

NetworkAppliance.NS0-304.v2024-09-30.q22

Exam Code:	NS0-304
Exam Name:	Hybrid Cloud - Administrator Exam
Certification Provider:	Network Appliance
Free Question Number:	22
Version:	v2024-09-30
# of views:	346
# of Questions views:	220
https://www.exam-tests.com/NS0-304-exam/NetworkAppliance.NS0-304.v2024-09-30.q22.html	

NEW QUESTION: 1

An administrator must configure SVM-DR between two instances of Cloud Volumes ONTAP (CVO); one is deployed in Azure, and the other in AWS.

What must be configured to enable replication traffic between the two CVO instances?

- A. Internet Gateway
- B. Direct Connect
- C. ExpressRoute
- D. Virtual Private Network

Answer: D (LEAVE A REPLY)

To enable replication traffic between two instances of Cloud Volumes ONTAP (CVO) deployed in Azure and AWS, a Virtual Private Network (VPN) must be configured. This setup is crucial because it provides a secure and private communication channel over the internet, which is necessary for the replication of data between different cloud providers. Here's the process:

* Setup VPN Connection: Establish a VPN connection between the Azure and AWS environments. This involves configuring VPN gateways in both clouds to enable encrypted traffic flow between the two instances of CVO.

* Configure Network Routing: Ensure that the routing rules are set to direct the replication traffic through the VPN connection. This might include setting up appropriate route tables that point to the VPN gateway.

* Test and Verify Connectivity: After setting up the VPN, conduct tests to verify that the replication traffic is flowing correctly and securely between the two cloud environments.

Using a VPN is the most straightforward and typically the most cost-effective method to securely link AWS and Azure for the purpose of data replication, without the need for direct connectivity services like AWS Direct Connect or Azure ExpressRoute, which are more complex and costly solutions.

For guidance on setting up VPNs between AWS and Azure, refer to the respective cloud provider's documentation on VPN configuration.

NEW QUESTION: 2

How many private IP addresses are required for an HA CVO configuration in AWS using multiple Availability Zones?

- A. 15
- B. 13
- C. 6
- D. 12

Answer: B (LEAVE A REPLY)

In an HA (High Availability) Cloud Volumes ONTAP (CVO) configuration within AWS that spans multiple Availability Zones, a total of 13 private IP addresses are required. This includes IP addresses for various components such as management interfaces, data LIFs (Logical Interfaces), and intercluster LIFs for both nodes in the HA pair. The distribution of these IP addresses ensures redundancy and failover capabilities across the Availability Zones, which is essential for maintaining high availability and resilience of the storage environment.

References:

* NetApp Hybrid Cloud Administrator Course Material (HA Configuration in AWS module)

* NetApp Learning

Center:https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/leclassview/dowbt-00368390

NEW QUESTION: 3

Which two network connections are required by the Connector to enable Cloud Tiering from on-premises to a public cloud? (Choose two.)

- A. An HTTPS connection to the ONTAP cluster management LIF
- B. An SSH connection to the ONTAP cluster management LIF
- C. An inbound Internet connection to the Cloud Tiering service
- D. An outbound Internet connection to the Cloud Tiering service

Answer: A,D (LEAVE A REPLY)

To enable Cloud Tiering from on-premises to a public cloud, the Connector requires two specific network connections:

* HTTPS Connection to ONTAP Cluster Management LIF: This connection allows the Connector to communicate securely with the management interface of the ONTAP cluster. It's essential for managing storage operations and configuring cloud tiering.

* Outbound Internet Connection to the Cloud Tiering Service: This is necessary for the Connector to reach the Cloud Tiering service hosted in the cloud. It ensures that data can be moved between the on-premises environment and the cloud tiering service, facilitating storage tiering operations.

These connections ensure that the on-premises systems can effectively interact with cloud services, maintaining operational continuity and enabling efficient data management.

For additional information on setting up network connections for Cloud Tiering, you can refer to the NetApp Cloud Tiering documentation: [NetApp Cloud Tiering Documentation](#).

NEW QUESTION: 4

How many VPCs are required to deploy CVO in Google Cloud?

- A. 4
- B. 6
- C. 2
- D. 3

Answer: C ([LEAVE A REPLY](#))

To deploy Cloud Volumes ONTAP (CVO) in Google Cloud, typically two Virtual Private Clouds (VPCs) are required. This configuration generally involves:

- * A VPC for the management of CVO operations, handling management traffic, control plane operations, and other administrative activities.
- * A VPC dedicated to data traffic, ensuring data security and optimal network performance for storage operations.

This dual-VPC architecture helps in isolating management operations from data operations, providing enhanced security and performance. The management VPC can handle tasks like software updates and system monitoring, while the data VPC focuses purely on serving storage requests, thereby optimizing traffic flows and security policies accordingly.

For more detailed deployment instructions and VPC configuration guidelines, the official NetApp documentation on deploying Cloud Volumes ONTAP in Google Cloud provides comprehensive guidance.

NEW QUESTION: 5

An administrator needs to monitor their storage and compute resources in their hyperscaler and their private data center. Which tool meets this requirement?

- A. SPOT by NetApp
- B. Active IQ Digital Advisor
- C. BlueXP Observability
- D. BlueXP Classification

Answer: ([SHOW ANSWER](#))

To monitor storage and compute resources across both a hyperscaler and a private data center, BlueXP Observability is the appropriate tool. This part of the BlueXP suite offers a unified view of infrastructure health, performance, and capacity. Here's the benefit of using BlueXP Observability:

- * **Unified Monitoring:**BlueXP Observability provides a single pane of glass for monitoring resources, regardless of their location-whether in the cloud or on-premises. This includes real-time data on performance, capacity utilization, and system health.
- * **Cross-Environment Support:**It supports various environments, making it suitable for hybrid deployments. This capability allows administrators to have a holistic view of their entire infrastructure.
- * **Alerts and Metrics:**The tool offers customizable alerts and detailed metrics that help in proactive management and troubleshooting of storage and compute resources.

BlueXP Observability's extensive capabilities in monitoring and managing diverse IT environments make it an ideal choice for enterprises that operate across multiple platforms.

For more information on how to utilize BlueXP Observability for infrastructure monitoring, refer to the NetApp BlueXP documentation: [NetApp BlueXP Documentation](#).

NEW QUESTION: 6

An administrator sets up BlueXP Observability to monitor their hybrid cloud environment. After configuring the necessary data collectors, the administrator observes discrepancies in their topology view.

What should the administrator do?

- A. Upgrade the subscription
- B. Perform device resolution
- C. Add an Acquisition Unit
- D. Create a custom dashboard

Answer: B ([LEAVE A REPLY](#))

When discrepancies are observed in the topology view of BlueXP Observability, the likely cause is related to incomplete or inaccurate data collection. Performing device resolution helps in identifying and correcting any mismatches or errors in the device information being collected. This process ensures that all devices are correctly identified and their relationships accurately represented in the topology view. This step is crucial for maintaining the integrity and accuracy of the monitoring data.

References:

* NetApp Hybrid Cloud Administrator Course Material (BlueXP Observability module)

* NetApp Learning

Center:<https://learningcenter.netapp.com/LC?ObjectType=WBT&ObjectID=00371904>

NEW QUESTION: 7

When deploying CVO, which two network types are used in HA configurations? (Choose two.)

- A. Intracluster
- B. iWARP
- C. Transit Gateway
- D. Intercluster

Answer: A,D ([LEAVE A REPLY](#))

When deploying Cloud Volumes ONTAP (CVO) in a High Availability (HA) configuration, two critical network types are used:

* Intracluster: This network type is used for communication within the same cluster, particularly between nodes within the same HA pair. It is crucial for the synchronization and coordination of operations that support the cluster's internal processes and data management.

* Intercluster: This network type facilitates communication between different clusters or between nodes across different data centers or geographical locations. It is typically used for data replication and disaster recovery purposes, ensuring data continuity and availability across diverse environments.

Understanding and configuring these network types correctly is essential for maintaining high availability and ensuring robust disaster recovery in CVO deployments.

For more details on network configuration in CVO HA setups, refer to the NetApp documentation on network management for Cloud Volumes ONTAP: NetApp CVO Network Documentation.

NEW QUESTION: 8

An administrator deploys an FSx NetApp ONTAP in AWS as an archive destination. Which feature must be disabled?

- A. Compression
- B. Daily automatic backup
- C. Deduplication
- D. Capacity pool tiering policy

Answer: (SHOW ANSWER)

When deploying an FSx NetApp ONTAP in AWS as an archive destination, the daily automatic backup feature must be disabled. This is because the primary purpose of an archive destination is to store data that is infrequently accessed and does not require regular backups. Disabling daily automatic backups helps in reducing unnecessary storage costs and resource usage associated with maintaining daily backups of archival data.

References:

* NetApp Hybrid Cloud Administrator Course Material (FSx NetApp ONTAP module)

* NetApp Learning

Center:https://netapp.sabacloud.com/Saba/Web_spf/NA1PRD0047/common/leclassview/dowbt-00368390

NEW QUESTION: 9

An administrator is configuring a Red Hat Enterprise Linux system as a Workload Security Agent and wants to make sure that it meets requirements.

Which two changes should the administrator make to the system? (Choose two.)

- A. Disable SELinux
- B. Install the ansible-core application
- C. Disable the system firewall
- D. Install the unzip application

Answer: A,D (LEAVE A REPLY)

When configuring a Red Hat Enterprise Linux system as a Workload Security Agent, there are specific system requirements and preparations needed to ensure compatibility and functionality of the security agent. Among the potential adjustments:

* Disable SELinux: Security-Enhanced Linux (SELinux) can interfere with the operation of various security agents due to its strict access controls. Disabling SELinux may be recommended by certain security applications to ensure they can function without restrictions. This should be carefully considered in the context of overall system security policies.

* Install the unzip application: Many security agents requireunzip to extract and install necessary files. Ensuring thatunzip is installed on the system can facilitate the installation and updating of the security agent.

Install the ansible-core application and Disable the system firewall are not typically required or recommended universally for configuring a Workload Security Agent:

* Ansible-core is used for automation and configuration management but is not a prerequisite for most security agents unless specifically stated.

* Disabling the system firewall can significantly reduce the system's security posture and is generally not advisable unless specifically required by the security agent, and even then, such advice should be critically evaluated.

For specific guidelines and requirements, the installation documentation of the Workload Security Agent should be consulted.

NEW QUESTION: 10

Which feature of BlueXP Analysis and Control is used to uncover risk factors, and identify opportunities to improve system security?

- A. Observability
- B. Ransomware protection
- C. Digital Advisor
- D. Classification

Answer: C (LEAVE A REPLY)

The feature of BlueXP Analysis and Control used to uncover risk factors and identify opportunities to improve system security is the Digital Advisor. Here's why:

* Role of Digital Advisor: Digital Advisor provides analytics, insights, and actionable intelligence based on the data gathered from the NetApp environment. It helps administrators identify potential risks, security vulnerabilities, and operational inefficiencies.

* Security and Risk Analysis: By analyzing performance metrics, configuration details, and other critical data, Digital Advisor can pinpoint areas where security improvements are needed and suggest best practices for system optimization.

* Benefits of Using Digital Advisor: This tool aids in proactive management of the storage environment, ensuring that security measures are not only reactive but preventive, providing recommendations to mitigate potential threats before they impact the system.

For further details on how to utilize Digital Advisor for security improvements, visit the NetApp BlueXP documentation: [NetApp Digital Advisor Documentation](#).

NEW QUESTION: 11

An administrator is using the NetApp BlueXP API to perform actions within an CI/CD process. What information is needed for authentication?

- A. API endpoint and Java web token
- B. API endpoint and API token
- C. API endpoint and username/password
- D. API endpoint with bearer token

Answer: D (LEAVE A REPLY)

For authenticating with the NetApp BlueXP API, particularly within a CI/CD process, you will need the API endpoint and a bearer token. Here's why this is important:

- * **API Endpoint:**The API endpoint is the URL where the API requests are sent. It serves as the access point for the BlueXP services.
- * **Bearer Token:**A bearer token is a type of access token that is often used in OAuth 2.0 authentication. It must be included in the header of each API request to authenticate and authorize the request. This token ensures that the person or system making the API request has the correct permissions.
- * **Setup Authentication:**To set up authentication, you must first obtain a bearer token, typically through a login API endpoint that provides this token after verifying your credentials. Subsequently, include this token in the "Authorization" header of your API requests.

For more information on using APIs with NetApp BlueXP, including obtaining and using bearer tokens, refer to the NetApp BlueXP API documentation: [NetApp API Documentation](#).

NEW QUESTION: 12

Refer to the exhibit.



The administrator wants to replicate all the data from their On-Premises ONTAP to Cloud Volumes ONTAP.

What should the administrator do first?

- A.** Drag and Drop Cloud Volumes ONTAP to On-Premises
- B.** Drag and Drop On-Premises to Cloud Volumes ONTAP
- C.** Add a third Working Environment with a Data Broker
- D.** Update the Cloud Volumes ONTAP License from Freemium to Essentials

Answer: B (LEAVE A REPLY)

To replicate all data from an On-Premises ONTAP to Cloud Volumes ONTAP, the first step within the BlueXP (formerly NetApp Cloud Manager) interface is to establish a replication relationship. Here's how:

- * **Setup Data Replication:**In the BlueXP interface, drag and drop the On-Premises ONTAP environment onto the Cloud Volumes ONTAP environment. This action initiates the setup of a SnapMirror relationship, where the on-premises system acts as the source, and the cloud volumes serve as the destination.
- * **Configure Replication Settings:**After dragging and dropping, you will be prompted to configure the replication settings, including schedules, policies, and the volumes to be replicated.
- * **Initiate and Monitor Replication:**Once the configuration is completed, start the replication process.

BlueXP provides tools to monitor the status and health of the replication, ensuring data is synchronized according to the defined settings.

This method leverages the integrated tools in BlueXP to simplify the management of hybrid cloud environments and ensures data continuity between on-premises and cloud-based systems.

For detailed instructions and best practices on setting up SnapMirror with BlueXP, refer to the NetApp documentation: [NetApp SnapMirror Documentation](#).

NEW QUESTION: 13

A company is setting up FlexCache in CVO to scale-out an on-premises system. What should the administrator do on the on-premises system?

- A. Create a new volume as a cache
- B. Generate cluster peering passphrase
- C. Configure NFS export policies
- D. Apply a FlexCache license

Answer: B ([LEAVE A REPLY](#))

When setting up FlexCache in Cloud Volumes ONTAP (CVO) to scale out an on-premises system, the critical first step on the on-premises system is to generate a cluster peering passphrase. This passphrase is used to establish a secure cluster peering relationship between the on-premises ONTAP system and the CVO in the cloud. Here's the process:

- * **Cluster Peering Setup:** Cluster peering is essential for FlexCache because it allows the on-premises system to communicate and share data with the CVO instance. The cluster peering passphrase is used to authenticate the peering session, ensuring security.
- * **Generate the Passphrase:** In the ONTAP system manager on the on-premises cluster, navigate to the cluster peering settings and generate or configure the passphrase that will be used for peering with the CVO.
- * **Establish Peering:** Once the passphrase is set, use it to create the cluster peer relationship from the on-premises ONTAP to the CVO, following the guided steps in ONTAP System Manager or using CLI commands.

For detailed instructions on setting up cluster peering for FlexCache, refer to the NetApp documentation on FlexCache and cluster peering: [NetApp FlexCache Documentation](#).

NEW QUESTION: 14

An outbound Internet connection is not available to send AutoSupport messages. BlueXP has automatically configured the Cloud Volumes ONTAP systems to use the Connector as a proxy server. The Connector requires an inbound connection on port 3128.

What must the administrator do?

- A. Modify the policy on the cluster-mgmt LIF
- B. Add the Internet gateway IP to the allow list
- C. Configure BlueXP with an external IP address
- D. Modify the associated security group

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 15

An administrator tries to deploy an SMB volume in Azure NetApp Files in the same region as their AD DS.

The deployment fails with the following error message:

```
{ "code": "DeploymentFailed", "message": "At least one resource deployment operation failed. Please list deployment operations for details. Please see https://aka.ms/DeployOperations for usage details.", "details": [ { "code": "InternalServerError", "message": "Error when creating - Could not query DNS server. Verify that the network configuration is correct and that DNS servers are available." } ] }
```

What are two configuration options that must be verified? (Choose two.)

- A. The volume is in the same VNet.
- B. The Azure subscription has been activated.
- C. The Global Administrator role is configured.
- D. The Network Security Groups allows DNS traffic.

Answer: A,D (LEAVE A REPLY)

Based on the error message indicating an issue with querying the DNS server, two critical network-related configurations must be verified to successfully deploy an SMB volume in Azure NetApp Files:

* VNet Configuration: Ensure that the Azure NetApp Files volume and the Active Directory Domain Services (AD DS) are configured within the same Virtual Network (VNet). This is crucial as it ensures that the volume can communicate effectively with the AD DS, which is necessary for SMB authentication and service location.

* Network Security Group (NSG) Settings: Verify that the Network Security Groups associated with the subnet or the VNet where the Azure NetApp Files volume is deployed allows DNS traffic. Specifically, inbound and outbound rules should permit traffic over the ports typically used by DNS (usually TCP/UDP 53). This allows the volume to successfully resolve DNS queries which are essential for integrating with AD DS.

These two checks are aimed at resolving connectivity and DNS resolution issues that are likely causing the deployment to fail. For more detailed troubleshooting and setup instructions, please refer to Azure's official documentation on Network Security Groups and VNet configurations: [Azure Networking Documentation](#).

NEW QUESTION: 16

An administrator wants to automatically optimize their scale-out web application in GCP. Which product should the administrator use?

- A. Ocean
- B. Instaclustr
- C. Eco
- D. Elastigroup

Answer: D (LEAVE A REPLY)

To automatically optimize a scale-out web application in Google Cloud Platform (GCP), an administrator should consider using Elastigroup. This tool, offered by Spot by NetApp (formerly Spotinst), is designed to enhance cloud resource utilization by automatically scaling compute resources based on workload demands.

Here's why Elastigroup is suitable:

- * **Automatic Scaling:** Elastigroup dynamically manages your compute resources, scaling them up or down based on the application demands. This ensures that your application always has the right amount of resources without over-provisioning.
- * **Cost Optimization:** By intelligently leveraging spot instances along with on-demand and reserved instances, Elastigroup reduces costs without compromising application availability or performance.
- * **Integration with GCP:** Elastigroup seamlessly integrates with Google Cloud, making it straightforward to manage scaling policies directly within the cloud environment.

Elastigroup's capabilities make it an excellent choice for optimizing scale-out applications in cloud environments, particularly for managing the balance between performance, cost, and availability. For more information on using Elastigroup in GCP, visit the Spot by NetApp website or access their documentation directly: [Spot by NetApp - Elastigroup](#).

Valid NS0-304 Dumps shared by BraindumpsPass.com for Helping Passing NS0-304 Exam!

BraindumpsPass.com now offer the **newest NS0-304 exam dumps**, the BraindumpsPass.com NS0-304 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com NS0-304 dumps with Test Engine here:

<https://www.braindumpspass.com/NetworkAppliance/NS0-304-practice-exam-dumps.html> (141 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 17

An administrator configures the trident ontap-san driver and specifies useCHAP=true.

```
{  
  "version": 1,  
  "storageDriverName": "ontap-san",  
  "backendName": "ontap_san_chap",  
  "managementLIF": "192.168.0.135",  
  "svm": "ontap_iscsi_svm",  
  "useCHAP": true,  
  "username": "vsadmin",  
  "password": "FakePaSsWoRd",  
  "igroupName": "trident",  
  "chapInitiatorSecret": "cl9qxIm36DKyawxy",  
  "chapTargetInitiatorSecret": "rqxigXgkesIpwxyz",  
  "chapTargetUsername": "iJF4heBRT0TCwxyz",  
}
```

Which parameter is missing from the configuration?

- A. dataUF
- B. chapSecret
- C. clientPrivateKey
- D. chapUsername

Answer: (SHOW ANSWER)

When configuring the Trident ONTAP-SAN driver with CHAP (Challenge Handshake Authentication Protocol) enabled (useCHAP: true), it is essential to specify both the initiator and target CHAP secrets

and their corresponding usernames. In the configuration provided, while the CHAP secrets for both initiator and target are specified (chapInitiatorSecret and chapTargetInitiatorSecret), only the CHAP target username (chapTargetUsername) is listed. The missing parameter necessary for the complete CHAP configuration is the CHAP initiator username (chapUsername). This username is used along with thechapInitiatorSecretto authenticate the initiator to the storage system.

To correct this, add thechapUsernamefield to the configuration file, ensuring that the initiator's username matches the configured environment and that it is correctly paired with thechapInitiatorSecret. This inclusion ensures that both sides of the CHAP authentication process are properly identified, thereby providing the necessary security for SAN communication.

For further guidance on configuring CHAP with the Trident ONTAP-SAN driver, refer to the NetApp Trident documentation:NetApp Trident Documentation.

NEW QUESTION: 18

An administrator is configuring Cloud Volumes ONTAP (CVO). The CVO instance does not have outbound network connectivity to send AutoSupport messages.

What will BlueXP automatically configure as the proxy server for AutoSupport?

- A. Page blob
- B. Mediator
- C. Collector
- D. Connector

Answer: D (LEAVE A REPLY)

In a scenario where a Cloud Volumes ONTAP (CVO) instance lacks outbound network connectivity to send AutoSupport messages, BlueXP (formerly known as NetApp Cloud Manager) will automatically configure the Connector as the proxy server for AutoSupport. The Connector serves as a bridge between the customer's environment and NetApp cloud services, facilitating communication and data transfer, including AutoSupport messages, when direct connectivity is unavailable.

* Page blobis a type of storage in Azure, not related to network functions.

* MediatorandCollectorare not standard terms used within NetApp for describing components involved in managing or proxying AutoSupport messages.

BlueXP's configuration to use the Connector as a proxy ensures that all monitoring and telemetry data crucial for the health and performance diagnostics of the CVO instance are relayed effectively, even in environments with restrictive outbound network policies. More details on this setup can be explored in the BlueXP or Cloud Volumes ONTAP documentation available on NetApp's website.

NEW QUESTION: 19

ONTAP's Autonomous Anti-ransomware engine reports a potential ransomware attack. The administrator finds the majority of the files appear encrypted and disables the share.

What should the administrator do to minimize data loss?

- A. Create a FlexClone using the locked snapshot and re-enable the share
- B. Perform a SnapRestore using the weekly snapshot and re-enable the share
- C. Rehost the volume to a different SVM and create a new share

D. Take a manual snapshot and re-enable the share

Answer: B ([LEAVE A REPLY](#))

When dealing with a potential ransomware attack where files appear encrypted, it is crucial to restore the affected data to a point before the corruption occurred. The best course of action in this scenario is to perform a SnapRestore using a known good weekly snapshot and then re-enable the share. Here's how:

- * **Assess the Snapshots:** Verify that you have snapshots that predate the ransomware attack. These snapshots should be intact and free from encryption or corruption.
- * **Perform a SnapRestore:** Use the SnapRestore operation to quickly revert the entire volume to the state captured in the selected weekly snapshot. SnapRestore is efficient because it does not involve data movement; it simply reverts pointers in the filesystem.
- * **Re-enable the Share:** After successfully reverting the volume to a good state, the share can be safely re-enabled, allowing users to access the clean, restored data.
- * **Verify System Integrity and Security:** Before re-enabling the share, ensure that all system vulnerabilities are addressed to prevent future attacks. Implement improved security measures as needed.

For more details on using SnapRestore in ONTAP systems, refer to the NetApp documentation on data protection and recovery: [NetApp SnapRestore Documentation](#).

NEW QUESTION: 20

An administrator is preparing to automate firmware updates with the help of Active IQ Digital Advisor. Which automation tool should the administrator use?

- A.** Puppet
- B.** Terraform
- C.** Ansible
- D.** Pulumi

Answer: ([SHOW ANSWER](#)**)**

To automate firmware updates effectively using Active IQ Digital Advisor, the best tool to use is Ansible. Here's why:

- * **Ansible Integration with NetApp:** Ansible is widely recognized for its powerful automation capabilities across various IT environments. NetApp provides specific Ansible modules designed to interact with its storage solutions and services, including the automation of firmware updates.
- * **Active IQ Digital Advisor Integration:** Active IQ Digital Advisor offers predictive analytics, actionable intelligence, and proactive recommendations. By using Ansible, administrators can automate the implementation of these recommendations, including firmware updates, to enhance efficiency and reliability in operations.

To implement this, the administrator needs to leverage the NetApp Ansible modules that are specifically designed for storage management tasks. This can be found in the NetApp Automation Store, where administrators can access pre-built playbooks for firmware updates, simplifying the automation process. For further details and specific implementation steps, please refer to the NetApp Automation Store and the official NetApp documentation on Ansible integration: [NetApp Ansible Modules Documentation](#).

NEW QUESTION: 21

In an environment using Cloud Backup Service, a user reports that an urgently needed file cannot be found.

The end user knows the file name but does not know when the file was last accessed or when it was deleted.

Which feature should be used?

- A. Restore Volume
- B. Browse & Restore
- C. Search & Restore
- D. Previous Versions

Answer: C (LEAVE A REPLY)

In a situation where an end user needs to find and restore a file whose last access or deletion time is unknown, the best feature to use within the Cloud Backup Service is Search & Restore. Here's why:

- * Search Functionality: The Search & Restore feature allows users to quickly locate files within backup datasets using just the file name or other metadata. This is particularly useful when the exact details of the file, such as its last access date or deletion date, are unknown.
- * Efficient File Restoration: Once the file is located using the search functionality, it can be selectively restored to the desired location without the need to restore an entire volume, making the process efficient and tailored to the specific recovery need.
- * User-Friendly Interface: Cloud Backup Service typically provides a user-friendly interface for conducting searches and performing restores, making it accessible even to users who may not be deeply technical. For detailed instructions on using the Search & Restore feature in NetApp Cloud Backup Service, refer to the service's user guide or online help available at: [NetApp Cloud Backup Service Documentation](#).

NEW QUESTION: 22

A customer requires unlimited backups be included for their CVO instance. Which two subscription models should the customer use? (Choose two.)

- A. Professional
- B. Essentials
- C. Premium
- D. Optimized
- E. Edge Cache

Answer: B,C (LEAVE A REPLY)

For a customer requiring unlimited backups in their Cloud Volumes ONTAP (CVO) instance, the Essentials and Premium subscription models are the appropriate choices. Both these subscription models offer unlimited backups as part of their service package, which is ideal for customers who prioritize extensive backup capabilities without the concern of hitting limits.

The Professional, Optimized, and Edge Cache plans typically have different focuses or limitations concerning backup capabilities:

- * Professional: Geared more towards smaller or less critical deployments without the breadth of features found in Premium or Essentials.
- * Optimized: Often focuses on performance optimization rather than extensive backup functionalities.

* Edge Cache: Is used for caching services at the edge rather than core data management and backup functionalities.

Detailed information on these subscription models and their backup capabilities can be found in the NetApp Cloud Volumes ONTAP documentation or through consultation with NetApp sales representatives.

Valid NS0-304 Dumps shared by BraindumpsPass.com for Helping Passing NS0-304 Exam!
BraindumpsPass.com now offer the **newest NS0-304 exam dumps**, the BraindumpsPass.com NS0-304 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com NS0-304 dumps with Test Engine here:
<https://www.braindumpspass.com/NetworkAppliance/NS0-304-practice-exam-dumps.html> (141 Q&As
Dumps, **40%OFF** Special Discount: **Exam-Tests**)