

FCP_FAZ_AD-7.4 Dumps

FCP - FortiAnalyzer 7.4 Administrator

https://www.certleader.com/FCP_FAZ_AD-7.4-dumps.html



NEW QUESTION 1

An administrator has moved a FortiGate device from the root ADOM to ADOM1. Which two statements are true regarding logs? (Choose two.)

- A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.
- B. Archived logs will be moved to ADOM1 from the root ADOM automatically.
- C. Logs will be present in both ADOMs immediately after the move.
- D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the database.

Answer: AD

Explanation:

When a device is moved from one ADOM to another, analytics logs can be moved automatically, but you may need to rebuild the database for the logs to be fully transferred and usable in the new ADOM. Archived logs, however, do not move automatically between ADOMs.

NEW QUESTION 2

What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

- A. There is no need to do anything because the disk will self-recover.
- B. Run execute format disk to format and restart the FortiAnalyzer device.
- C. Perform a hot swap of the disk.
- D. Shut down FortiAnalyzer and replace the disk.

Answer: C

Explanation:

In a hardware RAID setup, FortiAnalyzer supports hot swapping, which allows you to replace a failed disk without shutting down the device. The RAID controller will automatically rebuild the array using the new disk, minimizing downtime and maintaining data integrity.

NEW QUESTION 3

Refer to the exhibit.

```
FortiGate # diagnose test application fgtlogd 4
Queues in all miglogds: cur:31 total-so-far:4642589
global log dev statistics:
faz=180191781, faz_cloud=0, fds_log=0
faz 0: sent=180189698, failed=4507, cached=0, dropped=0
```

Based on the output, what can you conclude about the FortiAnalyzer logging status?

- A. The connection between FortiGate and FortiAnalyzer is overloaded.
- B. FortiGate has logs to send, but FortiAnalyzer is unavailable.
- C. FortiGate is configured to send logs in batches.
- D. FortiGate is sending logs again after it performed a reboot.

Answer: B

Explanation:

The output shows that FortiGate has sent a large number of logs (sent=180189698), but some logs have failed to be sent (failed=4507). This suggests that FortiAnalyzer was temporarily unavailable or had an issue receiving logs, leading to the failure count. There are no logs cached or dropped, indicating FortiGate is still attempting to send logs but with some failures.

NEW QUESTION 4

Refer to the exhibit, which shows the HA configuration settings of a FortiAnalyzer device.

FortiAnalyzer HA cluster settings

Cluster Settings

Operation Mode

StandaloneActive-PassiveActive-Active

Preferred Role

SecondaryPrimary

Cluster Virtual IP

IP Address and Interface

IP Address

Interface

Action

192.168.101.222

port1

✕

+

Cluster Settings

Peer IP and Peer SN

Peer IP

Peer SN

Action

10.0.1.210

FAZ-VM0000065040

✕

+

Group Name

Training

Group ID

1

(1-255)

Password

••••••••

🔒

Heart Beat Interval

10

Seconds

Heart Beat Interface

port1

▼

Failover Threshold

30

Priority

120

(80-120)

Log Data Sync

☒

The administrator wants to join this FortiAnalyzer to an existing HA cluster. What can you conclude from the configuration displayed?

- A. After joining the cluster, this FortiAnalyzer will forward received logs to its peers.
- B. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
- C. This FortiAnalyzer is configured to route HA traffic through a gateway.
- D. This FortiAnalyzer will join the existing HA cluster as the secondary.

Answer: B

Explanation:

The "Preferred Role" is set to Secondary, which means this FortiAnalyzer is configured to join the cluster as the secondary unit in an Active-Passive HA configuration. Other settings, such as the peer IP and serial number, confirm its setup to communicate with the primary unit.

NEW QUESTION 5

Which two statements about FortiAnalyzer operating modes are true? (Choose two.)

- A. When in collector mode, FortiAnalyzer offloads the log receiving task to the analyzer.
- B. When in analyzer mode, FortiAnalyzer supports event management and reporting features.
- C. For the collector, you should allocate most of the disk space to analytics logs.
- D. Analyzer mode is the default operating mode.

Answer: B

Explanation:

When in analyzer mode, FortiAnalyzer supports event management and reporting features.

In analyzer mode, FortiAnalyzer provides full support for log analysis, event management, and reporting capabilities.

Analyzer mode is the default operating mode.

By default, FortiAnalyzer operates in analyzer mode, which allows for log analysis and reporting. The other options are incorrect because:

In collector mode, the FortiAnalyzer primarily stores logs and forwards them to another FortiAnalyzer in analyzer mode, not the other way around.

In collector mode, most disk space is usually allocated to storage rather than analytics, as the logs are primarily stored for forwarding.

NEW QUESTION 6

Which three RAID configurations provide fault tolerance on FortiAnalyzer? (Choose three.)

- A. RAID0
- B. RAID 5
- C. RAID1

The Leader of IT Certification

visit - <https://www.certleader.com>

- D. RAID 6+0
E. RAID 0+0

Answer: BCD

Explanation:

RAID 1 provides fault tolerance through disk mirroring.
RAID 5 provides fault tolerance by using distributed parity across multiple disks. RAID 6+0 combines striping with double parity, offering enhanced fault tolerance.
RAID 0 and RAID 0+0 do not provide any fault tolerance, as they focus on performance through data striping but offer no redundancy.

NEW QUESTION 7

Refer to the exhibit.

Cluster Settings

Operation Mode

StandaloneHigh Availability

Preferred Role

SecondaryPrimary

Cluster Virtual IP

IP Address and Interface

IP Address

Interface

192.168.101.222

port1

Cluster Settings

Peer IP and Peer SN

Peer IP

Peer SN

10.0.1.210

FAZ-VM0000065040

Group Name

NSE6

Group ID

1

(1-255)

Password

.....

Heart Beat Interval

10

Seconds

Failover Threshold

30

Priority

120

The image displays "he configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster.

What can you conclude from the configuration displayed?

- A. After joining to the cluster, this FortiAnalyzer will keep an updated log database.
B. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
C. This FortiAnalyzer will join to the existing HA cluster as the primary.
D. This FortiAnalyzer is configured to receive logs in its port1.

Answer: A

Explanation:

Operation Mode: The mode is set to "High Availability" which indicates that this FortiAnalyzer is intended to be part of an HA cluster.

Preferred Role: The "Primary" role is selected, meaning this device is configured to act as the primary unit in the HA cluster. This is a crucial setting as it determines the device's behavior and responsibilities within the cluster.

Cluster Virtual IP: A specific IP address (192.168.101.222) is assigned to be used by devices in the network to communicate with the cluster. This Virtual IP will be shared between the units in the cluster.

Cluster Settings: These include configurations for heartbeat interval, failover threshold, and priority which are crucial for maintaining cluster health and managing failover scenarios.

Given these points, the correct conclusion from the options provided is:

* C. This FortiAnalyzer will join the existing HA cluster as the primary.

NEW QUESTION 8

Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark

No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
131	9.114194	10.0.1.200	10.0.1.210	Syslog	1003	22486	514	@\000\020\017\003\006eJ\004FGVM010000064692Local-FortiGateroot\002\002S\
132	9.114245	10.0.1.200	10.0.1.210	Syslog	1115	22486	514	@\020\020\017\003\0aBeJ\004FGVM010000064692Local-FortiGateroot\002\002S\
133	9.114311	10.0.1.200	10.0.1.210	Syslog	1135	22486	514	@\002\020\017\004\b\b\reJ\004FGVM010000064692Local-FortiGateroot\0027\002\0
134	10.0013...	10.0.1.200	10.0.1.210	Syslog	871	7262	514	%\000\020\004\002\t\teJ\000FGVM010000077646ISFWroot\001\001\002\017\00
135	11.1086...	10.0.1.200	10.0.1.210	Syslog	872	22486	514	%\000\020\017\003\001\004\teJ\004FGVM010000064692Local-FortiGateroot\002\0
142	15.0058...	10.0.1.200	10.0.1.210	Syslog	572	7262	514	%\000\020\004\001\003\teJ\006FGVM010000077646ISFWroot\001\001\000\000\
143	16.1088...	10.0.1.200	10.0.1.210	Syslog	555	22486	514	%\000\020\017\001\002\017eJ\bFGVM010000064692Local-FortiGateroot\002\017\
150	20.0103...	10.0.1.200	10.0.1.210	Syslog	639	7262	514	%\000\020\004\002\033\aeJ\nFGVM010000077646ISFWroot\001\001\001\001\
151	20.0574...	10.0.1.200	10.0.1.210	Syslog	332	7262	514	@\001\020\004\000\000\teJ\017FGVM010000077646ISFWroot\000\002\024date=2024
152	20.0575...	10.0.1.200	10.0.1.210	Syslog	907	7262	514	@\000\020\004\0033\aeJ\017FGVM010000077646ISFWroot\003\003\002\024date
153	20.0576...	10.0.1.200	10.0.1.210	Syslog	1025	7262	514	@\000\020\004\003\0068eJ\017FGVM010000077646ISFWroot\003\002\002\024date
154	20.0576...	10.0.1.200	10.0.1.210	Syslog	648	7262	514	@\000\020\004\0020\005\004eJ\017FGVM010000077646ISFWroot\002\002\002\024da
155	20.0577...	10.0.1.200	10.0.1.210	Syslog	317	7262	514	@\001\020\004\000\000\teJ\017FGVM010000077646ISFWroot\000\002\024date=2024
156	20.0577...	10.0.1.200	10.0.1.210	Syslog	555	7262	514	@\b\020\004\001\002\003eJ\017FGVM010000077646ISFWroot\002\003\024date=2

Frame 131: 1003 bytes on wire (8024 bits), 1003 bytes captured (8024 bits)
 Ethernet II, Src: Fortinet_09:01:00 (00:09:0f:09:01:00), Dst: VMware_a9:73:0f (00:0c:29:a9:73:0f)
 Internet Protocol Version 4, Src: 10.0.1.200, Dst: 10.0.1.210
 User Datagram Protocol, Src Port: 22486, Dst Port: 514
 Source Port: 22486
 Destination Port: 514
 Length: 969

```

0000  00 0c 29 a9 73 0f 00 09 0f 09 01 00 08 00 45 00  ..).s...E.
0010  03 dd fe 51 00 00 40 11 61 25 0a 00 01 c8 0a 00  ...Q.@.a%...
0020  01 d2 57 d6 02 02 03 c9 a1 55 ec cf 20 40 00 10  ..W....U..@..
0030  0f 04 00 03 03 86 06 f0 65 c1 4a 04 46 47 56 4d  ....e.J-FGM
0040  30 31 30 30 30 30 30 36 34 36 39 32 4c 6f 63 61  01000006 4692Loca
0050  6c 2d 46 6f 72 74 69 47 61 74 65 72 6f 6f 74 02  l-FortiG ateroot
0060  92 02 2f 02 2f f2 14 64 61 74 65 3d 32 30 32 34  ..-/..d ate=2024
0070  2d 30 32 2d 30 35 20 74 69 6d 65 3d 31 32 3a 35  -02-05 t ime=12:5
0080  30 3a 31 32 20 65 76 65 6e 74 13 00 f3 17 37 30  0:12 eve nt...70
  
```

The capture displayed was taken on a FortiAnalyzer.
Why is a single IP address shown as the source for all logs received?

- A. FortiAnalyzer is using the device MAC addresses to differentiate their logs.
- B. The logs belong to devices that are part of a high availability (HA) cluster.
- C. FortiAnalyzer is receiving logs from the root FortiGate of a Security Fabric.
- D. The device sending logs has two VDOMs in the same ADOM.

Answer: C

Explanation:

In a Fortinet Security Fabric, logs from downstream devices can be sent to FortiAnalyzer through the root FortiGate. This is why all the logs have the same source IP address (the root FortiGate). The root FortiGate aggregates and forwards the logs from all downstream devices, so the source IP in the log capture will appear to be from the root FortiGate itself, even though the logs originate from multiple devices within the fabric.

NEW QUESTION 9

Refer to the exhibit.

Create New Administrator

User Name

Remote-Admin

Avatar

R + Add Photo - Remove Photo

Description

Admin Type

LDAP

LDAP Server

External_Server

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

Admin Profile

Restricted_User

The exhibit shows the creation of a new administrator on FortiAnalyzer. The new account uses the credentials stored on an LDAP server. Why would an administrator configure a password for this account?

- A. This password is used if the authentication server becomes unreachable.
- B. This password authenticates FortiAnalyzer against the LDAP server.
- C. This password is set to comply with FortiAnalyzer password policy
- D. This password is required because this is a restricted user.

Answer: A

Explanation:

When using LDAP for authentication, a password can be set locally on FortiAnalyzer as a fallback option in case the LDAP server becomes unreachable. This ensures that the administrator can still log in if there are issues with the LDAP server.

NEW QUESTION 10

An administrator has configured the following settings:

```
#config system global
set log-checksum md5-auth
end
```

What is the purpose of executing these commands?

- A. To record the hash value and authentication code of log file
- B. To encrypt log transfer between FortiAnalyzer and other device
- C. To create the secure channel used by the OFTP proces
- D. To verify the integrity of the log files received.

Answer: A

Explanation:

The command set log-checksum md5-auth configures FortiAnalyzer to generate an MD5 hash for each log file, along with an authentication code. This ensures that the integrity of the logs can be verified, confirming that the logs have not been tampered with.

NEW QUESTION 10

Which statement correctly describes RAID 10 (1+0) on FortiAnalyzer?

- A. A configuration with four disks, each with 2 TB of capacity, provides a total space of 4 T
- B. 11 combines mirroring striping and distributed parity to provide performance and fault toleranc
- C. A configuration with four disks, each with 2 TB of capacity, provides a total space of 2 T
- D. It uses striping to provide performance and fault tolerance.

Answer: A

Explanation:

RAID 10 combines mirroring (RAID 1) and striping (RAID 0). In a RAID 10 setup with four disks, data is mirrored across two pairs of disks, and those pairs are striped for performance. This results in improved performance and fault tolerance, but the total usable storage is 50% of the total raw storage, meaning four 2 TB disks provide 4 TB of usable space.

NEW QUESTION 13

You finished registering a FortiGate device. After traffic starts to flow through FortiGate, you notice that only some of the logs expected are being received on FortiAnalyzer.

What could be the reason for the logs not arriving on FortiAnalyzer?

- A. This FortiGate is part of an HA cluster but it is the secondary device.
- B. This FortiGate model is not fully supported.
- C. FortiGate does not have logging configured correctly.
- D. FortiGate was added to the wrong ADOM type.

Answer: C

Explanation:

When only some of the expected logs from a FortiGate device are being received on FortiAnalyzer, it often indicates a configuration issue on the FortiGate side. Proper logging configuration on FortiGate involves specifying what types of logs to generate (e.g., traffic, event, security logs) and ensuring that these logs are directed to the FortiAnalyzer unit for storage and analysis. If the logging settings on FortiGate are not correctly configured, it could result in incomplete log data being sent to FortiAnalyzer. This might include missing logs for certain types of traffic or events that are not enabled for logging on the FortiGate device. Ensuring comprehensive logging is enabled and correctly directed to FortiAnalyzer is crucial for full visibility into network activities and for the effective analysis and reporting of security incidents and network performance.

NEW QUESTION 17

It is a best practice to upload FortiAnalyzer local logs to a remote server. Which two remote servers are supported for the upload? (Choose two.)

- A. FTP
- B. SFTP
- C. UDP
- D. TFTP

Answer: AB

Explanation:

When it's considered a best practice to upload FortiAnalyzer local logs to a remote server, the following two remote server protocols are commonly supported: These protocols provide secure and reliable ways to transfer logs and data to remote servers for storage and analysis while maintaining data integrity and confidentiality.

NEW QUESTION 18

What are two potential advantages of deploying RAID on FortiAnalyzer? (Choose two.)

- A. It provides redundancy.
- B. It improves performance.
- C. It provides backups.
- D. It reduces system resource usage.

Answer: AB

Explanation:

Here are two potential advantages of deploying RAID on FortiAnalyzer:

RAID configurations can mirror or stripe data across multiple disks. This redundancy helps ensure that even if one disk fails, the data remains accessible and recoverable. This is crucial for FortiAnalyzer as it stores security logs which are critical for analysis and forensic investigations.

Certain RAID configurations, like RAID 0 (striping) can improve read performance by distributing data reads across multiple disks. This can be beneficial for FortiAnalyzer when performing faster searches or retrieving large log sets.

Here's why the other options are not necessarily advantages:

While RAID can improve data availability in case of disk failures, it's not a replacement for proper backups. Backups should be done regularly to a separate location to ensure data recovery in case of catastrophic events like hardware failures or ransomware attacks.

RAID itself doesn't necessarily reduce system resource usage. In fact, some RAID configurations can introduce additional overhead for managing the redundant data.

NEW QUESTION 21

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your FCP_FAZ_AD-7.4 Exam with Our Prep Materials Via below:

https://www.certleader.com/FCP_FAZ_AD-7.4-dumps.html