



- Expert Verified, Online, **Free**.



CERTIFICATION TEST

- CertificationTest.net - Cheap & Quality Resources With Best Support

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.

Suggested Answer: CD

🗨️ 👤 **GnXxUbik** 1 month ago

Selected Answer: CD

The questions displayed here are enough? There are only 49 and some other sites brag themselves with 180
upvoted 1 times

🗨️ 👤 **GnXxUbik** 3 weeks, 4 days ago

I graduated with the material presented here, only two questions were new
upvoted 1 times

🗨️ 👤 **81a989b** 4 months, 3 weeks ago

Selected Answer: CD

C&D, Page 96 of the Study Guide
upvoted 1 times

🗨️ 👤 **Slikings** 7 months, 2 weeks ago

C&D are correct.

- a. Is not true because disk quota is not affected by the mode. Disk Quota is set per ADOM.
 - b. You can change mode w/o CLI Access
 - c. This is correct because in advanced mode you can assign multiple VDOMs to multiple Fortianalyzer Adoms. FortiAnalyzer 7.4 Administrator Study Guide Page 96
 - d. This is correct Normal mode is default mode. FortiAnalyzer 7.4 Administrator Study Guide Page 96
- upvoted 4 times

🗨️ 👤 **Karoly** 7 months, 4 weeks ago

I've checked, my "new" questions are in the Fortianalyzer 7.0 Exam there, looks like Fortinet is using the questions between FAZ versions... :(
upvoted 2 times

🗨️ 👤 **Beatledrew** 8 months, 3 weeks ago

C&D, Page 96 of the Study Guide
upvoted 3 times

What is the purpose of the FortiAnalyzer command diagnose system print netstat?

- A. It provides network statistics for active connections, including the protocols, IP addresses, and connection states.
- B. It provides the complete routing table, including directly connected routes.
- C. It provides the static DNS table, including the host names and their expiration timers.
- D. It provides NTP server information, including server IPs, stratum, poll time, and latency.

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **je2884** 5 months, 1 week ago

Selected Answer: A

A es correcta

upvoted 1 times

🗳️ 👤 **Slikings** 7 months, 2 weeks ago

- A. Is correct
- B. #Diagnose System Print Route, would display the routing table
- C. #Diagnose system print hosts, shows static table for hostnames
- D. #Diagnose system ntp status, provides NTP server information, including server IPs, stratum, poll time, and latency.

As per page 65 of FortiAnalyzer 7.4 Administrator Study Guide

upvoted 3 times

🗳️ 👤 **Beatledrew** 8 months, 3 weeks ago

Answer is A page 65 of the Study Guide

upvoted 3 times

🗳️ 👤 **juniou82** 8 months, 3 weeks ago

Selected Answer: A

Print the network statistics for active Internet connections (servers and established).

upvoted 3 times

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 ☒

The exhibit shows the creation of a new administrator on FortiAnalyzer.

What are two effects of enabling the choice Match all users on remote server when configuring a new administrator? (Choose two.)

- A. It allows user accounts in the LDAP server to use two-factor authentication.
- B. It creates a wildcard administrator using an LDAP server.
- C. User Remote-Admin from the LDAP server will be able to log in to FortiAnalyzer at any time.
- D. Administrators can log in to FortiAnalyzer using their credentials on the remote LDAP server.

Suggested Answer: BD

Community vote distribution

BD (100%)

sandking 3 months, 3 weeks ago

Selected Answer: BD

page 80 from study guide

upvoted 1 times

Slikings 7 months, 2 weeks ago

A. is incorrect because, This is part of the process of setting up two factor authentication however it is not part of the match all users on remote server command as you do not need to enable this

to have Two-Factor work properly. Per page 81 of FortiAnalyzer 7.4 Administrator Study Guide

B. is correct as the use of the match all users on remote server command is what creates

the wildcard administrator. per page 80 of FortiAnalyzer 7.4 Administrator Study Guide

C. User Remote-Admin from the LDAP server will not be able to login if the server becomes unavailable. They would have to assign a local password and thus not use the wildcard feature.

D. Is correct because it allows the use of an administrator to log in to Fortianalyzer using their creds.

upvoted 4 times

DBFront 8 months, 1 week ago

Selected Answer: BD

B & D are correct

upvoted 4 times

The connection status of a new device on FortiAnalyzer is listed as Unauthorized.
What does that status mean?

- A. It is a device whose registration has not yet been accepted in FortiAnalyzer.
- B. It is a device that has not yet been assigned an ADOM.
- C. It is a device that is waiting for you to configure a pre-shared key.
- D. It is a device that FortiAnalyzer does not support.

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **Slikings** 7 months, 2 weeks ago

- A. Is correct because the Unauthorized status means that it is waiting to be authorized by an admin. As Per FortiAnalyzer 7.4 Administrator Study Guide
 - B. Is Incorrect, If ADOMs are enabled (Not default Enabled) then the device will land in the root ADOM, you can optionally move the device to a new adom.
 - C. Is Incorrect because to get to the stage of unauthorized you must have already either registered the device via S/N or PSK
 - D. Is incorrect because it would not get to the stage of being unauthorized if it was not supported.
- upvoted 2 times

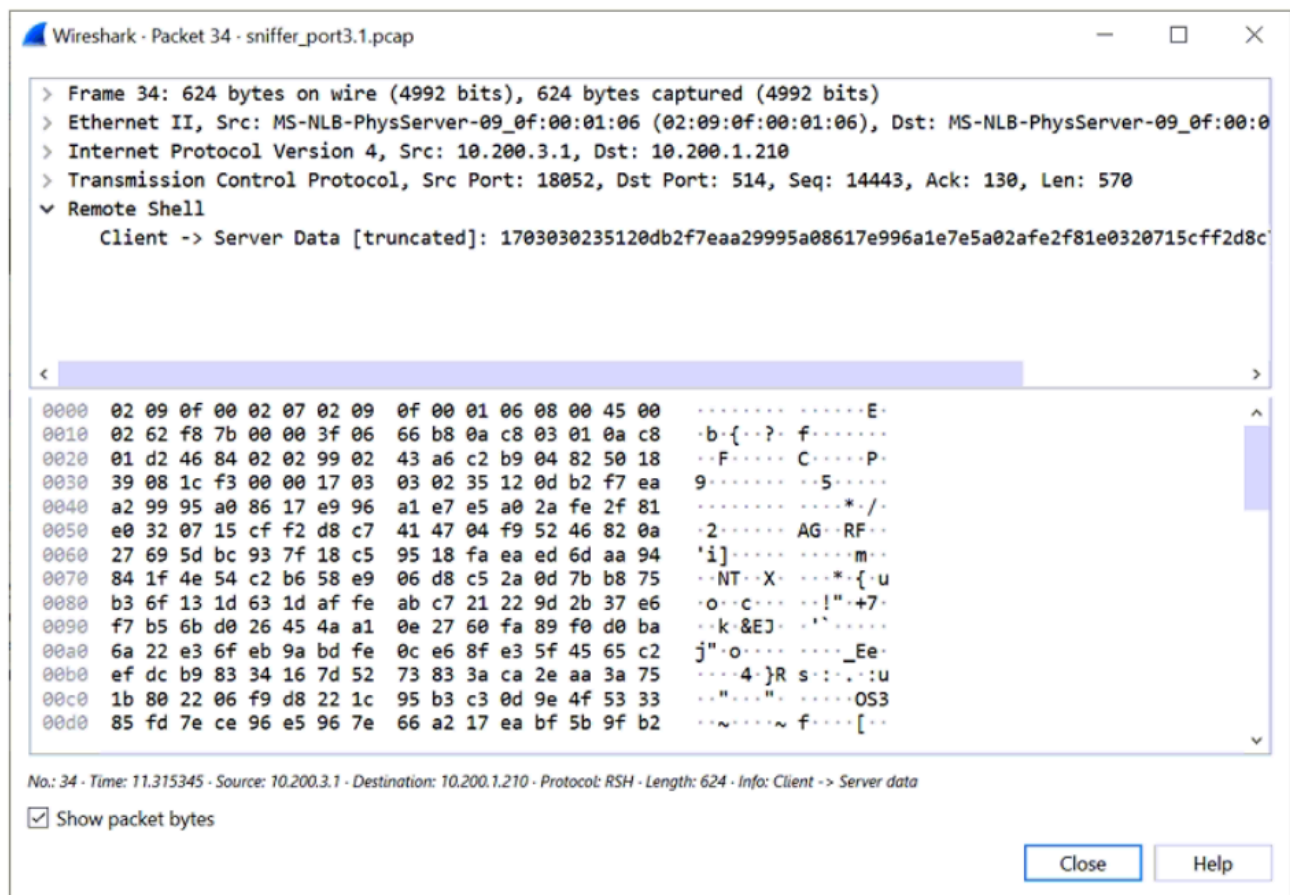
🗨️ 👤 **DBFront** 8 months, 1 week ago

Selected Answer: A

A is correct, page 149 of the FortiAnalyzer 7.4 Admin Study Guide.
upvoted 3 times

Refer to the exhibit.

FortiAnalyzer packet capture on Wireshark



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

- A.

Device Name	IP Address	Connectivity	Logging Mode	Average Log Rate(Logs/Sec)
Remote-FortiGate	10.200.3.1	Connection Up	Real Time	0
- B.

Device Name	IP Address	Connectivity	Logging Mode	Average Log Rate(Logs/Sec)
Remote-FortiGate	10.200.3.1	Connection Up	Real Time	0
- C.

Device Name	IP Address	Connectivity	Logging Mode	Average Log Rate(Logs/Sec)
Remote-FortiGate	10.200.3.1	Connection Down	Real Time	0
- D.

Device Name	IP Address	Connectivity	Logging Mode	Average Log Rate(Logs/Sec)
Remote-FortiGate	10.200.3.1	Connection Down	Real Time	0

Suggested Answer: A

066c9f3 8 months, 2 weeks ago



FortiAnalyzer Administrator 7.2 Study Guide p. 183

OFTP is used over SSL when information is synchronized between FortiAnalyzer and FortiGate. OFTP listens

on port TCP/514. Port UDP/514 is used for unencrypted log communication.




In WireShark, we see TCP_514 being used, so A is correct.

upvoted 6 times

  **066c9f3** 7 months, 3 weeks ago

Or 7.4 Guide p. 190



upvoted 3 times

  **darkstar15**  7 months, 1 week ago

To better understand this scenario, read the FortiAnalyzer 7.4.1 Administration Guide on page 412.

By taking a screenshot with the "set reliable enable" setting, you will understand the differences a little better.



upvoted 1 times

  **Slikings** 7 months, 2 weeks ago

A is correct, this was a hard one for me as the question is not immediately obvious as to what the real question is.

The key is to observe that the protocol being used is secure.



upvoted 2 times

  **ChandraH** 8 months, 2 weeks ago

A is correct!

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.

upvoted 3 times

  **066c9f3** 7 months, 3 weeks ago

Be careful here, it's not only about a consistent connection but rather about understanding different protocols for different communication of OFTP (TCP 514 encrypted / UDP 514 unencrypted). Refer to the little green lock.

upvoted 6 times

Refer to the exhibit.

Create New Network Interface	
Name	VLAN100
Alias	FortiGate-VLAN
Type	VLAN Aggregate
VLAN ID	100
Interface	port5

What is the purpose of configuring FortiAnalyzer with the settings displayed in the image?

- A. To increase reliability
- B. To expand bandwidth
- C. To maximize resiliency
- D. To improve security

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **darkstar15** 7 months, 1 week ago

D. is correct, FAZ Admin Study Guide, page 62.

upvoted 2 times

🗳️ 👤 **Slikings** 7 months, 2 weeks ago

D is Correct, Vlans provide security by creating a virtual separation of networks.

A is incorrect because it does not increase reliability

B is incorrect because Vlans dont inherently expand bandwidth

C is incorrect because Vlans dont increase resiliency

upvoted 3 times

🗳️ 👤 **DBFront** 8 months, 1 week ago

Selected Answer: D

D is correct

upvoted 2 times

What are offline logs on FortiAnalyzer?

- A. Compressed logs, also known as archive logs
- B. Logs that are indexed and stored in the SQL database
- C. Any logs collected from offline devices after they boot up
- D. Real-time logs that are not yet indexed

Suggested Answer: C

Community vote distribution

A (100%)

🗳️ 👤 **SmilinJoe** 6 months, 3 weeks ago

Selected Answer: A

A is correct. Page 183 of the Study Guide
upvoted 1 times

🗳️ 👤 **Slikings** 7 months, 2 weeks ago

A is correct, all offline logs are archive files that are rolled which compresses and creates a timestamp.
upvoted 2 times

🗳️ 👤 **915e31d** 7 months, 2 weeks ago

A is the correct
upvoted 1 times

🗳️ 👤 **DBFront** 8 months ago

Selected Answer: A

A is correct
upvoted 1 times

🗳️ 👤 **Beatledrew** 8 months, 3 weeks ago

A is correct. Page 183 of the Study Guide
upvoted 2 times

🗳️ 👤 **fa7474b** 8 months, 3 weeks ago

Selected Answer: A

"Archive logs: When a real-time log file in Archive has been completely inserted, that file is compressed and considered to be offline."
<https://docs.fortinet.com/document/fortianalyzer/7.4.3/administration-guide/381919/logs>
upvoted 3 times

🗳️ 👤 **Noreki** 9 months ago

A is correct.
FortiAnalyzer 7.6.0 Admin Guide says:

When FortiAnalyzer receives a log, it is stored in a file. Logs will continue to populate this file until its limit is reached, at which time the file is "rolled" which involves compressing the file and creating a new one for further logs of that type. These files (rolled or otherwise) count against the archive retention limits and are referred to as Archived or Offline logs.

upvoted 4 times

🗳️ 👤 **ChandraH** 9 months ago

When a real-time log file in Archive has been completely inserted, that file is compressed and considered to be offline. A is Correct
upvoted 2 times

Which two elements are contained in a system backup created on FortiAnalyzer? (Choose two.)

- A. Logs from registered devices
- B. Database snapshot
- C. Report information
- D. System information

Suggested Answer: CD

Community vote distribution

CD (100%)

🗳️ 👤 **je2884** 5 months, 1 week ago

Selected Answer: CD

C y D son correctas pagina 114

upvoted 1 times

🗳️ 👤 **Toh85** 6 months, 1 week ago

Selected Answer: CD

C&D is correct

upvoted 2 times

🗳️ 👤 **Slikings** 7 months, 2 weeks ago

- A. Logs are not part of backups
- B. Snapshots can be taken is your FAZ is a VM but this is not part of the backup
- C. Report information is saved in the backup but not generated reports or logs. This is correct
- D. System information and configuration information is saved in the backup. This is correct

upvoted 2 times

🗳️ 👤 **DBFront** 8 months, 1 week ago

Selected Answer: CD

C & D are correct

upvoted 3 times

🗳️ 👤 **Beatledrew** 8 months, 3 weeks ago

C&D is correct. Page 114 of the Study Guide

upvoted 4 times

Refer to the exhibit.

FortiAnalyzer partial configuration output

FortiAnalyzer1# 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 : FortiAnalyzer1 Max Number of Admin Domains : 5 Admin Domain Configuration : Enabled FIPS Mode : Disabled HA Mode : Stand Alone Branch Point : 2308 Release Version Information : GA Time Zone : (GMT-8:00) Pacific Time (US & Canada) Disk Usage : Free 43.60GB, Total 58.80GB File System : Ext4 License Status : Valid	
FortiAnalyzer2# get system global adom-mode : normal adom-select : enable adom-status : enable console-output : standard country-flag : enable enc-algorithm : high ha-member-auto-grouping : enable hostname : FortiAnalyzer2 log-checksum : md5 log-forward-cache-size : 5 log-mode : collector longitude : (null) max-aggregation-tasks : 0 max-running-reports : 5 oftp-ssl-protocol : tls1.2 ssl-low-encryption : disable ssl-protocol : tls1.3 tls1.2 task-list-size : 2000 webservice-proto : tls1.3 tls1.2	
FortiAnalyzer3# get system status Platform Type : FAZVM64 Platform Full Name : FortiAnalyzer-VM64 Version : v7.4.1-build2308 230831 (GA) Serial Number : FAZ-VM0000065042 BIOS version : 04000002 Hostname : FortiAnalyzer3 Max Number of Admin Domains : 5 Admin Domain Configuration : Enabled FIPS Mode : Disabled HA Mode : Stand Alone Branch Point : 2308 Release Version Information : GA Time Zone : (GMT-8:00) Pacific Time (US & Canada) Disk Usage : Free 53.06GB, Total 79.80GB File System : Ext4 License Status : Valid	
FortiAnalyzer3# get system global adom-mode : normal adom-select : enable adom-status : enable console-output : standard country-flag : enable enc-algorithm : high ha-member-auto-grouping : enable hostname : FortiAnalyzer3 log-checksum : md5 log-forward-cache-size : 5 log-mode : analyzer longitude : (null) max-aggregation-tasks : 0 max-running-reports : 5 oftp-ssl-protocol : tls1.2 ssl-low-encryption : disable ssl-protocol : tls1.3 tls1.2 task-list-size : 2000 webservice-proto : tls1.3 tls1.2	

Based on the partial outputs displayed, which devices can be members of a FortiAnalyzer Fabric?

- A. FortiAnalyzer1 and FortiAnalyzer3
- B. All devices listed can be members.
- C. FortiAnalyzer1 and FortiAnalyzer2
- D. FortiAnalyzer2 and FortiAnalyzer3

Suggested Answer: C

Community vote distribution

A (100%)

Noreki Highly Voted 9 months ago

As far as I'm concerned, FortiAnalyzer#2 can't be a fabric member because it is in collector mode. Fabric Members must be in analyzer mode, according to the study guide.

The exhibit doesn't provide information about the logging mode of FortiAnalyzer#1, so technically it could be a member.

So in my opinion the correct answer is A.

upvoted 8 times

fangeel Most Recent 4 months, 2 weeks ago

Selected Answer: A

FAZ2 is not an option - therefore A is right

upvoted 1 times

🗨️ 👤 **Slikings** 7 months, 2 weeks ago

I see a lot of comments about HA and Security Fabric. The question specifically states analyzer fabric! this means that we have to go based off of the FAZ Fabric rules as per page 50. Therefore 2 cannot be part of the Fabric so therefore only Analyzer modes FAZ can work. therefore A is the correct answer.

upvoted 2 times

🗨️ 👤 **915e31d** 7 months, 2 weeks ago

A is correct, collectors cant be members of FortiAnalyzer Fabric

upvoted 1 times

🗨️ 👤 **felixliao** 8 months ago

Selected Answer: A

Study Guide Page50, members must be in analyzer mode, conllectors cannot be members.

upvoted 3 times

🗨️ 👤 **fa7474b** 8 months ago

Selected Answer: A

A, Collectors can't be a fabric member.

upvoted 2 times

🗨️ 👤 **migdadcom** 8 months ago

Selected Answer: A

collector can't be a member

upvoted 2 times

🗨️ 👤 **ChandraH** 8 months, 1 week ago

All devices in the cluster must be same fortianalyzer seriess, use the same fireware on visual to eachother on the network

all devices must runing same operation mode Analyzer or collector.

2 & 3 Can't be HA (D is wrong)

although the available diskpace does not match but all the cluster member must have enough storage expected logs and it's important all members same avialable storage

when using fortianalyzer VMs as cluster members all VMs must be running on the same platform Ex: VM runing VMware can't form the cluster VM running on KVM

1& 3 Can't be HA (A is wrong)

B is Wrong

C is Correc

upvoted 2 times

🗨️ 👤 **fa7474b** 8 months ago

The question is about joining a fabric, NOT an HA cluster. Fabric and HA are two distinct concepts with different requirements. The answer is A.

upvoted 3 times

🗨️ 👤 **Beatledrew** 8 months, 3 weeks ago

Noreki is correct because it can't be either B, C or D because according to page 50 of the Study Guide a Collector can't be a member. Therefore all devices isn't correct, and any answer with FortiAnalyzer 2 in it as an option would be incorrect.

upvoted 3 times

🗨️ 👤 **Beatledrew** 8 months, 3 weeks ago

Page 50 of the Study Guide

upvoted 1 times

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

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **darkstar15** 7 months, 1 week ago

Perhaps to better understand the context we can use FAZ admin study guide page 157. C is correct.
upvoted 3 times

🗨️ 👤 **Slikings** 7 months, 2 weeks ago

This question is trying to get you to understand why the wrong answers are wrong.

- A. Is incorrect because the Fortigate would still be showing logs sending to the ADOM you assigned it to. There are no wrong ADOM types.
 - B. Is incorrect because, If the device was not supported then you would not have gotten past the registration step.
 - C. Is correct, If fortigate does not have the proper logging configuration in the Policies then it will not properly generate logs.
 - D. Is incorrect, Fortigate HA cluster acts as one unit.
- upvoted 4 times

🗨️ 👤 **DBFront** 8 months, 1 week ago

Selected Answer: C

C is correct,
upvoted 3 times

An administrator, fortinet, can view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mail server that can be used to send alert emails. What can be the problem?

- A. ADOM mode is configured with Advanced mode.
- B. A trusted host is configured.
- C. fortinet is assigned the default Standard_User administrative profile.
- D. fortinet is assigned the default Restricted_User administrative profile.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **Slikings** 7 months, 2 weeks ago

- A. is Incorrect because ADOM mode is unrelated to email alert generation.
 - B. is Incorrect because Trusted hosts don't relate to administrator profiles.
 - C. is correct because standard user will allow configurations of devices but not system settings. Only a Super User can affect system privileges Per Page 76
 - D. Is incorrect because a restricted_user administrator would not have been able to perform device management tasks.
- upvoted 3 times

🗨️ 👤 **DBFront** 8 months ago

Selected Answer: C

C is correct
upvoted 1 times

🗨️ 👤 **Beatledrew** 8 months, 3 weeks ago

Page 76 of the Study Guide
upvoted 4 times

Which two parameters are used to calculate the Total Quota value available on FortiAnalyzer? (Choose two.)

- A. Used storage
- B. Retention policy
- C. Reserved space
- D. Total system storage

Suggested Answer: CD

Community vote distribution

CD (100%)

🗲️ 👤 **DBFront** Highly Voted 8 months, 1 week ago

Selected Answer: CD

C & D are correct, page 106 of the FortiAnalyzer 7.4 Admin Study Guide.

upvoted 6 times

🗲️ 👤 **fangeel** Most Recent 4 months, 2 weeks ago

Selected Answer: CD

TSS-RS = TQ - so C and D

upvoted 1 times

🗲️ 👤 **Slikings** 7 months, 2 weeks ago

- A. Is incorrect
- B. Is incorrect, Retention Policy is per ADOM
- C. Reserved space is correct because total quota = total system storage - reserved space
- D. Correct ^

upvoted 4 times

🗲️ 👤 **migdadcom** 8 months ago

Selected Answer: CD

C & D

upvoted 4 times

Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate on FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

- A. A local wildcard administrator account
- B. An administrator group
- C. One or more remote LDAP servers
- D. LDAP servers IP addresses added as trusted hosts

Suggested Answer: AC

Community vote distribution

BC (100%)

 **ae0cbf3** 1 week, 4 days ago

Selected Answer: AC

A and C.

Why A and C correct:

A. A local wildcard administrator account

- This is required to allow any LDAP user or group of users to log in without creating individual accounts for each user. The wildcard admin acts as a template that applies to all matching users.

C. One or more remote LDAP servers

- Required so FortiAnalyzer can query the LDAP directory to authenticate users in the group


Why B and D incorrect:

B. An administrator group

- Not needed when using wildcard admin account. You're not mapping group names directly in this case.

D. LDAP servers' IP addresses added as trusted hosts

- Not required for LDAP Auth, trusted hosts restrict WHO can login to FAZ, not HOW FAZ connects to LDAP
upvoted 1 times

 **aamrcl** 1 month, 1 week ago

Selected Answer: AC

A-C Page 80 FAZ 7.4

upvoted 1 times

 **12_tst2025** 3 months, 3 weeks ago

Selected Answer: AC

same answer as NSE5, mistake on last comment

upvoted 2 times

 **12_tst2025** 3 months, 3 weeks ago

Selected Answer: AB

same answer as NSE5

upvoted 1 times

 **truserud** 4 months, 1 week ago

Selected Answer: AC

Page 80 in the study guide specifically states:

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.

You can allow "MATCH ALL USERS ON REMOTE SERVER" option to allow administrators to log into FortiAnalyzer using their credentials on a remote authentication server. This option is useful for creating wildcard administrators and removed the need for FortiAnalyzer to store local credentials.

Thus A - A local wildcard administrator
and C - One or more LDAP servers
should be the correct answers.

upvoted 1 times

🗲️ 👤 **tovich** 4 months, 2 weeks ago

Selected Answer: B

True that this question is tricky, but here we have to think about configuring setting for a local wildcard administrator account. When you create a local wildcard administrator, after typing the user name field, you have to choose the admin type (local, radius, ldap, tacas+, pki, group, sso). if you choose local then you enter credentials and this is a local admin account, but if you choose one of the any remaining option, then you can select a remote server or remote server group. The answers are B and C

upvoted 1 times

🗲️ 👤 **JoyBoyMx** 5 months, 1 week ago

Selected Answer: AC

I believe it's A and C

Because the local wildcard administrator is not the administrator user itself, this wildcard calls to the remote LDAP users

upvoted 3 times

🗲️ 👤 **Toh85** 6 months, 1 week ago

Selected Answer: BC

Correct B and C

upvoted 1 times

🗲️ 👤 **darkstar15** 7 months, 1 week ago

The question is difficult to interpret, from my point of view if we respect the order of creating what is requested, first we would have to register the server and then the group.

The key word is in the question when it says: a single group.

I think "Wildcard" should be ruled out because it is not talking about "multiple remote admin".

Correct B and C

upvoted 3 times

🗲️ 👤 **Slikings** 7 months, 2 weeks ago

This question is tricky. In order to understand it you have to focus on the wording. "non-local" implies to not storing credentials locally on the FAZ.

There is no specific interpretation in the study guide on non-local administrators however we can assume that a local wildcard admin would not fulfill the non local portion of the question.

Therefore B & C is correct.

upvoted 2 times

🗲️ 👤 **TigerL** 7 months, 3 weeks ago

A & C are correct.

To ensure non-local administrators can login to a fortinet device, you need:

1. One or more remote LDAP servers configured.

2. Configure local wildcard administrator account by enabling the "Match all users on remote server"

upvoted 3 times

🗲️ 👤 **migdadcom** 8 months ago

Selected Answer: BC

B & C are correct,

most likely

upvoted 3 times

🗲️ 👤 **DBFront** 8 months, 1 week ago

Selected Answer: BC

B & C are correct, page 80 of the FortiAnalyzer 7.4 Admin Study Guide.



The answer cannot be "A" because that is a "local wildcard administrator account" and the question is how to configure to allow "non-local administrators" to authenticate.

upvoted 4 times

🗲️ 👤 **truserud** 4 months, 1 week ago

Where it states that you create a wildcard admin for the specific reason to not create local users, and allow remote users to authenticate against remote LDAP servers... So A & C is most correct.

upvoted 1 times


  **cheloreina3** 8 months, 2 weeks ago

To allow non-local administrators to authenticate on FortiAnalyzer using any account in an LDAP group, you need to configure two key settings:

One or more remote LDAP servers (C): You need to configure LDAP servers so that FortiAnalyzer can authenticate non-local users through LDAP. This allows LDAP users to log in without having to create local accounts on FortiAnalyzer.

A local wildcard administrator account (A): The wildcard administrator account allows any user authenticated through the LDAP server to log in as an administrator without creating individual admin accounts. Enabling the "Match all users on remote server" option simplifies authentication.

upvoted 3 times

  **Beatledrew** 8 months, 3 weeks ago

C and D, Page 106 of the Study Guide

upvoted 1 times

  **JoyBoyMx** 5 months, 1 week ago

Your answer should be for question 12, not this one

upvoted 1 times

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.

Suggested Answer: BD




Community vote distribution

BD (100%)

  **Slikings**  7 months, 2 weeks ago

- A. Is incorrect, Analytic logs are only available after you rebuild the DataBase.
- B. Is correct because Archived logs are moved when you move the device.
- C. Is incorrect because not all logs will be present. Analytical logs will not follow.
- D. Is correct because analytics are only available after you rebuild the DataBase.

upvoted 5 times

  **Noreki**  9 months ago

Correct are answers B and D.

Study Guide:

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.



upvoted 5 times

  **DBFront**  8 months, 1 week ago

Selected Answer: BD

B & D are correct, correct, page 175 of the FortiAnalyzer 7.4 Admin Study Guide.



upvoted 3 times

  **fa7474b** 8 months, 3 weeks ago

Selected Answer: BD

B and D are correct.

upvoted 3 times

  **juniou82** 8 months, 3 weeks ago

Selected Answer: BD

Correct are answers B and D.

upvoted 3 times

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 headers.
- 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.

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Slikings** 7 months, 2 weeks ago

A. Is correct because the Fortianalyzer discovers automatically if a device is in an HA cluster. However, if you register your device with FAZ before adding it to a cluster you can manually add the cluster within FAZ.

Per Page 176

- B. Is incorrect, this would be correct if they said Serial number.
- C. Is incorrect, I cannot find anything specifically on it detecting unavailable devices.
- D. Is incorrect, I have not seen anything about whether an HA cluster in A-P would cause conflict. It is also important to understand this is in the context of a Fortigate cluster in HA mode. Not a FAZ cluster in HA mode.

upvoted 4 times

🗳️ 👤 **migdadcom** 8 months ago

Selected Answer: A

A is the correct answer, adding a FortiGate HA Cluster it says you can add them together manually

upvoted 3 times

🗳️ 👤 **fa7474b** 8 months, 3 weeks ago

Selected Answer: A

This is A. In the self paced training - Managing Devices - Adding a Fortigate HA Cluster it says you can add them together manually. Also B is incorrect, the log message uses the SERIAL NUMBER, not the IP address to distinguish each cluster member.

upvoted 2 times

🗳️ 👤 **juniou82** 8 months, 3 weeks ago

Selected Answer: A

FortiAnalyzer_7.4_Administrator_Study_Guide-Online.pdf Pag. 176

upvoted 4 times

🗳️ 👤 **Noreki** 8 months, 3 weeks ago

Can someone confirm this?

Study Guide says it is recommended to add the devices before forming a cluster, so A) should be correct. Also I have read about the members being differentiated by serial number, but I'm not sure about that being the case in the log message headers.

upvoted 1 times

🗳️ 👤 **Beatledrew** 8 months, 2 weeks ago

Not by IP but by serial number. And it is in the log message headers. Right from page 176 of the study guide.

upvoted 2 times

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.

Suggested Answer: C

Community vote distribution

C (100%)

🗲️ 👤 **Slikings** 7 months, 2 weeks ago

Hardware raid supports hot swapping

Software raid requires a reboot and an extend LVM command

upvoted 2 times

🗲️ 👤 **066c9f3** 7 months, 3 weeks ago

Selected Answer: C

Hardware Raid supports hot swapping

upvoted 2 times

🗲️ 👤 **juniou82** 8 months, 3 weeks ago

Selected Answer: C

FortiAnalyzer_7.4_Administrator_Study_Guide-Online.pdf PAG. 130

upvoted 4 times

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 files.
- B. To encrypt log transfer between FortiAnalyzer and other devices.
- C. To create the secure channel used by the OFTP process.
- D. To verify the integrity of the log files received.

Suggested Answer: A

Community vote distribution

A (67%)

D (33%)

 **Slikings** Highly Voted 7 months, 2 weeks ago

It is important to understand that there are two right answers but one is only partly right. A and D both with verify the integrity by using the hash however, the question includes the md5-auth portion. The Auth tells me that the question is asking you to define the difference between the md5 command and the md5-auth command.

A. is correct because the command sets the hash and authentication code due to the md5-auth portion of the command.

B. is incorrect because encryption is different than the checksum encryption concerns log security Checksums involve the hash which confirms integrity.

C. is incorrect because OFTP process involves encryption and the transfer of data not the integrity of it.

D. is incorrect but only partly, the addition of the -auth adds the authentication code. Without the auth then it would only verify the integrity.

upvoted 6 times

 **PazUK** Highly Voted 7 months, 2 weeks ago

---According to Fortinet, the correct answer is A.

MD5: Record the log file's MD5 hash value only.

MD5-auth: Record the log file's MD5 hash value and authentication code.

```
configure system global
```

```
set log-checksum {md5 | md5-auth | none}
```

```
end
```


upvoted 6 times

 **Toh85** Most Recent 6 months ago

Selected Answer: A

MD5-auth: Record the log file's MD5 hash value and authentication code.

upvoted 2 times


 **DrazenSego** 6 months, 2 weeks ago

Selected Answer: A

I thought it was D, but looking at: docs.fortinet.com/document/fortianalyzer/7.6.1/administration-guide/410387/appendix-b-log-integrity-and-secure-log-transfer it is A.

A is correct.



upvoted 1 times

 **jdubyah_** 6 months, 2 weeks ago

Selected Answer: A

Per page 191 of the Study Guide.



upvoted 1 times

  **aamrcl** 7 months, 1 week ago

Selected Answer: A

A is correct.



upvoted 2 times

  **066c9f3** 7 months, 3 weeks ago

Selected Answer: D

Study Guide page 191, "To prevent logs from being tamperd (...)"



upvoted 3 times

  **066c9f3** 7 months, 3 weeks ago

Selected Answer: A


Study Guide page 191, "To prevent logs from being tamperd (...)" - so I'd go with A, anti-tampering has to do with integrity

upvoted 2 times

  **066c9f3** 7 months, 3 weeks ago

D, sorry



upvoted 2 times

  **ajgonzal** 8 months ago

Selected Answer: D



El comando set log-checksum md5-auth se utiliza para generar un valor de hash que permita verificar la integridad de los archivos de registro. Este mecanismo asegura que los registros no hayan sido alterados desde que fueron generados.

upvoted 1 times

  **darkstar15** 7 months, 1 week ago

ajgonzal, a mi parecer es como esta planteando la pregunta. esta preguntando que hace propiamente el comando. la respuesta seria la A. Saludos.


upvoted 1 times

  **DBFront** 8 months, 1 week ago

Selected Answer: A

A is correct,

upvoted 2 times

  **Beatledrew** 8 months, 3 weeks ago

Page 191 of the Study Guide

upvoted 1 times

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

Suggested Answer: A

Community vote distribution

A (83%)




C (17%)

  **juniou82**  8 months, 3 weeks ago

Selected Answer: A

FortiAnalyzer_7.4_Administrator_Study_Guide-Online.pdf PAG. 128

upvoted 5 times

  **ae0cbf3**  1 week, 4 days ago

Selected Answer: A

A is correct because:

- Raid 10 (1+0) combines mirroring (Raid 1) and striping (Raid 0)
- Requires a minimum of 4 disks
- Disks are paired into mirrored sets, then those sets are striped for performance
- With 4 disks, each of 2TB the disks are paired into two mirrors (each mirror = 2TB, because one disk is a copy of the other), then the mirrors are striped, so: 2TB + 2TB = 4TB total usable space.

The rest are incorrect because:

- B - describes Raid 5 or 6 (which use parity), Raid 10 does NOT use distributed parity
- C - that would be true for RAID 1 only, not raid 10. This statement underestimates the total usable space in a Raid 10. Raid 1 uses mirroring only with 4 disks = 2TB usable (if all mirror each other). Raid 10 (mirroring and striping) with 4 disks = 4TB usable.
- D - describes Raid 0, which has no fault tolerance, raid 10 uses mirroring and striping, not just striping

upvoted 1 times

  **txami** 5 months, 1 week ago

Selected Answer: A



Regardless a FAZ systems, RAID 10 with four 2TB disk capacity is:

- 2TB + 2TB mirrored= 2TB
- 2TB + 2TB mirrored= 2TB

Then, both mirrors runs in stripe, providing a total of 4TB

A is the Correct.

upvoted 1 times

  **Slikings** 7 months, 2 weeks ago

- A. is Correct because Raid 10 uses mirroring and striping. Therefore for each disk there must be one mirrored disk.
- B. is incorrect, it does not include distributed parity.
- C. is incorrect, it does not represent raid 10 rather more closely to raid 1
- D. Is incorrect, striping does not provide fault tolerance. It increases space and performance. Mirroring increases fault tolerance by creating a mirrored drive to replace in the case of failure.

upvoted 3 times

  **ajgonzal** 8 months ago

Selected Answer: C

RAID 10 (1+0) combina espejado (mirroring) y división de datos (striping), lo cual ofrece tanto tolerancia a fallos como mejoras en el rendimiento. En esta configuración, la capacidad efectiva es la mitad de la suma de los discos, debido al uso del espejado. Por lo tanto, con cuatro discos de 2 TB cada uno, el espacio total disponible es de 2 TB.

upvoted 2 times

  **DBFront** 8 months ago

Wrong, answer is A. (4 drives, each at 2TB in a RAID 10 will result in a 4TB volume)



upvoted 5 times

  **migdadcom** 8 months ago

Selected Answer: A

RAID 1 will be mirroring and still RAID 0 use striped data storage technique!

upvoted 2 times

  **cheloreina3** 8 months, 2 weeks ago

When configuring RAID 10 (1+0) on FortiAnalyzer, it combines both mirroring (RAID 1) and striping (RAID 0), providing fault tolerance and performance. With RAID 10, half of the total disk space is used for mirroring (data redundancy), while the other half is available for use.



For example, if you have four disks, each with 2 TB of capacity, RAID 10 will mirror the data between pairs of disks. As a result, you will have 2 TB of usable space because half of the total storage is dedicated to mirroring for redundancy.

A is incorrect because the total usable space cannot be 4 TB due to mirroring.

C is correct: a four-disk configuration (2 TB each) provides 2 TB of usable space.

So, the correct answer is C.

upvoted 3 times

  **cheloreina3** 8 months, 2 weeks ago

I realize I made an error in my previous response. After reviewing the concept of RAID 10, the correct answer is A.

In RAID 10, with four 2 TB disks, you have a total capacity of 8 TB. Since RAID 10 uses mirroring, it effectively halves the usable space, leaving you with 4 TB of usable storage.

I apologize for the confusion in my earlier response, and thank you for pointing that out!

upvoted 5 times

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

FortiAnalyzer HA cluster settings

Cluster Settings			
Operation Mode	<input type="radio"/> Standalone <input checked="" type="radio"/> Active-Passive <input type="radio"/> Active-Active		
Preferred Role	<input type="radio"/> Secondary <input checked="" type="radio"/> Primary		
Cluster Virtual IP			
IP Address and Interface	IP Address	Interface	Action
	192.168.101.222	port1	<input type="button" value="x"/> <input type="button" value="+"/>
Cluster Settings			
Peer IP and Peer SN	Peer IP	Peer SN	Action
	10.0.1.210	FAZ-VM0000065040	<input type="button" value="x"/> <input type="button" value="+"/>
Group Name	Training		
Group ID	1 (1-255)		
Password <input type="button" value="eye"/>		
Heart Beat Interval	10 Seconds		
Heart Beat Interface	port1		
Failover Threshold	30		
Priority	120 (80-120)		
Log Data Sync	<input checked="" type="checkbox"/>		

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.

Suggested Answer: D

Community vote distribution

D (100%)

Slikings 7 months, 2 weeks ago

- A. Is incorrect because FAZ only forwards logs to peers in active active
- Active-passive acts as a redundant FAZ.
- B. Is incorrect, I think because the heart beat interval does not dictate the failover threshold rather just each heart beat.
- C. Is incorrect, While the FAZ does route traffic through a gateway it is not part of the HA cluster process.
- D. Is correct, without a failover even if the device is set to primary as a preferred role it only matters in the initial election process and does not trigger a failover of an existing cluster. If a failover were to be triggered to an existing cluster then priority would be the deciding factor followed by highest IP.

upvoted 3 times



DBFront 8 months, 1 week ago

Selected Answer: D

D is correct, page 138 of the FortiAnalyzer 7.4 Admin Study Guide.

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.

upvoted 3 times

  **juniou82** 8 months, 3 weeks ago

Correct is D

seems to be a trick question.

The answer can be found in FortiAnalyzer_7.4_Administrator_Study_Guide-Online.pdf page 138

upvoted 3 times

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

Suggested Answer: CD

Community vote distribution

CD (100%)

  **Slikings**  7 months, 2 weeks ago

- A. Incorrect, Total Quota = Total space - reserved space
- B. Incorrect, License type only affects data pushed through per day not total storage
- C. Correct, Raid level determines how much space is used for processes
- D. Correct, Disk size determines the overall size of space that the raid array has to work with.

upvoted 5 times

  **secced**  7 months, 1 week ago

Selected Answer: CD

duplicate question, i't normal?

upvoted 1 times

  **migdadcom** 8 months ago

Selected Answer: CD

Correct answer is C & D

upvoted 2 times

  **Beatledrew** 8 months, 3 weeks ago

Correct C&D page 164 of the Study Guide

upvoted 4 times

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: [masked] [X] [eye] [!]

Confirm Password: [masked] [X] [eye] [!]

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.

Suggested Answer: A

Community vote distribution

A (100%)

darkstar15 7 months, 1 week ago

The answer is A. You are asking why you need to set a password.
upvoted 1 times

Slikings 7 months, 2 weeks ago

- A. Is correct, since the admin type is set to LDAP it will verify credentials against the LDAP server. Without the wildcard, a password is required locally.
- B. is incorrect, in this case the password is for when it cant validate against the LDAP server.
- C. is incorrect, Policy doesnt matter in this case
- D. Is incorrect, there is no requirement for restricted users

It is important to remember in this case that they want you to understand the function of the wildcard setting. without enabling it, if you have LDAP selected and an LDAP server configured then you must provide a password.

upvoted 2 times

DBFront 8 months, 1 week ago

Selected Answer: A

A is correct, page 80 of the FortiAnalyzer 7.4 Admin Study Guide.
upvoted 2 times

In a Fortinet Security Fabric, what can make an upstream FortiGate create traffic logs associated with sessions initiated on downstream FortiGate devices?

- A. The traffic destination is another FortiGate in the fabric.
- B. The upstream FortiGate is configured to do NAT.
- C. Log redundancy is configured in the fabric.
- D. The downstream device cannot connect to FortiAnalyzer.

Suggested Answer: B

🗲️ 👤 **Slikings** Highly Voted 👍 7 months, 2 weeks ago

- A. Incorrect, the only thing that changes the log it was received by is UTM and NAT logs
- B. Correct, UTM and NAT
- C. incorrect
- D. incorrect, all logs in the fabric appear as coming from the root FG

A session's traffic logging is always done by the first FG that handled it in the Fabric. FG devices in the fabric know the MAC of their upstream and downstream peers. It does not generate a log for packets coming from other FG's to eliminate the repeated logging of a session. The exception is if the upstream FG performs NAT, this is needed to record details such as translated ports and addresses. UTM logs are another exception.

upvoted 5 times

🗲️ 👤 **066c9f3** Most Recent 🕒 7 months, 3 weeks ago

Selected Answer: B

NATting needs to be performed, otherwise the session / log will count as one across all firewalls in the fabric. After NAT, a new log is generated.

upvoted 1 times

🗲️ 👤 **Beatledrew** 8 months, 3 weeks ago

Correct. B. Page 48 of the Study Guide

upvoted 4 times

Which two statements about high availability (HA) on FortiAnalyzer are true? (Choose two.)

- A. FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
- B. FortiAnalyzer HA active-passive mode can function without VRRP.
- C. All devices in a FortiAnalyzer HA cluster must run in the same operation mode, either analyzer mode or collector mode.
- D. All devices in a FortiAnalyzer HA cluster must have the same available disk space.

Suggested Answer: A

Community vote distribution

C (100%)

🗲️ 👤 **Beatledrew** Highly Voted 👍 8 months, 3 weeks ago
A&C. Page 135 and 137 of the Study Guide
upvoted 6 times

🗲️ 👤 **Slikings** Highly Voted 👍 7 months, 2 weeks ago
A. Is correct because HA supports synch of logs as well as configuration settings.
B. Is incorrect, A-P uses a layer 2 connection to create a virtual IP to communicate between devices.
C. Is correct, HA requires each device to function the same way in the case of a failover it must assume the primary role.
D. Is incorrect because the book says they dont have to have the same disk space
upvoted 5 times

🗲️ 👤 **Pomo1979** Most Recent ⌚ 2 months ago
Selected Answer: A
It should have two answers. Others gave explanation.
upvoted 1 times

🗲️ 👤 **harizmr** 4 months ago
Selected Answer: A
A&C, it should be 2 answer
upvoted 1 times

🗲️ 👤 **jdubyah_** 6 months, 2 weeks ago
Selected Answer: C
A and C per page 135 of the Study Guide.
upvoted 1 times

🗲️ 👤 **migdadcom** 8 months ago
Selected Answer: C
A & C make scene
upvoted 5 times

🗲️ 👤 **juniou82** 8 months, 3 weeks ago
A and C
upvoted 4 times

🗲️ 👤 **Noreki** 8 months, 3 weeks ago
It's A and C.
upvoted 4 times