

Expert - Isilon Solutions Exam

EMC DEE-1421

Version Demo

Total Demo Questions: 9

Total Premium Questions: 92

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Isilon Scale-out NAS	7
Topic 2, Isilon Implementation	22
Topic 3, Isilon Administration	24
Topic 4, Isilon Data Protection	28
Topic 5, Isilon Troubleshooting	11
Total	92

QUESTION NO: 1

A company has a cluster with two subnets. The first subnet has 1 GbE interfaces dedicated for management and the second subnet has 10GbE interfaces dedicated for handling all data access. When the cluster started serving the production environment, poor performance was observed while the data is accessed through the data subnet. While troubleshooting the network, the administrator discovered that the return traffic is going through the management network.

Which recommended solution will resolve this issue?

- A. Change the gateway priorities
- B. Enable destination-based routing with static routes
- C. Enable source-based routing
- D. Configure static routes for both subnets

ANSWER: C

Explanation:

Enable source-based routing. In a multi-subnet PowerScale cluster, source-based routing makes route selection dependent on the source IP address selected for the outbound response. A client request that arrives through an address on the 10 GbE data network is therefore answered using a route associated with that data network, rather than being sent through the management network's preferred default gateway. This preserves symmetric traffic flow and keeps high-volume client data traffic on the interfaces designed to carry it.

Symmetric routing is particularly important when management and client networks have substantially different bandwidth and intended workloads. It avoids placing production response traffic onto the 1 GbE management interfaces, where congestion and throughput limitations can produce the reported poor performance. Source-based routing also provides a cluster-wide policy appropriate for hosts with interfaces on separate networks, rather than relying on an individual route to happen to match a destination. Configure and validate the policy alongside the cluster's IP-pool and gateway configuration, then confirm the selected routes from each relevant source address. Dell's PowerScale documentation is available through the [OneFS product documentation portal](#); see also Dell's [PowerScale Info Hub](#) for OneFS networking guidance.

QUESTION NO: 2

Case Study 3

A financial services company has file sharing workflows and 2000 home directories which include 70% Microsoft Windows and 30% Linux. The Security team is also interested in credit card usage data analytics such as point of sale, geolocation, and authorization and transaction data. Home directories and file shares do not require D@RE or SEC compliance.

However, due to the sensitivity of the credit card data, the company requires D@RE for credit card information and must adhere to the U.S. SEC 17a-4(f) compliance standards. Additionally, they are interested in auditing user access and anti-virus features. The compute and storage environment consists of the following:

- 200 TB of Fibre Channel drives on NetApp ONTAP 7
- Environment is expected to grow 200 TB over the next three years

Which type of encryption is used in a D@RE-enabled Dell EMC Isilon cluster?

- A. 128-bit AES encryption key
- B. 256-bit AES encryption key
- C. 1024-bit SHA encryption key
- D. 2048-bit SHA encryption key

ANSWER: B

Explanation:

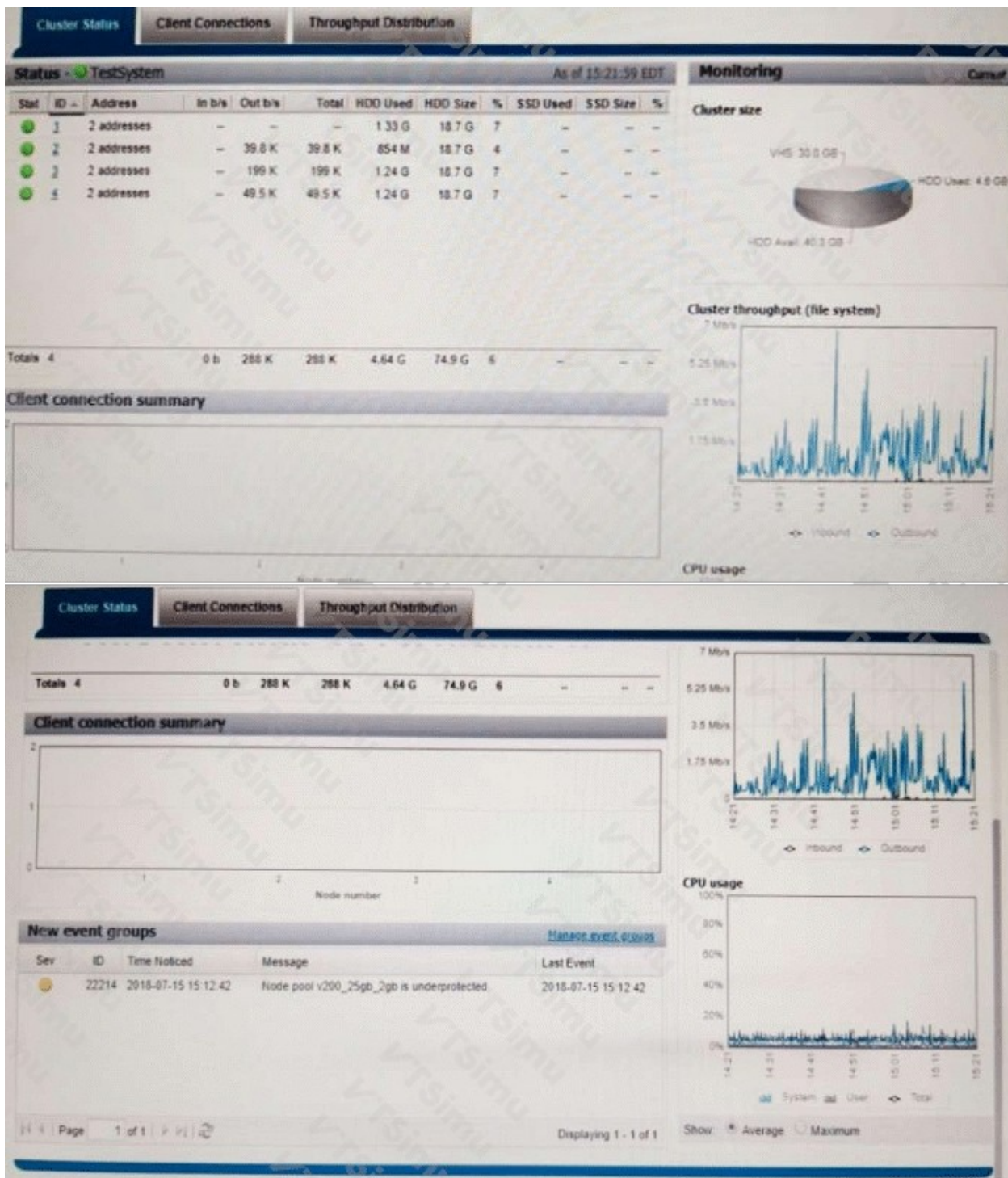
A D@RE-enabled Dell EMC Isilon (PowerScale) cluster uses 256-bit AES encryption to protect data at rest. OneFS Data-at-Rest Encryption encrypts the data stored on cluster drives, helping protect sensitive content if physical media is removed, lost, or accessed outside the normal cluster security controls. The cluster uses encryption keys as part of its key-management architecture; data-encryption keys are protected through wrapping and can be managed using the cluster's internal key manager or an external key-management service, depending on the OneFS configuration and deployment requirements.

AES is the appropriate cryptographic algorithm for this purpose because it is a symmetric encryption standard designed for confidentiality of stored data. AES supports several key lengths, including 256 bits, and the D@RE implementation uses the 256-bit variant. This provides the encryption strength expected for highly sensitive financial and payment-card information while allowing OneFS to deliver transparent storage access to authorized clients and services. Dell's OneFS documentation is available through the [Dell Technologies OneFS documentation portal](#). The underlying AES standard is defined by [NIST FIPS 197](#).

QUESTION NO: 3

You have been asked to design a Dell EMC Isilon cluster running OneFS 8.x for a service provider. One of the most critical areas to the provider is data segregation with multi-tenants. Use the "Launch Simulator" button to identify the current condition of the cluster: Note: It is necessary to "close" (x) the simulator window to answer the question.

Based on your findings, what is the cluster's current condition?



- A. All non-System Access zones are connected to the same groupnet, each with its own DNS server
- B. Each non-System Access zone is connected to an individual groupnet, each with its own DNS server
- C. All non-System Access zones are connected to the same groupnet with the same DNS server
- D. Each non-System Access zone is connected to an individual groupnet with the same DNS server.

ANSWER: B

Explanation:

Each non-System Access zone is connected to an individual groupnet, each with its own DNS server. In OneFS, an access zone provides logical separation for a tenant's authentication, identity mapping, protocol access, and client-facing configuration. A groupnet is the network-configuration container associated with an access zone and holds network-related services, including DNS configuration. The simulator's configuration shows that the non-System zones are each associated

with separate groupnets and that each groupnet has its own DNS-server setting. This arrangement provides the required network-service separation between tenants: DNS queries for one tenant zone are resolved using that tenant's designated DNS infrastructure rather than a shared groupnet DNS configuration. Separate groupnets are therefore an important part of preserving multi-tenant administrative and network isolation when distinct DNS domains or resolvers are required. The System zone remains the default administrative access zone and is not included in the stated non-System-zone condition. Dell's PowerScale documentation describes access zones and groupnets as the configuration objects used to segment client access and network services; see the [Dell PowerScale OneFS documentation portal](#) and the [Dell PowerScale OneFS best-practices guidance](#).

QUESTION NO: 4

A company must retain financial records on a Dell PowerScale cluster for seven years. The records must not be modified or deleted before the retention period expires, including by a privileged administrator.

Which SmartLock mode meets the requirement?

- A. SmartLock Compliance
- B. SmartLock Enterprise
- C. SnapshotIQ
- D. SmartQuotas

ANSWER: A

Explanation:

SmartLock Compliance is correct because SmartLock Compliance mode provides WORM protection intended for regulated retention requirements. After files are committed and their retention periods are set, they cannot be altered or deleted before expiration, including by privileged users. This provides the immutability required when administrative deletion must also be prevented.

SmartLock Enterprise mode supports retention controls but includes privileged-delete capabilities for authorized users. Organizations should select Compliance mode when the retention requirement prohibits deletion by administrators before the retention date. See the [Dell PowerScale OneFS SmartLock overview](#) and the [Dell PowerScale OneFS documentation](#) for SmartLock configuration guidance.

QUESTION NO: 5

Which protocol is used to send isi diagnostic gather logs from a Dell EMC Isilon cluster to Dell EMC Support when the ESRS gateway is unavailable?

- A. SCP
- B. HTTPS
- C. FTP
- D. FTPS

ANSWER: C

Explanation:

FTP is the supported fallback transport for sending an `isi_diagnostics_gather` archive to Dell EMC Support when the ESRS gateway cannot be used. The diagnostic gather process collects the cluster's logs and configuration information into a support archive. When a functioning ESRS connection is available, it provides the preferred secure path for support connectivity and delivery. If that gateway path is unavailable, OneFS support procedures use FTP to transfer the gathered archive to Dell's support upload service, allowing Dell Support to retrieve the material associated with the service request.

This distinction is important operationally: the protocol in this scenario describes the transfer mechanism used by the cluster's support-data submission workflow, rather than a general management protocol or an administrator-selected file-copy method. Administrators should ensure that the required outbound FTP connectivity is permitted when using this fallback and should provide the service-request details as directed by Dell Support so the uploaded diagnostic material can be matched to the case. Dell's OneFS documentation is available through the [Dell PowerScale OneFS manuals portal](#), and Dell's support workflow and service-request resources are available from [Dell Support](#).

QUESTION NO: 6

A company has an 8-node X410 installed as a single Dell EMC Isilon cluster. The company expressed concerns about cluster performance, particularly about NFS being slow. The output shown in the exhibit was presented to the Dell EMC technician.

Based on this output, what is a reason for the cluster performance issue?

# isi statistics protocol --nodes-all --limit 10 --long --protocols-nfs3															
Timestamp	NumOps	Ops	InMax	InMin	In	InAvg	TimeMax	TimeMin	TimeAvg	TimeStdDev	Node	Proto	Class	Op	
1526376786	937.0	161.8	27.3k	84.0	728.0k	4.5K	125484.0	449.0	13289.4	29986.6	1	nfs3	write	write	
1526376786	126.0	24.3	120.0	108.0	2.6k	108.2	1540.0	68.0	132.8	146.2	3	nfs3	namespace_read	getattr	
1526376786	50.0	8.6	124.0	104.0	974.1	112.8	174.0	72.0	111.7	28.5	1	nfs3	namespace_read	getattr	
1526376786	44.0	8.5	124.0	112.0	951.1	112.3	485.0	140.0	187.8	59.2	3	nfs3	namespace_read	access	
1526376786	37.0	7.1	120.0	104.0	781.1	109.6	447.0	86.0	141.8	76.5	8	nfs3	namespace_read	getattr	
1526376786	28.0	5.6	124.0	108.0	657.1	117.6	1733.0	70.0	214.7	391.5	2	nfs3	namespace_read	getattr	
1526376786	20.0	4.0	120.0	108.0	467.4	119.6	401.0	55.0	124.8	76.7	6	nfs3	namespace_read	getattr	
1526376786	13.0	2.6	112.0	104.0	279.9	106.5	485.0	78.0	167.8	135.8	5	nfs3	namespace_read	getattr	
1526376786	12.0	2.1	128.0	108.0	259.8	125.3	291.0	147.0	200.3	39.2	1	nfs3	namespace_read	access	
1526376786	11.0	2.2	124.0	112.0	255.5	116.4	536.0	142.0	221.8	113.3	2	nfs3	namespace_read	access	

Total:10															

- A. Too many namespace_read operations against the cluster
- B. Average NFSv3 write latency is too high
- C. Number of I/O for a single node is too high
- D. SmartConnect is not properly balancing the connections

ANSWER: D

Explanation:

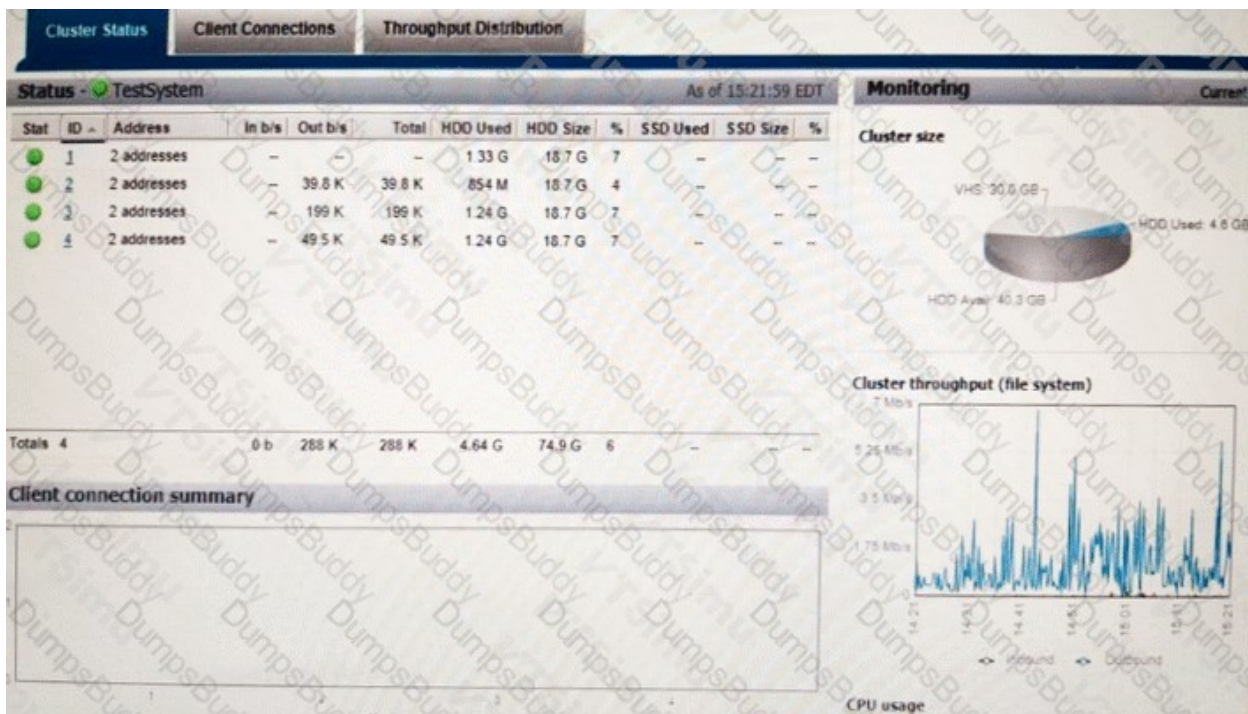
SmartConnect is not properly balancing the connections is the reason indicated by the output. In a PowerScale cluster, NFS clients normally connect through a SmartConnect service IP address. SmartConnect answers DNS requests using the configured connection-balancing policy and directs clients to node interfaces in the appropriate IP pool. This distribution is important because an NFS client is generally served by the node to which it initially connects; a busy node can therefore become a bottleneck even while other nodes in the cluster have available CPU, network, and disk capacity.

The exhibit's uneven per-node workload is consistent with client connections being concentrated on one node rather than spread across the eight-node cluster. Such concentration raises latency and makes NFS appear slow from the client perspective. The relevant remediation is to verify that clients resolve and mount the SmartConnect zone name rather than an individual node address, and then review the pool's DNS delegation, subnet, available interfaces, and connection-balancing policy. Existing client sessions may need to reconnect before a corrected balancing configuration is reflected in their connections. Dell's [SmartConnect best-practices guidance](#) and [PowerScale Info Hub](#) provide configuration and operational guidance for SmartConnect.

QUESTION NO: 7 - (SIMULATION)

A Dell EMC Isilon administrator has reported that in Access zone "ProdZone" on the OneFS file system "nfs1", Microsoft Windows "DEES\user1" has root level permission on nfs1. Use the "Launch Situation" button to examine the environment and validate the reason for this condition. Note: It is necessary to "close" (x) the simulation windows to answer the question.

Based on your findings, what is the reason for the condition?



ANSWER: See the explanation for the answer

Explanation:

Reason: The access-zone user mapping configuration maps the AD account DEES\user1 to the UNIX root identity (UID 0).

Because the user's authentication token is mapped to UID 0 in ProdZone, OneFS evaluates that Windows user as root when accessing the nfs1 file system. This is why the user has Root-level access; it is not caused by a normal NTFS/SMB share permission.

QUESTION NO: 8

A Dell PowerScale cluster has a file pool policy that moves inactive data to an archive node pool. The administrator changes the policy so that files are eligible for archive placement after 90 days rather than 180 days.

Which Job Engine job applies the revised file pool policy to existing files?

- A. SmartPools
- B. AutoBalance
- C. FlexProtect
- D. MediaScan

ANSWER: A

Explanation:

SmartPools is correct. The SmartPools job evaluates files against file pool policies and moves eligible file data between node pools and tiers. After the inactivity criterion is changed, running SmartPools causes existing files that meet the new 90-day condition to be evaluated for archive placement.

AutoBalance balances data across nodes, FlexProtect restores protection after a failure, and MediaScan verifies disk media. These jobs do not perform policy-based file placement. Dell provides Job Engine and SmartPools guidance in the [PowerScale OneFS documentation](#).

QUESTION NO: 9

You have been asked to design a Dell EMC Isilon cluster running OneFS 8.x for a service provider. One of the most critical areas to the provider is data segregation with multi-tenants. Use the "Launch Simulator" button to identify the current condition of the cluster: Note: It is necessary to "close" (x) the simulator window to answer the question.

Based on your findings, what is the cluster's current condition?

- A. All non-System Access zones are connected to the same groupnet, each with its own DNS server
- B. Each non-System Access zone is connected to an individual groupnet, each with its own DNS server
- C. All non-System Access zones are connected to the same groupnet with the same DNS server
- D. Each non-System Access zone is connected to an individual groupnet with the same DNS server.

ANSWER: A

Explanation:

The cluster condition is that all non-System Access zones are connected to the same groupnet, while each zone is configured with its own DNS server. The simulator's Access Zones and networking information must be correlated: the non-System zones reference one common groupnet rather than separate groupnets, and the DNS values shown for those zones differ. This identifies a shared underlying network container with tenant-specific name-resolution settings.

In OneFS, access zones are the primary mechanism for separating tenant-facing protocol access, authentication, and namespace usage. Groupnets organize network configuration and provide the network association used by access zones. Reviewing both objects is therefore essential: seeing different DNS settings alone does not establish that tenants use separate groupnets, and seeing multiple zones alone does not establish their network isolation model. The relevant current state is determined by the common groupnet association together with the individual DNS-server entries displayed for each non-System zone.

Dell's OneFS documentation describes access-zone and network configuration concepts in the [PowerScale OneFS documentation library](#). Additional OneFS networking guidance is available from the [Dell Technologies Info Hub](#).