Exam : **VMCE+_v13**

Title : Veeam Certified Engineer Plus v13

Version : DEMO

1.Scenario: A healthcare organization wants to deploy a new Linux Hardened Repository to protect against ransomware. They need to prepare the physical server according to Veeam's strict security guidelines before adding it to the VBR console.
Which two actions are mandatory prerequisites or best practices for configuring a Linux Hardened Repository? (Choose two)
A. Format the dedicated backup storage volume using the XFS file system with the reflink feature enabled to fully support Fast Clone.
B. Assign explicit ownership and exclusive permissions of the backup directory path to the designated non-root single-use credential account.
C. Ensure the SSH daemon remains actively running and accessible so the Veeam transport service can routinely update immutable time flags.
D. Add the designated single-use Veeam account to the administrative root group to ensure the initial transport service deployment succeeds.
E. Enable the Veeam CDP filter driver directly within the Linux kernel modules to proactively intercept and block ransomware write IOPS.
Answer: A, B
Explanation:
Correct Logic (A, B): To properly deploy a Linux Hardened Repository (LHR), the underlying volume should be formatted as XFS with Block Cloning (reflink) enabled for performance and space efficiency. Furthermore, Veeam strictly requires using Single-Use Credentials, meaning the specified non-root account (e.g., `veeamuser`) must have explicit ownership of the backup directory to write data and set immutability flags via the local service.
Teardown of Distractors:
C is incorrect: SSH should be completely disabled or tightly restricted after the initial deployment. The local `veeamimmureposvc` service updates time flags autonomously; it does not rely on persistent SSH connections from the VBR server.
D is incorrect: Adding the Veeam account to the root group or the `sudoers` file completely invalidates the zero-trust architecture. If VBR is compromised, the attacker could use those elevated privileges to destroy the repository.
E is incorrect: CDP (Continuous Data Protection) filter drivers are deployed on ESXi hosts to intercept vSphere I/O for replication purposes. They have absolutely nothing to do with Linux storage repositories or ransomware interception.

2.Scenario: An enterprise uses a Scale-Out Backup Repository (SOBR) with a local performance tier and an AWS S3 capacity tier. The operational policy states that backups must be kept locally for 14 days, after which they should solely reside in the cloud. The administrator configured the Capacity Tier with the "Move" policy set to 14 days. However, the performance tier is rapidly running out of space, and 20-day-old backup files are still residing locally.
What is the most likely technical reason the 20-day-old backups have not been moved?
A. The SOBR performance tier has exceeded the 90% capacity warning threshold, which automatically suspends all outbound data movement to the cloud.
B. The targeted AWS S3 bucket was deployed without Object Lock enabled, causing the Veeam movement engine to reject the transaction for compliance.
C. The 20-day-old backup files belong to an active, unsealed backup chain that still relies on those

specific blocks for ongoing incremental operations.
D. The associated backup job is utilizing a proprietary transport mode algorithm, which restricts the SOBR Capacity Tier move policy from executing.
Answer: C
Explanation:
Correct Logic (C): The SOBR "Move" policy operates strictly on *sealed* backup chains (inactive chains). If a backup job is configured as Forever Forward Incremental, the chain is never completely sealed until a synthetic or active full is created. Because the active chain still relies on the oldest full backup and its subsequent incrementals to function, Veeam will absolutely not move those files to the Capacity Tier, regardless of how many days have passed.
Teardown of Distractors:
A is incorrect: Exceeding a capacity threshold on the performance tier does not suspend outbound cloud movement. In fact, running out of space is exactly why the Move policy exists.
B is incorrect: While Object Lock is required for Immutability, the standard "Move" policy will function perfectly fine without Object Lock enabled on the S3 bucket.
D is incorrect: Transport modes (NBD, HotAdd, Direct SAN) only dictate how data is read from the production datastore to the proxy. They have no impact on backend SOBR tiering mechanisms.

3.Scenario: A customer wants to leverage Veeam Data Platform v13 to identify potential ransomware infections as early as possible. They want to analyze data blocks for malicious encryption during the backup process itself, rather than waiting for post-backup scans or relying purely on hypervisor metrics. Which mechanism should the administrator configure to meet this exact requirement?
A. Configure a SureBackup job with an antivirus scanning step to automatically mount and inspect the backup files immediately after the job completes.
B. Enable Inline Entropy Analysis within the VBR global malware detection settings to inspect data blocks dynamically as they flow through the proxy.
C. Deploy the dedicated Veeam Recon Scanner lightweight agent onto the production virtual machines to monitor live file system modifications directly.
D. Configure the Veeam ONE server to aggressively trigger the suspicious incremental backup size alarm whenever the data change rate exceeds baselines.
Answer: B
Explanation:
Correct Logic (B): Veeam Data Platform v13 introduces advanced Inline Entropy Analysis. This feature actively analyzes the data blocks for signs of encryption (high entropy/randomness) as the data is streaming through the Veeam Proxy during the actual backup window, providing the earliest possible detection without requiring external agents.
Teardown of Distractors:
A is incorrect: SureBackup antivirus scanning is a *post-process* operation. It mounts the backup after it is fully written to the repository, which directly contradicts the scenario's requirement for detection "during the backup process itself."
C is incorrect: Veeam does not use "Recon Scanner lightweight agents" deployed inside production guest OSs for malware detection. Veeam's architecture is fundamentally agentless at the hypervisor level.
D is incorrect: The Veeam ONE "suspicious incremental size" alarm is a reactive, post-backup alert

based on metadata analysis after the backup file has already been generated.

4.Scenario: A critical database server has crashed. The administrator successfully initiated an Instant VM Recovery, and the database is now running directly from the backup repository using vPower NFS. Users are actively connected and writing new data. The administrator now needs to finalize the recovery and move the VM back to production storage without losing the newly written data or causing prolonged downtime.
Which two methods are officially supported to migrate this instantly recovered VM? (Choose two)
A. Utilize the native VMware Storage vMotion feature directly via the vSphere Client to seamlessly migrate the VM disks to the production datastore.
B. Execute the "Migrate to production" action directly within the Veeam Backup & Replication console to orchestrate the background data transfer.
C. Manually detach the delta redo logs from the vPower NFS datastore and consolidate them onto the production SAN using the ESXi command line.
D. Configure a Veeam Continuous Data Protection (CDP) policy targeting the vPower NFS mount to synchronize the I/O streams back to the host.
E. Deploy the Veeam Recovery Orchestrator agent to perform a reverse synchronization of the active memory state and storage blocks to the host.
Answer: A, B
Explanation:
Correct Logic (A, B): To finalize an Instant VM Recovery, you can either trigger VMware's native Storage vMotion (if your vSphere licensing supports it) to non-disruptively move the VM from the vPower NFS datastore to the production datastore, or you can use Veeam's built-in "Migrate to production" wizard. The Veeam wizard will automatically orchestrate a Quick Migration (using SmartSwitch) or invoke Storage vMotion in the background to safely consolidate the original backup state with the live delta changes.
Teardown of Distractors:
C is incorrect: Manually hacking ESXi redo logs via CLI is completely unsupported, highly dangerous, and guarantees data corruption for a running VM.
D is incorrect: CDP policies are for real-time replication from production to DR sites. You cannot target a vPower NFS mount running an Instantly Recovered VM with a CDP policy.
E is incorrect: VRO orchestrates recovery plans; it does not deploy agents to perform reverse memory synchronizations for Instant VM Recovery finalization.

5.Scenario: A financial institution is implementing Veeam Continuous Data Protection (CDP) for a Tier-1 trading application to achieve a Recovery Point Objective (RPO) of 10 seconds. The source environment is a highly optimized vSAN cluster, and the target replica datastore is a traditional mid-tier FC SAN. Shortly after configuring the CDP policy, the administrator notices the policy consistently falls out of the SLA, and the target datastore latency frequently spikes above 50ms.
A. The VMware vSphere APIs for I/O Filtering (VAIO) framework natively restricts outbound CDP stream bandwidth to 1 Gbps per host to prevent source storage performance degradation.
B. The CDP policy is explicitly configured to perform application-aware processing, which forces a Microsoft VSS snapshot every 10 seconds and overwhelms the guest operating system.
C. The target datastore subsystem cannot sustain the continuous stream of high-frequency write I/O,

which is often significantly higher than the source read I/O due to CDP journal overhead.
D. The designated Veeam CDP Proxy lacks the minimum required CPU cores to perform real-time AES-256 encryption on the data stream before transmitting it to the target cluster.
Answer: C
Explanation:
Correct Logic (C): Veeam CDP captures I/O continuously using the VAIO filter driver. The target storage must be extremely performant because it must handle not only the replicated data blocks but also the high-frequency writes required to maintain the short-term CDP journal (the undo/redo logs for granular point-in-time recovery). A mid-tier traditional SAN will easily become a bottleneck when bombarded with this intense, continuous write I/O, causing the policy to miss its SLA.
Teardown of Distractors:
A is incorrect: VAIO does not natively throttle outbound traffic to 1 Gbps. It intercepts I/O at the ESXi host level, but bandwidth limitations would be managed by Veeam network traffic rules, not an inherent VAIO hard limit.
B is incorrect: Application-aware processing in a CDP policy is used to create application-consistent restore points (typically scheduled every few hours). It is physically impossible and unsupported to trigger VSS every 10 seconds.
D is incorrect: While CDP Proxies do require adequate CPU and RAM to compress and route traffic, the classic symptom of SLA failure accompanied by target datastore latency spikes is fundamentally a target storage IOPS bottleneck, not proxy CPU exhaustion.