Cloud-connected OS upgrade — SQE sign-off (E2E test plan)

Context

This document is the E2E test plan I used to validate a cloud-connected (HTTPS delivery) upgrade flow for Windows-based endpoints. The emphasis was stability after install and a repeatable restore path when needed.

Scope

- Validate cloud-delivered installation workflow and post-install stability.
- Exercise both preflight/download checks and the OS/database upgrade steps.
- Confirm core workflows and key peripherals remain stable.
- Validate restore operations return endpoints to a functional baseline.

Validation plan (matrix summary)

	Connectivity	Coverage	Validated
nts (VMs and consoles)	HTTPS	Representative spread of supported app versions	End-to-end install, service startup, logs/trac
	HTTPS	Repeated passes on the final build	Repeatability and “no new defects” confider

Acceptance criteria

- Preflight checks succeed and required artifacts download reliably.
- Upgrade completes without unexpected service failures or workflow regressions.
- Restore can be executed cleanly, followed by a post-restore validation pass.
- No high-severity new defects introduced within the tested coverage set.

Rollback / contingency

- Treat restore as the primary rollback mechanism; if any step fails, restore and re-validate baseline.
- If an endpoint is not eligible (unsupported version/config), fail closed and do not proceed with upgrade.

Outcomes / sign-off notes (sanitized)

- Used to coordinate validation coverage and define what “good” looks like before release.
- Raw logs and internal artifact locations are intentionally excluded from this portfolio edition.

What this demonstrates

- A structured validation approach for remote upgrades (repeatable steps, clear gates, measurable outcomes).
- Eligibility checks and restore verification as core safety rails.

Redactions performed

- Removed/replaced: names, internal share/URL paths, internal environment identifiers, and internal test-case identifiers.