Communication With Downstream Clusters

Unit 1.1.2

Authentication Proxy

The authentication proxy receives requests from the user, performs authentication, and then sets Kubernetes impersonation headers before forwarding the request to the Kubernetes cluster's API server.

Cluster Controller

The cluster controller runs in the Rancher Server environment and performs the following functions:

- Watches for resource changes in the downstream cluster
- Brings the current state of the downstream cluster to the desired state
- Configures access control policies to clusters and projects
- Provisions clusters by calling the required Docker machine drivers and Kubernetes engines, such as RKE and GKE

The Cluster Controller connects to the Cluster Agent by default. If the Cluster Agent is unavailable, it can use a Node Agent as a fallback channel.

Cluster Agent

Each downstream cluster has an agent that opens a tunnel back to the controller that's running on the Rancher server cluster. It is responsible for:

- Connecting to the Kubernetes API of Rancher-launched Kubernetes clusters
- Managing workloads, pod creation and deployment within each cluster
- Applying the roles and bindings defined in each cluster’s global policies

- Communicating through the tunnel between the cluster and Rancher server about events, stats, node info, and health

Node Agent

The Node Agent runs as a DaemonSet, launching one Pod on every node in the cluster. Its primary function is to interact with node-specific functions, such as upgrading Kubernetes or restoring etcd snapshots.
If the Cluster Agent is unavailable, one of the Node Agents will establish a tunnel back to the Rancher Server and take over the Cluster Agent role.

Authorized Cluster Endpoint

Rancher-launched RKE clusters (Custom or Infrastructure clusters) also run a `kube-api-auth` microservice that acts as a direct endpoint for managing that cluster with `kubectl`. Authorized cluster endpoints are included in the Kubeconfig file available at the Cluster overview screen in Rancher.
The Authorized Cluster Endpoint exists so that users can communicate with a cluster if Rancher itself is down and the Authentication Proxy is unavailable, or so that users can communicate directly with a cluster that is geographically closer to them instead of adding additional latency by proxying through the Rancher Server in another location.
When communicating with the Authorized Cluster Endpoint, all security boundaries for the user are maintained.

References

Rancher Architecture - https://rancher.com/docs/rancher/v2.x/en/overview/architecture