

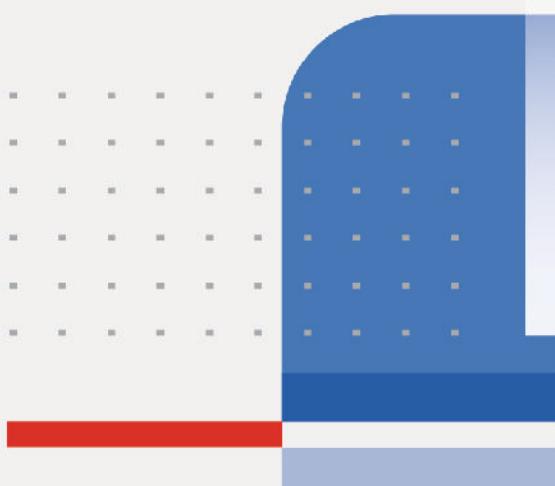
DO NOT REPRINT
© FORTINET



FortiAnalyzer Administrator Study Guide

FortiAnalyzer 7.4

FORTINET®
Training Institute



DO NOT REPRINT

© FORTINET

Fortinet Training Institute - Library

<https://training.fortinet.com>

Fortinet Product Documentation

<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 Product Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguard.com>

Fortinet Training Program Information

<https://www.fortinet.com/nse-training>

Fortinet | Pearson VUE

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

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

<https://helpdesk.training.fortinet.com/support/home>



TABLE OF CONTENTS

00 SQL and Datasets.....	4
01 Introduction and Initial Configuration.....	38
02 Administration and Management.....	69
03 RAID and HA.....	120
04 Managing Devices.....	145
05 Logs and Reports Management.....	180

DO NOT REPRINT

© FORTINET



FortiAnalyzer Administrator

SQL and Datasets

 FortiAnalyzer 7.4.1

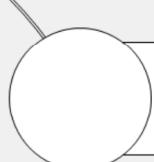
Last Modified: 19 December 2023

This supplemental material provides an overview of SQL and datasets. Teaching a comprehensive lesson on SQL is out of scope for FortiAnalyzer training, so the goal of this material is to provide you with the information you need to modify or create datasets for the purpose of extracting data for reports.

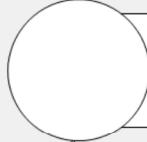
DO NOT REPRINT

© FORTINET

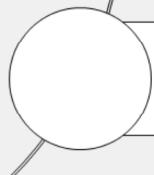
Lesson Overview



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

The supplemental material is covered in the topics shown on this slide.

DO NOT REPRINT

© FORTINET

Datasets and SQL

Objectives

- Describe datasets
- Understand SQL basics



© Fortinet Inc. All Rights Reserved.

3

This section covers datasets. Datasets define what data is extracted from the database and represented in the chart on a report.

FortiAnalyzer provides predefined datasets that address the most common queries. However, if you need to modify those datasets or create your own, you need to understand SQL.

DO NOT REPRINT

© FORTINET

Datasets

- Datasets are SQL SELECT queries to the database
 - Data populates a chart

ADOM specific

The screenshot shows the FortiAnalyzer interface with the following details:

- Left Sidebar:** Includes links for Dashboard, Device Manager, FortiView, Log View, Fabric View, Incidents & Events, Reports (selected), Generated Reports, Report Definitions (selected), Advanced Settings, and System Settings.
- Top Navigation Bar:** Contains All Reports, Templates, Chart Library, Macro Library, and Datasets (selected).
- Toolbar:** Includes Create New, View, Delete, More, Show Predefined (checked), Show Custom (checked), and a Search bar.
- Dataset List:** Shows a list of predefined datasets with columns for Name, Device Type, and Log Type. The 'App-Sessions-By-Category' dataset is selected (highlighted in blue) and has a checkmark next to it.
- Callout:** A blue callout points to the 'App-Sessions-By-Category' dataset, labeled "Dataset (example App-Sessions-By Category)".
- Code Block:** A code box shows the SQL query for the selected dataset:


```
select appcat, count(*) as sessions from
$log where $filter and (logflag&1>0) and
nullifna(appcat) is not null group by
appcat order by sessions desc
```
- Page Footer:** Includes the Fortinet Training Institute logo and copyright information: © Fortinet Inc. All Rights Reserved. 4

A dataset is an SQL SELECT query. The result of 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. You can view the predefined datasets from the **Datasets** page.

This slide shows an example of the default **App-Sessions-By-Category** dataset.

DO NOT REPRINT

© FORTINET

Designing SQL Queries

- FortiAnalyzer uses SQL as the local database
- Proper query syntax required

The screenshot shows the FortiAnalyzer interface for designing SQL queries. On the left, there's a sidebar with 'Name' (App-Sessions-By-Category), 'Log Type' (Traffic), and 'Query'. The main area contains a code editor with the following SQL query:

```

1 SELECT
2     appcat,
3     count(*) AS sessions
4 FROM
5     $log
6 WHERE
7     $filter
8     AND (logflag & 1 > 0)
9     AND nullifna(appcat) IS NOT NULL
10 GROUP BY
11     appcat
12 ORDER BY
13     sessions DESC

```

Below the code editor are 'Recommendations', 'Validate', 'Analyze Query', and 'Format' buttons. A 'Variables' section allows defining variables like 'group' and 'User or Source'. To the right, a results table displays session counts for various application categories. A blue speech bubble points to the 'Go' button in the top right of the results table, which is highlighted with a red box. Another blue speech bubble says 'SQL queries are not case sensitive'.

appcat	sessions
unscanned	189
Web.Client	166
Storage.Backup	56
Social.Media	32
Video/Audio	21
Collaboration	15
im	8

© 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, you can click **Validate** to check if the SQL query is valid, or see what errors are returned. You can also click **Go** to test your query. If the query is formed correctly, and the data you are querying is available in the database, the results appear. If the query is not formed correctly, you will see an error message.

You can also click **Format** to format the entered SQL query, making it easier to read, update, and detect errors. The screenshot on this slide shows a formatted SQL query.

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



© Fortinet Inc. All Rights Reserved.

6

Now 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 a SQL database all information is represented as tables, and 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
- System tables, which contain the database description

DO NOT REPRINT**© FORTINET**

Basic Data Manipulation Constructs

- **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



© Fortinet Inc. All Rights Reserved.

7

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 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. 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 the ones you do use must 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
(for example, traffic, web filter, and so on)

- 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 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.

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	Antivirus 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

```
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
```

Name	Example Dataset
Log Type	Traffic
Query	1 SELECT dstip as Destination_IP FROM \$log WHERE \$filter and dstip is not null

Go Stop
Time Period
Today
Devices:
All Devices ▾
destination_ip
1.1.1.32
94.229.20.61
54.83.43.69
175.126.123.219
224.141.85.77

© 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 are also covered in this material.

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 want to retrieve only a subset of records, you can place a limit on the number of records returned. To do this, use the **LIMIT** clause and specify the number of results you want. For example, **LIMIT 7**. Applying limits can ensure that the query doesn't use unnecessary CPU or memory, especially if you have a large-scale deployment with lots of devices logging to 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 seven records and an offset of one, the first record that would normally be returned is skipped and two through eight are returned instead.

DO NOT REPRINT

© FORTINET

Creating a Dataset in FortiAnalyzer

The screenshot shows the 'Reports > Report Definitions > Datasets' section. A dataset named 'Example Dataset' is being created with 'Traffic' as the Log Type. The Query is:

```
1 SELECT dstip as "Destination_IP", count(*) as "Session" FROM $log
WHERE $filter and dstip is not null GROUP BY "Destination_IP" ORDER BY
"Session" desc LIMIT 7 OFFSET 1
```

The results table shows the following data:

Destination IP	Session
1.1.1.32	177
175.126.123.219	79
54.83.43.69	60
e08d:554d::	59
216.218.135.114	44
31.13.80.36	40
96.45.46.46	37

At the bottom left, the Fortinet Training Institute logo is visible. At the bottom right, there is a copyright notice: © Fortinet Inc. All Rights Reserved. 15.

As you have been learning about the main SQL clauses, you have also been forming a full dataset query along the way. To see a visual of the query, you can use the dataset **Go** 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 `$log`, but it references the log type specified in the **Log Type** field (in this example, **Traffic**). You can enter the specific log type in the query instead (for example, `$log-traffic`). If you want to view this query on a different log type later, it's less risky and easier to change your selection in the **Log Type** field than in the actual dataset query itself.

You must also specify the device or devices on which to use this query. In this example, **All Devices** is specified.

You must also specify a time period for this query. You can use the `$filter` expression with the WHERE clause to limit the results to the time period that you specify in the **Time Period** field.

DO NOT REPRINT
© FORTINET

Analyzing a Dataset in FortiAnalyzer

The screenshot shows the FortiAnalyzer interface for managing datasets. On the left, under 'Reports > Report Definitions > Datasets', a configuration window is open for an 'Example Dataset'. It includes fields for Name ('Example Dataset'), Log Type ('Traffic'), and a SQL query:

```
1 SELECT dstip as "Destination IP", count(*) as "Session" FROM $log
WHERE $filter and dstip is not null GROUP BY "Destination IP" ORDER BY
"Session" desc LIMIT 7 OFFSET 1
```

Below the query are buttons for 'Recommendations', 'Validate', 'Analyze Query', and 'Format'. A 'Validate Result' section indicates 'No Validation Issues Found'. On the right, the results are displayed in a table titled 'Destination IP' with columns 'Destination IP' and 'Session'. The results are:

Destination IP	Session
1.1.1.32	177
175.126.123.219	79
54.83.43.69	60
e08d:554d::	59
216.218.135.114	44
31.13.80.36	40
96.45.46.46	37

At the bottom left is the Fortinet Training Institute logo, and at the bottom right is the copyright notice '© Fortinet Inc. All Rights Reserved. 16'.

Now 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** field.

`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** field, and provide only the 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. You previously specified that the destination IP should be 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 (177) to low (37).

`LIMIT 7:` This says, provide only the first seven results.

`OFFSET 1:` This says, skip the first result, but still limit the results to the next seven (that is, two through eight).

DO NOT REPRINT

© FORTINET

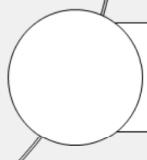
Lesson Progress



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

Good job! You now understand datasets and SQL.

Now, you will learn about SQL functions and operators.

DO NOT REPRINT

© FORTINET

SQL Functions and Operators

Objectives

- Understand SQL functions
- Understand operators



© Fortinet Inc. All Rights Reserved.

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

Aggregate Functions vs “Normal” 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



© Fortinet Inc. All Rights Reserved. 19

SQL has two types of functions: aggregate functions and “normal” functions.

Aggregate functions use the entire column of data as their input and produce a single output. “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

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 returns 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



© Fortinet Inc. All Rights Reserved. 23

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 a condition. Like comparison operators, they return a Boolean data type with a value of TRUE, FALSE, or UNKNOWN.

DO NOT REPRINT

© FORTINET

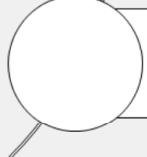
Lesson Progress



Datasets and SQL



SQL Functions and Operators



FortiAnalyzer Functions and Macros

Good job! You now understand SQL functions and operators.

Now, you will learn about FortiAnalyzer functions and macros.

DO NOT REPRINT**© FORTINET**

FortiAnalyzer Functions and Macros

Objectives

- Understand FortiAnalyzer functions
- Understand macros



© Fortinet Inc. All Rights Reserved. 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 specified by the query, in this example `root_domain(hostname)` is listed under the **website** column in ascending order. Unless otherwise specified, ascending order is the default for the **ORDER BY** clause.

DO NOT REPRINT

© FORTINET

nullifna

- 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.

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 comes after the @ symbol in an email address—the domain. `email_user` retrieves anything that comes before the @ symbol in an email address.

As specified by 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 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
1699305243	2023-11-06 13:14:03	1699276391	2023-11-06 13:13:11
1699305243	2023-11-06 13:14:03	1699276391	2023-11-06 13:13:11
1699305243	2023-11-06 13:14:03	1699276399	2023-11-06 13:13:19

`from_dtime` and `from_itime` are other FortiAnalyzer-specific functions. `from_dtime` returns the device timestamp without the time zone, while `from_itime` returns the FortiAnalyzer's timestamp without the time zone.

As specified by 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 and 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 come to the end of this material.

DO NOT REPRINT**© FORTINET**

FortiAnalyzer Administrator

Introduction and Initial Configuration

A small red square icon containing a white square with a diagonal line.

FortiAnalyzer 7.4.1

Last Modified: 19 December 2023

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



© Fortinet Inc. All Rights Reserved.

2

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

DO NOT REPRINT**© FORTINET**

Key Features and Concepts

Objectives

- Describe the purpose of FortiAnalyzer
- Describe FortiAnalyzer operating modes
- Understand logging in a Security Fabric environment
- Describe FortiAnalyzer Fabric
- Describe administrative domains
- Identify the tools used to configure FortiAnalyzer

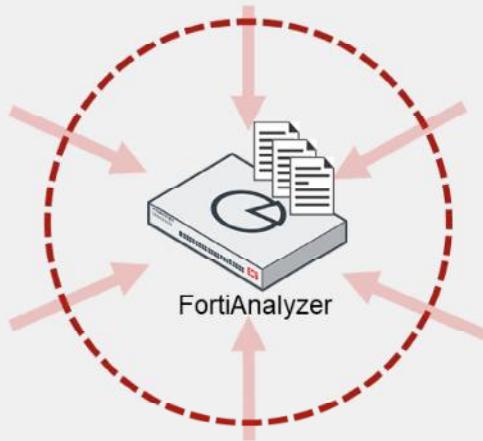
After completing this section, you should be able to achieve the objectives shown on this slide.

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

- FortiAnalyzer aggregates log data from one or more Fortinet devices
- Single view of security events taking place on a range of devices



Supported devices:

- FortiGate/FortiCarrier
- FortiAnalyzer
- FortiCache
- FortiClient
- FortiDDoS
- FortiMail
- FortiManager
- FortiNAC
- FortiSandbox
- FortiSOAR
- FortiWeb
- Syslog
- Chassis

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.

FortiAnalyzer can be integrated with many different Fortinet solutions. For a complete list, refer to the release notes at docs.fortinet.com.

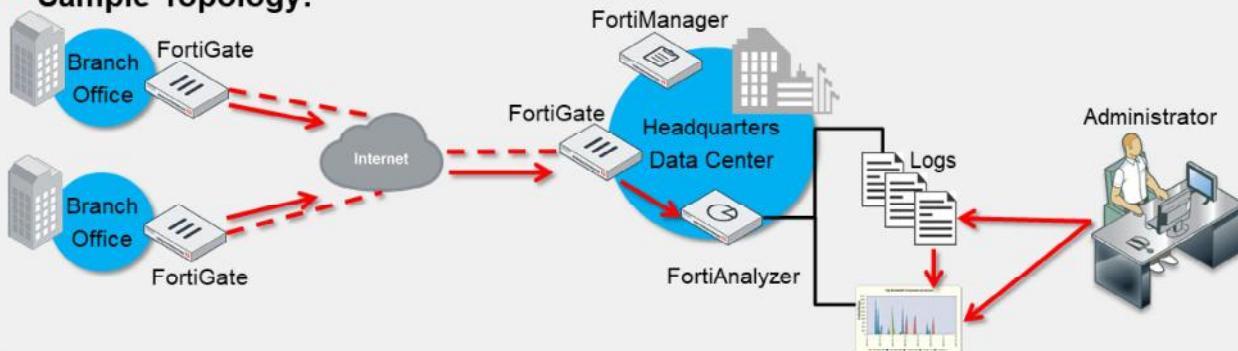
DO NOT REPRINT
© FORTINET

Centralized Log Repository (Contd)

Workflow:

1. Registered devices send logs to FortiAnalyzer
2. FortiAnalyzer buffers, reorganizes, and stores the logs
3. Administrators:
 - View and search the logs
 - Configure, request, and view reports (based on log data)

- **Sample Topology:**



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 is 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.

FortiAnalyzer can be easily integrated into a network, even if there are multiple sites. A sample topology can include multiple branches and a headquarters. Each location's firewall is added into FortiAnalyzer, and the administrator can view logs and generate reports for the entire network, under one interface.

DO NOT REPRINT**© FORTINET**

Reports, Events, and Content Archiving

- **Reports**

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

- **Events**

- Identify and react to security threats quickly when configured conditions are met
- View events through **Event Monitor** (in the GUI), email, SNMP, or syslog
- Events that require further investigation can be used to generate new incidents

- **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



© Fortinet Inc. All Rights Reserved.

6

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

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, File Transfer Protocol (FTP), Network New Transfer Protocol (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**

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.

For more information on SQL and FortiAnalyzer, refer to the supplementary lesson *SQL Datasets*.

DO NOT REPRINT
© FORTINET

FortiAnalyzer Operating Modes—Analyzer

Dashboard > System Information

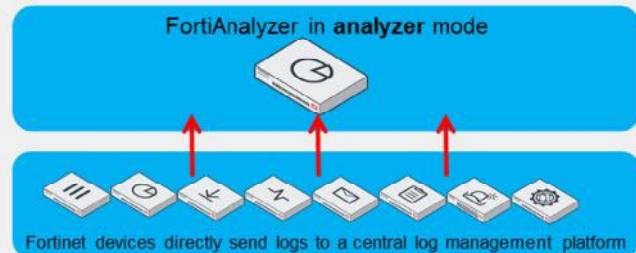
Operation Mode

Analyzer

Collector

Analyzer is the default mode

- 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)



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

8

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

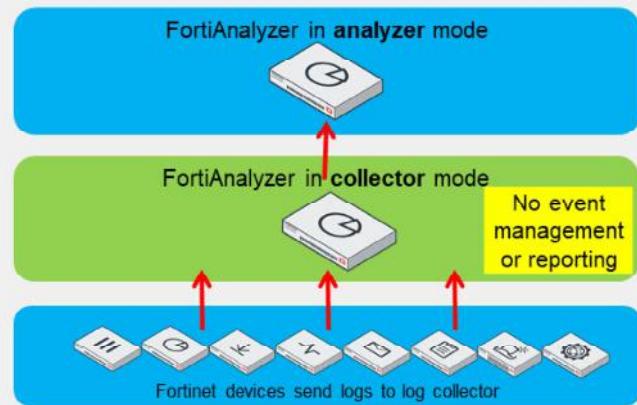
You can change the operating mode in the **System Information** widget on the dashboard.

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.

DO NOT REPRINT
© FORTINET

FortiAnalyzer Operating Modes—Collector

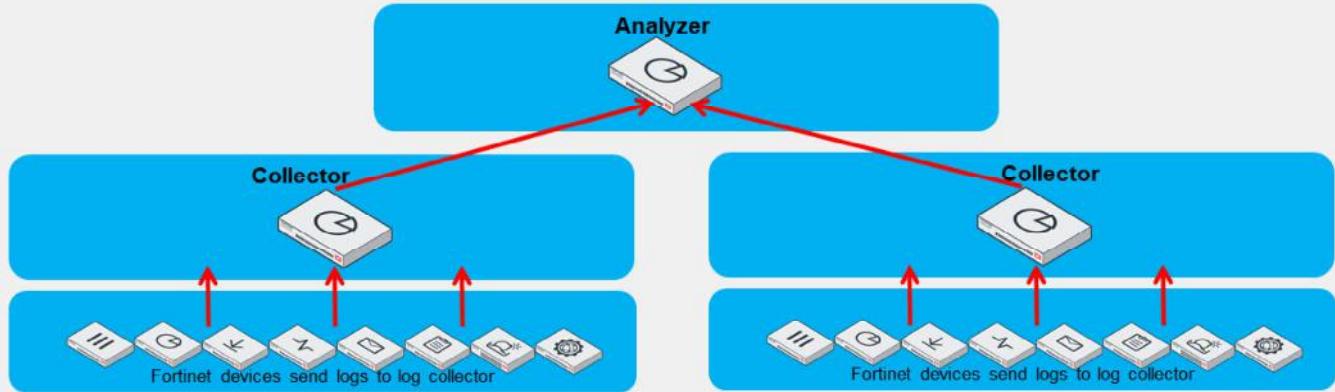
- Collects logs from multiple devices and forwards them to FortiAnalyzer in analyzer mode
 - Can aggregate logs to another FortiAnalyzer
 - However, can forward to syslog/CEF server in real-time forwarding mode only
- Not used for analytics—archiving only



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.

DO NOT REPRINT
© FORTINET

Analyzer—Collector Collaboration



- Increase FortiAnalyzer performance by using both modes
- Offload the log receiving task to the collector
- Analyzer node focuses on data analysis and reporting
- Collector can help with slow or unreliable links by storing logs and forwarding them later
- 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.

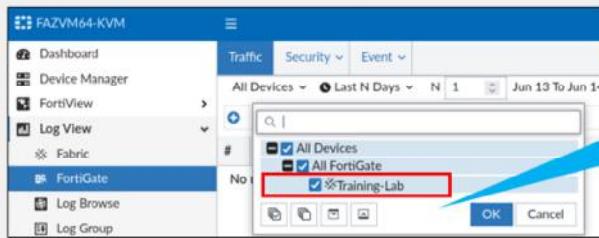
Furthermore, because a collector is strictly dedicated to log collection, its log receiving rate and speed are maximized. If bandwidth is an issue, like in the case of slow WAN links, you can use the store and upload option to send logs only during low-bandwidth periods.

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

Security Fabric Logging

- Store and analyze logs from devices in a Security Fabric group as if the logs are from a single device
- The Security Fabric logs each session once
 - The first FortiGate that handles a session
 - No duplicate traffic logs for sessions coming from another fabric member's MAC address with the following exceptions:
 - If an upstream FortiGate performs NAT
 - Upstream FortiGate devices still log UTM events
- UTM and traffic logs are correlated so session details, UTM events, reporting and automation in the Security Fabric work correctly



Training-Lab is the name of the Security Fabric containing two or more FortiGate devices

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

11

FortiAnalyzer supports the Security Fabric by storing and analyzing the logs from the devices in a Security Fabric group as if the logs are from a single device. FortiAnalyzer correlates traffic logs to corresponding UTM logs so that it can report sessions and bandwidth together with its unified traffic management (UTM) threats.

A session's traffic logging is always done by the first FortiGate that handled it in the Security Fabric. FortiGate devices in the Security Fabric know the MAC addresses of their upstream and downstream peers. If FortiGate receives a packet from a MAC address that belongs to another FortiGate in the Security Fabric, it does not generate a new traffic log for that session. This helps to eliminate the repeated logging of a session by multiple FortiGate devices.

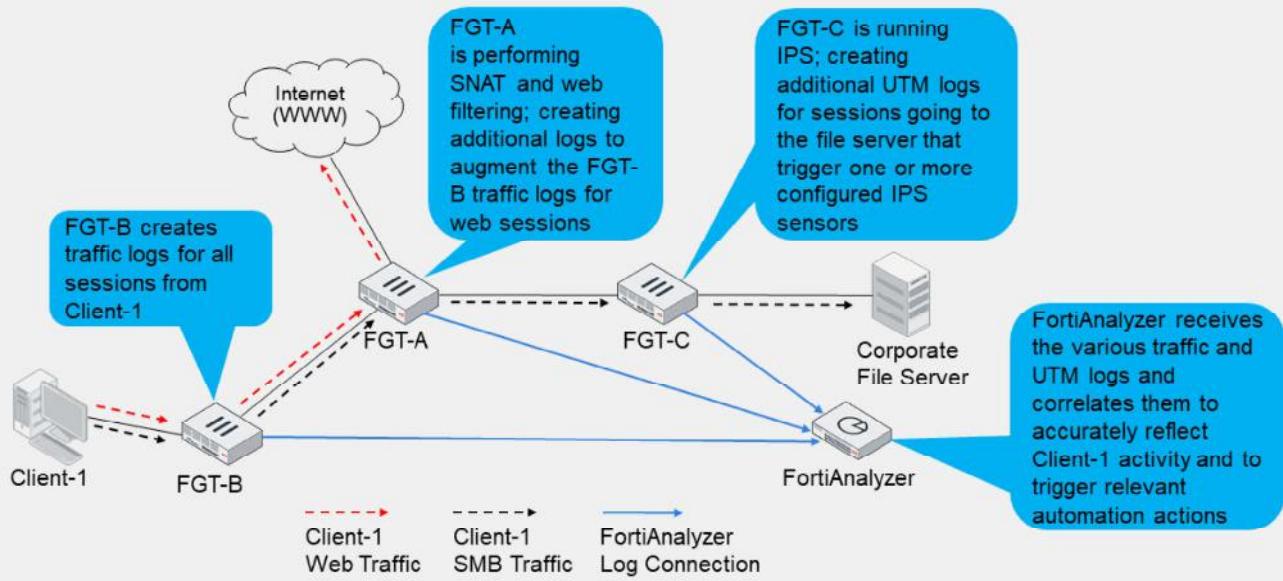
One exception to this behavior is that if the upstream FortiGate performs network address translation (NAT), then another log is generated. The additional log is needed to record NAT details, such as translated ports and addresses.

Upstream devices complete UTM logging, if configured, and FortiAnalyzer performs UTM and traffic log correlation for the Security Fabric, in order to provide a concise and accurate record of any UTM events that may occur. No additional configuration is required for this to take place because FortiAnalyzer performs this function automatically.

Note that each FortiGate in the Security Fabric logs traffic to FortiAnalyzer independent of the root or other leaf devices. If the root FortiGate is down, logging from leaf FortiGate devices to FortiAnalyzer continues to function.

DO NOT REPRINT
© FORTINET

Security Fabric Logging (Contd)



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

12

This slide shows how logging functions in the Security Fabric to give full visibility while eliminating duplicate logs throughout the environment. There are three FortiGate devices configured in a Security Fabric along with a FortiAnalyzer device:

- FGT-A is installed between the corporate network and its internet service provider, where it performs SNAT on outbound communications for RFC-1918 hosts, as well as web filtering for HTTP/HTTPS sessions.
- FGT-B is installed in the access layer, providing device detection, breach isolation, and basic denial-of-service (DoS) protection from the attached end-user LANs.
- FGT-C is installed in the data center where it runs intrusion prevention system (IPS) for all inbound communications to the servers behind it.

All traffic from Client-1 is received by FGT-B, which creates traffic logs for the initial session.

The web session is forwarded to FGT-A, which doesn't duplicate the initial traffic log, but does generate a traffic log as a result of source network address translation (SNAT) being applied to the session. Additionally, FGT-A applies a web filtering policy to this session and generates the relevant UTM logs, if appropriate.

The server message block (SMB) session is forwarded to FGT-A, which does not duplicate the initial traffic log. FGT-A doesn't need to perform NAT or apply web filtering, so it forwards the traffic to FGT-C. FGT-C also does not generate a duplicate traffic log, but it performs IPS inspection based on its configuration and, should a signature match be triggered that results in an action generating a log, logs the event.

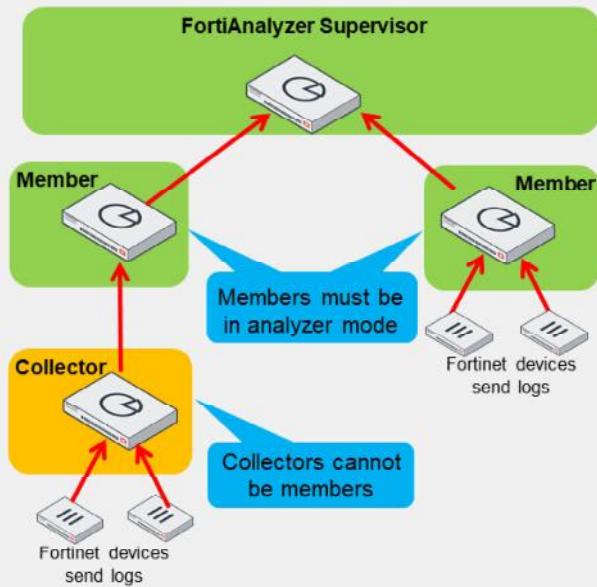
FortiAnalyzer receives the various traffic and UTM logs and correlates them automatically so that they are linked for proper viewing, reporting, and automation actions.

DO NOT REPRINT**© FORTINET**

FortiAnalyzer Fabric

- Centralized viewing of devices, incidents, and events across multiple FortiAnalyzers devices
- Ideal for environments with many FortiAnalyzers and high log volume
- Two operation modes:
 - Supervisor—one per fabric; acts as the root
 - Member—sends information to supervisor
- Supervisor and members must be configured in the same time zone
- Supervisor includes only the following modules:
 - Device Manager
 - Log View
 - Incidents & Events
 - System Settings
 - Management Extensions

The supervisor can view the information on the members using an API. Members *do not* forward their logs to the supervisor.



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

13

The FortiAnalyzer Fabric enables centralized viewing of devices, incidents, and events across multiple FortiAnalyzers.

FortiAnalyzer Fabric includes two operation modes: supervisor and member.

Supervisors act as the root device in the FortiAnalyzer Fabric. Security operations center (SOC) administrators can use the supervisor to view member devices and their administrative domains (ADOMs), authorized logging devices, as well as incidents and events created on members. Incident and event information is synced from members to the supervisor using the API.

Members are devices in the FortiAnalyzer Fabric that send information to the supervisor for centralized viewing. When configured as a member, FortiAnalyzer devices continue to have access to the FortiAnalyzer features identified in the *FortiAnalyzer Administration Guide*. Incidents and events are created or raised from each member.

FortiAnalyzers configured with high availability (HA) can become members. However, HA is not supported for FortiAnalyzers acting as the fabric supervisor.

All FortiAnalyzer Fabric members must be configured with the same time zone settings as the supervisor.

DO NOT REPRINT

© FORTINET

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 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

Dashboard > System Information

System Information	
Host Name	FAZ
Serial Number	FAZ-VM0000065040
Platform Type	FAZVM64-KVM
HA Status	Standalone
System Time	Mon Oct 23 12:53:08 2023 PDT
Firmware Version	v7.4.1-build2308 230831 (GA)
System Configuration	Last Backup: Sun Oct 22 15:35:29 2023
Current Administrato...	admin / 1 in total
Up Time	21 hours 23 minutes 36 seconds
Administrative Dom...	<input type="checkbox"/>

Operation Mode Analyzer Collector

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

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).

All Fortinet devices included in a Security Fabric can be placed into an ADOM of the *Fabric* type, allowing for fast data processing and log correlation.

You will learn more about ADOMs in this course.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What is the default FortiAnalyzer operation mode?
 A. Analyzer
 B. Collector

2. Which FortiAnalyzer operating mode do you use to collect logs from multiple devices and then forward those logs to another device?
 A. Analyzer
 B. Collector

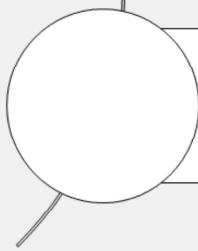
DO NOT REPRINT

© FORTINET

Lesson Progress



Key Features and Concepts



Initial Configuration

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

Now, you will learn to perform the most common initial configurations on FortiAnalyzer.

DO NOT REPRINT**© FORTINET**

Initial Configuration

Objectives

- Identify the tools you can use to configure FortiAnalyzer
- Access FortiAnalyzer for the first time
- Configure network settings



© Fortinet Inc. All Rights Reserved.

17

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 configuration
 - You can find default settings in your FortiAnalyzer *QuickStart* guide (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

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 the *FortiAnalyzer QuickStart Guide* that is specific to your FortiAnalyzer model. 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. Visit docs.fortinet.com for more details.

You can also configure your management IP on the CLI using the `config system interface` command.

DO NOT REPRINT
© FORTINET

Available Tools to Configure FortiAnalyzer

The screenshot shows two side-by-side interfaces. On the left is the 'FortiAnalyzer GUI' dashboard, which includes links for Device Manager, FortiView, Log View, Fabric View, Incidents & Events, Reports, and System Settings. A note below the dashboard states: 'X = Not available in Collector mode'. On the right is the 'FortiAnalyzer CLI' interface, featuring a 'CLI Console' window titled 'Connected FAZVM64-KVM #'. A yellow callout box over this window contains the text: 'Can use the CLI Console widget on dashboard of GUI and terminal emulation program (for example, PuTTY)'. Below the CLI console is a 'PUTTY Configuration' dialog box showing connection settings for host 10.0.1.210, port 22, and protocol SSH. A blue callout box points to this dialog with the text: 'Requires a separate Telnet, SSH, or local console connection'. At the bottom left is the Fortinet Training Institute logo, and at the bottom right is the copyright notice: '© Fortinet Inc. All Rights Reserved. 19'.

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**, **Reports**, or **Incidents & Events**. 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 upon applying the settings, 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.

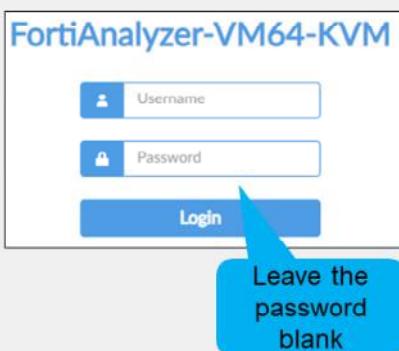
DO NOT REPRINT

© FORTINET

Logging In for the First Time

FortiAnalyzer GUI

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

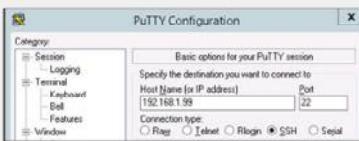


FortiAnalyzer CLI

- Log in to the GUI and click the >_ icon
- Click inside the CLI Console widget (you are automatically logged in)



- Or use a terminal emulator



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.

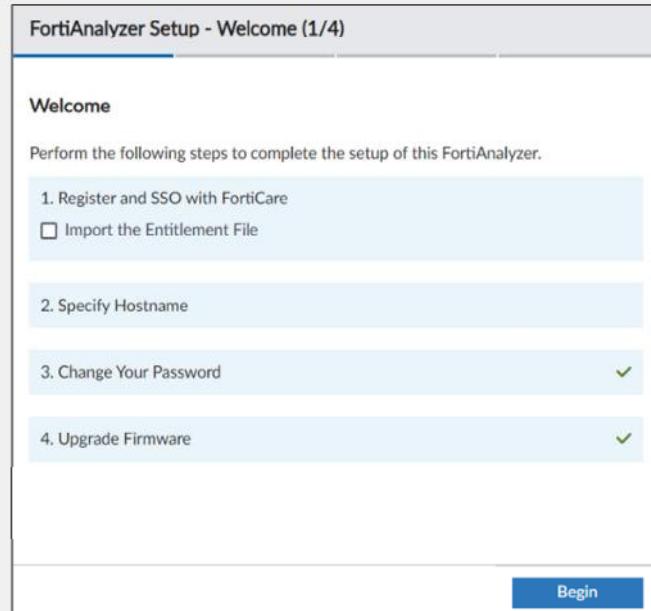
To log in to the CLI for the first time, you can use one of two methods:

- Integrated CLI console: Log in to the GUI and click on the CLI icon located on the upper-right corner. 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
- Option to enable login with FortiCloud SSO users



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

21

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

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

For air-gap environments where the FortiAnalyzer has no direct internet access to contact FortiGuard, you can obtain an entitlement file by contacting Fortinet Customer Service.

You can choose to complete all or some of the steps now or at a later time. A green check mark is displayed beside each completed step.

DO NOT REPRINT
© FORTINET

Configuring FortiAnalyzer for Your Own Network

The screenshot shows the FortiAnalyzer configuration interface with three main sections:

- Interface:** A table listing physical interfaces (port1 to port9). The first three rows (port1, port2, port3) are highlighted with a red border. A blue callout points to this row with the text "Set IPs and admin access".
- DNS:** A section for setting Primary and Secondary DNS servers. Both fields are highlighted with a red border. A blue callout points to this section with the text "Set DNS".
- Routing Table:** A table for defining default routes. One route entry (ID 1) is highlighted with a red border. A blue callout points to this entry with the text "Set gateway".

At the bottom left is the **FORTINET Training Institute** logo. At the bottom right are copyright and page number information: © Fortinet Inc. All Rights Reserved. 22.

The initial configuration of FortiAnalyzer is very similar to the initial configuration of 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 also specify a primary and a secondary DNS server. 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' page under 'System Settings > Network'. The interface is named 'port1'. The 'IP Address/Netmask' field is set to '10.0.1.210/255.255.255.0'. A callout bubble points to this field with the text 'Configure management IP address'. The 'Administrative Access' section includes checkboxes for HTTPS, HTTP, PING, SSH, SNMP, Web Service, and FortiManager. A callout bubble points to the checkboxes for HTTPS, HTTP, PING, and SSH with the text 'Enable protocols to support (default = HTTPS and SSH)'. The 'IPv6 Address' field is set to '::/0'. The 'IPv6 Administrative Access' section has checkboxes for HTTPS, HTTP, PING, SSH, SNMP, Web Service, and FortiManager, all of which are currently unchecked. The 'Status' field is set to 'Up'.

System Settings > Network

Edit Network Interface

Name	port1
Alias	
IP Address/Netmask	10.0.1.210/255.255.255.0
IPv6 Address	::/0
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> Web Service <input type="checkbox"/> FortiManager
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> HTTP <input type="checkbox"/> PING <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> Web Service <input type="checkbox"/> FortiManager
Status	Up

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 23

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. You should be careful if you need to change the management IP address because you will lose access to FortiAnalyzer unless you have another interface with administrative access enabled.

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

- Web Service: Allows access to the FortiAnalyzer API using Simple Object Access Protocol (SOAP) on port 8080.
- FortiManager: Allows FortiAnalyzer to be managed by a FortiManager.

DO NOT REPRINT
© FORTINET

Other Network Settings

- 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

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

Routing Table		
<input type="button" value="+ Create New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>		
	ID ↴	Type ↴

Create New Network Route	
IP Type	IPv4
Destination IP/Mask	0.0.0.0/0.0.0.0
Gateway	
Interface	None
	<input type="text"/>
	port1

FORTINET
 Training Institute

© Fortinet Inc. All Rights Reserved.

24

If you want to be able to resolve host names 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, including your internal DNS servers. It is a best practice to have both a primary and a secondary server. Furthermore, response times are a consideration for DNS, so choose DNS servers as close as possible to your network.

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.

DO NOT REPRINT
© FORTINET

Other Network Settings (Contd)

- Configure a reliable NTP server to ensure the system time is accurate
- Configure link aggregation to increase the available bandwidth and to add network redundancy
 - Can set the minimum number of ports to consider the link status as up
- Configure VLAN interfaces to isolate sensitive traffic from the rest
 - Two protocol options: 802.1Q and 802.1AD

The first screenshot shows the 'NTP Server' configuration with 'Synchronize with NTP Server' checked and a server entry for 'ntp1.fortinet.net'. The second screenshot shows the 'Create New Network Interface' dialog for 'LinkAggregate-1' with 'Type' set to 'Aggregate'. The third screenshot shows the same dialog for 'VLAN100' with 'Type' set to 'VLAN'.

Many FortiAnalyzer features require an accurate system time to work properly. It is highly recommended to synchronize the system time with a reliable NTP server. This can be done under the **System Information** widget included on the default dashboard.

To increase the bandwidth available to receive logs, and to add network redundancy to FortiAnalyzer, you can configure one or more aggregate links. These are logical links that combine two or more physical interfaces, effectively combining their bandwidth. Additionally, these links will remain active if there is at least one working physical interface, hence adding network redundancy to your device.

VLANs are used to isolate different types of traffic in your network. This adds security and, if needed, allows the application of different policies or priorities to that traffic. You can configure VLAN interfaces in FortiAnalyzer to make use of the existing VLANs in your environment. FortiAnalyzer supports both IEEE 802.1Q and 802.1AD protocols.

DO NOT REPRINT**© FORTINET**

Resetting the Configuration

- To reset to factory default settings from flash:

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

Note: The FortiAnalyzer configuration is stored on flash, but logs are stored on disks

- To reset all settings from flash 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 to the console port before running these commands



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` command to perform a low-level format of the disk one or more times. FortiAnalyzer will overwrite the hard disk with random data to ensure data cannot be recovered. 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 Displayed
# get system status	General status of your FortiAnalyzer device
# get system interface	Network interfaces configuration, such as port status, speed, and associated IP address
# show system dns	Configured DNS servers addresses
# show system ntp	Time setting using a network time protocol (NTP) server
# show system route	Configured static routes entries
# execute ping <remote>	Tests connectivity between FortiAnalyzer and another network device

- Example:


```
FAZVM64-KVM # get system interface
== [ port1 ]
name: port1    status: disable   ip: 10.0.1.210  255.255.255.0   speed: auto
== [ port2 ]
name: port2    status: enable    ip: 172.16.100.6 255.255.255.0   speed: auto
```

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

In general, the first word of a command indicates what you are trying to achieve in the CLI:

- The `get` commands allow you to view information in a more readable format.
- The `show` commands allow you to view the exact CLI configuration for that section, including the proper indentation.
- The `execute` commands allow you to perform a function in FortiAnalyzer.

You can use the `?` key to view available syntax options. You can also use the `Tab` key to auto complete your command or cycle through possible commands.

DO NOT REPRINT
© FORTINET

Viewing Server Information

- Use these commands to view system information:

Command	Information Displayed
# diagnose system ntp status	NTP servers' information, such as IPs, stratum, poll time, latency
# diagnose system print cpuinfo	CPU information, such as vendor ID, CPU family, model, stepping, CPU MHz, cache size, physical ID, cores, and many more
# diagnose system print df	File system disk space details, such as file system, 1K-blocks, used and available space, percent used, mount directories
# diagnose system print hosts	Static table lookup for host names
# diagnose system print netstat	Network statistics for active connections including protocol, local address, foreign address, and state
# diagnose system print route	Complete routing table, including directly connected routes

- Example:

```
FAZVM64-KVM # diagnose system print route
Destination Gateway      Genmask      Flags Metric Ref Use     Iface
10.0.1.0    0.0.0.0      255.255.255.0 U        0      0      0      port1
10.200.1.0   0.0.0.0      255.255.255.0 U        0      0      0      port3
10.200.3.0   10.200.1.254 255.255.255.0 UG       1      0      0      port3
172.16.100.0 0.0.0.0      255.255.255.0 U        0      0      0      port2
```

To access and view detailed system-related information, use the `diagnose system` commands.

For a complete list of arguments, refer to the *FortiAnalyzer CLI Reference*, which you can obtain from docs.fortinet.com.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What is the purpose of configuring NTP on FortiAnalyzer?
 - A. To increase the available bandwidth
 - B. To have a reliable system time

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

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 FortiAnalyzer
- ✓ Describe the FortiAnalyzer operating modes
- ✓ Understand logging in a Security Fabric environment
- ✓ Describe FortiAnalyzer Fabric
- ✓ Describe ADOMs
- ✓ Identify the tools used to configure FortiAnalyzer

This slide shows the objectives that you covered in this lesson. By mastering the objectives covered in this lesson, you learned about FortiAnalyzer key features and concepts and how to configure FortiAnalyzer.

DO NOT REPRINT**© FORTINET**

FortiAnalyzer Administrator

Administration and Management

 FortiAnalyzer 7.4.1

Last Modified: 19 December 2023

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

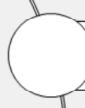
DO NOT REPRINT

© FORTINET

Lesson Progress



Administrative Access Controls



Monitoring Administrative Events and Tasks



ADOMs



Manage Disk Quota



System Backup and Best Practices

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

DO NOT REPRINT**© FORTINET**

Administrative Access Controls

Objectives

- Configure secure administrative access
- Validate administrators using external servers
- Configure two-factor authentication



© Fortinet Inc. All Rights Reserved.

3

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 of your FortiAnalyzer device and the sensitive data it collects.

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

The screenshot shows the FortiAnalyzer interface. In the top navigation bar, it says "System Settings > Administrators". Below this, there is a table listing two users: "admin" and "admin2". The "admin" row has a context menu open, with the "Change Password" option highlighted and surrounded by a red box. Below the table is a "Change Password" dialog box. It contains three input fields: "Old Password" (containing a masked password), "New Password" (containing a masked password), and "Confirm Password" (containing a masked password). At the bottom of the dialog are "OK" and "Cancel" buttons.

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 > Settings > Password Policy

Password Policy	<input checked="" type="checkbox"/>
Minimum Length	8 <input type="button" value="▼"/> Characters (8-32)
Must Contain	<input checked="" type="checkbox"/> Uppercase Letters <input checked="" type="checkbox"/> Lowercase Letters <input checked="" type="checkbox"/> Numbers (0-9) <input checked="" type="checkbox"/> Special Characters
Admin Password Expires after	0 <input type="button" value="▼"/> 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 in a protected and trusted private network
- Use secure communication methods (HTTPS or SSH), even in a private network
- Configure trusted hosts
- Open only the ports necessary for your network (consult docs.fortinet.com)
- If access from the outside is required, set up special users and use only secure protocols
- Always use secure passwords; enforce password policy



© Fortinet Inc. All Rights Reserved.

6

Before you review the configuration settings, you must understand 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 that they can use to breach your network.
- Use trusted hosts 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 (consult *FortiAnalyzer Ports and Protocols* documentation at docs.fortinet.com). Unnecessary 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 purpose 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.
- Store your administrator password in a secure place because FortiAnalyzer does not support password recovery.

DO NOT REPRINT
© FORTINET

Multiple Administrators and Security

- Divide administrative tasks by creating additional administrative accounts
- Every additional administrator causes an increase in risk
- To better protect your network, control administrator access using:
 - Administrative profiles
 - Trusted hosts
 - ADOMs

Assign one or more ADOMs to the administrator account

Administrative profile type

System Settings > Administrators

Create New Administrator	
User Name	Admin1
Avatar	A <input type="button" value="+ Add Photo"/> <input type="button" value="Remove Photo"/>
Description	
Admin Type	LOCAL
New Password	
Confirm Password	
Administrative Domain	<input checked="" type="radio"/> All ADOMs <input type="radio"/> All ADOMs except specified ones <input type="radio"/> Specify
Admin Profile	Restricted_User
JSON API Access	None
Theme Mode	<input checked="" type="radio"/> Use Global Theme <input type="radio"/> Use Own Theme
Trusted Hosts	<input checked="" type="radio"/> Trusted IPv4 Host 1: 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

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 potential growth in risk.

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

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

By dividing administrative access among 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 require
- Assign the appropriate profile—you can modify and create profiles
 - Access profiles define administrator privileges

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

System Settings > Admin Profiles

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

Create custom profiles

Modify individual privileges in profiles

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 8

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 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, and removes all access to the management extensions.
- No_Permission_User, which provides no system or device privileges, and 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 > Administrators

Trusted Host Type	Value
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

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.

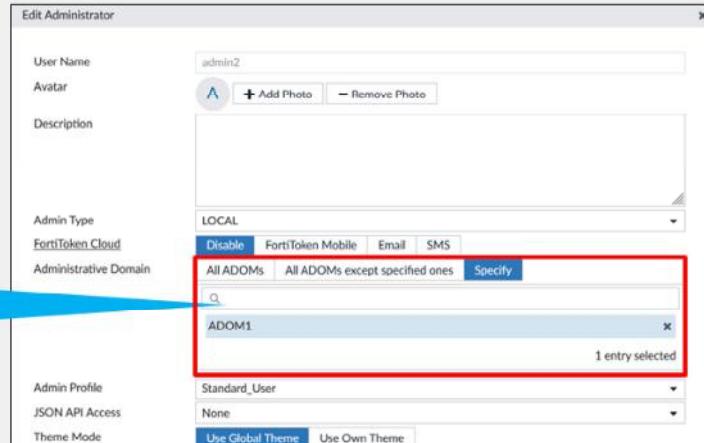
The trusted hosts you define apply to both the GUI and the CLI when accessed through SSH.

DO NOT REPRINT
© FORTINET

Controlling Access Through ADOMs

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

Assign one or more
ADOMs to the
administrator account



Another way you can control administrative access is through ADOMs. Using ADOMs makes device management more effective because administrators need to monitor and manage only 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.

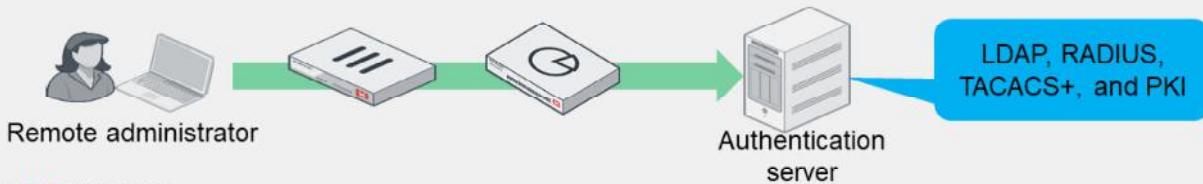
DO NOT REPRINT
© FORTINET

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 > 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 Specify



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

11

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
- One user on FortiAnalyzer that points to a remote authentication server
 - No local credentials on FortiAnalyzer
- Supports LDAP, RADIUS, TACACS+, GROUP
 - The **Admin Type GROUP** supports multiple authentication server types (configured in CLI)

System Settings > Administrators

Edit Administrator

User Name	admin1
Avatar	
Description	
Admin Type	GROUP
GROUP	AuthServers
<input checked="" type="checkbox"/> Match all users on remote server	

System Settings > Remote Authentication Server

In this example, two external authentication servers have been added

+ Create New Edit Delete			
Name	Type	ADOM	Details
External_Server	LDAP	All ADOMs	10.0.1.150.389/uid: ou=Training,dc=trainingAD,dc=fr
LDAP2	LDAP	All ADOMs	10.0.1.155.389/uid: ou=training,dc=trainad,dc=fr

You can enable the **Match all users on remote server** option to allow 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** field, to extend administrator access. Usually, you create a wildcard administrator for only 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 has login credentials on both servers, then the administrator can 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, under config system admin group, 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) + something you have (token)
 - Example: 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 > Remote Authentication Server

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

FORTINET
Training Institute

System Settings > Administrators

Create New Administrator

User Name	2FA-Admin
Avatar	2 Add Photo Remove Photo
Description	
Admin Type	RADIUS
RADIUS Server	RADIUS1
Match all users on remote server	
New Password	*****
Confirm Password	*****
FortiToken Cloud	Disable FortiToken Mobile Email SMS
Administrative Domain	
All ADOMs All ADOMs except specified ones Specify	

© Fortinet Inc. All Rights Reserved.

13

To add additional security to external administrators, you can configure two-factor authentication. To do this, you can 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

Two-Factor Authentication (Contd)

- Can also use FortiToken Cloud to deliver two-factor credentials:
 - FortiToken Mobile app
 - Email
 - SMS

The image shows two screenshots related to two-factor authentication.

Administrator Settings Screenshot:

- User Name: admin-2fa
- Avatar: A placeholder icon with the letter 'A'.
- Description: An empty text area.
- Admin Type: LOCAL
- FortiToken Cloud: Set to Disable.
- FortiToken Mobile: Selected (highlighted with a red box).
- Email: Set to trainingtest@fortinet.com.
- SMS: Not selected.

FortiAnalyzer Login Interface Screenshot:

Please input FortiToken code:

- Username: admin-2fa
- Password: (Redacted)
- Token Code: (Redacted, highlighted with a red box)
- Login Button

Fortinet Training Institute Logo:

© Fortinet Inc. All Rights Reserved. 14

FortiAnalyzer also supports two-factor authentication with FortiToken Cloud. With an active FortiToken Cloud license, you have three options for delivering two-factor credentials. You can install the FortiToken Mobile application on your smart phone, receive the verification code through email, or get the verification code through SMS.

DO NOT REPRINT
© FORTINET

SAML Admin Authentication

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

System Settings > SAML SSO

Single Sign-On Settings

Server Address: 172.16.9.20:14002

Allow admins to login with FortiCloud:

Single Sign-On Mode: Disabled Identity Provider (IdP) Service Provider (SP) Fabric SP

IdP Certificate: Click to select

Login Page Template:

SP Settings

<input type="checkbox"/> Name	<input type="checkbox"/> Entity ID
FortiGate	http://10.200.1.1/metadata/

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved. 15

FortiAnalyzer supports single-sign on (SSO) in multiple ways. It can play the role of the identity provider (IdP), the service provider (SP), or Fabric SP.

When FortiAnalyzer is configured as a Fabric SP, it automatically registers itself to the Fabric root FortiGate as an SP, allowing for simplified configuration. A default SSO administrator is automatically created for each Security Fabric. The IdP certificate is also automatically uploaded to FortiAnalyzer.

You can also create a wildcard SSO administrator that will match multiple users with an IdP. If the IdP leverages a remote authentication server, such as LDAP, this drastically reduces configuration requirements. If you don't enable the **Match all users on remote server** wildcard option, then you must create all those users in FortiAnalyzer.

There is also an option to use SSO with a FortiCloud account or its identity and access management (IAM) users. However, FortiAnalyzer must be registered under that account.

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****ADOMs****Manage Disk Quota****System Backup and Best Practices**

Good job! You now understand administrative access controls.

Now, you will learn how to monitor administrative events.

DO NOT REPRINT**© FORTINET**

Monitoring Administrative Events and Tasks

Objectives

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



© Fortinet Inc. All Rights Reserved.

18

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 administrator accounts that are currently logged in
 - Logged in users are identified by the green check mark
 - CLI command:

```
# diagnose system admin-session status
```
- By default, the list is available only to administrators with Super_User access

System Settings > Administrators

Create New Edit Clone Delete Move Table View <input type="text" value="Search..."/>						
<input type="checkbox"/>	Name	Type	Profile	JSON API Access	ADOMs	Trusted IPv4 Hosts
System Administrator (2)						
<input type="checkbox"/>	 admin	LOCAL	Super_User	None	All ADOMs	0.0.0.0/0.0.0.0
<input type="checkbox"/>	 admin2	LOCAL	Super_User	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 list of administrators.

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 Logs

#	Date/Time	Device ID	Sub Type	User	Message	Operation	Performed On
1	09:15:41	FAZ-VM0000065040	dvm	admin		Switch to new	ADOM1
2	09:15:14	FAZ-VM0000065040	system	admin	User 'admin' with	login	GUI(172.16.100.1)
3	09:15:10	FAZ-VM0000065040	system	admin	User 'admin' with	logout	GUI(172.16.100.1)



© Fortinet Inc. All Rights Reserved. 20

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 > Advanced > Task Monitor

System Settings > Advanced > Task Monitor									
Log Forwarding		Logging Topology		Device Log Settings		Mail Server		Syslog Server	
	ID	Source	Description	User	Status	Time Used	ADOM	Start Time	End Time
<input type="checkbox"/>	19	Device Manager	dvmdb adom ADOM2 object member	A admin	Success: 1	2s	ADOM2	Fri Aug 19 2022 12:01:59 A...	Fri Aug 19 2022 12:02:00 A...
<input type="checkbox"/>	18	Device Manager	dvmdb adom ADOM2 object member	A admin	Success: 1	2s	ADOM2	Fri Aug 19 2022 12:01:13 A...	Fri Aug 19 2022 12:01:15 A...
<input type="checkbox"/>	17	Device Manager	Add/delete Unauthorized Devices	A admin	Success: 1	<1s	root	Thu Aug 18 2022 11:27:30 ...	Thu Aug 18 2022 11:27:30 ...
<input type="checkbox"/>	16	Device Manager	Delete Device	A admin	Success: 1	<1s	root	Thu Aug 18 2022 11:11:45 ...	Thu Aug 18 2022 11:11:45 ...

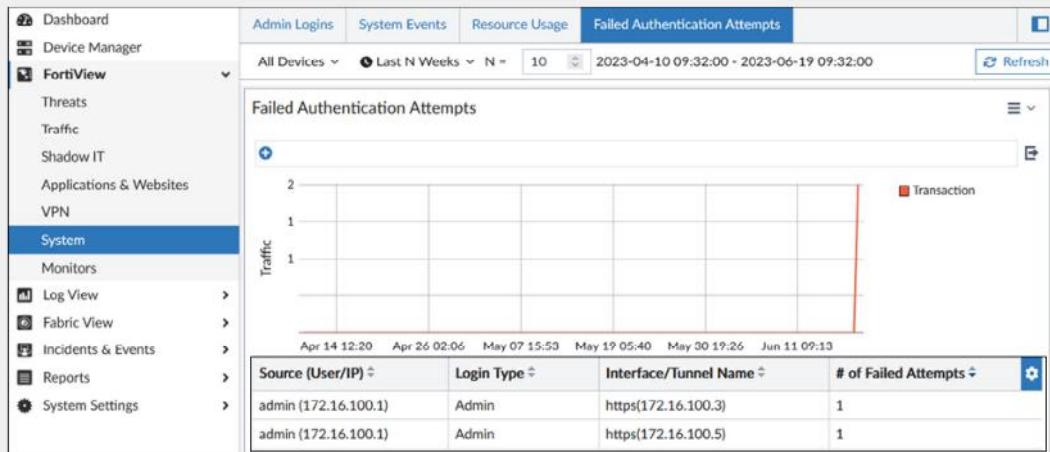
The **Task Monitor** page allows you to view administrator tasks, as well as the progress and status of those tasks.

You can right-click on a task to view more details, including a progress report for each subtask inside the main task.

DO NOT REPRINT
© FORTINET

Monitoring FortiGate Administrator Logins

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



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 22

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, the protocol used, and the number of failed login attempts.

The **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

#	Event Name (Description)	Severity
1	System performance statistics	Low
2	Synchronization of global object report.	Low
3	AV, IPS, GeoIP, SRC-VIS, FortiFlow, URL White-list, Certificate	Critical
4	FortiGate update succeeded	Low

This entry shows that several databases were updated

Log View

13:36:10 critical FGVM01000006469
13:36:10 critical FGVM01000006469
13:36:12 critical FGVM01000007764
13:36:12 critical FGVM01000007764

Identity
Device ID: FGVM01000007764
Device Name: ISFW
User Interface: auto-script
Type
Sub Type: system
Type: event
Alerts
Action: update
Level: critical
General
Log Description: AV, IPS, GeoIP, SRC-VIS, FortiFlow, URL White-list, Certificate
Update databases succeeded

© Fortinet Inc. All Rights Reserved. 23

FortiAnalyzer also 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 **Log View** 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 requires them to manage devices but not system settings, what is the most appropriate default administrator profile to assign them?
 - A. Super_User
 - B. Standard_User

DO NOT REPRINT**© FORTINET**

Lesson Progress



Administrative Access Controls



Monitoring Administrative Events and Tasks



ADOMs



Manage Disk Quota



System Backup and Best Practices

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

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

DO NOT REPRINT**© FORTINET**

Administrative Domains (ADOMs)

Objectives

- Enable and create administrative domains (ADOMs)



© Fortinet Inc. All Rights Reserved. 26

After completing this section, you should be able to achieve the 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

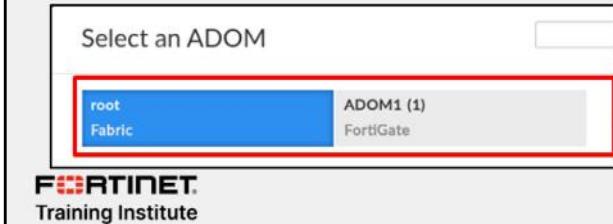
© FORTINET

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



Dashboard > System Information

System Information	
Host Name	FAZ
Serial Number	FAZ-VM0000065040
Platform Type	FAZVM64-KVM
HA Status	Standalone
System Time	Mon Oct 23 12:53:08 2023 PDT
Firmware Version	v7.4.1-build2308 230831 (GA)
System Configuration	Last Backup: Sun Oct 22 15:35:29 2023
Current Administrato...	admin / 1 in total
Up Time	21 hours 23 minutes 36 seconds
Administrative Dom...	<input checked="" type="checkbox"/>
Operation Mode	<input type="radio"/> Analyzer <input type="radio"/> Collector

ADOMs are not enabled by default

With ADOMs enabled, you must select an ADOM after login

© Fortinet Inc. All Rights Reserved. 27

ADOMs are not enabled by default. In addition, by default only administrators with Super_User access can enable and configure ADOMs.

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) or advanced mode
- **Normal:** *Cannot* assign VDOMs from the same FortiGate to multiple FortiAnalyzer ADOMs
 - Must assign the FortiGate device and all of its VDOMs to a single ADOM
- **Advanced:** *Can* assign VDOMs from the same FortiGate to multiple FortiAnalyzer ADOMs
 - Can use FortiView, Event Management, and Reports functions to analyze data for individual VDOMs

The screenshot shows the 'System Settings > Advanced > Misc Settings' interface. At the top, there are tabs for Log Forwarding, Logging Topology, Device Log Settings, Mail Server, and Misc Settings (selected). Below these tabs is a sub-header 'Advanced Settings'. In the main content area, there is a section titled 'ADOM Mode' with two buttons: 'Normal' (highlighted with a red box) and 'Advanced'. To the right of this section is a code block containing a configuration command:

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



© Fortinet Inc. All Rights Reserved. 28

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

In normal mode, you *cannot* assign 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, it is not possible to assign different VDOMs to different ADOMs.

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

DO NOT REPRINT

© FORTINET

Creating an ADOM

- Create new ADOMs if default ones do not fit your requirements
 - Devices can be registered to their *device-specific* ADOMs only
- Disk quota configured per ADOM (not per device)
- Cannot delete a custom ADOM if a device is still assigned to it
- CLI command to view ADOMs: `# diagnose dvm adom list`

The screenshot shows the 'System Settings > ADOMs' page. On the left, a list of existing ADOMs is shown, categorized by type: Security Fabric (root, ADOM1), FortiGates (FortiProxy, FortiFirewallCarrier, FortiFirewall, FortiDeceptor, FortiCarrier, ADOM2), and Other Device Types (Chassis, Syslog). On the right, a 'Create ADOM' dialog box is open. It has fields for 'Name' (set to 'ADOM1') and 'Type' (set to 'Fabric'). Below these are sections for 'Devices' (with a 'Select Device' button and a search bar), 'Data Policy' (with dropdowns for 'Keep Logs for Analytics' and 'Keep Logs for Archive'), and 'Disk Utilization' (with fields for 'Allocated' storage and 'Maximum Available'). Two callout boxes point to specific settings: one labeled 'Retention policy' points to the 'Data Policy' section, and another labeled 'Configure disk quota' points to the 'Disk Utilization' section.

On the **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 device, 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** to the individual devices added to it.

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

- 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
 - Device Manager
 - LogView

System Settings > ADOMs

Create ADOM	
Name	Fabric_ADOM
Type	Fabric
Time Zone	Default

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**, **Log View**, **Incidents & Events**, 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 _____.
 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 ADOMs.

DO NOT REPRINT**© FORTINET**

Lesson Progress



Administrative Access Controls



Monitoring Administrative Events and Tasks



ADOMs



Manage Disk Quota



System Backup and Best Practices

Good job! You now understand ADOMs.

Now, you will learn how to manage disk quotas.

DO NOT REPRINT

© FORTINET

Disk Quota

Objectives

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



© Fortinet Inc. All Rights Reserved. 34

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 allotted log disk space is *full*:
 - An automatic alert is generated
 - The oldest logs are overwritten (default behavior)
 - However, to stop logging when the disk is full:

```
# config system locallog disk setting
    set diskfull nolog
end
```
- 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.

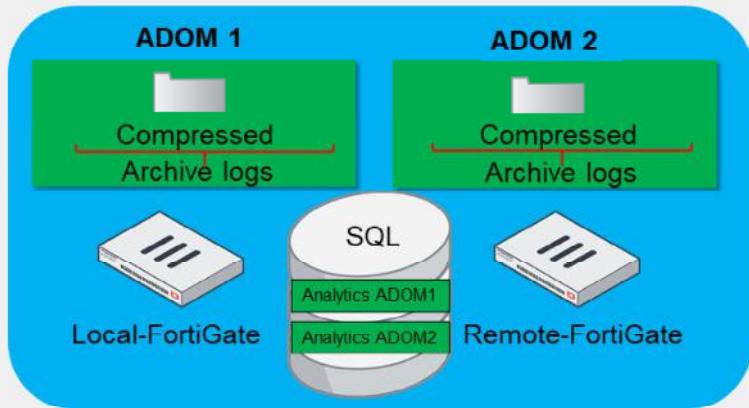
No administrator wants to lose valuable log data and run the risk of noncompliance with regard to data retention. As such, it is vital you know your FortiAnalyzer disk quota, how it is enforced, and what space is reserved and thus not available for storing logs.

DO NOT REPRINT

© FORTINET

Disk Quota

- Disk quota includes:
 - Archive logs
 - Analytics logs



FortiAnalyzer disk quota includes two types of logs:

- 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 600 bytes in size, and an average compressed log is only 80 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**

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

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 20% disk space for compression files, upload files, and temporary report files, leaving about 80% 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

Example—Understanding Disk Quota

```
# diagnose log device
```

Total Quota Summary:

Total Quota	Allocated	Available	Allocate%
48.0GB	19.5GB	28.5GB	40.7%

System Storage Summary:

Total	Used	Available	Use%
59.0GB	4.7GB	54.3GB	8.0 %

Reserved space: 11.0GB (18.6% of total space).

59.0GB (Total System Storage)

- 11.0GB (Reserved Space)

= 48.0 (Total Quota)

19.5GB (Allocated) = Archive + Analytics Quota
for all ADOMs

4.7GB (Used) = Logs + all system files on mounted
drive (# diagnose system print df)

Archive										Analytics									
AdomName	AdomOID	Type	[Retention	Quota	Used	Logs/Logs/	Quaranti/	content/	IPS	Used%	[Retention	Quota	Used	SiemDB/	hache/	Used%			
ADOM1	185	FSF	365days	600.0MB	10.7MB	10.7MB/	0.0KB/	0.0KB/	0.0KB	1.0%	60days	1.4GB	5.5MB	927.4KB/	0.0KB/	0.4%			
ADOM2	207	FGT	365days	300.0MB	104.0KB	104.0KB/	0.0KB/	0.0KB/	0.0KB	0.0%	60days	700.0MB	984.0KB	0.0KB/	0.0KB/	0.1%			
FortiAnalyzer	122	FAZ	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0KB	0.0%	60days	700.0MB	0.0KB	0.0KB/	0.0KB/	0.0%			
FortiAuthenticator	138	FAC	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0KB	0.0%	60days	700.0MB	0.0KB	0.0KB/	0.0KB/	0.0%			
FortiCache	126	FCH	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0KB	0.0%	60days	700.0MB	0.0KB	0.0KB/	0.0KB/	0.0%			
FortiCarrier	118	FGT	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0KB	0.0%	60days	700.0MB	0.0KB	0.0KB/	0.0KB/	0.0%			
... (output truncated) ...																			
root	3	FSF	365days	300.0MB	0.0KB	0.0KB/	0.0KB/	0.0KB/	0.0KB	0.0%	60days	700.0MB	1.9MB	120.2KB/	0.0KB/	0.3%			
Total usage: 19 ADOMs, logs=10.9MB(10.8MB/0.0KB/0.0KB/0.0KB) database=162.6MB(ADOMs usage:8.4MB(1.0MB, 0.0KB) + Internal Usage:154.2MB)																			



© Fortinet Inc. All Rights Reserved. 38

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.

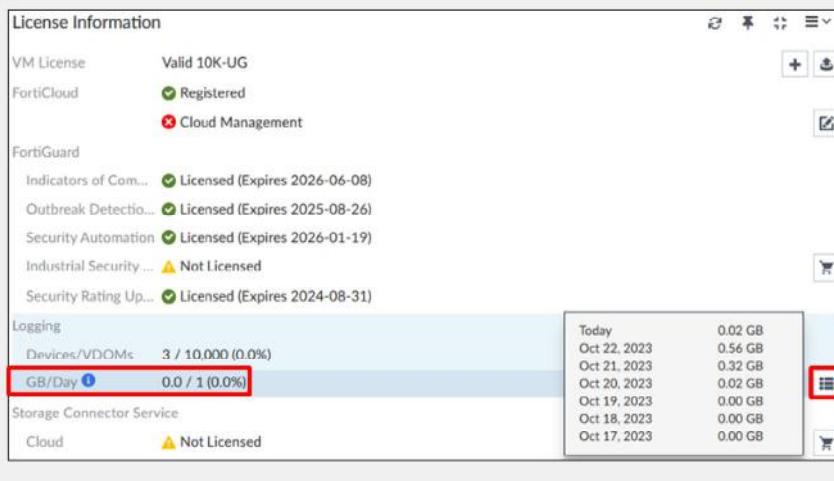
The allocated space is determined by adding the archive and analytics quota for all ADOMs.

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*
 - 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



FORTINET.
 Training Institute

© Fortinet Inc. All Rights Reserved.

39

Note that the **License Information** widget shows a lower value than the disk quotas. This is because it reports only on the number of logs pushed to FortiAnalyzer *on that day*. You can click the show details icon to see the log volume for the previous 6 days. 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.

You must pay attention to both the daily log limit and the configured disk quotas. If you find that either is consistently approaching or going over the threshold, see if you can optimize your FortiAnalyzer configuration by reducing unnecessary logs, such as by filtering logs and removing unnecessary devices from being logged. If the network consistently generates traffic that exceeds the daily log limit, you can increase your licensing level. If you find that the disk quota is not sufficient to meet your logging requirements, you must allocate more resources.

DO NOT REPRINT
© FORTINET

Disk Quota Enforcement

- Processes used for disk quota enforcement:

logfiled	sqlplugind	oftpd
<ul style="list-style-type: none">• Monitors log file size, SQL database size, and archive file size; sends commands to the other daemons to process• Enforces log file size	<ul style="list-style-type: none">• Enforces the SQL database size	<ul style="list-style-type: none">• 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%



© Fortinet Inc. All Rights Reserved. 40

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**

Modify ADOM Disk Quota

- Monitor log utilization and quotas

```
# diagnose log device
```
- If a high volume of logs exists, consider increasing the ADOM log quota so the oldest logs are not lost
- Allocating an insufficient quota to an ADOM can:
 - Prevent log retention objectives
 - Draw unnecessary CPU resources to enforce the quota with log deletion and database trims
 - Affect reporting if the quota enforcement acts on analytical data before a report is complete

System Settings > ADOMs

The screenshot shows the 'System Settings > ADOMs' page. Under 'Data Policy', 'Keep Logs for Analytics' is set to 60 days and 'Keep Logs for Archive' is set to 365 days. Under 'Disk Utilization', 'Allocated' is set to 3000 MB (Maximum Available: 30.4 GB). Under 'Analytics: Archive', 'Alert and Delete When Usage Reaches' is set to 90%. A note at the bottom states: "If analytic or archive log usages exceed the configured disk quota before the retention period expires, the oldest logs will be deleted."

Based on your log rate and device usage statistics, you may need to adjust your ADOM disk quota so that 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 an insufficient quota to an ADOM can cause many problems:

- It can prevent you from reaching your log retention objective.
- It can cause unnecessary CPU resources enforcing quota with log deletion and database trims.
- It can adversely affect reporting if the quota enforcement acts on analytical data before a report is complete.

DO NOT REPRINT**© FORTINET**

Increasing Disk Space

- With FortiAnalyzer VMs, you can dynamically add more disk space:
 1. Power off the VM and add a new virtual disk
 2. Start the VM and run `lvm info` to confirm the new disk was detected
 - The new disk is labeled as **Unused**
 3. Run `lvm extend`
 - This command will add the space of the additional disk to the lvm volume
 4. Reboot the VM, and then run the command `get system status` to see the new disk space available
- With hardware FortiAnalyzer, you must add one or more disks to the device
 - 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!



© Fortinet Inc. All Rights Reserved. 42

If increasing the 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 must add one or more disks. If you are using RAID, you will also have to rebuild your RAID array if you add another disk. Therefore, it is important to account for future 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?

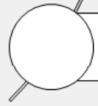
- A. The oldest logs are overwritten.
- B. Logging stops.

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

**Administrative Access Controls****Monitoring Administrative Events and Tasks****ADOMs****Manage Disk Quota****System Backup and Best Practices**

Good job! You now understand disk quotas.

Now, you will learn how to back up your FortiAnalyzer and some general best practices.

DO NOT REPRINT**© FORTINET**

System Backup and Best Practices

Objectives

- Perform a system configuration backup
- Describe best practices



© Fortinet Inc. All Rights Reserved. 45

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

By demonstrating competence in performing a system configuration backup and following best practices, you will be able to minimize the downtime in the case of a system failure or accidental misconfiguration.

DO NOT REPRINT

© FORTINET

Performing a System Configuration Backup

- System configuration backups contain:
 - System information
 - Device list
 - Report information
- Logs and generated reports are *not included*
- You can restore a backup to only the same model and firmware version
- You can encrypt a backup file
- You can restore a system configuration from any previous backup
- If your FortiAnalyzer is a VM, you can also use VM snapshots

System Settings > Dashboard

System Information	
Host Name	FAZ
Serial Number	FAZ-VM0000065040
Platform Type	FAZVM64-KVM
HA Status	Standalone
System Time	Mon Oct 23 12:53:08 2023 PDT
Firmware Version	v7.4.1-build2308 230831 (GA)
System Configuration	Last Backup: Sun Oct 22 15:35:29 2023
Current Administrato...	admin / 1 in total
Up Time	21 hours 23 minutes 36 seconds
Administrative Dom...	●
Operation Mode	Analyzer Collector

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

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

The system configuration backup includes:

- 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 details are not the actual reports.
- Automation and Incident & Events configurations, such as playbooks and event handlers

You can save the backup file as an encrypted file for additional security. Be aware that you can restore a backup to only 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**

Performing a System Configuration Backup (Contd)

- Use the following commands to schedule your FortiAnalyzer backups and send them to a remote server:

```
config system backup all-settings
    set status {enable | disable}
    set server {<ipv4_address>|<fqdn_str>}
    set user <username>
    set directory <string>
    set week_days {monday tuesday wednesday thursday friday saturday sunday}
    set time <hh:mm:ss>
    set protocol {ftp | scp | sftp}
    set passwd <passwd>
    set cert <certificate_name>
    set crptpasswd <passwd>
end
```

Supported servers include FTP, SCP and SFTP

- You must configure the destination server before you send the backup files



© Fortinet Inc. All Rights Reserved. 47

You can schedule your backups and store them on a remote server. FortiAnalyzer supports sending its backup files to FTP, SCP, and SFTP servers. You must configure the destination server to which you send the backup files. You must have valid credentials with read-write permissions in the destination folder.

This slide shows the commands you use to schedule the backup jobs.

DO NOT REPRINT
© FORTINET

Best Practices

- Shut down FortiAnalyzer gracefully—not doing so can damage the databases

```
# execute shutdown
```
- Run on an uninterruptable power supply (UPS)
- Save an unencrypted backup to a secure location
 - Allows for offline access to the database configuration file
 - Recommended when dealing with Fortinet Support
- Synchronize the time on FortiAnalyzer and all registered devices with an NTP server



© Fortinet Inc. All Rights Reserved. 48

The following are some best practices for operating FortiAnalyzer:

- Always shut down FortiAnalyzer *gracefully* because not doing so can damage the databases.
- Run FortiAnalyzer on a UPS to prevent unexpected power-off events. Also, ensure your UPS is stable and has enough current to ensure the 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.

DO NOT REPRINT**© FORTINET**

Best Practices (Contd)

- Implement a comprehensive backup plan that includes the configuration and the logs
- Increase reliability by configuring high availability (HA) and link aggregation
- Check the compatibility matrix for FortiAnalyzer and other Fortinet products
 - This includes the firmware compatibility on both ends
- Check and follow the recommended upgrade path
 - You can verify the upgrade history on your FortiAnalyzer device:

```
# diagnose cdb upgrade summary
===== New configuration database initiated =====
2023-05-26 16:28:58      v7.2.2-build1334 230201 (GA)
2023-05-26 16:33:21      v7.4.0-build2223 230514 (GA)
2023-09-01 15:05:24      v7.4.1-build2308 230831 (GA)
```



In addition, there are a few more best practices that should be followed:

- Implement a comprehensive backup plan that includes the configuration and the logs. Log backups will be discussed in Lesson 5 – *Logs and Reports Management*.
- Increase reliability by configuring high availability (HA) and link aggregation.
- Check the compatibility matrix for FortiAnalyzer and other Fortinet products. This include the firmware compatibility on both ends.
- Check and follow the recommended upgrade path. Consult docs.fortinet.com to find the appropriate upgrade path.

DO NOT REPRINT**© FORTINET**

Lesson Progress

**Administrative Access Controls****Monitoring Administrative Events and Tasks****ADOMs****Manage Disk Quota****System Backup and Best Practices**

Congratulations! You have completed this lesson.

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

DO NOT REPRINT**© FORTINET**

Review

- ✓ Configure secure administrative access
- ✓ Validate administrators using external servers
- ✓ Configure two-factor authentication
- ✓ Monitor FortiAnalyzer administrators, events, and tasks
- ✓ Monitor FortiGate administrator logins and activity
- ✓ Enable and create ADOMs
- ✓ Understand what comprises the disk quota
- ✓ Understand the disk quota
- ✓ Modify the disk quota
- ✓ Perform a system configuration backup
- ✓ Describe best practices



© Fortinet Inc. All Rights Reserved. 51

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 and internal threats.

DO NOT REPRINT

© FORTINET



FortiAnalyzer Administrator

RAID and HA

 FortiAnalyzer 7.4.1

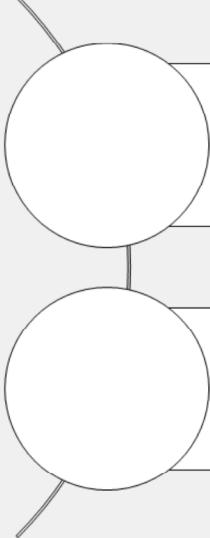
Last Modified: 19 December 2023

In this lesson, you will learn how to use RAID and high availability (HA) to make your FortiAnalyzer device more resilient to hardware failures.

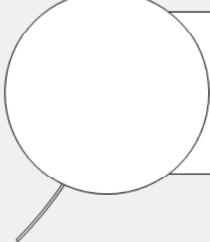
DO NOT REPRINT

© FORTINET

Lesson Overview



Protecting Log Data Using RAID



Using HA



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

2

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

DO NOT REPRINT

© FORTINET

Protecting Log Data Using RAID

Objectives

- Understand high performance log storage (RAID)
- Configure RAID
- Troubleshoot RAID



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

3

After completing this section, you should be able to achieve objectives shown on this 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**

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 (check device specifications)



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

4

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

RAID is not supported on all FortiAnalyzer models.

DO NOT REPRINT**© FORTINET**

Protecting Log Information Through RAID

- RAID is a high-performance storage solution
 - Stands for redundant array of independent disks
- Combines multiple, equal-sized disk drives into a logical unit
 - Data is distributed in different ways—determined by the RAID level used
 - Different RAID levels provide different benefits regarding capacity, performance, and availability
 - Not all RAID levels provide fault tolerance
- Requires multiple identical drives
- Some RAID levels provide redundancy of log data, increasing the availability of your logs against critical events
- RAID is *not* a replacement for backups
 - Make log backups even if you employ RAID



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

5

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 to act as a backup, should your system stops running. The most commonly used method for high performance storage is RAID.

You can protect your logs by using a fault tolerant RAID solution. This improves your log availability, should a critical event on your FortiAnalyzer occur. However, keep in mind that not all FortiAnalyzer models support RAID. Check your device specifications to verify if RAID is supported.

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 mirroring only, others do striping only, others do both, and some include parity (distributed)
 - Some can handle one failed drive, others two
 - *Having 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



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

6

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, having too many failed drives results in the loss of data.

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

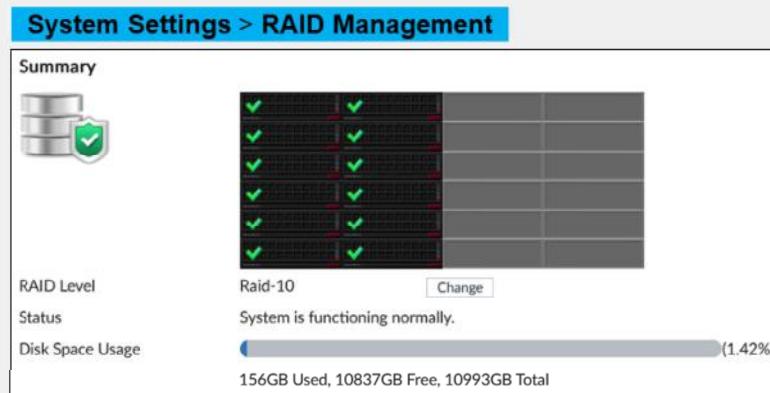
Hardware RAID is always recommended because a dedicated controller card handles all the RAID operations faster and more efficiently.

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



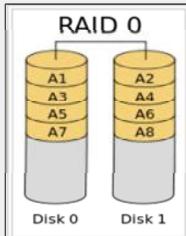
Not all FortiAnalyzer models support RAID, so the menu option to configure RAID may not appear on the GUI. Be sure to check the model specifications to see if RAID is supported, and to what level.

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.

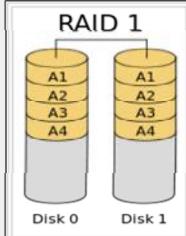
DO NOT REPRINT

© FORTINET

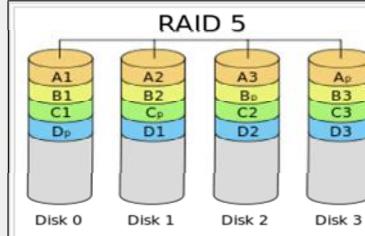
RAID Levels 0, 1, 5, and 6



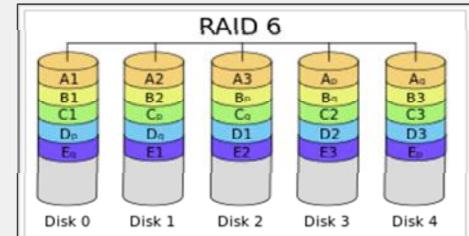
Striping
Example: RAID 0 with two 1-TB disks provides 2 TB of space



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

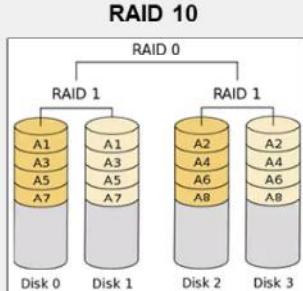
Some common RAID levels are: RAID 0 (striping), RAID 1 (mirroring) and its variants, RAID 5 (distributed parity), RAID 6 (double parity), RAID 50 (striping and distributed parity), and RAID 60 (striping and distributed double parity):

- RAID 0 consists of data split evenly across two or more disks. Speed and performance are the main goals, since the FortiAnalyzer device can distribute disk operations across multiple disks. However, 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. Write performance is not increased because data needs to be mirrored to all disks. 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.

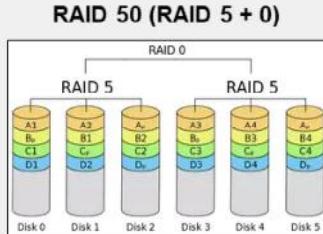
DO NOT REPRINT

© FORTINET

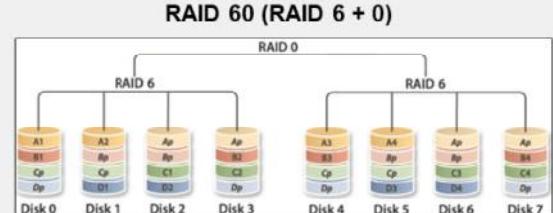
RAID Levels 10, 50, and 60



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:
 - Good
 - Rebuilding
 - Initializing
 - Verifying
 - Degraded
 - Inoperable

System Settings > RAID Management

Disk Management				
<input type="checkbox"/>	Disk Number	Disk Status	Size (GB)	Disk Model
<input type="checkbox"/>	0	Good	1862	WDC WD2000FYYZ-01UL1B1
<input type="checkbox"/>	1	Good	1862	WDC WD2000FYYZ-01UL1B1
<input type="checkbox"/>	2	Good	1862	WDC WD2000FYYZ-01UL1B1
<input type="checkbox"/>	3	Good	1862	WDC WD2000FYYZ-01UL1B1
<input type="checkbox"/>	4	Good	1862	WDC WD2000FYYZ-01UL1B1
<input type="checkbox"/>	5	Good	1862	WDC WD2000FYYZ-01UL1B1
<input type="checkbox"/>	6	Good	1862	WDC WD2000FYYZ-01UL1B1
<input type="checkbox"/>	7	Good	1862	WDC WD2000FYYZ-01UL1B1
<input type="checkbox"/>	8	Good	1862	WDC WD2000FYYZ-01UL1B1
<input type="checkbox"/>	9	Good	1862	WDC WD2000FYYZ-01UL1B1
<input type="checkbox"/>	10	Good	1862	WDC WD2000FYYZ-01UL1B1
<input type="checkbox"/>	11	Good	1862	WDC WD2000FYYZ-01UL1B1

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 states:

- **Good:** The disk is functioning normally.
- **Rebuilding:** FortiAnalyzer is writing data to a newly added hard drive to restore logical drive to an optimal state. It is not fully fault tolerant until rebuilding is complete.
- **Initializing:** FortiAnalyzer is writing to all the hard drives in the device in order to make the array fault tolerant.
- **Verifying:** FortiAnalyzer is ensuring the parity data of a redundant drive is valid.
- **Degraded:** The hard drive is no longer being used by the RAID controller.
- **Inoperable:** One or more drives is missing—the drive is no longer available to the OS. Data in an inoperable state cannot be accessed.

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 FortiAnalyzer is still running (*hot swapping*)
 - Software RAID: You must shut down FortiAnalyzer prior to exchanging the hard disk (hot swapping is supported with hardware RAID only)



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

11

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 before exchanging the hard disk.

DO NOT REPRINT**© FORTINET**

Diagnosing RAID

- You can check the RAID and disk status using the following commands for a 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 disk usage` command is available



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

12

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` command 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.



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 13

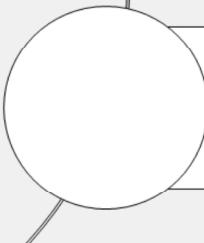
DO NOT REPRINT

© FORTINET

Lesson Overview



Protecting Log Data Using RAID



Using HA

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

14

Good job! You now know how to use RAID to protect the log data.

Now, you will learn about using HA.

DO NOT REPRINT**© FORTINET**

Using HA

Objectives

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



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

15

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

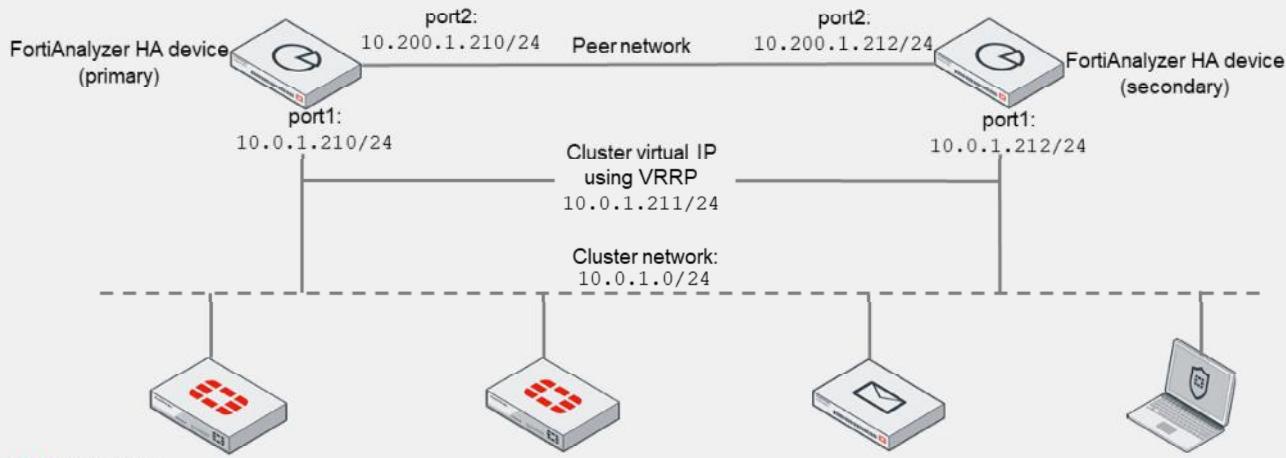
By demonstrating competence in the configuration and troubleshooting of HA, you will be able to increase the availability of your FortiAnalyzer implementation.

DO NOT REPRINT

© FORTINET

HA

- FortiAnalyzer HA provides:
 - 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



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

16

A FortiAnalyzer HA cluster provides the following:

- Applies 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 and sharing load for FortiView widgets.

A 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 from the same FortiAnalyzer series, use the same 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 on the same platform. For example, a VM running on VMware can't form a cluster with a VM running on KVM. 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**

Active-Active HA

- FortiAnalyzer in active-passive HA mode requires layer 2 connectivity between devices to form a cluster
- However, FortiAnalyzer in active-active mode can form a cluster with devices on different subnets
 - This allows FortiAnalyzer HA to form between devices in different geographic locations
- There are additional differences:

Active-Passive	Active-Active
Only the HA primary device can receive logs and archive files from its directly connected devices and forward them to the HA secondary devices	All HA members can receive logs and archive files from their directly connected devices and forward them to their HA peers
Only the HA primary device can forward logs and archive files to a remote server	All HA members can forward their directly received logs and archive files to a remote server



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved.

17

FortiAnalyzer HA in active-passive mode requires a layer 2 connection between HA members in order to set up the HA cluster virtual IP. However, in active-active mode, members can be in different geographic locations and form a cluster. Instead of using a virtual IP address, you define the heartbeat interface as the interface used to communicate with the peer across different networks.

Furthermore, in active-active mode, all HA members can receive logs and archive files from their directly connected devices, and then forward them to other HA members. All HA members can also forward their directly received logs and archive files to a remote server.

DO NOT REPRINT

© FORTINET

HA Options

- FortiAnalyzer has three HA operation modes:
 - Standalone
 - Active-Passive
 - Active-Active
- Most common HA settings are available in the GUI
- However, some options are available only in the CLI. For example:

```
# set unicast enable
```

System Settings > HA

Cluster Settings	
Operation Mode	Standalone Active-Passive Active-Active
Preferred Role	Secondary Primary
Cluster Virtual IP	
IP Address and Interface	IP Address 10.200.4.100 Interface port4
Cluster Settings	
Peer IP and Peer SN	Peer IP 10.200.1.224 Peer SN FAZ-VMTM23008175
Group Name	FAZ-HA
Group ID	1 {1-255}
Password	*****
Heart Beat Interval	4 Seconds
Heart Beat Interface	port1
Failover Threshold	12
Priority	100 {80-120}
Log Data Sync	<input checked="" type="checkbox"/>

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**, and then 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. The virtual IP is optional for active-active mode.

Once the cluster is up, the devices sending their logs must point to this IP. By default, the VRRP heartbeat packets are sent to the multicast address 224.0.0.18, and sourced from the primary IP address of the first virtual IP interface configured. You can configure a different interface to send the heartbeats, as well as set it to use unicast.

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 log synchronization traffic. As shown on this slide and the previous one, these IP addresses don't have to be on the same subnet as the cluster virtual IP. On the contrary, it is recommended they are on separate subnets.

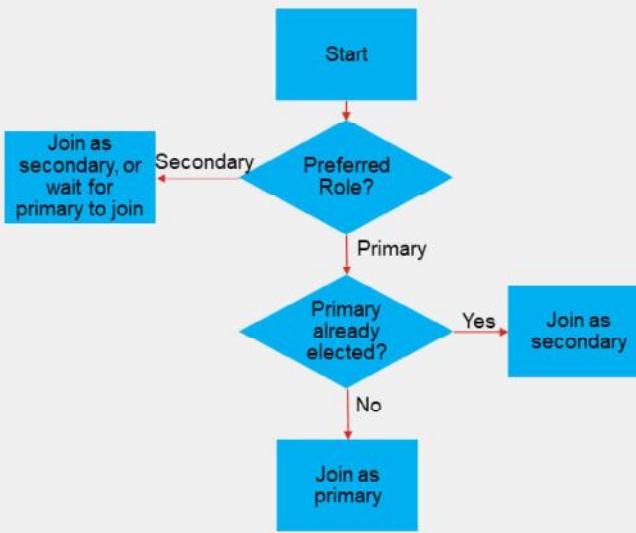
The primary device and all secondary devices must have the same **Group Name**, **Group ID**, and **Password**. The **Priority** setting is used during the selection of the primary device in the cluster. You can assign a value from 80 to 120, where a higher number has higher priority. The **Log Data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

DO NOT REPRINT

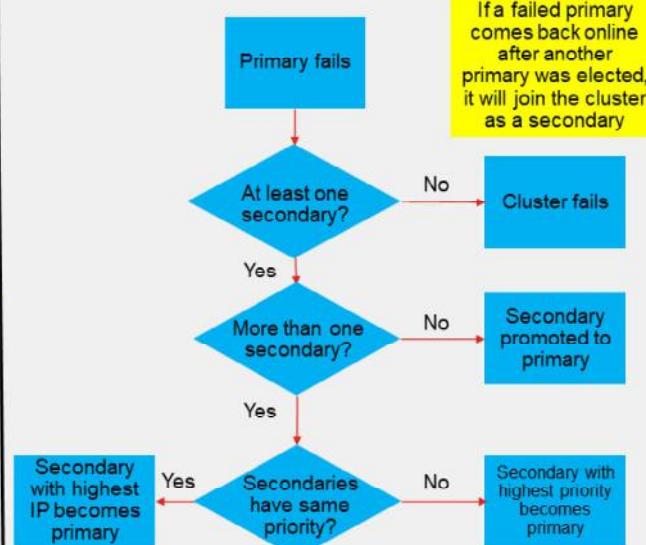
© FORTINET

HA Primary Election Process

- Initial primary election



- Primary election after failure



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 19

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 from the CLI with the command `set healthcheck DB`, under the `system ha` configuration mode.

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 their firmware
 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.



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 21

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							
<input type="checkbox"/>	Role	Serial Number	IP	Host Name	Uptime/Downtime	Initial Logs Sync	Configuration Sync
<input type="checkbox"/>	Primary	FAZ-VM0000065040	10.200.1.210	FAZ1	↑04m 13s	-	Config will be synced to secondaries
<input type="checkbox"/>	Secondary	FAZ-VMTM23008175	10.200.1.224	FAZ2	↑02m 50s	Syncing100%	In-Sync

- 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.

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



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 23

DO NOT REPRINT

© FORTINET

Lesson Overview



Protecting Log Data Using RAID



Using HA

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 24

Congratulations! You have completed this lesson.

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

DO NOT REPRINT

© FORTINET

Review

- ✓ Understand high performance log storage (RAID)
- ✓ Configure RAID
- ✓ Troubleshoot RAID
- ✓ Understand FortiAnalyzer HA
- ✓ Configure HA
- ✓ Understand HA synchronization and load balancing
- ✓ Upgrade the firmware of an HA cluster
- ✓ Verify the normal operation of an HA cluster



© Fortinet Inc. All Rights Reserved.

© Fortinet Inc. All Rights Reserved. 25

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

You learned how to use RAID and HA to make your FortiAnalyzer device more resilient against hardware failures.

DO NOT REPRINT**© FORTINET**

FortiAnalyzer Administrator

Managing Devices

FortiAnalyzer 7.4.1

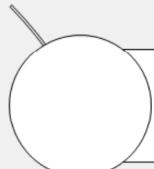
Last Modified: 19 December 2023

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.

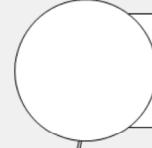
DO NOT REPRINT

© FORTINET

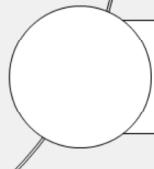
Lesson Overview



Registering Devices



Communication Troubleshooting



Managing Registered Devices

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
- Create device groups



© Fortinet Inc. All Rights Reserved.

3

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 device registration states:
 - Registered: *authorized* to store logs on FortiAnalyzer
 - Unregistered: *requesting* to store logs on FortiAnalyzer
- Various ways to register a device with FortiAnalyzer:
 - Initiate registration from FortiAnalyzer or from the remote device
 - Stage devices on FortiAnalyzer by prepopulating information
 - Add individual devices or a Security Fabric



© Fortinet Inc. All Rights Reserved.

4

For FortiAnalyzer to start collecting logs from a device, that device must become a registered device 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 various ways you can register a device with FortiAnalyzer.

A supported device can send a registration request. When the FortiAnalyzer administrator receives that request, the request can be accepted or denied.

You can also add devices on FortiAnalyzer using the **Add Device** wizard. The device can be added based on its serial number or a pre-shared key. If the device is supported, and all the details of the device are correct, the device is registered.

FortiGate can also initiate a connection to the FortiAnalyzer **Security Fabric Authorization** window, log in to FortiAnalyzer, and approve devices.

DO NOT REPRINT

© FORTINET

Method 1: Request From a Supported Device—I

1. The FortiGate administrator enables remote logging to FortiAnalyzer

2. The FortiAnalyzer administrator accepts (or rejects) the registration request
 - If ADOMs are enabled, you must add the requesting device to the desired ADOM
 - Optionally, you can assign a new name to the device (not shown in the image)

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

5

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

In the first method, FortiGate requests registration on FortiAnalyzer by enabling FortiAnalyzer logging and entering its IP.

After you click **Apply**, and if the request reaches the FortiAnalyzer successfully, you receive a message asking you to confirm the serial number of the FortiAnalyzer device if **Verify FortiAnalyzer certificate** is enabled.

Note that if you click **Test Connectivity**, you will 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

- The FortiGate administrator enables the Security Fabric and enters FortiAnalyzer IP

Logging Settings

FortiAnalyzer Cloud Logging

Status Server Connection status

10.0.1.210

Upload option Real Time Every Minute Every 5 Minutes

Allow access to FortiGate REST API Verify FortiAnalyzer certificate FAZ-VM0000065040

Security Fabric > Fabric Connectors > Security Fabric Setup

Security Fabric Settings

Security Fabric role Standalone Serve as Fabric Root

Join Existing Fabric

Allow other Security Fabric devices to join port3

Fabric name Training

Device authorization 1 Connected / 1 Total Edit

- The FortiAnalyzer administrator accepts (or rejects) the registration request

- If ADOMs are enabled, you must add the requesting device to the desired ADOM
- Optionally, you can assign a new name to the device (not shown in the image)

Device Manager

Device Manager

ADOM: root 2 unauthorized device(s)

All Logging Devices Unauthorized Devices

Device Name	Platform	IP Address	Firmware Version
FortiFW	FortiGate-VM...	10.0.1.200	FortiGate 7.4.build2360
Local-FortiGate	FortiGate-VM...	10.0.1.254	FortiGate 7.4.build2360

Another method involves creating a Security Fabric. By enabling the Security Fabric on FortiGate, FortiAnalyzer logging is enabled by default. After configuring the FortiAnalyzer IP on the root FortiGate, all the fabric member devices receive the configuration for FortiAnalyzer, and they will all request to register. If **Verify FortiAnalyzer certificate** is enabled, you will need to confirm the FortiAnalyzer serial number on the root FortiGate.

While the registration requests of the fabric members are sent together, the FortiAnalyzer administrator must still review and authorize them individually. 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

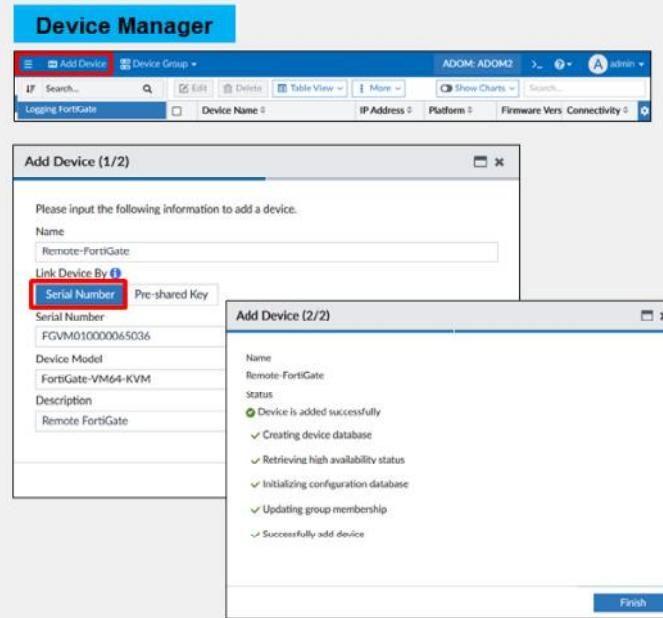
© FORTINET

Method 2: Add Device Wizard Using a Serial Number

- Add a device using **Device Manager**

- 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 that ADOM *before* adding a device using the wizard



FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

7

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 have 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

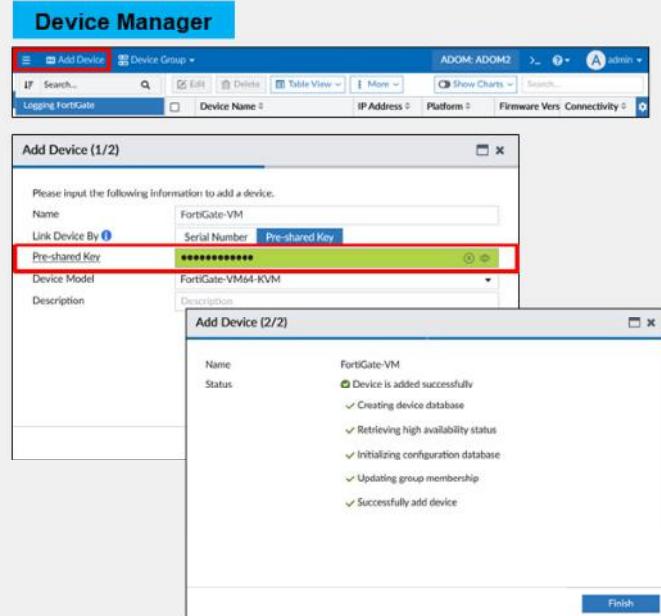
© FORTINET

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

- Switch to the desired ADOM *before* adding a device using the wizard



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 have 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

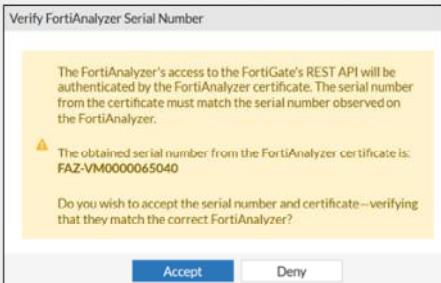
© FORTINET

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

3. Enter the pre-shared key on the FortiGate CLI

```
# config log fortianalyzer setting
  set status enable
  set server "<FortiAnalyzer IP>"
  set serial "<FortiAnalyzer Serial>"
  set preshared-key "<password>"
end
```

4. Authorize FortiAnalyzer on FortiGate



Next, configure the pre-shared key on the FortiGate CLI, along with the FortiAnalyzer IP address and serial number. After you configure the device, you need to verify the FortiAnalyzer serial number and authorize the connection if **Verify FortiAnalyzer certificate** is enabled on FortiGate.

Note that you can add only FortiGate devices using this method.

DO NOT REPRINT

© FORTINET

Method 4: Using Fortinet Security Fabric Authorization

1. Configure the FortiAnalyzer IP and port that will accept authorizations through fabric connectors
2. The FortiGate administrator enables the 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

Fabric Authorization

Authorization Address: 10.0.1.210
Authorization Port: 443

Note: This IP must be reachable from the management computer because a pop-up window will open

FortiAnalyzer

Status: Enabled
Server: 10.0.1.210
Connection status: Unauthorized
Upload option: Real Time / Every Minute / Every 5 Minutes

Confirm

FortiGate is unauthorized or denied on FortiAnalyzer. Would you like to open a window and authorize FortiGate on FortiAnalyzer?

OK **Cancel**

Fortinet Security Fabric

FortiAnalyzer VM44-KVM

Login

Select an action for the following unregistered devices.

FGVM0100000046692	Approve	Deny	Later
Local-FortiGate	10.0.1.254		
Model	FortiGate-VM44-KVM		
Management Mode	Logging Only		
Serial Number	FGVM0100000046692		
Firmware Version	FortiGate 7.4		

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

10

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

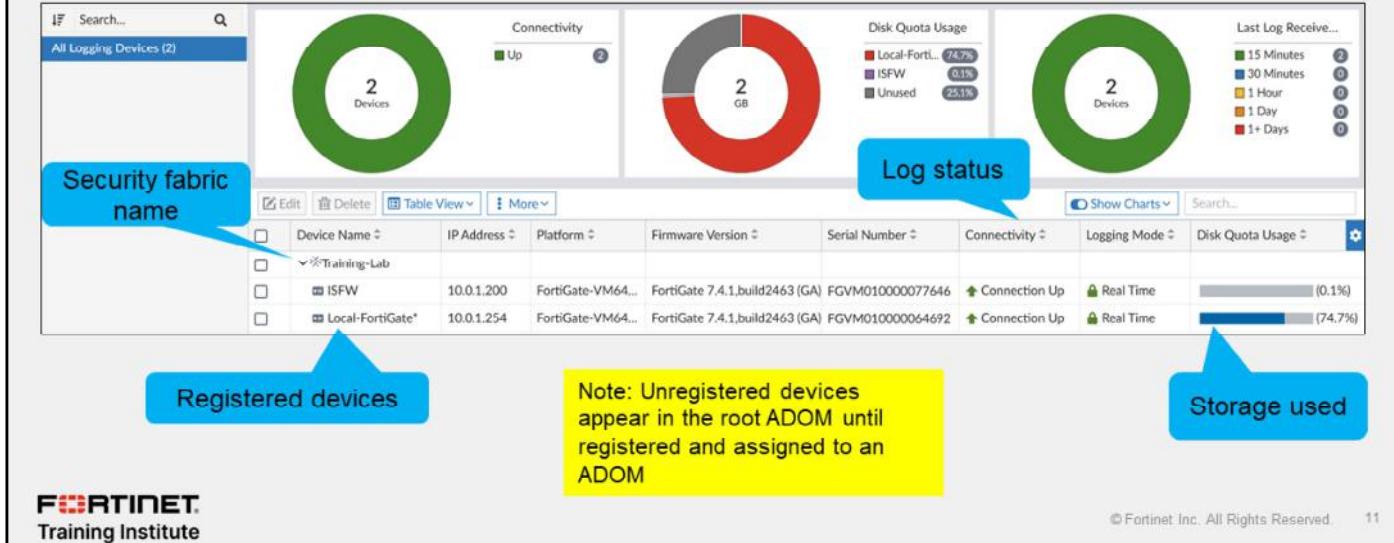
Next, the FortiGate administrator enables the Security Fabric to use FortiAnalyzer for logging, and then initiates the authorization process by clicking **OK** in the pop-up window shown in step 3. Alternatively, you can click on **Authorize** as shown in step 2.

The FortiGate administrator must have valid credentials on 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



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

Device Groups

- Create device groups to organize your devices in a logical and efficient manner

Default group

Custom group

Note: Device groups can be nested

All Logging Devices

Canada_Offices (0)

Ottawa_HQ

Toronto_Branch

OT

Only devices from the selected group are displayed

Add Device Device Group

Search... Edit Delete Table View More

All Logging Devices

Canada_Offices (0)

Ottawa_HQ

Toronto_Branch

© Fortinet Inc. All Rights Reserved. 12

By default, all registered devices are included in a default device group. You can create custom device groups for better organization and more efficient management of those devices. For example, you can create custom groups based on physical location and functionality.

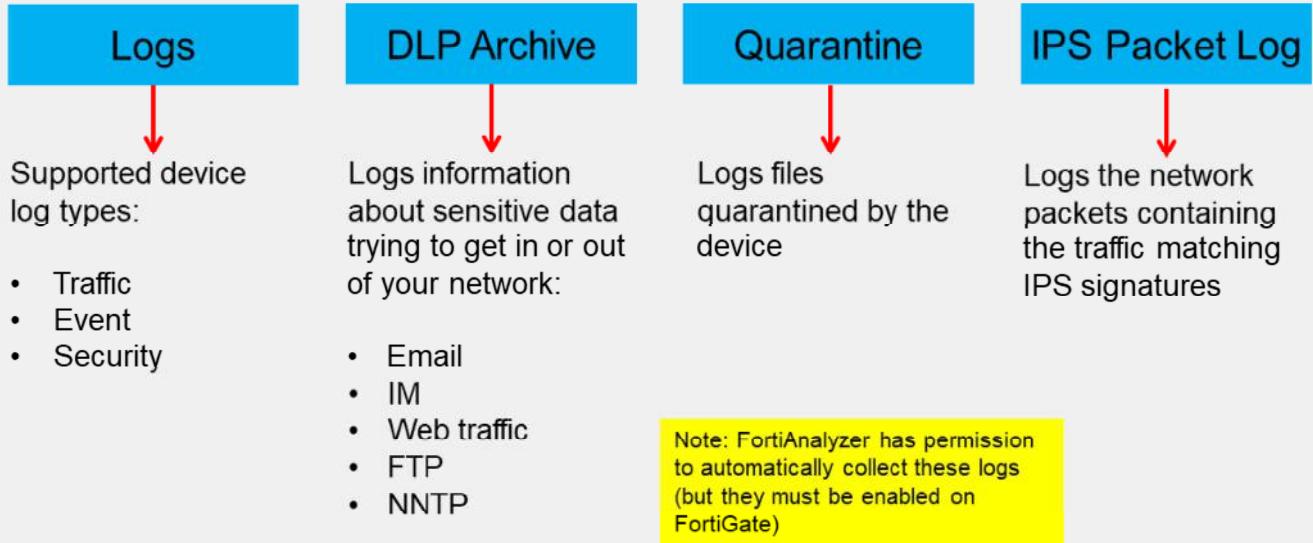
Additionally, if your environment justifies it, device groups can be nested. In the example shown on this slide, a device group named **Canada_Offices** contains a nested group with two branches.

Spaces are not allowed in the names of custom device groups.

DO NOT REPRINT

© FORTINET

Which Logs Are Collected From 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. Which statement about device registration is correct?
 - A. The logging device must initiate the registration request.
 - B. The logging device and FortiAnalyzer can both initiate the registration request.

DO NOT REPRINT

© FORTINET

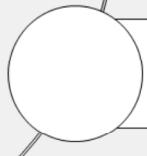
Lesson Progress



Registering Devices



Communication Troubleshooting



Managing Registered Devices

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

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

DO NOT REPRINT**© FORTINET**

Communication Troubleshooting

Objectives

- Troubleshoot device communication issues



© Fortinet Inc. All Rights Reserved.

16

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
Which processes are using the most resources?	# execute top



© Fortinet Inc. All Rights Reserved.

17

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

DO NOT REPRINT**© FORTINET****get system status: Helpful Troubleshooting Data**

```

FAZ # get system status
Platform Type : FAZVM64-KVM
Platform Full Name : FortiAnalyzer-VM64-KVM
Version : v7.4.1-build2308_230831 (GA)
Serial Number : FAZ-VM0000065040
BIOS version : 04000002
Hostname : FAZ
Max Number of Admin Domains : 5
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
HA Mode : Stand Alone
Branch Point : 2308
Release Version Information : GA
Current Time : Tue Oct 24 14:33:00 PDT 2023
Daylight Time Saving : Yes
Time Zone : (GMT-8:00) Pacific Time (US & Canada).
x86-64 Applications : Yes
Disk Usage : Free 53.15GB, Total 58.99GB
File System : Ext4
License Status : Valid

```



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 you are 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

```

FAZ # get sys performance
CPU:
Used: 37.77%
Used(Excluded NICE): 37.77%
%used %user %nice %sys %idle %iowait %irq %softirq
CPU0 42.29 18.54 0.00 22.92 57.71 0.62 0.00 0.21
CPU1 37.32 9.64 0.00 27.46 62.68 0.00 0.00 0.21
Memory:
Total: 10,264,016 KB
Used: 5,222,084 KB 50.9%
Total (Excluding Swap): 8,166,868 KB
Used (Excluding Swap): 5,222,084 KB 63.9%
Hard Disk:
Total: 61,857,580 KB
Used: 6,577,288 KB 10.6%
Inode-Total: 3,932,160
Inode-Used: 39,714 1.0%
IOStat: tps r_tps w_tps r_kB/s w_kB/s queue wait_ms svc_ms %util sampling_sec
       6.4   0.2   6.3    4.6   115.0   0.0     1.7    0.0     0.0      0.0   580831.56
Flash Disk:
Total: 1,007,512 KB
Used: 416,460 KB 41.3%
Inode-Total: 65,536
Inode-Used: 43 0.1%
IOStat: tps r_tps w_tps r_kB/s w_kB/s queue wait_ms svc_ms %util sampling_sec
       0.0   0.0   0.0    0.7   0.0     0.0     0.7    0.1    0.0      0.0   580831.57

```

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 does not need to be at 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.

For FortiAnalyzer VMs, note that a minimum of 16 GB memory is recommended.

DO NOT REPRINT

© FORTINET

diagnose hardware info: Helpful Troubleshooting Data

FAZ # diagnose hardware info		### Memory info	### Disk info
### CPU info		MemTotal:	major minor #blocks name
processor	: 0	MemFree:	4096 ram0
vendor_id	: GenuineIntel	MemAvailable:	4096 ram1
cpu family	: 6	Buffers:	4096 ram2
model	: 63	Cached:	4096 ram3
model name	: Intel(R) Xeon(R) CPU E5-2680 v3 @ 2.50GHz	SwapCached:	4096 loop0
stepping	: 0	Active:	4096 loop0
microcode	: 0x1	Inactive:	4096 loop0
cpu MHz	: 2500.000	Active(anon):	4096 vda
cache size	: 16384 KB	Inactive(anon):	4096 vda1
physical id	: 0	Active(file):	4096 vdb
siblings	: 1	Inactive(file):	4096 vdb
core id	: 0	Unevictable:	4096 vdb
cpu cores	: 1	Mlocked:	N/A
apicid	: 0	SwapTotal:	4096 RAID info
initial apicid	: 0	SwapFree:	4096 System time
fpu	: yes	AnonPages:	local time: Tue Jul 4 10:25:55
fpu_exception	: yes	Mapped:	2023
cpuid level	: 13	Shmem:	UTC time: Tue Jul 4 17:25:55 2023
wp	: yes	PageTables:	
flags	: fpu vme de pse tsc msr pae mce cx8	CommitLimit:	
bugs	: cpu_meltdown spectre_v1 spectre_v2	Committed_AS:	
spec_store_bypass_l1tf l1tf mds swapgs itlb_multihit		VmallocTotal:	

Note: This slide does not show the complete output of the command

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 the `get system performance` command 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

execute top: Helpful Troubleshooting Data

top - 11:03:59 up 19:30, 0 users, load average: 0.29, 0.27, 0.22								
Tasks: 245 total, 1 running, 244 sleeping, 0 stopped, 0 zombie								
%Cpu(s): 1.8/1.0 3[]								
FID	USER	PR	NI	VIRT	RES	%CPU	%MEM	TIME+ S COMMAND
2585	root	20	0	165.3m	133.2m	2.6	0.8	34:19.03 S /bin/python /u
1025	root	20	0	97.6m	39.0m	1.3	0.2	11:04.17 S forticlidd.main
1032	root	20	0	833.3m	105.2m	1.3	0.7	12:36.29 S oftpd
3486	postgres	20	0	2844.2m	30.5m	1.0	0.2	0:20.11 S postgres
249	root	20	0	87.6m	35.1m	0.7	0.2	5:06.77 S cmdbsvr
1028	root	20	0	395.1m	39.2m	0.7	0.2	10:54.60 S logfwd.main
2607	root	20	0	158.6m	128.2m	0.7	0.8	7:22.42 S airflow schedul
8	root	20	0	0.0m	0.0m	0.3	0.0	1:27.66 I rcu_sched

Note: This slide does not show the complete output of the command

The execute top command provides real-time information about processes on FortiAnalyzer. You can see the process ID, CPU usage, memory usage, and other fields for each process. If you see high resource usage from the get system performance command, you can use execute top to look deeper into how the resources are allocated.

You can press h while the command is running to bring up a help window, which lists common shortcuts and their descriptions. Depending on which shortcut you press, you can sort by different criteria or toggle different summaries.

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 or 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 IP addresses 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
Is FortiAnalyzer receiving logs?	# diagnose debug application oftpd 8
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?	FortiGate: # show log fortianalyzer filter
Is FortiGate capable of generating logs?	FortiGate: # diagnose log test



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).

Other questions to ask:

- Is FortiGate configured for remote logging to FortiAnalyzer?
- Is the FortiAnalyzer receiving logs? You can run an `oftpd` debug to verify log forwarding.
- Is the FortiAnalyzer source IP set on FortiGate? This is important if FortiAnalyzer is accessed over a VPN that allows only 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

Troubleshooting Communication Issues (Contd)

What to Investigate	CLI Command to Use
Are packets leaving FortiGate, but not reaching FortiAnalyzer? Is traffic blocked? Is there a routing issue?	# diagnose sniff packet <interface> <filter> <level> <count> <timestampl>

- Example output

```
FAZ# diag sniffer packet port1 'udp and port 53' 1 4 1
interfaces=[port1]
filters=[udp and port 53]
2023-06-28 16:29:17.741947 192.168.42.210.14610 -> 208.91.112.52.53: udp 27
2023-06-28 16:29:17.742016 192.168.42.210.14610 -> 208.91.112.52.53: udp 27
2023-06-28 16:29:17.745001 208.91.112.52.53 -> 192.168.42.210.14610: udp 155
2023-06-28 16:29:17.745047 208.91.112.52.53 -> 192.168.42.210.14610: udp 195
```

System Settings > Network

Create New Edit Delete						Search...
Interface	Filter Criteria	# Packets	Max Packet Count	Progress	Actions	
port1	port=53	4	4000	(4/4000)		

Can also capture using the GUI

You can also run sniffers 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.

FortiAnalyzer has a built-in packet sniffer, available on the GUI and CLI. It supports versatile filters and verbosity (1-3) levels. The higher the verbosity level, the more information the capture contains. For troubleshooting purposes, Fortinet Technical Support may request level 3 captures.

In the CLI example shown on this slide, the capture has the following characteristics:

- Traffic on port1
- UDP port 53 (DNS traffic)
- Level 1 verbosity
- Capture limit of four packets
- Local time

For more syntax information, consult the *CLI Reference* guide for FortiAnalyzer on docs.fortinet.com.

DO NOT REPRINT

© FORTINET

Troubleshooting Communication Steps

1- Debug the `oftpd` process

```
FortiAnalyzer # diagnose debug application oftpd 8

[OFTP_destroy_SSL_context:1898 FGVM010000064692] SSL socket[24] pid[988] ssl[0x162d260]
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:
```

2- Generate test logs on FortiGate

```
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
```

Verify logs are received in
FortiAnalyzer

Note: The debug command in FortiAnalyzer must be running before you generate the test logs in FortiGate.

3- Verify logs are received



© Fortinet Inc. All Rights Reserved.

25

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

1. Run the `diagnose debug application oftpd 8` command on FortiAnalyzer to view current log activity.
2. Run the `diagnose log test` command on FortiGate to send some test logs to FortiAnalyzer.
3. 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 the FortiAnalyzer connection is restored, *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

```
Remote-FortiGate # diagnose test application miglogd 6
mem=0, disk=9036, alert=0, alarm=0, sys=0, faz=3113, faz-cloud=0, webt=0, fds=0
interface-missed=170
Remote-FortiGate # diagnose test application fgtlogd 4
Queues in all miglogds: cur:0 total-so-far:23437
global log dev statistics:
faz=3115, faz_cloud=0, fds_log=0
faz 0: sent=3087, failed=0, cached=0 dropped=0
```

Current cache size and total cache size

If there are bursts or the link is overloaded, failed increases; if the FortiAnalyzer is unavailable, cached increases

```
Remote-FortiGate # diagnose log kernel-stats
fgtlog: 1
fgtlog 0: total-log=16838, failed-log=0 log-in-queue=0
```

If the queue is full, failed-log value increases

If FortiAnalyzer becomes unavailable to FortiGate for any reason, 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 restart of FortiAnalyzer (if you are upgrading the firmware, for example). This is not intended for a lengthy FortiAnalyzer outage.

On FortiGate, the CLI commands `diagnose test application miglogd 6` and `diagnose test application fgtlogd 4` display logging statistics, including the current cache size and maximum 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 after 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 determine?
 A. That ADOMs are enabled and configured
 B. The devices and IP addresses that are connecting to FortiAnalyzer

DO NOT REPRINT

© FORTINET

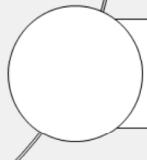
Lesson Progress



Registering Devices



Communication Troubleshooting



Managing Registered Devices

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

Now, you will learn how to manage registered devices.

DO NOT REPRINT**© FORTINET**

Managing Registered Devices

Objectives

- Move registered devices between ADOMs
- Add FortiGate devices in an HA cluster to FortiAnalyzer



© Fortinet Inc. All Rights Reserved.

29

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 FortiGate devices in an HA cluster, 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
- You 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
Remote-FortiGate	7.4	ADOM2
FortiGate-VM64-KVM, 10.200.3.1		

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 30

You can move devices between ADOMs after registration on the **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 you want to add the device to, and then selecting the device 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
- 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 not, you need to rebuild the old ADOM SQL database. Otherwise, they are removed according to the data policy.

DO NOT REPRINT

© FORTINET

Adding a FortiGate HA Cluster

- FortiAnalyzer automatically discovers if a FortiGate device is in an HA cluster
 - If devices were registered to FortiAnalyzer before forming a cluster, you can manually add them together
- In an HA cluster, each device generates its own logs (separate serial number in logs)
 - The primary device is responsible for sending all logs from the other devices to FortiAnalyzer
- FortiAnalyzer distinguishes different devices by their serial number
 - Serial numbers are located in log message headers

HA			
HA Cluster	From Existing Devices	HA Member	Action
HA Cluster List		Local-FortiGate (FGVM010000064692)	<input type="button" value="+"/>
		Remote-FortiGate (FGVM010000065036)	<input type="button" value="x"/> <input type="button" value="+"/>

Edit in Device Manager

FortiAnalyzer automatically discovers if a FortiGate device is in an HA cluster. However, if you register your device with FortiAnalyzer before adding it to a cluster, you can manually add the cluster within FortiAnalyzer.

In 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 **HA Cluster**. 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 log messages it receives.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. When you move a FortiGate device from one ADOM to a new ADOM, which type of log is migrated to the new ADOM without requiring a SQL database rebuild?
 A. Archive logs
 B. Analytic logs

DO NOT REPRINT

© FORTINET

Lesson Progress



Registering Devices



Communication Troubleshooting



Managing Registered Devices

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
- ✓ Create device groups
- ✓ Troubleshoot device communication issues
- ✓ Move registered devices between ADOMs
- ✓ Add devices in an HA cluster to FortiAnalyzer

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 Administrator

Logs and Reports Management

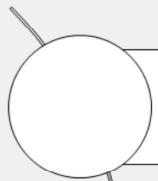
FortiAnalyzer 7.4.1

Last Modified: 19 December 2023

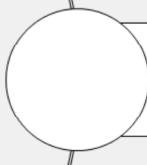
In this lesson, you will learn how to protect and manage logs on FortiAnalyzer. You will also learn about basic report concepts and common report management tasks.

DO NOT REPRINT**© FORTINET**

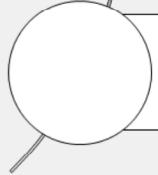
Lesson Overview



Managing Log Data



Reports Concepts



Managing Reports

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

DO NOT REPRINT**© FORTINET**

Managing Log Data

Objectives

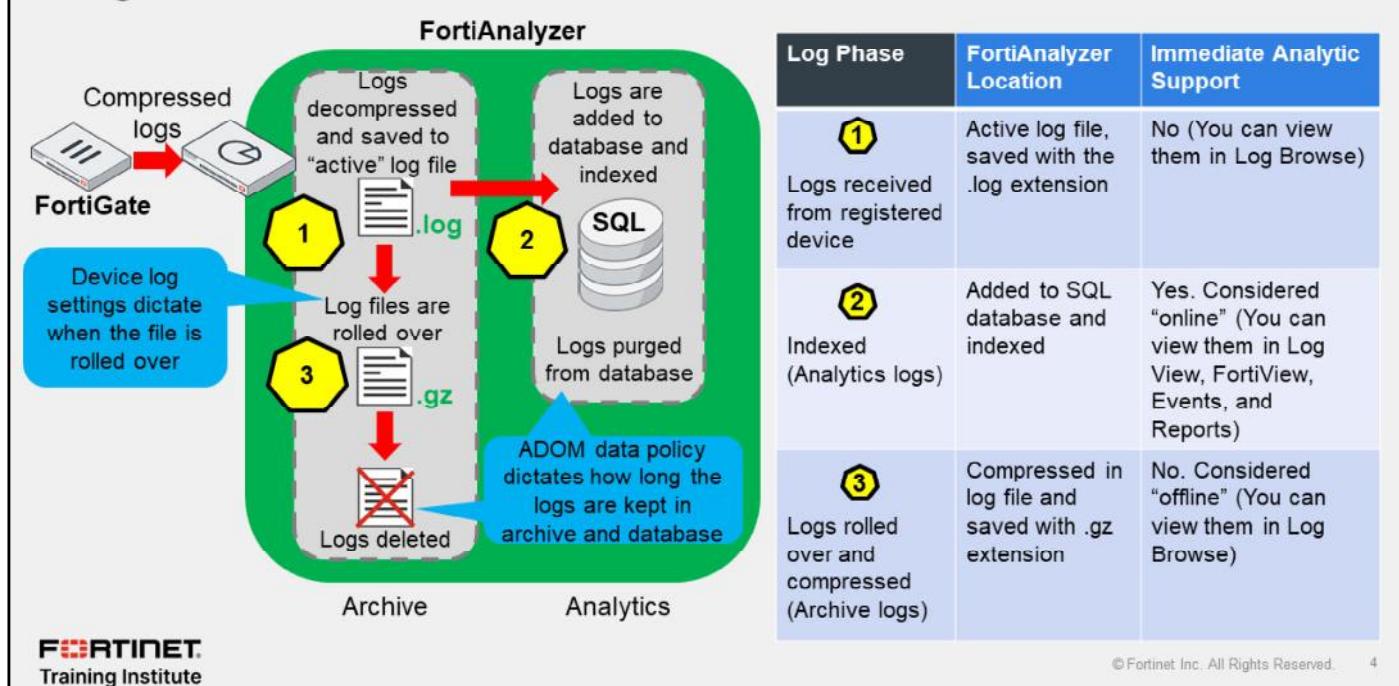
- Describe the log file workflow
- Perform log backups
- Understand fabric connectors
- Configure log redundancy
- Configure log encryption
- Configure a log roll-over and retention policy

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

By demonstrating competence in understanding the log file workflow and the different ways you can protect your log data, you will be able to meet organizational and legal requirements for logs.

DO NOT REPRINT
© FORTINET

Log File Workflow



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

1. Logs received are decompressed and saved in a log file on the FortiAnalyzer disk. The log file has the extension `.log`. For example, FortiAnalyzer saves FortiGate logs with the names `tlog.log` and `elog.log`, for traffic and event logs, respectively. Note that the `tlog.log` file includes FortiGate security logs.
2. At the same time, FortiAnalyzer indexes the saved logs in the SQL database to support analysis. Logs in the indexed phase are known as *analytics* logs. These logs are considered online and offer immediate analytic support. You can view these logs using **Log View**, **FortiView**, **Incident & Events**, and **Reports**. FortiAnalyzer purges analytics logs from the SQL database as specified in the ADOM data policy.
3. Eventually, when the log file reaches a configured size, or at a set schedule, it is rolled over. The process of rolling over consists of renaming the file, adding a timestamp, and then compressing it, which adds the `.gz` extension. These files 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 FortiAnalyzer deletes them based on the ADOM data policy. You can view these logs using **Log Browse**.

DO NOT REPRINT

© FORTINET

Log Backup

- Protect log data from disk failure, deletion, or corruption
- Backup mechanisms include:
 - Using the GUI or CLI
 - GUI (**Log View**) provides control to download a specific filtered view →
 - GUI (**Log Browse**) provides rolled log download (can schedule upload of logs via **System Settings > Advanced > Device Log Settings**) ↓

Log View > Log Browse

All Devices									Last 1 Day	Jul 10 To Jul 11	Display	Delete	Download	Import
logtype_name != VoIP													x' Q	
Device Name	Device ID	VDOM Name	Type	File Name	From	To	Size	Checksum						
Local-FortiGate	FGVM010000064692	root	Traffic	tlog.log	2023-07-09 00:03...	2023-07-11 10:48:52	3,082,708							

- CLI more suitable for bulk data dumps

```
# execute backup logs <device name|all> <ftp|sftp|scp> <server IP> <user> <password> <file path>
```

Includes logs, archives, and quarantine (use logs-only if only log files needed)

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

5

You should not consider RAID as 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. FortiAnalyzer compresses the data before sending, 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 also restore logs using the GUI and the CLI.

DO NOT REPRINT
© FORTINET

Log Backup (Contd)

- You can configure logs to upload to a remote server whenever a log file is rolled, or per a daily schedule

System Settings > Advanced > Device Log Settings

The screenshot shows the 'Device Log Settings' configuration page. It includes fields for 'Upload logs using a standard file transfer protocol' (selected), 'Upload Server Type' (set to 'FTP'), 'Upload Server' (IP address '10.0.1.10'), 'User Name' ('admin'), 'Password' (redacted), 'Remote Directory' ('/logs'), 'Upload Log Files' (selected), 'Upload log files in compressed file format' (selected), and 'Delete log files after uploading' (selected). A tooltip indicates that supported protocols are FTP/SFTP/SCP.

Supported protocols are FTP/SFTP/SCP

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved.

6

You can configure FortiAnalyzer to upload logs to a remote server whenever a log file is rolled, or based on a daily schedule.

The supported protocols for the remote server are FTP, SFTP, and SCP.

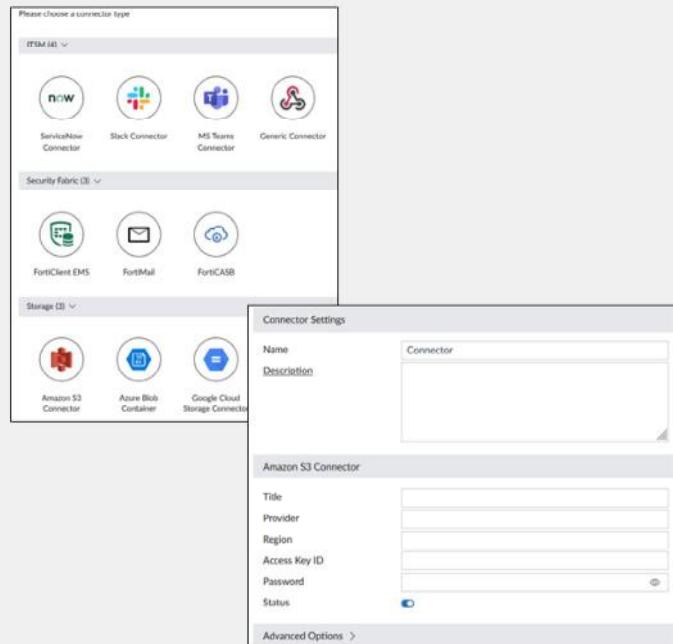
If you enable **Upload log files in compressed file format**, the device log files are compressed before uploading, which results in smaller logs and faster upload times.

If you enable **Delete log files are uploading**, the device log files are removed from FortiAnalyzer after they have been uploaded to the server.

DO NOT REPRINT**© FORTINET**

Fabric Connectors

- Configure FortiAnalyzer to send logs or notification events to:
 - External cloud platforms: AWS, Azure, Google
 - ITSM: ServiceNow, Slack, MS Teams, Webhook
 - Security Fabric: FortiClient EMS, FortiMail, FortiCASB
- Improve data redundancy
- Reduce performance degradation
- Enrich incident response actions



© Fortinet Inc. All Rights Reserved.

7

FORTINET
Training Institute

FortiAnalyzer supports integration with other products through fabric connectors.

Storage connectors allow you to back up data 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.

ITSM connectors 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 FortiAnalyzer, such as automating actions by triggering playbooks.

DO NOT REPRINT
© FORTINET

Storage Connector Service

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

License Information

VM License: Valid 10K-UG

FortiGuard

Indicators of Compromise: Licensed (Expires 2024-06-04)

Outbreak Detection: Licensed (Expires 2024-06-04)

Security Automation: Licensed (Expires 2024-06-04)

Industrial Security: Licensed (Expires 2024-06-04)

Security Rating Updates: Licensed (Expires 2024-06-04)

Server Location: Servers located in US only

Storage Connector Service

Cloud: 37.1 GB / 10.0 TB (0.0%)

Update Servers

Upload logs to cloud storage

Name	Cloud Storage Connector	Upload Option	Remote Path
AWSStorage	AWSConnector	On Rolling	fazvmwest
AzureStorage	AzureConnector	On Rolling	fazfabriccontainer
GoogleStorage	GoogleConnector	On Rolling	fazfabricbucket

FORTINET.
Training Institute

```
# diagnose fmupdate dbcontract
FAZ-VMTM23008175 [SERIAL_NO]
AccountID: *****@fortinet.com
Industry: Technology
Company: Fortinet
Contract: 10
ENHN-1-10-20240604
FGSA-1-06-20240604
FMWR-1-06-20240604
FOAS-1-06-20240604
FRVS-1-06-20240604
ISSS-1-06-20240604
PBDS-1-06-20240604
SCPC-1-06-20230912
SOAR-1-06-20240604
SPRT-1-10-20240604
```

```
# diagnose test application uploadd 63
Cloud Storage Usage:
Status:
    Expire in: 61 days 12 hours 30 minutes
Usage:
    Total Gigabytes Uploaded: 37 GB
    Number of Files Uploaded: 10226 Files
    Quota: 10 TB
    Number of Upload Requests Dropped: 0 Requests
```

© Fortinet Inc. All Rights Reserved.

8

In order to send logs to cloud platforms, you must purchase 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 you can send the storage data. This is usually 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 > Advanced > 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.

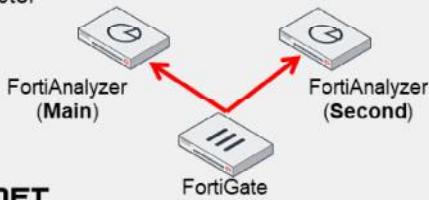
DO NOT REPRINT

© FORTINET

Log Redundancy Options

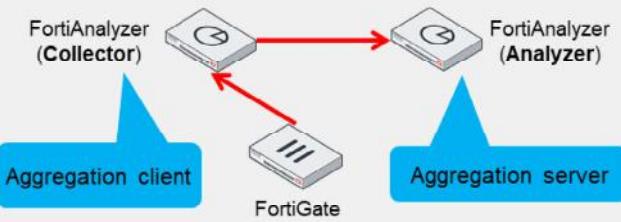
1. FortiAnalyzer HA cluster
 - Real-time redundancy when primary fails
 - Log and configuration synchronization

2. Send identical logs to a second logging server
 - FortiAnalyzer or syslog
 - CPU, RAM load is higher on FortiGate (more if SSL is 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



FORTINET
Training Institute

3. 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 analyzer fails, collector sends all the data and repopulates the analyzer automatically
 - Aggregation mode supported only between two FortiAnalyzers



© Fortinet Inc. All Rights Reserved. 9

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 HA cluster is selected as the primary device. It synchronizes logs and data securely among multiple FortiAnalyzer devices. It also synchronizes system and configuration settings applicable to HA, and 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 server. 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 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 reduces the amount of traffic that is sent, and provides a level of redundancy. If there is a 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

- Set log forwarding mode

```
# config system log-forward
  edit <log forwarding 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

- Configure the server (FortiAnalyzer or syslog/CEF that receives logs)

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

- 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. In forwarding mode, FortiAnalyzer can also forward logs in real-time mode to a syslog server (such as FortiSIEM), a Common Event Format (CEF) server, or another FortiAnalyzer. You can also forward logs to a public cloud service through an output plugin. 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.
 - Aggregation mode stores logs and content files and uploads them to the FortiAnalyzer server at a scheduled time.
- Configure the server (the log recipient). Forwarding mode only requires configuration on the client side. In aggregation mode, the FortiAnalyzer acting as the server must be configured to accept the logs from the client.
- Configure the client (the FortiAnalyzer forwarding the logs). Here you can also specify which device logs to forward and set log filters to send only 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 is 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 uses the OFTPS protocol only if being used by the connecting FortiGate

FortiGate:

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

Logs also use TCP/514 once enabled

FortiGate:

```
# 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)

FortiAnalyzer:

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

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

You can protect log communication between devices by encryption, with the desired encryption level, using the commands shown on the slide. After you enable secure log transfer, logs are transferred between FortiGate and FortiAnalyzer using port TCP/514 as well.

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. If you set the algorithm to *custom* on FortiAnalyzer, you can manually define a list of cipher suites.

DO NOT REPRINT
© FORTINET

Preventing Log Modification

- To prevent log modification, you can add a log checksum
- 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 mode custom
    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 need a Privacy-Enhanced Mail (PEM) formatted certificate and associated PEM-formatted private key.

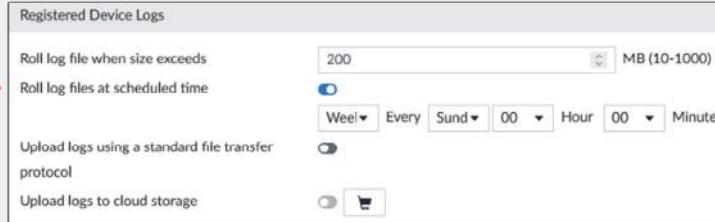
DO NOT REPRINT
© FORTINET

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



The screenshot shows the 'Device Log Settings' page under 'System Settings > Advanced'. It has two main sections: 'Registered Device Logs' and 'Automatically Delete'. In 'Registered Device Logs', there are options to 'Roll log file when size exceeds' (set to 200 MB) and 'Roll log files at scheduled time' (set to every Sunday at 00:00). In 'Automatically Delete', there are four entries: 'Device log files older than 365 Days' (Scheduled daily at 00:00), 'Reports older than 365 Days' (Scheduled daily at 00:00), 'Content archive files older than 365 Days' (Scheduled daily at 00:00), and 'Quarantined files older than 365 Days' (Scheduled daily at 00:00).

- Automatically delete logs of a specified age

FORTINET
Training Institute

© Fortinet Inc. All Rights Reserved. 13

Aside from changing your disk log quota, you can enforce global settings to help manage your logs.

You can configure the following:

- 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.

All deletion policies are active on the FortiAnalyzer unit at all times. Therefore, you should carefully configure each policy. For example, if the disk utilization policy reaches its threshold before the global automatic file deletion policy for the FortiAnalyzer device, FortiAnalyzer automatically deletes the archive logs for the affected device. Conversely, if the global automatic file deletion policy reaches its threshold first, FortiAnalyzer deletes the oldest archive logs regardless of the log storage settings associated with the device.

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. Compressed logs on FortiAnalyzer are known as _____ logs.
 A. Archive logs
 B. Analytics logs

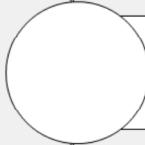
DO NOT REPRINT

© FORTINET

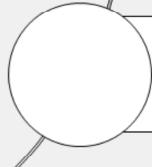
Lesson Overview



Managing Log Data



Reports Concepts



Managing Reports

Good job! You now understand how to manage your log data.

Now you will learn about basic report concepts.

DO NOT REPRINT**© FORTINET**

Reports Concepts

Objectives

- Describe the elements that constitute a report
- Describe how reports function within ADOMs



© Fortinet Inc. All Rights Reserved.

16

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 retrieves the information collected from the log files of managed devices and presents it in tabular and graphical reports
- Reports provide a quick and detailed analysis of activity on your network

Default reports categories

	Application Reports
	Asset and User Reports
	Compliance Reports
	Fabric Reports
	FortiCache Reports
	FortiClient Reports
	FortiDoS Reports
	FortiDeceptor Reports
	FortiFirewall Reports
	FortiGate Reports
	FortiMail Reports
	FortiNAC Reports
	FortiNDR Reports
	FortiProxy Reports
	FortiSandbox Reports
	FortiWeb Reports
	Network Reports
	Outbreak Alert Reports
	SOC Reports
	Daily Summary Report

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 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 generally 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

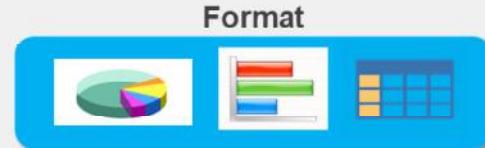
- A FortiAnalyzer report is a set of data in organized charts



- What **data** from the SQL database is displayed
- What **format** the data is displayed in



Datasets are specific SQL SELECT queries



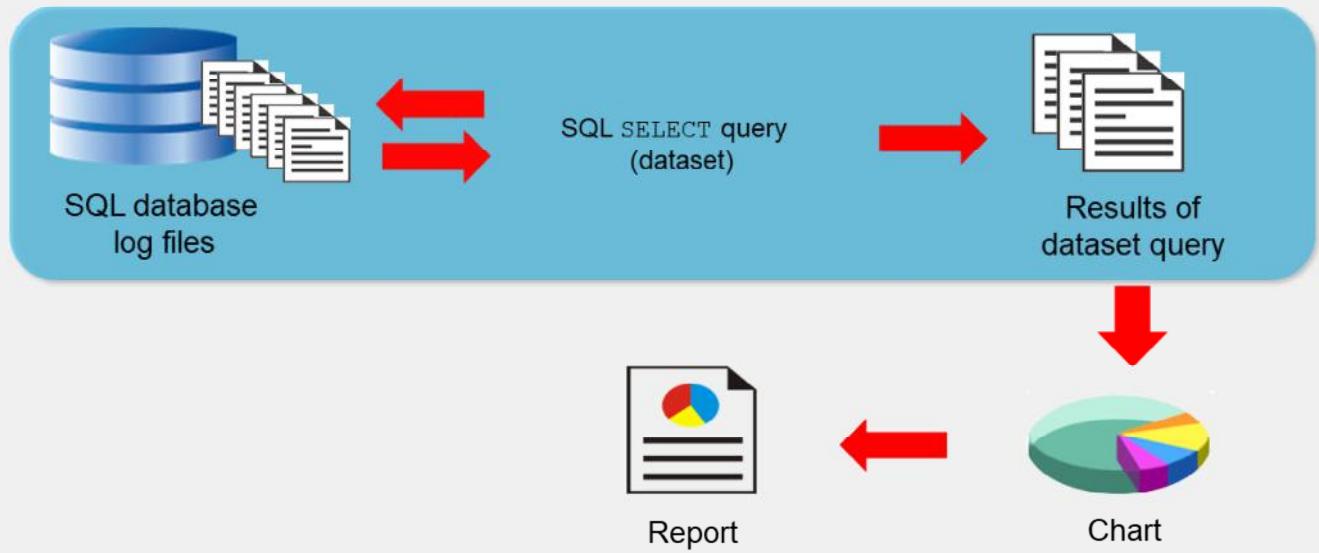
Format options include:
pie charts, bar charts, or tables

A FortiAnalyzer report is a set of data organized in charts. Charts consist of two elements:

- Datasets:** 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**

Report Workflow



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 are available when specific ADOMs are enabled
- Verify you are in the right ADOM when creating reports

Note: A fabric ADOM has default reports for multiple device types

<input type="checkbox"/>	Title
<input type="checkbox"/>	Application Reports
<input type="checkbox"/>	Asset and User Reports
<input type="checkbox"/>	Compliance Reports
<input type="checkbox"/>	Fabric Reports
<input type="checkbox"/>	FortiCache Reports
<input type="checkbox"/>	FortiClient Reports
<input type="checkbox"/>	FortiDDoS Reports
<input type="checkbox"/>	FortiDeceptor Reports
<input type="checkbox"/>	FortiFirewall Reports
<input type="checkbox"/>	FortiGate Reports

When you enable ADOMs, 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 you enable ADOMs. This slide does not show all the available default report types. 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

Knowledge Check

1. On FortiAnalyzer, what is a dataset?
 - A. The database schema available to perform queries
 - B. A specific SQL SELECT query that retrieves data from the database

DO NOT REPRINT

© FORTINET

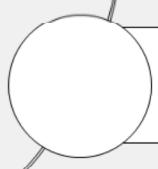
Lesson Overview



Managing Log Data



Reports Concepts



Managing Reports

Good job! You now understand the basic concepts of reports on FortiAnalyzer.

Now, you will learn how to manage reports.

DO NOT REPRINT**© FORTINET**

Managing Reports

Objectives

- Configure external storage for reports
- Enable auto-cache



© Fortinet Inc. All Rights Reserved. 23

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

Configure External Storage for Reports

- Send or store reports externally for backup purposes
- Requires configuration of a mail server to email reports
- Can also upload generated reports to a server (FTP/SFTP/SCP)

System Settings > Advanced > Mail Server

Edit Mail Server Settings	
SMTP Server Name	Mail_Server
Mail Server	10.200.1.254
SMTP Server Port	25
Enable Authentication	<input checked="" type="checkbox"/>
E-Mail Account	admin@training.lab
Password	*****
From (Optional)	

You can configure FortiAnalyzer to email generated reports to specific administrators, or to upload generated reports to an external server.

In order to use any of these external storage methods, you must first set up the back end. To email generated reports, you must first configure a mail server, as shown on this slide. To upload logs to a server, you must first configure the mail server to accept connections from FortiAnalyzer.

DO NOT REPRINT
© FORTINET

Configure External Storage for Reports (Contd)

- Configure output profiles per ADOM
- Email reports or upload to server (HTML, PDF, XML, CSV, and JSON)
- First configure an output profile, then enable notifications for each report

Reports > Report Definitions > All Reports

Enable Notification <input checked="" type="checkbox"/>	Output Profile Email Profile
---	------------------------------

Reports > Advanced Settings > Output Profile

Name: Email Profile
Comments:
Output Format: HTML PDF XML CSV JSON
 Email Generated Reports
Subject: Generated Reports
Body: Please review these reports
27/1023
Recipients: Email Server
Mail_Server: 10.200.1.254
From: admin@training.lab
To: admin@training.lab
Action: + x +
 Upload Report to Server
Server Type: **FTP**
Server: 10.1.1.1
User: user
Password: *********
Directory: reports
 Delete file(s) after uploading

© Fortinet Inc. All Rights Reserved.

25

FORTINET
Training Institute

To send reports to an external location, each report must have notifications enabled and an appropriate output profile selected.

An output profile specifies the following:

- The format of the report, such as HTML, PDF, XML, CSV, and JSON
- Whether to email generated reports or upload to a server. You can specify one option, both, or create multiple output profiles. Server options include FTP, SFTP, and SCP.
- Whether to delete the report locally after uploading to the server

If you enable ADOMs, each ADOM has its own output profiles.

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
 - The hcache automatically updates when new logs come in and FortiAnalyzer generates new log tables
- 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)

Reports > Report Definitions > All Reports

Generated Reports Settings Editor

Enable Auto-cache

Extended Log Filtering

Default Filtering Device Source IP Destination IP Endpoint ID Source End User ID

Additional Log Fields

Policy Name (policyname)

1 entry selected

Enable **Extended Log Filtering** to cache specific log fields for faster filtering

Note: Hcache is automatically enabled for scheduled reports

FORTINET.
Training Institute

© Fortinet Inc. All Rights Reserved. 26

When a report generates, the system builds the charts from precompiled SQL hard-cache data, known as the 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 FortiAnalyzer does not receive any new logs 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. Monitor your system to ensure it can handle it.

Additionally, you can opt for enabling **Extended Log Filtering** to cache specific log fields for faster filtering.

DO NOT REPRINT**© FORTINET**

Knowledge Check

1. What is a benefit of enabling hcache in FortiAnalyzer reports?
 A. Increase the efficiency of the storage used by reports
 B. Reduce the time required to generate reports

DO NOT REPRINT

© FORTINET

Lesson Overview



Managing Log Data



Reports Concepts



Managing Reports

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 log file workflow
- ✓ Perform log backups
- ✓ Understand fabric connectors
- ✓ Configure log redundancy
- ✓ Configure log encryption
- ✓ Configure a log roll-over and retention policy
- ✓ Describe the elements that constitute a report
- ✓ Describe how reports function within ADOMs
- ✓ Configure external storage for reports
- ✓ Enable auto-cache



© Fortinet Inc. All Rights Reserved. 29

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

By mastering the objectives covered in this lesson, you learned how to manage the log data and reports on FortiAnalyzer.

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© 2023 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.