Free Questions for C90.03 by actualtestdumps

Shared by Spears on 06-06-2022
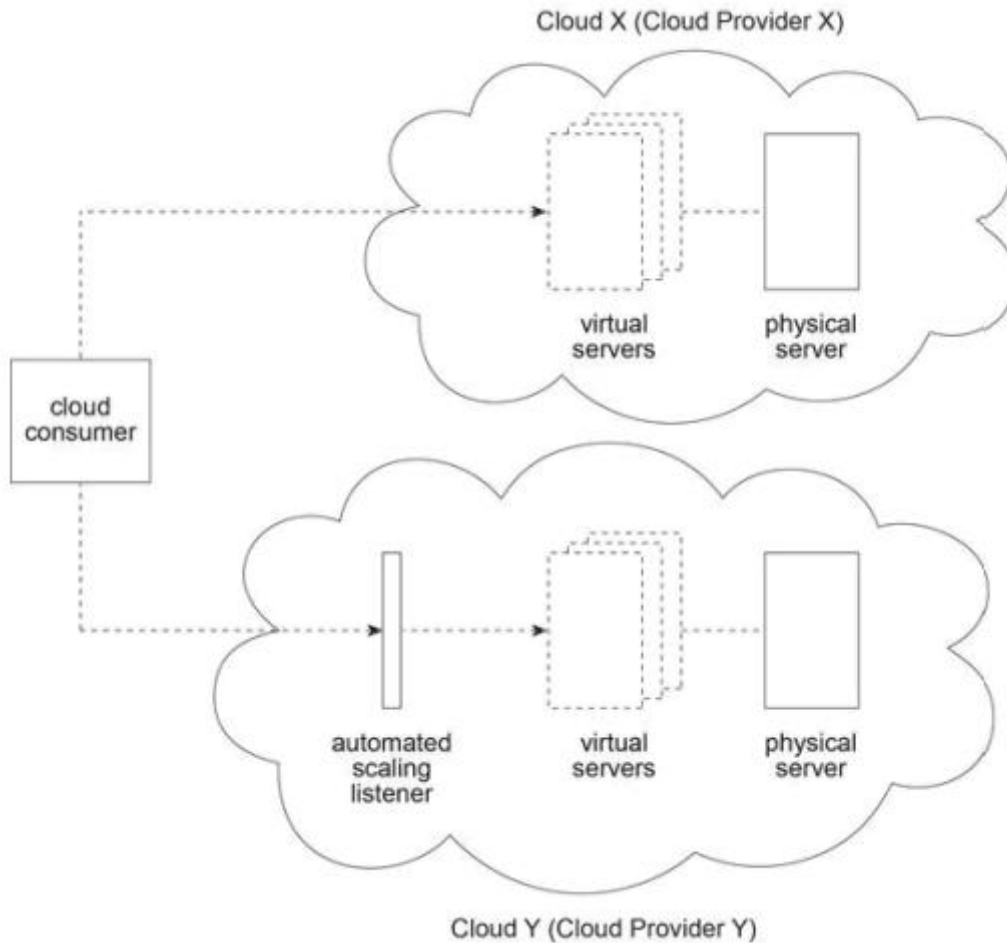
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

A cloud consumer is interested in leasing cloud-based virtual servers. It compares the virtual servers offered by Cloud Provider X and Cloud Provider Y. Cloud X (owned by Cloud Provider X) and Cloud Y (owned by Cloud Provider Y) both provide shared physical servers that host multiple virtual servers for other cloud consumers. The virtual servers on Cloud X are accessed directly, whereas the virtual servers on Cloud Y are accessed via an automated scaling listener. On Cloud X, virtual servers are pre-configured to support a specific amount of concurrent cloud service consumers. When this threshold is exceeded, cloud service consumer requests are rejected. Due to the use of the automated scaling listener, virtual servers on Cloud Y can provide a greater level of elasticity.

Cloud X (Cloud Provider X)

virtual servers

physical server

cloud consumer

automated scaling listener

virtual servers

physical server

Cloud Y (Cloud Provider Y)

The hourly cost to the cloud consumer to use a virtual server on Cloud X is half that of the cost to use a virtual server on Cloud Y. Within a one month period, Cloud Provider X bases its hourly charge on the maximum number of virtual servers used. Within a one month period, Cloud Provider Y bases its hourly charges on actual virtual server usage. Cloud Provider Y charges $20 for each hour that a cloud consumer uses a virtual server. The cloud consumer predicts its monthly usage requirements to be as follows:

Number Of Virtual Servers

Usage

3

20 Hours

4

30 Hours

5

50 Hours

The cloud consumer is required to choose the cloud provider with the lowest on-going cost, based on its predicted usage. Which of the following statements accurately calculates the on-going usage costs of Cloud Providers X and Y and correctly states the cloud provider that the cloud consumer must choose?

Options:

A- The total usage duration is (20 + 30 + 50) x 12 hours = 1,200 hours.
The actual usage is (20 X 3) + (30 X4) + (50 X 5) server hours = 430 server hours.
The cost of using virtual servers from Cloud ProviderXis12X5X$10 = $600.
The cost of using virtual servers from Cloud Provider Y is 430 X $20 = $8,600.
The cloud consumer must therefore choose Cloud Provider X.

B- The total usage duration is (20 + 30 + 50) hours = 100 hours.

The actual usage is (20 + 30 + 50) X 5 server hours = 500 server hours.

The cost of using virtual servers from Cloud Provider X is (500 X 5 X$10) = $25,000.

The cost of using virtual servers from Cloud Provider Y is (500 X $20) = $10,600.

The cloud consumer must therefore choose Cloud Provider Y.

C- The total usage duration is (3 x 20) + (4 x 30) + (5 x 50) hours = 430 hours.

The actual usage is (20 + 30 + 50) hours = 100 hours.

The cost of using virtual servers from Cloud Provider X is (430 X $10) = $4,300.

The cost of using virtual servers from Cloud Provider Y is (100 X $20) = $2,000.

The cloud consumer must therefore choose Cloud Provider Y.

D- The total usage duration is (20 + 30 + 50) hours = 100 hours.

The actual usage is (20X3)+ (30X4) + (50X5) hours =430 hours.

The cost of using virtual servers from Cloud Provider Xis100X5X$10 = $5,000.

The cost of using virtual servers from Cloud Provider Y is 430 X $20 = $8,600.
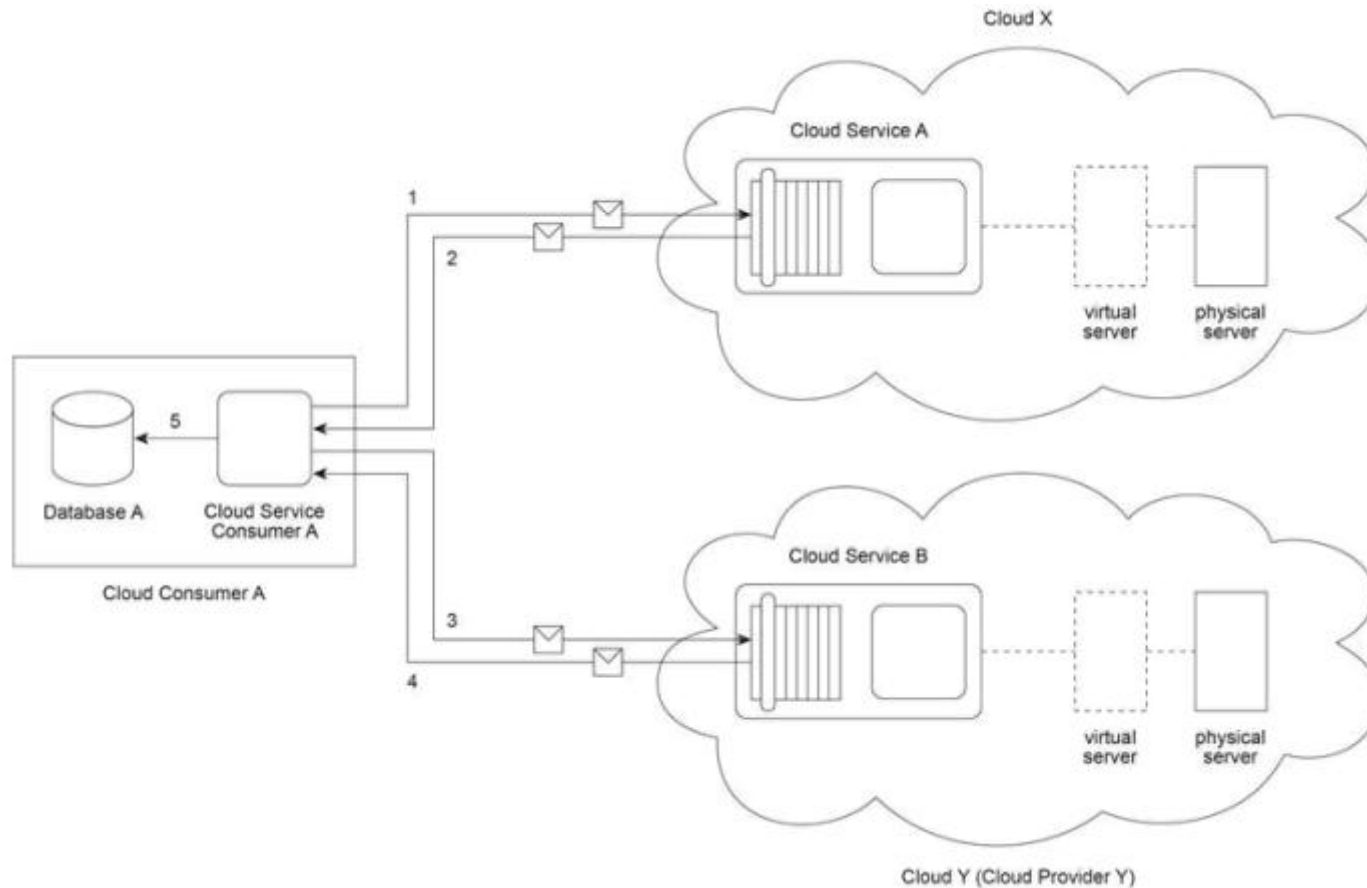
The cloud consumer must therefore choose Cloud Provider X.

Answer:

D

Question 2

Question Type: **MultipleChoice**

Cloud Service Consumer A accesses Cloud Service A (1) that resides in Cloud X. a private cloud owned by the same organization acting as Cloud Consumer A . Cloud Service A processes the message from Cloud Service Consumer A and then sends back a response with the requested data (2). Next, Cloud Service Consumer A sends a message containing some of this data to Cloud Service B (3), which resides in public Cloud Y that is owned by Cloud Provider Y. After processing the message, Cloud Service B sends back a response with additional data to Cloud Service Consumer A (4). Finally, Cloud Service Consumer A writes the data it collected from Cloud Services A and B to Database A (5).

Cloud X

Cloud Service A

virtual
server

physical
server

Database A

Cloud Service
Consumer A

Cloud Consumer A

Cloud Service B

virtual
server

physical
server

Cloud Y (Cloud Provider Y)

Recently, Cloud Service Consumer A has been required to access Cloud Services A and B at a significantly higher rate, sometimes over 1,000 times within a given workday. This increased usage has not affected Cloud Service B's performance. Cloud Service A, however, has been generating runtime exceptions and responses to Cloud Service Consumer A have become increasingly slow and unreliable. It is determined that this decline in performance is due to infrastructure limitations within private Cloud X's environment. Instead of investing in new infrastructure for Cloud X, it is decided to explore the feasibility of moving Cloud Service A to Cloud Y instead. Which of the following statements describe valid financial considerations that can be taken into account for assessing the feasibility of this move?

Options:

A- Moving Cloud Service A to Cloud Y will require that Database A also be moved to Cloud Y due to the need for Cloud Service A and Database A to share a common virtual server within the same organizational boundary, as required by the cloud-based security group. The move of Database A will increase the integration testing effort and. as a result, will also increase the overall integration costs.

B- Once Cloud Service A is deployed in Cloud Y, it may form dependencies upon proprietary parts of Cloud Y that may limit its mobility should it be decided to move it outside of Cloud Y in the future. This can incur further locked-in costs that need to be accounted for.

C- By moving Cloud Service A to Cloud Y, the SaaS delivery model will be established for Cloud Service A, thereby allowing the service implementation to build upon existing infrastructure from underlying PaaS and laaS delivery models that would have been required for Cloud Service B to be implemented in Cloud Y.

D- Public Cloud Y charges for the use of its IT resources. Moving Cloud Service A to Cloud Y can therefore result in new on-going costs. Although Cloud Service A may be able to share some of the existing IT resources used by Cloud Service B, it will likely incur new on-going costs that need to be budgeted for.

Answer:

B, D

Question 3

Question Type: MultipleChoice

Cloud Provider X has deployed a virtualization environment in Cloud X comprised of Physical Server A hosting Virtual Servers A and B. Cloud Provider X implements Cloud Service A on Virtual Server A and makes it available to Cloud Service Consumer A, which interacts with Cloud Service A by sending and receiving messages (1, 2). Cloud Provider Y has deployed a virtualization environment comprised of Physical Server B hosting Virtual Servers C and D. Virtual Server C is made available to Cloud Service Consumer B, which interacts with Virtual Server C (3,4) in order to prepare for the deployment of a new cloud service that will be used internally by Cloud Provider Y to process data obtained from Cloud Service A .

Cloud X (Cloud Provider X)

Cloud Service A

Virtual Server A

Virtual Server B

Physical Server A

Cloud Service Consumer A

Cloud Service Consumer B

Cloud Consumer Z

Virtual Server C

Virtual Server D

Physical Server B

Cloud Y (Cloud Provider Y)
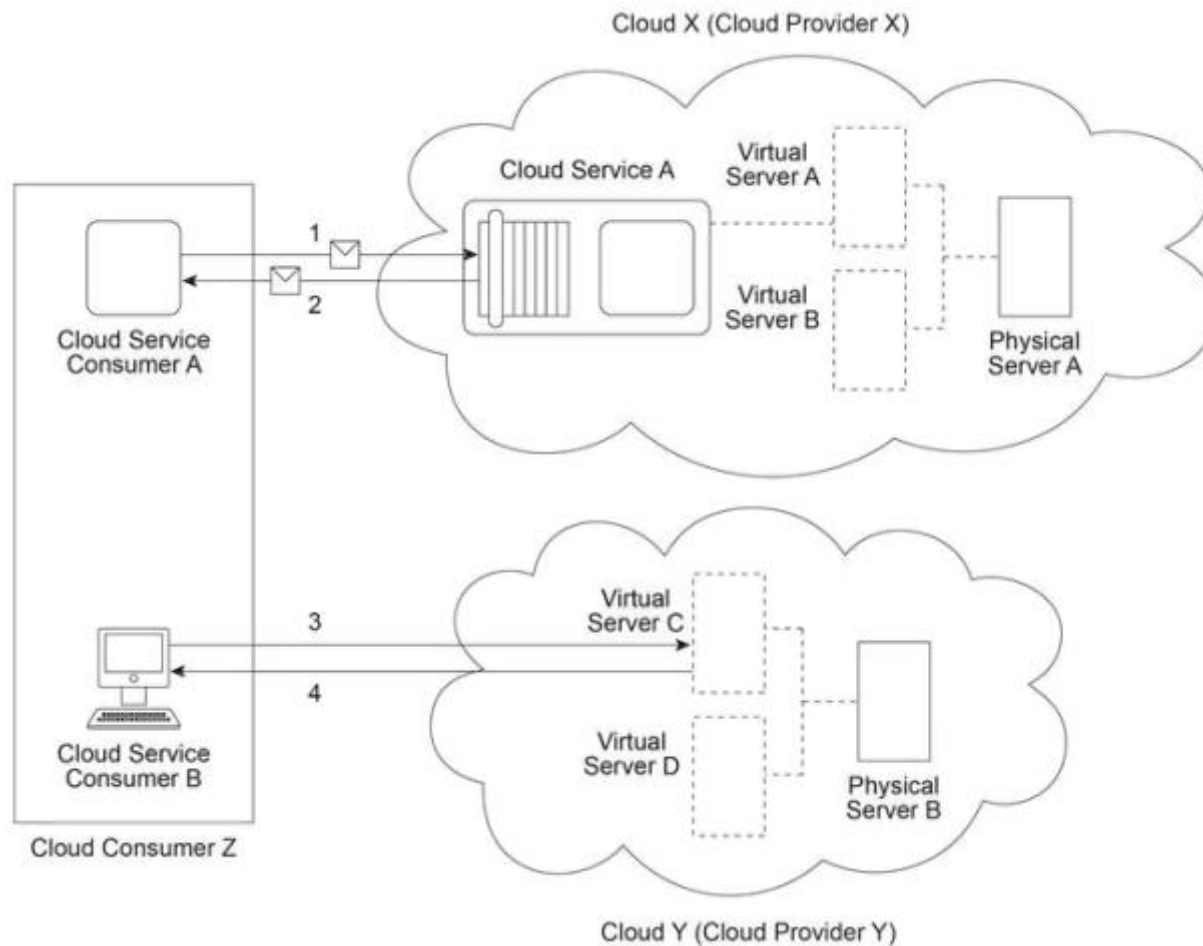
Cloud X is administered by a group of organizations and makes Cloud Service A available only to cloud service consumers from that group. Cloud Consumer Z belongs to one of the organizations within this group. Cloud Y and Cloud Consumer Z are owned by the same organization. Which of the following statements provides a valid scenario that accurately describes the involvement of cloud deployment models, cloud delivery models, roles and/or boundaries? (Note that the correct answer represents one of multiple valid scenarios that can exist.)

Options:

A- Clouds X and Y are based on the community cloud deployment model. Cloud Service A is based on the SaaS delivery model. Virtual Server C is being offered as part of the PaaS delivery model. A cloud resource administrator working for Cloud Provider X uses Virtual Server A to access the Cloud Service A implementation Cloud Consumer T s trust boundary encompasses Cloud Service Consumers A and B, Cloud Service A and Virtual Server C . The organization that owns Cloud Consumer Z is the cloud service owner of Cloud Service A .

B- Cloud X is based on the hybrid cloud deployment model. Cloud Service A is based on the SaaS delivery model. Cloud Y is based on the community cloud deployment model. Virtual Server C is being offered as part of the IaaS delivery model. A cloud resource administrator working for Cloud Consumer Z uses Cloud Service Consumer A to access Cloud Service A . Cloud Consumer Z's organizational and trust boundaries encompass Cloud Service Consumers A and B, Cloud Service A and Virtual Server C .

C- Cloud X is based on the community cloud deployment model. Cloud Service A is based on the SaaS delivery model. Cloud Y is based on the private cloud deployment model. Virtual Server C is being offered as part of the IaaS delivery model. A cloud resource administrator working for Cloud Consumer Z uses Cloud Service Consumer B to access Virtual Server C . Cloud Consumer Z' s trust boundary encompasses Cloud Service Consumers A and B, as well as Cloud Service A and Virtual Server C . The organization that owns Cloud Consumer Z will be the cloud service owner of the new cloud service that will be deployed on Virtual Server C .

D- Cloud X is based on the community cloud deployment model. Cloud Service A is based on the SaaS delivery model. Cloud Y is based on the private cloud deployment model. Virtual Server C is being offered as part of the IaaS delivery model. A cloud resource administrator working for Cloud Consumer Z uses Cloud Service Consumer B to access Virtual Server C . Cloud Consumer Z is the cloud service owner of Cloud Service A . Cloud Consumer T's organizational boundary encompasses Cloud Service Consumers A and B. Cloud Consumer Z's trust boundary encompasses Cloud Service A and Virtual Server C .

Question 4

Question Type: **MultipleChoice**

Cloud X (owned by Cloud Provider X) provides Physical Server A which hosts Virtual Servers A and B. Virtual Server B hosts Ready-Made Environments A and B . Cloud Service Consumer A uses Virtual Server A as part of an IaaS leasing agreement in which Cloud Consumer A is charged a fixed monthly fee for unlimited access. Cloud Service Consumers B and C use Ready-Made Environments A and B respectively as part of a PaaS leasing agreement based on per-minute usage fees. In both cases, access is monitored via Pay-For-Use Monitor A, which keeps track of log-in and log-out times in order to calculate the usage charges that are billed to Cloud Consumers B and C .

Cloud Service Consumer A (Cloud Consumer A)

Cloud Service Consumer B (Cloud Consumer B)

Cloud Service Consumer C (Cloud Consumer C)

Pay-For-Use Monitor A

Ready-Made Environment A

Ready-Made Environment B

Virtual Server A

Virtual Server B

Physical Server A

Cloud X (Cloud Provider X)
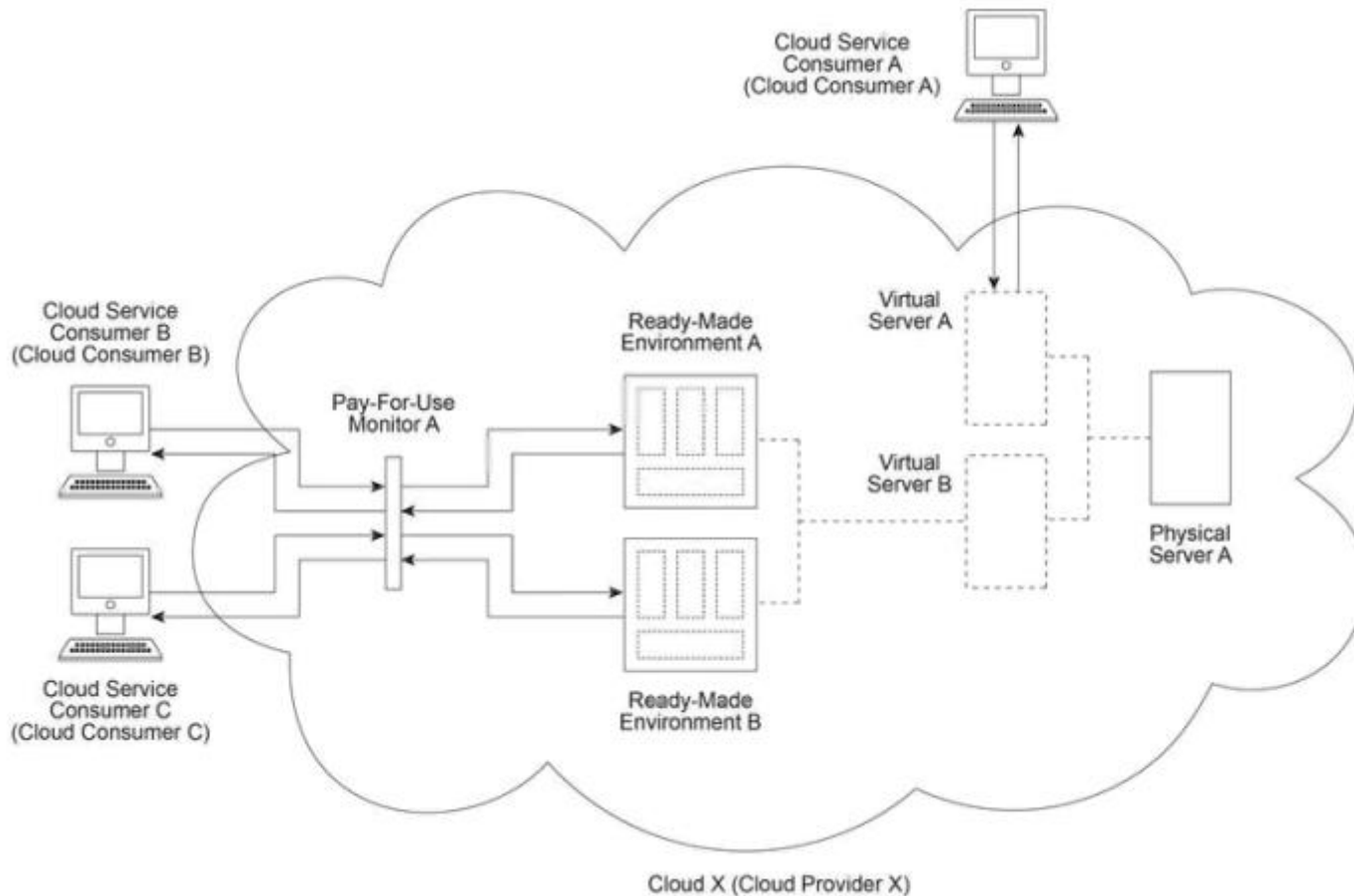
Physical Server A begins to become unstable. Over the course of a 24 hour period, the server shuts down three times, taking down Virtual Servers A and B with it. This causes numerous problems for Cloud Service Consumers A, B and C, which lose connections and encounter a variety of exceptions. A subsequent investigation of the log files generated by Pay-For-Use Monitor A reveals that the three server crashes coincided with the usage periods of Ready-Made Er n'ronment B b> Cloud Service Consumer B. De 'elopers at the Cloud Consumer 3 organization confirm they did not actually log in during those periods, which leads Cloud Provider X to discover that another cloud service consumer has been posing as Cloud Service Consumer B in order to maliciously access Ready-Made Environment B,

Virtual Server B, and Physical Server B on Cloud X. The investigation concludes that the malicious cloud service consumer was able to carry out the attack successfully by obtaining a weak password being used by developers from Cloud Consumer B . Which of the following statements accurately identifies the type of security threat that corresponds to the described attack - and -provides a solution that can directly mitigate this type of security threat within Cloud X?

Options:

A- Ready-Made Environment B. Virtual Server B and Physical Server B were subjected to a weak authentication attack that can be mitigated by implementing the encryption and digital signature mechanisms.

B- Ready-Made Environment B. Virtual Server B and Physical Server B were subjected to a malicious intermediary attack that can be mitigated by implementing the cloud-based security groups and hardened virtual server images mechanisms.

C- Ready-Made Environment B, Virtual Server B and Physical Server B were subjected to a virtualization attack that can be mitigated by implementing the encryption and digital signature mechanisms.

D- Ready-Made Environments, Virtual Server B and Physical Server B were subjected to an attack that succeeded due to overlapping trust boundaries. This type of attack can be mitigated by implementing the single sign-on mechanism.

Answer:

A

Question 5

Organization A has been expanding and, as a result, is outgrowing the processing capacity of its on-premise Service A implementation. It is determined that this is due to usage thresholds of Service A and complex data processing limitations in Database A . The diagram depicts Organization A's current on-premise environment, where Service Consumers A . B and C attempt to access Service A at the same time. Service Consumer A successfully accesses Service A, which then successfully retrieves the requested data (1). Service Consumer B successfully accesses Service A, but due to the complex data structure, the request for the data times out and fails (2). Finally, Service Consumer C attempts to access Service A, but is rejected because Service A is unable to accept more concurrent requests.
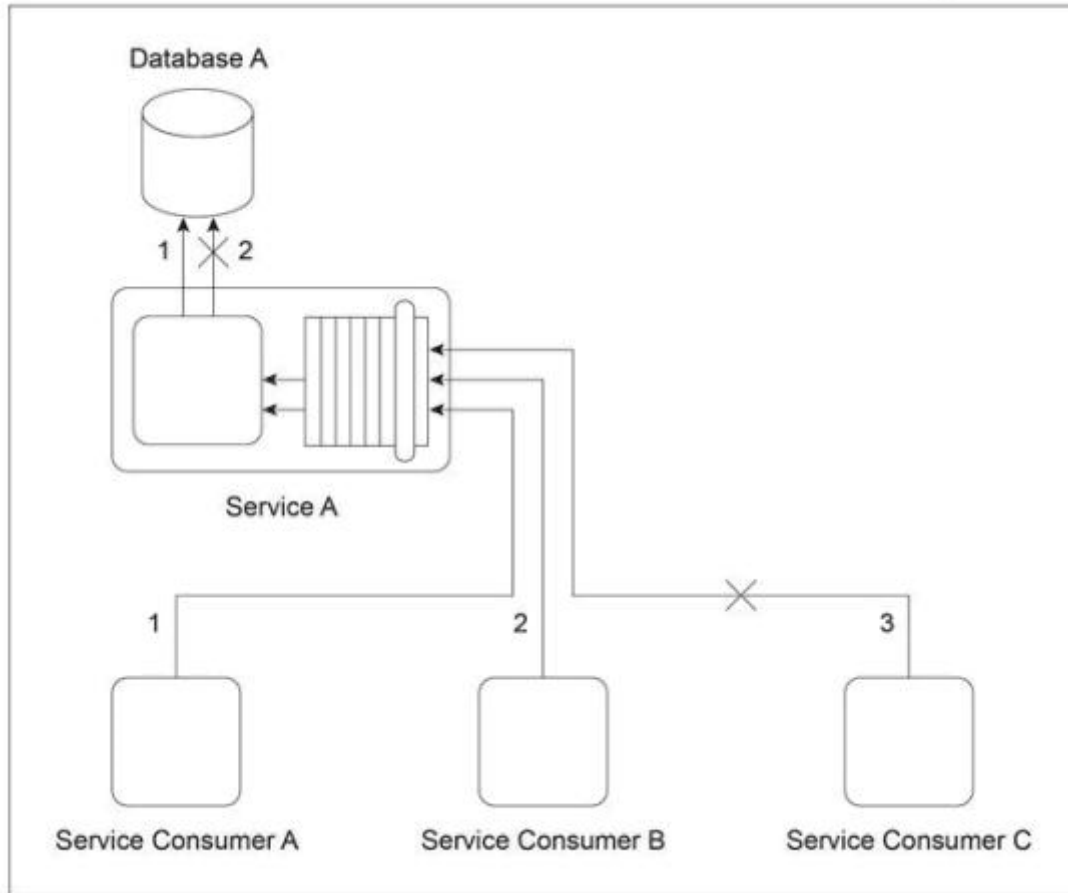
Organization A is required to continue using its on-premise Service A implementation, with the exception of Database A, which does not need to remain on-premise. Database A is dedicated to Service A and is comprised of relational data. Which of the following statements provides a solution that uses cloud-based IT resources to solve the performance limitations of Service A and Database A?

Options:

A- A failover system can be implemented in a hybrid architecture comprised of Organization A's existing on-premise environment and a public cloud environment. The failover system would span both environments so that when Service A is unable to process request messages from Service Consumers A, B or C, the failover system can automatically route messages to a redundant implementation of Service A residing in the public cloud. Similarly, when Database A is unable to process a data access request from Service A . the failover system can automatically route this request to a redundant implementation of Database A, also residing in the public cloud.

B- The state management database and resource replication mechanisms can be implemented to establish redundant implementations of Service A and Database A in both on-premise and cloud environments. Using resource replication, a cloud-based duplicate of Service A (Cloud Service A) will be established in a public cloud and will remain in synch with Service A via regular replication cycles. Using the resource replication mechanism together with the state management database mechanism allows for Database A to be dynamically replicated in an independent state management database that has redundant implementations in both on-premise and cloud environments. The state management database can be further optimized to support non-relational data to improve data access performance.

C- A cloud bursting solution can be implemented, whereby a redundant copy of Service A is implemented within a public cloud. This cloud-based, redundant implementation of Service A is referred to as Cloud Service A . A copy of Database A is also implemented within the cloud and both the on-premise and cloud-based copies of Database A are redesigned to be nonrelational in order to improve data access performance. Service A continues to act as a first point of contact for Service Consumers A, B and C. An automated scaling listener is deployed so that when Service A's thresholds are met, requests are automatically routed to Cloud Service A .
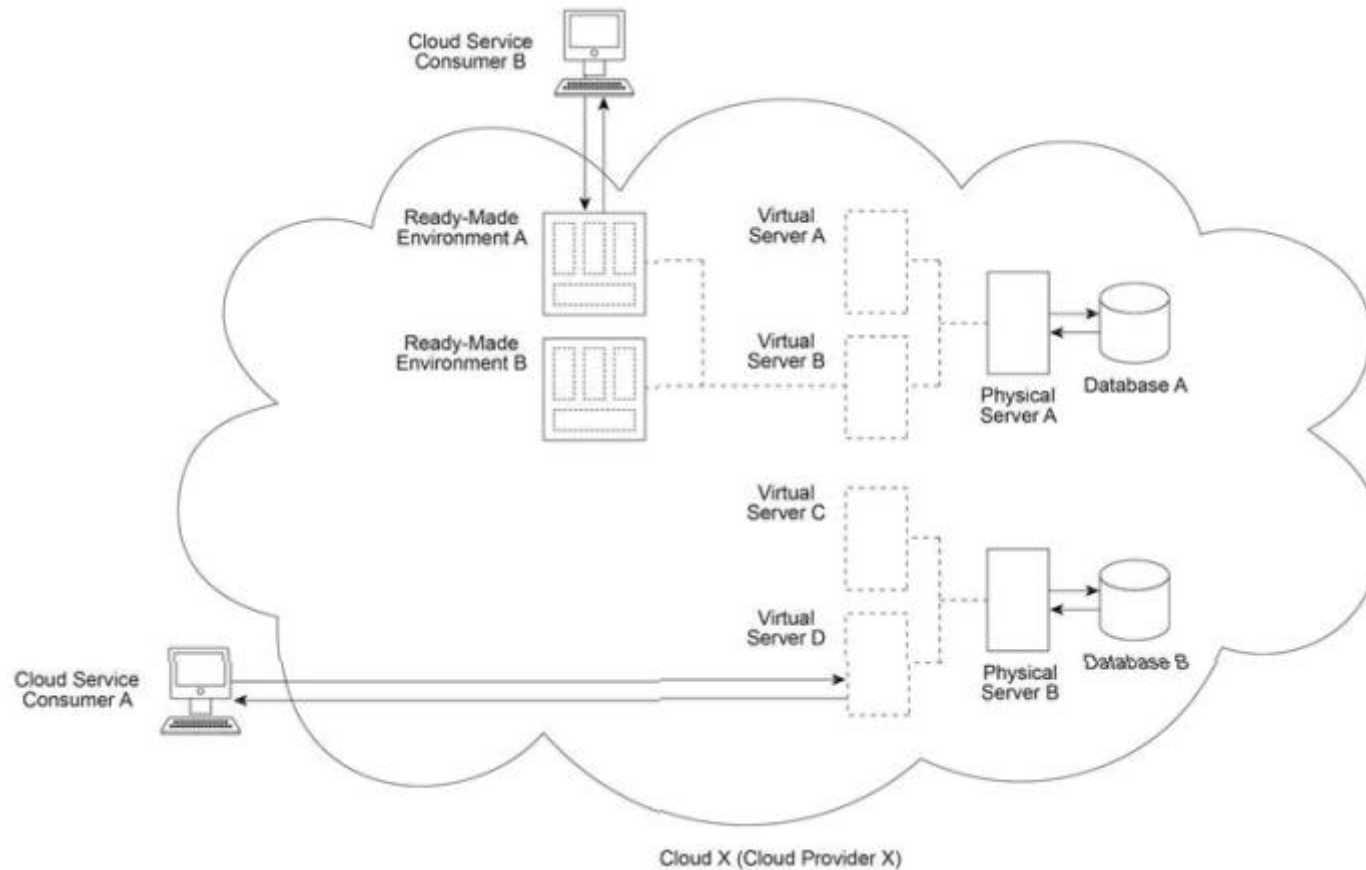
D- None of the above

Answer:

C

Question 6

Cloud Provider X (which owns Cloud X) deploys two physical servers (Physical Servers A and B) and two databases (Databases A and B). Virtual Servers A and B are hosted by Physical Server A and Ready-Made Environments A and B are hosted by Virtual Server B . Virtual Servers C and D are hosted by Physical Server B . Cloud Service Consumer A regularly accesses Virtual Server D in order to test and deploy a new cloud service that was developed on-premise by the cloud consumer organization operating Cloud Service Consumer A . Cloud Service Consumer B (operated by a different cloud consumer organization) has been regularly accessing Ready-Made Environment A in order to develop and deploy a different new cloud service.

Cloud Service Consumer B

Ready-Made Environment A

Ready-Made Environment B

Virtual Server A

Virtual Server B

Physical Server A

Database A

Virtual Server C

Virtual Server D

Physical Server B

Database B

Cloud Service Consumer A

Cloud X (Cloud Provider X)

Cloud X is a private cloud that, to-date, has been set up within the cloud provider company to provision IT resources free of charge to internal cloud consumers, via PaaS and IaaS delivery models. The cloud consumers that have been operating Cloud Service Consumers A and B represent different IT departments within the company that have been working separately on the development of new cloud services. Cloud Service Consumer A has been accessing Virtual Server D to make necessary configurations and administration settings for the upcoming deployment of a new cloud service that was previously developed outside of Cloud X. Cloud Service Consumer B has been accessing Ready-Made Environment A to develop and now deploy a different new cloud service. Cloud

Provider X (which is represented by a separate IT department dedicated to governing and administering Cloud X) determines that it will need to introduce three specific enhancements to Cloud X in order to accommodate both upcoming cloud services. First, it needs to add a way to charge cloud consumers for the usage of cloud services. Secondly, it needs to add a way for new cloud services to be automatically scaled. Finally, it needs to add a way for a cloud consumer to be automatically notified when a cloud service encounters runtime loads that exceed its allocated usage threshold. Which of the following statements accurately describes a solution that fulfills all three identified requirements?

Options:

A- The pay-for-use monitor mechanism can be installed to address the requirement for cloud service usage charges to be tracked and recorded. The automated scaling listener mechanism can be implemented to address the requirement for cloud services to be automatically scaled. The multi-device broker mechanism can be implemented to address the requirement for notifications to be issued when cloud service loads exceed thresholds.

B- The pay-for-use monitor mechanism can be installed to address the requirement for cloud service usage to be tracked and recorded. The automated scaling listener mechanism can be implemented to address both the requirement for cloud services to be automatically scaled and for notifications to be issued when cloud service loads exceed thresholds.

C- The pay-for-use monitor mechanism can be implemented to address the requirement for cloud service usage charges to be tracked and recorded, for cloud services to be automatically scaled, and for notifications to be issued when cloud service loads exceed thresholds.

D- The state management database mechanism together with the virtual server mechanism and the automated scaling listener mechanism can be implemented to address the requirement for cloud service usage charges to be tracked and recorded, for cloud services to be automatically scaled, and for notifications to be issued when cloud service loads exceed thresholds.

Question 7

Question Type: MultipleChoice

Cloud Provider Y owns Cloud Y, which provides a set of cloud services, virtual servers, and one physical server. Cloud Services A and B are hosted on Virtual Server A, which is hosted by Physical Server A . Physical Server A also hosts Virtual Server B, which hosts redundant implementations of Cloud Services A and B for load balancing purposes. Cloud Service Consumer A is accessing Cloud Service A located on Virtual Server A . Cloud Service Consumer B is accessing Cloud Service B located on Virtual Server B . Cloud Service Consumers A and B are both owned by Cloud Consumer X. Cloud Consumer X has recently complained that Cloud Service A is becoming increasingly unreliable. Cloud Provider Y launches an investigation that reveals that Virtual Server A has been crashing sporadically due to successful malicious intermediary attacks where malicious service agents have been inserting harmful data into messages sent by Cloud Service Consumer A to Cloud Service A

Cloud Service A

Cloud Service Consumer A
(Cloud Consumer X)

Cloud Service B

Cloud Service A

Cloud Service B

Cloud Service Consumer B
(Cloud Consumer X)

Virtual Server A

Virtual Server B

Physical Server A

Cloud Y (Cloud Provider Y)
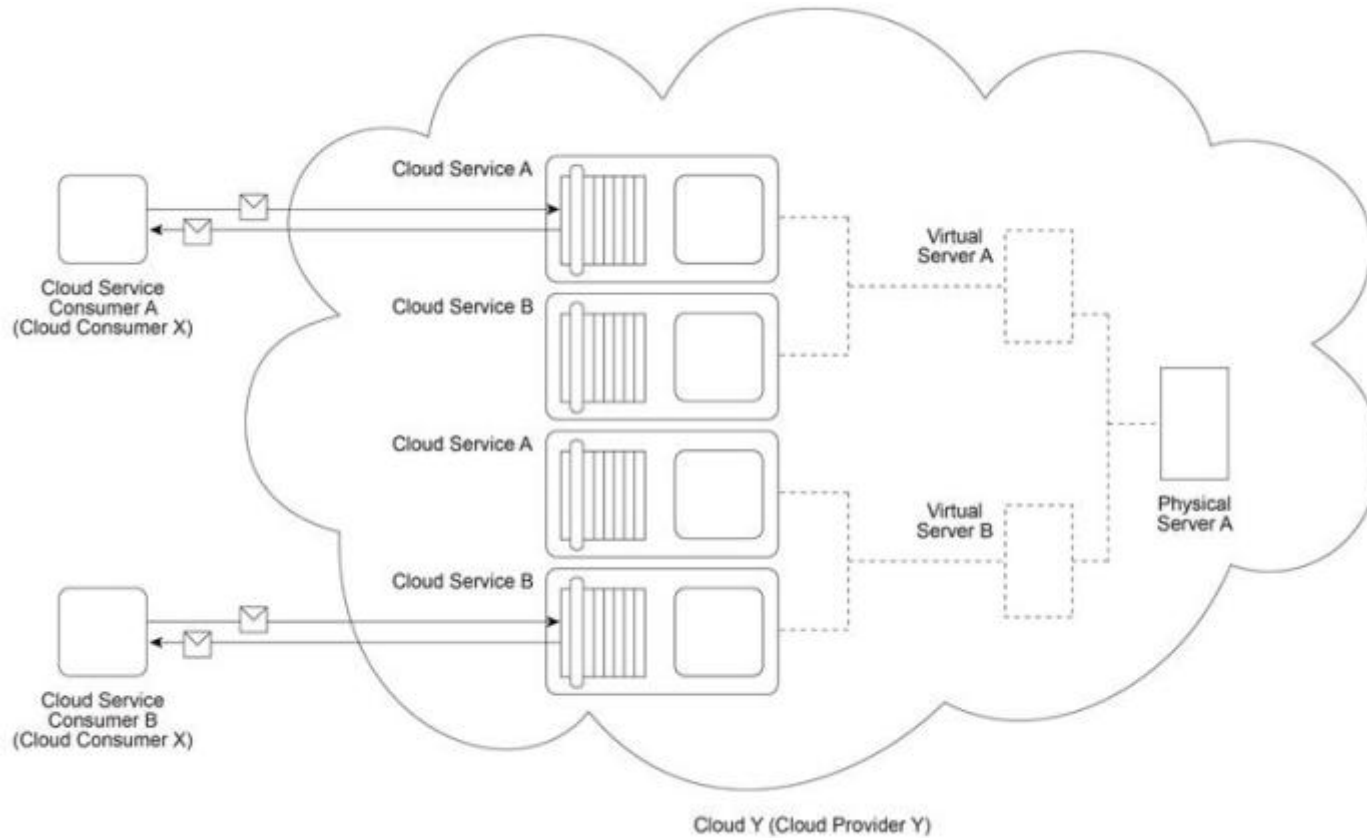
Which of the following statements describes a solution that can mitigate the malicious intermediary attacks that have been occurring on Virtual Server A - and - can further help prevent the same types of attacks from occurring on Virtual Server B?

Options:

A- Cloud Provider Y can implement the cloud-based security group mechanism that establishes a logical trust boundary that

encompasses Virtual Servers A and B

B- Cloud Provider Y can implement the encryption and digital signatures mechanisms to protect the contents of messages from being augmented by malicious service agents.

C- Cloud Provider Y can implement the failover system mechanism by requiring that redundant copies of all service agents be deployed. This will reduce the chances of any one service agent performing malicious actions at runtime.

D- Cloud Provider Y can implement the identity and access management mechanism for Virtual Servers A and B by physically deploying this mechanism on Physical Server A and then further implementing the resource replication mechanism to propagate the identity and access management system across Virtual Servers A and B.

Answer:

B

Question 8

Question Type: **MultipleChoice**

Cloud Service A is being made available on public Cloud X by Cloud Provider X via the SaaS delivery model. Cloud Service A is hosted by Physical Server A that also hosts cloud services being used by different cloud service consumers (and owned by different cloud service owners). Cloud Service Consumers A and B access Cloud Service A on a regular basis and Physical Server A has been able to accommodate the resulting usage load After reviewing the implementation environment for Cloud Service A . Cloud Provider X determines it needs to enhance the ubiquitous access and multi-tenancy characteristics within this part of Cloud X.

Cloud Service Consumer A

Cloud Service Consumer B

Cloud Service A

Physical Server A

Cloud X (Cloud Provider X)
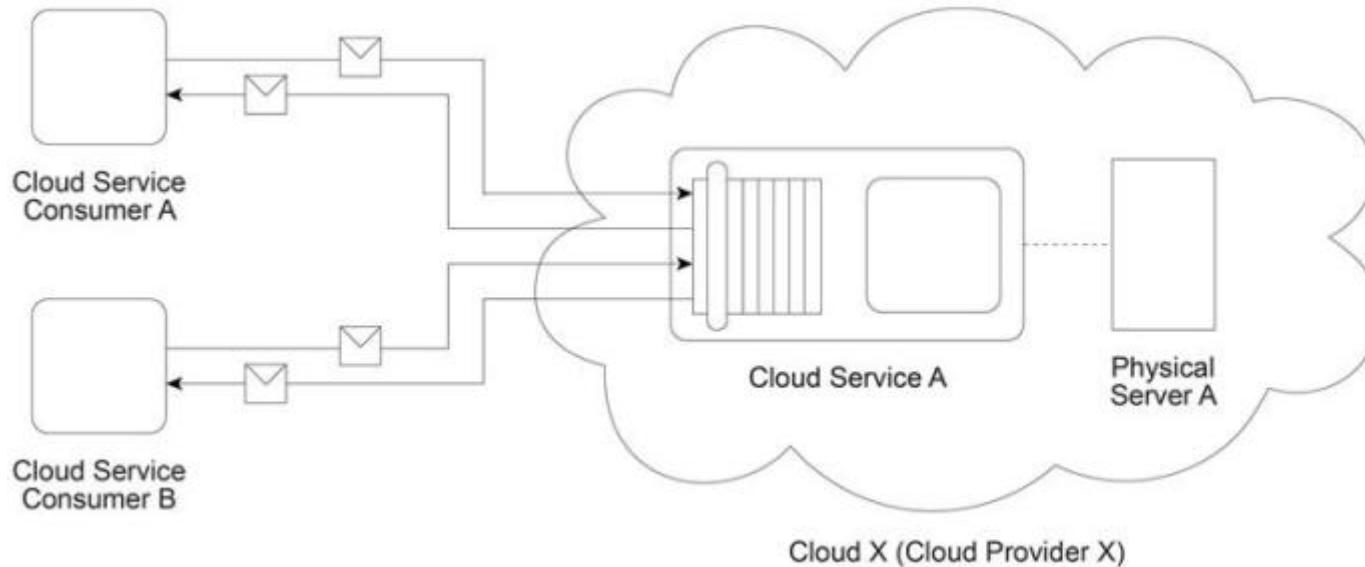
Which of the following statements accurately describes a solution that fulfills all of these requirements?

Options:

A- The multi-device broker mechanism can be implemented to address ubiquitous access requirements by broadening the range of cloud service consumers that can access Cloud Service A . The resilient computing mechanism can be implemented to establish the multitenancy capabilities of Cloud Service A so that it will be able to resiliency accommodate the additional cloud service consumer devices that will gain access to it.

B- The resilient computing mechanism can be implemented to address ubiquitous access requirements by making Cloud Service A available to a broader range of cloud service consumer devices, including desktops running Web browsers and various mobile devices. The resource replication mechanism can be implemented to enable multi-tenancy within the Cloud Service A implementation.

C- The resource replication mechanism can be introduced to address ubiquitous access requirements by broadening the range of cloud service consumers that can use Cloud Service A via standard service replication. The virtual server mechanism can be implemented to enable multi-tenancy via each service replication resulting from the application of the resource replication mechanism.

D- The multi-device broker mechanism can be implemented to address ubiquitous access requirements by broadening the range of cloud service consumers that can access Cloud Service A . The virtual server mechanism can be implemented to establish the multitenancy capabilities of Cloud Service A .

Answer:

D

Question 9

Question Type: MultipleChoice

Cloud Provider X (which owns Cloud X) deploys two physical servers (Physical Servers A and B) and two databases (Databases A and B). Virtual Servers A and B are hosted by Physical Server A and Ready-Made Environments A and B are hosted by Virtual Server B . Virtual Servers C and D are hosted by Physical Server B . Cloud Service Consumer A regularly accesses Virtual Server D in order to test and deploy a new cloud service that was developed on-premise by the cloud consumer organization operating Cloud Service Consumer A . Cloud Service Consumer B (operated by a different cloud consumer organization) has been regularly accessing Ready-Made Environment A in order to develop and deploy a different new cloud service. The cloud consumer organizations that own and operate Cloud Service Consumers A and B will soon be ready to launch their respective cloud services for use by their customers. Both cloud consumer organizations are concerned that Cloud X does not provide sufficient security and they demand that Cloud Provider X

take the necessary steps to mitigate the denial of service, insufficient authorization and overlapping trust boundaries security threats.

Cloud X (Cloud Provider X)
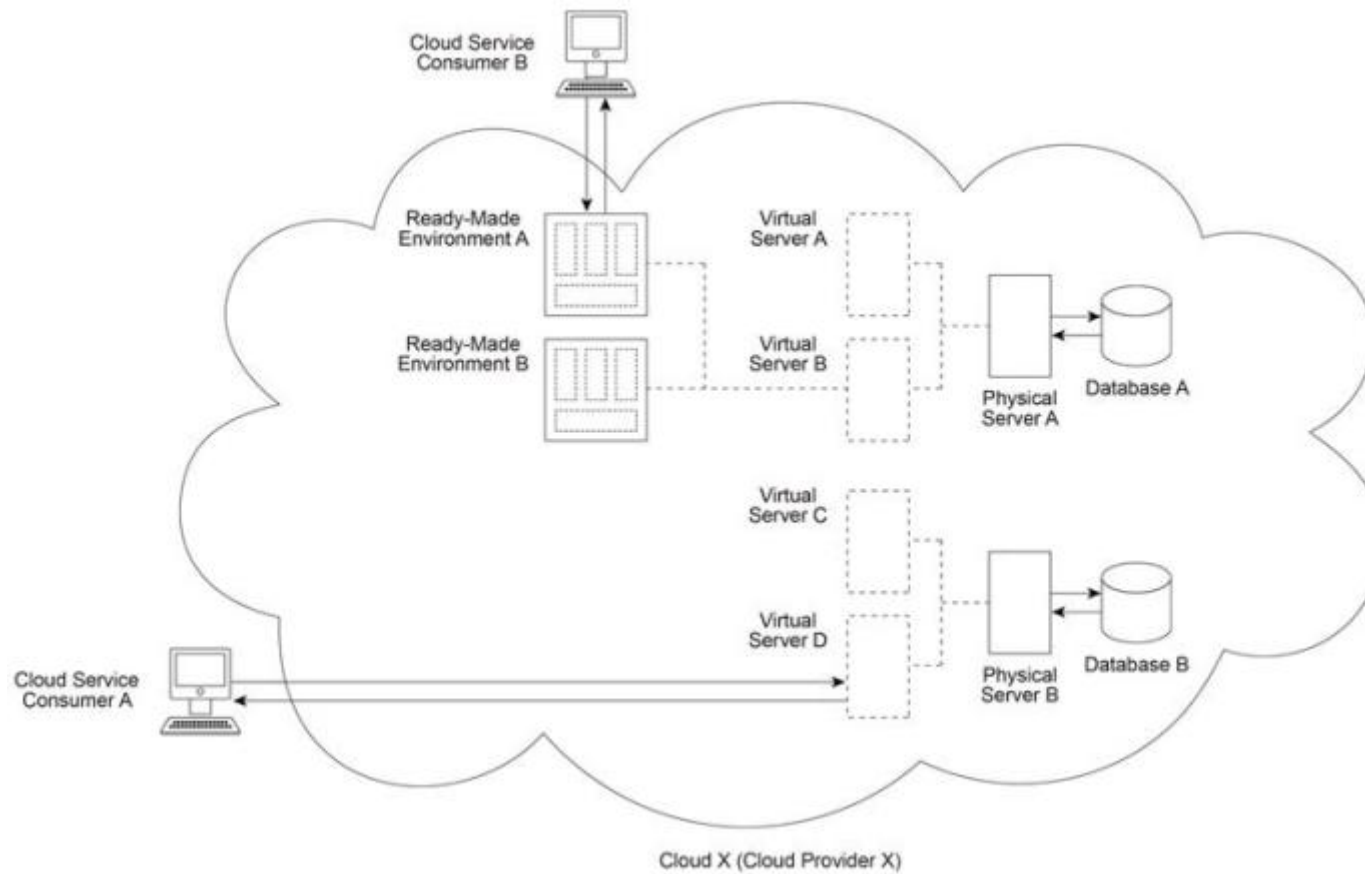
Which of the following statements accurately describes the cloud delivery models used now by the cloud service consumers and in the future by their customers - and - further describes a solution that fulfills the identified security requirements by implementing a single cloud security mechanism?

Options:

A- Cloud Service Consumer A is using the IaaS delivery model. Cloud Service Consumer B is using the SaaS delivery model. Customers of the cloud services will be using the PaaS delivery model. The encryption mechanism can be implemented to mitigate the denial of service, insufficient authorization and overlapping trust boundaries security threats.

B- Cloud Provider X is providing a hybrid delivery model comprised of a combination of the IaaS and PaaS delivery models, which means that Cloud Service Consumers A and B are using both the IaaS and PaaS delivery models. Customers of the cloud services will be using the PaaS delivery model. The single sign-on mechanism can be implemented to mitigate the denial of service and insufficient authorization security threats. The encryption mechanisms can be implemented to mitigate the overlapping trust boundaries security challenges.

C- Cloud Service Consumer A is using the IaaS delivery model. Cloud Service Consumer B is using the PaaS delivery model. Customers of the cloud services will be using the SaaS delivery model. An identity and access management mechanism can be implemented to mitigate the denial of service, insufficient authorization and overlapping trust boundaries security challenges.

D- Cloud Service Consumer A is using the IaaS delivery model. Cloud Service Consumer B is using the PaaS delivery model. Customers of the cloud services will be using the SaaS delivery model. The digital signatures mechanism can be implemented to mitigate the denial of service, insufficient authorization and overlapping trust boundaries security challenges.
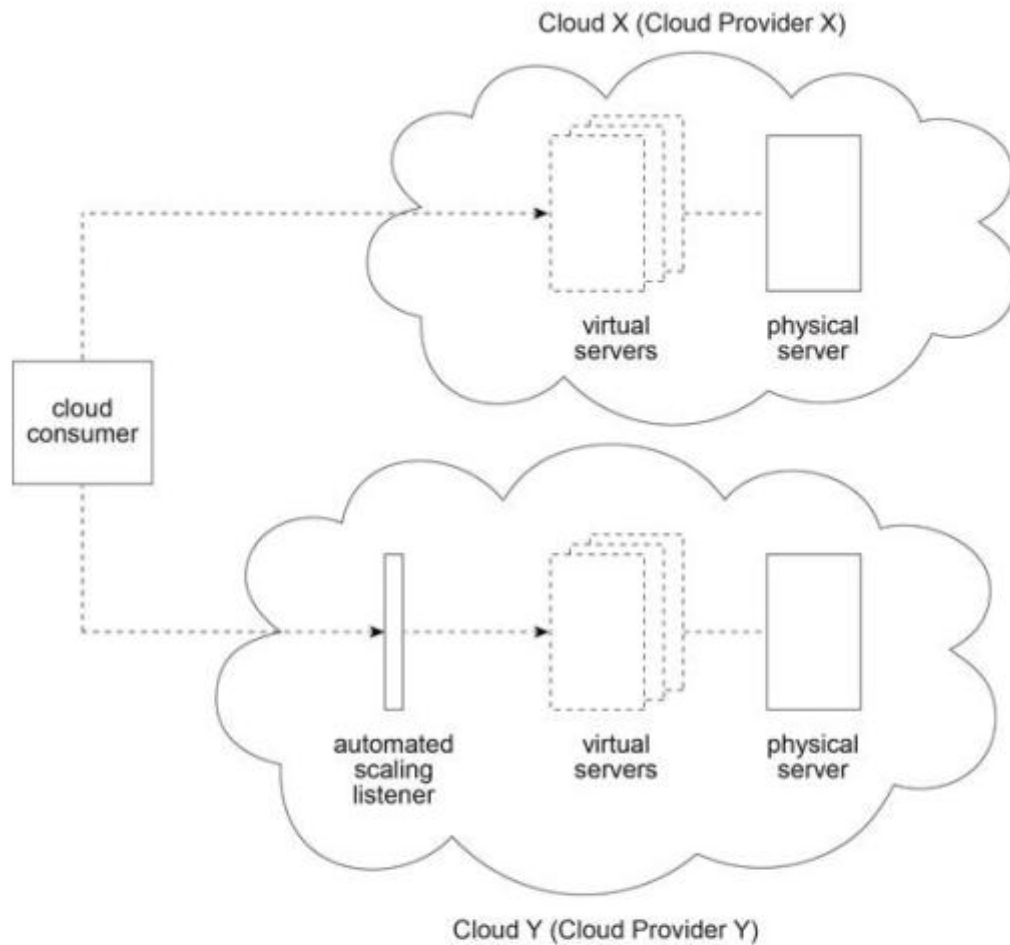
Answer:
C

Question 10

A cloud consumer is interested in leasing cloud-based virtual servers. It compares the virtual servers offered by Cloud Provider X and Cloud Provider Y. Cloud X (owned by Cloud Provider X) and Cloud Y (owned by Cloud Provider Y) both provide shared physical servers that host multiple virtual servers for other cloud consumers. The virtual servers on Cloud X are accessed directly, whereas the virtual servers on Cloud Y are accessed via an automated scaling listener. On Cloud X, virtual servers are pre-configured to support a specific amount of concurrent cloud service consumers. When this threshold is exceeded, cloud service consumer requests are rejected. Due to the use of the automated scaling listener, virtual servers on Cloud Y can provide a greater level of elasticity. The hourly cost to the cloud consumer to use a virtual server on Cloud X is half that of the cost to use a virtual server on Cloud Y. Within a one month period, Cloud Provider X bases its hourly charge on the maximum number of virtual servers used. Within a one month period, Cloud Provider Y bases its hourly charges on actual virtual server usage. Cloud Provider Y charges $20 for each hour that a cloud consumer uses a virtual server.

Cloud X (Cloud Provider X)

virtual
servers

physical
server

cloud
consumer

automated
scaling
listener

virtual
servers

physical
server

Cloud Y (Cloud Provider Y)

The cloud consumer predicts its monthly usage requirements to be as follows:

Number of virtual servers	Usage (hours)
2	70
4	20
6	10

The cloud consumer is required choose the cloud provider with the lowest on-going cost based on its predicted usage. Which of the following statements accurately calculates the on-going usage costs of Cloud Providers X and Y and correctly states the cloud provider that the cloud consumer must choose?

Options:

A- The total usage duration is (10 + 20 + 70) hours = 100 hours.

The actual usage is (10 X 6) + (20 X 4) + (70 X 2) hours = 280 hours.

The cost of using virtual servers from Cloud Provider X is 100X6X$10 = $6,000.

The cost of using virtual servers from Cloud Provider Y is 280 X $20 = $5,600.

The cloud consumer must therefore choose Cloud Provider Y.

B- The total usage duration is (10 + 20 + 70) hours = 100 hours.

The actual usage is ((10 X 6) + (20 X 4) + (70 X 2)) x ((2 + 4 + 6) / 3) hours = 1,120 hours

The cost of using virtual servers from Cloud Provider Xis10QX6X$10 = $6,000.

The cost of using virtual servers from Cloud Provider Y is 1,120 X $20 = $22,400.

The cloud consumer must therefore choose Cloud Provider X.

C- The total usage duration is (10 + 20 + 70) hours = 100 hours.

The actual usage is ((10 X 6) + (20 X 4) + (70 X 2)) x ((2 + 4 + 6) / 3) hours = 1,120 hours

The cost of using virtual servers from Cloud Provider X is 6 X 100 X $10 = $6,000.

The cost of using virtual servers from Cloud Provider Y is 1,120 X $20 = $22,400.

The cloud consumer must therefore choose Cloud Provider Y.

D- The total usage duration is (10 + 20 + 70) x 12 hours = 1.200 hours.

The actual usage is (10X6) + (20X4) + (70X2) hours = 280 server hours.

The cost of using virtual servers from Cloud Provider Xis12X100X5X$10 = $60,000.

The cost of using virtual servers from Cloud Provider Y is 280 X $20 = $5,600.

The cloud consumer must therefore choose Cloud Provider Y.

Answer:

A