KTest

更に上のクオリティ　更に上のサービス

問題集

http://www.ktest.jp

1年で無料進級することに提供する

Exam : **VMCA2022**

Title : Veeam Certified Architect 2022

Version : DEMO

1. Topic 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.

In order to improve the likelihood that a ransomware attack on the Veeam infrastructure will not be successful, which of the following should Veeam Life and Indemnity do?
A. Implement a strong password security policy on shared administrative accounts
B. Remove all remote access from Veeam administrators.
C. Ensure that none of then Veeam components are on the production Active Directory domain
D. Protect the Veeam components on the production Active Directory Forest with multi-factor authentication
Answer: D
Explanation:
The action that Veeam Life and Indemnity should take to improve the likelihood that a ransomware attack on the Veeam infrastructure will not be successful is to protect the Veeam components on the production Active Directory Forest with multi-factor authentication. Multi-factor authentication (MFA) is a security mechanism that requires users to provide two or more pieces of evidence to prove their identity before accessing a system or resource. MFA can prevent unauthorized access to the Veeam components even if the user credentials are compromised by ransomware or other means.

2.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.
References: [Backup Copy], [Backup Methods], [Continuous Data Protection]

3.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.
Answer: A
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.

4.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: A B C

5.When deciding on the design of the primary backup repository, which option best fits the requirements in the case study?
A. Dedupe appliance leveraging vendor API for access
B. Public cloud storage with S3 object-lock for immutability
C. Windows repository using ReFS integration, single-use credential and persistent VSS snapshot
D. Linux Repository using XFS integration, single-use credentials, and immutability
Answer: D
Explanation:
The best option for the primary backup repository design that fits the requirements in the case study is a Linux Repository using XFS integration, single-use credentials, and immutability. A Linux Repository is a type of backup repository that uses a Linux server as a backup target. A LinuxRepository can leverage XFS integration to enable fast creation and transformation of synthetic full backups by using XFS file system features such as reflink and copy-on-write. A Linux Repository can also use single-use credentials to enhance security by generating unique credentials for each backup job session. A Linux Repository can also provide immutability and ransomware protection for backup files by using Linux access control mechanisms such as immutable flag or chattr command.