



# Introduction



# RKE2

RKE2 is Rancher's enterprise-ready next-generation Kubernetes distribution. It has also been known as RKE Government.

It is a fully [conformant Kubernetes distribution](#) that focuses on security and compliance within the U.S. Federal Government sector.

To meet these goals, RKE2 does the following:

- Provides [defaults and configuration options](#) that allow clusters to pass the CIS Kubernetes Benchmark [v1.7](#) or [v1.8](#) with minimal operator intervention
- Enables [FIPS 140-2 compliance](#)
- Regularly scans components for CVEs using [trivy](#) in our build pipeline

## How is this different from RKE or K3s?

RKE2 combines the best-of-both-worlds from the 1.x version of RKE (hereafter referred to as RKE1) and K3s.

From K3s, it inherits the usability, ease-of-operations, and deployment model.

From RKE1, it inherits close alignment with upstream Kubernetes. In places K3s has diverged from upstream Kubernetes in order to optimize for edge deployments, but RKE1 and RKE2 can stay closely aligned with upstream.

Importantly, RKE2 does not rely on Docker as RKE1 does. RKE1 leveraged Docker for deploying

and managing the control plane components as well as the container runtime for Kubernetes. RKE2 launches control plane components as static pods, managed by the kubelet. The embedded container runtime is containerd.

## Why two names?

It is known as RKE2 as it is the next iteration of the Rancher Kubernetes Engine for datacenter use cases. The distribution runs standalone or integrated into Rancher. Automated provisioning of new RKE2 clusters is available in Rancher v2.6+.

It has also been known as RKE Government as it was designed to target sectors with heightened security requirements.

## Security

SUSE supports responsible disclosure and endeavors to resolve security issues in a reasonable timeframe. To report a security vulnerability, email [security@rancher.com](mailto:security@rancher.com).

*Last updated on May 6, 2026*