DUMPSBOSS.

Nutanix Certified Services Core Infrastructure Professional

Nutanix NCS-Core

Version Demo

Total Demo Questions: 44

Total Premium Questions: 445

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Plan and Design a Nutanix Solution	83
Topic 2, Deploy a Nutanix Solution	93
Topic 3, Configure a Nutanix Solution	124
Topic 4, Troubleshoot a Nutanix Solution	143
Topic 5, Mix Questions	2
Total	445

QUESTION NO: 1

A consultant is preparing for a cluster deployment and evaluates portable Foundation.

Laptop configuration is as follows:

•CPU: 2.8 GHz Quad-Core Intel Core i7

•Memory: 4GB RAM

During the installation, the consultant encounters some errors and tries to troubleshoot.

What could prevent successful installation and Foundation usage?

A. Gatekeeper must be enabled

B. Oracle VirtualBox is installed on the laptop

C. Laptop configuration does not meet installation requirements

D. Firewall Stealth Mode is disabled

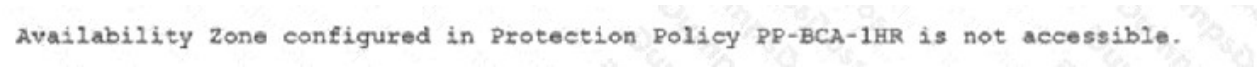
ANSWER: C

Explanation:

Laptop configuration does not meet installation requirements is correct because portable Foundation is delivered as a virtual appliance and therefore depends on the host computer having sufficient CPU, memory, disk capacity, and supported virtualization resources. Although the listed quad-core Intel processor is appropriate, 4 GB of physical RAM is insufficient for reliably running the portable Foundation virtual machine and its required services alongside the host operating system. Insufficient host memory can prevent the appliance from starting correctly, cause installation or service failures, or make discovery and imaging operations unstable. Before deployment, the consultant should validate the current portable Foundation requirements for the selected Foundation release, including the supported host operating system, hypervisor version, available RAM, available disk space, and networking configuration. Nutanix Foundation documentation describes Foundation's role in imaging nodes and creating clusters, while the Nutanix Support Portal provides the release-specific Foundation guides and deployment prerequisites that should be used for the final compatibility check. See Nutanix Foundation Guide and Nutanix Support Portal.

QUESTION NO: 2

The following critical Availability Alert displays in prism Central:



The protection Policy PP-BCA-1HR includes a business critical application with a 1-hour snapshot frequency.

What is causing this issue?

A. There is a scheduled outage for the Availability Zone referenced in Protection Policy PP-BCA-1HR.

B. Workloads included in PP-BCA-1HR are no longer within their intended RPO.

C. Prism Central in the Availability Zone for PP-BCA-1HR is unavailable.

D. NearSync replication between the Availability Zones has fallen out of scope.

ANSWER: B

Explanation:

Workloads included in PP-BCA-1HR are no longer within their intended RPO. A protection policy with a one-hour snapshot schedule is designed to maintain a recovery point objective of approximately one hour for the protected application. Prism

Central tracks whether the protection activity is occurring frequently enough for the policy's configured RPO and availability requirements. When scheduled snapshots or replication operations do not complete in time, the age of the most recent recoverable point can exceed the allowed recovery interval. For a business-critical application, this represents an availability risk because recovery could require accepting more data loss than the policy permits. Prism Central therefore raises a critical Availability Alert to show that the protected workloads are outside the expected protection objective and require investigation and remediation. The alert identifies a protection-state condition rather than merely reporting the configured snapshot frequency; the one-hour schedule supplies the threshold against which the current recoverable point is evaluated. Restoring successful, timely protection operations returns the workload to its intended RPO posture. Nutanix data-protection and disaster-recovery capabilities are documented through the Nutanix Documentation portal and the Nutanix Disaster Recovery overview.

QUESTION NO: 3

A consultant is unable to install virtualization software on a laptop.

Which two versions of Foundation can be used to resolve this issue? (Choose two.)

A. Foundation VM

B. Foundation Portable

C. Foundation Central

D. Foundation Applet

ANSWER: B D

Explanation:

Foundation Portable and **Foundation Applet** are the appropriate Foundation deployment methods when the consultant cannot install a local virtualization platform on the laptop. Foundation Portable is designed for situations where a separate, portable Foundation environment can be used rather than requiring the consultant's laptop to host the Foundation virtual machine. This makes it useful for field deployments where workstation permissions, corporate security controls, or hardware limitations prevent installation of a hypervisor.

Foundation Applet is also intended to allow Foundation operations without the laptop itself needing to run Foundation as a locally hosted virtual machine. It provides an alternate workflow for accessing the Foundation service during node imaging and cluster deployment, avoiding the requirement to install virtualization software on the consultant endpoint.

These methods support the core Foundation purpose: imaging Nutanix nodes with the required hypervisor and Nutanix software, then creating the cluster. Nutanix documents Foundation as its deployment utility and provides Foundation resources through the Nutanix Support Portal. See the Nutanix Foundation Guide and Nutanix Product Support.

QUESTION NO: 4

After an onsite cluster deployment, a consultant prepares the deliverables for a project closeout.

Which two data in the As-Built Guide require adjustment or might be missing completely? (Choose two.)

A. Nutanix Node Port Layout

B. AHV Host information

C. Physical Rack Layout

D. Cluster information

ANSWER: A C

Explanation:

Nutanix Node Port Layout and **Physical Rack Layout** are the deliverable sections most likely to need onsite validation and updates before project closeout. The node port layout must reflect the actual physical cabling, port selections, interface usage, and connectivity implemented during installation. Although a planned design may exist before arrival, real-world rack and network conditions can require changes during deployment. Capturing the final state is essential so that the customer's operations team can troubleshoot, expand, or replace hardware without relying on assumptions from the original design.

The physical rack layout likewise needs confirmation against the completed installation. It documents the actual rack position of nodes and related equipment, allowing personnel to identify hardware quickly and to understand the installed physical arrangement. This information may be incomplete before onsite work because final placement can depend on available rack units, power distribution, cable lengths, and customer-directed changes. Reviewing and correcting these two visual physical-infrastructure records ensures the As-Built Guide represents the deployed environment rather than only the intended design. Nutanix documentation resources are available through the Nutanix Support Portal documentation page; broader implementation and lifecycle best-practice resources are available from Nutanix Support and Services.

QUESTION NO: 5

A VDI environment based on AHV Cluster is not performing well. The current environment isusing only one bridge (Bridge0). The administrator needs to verify if nodes are using all network cards associated to Bridge0.

Which two menus should be used to check the current configuration? (Choose two.)

A. Network Configuration item in Settings menu

B. Host view in Network menu

C. Host NICs tab in Hardware menu

D. I/O Metrics tab in VM menu

ANSWER: B C

Explanation:

Host view in Network menu and **Host NICs tab in Hardware menu** provide the complementary host-level information needed to validate Bridge0 NIC use in an AHV cluster. The Network host view lets an administrator select individual hosts and inspect the network configuration presented for each node, including the bridge and its uplink relationships. This is useful for confirming that the expected physical NICs are associated with Bridge0 consistently across the VDI cluster.

The Hardware host-NIC view exposes the physical network adapters on each host and their operational state. Reviewing this view alongside the bridge configuration verifies that all intended adapters are present, connected, and available as uplinks rather than relying on a single active physical path. This is particularly important for VDI, where a large number of concurrent desktop sessions can make an unintended single-NIC uplink a network-performance bottleneck. Nutanix documents AHV networking and host NIC/bridge configuration in the Prism web-console documentation and AHV administration materials: Nutanix Prism Web Console Guide: Network Configuration and Nutanix AHV Administration Guide: Networking.

QUESTION NO: 6

Based on customer requirements, a consultant conducted an AHV cluster deployment. Each node is configured with four NICs.

Which two components should the consultant manually update in the As-Built Guide? (Choose two.)

A. Node Port Layout Diagram

B. Network Cabling Diagram

C. Logical Design Diagram

D. Site installation Diagram

ANSWER: A B

Explanation:

Node Port Layout Diagram and **Network Cabling Diagram** should be manually updated because they record the physical network implementation actually delivered at the customer site. A four-NIC configuration requires the As-Built Guide to show each host interface, its port assignment, intended traffic role, and the corresponding physical-switch connectivity. The Node Port Layout Diagram captures the node-level view: which NIC ports are present and how the deployed interface layout maps to the host. The Network Cabling Diagram captures the end-to-end physical view, including the connections from each node NIC to switch ports. Together, these diagrams provide an accurate operational record for support, troubleshooting, maintenance, and future expansion. They also ensure that the completed deployment documentation reflects customer-specific cabling and port choices rather than an initial design assumption or generic template. Nutanix deployment and support resources emphasize retaining accurate environment and configuration details for lifecycle operations; see the Nutanix Documentation Portal and Nutanix Product Support.

QUESTION NO: 7

After imaging the nodes and creating the cluster successfully, the consultant connects the cluster to the customer network. When logging into Prism, the events dashboard is full of errors.

What is causing the issue?

A. The cluster was not stopped prior to connecting to the customer network.

B. The Cluster Virtual IP Address (VIP) was not set up during the process.

C. Foundation did not create the cluster successfully.

D. The consultant did not run Nutanix Cluster Check (NCC..

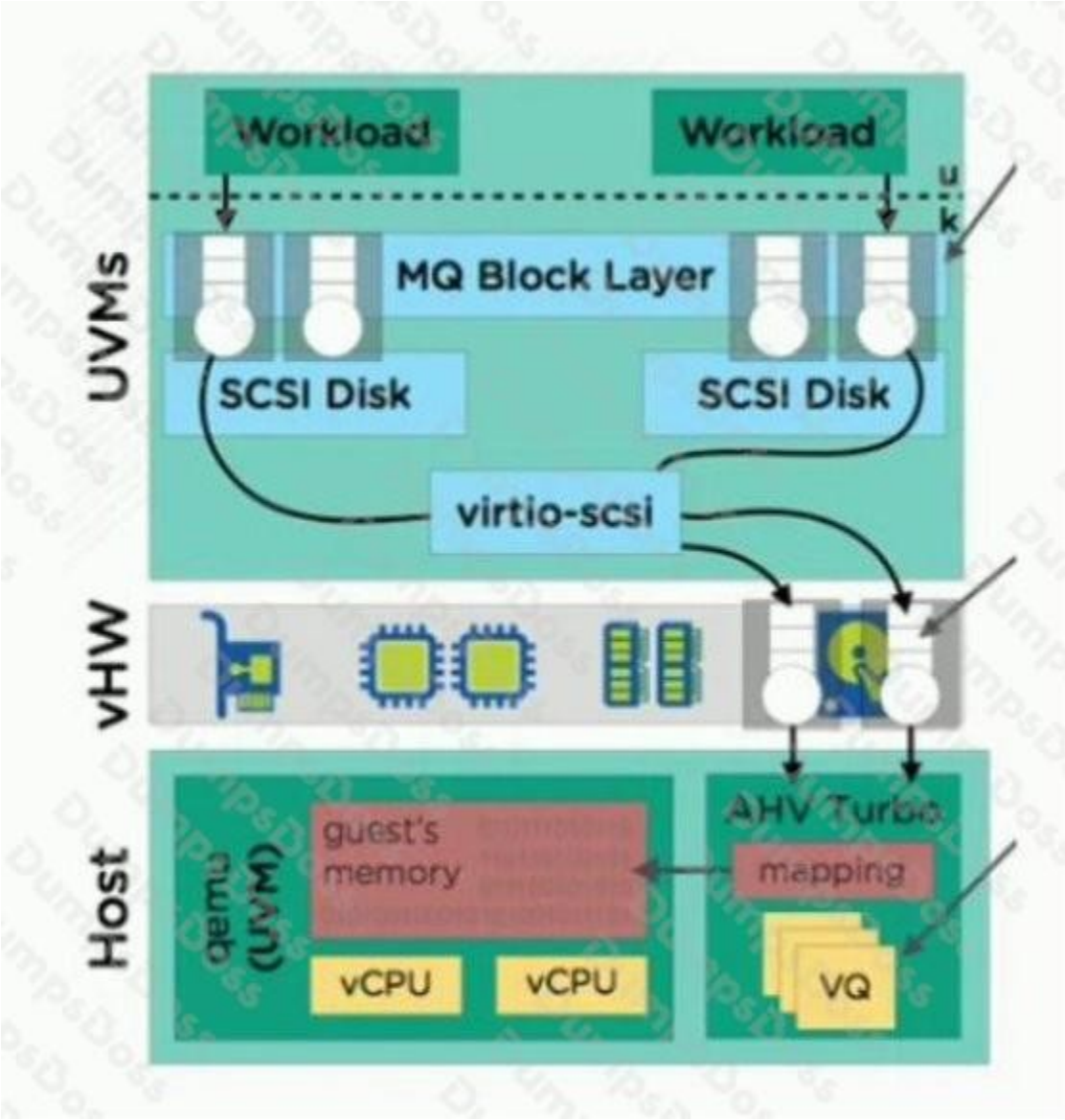
ANSWER: A

Explanation:

The cluster was not stopped prior to connecting to the customer network. A newly imaged and configured Nutanix cluster is commonly staged on an isolated deployment network before it is attached to the customer's production network. The cluster should be shut down before that connection or cutover activity so that CVMs and cluster services do not remain active while network reachability, VLAN placement, routing, and external-service access are changing. If the live cluster is connected directly to the customer network, its running services can immediately attempt communication with configured infrastructure and peers while the network transition is incomplete. Those failed or changing communications are recorded by Prism as event and alert entries, producing the large number of errors described. Stopping the cluster before attaching it to the customer network provides a controlled transition: the physical connectivity and required network configuration can be finalized first, then the cluster can be started and its services can establish communication in the intended environment. Nutanix deployment guidance treats post-foundation configuration and network integration as controlled implementation steps, while Nutanix operational documentation describes Prism as the interface for monitoring cluster health and events. See the Nutanix Foundation Guide and the Prism Web Console Guide.

QUESTION NO: 8

Refer to the exhibit.



An administrator has an existing cluster and needs to improve performance using AHV

Turbo. Which two items are required to achieve even greater performance? (Choose two.)

A. Workloads are multi-threaded.

B. VMs have one vCPU configured.

C. VMs have multi-queue disabled.

D. VMs have more than one vCPU.

ANSWER: A D

Explanation:

“Workloads are multi-threaded.” and “VMs have more than one vCPU.” are required because Turbo improves processor performance by enabling more effective concurrent execution for eligible virtual-machine workloads. A multi-threaded application can distribute its work across several execution threads instead of limiting activity to a single processing path. Assigning more than one virtual CPU to the virtual machine provides the processing resources needed for those threads to run in parallel. Together, these conditions allow the application to take advantage of the additional CPU concurrency that Turbo is designed to provide, improving throughput and reducing the likelihood that a single virtual CPU becomes the limiting resource.

CPU configuration should remain aligned with the workload’s actual level of parallelism. After enabling the feature, an administrator should validate the result with application-level performance measurements and virtual-machine CPU

utilization, rather than relying only on host-level metrics. Nutanix maintains its product documentation, including virtualization administration guidance, in the Nutanix Support Portal documentation library. Additional platform and virtualization information is available on the Nutanix AHV product page.

QUESTION NO: 9

For several days, an administrator notices the following alerts:

• CVM NIC Speed Low Warning Alerts

• Warning Alerts of CVM NIC not performing at optimal speed

• CVM is disconnected from the network Critical Alert

• Network Visualization page shows excessive dropped packets on CVM/Host

Which steps should be taken to determine which problem should be addressed first?

A. • Access the Hardware Page to verifyresources are available
• Analyze ail CVM Speed Alerts in the Alerts/Events page
• Analyze output for the network and interface properties and connectivity issues

B. • Verify Host/CVM connectivity on the Network Visualization page
• Use toverify the bridge and bond configuration
• Review alerts/events page for the CVM disconnected error

C. • Review Alerts page for NIC speed alerts and alert timing
• Analyze the genesis.out log file for process failures
• Assess the NIC properties inthe Network Visualization > Host Properties page

D. • Restart networking services on the CVM
• Determine the current configuration of the affected CVM via output
• Access the Alerts/Events page for the CVM network connection failures

ANSWER: B

Explanation:

"• Verify Host/CVM connectivity on the Network Visualization page
• Use toverify the bridge and bond configuration
• Review alerts/events page for the CVM disconnected error
" is correct because it starts by validating the active communication path and gives priority to the critical CVM network-disconnection condition. Network Visualization provides a topology-oriented view of host, CVM, and uplink connectivity, helping the administrator determine whether the observed packet drops are localized to a CVM interface, the host virtual-switch path, or physical uplinks. This establishes the current impact before focusing on lower-severity NIC-speed warnings.

Next, checking the Open vSwitch bridge and bond configuration confirms that the CVM-facing interfaces and physical uplinks are associated correctly and that the intended uplink/bond design is in effect. This is essential context when packet loss and degraded link-speed symptoms coexist. Finally, reviewing the alert and event history for the disconnection identifies timing, recurrence, and related events, allowing the administrator to correlate the critical loss of connectivity with the topology and configuration findings. This sequence supports a safe, evidence-based prioritization of the underlying network issue before making changes. Nutanix AHV networking concepts and operational documentation are available through the Nutanix Documentation portal and the Nutanix Support Portal.

QUESTION NO: 10

When utilizing the Nutanix cluster As Built Document generator, which two configuration elements should a consultant provide when running the run_as_built.exe command? (Choose two.)

A. Data Services IP

B. Cluster IP

C. Remote Site IP

D. Customer Name

ANSWER: B D

Explanation:

The required inputs are **Cluster IP** and **Customer Name**. The Cluster IP identifies the target Nutanix cluster that the As Built Document generator connects to in order to collect the inventory, configuration, and operational details used to populate the document. It should be the cluster's management-facing address that is reachable from the system running the utility, so the generator can authenticate to the cluster and retrieve the required information through the Nutanix management interfaces.

Customer Name is supplied as document metadata. The generator uses it to identify the customer environment in the produced As Built output, supporting clear ownership, handoff, service records, and later operational reference. In practice, providing both values associates the generated documentation with the intended customer while ensuring that its technical content is gathered from the correct cluster. This aligns with Nutanix's emphasis on managing cluster configuration through Prism and retaining accurate deployment information for lifecycle and support operations. See the Nutanix Support Portal documentation library and Nutanix Product Support resources for Nutanix documentation and support guidance.

QUESTION NO: 11

How should a consultant verify that a Nutanix cluster can tolerate a single-node failure?

A. [root@cvm~]# ncli cluster get-domain-fault-tolerance-statustype=node

B. nutanix@cvm~$ ncli cluster get-domain-fault-tolerance-statustype=node

C. [root@avh~]# ncli cluster fault-tolerance-status type=node

D. nutanix@cvm~$ ncli cluster status type=node

ANSWER: B

Explanation:

The correct command is `nutanix@cvm~$ ncli cluster get-domain-fault-tolerance-status type=node`. It is run from a Controller VM using the standard Nutanix CVM account and requests the cluster's domain fault-tolerance assessment for the node failure domain. The `type=node` parameter is important because it specifically evaluates whether the current data-placement and replication configuration can sustain the loss of one entire physical node while preserving the required data availability and resiliency policy. Consultants should perform this validation as part of a health, readiness, or post-change assessment, particularly before maintenance that could take a node offline. The returned status helps confirm that the cluster has sufficient fault-tolerance capacity at that moment; it should be checked again if there are node failures, replication-factor changes, storage-resiliency alerts, or significant capacity changes. Nutanix documents `ncli` as the cluster-management CLI run from a CVM, and its command reference includes cluster fault-tolerance status operations. See the Nutanix AOS Command Reference: ncli and the Nutanix AOS Cluster Health documentation.

QUESTION NO: 12

A consultant is preparing to foundation over a customer network that has the following criteria:

* VLAN segmented network

* VLAN tags on the nodes must be imaged prior to starting the foundation process.

For each node, the consultant has done the following:

* Connected to the Network Crash Cart of the Node

* Logged in using “root” credentials

What should the consultant do next?

A. 1. CD to /root/nutanix-network-crashcart/
2. Start Network Utility tool by running: ./network_configuration
3. Change Values

B. 1. CD to /home/data/nutanix/nutanix-network-crashcart/
2. Start Network Utility tool by running: ./network_configuration
3. Change Values

C. 1. Log into CVM using nutanix@192.168.5.254
2. CD to /root/Nutanix-network-crashcart/
3. Start Network Utility tool by running: ./network_configuration
4. Change Values

D. 1. Log into CVM using nutanix@192.168.5.254
2. CD to /home/data/nutanix/nutanix-network-crashcart/
3. Start Network Utility tool by running: ./network_configuration
4. Change Values

ANSWER: A

Explanation:

After connecting to the node’s Network Crash Cart and authenticating as `root`, the consultant should change to `/root/nutanix-network-crashcart/` and run `./network_configuration`. This is the node-local Network Crash Cart utility used before imaging when the environment requires VLAN-tagged connectivity. The utility provides the supported workflow for entering or modifying the network settings required for the node to communicate correctly on the designated tagged network.

Configuring this information before Foundation begins is important because Foundation relies on reachable node and management-network connectivity throughout imaging and initial cluster deployment. In a VLAN-segmented design, the appropriate VLAN values must be applied at the node level so that the required deployment traffic is sent and received on the intended network. The Network Crash Cart is specifically intended for this pre-deployment, per-node configuration task, and it is accessed locally using the root account already established in the scenario. See Nutanix guidance and Foundation resources at Nutanix Support Portal and Nutanix Foundation.

QUESTION NO: 13

An administrator receives an error indicating that the CVMs in the cluster are not syncing to any NTP servers. An investigation of the issue finds:

• The NTP servers are configured in Prism

• The time on all CVMs is the same

• Both the CVMs and AHV hosts are configured for the UTC time zone

Which two steps can be taken to troubleshoot this issue? (Choose two.)

A. Confirm that the NTP servers are reachable from the CVMs.

B. Restart genesis on all CVMs.

C. On a CVM, run the command `ntpq -pn`.

D. Restart the chronosservice on all CVMs.

ANSWER: A C

Explanation:

Confirming that the NTP servers are reachable from the CVMs is an essential first troubleshooting step because NTP synchronization requires network connectivity between each CVM and its configured time sources. The administrator should validate that the CVM can resolve the NTP server name when a hostname is configured, route traffic to the server, and communicate over NTP's UDP port 123. Configuration in Prism alone does not prove that the CVMs can actually contact the selected servers.

Running `ntpq -pn` on a CVM provides the local NTP peer status needed to diagnose synchronization. Its output identifies configured peers by address, shows reachability information, offset, delay, and jitter, and indicates the currently selected synchronization source with an asterisk. This lets the administrator determine whether the CVM is receiving replies from an NTP peer and whether a peer has been selected as the system time source. Because all CVMs already show the same time and use UTC, connectivity and peer-state verification are the most direct next actions. Nutanix documents use of `ntpq` for reviewing NTP peer status in its NTP troubleshooting knowledge base article. General NTP peer-status command behavior is also documented in the ntpq documentation.

QUESTION NO: 14

An administrator needs to make sure an RF2 cluster can survive a complete rack failure without negatively effecting workload performance. The current cluster configuration consists of the following:

• 30 nodes: distributed 10 nodes per rack across three 42U rack

• Each nodes is configured with 40TB usable storage all flash (Cluster Total 1.2 PB Usable)

• Current cluster utilization is 900TB storage

Which configuration changes should be made to make sure that the cluster meets the requirements?

A. Expand the cluster by adding 3 additional nodes per rack, 9 nodes total.

B. Expand the cluster by adding 2 additional nodes per rack, 6 nodes total.

C. Expand the cluster by adding 9 nodes to a new 42U rack

D. Expand the cluster by adding 8 nodes to a new 42U rack

ANSWER: A

Explanation:

Expand the cluster by adding 3 additional nodes per rack, 9 nodes total. is the appropriate configuration change. The existing cluster has 1.2 PB of usable capacity distributed evenly across three racks, so each rack contributes 400 TB. A full rack failure removes 400 TB of usable capacity and leaves only 800 TB across the surviving racks, which is less than the current 900 TB consumption. The cluster therefore needs additional capacity distributed across all rack fault domains rather than concentrated in one location.

Adding three 40 TB nodes to each rack adds 360 TB to the cluster, resulting in 1.56 PB total usable capacity. If any one rack subsequently fails, the two remaining racks retain approximately 1.04 PB of usable capacity. This accommodates the existing 900 TB of data while retaining operational headroom for data rebuild activity, normal cluster services, and workload operation. Even distribution also preserves balanced compute and storage resources across the surviving racks, which supports the requirement to avoid a performance impact following the rack outage.

Rack-awareness configuration must also be enabled and correctly mapped to the physical rack fault domains so RF2 replicas are placed across racks. Nutanix describes rack fault tolerance and fault-domain behavior in its Prism Central Web Console Guide and AHV Administration Guide.

QUESTION NO: 15

A consultant is reimaging a Nutanix cluster with a supported ISO, but Foundation returns an error that the media is not a supported ISO.

Which two actions should the consultant take to resolve this issue? (Choose two.)

A. Restart the imaging process in Foundation.

B. Obtain the MD5 checksum of the ISO and confirm that the checksum is listed.

C. Edit the whitelist file in Foundation.

D. Download and replace the iso_whitelist.json file with the latest version from the Support Portal.

ANSWER: B D

Explanation:

Foundation validates an ISO against its supported-ISO whitelist before allowing the imaging workflow to use it. Therefore, obtaining the ISO's MD5 checksum and confirming that the checksum is listed is required to establish that the downloaded media exactly matches a Nutanix-approved ISO entry. The checksum is the value Foundation uses to identify the specific supported ISO file; merely having an ISO with a familiar filename or version is insufficient if its checksum does not match the whitelist entry.

Downloading and replacing the local `iso_whitelist.json` with the latest version from the Nutanix Support Portal is also appropriate because the whitelist packaged with the current Foundation installation may not contain a newer supported ISO. Updating the file supplies Foundation with the current supported-image checksum definitions, allowing it to recognize the validated ISO during reimaging. The replacement file should be obtained from Nutanix's official support resources so that its contents are trusted and aligned with the applicable Foundation release. Nutanix documentation and support downloads are available through the Nutanix Support Portal; broader Foundation product documentation is available at Nutanix Documentation.

QUESTION NO: 16

An administrator needs to configure asynchronous replication for selected VMs from a primary Nutanix cluster to a remote Nutanix cluster.

Which two configuration tasks are required? (Choose two.)

A. Configure the remote site relationship between the clusters.

B. Create a protection policy or protection domain with a replication schedule.

C. Configure a shared VLAN for all guest VM networks at both sites.

D. Configure the same Cluster Virtual IP address at both sites.

ANSWER: A B

Explanation:

Configure the remote site relationship between the clusters is required so that the primary cluster can authenticate and communicate with the recovery cluster. The remote-site configuration establishes the destination that can receive replicated recovery points.

Create a protection policy or protection domain with a replication schedule is also required. The policy identifies the workloads to protect and defines the schedule used to create and replicate recovery points to the configured remote site. Together, the remote-site relationship and replication schedule provide the basis for asynchronous disaster-recovery protection. Nutanix documents replication and recovery configuration in the Nutanix Data Protection replication documentation.

QUESTION NO: 17

A systems administrator needs to add more VMs to their Nutanix cluster.

Which two actions should the administrator perform to determine if the current cluster can accommodate the new VMs? (Choose two.)

A. Perform an Inventory with Life Cycle Management.

B. Determine utilization with Cluster Runway.

C. Enable Deduplication and Erasure Coding.

D. Utilize Optimize Resources for VM efficiency.

ANSWER: B D

Explanation:

Determining utilization with Cluster Runway and utilizing Optimize Resources for VM efficiency provide the capacity and rightsizing information needed before placing additional virtual machines on a cluster. Cluster Runway uses historical resource-consumption trends to forecast when cluster resources, including CPU, memory, and storage, may become constrained. This allows the administrator to evaluate available headroom and make an informed decision about whether the expected workload can be supported for the required planning period. Optimize Resources complements that forecast by identifying virtual machines whose allocated CPU or memory does not align with actual utilization. Reviewing these recommendations can expose recoverable capacity through rightsizing, helping the administrator establish the cluster's effective capacity before adding workloads. Together, the forecast and optimization findings support capacity planning based on measured demand rather than configured allocations alone. Nutanix describes capacity-planning and operational analytics capabilities within Prism Central in its Prism overview. Additional information about Nutanix capacity planning and infrastructure management is available in the Nutanix documentation portal.

QUESTION NO: 18

A customer is deploying Nutanix AHV clusters over hundreds of remote sites worldwide. Prism Central will be used to centrally manage all clusters. Customer security policy requires the use of MS Active Directory (AD).groups to authenticate all network devices.

Which method should be consultant use to meet the requirements?

A. Integrate AD authentication on all CVMs.

B. Integrate AD authentication on Prism Central Only.

C. Proxy Prism Element traffic through Prism Central.

D. Integrate AD authentication on all Prism Element Clusters.

ANSWER: B

Explanation:

Integrate AD authentication on Prism Central Only. Prism Central is the centralized management plane for the distributed AHV environment described. It can be configured with an Active Directory directory service and role mappings that associate AD users and groups with Nutanix roles. Administrators then authenticate to Prism Central with their corporate AD identities, while authorization is consistently governed through the assigned group-to-role mappings. This avoids having to duplicate directory configuration and role assignments across hundreds of independently deployed remote-site clusters, which is operationally difficult and prone to configuration drift.

Once the remote Prism Element clusters are registered with Prism Central, authorized administrators can use the Prism Central interface to monitor and manage those clusters centrally. This approach aligns with the requirement to use AD groups and with the stated management model, because authentication and access control for the central management interface are administered in one place. Nutanix documents directory-service integration and role mapping as Prism Central identity-management capabilities. See the Prism Central authentication documentation and Nutanix's product documentation portal for the release-specific Prism Central guide.

QUESTION NO: 19

A consultant is performing a Nutanix Cluster installation on Dell XC Core hardware. The consultant decides to use Foundation Portable for Mac to perform the installation. When the consultant arrives onsite, Foundation Portable is unable to locate the new nodes.

Which log should the consultant check to troubleshoot this issue?

A. /home/nutanix/foundation/log

B. ~/data/logs/foundation.out

C. foundation.app/contents/resouces/log

D. ~/data/logs/foundation

ANSWER: C

Explanation:

The appropriate log location is **foundation.app/contents/resouces/log**. Foundation Portable for Mac runs as a macOS application rather than as the Linux-based Foundation VM. Consequently, troubleshooting information produced by the portable application—including service startup, network-interface activity, discovery attempts, and node-detection failures—is kept with the Foundation application resources. Reviewing this log helps the consultant establish whether Foundation is using the intended local network interface and whether discovery traffic is reaching the Dell XC Core nodes. This is particularly important onsite, where incorrect VLAN connectivity, a missing link-local route, macOS firewall behavior, or an incorrect physical adapter can prevent newly imaged nodes from appearing in the Foundation interface. The log can also provide timestamps and discovery-service messages that are useful when escalating an issue to Nutanix Support. Nutanix Foundation documentation describes Foundation as the deployment tool used to discover and image Nutanix nodes, while Nutanix Support resources provide the procedures for gathering the relevant diagnostic information during deployment troubleshooting. See the Nutanix Foundation documentation and the Nutanix Support Knowledge Base.

QUESTION NO: 20

An administrator is deploying a three-tier application on a Nutanix Enterprise Cloud consisting of web, application, and database VMs. Traffic between the servers must be limited to specific services/ports. There is an application layer firewall VM deployed on one host in the cluster.

In which way should the administrator meet this requirement?

A. Create a network for each type of VM, and use policy-based routing to control the traffic flow

B. Configure a security policy and service chain redirecting the server traffic through the firewall

C. Separate the web. application and database VMs on to dedicated VLANs

D. Categorize the VMs in Prism Central and utilize Flow to set a security policy

ANSWER: D

Explanation:

Categorize the VMs in Prism Central and utilize Flow to set a security policy is the appropriate approach because Nutanix Flow Network Security provides distributed microsegmentation for workload-to-workload communication. The administrator can assign categories that identify the web, application, and database tiers, then use those categories as policy endpoints in Prism Central. Security rules can explicitly permit only the required services and ports between tiers, such as allowing web traffic to the application tier and database traffic only from the application tier. Enforcement occurs at the VM virtual-network-interface level across the cluster, so protection follows the workloads and does not depend on their placement on a particular host. This model supports a least-privilege design: traffic not explicitly permitted by the applicable policy can be blocked, limiting lateral movement while retaining the required application flows. Categories also make the policy operationally scalable, because newly deployed VMs inherit the appropriate controls when assigned to the relevant application-tier

category. Nutanix describes Flow Network Security as its microsegmentation capability for controlling east-west VM traffic through centrally managed policy. See Nutanix Flow Network Security and the Flow Network Security Administration Guide.

QUESTION NO: 21

An administrator needs to protect a Microsoft SQL Server VM with application-consistent Nutanix snapshots.

Which two actions should the administrator take? (Choose two.)

A. Install Nutanix Guest Tools on the SQL Server VM.

B. Enable application-consistent snapshots in the protection policy.

C. Attach the SQL Server database disks through a Volume Group.

D. Disable the Windows Volume Shadow Copy Service.

ANSWER: A B

Explanation:

Install Nutanix Guest Tools on the SQL Server VM because Nutanix Guest Tools provides the guest integration required for application-consistent snapshot operations. For supported Windows workloads, NGT coordinates with guest services to quiesce the application before the snapshot is created.

Enable application-consistent snapshots in the protection policy so that the configured protection operation requests guest quiescing rather than taking only a crash-consistent snapshot. The SQL Server VM must also meet the applicable guest operating system, VSS, and NGT requirements for application-consistent protection to complete successfully. Nutanix documents guest tools and VM data-protection configuration in the Nutanix Documentation portal.

QUESTION NO: 22 - (HOTSPOT)

HOTSPOT

An administrator is configuring an All Flash cluster to support the following workloads:

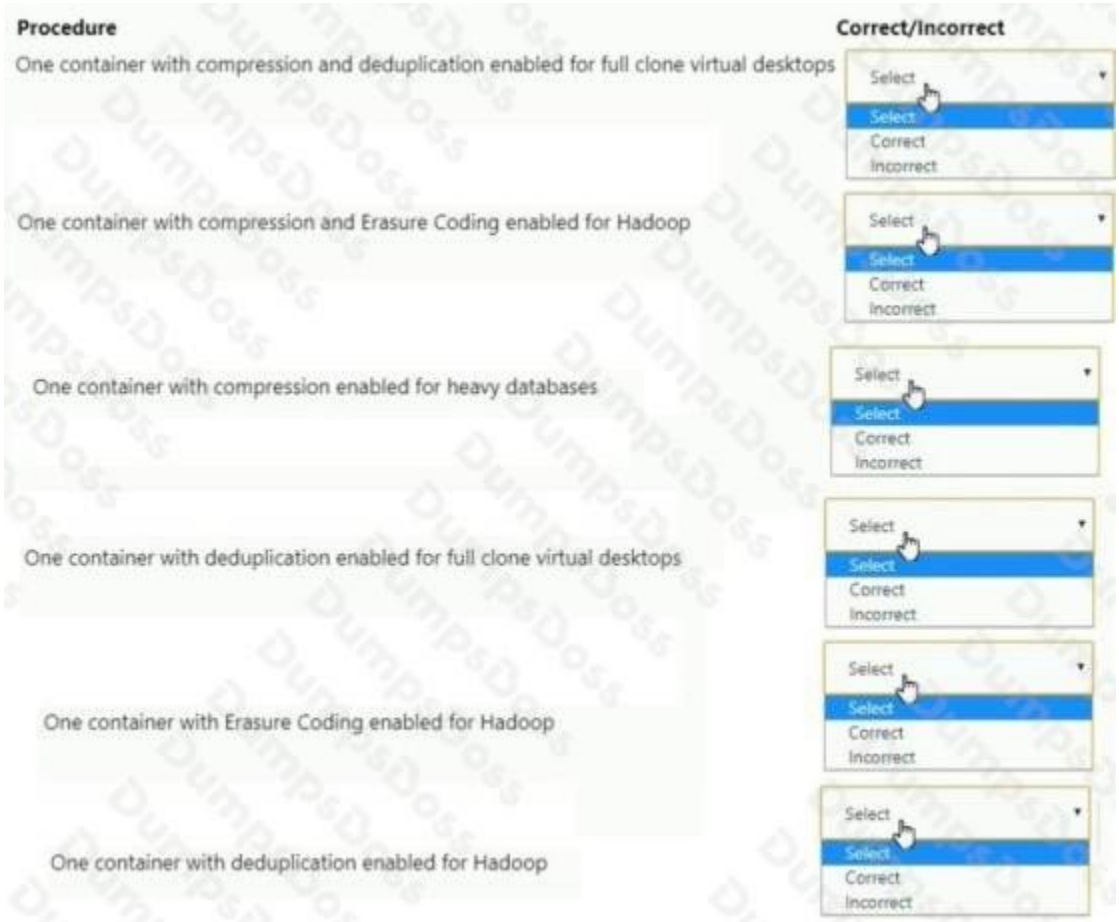
• Full clone virtual desktops

• Hadoop

• Write heavy databases

Whichthree correct configuration options should the administrator use to meet the item requirements? (Choose three.)

For each procedure, indicate whether it is a correct or incorrect procedure that must be configured to meet the item requirements using the drop-down option.


Procedure
Correct/Incorrect
One container with compression and deduplication enabled for full clone virtual desktops
One container with compression and Erasure Coding enabled for Hadoop
One container with compression enabled for heavy databases
One container with deduplication enabled for full clone virtual desktops
One container with Erasure Coding enabled for Hadoop
One container with deduplication enabled for Hadoop
Select
Correct
Incorrect

ANSWER:

Procedure
Correct/Incorrect
One container with compression and deduplication enabled for full clone virtual desktops
One container with compression and Erasure Coding enabled for Hadoop
One container with compression enabled for heavy databases
One container with deduplication enabled for full clone virtual desktops
One container with Erasure Coding enabled for Hadoop
One container with deduplication enabled for Hadoop
Select
Correct
Incorrect

Explanation:

For the full-clone virtual desktop workload, configure a container with both compression and deduplication enabled. Full clones create many virtual machines with substantial common operating-system, application, and image data. Deduplication is well suited to reducing repeated blocks across that shared content, while compression further reduces the physical capacity consumed by stored data. This combination helps an all-flash cluster support a high number of desktop clones efficiently while preserving the performance expected for VDI.

For Hadoop, configure compression and Erasure Coding on the container. Hadoop data sets can be large, and this workload commonly benefits from capacity-efficient storage. Compression reduces the amount of physical flash consumed by compressible data, and Erasure Coding provides a space-efficient data-protection method for eligible data. Together, these features are appropriate for increasing usable capacity for a Hadoop-oriented container while retaining Nutanix distributed data resilience. Nutanix documents the container-level data reduction and protection capabilities in its Prism storage container data reduction documentation.

For write-heavy databases, configure compression on the container. Compression provides capacity savings without requiring the database workload to rely on deduplication as its principal efficiency mechanism. This aligns the container configuration to a workload that produces significant writes while still using the all-flash platform effectively. Nutanix's enterprise cloud platform overview describes the platform's distributed storage and data-efficiency capabilities, including storage optimization features that can be applied according to workload needs.

QUESTION NO: 23

A customer wants to expand an existing cluster with three additional nodes. After running the Foundation process on the new nodes, the customer realizes that the wrong IPs where used and the nodes are configured on a different network. The customer decides to create a new cluster instead.

Which method should be used to recreate the cluster?

A. Log into IPMI and use cluster create command to create the cluster.

B. Log into CVM and use cluster create command to create the cluster.

C. Log into Hypervisor and use cluster create command to create the cluster.

D. Foundation all nodes again and create the cluster.

ANSWER: B

Explanation:

Log into CVM and use cluster create command to create the cluster. Foundation performs the imaging and initial configuration work required to prepare the nodes, including deploying the Controller VMs. Cluster formation is then performed from a Controller VM, where an administrator uses the `cluster create` command and supplies the Controller VM IP addresses for the nodes that will comprise the new cluster. The command establishes the distributed AOS cluster services across those CVMs and creates the cluster configuration.

Before issuing the command, the administrator should ensure that the intended Controller VM addresses are correctly configured and that all participating CVMs can communicate over the required network. Once the nodes are reachable on the correct network, connecting through SSH to one of the unclustered CVMs provides the appropriate execution context for cluster creation. This approach separates node imaging from cluster formation: Foundation prepares the nodes, while the CVM-based cluster command creates the Nutanix cluster. Nutanix documentation describes cluster creation as a CVM command-line operation and provides the associated workflow and requirements in the Prism Web Console Guide and the AOS Command Reference.

QUESTION NO: 24

Which two files should be downloaded to deploy Foundation VM on VMware ESXI or AHV Hypervisors? (Choose two.)

A. foundation_VM-version-disk-0.geow2

B. foundation_VM-version. tar

C. foundation_VM-version. vmdk

D. foundation-version.tar.gz

ANSWER: B C

Explanation:

The Foundation VM deployment package requires the Foundation VM archive, `foundation_VM-version. tar`, together with the VMware virtual-disk file, `foundation_VM-version. vmdk`. The archive provides the Foundation VM deployment content and associated metadata, while the VMDK supplies the virtual machine's disk image for a VMware ESXi deployment. These files are obtained from the Nutanix Support Portal for the Foundation release being used and should be kept at the corresponding release versions so that the VM is deployed with its intended software and disk image. After the Foundation VM is available on the target environment, it can be used to image and configure the target Nutanix nodes during cluster deployment. Nutanix documentation and release-specific Foundation downloads are available through the Nutanix Support Portal. For access requirements and supported-product assistance, see Nutanix Product Support.

QUESTION NO: 25

Over the period of 2 to 3 weeks, a cluster displays the following:

•Periods where Warning Alerts of memory usage over 75% are asserted

•Periods where Critical Warnings of memory usage over 90% are asserted

•Periods of slow of frozen VDI desktops have caused work stoppage or slowdown

•VDI clones have periodically not powered up when called, causing work stoppage

Which steps should be used to prioritize the administrator's troubleshooting efforts?

A. •Review the Analysis page for memory usage demand

B. •Analyze VM table page to access the VM functionality

C. •Verify VDI workload property for memory subscription

D. •Correlate the memory alerts with VDI workload demand, then evaluate current and projected memory capacity in Capacity Runway.

ANSWER: D

Explanation:

Correlate the memory alerts with VDI workload demand, then evaluate current and projected memory capacity in Capacity Runway. This is the appropriate priority because the symptoms indicate a recurring resource-contention condition that is directly affecting business-critical VDI availability and user experience. The administrator should first establish whether the warning and critical memory periods align with desktop slowdowns, freezes, and clone power-on failures. Correlating demand with the alert timeline distinguishes a transient peak from a sustained capacity shortfall and helps identify the time periods that require closer investigation. Capacity Runway then provides the forward-looking context needed to determine whether the cluster has sufficient headroom for the current VDI footprint and expected growth. This evidence supports a prioritized remediation plan, such as adjusting the VDI workload, reducing resource pressure, or planning a memory or node expansion before the condition becomes more frequent. Nutanix Prism Central provides monitoring, alerting, and capacity-planning capabilities intended for this operational workflow. See the Nutanix Documentation portal for Prism Central administration documentation and the Nutanix Product Support resources for operational guidance.

QUESTION NO: 26

A customer needs to meet the following requirements for their business critical application:

* SQL Servers must be on specific hosts to lower licensing costs.

* Oracle RAC servers must be on separate hosts for licensing reasons

Which policy or policies should be implemented to meet these requirements?

A. Configure VM-VM anti-affinity policy.

B. Configure VM-VM affinity policy.

C. Configure both VM-Host affinity and VM-VM anti-affinity policy.

D. Configure VM-Host affinity policy.

ANSWER: C

Explanation:

Configure both VM-Host affinity and VM-VM anti-affinity policy. VM-Host affinity is used to constrain the SQL Server virtual machines to a defined set of hosts. This supports processor-based licensing optimization because the workload is kept within the hosts that are licensed for the SQL Server software. The policy can be configured as a hard requirement when the virtual machines must not run outside the selected host group, subject to normal operational considerations such as host availability and maintenance planning.

VM-VM anti-affinity is required for the Oracle Real Application Clusters virtual machines because it directs the scheduler to place the specified virtual machines on different AHV hosts. Separating the cluster members provides the required host-level placement separation while also improving resilience to an individual host failure. Together, these policies independently enforce the licensing boundary for the SQL workload and the host-separation requirement for the Oracle RAC workload. Nutanix describes VM-host and VM-VM affinity capabilities in the Prism Central Guide; configuration and operational guidance is also available through the Nutanix Support Portal documentation.

QUESTION NO: 27

An administrator is configuring a Prism Central project for a development team. The team must be able to deploy VMs while being limited to an approved amount of cluster resources.

Which two settings should the administrator configure for the project? (Choose two.)

A. Assign project users or user groups.

B. Configure resource quotas.

C. Configure an IPMI administrator account for every project user.

D. Create a separate CVM for the project.

ANSWER: A B

Explanation:

Assign project users or user groups so that the development team has authorization to access and consume resources through the project. Prism Central projects provide a logical boundary for delegating self-service infrastructure access to specific users or directory groups.

Configure resource quotas to limit the amount of compute, memory, and storage resources that project members can consume. Quotas help prevent one project from exhausting shared cluster capacity and support governance in multitenant environments. Nutanix documents project administration and quota configuration in the Prism Central projects documentation.

QUESTION NO: 28

An administrator iscurrently using both 10g uplink with LACP and balance-tcp. A single VM should not be allowed to use more than a single 10G uplink, and both uplinks should be utilized.

Which two command should be used to configure the bond? (choose two)

A. Ovs-vsctl set port br0-up bond_mode=balance-slb

B. Ovs-vsctl set port br0-up bond_mode=balance-tcp

C. Ovs-vsctl set port br0-up bond_mode=active-backup

D. Ovs-vsctl set port br0-up other_config: bond-rebalance-interval=30000

ANSWER: A D

Explanation:

The correct configuration uses `Ovs-vsctl set port br0-up bond_mode=balance-slb` together with `Ovs-vsctl set port br0-up other_config: bond-rebalance-interval=30000`. In AHV/Open vSwitch, source-load-balancing (balance-slb) assigns traffic to an uplink based on the VM interface source MAC address. Consequently, traffic originating from a given VM interface remains associated with one physical 10 Gb uplink rather than having that VM's traffic distributed across both links. This satisfies the requirement that an individual VM not consume more than one uplink.

The bond rebalance interval enables Open vSwitch to periodically evaluate the member-link load and move eligible source-MAC assignments when necessary. Setting it to 30,000 milliseconds permits the bond to improve utilization of both uplinks over time while retaining the one-uplink-per-VM behavior at a given time. This is appropriate when aggregate traffic from multiple VMs should use both available 10 Gb links, but a single VM must remain constrained to a single link. Nutanix AHV networking uses Open vSwitch bonds for this uplink behavior; see the Nutanix AHV Administration Guide and the Open vSwitch bond configuration reference.

QUESTION NO: 29

An administrator is creating an AHV VM from a Linux image. The VM must automatically configure an SSH public key and a hostname during its first boot.

Which two actions should the administrator take? (Choose two.)

A. Use a Linux image with cloud-init installed.

B. Provide cloud-init user-data when creating the VM.

C. Install Nutanix Guest Tools before powering on the VM.

D. Enable Erasure Coding on the storage container.

ANSWER: A B

Explanation:

The Linux guest image must include **cloud-init**, and the administrator must provide the required **cloud-init user-data** configuration when creating the VM. Cloud-init is the guest-side initialization service that processes instance metadata and user-data at first boot. It can configure hostnames, users, SSH keys, network settings, and startup commands without requiring manual console access to each new VM.

Providing user-data without cloud-init installed in the guest does not configure the VM, because there is no guest service available to process the supplied configuration. Nutanix Guest Tools is useful for supported guest integration features, but it does not replace cloud-init for initial Linux guest customization. See the Nutanix Documentation portal and the cloud-init documentation.

QUESTION NO: 30

A consultant has been tasked with increasing security on a Nutanix cluster by disabling password authentication when accessing the CVM and AHV hosts and instead moving to key-based SSH.

What is the easiest way for the consultant to meet these requirements?

A. Enable STIGs via command line on SSH to a CVM.

B. Configure LDAP authentication through a secure server.

C. Enable Cluster Lockdown and provide an RSA key.

D. Restrict access with User Management in Prism.

ANSWER: C

Explanation:

Enable Cluster Lockdown and provide an RSA key. Cluster Lockdown is Nutanix's purpose-built control for securing SSH access to Controller VMs and AHV hosts at the cluster level. When enabled, it disables password-based SSH authentication for the protected Nutanix components and establishes public-key authentication as the approved access mechanism. The administrator supplies the authorized SSH public key, allowing personnel who hold the corresponding private key to authenticate securely without transmitting or relying on a password. This provides a centrally applied, consistent control across the cluster rather than requiring separate, manual SSH configuration changes on every CVM and hypervisor host. Cluster Lockdown also supports the operational need for controlled support and administrative access while reducing the exposure associated with password guessing, credential reuse, and unmanaged local SSH settings. Nutanix documents Cluster Lockdown in its Security Guide as a cluster security feature for restricting SSH access and managing authorized public keys. Review the current documentation in the Nutanix Support Portal documentation library and the Nutanix security overview for platform security capabilities and guidance.

QUESTION NO: 31

The networking team makes changes to the Top of Rack switches to which the Nutanix cluster are attached. A few VMs are able to communicate with each other on the same node but are unable to connect to other parts of the network.

What is the likely cause of this issue?

A. There is a VLAN misconfiguration on the VMs.

B. The vNIC port is disconnected on the affected VMs.

C. There is a VLAN misconfiguration on the switch.

D. Jumbo Frame are misconfigured across ports.

ANSWER: C

Explanation:

There is a VLAN misconfiguration on the switch. The observed behavior is consistent with traffic being switched locally between VMs on the same Nutanix host while traffic that must leave that host cannot reach the intended external network. On AHV, VMs connected to the same logical network and resident on the same node can communicate through the local Open vSwitch datapath. Communication to systems on other hosts or outside the cluster, however, depends on the physical uplinks and the Top of Rack switch configuration carrying the required VLAN correctly.

Because the issue began after networking changes at the Top of Rack switches, the most likely source is an incorrect VLAN assignment, missing VLAN from a trunk/allowed-VLAN list, or an inconsistent tagging configuration on the switch ports connected to the Nutanix nodes. The switch configuration must preserve the VLAN associated with the AHV virtual network across all relevant host-facing ports and upstream paths. Nutanix networking documentation describes the relationship between AHV virtual networks, VLAN IDs, Open vSwitch bridges, and physical network uplinks; these dependencies should

be validated following switch changes. See the Nutanix Documentation Portal and Nutanix's Product Support resources for AHV networking guidance and supported configuration references.

QUESTION NO: 32

A consultant is deploying a Nutanix cluster at a customer location. The consultant will be deploying the latest AOS along with the latest Nutanix hardware.

Which three references should the consultant review prior to this installation? (Choose three.)

A. Release Notes

B. Software Product Interoperability

C. Field & Security Advisories

D. End-Of-Life (EOL) Information

E. Acropolis Advanced Administration Guide

ANSWER: A B C

Explanation:

Release Notes, **Software Product Interoperability**, and **Field & Security Advisories** should be reviewed before installing a new Nutanix cluster with current hardware and the latest AOS release. Release notes provide release-specific information that directly affects deployment planning, including new capabilities, known limitations, upgrade or installation considerations, and resolved issues. Reviewing them ensures that the selected AOS version is appropriate for the intended environment and that any required precautions are identified before work begins.

Software Product Interoperability confirms that the planned AOS release is supported with the selected Nutanix hardware platform and with related software components that may be used in the deployment. This validation is especially important when both the platform and software are newly released. Field and Security Advisories provide time-sensitive operational information, including hardware notices, vulnerability mitigations, affected versions, and required corrective actions. Checking advisories before deployment helps the consultant apply recommended updates or configuration guidance from the outset. Nutanix publishes product documentation and release materials through the Nutanix Support Portal documentation page; current advisories and support communications are available through the Nutanix Support Portal.

QUESTION NO: 33 - (SIMULATION)

An administrator is configuring an All Flash cluster to support the following workloads:

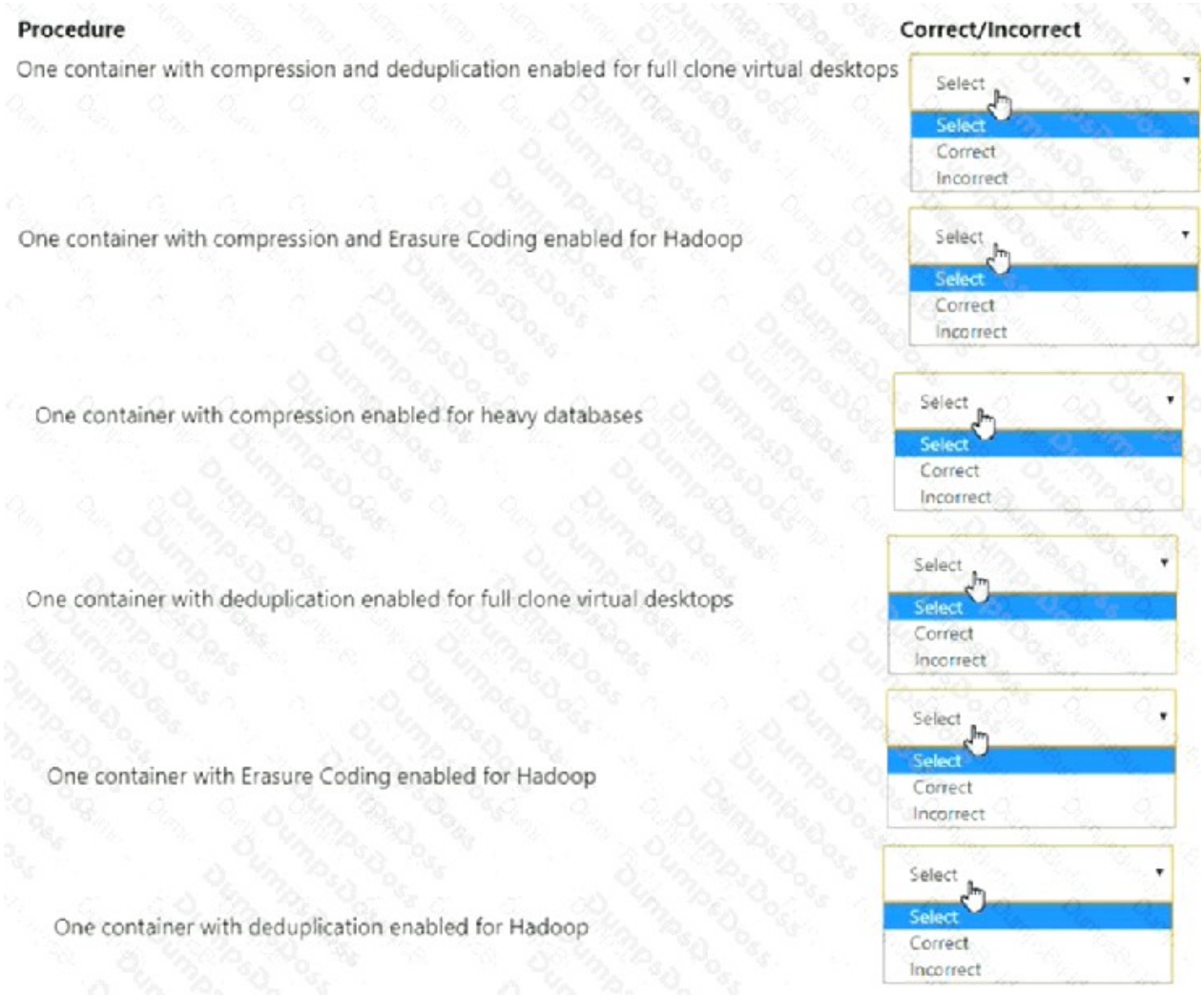
• Full clone virtual desktops

• Hadoop

• Write heavy databases

Which three correct configuration options should the administrator use to meet the item requirements? (Choose three.)

For each procedure, indicate whether it is a correct or incorrect procedure that must be configured to meet the item requirements using the drop-down option.



ANSWER: See the explanation for the answer

Explanation:

Configure the drop-downs as follows:

Full-clone VDI has many identical blocks, making **deduplication** the appropriate optimization. Write-heavy databases are suited to **compression**. Hadoop is suited to **Erasure Coding** for capacity efficiency; Hadoop data is commonly already compressed, so adding compression is not the required configuration.

QUESTION NO: 34

After a consultant runs a bare metal Foundation, the imaging process fails.

In which two locations can the consultant find the logs? (Choose two.)

A. On the CVM - /home /nutanix/foundation/logs

B. On the Hypervisor - /home/nutanix/foundation/logs

C. On the Foundation VM - /home/nutanix/foundation/logs

D. View Logs link on the Foundation Imaging progress screen

ANSWER: C D

Explanation:

The Foundation VM is the primary service host for a bare-metal Foundation deployment, so its local Foundation log directory, `/home/nutanix/foundation/logs`, contains the detailed records generated by the imaging workflow. These records are useful for tracing each imaging phase, including node discovery, network configuration, ISO or package handling, hypervisor installation, and CVM deployment. Reviewing the files on the Foundation VM gives the consultant access to persistent diagnostic data after an imaging failure and supports collection of the relevant evidence for escalation if necessary.

The *View Logs* link on the Foundation Imaging progress screen provides the immediate, task-oriented view of the same imaging activity while Foundation is reporting progress or an error. It is particularly valuable for quickly identifying the phase that failed and reading the associated messages without first connecting to the Foundation VM. Together, these locations provide both the convenient UI-based troubleshooting view and the underlying log files needed for deeper analysis. Nutanix publishes Foundation documentation and related deployment resources through the Nutanix Support Portal documentation library; additional Foundation operational guidance is available in the Nutanix Bible.

QUESTION NO: 35

An administrator manages the following two Nutanix AOS 5.15 cluster environment:

• Corp-cluster-01

• Corp-cluster-02

The VM images must be available only on Corp-cluster-01, but cannot be checked out to cluster Corp-cluster-02. The images also cannot be checked out to any other clusters that are registered with Prism Central in the future.

Which two configuration settings must the administrator choose when creating the image placement policy that satisfies the stated requirements? (Choose two.)

A. Create an image placement policy that identifies cluster Corp-cluster-01 as the target cluster

B. Set the policy enforcement to Soft.

C. Set the policy enforcement to Hard.

D. Create an image placement policy that identifies cluster Corp-cluster-02 as the target cluster.

ANSWER: A C

Explanation:

The administrator should create an image placement policy that identifies cluster Corp-cluster-01 as the target cluster and set the policy enforcement to Hard. In Prism Central image management, an image placement policy determines the clusters to which an image may be checked out. Specifying Corp-cluster-01 as the target confines the intended image availability to that cluster rather than making the image eligible for checkout throughout the Prism Central environment.

Hard enforcement is required because the requirement is restrictive and must continue to apply as the environment changes. A hard image placement policy prevents checkout of the image to clusters that are not explicitly included in the policy. Therefore, Corp-cluster-02 cannot receive the image, and clusters registered with Prism Central later also remain unable to check it out unless the policy is deliberately updated to include them. This creates an explicit allow-list model: only Corp-cluster-01 is authorized for image checkout. Nutanix describes centralized image management and image placement policies through Prism Central in its AHV image-management overview. For broader product documentation and version-specific administration guidance, consult the Nutanix Documentation Portal.

QUESTION NO: 36

Refer to Exhibit:

Basic Cluster Inventory					
Rack Unit	Node ID	Hypervisor Host Name	BMC IP Address	Hypervisor IP Address	CVM IP Address
S4-B13-U36-37	A	AHV-CLUSTER-01	172.25.16.10/24	172.25.17.10/24	172.25.17.20/24
	B	AHV-CLUSTER-02	172.25.16.11/24	172.25.17.11/24	172.25.17.21/24
	C	AHV-CLUSTER-03	172.25.16.12/24	172.25.17.12/24	172.25.17.22/24
	D	AHV-CLUSTER-04	172.25.16.13/24	172.25.17.13/24	172.25.17.23/24

A customer has completed and given the pre-delivery questionnaire to the consultant. The customer has indicated that they are using HPE/OEM hardware.

Which action should the consultant take to prepare the laptop and Foundation networking for the installation?

A. Configure Backplane Traffic Isolation.

B. Set IP Addresses in CVM/Host subnet only.

C. Set IP Addresses in both CVM/Host and IPMI subnets.

D. Enable network segmentation.

ANSWER: C

Explanation:

Set IP Addresses in both CVM/Host and IPMI subnets. is the appropriate preparation for a Foundation deployment on HPE/OEM hardware. Foundation must be able to communicate with the server management interfaces as well as the interfaces used for host and Controller VM deployment. The IPMI network provides out-of-band access to the physical servers, which Foundation uses to discover, control, and image the nodes during the initial build process. The CVM/Host network is required for the in-band deployment workflow and for configuring the host and CVM network settings specified in the installation plan.

Accordingly, the consultant's laptop and the Foundation environment need network connectivity and valid addressing in both networks. This may be achieved using separate laptop network adapters, VLAN-capable switching, or another supported network design, provided that the Foundation instance can reach the target IPMI addresses and the host/CVM deployment network. Confirming this connectivity before the installation avoids discovery and imaging failures and supports a controlled Foundation workflow. Nutanix publishes Foundation deployment documentation through its Documentation Portal; product lifecycle and supported software information are also available through the Nutanix Product Support page.

QUESTION NO: 37

Refer to the exhibit.

A system administrator is using Range-Autofill tool to assign IP addresses to setup a multi-block cluster based on the following configuration:

Which additional changes must be made during the Foundation process to configure the cluster correctly?

A. Change host names

B. Reorder block serial

C. Change IP address

D. Reorder blocks

ANSWER: A

Explanation:

Change host names is required. Foundation's Range Autofill capability simplifies deployment by applying sequential address ranges to the selected nodes, but the administrator must still validate that the per-node identity information is appropriate for the intended multi-block cluster layout. In particular, every hypervisor host requires a unique hostname that conforms to the organization's naming convention and maps to the correct physical node after the IP ranges have been

populated. This is especially important in a multi-block deployment, where the order in which nodes are displayed or discovered can differ from the desired hostname sequence. Updating the hostnames during Foundation ensures that each generated host configuration has the proper unique identity before imaging and cluster creation proceed. Correct host naming supports clear operational identification in Prism, hypervisor management, monitoring, DNS integration, and subsequent support activities. The Foundation workflow is designed to allow administrators to review and edit node-specific configuration values, including hostnames, before starting the imaging process. See the Nutanix Foundation documentation for Foundation deployment and configuration guidance, and the Nutanix Field Installation Guide for cluster installation requirements.

QUESTION NO: 38

A customer has a primary datacenter with 12 Nutanix blocks distributed across three racks. The customer wants toachieve the most resiliency possible. They also have a datacenter in a branch office that is 400 kilometers away from the primary datacenter.

Which two solutions should be used? (Choose two.)

A. Time Stream to a remote site

B. Async DR to a remote site

C. Rack awareness

D. Block awareness

ANSWER: B C

Explanation:

Async DR to a remote site provides the appropriate inter-site protection for a branch-office datacenter located 400 kilometers away. Nutanix asynchronous replication uses protection domains and recovery point objectives to replicate selected workloads to a remote Nutanix environment without requiring the low latency needed for synchronous replication. This enables recoverability following a primary-datacenter outage while allowing replication schedules to be aligned to the customer's recovery objectives. Nutanix disaster recovery capabilities, including asynchronous replication and recovery workflows, are described at Nutanix Disaster Recovery.

Rack awareness improves local resiliency across the three-rack primary site. When rack awareness is configured, Nutanix places data replicas across distinct racks, helping ensure that a single rack-level failure—including loss of rack power, networking, or multiple nodes in that rack—does not make protected data unavailable. With 12 blocks distributed among three racks, the environment has the physical layout needed to take advantage of rack-level fault-domain placement. This complements replication to the remote site by addressing failures within the primary datacenter as well as site-level recovery requirements. Nutanix explains its distributed data-resiliency architecture and failure-domain approach in the Nutanix Bible.

QUESTION NO: 39

Refer to the exhibit.

User	Quota	Enforcement
All Users	No quota limit	
fileslab\user1	5 GiB	Soft
All Users in "AAPM"	10 GiB	Hard

User 1 and User 2 belong to the AAPM group

What are two descriptions of how Files perform quota management? (Choose two.)

A. User 2 can continue to add another 3GB file butwill receive a daily notification email.

B. User 1 can continue to add another 5GB file but will receive a daily notification email.

C. User 1 can add an 8GB file to the share without receiving notification.

D. User 2 can add an 8GB file without receivinga notification email.

ANSWER: B D

Explanation:

“User 1 can continue to add another 5GB file but will receive a daily notification email.” is correct because the quota configuration shown for User 1 is a soft quota condition: the user is permitted to write beyond the configured warning threshold, while Nutanix Files generates the configured daily notification. The additional 5 GB remains allowable because the applicable hard enforcement limit has not been reached.

“User 2 can add an 8GB file without receiving a notification email.” is also correct because the applicable quota evaluation for User 2 does not place that write at or above a notification threshold. Nutanix Files evaluates quotas according to the configured scope, such as an individual user, an Active Directory group, or a directory, and sends notifications only when the relevant configured threshold is crossed. Membership in the AAPM group does not by itself mean that every user receives the same warning at the same storage-consumption point; the effective quota and current usage shown in the exhibit determine the outcome.

For quota behavior, including soft-limit notifications and enforcement based on quota scope, see the Nutanix Files quota documentation.

QUESTION NO: 40

A consultant needs to verify the make and model of the systems that will be imaged with

Foundation. The consultant does not have the Bill of Materials (BOM) available to review.

When should the consultant verify the make and model to prepare for the cluster deployment?

A. During the Foundation Process

B. While conducting the Tech Review Call

C. Upon arriving on-site

D. When reviewing the Statement of Work (SOW)

ANSWER: B

Explanation:

While conducting the Tech Review Call is correct because the technical review is the predeployment checkpoint for validating the implementation scope, site readiness, and the specific hardware that will be built. When a Bill of Materials is not available, the consultant should obtain and confirm the system make and model with the customer during this call, before scheduling or beginning the imaging activity. This allows the consultant to confirm that the intended nodes are supported and to prepare the appropriate Foundation workflow, software, and platform-specific deployment requirements. It also provides time to resolve discrepancies between the planned solution and the hardware actually present, avoiding delays once deployment work begins. Foundation is Nutanix’s cluster-imaging tool, and successful imaging depends on having the correct target-node and software information established as part of deployment planning. Nutanix documentation describes Foundation requirements and imaging procedures in the Nutanix Foundation Guide; the current documentation catalog is available through the Nutanix Support Portal documentation page.

QUESTION NO: 41

During a Site Readiness Check, a customer informed the consultant that there is no NTP server currently configured in the environment.

Which two statements should the consultant consider for continuing the cluster deployment? (Choose two.)

A. An NTP server is not required for cluster Foundation and can be added later.

B. If an NTP server is provided using FQDN, a DNS server is required.

C. At least 3 NTP servers must be provided in a comma-separated list.

D. At least one external NTP server must be used to complete Foundation process.

ANSWER: A B

Explanation:

“An NTP server is not required for cluster Foundation and can be added later.” is correct because Foundation can be used to image and configure a Nutanix cluster without NTP information being available at that moment. The consultant can continue the initial deployment, provided that time synchronization is planned and configured as part of the post-deployment configuration. Consistent time across Controller VMs, hypervisor hosts, and management services is an important operational requirement for reliable logging, authentication, certificates, alerting, and distributed-service behavior, so NTP should be configured promptly once a suitable source is available.

“If an NTP server is provided using FQDN, a DNS server is required.” is also correct. An FQDN is a hostname rather than a directly routable address; therefore, each system that must contact the NTP source needs DNS resolution to translate that name into an IP address. The deployment design must include reachable DNS services and valid forward lookup records when the NTP source is specified by name. Alternatively, an IP address can be supplied where appropriate, avoiding hostname resolution for that entry. See the Nutanix Foundation Guide and Nutanix Documentation for Foundation and cluster network-configuration guidance.

QUESTION NO: 42

While reviewing the cluster questionnaire, the consultant identifies that the VLAN numbers for the CVM, AHV, and IPMI networks are missing.

Which statement is correct regarding this scenario?

A. The consultant should remind the customer to provide the same VLAN for CVM and AHV, and a separate VLAN for IPMI.

B. The CVM and AHV networks should be on the native VLAN, and there is no need to ask.

C. Foundation automatically assigns VLANs when the switch cables are connected to the nodes.

D. The customer is supposed to provide this information when the consultant is onsite.

ANSWER: A

Explanation:

The consultant should remind the customer to provide the same VLAN for CVM and AHV, and a separate VLAN for IPMI. Network details must be collected before deployment because Foundation and the cluster configuration require the correct management-network addressing and VLAN design. In a standard AHV deployment, the Controller VM and its AHV host use the same management network/VLAN. This arrangement provides the required connectivity between the hypervisor and its local CVM and lets the Nutanix cluster-management services communicate consistently across all nodes. The VLAN must therefore be identified and configured on the relevant physical-switch ports before imaging and cluster creation.

IPMI is the server’s out-of-band hardware-management interface. Placing it on a dedicated management VLAN separates remote power control, hardware monitoring, and console access from the in-band AHV/CVM management traffic. This supports administrative isolation and allows infrastructure teams to apply appropriately restrictive access controls to the out-of-band network. The consultant should obtain the VLAN IDs, IP addressing, gateway, and associated switch-port configuration from the customer as part of the predeployment questionnaire, then validate that the intended network design

is available before starting Foundation. Nutanix deployment guidance and networking concepts are available in the Nutanix Foundation Guide and the Nutanix AHV overview.

QUESTION NO: 43

Over the period of 2 to 3 weeks, a cluster displays the following:

â€¢Periods where Warning Alerts of memory usage over 75% are asserted

â€¢Periods where Critical Warnings of memory usage over 90% are asserted

â€¢Periods of slow of frozen VDI desktops have caused work stoppage or slowdown

â€¢VDI clones have periodically not powered up when called, causing work stoppage

Which steps should be used to prioritize the administratorâ€™s troubleshooting efforts?

A. â€¢Assess resource health on Hardware pageâ€¢Review the Analysis page for memory usage demandâ€¢Determine the VDI workload-to-host affinity across the cluster

B. â€¢Analyze Alert Pages for a root cause of memory problemâ€¢Analyze VM table page to access the VM functionalityâ€¢Analyze the VDI Clone properties for possible VDI Workload stress

C. â€¢Check Analysis page for CPU demandâ€¢Verify VDI workload property for memory subscriptionâ€¢Review the Hardware page to determine if the cluster has sufficient RAM

D. â€¢Review Analysis Page for memory use patternâ€¢Correlate alerts with VDI workload demandâ€¢Analyze current and future workload in the Capacity Runway tab for sufficient resources

ANSWER: D

Explanation:

Review Analysis Page for memory use pattern; correlate alerts with VDI workload demand; and analyze current and future workload in the Capacity Runway tab for sufficient resources is the appropriate prioritization because the reported symptoms point first to a recurring cluster-memory contention condition. Prism analysis data lets the administrator establish when memory pressure occurs, how long it persists, and whether it aligns with periods of increased desktop activity, clone creation, or login demand. Correlating alert timestamps with VDI workload behavior distinguishes a sustained capacity shortfall from a short-lived operational peak and helps focus investigation on the condition affecting users.

After identifying the pattern, capacity planning is essential. The Capacity Runway view evaluates resource consumption trends and projects when available cluster capacity will be exhausted. Reviewing both present utilization and projected growth allows the administrator to determine whether the immediate remediation should be workload scheduling or tuning, reducing demand, or adding cluster resources. This sequence directly addresses the observed inability to power on some clones and the degraded desktop experience while providing evidence for a durable capacity decision. Nutanix describes Prism's monitoring and management capabilities at Nutanix Prism; current product documentation is available through the Nutanix Support Portal documentation library.

QUESTION NO: 44

A customer is running out of storage in an ESXi cluster. The customer wants to add storage without paying for an additional hypervisor license.

Which option should the consultant recommend to meet the requirement?

A. Convert the cluster to AHV to support storage-only node requirements.

B. Select the storage-only checkbox during Foundation and then expand the cluster in Prism.

C. Buy a new node to meet the requirements of the storage-only node specifications.

D. Edit the factory_config.json file to configure the node as storage-only and then expand the cluster in Prism

ANSWER: B

Explanation:

Select the storage-only checkbox during Foundation and then expand the cluster in Prism. A Nutanix storage-only node contributes its local disks to the cluster's distributed storage fabric while not hosting user virtual machines. Because the node does not need to run the ESXi hypervisor for VM workloads, it addresses the customer's need for additional capacity without requiring an additional ESXi hypervisor license for that node.

For this deployment type, the node must be prepared as a storage-only node during the Foundation imaging workflow. Foundation applies the appropriate node configuration before it joins the existing environment. After imaging is complete and the node is connected to the cluster network, the administrator expands the cluster through Prism so that the new node is discovered, added, and its storage capacity becomes available to the Nutanix Distributed Storage Fabric. This approach preserves the existing ESXi cluster architecture while scaling storage independently of compute and hypervisor licensing. Consult the applicable Nutanix software release documentation and platform compatibility information before deployment, because storage-only-node support depends on the hardware platform and supported software versions. See the Nutanix product documentation portal and Nutanix Support Portal for the relevant Foundation and cluster-expansion procedures.