DUMPSARENA

Dell Cloud Infrastructure and Services Foundations v2 Exam

EMC D-CIS-FN-01

Version Demo

Total Demo Questions: 14

Total Premium Questions: 143

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, IT Transformation and Emerging Technologies	50
Topic 2, Cloud Computing	35
Topic 3, Virtualization	15
Topic 4, Data Protection	21
Topic 5, Security	21
Topic 6, Mix Questions	1
Total	143

QUESTION NO: 1

Which attribute of software-defined infrastructure is responsible for providing abstracted view of the IT infrastructure?

A. Abstraction and Pooling

B. Unified Management

C. Self-Service Portal

D. Metering

ANSWER: A

Explanation:

Abstraction and Pooling is correct because software-defined infrastructure separates the logical, consumable representation of compute, storage, and networking resources from the underlying physical hardware. This abstraction lets administrators and users work with virtual resource pools and services rather than needing to understand the configuration, location, or individual characteristics of each server, array, switch, or hypervisor component. Pooling then aggregates those underlying resources so they can be allocated dynamically to workloads according to policy and demand. Together, these capabilities present infrastructure as a flexible shared service, while software controls provisioning and placement behind the scenes. This model is foundational to cloud-style infrastructure delivery: consumers request capacity or services through logical interfaces, and the platform maps those requests to available physical resources. NIST describes resource pooling as a core cloud characteristic in which provider resources are pooled to serve multiple consumers dynamically, while virtualization provides the key abstraction layer that decouples services from physical infrastructure. See NIST SP 800-145: The NIST Definition of Cloud Computing and VMware's virtualization overview.

QUESTION NO: 2

What is a benefit of secure multitenancy?

A. Reduces unauthorized access to resources

B. Blocks unauthorized access to resources

C. Eliminates data breach risks

D. Protects cloud infrastructure

ANSWER: D

Explanation:

Protects cloud infrastructure is correct because secure multitenancy applies isolation and access-control boundaries between customers, workloads, applications, and administrative domains that share a cloud environment. In a multitenant design, compute, storage, network, and management-plane resources may be physically shared; security controls must therefore ensure that one tenant cannot affect, view, or use another tenant's resources outside of explicitly authorized access. This isolation protects the underlying cloud infrastructure as well as the workloads running on it. Typical mechanisms include identity and access management, role-based authorization, network segmentation, virtual-machine or container isolation, encryption, and monitoring. Together, these controls allow a provider to deliver pooled resources efficiently while maintaining separation, confidentiality, integrity, and controlled availability for each tenant. NIST identifies resource pooling and broad network access as essential cloud characteristics, which makes robust isolation a foundational security concern in shared cloud environments. The Cloud Security Alliance likewise emphasizes tenant isolation and secure separation as central considerations for cloud architectures. See NIST SP 800-145: The NIST Definition of Cloud Computing and the Cloud Security Alliance Security Guidance.

QUESTION NO: 3

Which cloud service management option defines the suite of service offerings and aligns it to the service provider's strategic business goals?

A. Portfolio

B. Capacity

C. Demand

D. Operation

ANSWER: A

Explanation:

Portfolio is correct because service portfolio management provides the strategic view of a service provider's complete set of services. It defines which services are being considered, developed, delivered, maintained, or retired, enabling the provider to make deliberate investment and lifecycle decisions. In a cloud environment, this portfolio perspective connects the available service offerings—such as compute, storage, protection, and platform services—to customer needs, business priorities, expected value, costs, risks, and the provider's overall strategy.

By managing services as a portfolio, the provider can ensure that its catalog of active offerings supports defined business outcomes rather than growing as an uncoordinated collection of technical capabilities. It also supports governance over service investment decisions, helping determine which offerings should be introduced, enhanced, retained, or withdrawn as strategic objectives evolve. This strategic alignment is a core service-management principle: services must create value for consumers while supporting the service provider's organizational goals. The ITIL guidance describes service management as enabling value co-creation through services and includes portfolio-level strategic decision-making as part of managing service offerings. See the ITIL service value system overview and the ITIL 4 Foundation overview.

QUESTION NO: 4

An organization requires double the processing capacity for a specific duration to handle increased workload. For the remaining period, the organization might want to release the idle resources to save costs. The workload variations may be seasonal or transient.

Which cloud characteristic enables the consumer to handle such variations in workloads and IT resource requirements?

A. Resource pooling

B. On-demand self-service

C. Rapid elasticity

ANSWER: C

Explanation:

Rapid elasticity is the cloud characteristic that enables an organization to scale processing capacity up when workload demand increases and scale it back down when that demand subsides. In this scenario, the consumer needs additional compute resources for a limited period, such as a seasonal business peak or a temporary surge in transactions, and then wants to release unused capacity to avoid paying for idle resources. Rapid elasticity supports this dynamic expansion and contraction of resources, often automatically or with minimal administrative effort. From the consumer's perspective, capacity can appear to be available in virtually any quantity when needed, without requiring permanent investment in infrastructure sized for peak demand. This capability is central to the cost-efficiency and operational flexibility of cloud computing because resources are aligned more closely with actual consumption over time. The NIST cloud-computing definition identifies rapid elasticity as an essential characteristic and describes capabilities that can be elastically provisioned and released to scale rapidly outward and inward commensurate with demand. Dell's cloud foundations material likewise presents elasticity as the ability to adjust resources according to changing workload requirements. See the NIST SP 800-145 cloud computing definition and Dell Technologies cloud computing resources.

QUESTION NO: 5

Which fault-tolerant mechanism, in a highly available application design is implemented within a code to handle service that is temporarily down?

A. Checkpointing

B. Monitoring Application Availability

C. Graceful Degradation

D. Retry Logic

ANSWER: D

Explanation:

Retry Logic is the fault-tolerance mechanism implemented in application code to address temporary service interruptions. A distributed application can encounter transient failures when a dependency is briefly unavailable because of network congestion, service maintenance, throttling, a failover event, or a short-lived internal error. Retry logic allows the application to repeat an operation after such a failure rather than immediately treating it as a permanent error. This gives the affected service time to recover and can preserve availability from the user's perspective.

Effective retry behavior is selective and controlled. The application should retry only failures that are likely to be transient, use a bounded number of attempts, and introduce a delay between attempts. Exponential backoff, often with random jitter, reduces the chance that many clients retry simultaneously and overload a recovering service. Operations should also be designed to be idempotent where possible, so that retrying a request does not unintentionally create duplicate updates or transactions. These practices make retry logic a core resiliency pattern for highly available application designs. Guidance on transient-fault handling and retry strategies is available in Microsoft Azure Architecture Center and the AWS Prescriptive Guidance retry-with-backoff pattern.

QUESTION NO: 6

What term refers to businesses that cautiously and gradually embrace digital transformation?

A. Digital Evaluators

B. Digital Laggards

C. Digital Leaders

D. Digital Adopters

ANSWER: A

Explanation:

Digital Evaluators is the term used for organizations that are progressing with digital transformation, but do so carefully and incrementally. These businesses recognize that modernizing technology, processes, and operating models is important, yet they tend to evaluate initiatives closely before committing broadly. Their transformation efforts commonly proceed through limited projects, validation of business value, and measured adoption rather than through a rapid, enterprise-wide shift. This position reflects an organization that has moved beyond ignoring digital change but has not yet established the speed, scale, and organizational confidence associated with more advanced transformation maturity. Dell Technologies' Digital Transformation Index describes maturity segments that help organizations benchmark their progress and identify the steps needed to strengthen digital capabilities. The evaluator profile is characterized by a cautious approach to adopting and scaling digital technologies, which directly matches the wording in the question. Understanding these maturity categories helps technology and business leaders align investment priorities, skills development, data use, and modernization plans with their current readiness level. See Dell Technologies' Digital Transformation Index and its discussion of digital transformation.

QUESTION NO: 7

Which cloud service lifecycle phase involves discovering services assets

A. Service Planning

B. Service Termination

C. Service Operation

D. Service Creation

ANSWER: A

Explanation:

Service Planning is the cloud service lifecycle phase that includes discovering service assets. Before a cloud service can be designed, provisioned, or operated, the provider needs a clear understanding of the available and required resources, capabilities, dependencies, and existing service components. Asset discovery establishes this baseline by identifying infrastructure, platforms, applications, and related operational capabilities that may be used to support the proposed service. This information enables informed service definition, capacity considerations, cost estimation, governance decisions, and alignment of the service with business requirements. In practical cloud-service management, planning converts business demand into an actionable service strategy and identifies the assets needed to deliver that strategy. Discovery is therefore an early lifecycle activity: it supplies the inventory and context used to plan the service rather than being an activity that begins only after the service is already running. Dell's cloud and infrastructure portfolio emphasizes assessing existing environments and capabilities as a foundation for modernization and cloud-service decisions; see Dell Cloud Solutions. This also aligns with IT service-management guidance, where planning and design activities use knowledge of resources and service components to ensure services can meet agreed requirements; see AXELOS ITIL.

QUESTION NO: 8

What involves the automated arrangement, coordination, and management of various systems components that enable a user to make a service request using the self-service portal?

A. Orchestrated service catalog updates

B. Automated service catalog management

C. Automated portfolio management

D. Orchestrated service delivery

ANSWER: D

Explanation:

Orchestrated service delivery is the automated coordination of the infrastructure and operational tasks needed to fulfill a service requested through a self-service portal. A catalog item presents the consumer with a standardized request, such as a virtual machine, application environment, storage allocation, or other IT service. After the request is submitted, orchestration executes the associated workflow across the required systems and domains. This can include applying policies, triggering provisioning tools, configuring compute, network, and storage resources, integrating approval steps, and reporting completion back to the requester. The key characteristic is that separate automated activities are arranged into an end-to-end service-delivery process rather than requiring an administrator to manually coordinate each task. This approach makes service fulfillment repeatable, faster, policy-driven, and consistent with the organization's defined service offerings. It also supports the self-service cloud model by allowing users to request approved services on demand while the underlying platform handles fulfillment through coordinated automation. The National Institute of Standards and Technology describes on-demand self-service as a core cloud characteristic in its Cloud Computing definition, while Red Hat explains how orchestration coordinates multiple automated tasks into complete workflows in its orchestration overview.

QUESTION NO: 9

Which host-based security attribute supports audit, multifactor authentication, and IP address filtering?

A. Virtual machine hardening

B. Application hardening

C. Operating system hardening

D. Hypervisor hardening

ANSWER: D

Explanation:

Hypervisor hardening is correct because the hypervisor is the foundational host layer that controls access to virtual machines and the virtualization platform's management functions. Hardening this layer includes enforcing strong administrative authentication, which can include multifactor authentication; generating and retaining audit records for administrative actions and security-relevant events; and restricting management-plane connectivity through IP-based access controls or firewall rules. These measures reduce the attack surface of the virtualization host and help ensure that only authorized administrators and approved management systems can interact with it. Audit capabilities also provide accountability and support investigation of configuration changes, login activity, and other events affecting the virtual infrastructure. NIST identifies secure configuration, access control, and monitoring of the hypervisor as central requirements for virtualization security because compromise of this layer can affect every workload it hosts. VMware's vSphere security guidance similarly addresses authentication, logging and auditing, and network protections for ESXi hosts and the management environment. See NIST SP 800-125, Guide to Security for Full Virtualization Technologies and VMware vSphere Security documentation.

QUESTION NO: 10

Which component presents service catalog and cloud interfaces, enabling consumers to order and manager cloud services?

A. Cloud Operating System

B. Orchestrator

C. Cloud Portal

D. Service automation

ANSWER: C

Explanation:

Cloud Portal is correct because it is the consumer-facing layer of a cloud-management environment. It provides a unified web-based interface through which authorized users can browse a service catalog, request approved infrastructure or application services, monitor request status, and manage the services available to them. The portal simplifies consumption by exposing standardized offerings rather than requiring consumers to interact directly with the underlying compute, storage, network, and automation platforms. When a consumer submits a catalog request, the portal passes the request into the cloud-management and orchestration processes, where policy, approval, provisioning, and lifecycle activities can be applied. This separation enables IT to present services in a consistent, business-oriented form while retaining governance and operational control behind the interface. Service catalogs are specifically designed to make entitled services discoverable and requestable by users, as described in the VMware Aria Automation Service Broker documentation. This role also aligns with the NIST cloud-computing characteristic of on-demand self-service, in which consumers can provision capabilities through a provider's interface without direct interaction with provider personnel; see NIST SP 800-145.

QUESTION NO: 11

Which compute system component contains boot firmware?

A. Operating System

B. Hard Disk Drive

C. Read Only Memory

D. Random Access Memory

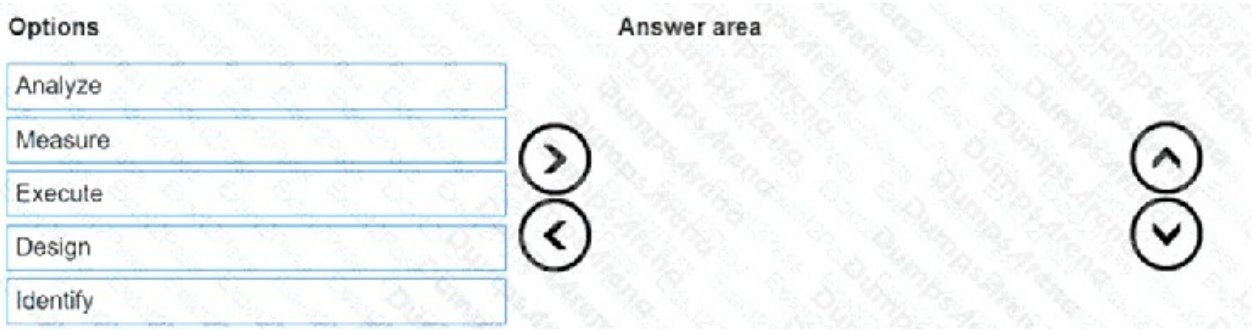
ANSWER: C

Explanation:

Read Only Memory is correct because a compute system needs boot firmware to remain available when the system is powered off. This firmware provides the initial instructions executed at startup: it initializes essential hardware, performs early platform checks, identifies a bootable device, and transfers control to the next stage of the boot process. Traditionally, these instructions were stored in ROM; in contemporary systems, the firmware is commonly held in rewritable flash memory, but this is still categorized as nonvolatile ROM in foundational computer architecture terminology. The firmware is commonly known as BIOS or UEFI. Its nonvolatile storage is essential because startup code must be present before an operating system is loaded and before working memory can be used for normal program execution. Dell documentation describes BIOS as firmware that controls the system's basic hardware functions and can be updated through a BIOS flash process, reflecting its storage in persistent firmware memory. UEFI likewise defines the firmware environment that begins platform initialization and boot management before the operating system starts. See Dell's BIOS overview and the UEFI specifications for additional technical context.

QUESTION NO: 12 - (SIMULATION)

What is the correct order of the business continuity plan principles?



ANSWER: See the explanation for the answer

Explanation:

The correct order of the business continuity plan principles is:

Add the options to the answer area in this order, then use the up/down arrows if needed to arrange them.

QUESTION NO: 13

What is true about change management?

A. Defines SLA compliance

B. Triggers alerts

C. Monitors compliance

ANSWER: C

Explanation:

Monitors compliance is correct because change management is a controlled governance process that verifies changes are requested, assessed, authorized, implemented, documented, and reviewed according to established organizational policies

and procedures. Compliance monitoring is integral to this process: change records provide an auditable trail showing that the required approvals, risk evaluations, implementation steps, validation activities, and post-implementation reviews occurred. This oversight helps maintain the integrity and availability of services while ensuring that operational changes meet internal controls, regulatory obligations, and security requirements. In an infrastructure environment, the change-management process also establishes accountability by recording who requested and approved a change, when it was performed, and whether the intended result was achieved. These records allow service-management and audit teams to measure adherence to the change process and identify areas where process controls need improvement. NIST configuration-management guidance similarly identifies change control, documentation, and monitoring as essential elements of maintaining secure and compliant information systems. See NIST SP 800-128, Guide for Security-Focused Configuration Management and the ISO/IEC 27001 information-security management standard.

QUESTION NO: 14

What is a characteristic of reporting?

A. Provides tabular or graphical views of monitored information

B. Provides information about events or impending threats or issues

C. Displays a personalized functional interface

D. Presents service instances to consumers in real time

ANSWER: A

Explanation:

Provides tabular or graphical views of monitored information is correct because reporting converts collected monitoring data into a structured presentation that can be reviewed, shared, and used to identify trends over a selected period. A report commonly organizes metrics, status data, capacity figures, performance measurements, and historical results into tables, charts, or graphs. This presentation makes raw monitored data understandable and supports operational decisions, planning, auditing, and service-level evaluation. Reporting is generally based on stored or aggregated monitoring information, so it is particularly useful for examining utilization patterns, comparing values over time, and communicating infrastructure health to technical and business stakeholders. Dell's CloudIQ documentation describes monitoring and reporting capabilities that present infrastructure data through dashboards, charts, and reports, illustrating how visual and tabular views help users interpret collected telemetry. Dell also explains that its management tools provide visibility into infrastructure health, performance, and capacity information, which can be consumed in report-oriented views. See Dell CloudIQ: A Detailed Review and Dell CloudIQ overview.