➢ **Vendor: CompTIA**

➢ **Exam Code: CV0-002**

➢ **Exam Name: CompTIA Cloud+ Certification Exam**

➢ **New Updated Questions from Braindump2go (Updated in Feb./2021)**

Visit Braindump2go and Download Full Version CV0-002 Exam Dumps

QUESTION 505
A company has implemented a change management process that allows standard changes during business hours. The company's private cloud hardware needs firmware updates and supports rolling upgrades. Which of the following considerations should be given to upgrade firmware and make the change as transparent as possible to users?

A. Implement the change as a standard change.
B. Notify users before applying the change during the day.
C. Fail the application over to perform the upgrade.
D. Perform the change during off-hours to minimize the impact on users.

Answer: B

QUESTION 506
A company's cloud administrator receives an advisory notice from the CSP. The CSP runs quarterly tests on its platform and customer's environments. The cloud administrator reads the notice and sees the

company's environment is at risk of buffer over-read exploits. Which of the following tests is the CSP MOST likely running on a quarterly basis?

A. Load testing
B. Data integrity testing
C. Vulnerability testing
D. Performance testing

Answer: C

QUESTION 507
A cloud security analyst recently performed a vulnerability scan on a web application server across all staging environments. The vulnerability scan determines the directory that houses web content is located on the same drive as the operating system. The analyst then attempts to mitigate the vulnerability in all staging environments. The vulnerability scan is performed again and produces the following results:
PROD
Website XYZ web content is housed on the C: drive.
QA
Website XYZ web content is housed on the G: drive.
DEV
Website XYZ web content is housed on the G: drive.
Given this scenario, which of the following should the test results conclude about the vulnerability?

A. The mitigation results were unsuccessful, and the PROD staging environment requires remediation and/or mitigation.

B. The mitigation results were unsuccessful, and the DEV staging environment requires remediation and/ or mitigation.
C. The mitigation results were unsuccessful, and each staging environment requires remediation and/or mitigation.
D. The mitigation results were unsuccessful, and the QA staging environment requires remediation and/or mitigation.

Answer: B

QUESTION 508
A company moved its on-premises applications to several SaaS providers. As a result, the security team is concerned about accounts being compromised. Which of the following should the security tem implement to reduce this risk?

A. Multifactor authentication
B. Single sign-on
C. Federation
D. Role-based access control
E. Virtual private network

Answer: D

QUESTION 509
A company is consuming a SaaS solution with a large user base and wants to minimize user management, but also ensure access is as secure as possible. Which of the following should the cloud administrator select to help meet these requirements? (Choose two.)

A. MFA
B. ACL
C. AAA
D. SSO
E. NAC

Answer: AD

QUESTION 510
A cloud engineer is required to ensure all servers in the cloud environment meet requirements for PCI compliance. One of the requirements is to make certain all administrator logins and commands are logged. Which of the following is the BEST approach to meet these requirements?

A. Enable configuration change tracking for all servers in the public cloud provider's dashboard.
B. Enable detailed monitoring for all servers in the public cloud provider's dashboard.
C. Define and enable audit tracking rules on each server in the public cloud environment.
D. Modify the cloud provider's role-based authorization policies to log user session activity.

Answer: A

QUESTION 511
A financial services company has a requirement to keep backups on premises for 30 days and off-site for up to seven years to a location that is within 100mi (161km) of the primary datacenter location. Recovery times for backups kept on-site have an RTO of one hour, while recovery times for backups kept off-site have an RTO of four hours. Which of the following solutions BEST solves this requirement?

A. Implement a full-based backup and recovery solution for backups within 30 days or less. For backups kept longer than 30 days, migrate them to a cloud provider that will host the data within 100mi (161km) of the financial services company's primary

datacenter.

B. Implement a clone-based backup and recovery solution for backups within 30 days or less. For backups kept longer than 30 days, migrate them to a cloud provider that will host the data within 100mi (161km) of the financial services company's primary datacenter.

C. Implement an incremental-based backup and recovery solution for backups within 30 days or less. For backups kept longer than 30 days, migrate them to a cloud provider that will host the data within 62mi (100km) of the financial services company's primary datacenter.

D. Implement a snapshot-based backup and recovery solution for backups within 30 days or less. For backups kept longer than 30 days, migrate them to a cloud provider that will host the data within 100mi (161km) of the financial services company's primary datacenter.

Answer: B

QUESTION 512
A company is seeking a new backup solution for its virtualized file servers that fits the following characteristics:
- The files stored on the servers are extremely large.
- Existing files receive multiple small changes per day.
- New files are only created once per month.
- All backups are being sent to a cloud repository.
Which of the following would BEST minimize backup size?

A. Local snapshots
B. Real-time backups
C. File-based replication
D. Change block tracking

Answer: D

QUESTION 513
A company's Chief Information Officer (CIO) wants to manage PII by delegating access to sensitive files to the human resources department. The cloud engineer is tasked with selecting and implementing an appropriate technique to achieve the stated objective.
Which of the following control methods would be BEST for the cloud engineer to implement?

A. Create a group, add users to the group, and apply the appropriate ACL.
B. Restrict the access to originate from the home office only.
C. Create a shared account for users in the human resources department.
D. Implement multifactor authentication for users in the human resources department.

Answer: A

QUESTION 514
A company hired a consultant to diagnose and report performance issues of an application hosted on an IaaS, three-tier application. The cloud administrator must provision only the access required by the consultant to complete the job.
Which of the following resource configurations should be applied to the consultant's account? (Choose two.)

A. Read/write access to the load balancer and its configuration settings
B. Administrator account on the resources in that region
C. Read/write access to the cloud compute resources
D. Read-only access to the server OS logs
E. Read-only access to the cloud resource diagnostic logs
F. Administrator account in the server OS

CV0-002 Exam Dumps CV0-002 Exam Questions CV0-002 PDF Dumps CV0-002 VCE Dumps

https://www.braindump2go.com/cv0-002.html

Answer: CE

QUESTION 515
Ann, an internal user, has been accessing an internal SaaS solution on a different subnet for the last several months. When Ann tries to connect to the application today, she receives an error stating the resource cannot be found. When checking with her teammates, she discovers some users can access the resource and others cannot. Which of the following tools would be the BEST option to determine where the issue is located?

A. ipconfig or ifconfig
B. ping
C. netstat
D. tracert or traceroute

Answer: B

QUESTION 516
Which of the following solutions BEST complies with laws requiring secure data-at-rest for a critical application while keeping in mind the need for reduced costs?

A. Install a new array with hardware encryption disks.
B. Enable encryption on the back-end database.
C. Use IPSec on the storage array.
D. Enable HTTPS on the application.

Answer: B

QUESTION 517
A manufacturing company has the following DR requirements for its IaaS environment:
```
– RPO of 24 hours
– RTO of 8 hours
```
The company experiences a disaster and has a two-site hot/cold configuration. Which of the following is the BEST way for the company to recover?

A. Restore data from the archives on the hot site, point users to it, and resume operations.
B. Bring the cold site online, point users to it, and resume operations.
C. Rebuild the site from the cold site, bring the site back online, and point users to it.
D. Replicate data from the non-failed site to another cloud provider, point users to it, and resume operations.

Answer: C

QUESTION 518
A company has developed a SaaS product for the financial services industry. The Chief Executive Officer (CEO) of the SaaS company has engaged an independent third party to run tests against its platform. Which of the following is the MOST likely test the third party has been engaged to perform?

A. Penetration testing
B. Load testing
C. Vulnerability testing
D. Functionality testing

Answer: A

QUESTION 519
A user cannot consume SaaS services while working remotely. IP whitelisting is implemented to connect to a SaaS provider as a security mechanism. Which of the following describes the MOST likely reason why the user cannot

access the SaaS resources?

A. The user is not utilizing VPN to connect to the home office.
B. The user account does not exist in the SaaS provider.
C. The user account is not assigned the correct role in RBAC policy.
D. The user account has consumed all of the available subscriptions.

Answer: C

QUESTION 520
A systems administrator needs to deploy a database that saves a unique ID/hash at the beginning of each block into a private cloud. The administrator needs to maximize storage savings. The administrator has multiple storage policies set. Which of the following would be the BEST option for this deployment?

A. Compression enabled
B. Deduplication enabled
C. Mirroring enabled
D. Tokenization enabled

Answer: B