

Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator

https://www.2passeasy.com/dumps/FCP_FAZ_AD-7.4/



NEW QUESTION 1

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

x

+

Cluster Settings

Peer IP and Peer SN

Peer IP

Peer SN

Action

10.0.1.210

FAZ-VM0000065040

x

+

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 2

Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark

Wireshark - Packet 34 - sniffer_port3.1.pcap

- > Frame 34: 624 bytes on wire (4992 bits), 624 bytes captured (4992 bits)
- > Ethernet II, Src: MS-NLB-PhysServer-09_0f:00:01:06 (02:09:0f:00:01:06), Dst: MS-NLB-PhysServer-09_0f:00:01:06
- > Internet Protocol Version 4, Src: 10.200.3.1, Dst: 10.200.1.210
- > Transmission Control Protocol, Src Port: 18052, Dst Port: 514, Seq: 14443, Ack: 130, Len: 570
- > Remote Shell
 - Client -> Server Data [truncated]: 1703030235120db2f7eaa29995a08617e996a1e7e5a02afe2f81e0320715cff2d8c

No.: 34 - Time: 11.315345 - Source: 10.200.3.1 - Destination: 10.200.1.210 - Protocol: RSH - Length: 624 - Info: Client -> Server data

☒ Show packet bytes

Close Help

Which image corresponds to the packet capture shown in the exhibit?

A)

					Search...
<input type="checkbox"/>	Device Name	IP Address	Connectivity	Logging Mode	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-FortiGate	10.200.3.1	↑ Connection Up	Real Time	0

B)

					Search...
<input type="checkbox"/>	Device Name	IP Address	Connectivity	Logging Mode	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-FortiGate	10.200.3.1	↑ Connection Up	Real Time	0

C)

					Search...
<input type="checkbox"/>	Device Name	IP Address	Connectivity	Logging Mode	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-FortiGate	10.200.3.1	↓ Connection Down	Real Time	0

D)

					Search...
<input type="checkbox"/>	Device Name	IP Address	Connectivity	Logging Mode	Average Log Rate(Logs/Sec)
<input type="checkbox"/>	Remote-FortiGate	10.200.3.1	↓ Connection Down	Real Time	0

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Chosen image shows the device Remote-FortiGate with the IP 10.200.3.1 and a connection status of "Connection Up," which is consistent with the packet capture details showing active communication between the client and server.

NEW QUESTION 3

Which feature can you configure to add redundancy to FortiAnalyzer?

- A. Primary and secondary DNS
- B. VLAN interfaces
- C. IPv6 administrative access
- D. Link aggregation

Answer: D

Explanation:

Link aggregation is a method used to combine multiple network connections in parallel to increase throughput and provide redundancy in case one of the links fail. This feature is used in network appliances, including FortiAnalyzer, to add redundancy to the network connections, ensuring that there is a backup path for traffic if the primary path becomes unavailable.

Reference: The FortiAnalyzer 7.4.1 Administration Guide explains the concept of link aggregation and its relevance to

NEW QUESTION 4

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.

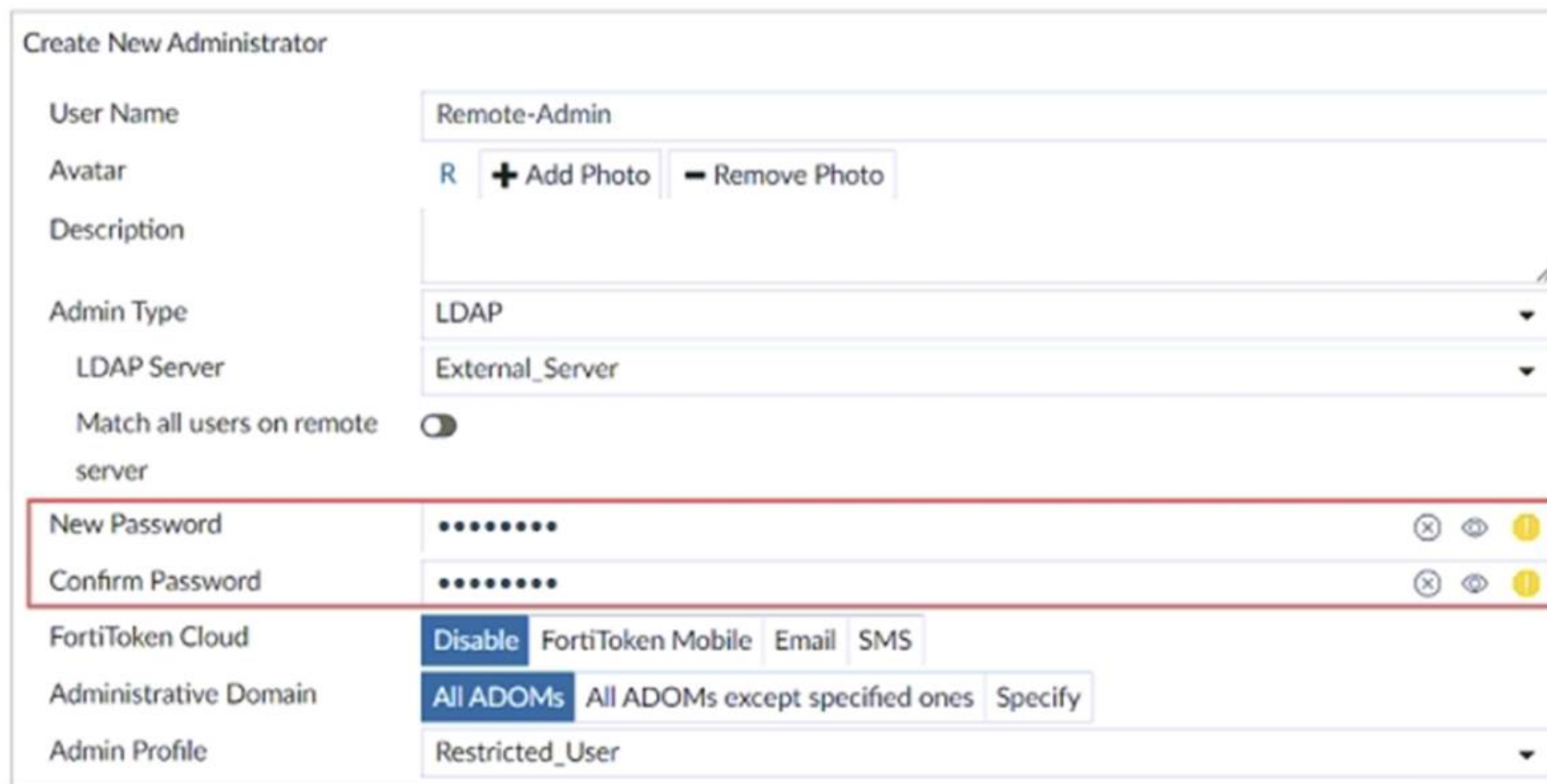
Answer: B

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 5

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 6

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 7

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 8

What FortiGate process caches logs when FortiAnalyzer is not reachable?

- A. logfiled
- B. sqlplugind
- C. oftpd
- D. miglogd

Answer: D

Explanation:

The miglogd process on FortiGate is responsible for caching logs when FortiAnalyzer is unreachable. It temporarily stores logs in memory and, if the memory buffer fills up, it starts storing logs on disk. Once the connection to FortiAnalyzer is restored, miglogd sends the cached logs to the FortiAnalyzer.

NEW QUESTION 10

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual FCP_FAZ_AD-7.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the FCP_FAZ_AD-7.4 Product From:

https://www.2passeasy.com/dumps/FCP_FAZ_AD-7.4/

Money Back Guarantee

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