PassQueen
a.k.a dumpsqueen.com

Associate - Data Protection and Management Version 2 Exam

Dell DEA-3TT2

Version Demo

Total Demo Questions: 8

Total Premium Questions: 83

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Data Protection and Management	29
Topic 2, Data Protection Infrastructure	18
Topic 3, Data Protection Technologies	31
Topic 4, Data Protection Solutions	3
Topic 5, Mix Questions	2
Total	83

QUESTION NO: 1

Which cloud service model allows the deployment of consumer-created applications on the provider's infrastructure?

A. Platform as a Service

B. Infrastructure as a Service

C. Disaster recovery as a Service

D. Software as a Service

ANSWER: A

Explanation:

Platform as a Service is correct because it provides a provider-managed application platform on which the consumer can deploy applications that they created or acquired. The cloud provider operates and maintains the underlying infrastructure, including servers, storage, networking, operating systems, and typically the runtime environment, while the consumer focuses on application deployment and configuration. This division of responsibility enables developers to build, test, deploy, and manage applications without administering the foundational compute infrastructure themselves. The wording in the question closely matches the National Institute of Standards and Technology definition of Platform as a Service: the consumer is given the capability to deploy consumer-created or acquired applications onto the cloud infrastructure using supported programming languages, libraries, services, and tools. This is the essential characteristic used to identify the Platform as a Service model in cloud-computing concepts and data-protection training. Dell environments may use Platform as a Service offerings to host custom applications while relying on the provider’s platform controls and infrastructure operations. See the NIST SP 800-145 cloud-computing definition and the Dell cloud overview.

QUESTION NO: 2

Which plane of SDDC is used to perform administrative operations such as configuring a system and changing policies?

A. Management Plane

B. Service Plane

C. Control Pane

D. Data Plane

ANSWER: A

Explanation:

The **Management Plane** is used for administrative operations in a software-defined data center (SDDC). It provides the management interfaces, tools, and services through which administrators configure infrastructure, apply and modify policies, manage users and access controls, monitor health, and coordinate lifecycle activities such as upgrades. Rather than directly carrying application workload traffic, this plane supplies the centralized operational layer that administrators use to define the desired state of compute, storage, and network resources.

In an SDDC, management capabilities are commonly delivered through management appliances and orchestration components. These components expose administrative consoles and APIs, enabling consistent configuration and policy-driven operation across the virtualized environment. For example, VMware Cloud Foundation identifies management-domain components as the foundation for deploying, operating, and managing the SDDC, while vSphere documentation describes centralized management through vCenter Server. This makes the Management Plane the appropriate plane for system configuration and policy changes. See the VMware Cloud Foundation documentation and the VMware vSphere documentation for further details on SDDC management functions.

QUESTION NO: 3

A customer has created a change management window to perform scheduled system maintenance. During the scheduled downtime window, information will be transferred to another system to ensure continuous availability. What is this process an example of?

A. Data governance

B. Data migration

C. Automated failback

D. Disaster recovery

ANSWER: B

Explanation:

Data migration is the correct term for the planned transfer of information from one system, storage platform, application environment, or infrastructure location to another. In this scenario, the customer has established a scheduled maintenance window and will move information to another system so that services and data remain available while maintenance is performed. This is a deliberate, controlled operational activity: the data is being relocated as part of an infrastructure change, rather than being recovered after an unexpected outage.

Successful data migration commonly includes identifying the source and destination systems, copying or moving the required data, validating integrity and accessibility at the destination, and coordinating the cutover within an approved change window. The maintenance window is important because it provides an authorized period to manage service impacts, perform synchronization or final cutover tasks, and verify that the destination system can support continued operations. Dell's data-mobility capabilities are designed to support moving data between systems while minimizing disruption and maintaining access to protected workloads. For additional context on migration planning and execution, see Dell Technologies: Data Migration and NIST: Data Migration Guide.

QUESTION NO: 4

An application developer is exploring the best technology to have the application easily transportable and have a small image footprint. Which technology satisfies the request?

A. Containers

B. Traditional application

C. Virtual machines

D. Monolithic application

ANSWER: A

Explanation:

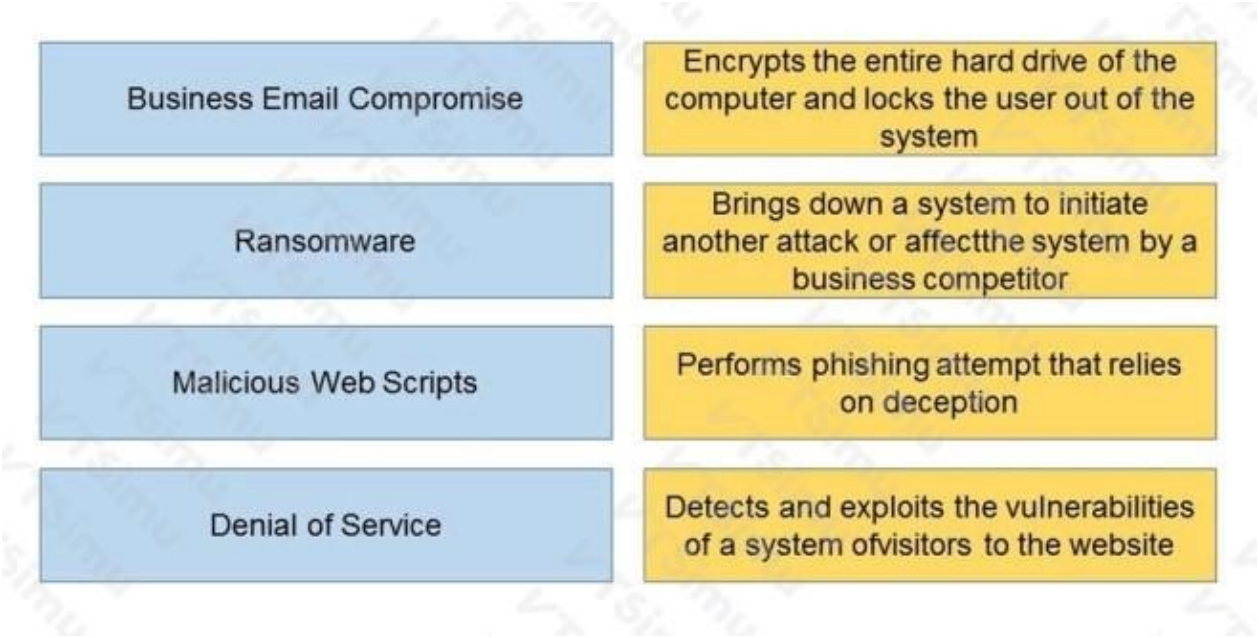
Containers are the appropriate technology because they package an application with its required libraries, dependencies, and configuration into a portable image that can run consistently across supported environments. This packaging approach helps developers move the same workload between a laptop, test environment, private cloud, and public cloud without rebuilding the application for each platform. Container images are generally small relative to machine images because containers share the host operating system kernel rather than including a complete guest operating system for every application instance. That reduced overhead supports faster image transfer, quicker startup, and more efficient use of compute and storage resources. Containerization also encourages a standardized, repeatable deployment process: the image is built once, stored in an image registry, and deployed wherever a compatible container runtime is available. Docker describes containers as isolated processes that package an application and its dependencies, while Kubernetes documentation highlights containers as lightweight and portable executable images. These characteristics directly address the requirements for easy transportability and a small image footprint. See the Docker documentation on containers and the Kubernetes containers overview.

QUESTION NO: 5 - (DRAG DROP)

DRAG DROP

Match the types of cyber-attack with their respective description.

Select and Place:



ANSWER:

Explanation:

The completed mapping correctly associates each attack with its defining behavior. Ransomware is malware that encrypts data or a device's storage and prevents normal access until the attacker's demand is addressed. In this question, the description explicitly says the entire hard drive is encrypted and the user is locked out of the system, which is the central operating characteristic of ransomware. The Cybersecurity and Infrastructure Security Agency describes ransomware as a form of malware that encrypts files and systems, disrupting access to data and operations: CISA Ransomware Guide.

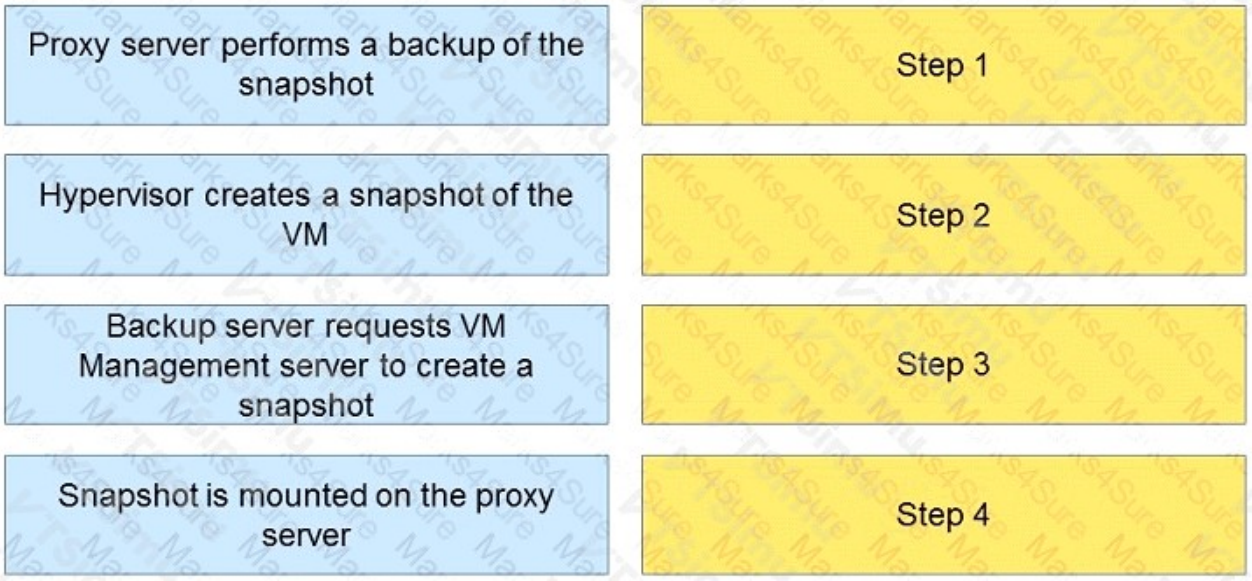
Denial of Service correctly matches the activity of taking a system down. A DoS attack attempts to make a host, service, or network unavailable, which can interrupt business operations and may support a wider attack campaign. Business Email

Compromise correctly matches a deception-based phishing attack because these campaigns impersonate trusted business contacts or executives to manipulate recipients into taking an unsafe action, often involving money or sensitive information. The FBI explains the business-email impersonation and social-engineering nature of this threat at its Business Email Compromise public-service announcement.

Finally, Malicious Web Scripts correctly matches exploitation involving website visitors. Attackers can inject or serve hostile scripts through a compromised web application or vulnerable web component; the script then executes in a visitor's browser and can steal information or perform unauthorized actions. This behavior aligns with the web-based vulnerability exploitation description. Therefore, all four displayed placements form a complete and technically correct set of mappings.

QUESTION NO: 6 - (SIMULATION)

What is the correct sequence of steps during an image-based backup?



ANSWER: See the explanation for the answer

Explanation:

The correct image-based backup sequence is:

Step 1: Backup server requests VM Management server to create a snapshot.
Step 2: Hypervisor creates a snapshot of the VM.
Step 3: Snapshot is mounted on the proxy server.
Step 4: Proxy server performs a backup of the snapshot.

This sequence allows the VM backup to be processed from the snapshot through the proxy, rather than backing up the active VM disks directly.

QUESTION NO: 7

What is a characteristic of data archiving?

A. Secondary copy of data

B. Primary copy of data

C. Short-term retention

D. Used for operational recovery

ANSWER: B

Explanation:

Primary copy of data is correct because archiving preserves the authoritative, original business record for an extended retention period. When data is archived, it is generally moved from active production storage to lower-cost storage while remaining available for search, retrieval, compliance, legal, historical, or business-reference purposes. The archived item is therefore treated as the primary retained version of that information, rather than simply being an additional recovery copy.

This distinction is central to data-protection design. A backup is a separately maintained copy intended to restore data after deletion, corruption, failure, or disaster. An archive, by contrast, manages inactive information that must be retained as the record of reference, often according to retention and governance requirements. Archiving systems commonly preserve metadata, indexing, retention controls, and accessibility so that the primary record can be located and produced when needed. Dell's data-protection portfolio similarly distinguishes long-term retention and governance use cases from operational recovery workflows. See Dell's overview of data protection and the explanation of the distinction between data backup and archiving.

QUESTION NO: 8

Which recovery mode involves rolling back a system to a previous recovery point instead of finding the cause of a fault?

A. Forward recovery

B. Complete functional recovery

C. Backward recovery

D. Degraded functional recovery

ANSWER: C

Explanation:

Backward recovery is the recovery mode that returns a system to a known-good state from an earlier recovery point, rather than first diagnosing and correcting the underlying source of the fault. This approach is appropriate when a valid backup, snapshot, checkpoint, or other saved recovery point is available and the immediate operational goal is to undo the effects of a failure, corruption, erroneous change, or other unwanted event. By restoring the prior state, the environment can resume from data and configuration known to have been consistent at the selected point in time. The recovery-point objective determines how much recent data or work may need to be recreated after the rollback, since changes made after that point are not part of the restored state. Dell's data-protection documentation describes using protected copies and recovery operations to restore workloads and data after an incident, while its cyber-recovery guidance emphasizes recovery to a clean, validated copy. These practices align with backward recovery's central idea: move back to a previously usable system state. See Dell Data Protection and Dell Cyber Recovery.