EMC.D-VPX-DY-A-24.v2025-03-20.q22

Exam Code:	D-VPX-DY-A-24
Exam Name:	Dell VPLEX Deploy Achievement
Certification Provider:	EMC
Free Question Number:	22
Version:	v2025-03-20
# of views:	276
# of Questions views:	220
https://www.freeqas.com/qa/EMC/D-VPX-DY-A-24/EMC.D-VPX-DY-A-24.v2025-03-20.q22.html	

NEW QUESTION: 1
A customer engineer has installed VS2 VPLEX hardware, assigned IPs, and made the VPLEX ready to be configured. Which interface and port should be used to ssh to when using the EZ Setup wizard?
A. MMCS-B; eth3
B. MMCS-A; eth3
C. Management Server; eth3
D. Management Server; eth1
Answer: (SHOW ANSWER)
When using the EZ Setup wizard for VPLEX, the correct interface and port to SSH into is the Management Server's eth1 interface. This is typically the interface configured for management access and is used during the initial setup process.
* Management Server Access: The Management Server is the primary interface for managing and configuring the VPLEX system. It is through this server that the EZ Setup wizard is accessed1.
* eth1 Interface: The eth1 interface on the Management Server is usually dedicated to management traffic. This interface is configured with an IP address that allows SSH access for configuration purposes1.
* EZ Setup Wizard: The EZ Setup wizard is a guided setup tool that simplifies the initial configuration of the VPLEX system. It prompts the user for necessary information to configure the system1.
* SSH Protocol: Secure Shell (SSH) is a network protocol used to securely access network services over an unsecured network. When configuring VPLEX, SSH is used to connect to the Management Server and run the EZ Setup wizard1.

* Configuration Steps: To SSH into the Management Server, the customer engineer would use an SSH client, input the IP address assigned to the eth1 interface, and connect using the appropriate credentials provided during the VPLEX installation1.
In summary, to use the EZ Setup wizard for configuring VPLEX, the customer engineer should SSH into the Management Server using the eth1 interface. This interface is set up during the initial installation and is used for management access to the system.

NEW QUESTION: 2
A storage administrator has just been informed by their network team that a WAN outage has been restored.
How can the administrator verify that their VPLEX Metro WAN COM link is restored?
A. Run 11 /engines/ ** /sfps
Verify that all ports have good Rx and Tx power levels
B. Run vpn status
Verify that the peer IP is reachable
C. Run cluster summary
Verify that each cluster is listed under island 1
D. Run connectivity validate-local-com
Verify that all expected connectivity is present
Answer: D (LEAVE A REPLY)
To verify that the VPLEX Metro WAN COM link is restored, the storage administrator should run the connectivity validate-local-com command. This command checks the connectivity status of the local communication links within the VPLEX cluster.
* Command Execution: The administrator should access the VPLEX CLI and execute the connectivity validate-local-com command. This will initiate a check of the local COM ports' connectivity status1.
* Interpreting Results: After running the command, the administrator should review the output to verify that all expected connectivity is present. The output will indicate whether each local COM port is communicating as expected1.
* WAN COM Link: The WAN COM link is responsible for the communication between VPLEX clusters over a wide area network. Ensuring that the local COM links are operational is a prerequisite for the WAN COM link to function properly1.
* Post-Outage Verification: Following a WAN outage, it's crucial to confirm that the communication links are fully operational to maintain the high availability and data mobility features of VPLEX Metro1.
* Best Practices: It is recommended to follow the Dell EMC VPLEX best practices for post-outage recovery, which include running the connectivity validate-local-com command to ensure that the system is ready to resume normal operations1.
In summary, the connectivity validate-local-com command is the correct procedure to verify that the VPLEX Metro WAN COM link is restored, as it checks and confirms the presence of all expected local communication link connectivity within the VPLEX cluster.

NEW QUESTION: 3
A VPLEX Metro cluster is being installed for a company that is planning to create distributed volumes with
200 TB of storage. Based on this requirement, and consistent with
EMC best practices, what should be the minimum size for logging volumes at each cluster?
A. 10 GB
. 12.5 GB
B. 16.5 GB
C. 20 GB
Answer: A (LEAVE A REPLY)
When configuring a VPLEX Metro cluster, especially for a company planning to create distributed volumes with a large amount of storage like 200 TB, it is essential to adhere to EMC best practices for the size of logging volumes.
* Purpose of Logging Volumes: Logging volumes in VPLEX are used to store write logs that ensure data integrity and consistency across distributed volumes. These logs play a critical role during recovery processes1.
* Size Considerations: The size of the logging volumes should be proportional to the amount of active data being written to ensure that all write operations are captured in the logs. For 200 TB of distributed storage, a minimum size of 10 GB for each logging volume is recommended to handle the logging requirements1.
* Configuration: The logging volumes should be configured on each cluster to provide redundancy and high availability. This means that both clusters in a VPLEX Metro configuration should have logging volumes of at least the minimum recommended size1.
* Best Practices: EMC best practices suggest that the logging volume should be sized appropriately to support the operational workload and to ensure that there is sufficient space to capture all write operations without any loss of data1.
* Verification and Monitoring: After setting up the logging volumes, it is important to monitor their utilization to ensure they are functioning correctly and to adjust their size if necessary based on the actual workload1.
In summary, consistent with EMC best practices, the minimum size for logging volumes at each cluster in a VPLEX Metro cluster being installed for creating distributed volumes with 200 TB of storage should be 10 GB. This size ensures that the logging volumes can adequately support the write logging requirements for the amount of storage being used.

NEW QUESTION: 4
A RAID-C device has been built from a 100 GB extent and a 30 GB extent. How can this device be expanded?
A. RAID-C device cannot be expanded with unequal extent sizes
B. Add another RAID-C device to create a top-level device
C. Expand the 100 GB or 30 GB storage volume on the back-end array

D. Use concatenation by adding another extent to the device

Answer: D (LEAVE A REPLY)

To expand a RAID-C device that has been built from extents of unequal sizes, such as a 100 GB extent and a

30 GB extent, concatenation can be used. Concatenation allows for the addition of another extent to the existing RAID-C device, thereby increasing its overall size.

* Understanding RAID-C: RAID-C is a type of RAID configuration used in VPLEX that allows for concatenation, which is the process of linking multiple storage extents to create a larger logical unit1.

* Adding an Extent: To expand the RAID-C device, a new extent of the desired size can be added to the existing device. This new extent is concatenated to the end of the current extents, increasing the total capacity of the RAID-C device1.

* VPLEX CLI Commands: The expansion is performed using VPLEX CLI commands. The specific command to add an extent to a RAID-C device would be similar to the storage-volume expand command, which instructs the system to include the new extent in the RAID-C device1.

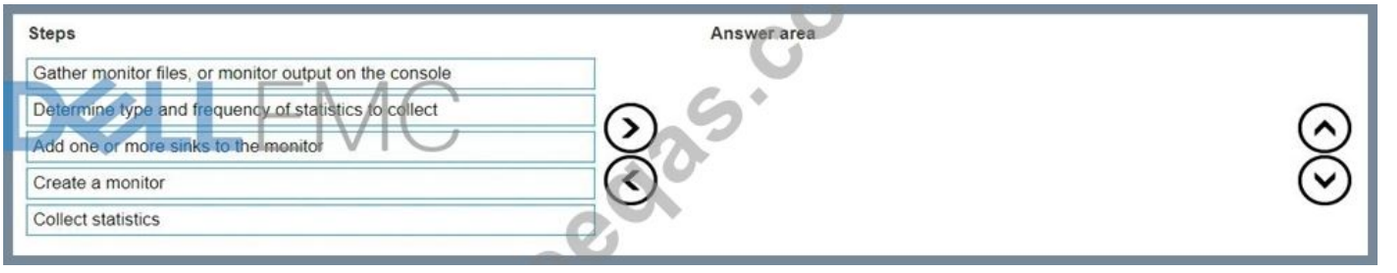
* Resizing Back-End Storage: If necessary, the back-end storage volumes (the physical storage on the array) that correspond to the extents may need to be resized to match the new configuration1.

* Verification: After the expansion, it's important to verify that the RAID-C device reflects the new size and that all extents are properly concatenated and functioning as expected1.

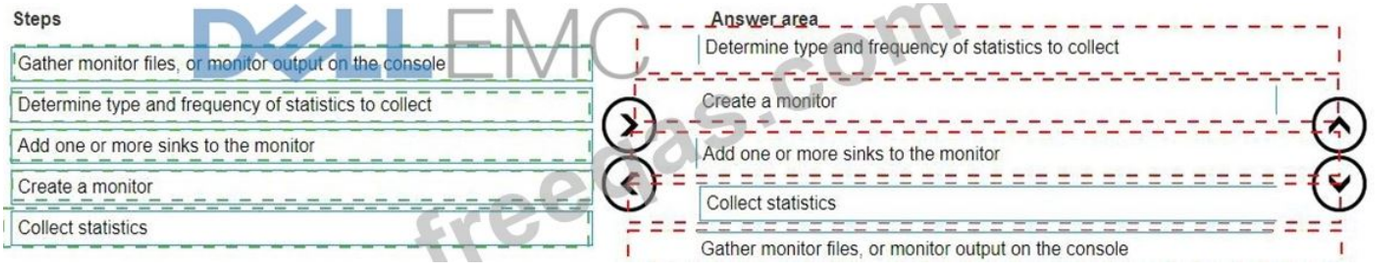
In summary, a RAID-C device built from extents of unequal sizes can be expanded by using concatenation to add another extent to the device. This method allows for flexibility in managing storage capacity within a VPLEX environment.

NEW QUESTION: 5

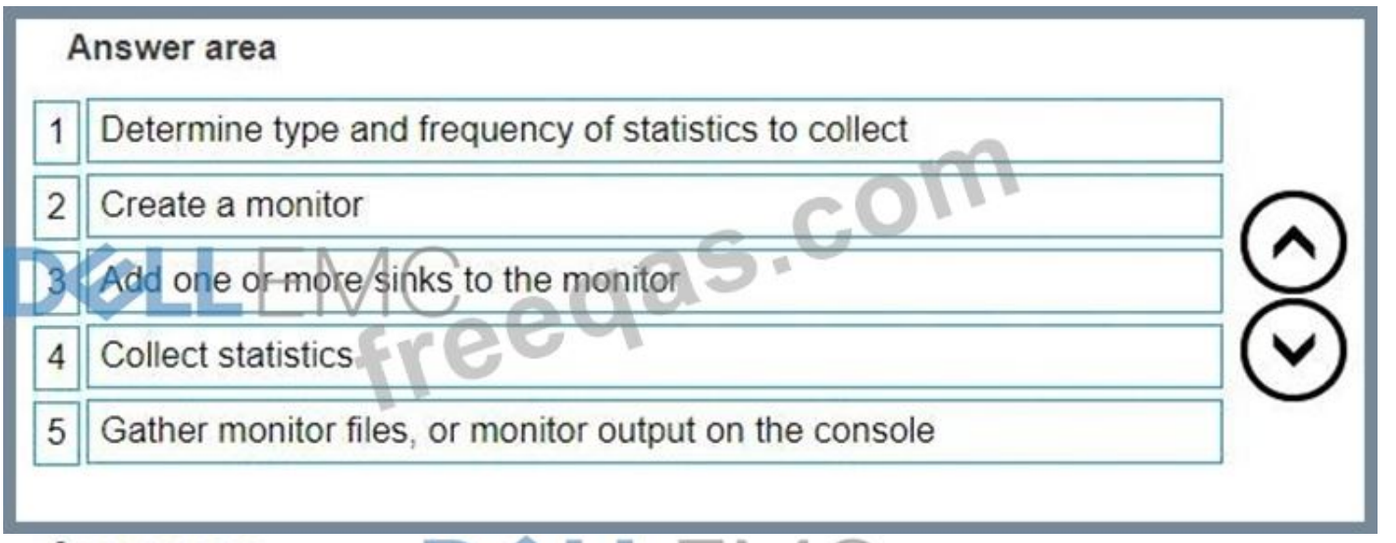
What is the correct order of steps to create and operate a custom monitor?

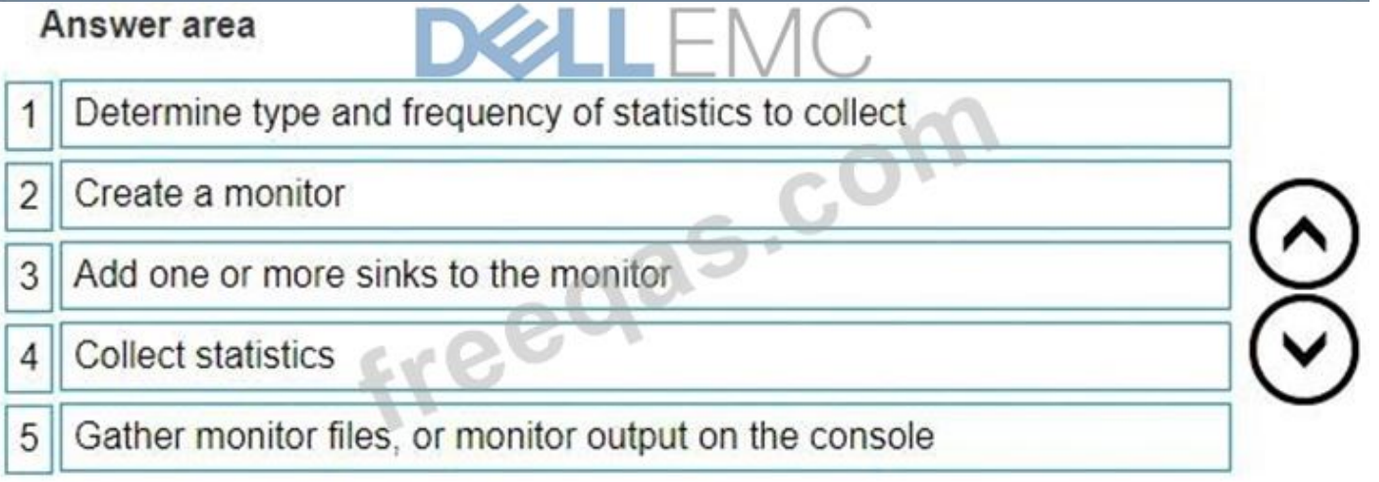


Answer:



Explanation:





The correct order of steps to create and operate a custom monitor is:

* Determine the type and frequency of statistics to collect.
* Create a monitor.
* Add one or more sinks to the monitor.
* Collect statistics.
* Gather monitoring files, or monitor output from the console.

To create and operate a custom monitor within the Dell VPLEX environment, follow these steps:

* Determine the Type and Frequency of Statistics to Collect: Identify what statistics are relevant for your monitoring purposes and how frequently they should be collected. This will depend on the specific needs of your environment and the performance metrics you wish to track.
* Create a Monitor: Using the VPLEX CLI or Unisphere for VPLEX, create a new monitor instance.

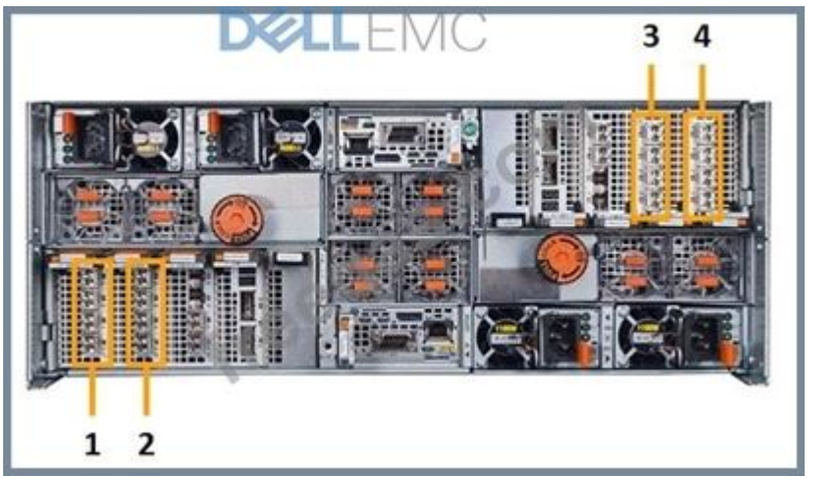
Configure the monitor with the types of statistics you determined in the previous step.

* Add One or More Sinks to the Monitor: Sinks are the destinations where the collected statistics will be sent. These could be files, databases, or external systems. Set up one or more sinks in the monitor configuration to ensure that the data is stored or transmitted as needed.
* Collect Statistics: Start the monitor to begin collecting statistics. The monitor will gather data from the VPLEX system according to the type and frequency settings you have specified.

* Gather Monitoring Files, or Monitor Output from the Console: After the statistics have been collected, retrieve the monitoring files from the specified sinks, or view the output directly from the console if real-time monitoring is configured.
These steps are based on the standard procedures for setting up and managing custom monitors in a Dell VPLEX environment, as detailed in the Dell EMC VPLEX documentation. By following these steps, you can effectively monitor the performance and health of your VPLEX system.

NEW QUESTION: 6
What is a consideration when using Advanced provisioning?
A. Requires each provisioning step to be executed simultaneously
B. Can only create one extent per storage volume
C. Allows the user to divide storage volumes into extents
D. Used only when storage volumes are provisioned from third-party arrays
Answer: C (LEAVE A REPLY)
Advanced provisioning in Dell VPLEX systems allows for more granular control over storage volumes by enabling the division of storage volumes into multiple extents. This capability is particularly useful for optimizing storage utilization and performance.
* Division into Extents: Advanced provisioning allows administrators to divide a larger storage volume into smaller, more manageable extents. This can help in aligning storage allocation with application requirements and improving performance by distributing I/O loads1.
* Flexibility: By dividing storage volumes into extents, administrators have the flexibility to manage storage more efficiently, such as allocating different extents to different virtual volumes or applications as needed1.
* Efficient Storage Utilization: This approach can lead to more efficient utilization of storage resources, as extents can be allocated and de-allocated dynamically based on changing needs1.
* Provisioning Steps: While advanced provisioning offers this flexibility, it does not require each provisioning step to be executed simultaneously. Instead, it allows for a more tailored approach to storage management1.
* Third-Party Arrays: Advanced provisioning is not limited to storage volumes from third-party arrays; it can be used with storage volumes from a variety of sources, including those directly managed by VPLEX1.
In summary, the consideration when using Advanced provisioning in Dell VPLEX systems is that it allows the user to divide storage volumes into extents, providing greater flexibility and efficiency in storage management.

NEW QUESTION: 7



Which number in the exhibit highlights the Director-B back-end ports?

A. 3

B. 4

C. 2

D. 1

Answer: B (LEAVE A REPLY)

To identify the Director-B back-end ports in a VPLEX system, one must understand the standard port numbering and layout for VPLEX directors. Based on the information provided in the Dell community forum1, the back-end ports for Director-B can be identified by the following method:

* Director Identification: Determine which director is Director-B. In a VPLEX system, directors are typically labeled as A or B, and each has a set of front-end and back-end ports1.
* Port Numbering: The port numbering for a VPLEX director follows a specific pattern. For example, in a VS2 system, the back-end ports are typically numbered starting from 10 onwards, following the front-end ports which are numbered from 001.
* Back-End Ports: Based on the standard VPLEX port numbering, the back-end ports for Director-B would be the second set of ports after the front-end ports. This is because the front-end ports are used for host connectivity, while the back-end ports connect to the storage arrays1.
* Exhibit Analysis: In the exhibit provided, if the numbering follows the standard VPLEX layout, number 4 would highlight the Director-B back-end ports, assuming that number 3 highlights the front-end ports and the numbering continues sequentially1.
* Verification: To verify the correct identification of the back-end ports, one can refer to the official Dell VPLEX documentation or use the VPLEX CLI to list the ports and their roles within the system1.

In summary, based on the standard layout and numbering of VPLEX systems, number 4 in the exhibit likely highlights the Director-B back-end ports. This identification is crucial for proper configuration and management of the VPLEX system.

NEW QUESTION: 8

A company has VPLEX Metro protecting two applications without Cluster Witness:

. App1 distributed virtual volumes are added to CG1, which has detach-rule set cluster-1 as winner

. App2 distributed virtual volumes are added to CG2, which has detach-rule set cluster-2 as winner What should be the consequence if cluster-2 fails for an extended period?

A. I/O for CG1 is suspended at cluster -1; I/O is serviced at cluster-2I/O for CG2 is serviced at cluster -1; I/O is suspended at cluster-2

B. I/O for CG1 is suspended at cluster -1; I/O is serviced at cluster-2I/O for CG2 is serviced at cluster -2; I/O is suspended at cluster-1

C. I/O for CG1 is detached at cluster -1; I/O is serviced at cluster-2I/O for CG2 is detached at cluster -2; I/O is serviced at cluster-1

D. I/O for CG1 is serviced at cluster -1; I/O is suspended at cluster-2I/O is serviced for CG2 at cluster -2; I/O is suspended at cluster-1

Answer: A (LEAVE A REPLY)

In a VPLEX Metro environment without a Cluster Witness, consistency groups (CGs) are used to manage distributed virtual volumes with detach rules that determine the behavior during a cluster failure.

* CG1 with Cluster-1 as Winner: For App1, the distributed virtual volumes are added to CG1, which has a detach rule set with cluster-1 as the winner. This means that if cluster-2 fails, I/O for CG1 will continue to be serviced at cluster-1 after it automatically attaches the volumes that were distributed across both clusters1.
* CG2 with Cluster-2 as Winner: For App2, the distributed virtual volumes are added to CG2, which has a detach rule set with cluster-2 as the winner. In the event of a cluster-2 failure, I/O for CG2 will be serviced after the volumes are detached from cluster-2, allowing cluster-1 to take over and service the I/O1.
* Extended Cluster-2 Failure: If cluster-2 fails for an extended period, the VPLEX Metro will follow the detach rules set for each consistency group. CG1 will have its I/O serviced at cluster-1, and CG2 will also have its I/O serviced at cluster-1 after detaching from the failed cluster-21.
* No Cluster Witness: Without a Cluster Witness, the VPLEX Metro relies on the detach rules defined in the consistency groups to determine how to handle I/O in the event of a cluster failure1.
* Operational Continuity: The goal is to maintain operational continuity for both applications. By servicing I/O for both CG1 and CG2 at cluster-1, VPLEX ensures that both applications remain operational despite the failure of cluster-21.

In summary, if cluster-2 fails for an extended period in a VPLEX Metro setup without a Cluster Witness, I/O for CG1 will be serviced at cluster-1, and I/O for CG2 will also be serviced at cluster-1 after detaching from cluster-2, as per the detach rules set for each consistency group.

NEW QUESTION: 9

An administrator reports performance issues with a virtual volume that is presented through a VPLEX Local cluster. Which command can provide the underlying storage volume information?

A. 11 ** /virtual volumes

B. 11 ** /storage-volumes

C. storage-volume summary

D. show-use-hierarchy

Answer: C (LEAVE A REPLY)
The storage-volume summary command in VPLEX is used to provide a summary of the storage volumes, including their operational status and health state. This command can be particularly useful when an administrator needs to troubleshoot performance issues with a virtual volume presented through a VPLEX Local cluster.
* Command Usage: The storage-volume summary command is executed in the VPLEX CLI (Command Line Interface). It provides a high-level overview of the storage volumes, including their I/O status, operational status, and health state1.
* Performance Troubleshooting: When performance issues are reported, it's important to check the underlying storage volumes for any signs of degradation or operational problems that could be impacting the virtual volume's performance1.
* Health State Information: The command's output includes the health state of the storage volumes, which can indicate if there are any degraded volumes or other issues that need to be addressed1.
* Operational Status: The operational status provided by the command helps determine if the storage volumes are functioning correctly or if there are any issues that could be causing the reported performance problems1.
* Further Investigation: If the storage-volume summary command reveals any issues with the underlying storage volumes, further investigation and corrective actions may be necessary to resolve the performance issues1.
In summary, the storage-volume summary command is the appropriate command to provide the underlying storage volume information when troubleshooting performance issues with a virtual volume in a VPLEX Local cluster.

NEW QUESTION: 10
When are the front-end ports enabled during a VPLEX installation?
A. Before launching the VPLEX EZ-Setup wizard
B. Before creating the metadata volumes and backup
C. After exposing the storage to the hosts
D. After creating the metadata volumes and backup
Answer: D (LEAVE A REPLY)
During a VPLEX installation, the front-end ports are enabled after the metadata volumes and backup have been created. This sequence ensures that the system's metadata, which is crucial for the operation of VPLEX, is secured before the storage is exposed to the hosts.
* Metadata Volumes Creation: The first step in the VPLEX installation process involves creating
* metadata volumes. These volumes store configuration and operational data necessary for VPLEX to manage the virtualized storage environment1.
* Metadata Backup: After the metadata volumes are created, it is essential to back up this data. The backup serves as a safeguard against data loss and is a critical step before enabling the front-end ports1.

* Enabling Front-End Ports: Once the metadata is secured, the front-end ports can be enabled. These ports are used for host connectivity, allowing hosts to access the virtual volumes presented by VPLEX1.
* Exposing Storage to Hosts: With the front-end ports enabled, the storage can then be exposed to the hosts. This step involves presenting the virtual volumes to the hosts through the front-end ports1.
* Final Configuration: The final configuration steps may include zoning, LUN masking, and setting up host access to the VPLEX virtual volumes. These steps are completed after the front-end ports are enabled and the storage is exposed1.
In summary, the front-end ports are enabled during a VPLEX installation after the metadata volumes and backup have been created, which is reflected in option D. This ensures that the system metadata is protected and available before the storage is made accessible to the hosts.

NEW QUESTION: 11
What is the default subnet mask value for management server network 128.221.252.0?
A. 255.255.255.248
B. 255.255.255.192
C. 255.255.255.128
D. 255.255.255.224
Answer: (SHOW ANSWER)
The default subnet mask for a management server network, specifically for the network 128.221.252.0, is typically a subnet mask that allows for a small number of hosts, as management networks do not usually require a large number of IP addresses.
* Subnet Mask Purpose: A subnet mask is used in IP networking to divide the IP address into a network and host identifier. The default subnet mask for a particular network depends on the class and configuration of the network1.
* Management Server Network: For a management server network like 128.221.252.0, a common default subnet mask is 255.255.255.248. This subnet mask allows for up to 6 usable IP addresses, which is generally sufficient for management purposes1.
* Network Configuration: The choice of subnet mask can affect the number of hosts that can be accommodated within a network. A subnet mask of 255.255.255.248 indicates a very small network, often used for specialized network segments such as management interfaces1.
* Dell VPLEX Configuration: In the context of Dell VPLEX Deploy Achievement, the management server network would be configured with a subnet mask that supports the network architecture and design best practices as outlined in Dell's documentation1.
* Best Practices: It is important to follow the recommended settings and configurations provided in the Dell VPLEX Deploy Achievement documents to ensure proper network segmentation, security, and performance1.
In summary, the default subnet mask value for a management server network like 128.221.252.0 is typically

255.255.255.248, which aligns with the standard practices for configuring management networks in a Dell VPLEX environment.

NEW QUESTION: 12
How many copies can RecoverPoint maintain in a MetroPoint topology?
A. 8
B. 6
C. 4
D. 5
Answer: D (LEAVE A REPLY)
"The MetroPoint topology can maintain up to five copies of data, including one remote copy and one local copy at each VPLEX site. It provides protection for each of the VPLEX Metro sites with continuous local replication via RecoverPoint"..

NEW QUESTION: 13
A database administrator would like to have access to the diagnostic files from the shell, but has no shell access. How can they gain access to the files?
A. Copy the files using SCP
B. Use access to root directory of the management server
C. Cannot access the file system without admin credentials
D. Cannot access the file system without service credentials
Answer: A (LEAVE A REPLY)
For a database administrator who needs access to diagnostic files from the VPLEX system but does not have shell access, the recommended method is to use Secure Copy Protocol (SCP) to copy the files. SCP is a secure file transfer protocol that allows files to be copied over a network.
* Access the Management Server: First, the administrator must access the VPLEX management server for the cluster from which they need to collect the logs1.
* SSH to the Director: Using SSH, the administrator logs in as root to the director from which the logs need to be collected1.
* Navigate to Log Directory: Change the directory to /var/log on the director to access the log files1.
* Create a Tarball of Logs: Use the tar command to create a compressed archive (tarball) of the log files1.
* Copy the Tarball Using SCP: Use SCP to copy the tarball to the management server's /tmp directory.
The administrator will be prompted for the service account password before the file can be transferred1.
* Access the Files: Once the files are on the management server, the database administrator can download them from the /tmp directory using SCP from their workstation1.
This process allows the database administrator to obtain the necessary diagnostic files without having direct shell access to the VPLEX system.

NEW QUESTION: 14

Refer to the exhibit.
Which Director-A port can be zoned to a host initiator?
A. B
B. C
C. D
D. A
Answer: D (LEAVE A REPLY)
In a VPLEX system, zoning a host initiator to a Director-A port requires identifying the front-end ports, which are used for host connectivity. Based on the standard VPLEX director port configuration:
* Director Identification: Determine which unit is Director-A. In a VPLEX system, directors are typically labeled as A or B, and each has a set of front-end and back-end ports1.
* Front-End Port Selection: The front-end ports on Director-A are used for connecting to host initiators.
These ports are typically numbered starting with 01.
* Zoning Process: Zoning involves configuring the SAN fabric to allow communication between the host's HBA (Host Bus Adapter) and the VPLEX front-end port. This is done using the SAN switch management interface1.
* Port Identification in Exhibit: Based on the exhibit provided, if the black arrow points to the first port on Director-A, it would be the front-end port 0, which can be zoned to a host initiator1.
* Verification: To confirm the correct port for zoning, one would typically refer to the official Dell EMC VPLEX documentation for hardware installation and setup, which would provide clear labeling of each port1.
In summary, based on the standard VPLEX port configuration, the Director-A port that can be zoned to a host initiator is the front-end port 0, which is indicated by the letter D in the exhibit provided.

NEW QUESTION: 15
What are the two common use cases of the VPLEX Mobility feature?
A. Workload Rebalance
Deduplication

B. NDU upgrades
Continuous Data Protection
C. Workflow Automation
Tech Refresh
D. Tech Refresh
Workload Rebalance
Answer: (SHOW ANSWER)
The VPLEX Mobility feature is designed to address various operational needs in a data center environment.
Two of the most common use cases for this feature are Tech Refresh and Workload Rebalance.
* Tech Refresh: The Tech Refresh use case involves using VPLEX to migrate data from older storage arrays to newer ones without disrupting the applications. This is crucial for organizations that need to update their storage infrastructure without downtime1.
* Workload Rebalance: Workload Rebalance refers to the ability to move workloads across different storage systems to balance performance and capacity needs. VPLEX enables this by allowing data to be moved non-disruptively, ensuring continuous application availability1.
* Operational Flexibility: VPLEX Mobility provides operational flexibility by enabling data to be moved within the same data center, across a campus, or within a geographical region. This capability is essential for dynamic environments where workload demands can change rapidly1.
* Enhanced Resource Utilization: By leveraging VPLEX Mobility for Tech Refresh and Workload Rebalance, organizations can optimize resource utilization, reduce operational costs, and improve overall system performance1.
* Best Practices: It is recommended to follow Dell's best practices when using VPLEX Mobility features.
This includes planning migrations during low-activity periods and ensuring that all systems are properly zoned and configured1.
In summary, the two common use cases of the VPLEX Mobility feature are Tech Refresh, which allows for seamless data migrations during technology upgrades, and Workload Rebalance, which facilitates the dynamic allocation of resources to meet changing workload demands.

NEW QUESTION: 16
What condition would prevent volume expansion?
A. Logging volume in re-synchronization state
B. Metadata volume being backed up
C. Rebuild currently occurring on the volume
D. Volume not belonging to a consistency group
Answer: (SHOW ANSWER)
In the context of Dell VPLEX, a rebuild occurring on a volume is a condition that would prevent the expansion of that volume. This is because the system needs to ensure data integrity and consistency during the rebuild process before any changes to the volume size can be made.

* Rebuild Process: A rebuild is a process where VPLEX re-synchronizes the data across the storage volumes, typically after a disk replacement or a failure1.
* Volume Expansion: Expanding a volume involves increasing its size to accommodate more data. This process requires that the volume is in a stable state without any ongoing rebuild operations1.
* Data Integrity: During a rebuild, the system is focused on restoring the correct data across the storage volumes. Attempting to expand a volume during this process could lead to data corruption or loss1.
* System Restrictions: VPLEX systems have built-in mechanisms to prevent administrators from performing actions that could jeopardize the system's stability or data integrity, such as expanding a volume during a rebuild1.
* Post-Rebuild Expansion: Once the rebuild process is complete and the volume is fully synchronized, the administrator can then proceed with the volume expansion1.
In summary, a rebuild currently occurring on a volume is a condition that would prevent the expansion of that volume in a Dell VPLEX system. The system must first ensure that the rebuild process is completed successfully before allowing any changes to the volume's size.

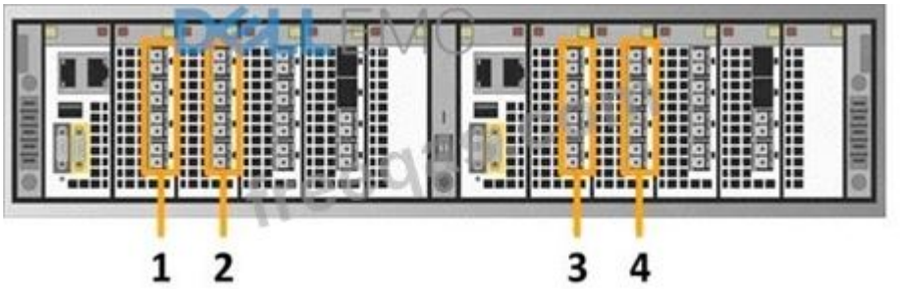
NEW QUESTION: 17
LUNs belonging to an ESXi cluster were encapsulated behind VPLEX. What information must be shared with the ESXi administrator so that they can re-discover the datastore and the RDM LUNs?
A. WWN:WWPN
B. UUID of back-end LUN
C. Virtual volume VPD
D. VML ID
Answer: C (LEAVE A REPLY)
When LUNs belonging to an ESXi cluster are encapsulated behind VPLEX, the ESXi administrator needs to be provided with the Virtual Volume Page Data (VPD) of the virtual volumes. The VPD contains metadata about the virtual volumes that allows the ESXi host to properly identify and interact with them.

* Encapsulation Process: During the encapsulation process, the physical LUNs are virtualized and presented as virtual volumes through VPLEX. This process involves the VPLEX claiming the LUNs and presenting them to the ESXi hosts as new devices1.
* Re-discovery of Datastore and RDM LUNs: After encapsulation, the ESXi administrator must perform a rescan of the storage adapters to discover the new virtual volumes. The VPD of the virtual volumes, which includes information such as the device identifiers and characteristics, is crucial for the ESXi host to recognize and mount the datastores and RDM LUNs2.
* Importance of VPD: The VPD is essential because it provides the ESXi host with the necessary information to differentiate between the virtual volumes and other storage devices. Without the VPD, the ESXi host may not be able to properly identify the encapsulated LUNs, leading to issues with datastore accessibility1.
* Best Practices: It is recommended to follow the best practices and required configurations for a vSphere Metro Storage Cluster using EMC VPLEX Storage array as outlined in VMware KB articles and Dell support documents. This ensures a smooth encapsulation process and proper functioning of the ESXi hosts with the VPLEX storage volumes1.
In summary, sharing the Virtual Volume VPD with the ESXi administrator is a critical step in ensuring that the ESXi cluster can successfully re-discover the datastore and the RDM LUNs after they have been encapsulated behind VPLEX.

NEW QUESTION: 18
What is a consideration when using VPLEX RecoverPoint enabled consistency groups?
A. Production and local copy journals must be in different consistency groups.
B. Local copy volumes and production volumes must reside in separate consistency groups.
C. Repository volume and journal volumes must be in different consistency groups.
D. Local virtual volumes and distributed virtual volumes can be in the same consistency group.
Answer: B (LEAVE A REPLY)
When using VPLEX with RecoverPoint enabled consistency groups, it is important to ensure that local copy volumes and production volumes are placed in separate consistency groups. This separation is crucial for maintaining the integrity of the data replication and recovery processes.
* Consistency Group Configuration: Consistency groups in VPLEX are logical groupings of virtual volumes that VPLEX treats as a single unit for operations such as data mobility and recovery. When RecoverPoint is enabled, these groups also align with RecoverPoint consistency groups for replication purposes1.
* Separation of Volumes: Keeping local copy volumes (volumes used for local replication) and production volumes (active volumes serving data to hosts) in separate consistency groups helps to prevent any potential conflicts or issues with replication and ensures that the local copies are consistent and usable for recovery1.
* RecoverPoint Replication: RecoverPoint provides continuous data protection and replication for recovery to any point in time. The separation of volumes into different consistency groups helps to manage and maintain the replication process effectively1.

* Operational Management: By separating these volumes into different consistency groups, administrators can manage operations such as replication, failover, and recovery with greater precision and control1.
* Best Practices: This separation is part of the best practices recommended by Dell EMC when configuring VPLEX with RecoverPoint, ensuring that the system operates efficiently and that data is protected in case of any failures1.
In summary, when using VPLEX with RecoverPoint enabled consistency groups, local copy volumes and production volumes must be placed in separate consistency groups to ensure proper replication and recovery processes.

NEW QUESTION: 19



Which number in the exhibit highlights the Director-B front-end ports?

A. 4

B. 2

C. 1

D. 3

Answer: B (LEAVE A REPLY)

In a VPLEX system, each director module has front-end (FE) and back-end (BE) ports for connectivity. The FE ports are used to connect to hosts or out-of-fabric services such as management networks. Based on standard configurations and assuming that Director-A and Director-B are mirrored in layout, the number that highlights the Director-B front-end ports is typically 21.
* Director Modules: VPLEX systems consist of director modules, each containing ports designated for specific functions. Director-B is one of these modules1.
* Front-End Ports: The front-end ports on Director-B are used for host connectivity and are essential for the operation of the VPLEX system1.
* Port Identification: During the installation and setup of a VPLEX system, correctly identifying and utilizing the FE ports is crucial. This includes connecting the VPLEX to the host environment and ensuring proper communication between the storage system and the hosts1.
* Documentation Reference: For precise identification and configuration of the FE ports on Director-B, the Dell VPLEX Deploy Achievement documents provide detailed instructions and diagrams1.

* Best Practices: It is recommended to follow the guidelines provided in the Dell VPLEX documentation for port identification and installation utilities to ensure correct setup and configuration of the VPLEX system1.
In summary, the number 2 in the exhibit corresponds to the Director-B front-end ports in a Dell VPLEX system, which are critical for host connectivity and system operation.

NEW QUESTION: 20

Refer to the exhibit.
Which MMCS-A cable should be connected to the customer management network?
A. A
B. D
C. C
D. B
Answer: D (LEAVE A REPLY)
For connecting the MMCS-A to the customer management network in a Dell VPLEX system, it is essential to use the correct port that is designated for management traffic. According to the Dell EMC VPLEX documentation1, each MMCS (Management Module Control Station) has two network connections that connect to the customer's network. One of these is used for system monitoring and remote connectivity for Dell Technologies Customer Support, and the other is for use by the Network Address Translation (NAT) Gateway.
In the context of the VS6 VPLEX cluster, the management ports are located on MMCS-A and MMCS-B, and both must be configured and connected to the customer network. MMCS-A is the management port that will be accessed for all management and monitoring purposes1. Therefore, the cable that should be connected to the customer management network is the one associated with MMCS-A.
Based on the information provided in the search results and the description of the image, the correct cable to connect to the customer management network for MMCS-A is indicated by the letter B in the exhibit. This connection is crucial for enabling management and monitoring access to the VPLEX system.

NEW QUESTION: 21

Using the Storage Volume expansion method for virtual volumes built on RAID-1 or distributed RAID-1 devices, what is the maximum number of initialization processes that can run concurrently, per cluster?

A. 100

B. 500

C. 250

D. 1000

Answer: D (LEAVE A REPLY)

* Context: The Dell VPLEX system allows for the expansion of virtual volumes to accommodate growing data storage needs without disrupting ongoing operations.
* Initialization Process: When expanding storage volumes, the system undergoes initialization processes to integrate the new storage capacity effectively.
* Concurrent Processes Limit: For virtual volumes built on RAID-1 or distributed RAID-1 devices, the maximum number of initialization processes that can run concurrently per cluster is 1000. This limit ensures optimal performance and resource management within the cluster.
* Implications: If the limit of 1000 concurrent processes is reached, no new storage volume expansions can be initiated until some of the ongoing initialization processes are completed.

References:

* Dell EMC Metro Node Administrator Guide

NEW QUESTION: 22

What is an EMC best practice for connecting VPLEX to back-end arrays?

A. One multiple switch fabric should be used for each VPLEX engine

B. Back-end connections should be distributed across one director

C. Each VPLEX director should have four active paths to every back-end array storage volume

D. Two active paths per VPLEX engine to any storage volume is optimal

Answer: C (LEAVE A REPLY)

EMC recommends specific best practices for connecting VPLEX to back-end storage arrays to ensure high availability and optimal performance. One of these best practices is that each VPLEX director should have four active paths to every back-end array storage volume.

* Multiple Paths: Having multiple active paths from each VPLEX director to the storage volumes ensures that there is no single point of failure. If one path fails, the other paths can continue to provide connectivity1.
* Load Balancing: Multiple paths also allow for load balancing of I/O operations across the different paths, which can improve performance and reduce the risk of bottlenecks1.
* Path Redundancy: Path redundancy is crucial for maintaining continuous availability, especially in environments where the VPLEX is used for mission-critical applications1.
* Configuration: The configuration of the paths should be done in accordance with EMC's best practices, which include proper zoning and masking in the SAN environment1.

* Documentation: Detailed guidelines and best practices for VPLEX SAN connectivity, including back-end array connections, are available in EMC's documentation, which provides comprehensive instructions for setting up and managing these connections1.
In summary, EMC's best practice for connecting VPLEX to back-end arrays is to ensure that each VPLEX director has four active paths to every back-end array storage volume. This setup provides the necessary redundancy and performance for a robust and reliable storage environment.