

Azure DevOps Service Hook Reviewer — R10 Local Candidate (MC #105993)

Azure DevOps Service Hook Reviewer — R10 Local Candidate (MC #105993)

“ **Status:** Accepted local exact-SHA candidate only. Not deployed. Live rollout remains blocked.

Candidate

- Commit: `ba1714499a5be29d8112fea16e967f15144df821`
- Tree: `5b5ea20fa17623baf9cabf34d145711863aa578`
- Worktree: `/private/tmp/alai/flowforge-105961-stage1-r5`
- Accepted base: R4 `437e64fd54574e6ff7e6a2665d081c3e6125d080`

R10 adds a separately deployable, dedicated Key Vault prerequisite and preserves the main private-endpoint/DNS integration candidate. It also provides an approval-gated helper for exactly three fixed secret child resources through Azure Resource Manager control-plane APIs. No secret value is stored in source, command arguments, environment variables, files, deployment parameters, logs, or evidence.

R10 security remediation

Every ARM HTTP response path uses a centralized 64 KiB reader. `Content-Length` is accepted only when, after trimming HTTP `SP`/`HTAB` optional whitespace, it is non-empty ASCII decimal digits `0-9`

. Plus signs, underscores, Unicode digits, CR/LF, embedded whitespace, empty values, comma/duplicate forms, negatives, and over-limit lengths fail closed before reading. Missing and lying headers remain bounded by `read(MAX+1)`.

Transport is direct and fail closed:

- no ambient proxies (`ProxyHandler({})`)
- no redirects
- HTTPS only to exact `management.azure.com` on the default/443 port
- standard platform certificate and hostname verification
- bounded response reads and sanitized failures

Preserved controls

- account, token, and locked-vault verification before confirmation or secret prompts
- hidden in-memory secret collection and local input validation
- minimal nonsecret Azure CLI environment
- exact secret-name and child-resource-ID metadata binding
- dedicated RBAC-enabled, purge-protected, public-network-disabled Key Vault
- private endpoint and `privatelink.vaultcore.azure.net` DNS integration
- closed live gate by default
- immutable image, managed-identity `AcrPull`, restricted Service Bus, private Table Storage, NAT egress
- accepted R4/R11 runtime/provider bytes unchanged

Validation and acceptance

- Python tests: 18/18
- Node tests: 157/157
- lint, local IaC validation, both Bicep compiles, offline production audit, diff check, Gitleaks, and byte comparison: PASS
- Proveo exact-SHA review: PASS
- Securion exact-SHA audit: PASS
- Company Mesh P2P: PASS, `mesh-msg-d904645a-7404-42dd-8edf-728769280ffe`

Canonical acceptance evidence: `/Users/makinja/system/evidence/105993/R10-LOCAL-CANDIDATE-ACCEPTANCE.md`

Operational gate

This page does **not** authorize Azure `what-if`, prerequisite deployment, role assignment, helper `--execute`, secret mutation, image push, main deployment, ingress binding, Service Hook creation, provider invocation, PR comments, repository push/merge, or Bilko v1 retirement.

If separately approved, the next action is only the dedicated Key Vault prerequisite `what-if`. Every later action remains a separate gate. Azure DevOps minimum-permission identity and reviewed ingress snapshot/drift semantics remain unresolved rollout prerequisites.

Revision #2

Created 2026-07-19 00:48:28 UTC by John

Updated 2026-08-10 07:37:45 UTC by John