Exam : **2H0_25**

Title : Horizon Engineer - 2025

Version : DEMO

1.An external user connects to a Horizon 8 desktop through Unified Access Gateway (UAG). Authentication succeeds and the assigned desktop appears, but launching the desktop fails. This deployment deliberately uses Blast over TCP only; UDP is disabled for this test. The desktop is ready, its Blast listener is running, and an internal launch succeeds. The engineer may request one narrowly scoped firewall correction.
Which correction is best supported by the observations?
Select ONE answer.

Observation during the same launch attempt	Result
Client to UAG, TCP 443	Allowed; authentication completes
UAG to Connection Server, TCP 443	Allowed
UAG to the assigned desktop, TCP 22443	Dropped by the internal firewall
Internal client to the same desktop, TCP 22443	Allowed; desktop launches

A. Allow client-to-UAG TCP 22443 for the external launch.
B. Allow UAG-to-desktop UDP 4172 for the external launch.
C. Allow UAG-to-desktop TCP 22443 for the assigned desktop.
D. Allow UAG-to-Connection-Server TCP 8443 for the launch.
Answer: C
Explanation:
C is correct: the observed drop is on the UAG-to-Agent TCP Blast path. Authentication success does not prove that the display connection can reach the Agent. After the approved rule change, repeat the same launch, confirm that this flow is allowed, and verify desktop display. Keep the rule limited to the required sources and destinations; restore the previous rule if validation fails or unexpected access is introduced.

2.During maintenance of an automated instant-clone RDSH farm in Horizon 8 2206, an administrator has selected Stop at first error. The reviewed records show that a new clone fails during customization, while other clones continue to be provisioned and customized. No provisioning-stage error is recorded. The administrator asks whether the continued work proves that the option was ignored.
Which explanation is correct?
Select ONE answer.
A. The option stops work for provisioning errors; a customization error does not stop other clones.
B. The option stops work for either error type, so continued work proves it was ignored.
C. The option stops work only after all RDS hosts have completed the maintenance cycle.
D. The option stops work only for manual farms, so it cannot affect this automated farm.
Answer: A
Explanation:
A is correct. The option applies to provisioning errors; customization failures do not halt provisioning and customization of other clones. The observations therefore do not prove that the option was ignored. The customization failure still needs investigation; the explanation does not establish its root cause or claim that the affected clone is healthy.

3.A Horizon 8 engineer investigates poor Blast Extreme interaction through a required TCP-based SSL VPN. The VPN encapsulates the client's Blast UDP traffic inside TCP. Blast establishes its UDP session

successfully, but the session becomes sluggish during normal work. The same desktop, client, resolution, and workload perform well on an approved direct path. The VPN cannot be replaced during this investigation.
Which controlled test should the engineer perform first?
Select ONE answer.

Matched test	Direct path	Required SSL VPN path
Agent CPU and memory pressure	Low	Low
Session starts successfully	Yes	Yes
Initial Blast transport	UDP	UDP encapsulated in TCP
Interactive response	Responsive	Repeated pauses

A. Raise the Blast bandwidth ceiling while retaining UDP and the same VPN path.
B. Lower the display image quality while retaining UDP and the same VPN path.
C. Add desktop vCPUs while retaining UDP and the same VPN path.
D. Use Blast TCP for a matched test through the same VPN, without changing other settings.
Answer: D
Explanation:
D is correct. A TCP-based VPN that repackages UDP is a documented case for testing Blast TCP. Automatic fallback after an initial UDP connection failure does not resolve this scenario: the UDP session already starts successfully. Compare responsiveness and resource use with the same workload and VPN path. Make the change only for the approved test cohort, and restore the previous transport setting if the result is worse or fails the acceptance criteria.

4.An engineer designs external access to Horizon 8 through two Unified Access Gateway appliances. The security requirement is that UAG itself validates the client's certificate during client certificate authentication. This design does not use an identity-bridging or header-based authentication alternative. The engineer must retain load balancing and choose a supported TLS topology.
Which design meets the requirement?
Select ONE answer.
A. Terminate client TLS at the load balancer and use plaintext HTTP to the selected UAG.
B. Pass client TLS through a layer-4 TCP load balancer and terminate it at the selected UAG.
C. Terminate client TLS at the load balancer and re-encrypt to UAG using the same server certificate.
D. Terminate client TLS at the load balancer and re-encrypt to UAG using different server certificates.
Answer: B
Explanation:
B is correct: direct client certificate authentication requires the client TLS connection to reach UAG without termination at the load balancer. Validate the approved design with a trusted test client certificate and a rejected certificate, and verify TLS termination and normal access. Roll back the test topology if authentication or access validation fails.

5.A Horizon engineer must prepare UAG-A (Unified Access Gateway 2412) for maintenance while UAG-B remains available. New sessions must stop arriving at UAG-A, and existing sessions must not be

forcibly disconnected. UAG-B has verified spare capacity and working session affinity. The load balancer uses HTTPS GET /favicon.ico, treats only HTTP 200 as healthy, and does not close established connections when a health check fails. The existing sessions on UAG-A are expected to end naturally within one hour, within the applicable session-retention limit.
Which TWO actions together meet the maintenance requirements?
Select TWO answers.
Synthetic maintenance observation, not a product log format:
2026-10-10 01:00 UTC UAG-A: active sessions 23; health response HTTP 200
2026-10-10 01:00 UTC UAG-B: health response HTTP 200; spare capacity verified
Maintenance prerequisite: confirm UAG-A active sessions = 0 before power-off.
A. Enable Quiesce Mode on UAG-A and verify that its HTTP 503 health response removes it from new-session selection.
B. Keep UAG-A eligible for new sessions until its active-session count happens to reach zero.
C. Replace the HTTP health check with a TCP-port check so that UAG-A remains eligible while quiesced.
D. Monitor UAG-A until its active-session count reaches zero and verify UAG-B service before powering off UAG-A.
E. Power off UAG-A as soon as its health response changes, relying on UAG-B capacity to preserve active sessions.
Answer: AD
Explanation:
A and D are correct together. Quiescing makes the health check report HTTP 503, preventing new selection under the stated policy; the engineer then verifies natural session drain before power-off. A alone does not establish that existing sessions have ended, and D alone does not prevent new arrivals. Observe the retention limit and reschedule rather than force disconnection if sessions do not drain in time. Before power-off, a failed drain or peer-service check calls for postponing maintenance and restoring normal eligibility after validation.