

Kompass Insights agent permissions

The Kompass Insights agent requires read-only access to specific Kubernetes resources to collect data and generate actionable insights. These permissions are defined in a Kubernetes ClusterRole and scoped for observability only, ensuring that no cluster resources are modified.

Allowed actions

The Kompass Insights agent uses the following read actions across all required resources:

- get
- list
- watch

Restricted actions

The following actions are not required by the Kompass Insights agent (and are implicitly denied):

- create
- patch
- update
- delete
- deletecollection

Exception: Write permissions are necessary only for certain Zesty CRDs in the qscaler.qubex.ai API group, described in the following table.

Required Kubernetes resources

The following table describes the required resources:

Resource	API group	Purpose
ConfigMaps	Core ("")	Access configuration data attached to workloads
Events	Core ("")	Monitor node and pod lifecycle events and timings

Resource	API group	Purpose
Namespaces	Core (""")	Identify and categorize resources by logical boundaries
Nodes	Core (""")	Retrieve metadata about the cluster's compute resources
PersistentVolumeClaims	Core (""")	Track usage of requested storage volumes
PersistentVolumes	Core (""")	Report on provisioned backing storage across the cluster
Pods	Core (""")	Inspect workload scheduling, status, and resource usage
ReplicationControllers	Core (""")	Access metadata for legacy workload controllers
Services	Core (""")	Understand service discovery and network access patterns
DaemonSets	apps	Observe node-affinity workloads that run on every node
Deployments	apps	Analyze rollout strategies and workload configuration
ReplicaSets	apps	Understand backend scaling objects supporting Deployments
StatefulSets	apps	Track stateful workload behavior and identity-based scheduling
HorizontalPodAutoscalers	autoscaling	Inspect autoscaling rules based on CPU, memory, or custom metrics
CronJobs	batch	Analyze scheduled, recurring job definitions and executions
Jobs	batch	Track ad hoc or one-time batch job completions
PodDisruptionBudgets	policy	Monitor availability guarantees during pod disruptions
StorageClasses	storage.k8s.io	Track storage provisioning policies across the cluster
Nodes (metrics)	metrics.k8s.io	Collect CPU and memory utilization for each node
Pods (metrics)	metrics.k8s.io	Measure resource usage across all workloads

Resource	API group	Purpose
CustomResourceDefinitions	apiextensions.k8s.io	Detect and identify CRDs used by Karpenter and Zesty products
NodeClaims	karpenter.sh	Analyze how Karpenter provisions new capacity
NodePools	karpenter.sh	Understand the configuration of node group templates
ScaledJobs	keda.sh	Track event-driven job executions and scale settings
ScaledObjects	keda.sh	Monitor dynamic scaling policies tied to external triggers
QNodes	qscaler.qubex.ai	Zesty CRD for cluster-aware scaling decisions
WorkloadProtections	qscaler.qubex.ai	Zesty CRD for workload disruption safeguards

Justification

The read-only permissions are essential for the Kompas Insights agent to:

- collect real-time and historical metrics across workloads and infrastructure
- track workload configurations, scaling behavior, and storage usage
- observe autoscaling trends and scheduling patterns
- detect and respond to changes in custom resources like Karpenter, KEDA, and Zesty QScaler
- operate with minimal privileges necessary for functionality and insight generation

Security considerations

This ClusterRole is designed with the principle of least privilege in mind. All access is read-only, with the exception of Zesty CRDs which require write access to support active cluster management.