Vendor: Veeam

Exam Code: VMCA2022

Exam Name: Veeam Certified Architect 2022

Version: DEMO

QUESTION 1
Case Study 1, Veeam Life and Indemnity

Executive Summary:

Veeam Life and Indemnity is expanding its existing Veeam backup infrastructure to protect additional virtual machines, physical server and NAS workloads at their Fresno, CA and Carson City, NY data centers.
The original installation and configuration of Veeam software occurred two years ago. Since the installation, the organization has grown, and as a result, the Veeam Infrastructure needs to be resized to accommodate the existing and new workloads.
For the past three months, Veeam Life and Indemnity has noticed that they are having issues with backups completing within the allotted backup window. Only 40% of backup jobs complete successfully, so they have broken the backups into two sets, and they run them on alternating days. They have also stopped all backups for their development environment. In addition, the original configuration required a daily backup copy job, but to the issue with backups completing, this has been modified to run only on Sundays. They have also noticed a degradation in storage performance and are having to purchase new storage on a quarterly basis to accommodate data growth.

Solution Concept:

Veeam Life and Indemnity is upgrading Veeam Backup & Replication to the last version. They are also replacing all legacy physical hardware and storage with current generation equipment.
Veeam Life and Indemnity wants to be able to ensure that all backups, including production and dev test workloads, can run every night and that all backups complete within the required backup window. In addition, Veeam Life and Indemnity would like to run daily copy jobs to ensure that a copy of all backed up data resides at both physical sites.
Veeam Life and Indemnity has also expressed concern about the threat of ransomware. They have not experienced a data breach of any kind but would like to ensure the ability of recover should one occur.

Existing Technical Environment:

Veeam Life and Indemnity has VMware clusters in all locations. These clusters are broken into two categories: general use virtual workloads, and application specific workloads, such as MSSQL and Oracle.
All customer data is subject to government regulation and must be kept secure at all times.
Veeam Life and Indemnity has a proprietary CRM system that must be quiesced prior to backup.
All email is hosted in Office 365.
All database servers are virtualized.
All virtual machines are categorized as either gold, silver, or bronze, with different service-level agreements based on tier.
All backups currently encrypted in flight and at rest. Internet connectivity at both sites is current 1 Gbps, with plans to increase to 2 Gbps soon. All field sales reps are assigned a company laptop that runs a CRM client. The LAN at each location supports up to 40 Gbps bandwidth. All backups are currently written to Scaled-out Backup Repositories with each extent residing on a CIFS share.
Each department has its own vLAN, with a total of 30 vLANs for production traffic.
A single management vLAN is stretched between sites.
All unstructured data resides either on 10 NFS shares on the company's incumbent NAS devices, or Windows file servers as file shares.
VMware uses vSAN for VM datastores.
All vLAN must traverse a firewall to communicate, and the backup network itself is no routable. All network traffic between clusters is required to traverse a firewall.
The firewall devices can support up to 20 Gbps.

Business Requirements:

Due to limited manpower, all backups should be dynamically scope. All backups must be copied across site outside of the current backup window to avoid any backup performance issues.
Due to the sensitivity of customer data, tier 1 helpdesk personnel must not be able to access these backups. They should have access to restore non-customer data. Backup administrators are subject toa rigorous background check and should be the only staff able to perform restores of confidential customer data.
For any legal issues, fast and timely discovery from backup data should be supported. For security purposes, all storage should be hardened to prevent data breaches. Remote sales staff should have the ability to start a backup oh their devices.
Due to regulatory requirements, audits must be performed periodically to ensure successful and consistent backups, as well adherence to security policies.

Technical Requirements:

All backups must complete within the hours of 5 p.m. to 8 a.m. local time Backup copy jobs must successfully complete daily outside of the backup window.
Gold tier virtual machines have a recovery point objective of the one hour for image backup, and 15 minutes for traction log backup, with a recovery time objective of four hours. Silver tier virtual machines have a recovery point objective of 24 hours, with a recovery time objective of eight hours.
Bronze tier virtual machines have a recovery point objective of seven days, with no defined recovery time objective.
NAS devices and file servers have a recovery point objective of four hours, with no specified recovery time objective.
Eight weekly backup, three monthly backups, and seven yearly backups should be retained for regulatory requirements.
All data must be encrypted in flight and rest.
Alternative decryption capabilities on encrypted backups must be possible in the event of lost passwords.
Role Based Access Control must be used to prevent unauthorized access to backup data. New storage must be hardened to prevent intrusion, and if possible, the data written must be unchangeable to prevent ransomware attacks.
All backups must be scanned prior to any restore operations for malware. All gold level systems must have a custom script run before restore to ensure compliance to specific legal statutes.
Gold tier backups must be tested to verify recoverability. Only silver tier systems should be indexed during backups, with the exception of laptops belonging to the sales field.
All personal files on laptops should be excluded from backup All MSSQL server backups should exclude the H: drive.

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

Answer: C
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 2
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

Answer: AD
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 3
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

Answer: ABC

QUESTION 4

Case Study 2, 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.

What information is necessary for designing a solution and must be gathered during discovery? (Choose 3)
Size of the backup create by the incumbent backup solution.

A. Operating systems used to run the workloads.
B. Allowed backup windows.
C. Size of IT team.
D. Amount of used disk space.
E. Amount of disk space provisioned.

Answer: ABE
Explanation:
To design a solution that meets the needs and requirements of Veeam University Hospital, you need to gather some information during the discovery phase. This information will help you to understand the current state of the environment, the goals and expectations of the stakeholders, and the constraints and challenges of the project.
According to the Veeam Backup & Replication Best Practice Guide1, some of the information that is necessary for designing a solution and must be gathered during discovery are:
- Operating systems used to run the workloads. This information will help you to determine the compatibility and supportability of the workloads with Veeam products and features, as well as the licensing and configuration requirements.
- Allowed backup windows. This information will help you to plan and schedule the backup jobs according to the availability and performance of the workloads, as well as the service level agreements (SLAs) and recovery point objectives (RPOs) of the organization.
- Amount of used disk space. This information will help you to estimate the backup storage requirements, as well as the backup compression and deduplication ratios, based on the type and size of the data.

QUESTION 5
While examining the requirements for offsite copies and archives, you notice that it might be assumed that the offsite copies should only go to a cloud provider that supports immutability. Which of the stated requirements needs additional information to help clarity the customer

expectation?

A. For archival purposes, 12 monthly backups and three yearly backups must be storage off site.
B. For quick restores and recovery, at least one copy of protected data must reside on-premise.
C. Backups must take advantage of public cloud storage for long term archival purposes.
D. Due to the threat of ransomware, at least one immutable or air gapped copy of protected data must reside off site.

Answer: C
Explanation:
To design a solution that meets the offsite copies and archives requirements for Veeam University Hospital, you need to clarify some of the assumptions and expectations of the customer. This will help you to avoid any misunderstandings or conflicts that may arise during the implementation or operation of the solution.
According to the Veeam Backup & Replication Best Practice Guide, offsite copies and archives are two different concepts that serve different purposes. Offsite copies are backups that are stored in a different location than the primary backup storage, and are used for disaster recovery purposes. Archives are backups that are stored for a longer retention period than the regular backups, and are used for compliance or historical purposes.

QUESTION 6
What information related to the virtual infrastructure is missing and must be collected during the discovery phase? (Choose 2)

A. Local area network speed.
B. Recovery point objective.
C. Backup window.
D. Size of the source data set.
E. number of Microsoft Exchange mailboxes.

Answer: AD
Explanation:
To design a solution that meets the virtual infrastructure requirements for Veeam University Hospital, you need to collect some information during the discovery phase. This information will help you to understand the configuration and performance of the VMware clusters, the size and type of the data, and the backup and recovery objectives.
According to the Veeam Backup & Replication Best Practice Guide, some of the information related to the virtual infrastructure that is missing and must be collected during the discovery phase are:
- Local area network speed. This information will help you to determine the network bandwidth and throughput that are available for backup and replication traffic, as well as the impact of backup and replication activities on the network performance and latency.
- Size of the source data set. This information will help you to estimate the backup storage requirements, as well as the backup compression and deduplication ratios, based on the size and type of the data.

QUESTION 7
while going through the discovery data for the NAS environment, you determine several key metrics are missing for later design and sizing. Which of the following should you collect from the customer about the data stored on the NAS per site? (Choose 2)

A. Which version of SMB protocol the NAS supports.

B. Amount of source data after dedupe and compression.
C. Total number of files (in millions) to be backed up.
D. Amount of source data before dedupe and compression.
E. Largest file size.

Answer: CE
Explanation:
To design a solution that meets the NAS environment requirements for Veeam University Hospital, you need to collect some information during the discovery phase. This information will help you to understand the characteristics and performance of the NAS systems, the size and type of the data, and the backup and recovery objectives.
According to the Veeam Backup & Replication Best Practice Guide, some of the information that you should collect from the customer about the data stored on the NAS per site are:
- Total number of files (in millions) to be backed up. This information will help you to estimate the backup storage requirements, as well as the backup performance and scalability, based on the number and distribution of files.
- Largest file size. This information will help you to determine the optimal backup block size and alignment, as well as the backup compression and deduplication ratios, based on the size and type of files.

QUESTION 8
Case Study 3, Veeam Financial Services

Solution Overview

Veeam Financial Services will replace the current backup solution with Veeam Backup & Replication. They plan to protect their virtual infrastructure in New York, San Francisco, London and Singapore. Each branch houses a single physical Windows server that will also need to be backed up. With their stance towards the cloud, Veeam Financial Services would also benefit from any cloud integration where possible. A user portal is also being developed that will enable limited self-service restores for its user base.

Business requirements

Any backup solution should leverage public cloud storage. Mission-critical applications should not be affected by backup processes. To reduce the workload on the backup management team, every possible way to automate the solution should be used. To meet regulatory requirements, backups must be retained for four years. Veeam Financial Services has plans to develop a self-service portal and integration with the new backup solution is required. Ticket creation in their current help desk system must be automated based on alerts generated. Local privacy and data locality laws must be followed for each branch. Due to the confidential nature of internal financial data, all security features available in backup software should be utilized. Backups should be dynamically scoped to reduce administrative overhead. The backup solution should not require proprietary hardware or storage.

Existing technical environment

Each site has multiple VMware clusters, including a management cluster, general purpose clusters, application clusters, and Linux/Oracle clusters.
Each site has a virtualized stock trading application that has extremely high disk I/O that is very latency sensitive.
A custom financial application resides on AIX servers at each site.
There is a 2 Gbps link between all major sites.
Each branch office has a 100 Mbps connection to the nearest main site.

Clustered NAS devices at each primary site house financial transaction and regulatory information, as well as the company's document repository.
Each NAS cluster has an average of 100 shares, consisting of NFS 4.1 and SMB 3.0 shares.
All traffic routed between LANs must pass through a firewall.
Local network bandwidth at each site is 10 Gbps.
Each primary site has multiple SQL instances, to include physical, virtual and always-on clusters.
Each site has multiple physical and virtual Oracle servers. o Each region has a separate Active Directory with no trusts established in any other region to meet regulatory requirements.
Current backup storage is proprietary deduplication appliances that only support the current vendor's software.
Each site has 10 production VLANs, one management LAN and three VLANs for physical servers.
In North America, there is one VLAN that spans between New York and San Francisco.
All virtual machines reside on a combination of SAN storage and NFS datastores.
Each location has multiple physical Windows servers that act as file servers.
VMware clusters can communicate, but all traffic between them must pass through a firewall.

Technical requirements

All backups should be completed between 7 p.m. and 7 a.m. local time. o All workloads should be dynamically grouped for ease of administration when creating and maintaining backup jobs.
A copy of the backup data should reside in a local public cloud for each region.
All backup repositories should be hardened.
Any space-saving capabilities within the backup product should be leveraged.
Any data transporter should scale horizontally rather than incrementally.
The disaster recovery capabilities of the solution shall be utilized in the North American region between New York and San Francisco.
Any storage integration shall be implemented in software.
An immutable copy of all backups must be stored off-site.
Twelve weekly backups, six monthly backups, and seven annual backups must be stored for archival purposes.
Oracle backups must be native to Veeam software, with no Oracle administrative plug-ins.
All data must be encrypted in flight and at rest.
There must be three copies of data, on two different types of media, with one copy off-site that is unalterable or air-gapped.
Only non-domain accounts are allowed for vendor components.
Depending on regulatory requirements, some data may need to be deleted from backups before a restore can be performed.
All backups must be scanned for malware prior to performing a restore.
Gold level machines have a recovery time target of 30 minutes and a recovery point target of one hour.
Silver level machines have a recovery time objective of six hours and a recovery point objective of 24 hours.
Bronze level machines, which consist of development machines and field portables, have a recovery point target of seven days, with no recovery time target set.
On-site storage must accommodate three years of projected capacity.
All gold and silver machines require backups to be verified.
All laptop backups must be managed completely without user interaction.
Alternate backup methods should be used for virtual machines that are mission critical and susceptible to stuns

While examining the requirements for archived backups, you notice that a copy should go to a cloud provider. Which of the stated requirements needs additional information to help clarify the customer expectation?

A. 12 weekly backups, six monthly backups and seven yearly backups must be stored for archival

purposes.

B. There must be the copies of data, on two different kinds of media, with one off site copy that is either air gapped or immutable.
C. A copy of backup data must reside in a public cloud local to each region.
D. All backup repositories must be hardened.

Answer: C
Explanation:
The requirement C is vague and needs more clarification from the customer. It does not specify which public cloud provider, service, or storage tier should be used for the backup data. It also does not indicate how the backup data should be transferred, secured, or managed in the public cloud.

QUESTION 8
What additional stakeholders would it be beneficial to talk to in order to collect business and technical requirements related to virtual infrastructure? (Choose 2)

A. Database administrators
B. Web design team
C. Operations team
D. Sales staff
E. Laptop users

Answer: AC
Explanation:
Database administrators and operations team are the most relevant stakeholders to talk to in order to collect business and technical requirements related to virtual infrastructure. Database administrators can provide information about the performance, availability, and recovery needs of the SQL and Oracle servers, as well as the custom financial application on AIX servers. Operations team can provide information about the network bandwidth, firewall rules, storage capacity, and backup windows for the virtual machines and NAS devices.

QUESTION 10
What information related to the virtual infrastructure is missing and must be collected during the discovery? (Choose 2)

A. Recovery time objective
B. Total number of virtual machines
C. Speed of Fibre Channel fabric
D. Backup window
E. Size of the source data set

Answer: BE
Explanation:
The information related to the virtual infrastructure that is missing and must be collected during the discovery are the total number of virtual machines and the size of the source data set. These are essential metrics for sizing the backup components, such as proxies, repositories, and transporters, as well as estimating the backup storage requirements and bandwidth consumption.

QUESTION 11
What additional information is necessary for sizing the backup solution and must be gathered

during further discovery? (Choose 2)

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: BC
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.

QUESTION 12
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.

Answer: A
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 systems.

QUESTION 13
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.

Answer: C
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.

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**