Project Security

Unit 4.4.3

Project Security

User Authorization

Users who have access to a project have access to all of the namespaces and resources inside of it. Project members can be given four levels of access:

- Owner - This account has full control over the project and all its resources.
- Member - This account can manage resources in the project but cannot change the project itself.
- Read Only - This account can view resources in the project but cannot change them.
- Custom - This account has access according to the individual roles selected for it.

Network Isolation

If the cluster was launched with Canal as its network provider, Project Network Isolation is an available option. If you select this option, resources in one project will not be able to see or communicate with resources in any other project. This creates single-cluster multi-tenancy, because users can only see the resources in their project, and those resources can only see other resources in the same project.

If Project Network Isolation is enabled, it does not apply to the System project or its namespaces. Resources that run within this project have access to all resources in other projects to operate correctly.

Pod Security Policies

Rancher allows operators to assign Pod Security Policies to Projects but for the best management experience and easy troubleshooting recommends that PSPs are only assigned to clusters.

Whether you adjust PSPs at the project or cluster level, remember that they only apply to workloads that are created *after* the PSP is applied. If you have any running workloads, redeploy them from the Rancher UI.

References

Adding Users to Projects - https://rancher.com/docs/rancher/v2.x/en/project-admin/project-members/

Cluster and Project Roles - https://rancher.com/docs/rancher/v2.x/en/admin-settings/rbac/cluster-project-roles/

Pod Security Policies - https://rancher.com/docs/rancher/v2.x/en/admin-settings/pod-security-policies/

Assigning Pod Security Policies - https://rancher.com/docs/rancher/v2.x/en/cluster-provisioning/rke-clusters/options/pod-security-policies/