DUMPSBOSS.

Nutanix Certified Professional - Multi cloud Infrastructure (NCP-MCI 5.15)

Nutanix NCP-MCI-5.15

Version Demo

Total Demo Questions: 29

Total Premium Questions: 297

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Cloud Concepts	26
Topic 2, Planning	23
Topic 3, Deploying a Nutanix Cluster	10
Topic 4, Configuring a Nutanix Cluster	110
Topic 5, Managing a Nutanix Cluster	99
Topic 6, Troubleshooting a Nutanix Cluster	29
Total	297

QUESTION NO: 1

Which two features require the Nutanix Guest Tools package is installed (Choose Two)

A. Self-Service Restore

B. Volume Snapshot Services

C. Network Visualization

D. Image service

E. Prism Central

ANSWER: A B

Explanation:

Self-Service Restore requires Nutanix Guest Tools (NGT) because the feature depends on the guest-side NGT components to coordinate restore-related actions within the virtual machine. NGT establishes the communication channel between the Nutanix platform and the guest operating system, allowing authorized users to initiate and complete supported restore operations without requiring direct administrator intervention for each request. This guest integration is an essential part of providing a controlled, VM-aware self-service recovery workflow.

Volume Snapshot Services requires NGT because NGT includes the guest-side integration needed to work with Microsoft Volume Shadow Copy Service (VSS). VSS coordinates a consistent point-in-time view of application data on supported Windows guests, helping ensure that snapshots are application-consistent rather than merely crash-consistent. During a protection operation, the guest tools coordinate the VSS quiescing process so applications and their data are placed into an appropriate state before the snapshot is created. Nutanix documents NGT as the mechanism that enables guest OS services, including VSS-based application-consistent snapshots and self-service restore capabilities. See the Nutanix Prism Web Console Guide: Nutanix Guest Tools and Nutanix Prism Web Console Guide: Self-Service Restore.

QUESTION NO: 2

A Nutanix administrator receives a request from the networking team to start SNMP Traps to their central reporting solution. The administrator creates the transport. The central monitoring tool is not able to clearly read the SNMP traps that are being sent.

What does the administrator need to provide to read SNMP traps correctly?

A. Cluster Virtual IP address

B. SNMP Trap Port

C. TCP/IP address

D. Nutanix MIB file.

ANSWER: D

Explanation:

The administrator needs to provide the **Nutanix MIB file.** An SNMP management or central monitoring platform can receive trap messages using the configured transport, but it needs the relevant Management Information Base (MIB) definitions to translate Nutanix-specific object identifiers (OIDs), event names, severity values, and associated variables into meaningful, human-readable alerts. Without the Nutanix MIB loaded or imported into the monitoring tool, traps may appear as numeric OIDs or otherwise lack the contextual labels needed for the operations team to interpret them clearly.

Nutanix makes its MIB available for integration with external SNMP monitoring systems. The monitoring team should import the Nutanix MIB into its central reporting solution and ensure that the tool is configured to use it when decoding incoming traps. This supplies the vendor-specific schema required to map the trap payload to recognizable Nutanix event information. Nutanix documentation describes configuring SNMP alert transport and obtaining the MIB file for third-party monitoring

integration. See the Nutanix Prism Central SNMP alerts documentation and the Nutanix Support Portal for Nutanix MIB downloads and product documentation.

QUESTION NO: 3

An administrator is preparing to migrate VMs from a legacy ESXi cluster to a new AHV cluster.

Which action must be the administrator perform on the AHV cluster to migrate VM data?

A. Install the Nutanix Virt0 drivers

B. Whitelist the ESXi cluster IP address

C. Create placeholder VMs

D. Install Nutanix Self servicing restore.

ANSWER: B

Explanation:

Whitelist the ESXi cluster IP address is required because the AHV target environment must permit the source ESXi hosts to communicate with the Nutanix cluster during the VM data-transfer workflow. Nutanix migration operations, typically orchestrated through Nutanix Move, establish connectivity between the source vSphere environment and the target cluster so that VM disks can be replicated and cut over safely. Adding the relevant ESXi source IP addresses to the AHV cluster whitelist ensures that required source-host communications are accepted rather than blocked by the target cluster's access controls. This preparation should be completed before initiating replication, along with validating routing, DNS where applicable, and the required ports between the migration appliance, vCenter/ESXi environment, and the Nutanix cluster. The whitelist should contain the applicable management IP address or addresses for the ESXi hosts participating in the migration, using the organization's approved network-access process. Nutanix documents the required source and target connectivity prerequisites as part of Move migration planning and preparation. See the Nutanix Move documentation and the Nutanix Move product overview for migration workflow and planning guidance.

QUESTION NO: 4

An administrator needs to ensure that two VMs running separate instances of a database application are not placed on the same AHV host.

Which configuration should the administrator use?

A. VM-VM anti-affinity

B. VM-Host affinity

C. VM HA Reservation

D. Acropolis Dynamic Scheduling

ANSWER: A

Explanation:

VM-VM anti-affinity is the correct configuration. A VM-VM anti-affinity policy instructs AHV to place the specified virtual machines on different hosts whenever possible. This reduces the likelihood that a single host failure affects both database instances.

The policy is appropriate when application availability depends on separating redundant workload components across hosts. It does not reserve host capacity, configure storage replication, or restrict a VM to a specific subset of hosts. Nutanix documents VM placement policies in the Nutanix Documentation portal.

QUESTION NO: 5

Which CVM service is primary responsible for handling all metadata operation with a Nutanix cluster?

A. Stargate

B. Zeus

C. Genesis

D. Cassandra

ANSWER: D

Explanation:

Cassandra is the distributed database service in a Nutanix cluster that is primarily responsible for storing and managing the cluster's metadata. This metadata describes the logical structure and state of data managed by the Nutanix Distributed Storage Fabric, including information needed to locate data and maintain its consistency across the cluster. Cassandra runs on the Controller VMs as a distributed, replicated service, allowing metadata to remain available even if an individual CVM or node is unavailable. Its distributed design also enables the metadata layer to scale as nodes are added to the cluster.

Metadata management is fundamental to Nutanix's ability to present storage as a unified pool while placing, replicating, and recovering data across local disks and nodes. The Cassandra service maintains this metadata independently of the user virtual-machine data path, providing the durable database foundation required for cluster operations. Nutanix architecture documentation identifies Cassandra as the metadata store within the platform. For additional architecture context, see the Nutanix Bible and Nutanix's Cloud Platform overview.

QUESTION NO: 6

An Engineer logs into a CVM to troubleshoot connectivity loss between two CVMs and find the following interfaces subnets and WLANs configured.

-eth0 – VLAN10-10.1.10.0/24

eth01–No VLAN-192.168.5.0/24

eth2 – LAN20-10.1.20.0/24

Which two Nutanix networking features are being utilized? (Choose two)

A. Internal vSwitch

B. IP address management (IPAM)

C. Network Load balancing

D. Backplane LAN

ANSWER: A D

Explanation:

Internal vSwitch and **Backplane LAN** are being utilized. Nutanix uses an internal virtual switch to provide the private connectivity required by controller services and local host-to-CVM communication. This internal switching construct is distinct from the externally reachable networks that carry management or guest-VM traffic. The interface without a VLAN assignment and using the private 192.168.5.0/24 subnet is characteristic of a private, non-routed infrastructure network rather than a tenant or externally presented VLAN.

The **Backplane LAN** provides the private network path used for inter-node and controller communication within the Nutanix cluster. A private backplane subnet supports cluster services that require reliable east-west connectivity between CVMs, including distributed storage and control-plane functions. The VLAN-tagged 10.1.10.0/24 and 10.1.20.0/24 networks show that the environment also carries segmented external traffic, while the untagged private subnet identifies the backplane-

oriented connectivity. This combination is consistent with Nutanix networking designs that separate cluster-internal traffic from externally accessible VLANs. Nutanix documents AHV networking concepts and virtual-switch configuration in its AHV Administration Guide; additional architecture and networking background is available in the Nutanix Bible.

QUESTION NO: 7

the analysis dashboard allows you to create which 2 type of charts? (Choose two)

A. entity (vm,host,disk,memory,etc.)

B. metric (IOPS, sequential reads, etc).

C. open support cases

D. out-of-band management

ANSWER: A B

Explanation:

The Analysis dashboard in Nutanix Prism Central is designed for customizable monitoring and visualization of infrastructure and workload behavior. It supports charts organized by **entity (vm,host,disk,memory,etc.)**, allowing an administrator to select a monitored object or entity type and view relevant performance information across the selected scope. This is useful for examining the health and behavior of specific virtual machines, hosts, storage-related objects, and other managed resources.

It also supports charts organized by **metric (IOPS, sequential reads, etc).**. Metric-based charts plot a selected performance measure over time, enabling analysis of values such as IOPS, throughput, latency, CPU utilization, memory utilization, and read/write activity. Administrators can tailor the time range, aggregation, and displayed entities to investigate trends and correlate resource consumption with workload activity. Together, entity and metric chart types provide the core Analysis dashboard workflow: select the resource context and then visualize the relevant operational measurements. Nutanix documents Analysis as a Prism Central capability for creating and viewing custom performance charts and monitoring cluster and workload metrics. See the Nutanix Prism Central Analysis dashboard documentation and the Nutanix Cloud Manager product overview.

QUESTION NO: 8

what does an administrator do before shutdown nutanix node for maintenance in the cluster? (Choose two)

A. verify data resiliency status in the cluster

B. reclaim license

C. migrate all guests vm from the host

D. shutdown the cluster in that host

ANSWER: A C

Explanation:

Before taking a Nutanix node offline for planned maintenance, the administrator should verify data resiliency status in the cluster and migrate all guests VM from the host. Checking resiliency confirms that the cluster is healthy and that required replicas are available before a node is removed from service. This is particularly important because the cluster must retain sufficient fault tolerance while the node is unavailable. The administrator should review cluster health and any active alerts, then ensure that data-resiliency operations have completed or that the environment can safely tolerate the maintenance event.

Guest virtual machines should also be moved off the host before shutdown. Nutanix supports live migration of running VMs, allowing workloads to continue with minimal or no interruption while the underlying host undergoes maintenance. In practice, putting a host into maintenance mode coordinates this workflow by evacuating eligible VMs and preparing the node for

service. These actions protect workload availability and help ensure that the cluster continues to satisfy its configured redundancy requirements throughout maintenance. Nutanix documents node-maintenance workflows and the associated health checks in the Prism Web Console Guide and provides operational guidance in its Nutanix Support Knowledge Base.

QUESTION NO: 9

A Nutanix administrator needs to replace a self-signed SSL certificate with a CA generated certificate in Prism.

Which three files are required to install the CA generated certificate in Prism? (Choose three)

A. CA Certificate or Chain (ca_chain_certs.cer)

B. Public Certificate (PublicCert.cer)

C. Certificate Signing Request (server.csr)

D. Private Server Key (private_server.key)

E. Public Server Key (public_server.key)

ANSWER: A B D

Explanation:

Installing a CA-issued certificate in Prism requires the certificate material that establishes the server identity, proves control of that identity, and supplies the trust path to the issuing authority. **Public Certificate (PublicCert.cer)** is the signed server certificate returned by the CA after it processes the certificate request. This certificate contains the Prism endpoint identity and is what clients receive during the TLS handshake. **Private Server Key (private_server.key)** is the private cryptographic key that corresponds to the public key embedded in the signed certificate. Prism uses this key to prove possession of the certificate identity and to establish secure TLS sessions. **CA Certificate or Chain (ca_chain_certs.cer)** provides the intermediate and, where applicable, root CA certificates needed for clients to construct and validate the chain of trust from the Prism server certificate to a trusted CA. These three artifacts are therefore uploaded together when replacing Prism's default self-signed certificate. The certificate-signing request is used earlier to obtain the signed certificate from the CA; it is not part of the installed certificate bundle. Nutanix documents certificate management in the Prism Central Guide; TLS certificate and chain concepts are also described in DigiCert's PEM certificate guidance.

QUESTION NO: 10

A node with Erasure Coding fails.

What is the impact?

A. The node stops utilizing Erasure Coding.

B. Potentially increased amount of data stored in the SSD tier.

C. Increased Controller VM CPU Load.

D. AQS unable to do deduplication during the Erasure Coding failure.

ANSWER: C

Explanation:

Increased Controller VM CPU Load. is the expected impact. Nutanix Erasure Coding stores data in a distributed stripe composed of data fragments and parity information. When a node that contains a fragment is unavailable, the affected data remains accessible because the Controller VMs can reconstruct the required information from the surviving fragments and parity. This reconstruction process requires additional calculation, and the participating Controller VMs perform the encoding and decoding work. Consequently, a node failure can temporarily increase Controller VM CPU utilization, particularly when workloads read data affected by the unavailable node or while the cluster performs recovery and re-protection activity.

Erasure Coding is designed to provide storage efficiency while preserving fault tolerance. Its operational tradeoff is that recovering data from an erasure-coded stripe is more computationally intensive than reading an intact local replica. The cluster automatically manages this behavior and restores the intended protection state after capacity and node availability permit. Nutanix describes Erasure Coding as a distributed data-reduction mechanism that uses parity and requires computation to reconstruct data when necessary; see the Nutanix Bible: AOS storage and data reduction and Nutanix's AOS platform overview.

QUESTION NO: 11

Prism Central will be installed manually on an AHV cluster.

Which three disk images must be downloaded from the portal for the Prism Central VM? (Choose three.)

A. var

B. tmp

C. boot

D. home

E. data

ANSWER: C D E

Explanation:

Manual deployment of a Prism Central virtual machine requires the three virtual disk images that make up its appliance layout: **boot**, **home**, and **data**. The boot image provides the operating-system boot volume required to start the appliance. The home image supplies the Prism Central application and supporting system content used by the appliance. The data image provides the persistent storage area used for Prism Central data, including the information required for ongoing operation after deployment. During the manual installation workflow, these images are obtained from the Nutanix Support Portal, uploaded to an image service, and attached to the newly created Prism Central virtual machine according to the documented disk configuration. All three are therefore required to create a complete, supported Prism Central appliance rather than merely a bootable virtual machine. Nutanix documents the manual Prism Central deployment process, including downloading and attaching the required disk images, in the Prism Central Guide. Additional Prism Central documentation and version-specific deployment resources are available through the Nutanix Support Portal.

QUESTION NO: 12

what additional features are available with prism pro(prism central with pro license)? (Choose two)

A. centralized upgrades

B. VM right-sizing

C. vm tagging

D. Capacity planning

ANSWER: B D

Explanation:

VM right-sizing is a Prism Pro capability because Prism Pro includes resource-optimization analytics that evaluate VM utilization over time and provide recommendations for adjusting allocated compute resources. These recommendations help administrators align vCPU and memory assignments with actual workload demand, reducing waste while maintaining appropriate headroom. This is part of Prism Pro's intelligent operations and analytics functionality, which extends the core multicluster management features of Prism Central.

Capacity planning is also provided by Prism Pro. It uses historical utilization and projected growth trends to forecast when infrastructure resources may be exhausted. Administrators can model future demand and assess the effect of adding workloads or hardware, allowing them to make proactive purchasing and placement decisions. Together, right-sizing and capacity planning represent the optimization and predictive-planning functions associated with the Prism Pro license. Nutanix describes Prism's management and operations capabilities at Nutanix Prism; additional product documentation and version-specific guides are available through the Nutanix Support Portal documentation library.

QUESTION NO: 13

An administrator has just executed a maintenance window for some applications running on their nutanix cluster. After completing the maintenance, they want to assess the health of the cluster and make sure that there is no impact during the maintenance.

Which three dashboards in prism will assist the administrator in making this determination? (Choose Three)

A. Data Protection

B. Cluster Health

C. Tasks

D. Alerts

E. Analysis

ANSWER: B D E

Explanation:

Cluster Health, **Alerts**, and **Analysis** provide the complementary operational views needed after maintenance. Cluster Health presents the current health state of the cluster and its components, allowing the administrator to verify that core services, hosts, storage, and resiliency-related checks have returned to a healthy state. Alerts supplies the active and historical warning and critical events that may have been raised during the maintenance period, helping the administrator identify conditions requiring follow-up and confirm they have cleared. Analysis provides time-based performance charts for key cluster and workload metrics, such as CPU, memory, storage, I/O latency, and throughput. Reviewing the maintenance time range against the periods before and after it makes it possible to identify whether the activity caused abnormal resource consumption or performance degradation. Together, these views validate both present cluster health and the operational impact observed throughout the maintenance window. Nutanix describes Prism Element as the interface for monitoring cluster health, alerts, and performance information; see the Nutanix Prism overview and the Prism Element Cluster Health documentation.

QUESTION NO: 14

Which three cluster operations require an administrator to reclaim licenses?(Choose three)

A. Destroy a cluster.

B. Upgrade a cluster

C. Migrate a cluster

D. Remove a Node from a cluster

E. Move Nodes between clusters.

ANSWER: A D E

Explanation:

License reclamation is required whenever licensed capacity is permanently removed from its current cluster assignment or the cluster that holds the entitlement is no longer in service. **Destroy a cluster.** requires reclamation because the cluster's

assigned license capacity must be returned to the organization's available license inventory after the cluster is decommissioned. **Remove a Node from a cluster** requires reclamation because the removed node's licensed CPU-core capacity is no longer consumed by that cluster and should be made available for a future assignment. **Move Nodes between clusters.** also requires reclamation from the source cluster before the relevant capacity can be allocated to the destination cluster. This process keeps the licensing inventory aligned with the actual cluster and node topology, prevents capacity from remaining assigned to infrastructure that no longer uses it, and ensures that the destination environment can be licensed correctly. Nutanix licensing guidance describes managing assignments and reclaiming capacity through the Nutanix Support Portal's license-management workflow. See the Nutanix Licensing Guide and the Nutanix Support Portal for license administration resources.

QUESTION NO: 15

An administrator recently executed maintenance on their network. After they would like to verify that this maintenance window did not have any adverse effects on their Nutanix Cluster by running Nutanix Cluster Check (NCC)

Which two interface can be used to run NCC? (Choose two)

A. REST API

B. PowerShell

C. Prism

D. CLI

E. IPMI

ANSWER: C D

Explanation:

Prism and **CLI** are the supported interfaces for running Nutanix Cluster Check (NCC). Prism provides a graphical workflow for administrators to initiate and review cluster health checks without requiring command-line access. This is useful after planned maintenance because the results are presented in the management interface and can quickly identify health conditions that require attention. In Prism Element, NCC checks are available through the cluster health and diagnostic functionality.

The command-line interface provides direct access to NCC from a Controller VM, using the `ncc` command. Administrators can run the complete suite or targeted checks, making the CLI particularly useful for detailed operational validation, troubleshooting, automation through shell tooling, and collecting output for support cases. Running NCC after network maintenance helps validate Nutanix services, connectivity, configuration, and overall cluster health from the Nutanix software perspective.

Nutanix documents NCC as a cluster-health utility and provides its operational guidance through the Nutanix Support Portal. See the Nutanix Support Portal documentation library and Nutanix's Product Support resources for the applicable NCC guide and version-specific command reference.

QUESTION NO: 16

A VM in a 12-node Nutanix cluster is hosting an application that has specific Physical GPU requirements. Only three nodes in the cluster meet this requirement.

The administrator wants to allow a general workload to be distributed across all nodes in the cluster and must make sure that the node hosting the VM meets its requirements.

How should the administrator perform this task?

A. Create a sperate three-node cluster using the nodes that meet the requirement.

B. Configure VM-Host affinity for the nodes that meet the application's GPU requirement.

C. Over-Provision the application VM with additional virtual GPUs.

D. Configure anti-affinity rules between the application VM and the other VMs running on the cluster.

ANSWER: B

Explanation:

Configure VM-Host affinity for the nodes that meet the application's GPU requirement. A VM-host affinity policy constrains placement of the specified VM to a defined set of eligible AHV hosts. In this case, the administrator creates an affinity rule for the application VM and selects the three nodes equipped with the required physical GPUs. This preserves the application's hardware requirement while leaving the remaining cluster nodes available for normal placement, balancing, and migration of general workloads.

The policy is particularly appropriate because physical GPUs are host-attached resources: simply assigning virtual GPU resources to a VM does not ensure that every potential destination host has the necessary compatible physical GPU hardware. VM-host affinity supplies that placement guarantee during lifecycle events such as VM startup, live migration, and recovery placement, subject to available eligible hosts and resources. The cluster remains a single 12-node cluster, retaining its unified management and resource pool rather than partitioning infrastructure solely for one workload. Nutanix documents VM affinity controls in its AHV administration material and provides product documentation through the Nutanix Documentation portal. Additional AHV operational guidance is available in the Nutanix Product Support resources.

QUESTION NO: 17

How should an administrator configure a custom alert for a specific VM in Prism?

A. Modify an existing alert to only alert on the specific VM.

B. Modify VM settings to add the custom alert.

C. Modify the alerts to add a new custom alert policy.

D. Modify node settings to add the custom alert.

ANSWER: C

Explanation:

Modify the alerts to add a new custom alert policy. In Prism Central, alert policies are the mechanism for defining administrator-specific monitoring rules beyond the built-in alert set. The administrator creates a policy from the Alerts area, selects the applicable entity scope and condition, and targets the policy to the required virtual machine. The policy can then evaluate a relevant metric or event against a defined threshold and generate an alert when that condition is met. This approach keeps alerting centrally managed and allows the rule to be enabled, adjusted, or assigned to notification recipients without changing the VM's core configuration. A policy can be made sufficiently specific by using VM-level entity selection and the appropriate filter or scope, so alerts produced by the rule apply to the intended workload. Nutanix documents alert-policy creation and management as a Prism Central Alerts function, including the selection of alert conditions and affected entities. See the Nutanix Prism Central Guide: Alert Policies for the policy workflow and configuration details.

QUESTION NO: 18

An administrator wants to use Volumes to connect to physical servers that are not able to be virtualized.

Which three things must be configured for Volumes to support iSCSI clients? (Choose three)

A. Enable external client access

B. Client OS iSCSI initiator

C. iSCSI Multipathing I/O

D. Cluster Virtual IP address

E. Data Services IP address

ANSWER: A B E

Explanation:

To present Nutanix Volumes to a physical, non-virtualized server over iSCSI, external access must first be enabled for the relevant Volume Group. **Enable external client access** permits hosts outside the Nutanix virtualization environment to connect to the Volume Group using the iSCSI protocol. The physical host must also have a functioning **Client OS iSCSI initiator**, since this software component discovers the Nutanix iSCSI target, establishes authenticated sessions where applicable, and exposes the attached volume as a disk to the operating system.

A **Data Services IP address** is required because it provides the client-facing iSCSI target endpoint. Nutanix data services, including Volumes, are accessed through these IP addresses rather than through management interfaces. The administrator uses the Data Services IP address and the Volume Group's iSCSI target information when configuring discovery and login from the external host. Nutanix recommends following the Volumes administration guidance for creating Volume Groups, enabling external client access, and attaching external iSCSI clients. See the Nutanix Documentation portal and the Nutanix Data Services overview for product documentation and architecture context.

QUESTION NO: 19

A customer has a 4-node cluster running at 80% capacity. One node fails due to a motherboard issue.

What is the effect?

A. The cluster continues to run but in a degraded state.

B. Zeus becomes available after 60 minutes.

C. Zeus becomes unavailable for 30 minutes.

D. The cluster continues to run normally.

ANSWER: A

Explanation:

The cluster continues to run but in a degraded state. Nutanix Distributed Storage Fabric is designed to tolerate a node failure by maintaining replicated data on other nodes and allowing the surviving CVMs and hosts to continue servicing workloads. A motherboard failure makes the affected node and its local storage unavailable, but it does not inherently stop the cluster when the remaining nodes can provide the required services and data replicas.

Because the cluster began at 80% capacity, losing one of four nodes substantially reduces the available storage and compute headroom. The cluster must operate without that node while preserving its configured resiliency requirements and may need to rebuild or re-protect data replicas on the surviving nodes when capacity permits. This condition is degraded: workloads can remain available, but fault tolerance, usable headroom, and the ability to sustain further failures are reduced until the failed node is repaired or replaced and the cluster returns to a fully healthy state.

Nutanix describes its distributed architecture and fault-tolerance approach in its data resiliency overview. For current product documentation and operational guidance, consult the Nutanix Documentation portal.

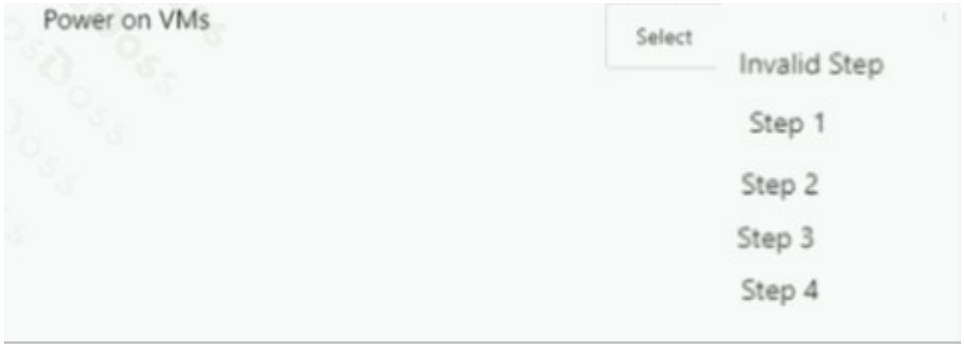
QUESTION NO: 20 - (HOTSPOT)

Async DR is configured between two sites. A network outage occurs at the primary site.

Which steps must the administrator perform to bring the VMs back into service at the backup site?

Item instructions: For each procedure, indicate the order in which that procedure must take place to meet the item requirements. Not all procedures are valid. Identify any invalid procedures using the drop-down option.

Procedure	Step
Log into Prism Element at the backup site	Select: Invalid Step, Step 1, Step 2, Step 3, Step 4
Reboot VMs	Select: Invalid Step, Step 1, Step 2, Step 3, Step 4
Go to the Async DR tab	Select: Invalid Step, Step 1, Step 2, Step 3, Step 4
Log into Prism Element at the primary Site	Select: Invalid Step, Step 1, Step 2, Step 3, Step 4
Select the Protection Domain and click Activate	Select: Invalid Step, Step 1, Step 2, Step 3, Step 4
Power on VMs	Select: Invalid Step



ANSWER:

Procedure
Step
Log into Prism Element at the backup site
Select
Invalid Step
Step 1
Step 2
Step 3
Step 4
Reboot VMs
Select
Invalid Step
Step 1
Step 2
Step 3
Step 4
Go to the Async DR tab
Select
Invalid Step
Step 1
Step 2
Step 3
Step 4
Log into Prism Element at the primary Site
Select
Invalid Step
Step 1
Step 2
Step 3
Step 4
Select the Protection Domain and click Activate
Select
Invalid Step
Step 1
Step 2
Step 3
Step 4
Power on VMs
Select
Invalid Step

Explanation:

When the primary site has suffered a network outage, the recovery workflow is performed from the backup cluster, because that is the cluster that holds the replicated protection-domain data and remains available to provide service. The administrator first accesses Prism Element on the backup site. From that Prism Element instance, the administrator opens the Async DR area, where the remote protection domain and its recovery state can be managed. The protection domain is then selected and activated. Activation is the key recovery operation: it makes the replicated data at the backup site available for use there and transitions the protection domain into the appropriate state for running the protected workloads from the recovery location.

After the protection domain has been activated successfully, the recovered virtual machines can be powered on at the backup site. This ordering is important because the VMs depend on their protected storage and replication recovery state being made available before they are started. The resulting sequence is therefore: log in to Prism Element at the backup site first; go to the Async DR tab second; select the protection domain and click Activate third; and power on the VMs fourth. This follows Nutanix asynchronous disaster-recovery recovery operations, in which the recovery-site protection domain is activated before workloads are brought online. Nutanix documentation for protection domains and asynchronous replication is available in the Prism Web Console Guide and the Nutanix data protection documentation.

QUESTION NO: 21

Which two methods should an administrator employ to set up the AHV host VLAN in a cluster to follow Nutanix recommendations? (Choose two)

A. Avoid adding guest VMs to the CVM and host VLAN.

B. Add all VMs to the default VLAN0 on bridge br1.

C. Add the CVM and the AHV host to the same VLAN.

D. Add all VMs to a new VLAN other than VLAN 0.

ANSWER: C D

Explanation:

Nutanix recommends placing the Controller VM and its associated AHV host on the same management VLAN. This arrangement ensures that the cluster's core management and storage communication uses a consistent, reachable network path between each hypervisor and its local Controller VM, while allowing the CVMs across the cluster to communicate correctly. The management VLAN can be VLAN 0 in environments using an untagged native network, or it can be a tagged VLAN when the physical-switch and host-network configuration supports it.

Nutanix also recommends separating guest virtual-machine traffic from the AHV/CVM management network. Therefore, guest VMs should be attached to a newly created VLAN other than VLAN 0. Using a dedicated guest VLAN provides network segmentation between tenant or application workloads and cluster management services, improves operational clarity, and enables network policies to be applied independently to workload traffic. In Prism, this is commonly implemented by creating the guest VLAN network and attaching VM NICs to that network while leaving AHV and CVM management interfaces on their shared management VLAN.

See the Nutanix AHV Administration Guide and Nutanix AHV documentation resources for AHV networking and VLAN configuration guidance.

QUESTION NO: 22

An administrator is working with Nutanix Support and needs to provide logs for troubleshooting an issue. The cluster is located in a secure environment. Data such as IP addresses and VM names cannot be shared.

Which method should be used to anonymize the log data sent to Nutanix Support?

A)

Under the **User Profile** in Prism, select **Anonymize Log Output**, then run **Log Collector** from the **Health** dashboard.

B)

Run the `ncc log_collector` tool on a CVM, setting the `--enhanced_log_collector` flag to `true`.

C)

Run the `ncc log_collector` tool on a CVM, setting the `--anonymize_output` flag to `true`.

D)

On the **Health** dashboard in Prism, use the **Log Collector** option under **Actions** and choose **Anonymize Logs**.

A. Option A

B. Option B

C. Option C

D. Option D

ANSWER: D

Explanation:

The appropriate method is to enable anonymization as part of the Nutanix log-collection/support-bundle workflow before the bundle is exported or uploaded to Nutanix Support. This feature is designed for environments in which infrastructure-identifying information must not leave the organization. It sanitizes sensitive identifiers in the collected diagnostic content, including items such as IP addresses, host names, and virtual-machine names, while retaining the operational events, timestamps, configuration relationships, and error information that Support needs to investigate the issue.

Using the built-in anonymization capability is important because it applies the expected sanitization consistently across the support bundle rather than relying on a manual edit of individual log files. The administrator should generate the anonymized bundle, review it if required by the organization's security process, and then provide that resulting bundle through the approved Support case or upload mechanism. Nutanix documentation for the applicable Prism version provides the exact navigation and controls for collecting and sharing diagnostic logs. See the Nutanix Documentation portal and the Nutanix Support portal for current product-specific procedures and support-case guidance.

QUESTION NO: 23

An administrator has a 5-node cluster configured for RF2 with 200 TB of raw disk space. The administrator decides to enable Erasure Coding to gain additional usable space.

Approximately how much usable space would be available after enabling Erasure Coding?

A. 100 TB

B. 125 TB

C. 150 TB

D. 175 TB

E. 160 TB

ANSWER: E

Explanation:

160 TB is the appropriate approximate usable-capacity figure. Nutanix Erasure Coding for an RF2 environment uses a 4+1 layout for eligible, cold data: four data fragments and one parity fragment. Thus, five units of physical capacity hold four units of user data, for a 1.25× capacity overhead. Applying that efficiency to 200 TB of raw capacity gives 200 ÷ 1.25 = 160 TB of usable capacity. This calculation assumes that the stated raw capacity is available for user data and that the data is eligible for erasure coding; real-world reported free capacity can be lower because of system-reserved space, metadata, replication requirements for data not eligible for EC, and operational headroom. A five-node cluster satisfies the node-count requirement for this 4+1 erasure-coding stripe layout. Nutanix describes Erasure Coding as a data-efficiency feature that protects data with parity while reducing the capacity overhead associated with RF2 replication. See the Nutanix documentation portal's Erasure Coding documentation and the Nutanix Bible Erasure Coding overview for the 4+1 protection model and capacity-efficiency context.

QUESTION NO: 24

An administrator manages a 4-block 16 node Nutanix cluster. One block experiences a Power Delivery Unit (PDU) failure. All nodes in that block power off. VMs on the affected nodes restart as expected. The cluster continues normal operation until power is restored.

Which Nutanix feature is responsible for maintaining operations in this scenario?

A. IO Redirection

B. Block Awareness

C. Async Disaster Recovery

D. Nutanix App Mobility Fabric

ANSWER: B

Explanation:

Block Awareness is the Nutanix data-placement capability that protects availability when an entire physical block becomes unavailable. A Nutanix block contains multiple nodes that can share physical infrastructure components, including power distribution. Therefore, a PDU failure can take every node in that block offline at the same time, which is a broader failure domain than the loss of a single node.

With Block Awareness, Nutanix Distributed Storage Fabric places data replicas across separate blocks whenever the cluster has sufficient block-level resources. This placement ensures that a block-level outage does not remove all copies of a VM's data. Surviving nodes in the remaining blocks retain access to the required replicated data and can continue serving storage operations. Nutanix high availability can then restart VMs that were running on the failed nodes elsewhere in the cluster, while the distributed storage layer remains available.

This behavior is particularly important in multi-block clusters because it combines VM recovery with resilience against shared-hardware failures at the block level, allowing the cluster to remain operational until the failed block is restored. Nutanix describes fault-tolerance concepts and replica placement in its Prism documentation and in the Nutanix Enterprise Cloud Platform Architecture Guide.

QUESTION NO: 25

How should an administrator make sure that the LCM Framework is always up to date and upgraded to the latest version?

A. From the Life Cycle Management page in Prism Element, click Perform Inventory, then edit settings and set LCM Auto Inventory to Daily

B. From the Life Cycle Management page in Prism Central, click Perform Inventory, then edit settings and click the Enable LCM Auto Inventory checkbox

C. From the Life Cycle Management page in Prism Element, click Perform Inventory, then edit settings and click the Enable LCM Auto Inventory checkbox

D. From the Life Cycle Management page in Prism Central, click Perform Inventory every morning

ANSWER: C

Explanation:

From the Life Cycle Management page in Prism Element, clicking Perform Inventory, editing settings, and selecting the Enable LCM Auto Inventory checkbox ensures that LCM automatically performs its inventory process on a scheduled basis. During inventory, LCM contacts Nutanix update services, refreshes its available-update metadata, and checks the LCM framework itself. This allows the framework to be updated when a newer compatible version is available, rather than relying on an administrator to remember to initiate inventory manually. Enabling automatic inventory is therefore the appropriate operational setting for keeping LCM current. The inventory is a prerequisite for LCM to identify the framework and component updates applicable to the cluster, so it should be enabled before relying on LCM for ongoing lifecycle operations. Nutanix documents LCM inventory and update workflows in the Life Cycle Management Guide. Additional Nutanix guidance on managing software and firmware updates through LCM is available in the Prism Web Console Guide.

QUESTION NO: 26

Which Nutanix product or feature would support the replacement of a storage appliance for shared home directories?

A. Storage container

B. Volumes

C. Files

D. Leap

ANSWER: C

Explanation:

Files is the Nutanix scale-out file-storage solution designed to provide centrally managed SMB and NFS file shares. Shared user home directories require file-level access, familiar network file-sharing protocols, identity integration, permissions, and quota management. Nutanix Files supplies these capabilities through file-server instances managed from Prism, allowing organizations to replace a traditional NAS or storage appliance that hosts users' home folders. For Windows-oriented home directories, Files can provide SMB shares integrated with Active Directory, so access control can use existing users, groups, and NTFS-style permissions. It also supports distributed scale-out capacity and performance, data protection features, and operational management within the Nutanix platform. This makes it appropriate for shared directories that must be accessed concurrently by end users and applications as standard network file shares. Nutanix describes Files as a software-defined, scale-out file-storage service supporting SMB and NFS protocols, with enterprise file-service functionality for use cases including home directories and user profiles. See the Nutanix Files product page and the Nutanix Files documentation overview.

QUESTION NO: 27

The feature that enables you to back up and restore copies of virtual machines and files to and from an on-prem cluster and a Nutanix Controller VM on the Amazon Web Service (AWS) or Microsoft Azure cloud.

A. XI-Leap

B. Cloud Connect

C. Acropolis Block Service

ANSWER: B

Explanation:

Cloud Connect is the Nutanix feature designed to extend data protection between an on-premises Nutanix cluster and a Nutanix Controller VM deployed in a public cloud. It enables administrators to protect VM data by replicating backup copies to a cloud-based cluster and to restore protected VMs and files either back to the on-premises environment or from the cloud location when needed. The cloud-side Controller VM provides the Nutanix storage and data-services endpoint required for this capability in supported AWS or Microsoft Azure deployments. This approach supports an off-site copy of protected data while retaining Nutanix-native backup, replication, and recovery workflows. In the terminology used in the NCP-MCI 5.15 curriculum, Cloud Connect specifically identifies the capability for backing up and restoring copies between an on-premises cluster and Nutanix infrastructure in AWS or Azure. Nutanix documents Cloud Connect as a data-protection capability for extending an on-premises environment to public cloud resources. See the Nutanix Prism Web Console Guide: Cloud Connect and the Nutanix Cloud Connect overview.

QUESTION NO: 28

An administrator is creating a network security policy using Nutanix Flow.

Which two items can be used to identify groups of VMs in the policy? (Choose two.)

A. Categories

B. VM names

C. Storage containers

D. Protection Domains

ANSWER: A B

Explanation:

Categories and **VM names** are correct. Nutanix Flow policies can identify workloads by using categories, which provide scalable grouping based on business or technical metadata. A policy can also target individual VMs when a more specific workload definition is required.

Categories are generally preferred for policy design because a category-based policy automatically applies to current and future VMs that receive the matching category. A storage container and a Protection Domain are storage and data-protection constructs, not workload selectors for Flow security rules. See the Nutanix Flow documentation for network security policy configuration details.

QUESTION NO: 29

Which two methods are valid for migrating a VM from a Nutanix vSphere cluster to AHV? (Choose two.)

A. Storage vMotion

B. Live Migration

C. Nutanix Move

D. Cross-Hypervisor DR

ANSWER: C D

Explanation:

Nutanix Move is a supported migration tool for moving virtual machines from VMware vSphere to Nutanix AHV. Move connects to the source vCenter environment and the target Nutanix cluster, performs an initial replication of the VM data, and can synchronize changes before the migration cutover. This minimizes downtime while converting and registering the workload for operation on AHV. The process is managed through the Move appliance and includes source and target validation, migration planning, replication, cutover, and post-migration verification.

Cross-Hypervisor DR is also valid when the VM is protected through Nutanix Disaster Recovery capabilities. Nutanix supports protection-domain-based replication and recovery between supported VMware ESXi and AHV environments. A planned migration or recovery operation can therefore fail over protected workloads from the vSphere-based source cluster to an AHV recovery cluster. This method is especially appropriate where the environment already uses replication-based protection and needs an orchestrated cross-hypervisor recovery or migration workflow. Nutanix documents supported migration workflows and prerequisites in the Nutanix Move User Guide and cross-hypervisor protection behavior in the Protection Domain Guide.