



Free Questions for CV0-004 by certsCare

Shared by Richardson on 19-02-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You are a cloud engineer working for a cloud service provider that is responsible for an IaaS offering.

Your customer, who creates VMs and manages virtual storage, has noticed I/O bandwidth issues and low IOPS (under 9000).

Your manager wants you to verify the proper storage configuration as dictated by your service level agreement (SLA).

The SLA specifies:

- . Each SFP on the hypervisor host must be set to the maximum link speed allowed by the SAN array. . All SAN array disk groups must be configured in a RAID 5.
- . The SAN array must be fully configured for redundant fabric paths. . IOPS should not fall below 14000

INSTRUCTIONS

Click on each service processor to review the displayed information. Then click on the drop-down menus to change the settings of each device as necessary to conform to the SLA requirements.

Hypervisor



Slot A fiber channel

Port 1 link speed

16 Gbps

Fabric switch A



Slot B fiber channel

Port 1 link speed

4 Gbps

Fabric switch B



Fabric switch A

(WWPN pool: 50:00:00:25)

Initiator table

SAN

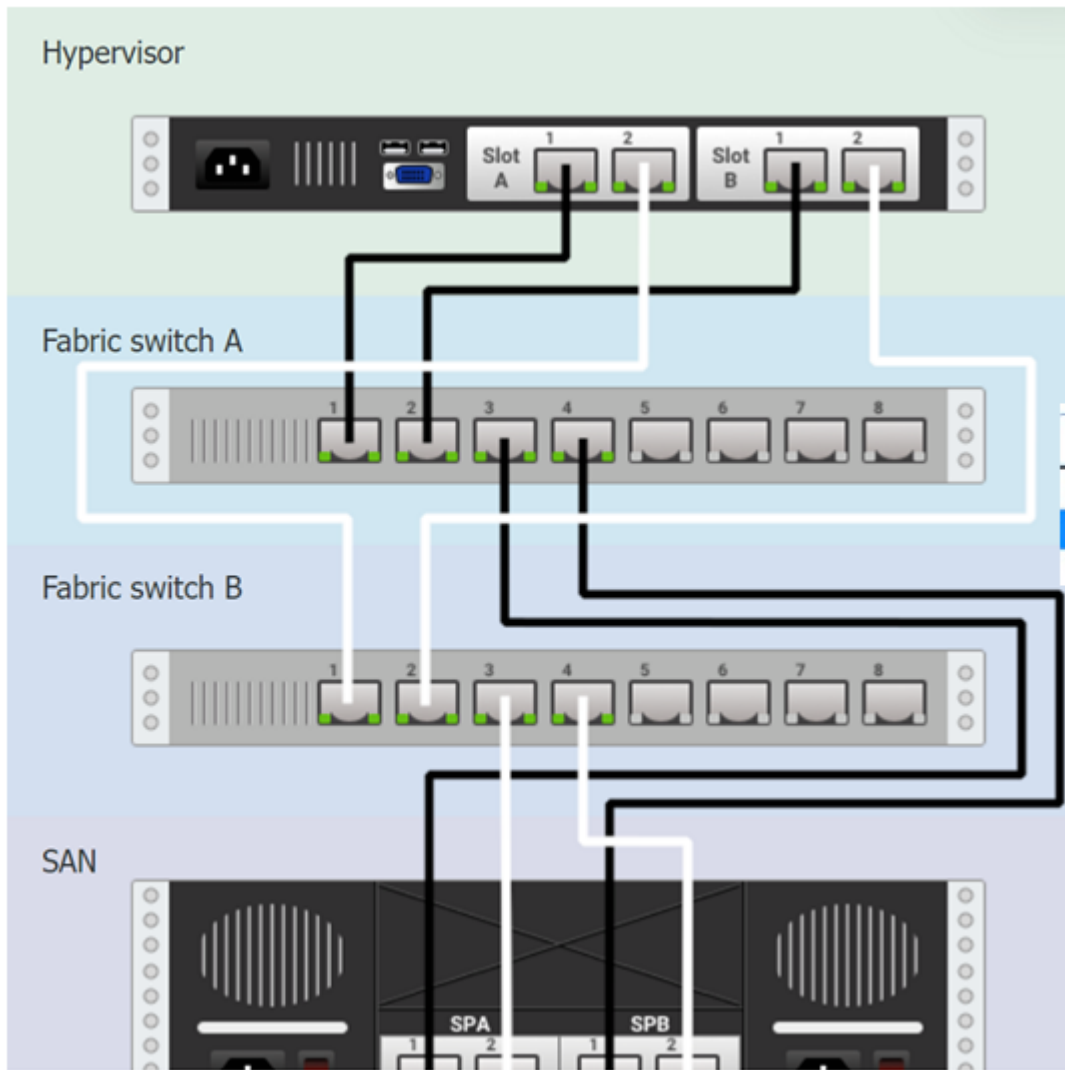


Fabric switch B

(WWPN pool: 50:00:00:25)

Initiator table

Search



Slot A fiber channel card

Port 1 link speed	Port 2 link speed
16 Gbps	16 Gbps
8 Gbps	8 Gbps
16 Gbps	16 Gbps
4 Gbps	4 Gbps

Slot B fiber channel card

Port 1 link speed	Port 2 link speed
16 Gbps	16 Gbps
8 Gbps	8 Gbps
16 Gbps	16 Gbps
4 Gbps	4 Gbps

Fabric switch A

(WWPN pool: 50:00:00:25:B5:A0:23:00 - 50:00:00:25:B5:A0:23:09)

Initiator table

- 50:00:00:25:B5:A0:23:02
- 50:00:00:25:B5:A0:23:02**
- 50:00:00:25:B5:B0:23:05
- 50:00:00:25:B5:D0:23:07
- 50:00:00:25:B5:B0:23:04
- 50:00:00:25:B5:A0:23:01
- 50:00:00:25:B5:D0:23:06

Fabric switch B

(WWPN pool: 50:00:00:25:B5:B0:23:00 - 50:00:00:25:B5:B0:23:09)

Initiator table

- 50:00:00:25:B5:A0:23:02
- 50:00:00:25:B5:A0:23:02**

Service processor A details



"no initiators currently logged in"

SP-A module 0 Port 0	8 Gbps
-----------------------------	--------

SP-A module 0 Port 1	8 Gbps
-----------------------------	--------

Disk groups	1
--------------------	---

RAID level	5
-------------------	---

Service processor B details

"50:00:00:25:B5:A0:23:02 - logged in"

"50:00:00:25:B5:B0:23:04 - logged in"

SP-B module 0 Port 0	8 Gbps
SP-B module 0 Port 1	8 Gbps
Disk groups	1
RAID level	5

Options:

A- See the explanation for complete solution

Answer:

A

Explanation:

Based on the SLA requirements and the information provided in the diagram:

For the Hypervisor:

Slot A fiber channel card:

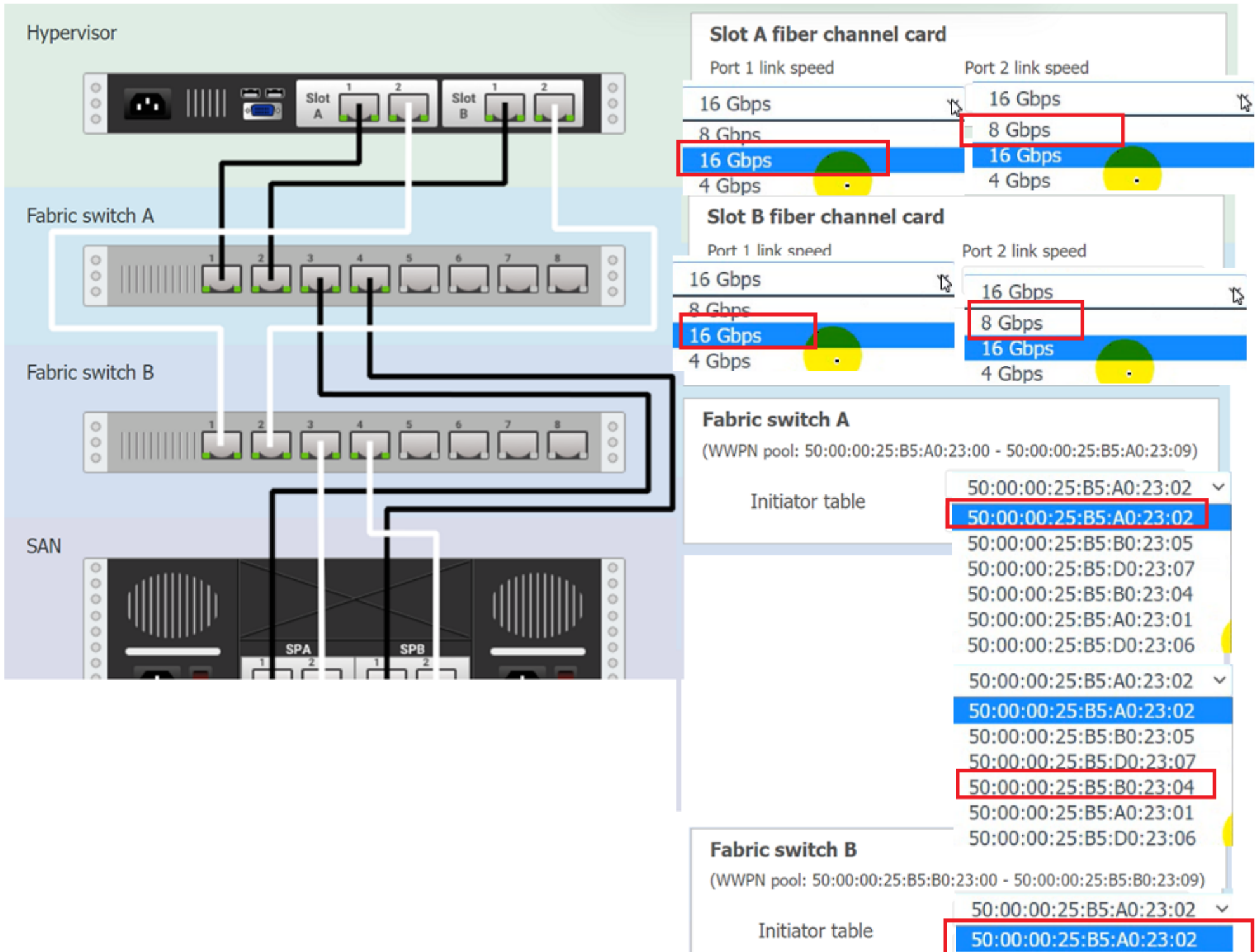
Port 1 link speed should be set to 16 Gbps since it's connected to Fabric switch A which supports 16 Gbps.

Port 2 link speed should be set to 8 Gbps because it's connected to Fabric switch B which supports up to 8 Gbps.

Slot B fiber channel card:

Port 1 link speed should be set to 16 Gbps since it's connected to Fabric switch A which supports 16 Gbps.

Port 2 link speed should be set to 8 Gbps because it's connected to Fabric switch B which supports up to 8 Gbps.



Hypervisor



Fabric switch A



Fabric switch B



SAN



Slot A fiber channel card

Port 1 link speed	Port 2 link speed
16 Gbps	16 Gbps
8 Gbps	8 Gbps
16 Gbps	16 Gbps
4 Gbps	4 Gbps

Slot B fiber channel card

Port 1 link speed	Port 2 link speed
16 Gbps	16 Gbps
8 Gbps	8 Gbps
16 Gbps	16 Gbps
4 Gbps	4 Gbps

Fabric switch A

(WWPN pool: 50:00:00:25:B5:A0:23:00 - 50:00:00:25:B5:A0:23:09)

Initiator table

- 50:00:00:25:B5:A0:23:02
- 50:00:00:25:B5:A0:23:02**
- 50:00:00:25:B5:B0:23:05
- 50:00:00:25:B5:D0:23:07
- 50:00:00:25:B5:B0:23:04
- 50:00:00:25:B5:A0:23:01
- 50:00:00:25:B5:D0:23:06

Fabric switch B

(WWPN pool: 50:00:00:25:B5:B0:23:00 - 50:00:00:25:B5:B0:23:09)

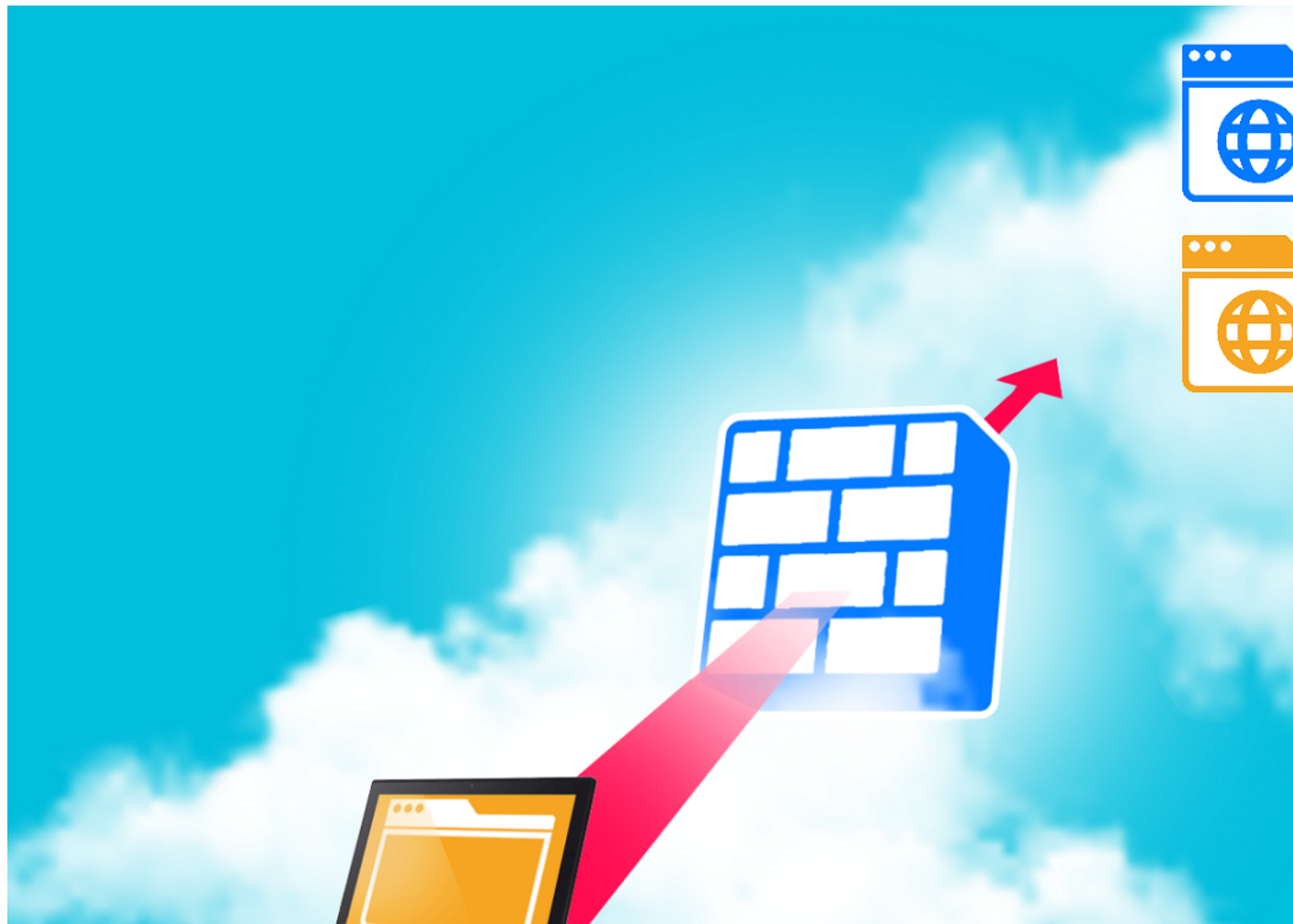
Initiator table

- 50:00:00:25:B5:A0:23:02
- 50:00:00:25:B5:A0:23:02**

Question 2

Question Type: MultipleChoice


A company hosts various containerized applications for business uses. A client reports that one of its routine business applications fails to load the web-based login prompt hosted in the company cloud.




INSTRUCTIONS

Click on each device and resource. Review the configurations, logs, and characteristics of each node in the architecture to diagnose the issue. Then, make the necessary changes to the WAF configuration to remediate the issue.


Web app 1

Web app 1 			
SVC_Host	SVC_Name	SVC IP	SVC_Port
webapp1	FIN	10.22.10.11	443

Web app 2

Web app 2 			
SVC_Host	SVC_Name	SVC IP	SVC_Port
webapp2	VIDEO	10.22.10.21	443

Web app 3

Web app 3 			
SVC_Host	SVC_Name	SVC IP	SVC_Port
webapp3	API	10.22.10.31	443

Web app 4

Web app 4



SVC_Host	SVC_Name	SVC IP	SVC_Port
webapp4	CHAT	10.22.10.41	443

Client app

Client app



Client laptop

App config

https_enabled

true

cert_status

valid

start

login

Client app



Client laptop

App config

Host

client142

IP

192.168.10.142

WAF

Edit config

WAF logs

Rule ID	Description	Service
1001	Brute-force attempt	<input type="text" value="^https://webapp[.]comptia[.]org/\$"/>
1002	Botnet	<input type="text" value="^https://webapp[.]comptia[.]org/\$"/>
1003	API web server	<input type="text" value="^https://webapp3[.]comptia[.]org/([0-9A-Za-z][0-9A-Za-z_-?]*/*)*\$"/>
1004	Chat web traffic	<input type="text" value="^https://webapp4[.]comptia[.]org/chat/request[.]php\$"/>
1005	Finance application 1	<input type="text" value="^https://webapp1[.]comptia[.]org/([0-9A-Za-z][0-9A-Za-z_-?]*/*)*\$"/>
1006	Finance application 2	<input type="text" value="^https://webapp1[.]comptia[.]org/login[.]html\$"/>
1007	Video application	<input type="text" value="^https://webapp2[.]comptia[.]org/video/stream\$"/>

WAF

Edit config

WAF logs

...

Dec 12 21:50:45 10.1.105.1 CEF:0|Sec|Gateway|1.0|WAF|WAF_INSPECT|5|src=192.168.11.129 spt=39110 method=POST request="PASS991!!" msg=Unauthorized content. cn1=2002 cn2=104 cs1= cs2= cs3= cs4=ALERT cs5=2020 act=blocked

Dec 12 22:20:17 10.1.105.1 CEF:0|Sec|Gateway|1.0|WAF|WAF_STARTURL|6|src=192.168.10.142 spt=48909 method=GET request=https://webapp1.comptia.org/FIN/login.html msg=Start URL Check Failed. cn1=1005 cn2=248 cs1= cs2= cs3=

Dec 12 22:23:20 10.1.105.1 CEF:0|Sec|Gateway|1.0|WAF|WAF_STARTURL|1|src=192.168.11.129 spt=38995 method=GET request=https://webapp2.comptia.org/VIDEO/stream msg=Start URL Check Passed. cn1=1007 cn2=106 cs1= cs2= cs3=

Dec 12 22:23:20 10.1.105.1 CEF:0|Sec|Gateway|1.0|WAF|WAF_STARTURL|1|src=192.168.10.142 spt=49015 method=GET request=https://webapp4.comptia.org/CHAT/request.php msg=Start URL Check Passed. cn1=1004 cn2=332 cs1= cs2= cs3=

Dec 12 22:25:01 10.1.105.1 CEF:0|Sec|Gateway|1.0|WAF|WAF_URIINSPECT|2|src=192.168.10.142 spt=49117 method=G request=https://webapp3.comptia.org/api?reqStatus=1 msg=Log sensitive request. cn1=1003 cn2=432 cs1= cs2= cs3=

...

Reset to Default

Options:

A- Check the Explanation for the complete Solution

Answer:

A

Explanation:

The issue is with Web app 1 (Finance application).

From the WAF logs, we can see that requests to <https://webapp1.comptia.org/FIN/login.html> are being blocked (Rule ID 1006). The rule is configured to block access to the finance application's login page. This corresponds to the reported issue of the web-based login prompt not loading.

To remediate the issue, the WAF configuration for Rule ID 1006 should be changed from 'Block' to 'Allow'. This will enable the web-based login prompt to load for the client.

Additionally, the client app configuration indicates that the client laptop (IP 192.168.10.142) is trying to access the service, and the WAF logs show that requests from this IP are being blocked due to the current rule set. Changing the action for Rule ID 1006 will also ensure that legitimate attempts to access the login page from this IP are not blocked.

Steps for remediation:

Go to the WAF configuration.

Find Rule ID 1006 for the Finance application 1.

Change the action from 'Block' to 'Allow'.

Save the changes.

Web application firewall (WAF) configurations typically include rules that define which traffic should be allowed or blocked. Blocking legitimate traffic to login pages can prevent users from accessing the application, which seems to be the case here.

Client application configurations and WAF logs provide valuable insights into the source of the traffic and the rules that are affecting it. It's important to ensure that the rules align with the intended access policies for the application.

Question 3

Question Type: MultipleChoice

A company serves customers globally from its website hosted in North America

a. A cloud engineer recently deployed new instances of the website in the Europe region. Which of the following is the most likely reason?

Options:

- A- To simplify workflow
- B- To enhance security
- C- To reduce latency
- D- To decrease cost

Answer:

C

Explanation:

The most likely reason for deploying new instances of a website in the Europe region, in addition to the ones hosted in North America, is to reduce latency for users located in Europe. By having the website's resources closer to the end-users, the data has a shorter distance to travel, resulting in faster load times and better performance. Reference: CompTIA Cloud+ Study Guide (Exam CV0-004) by Todd Montgomery and Stephen Olson

Question 4

Question Type: MultipleChoice

A cloud administrator recently created three servers in the cloud. The goal was to create ACLs so the servers could not communicate with each other. The servers were configured

with the following IP addresses:

	Server 1	Server 2	Server 3
IP address	172.16.12.7	172.16.12.14	172.16.13.4
Subnet mask	255.255.255.240	255.255.255.240	255.255.255.240
Default gateway	172.16.12.1	172.16.12.17	172.16.13.15

After implementing the ACLs, the administrator confirmed that some servers are still able to reach the other servers. Which of the following should the administrator change to

prevent the servers from being on the same network?

Options:

A- The IP address of Server 1 to 172.16.12.36

B- The IP address of Server 1 to 172.16.12.2

C- The IP address of Server 2 to 172.16.12.18

D- The IP address of Server 2 to 172.16.14.14

Answer:

B

Explanation:

To prevent the servers from being on the same network and communicating with each other, the administrator should change the IP address of Server 1 to 172.16.12.2. This IP address is outside the subnet defined by the subnet mask 255.255.255.240, which would place Server 1 on a different subnet, preventing direct communication without routing. Reference: CompTIA Cloud+ Study Guide (Exam CV0-004) by Todd Montgomery and Stephen Olson

Question 5

Question Type: MultipleChoice

A systems administrator is configuring backups on a VM and needs the process to run as quickly as possible, reducing the bandwidth on the network during all times from Monday through Saturday. In the event of data corruption, the management team expects the mean time to recovery to be as low as possible. Which of the following backup methods can the administrator use to accomplish these goals?

Options:

- A- Incremental backup daily to the cloud
- B- Full backup on Sunday and incremental backups on all other days of the week
- C- Differential backup daily to the cloud
- D- Incremental backups during off-hours on Monday, Wednesday, and Friday

Answer:

B

Explanation:

To achieve a quick backup process and reduce bandwidth use, the administrator should perform a Full backup on Sunday and incremental backups on all other days of the week. This method ensures that only the changes made since the last full backup are copied, reducing the amount of data that needs to be transferred each time, and thus the time and bandwidth required. Reference: CompTIA Cloud+ Study Guide (Exam CV0-004) by Todd Montgomery and Stephen Olson

Question 6

Question Type: MultipleChoice

An IT manager needs to deploy a cloud solution that meets the following requirements:

. Users must use two authentication methods to access resources.

* Each user must have 10GB of storage space by default.

Which of the following combinations should the manager use to provision these requirements?

Options:

A- OAuth 2.0 and ephemeral storage

B- OIDC and persistent storage

C- MFA and storage quotas

D- SSO and external storage

Answer:

C

Explanation:

The combination that should be used to provision the requirements of two authentication methods and 10GB of storage space by default for each user is Multi-Factor Authentication (MFA) and storage quotas. MFA provides an additional layer of security beyond just a username and password, and storage quotas can be used to allocate a specific amount of storage space for each user. Reference: CompTIA Cloud+ Study Guide (Exam CV0-004) by Todd Montgomery and Stephen Olson

Question 7

Question Type: MultipleChoice

A systems administrator notices a surge of network traffic is coming from the monitoring server. The administrator discovers that large amounts of data are being downloaded to an external source. While investigating, the administrator reviews the following logs:

Protocol	Local address	Foreign address	State
TCP	10.181.12.5:20	172.17.250.12	ESTABLISHED
TCP	10.181.12.5:22	172.32.58.39	ESTABLISHED
TCP	10.181.12.5:443	172.30.252.204	ESTABLISHED
TCP	10.181.12.5:4443	10.11.15.82	ESTABLISHED
TCP	10.181.12.5:8048	172.24.255.192	TIME_WAIT

Which of the following ports has been compromised?

Options:

A- Port 20

B- Port 22

C- Port 443

D- Port 4443

E- Port 8048

Answer:

E

Explanation:

Based on the logs provided, the port that has been compromised is Port 8048. The state 'TIME_WAIT' indicates that this port was recently used to establish a connection that has now ended. This could be indicative of the recent activity where large amounts of data were downloaded to an external source, suggesting a potential security breach. Reference: CompTIA Cloud+ Study Guide (Exam CV0-004) by Todd Montgomery and Stephen Olson

Question 8

Question Type: MultipleChoice

Which of the following best describes a system that keeps all different versions of a software separate from each other while giving access to all of the versions?

Options:

- A- Code documentation
- B- Code control
- C- Code repository
- D- Code versioning

Answer:

D

Explanation:

A system that keeps all different versions of software separate from each other while providing access to all of the versions is best described by Code versioning. Code versioning systems, such as Git, allow developers to keep track of changes, revert to previous

states, and manage multiple versions of codebases. Reference: CompTIA Cloud+ Study Guide (Exam CV0-004) by Todd Montgomery and Stephen Olson

Question 9

Question Type: MultipleChoice

A company wants to implement a work environment that will have low operational overhead and highly accessible enterprise resource planning, email, and data resources. Which of the following cloud service models should the company implement?

Options:

- A- IaaS
- B- PaaS
- C- DBaaS
- D- SaaS

Answer:

D

Explanation:

A company that requires low operational overhead and highly accessible enterprise resources would benefit from implementing Software as a Service (SaaS). SaaS provides access to applications hosted in the cloud, eliminating the need for internal infrastructure or application development, which aligns with the requirement of having low operational overhead. Reference: CompTIA Cloud+ Study Guide (Exam CV0-004) by Todd Montgomery and Stephen Olson

Question 10

Question Type: MultipleChoice

A cloud service provider requires users to migrate to a new type of VM within three months. Which of the following is the best justification for this requirement?

Options:

- A- Security flaws need to be patched.
- B- Updates could affect the current state of the VMs.
- C- The cloud provider will be performing maintenance of the infrastructure.
- D- The equipment is reaching end of life and end of support.

Answer:

D

Explanation:

The best justification for a cloud service provider requiring users to migrate to a new type of VM within a specific time frame is that the equipment is reaching end of life and end of support (EOL/EOS). This means that the older type of VM will no longer receive updates or support, which could include important security patches, so it is necessary to move to newer VM types to maintain security and performance. Reference: CompTIA Cloud+ Study Guide (Exam CV0-004) by Todd Montgomery and Stephen Olson

Question 11

Question Type: MultipleChoice

Following a ransomware attack, the legal department at a company instructs the IT administrator to store the data from the affected virtual machines for a minimum of one year.

Which of the following is this an example of?

Options:

- A- Recoverability
- B- Retention
- C- Encryption
- D- Integrity

Answer:

B

Explanation:

The instruction by the legal department to store data from the affected virtual machines for a minimum of one year is an example of data Retention. Retention policies are often driven by regulatory compliance requirements and dictate how long certain types of data must be kept before they can be securely disposed of. Reference: CompTIA Cloud+ Study Guide (Exam CV0-004) by Todd Montgomery and Stephen Olson

To Get Premium Files for CV0-004 Visit

<https://www.p2pexams.com/products/cv0-004>

For More Free Questions Visit

<https://www.p2pexams.com/comptia/pdf/cv0-004>

