



Fortinet

Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator

NEW QUESTION 1

Which two parameters impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

- A. Total quota
- B. License type
- C. RAID level
- D. Disk size

Answer: C

Explanation:

RAID level affects how much disk space is reserved for redundancy and fault tolerance. For example, RAID 1 mirrors data, meaning you need more space for redundancy, while RAID 5 or RAID 6 reserves space for parity.

Disk size directly influences the total available and reserved space since the larger the disk, the more space may need to be reserved for system functions, logs, and other operations.

The total quota and license type do not directly impact the reserved disk space, though they do influence other aspects of capacity and functionality.

NEW QUESTION 2

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 3

Which two statements regarding ADOM modes are true? (Choose two.)

- A. In normal mode, the disk quota of the ADOM is fixed and cannot be modified, but in advanced mode, the disk quota of the ADOM is flexible.
- B. You can change ADOM modes only through the CLI.
- C. In an advanced mode ADOM, you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.
- D. Normal mode is the default ADOM mode.

Answer: CD

NEW QUESTION 4

What are analytics logs on FortiAnalyzer?

- A. Logs that are compressed and saved to a log file
- B. Logs that roll over when the log file reaches a specific size
- C. Logs that are indexed and stored in the SQL
- D. Logs classified as type Traffic, or type Security

Answer: C

Explanation:

On FortiAnalyzer, analytics logs refer to the logs that have been processed, indexed, and then stored in the SQL database. This process allows for efficient data retrieval and analytics. Unlike basic log storage, which might involve simple compression and storage in a file system, analytics logs in FortiAnalyzer undergo an indexing process. This enables advanced features such as quick search, report generation, and detailed analysis, making it easier for administrators to gain insights into network activities and security incidents.

Reference: FortiAnalyzer 7.2 Administrator Guide - "Log Management" and "Data Analytics" sections.

NEW QUESTION 5

Which two methods can you use to restrict administrative access on FortiAnalyzer? (Choose two.)

- A. Configure trusted hosts.
- B. Limit access to specific virtual domains.
- C. Fabric connectors to external LDAP servers.
- D. Use administrator profiles.

Answer: AD

Explanation:

Configure trusted hosts.

Trusted hosts restrict administrative access to FortiAnalyzer by limiting the IP addresses or subnets from which administrators can log in.

Use administrator profiles.

Administrator profiles define roles and permissions, restricting what specific administrators can access and manage on FortiAnalyzer.

The other options are not applicable because:

Limiting access to specific virtual domains is not applicable to FortiAnalyzer, as virtual domains (VDOMs) are a concept used in FortiGate, not FortiAnalyzer.

Fabric connectors to external LDAP servers are used for authentication purposes but do not directly restrict administrative access based on roles or IP addresses.

NEW QUESTION 6

What does the disk status Degraded mean for RAID management?

- A. The hard drive is no longer being used by the RAID controller.
B. One or more drives are missing from the FortiAnalyzer unit.
C. The device is writing data to the disk to restore the volume to an optimal state.
D. FortiAnalyzer determined that the parity data in the disk is not valid.

Answer: B

Explanation:

When the RAID status is Degraded, it typically indicates that one or more drives in the RAID array have failed or are missing, causing the RAID array to operate with reduced redundancy. In this state, the array is still functioning, but it's at risk because the fault tolerance provided by RAID is compromised.

NEW QUESTION 7

Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark

sniffer_port1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.dstport == 514

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\ceJ\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\ceJ\004FGVM010000064692Local-FortiGateroot\002\017\
142	15.0058...	10.0.1.200	10.0.1.210	Syslog	572	7262	514	\$@\000\020\004\001\003\ceJ\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\ceJ\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\024d
155	20.0577...	10.0.1.200	10.0.1.210	Syslog	317	7262	514	@\001\020\004\000\000\ceJ\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\002\024date=20

> 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-FGVM
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

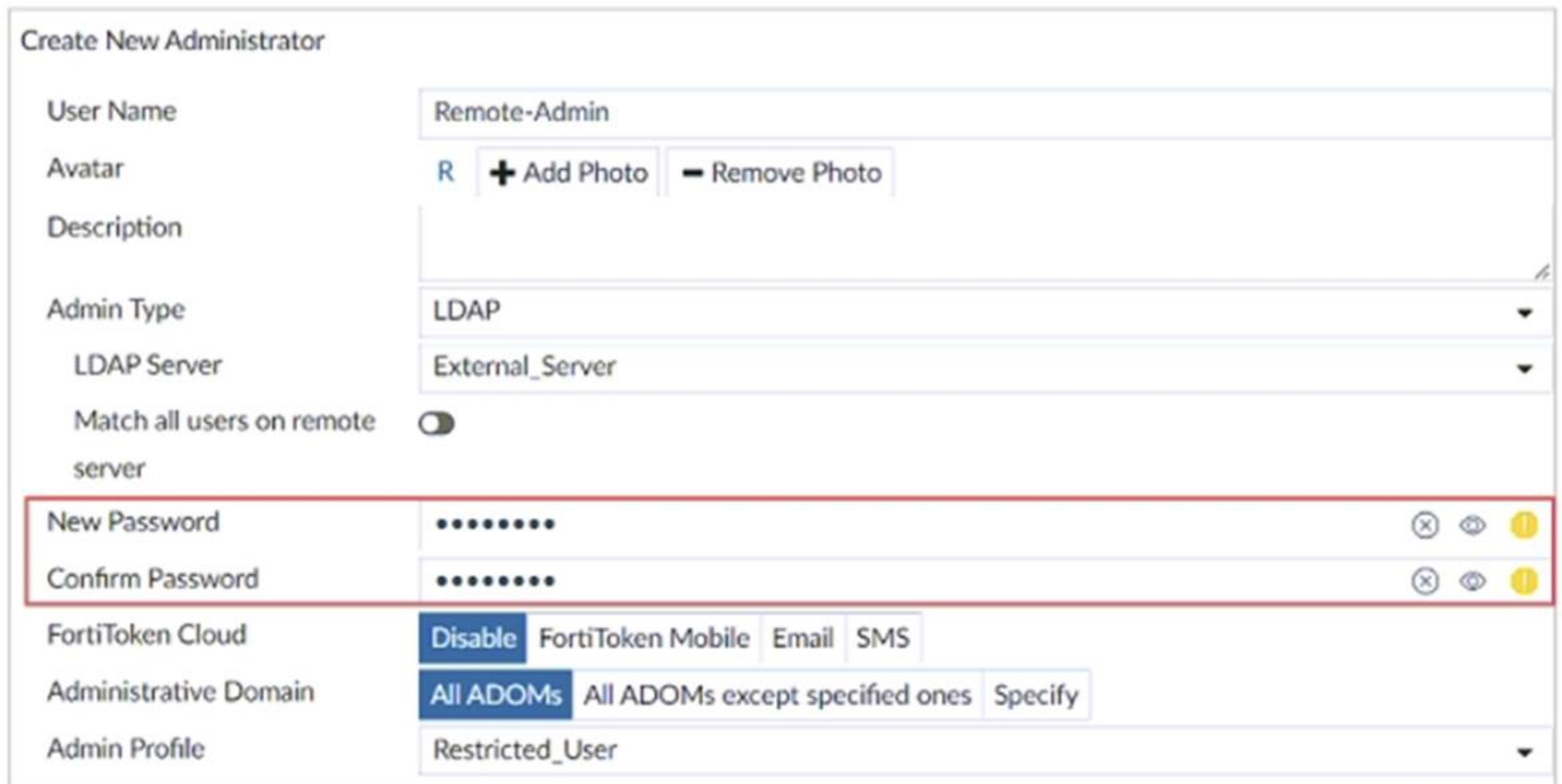
Explanation:

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 8

Refer to the exhibit.



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 9

Which statement about the communication between FortiGate high availability (HA) clusters and FortiAnalyzer is true?

- A. If devices were registered to FortiAnalyzer before forming a cluster, you can manually add them together
- B. FortiAnalyzer distinguishes each cluster member by the IP addresses in log message header
- C. If the HA primary device becomes unavailable, you must remove it from the HA cluster list on FortiAnalyzer
- D. The FortiGate HA cluster must be in active-passive mode in order to avoid conflict.

Answer: B

Explanation:

This allows FortiAnalyzer to correctly identify and process logs from different members of the HA cluster.

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 tolerance
- 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 10

What is the recommended method of expanding disk space on a FortiAnalyzer VM?

- A. From the VM host manager, add an additional virtual disk and use the #execute lvm extendcommand to expand the storage.
- B. From the VM host manager, expand the size of the existing virtual disk.
- C. From the VM host manager, expand the size of the existing virtual disk and use the # executeformat disk command to reformat the disk.
- D. From the VM host manager, add an additional virtual disk and rebuild your RAID array.

Answer: A

Explanation:

Adding an Additional Virtual Disk:

From the VM host manager (such as VMware vSphere or Hyper-V), you can add a new virtual disk to the FortiAnalyzer VM.

Extending the Logical Volume:

After adding the new disk, use commands like #execute lvm extend within the FortiAnalyzer to extend the logical volume, making the additional storage available to the VM. This is particularly useful when you need to add more storage without disrupting existing data.

This approach is recommended when you need to ensure the FortiAnalyzer VM can handle more storage without reformatting or affecting existing data.

NEW QUESTION 12

What is the purpose of employing RAID with FortiAnalyzer?

- A. To introduce redundancy to your log data
- B. To provide data separation between ADOMs
- C. To separate analytical and archive data
- D. To back up your logs

Answer: A

Explanation:

RAID (Redundant Array of Independent Disks) is used in FortiAnalyzer primarily to provide data redundancy and ensure data integrity. Here,s how it relates to each option:

To Introduce Redundancy to Your Log Data (Option A):

The main purpose of employing RAID in FortiAnalyzer is to add redundancy to the storage system. By using RAID configurations (such as RAID 1, RAID 5, or RAID 6), data is replicated across multiple disks, which helps in protecting against disk failures and ensures that log data is not lost if a disk fails. This redundancy enhances the reliability and availability of the log data.

NEW QUESTION 13

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 17

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 22

How do you restrict an administrator's access to a subset of your organization's ADOMs?

- A. Set the ADOM mode to Advanced
- B. Assign the ADOMs to the administrator's account
- C. Configure trusted hosts
- D. Assign the default Super_User administrator profile

Answer: B

Explanation:

To restrict an administrator's access to a subset of your organization's ADOMs (Administrative Domains) in FortiAnalyzer, you need to assign the specific ADOMs to the administrator's account. Here's how this works:

Assign the ADOMs to the Administrator's Account (Option B):

In FortiAnalyzer, you can configure which ADOMs an administrator has access to by assigning them directly to the administrator's account. This allows you to control and limit the administrator's access to only the ADOMs they are authorized to manage or view.

NEW QUESTION 24

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

FCP_FAZ_AD-7.4 Practice Exam Features:

- * FCP_FAZ_AD-7.4 Questions and Answers Updated Frequently
- * FCP_FAZ_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FAZ_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCP_FAZ_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FAZ_AD-7.4 Practice Test Here](#)