VEEAM VMCA2022 Practice Questions

Shared by Whitfield on 20-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Case Study: Veeam University Hospital

Executive Overview:

Veeam University Hospital is a healthcare network with located is Boston, Salt Lake City and Columbus. They are considered a pioneer in breakthrough treatments to many illnesses and recognized worldwide as a leader in their field. They have decided to modernize their data protection strategy due to new regulatory requirements as well as ever evolving malware issues. They suffered a ransomware attack recently as well, which affected several systems with patient treatment.

Furthermore, they have expressed interest in replication of virtual workloads between sites in case of a disaster to allow for timely failover between sites with would ensure continuity in the level of patient care offered.

Their board of directors is concerned that all virtual workloads at this point can be considered a single point of failure.

Veeam University Hospital has also been experiencing issues with the time required to back up NAS systems. Not only are they taking too long, the amount of space required is considered excessive, and a reduction of storage space for these backups is desired.

Veeam University Hospital had issues with the time required to restore Exchange items. The current solution will only restore entire mailboxes, and no granularity is possible.

For this implementation to be successful, backups must complete in the allotted backup window, and the recovery of data should be faster than the current solution, which can amount to 24 to 48 hours for a full system restore.

Solution Concept:

Veeam University Hospital is replacing their current backup solution Veeam. They plan to protect data at all three sites, with backups copied off-site for disaster recovery purposes. They have also expressed an interest in taking action to prevent another data lost due to ransomware. The offenders were also able to encrypt the existing backups as part of the attack, so data recovery is impossible. Veeam University Hospital is also interested in any posible public cloud technologies that might help mitigate this risk.

In addition, replication of running workloads to secondary sites will also be implemented to allow for site failover in the event of a disaster for reduced down time.

Existing Technical Environment:

Veeam University Hospital has VMware cluster in all locations. For security purposes, each cluster is

dedicated to the department that it servers. No communication between cluster is possible. These cluster are broken into two categories, one hosting database workloads and the other hosting general use virtual machines.

Confidential patient data exists on several NAS systems as unstructured data. These NAS systems are only presenting backups to ensure consistency of the database.

Veeam University Hospital has an in-house patient database required a custom script to be execute before backups to ensure consistency of the database.

MSSQL and Oracle are used by most of the departments, with a mix of virtual and physical deployments.

Each site as a 10 GbE link to the public internet, and all traffic between sites is routed through these connections via VPN.

Each site has 20 vLANs in use, with 16 being used for VMware workloads.

For security and regulatory purposes, all vLANs are firewalled off from each other.

The current backups write to NFS storage.

All doctor and lab staff are assigned their laptops, which will also need to be protected. The location of data on these devices is enforced through group policy, and consistent throughout the organization.

No current disaster recovery solution, apart from restoring from backup files, exists at this time.

Business Requirements:

Any new solution must take advantage of automation and self-service functionality. Both features are needed to cut down on administrative costs. Role based access (RBAC) is mandatory. For example, only Oracle administrators can have the ability to perform self-service restore of Oracle Data.

Mission critical applications must not be impacted during business hours. All backups must complete between 6 p.m. and 8 a.m. local time.

To meet regulatory requirements all data must be retained for three years.

For archival purposes, 12 monthly backups and three yearly backups must be stored offsite.

Veeam University Hospital will only purchase on-premises storage to accommodate growth for three years of backup retention.

For any replicated virtual workloads, the data must not more than one hour old.

Due regulatory requirements, all protected data must be encrypted in flight and rest.

To meet customer service-level agreements, a commercially available helpdesk ticketing system is in use. All alerts generated must be integrated with this system to create support tickets.

Technical requirements:

Backups must take advantage of public cloud storage for long term archival purposes.

The solution must keep a local backup and be able to create an additional copy of production data. Both backups should reside on site with production systems being protected.

For quick restores and recovery, at least copy of protected data must reside on-premises.

Due to the threat of ransomware, at least one immutable or air gapped copy of protected data must reside off-side.

To ensure data integrity, backups must be verified and scanned for malware before any restore Is performed.

In addition to Self-service Oracle restores, native Oracle tools must be available and PowerShell script ready to perform ad-hoc backups and restores.

The backup solution must support VMware encrypted datastores.

Backups must be stored in logical scalable storage systems that can be expanded non-disruptively.

For end user laptop backups, only user data should be backed up. Operating system files should be excluded.

Personal files such as music, photos, and videos must be excluded for backup.

Based on the requirements, and the assumption that Veeam University Hospital will keep their existing backup storage, which answer describes which components are needed for the on-premises design?

Options:

A- Backup server, backup proxy, Backup Enterprise Manager, log shipping servers.
B- Backup server, backup proxy, Backup Enterprise Manager, mount server, backup repository.
C- Backup server, backup proxy, backup repository, Veeam vPower NFS service.
D- Backup server, backup proxy, backup repository, mount server, guest interaction proxy, gateway server.

Answer:

D

Explanation:

To design a solution that meets the backup and replication requirements for Veeam University

Hospital, you need to consider some of the components that are needed for the on-premises design. This will help you to ensure the performance and reliability of the backup and replication operations, as well as the scalability and manageability of the backup infrastructure.

According to the Veeam Backup & Replication Best Practice Guide1, some of the components that are needed for the on-premises design are:

* Backup server. This is the core component of Veeam Backup & Replication that controls and coordinates backups, replication, recovery verification, and restore tasks. It also manages backup infrastructure components, such as proxy servers, repository servers, WAN accelerators, etc. You need to have a backup server at each site, as recommended by the best practice guide2.

* Backup proxy. This is a component that retrieves data from the source host, processes it and transfers to the backup repository. It also performs data compression, deduplication, encryption, etc. You need to have at least one backup proxy at each site, as recommended by the best practice guide3.

* Backup repository. This is a server where Veeam Backup & Replication keeps backup files, backup copies and metadata of replicated VMs. It can be a Windows or Linux server, a NAS device, a deduplication appliance, etc. You need to have at least one backup repository at each site, as recommended by the best practice guide4.

* Mount server. This is a component that mounts backup files from the backup repository to the backup proxy during restore operations. It also performs data decompression, deduplication, decryption, etc. You need to have a mount server at each site where you plan to perform restores, as recommended by the best practice guide5.

* Gateway server. This is a component that acts as a data mover between the backup proxy and the backup repository when they are located in different sites or networks. It also performs data encryption and decryption for secure data transfer. You need to have a gateway server at each site where you have a backup repository that is accessed by a remote backup proxy, as recommended by the best practice guide.

Therefore, based on these components, the answer that describes which components are needed for the on-premises design is D. Backup server, backup proxy, backup repository, mount server, gateway server.

Question 2

Question Type: MultipleChoice

What additional information is necessary for sizing the backup solution and must be gathered

during further discovery? (Choose 2)

Options:

A- The available bandwidth per site
B- The amount of virtual machines to be protected
C- The total amount of production storage provisioned space
D- Repository storage file system
E- The replication schedule

Answer:

B, C

Explanation:

The additional information that is necessary for sizing the backup solution and must be gathered during further discovery are the amount of virtual machines to be protected and the total amount of production storage provisioned space. These metrics are used to calculate the backup storage requirements, the backup proxy and transporter resources, and the backup job configuration. The other options are either not relevant for sizing the backup solution (repository storage file system, replication schedule) or already provided in the scenario (the available bandwidth per site).Reference:Veeam Certified Architect 2022 Exam Guide, page 10;Veeam Backup & Replication v11: Architecture and Design course, module 3.

Question 3

Question Type: MultipleChoice

When talking to someone who works for the hospital, they mention they are working on a project with a major cloud provider that does not currently support immutability. After further conversations, the customer has decided that they would like daily immutable backups to be sent off-site. Which of the following is the best option to still satisfy the requirements for off-site immutable backups?

Options:

A- Backup copy to a hardened repository.
B- Backup copy to repository on a Cloud-based Windows Instance that scheduled to power off outside the backup window.
C- Set up capacity tier with object that supports immutability at the primary site.
D- Back up to tape and leverage a service to rotate tapes off-site weekly.

Answer:

A

Explanation:

To design a solution that meets the requirements for off-site immutable backups for Veeam University Hospital, you need to consider some of the options and features that Veeam products and features offer. This will help you to ensure the security and integrity of your backup data, as well as the compatibility and supportability of the cloud provider that does not currently support immutability.

According to the Veeam Backup & Replication Best Practice Guide, immutability is a feature that prevents backup files from being deleted or modified by anyone until the specified retention period expires. Immutability can be achieved by using S3 Object Lock or Hardened Repository, which are two different solutions that Veeam Backup & Replication supports.

Based on this definition, the best option to still satisfy the requirements for off-site immutable backups is A. Backup copy to a hardened repository.

This option means that:

* The backup copy is a type of job that allows you to create and maintain copies of your backup data on a secondary backup repository. You can use backup copy jobs to send your backup data off-site, as well as to apply different retention settings and policies.

* The hardened repository is a solution that allows you to add a hardened repository based on a Linux server to your backup infrastructure. You can use hardened repository with Veeam Backup & Replication to make your backups immutable on-premises or off-site.

* The backup copy to a hardened repository can be configured and managed by Veeam Backup & Replication, regardless of the cloud provider that does not currently support immutability. You only need to deploy and connect a Linux server with a hardened repository in the cloud environment, and then use it as a target for your backup copy jobs.

Question 4

Question Type: MultipleChoice

Veeam University Hospital perform a proof of concept of the design outline in the architecture. Backups completed successfully, but it is determined that backup copy jobs between sites are not completing in the required timeframe. During the result analysis, it was discovered that the bandwidth between sites was heavily saturated. What adjustments within the Veeam infrastructure would best address this issue?

Options:

A- Increase the proxy computer resources at each site.
B- Increase the computer resources on the repository servers at each site.
C- Add WAN accelerators to each site.
D- Have the customer implement Quality of Service on their WAN connections.

Answer:

C

Explanation:

WAN accelerators are dedicated components that Veeam Backup & Replication uses for WAN acceleration. WAN accelerators are responsible for global data caching and data deduplication, which reduce the amount of data that needs to be transferred over the network. By adding WAN accelerators to each site, you can improve the performance of backup copy jobs between sites, and reduce the bandwidth consumption and network traffic3

1: Gateway Server - User Guide for VMware vSphere 2: Gateway Server - User Guide for VMware vSphere 3: WAN Accelerators - User Guide for VMware vSphere

Question 5

Question Type: MultipleChoice

Veeam Financial Services received notification from their legal team that retention of backups should be five years on-site instead of four. What component sizing should be adjusted?

Options:

A- The amount of object storage purchased in a public cloud for archival purposes.
B- Physical storage in the repositories.
C- The CPU and memory of the Veeam Backup & Replication database.
D- CPU and memory requirements for the Veeam repositories.

Answer:

B

Explanation:

The component sizing that should be adjusted is the physical storage in the repositories.The repositories are the backup storage locations where Veeam Backup & Replication stores backup files, VM copies and metadata for replicated VMs1. Increasing the retention period from four to five years means that more backup files will be kept on the repositories, and thus more storage space will be required. The other options are not affected by the retention period change, as they are either related to off-site backups (option A), Veeam Backup & Replication server performance (option C), or backup proxy performance (option D).Reference:Backup Repositories.

Question 6

Question Type: MultipleChoice

Based on customer recovery requirements, which component will help them meet their stated objectives?

Options:

A- Add a Windows server and enable encryption of backups to ensure alternative decryption capabilities.
B- Deploy and configure Enterprise Manager with RBAC policies.
C- Deploy Veeam Backup & Replication console and set RBAC policies to Administrator Role
D- Add a Windows and Linux server, enable indexing of backups and ensure authenticated users are configured to appropriate RBAC policies.

Answer:

B

Explanation:

The component that will help the customer meet their stated objectives of role-based access control (RBAC) and alternative decryption capabilities is Veeam Backup Enterprise Manager. Veeam Backup Enterprise Manager is a web-based interface that allows centralized management of multiple Veeam backup servers. It also provides RBAC policies that enable granular control over user permissions and access to backup data. For example, you can assign different roles to different users or groups based on their responsibilities and needs, such as backup administrator, restore operator, security officer, etc. Veeam Backup Enterprise Manager also provides password loss protection feature that enables authorized users to restore encrypted backups without entering passwords if they forget or lose them.

Question 7

Question Type: MultipleChoice

Which tier(s) of Veeam Financial Services' backups will require SureBackup jobs?

Options:

A- Gold tier.
B- Silver and gold tiers.
C- Gold, silver and bronze tiers.
D- All virtual machine and laptop backups.

Answer:

B

Explanation:

The tiers of Veeam Financial Services' backups that will require SureBackup jobs are the silver and gold tiers.SureBackup jobs are used to verify the recoverability of backup files by running virtual machines from backups in an isolated environment and performing tests against live applications1. This feature is suitable for the silver and gold tiers, which have recovery time objectives of six hours and 30 minutes, respectively, and require backups to be verified. The bronze tier, which consists of development machines and field portables, has a recovery point target of seven days, with no recovery time target set, and does not require backup verification. Therefore, SureBackup jobs are not necessary for the bronze tier.Laptop backups are performed by Veeam Agent for Microsoft Windows, which does not support SureBackup jobs2.Reference:SureBackup,Veeam Agent for Microsoft Windows.

Question 8

Question Type: MultipleChoice

Which Veeam feature can be used to help achieve compliance with privacy regulations?

Options:

A- Preferred networks.
B- Location tags on Veeam Backup & Replication servers.
C- Location tags on the subnets.
D- Location tags on repositories.

Answer:

D

Explanation:

The Veeam feature that can be used to help achieve compliance with privacy regulations is location tags on repositories.Location tags are labels that can be assigned to backup repositories to indicate their physical or logical location, such as country, region, or data center1.Location tags can help ensure that backup data is stored and processed in compliance with data residency and privacy laws, such as GDPR or CCPA, by allowing backup administrators to create backup policies based on the location of the source and target data2. The other options are not related to privacy compliance, as they are either used for network optimization (preferred networks), server identification (location tags on Veeam Backup & Replication servers), or backup scope (location tags on subnets).Reference:Location Tags,Using Location Tags.

Question 9

Question Type: MultipleChoice

What assumption can be made for the conceptual design?

Options:

A- All new backup storage should utilize Windows ReFS block cloning.
B- Tape backups of all servers will be used for ransomware protection.
C- Veeam Agent backups of sale staff laptops should be managed by the backup server.
D- VMware tagging will be used to enable dynamic scoping of backups.

Answer:

C

Explanation:

The assumption that can be made for the conceptual design is that Veeam Agent backups of sale staff laptops should be managed by the backup server. This assumption is based on the best practice and recommendation for using Veeam Backup & Replication. Veeam Agent backups of sale staff laptops should be managed by the backup server to enable centralized management, monitoring, and reporting of all agent-based backups. This can also simplify the backup configuration, scheduling, and retention for the laptop agents.

Question 10

Question Type: MultipleChoice

Veeam Financial Services performed a proof of concept of the design outlined in the architecture. Backups completed successfully, but it was determined that the offloading of data to public cloud storage is consuming all available bandwidth on several branch sites and business applications are lacking performance as a result. What adjustments within the Veeam Infrastructure would best address this issue?

Options:

A- Configure Network Traffic Rules.
B- Increase the compute resources on the repository servers at each site.
C- Increase the proxy compute resources at each site.
D- Add WAN accelerators to each site

Answer:

A

Explanation:

Network traffic rules are settings that allow you to control the network traffic transferred between backup infrastructure components, such as backup proxies, repositories, and WAN accelerators.You can use network traffic rules to throttle or encrypt the network traffic, or to specify preferred networks for data transfer1.

By configuring network traffic rules, you can reduce the bandwidth consumption for the offloading of data to public cloud storage, and avoid affecting the performance of business applications on the branch sites.You can set limits for the network traffic speed, or schedule the offloading tasks to run during off-peak hours2.You can also select the optimal network routes for the offloading tasks, and avoid congested or slow networks3.

You can find more information about network traffic rules and how to configure them in the following resources:

Configuring Network Traffic Rules

Enabling Traffic Throttling

Specifying Preferred Networks

P2P exams

P2P exams

To Get Premium Files for VMCA2022 Visit

https://www.p2pexams.com/products/vmca2022

For More Free Questions Visit

https://www.p2pexams.com/veeam/pdf/vmca2022

