

Exact read access, before installation

The published Helm chart declares every Kubernetes resource and verb used by the KrevoPilot agent. Render the chart with the intended collectors and review the resulting RBAC before installation.

Published: 23 August 2026

BOUNDARY

The agent initiates outbound HTTPS. The SaaS backend does not require the customer's kubeconfig and does not initiate inbound connections to the Kubernetes API.

What is installed

- One Kubernetes Deployment for the agent.
- One dedicated ServiceAccount, ClusterRole and ClusterRoleBinding.
- One Kubernetes Secret containing the cluster connection key and optional identifier hash salt.
- An optional egress NetworkPolicy when explicitly enabled.

Baseline permissions

API group	Resources	Verbs	Purpose
core	Pods, events, nodes, namespaces, services	get, list	Workload state, health, topology and event evidence
metrics.k8s.io	Pods, nodes	get, list	Current CPU and memory observations
apps	replicasets	get, list	Resolve pod ownership to the owning workload

Conditional collectors

Setting	Additional read access	Data boundary
logs.enabled=true	Pods/log: get	Current and previous container log evidence, bounded and redacted
manifests.enabled=true	deployments, statefulsets, daemonsets, jobs, cronjobs, services, endpointslices, networkpolicies, ingresses, PVCs, storageclasses, configmaps, secrets: get/list	Selected manifests and summaries; Secret values and key names are excluded
diagnostics.enabled=true	Uses already declared read access	Bounded live checks requested through the authenticated agent channel

Mutation boundary and sensitive data

- The collector role has no Kubernetes create, update, patch or delete verbs.
- Secret values and Secret key names are never transmitted; only existence, type and value counts may be summarized when manifest collection is enabled.
- ConfigMap values are excluded by default. Generated YAML and commands remain review-first.

Runtime hardening

Execution	Filesystem	Privileges	Default resources
Non-root user	Read-only root filesystem	Capabilities dropped; no privilege escalation	50m CPU / 96Mi request; 250m CPU / 256Mi limit

Verify before applying

Render the exact chart and values selected for your environment, then inspect the resulting ClusterRole. Public chart source: github.com/KreateRevo/Krevopilot-agent-helm-charts.

VERSION

Published reference: agent 2.0.32, Helm chart 0.1.32. Re-check the rendered chart whenever collectors or chart versions change.

This is a technical description of the published chart, not a certification or contractual security addendum. Organizations may further restrict collectors, retention and egress according to policy.