. The custom message can include variables and log fields that you consider relevant or important.

All the event information can be included in notifications sent by email, as SNMP traps, to a fabric connector, or to a syslog server. Using this feature, admins can see the event details without going into the logs. In order to use any of these notification methods, you must first set up the back end (for example, an email server for email notifications).

**DO NOT REPRINT**  
**© FORTINET**

## Exporting Event Handlers

- Event handlers are configured per ADOM
- To reuse existing event handlers, export them from one ADOM and import them in a different one
- Exported event handlers are saved using JSON format

The screenshot shows the 'Event Handler List' page in FortiSoC. A context menu is open over a selected event handler named 'Default-Botnet-Communication-Detect'. The menu includes options like 'Enable', 'Disable', 'Collapse All', 'Expand All', 'Show Predefined', 'Show Custom', 'Import', and 'Export'. The 'Export' option is highlighted with a red box.

The screenshot shows the 'Export Event Handler' dialog. It asks if you want to include Subnet Group information (unchecked) and offers two export formats: 'text' (radio button) and 'zipped' (radio button, selected). At the bottom are 'OK' and 'Cancel' buttons.

By default, event handlers are restricted to the ADOM where they were created. If you need to use the same settings in a different ADOM, exporting the event handlers will save you the time of creating them again.

To export an event handler, go to **Event Handler List**, select one or more handlers from the list, right click and select **Export**.

A new window will open where you need to choose if you want to include Subnet Group information and the type of file to be created, text or zipped. Click **OK** to finish and save the file.

Subnets and Subnet groups can be created in **Fabric View**, and they can be used as filters in Event Handlers and Reports.

Use the text format if you need to read the file in plaintext. The exported file is saved using a JSON format.

**DO NOT REPRINT**  
**© FORTINET**

## Importing Event Handlers

- To import an event handler go to the desired ADOM
- If there is a name conflict, FortiAnalyzer will add a time stamp to the imported handler

The screenshot shows the 'Event Handler List' page in FortiSoC. At the top, there are buttons for 'Create New', 'Edit', 'Delete', 'Clone', and 'More'. Below this is a table with columns for 'Status' and 'Name'. Several event handlers are listed, including 'Local Device Event', 'Default-Botnet-Communication-Detect', 'Default-Compromised Host-Detection', etc. On the right side of the table, there are checkboxes for 'Enable' and 'Disable', and dropdown menus for 'Collapse All' and 'Expand All'. Below the table, there are checkboxes for 'Show Predefined' and 'Show Custom'. At the bottom right of the table area, there is a red box around the 'Import' button.

The screenshot shows a modal dialog titled 'Import Event Handlers'. It contains a file upload section with a placeholder 'Upload file by drag & drop here or' and a 'Browse' button. Below this, it says 'inc test.json'. There is a question 'Do you want to proceed without Subnets?' followed by 'The data type is: zipped'. At the bottom are 'OK' and 'Cancel' buttons.

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

21

To import an event handler, go to **Event Handler List**, right click, and select **Import**.

A new window will open where you need to choose the desired JSON formatted file and click **OK**.

If the imported handler's name already exists, a timestamp will be automatically appended to the name of the one being imported.

**DO NOT REPRINT**  
**© FORTINET**

## Managing Events

- **Event Monitor** displays events generated by the configured event handlers

The screenshot shows the FortiSoC interface with the title "FortiSoC > Event Monitor > All Events". The main pane displays a table of events with columns: #, Event, Event Status, Event Type, Count, Severity, First Occurrence, Last Update, Additional Info, Handler, Tags, and Device Name. Below the table are two callout boxes: one pointing to an event row with the text "Double click an event for more details", and another pointing to a back arrow icon with the text "Click on the arrow to go back to the list of events". A smaller inset window titled "Add Filter" is shown, displaying a single event entry with columns: #, Date/Time, Device ID, Severity, Source, Destination IP, Action, Service, User, and Count.

#	Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info	Handler	Tags	Device Name
1	> Web.Client (3)	Mitigated	Application Control	234	Medium	7 hours ago	3 hours ago	Web.Client	appctrl custom		ISFW
2	> WS_FTP.Sensitive.File.A... (1)	Mitigated	IPS	8	Medium	8 hours ago	8 hours ago	...	Default-Malicious-Code-Det...		Local-FortiGate
3	> VoIP (2)		Application Control	64	Medium	7 hours ago	7 hours ago	VoIP	appctrl custom		ISFW
4	> Video/Audio (2)		Application Control	135	Medium	7 hours ago	7 hours ago	Video/Audio	appctrl custom		ISFW
5	> Update (1)		Application Control	1	Medium	7 hours ago	7 hours ago	Update	appctrl custom		ISFW
6	> Storage.Backup (3)		Application Control	54	Medium	7 hours ago	3 hours ago	Storage.Backup	appctrl custom		ISFW
7	> Social.Media (3)	Mitigated	Application Control	248	Medium	7 hours ago	3 hours ago	Social.Media	appctrl custom		ISFW

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

22

After event handlers start generating events, the latter can be examined in **All Events**.

You can see them all combined under **All Events**, or further divided by endpoint, threat, and system events.

Double-clicking an event provides more details about it, including the information from the associated logs.

**DO NOT REPRINT**  
**© FORTINET**

## Available Management Actions For Events

- You can acknowledge an event, add a comment, assign it to an administrator, or create an incident from it.

The screenshot shows the FortiSoC Event Monitor interface with the title 'FortiSoC > Event Monitor > All Events'. The main table lists 10 events, each with columns for #, Event, Event Status, Event Type, Count, Severity, and First Occurred. A red box highlights the 'Add Filter' button at the top left. A blue callout points to this button with the text 'Right click an event to see the list of available actions'. Another blue callout points to the 'Show Acknowledged' checkbox at the top right with the text 'Acknowledged events are not shown by default'. The right-click context menu for the first event (ID 1) is displayed, showing options: Acknowledge (checked), Comment (checked), Assign To, View Log, Create New Incident (highlighted with a red box), Add to Existing Incident, Search in Log View, and two search filters: 'Search "Event Type=app-ctrl"' and 'Search "Event Type!=app-ctrl"'. A blue callout points to the 'Create New Incident' option with the text 'Create incidents for further investigation'. A blue callout points to the search filters with the text 'Filter based on the columns values'.

Right-clicking on an event allows you to leave a comment for your records, to acknowledge the event, to assign it to an administrator (or yourself) for further investigation, or to create an incident from it. Incidents will be discussed in the next section.

Acknowledging an event removes it from the event list but it can be shown again by clicking **Show Acknowledged**.

Additionally, you can use filters to display only the events of interest. You can filter events based on any of the columns available in this view.

# DO NOT REPRINT

## © FORTINET

### Events Statuses

- Events can be in one of four statuses
  - It is important to understand what each one of them means

<input type="checkbox"/>	#	Event	Event Status
<input checked="" type="checkbox"/>	1	> Cross.Site.Scripting (2)	Mitigated
<input type="checkbox"/>	2	> 10.0.1.10 (36)	Unhandled
<input type="checkbox"/>	3	> 10.200.1.254 (36)	Unhandled
<input type="checkbox"/>	4	> Nikto.Web.Scanner (6)	Unhandled
<input type="checkbox"/>	5	> redginapic.blogspot.com (2)	Mitigated
<input type="checkbox"/>	6	> 10.0.3.20 (12)	Unhandled
<input type="checkbox"/>	7	> theameridesk.com (2)	Unhandled
<input type="checkbox"/>	8	> HTTP.URI.Script.XSS (2)	Mitigated
<input type="checkbox"/>	9	> www.blissyogawithannu.co...	Mitigated

Event Status	Description
Unhandled	The security event risk is not mitigated or contained, so it is considered open
Contained	The risk source is isolated
Mitigated	The security risk is mitigated by being blocked or dropped
Blank	Other scenarios

Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not.

The possible statuses are:

- Unhandled:** The security event risk is not mitigated or contained, so it is considered open.  
For example, an IPS/AV log with `action=pass` will have the event status **Unhandled**.  
Botnet and IoC events are also considered **Unhandled**.
- Contained:** The risk source is isolated.  
For example, an AV log with `action=quarantine` will have the event status **Contained**.
- Mitigated:** The security risk is mitigated by being blocked or dropped.  
For example, an IPS/AV log with `action=block/drop` will have the event status **Mitigated**.
- (Blank):** Other scenarios

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. What are event handlers?
  - A. Threats identified by FortiGuard
  - B. Specific matched conditions in the logs
  
2. What file format is used for exported event handlers?
  - A. JSON
  - B. CSV

**DO NOT REPRINT**

**© FORTINET**

## Lesson Overview



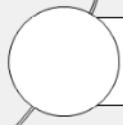
**FortiSoC Dashboards**



**Managing Events**



**Managing Incidents**



**Threat Hunting and Outbreak Alerts**

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

26

Good job! You now know how to manage events.

Now, you will learn how to manage incidents.

**DO NOT REPRINT**

**© FORTINET**

## Managing Incidents

### Objectives

- Create incidents
- Analyze incidents
- Configure incident settings

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in managing incidents, you will be able to improve your efficiency in investigating security incidents in your organization.

# DO NOT REPRINT

## © FORTINET

## Creating an Incident

- An incident should be created when an event needs further analysis
- Incidents can be created manually or automatically (with a playbook)

The screenshot illustrates the process of creating an incident from an event in FortiAnalyzer. It consists of three main panels:

- FortiSoC > Events > All Event**: Shows a list of events with columns for #, Event, Event Type, Count, and Severity. An event (ID 1) is selected, and a context menu is open, with the "Create New Incident" option highlighted.
- Raise Incident**: A modal dialog box where incident details are being entered. The fields include Incident Category (Unauthorized Access), Severity (High), Status (New), Affected Endpoint (10.0.1.10), and Description. The "Assigned To" field is set to "admin". The "OK" button is highlighted with a red arrow.
- FortiSoC > Incidents**: Shows a list of incidents with columns for #, Incident Number, Incident Date, Incident Reporter, Incident Category, and Severity. Two incidents are listed: Incident 1 (IN00000002) with category Malicious Code and severity Medium; and Incident 2 (IN00000001) with category Unauthorized Access and severity High. Incident 2 is highlighted with a red arrow.

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

28

Not all events have the same impact or importance on your network. Some of them might need to be further analyzed to prevent or mitigate security breaches. When an analyst finds an event that requires further scrutiny, a new incident should be created from that event. An incident can be seen as an event that can have some negative consequence in your everyday operations.

Incidents can be created manually or, preferably, automatically with the use of playbooks, taking advantage of FortiAnalyzer automation capabilities.

In FortiAnalyzer, incidents are manually created from **Event Monitor** by right-clicking on the desired event and selecting the corresponding option. Incidents can also be created from one of the default views under **Event Monitor**.

Every incident includes a category, severity, status, affected endpoint and, optionally a description and an assigned admin.

Once created, incidents can be viewed at **Incidents**.

**DO NOT REPRINT**  
**© FORTINET**

## Analyzing an Incident

The screenshot shows the FortiSoC interface for analyzing an incident. The main header is "FortiSoC > Incidents". The incident details are for IN00000002, which is a "Malicious Code" incident assigned to "remote-admins" and is "New". The "Affected Endpoint/User" section shows no related user available. The "Executed Playbooks" section is empty. The "Audit History" section shows a timeline from 2021-09-08 18:57:00 to NOW, with events attached to the incident. One event is labeled "New Incident Created" and another is "Incident IN00000002 is created." The "Incident Timeline" shows activity from 2021-09-07 16:18:40 to 2021-09-07 20:52:45. At the bottom, there are tabs for Comments, Events, Reports, Indicators, Affected Assets, Processes, Software, and Vulnerabilities. The "Events" tab is selected, showing two entries:

#	Event	Event Status	Event T Count	Severity	First Occurrence	Last Update	Additio...	Handler Tags	Device
1	appc...	■ A...	98	Medium	2021-09-07	07 16:29:56	Web...	appc...	ISFW
2	appc...	■ A...	131	Medium	2021-09-07	07 16:52:05	Web...	appc...	ISFW

**NSE Training Institute** © Fortinet Inc. All Rights Reserved. 29

To view an incident's details, go to **Incidents**, and double-click on the desired one. You can also right-click on an incident and select **Analysis**.

The analysis page provides all the relevant information and access to the tools an admin will need to perform a full investigation of the incident. Some of the details shown in this page include: the affected endpoint and user (if available), the incident's timeline, any executed playbooks and the ability to run them, audit history with any attached events and reports, and several more.

At the bottom, these tabs provide more details: **Comments**, **Events**, **Reports**, **Indicators**, **Affected Assets**, **Processes**, **Software**, and **Vulnerabilities**.

For example, under the **Comments** tab you will see any comments added by other analysts, and you will be able to add new ones.

The list of events associated to the incident is also available under the tab with that name. From here, you can access the related logs by right clicking on the event of interest. This will open **Log View** on a different window.

Existing reports, and the ability to create new ones, is also possible under the **Reports** tab.

**DO NOT REPRINT**

**© FORTINET**

## Editing an Incident

- Update each incident setting while working in it
- It is important to keep all settings up to date
- Close any solved incident
- Once closed you can delete the incident from the list
- Notifications can be configured for each status change

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

30

It is important to keep all incidents settings up to date. This will allow you to keep track of the work being done to solve them.

When an incident is considered closed, its status should be changed accordingly. Additionally, solved incidents can be deleted from the list.

FortiAnalyzer can be configured to send notifications after any changes to an incident status.

DO NOT REPRINT  
© FORTINET

## Configure Incidents Settings

The screenshot shows the FortiSoC interface. At the top, there's a navigation bar with 'FortiSoC > Incidents'. Below it is a table with two rows of incident data:

#	Incident Number	Incident Date / Time	Incident Reporter
1	IN00000002	2021-08-08 00:29:40	admin
2	IN00000001	2021-08-31 21:51:36	admin

A red arrow points from the bottom of the table down to a 'Notifications' section. This section includes a 'Fabric Connector 1' dropdown set to 'Connector1' and three checkboxes:

- Send notification when an incident is created
- Send notification when an incident is updated
- Send notification when an incident is deleted

Incidents will usually go through several stages during the analysis process. In most cases, it is important to make sure all parties involved are notified when the incident status is updated.

You can configure FortiAnalyzer to send a notification to external platforms using preconfigured fabric connectors.

To configure notifications, go to **Settings**, select a fabric connector from the dropdown list and choose the incident activity for which you wish to send the notifications.

You can add more than one fabric connector, each with the same or different notification settings. The receiving side of the connector must be configured for the notifications to be sent successfully.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. When would a security administrator raise an incident?
  - A. To change the status of an incident to “Unhandled”
  - B. To further analyze events of interest
  
2. What is required to send notifications about incident updates?
  - A. Existing fabric connectors
  - B. Attaching a report to an incident

**DO NOT REPRINT**

**© FORTINET**

## Lesson Overview



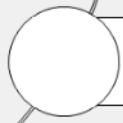
**FortiSoC Dashboards**



**Managing Events**



**Managing Incidents**



**Threat Hunting and Outbreak Alerts**

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

33

Good job! You now understand how to manage incidents.

Now, you will learn how about threat hunting and outbreak alerts..

**DO NOT REPRINT****© FORTINET**

## Threat Hunting And Outbreak Alerts

### Objectives

- Understand threat hunting
- Use the log count chart
- Use SIEM log analytics table
- Understand outbreak alerts

After completing this section, you should be able to achieve the objectives shown on this slide.

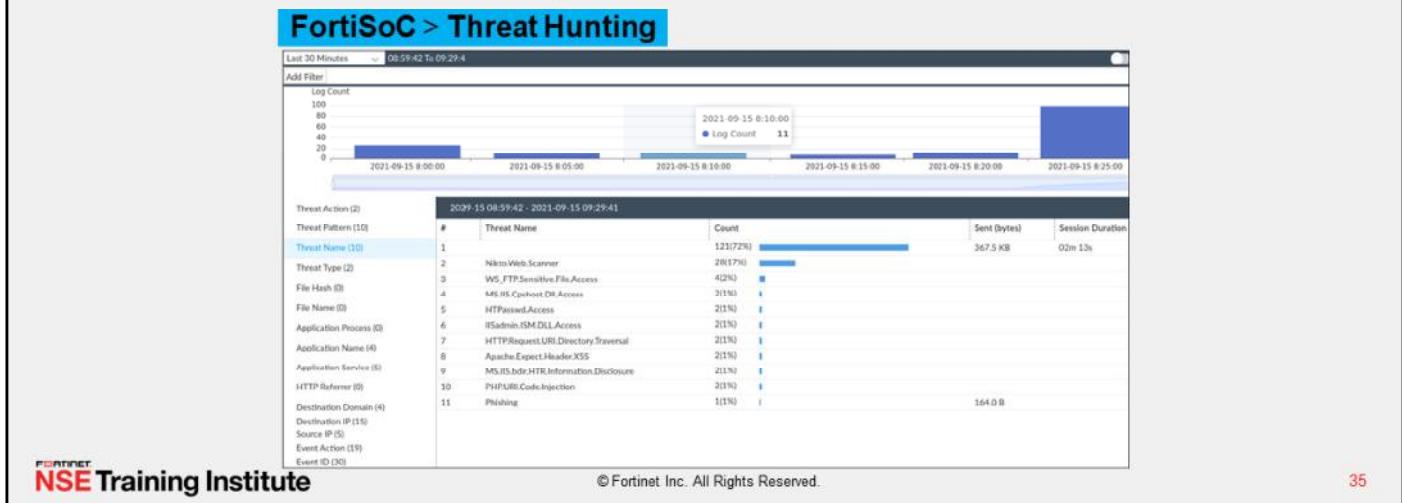
By understanding how to use the threat hunting and the outbreak alerts tools, you will be able to use a more proactive approach in your SOC duties and keep your FortiAnalyzer updated with the latest outbreak information provided by FortiGuard.

# DO NOT REPRINT

## © FORTINET

## Threat Hunting

- Threat hunting consists in proactively searching for suspicious or potentially risky network activity that may have gone undetected
- The **Threat Hunting** pane in FortiSoC takes advantage of the SIEM framework to allow for advanced correlation and analysis to hunt for threats



Threat hunting consists in proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach will help administrator find any threats that might have eluded detection by the current security solutions or configurations.

FortiSoC includes the **Threat Hunting** pane which offers a SOC analytics dashboard using the SIEM database.

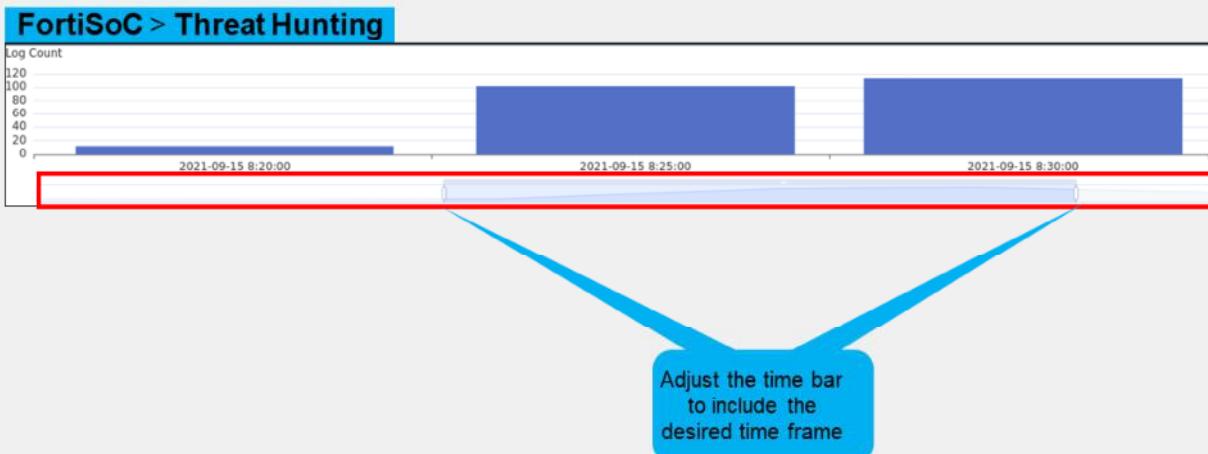
**Threat Hunting** uses cached data to allow SOC analysts to quickly drilldown on logs in fields of interest. To view the **Threat Hunting** dashboard, go to **Threat Hunting**. This dashboard includes a Log Count chart and SIEM log analytics table.

To change the displayed time range, select a time from the dropdown in the top-left corner of the dashboard. You can configure custom time ranges by selecting either *Last N Minutes*, *Last N Hours*, or *Last N Days*. Apply filters to the dashboard using *Add Filter* or by right-clicking on a value in the table and selecting the corresponding filter. Only logs matching the selected time range and filter are displayed in the SIEM log analytics table.

**DO NOT REPRINT****© FORTINET**

## Log Count Chart

- The Log Count chart allows the administrators to narrow down what logs will be analyzed based on a time range
- The details shown in the SIEM log table will adjust to the timeframe selected in this chart

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

36

A chart displaying the total log count during the specified time range is presented at the top of the **Threat Hunting** dashboard. This section is called the **Log Count** chart.

You can zoom in and out on the displayed time range by using your mouse's scroll wheel or by adjusting the time bar below the graph. You can adjust the time bar by dragging the start and stop bars on either side of the selected time range, or by clicking and dragging the entire time range to the left or right. For example, you could search for suspicious activity occurring during off work hours.

Only logs displayed within the time period visible in the chart are shown in the SIEM log analytics table.

**DO NOT REPRINT**  
**© FORTINET**

## SIEM Log Analytics Table

- The SIEM log analytics table contains many critical elements to gain insights in SOC
- Statistical data is available for each field of interest and log details can be viewed and filtered for better analysis

FortiSoC > Threat Hunting

2021-09-15 09:09:02 - 2021-09-15 09:39:01

#	Threat Name	Count	Sent (bytes)	Session Duration
1	Nikto.Web.Scanner	187(58%)	371.1 KB	01m 33s
2	HTTPRequest.URI.Directory.Traversal	57(18%)		
3	HTTPGet.Request.Directory.Traversal	32(10%)		
4	Novell.NetBasic.Scripting.Server.Directory.Traversal	16(5%)		
5	WS_FTP.Sensitive.File.Access	4(1%)		
6	MS.IIS.Web.Server.Folder.Traversal	4(1%)		
7	Php.Exe.Disclosure	4(1%)		
8	Apache.DOS.Batch.Script.Parsing.Command.Execution	2(1%)		
9	MS.IIS.Cpshost.Dll.Access	2(1%)		
10	HTPasswd.Access	2(1%)		
11	IISadmin.ISM.DLL.Access	2(1%)		
12	HTTPGET.Request.Directory.Traversal	2(1%)		
13	NaviCOPA.Source.Code.Information.Disclosure	2(1%)		
14	Apache.Expect.Header.XSS	2(1%)		
15	MS.IIS.bdir.HTR.Information.Disclosure	2(1%)		
16	PHPURI.Code.Injection	2(1%)		
17	Phishing	1(< 1%)	164.0 B	

Select the desired element to get details and statistics

Double click to see log details

NSE Training Institute © Fortinet Inc. All Rights Reserved. 37

The SIEM log analytics table contains a list of fields of interest in the left pane as well as the analytics table on the right. The information displayed matches the time frame selected on the Log Count chart.

Click on the desired field from the left pane to view corresponding data in the table. The table displays detailed statistics, including count (number of logs), percentage, sent bytes and session duration information.

Double-click an item in the table to open the detailed log information. The resulting view includes the same filtering functions available in **Log View** without the need to leave the page.

**DO NOT REPRINT**  
**© FORTINET**

## Outbreak Alerts Overview

- Licensed feature
- Allows customers to receive information about malware outbreaks
- Automatically downloads new event handlers and reports related to the outbreaks
- Each alert consists of:
  - FortiGuard report
  - Event Handler
  - Report template

The screenshot shows the FortiSoC interface with the 'Outbreak Alerts' section selected. It details the 'DearCry Ransomware' threat, mentioning the earliest vulnerability detection on January 6, 2021, Microsoft's announcement on March 11, 2021, and latest developments on March 12, 2021.

Date	Category
January 6, 2021	Earliest Vulnerability Detection
March 11, 2021	MSFT Announcement
March 12, 2021	Latest Developments

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

38

The FortiAnalyzer Outbreak Alert Service is a licensed feature that allows FortiAnalyzer administrators to receive and view outbreak alerts, and automatically download related event handlers and reports from FortiGuard. Outbreak event handlers and reports are created in real-time by Fortinet to detect and respond to emerging outbreaks.

Outbreak alerts from Fortinet are displayed in the **Outbreak Alerts** pane and are available on all ADOMs.

**DO NOT REPRINT**  
**© FORTINET**

## Outbreak Alerts Handlers and Reports

The screenshot shows the FortiSoC interface with the following sections:

- Left Sidebar:** Handlers > Event Handler List, FortiGate Event Handlers, Threat Hunting, Incidents.
- Top Right Panel:** Default-Compromised Host-Detection-IOC-By-Endpoint, listing several event handlers with green checkmarks. A red box highlights the list, and a callout bubble says: "Event handlers downloaded through the outbreak alerts service".
- Middle Panel:** Network Reports, Outbreak Alert Reports, SOC Reports. A red box highlights the Outbreak Alert Reports section, which contains three reports: Outbreak Alert - DearCry Ransomware Detection Report, Outbreak Alert - MS.Exchange-HAFNIUM Attack Detection Report, and Outbreak Alert - SolarWinds Compromised Host Detection Report. A callout bubble says: "Reports downloaded via the outbreak alerts service".

- The new event handlers will be added to the list of available handlers, and they can be used in the same way as the rest in the list. They can be cloned, exported, imported, and so on
- The same is true for the newly downloaded reports

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

39

Once downloaded, the new handlers are available under the Event Handler list, and they can be used in the same ways described in an earlier section. That is, they can be cloned, exported, imported, and so on.

The same is true for the new reports.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. What feature allows for the automatic download of new event handlers?  
 A. Threat hunting  
 B. Outbreak alerts

**DO NOT REPRINT**

**© FORTINET**

## Lesson Overview



**FortiSoC Dashboards**



**Managing Events**



**Managing Incidents**



**Threat Hunting and Outbreak Alerts**

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

41

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Understand FortiSoC features
- ✓ Summarize FortiSoC dashboards information
- ✓ Manage event handlers
- ✓ Create and analyze incidents
- ✓ Understand threat hunting
- ✓ Use the log count chart
- ✓ Use SIEM log analytics table
- ✓ Understand outbreak alerts

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to use FortiSoC components, FortiSoC features, and how to use them in your network.

**DO NOT REPRINT**

© FORTINET



## FortiAnalyzer

FortiSoC—Playbooks



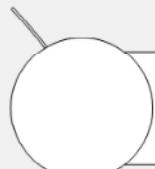
Last Modified: 1 December 2021

In this lesson, you will learn how to use the automation capabilities included in FortiAnalyzer.

DO NOT REPRINT

© FORTINET

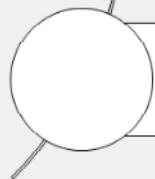
## Lesson Overview



### Playbook Components



### Creating Playbooks



### Managing Playbooks

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

2

In this lesson, you will explore the topics shown on this slide.

**DO NOT REPRINT****© FORTINET**

## Playbooks' Components

### Objectives

- Understand FAZ automation capabilities
- Understand playbook concepts
- Understand trigger types and characteristics
- Understand connector types
- Understand playbook tasks

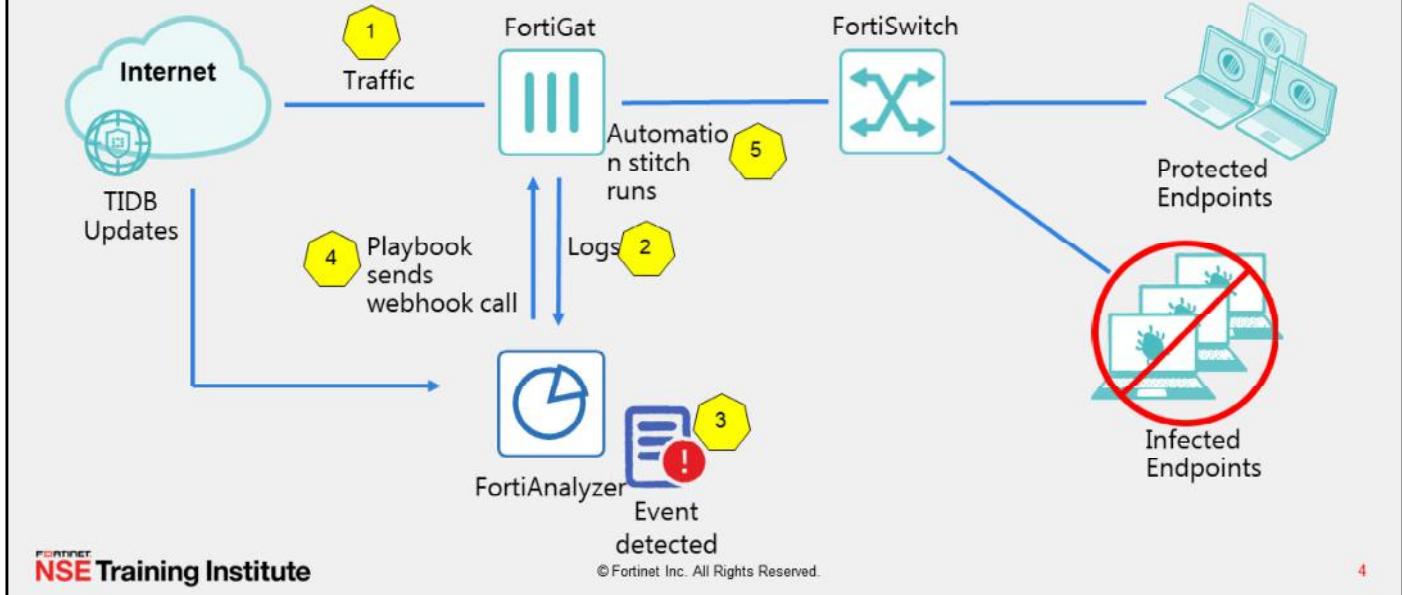
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the purpose of playbooks and their components, you will be able to use playbooks effectively.

# DO NOT REPRINT

## © FORTINET

### The Big Picture



Automation is a critical aspect for security teams facing the ever-changing threat landscape.

FortiAnalyzer allows SOC analysts to automate common and repetitive tasks using playbooks.

FortiAnalyzer works with standalone devices, but it is also integrated with the Security Fabric. This integration, allows it to communicate with other devices in the fabric to detect security events, and trigger corrective or preventive actions automatically.

You can create playbooks that automatically generate a report, or instructs a FortiGate device to quarantine an compromised host. The available actions depend on the device type. Using devices compatible with the security fabric allows us to exploit the fabric capabilities to their full extent.

One possible scenario is shown on the slide:

1. Traffic flows through the FortiGate
2. FortiGate sends logs to FortiAnalyzer
3. FortiAnalyzer detects some suspicious traffic and generates an event
4. The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate so that it runs an automation stitch
5. FortiGate runs the automation stitch with the corrective or preventive actions

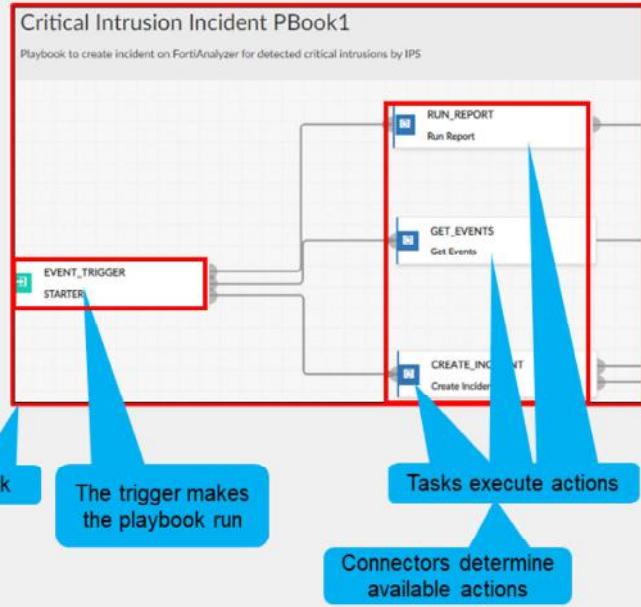
In this lesson you will explore these important capabilities.

# DO NOT REPRINT

## © FORTINET

## Playbook Concepts

- Playbooks allow you to automate common SOC tasks
  - They are created per ADOM
- Playbooks have only one trigger
  - Determines when playbook is to be executed
- Playbooks have one or more tasks
  - Automated actions that will take place
- The actions that can be performed by a task depend on the connector used
  - Different devices allow different actions
- Playbooks can be created from built-in templates or from scratch
- Playbooks are created using an intuitive playbook designer
  - Flow diagrams help to visualize work flow



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

5

Playbooks include a starter event (trigger), that determines when a playbook is to run, and one or more tasks to be executed.

After a playbook is triggered, it flows through the existing tasks defined within the playbook designer.

Each task includes the automated action that needs to take place. The available actions depend on the connector used. Connectors allow tasks to be performed on supported devices.

You can create playbooks from scratch or using predefined templates. Playbooks are available only in the ADOM where they were created, unless they are exported to a different ADOM.

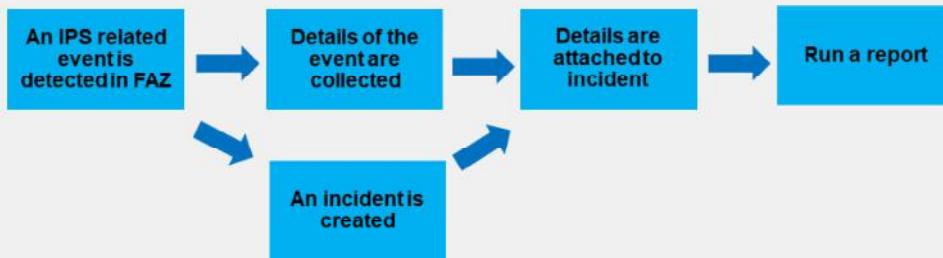
**DO NOT REPRINT**  
**© FORTINET**

## Playbook Concepts (Contd)

- A simple playbook execution sequence



- Multiple tasks can be triggered
- This is an example



In the simplest case, a playbook consists of a trigger and a series of tasks that are executed one after the other.

However, playbooks can also allow for more complex designs that involve multiple tasks. Additionally, if needed, the output of one task can be used by the task or tasks that follow it.

# DO NOT REPRINT

## © FORTINET

## Triggers

Trigger	Description
EVENT_TRIGGER	The playbook is run when an event is created that matches the configured filters When no filters are set, all events will trigger the playbook
INCIDENT_TRIGGER	The playbook is run when an incident is created that matches the configured filters When no filters are set, all incidents will trigger the playbook
ON_SCHEDULE	The playbook is run during the configured schedule You can define the start time, end time, interval type, and interval frequency for the schedule
ON_DEMAND	The playbook is run when manually started by an administrator

Every playbook starts with a trigger, that determines when the playbook is executed. Each playbook can include only one trigger.

After a playbook is triggered, it flows through the configured tasks, as defined in the playbook designer.

The following four triggers are available:

**EVENT\_TRIGGER:** The playbook runs when an event is created that matches the configured filters. When no filters are set, all events will trigger the playbook.

**INCIDENT\_TRIGGER:** The playbook runs when an incident is created that matches the configured filters. When no filters are set, all incidents will trigger the playbook.

**ON\_SCHEDULE:** The playbook runs during the configured schedule. You can define the start time, the end time, the interval, and the interval frequency for the schedule.

**ON\_DEMAND:** The playbook runs when manually started by an administrator.

To run a playbook manually, go to **Playbook**, select the desired playbook, and click **Run**. Additionally, if present, you can run playbooks from the incident **Analysis** page.

Note that playbooks with the **ON\_SCHEDULE** trigger can also be executed manually. This allows you to test them outside of their configured timeframe.

**DO NOT REPRINT**  
**© FORTINET**

## Triggers (Contd)

- A wide variety of categories can be used as filters for the event and incident triggers
  - You can use more than one condition to narrow down when the playbook will run
  - All conditions must be met for a match
- ON\_SCHEDULE triggers parameters are all based on timeframes
- ON\_DEMAND triggers have no extra configurable parameters

NSE Training Institute

The start time of the schedule  
 2021/09/07

The end time of the schedule  
 2022/09/09

The interval of the schedule  
 The frequency of the interval

**Example**

Field	Match Criteria	Value
Severity	Equal To	High
Device ID	Equal To	FGVM01000064692

Depending on the trigger type selected, you will have several options that can be used to specify exactly when you want the playbook to run.

For example, you can configure an Event trigger to run only when an Event with severity High is detected on a specific device.

Keep in mind that when a trigger has more than one condition for its filter, all conditions must be met for the playbook to start running.

# DO NOT REPRINT

## © FORTINET

## Connectors

- Allow playbooks to interact with devices in the Security Fabric and standalone
- Determine what actions can be performed by playbook tasks
- Several connector types available:
  - EMS
  - FOS
  - FGD
  - FML
  - FCASB
  - Localhost
- Only the FAZ-Localhost Connector is ready to be used by default
- Other connectors need to be configured
- Status of each connector is shown:
  - Green: connection successful
  - Black: connection unknown
  - Red: connection down

Automation Rule	Automation Action(s)	Parameters
Incoming Webhook Call	Compromised Host Quarantine_quarantine Compromised Host Quarantine_forticlient	mac uuid

Connectors determine which automated actions can be performed in playbooks. The available actions will vary depending on the connector type used. Each type allows for different actions.

The connectors supported are Localhost (FortiAnalyzer), FortiOS, FortiMail, FortiGuard, FCASB, and FortiClient EMS.

To view FortiSoC connectors, click **Connectors**.

The status of FortiSoC connectors is indicated by a colored icon:

- Green: The API connection successful.
- Black: The API connection is unknown.
- Red: The API connection is down.

You can see when the status was last updated by hovering your mouse over the status icon. Click the refresh icon to get an updated status.

By default, the FAZ-Localhost Connector is ready to be used. Other connector types require extra configuration.

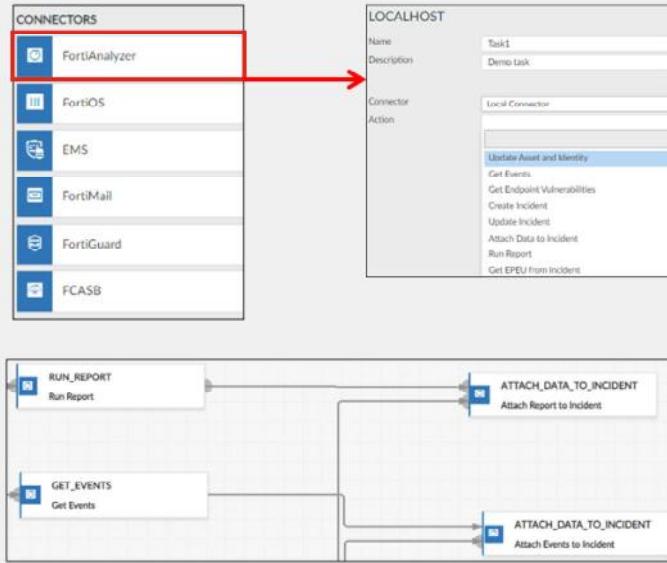
For example, the FOS-FortiOS connector will be listed as soon as the first FortiGate is added to FortiAnalyzer. However, in order to see the actions related to the FOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on the FortiGate side.

# DO NOT REPRINT

## © FORTINET

### Tasks

- Tasks are the actions that are executed when the playbook runs
- The available actions depend on the connector chosen
- You can chain one task to another task in order to execute a sequence of actions
- The output of a task can be used as the input of the next task in the sequence



Tasks are the actions that take place after a playbook starts running. Each starter can trigger the execution of one or more tasks, and each task can perform one action.

Tasks can also be chained so that the output of one task becomes the input of the next task. For example, a task can be created to get some data and then provide that data to the next task, where it can then be added to a report.

When adding a new task, you must choose a relevant connector before you can select the desired action. On the slide, the actions associated with the FAZ-Localhost Connector are shown. The available actions will vary depending on the connector type that you select.

You can configure tasks that use default input values, or take inputs from the trigger, or the preceding tasks.

You must configure automation rules on FortiGate before you can see the list of available actions on FortiOS connectors.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. What determines which actions are available in a playbook task?

- A. The type of connector used
- B. The type of trigger used

2. Which type of connector is enabled by default?

- A. Localhost
- B. FortiOS

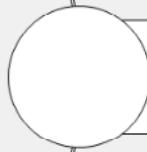
DO NOT REPRINT

© FORTINET

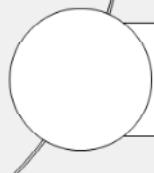
## Lesson Overview



### Playbook Components



### Creating Playbooks



### Managing Playbooks

 NSE Training Institute

© Fortinet Inc. All Rights Reserved.

12

Good job! You now understand playbook components.

Now, you will learn how to create playbooks and use them to automate tasks.

**DO NOT REPRINT**

**© FORTINET**

## Creating Playbooks

### Objectives

- Create new playbooks from a template
- Customize playbooks settings
- Create new playbooks from scratch
- Understand the use of variables in tasks

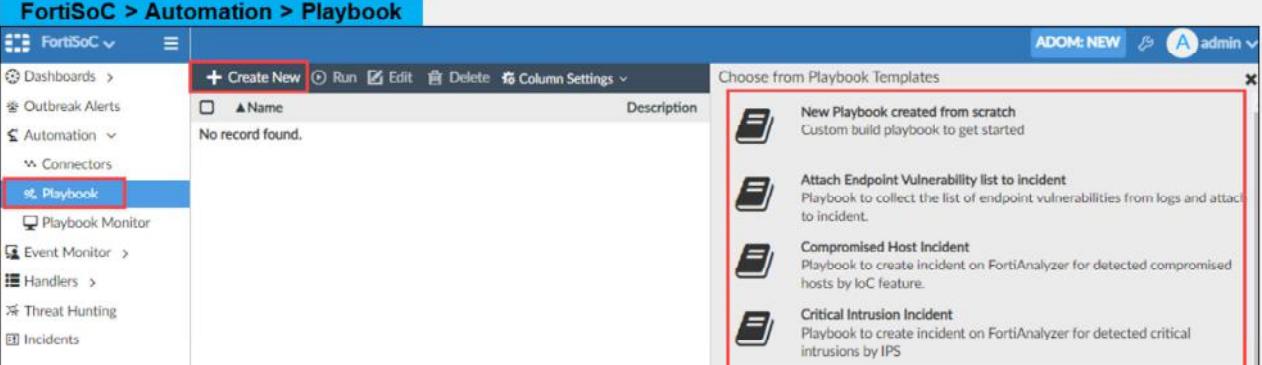
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in automating tasks with playbooks, you will be able to increase efficiency in your organization's SOC operations.

**DO NOT REPRINT**  
**© FORTINET**

## Creating Playbooks From a Template

- FortiAnalyzer includes several playbook templates
- Playbooks created from these templates can be customized to fit your needs



The screenshot shows the FortiSoC interface with the 'Automation > Playbook' section selected. A red box highlights the '+ Create New' button. To the right, a modal window titled 'Choose from Playbook Templates' displays four options:

- New Playbook created from scratch**: Custom build playbook to get started.
- Attach Endpoint Vulnerability list to incident**: Playbook to collect the list of endpoint vulnerabilities from logs and attach to incident.
- Compromised Host Incident**: Playbook to create incident on FortiAnalyzer for detected compromised hosts by IoC feature.
- Critical Intrusion Incident**: Playbook to create incident on FortiAnalyzer for detected critical intrusions by IPS.

FortiAnalyzer includes several playbook templates that can be quickly customized by SOC analysts. The included templates allow to:

- Investigate compromised host incident and critical intrusion incident
- Enrich data for assets and identity, and for hosts under investigation
- Block C&C IPs

To create a new playbook from a template, click **Playbook > Create New**.

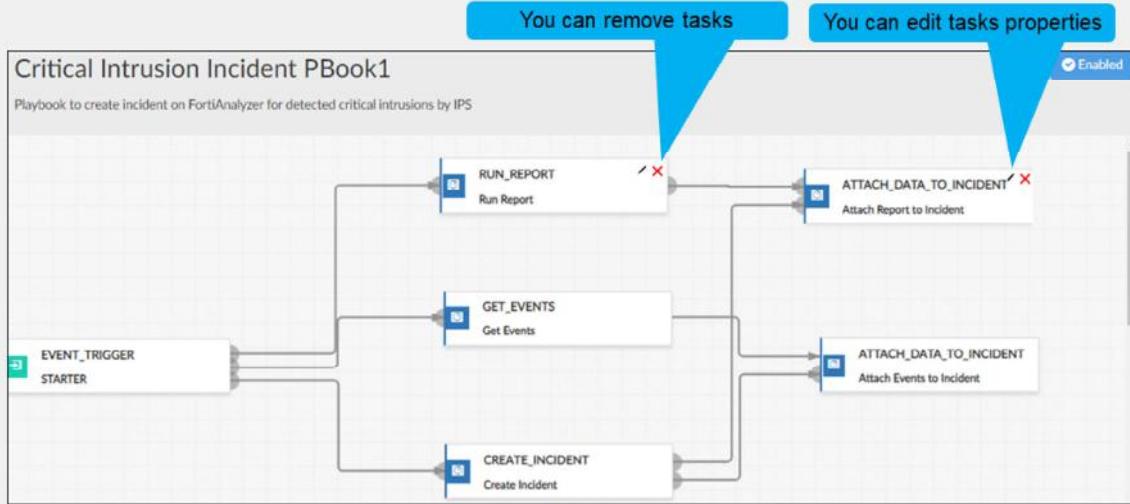
Next, select a playbook template with a description that responds to your needs and the playbook designer will open.

The option to create a playbook from scratch will be discussed later in this lesson.

**DO NOT REPRINT**  
**© FORTINET**

## Customizing Playbooks Settings

- A new playbook created from a template comes with all required components
- You can remove or customize tasks to meet your needs



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

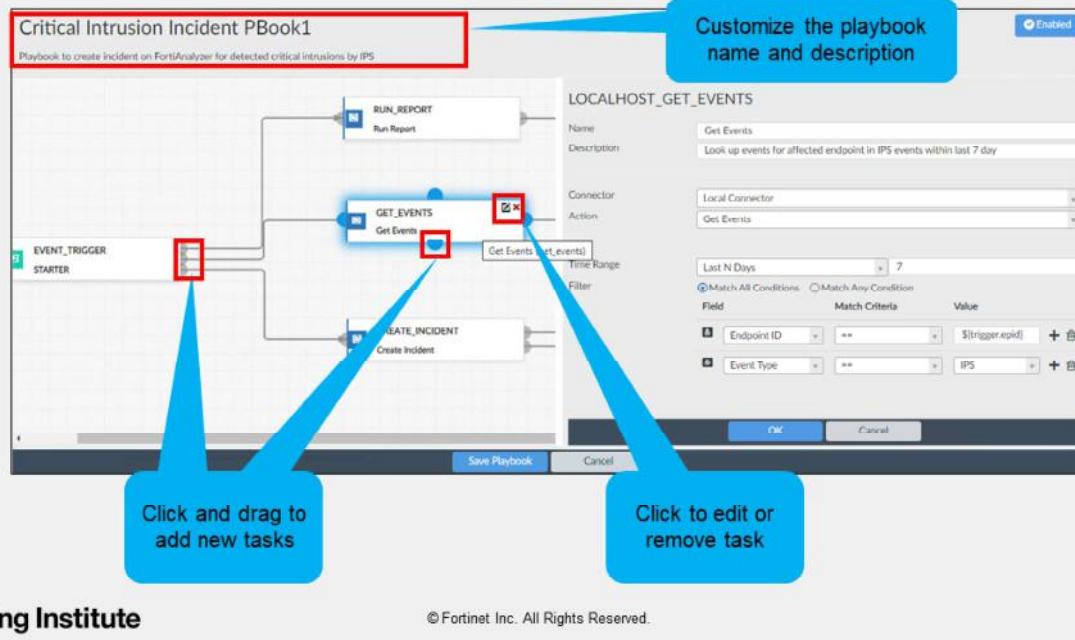
15

When you select a playbook template, the playbook designer is displayed and automatically populated with a trigger and one or more tasks, depending on the template you selected.

You can configure, add, or remove tasks to customize the playbook.

**DO NOT REPRINT**  
**© FORTINET**

## Customizing Playbooks Settings (Contd)



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

16

By default, every new playbook created from a template comes with the same generic name, plus the date it was created at the end. This can make them difficult to distinguish from the others so, it's highly recommended that you edit the names and descriptions of the new playbooks to something easily recognizable.

To add new tasks, click and drag the connector tabs attached to the current tasks or the trigger. An empty task will be displayed and you will need to edit its settings.

To edit any of the tasks, click on the pencil next to the top right corner. Remember to save the changes.

To remove a task, click on the red cross on its upper right corner.

**DO NOT REPRINT**  
**© FORTINET**

## Creating a New Playbook From Scratch

The screenshot shows the FortiSoC interface for creating a new playbook. At the top, there's a navigation bar with 'FortiSoC > Automation > Playbook'. Below it, a table lists 'No record found.' with columns for 'Name', 'Description', and 'Status'. To the right, a 'Choose from Playbook Templates' section displays two options: 'New Playbook created from scratch' (selected) and 'Attach Endpoint Vulnerability list to Incident'. A red arrow points from the 'New Playbook created from scratch' option to the main workspace. The workspace itself is titled 'Custom build playbook to get started' and contains a 'NEW TASK' box with 'Select a Step' and a 'TRIGGERS' sidebar listing 'EVENT\_TRIGGER', 'INCIDENT\_TRIGGER', 'ON\_SCHEDULE', and 'ON\_DEMAND'. A blue callout box on the left says 'FAZ needs a few minutes to parse a newly created playbook'. A red callout box at the bottom says 'Server error: FAZ is parsing the recent created playbook: d5f9c819-3d82-43d2-9cc5-4a80f0d10376. Please wait for about 5 minutes.' The footer includes the NSE Training Institute logo and copyright information.

If none of the templates responds to your needs, you can always create a playbook from scratch. To do so, click **Playbook > Create New**, and select the first choice in the list. The playbook designer will open.

First, you must select a trigger. Remember that, depending on the trigger type chosen, you have the option to add filters to make the playbook run only if the specified criteria is matched.

You then will need to add the desired task(s) you want to be executed by dragging and dropping the connector tabs.

When editing tasks, keep in mind that the actions can also use filters that will reduce the processing of unneeded data. For example, a task set to **Get Events** can use a filter to include only events generated by a specific event handler, or only events with a specific severity, just to mention two examples.

Keep in mind that after a new playbook is created, FortiAnalyzer will need a few minutes to parse it. For example, if you try to run a newly created playbook configured with an **ON\_DEMAND** trigger before that time, you will get an error telling you why it failed to run.

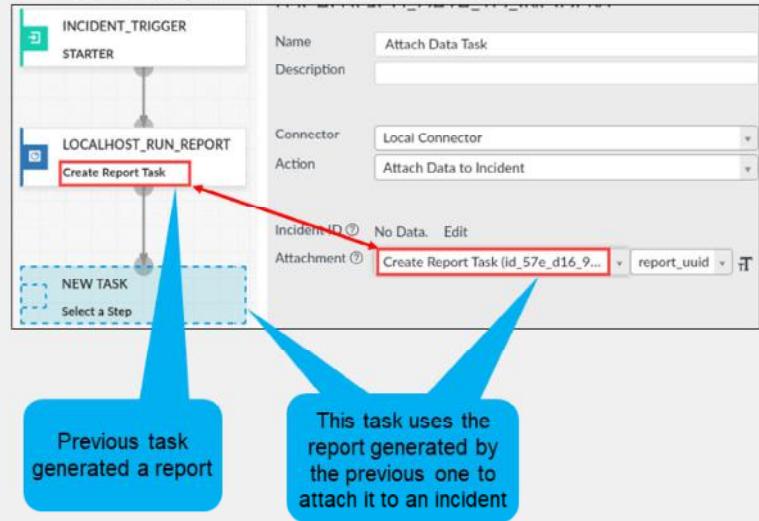
**DO NOT REPRINT**

**© FORTINET**

## Using Variables in Tasks

- You can use Output variables and Trigger variables in playbooks tasks
- Output variables: output of previous task is the input of current task
  - Format \${task\_id.output}
  - Previous task id is needed
- Trigger variables: use some the information from the trigger to filter the action in the task
  - Format \${trigger.variable}

- An example of the use of variables



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

18

You can use variables when configuring tasks. There are two types of playbook variables available: output variables and trigger variables.

Output variables allow you to use the output from a preceding task as an input to the current task.

Output variables use the format: \${<task\_id>.<output>}.

On the slide, the new task being created will use the report generated by the previous task to add it to an incident.

Trigger variables allow you to use information from the trigger of a playbook when it has been configured with an incident or event trigger. For example, a single playbook can be triggered by more than one device. A **Run Report** action can include a filter for the endpoint IP address from the event that triggered the playbook.

Trigger variables use the following format: \${trigger.<variable>}.

**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. What is the purpose of an output variable?
  - A. To use the input of one task as the output of another task
  - B. To use the output of a task as the input of another task
  
2. What is the first thing that you need to configure when creating a playbook from scratch?
  - A. The connector type that will be used
  - B. The trigger type that will be used

**DO NOT REPRINT**

**© FORTINET**

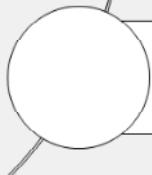
## Lesson Overview



### Playbook Components



### Creating Playbooks



### Managing Playbooks

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

20

Good job! You now know how to create playbooks and use them to automate tasks.

Now, you will learn how to manage playbooks.

**DO NOT REPRINT**

**© FORTINET**

## Managing Playbooks

### Objectives

- Monitor playbooks
- Export and import playbooks

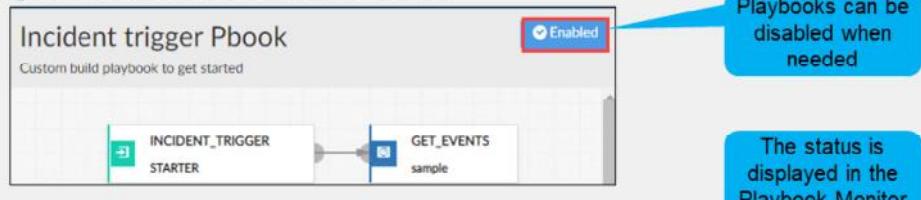
After completing this section, you will be able to achieve the objectives shown on this slide.

By demonstrating competence in monitoring playbooks, you will be able to identify if all automated tasks ran successfully or not. You will also be able to export playbooks to another ADOM or device.

**DO NOT REPRINT**  
**© FORTINET**

## Monitoring Playbooks

- Edit the playbook setting to disable it when not needed



- The status of all your playbooks jobs is available in **Playbook Monitor**

FortiSoC > Automation > Playbook Monitor

<input type="checkbox"/> Job ID	Playbook	Trigger	Start Time	End Time	Status	De
<input type="checkbox"/> 2021-09-10 15:46:19.781959-06	event test	event [2021091010002	2021-09-10 15:46:19 -0600	2021-09-10 15:47:46 -0600	Success (Scheduled:0/Running:0/Success:1/Failed:0)	<input type="checkbox"/>
<input type="checkbox"/> 2021-09-10 15:46:19.740144-06	event test	event [2021091010002	2021-09-10 15:46:19 -0600	2021-09-10 15:47:46 -0600	Success (Scheduled:0/Running:0/Success:1/Failed:0)	<input type="checkbox"/>
<input type="checkbox"/> 2021-09-10 15:37:19.216451-06	event test	event [2021091010002	2021-09-10 15:37:19 -0600	2021-09-10 15:38:27 -0600	Success (Scheduled:0/Running:0/Success:1/Failed:0)	<input type="checkbox"/>
<input type="checkbox"/> 2021-09-10 15:37:19.175788-06	event test	event [2021091010002	2021-09-10 15:37:19 -0600	2021-09-10 15:38:27 -0600	Success (Scheduled:0/Running:0/Success:1/Failed:0)	<input type="checkbox"/>
<input type="checkbox"/> 2021-09-10 15:36:19.071648-06	event test	event [2021091010002	2021-09-10 15:36:19 -0600	2021-09-10 15:37:25 -0600	Success (Scheduled:0/Running:0/Success:1/Failed:0)	<input type="checkbox"/>

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

22

After you create a playbook, you can enable or disable it through the playbook editor.

Enabled playbooks are monitored and each task execution is tracked. You can view the status of playbook jobs in **Playbook Monitor**.

A playbook's status can be one of the following:

- Running
- Success
- Failed

# DO NOT REPRINT

## © FORTINET

## Monitoring Playbooks (Contd)

- To see details of a playbook job, click on **Details** and then on **View Log**.

The screenshot shows a table of playbook jobs. One job has two tasks listed under it. The second task, 'incident auto', is highlighted with a red box and has a red arrow pointing to its 'Failed' status in the 'Status' column. A blue callout bubble says: 'This playbook has two tasks. One task ran successfully but the other one failed'. Below the table is a large text box containing the log output for the failed task. The log shows several INFO messages and ends with an ERROR message: '[2021-09-16 14:50:11,730] {taskinstance.py:1128} ERROR - invalid literal for int() with base 10: 'as''. A red box highlights this error message.

Trigger	Start Time	End Time	Status	Details	
user (admin)	2021-09-16 14:49:28 -0600	2021-09-16 14:50:37 -0600	Failed (Scheduled:0/Running:0/Success:1/Failed:1)		
<input type="checkbox"/> Task ID	Task	Start Time	End Time	Status	Raw Log
<input type="checkbox"/> id_crc_ebd_27c_686	test pbook	2021-09-16 14:50:11 -0600	2021-09-16 14:50:11 -0600	Success	
<input type="checkbox"/> id_ab6_ed0_2ce_0c9	incident auto	2021-09-16 14:50:11 -0600	2021-09-16 14:50:11 -0600	Failed	

```
[2021-09-16 14:50:11,643] {taskinstance.py:867} INFO - Starting attempt 1 of 1
[2021-09-16 14:50:11,643] {taskinstance.py:868} INFO -
[2021-09-16 14:50:11,648] {taskinstance.py:887} INFO - Executing <Task(IncidentAddOperator): id_ab6_ed0_2ce_0c9>
[2021-09-16 14:50:11,650] {standard_task_runner.py:53} INFO - Started process 6485 to run task
[2021-09-16 14:50:11,697] {logging_mixin.py:112} INFO - Running %s on host %s <TaskInstance: 199_d5f9c819-3d82-43
[2021-09-16 14:50:11,711] {incident_operator.py:173} INFO - Calling IncidentAddOperator
[2021-09-16 14:50:11,723] {logging_mixin.py:112} INFO - [2021-09-16 14:50:11,723] {base_hook.py:84} INFO - 
[2021-09-16 14:50:11,728] {logging_mixin.py:112} INFO - [2021-09-16 14:50:11,728] {base_hook.py:84} INFO - 
[2021-09-16 14:50:11,730] {taskinstance.py:1128} ERROR - invalid literal for int() with base 10: 'as'
Traceback (most recent call last):
  File "/usr/local/lib/python3.8/site-packages/airflow/models/taskinstance.py", line 961, in _run_raw_task
    result = task_copy.execute(context=context)
  File "/drive0/private/airflow/plugins/incident_operator.py", line 207, in execute
    self.euid = int(FAZUtilsOperator.parse_input(context, self.euid, context_dict))
ValueError: invalid literal for int() with base 10: 'as'
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

23

When troubleshooting playbooks, it is very useful to review their logs. Details about the execution of a playbook job are available by checking the respective log.

To see detailed logs, go to **Playbook Monitor**, select the desired entry, click on the **Details** icon, and then click **View Log**.

A summary of this entry is also available in **Log View** under the **FortiAnalyzer** section.

Playbook jobs that include one or more failed tasks are labeled as **Failed** in **Playbook Monitor**. A failed status, however, does not mean that all tasks failed. Some individual actions may have been completed successfully.

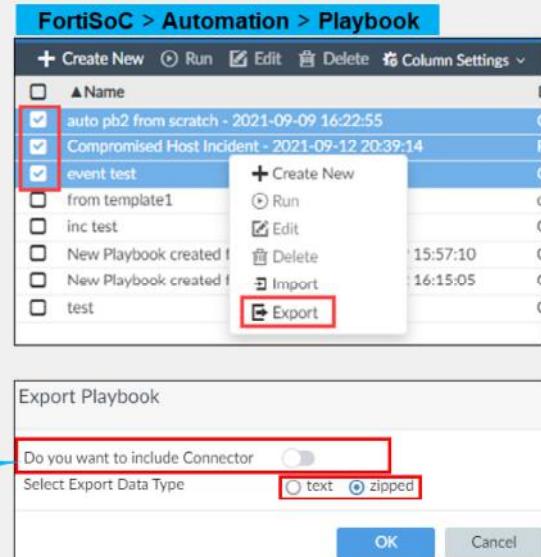
In the example shown on the slide, the playbook has two tasks configured and only the task named `incident auto` failed to run. However, the playbook job is considered to have failed.

**DO NOT REPRINT**  
**© FORTINET**

## Exporting Playbooks

- Playbooks are defined per ADOM
- Export playbooks to be used in a different ADOM or device
- The connectors can be included in the exported file
- The resulting file uses a JSON format
  - You can choose to compress the file

Including the connectors will make sure all required components are exported



Playbooks are defined per ADOM. If you want to use an existing playbook on a different ADOM, or a different FortiAnalyzer, you can export it very easily.

To export a playbook, right-click on the playbook that you want to export, and click **Export**. You can export more than one playbook at the same time by selecting them. The **Export Playbook** window opens.

Configure the settings to export the selected playbook:

- **Do you want to include Connector:** When this setting is enabled, connectors required to run this playbook will be included in the exported file. This is recommended, for example, if a non-default connector like the EMS connector is configured, so that all required components are included in the resulting file.
- **Select Export Data Type:** Select the export file type as either plain text JSON or zipped/base 64 encoded JSON.

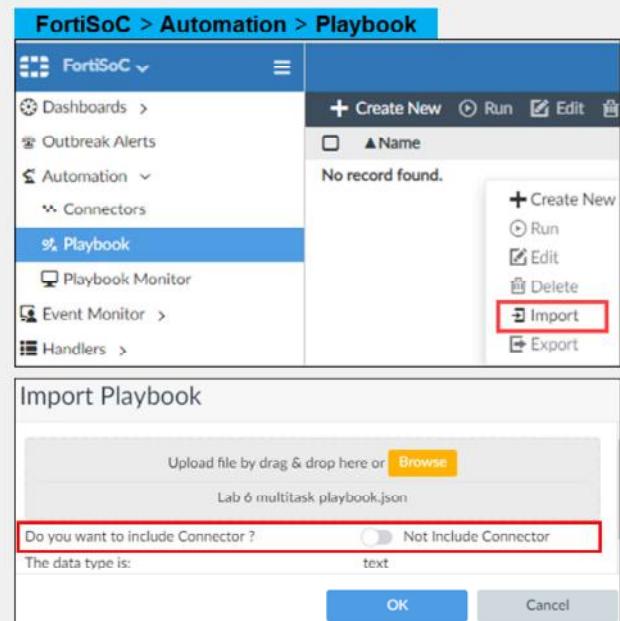
If you need to be able to read the contents of the JSON file in plaintext, you must choose the text version during your export process.

**DO NOT REPRINT**

© FORTINET

## Importing Playbooks

- Import a previously exported playbook on the destination ADOM or device
- If available, you can choose to import the connector or not



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

25

To import a playbook, right-click anywhere in the playbook dashboard and click **Import**.

The **Import Playbook** window appears. Browse to select the playbook file to be imported. If available, you can include any connectors in the file. This is the recommended choice.

If the imported playbook has the same name as an existing one, FortiAnalyzer will create a new name that includes a timestamp to avoid conflicts.

Playbooks are imported with the same status they had (enabled or disabled) when they were exported. Playbooks set to run automatically should be exported while they are disabled to avoid unintended runs on the destination.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

1. The execution of a playbook with three tasks is considered to have failed when:
  - A. The three tasks fail
  - B. Any of the tasks fail
  
2. At what level are playbooks created?
  - A. Per ADOM
  - B. Per device

**DO NOT REPRINT**

**© FORTINET**

## Lesson Overview



### Playbook Components



### Creating Playbooks



### Managing Playbooks

 **NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

27

Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

**DO NOT REPRINT**

**© FORTINET**

## Review

- ✓ Understand FAZ automation capabilities
- ✓ Understand Playbooks concepts
- ✓ Understand Triggers types and characteristics
- ✓ Understand Connectors types
- ✓ Create new playbooks
- ✓ Understand the use of variables in tasks
- ✓ Monitor playbooks
- ✓ Export and import playbooks

This slide shows the objectives that you covered in this lesson.

You learned what playbooks are and how you can create them to automate tasks in FortiAnalyzer. You also learned how to monitor and manage playbooks.

**DO NOT REPRINT**

**© FORTINET**



## FortiAnalyzer

### Reports



FortiAnalyzer 7.0

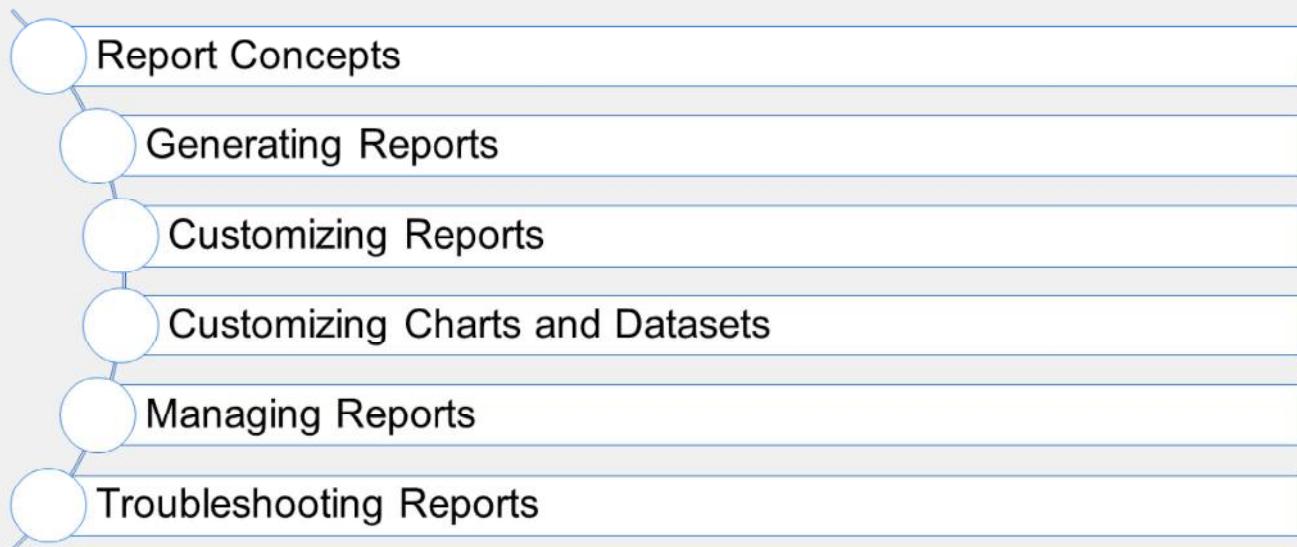
Last Modified: 1 December 2021

In this lesson, you will learn how to extract useful information from your logs for analysis purposes. To do this, you will learn how data is formatted, stored, and organized in the database, and how to use the FortiAnalyzer reporting feature to view captured data for forensics and compliance.

**DO NOT REPRINT**

**© FORTINET**

## Lesson Overview



In this lesson, you will explore the topics shown on this slide.

**DO NOT REPRINT**

**© FORTINET**

## Report Concepts

### Objectives

- Describe the elements that constitute a report
- Describe how FortiAnalyzer extracts data from the database
- Describe how reports function within ADOMs

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding report concepts, you will be able to use reports more effectively to extract collected log data from your database.

**DO NOT REPRINT**

© FORTINET

## Purpose of Reports

- Reports summarize a large amount of log (text) data
- FortiAnalyzer analyzes information collected from the log files of managed devices and presents the information in tabular and graphical reports
- Reports provide a quick and detailed analysis of activity on your network

Default reports

Reports do not provide any recommendations  
You must look beyond the data

Application
Detailed User Report
FortiClient Report
Outbreak Alert Reports
Web
360 Protection Report
360-Degree Security Review
Admin and System Events Report
Application Risk and Control
Bandwidth and Applications Report
Client Reputation
Cyber Threat Assessment
Cyber-Bullying Indicators Report
Data Loss Prevention Detailed Report
Detailed Application Usage and Risk
DNS Report
Email Report
Endpoint Sandbox Detections Report
FortiCache Default Report
FortiCache Security Analysis
FortiCache Web Usage Report
FortiDoS Default Report
FortiGate Performance Statistics Report
FortiMail Analysis Report
FortiMail Default Report
FortiNAC Endpoints and Network Report
Fortinet Email Risk Assessment
FortiProxy Default Report
FortiProxy Security Analysis

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

4

The purpose of a report is to summarize large amounts of logged data. Based on configured report parameters, FortiAnalyzer extracts data and presents it in a graphical manner that makes it easier—and quicker—to digest. The patterns and trends that reports reveal already exist as several points of data within your database, but it would be difficult and time consuming to manually locate, cross-reference, and analyze multiple log files, especially if you don't know what trend or pattern you are looking for. Once configured, reports do the investigation for you and provide a quick and detailed analysis of activity on your network. You can then use that information to better understand your network or improve your network security.

Note that reports do not provide any recommendations or give any indication of problems. Administrators must be able to look beyond the data and charts to see what is happening within their network.

# DO NOT REPRINT

## © FORTINET

### Elements That Comprise a Report

- A FortiAnalyzer report is a set of data in organized *charts*

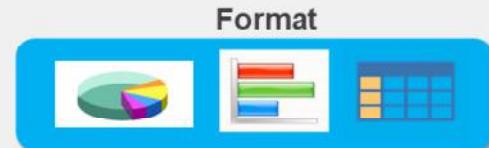


Charts define:

- What **data** from the SQL database is displayed
- What **format** the data is displayed in



Datasets are specific SQL SELECT queries



Format options include:  
pie charts, bar charts, or tables

A FortiAnalyzer report is a set of data organized in charts. Charts consist of two elements:

- Datasets:** Structured Query Language (SQL) SELECT queries that extract specific data from the database
- Format:** how the data is displayed (for example, pie charts, bar charts, or tables)

**DO NOT REPRINT**  
**© FORTINET**

## How Do Charts Extract Data From the Database?

- Datasets are SQL SELECT queries to the database
  - Data populates a chart
- FortiAnalyzer only uses the SELECT SQL statement for reports
  - Read-only statement that retrieves data from the database
  - First word used in a query

```
select (case when severity='critical' then 'Critical' when severity='high' then 'High' when severity='medium' then 'Medium' when severity='low' then 'Low' when severity='Info' then 'Info' end) as severity, count(*) as totalnum
from $log where $filter group by severity order by totalnum desc
```

In order to populate a chart with specific log data that has been collected, stored, and sorted in the SQL database, reports rely on a dataset query to extract that log data. A dataset is a specific SQL SELECT query—a read-only statement that retrieves data from the database.

The SELECT statement is the first word used in a query—it is the declarative verb describing what you want done—and is followed by the column(s) from which you want to extract information. You can extract all entries or you can use clauses to make the query more specific.(See the next slide.)

**DO NOT REPRINT**

© FORTINET

## SELECT Statement

- The SELECT statement retrieves the log data you want from the database
- Must specify criteria using a recognized and supported clause

Clause	Definition
FROM	From which table(s) or view(s) the data will be extracted
WHERE	Sets the conditions (all rows that do not satisfy the condition are not shown in the output)
GROUP BY	Collects data across multiple records and groups the results by one or more columns
ORDER BY	Orders the results by specific column(s), ascending or descending
LIMIT	Limits the number of records returned based on a limit value.
OFFSET	Often used with the LIMIT clause to offset the results by a set value

Clauses must be coded in a specific sequence!

- For more information on SQL and datasets for use with FortiAnalyzer reports, see the supplementary *FortiAnalyzer SQL and Datasets* lesson

To extract the desired data, you need to specify the criteria to be used. In order to put this criteria into a language that SQL understands, you must use one or more clauses recognized by the SELECT statement.

The main clauses FortiAnalyzer reports use are as follows:

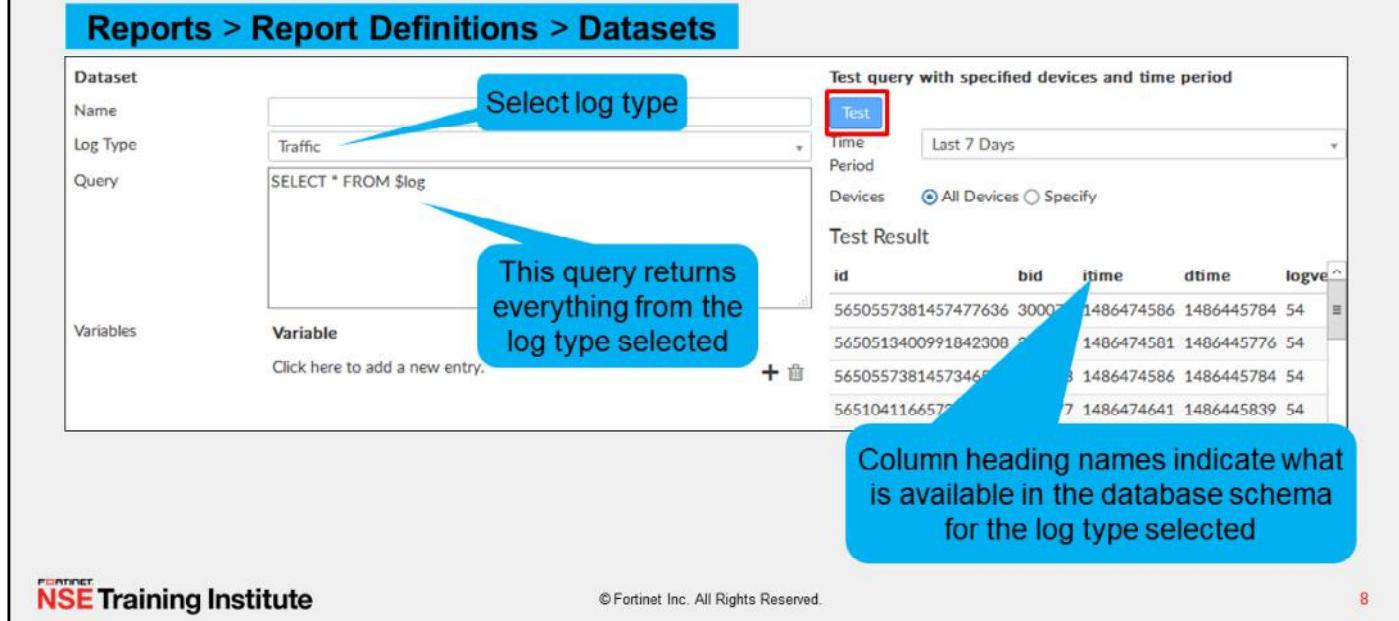
- FROM, which specifies from which table(s) or view(s) the data is extracted
- WHERE, which specifies the conditions. All rows that don't satisfy the condition are not shown in the output.
- GROUP BY, which collects data across multiple records and groups the results by one or more columns
- ORDER BY, which orders the results by specific column(s). If ORDER BY is not given, the records are returned in whatever order the system finds the fastest to produce.
- LIMIT, which limits the number of records returned based on a specified value.
- OFFSET, clause often used along with LIMIT, which offset results by the number specified. For example, if you place a limit of three records and an offset of one, the first record that would normally be returned is skipped and, instead, the second, third, and fourth records (three in total) are returned.

FROM is the only mandatory clause required to form a SELECT statement. The rest of the clauses are optional and serve to filter or limit, aggregate or combine, and control the sort. It is also important to note that the clauses must be coded in a specific sequence. Accordingly, following the SELECT keyword, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide. For example, you can't use the WHERE clause before the FROM clause. You don't have to use all optional clauses, but whichever ones you do use must be in the correct sequence.

For more information on SQL and datasets for use with FortiAnalyzer reports, see the supplementary *FortiAnalyzer SQL and Datasets* lesson.

**DO NOT REPRINT**  
**© FORTINET**

## Accessing the SQL Schema



The screenshot shows the 'Reports > Report Definitions > Datasets' section. A 'Dataset' is being created with the following details:

- Name:** Not specified.
- Log Type:** Set to 'Traffic' (highlighted with a red box).
- Query:** The query 'SELECT \* FROM \$log' is entered.
- Variables:** An empty list with a note to 'Click here to add a new entry.'

A large blue callout points from the 'Traffic' log type selection to the query editor, stating: 'Select log type' and 'This query returns everything from the log type selected'.

To the right, a 'Test' button is highlighted with a red box. Below it, the 'Test Result' shows a table with four columns: id, bid, itime, and dtime. The table contains several rows of log data.

A blue callout points from the test results table to the column headers, stating: 'Column heading names indicate what is available in the database schema for the log type selected'.

At the bottom left is the 'NSE Training Institute' logo, and at the bottom center is the copyright notice: '© Fortinet Inc. All Rights Reserved.' A small red number '8' is in the bottom right corner.

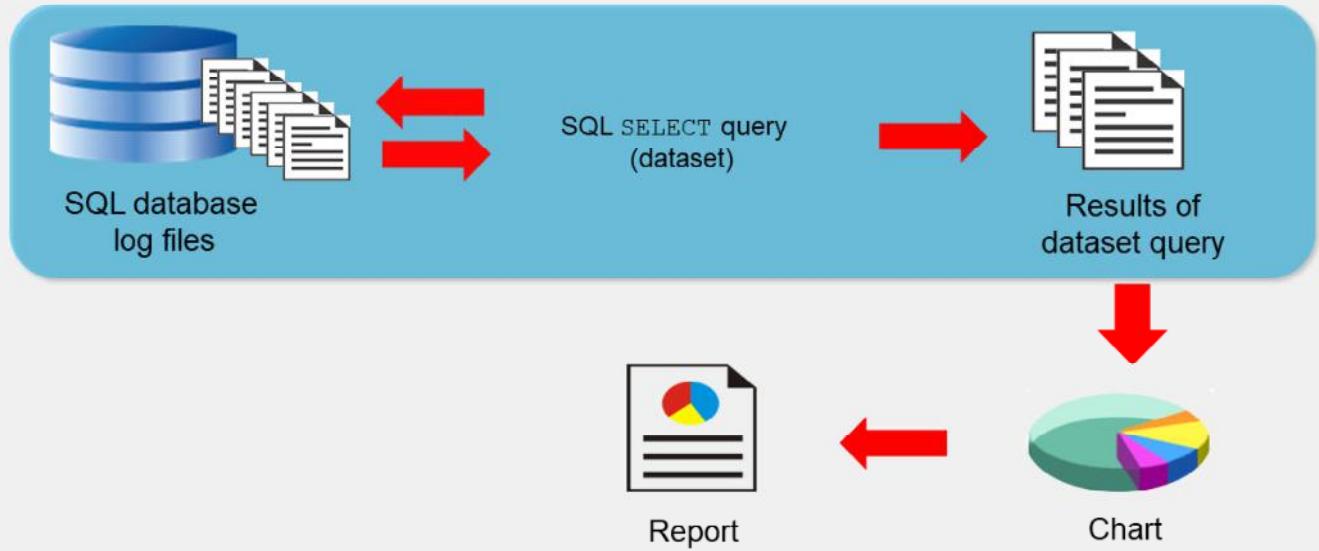
In order to create a query, you first need to know what is included in the database schema—you need to know what information is available to extract for reports. In FortiAnalyzer, you can obtain the schema for a specific log type by creating and testing the following dataset query:

```
SELECT * FROM $log
```

For traffic logs, for example, associate the **Traffic** log type with this dataset in the **Log Type** drop-down list. This query returns everything from the **Traffic** log type. The column heading names indicate what is available in the database schema for the log type selected. The \* symbol is used as a way to return all data.

**DO NOT REPRINT****© FORTINET**

## Report Workflow

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

9

As the graphic on this slide shows, the SQL database contains all the logs. A SQL SELECT query polls the database for specific information. Based on the query, a subset of information stored in the logs is extracted.

This subset of data populates a chart, and one or more charts exist within a report.

**DO NOT REPRINT****© FORTINET**

## Reports and ADOMs

- Each ADOM has its own reports, libraries, and advanced settings
- Additional reports for the following Fortinet devices are available when ADOMs are enabled:
  - FortiAuthenticator
  - FortiCarrier
  - FortiCache
  - FortiClient
  - FortiDDos
  - FortiDeceptor
  - FortiManager
  - FortiMail
  - FortiNAC
  - FortiProxy
  - FortiSandbox
  - FortiWeb

Configure and generate reports for these devices within their respective ADOMs

When ADOMs are enabled, each ADOM has its own reports, libraries, and advanced settings. As such, make sure that you are in the correct ADOM before selecting a report.

Additional reports for specific Fortinet devices are available only when ADOMs are enabled. You can configure and generate reports for these devices within their respective ADOMs. These devices also have device-specific charts and datasets.

**DO NOT REPRINT****© FORTINET**

## Report Considerations

- Audience
  - Level and type of information may vary depending on intended reader
- Purpose
  - What information do you want?
  - Align with dataset query
- Level of detail
  - Too much detail can overwhelm reader
  - Best practice → Keep reports short and concise
    - Too many charts in a report tie up the CPU for a long time
- Format
  - What is the best way to display the information?
  - Select the *right* chart format for your purpose

Before you configure or create a report, there are certain factors you need to consider to ensure the report is as effective as possible.

The first consideration is your audience. Who's going to be looking at this report? Depending on what they want to see and their level of skill, you may need to add, remove, or modify charts in order to convey the information appropriately.

The second consideration is your purpose. If you look at the predefined reports, each one focuses on a specific piece of information. They are based on specific datasets and contain charts that format that query. So, reports must be focused in order to be effective and easily digestible, and this is achieved by having a strong purpose.

The next consideration is the level of detail. A best practice is to keep reports short and concise. Not only do they focus your view of your network and users, but shorter reports have fewer charts and fewer queries to run. This helps with performance, because large reports affect CPU and memory.

The final consideration is the format. You need to know how you want to format the data so that it displays in the most digestible and informative way possible. A table chart, bar chart, and pie chart don't necessarily represent the same data with the same effectiveness. Based on your query, you may only be able to use one type of chart, but if options are available, you need to select the right chart. Think about how the data would best be represented visually, and about the audience consuming the data.

Aside from the chart format, you can also change the design of the report by adding separators, page breaks, images, and renaming charts.

**DO NOT REPRINT**

**© FORTINET**

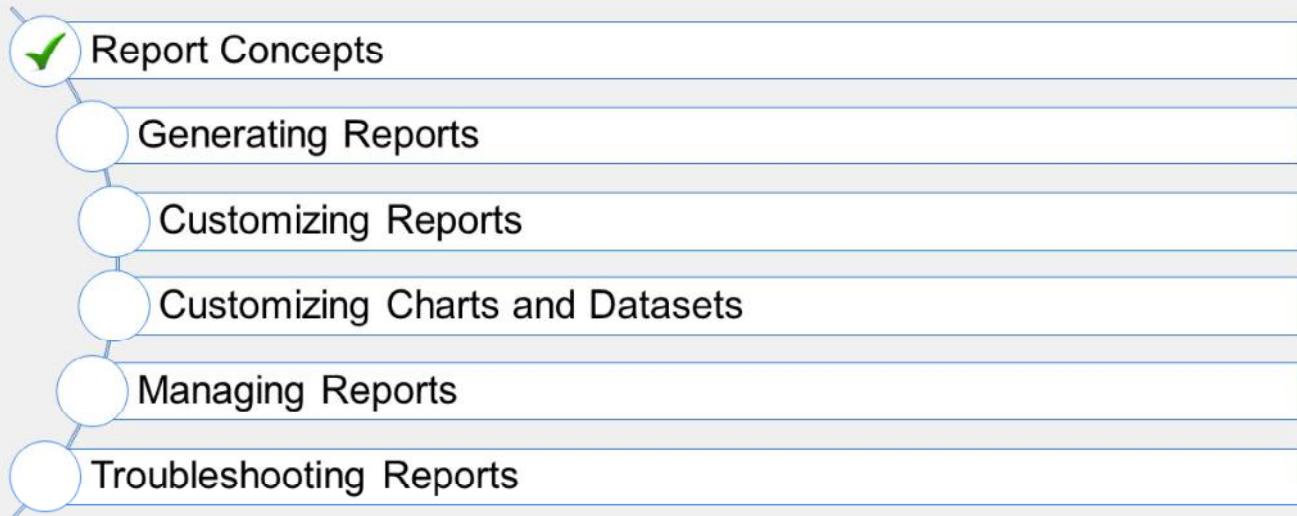
## Knowledge Check

1. In FortiAnalyzer, what is a dataset?
  - A. The database schema
  - B. A specific SQL SELECT query that retrieves data from the database

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



Good job! You now understand report concepts.

Now, you will learn how to generate reports in FortiAnalyzer.

**DO NOT REPRINT**

**© FORTINET**

## Generating Reports

### Objectives

- Run predefined reports
- Fine-tune reports
- Run reports on log groups

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in report generation, you will be able to quickly view a detailed analysis of activity on your network in a way that is consumable.

# DO NOT REPRINT

## © FORTINET

### Templates

- A template specifies the layout—text, charts, and macros—to include in the report that uses it
- FortiAnalyzer provides predefined templates (which match the predefined reports)
  - Can clone predefined templates OR create custom templates (can't edit or delete default templates)
- Don't contain data—data is added to the report when generated

The screenshot shows two panels of the FortiAnalyzer interface under 'Report Definitions'.

**Reports > Report Definitions > Templates**

Title	Language	Description	Category
Template - 360 Protection Report	English	Present a brief summary of hardware/software inventory of the FortiGate devices over a 30 day period.	System
Template - 360-Degree Security Review	English	Security review of Application Visibility and Control, Threat Detection, Data Exfiltration Detection, Endpoint Detection, Prevention and Recommended Actions.	Security
Template - Admin and System Events Report	English	Admin login and failed login attempts and system severity event counts.	System

**Reports > Report Definitions > All Reports**

Title
Application
Detailed User Report
FortiClient Report
Outbreak Alert Reports
Web
360 Protection Report
360-Degree Security Review
Admin and System Events Report
Application Risk and Control
Bandwidth and Applications Report

A red box highlights the 'Template - 360-Degree Security Review' entry in both lists, and a red arrow points from the template's description in the 'Templates' list to its corresponding entry in the 'All Reports' list.

NSE Training Institute © Fortinet Inc. All Rights Reserved. 15

FortiAnalyzer provides predefined templates for reports. A template specifies the layout—texts, charts, and macros—to include in the report that uses it. By default, these predefined templates are associated with their respective predefined reports. For example, the **Template – 360-Degree Security Review** template is the template used by the predefined **360-degree Security Review** report.

Templates don't contain any data. Data is added to the report when you generate it.

You can't edit a predefined template, but you can clone it and edit the clone to fit your requirements. You can also create your own template from scratch.

**DO NOT REPRINT**  
**© FORTINET**

## Running Predefined Reports

- Based on associated templates
  - Includes template layout
  - But also configured with basic, default settings
- Configure basic report settings:
  - Time period
  - Devices
  - Type
- Run report:
  - On demand
  - Schedule
- View reports in multiple formats
  - HTML, PDF, XML, CSV

The screenshot shows the 'Reports > Report Definitions > All Reports' section. A red box highlights the 'Run Report' button in the top left. Another red box highlights the 'Edit' option in the dropdown menu. A third red box highlights the 'View Report' button at the bottom left of the main panel. A large red arrow points from the 'Edit' box down to the 'View Report' button. The main panel displays report details: Path (All Reports), Name (360-Degree Security Review June 16-2021), Time Period (Last 7 Days), Devices (All Devices), Subnets (All Subnets), Type (Single Report), and a checked 'Enable Schedule' checkbox. Below this, there's a schedule configuration with 'Generate Report Every' set to 1 week. At the bottom, a 'Format' section shows 'HTML PDF XML CSV' options, with 'HTML' selected. The date range '2021/06/10 - 2021/06/16' is also visible.

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

16

FortiAnalyzer also provides predefined reports—each one associated with a predefined template (the layout). Predefined reports come with basic, default settings already configured. These basic settings define the time period in which to run the report; what device, or devices, to run the report on; and whether the report generates as a single report or multiple reports.

As such, you can run the predefined reports *as is*, but at minimum you should examine, and adjust if necessary, the basic default settings. For example, if today is the first day FortiAnalyzer has been collecting logs, your report contains no data if the time period is set to **Last 7 Days**. Last <n> days is handled differently in FortiView than reports. In reports, it does not include the current day.

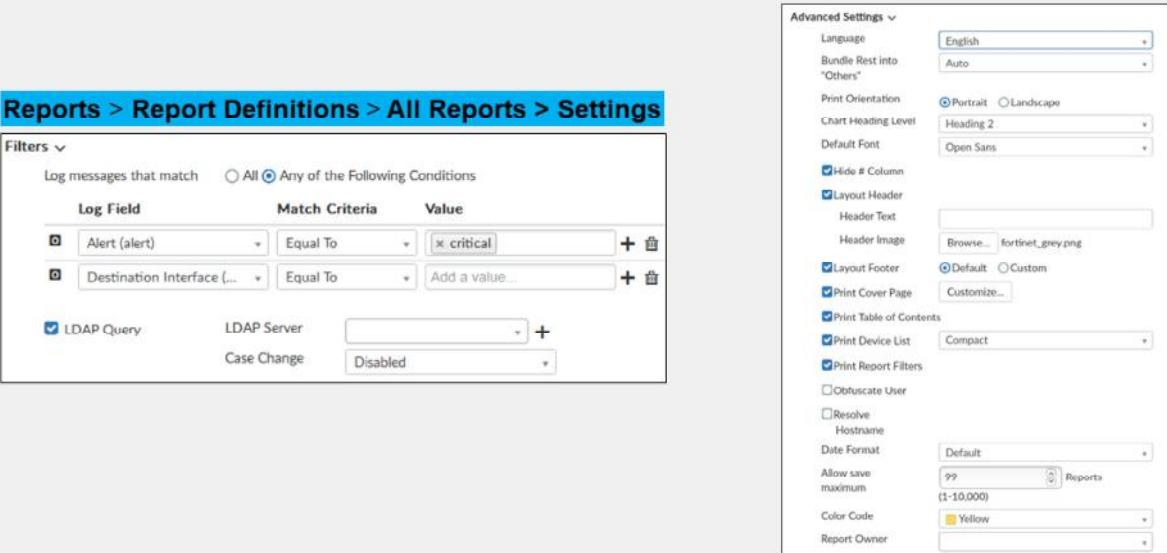
You can run reports on demand, or schedule them for a specific time by enabling scheduling.

After it is generated, the report is available to view in multiple formats, including HTML, PDF, XML, and CSV.

**DO NOT REPRINT**  
**© FORTINET**

## Fine-Tuning Predefined Reports

- If only minor modifications are required, you can fine-tune the report settings



The screenshot shows the 'Report Definitions > All Reports > Settings' page. On the left, there are two sections: 'Filters' and 'Advanced Settings'. The 'Filters' section contains a table with columns 'Log Field', 'Match Criteria', and 'Value'. It includes filters for 'Alert (alert)', 'Destination Interface', and an 'LDAP Query' entry. The 'Advanced Settings' section on the right covers various report configurations like language, orientation, font, and footer options.

**Reports > Report Definitions > All Reports > Settings**

**Filters**

Log Field	Match Criteria	Value
Alert (alert)	Equal To	[x critical]
Destination Interface	Equal To	Add a value...
LDAP Query	LDAP Server	
	Case Change	Disabled

**Advanced Settings**

- Language: English
- Print Orientation: Portrait
- Default Font: Open Sans
- Hide # Column: checked
- Layout Header: checked
- Header Text: [empty field]
- Header Image: Browse... fortnet\_grey.png
- Layout Footer: checked
- Print Cover Page: checked
- Print Table of Contents: checked
- Print Device List: checked
- Print Report Filters: checked
- Obfuscate User: unchecked
- Resolve Hostname: unchecked
- Date Format: Default
- Allow save maximum: 99 Reports (1-10,000)
- Color Code: Yellow
- Report Owner: [empty field]

NSE Training Institute © Fortinet Inc. All Rights Reserved. 17

If a predefined report comes extremely close to meeting all your requirements, but not quite, you may be able to fine-tune its settings to fit your needs.

Fine-tuning encompasses minimal report modifications, such as:

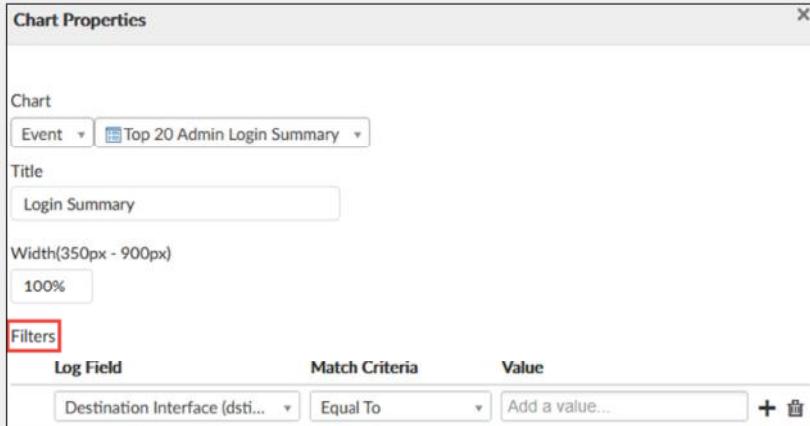
- Adding log message filters to further refine the log data that is included in the report
- Enabling queries to a pre-existing LDAP server to add an LDAP query to the report
- Configuring report language, print settings, and other settings. For example, you can print and customize the cover page, print the table of contents, print a device list, obfuscate users, and set the color code for the report to appear under **Report Calendar**.

# DO NOT REPRINT

## © FORTINET

### Chart Filters

- Can set filters on the charts used within a report
  - Right-click a chart under the report **Layout** tab and select **Chart Properties**
- The filters only apply to that chart in that report
  - Does not affect any other reports that use that same chart



You just learned about setting filters at the report level in the report settings. However, you can also set filters on the charts used within the report.

Within the report **Layout** tab, right-click the chart and select **Chart Properties**. The filters you set here only apply to that chart in that report. As such, they do not affect any other reports that use that same chart.

# DO NOT REPRINT

## © FORTINET

## Which Charts and Datasets Are Used in Reports?

The screenshot shows the 'Report Definitions > Templates' interface. A chart titled 'Score Summary for All Users/Devices' is selected. A context menu is open over the chart, with the 'Clone Chart' option highlighted. A callout bubble says: 'Right-click chart and select **Clone Chart** to see associated dataset'. Another callout bubble says: 'View dataset query under **Report Definitions > Datasets**'. Below the chart, another chart titled 'Top Users by Reputation Scores' is shown with a callout bubble saying: 'Charts included in report'. On the right, a detailed view of the 'Dataset' configuration for the 'Score Summary' chart is displayed, showing the dataset name and its SQL query.

**Report Definitions > Templates**

Name: Copy of Template - Client Reputation  
Description: Client and user network behaviour, incidents by user, devices, threat summary  
Category:  
Language: English

Score Summary for All Users/Devices

Top Users by Reputation Scores

Charts included in report

Right-click chart and select **Clone Chart** to see associated dataset

View dataset query under **Report Definitions > Datasets**

Name: Copy of Threat Score Summary  
Description: Threat score summary for all users and devices  
Dataset: reputation-Score-Summary-For-All-Users-Devices

Resolve Hostname: Inherit  
Chart Type: Area  
Data Bindings: hodex  
X-Axis (Timeline)  
Data Binding: hodex  
Lines: scores  
Format: Counter (K/M/G)

```
select $flex_timescale(timestamp) as hodex, sum(scores) as scores from ###(select $flex_timestamp as timestamp, sum(crscore%65536) as scores from $log where $filter and logid_to_int(logid) not in (4, 7, 14) and crscore is not null group by timestamp having sum(crscore%65536)>0 order by timestamp desc)### t group by hodex order by hodex
```

Score Summary for All Users

NSE Training Institute © Fortinet Inc. All Rights Reserved. 19

While the name of predefined reports aims to be indicative of what type of data is included in it, having a more complete view of the report contents is helpful—especially when trying to determine if a predefined report meets your needs. One way is to examine what charts are contained in the report, and on a more granular level, what datasets define those charts.

There are several ways to determine which charts and datasets are used in reports. One quick way is to view the template associated with the report. The template includes all the charts included in the report.

To discover which dataset is associated with a chart, you can start the process of cloning the desired template (you don't need to actually create the clone for this procedure). This gives you some capabilities that are not available in the default templates. While on the clone, right-click the chart and select **Clone Chart**. The dialog that appears lists the dataset.

You can view the specific query for the dataset on the **Report Definitions > Datasets** page.

# DO NOT REPRINT

## © FORTINET

## Reports for Log Groups

- Run reports on log groups
- Useful for:
  - Examining large networks as a whole
  - Grouping devices by purpose (geo-location, and so on)

The screenshot shows the FortiAnalyzer interface. On the left, there's a 'Reports' section with tabs for 'View Report', 'Settings' (which is selected), and 'Layout'. It includes fields for 'Paths', 'Name' (set to '360-Degree Security Review'), 'Time Period' (set to 'Last 7 Days'), 'Devices' (radio buttons for 'All Devices' and 'Specify' are shown, with 'Specify' selected and highlighted with a red box), and 'Subnets' and 'Type' options. A red arrow points from the 'Specify' button in the 'Devices' section to a 'Select Device' sidebar on the right. This sidebar lists 'Edit: 360-Degree Security Review' and shows a tree view under 'Select Device'. The tree starts with 'Name' and branches into 'All FortiGate', 'ISFW', 'Local-FortiGate', and finally 'Log-Group-Canada-FGTs' under 'Log Group'. The 'Log-Group-Canada-FGTs' node is also highlighted with a red box.

FortiAnalyzer also provides the ability to run reports on log groups so you can look at the log data from the group as if it were a single device.

One such use case for log groups is to determine how your network is performing as a whole, especially if you have a large network that has multiple FortiGate devices positioned at different points. You can obtain information about total traffic usage and get a complete picture of your network instead of receiving a fragmented look based on multiple, unconnected devices.

You may want to use log groups to determine how devices in specific geographical locations are performing as well.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

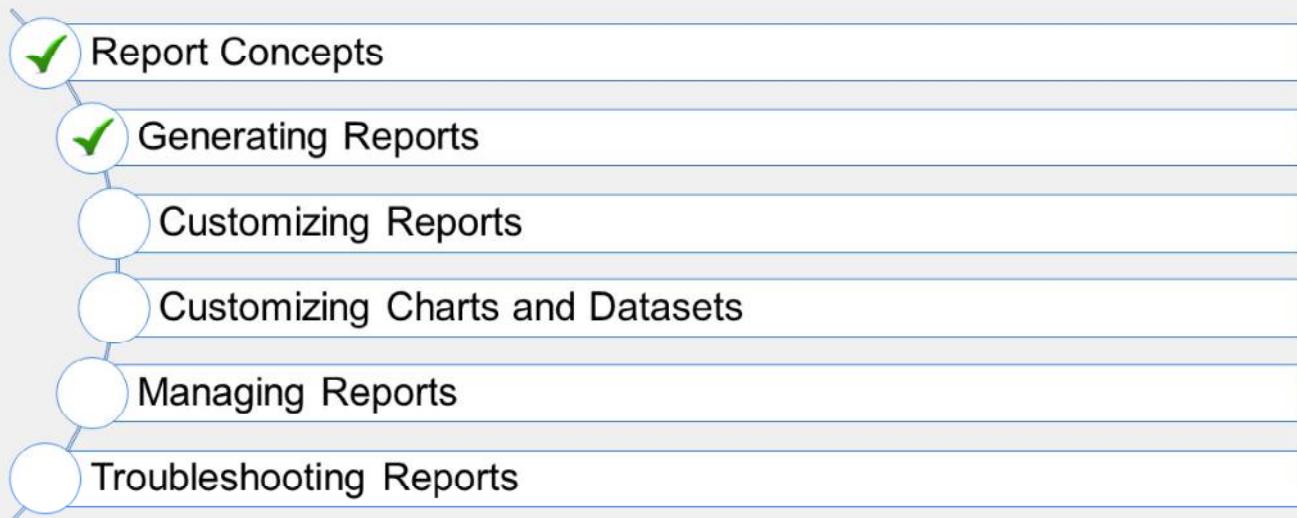
1. Templates do not contain \_\_\_\_\_.

- A. Data
- B. Charts

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



Good job! You now understand how to generate reports.

Now, you will learn how to customize reports.

**DO NOT REPRINT**

**© FORTINET**

## Customizing Reports

### Objectives

- Describe the difference between templates and reports
- Clone and edit templates and reports
- Create new templates and reports
- Insert macros

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in report customization, you will be able to generate reports specific to your requirements.

**DO NOT REPRINT****© FORTINET**

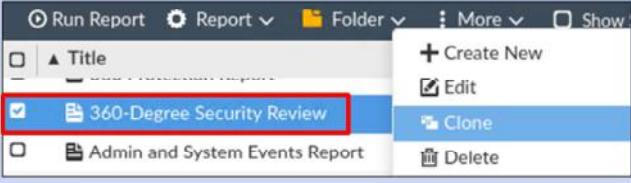
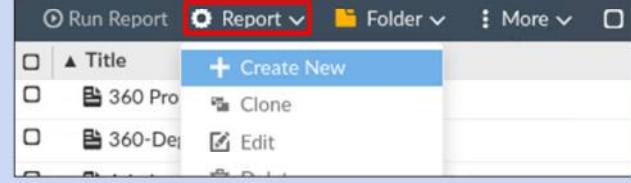
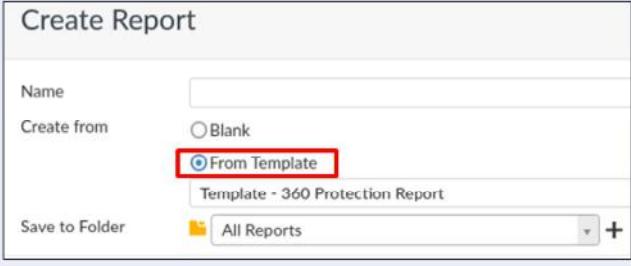
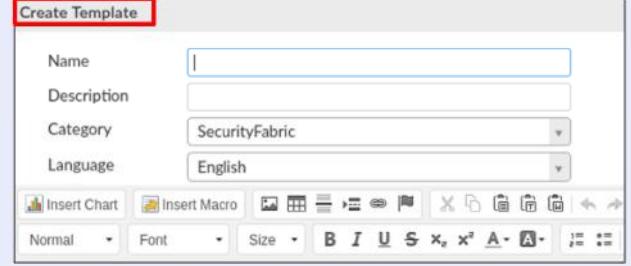
## If Predefined Reports Do Not Meet Requirements

- Fine-tuning the settings of predefined reports may not meet your requirements
  - This doesn't mean you must create a new template or report from scratch!
- Can customize existing templates or reports—don't waste time and effort if you don't have to!

Predefined reports may not meet all of your organization's requirements, even after fine-tuning the report settings. While FortiAnalyzer provides the option to create new templates and reports from scratch, there are customization options available.

**DO NOT REPRINT**  
**© FORTINET**

## Customization Options

Minor / Moderate Customizations	Major Customizations
<p>Clone a report or template, then edit the clone</p> 	<p>Create a new report from scratch (blank)</p> 
<p>Create a new report from an existing template, then edit</p> 	<p>Create a new template (which you can use in a report)</p> 

**NSE Training Institute** © Fortinet Inc. All Rights Reserved. 25

For minor or moderate changes to existing templates or reports, you can use cloning. For cloning, you would clone a report or template and then edit the clone to suit your requirements.

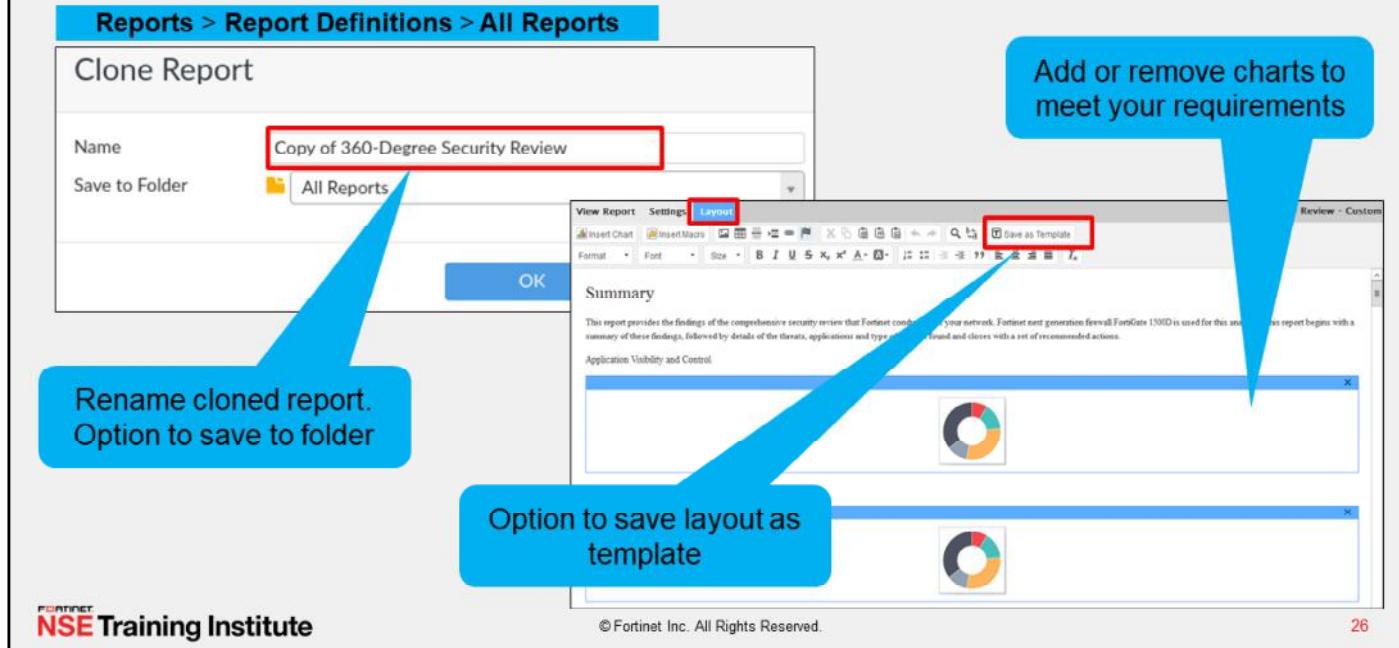
For reports only, you can create a new report, but base it on an existing template. Then edit that new report to suit your requirements.

While you can directly edit the layout of predefined reports (but not templates), it is a best practice to clone and edit predefined reports instead. This preserves the default reports if your direct edits to the report are not successful.

If major changes are required to existing templates or reports (that is, no report is close to your needs), you can create a new report or template from scratch.

**DO NOT REPRINT**  
© FORTINET

## Cloning and Editing Reports



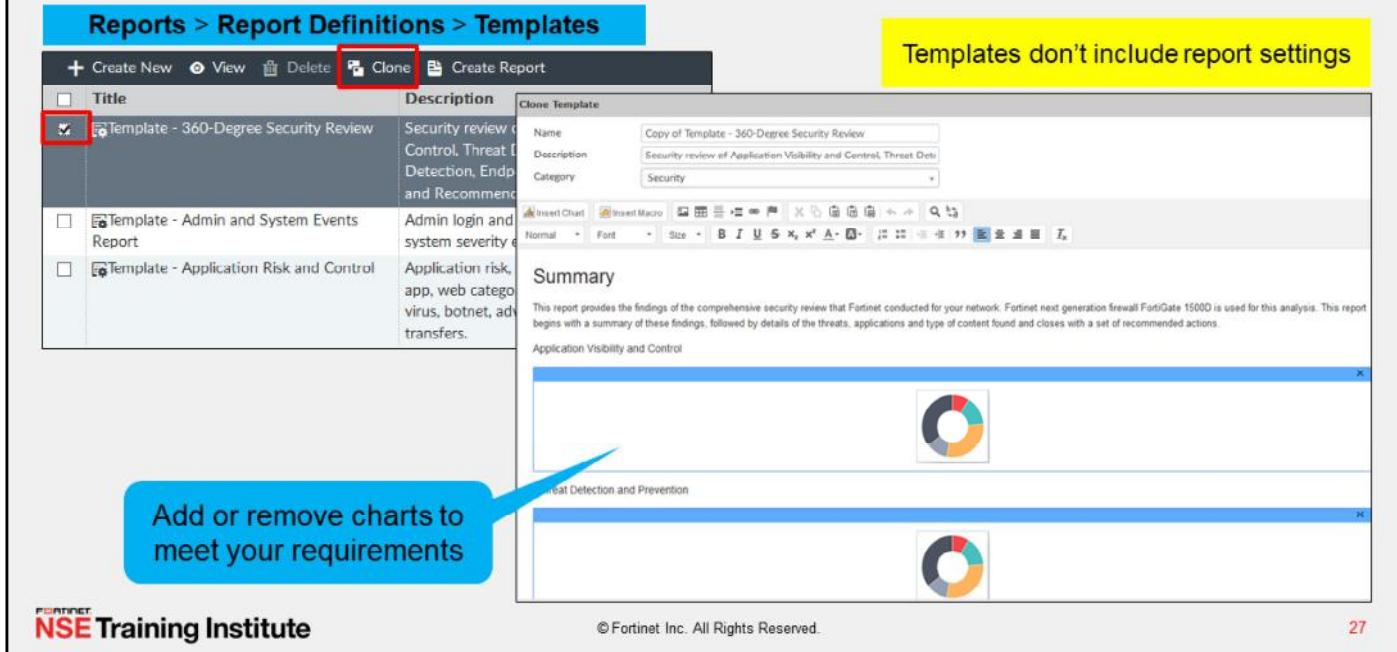
You can clone a report from the **All Reports** page. Again, you should clone when you need to make only minor to moderate changes. For example, when you want to borrow many of the elements, but not all, from an existing report.

In the cloned report, you can edit the settings as well as the layout. Note that the **Layout** tab provides the option to save the layout as a template, if necessary.

Unlike predefined reports, you can delete cloned reports.

**DO NOT REPRINT**  
**© FORTINET**

## Cloning and Editing Templates



The screenshot shows the 'Reports > Report Definitions > Templates' interface. A template titled 'Template - 360-Degree Security Review' is selected and highlighted with a red box. The 'Clone' button, also highlighted with a red box, is located in the top navigation bar. A yellow callout bubble to the right of the 'Clone' button states 'Templates don't include report settings'. A blue callout bubble with a blue arrow pointing to the 'Clone' button contains the text 'Add or remove charts to meet your requirements'. The 'Clone Template' dialog box is open, showing the cloned template's details: Name: 'Copy of Template - 360-Degree Security Review', Description: 'Security review of Application Visibility and Control, Threat Detection, Endpoints and Recommendations', and Category: 'Security'. The dialog also includes a rich text editor toolbar and a preview section for the 'Summary' report content.

Reports > Report Definitions > Templates

+ Create New View Delete Clone Create Report

Title Description

Template - 360-Degree Security Review Security review of Application Visibility and Control, Threat Detection, Endpoints and Recommendations

Template - Admin and System Events Report Admin login and system severity events

Template - Application Risk and Control Application risk, app, web category, virus, botnet, ad transfers.

Clone Template

Name: Copy of Template - 360-Degree Security Review  
Description: Security review of Application Visibility and Control, Threat Detection, Endpoints and Recommendations  
Category: Security

Add Insert Chart Insert Macro Normal Font Size B I S x² A- Search

**Summary**

This report provides the findings of the comprehensive security review that Fortinet conducted for your network. Fortinet next generation firewall FortiGate 1500D is used for this analysis. This report begins with a summary of these findings, followed by details of the threats, applications and type of content found and closes with a set of recommended actions.

Application Visibility and Control

Real Detection and Prevention

© Fortinet Inc. All Rights Reserved.

NSE Training Institute

27

You can clone a template from the **Templates** page. Again, you should clone when you need to make only minor to moderate changes. For example, when you want to borrow many of the elements, but not all, from an existing template. In the cloned template, you can edit only the layout.

Unlike predefined templates, you can delete cloned templates.

**DO NOT REPRINT**  
© FORTINET

## Creating a New Report From Blank

The screenshot shows the FortiAnalyzer interface for creating a new report. On the left, a 'Create Report' dialog box is open, showing fields for 'Name' (empty), 'Create from' (radio buttons for 'Blank' and 'From Template' with 'Blank' selected), and 'Save to Folder' (dropdown set to 'All Reports'). On the right, the 'Layout' tab of the report configuration page is active, displaying settings for 'Path' (set to 'All Reports'), 'Time Period' (set to 'Last 7 Days'), and 'Devices/Subnets/Type' (all options are 'All'). Below these are checkboxes for 'Enable Schedule', 'Enable Notification', and 'Enable Auto-cache'. A 'Filters' button and an 'Advanced Settings' link are also present.

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

28

You can create a new report by selecting **Blank** on the **Create Report** page. As shown in the graphic on this slide, you can configure both the settings and the layout. Because it is a new report, both the settings and the layout are blank and you must configure them.

After you create the layout, you do have the option to save it as a template. You can then use that template for other reports you create.

You can delete custom reports.

# DO NOT REPRINT

## © FORTINET

### Creating a New Template

The screenshot shows the 'Report Definitions > Templates' page. At the top, there's a toolbar with options: '+ Create New' (highlighted with a red box), 'Edit', 'Delete', 'Clone', 'Create Report', and 'Install Template Pack'. Below the toolbar is a table listing existing templates:

Title	Language	Description
Template - 360 Protection Report	English	Present a brief summary of hardware/software inventory of the FortiGate over a 30 day period.
Template - 360-Degree Security Review	English	Security review of Application Visibility and Control, Threat Detection, Exfiltration Detection, Endpoint Detection, Prevention and Recomme

A yellow callout box on the right side of the table says 'Templates don't include report settings'.

A blue callout box on the left side of the page says 'Layout is empty when creating from a blank template. Must create.' It points to a 'Create Template' dialog box which is partially visible on the right. The dialog box has fields for 'Name', 'Description', 'Category' (set to 'SecurityFabric'), and 'Language' (set to 'English'). Below these fields is a toolbar with various icons for inserting charts, macros, and other elements.

**NSE Training Institute** © Fortinet Inc. All Rights Reserved. 29

You can create a new template on the **Templates** page. The graphic shown on this slide shows that the **Layout** starts as a blank space. Use the layout toolbar on this page to build your layout. The toolbar allows you to insert existing charts and macros, and lets you add and format text, as well as add images and links.

After you create the layout, you can save it as a new custom template. You can then use that template in reports.

You can delete custom templates.

# DO NOT REPRINT

## © FORTINET

### Customization: Template vs. Report

- Which customization approach to take: template or report?
- Most important difference: templates only include the layout of the report—they don't include report settings (either basic configurations or advanced settings)
- There is no *correct* approach—you can get the same results by various methods
  - Best practice is to attack it from an efficiency and needs standpoint
- Think about:
  - The amount of customization required
  - Whether you want to preserve most of the report settings
  - Whether you want to use the layout for one report or many reports

The screenshot shows two windows side-by-side. The left window is titled 'Template' and has a blue header bar. It contains fields for 'Name' (Template - IPS Report), 'Description' (Intrusions detected by type, severity, victims, sox), 'Category', and 'Language'. Below these are toolbar buttons for 'Insert Chart', 'Insert Macro', and various document tools. A red box highlights a section labeled 'Summary' containing a chart titled 'Intrusions By Severity' with a pie chart icon. The right window is titled 'Report' and also has a blue header bar. It includes tabs for 'View Report', 'Settings', and 'Layout', with 'Layout' being highlighted by a red box and an arrow pointing to it. Below the tabs is another toolbar. The main area is labeled 'Summary' and contains the same 'Intrusions By Severity' chart as the template window.

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

30

There is a close association between templates and reports. As discussed earlier, you can clone and edit both reports and templates, and you can create both new reports and templates. So, how do you know which customization approach to take: Do you attack the customization from the template side or report side?

One of the most vital differences between templates and reports is that templates include only the details you can find under the **Layout** tab of the report—they don't include report settings (either the basic configuration or advanced settings). So, when deciding whether to perform customizations on the template side or the report side, it depends on what you want to preserve and what you want to modify.

In the end, there is no *correct* approach. You can achieve the same results through various methods. A best practice is to attack it from an efficiency and needs standpoint.

# DO NOT REPRINT

## © FORTINET

## Inserting Macros as Abbreviated Dataset Queries

- Macros specify what data to extract from the logs
  - Macros represent a sequence of instructions (dataset queries) in abbreviated form
- You can insert macros as data in your reports, without having to use a chart to display the data
- Can use predefined macros or create custom macros
  - ADOM-specific

Supported in FortiGate and  
FortiCarrier ADOMs only!

The screenshot shows the 'Macro Library' section of the FortiAnalyzer interface. On the left, a list of predefined macros is shown in a table format:

Name	Description	Device Type	Category
Application Category with Highest Session Count	Application category with the highest session count		
Application with Highest Bandwidth	Application with the highest bandwidth usage		
Application with Highest Session Count	Applications with the highest session count		
Attack with Highest Session Count	Attack with highest session count		
Botnet and Malware Infections	Botnet and Malware Infections		

A specific macro, 'Application Category with Highest Session Count', is highlighted with a red box and has a red arrow pointing to its detailed view on the right. The detailed view shows the following configuration:

**View Macro**

**Name:** Application Category with Highest Session Count  
**Description:** Application category with the highest session count  
**Dataset:** App-Sessions-By-Category  
**Query:** select appcat, count(\*) as sessions from Slog where \$filter and (logflag&1>0) and nullifno(appcat) is not null group by appcat order by sessions desc  
**Data Binding:** appcat  
**Display:** Text

**NSE Training Institute** © Fortinet Inc. All Rights Reserved. 31

In FortiAnalyzer, macros specify what data to extract from the logs—they represent dataset queries in abbreviated form. You can insert macros as data in your reports, without having to use a chart to display the data. FortiAnalyzer provides predefined macros, or you can create your own custom macros.

Note that macros are ADOM-specific and supported in FortiGate and FortiCarrier ADOMs only.

# DO NOT REPRINT

## © FORTINET

### Macro Example

**Reports > Report Definitions > Templates**

Create Template

Name: App-Category-with-Highest-Session-Count

Description:

Category: Application

Toolbar: Insert Chart, Insert Macro, Font, Bold, Italic, Underline, etc.

The application with the Highest Session Count [Application Category with Highest Session Count]

Report Date: March 6, 2017 12:45  
Data Range: 2017-02-01 00:00 - 2017-02-28 23:59 PST (FAZ local)  
The application with the Highest Session Count Network Service

Appendix A  
Devices  
Local-FortiGate

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

32

You can insert macros into custom templates, or into the layout of reports (either predefined or custom).

In the example shown on this slide, text is added before the inserted macro to give the macro some context. As you can see, when the report is generated, the data from the logs is extracted according to the query used in the macro. In this example, the macro **Application Category with Highest Count** returned **Network.Service** from the database.

**DO NOT REPRINT**

**© FORTINET**

## Knowledge Check

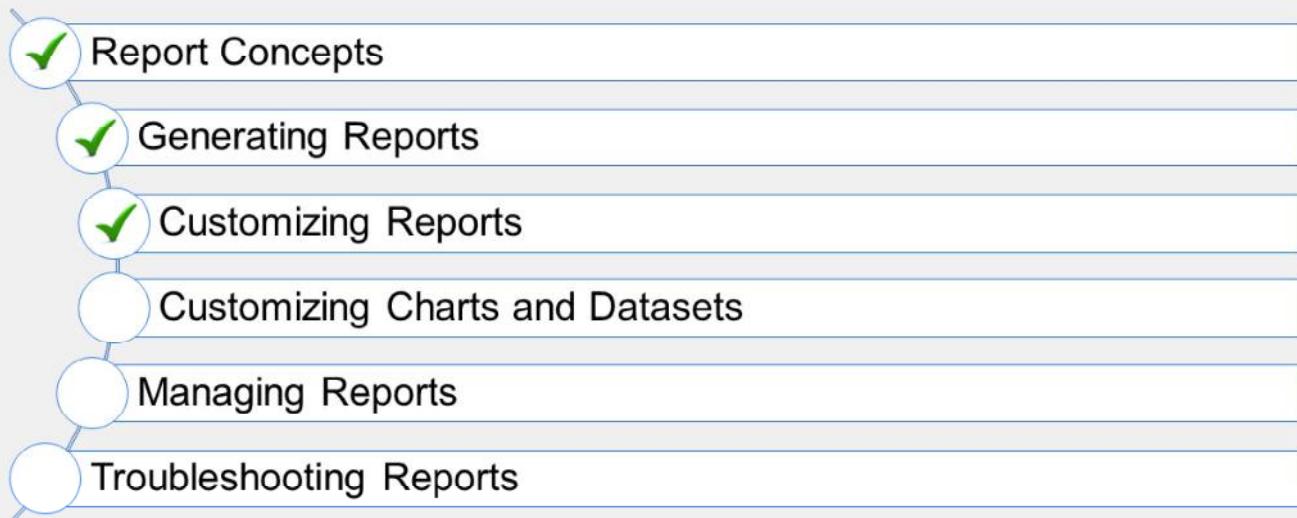
1. Which statement about macros is true?

- A. Macros are abbreviated dataset queries
- B. Macros cannot be customized

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



Good job! You now understand how to customize reports.

Now, you will learn how to customize charts and datasets.

**DO NOT REPRINT**

**© FORTINET**

## Customizing Charts and Datasets

### Objectives

- Clone and create new charts
- Clone and create new datasets

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in chart and dataset customization, you will be able to extract unique combinations of data from the database specific to your requirements.

# DO NOT REPRINT

## © FORTINET

### If Predefined Charts/Datasets Do Not Meet Requirements

- By default, the **Chart Library** contains more than 700 charts!
  - Can't edit default charts
- By default, the **Datasets** library contains more than 800 datasets!
  - Can't edit default datasets
- Just like templates and reports, you can clone and edit both charts and datasets and create new ones!
- Gives you the flexibility to pull a unique combination of data from the database that doesn't exist in any default chart or dataset

In some cases, simply adding or removing default charts from a report or template may not meet your requirements: you might need to pull a unique combination of data from the database when no predefined chart or dataset for that unique combination exists. In this case, you can either clone and edit charts and datasets, or create new charts and datasets from scratch.

# DO NOT REPRINT

## © FORTINET

## Cloning and Creating New Charts

- Create new charts or clone and modify existing charts

The screenshot shows the 'Create Chart' interface. At the top, there are buttons for '+ Create New', 'Edit', 'Delete', 'Clone' (highlighted with a red box), 'Export', 'Import', 'Show Predefined' (unchecked), and 'Show Custom' (checked and highlighted with a red box). Below this is a breadcrumb navigation: 'Reports > Report Definitions > Chart Library'. The main form has fields for 'Name', 'Description', 'Dataset' (set to 'App-Risk-App-Usage-By-Category'), 'Resolve Hostname' (set to 'Inherit'), 'Chart Type' (set to 'Table'), and 'Data Bindings' (set to 'Table Type: Regular'). The 'Columns' section shows two columns: 'Column 1' with title 'appcat' and 'Width 0%', and 'Column 2' with title 'bandwidth' and 'Width 0%'. A note below says 'Data Binding Format appcat Default' and 'Order By Show Top (0 for all results) 10'. The bottom of the interface includes the 'NSE Training Institute' logo, a copyright notice '© Fortinet Inc. All Rights Reserved.', and a page number '37'.

When creating a new chart, you first need a dataset that queries the database for the information you want. This is absolutely required. All a chart does is convert the text-based results of that query into a graphical format of your choosing (table, bar, pie, line, area, donut, and so on.).

After you select your dataset and chart type, the information in the **Data Bindings** section automatically adjusts based on those selections. Check the *FortiAnalyzer Administration Guide* for more information on the data bindings option for your specific dataset and chart type.

If FortiAnalyzer includes an existing chart that is very similar to the output you want, you can clone and modify the chart rather than create a brand new one. A cloned chart is categorized as a custom chart, so remember to enable **Show Custom** so that it appears in the chart library table for easy viewing or access.

# DO NOT REPRINT

## © FORTINET

## Cloning and Creating New Datasets

- Create new dataset, or clone and modify existing dataset
  - For more information on SQL and datasets for use with FortiAnalyzer reports, see the supplementary FortiAnalyzer SQL and Datasets lesson

The screenshot shows the 'Datasets' page in the FortiAnalyzer interface. A new dataset named 'Example dataset' is being created with a 'Traffic' log type. The 'Query' field contains an SQL SELECT statement. A red box highlights the 'Test' button, which is highlighted with a blue callout bubble: 'Always test query to ensure it's well formed!'. Below the query, a table titled 'Test Result' shows session statistics. A blue arrow points from the 'Test' button to the results table, with another blue callout bubble: 'Confirm results match expectations'.

domain	session
208.91.112.55	12330
10.200.3.1	11129
10.200.1.10	1555
104.193.88.103	252
104.239.213.7	221
89.248.169.50	208
114.32.154.51	208

At the bottom of the page, there is a toolbar with buttons for 'Create New', 'Edit', 'Delete', 'Clone', 'Validate', and 'Validate All Custom'. The 'Validate All Custom' button is highlighted with a red box and a blue callout bubble: 'Can also validate all custom datasets in one click on Datasets page'.

When creating a new dataset, you need to write an SQL SELECT query. For more information about writing queries, see the *FortiAnalyzer SQL and Datasets* lesson (supplemental training material).

After you write the query, be sure to test it to ensure it's well formed. Also, review the test results, and make sure the query is returning the data you expect.

If FortiAnalyzer includes an existing dataset that is very similar to what you want, you can clone and modify the dataset rather than create a brand new one.

Note that you can validate all custom datasets—which includes new and cloned datasets—in one click on the **Datasets** page. You should always validate your custom datasets after a firmware upgrade.

**DO NOT REPRINT**  
**© FORTINET**

## Building Datasets and Charts from Search Results

- In **Log View**, set filters to search for logs

**Log View > Tools > Chart Builder**

ADOM: NEW    Custom View       

Dest  
120  
52  
96  
120  
10.0

Real-time Log  
Display Raw  
Download  
Case Sensitive Search  
**Chart Builder**  
User Display Preferences

**Chart Builder**

Name: SQL and Code Injections  
Columns: Search...  
 Date/Time  
 Device ID  
 Severity  
 Source IP  
 Destination IP  
 Action  
 Service  
Group By: \_\_\_\_\_  
Order By: Date/Time  
Sort: Descending  
Show Limit: 50  
Device: All Devices  
Time Frame: last 12 hours  
Search: attack\*.Code.Injection.\*.Sql.Injection

Query:

```
select from _idma@itime as idme, 'devid', 'severity', 'srcip', 'attack' from $log where $filter and ( lower('attack') LIKE lower('%CodeInjection') OR lower('attack') LIKE lower('%SQLInjection')) order by 'id' desc, 'itime' desc
```

Preview

Date/Time	Device ID	Severity	Source IP	Attack Name
2016-12-20 06:32:10	FGVM010000064692	high	10.200.1.254	PHP.URI.Code.Inject
2016-12-20 06:31:59	FGVM010000064692	high	10.200.1.254	PHP.URI.Code.Inject
2016-12-20 06:29:50	FGVM010000064692	high	10.200.1.254	PHP.URI.Code.Inject
2016-12-20 06:29:39	FGVM010000064692	high	10.200.1.254	PHP.URI.Code.Inject
2016-12-20 06:29:39	FGVM010000064692	high	10.200.1.254	PHP.URI.Code.Inject

Preview    Save    Cancel

NSE Training Institute    © Fortinet Inc. All Rights Reserved.    39

A quick way to build a custom dataset and chart is to use the chart builder tool. This tool is located in **Log View**, and allows you to build a dataset and chart automatically, based on your filtered search results. In **Log View**, set filters to return the logs you want. Then, in the **Tools** menu, select **Chart Builder** to automatically build the search into a dataset and chart. You can also fine-tune the dataset further by:

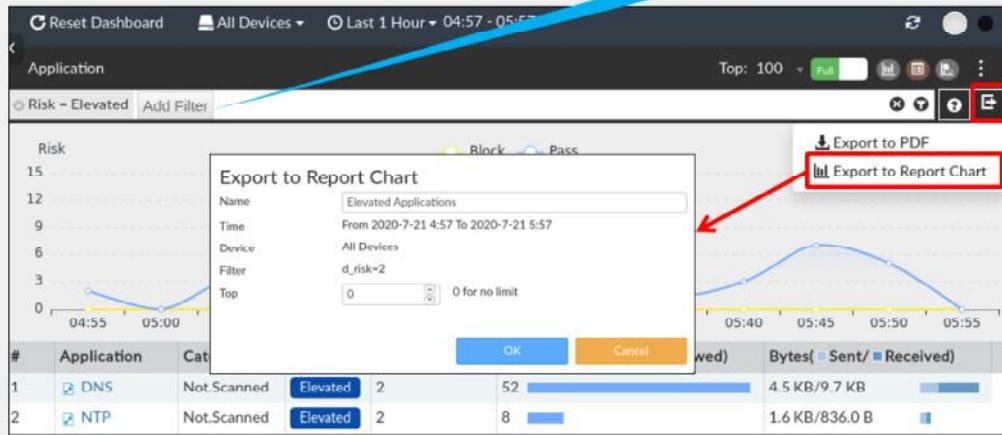
- Adding more columns
- Setting group by, order by, and sort filter
- Setting a limit on results
- Setting the device and time frame

DO NOT REPRINT  
© FORTINET

## Export a FortiView to a Chart

- Similar to the **Chart Builder** feature in **Log View**, you can export a chart from a FortiView
- Chart export includes any filters you set

Chart export will include any filters you set



**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

40

Similar to the **Chart Builder** feature in **Log View**, you can export a chart from a FortiView. The chart export includes any filters you set on the FortiView.

**DO NOT REPRINT****© FORTINET**

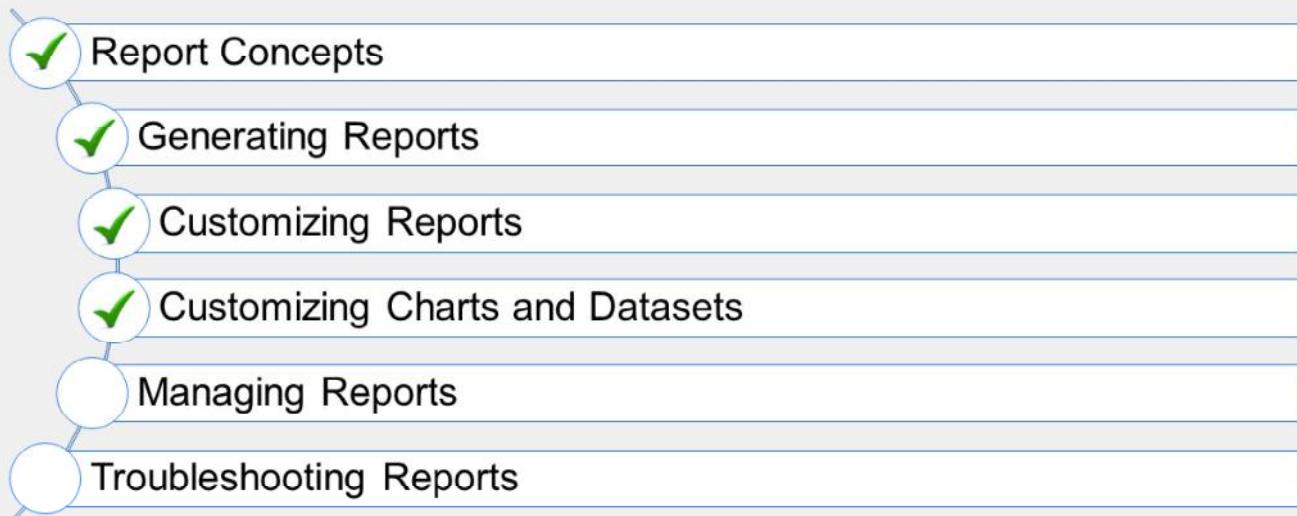
## Knowledge Check

1. Which report elements can be affected by a firmware upgrade?
  - A. Report settings
  - B. Custom datasets
  
2. Which FortiAnalyzer feature allows you to automatically build a dataset and chart based on a filtered search result?
  - A. Export to Report Chart (FortiView)
  - B. Dataset Library

**DO NOT REPRINT**

**© FORTINET**

## Lesson Progress



Good job! You now understand how to customize charts and datasets.

Now, you will learn how to manage reports.

**DO NOT REPRINT**

**© FORTINET**

## Managing Reports

### Objectives

- Configure external storage for reports
- Enable auto-cache
- Group reports
- Import and export reports and charts
- Attach reports to incidents
- Manage scheduled reports

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in report management, you will be able to handle, store, and more efficiently control reports and report generation.

**DO NOT REPRINT**  
**© FORTINET**

## External Storage of Generated Reports

- Send or store reports externally for backup purposes
  - Configured per ADOM
- Email reports or upload to server (PDF, HTML, XML, CSV formats)
- Requires back-end configuration, including:
  - Mail server (emailed reports only)
  - Output profile
  - Can create multiple profiles (email and server)

Configure for each report!

Output Profile  Enable Notification Email and Server Profile +

### Reports > Advanced > Output Profile

Create Output Profile  
 Name: Email and Server Profile  
 Comments:  
 Output Format:  PDF  HTML  XML  CSV  
 Email Generated Reports  
 Subject: Generated Report  
 Body: Please review generated report.  
 Recipients: Email Server Mail Server: 10.20.1.210... To fortinet@traininglab admin@trainir +  
 Upload Report to Server  
 Server Type: SFTP  
 Server: 0.0.0.0  
 User:  
 Password:  
 Directory:  
 Delete file(s) after uploading

Preconfigured mail server

Option to delete reports locally after uploading to server

### System Settings > Advanced > Mail Server

Create New Mail Server Settings  
 SMTP Server Name: Mail Server  
 Mail Server: 10.200.1.210  
 SMTP Server Port: 25  
 Enable Authentication:   
 E-Mail Account:  
 Password: \*\*\*\*\*

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

44

You can configure FortiAnalyzer to email generated reports to specific administrators, or to upload generated reports to a syslog server. This allows reports to exist externally, instead of remaining locally on FortiAnalyzer.

In order to use any of these external storage methods, you must first set up the back end. This includes configuring a mail server (for emailed reports only) and an output profile. If ADOMs are enabled, each ADOM has its own output profiles.

The output profile specifies the following:

- The format of the report, such as PDF, HTML, XML, and CSV
- Whether to email generated reports or upload to a server. You can specify one option, both, or create multiple outlook profiles. Server options include FTP, SFTP, and SCP.
- Whether to delete the report locally after uploading to the server

**DO NOT REPRINT**

**© FORTINET**

## SQL Hard Cache (hcache)

- The hcache must build before FortiAnalyzer can build the report
  - Increases report generation time
  - If no new logs are received for the reporting period, the hcache doesn't need to rebuild
  - If new logs come in, the hcache needs to rebuild
- To reduce report generation time, enable auto-cache from report settings
  - The hcache automatically updates when new logs come in and new log tables are generated
- Enable hcache for most reports to ensure they are efficiently generated
  - Caveat: hcache uses system resources (especially for reports that take a long time to generate datasets)

The screenshot shows the 'Settings' tab of a report definition. The 'Name' is set to 'Client Reputation', 'Time Period' is 'Last 7 Days', 'Devices' is 'All Devices', and 'Type' is 'Single Report'. Under the 'Settings' tab, there are three checkboxes: 'Enable Schedule', 'Enable Notification', and 'Enable Auto-cache'. The 'Enable Auto-cache' checkbox is checked and highlighted with a red border.

Hcache is automatically enabled for scheduled reports

When a report generates, the system builds the charts from precompiled SQL hard-cache data, known as hcache. If the hcache is not built when you run the report, the system must create the hcache first and then build the report. This adds time to the report generation. However, if no new logs are received for the reporting period, when you run the report a second time it is much faster, because the hcache data is already precompiled.

To boost the report performance and reduce report generation time, you can enable auto-cache in the settings of the report. In this case, the hcache is automatically updated when new logs come in and new log tables are generated.

Note that hcache is automatically enabled for scheduled reports. If you are not scheduling a report, you may want to consider enabling hcache. This ensures reports are efficiently generated. However, be aware that this process uses system resources (especially for reports that require a long time to assemble datasets), so you should monitor your system to ensure it can handle it.

# DO NOT REPRINT

## © FORTINET

### Grouping Reports to Improve Report Generation Time

- Group similar reports to improve report generation time
  - Useful if running a large number of reports
- Benefits:
  - Reduces the number of hcache tables
  - Improves auto-hcache completion time

[View report grouping information](#)

```
# configure system report group
edit 0
  set adom <ADOM-name>
  config group-by
    edit <SQL-column>
    next
    edit vd
    next
  end
  set report-like <report_name_string>
  next
end
```

SQL column is added to the hcache creation queries with any related report

```
# execute sql-report list-schedule
<ADOM-name>
```

```
# execute sql-report hcache-build
<ADOM-name> <schedule-name>
"<start-time>" "<end-time>"
```

Rebuild select

Group report function is applied to any report that contains this string (can use any word)

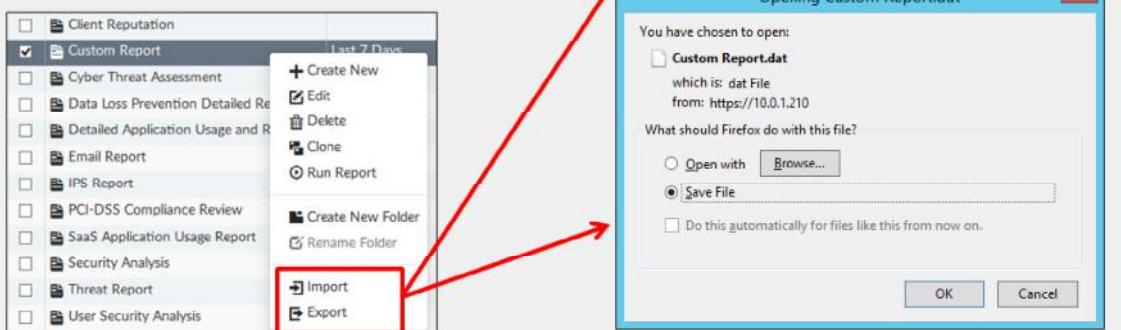
If the same (or similar) reports are run against many different FortiGate devices, you can significantly improve report generation time by grouping the reports. Report grouping can reduce the number of hcache tables and improve auto-hcache completion time and report completion time.

After you configure report grouping using the `configure system report group` CLI command, you must rebuild the report hcache tables. You can rebuild the hcache tables for those specific reports.

**DO NOT REPRINT**  
**© FORTINET**

## Moving Reports Between ADOMs

- Each ADOM has its own reports, libraries, and advanced settings
- Can export reports and charts (default and custom) and import into a different ADOM based on the same type (that is, FortiGate ADOM to FortiGate ADOM)
  - Chart imports dataset associated with chart
  - Can save layout of imported report as template



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

47

Remember, each ADOM has its own reports, libraries, and advanced settings. You can, however, import and export reports and charts (whether default or custom) into a different ADOM within the same FortiAnalyzer device or a different FortiAnalyzer device. The ADOM must be of the same type.

You can't export templates and datasets. However, when you import an exported report, you can save the layout of the report as a template. When you export a chart, the associated dataset is silently exported with it, so when you import an exported chart, the associated dataset is imported as well.

You can export and import reports through the right-click menu on the **Reports** page.

The **Chart Library** includes the export and import functions in the toolbar.

# DO NOT REPRINT

## © FORTINET

## Attach Reports to Incidents

- Attach a report to add historical data to an incident
- There are two ways to attach a report:
  - Manually, after incident creation
  - Automatically added by automation playbooks

The screenshot illustrates the manual attachment of a report to an incident. It consists of two main windows:

- Top Window (Reports > Generated Reports):** This window lists generated reports. One specific report, "Cyber Threat Assessment-2020-06-18-0902\_199", is highlighted with a red box. A red arrow points from this report to the second window.
- Bottom Window (Incident List):** This window shows a list of incidents. An incident with Incident Number IN000000899 is selected and highlighted with a red box. A blue arrow points from this incident to a red button labeled "Attach to Incident". A callout bubble next to this button contains the text "Manually attaching a report to an incident".

You can attach reports to incidents to add historical data in addition to real-time events. The following are the two ways that you can attach a report:

- You can attach reports manually, after incident creation.
- Reports can be attached automatically, by automation playbooks.

This slide shows how to manually attach reports from **Reports > Generated Reports**.

**DO NOT REPRINT**  
**© FORTINET**

## Attach Reports to Incidents (Contd)

- Attach a report from the **FortiSoC > Incidents** page

The screenshot shows the FortiSoC interface with the 'Incidents' tab selected. The main pane displays an 'Operating System' section with details like IP: 10.0.3.20/32 and a timeline from 14:30 to 18:30. Below this is the 'Incident Timeline' showing event counts per hour. A red arrow points from the 'Add' button in the top right of the main pane to the 'Attach Report' dialog box.

**Attach Report**

Report Name	Format	Time Range	Devices	Status
Cyber Threat Assessment-2020-06-18-0904_199	HTML PDF XML CSV	2020/06/11 - 2020/06/18	Training-Lab	8s
Cyber Threat Assessment-2020-06-18-0902_197	HTML PDF XML CSV	2020/06/11 - 2020/06/18	Training-Lab	8s

**Adding report to incident manually**

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

49

This slide shows how to manually attach report from **FortiSoC > Incidents**. On the **Incident Analysis** page, you can click the **Reports** tab and the select the **Format** column to open new browser tab to show the content of a report.

**DO NOT REPRINT**  
**© FORTINET**

## Viewing Scheduled Reports Through Calendar

- Graphic view of scheduled (generated and pending) reports

The screenshot shows a calendar for February 2017. Each day contains scheduled report entries. A tooltip indicates that hovering over a report entry will show its name, status, and device type. Another tooltip shows how to edit or disable pending reports and delete or download generated reports by right-clicking. A third tooltip shows the report color configuration, which is set to green. A dropdown menu lists various colors including Bold Blue, Blue, Turquoise, Green, Bold Green, Yellow, Orange, and Red.

NSE Training Institute © Fortinet Inc. All Rights Reserved. 50

The **Report Calendar** provides an overview of all your scheduled reports. A check icon means the report was generated, while a clock icon means it is pending.

When you hover your mouse cursor over a scheduled report, a notification box appears that displays the report name, status, and device type.

You can edit and disable upcoming scheduled reports, as well as delete or download completed reports, by right-clicking the name of the report in the calendar.

Note that the scheduling is not actually done on this page but is configured in the specific report configuration itself.

You can also configure reports to display using a specific color in the report **Advanced Settings** window.

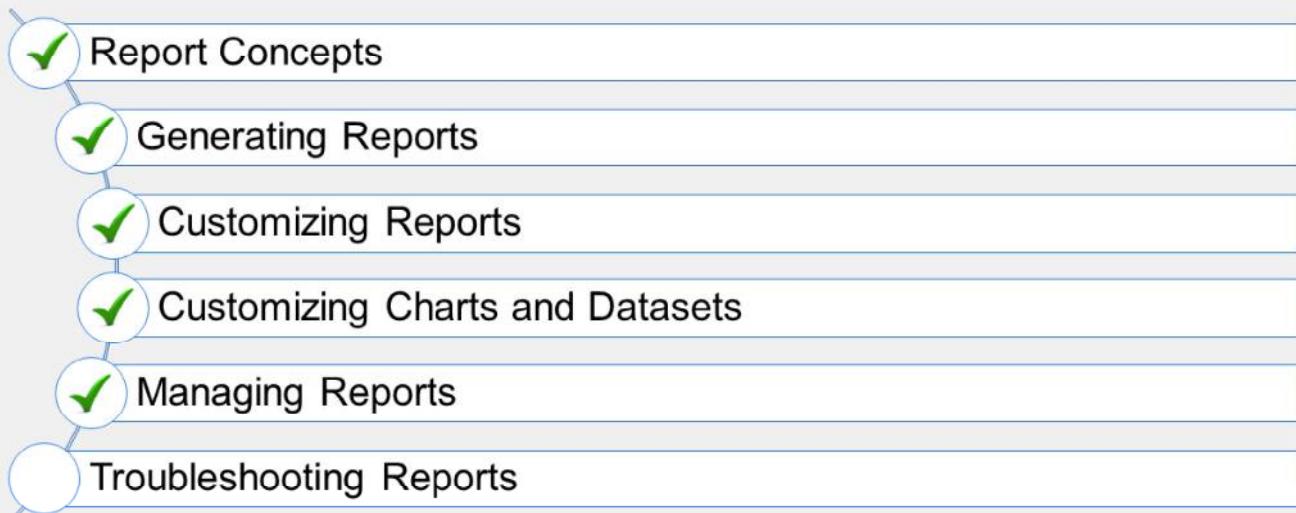
**DO NOT REPRINT****© FORTINET**

## Knowledge Check

1. What is the purpose of the auto-cache setting on reports?  
 A. To automatically update the hcache when new logs arrive  
 B. To reduce the log insert lag rate
  
2. If the same or similar reports will be run against many different FortiGate devices, which report feature can you use to improve report generation time?  
 A. Report grouping  
 B. Hcache

**DO NOT REPRINT****© FORTINET**

## Lesson Progress



Good job! You now understand how to manage reports.

Now, you will learn about report troubleshooting.

**DO NOT REPRINT**

**© FORTINET**

## Troubleshooting Reports

### Objectives

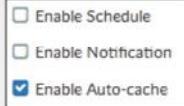
- Troubleshoot reports

After completing this section, you should be able to achieve the objective shown on this slide.

By demonstrating competence in report troubleshooting, you will be able to avoid, identify, and solve common reporting issues.

**DO NOT REPRINT**  
**© FORTINET**

## Troubleshooting Report Generation Run Time

- Retrieve report diagnostics
  - Check the **Report Summary** for details, including hcache building time
    - If hcache not precompiled, the report generation time increases
- Check log rates (see *Gathering Log Rate and Device Usage Statistics* slide)
- Check insert rate and receive rate
- Check log insert lag
- Enable auto-cache on report settings → 



The screenshot shows the FortiAnalyzer interface for generating reports. On the left, there's a list of reports with one selected: "360-Degree Security Review-2020-07-20-0527\_209". A context menu is open over this report, with the "Retrieve Diagnostic" option highlighted by a red box and arrow. To the right, a "Report Summary" window is displayed, also with its "HCACHE building time: 0.37s" entry highlighted by a red box and arrow. At the top of the interface, there are checkboxes for "Enable Schedule", "Enable Notification", and "Enable Auto-cache", with "Enable Auto-cache" checked.

If your network has a high volume of devices sending logs to FortiAnalyzer as well as high log volume, reports can take some time to generate. If you find reports are taking too long to generate, there are a few steps you can take to troubleshoot:

- Run diagnostics on your report and view the report summary at the end of the report. Look at the hcache time to see how long it took to build.
- Check your log rates (as described earlier) to get an idea of log volumes.
- Check the insert rate, receive rate, and the log insert lag. They can tell you the rate at which raw logs are reaching FortiAnalyzer (receive rate) and the rate at which they are indexed by the SQL database (insert rate) by the sqlplugind daemon. The log insert lag time tells you how many seconds the database is behind in processing the logs.
- Enable auto-cache in the report settings to boost the reporting performance and reduce report generation time. Scheduled reports have auto-cache enabled already.

**DO NOT REPRINT**  
**© FORTINET**

## Report Troubleshooting CLI Commands

- Use the following FortiAnalyzer CLI commands to troubleshoot report generation time issues

What to Investigate	CLI Command to Use
What is the SQL insertion status? What are the SQL query connections and hcache status?	# diagnose sql status sqlplugind # diagnose sql status sqlreportd
Is the hcache creation able to catch up? What are the log file-related activities (file rolled/deleted/uploaded)	# diagnose test application logfiled 2
What are the current SQL processes running (any log queries)?	# diagnose sql process list
What is the configuration status of all configured reports?	# execute sql-report list-schedule <ADOM>
What is the state of the hcache?	# diagnose test application sqlrptcached <level>
What is the hcache size on the file system?	# diagnose sql show hcache-size

This slide shows some CLI commands you can use to troubleshoot issues related to report generation time.

Run `# diagnose debug enable` at the beginning to display the output.

# DO NOT REPRINT

## © FORTINET

### Empty Reports

- Check the time frame covered by the report
- Compare the time frame to the logs and verify that you have the log file for the time in question
- Verify that you have logs from the time the report was run and from the device that the report was run for
- Test the datasets to ensure that they are retrieving the desired information
  - If they are not, check the SQL query associated with the dataset

The screenshot shows the FortiAnalyzer interface for report configuration and testing. On the left, there's a 'Dataset' configuration panel with tabs for 'Name' (App-Risk-High-Risk-Application), 'Log Type' (Traffic), and 'Query'. The 'Query' tab displays an SQL-like query:

```
select risk as d_risk, behavior as d_behavior, t2.id, t2.name, t2.app_cat, t2.technology, sum(coalesce(sentbyte, 0)+coalesce(rcvbyte, 0)) as bandwidth, count(*) as sessions from $log t1 inner join app_mdata t2 on t1.appid=t2.id where $filter and logid_to_int(logid) not in (4, 7, 14) and behavior is not null group by t2.id order by risk desc, sessions desc
```

Below the query is a 'Variables' section with two entries:

Variable	Expression	Description
User or Source IP (user_src)	coalesce(	User or Sou
Group (group)	group	

To the right, a 'Test Result' section is shown with a 'Test' button highlighted in red. It includes a 'Time Period' dropdown set to 'Last 7 Days', a 'Devices' section with a radio button for 'All Devices' (selected), and a table titled 'Test Result' showing the following data:

d_risk	d_behavior	id	name	app_cat	technology
3	Cloud	17459	Dropbox	Storage.Backup	Browser-Bas
3	Cloud	36660	Godaddy	Cloud.IT	Browser-Bas
3	Cloud	15832	Facebook	Social.Media	Browser-Bas
2	Cloud	16331	LinkedIn	Social.Media	Browser-Bas
2	Cloud	16001	Twitter	Social.Media	Browser-Bas

- Check the report advanced setting (such as user obfuscate)
  - Verify that the logs match any filter that you have set for the report

What happens if you run reports and they are empty or don't contain the desired information? Here are some troubleshooting tips:

- Check the time frame that is covered by the report. This is listed within the report itself.
- Compare the time frame to the logs and verify that you have the log file for the time in question
- Verify that you have logs from the time the report was run and from the device that the report was run for. A common issue is caused by logs being overwritten too quickly. The result is that the logs needed for the report are overwritten and, as such, are unavailable once the report is run. In this case, the solution is to increase the disk quota to ensure that logs are retained longer.
- Test the dataset in question and verify that it is retrieving the correct information. If it isn't, then troubleshoot the SQL query itself, because it is probably the dataset that contains the error.
- Check your report advanced settings. A setting such as user obfuscate can result in abnormal usernames in the report. Also verify the filters attached to a report. It is possible that your filter is filtering out the desired logs.

**DO NOT REPRINT**

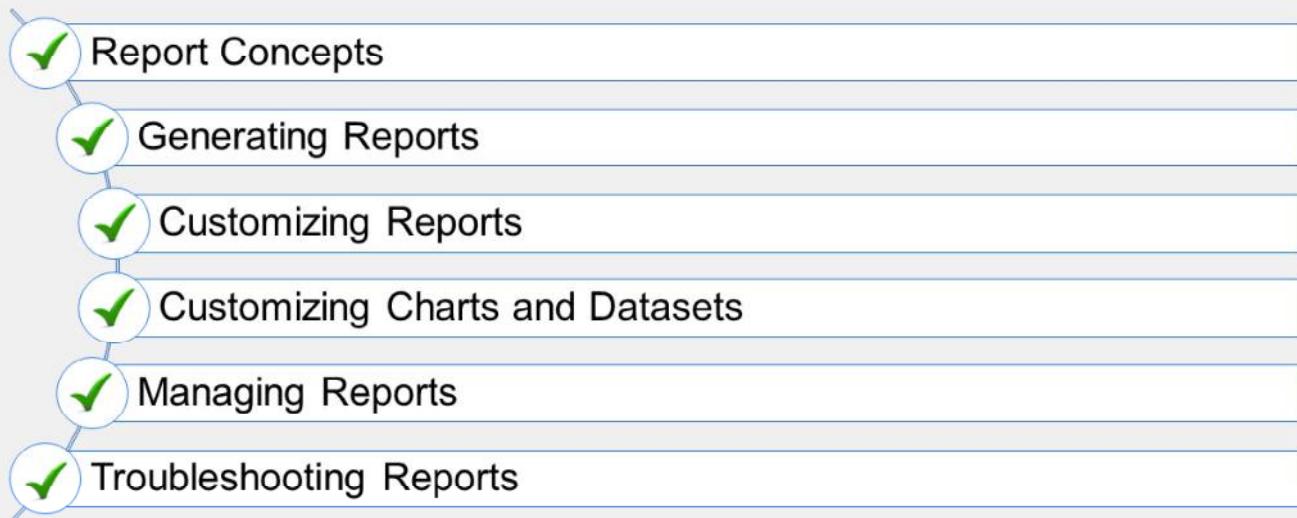
**© FORTINET**

## Knowledge Check

1. Which data does the CLI command # diagnose sql show hcache-size provide?  
 A. Hcache size on the file system  
 B. State of the hcache

**DO NOT REPRINT****© FORTINET**

## Lesson Progress



Congratulations! You have completed this lesson.

Now, you will review the objectives that you covered in this lesson.

**DO NOT REPRINT****© FORTINET**

## Review

- ✓ Describe the elements that constitute a report
- ✓ Describe how FortiAnalyzer extracts data from the database
- ✓ Describe how reports function within ADOMs
- ✓ Run predefined reports
- ✓ Fine-tune reports
- ✓ Run reports on log groups
- ✓ Describe the difference between templates and reports
- ✓ Attach reports to incidents
- ✓ Manage scheduled reports
- ✓ Troubleshoot reports

This slide shows the objectives that you covered in this lesson. By mastering the objectives covered in this lesson, you learned how to understand how data is formatted, stored, and organized in the database, and how to use the FortiAnalyzer reporting feature to view and extract useful information from logs.

DO NOT REPRINT

© FORTINET



## FortiAnalyzer

SQL and Datasets (supplementary material)



Last Modified: 1 December 2021

This supplemental material aims to provide an overview of SQL and datasets. While teaching SQL in its entirety is out of scope for FortiAnalyzer training, the goal is to provide you with enough information so you can modify or create datasets for the purpose of extracting data for reports.

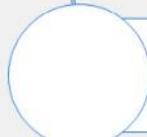
DO NOT REPRINT

© FORTINET

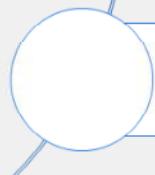
## Lesson Overview



### Datasets and SQL



### SQL Functions and Operators



### FortiAnalyzer Functions and Macros

These are the topics we will explore in this lesson, beginning with datasets and SQL.

DO NOT REPRINT

© FORTINET

## Datasets and SQL

 NSE Training Institute

3

This section covers datasets. Datasets define what data is extracted from the database and represented in a report's chart.

While FortiAnalyzer does provide pre-defined datasets that address the most common queries, you need to understand Structured Query Language, also known as SQL, in order to modify those datasets or create your own.

# DO NOT REPRINT

## © FORTINET

### Datasets

- Datasets are SQL SELECT queries to the database
  - Data populates a chart

ADOM specific!

The screenshot shows the 'Reports > Report Definitions > Datasets' section of the FortiAnalyzer interface. On the left is a sidebar with links like Generated Reports, Report Definitions, All Reports, Templates, Chart Library, Macro Library, Datasets (which is selected and highlighted in blue), Advanced, Output Profile, and Report Calendar. The main area has a toolbar with Create New, View, Delete, Clone, Validate, and Validate All Custom buttons. Below the toolbar is a table with columns for Name, Description, and Device Type. The table contains the following data:

Name	Description	Device Type
App-Risk-Top-Threat-Vectors		FortiGate
App-Risk-Top-User-Source-By-Sessions		FortiGate
App-Risk-Virus-Discovered		FortiGate
App-Risk-Vulnerability-Discovered		FortiGate
App-Risk-Web-Browsing-Activity-Hostname-Category		FortiGate
App-Risk-Web-Browsing-Summary-Category		FortiGate
<b>App-Sessions-By-Category</b>	<pre>select appcat, count(*) as sessions from \$log where \$filter and (logflag&amp;1&gt;0) and nullifna(appcat) is not null group by appcat order by sessions desc</pre>	FortiGate
app-Top-Allowed-Actions-By-Bandwidth		FortiGate

A callout box highlights the 'App-Sessions-By-Category' dataset with the text 'Dataset (example App-Sessions-By Category)'. The bottom of the page includes the NSE Training Institute logo, a copyright notice (© Fortinet Inc. All Rights Reserved.), and a small red number '4'.

A dataset is an SQL SELECT query. The result from that query—the specific data polled from the database—is what populates a chart.

FortiAnalyzer includes many predefined datasets that contain some of the most common database queries. These are available to view from the **Datasets** page.

This is an example of the default **Top-Destinations-By-Sessions** dataset.

**DO NOT REPRINT**  
**© FORTINET**

## Designing SQL Queries

- FortiAnalyzer uses SQL as the local database
- Proper query syntax required

Test that queries are well-formed and all keywords are spelled correctly

SQL queries are not case-sensitive

The screenshot shows the 'View Dataset' screen. In the 'Query' field, there is a SQL statement:

```
select appcat, count(*) as sessions from $log where $filter and
logid_to_int(logid) not in (4, 7, 14) and nullifna(appcat) is not null group by
appcat order by sessions desc;
```

A blue callout box points to this query with the text "SQL queries are not case-sensitive".

At the top right, there is a 'Test' button highlighted with a red box. A blue callout box points to it with the text "Test that queries are well-formed and all keywords are spelled correctly".

Below the 'Test' button, there are settings for 'Time' (Today), 'Period', and 'Devices' (All Devices). To the right, the 'Test Result' table is shown:

appcat	sessions
Network.Service	1803
unknown	904
unscanned	413
Video/Audio	45
SocialMedia	44
General.Interest	23
Storage.Backup	6
Collaboration	6
Proxy	4
Business	3
Update	1

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

5

When you are building your queries, you must use SQL syntax to interface with the database. When creating or editing datasets, there is a **Test** button where you can test your query. If it is not formed correctly, an error message appears. If it formed correctly, and the data you are querying is available in the database, the results appear.

Note that SQL queries are not case-sensitive.

**DO NOT REPRINT****© FORTINET**

## SQL – The Declarative Language

```
SELECT dstip as destination_ip, count(*) as Session  
FROM $log WHERE $filter and dstip is not null GROUP BY  
dstip ORDER BY session desc LIMIT 7
```

- Declarative language: Describes *what* needs to be done rather than *how* to do it
- All information in the database is represented as tables
  - Each table consists of a set of rows and columns
  - Two types of tables: User tables and System tables

Now let's take a closer look at the query itself. In order to understand this example dataset, and more specifically, what it is querying, you need to understand SQL. SQL is what is known as a declarative language—it describes *what* needs to be done rather than how to do it.

In an SQL database all information is represented as tables, each table consists of a set of rows and columns. There are two types of tables:

- User tables, which contain information that is in the database, and
- System tables, which contain the database description.

**DO NOT REPRINT****© FORTINET**

## Basic Data Manipulation Constructs (DML)

- **SELECT**
  - Retrieve and display data from one or more database tables (read-only query)
  - `SELECT ... FROM ... WHERE`
- **INSERT**
  - Add new rows of data into a table
  - `INSERT INTO ... VALUES ...`
- **UPDATE**
  - Modify existing data in a table
  - `UPDATE ... SET ... WHERE`
- **DELETE**
  - Remove rows of data from a table
  - `DELETE FROM ... WHERE`

This is the only query statement used by FortiAnalyzer for reports

In order to retrieve and manipulate data in the database, you need to use data manipulation language, which is a family of syntax elements used by SQL. These syntax elements are SELECT, INSERT, UPDATE, and DELETE. These are the first words used in a query—they are the declarative verbs describing what you want done.

As far as FortiAnalyzer reports are concerned, only the SELECT statement is used. It is purely a read-only query statement that is used to retrieve data from the database.

**DO NOT REPRINT****© FORTINET**

## SELECT Statement

- The SELECT statement retrieves the log data you want from the database
- Must specify criteria using a recognized/supported clause

Clauses must be coded in a specific sequence!

Clause	Definition
FROM	Selects the table or views.
WHERE	Sets the conditions (all rows that do not satisfy the condition are eliminated)
GROUP BY	Collects data across multiple records and groups the results by one or more columns.
ORDER BY	Orders the results by rows.
LIMIT	Limits the number of records returned based on a limit value. OFFSET clause can be used with the LIMIT clause to offset the results by a set value.

The SELECT statement is used to query the database and retrieve log data. In order to pull the data you want, you must specify the criteria. For example, let's say you want to query the database for a list of employees who work in the IT department. In order to put this criteria into a language that SQL understands, you must use a clause recognized by the SELECT statement.

The main clauses FortiAnalyzer reports use are:

- FROM, which specifies the table.
- WHERE, which specifies the conditions. All rows that do not satisfy the condition are eliminated from the output.
- GROUP BY, which collects data across multiple records and groups the results by one or more columns.
- ORDER BY, which orders the results by rows. If ORDER BY is not given, the rows are returned in whatever order the system finds the fastest to produce. And finally,
- LIMIT, which limits the number of records returned based on a specified value. OFFSET is another clause often used along with LIMIT, which offset the results by the number specified. For example, if you place a limit of 3 records and an offset of 1, the first record that would normally be returned is skipped and instead the second, third, and fourth records (3 in total) are returned.

FROM is the only mandatory clause required to form a SELECT statement; the rest of the clauses are optional and serve to filter or limit, aggregate or combine, and control the sort. It is also important to note that the clauses must be coded in a specific sequence. This is to say that following the SELECT keyword, the statement must be followed by one or more clauses in the order they appear in this table provided. For example, you cannot use the WHERE clause before the FROM clause. You do not have to use all optional clauses, but whichever ones you do use they have to be in the correct sequence.

**DO NOT REPRINT****© FORTINET**

## SELECT and FROM

- Use the SELECT query to ask specific questions of the database

```
SELECT column FROM log_type
```

Column from database that contains  
the value(s) you want to retrieve

The log type under which the data is  
contained (ie. Traffic, Web filter, etc.)

- When designing queries for SQL reports on the FortiAnalyzer device, the *Log Type* is assigned to a variable called \$log

```
SELECT dstip as destination_ip FROM $log
```

```
SELECT *
returns all
data
```

SELECT is the first word used in any SQL query that involves FortiAnalyzer reports. This is a declarative statement that instructs the program to query the column in the database for the information you want returned. For example:

```
SELECT dstip
```

Dstip is the column name for destination IP in the SQL schema. Note that you can select more than one column name and you can also have the column name appear under a more user friendly name in the results table by appending the command with "as <friendly\_name\_of\_column>. For example, `SELECT dstip as destination_ip`. In the results table, the values for dstip will now appear under a column named **destination\_ip**.

If you want to return all data, you can use the \* symbol. For example, `SELECT *`. Though most of the time that is more information that you require.

At minimum, you must use the FROM clause with your SELECT statement. This instructs the program where the information is located.

For example:

```
FROM $log
```

Here \$log refers to the logs in the log type selected for the dataset, such as traffic logs or web filter logs to name a few.

**DO NOT REPRINT****© FORTINET**

## Multiple Log Types

- Search multiple log types
  - Combine the data so that you can compare and contrast information

```
SELECT dstip, hostname FROM $log-traffic, $log-webfilter
```

Log type syntax	Log type
\$log-attack	Attack log
\$log-dlp	DLP log
\$log-event	Event log
\$log-netscan	NetScan log
\$log-app-ctrl	Application control log
\$log-emailfilter	Email filter log
\$log-traffic	Traffic log
\$log-virus	Anti-virus log
\$log-webfilter	Web filter log

You can search multiple log types in order to combine the data so that you can compare and contrast information. To do this, use the log type syntax associated with the specific log type. For example, if you want to search both the traffic logs and web filter logs, use:

```
FROM $log-traffic, $log-webfilter
```

# DO NOT REPRINT

## © FORTINET

### WHERE

- The WHERE clause requests data with certain characteristics
  - The expression specifies a stored value in the database

The screenshot shows the FortiAnalyzer GUI interface. On the left, there's a 'Dataset' configuration panel with fields for Name (Example Dataset), Log Type (Traffic), and Query (containing the SQL query). On the right, there's a 'Test query with specified devices and time period' panel with fields for Time (This Week), Period, and Devices (All Devices selected). Below these is a 'Test Result' table with columns for Variable, Expression, and Description, showing several IP addresses.

**SELECT** column **FROM** log\_type **WHERE** expression1 and expression2 not in expression3

Criteria you want to specify

Can use multiple expressions separated by AND/OR/NOT statements

**SELECT** dstip as destination\_ip **FROM** \$log **WHERE** \$filter and dstip is not null

Variable	Expression	Description
destination_ip		216.58.209.238 54.192.48.33 216.58.209.238 172.217.17.110

NSE Training Institute © Fortinet Inc. All Rights Reserved. 11

Out of all the optional clauses, the WHERE statement is really the heart of the query, because this is where you specify the criteria.

The WHERE statement must always come after the FROM statement.

In this example, the first expression is \$filter, which is used to restrict the results to the time period you select. While the time period is not added to the query itself, it is specified by way of a drop-down box when creating the dataset through the FortiAnalyzer GUI.

The second expression is dstip, which is the destination IP, while the third expression is NULL.

SQL supports logic operators as well, so you can use AND/OR/NOT statements in order to build out the query. Operators will be discussed later in this lesson.

# DO NOT REPRINT

## © FORTINET

### GROUP BY

- GROUP BY statement is usually used in conjunction with aggregate functions to group data by one or more columns.
- Returns one output row for each group
  - Can form groups within groups
- Each item in the SELECT list produces a single value per set

```
SELECT column, aggregate_function FROM log_type WHERE
expression1 and expression2 not in expression3 GROUP BY column
```

If GROUP BY is used without aggregates, it is similar to the DISTINCT clause.

```
SELECT dstip as destination_ip, count(*) as session FROM $log
WHERE $filter and dstip is not null GROUP BY dstip
```

The GROUP BY clause is used to create one output row for each group. It is usually used with an aggregate function within the SELECT statement. We will cover aggregate functions later, but essentially they perform a calculation on a set of values and return a single value. If it is not used with an aggregate function, it is similar to the DISTINCT clause, in that it removes duplicates from the result set of a SELECT statement.

In this example, the GROUP BY clause is used with an aggregate function. The aggregate function is count(\*), which selects all rows in a table, even if some columns contain a NULL value.

In this example, we are grouping by dstip (destination IP).

# DO NOT REPRINT

## © FORTINET

### ORDER BY

- By default, rows of an SQL query result table are not arranged in a particular order

```
SELECT column, aggregate_function FROM log_type WHERE expression1  
and expression2 not in expression3 GROUP BY column ORDER BY  
column_name|column_number asc|desc
```

Can sort data by  
column name or  
column number

Can sort data in ascending (asc)  
or descending (desc) order. By  
default, sorts in ascending order.

```
SELECT dstip as destination_ip, count(*) as session FROM $log WHERE  
$filter and dstip is not null GROUP BY dstip ORDER BY session desc
```

ORDER BY is a clause that allows you to sort queries by column name or column number. By default, rows of an SQL query result table are not arranged in a particular order, so you can use the ORDER BY clause to sort column values in either ascending (asc) or descending (desc) order. If you use this clause and do not specify ascending or descending, the default is ascending.

You can order multiple columns and specify different sort orders for each. For example, you can sort one column in ascending order and another column in descending order.

In this example, we are ordering by session in descending order.

**DO NOT REPRINT****© FORTINET**

## LIMIT and OFFSET

- The **LIMIT** clause limits the number of records retrieved from the query result
  - Useful in large deployments to help limit the CPU/memory usage for reports
  - Can be combined with **ORDER BY asc** to get the “top <x> results”

```
SELECT column, aggregate_function FROM log_type WHERE expression1  
and expression2 not in expression3 GROUP BY column ORDER BY  
column_name|column_number asc|desc LIMIT number OFFSET number
```

Specify how many records to return

Specify how many records to skip

```
SELECT dstip as destination_ip, count(*) as session FROM $log WHERE  
$filter and dstip is not null GROUP BY dstip ORDER BY session desc  
LIMIT 7 OFFSET 1
```

By default, all results that satisfy the conditions specified in the query are returned. However, if you only want to retrieve a subset of records, you can place a limit on the records returned. To do this, use the **LIMIT** clause and specify the number of results you want. For example, **LIMIT 7**. This is a great way of making sure that the query doesn't use unnecessary CPU or memory, especially if you have a large scale deployment with lots of devices logging to the FortiAnalyzer. You can also combine **LIMIT** with **ORDER BY asc** to get the “top <x> results” (or **desc** for the “bottom <x> results”).

In conjunction with the **LIMIT** clause you can use the **OFFSET** clause. This offsets the results by a set value. For example, if you place a limit of 7 records and an offset of 1, the first record that would normally be returned is skipped and instead 2 through 8 are returned.

# DO NOT REPRINT

## © FORTINET

## Creating a Dataset in FortiAnalyzer

### Reports > Report Definitions > Datasets

The screenshot shows the 'Create Dataset' dialog box. On the left, there's a 'Dataset' section with fields for 'Name' (set to 'Example Dataset') and 'Log Type' (set to 'Traffic'). Below that is a 'Query' section containing a SQL-like query:

```
SELECT dstip as destination_ip, count(*) as session FROM $log WHERE
$filter and dstip is not null GROUP BY dstip ORDER BY session desc LIMIT
7 OFFSET 1
```

To the right of the query, there's a 'Test' button, a 'Time Period' dropdown set to 'Today', and a 'Devices' section with 'All Devices' selected. A red box highlights the 'Test' button, the 'Time Period' dropdown, and the 'All Devices' radio button. Below these settings is a 'Test Result' table:

destination_ip	session
10.200.1.10	200
208.91.112.55	185
149.56.65.124	8
72.21.91.29	7
52.88.144.151	6
195.154.38.102	4
198.105.244.11	4

A red box highlights the entire 'Test Result' table.

At the bottom left is the 'NSE Training Institute' logo, and at the bottom center is the copyright notice '© Fortinet Inc. All Rights Reserved.' The page number '15' is at the bottom right.

As we've been introducing and explaining the main SQL clauses, we've been forming a full dataset query along the way. To visually see how it all ties together, we can use the dataset **Test** feature in the GUI. The feature is intended to test or modify a query in order to get the specific output you want.

Ensure you select the log type for the query. The query uses the generic `$log`, but it references the log type specified in the **Log Type** drop-down field (in this example, Traffic). You can enter the specific log type in the query instead (for example, `$log-traffic`), but should you want to view this query on a different log type later, it's less risky and easier to change from the **Log Type** drop-down field than in the actual dataset query itself.

On the right side of the dialog box, you must also specify the device or devices on which to use this query. Here, we have specified **All Devices**.

You must also specify a time period for this query. As mentioned earlier, the `$filter` expression used with our WHERE clause states that we want to limit the results to the time period we specify. The **Time Period** drop-down box is where we specify this time period.

If there is an error in the query, the error message appears in the window below. If the query is correct, the results appear in the window below. Since the results appear in the window below, we know our dataset has been correctly formed.

**DO NOT REPRINT**  
**© FORTINET**

## Analyzing the Dataset Test Results

Reports > Report Definitions > Datasets

The screenshot shows the 'Create Dataset' page. In the 'Dataset' section, the 'Name' is 'Example Dataset' and 'Log Type' is 'Traffic'. The 'Query' field contains the following SQL:

```
SELECT dstip as destination_ip, count(*) as session
FROM $log
WHERE $filter and dstip is not null
GROUP BY dstip
ORDER BY session desc
LIMIT 7
OFFSET 1
```

A red arrow points from the 'destination\_ip' column of the 'Test Result' table to the 'dstip' in the 'SELECT' clause. Another red arrow points from the 'session' column to the 'count(\*)' in the 'SELECT' clause.

destination_ip	session
10.200.1.10	200
208.91.112.55	185
149.56.65.124	8
72.21.91.29	7
52.88.144.151	6
195.154.38.102	4
198.105.244.11	4

**NSE Training Institute** © Fortinet Inc. All Rights Reserved. 16

Now let's align the written query with the visual results to fully understand how the query is interpreted by FortiAnalyzer.

`SELECT dstip as destination_ip, count(*) as session;` This says, select the destination IP address and call the column "destination\_ip". Select the count (all data) and call the column "session".

`FROM $log;` This says, query the traffic log for the data, which is specified in the **Log Type** drop-down list.

`WHERE $filter and dstip is not null;` This says, limit the results to the time period specified, which is **Today** according to the selection in the **Time Period** drop-down list, and only provide destination IP addresses that are not null. Note that "null" represents unknown data—it does not represent zero.

`GROUP BY dstip;` This says, group the results by destination IP. Remember, we specified we wanted dstip put in a column called "destination\_ip".

`ORDER BY session desc;` This says, order the results by session in descending order. Note that the results go from high (200) to low (4).

`LIMIT 7;` This says, only provide the first seven results.

`OFFSET 1;` This says, skip the first result, but still limit the results to the next 7 (i.e. 2 through 8).

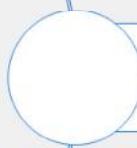
DO NOT REPRINT

© FORTINET

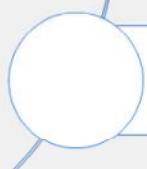
## Lesson Progress



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

 NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

Good job! You now understand datasets and SQL.

Now, let's examine SQL functions and operators.

DO NOT REPRINT

© FORTINET

## SQL Functions and Operators

 NSE Training Institute

18

This section covers a few of the most common functions and operators used in FortiAnalyzer datasets—it is not intended as a complete and exhaustive list.

**DO NOT REPRINT****© FORTINET**

## “Normal” Functions vs. Aggregate Functions

Aggregate functions	“Normal” functions
Use the entire column of data as their input and produce a single output	Operate on each element in the column of data

SQL has two types of functions: “normal” functions and aggregate functions.

Aggregate functions use the entire column of data as their input and produce a single output, while the “normal” functions operate on each element in the column of data.

**DO NOT REPRINT****© FORTINET**

## NULLIF

- NULLIF function takes two arguments: if the first two arguments are equal, then NULL is returned. Otherwise, the first argument is returned.

```
SELECT NULLIF(expression1, expression2)
```

Must be values that are of the same datatype

- NULL represents unknown data—it is not equal to zero

One common function used in FortiAnalyzer datasets is NULLIF. The NULLIF function takes two arguments. If the first two arguments are equal, then NULL is returned. Otherwise, the first argument is returned. Note that NULL represents unknown data—it does not represent zero.

**DO NOT REPRINT****© FORTINET**

## COALESCE

- Returns the first of its arguments that is not NULL. NULL is returned only if all arguments are NULL

```
SELECT coalesce(catdesc, 'unknown') as category,
coalesce(root_domain(hostname), 'unknown') as domain FROM $log
GROUP BY category, domain
```

category	domain
Malicious Websites	xnwipt.com
unknown	corolbugan.com
Unrated	agoinside.gq
Malicious Websites	40thousandwords.com
Malicious Websites	apple-ituncs-ios.com
Unrated	repeat-chief.ru
Malicious Websites	kir22.ru
Malicious Websites	blissyogawithannu.com
Unrated	ichiventures.com

**NSE Training Institute**

© Fortinet Inc. All Rights Reserved.

21

Another common function used in FortiAnalyzer datasets is COALESCE. The COALESCE function returns the first non-NULL expression among its arguments. Null is returned only if all arguments are null. It is often used to substitute a default value for null values when data is retrieved for display.

COALESCE is used with the SELECT statement. It takes one or more expressions as an argument. The values do not have to be string data types—they can be any data type (and also different data types). The syntax is:

COALESCE (expression 1, expression 2, ...)

**DO NOT REPRINT****© FORTINET**

## Aggregate Functions

- Aggregate functions perform a calculation on a set of values in a column and return a single value

### Aggregate functions

AVG(expression)	Returns the average value
COUNT(expression)	Returns the number of rows
COUNT(*)	Returns all rows, even if some columns contain a NULL value
FIRST(expression)	Returns the first value
LAST(expression)	Returns the last value
MAX(expression)	Returns the largest value
MIN(expression)	Returns the smallest value
SUM(expression)	Returns the sum

Aggregate functions are a special category with different rules, as they operate on entire columns of data instead of discrete values. These functions perform a calculation on a set of values in a column and returns a single value. Although aggregate functions are usually used in conjunction with the GROUP BY clause, these functions can be used on their own in a SELECT statement.

This table includes a list of aggregate functions used in SQL. All can take an expression as an argument and ignore null values, except for count. Count can take an asterisk as an argument. The asterisk in this case means all rows are returned, even if some columns contain a NULL value.

An example of an expression used with an aggregate function is `SELECT count(unauthuser)`. This would return the number of unauthorized users.

**DO NOT REPRINT**

**© FORTINET**

## Operators

- Reserved word or character used primarily in the WHERE clause to perform various operations
  - Arithmetic operators
  - Comparison operators
  - Logical operators

Now let's take a look at SQL operators. An operator is a reserved word or a character used primarily in an SQL statement's WHERE clause to perform various operations.

There are three types of operators:

- Arithmetic operators
- Comparison operators
- Logical operators

**DO NOT REPRINT****© FORTINET**

## Arithmetic Operators

- Perform mathematical operations on two expressions of one or more of the data types of the numeric data type category

Operator	Description
+	Addition – adds values on either side of the operator
-	Subtraction – Subtracts right hand operand from left hand operand
*	Multiplication – Multiplies values on either side of the operator
/	Division – Divides left hand operand by right hand operand
%	Modulus – Divides left hand operand by right hand operand and returns remainder

Here are some examples of arithmetic operators. Arithmetic operators perform mathematical operations on two expressions of one or more of the data types of the numeric data type category.

**DO NOT REPRINT****© FORTINET**

## Comparison Operators

- Test whether two expressions are the same
  - Can be used on all expressions except text, ntext, or image data types

Operator	Description
=	Equal to
>	Greater than
<	Less than
>=	Greater than or equal to
<=	Less than or equal to
<>	Not equal to
!=	Not equal to (not ISO standard)
!<	Not less than (not ISO standard)
!>	Not greater than (not ISO standard)

Here are some examples of comparison operators. Comparison operators test whether two expressions are the same and can be used on all expressions except expressions of the **text**, **ntext**, or **image** data types.

**DO NOT REPRINT****© FORTINET**

## Logical Operators

- Test for the truth of some condition
  - Return a boolean data type with a value of TRUE, FALSE, or UNKNOWN

Operator	Description
ALL	TRUE if all of a set of comparisons are TRUE.
AND	TRUE if both Boolean expressions are TRUE.
ANY	TRUE if any one of a set of comparisons are TRUE.
BETWEEN	TRUE if the operand is within a range.
EXISTS	TRUE if a subquery contains any rows.
IN	TRUE if the operand is equal to one of a list of expressions.
LIKE	TRUE if the operand matches a pattern.
NOT	Reverses the value of any other Boolean operator.
OR	TRUE if either Boolean expression is TRUE.
SOME	TRUE if some of a set of comparisons are TRUE.

Here are some examples of logical operators. Logical operators test for the truth of some condition. Like comparison operators, they return a Boolean data type with a value of TRUE, FALSE, or UNKNOWN.

DO NOT REPRINT

© FORTINET

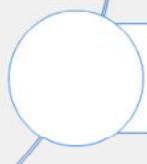
## Lesson Progress



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

 NSE Training Institute

© Fortinet Inc. All Rights Reserved.

27

Good job! You now understand SQL functions and operators.

Now, let's examine FortiAnalyzer functions and macros.

DO NOT REPRINT

© FORTINET

## FortiAnalyzer Functions and Macros

 NSE Training Institute

28

This section covers FortiAnalyzer functions and macros.

FortiAnalyzer includes some built-in functions that are based on known SQL functions, but scripted differently.

FortiAnalyzer also includes macros, which are best described as lengthy or complex SQL statements scripted more simplistically. An SQL macro can be used anywhere in a query where an ordinary SQL expression can be used.

**DO NOT REPRINT****© FORTINET**

## root\_domain

- **root\_domain(hostname)**

- Retrieves the root domain of the fully qualified domain name (FQDN)

```
SELECT devid, root domain(hostname) as website FROM
$log WHERE 'user'='USER01' GROUP BY devid, hostname
ORDER BY hostname LIMIT 7
```

devid	website
FGVM010000064692	01gtf.org
FGVM010000064692	024student.com
FGVM010000064692	0306737775.win
FGVM010000064692	0452luntan.com
FGVM010000064692	10yi6bh1fvlx3mt260kix2924l.net
FGVM010000064692	118.171.94.192
FGVM010000064692	132r4zp18tqz1ktk0yg6kj4y2p.org

One FortiAnalyzer-specific function is `root_domain(hostname)`. This provides the root domain of the fully qualified domain name. As per the query, in this example `root_domain(hostname)` is listed under the **website** column in ascending order (the default for the `ORDER BY` clause if not specified).

# DO NOT REPRINT

## © FORTINET

### nullifa

- **nullifna(expression)**
  - Inverse operation of COALESCE
  - Can be used to filter out values with N/A and n/a from logs
- SQL syntax → SELECT NULLIF(NULLIF(<value>, 'N/A'), 'n/a')

```
SELECT coalesce(nullifna('user'), 'srcip') as user src,
coalesce(nullifna(root_domain(hostname)), 'unknown') as domain FROM
$log WHERE dstport='80' GROUP BY user src, domain ORDER BY
user_src LIMIT 7
```

user_src	domain
user	fgtk77.club
user	itourongbao.com
user	yuamyyimgxh.com.ve
user	144.76.106.114
user	envelopeson.com
user	tritonship.com
user	10yi6bh1fvlx3mt260kix2924l.net

If user is n/a, the source IP is displayed, otherwise it returns the user name

Another FortiAnalyzer-specific function is nullifna, which takes an expression as an argument. The actual SQL syntax this is based on is SELECT NULLIF(NULLIF(expression, 'N/A'), 'n/a').

In this example, if the user is n/a the source IP is displayed, otherwise it returns the user name. It performs the inverse operation of the COALESCE function. As you can see in the **user\_src** column, there are some IP address and some user names.

**DO NOT REPRINT****© FORTINET**

## FortiAnalyzer Functions: email\_domain, email\_user

- **email\_domain:** Retrieves anything after the @ symbol in an email address
- **email\_user:** Retrieves anything before the @ symbol in an email address

```
SELECT 'from' as source, email user('from') as e_user,  

email domain('from') as e_domain FROM $log LIMIT 5 OFFSET 10
```

Source	e_user	e_domain
user11@example.com	user11	example.com
user12@hostname.com	user12	hostname.com
user13@exampleXYZ.com	user13	exampleXYZ.com
user14@hostnameXYZ.com	user14	hostnameXYZ.com
user15@example.com	user15	example.com

email\_domain and email\_user are other FortiAnalyzer-specific functions. email\_domain retrieves anything that is after the @ symbol in an email address—the domain. email\_user retrieves anything that is before the @ symbol in an email address.

As per the query, in this example email\_user displays in the column **e\_user**, while email\_domain displays in the column **e\_domain**.

**DO NOT REPRINT****© FORTINET**

## FortiAnalyzer Functions: from\_dtime, from\_itime

- `from_dtime(bigint)`: Returns device timestamp without time zone
- `from_itime(bigint)`: Returns FortiAnalyzer's timestamp without time zone

```
SELECT itime, from_itime(itime) as faz_local_time, dtime,
       from_dtime(dtime) as dev_local_time FROM $log LIMIT 3
```

itime	faz_local_time	dtime	dev_local_time
1486474586	2017-02-07 05:36:26	1486445784	2017-02-07 05:36:2
1486474581	2017-02-07 05:36:21	1486445776	2017-02-07 05:36:1
1486474586	2017-02-07 05:36:26	1486445784	2017-02-07 05:36:2

`from_dtime` and `from_itime` are other FortiAnalyzer-specific functions. `from_dtime` returns the device timestamp without the time zone, while `from_itime` returns FortiAnalyzer's timestamp without the time zone.

As per this query, `from_itime` appears in the column **faz\_local\_time**, while `from_dtime` appears in the column **dev\_local\_time**.

# DO NOT REPRINT

## © FORTINET

### Macros

- FortiAnalyzer Date/Time macros

Macros	PostgreSQL syntax	Result
\$hour_of_day	to_char(from_itime("itime"), 'HH24:00')	18:00
\$HOUR_OF_DAY	to_char(from_itime("itime"), 'YYYY-MM-DD HH24:00')	2021-01-01 18:00
\$day_of_week	to_char(from_itime("itime"), "'WDAY' D-Dy")	WDAY 2-Mon
\$DAY_OF_WEEK	XXX	XXX
\$day_of_month	to_char(from_itime("itime"), 'DD')	01
\$DAY_OF_MONTH	to_char(from_itime("itime"), 'YYYY-MM-DD')	2021-01-01
\$month_of_year	to_char(from_itime("itime"), 'YYYY-MM')	2021-01
\$MONTH_OF_YEAR	XXX	XXX

Here are some common date and time macros used in FortiAnalyzer. Macros are simple substitutions for more complex SQL statements—usually created for SQL statements that are frequently used.

DO NOT REPRINT

© FORTINET

## Lesson Progress



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

Congratulations! You have completed this lesson.

**DO NOT REPRINT**  
**© FORTINET**



**FORTINET®**



**No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.**

Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

<https://t.me/learningnets>