Number: VMCA2022
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: VMCA2022

Exam Name: Veeam Certified Architect 2022

Exam A

QUESTION 1
During a proof of concept deployment at Veeam University Hospital, it is noted that only some of the backup files in a specific Scale-out Backup Repository are immutable. What can cause this behavior?

A. The ReFS extents do not have immutable enabled.
B. Not all XFS extents in the Scale-out Backup Repository performance tier have the required flag enable.
C. All extents in the Scale-out Backup Repository performance tier are ReFS.
D. Not all EXT in the Scale-out Backup Repository performance archive tier have the required flag enabled.

Correct Answer: B
Section:
Explanation:
To make backup files immutable in a Scale-out Backup Repository, you need to use XFS extents with the reflink attribute enabled. This attribute allows Veeam Backup & Replication to create immutable backup files using the fast clone technology. If some of the XFS extents do not have this attribute enabled, they will not support immutability and the backup files stored on them will not be protected from deletion or modification1

QUESTION 2
While deciding which transport mode to use for the proxies, you notice that one of the requirements is support the encrypted datastore in VMware. Which processing modes can you leverage for the backup proxies? (Choose 3)

A. Network mode with Encryption (NBDSSL).
B. Virtual Appliance (HotAdd) mode.
C. Network (NBD) mode.
D. Direct SAN.
E. Direct SMB.
F. Direct NFS.

Correct Answer: A, B, E
Section:
Explanation:
To access encrypted datastores in VMware, you need to use a transport mode that supports encryption. The following transport modes support encryption:
* Network mode with Encryption (NBDSSL): This mode uses an encrypted network connection between the backup proxy and the ESXi host to read and write data from the encrypted datastore. This mode does not require direct access to the datastore, but it can be slower than other modes due to network traffic and encryption overhead2
* Virtual Appliance (HotAdd) mode: This mode uses a virtual backup proxy that runs on an ESXi host and attaches virtual disks of the encrypted VMs to itself using the VMware vSphere API. This mode requires that the backup proxy and the source VMs reside on the same datastore or on datastores that are accessible by the same ESXi host. This mode can offer better performance than network mode, but it can also cause SCSI reservation conflicts if multiple backup proxies access the same datastore simultaneously3
* Direct SMB: This mode uses a physical backup proxy that accesses the encrypted datastore over the SMB protocol. This mode requires that the datastore is configured as an SMB share and that the backup proxy has read and write permissions on it. This mode can offer high performance and scalability, but it also requires additional configuration steps and security considerations4
The following transport modes do not support encryption:
* Network (NBD) mode: This mode uses an unencrypted network connection between the backup proxy and the ESXi host, which cannot access encrypted datastores2
* Direct SAN: This mode uses a physical backup proxy that accesses the encrypted datastore over the SAN fabric, which cannot decrypt encrypted data5
* Direct NFS: This mode uses a physical backup proxy that accesses the encrypted datastore over the NFS protocol, which does not support encryption6
1: Hardened Repository - User Guide for VMware vSphere 2: Network Mode - User Guide for VMware vSphere 3: Virtual Appliance Mode - User Guide for VMware vSphere 4: Direct SMB Access Mode - User Guide for VMware vSphere 5: Direct SAN Access Mode - User Guide for VMware vSphere 6: Direct NFS Access Mode - User Guide for VMware vSphere

QUESTION 3
During architecture review, the engineers who will be implementing the designed architecture ask how they should proceed to fully meet the requirements for Oracle backup. How should the rellout be handled to meet these requirements?

A. Install and configure the RMAN plugin.
B. Create pre-freeze and post-thaw scripts for all Oracle backups.
C. Implement and configure Veeam Backup Enterprise Manager, and configure RMAN so that only Oracle administrators have access to the Oracle backups.
D. Deploy agents to all Oracle servers and ensure that application aware processing is configured.

Correct Answer: A
Section:
Explanation:
* The RMAN plugin is a component that integrates Veeam Backup & Replication with Oracle RMAN, which is a native tool for Oracle backup and recovery12.
* The RMAN plugin allows you to use Oracle RMAN commands to back up and restore Oracle databases to Veeam backup repositories, as well as perform log shipping and point-in-time recovery12.
* The RMAN plugin supports Oracle databases running on any supported operating system or hypervisor, as well as physical servers or cloud environments12.
* The RMAN plugin leverages the features and benefits of Veeam Backup & Replication, such as compression, deduplication, encryption, scalability, and reliability12.

QUESTION 4
Veeam University Hospital has been testing the potential to keep their existing NFS storage at each site: however, they have encountered poor backup throughput performance between sites. What would be an effective way to improve the performance?

A. Have a mount server at each location.
B. Ensure the Gateway Server is located close to the NFS backup storage.
C. Place the backup proxy and Gateway Server together at the source site.
D. Ensure you use location tags at the target location.

Correct Answer: C
Section:
Explanation:
The Gateway Server is a component that acts as a data mover between the backup proxy and the NFS storage. By placing the backup proxy and the Gateway Server together at the source site, you can reduce the network traffic and latency between them, and improve the data transfer speed. The Gateway Server will read data from the NFS storage and send it to the backup proxy over a local connection, and the backup proxy will process and compress the data before sending it to the target site1

QUESTION 5
It has been determined that the onsite repositories need to be immutable. Which configuration would ensure SLA compliance and provide protection against ransomware?

A. Provide a Veeam Backup & Replication server with Veeam replication and enable XFS with immutability on NFS targets.
B. Leverage hardened repositories at both primary and secondary sites, and offload to object storage in a public cloud with immutability enabled.
C. Leverage ReFS repositories as a primary target with a backup copy to a second site and offload to object storage in a public cloud with immutability enabled.
D. Provide Veeam Backup & Replication servers at two locations and leverage object storage.

Correct Answer: B
Section:
Explanation:
Immutable repositories are backup storage locations that prevent unauthorized modifications or deletions of backup data, ensuring its integrity and recoverability.Immutable repositories are essential for protecting backups against ransomware attacks, accidental deletions, or malicious insiders1.
Veeam Backup & Replication supports several types of immutable repositories, such as hardened repositories, immutable object storage repositories, and immutable deduplicating storage appliances2. Among these options, the best configuration for ensuring SLA compliance and providing protection against ransomware is to leverage hardened repositories at both primary and secondary sites, and offload to object storage in a public cloud with

immutability enabled.
Hardened repositories are Linux-based repositories that use XFS file system with immutability flag to protect backup files from changes or removals.Hardened repositories can be used as primary or secondary backup targets, and can be combined with Veeam Scale-out Backup Repository to simplify backup management and optimize storage utilization3.
Object storage repositories are cloud-based repositories that use object storage services, such as Amazon S3, Microsoft Azure Blob Storage, or Google Cloud Storage, to store backup data. Object storage repositories can be used as secondary backup targets, and can leverage the immutability feature of the cloud provider to prevent backup data from being overwritten or deleted.
By using hardened repositories at both primary and secondary sites, you can achieve high availability and redundancy for your backup data, as well as fast and reliable restores. By offloading to object storage in a public cloud with immutability enabled, you can achieve long-term retention and compliance, as well as cost savings and scalability. This configuration also follows the 3-2-1-1 backup rule, which recommends having three copies of data, on two different types of media, with one copy off-site and one copy immutable.
You can find more information about immutable repositories and how to configure them in the following resources:
Immutable Backup Solutions: Linux Hardened Repository
Unstructured Data Backups in Immutable Repositories
Hardened Repository
[Immutability for Object Storage Repositories]
[3-2-1-1 Backup Rule]

QUESTION 6
examining the list of requirements, you notice that it is necessary to have backups encrypted. If you use Veeam's native encryption, which repository type will be the most impacted?

A. Dedupe repositories
B. Immutable Linux Repository with XFS reflink cloning
C. NFS share repository
D. Windows ReFS with block cloning

Correct Answer: A
Section:
Explanation:
The repository type that will be most impacted by using Veeam's native encryption is dedupe repositories. Dedupe repositories are backup repositories that use deduplication appliances or software to reduce backup size and optimize storage utilization. However, if you use Veeam's native encryption for backup jobs that target dedupe repositories, you will lose most of the deduplication benefits, as encrypted data blocks cannot be deduplicated effectively. Therefore, it is recommended to use either the encryption feature of the deduplication device or software, or avoid encryption altogether for dedupe repositories.

QUESTION 7
Which type of backup job will you need more informacion on to properly plan backup copy job settings later to make sure you are creating the required number of restore point per day offsite?

A. Bronze tier backup jobs
B. Silver tier backup jobs
C. Gold tier backup jobs
D. Laptop backup jobs

Correct Answer: C
Section:
Explanation:
The gold tier backup jobs have the most stringent recovery point objective (RPO) of one hour for image backup and 15 minutes for transaction log backup. This means that they need to run more frequently than the other backup jobs and create more restore points per day. Therefore, to properly plan the backup copy job settings, you will need more information on the gold tier backup jobs, such as the number of VMs, the size of backups, the change rate, the retention policy, and the bandwidth available for copying backups to the offsite location.

QUESTION 8
What information related to the virtual infrastructure is missing and must be collected during the discovery phase) (Choose 2)

A. Number of vSphere clusters
B. Backup window
C. Recovery time objective
D. Total of virtual machines
E. Number of scale-out Backup Repository extents currently used

Correct Answer: A, D
Section:
Explanation:
The number of vSphere clusters and the total of virtual machines are important information related to the virtual infrastructure that are missing and must be collected during the discovery phase. These information can help you estimate the backup performance, scalability, and resource requirements for the Veeam backup infrastructure. For example, you can use the number of vSphere clusters to determine how many Veeam backup servers and proxies you need to deploy and how to distribute the backup load among them. You can also use the total of virtual machines to calculate the total amount of data to be backed up, the storage space required, and the network bandwidth needed.

QUESTION 9
While going through the discovery data for the NAS environment, you determine several key metrics are missing for later deign and sizing. Which of the following should you collect from the customer about the data stored on the on the NAS per site? (Choose 3)

A. Retention requirements
B. Total number of files (in millions) to be backed up
C. Amount of source data before dedupe and compression
D. Number of shares and compressed source data
E. Large file size

Correct Answer: A, B, C
Section:

QUESTION 10
The company has committed to providing the numbers for source in-use data for gold tier virtual machines. In order to attempt to collect metrics for hourly gold tier backups, which of the following additional metrics are need for proxy sizing?

A. Yearly growth rate
B. Change rate
C. Datastore type
D. Operating system type

Correct Answer: B
Section:

QUESTION 11
You are examining the requirement: ''If possible, the data written must be unchangeable to prevent ransomware attacks.'' Which types of jobs do not support using immutability from S3 Object Lock or hardened repositories? (Choose two)

A. NAS backups
B. Linux Agent backup copy jobs
C. VMware backup jobs
D. Agent for Mac backups

Correct Answer: A, D
Section:
Explanation:
The types of jobs that do not support using immutability from S3 Object Lock or hardened repositories are NAS backups and Agent for Mac backups. These types of jobs do not have the option to enable immutability in their settings, unlike VMware, Hyper-V, Linux Agent, or Windows Agent backup jobs. Therefore, they cannot leverage the immutability feature of S3 Object Lock or hardened repositories to protect their backups from ransomware or malicious deletion.

QUESTION 12
The customer has stated that they plan on purchasing new physical server component and repository storage. What additional information is needed to define the implementation process later?

A. Will the customer need to unencrypt the backups before being copied to new storage?
B. How much backup data is stored on the old hardware?
C. Will the customer be able to retain the original storage until the existing restore points expire?
D. Is the customer repurposing old hardware?

Correct Answer: B
Section:
Explanation:
The additional information that is needed to define the implementation process later is how much backup data is stored on the old hardware. This information is important for designing and sizing the migration strategy and timeline for moving the backups from the old hardware to the new hardware. For example, you can use the amount of backup data to estimate how long it will take to copy or move the backups to the new storage devices. You can also use the amount of backup data to determine whether you need to use compression, deduplication, or WAN acceleration to optimize the migration traffic.

QUESTION 13
What components can help meet the following requirement: ''Alternative decryption capabilities on encrypted backups must be possible in the event of lost passwords''?

A. Veeam Backup & Replication's Configuration Backups
B. Veeam Backup Enterprise Manager
C. Veeam Backup & Replication's Extraction Explorer
D. Veeam Backup & Replication's Extract Utility

Correct Answer: B
Section:
Explanation:
The component that can help meet the requirement of alternative decryption capabilities on encrypted backups in the event of lost passwords 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 a password loss protection feature that enables authorized users to restore encrypted backups without entering passwords if they forget or lose them. This feature requires enabling password loss protection in Veeam Backup Enterprise Manager settings and assigning a security officer role to a user who can approve password recovery requests.

QUESTION 14
In addition to scanning all backup for malware before restoring, what additional Veeam capabilities must be included in the conceptual design for gold level systems? (Choose 2)

A. File indexing
B. SureBackup
C. Stage Restore
D. SureReplica
E. Secure Restore

Correct Answer: B, E

Section:
Explanation:
The additional Veeam capabilities that must be included in the conceptual design for gold level systems are SureBackup and Secure Restore. SureBackup is a feature that allows you to automatically verify the recoverability of your backups by running them in an isolated virtual lab. This can help you meet the requirement of testing the gold tier backups to verify recoverability. Secure Restore is a feature that allows you to scan your backups for malware before restoring them to the production environment. This can help you meet the requirement of scanning all backups for malware before restoring.

QUESTION 15
What information is missing form discovery?

A. What the current LAN bandwidth is at Fresno.
B. What backup transport mode is currently used.
C. What type of backup storage is currently used.
D. What the available bandwidth is between Fresno and Carson City.

Correct Answer: D
Section:
Explanation:
The information that is missing from discovery is what the available bandwidth is between Fresno and Carson City. This information is important for designing and sizing the backup copy jobs that need to run daily between the two sites. The available bandwidth can affect the backup copy performance, duration, and size. For example, you can use the available bandwidth to estimate how much data can be transferred between the sites within the backup copy window. You can also use the available bandwidth to determine whether you need to use compression, deduplication, or WAN acceleration to optimize the backup copy traffic.

QUESTION 16
What is the retention requirement for gold tier virtual machines?

A. Must have on-premises backup on hardened backup repositories.
B. Gold tier virtual machines have a recovery point objective of one hour for imagen backup and 15 minutes for transaction lob backup.
C. Eight weekly backups, three monthly backups and seven yearly backups.
D. Gold tier virtual machine retention must be 14 daily, eight weekly, three monthly and seven yearly backups.

Correct Answer: D
Section:
Explanation:
The retention requirement for gold tier virtual machines is that they must have 14 daily, eight weekly, three monthly and seven yearly backups. This requirement can be derived from the technical requirement of having eight weekly backups, three monthly backups, and seven yearly backups for regulatory purposes, as well as the business requirement of having daily backups for gold tier virtual machines.

QUESTION 17
What assumption can be made for the conceptual design?

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.

Correct Answer: C
Section:
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 18
Assuming that you put the backup repositories in the backup network only, what possible issue could arise?

A. Laptop agents cannot communicate with the repository.
B. The proxies cannot communicate with the repositories.
C. Capacity Tier Could offload is no possible.
D. SQL logs cannot be shipped to repository.

Correct Answer: A
Section:
Explanation:
A possible issue that could arise if you put the backup repositories in the backup network only is that laptop agents cannot communicate with the repository. This is because laptop agents are not part of the backup network, which is non-routable according to the existing technical environment. Therefore, laptop agents cannot access or write data to the backup repositories in the backup network unless there is a proxy or gateway server that can bridge the communication between them.

QUESTION 19
The customer states that Veeam Backup & Replication is on the production domain. What direct risks does this present?

A. Unable to use two-factor authentication.
B. Compromised Domain Admin could gain access.
C. Cannot access the REST interface.
D. Compromised Domain User could gain access.

Correct Answer: B
Section:
Explanation:
The direct risk of having Veeam Backup & Replication on the production domain is that a compromised Domain Admin could gain access to the backup server and its data. This could pose a serious security threat to the backup infrastructure and the customer data, as a malicious Domain Admin could delete, modify, or encrypt the backups, or restore them to a compromised environment. Therefore, it is recommended to isolate the backup server from the production domain and use a separate local administrator account for managing it.

QUESTION 20
While reviewing the technical requirements for gold tier backups requiring periodic backups every hour, you determine this goes against one of the other requirements and you need to get clarification on which on has priority. Which of the following does the recovery point objective requirement directly conflict with?

A. All backups must complete within the hours of 5 p.m. to 8 a.m. local time.
B. Silver tier backups must be tested to verify recoverability.
C. Eight weekly backups, three monthly backups and seven yearly backups should be retained for regulatory requirements.
D. All backups must be copied across site of the current backup window to avoid any backup performance issues.

Correct Answer: A
Section:
Explanation:
The recovery point objective (RPO) requirement of periodic backups every hour for gold tier virtual machines directly conflicts with the technical requirement of all backups must complete within the hours of 5 p.m. to 8 a.m. local time. This is because these two requirements are mutually exclusive, as hourly backups would need to run during the daytime as well as the nighttime, while the backup window only allows backups to run during the nighttime. Therefore, you need to get clarification from the customer on which requirement has priority and how to adjust the other one accordingly.

QUESTION 21
Looking at the existing error, you suspect that most of the issues could be resolved with different repositories. Assuming the repositories will be able to accomplish much higher throughput, what new issue might come up?

A. The bandwidth between sites might not be sufficient.
B. The repository space consumption could decrease
C. The production firewall could become a bottleneck
D. The increased backup speed could completely bring down production storage.

Correct Answer: A
Section:
Explanation:
If the repositories are able to accomplish much higher throughput, a new issue that might come up is that the bandwidth between sites might not be sufficient to support the backup copy jobs that need to run daily between Fresno and Carson City. This could cause the backup copy jobs to fail, take longer than expected, or consume too much network resources. Therefore, it is important to measure the available bandwidth between the sites and compare it with the backup copy data size and window. If the bandwidth is not sufficient, some possible solutions are to use compression, deduplication, or WAN acceleration to reduce the backup copy traffic.

QUESTION 22
Which of the following could cause failures to meet the requirement to test gold tier backups?

A. Backup jobs run every hour.
B. You cannot firewall traffic between vLANs in the SureBackup job configuration.
C. The LAN bandwidth is not sufficient for vPower NFS datastores.
D. There may be too many networks.

Correct Answer: B
Section:
Explanation:
A possible cause of failures to meet the requirement to test gold tier backups is that you cannot firewall traffic between vLANs in the SureBackup job configuration. This could prevent the gold tier virtual machines from communicating with each other or with other required services in the isolated virtual lab. For example, if a gold tier virtual machine needs to access a database server or a domain controller in another vLAN, it might fail to start or function properly in the SureBackup job. Therefore, it is important to ensure that all necessary vLANs and network settings are configured correctly in the SureBackup job.

QUESTION 23
Based on the customer's security requirements around restore capabilities, which components should be deployed?

A. Veeam Business view with RBAC policies defined
B. The Veeam Backup & Replication console with RABC policies defined
C. Veeam Oracle integrations
D. Enterprise Manager with granular RABC policies defined

Correct Answer: D
Section:
Explanation:
The component that should be deployed based on the customer's security requirements around restore capabilities is Enterprise Manager with granular RBAC policies defined. Enterprise Manager is a web-based interface that allows centralized management of multiple Veeam backup servers. It also provides granular RBAC policies that enable control over user permissions and access to restore 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. You can also define custom scopes and rules for each role to limit their access to specific objects, jobs, or actions.

QUESTION 24
During discovery, it is determined that a group of MSSQL systems are running in an Always-On cluster and sensitive to virtual machine stun. How should these systems be configured for backups?

A. Deploy Veeam agents configured for failover clustering.
B. Perform a regular virtual machine backup without application aware processing.
C. Enable application aware processing on the virtual machine backup job.
D. Deploy Veeam agents in server mode.

Correct Answer: A
Section:
Explanation:
The best way to configure backups for a group of MSSQL systems running in an Always-On cluster and sensitive to virtual machine stun is to deploy Veeam agents configured for failover clustering. Veeam agents can provide application-aware processing and transaction log backup for MSSQL servers, as well as support for failover clustering and cluster shared volumes. Veeam agents can also reduce the impact of virtual machine stun by performing backups at the guest OS level, without using VMware snapshots.

QUESTION 25
To demonstrate SLA compliance during audits and protection against exposure to personally identifiable information, which configuration would verify this is possible in the event of exposure?

A. Implement Veeam Backup & Replication servers at one location and leverage hardened repositories as a primary target with a backup copy to a second site.
B. Create secure restore to ensure malware-free backups.
C. Create a virtual lab environment and periodically perform staged restores with custom scripts.
D. Scan backups with Veeam ONE to remove personally identifiable information.

Correct Answer: C
Section:
Explanation:
The configuration that would verify the SLA compliance during audits and protection against exposure to personally identifiable information in the event of exposure is to create a virtual lab environment and periodically perform staged restores with custom scripts. A virtual lab is an isolated environment where you can run your backups or replicas without affecting the production environment. A staged restore is a process that allows you to run custom scripts on the restored data before publishing it to the production environment. By using these features, you can demonstrate that your backups are recoverable and compliant with legal regulations, as well as remove or mask any sensitive data before restoring it.

QUESTION 26
Considering the security, throughput, and retention requirements, what would be part of an acceptable backup repository design? (Choose 2)

A. Use a backup job directly to an object storage appliance
B. Use backup jobs to Hardened Linux XFS-based repositories at the same site as the source data.
C. Use Backup copy jobs to Hardened Linux XFS-based repositories at the secondary site.
D. Use Backup copy jobs to Hardened Windows ReFS-based repositories at the secondary site.
E. Use a backup job directly to a deduplication appliance.

Correct Answer: B, C
Section:
Explanation:
The backup repository design that would meet the security, throughput, and retention requirements is to use backup jobs to Hardened Linux XFS-based repositories at the same site as the source data and use Backup copy jobs to Hardened Linux XFS-based repositories at the secondary site. A Hardened Linux repository is a type of backup repository that provides immutability and ransomware protection for backup files by using XFS file system features and Linux access control mechanisms. A Backup copy job is a type of backup job that copies backups from one repository to another, either on-site or off-site, with different retention settings. By using these features, you can ensure that your backups are secure, efficient, and compliant with regulatory and business needs.

QUESTION 27
What information related to sizing the NAS infrastructure is missing and must be collected during the discovery? (Choose 2)

A. Total number of network shares
B. Size of the source data set
C. Backup windows
D. Recovery point objective
E. Number of Scale-out Backup Repository extents currently used

Correct Answer: B, D
Section:
Explanation:
The information related to sizing the NAS infrastructure that is missing and must be collected during the discovery are the size of the source data set and the recovery point objective (RPO). These information are important for designing and sizing the NAS backup jobs and repositories. For example, you can use the size of the source data set to estimate how much storage space and network bandwidth are required for backing up NAS devices. You can also use the RPO to determine how frequently you need to run NAS backup jobs and how many restore points you need to keep on the backup repositories.

QUESTION 28
In order to improve the likelihood that a ransomware attack on the Veeam infrastructure will not be successful, which of the following should Veeam University Hospital do?

A. Remove all remote access from Veeam administrators.
B. Implement a strong password security policy on shared administrative accounts.
C. Ensure that none of the Veeam components are on the production Active Directory domain.
D. Protect the Veeam components on the production Active Directory Forest with multi-factor authentication.

Correct Answer: D
Section:
Explanation:
* MFA is a security method that requires users to provide two or more pieces of evidence to verify their identity, such as a password, a code, a token, or a biometric factor3.
* MFA adds an extra layer of protection against ransomware attacks, as it prevents attackers from accessing the Veeam components even if they manage to steal or guess the passwords of the administrative accounts12.
* MFA also helps to prevent unauthorized changes or deletions of backup data, as well as unauthorized restores or failovers of VMs or applications12.
The other options are not as effective or feasible, as they either do not provide enough security, limit the functionality, or disrupt the integration of the Veeam infrastructure.

QUESTION 29
The customer has asked you to review their existing backup storage. Jobs show the target is the bottleneck. What steps should you take to improve performance?

A. Make sure the gateway has enough CPU, RAM and enough task slots assigned.
B. Put a repository component on its own physical server, ensuring it has enough CPU, RAM and task slots assigned.
C. Look at the transport modes used.
D. No action is needed. It is an optimal design already, there is always something that is bottleneck.

Correct Answer: A
Section:
Explanation:
The gateway is a component that acts as a data mover between the backup proxy and the backup repository. If the gateway does not have enough CPU, RAM and task slots assigned, it may not be able to handle the incoming data from the backup proxy efficiently, and cause a bottleneck at the target. By increasing the resources and task slots for the gateway, you can improve its performance and throughput, and reduce the load on the target2

QUESTION 30
While looking through the requirements regarding database servers, you see that Veeam should manage the database backups and logs. Which configurations should you check for that are unsupported base on the technical requirements?

A. Physical windows server with Oracle.
B. Oracle cluster configurations.
C. Virtual machines with physical raw device mapping.
D. Virtual machines with Oracle Automatic Storage Management storage.

Correct Answer: A
Section:
Explanation:
The configuration that is unsupported by Veeam Plug-in for Oracle RMAN based on the technical requirements is physical windows server with Oracle.Veeam Plug-in for Oracle RMAN only supports Oracle databases running on Linux, Solaris, or AIX operating systems1. The other configurations are supported by either Veeam Plug-in for Oracle RMAN or Veeam Backup & Replication.Reference:Veeam Plug-in for Oracle RMAN,Oracle | Veeam Backup & Replication Best Practice Guide.

QUESTION 31
While examining the details for the remote sites each with a single server, you are trying to determine if a local repository will be needed or if backups can be transferred back to the central corporate site in the region. Which of the following requirements will act as a constraint on your decision?

A. The backup solution must not require proprietary hardware or storage.
B. All backups must complete between 8 p.m. and 6 a.m. local time.
C. Data locality and privacy laws local to each branch office must be followed.
D. A copy of backup data must reside in a public cloud local to each region.

Correct Answer: C
Section:
Explanation:
The requirement C will act as a constraint on the decision of whether to use a local repository or not for the remote sites. Data locality and privacy laws may vary by country or region, and may impose restrictions on where the backup data can be stored or transferred. For example, some countries may prohibit the export of personal data outside their borders, or require encryption or anonymization of sensitive data. Therefore, the Veeam solution must comply with these laws and regulations, and may need to use a local repository for each remote site, or use a cloud provider that has a local presence in each region. The other requirements are not constraints, as they can be met with either a local or a central repository, using the features and options of the Veeam solution.Reference:Veeam Certified Architect 2022 Exam Guide, page 11;Veeam Backup & Replication v11: Architecture and Design course, module 5.

QUESTION 32
Veeam Financial Services has determined that the recovery point objective for disaster recovery is one minute for two business critical virtual machines. What Veeam components will be required at each site?

A. Veeam CDP proxies.
B. Veeam guest interaction proxies.
C. Veeam backup repositories
D. Veeam backup proxies.

Correct Answer: A
Section:
Explanation:
The Veeam component that will be required at each site for disaster recovery with a one minute recovery point objective is the Veeam CDP proxy.Veeam CDP proxy is a data mover that transfers data between the source and target hosts, using VMware vSphere APIs for I/O Filtering (VAIO) to capture the changes in real time1.Veeam CDP proxy can achieve near-zero recovery point objectives for business critical virtual machines, as well as provide short-term restore points and data encryption2.The other components are not required for this scenario, as they are used for different purposes, such as guest processing, backup storage, or backup jobs3.Reference:VMware CDP Proxies,Continuous Data Protection,Backup Proxies.

QUESTION 33
Which tier(s) of Veeam Financial Services' backups will require SureBackup jobs?

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

Correct Answer: B
Section:
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 34
Based on customer recovery requirements, which component will help them meet their stated objectives?

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.

Correct Answer: B
Section:
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 35
You are trying to determine which feature would work the reliably for excluding the H: drive on MSSQL server virtual machines. The MSSQL servers are built on demand, not from virtual machine templates. Which is the preferred method to achieve this requirement?

A. Set up VMDK exclusion for the disk on which the H: resides in the Virtual Machines > Exclusions page for each virtual machine.
B. Use the Exclusion tab under Guest Processing > Applications for VM backups to exclude the H: volume in MSSQL jobs.
C. Use Veeam Agent Backups and set up Volume Backups and include everything but H:
D. Use Veeam Agent Backups and use the Exclusions tab under Gest Processing > Application for MSSQL jobs.

Correct Answer: A
Section:
Explanation:
The preferred method to achieve the requirement of excluding the H: drive on MSSQL server virtual machines is to set up VMDK exclusion for the disk on which the H: resides in the Virtual Machines > Exclusions page for each virtual machine. This method allows you to exclude specific virtual disks from being processed by backup jobs based on their SCSI IDs or disk labels. This can save backup time and storage space by skipping unnecessary data. This method also works reliably regardless of whether the MSSQL servers are built on demand or from virtual machine templates.

QUESTION 36

During architecture planning, Veeam Life and Indemnity decides that recovery point objective of gold tier machines should change from one hour to three hours with daily retention set to seven days. What will be impact on the Veeam design?

A. Proxies will require fewer resources
B. More proxy servers will be required
C. Repositories will require more resources.
D. The Veeam database size will increase.

Correct Answer: A
Section:
Explanation:
If the recovery point objective (RPO) of gold tier machines changes from one hour to three hours with daily retention set to seven days, the impact on the Veeam design is that proxies will require fewer resources. This is because the backup frequency and the number of restore points for gold tier machines will decrease, which means that less data will need to be processed and transferred by the proxies. Therefore, the proxies will have lower CPU, memory, disk, and network utilization and can handle more backup tasks with the same resources.

QUESTION 37
The decision has been made to separate out proxies for gold tier and silver/bronze tier. Which reason below justifies the decision?

A. Gold tier virtual machines are in their own VMware cluster
B. Gold tier virtual machines run frequently and should not share resources with lower priority virtual machines
C. Gold tier virtual machines are on their own VMware Datastores.
D. Gold tier virtual machines require their own backup server

Correct Answer: B
Section:
Explanation:
The reason that justifies the decision to separate out proxies for gold tier and silver/bronze tier is that gold tier virtual machines run frequently and should not share resources with lower priority virtual machines. This is because gold tier virtual machines have a high RPO of one hour or less, which means that they need to run backup jobs more often than silver/bronze tier virtual machines. Therefore, they should have dedicated proxies that can process their data without competing with other backup jobs for proxy resources. This can improve backup performance, reliability, and scalability for gold tier virtual machines.

QUESTION 38
Based on additional discovery, it was determined that a few critical workloads need to maintain a less than five-minute recovery point objective. Which of the following would be the recommended method to replicate VMware virtual machines?

A. Veeam backup copy with immediate mode
B. Veeam Continuous Data Protection.
C. Veeam Image-based replication
D. Custom PowerShell scripting.

Correct Answer: B
Section:
Explanation:
The recommended method to replicate VMware virtual machines with a less than five-minute RPO is Veeam Continuous Data Protection (CDP). CDP is a feature that allows near-continuous replication of VMware virtual machines to a secondary site or cluster with minimal data loss and downtime. CDP uses VMware vSphere APIs for I/O Filtering (VAIO) to capture every write operation from the source VMs and send them to the target VMs in near real-time. CDP can achieve RPOs as low as seconds and enable fast failover and failback in case of a disaster.

QUESTION 39
Based on Customer requirements, how should virtual machine backups be scoped? (Choose 2)

A. Create backups based on tags.
B. Create backups based on protection groups create with a CSV file.
C. Create backups based on resource pools
D. Create backups jobs with same retention requirements.
E. Scope each backup based the software running in each workload

Correct Answer: A, D
Section:
Explanation:
The methods that should be used to scope virtual machine backups based on customer requirements are to create backups based on tags and to create backup jobs with same retention requirements. Creating backups based on tags allows dynamic scoping of backups based on VMware tags assigned to virtual machines. This can simplify backup management, as new or modified virtual machines will be automatically included or excluded from backup jobs based on their tags. Creating backup jobs with same retention requirements allows consistent application of backup policies based on the backup tiers defined by the customer. This can ensure compliance with regulatory and business needs, as different tiers of virtual machines will have different retention periods and restore points.