Welcome to Cert007 - Your Ultimate IT Certification Partner

- Real Exam Questions
- Free Updates
- Expert Support
- Instant Access
- Money-Back Guarantee

Visit us at **https://www.cert007.com/** for more information

Exam : **NS0-304**

Title : NetApp Certified Hybrid Cloud Administrator

Version : DEMO

1.An administrator needs to back up their VMware virtual machines from on-premises AFF to AWS S3 using SnapCenter.
Which two requirements must be met to enable use of the SnapCenter Plug-in? (Choose two.)
A. The Plug-in must be installed on each VM.
B. The Plug-in must be registered with BlueXP.
C. The Plug-in must be installed in vCenter.
D. The Plug-in must register the S3 bucket.
Answer: B, C
Explanation:
To utilize the SnapCenter Plug-in for VMware vSphere to back up VMware virtual machines from on-premises AFF (All Flash FAS) systems to AWS S3, it's crucial to meet specific requirements:
Plug-in Installation in vCenter: The SnapCenter Plug-in for VMware vSphere must be installed directly within the VMware vCenter Server. This integration allows the plug-in to manage and coordinate the backup operations directly from the vCenter, providing centralized management and control over the backup processes.
Registration with BlueXP (formerly NetApp Cloud Manager): The plug-in must be registered with BlueXP. BlueXP serves as a unified control plane for orchestrating and managing NetApp’s hybrid cloud storage and data services. Registering the plug-in with BlueXP ensures it can communicate and operate seamlessly with other NetApp services, including storage orchestration to AWS S3.
These steps are designed to ensure the SnapCenter Plug-in operates effectively within the VMware environment and interacts correctly with NetApp's cloud data services, facilitating the backup process to AWS S3.
For more detailed guidance, reference the SnapCenter documentation available through the NetApp support site: NetApp SnapCenter Documentation.

2.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: C
Explanation:
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.

3.An administrator wants to migrate their SMB file server from on-premises to CVO using Cloud Sync. The NTFS ACLs need to be transferred.
What should the administrator do?
A. Select the "Copy Access Control Lists to the target" option in the DataBroker settings
B. Use the rsync command after the sync is complete
C. Select the "Copy Access Control Lists to the target" option in Cloud Sync
D. Create an SVM-DR relationship with "Identity preserve set to true"
Answer: C
Explanation:
To ensure a seamless migration of SMB file servers from on-premises environments to Cloud Volumes ONTAP (CVO) while preserving NTFS Access Control Lists (ACLs), the following steps should be followed using Cloud Sync:
Setting Up Cloud Sync: Initiate a new data sync relationship using the Cloud Sync service. This service is designed to simplify data migration across diverse environments, including on-premises to cloud migrations.
Preserving NTFS ACLs: During the setup process in Cloud Sync, select the option "Copy Access Control Lists to the target". This ensures that all NTFS ACLs associated with the files and directories are accurately replicated on the CVO system. This option is crucial for maintaining the security and access configurations that were in place on-premises.
Execute and Monitor the Migration: After configuring the settings, start the data migration process. Monitor the process via the Cloud Sync interface to ensure all data, including ACLs, is transferred without issues.
For more detailed instructions and best practices, refer to the NetApp Cloud Sync User Guide, which provides comprehensive steps and guidance on using Cloud Sync effectively: NetApp Cloud Sync User Guide.

4.An administrator wants to automate the configuration of SnapMirror policies between cloud and on-premises deployments in AWS using Ansible.
What must the administrator do first?
A. Set up AWS Control Tower for automation
B. Subscribe to Ansible Automation Platform
C. Install the ONTAP collection using Ansible Galaxy
D. Install the Ansible plugin for aws_ec2 inventory
Answer: C
Explanation:
To automate the configuration of SnapMirror policies between cloud and on-premises deployments in AWS using Ansible, the administrator needs to begin by installing the NetApp ONTAP collection from Ansible Galaxy. This collection contains modules specifically designed to manage NetApp ONTAP storage systems, including the management of SnapMirror configurations.
Here are the steps to do this:
Installation of ONTAP Collection: Open your command line interface and run the command ansible-

galaxy collection install netapp.ontap. This command pulls the ONTAP collection from Ansible Galaxy, which includes all necessary modules for managing NetApp ONTAP, including SnapMirror. Configuration of Ansible Environment: Ensure that your Ansible environment is set up to connect to both your AWS environment and the on-premises NetApp ONTAP systems. This typically involves configuring the appropriate credentials and network settings in your Ansible playbooks and inventory files.
Writing Ansible Playbooks: With the ONTAP collection installed, you can now write Ansible playbooks that utilize the SnapMirror modules to automate the configuration of SnapMirror policies as required.
For further information on using the NetApp ONTAP Ansible collection, please refer to the official documentation available at: NetApp ONTAP Ansible Collection Documentation.

5.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
Explanation:
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.