

Azure DevOps Ingress Drift Gate — R1 Local Candidate (MC #106024)

Azure DevOps ingress drift gate — R1 local candidate (MC #106024)

Status: exact-SHA local candidate accepted; not deployed and not authorized for live execution.

Candidate identity

- SHA: 00d5d5078eb4f19492a6fffd67eb6095c68183d1
- Tree: 854c70f32a9f7de8dd6a8b9f505f24477dc3f6af
- Parent accepted R10: ba1714499a5be29d8112fea16e967f15144df821

Any byte change invalidates this acceptance.

Purpose

This successor to the accepted R10 Service Hook candidate materializes the reviewed Microsoft Learn Azure DevOps inbound snapshot as exactly 19 canonical IPv4 CIDRs and adds a deterministic fail-closed pre-what-if drift verifier.

Security and drift properties

- Official source is pinned to the exact reviewed HTTPS URL and learn.microsoft.com host.

- Ambient proxies are disabled, redirects are rejected, and normal TLS certificate/hostname verification remains enabled.
- Response reading is bounded with an unconditional `MAX+1` read and strict ASCII-decimal `Content-Length` validation.
- Parsing accepts exactly one `Inbound connections` table with exact headers and rejects structural ambiguity.
- Missing/added ranges, duplicates, IPv6, global, malformed and noncanonical CIDRs block.
- Source metadata, body hash, format, table, normalized-set and deployment-parameter drift block.
- The verifier never auto-updates or auto-widens ingress and never prints or persists source bodies.
- `--validate-only` is strictly local and performs no network operation.
- The sole deployment parameter file contains only `allowedIngressCidrs` and exactly equals the ordered manifest.
- Container Apps receives 19 literal IPv4/CIDR `Allow` rules; other traffic is implicitly denied. No unsupported `AzureDevOps` service-tag shortcut is used.

Validation

- Builder: 157 Node tests and 37 Python tests PASS; lint, IaC/Bicep validation, local snapshot validation, offline audit, diff and scoped Gitleaks PASS.
- Proveo detached exact-SHA review: PASS.
- Securion detached exact-SHA security review: PASS.
- Company Mesh independent pre-verifier: PASS.
 - Thread `mesh-thr-6aebc304-9d39-472f-a07f-dc57fa99b515`
 - Response `mesh-msg-8009d6d5-34b6-4330-a6f7-f1f8643467c4`

Accepted R10 protected runtime/IaC/secret-helper paths are unchanged, and the inherited safety test verifies accepted R4/R11 provider/runtime bytes.

Mandatory future gates

This local acceptance does not authorize a live fetch, Azure `what-if`, deployment, identity/PAT/permission work, Key Vault changes, secret population, image push, Service Hook creation, provider execution, PR comment, push or merge.

Before any separately approved `what-if` or deployment:

1. MC #106000 dedicated minimum-permission PAT-capable reviewer identity must be approved and proven.
2. Run a fresh approved live drift check against the exact source; any drift blocks.
3. Prove Container Apps API acceptance of all 19 rules through the separately approved gate.

4. Preserve closed rollout default and all R10/R4/R11 controls.
5. Complete separate deployment, canary and rollback evidence.

Evidence index: `/Users/makinja/system/evidence/106024/R1-LOCAL-CANDIDATE-ACCEPTANCE.md`.

Revision #1

Created 2026-07-19 16:43:29 UTC by John

Updated 2026-07-19 16:43:29 UTC by John