Number: NS0-604
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: NS0-604

Exam Name: Hybrid Cloud - Architect

Exam A

QUESTION 1
A company is migrating on-premises SMB data and ACLs to the Azure NetApp Files storage solution. Which two Active Directory solutions are supported? (Choose two.)

A. Active Directory Domain Services (AD DS)
B. Azure Active Directory (Azure AD)
C. Azure Active Directory Domain Services (Azure AD DS)
D. Azure Identity and Access Management

Correct Answer: A, C
Section:
Explanation:
When migrating SMB data and Access Control Lists (ACLs) to Azure NetApp Files, Active Directory integration is necessary for user authentication and permission management. The following two solutions are supported:
Active Directory Domain Services (AD DS) (A): AD DS is the traditional, on-premises Active Directory solution that provides authentication and authorization services. Azure NetApp Files can integrate with on-premises AD DS, enabling the migration of SMB data along with the corresponding ACLs.
Azure Active Directory Domain Services (Azure AD DS) (C): Azure AD DS provides managed domain services in the cloud and supports Active Directory features such as domain join, group policies, and LDAP. It is compatible with Azure NetApp Files, allowing seamless migration and access control management for SMB workloads in the cloud.
Azure Active Directory (Azure AD) (B) and Azure Identity and Access Management (D) focus more on user identity management rather than direct SMB file system integration, and they are not suitable for handling file system ACLs and SMB shares.

QUESTION 2
A company has finished migrating all data to NetApp Cloud Volumes ONTAP. An application administrator needs to make sure that there are no interruptions in service for this new NFSv4 application.
Which feature must be registered on the Azure subscription to reduce unplanned failover times?

A. multipath HA
B. high availability
C. fault tolerance
D. redundancy

Correct Answer: B
Section:
Explanation:
NetApp Cloud Volumes ONTAP provides a High Availability (HA) configuration, which is crucial for ensuring that services remain available even during unplanned outages. When using NetApp Cloud Volumes ONTAP in environments such as Azure, ensuring continuous availability, especially for NFSv4 workloads, is vital.
The 'High Availability' (HA) feature creates a pair of ONTAP instances configured as an active-passive cluster. This setup reduces failover times by allowing one node to take over if the other fails, providing minimal service disruption. HA is designed to manage failovers automatically, which is essential for applications requiring constant availability, such as those using NFSv4. In Azure, enabling this feature via the appropriate subscription registration ensures that when an unexpected failure occurs, the system will automatically failover to the standby node, minimizing downtime and ensuring that the application continues to function smoothly without manual intervention.
In this case, 'multipath HA,' 'fault tolerance,' and 'redundancy' are related concepts, but they don't directly address the specific need to register and enable the high-availability feature in Azure. Registering HA on the Azure subscription ensures that the Cloud Volumes ONTAP can perform its failover processes effectively, keeping the application running.

QUESTION 3
Which network construct is required to enable nondisruptive failover between nodes in a Multi-AZ NetApp Cloud Volumes ONTAP cluster in AWS?

A. floating IPs
B. security groups
C. elastic network interfaces
D. Intercluster UFs

Correct Answer: A
Section:
Explanation:
In a Multi-AZ (Availability Zone) setup for NetApp Cloud Volumes ONTAP in AWS, ensuring nondisruptive failover between nodes is critical for high availability. 'Floating IPs' are required for seamless failover between nodes in such a configuration.
Floating IPs allow the primary node to automatically transfer its IP address to the secondary node during a failover event, ensuring that clients can continue to access the service without needing to reconfigure anything. This mechanism enables clients to access the same IP regardless of which node in the cluster is actively serving requests, thus maintaining nondisruptive operations.
Elastic Network Interfaces (ENIs) facilitate networking in AWS but do not inherently handle IP floating between nodes for failover. Security groups and Intercluster UFs manage security and inter-node communication, respectively, but do not address the failover requirements. Floating IPs are explicitly designed to enable failover in high-availability cloud storage environments like NetApp Cloud Volumes ONTAP.
Thus, 'floating IPs' are the required network construct that allows for nondisruptive failover between nodes in a multi-AZ setup, ensuring continuous service availability even in the event of an outage in one availability zone.

QUESTION 4
What are two ways to optimize cloud data storage costs with NetApp Cloud Volumes ONTAP? (Choose two.)

A. aggregate deduplication
B. thin provisioning
C. TCO calculator
D. volume deduplication

Correct Answer: B, D
Section:
Explanation:
NetApp Cloud Volumes ONTAP provides several storage efficiency features that help optimize cloud storage costs. Two of the key methods for reducing costs are:
Thin Provisioning: This feature allows users to allocate more storage capacity than is physically available. Instead of reserving full storage at the time of volume creation, space is only consumed as data is written. This reduces upfront costs and optimizes storage use by delaying actual storage allocation until necessary, making it cost-effective.
Volume Deduplication: Deduplication removes redundant copies of data within a volume, reducing the total storage footprint. By eliminating duplicate blocks of data, volume deduplication significantly cuts down on the amount of storage consumed, leading to lower storage costs in the cloud environment.
Other options like 'aggregate deduplication' and the 'TCO calculator' are not direct methods to optimize storage costs. Aggregate deduplication is not as granular as volume deduplication, and the TCO calculator is a tool for estimating total cost, not a method for optimization.

QUESTION 5
When considering security for Azure NetApp Files, what is a key security consideration to avoid a breach of confidentiality?

A. application of network security groups
B. Virtual Network Encryption
C. encryption using Kerberos with AES-256
D. double encryption at rest

Correct Answer: D
Section:
Explanation:
For securing Azure NetApp Files and ensuring the confidentiality of data, a critical security feature is double encryption at rest. This technique involves encrypting the data twice at rest, once at the storage level using Azure's default encryption and again using NetApp's built-in encryption features such as NetApp Volume Encryption (NVE). Double encryption provides an additional layer of protection, significantly reducing the risk of data breaches

or unauthorized access.
While network security groups (A) and Kerberos encryption (C) play roles in protecting network traffic and securing authentication, they do not address the need for data encryption at rest, which is critical for confidentiality.
Virtual Network Encryption (B) is also related to encrypting network data but doesn't focus on encryption at rest.
In highly regulated environments where data confidentiality is paramount, double encryption at rest ensures that even if one encryption layer is compromised, the data remains protected by the second encryption layer, thereby greatly enhancing security.

QUESTION 6
A customer has a cloud-first strategy and wants to protect data against ransomware. The customer wants to use the NetApp Autonomous Ransomware Protection feature.
Which solution should the customer use?

A. NetApp Cloud Volumes ONTAP
B. Azure NetApp Files
C. Amazon FSx for NetApp ONTAP
D. NetApp Cloud Volumes Service

Correct Answer: A
Section:
Explanation:
To protect data against ransomware, NetApp Cloud Volumes ONTAP offers the NetApp Autonomous Ransomware Protection feature. This feature uses machine learning and data analytics to detect and respond to abnormal file activities, helping prevent ransomware attacks.
Azure NetApp Files (B), Amazon FSx for NetApp ONTAP (C), and NetApp Cloud Volumes Service (D) provide robust data services, but Cloud Volumes ONTAP specifically includes the Autonomous Ransomware Protection feature.

QUESTION 7
A hospital needs to continuously scan a variety of data sources to verify that they are meeting regulatory compliance.
Which NetApp BlueXP cloud services solution should the hospital use?

A. operational resiliency
B. digital advisor
C. classification
D. ransomware protection

Correct Answer: C
Section:
Explanation:
For continuously scanning various data sources to ensure regulatory compliance, NetApp BlueXP Classification is the appropriate solution. This service helps organizations identify and classify sensitive data across their environments, ensuring that they meet compliance requirements such as healthcare regulations (HIPAA, for example).
Operational resiliency (A) focuses on system reliability, Digital advisor (B) offers system performance insights, and Ransomware protection (D) deals with security threats rather than compliance scanning.

QUESTION 8
A customer has an on-premises AFF cluster and needs to replicate a NAS volume to Azure NetApp Files. Which replication technology should the customer use?

A. NetApp BlueXP copy and sync
B. NetApp BlueXP tiering
C. NetApp BlueXP replication
D. Azure Site Recovery

Correct Answer: C

Section:
Explanation:
To replicate a NAS volume from an on-premises AFF (All-Flash FAS) cluster to Azure NetApp Files, the customer should use NetApp BlueXP Replication. This replication technology facilitates data synchronization and replication between ONTAP systems and Azure NetApp Files, making it ideal for hybrid cloud data mobility.
NetApp BlueXP copy and sync (A) is for file migration, BlueXP tiering (B) is for storage optimization, and Azure Site Recovery (D) is focused on VM disaster recovery, not NAS volume replication.

QUESTION 9
Which network configuration is required for NetApp BlueXP to discover an on-premises NetApp cluster?

A. outbound 443 access to the BlueXP service
B. inbound 443 access to the cluster-management UF
C. inbound 443 access from the BlueXP service
D. outbound 443 access to the Connector IP address

Correct Answer: A
Section:
Explanation:
For NetApp BlueXP to discover an on-premises NetApp cluster, the network must be configured to allow outbound 443 access to the BlueXP service. Port 443 is used for secure HTTPS communication, and BlueXP needs to establish an outbound connection from the on-premises NetApp cluster to the cloud-based BlueXP service for discovery and management.
Inbound 443 access (B and C) is not required for discovery, and outbound 443 access to the Connector IP address (D) is relevant only when interacting with the BlueXP Connector, not for cluster discovery.

QUESTION 10
A customer has on-premises NetApp systems and wants information about data to migrate to Azure. Which dashboard in NetApp BlueXP digital advisor should the customer use?

A. Valuable Insights
B. Health Check
C. Cloud Recommendations
D. Keystone Advisor

Correct Answer: C
Section:
Explanation:
To get insights about which data to migrate from on-premises NetApp systems to Azure, the customer should use the Cloud Recommendations dashboard in NetApp BlueXP Digital Advisor. This dashboard analyzes the on-premises environment and provides recommendations on which workloads or datasets are best suited for migration to the cloud, such as to Azure.
Other dashboards like Valuable Insights (A) and Health Check (B) provide general system health and performance information, while Keystone Advisor (D) relates to NetApp's subscription-based storage offering.

QUESTION 11
A company experienced a recent security breach that encrypted data and deleted Snapshot copies. Which two features will protect the company from this breach in the future? (Choose two.)

A. SnapLock
B. Data Lock
C. Snapshot technology
D. multi-admin verification

Correct Answer: A, D
Section:
Explanation:
To prevent security breaches like the one experienced by the company, where data was encrypted and Snapshot copies were deleted, two features are essential:

SnapLock (A): SnapLock is a feature that provides write once, read many (WORM) protection for files. It prevents the deletion or modification of critical files or snapshots within a specified retention period, even by an administrator. This feature would have protected the company's Snapshot copies by locking them, making it impossible to delete or alter them, thus preventing data loss during a ransomware attack.
Multi-Admin Verification (D): This feature requires approval from multiple administrators before critical operations, such as deleting Snapshots or making changes to protected data, can proceed. By requiring verification from multiple trusted individuals, it greatly reduces the risk of unauthorized or malicious actions being taken by a single user, thereby providing an additional layer of security.
While Snapshot technology (C) helps with regular backups, it doesn't protect against deliberate deletion, and Data Lock (B) is not a NetApp-specific feature for protecting against such breaches.

QUESTION 12
A customer wants to create a flexible solution to consolidate data in the cloud. They want to share files globally and cache a subset on distributed locations.
Which two components does the customer need? (Choose two.)

A. NetApp BlueXP edge caching Edge instances
B. Flash Cache intelligent caching
C. NetApp BlueXP copy and sync
D. NetApp Cloud Volumes ONTAP

Correct Answer: A, D
Section:
Explanation:
For a company looking to create a flexible, cloud-based solution that consolidates data and shares files globally while caching a subset in distributed locations, the following two components are required:
NetApp BlueXP edge caching Edge instances (A): This enables customers to create edge caches in distributed locations. The edge instances cache frequently accessed data locally, while the full data set remains in the central cloud storage. This setup optimizes performance for remote locations by reducing latency for cached data and improving access speeds.
NetApp Cloud Volumes ONTAP (D): Cloud Volumes ONTAP provides scalable and efficient cloud storage management for the customer's data. It supports global file sharing and allows for seamless integration with edge caching solutions. This component ensures that the data is centralized in the cloud and is available for caching to distributed locations using edge instances.
Flash Cache intelligent caching (B) is more relevant for on-premises storage performance rather than cloud-based solutions, and BlueXP copy and sync (C) is used for data migration or synchronization, but does not provide global file sharing or edge caching capabilities.

QUESTION 13
A company has an existing on-premises NetApp AFF array in their datacenter that is about to run out of storage capacity. Due to recent leadership changes, the company cannot add more storage capacity in the existing AFF array, because they need to move to cloud in 2 to 3 years. The current on-premises array contains a lot of cold data. The company needs to free some storage capacity on the existing on-premises AFF array relatively quickly, to support the new application.
Which NetApp BlueXP service should the company use to meet this requirement?

A. BlueXP tiering
B. BlueXP backup and recovery
C. BlueXP replication
D. BlueXP copy and sync

Correct Answer: A
Section:
Explanation:
In this scenario, the company needs to quickly free up storage capacity on its on-premises NetApp AFF array, especially since much of the data is cold. The best solution is BlueXP tiering (formerly Cloud Tiering), which moves infrequently accessed (cold) data from the high-performance on-premises storage to more cost-effective cloud storage.
By automatically tiering cold data to the cloud, BlueXP tiering enables the company to free up space on their existing AFF array without additional on-premises hardware, and it prepares them for a future cloud migration. This process can be implemented quickly and efficiently to meet their immediate storage needs.
Other options like BlueXP backup and recovery (B), BlueXP replication (C), and BlueXP copy and sync (D) are focused on data protection, replication, and synchronization, but they do not directly address the need to free up on-premises storage space.

QUESTION 14
A company is configuring NetApp Cloud Volumes ONTAP in Azure. All outbound Internet access is blocked by default. The company wants to allow outbound Internet access for the following NetApp AutoSupport endpoints:

* https://support.netapp.com/aods/asupmessage
* https://support.netapp.eom/asupprod/post/l.O/postAsup
Which type of traffic must be requested to allow access?

A. routing and firewall policy to allow HTTPS traffic
B. routing and firewall policy to allow NFS/SMB traffic
C. routing and firewall policy to allow SSH/RDP traffic
D. routing and firewall policy to allow DNS traffic

Correct Answer: A
Section:
Explanation:
NetApp AutoSupport requires outbound access to specific endpoints for delivering support data, and this communication occurs over HTTPS (port 443). The two provided NetApp AutoSupport URLs are accessed via secure HTTP (HTTPS), so the company must configure routing and firewall policies to allow outbound HTTPS traffic.
Blocking HTTPS traffic by default would prevent the AutoSupport service from functioning, which is critical for sending diagnostic information to NetApp support for monitoring and troubleshooting.
Options like NFS/SMB traffic (B), SSH/RDP traffic (C), and DNS traffic (D) are irrelevant in this context, as AutoSupport only requires secure web traffic via HTTPS.

QUESTION 15
A customer has different on-premises workloads with a need for less than 2ms latency.
Which two service levels in NetApp Keystone storage as a service (STaaS) does the customer need? (Choose two.)

A. Extreme
B. Standard
C. Premium
D. Performance

Correct Answer: A, C
Section:
Explanation:
NetApp Keystone Storage as a Service (STaaS) offers various service levels depending on performance and latency requirements. For workloads that require less than 2ms latency, the two relevant service levels are:
Extreme (A): This service level is designed for the most latency-sensitive and high-performance workloads. It provides ultra-low latency (<2ms) and is ideal for applications that demand top-tier performance.
Premium (C): The Premium service level also supports low latency, typically less than 2ms, making it suitable for workloads with moderate to high performance requirements.
Standard (B) and Performance (D) service levels provide higher latency and are not suitable for workloads requiring less than 2ms latency.

QUESTION 16
How should a customer monitor the operations that NetApp BlueXP performs?

A. NetApp Cloud Insights
B. NetApp Active IQ Unified Manager
C. Notification Center
D. NetApp BlueXP digital advisor

Correct Answer: C
Section:
Explanation:
The Notification Center within NetApp BlueXP is the primary tool used to monitor operations and activities performed by the platform. It provides real-time updates and alerts about tasks, performance issues, and general operational statuses. This central hub helps administrators track the ongoing processes and health of the system, including tasks like data replication, backups, and other key operational events.
While NetApp Cloud Insights (A) provides infrastructure monitoring and analytics, it is not specifically focused on the operational monitoring of NetApp BlueXP activities. NetApp Active IQ Unified Manager (B) focuses more

on managing ONTAP environments but not directly on BlueXP operations. NetApp BlueXP digital advisor (D) offers recommendations and insights, but it is not primarily a monitoring tool.
==========

QUESTION 17
A customer is implementing NetApp StorageGRID with an Information Lifecycle Management (ILM) policy. Which key benefit should the customer expect from using ILM policies in this solution?

A. improved data security
B. automated data optimization
C. real-time data analytics capabilities
D. simplified data access controls

Correct Answer: B
Section:
Explanation:
NetApp StorageGRID's Information Lifecycle Management (ILM) policies offer the key benefit of automated data optimization. ILM policies enable the system to automatically manage data placement and retention across different storage tiers and locations based on factors such as data age, usage patterns, and performance requirements. This ensures that frequently accessed data is placed on high-performance storage, while older or less critical data can be moved to lower-cost storage, optimizing resource use and reducing costs.
While ILM policies can contribute to improved data security (A) and simplified data access controls (D), their primary focus is on optimizing data storage over its lifecycle. Real-time data analytics capabilities (C) are not a core feature of ILM policies.

QUESTION 18
A customer is setting up NetApp Cloud Volumes ONTAP for a general-purpose file share workload to ensure data availability.
Which action should the customer focus on primarily?

A. enabling compression
B. enabling encryption
C. implementing backup
D. tiering inactive data

Correct Answer: C
Section:
Explanation:
When setting up NetApp Cloud Volumes ONTAP for a general-purpose file share workload, the primary focus should be on implementing backup to ensure data availability. Backups are essential to protect data from accidental deletion, corruption, or catastrophic failures. Implementing a solid backup strategy ensures that, in the event of an issue, the data can be recovered and made available again quickly.
While compression (A) and encryption (B) are important features for storage efficiency and data security, they do not directly address data availability. Tiering inactive data (D) helps optimize costs but is not a primary concern for ensuring availability in the event of a failure or loss.

QUESTION 19
A company wants a cost-effective storage solution to migrate their VMware environment from on-premises to Azure using Azure VMware Solution. Their current workload requires more storage than compute.
Which datastore storage solution should the company use?

A. Azure NetApp Files
B. Azure Files
C. Amazon FSx for NetApp ONTAP
D. Cloud Volumes ONTAP in Azure

Correct Answer: A
Section:

Explanation:
For a company migrating a VMware environment to Azure using Azure VMware Solution (AVS), and where the workload requires more storage than compute, Azure NetApp Files is the most suitable datastore storage solution. Azure NetApp Files offers high performance, scalability, and is fully integrated with Azure, making it ideal for large-scale workloads that require extensive storage capacity but less compute.
Azure Files (B) is generally not sufficient for high-performance VMware workloads, and Amazon FSx for NetApp ONTAP (C) is an AWS-based solution, not an Azure-compatible service. Cloud Volumes ONTAP (D) in Azure can be used for certain storage needs, but Azure NetApp Files (A) provides better performance and is specifically optimized for AVS.

QUESTION 20
A customer wants to back up on-premises data to Google by using NetApp BlueXP backup and recovery. What is the first step that is required to implement the backup solution?

A. Create a Google Cloud bucket.
B. Enable NetApp Cloud Volumes Service.
C. Install NetApp BlueXP Connector.
D. Install an Acquisition Unit.

Correct Answer: C
Section:
Explanation:
The first step in implementing NetApp BlueXP backup and recovery for backing up on-premises data to Google Cloud is to install the NetApp BlueXP Connector. The Connector acts as a central management component that facilitates communication between your on-premises storage and the cloud storage provider (Google Cloud in this case). It is a key part of the BlueXP infrastructure and is essential for managing backups, replication, and tiering to the cloud.
Creating a Google Cloud bucket (A) is necessary but not the first step. NetApp Cloud Volumes Service (B) is used for different scenarios, not specifically for backups. Installing an Acquisition Unit (D) is related to monitoring and gathering data for systems like Cloud Insights, not for the BlueXP backup process.

QUESTION 21
Which two widget types are available when creating dashboards in NetApp Cloud Insights? (Choose two.)

A. machine learning
B. VMware
C. note
D. single value

Correct Answer: C, D
Section:
Explanation:
When creating dashboards in NetApp Cloud Insights, two of the available widget types are:
Note (C): This widget allows users to add explanatory text or annotations to the dashboard. It helps provide context or details regarding the displayed metrics or data.
Single Value (D): This widget is used to display a single metric or value prominently. It is useful for tracking specific KPIs or performance metrics in a simple and easy-to-read format.
Machine learning (A) is not a widget type; rather, it is a feature that Cloud Insights uses to provide intelligent insights from collected data. VMware (B) is not a widget but can be a data source that Cloud Insights monitors.

QUESTION 22
A customer has an AFF MetroCluster IP configuration and needs to tier cold data to the public cloud. Which NetApp replication option must the customer use for the capacity tier?

A. FabricPool mirror
B. BlueXP copy and sync
C. BlueXP replication
D. SyncMlrror

Correct Answer: A

Section:
Explanation:
For an AFF MetroCluster IP configuration, the customer should use FabricPool mirror to tier cold data to the public cloud. FabricPool is a feature of ONTAP that allows automatic tiering of cold or inactive data from high-performance AFF (All-Flash FAS) systems to a lower-cost cloud-based object storage. It is designed to extend the capacity of on-premises systems by tiering cold data to cloud storage, reducing the need for additional local storage.
Other options like BlueXP copy and sync (B) and BlueXP replication (C) are related to data replication and migration, not specifically tiering of inactive data. SyncMirror (D) is a high-availability feature used for synchronous replication, not for cloud tiering.

QUESTION 23
A customer has an on-premises NetApp ONTAP based system with data from several workloads. The customer wants to create a backup of their on-premises data to Microsoft Azure Blob storage.
Which two of the customer's on-premises data sources are supported with NetApp BlueXP backup and recovery? (Choose two.)

A. Microsoft SQL Server
B. NetApp ONTAP volume data
C. Microsoft Azure Stack
D. NetApp ONTAP S3 data

Correct Answer: B, D
Section:
Explanation:
NetApp BlueXP (formerly Cloud Manager) provides a comprehensive backup and recovery solution that supports various data sources. For customers looking to back up their on-premises data to Microsoft Azure Blob storage, the following data sources are supported:
NetApp ONTAP Volume Data: BlueXP backup and recovery can efficiently back up volumes created on NetApp ONTAP systems. This is a primary use case, ensuring that on-premises ONTAP environments can be backed up securely to cloud storage like Azure Blob, which offers scalability and cost-efficiency.
NetApp ONTAP S3 Data: NetApp ONTAP supports object storage using the S3 protocol, and BlueXP can back up these S3 buckets to cloud storage as well. This allows for a seamless backup of object-based workloads from ONTAP systems to Azure Blob.
Microsoft SQL Server and Azure Stack are not directly supported by NetApp BlueXP backup and recovery, as it focuses specifically on ONTAP environments and data sources.

QUESTION 24
A customer wants to lower their TCO using a cloud solution to reduce their expenditure for on-premises third-party storage.
Which NetApp solution should the customer use?

A. BlueXP tiering
B. BlueXP backup and recovery
C. BlueXP copy and sync
D. BlueXP replication

Correct Answer: A
Section:
Explanation:
NetApp BlueXP tiering is the ideal solution for reducing total cost of ownership (TCO) by leveraging cloud storage. It enables automatic tiering of infrequently accessed data (cold data) from expensive on-premises storage to lower-cost object storage in the cloud (such as Azure Blob, AWS S3, or Google Cloud Storage). This reduces the need for high-performance, high-cost local storage for data that isn't frequently accessed, effectively lowering the overall storage costs.
By migrating cold data to more economical cloud storage tiers, BlueXP tiering helps organizations optimize their storage spend, thus reducing TCO for their on-premises third-party storage infrastructure.
Other solutions like BlueXP backup and recovery, copy and sync, and replication provide different services (such as data protection, data migration, and disaster recovery) but are not focused on cost reduction through tiering, which specifically helps reduce TCO.

QUESTION 25
A customer is looking to implement NetApp StorageGRID in a high-availability (HA) environment. Which benefit can the customer expect?

A. the use of virtual IP addresses (VIPs)
B. zero data loss in case of a catastrophic failure
C. the ability to focus on optimizing data retrieval speed.
D. a single instance of the system for redundancy

Correct Answer: A
Section:
Explanation:
NetApp StorageGRID provides high availability (HA) by leveraging several key technologies, and one of the primary benefits in an HA environment is the use of virtual IP addresses (VIPs). In a high-availability configuration, StorageGRID uses VIPs to ensure continuous access to the service, even if one of the StorageGRID nodes becomes unavailable.
By using VIPs, StorageGRID ensures that requests to the system can be dynamically rerouted to an available node, providing seamless failover and reducing downtime in the case of node failures. This ensures that clients continue to connect without disruptions, contributing to the overall resilience and availability of the environment.
While options like zero data loss (B) are important, they are not guaranteed in every failover scenario without a well-designed backup or data replication system. Focusing on data retrieval speed (C) or single-instance redundancy (D) doesn't directly pertain to how NetApp StorageGRID handles high availability.

QUESTION 26
A company wants to save on AWS infrastructure costs for NetApp Cloud Volumes ONTAP. They want to tier to Amazon Simple Storage Service (Amazon S3).
What is the best way for the company to create a connection to S3 without incurring egress charges?

A. peering
B. gateway endpoint
C. AWS PrivateLink
D. network address translation (NAT) device

Correct Answer: B
Section:
Explanation:
When setting up NetApp Cloud Volumes ONTAP to tier to Amazon S3, minimizing infrastructure costs, especially egress charges, is critical. The best way to create a connection to S3 without incurring egress charges is by using an AWS gateway endpoint.
Gateway endpoints enable a private connection between Amazon S3 and your Amazon Virtual Private Cloud (VPC), eliminating the need for internet-based routing, which would incur data transfer charges (egress fees). With this private connection, data is transferred directly between the VPC and S3 without crossing the public internet, thus avoiding egress costs.
Other options such as peering and PrivateLink are viable for connecting VPCs but do not specifically address the elimination of egress charges when connecting to S3. A NAT device is also unnecessary for this scenario and would not eliminate egress charges but could instead introduce additional costs. Therefore, the gateway endpoint is the most cost-effective and direct method for achieving the desired outcome.

QUESTION 27
A large life sciences customer wants to deploy Azure VMware Solution. They use Azure NetApp Files for high performance and closer access to their application within the EAST US region, instead of using the Azure VMware Solution reserved capacity.
Which two options does this customer need in their design topology? (Choose two.)

A. ensuring that the Azure VMware Solution and Azure NetApp Files volumes are in the Availability Zone
B. using a dark site and ensuring total security
C. choosing the Azure UltraPerformance Gateway and enabling Azure ExpressRoute FastPath.
D. using a single public IP address for all virtual machines

Correct Answer: A, C
Section:
Explanation:

In this scenario, the life sciences customer is looking to deploy Azure VMware Solution (AVS) while leveraging Azure NetApp Files for high performance and proximity to their applications in the EAST US region. The two critical components to consider in this design are:
Ensuring that the Azure VMware Solution and Azure NetApp Files volumes are in the same Availability Zone (A): This is crucial to reduce latency and ensure optimal performance for high-performance workloads. Placing both AVS and Azure NetApp Files in the same zone ensures that data access is faster and more efficient due to reduced network hops and minimal latency.
Choosing the Azure UltraPerformance Gateway and enabling Azure ExpressRoute FastPath (C): To further optimize performance and provide dedicated, low-latency connectivity between AVS and Azure NetApp Files, using ExpressRoute with FastPath and the UltraPerformance Gateway ensures high bandwidth and lower network latencies. FastPath enables direct traffic flow between the on-premises network and the virtual network hosting AVS, bypassing the need for extra routing hops, thus improving performance.
Using dark sites (B) or public IP addresses (D) is not relevant in this case, as they do not contribute to performance optimization or the integration of Azure NetApp Files and AVS in the same region.