RANCHER GOVERNMENT SOLUTIONS (RGS) RKE2 SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 4

24 January 2024

Developed by SUSE RGS and DISA for the DOD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The RKE2 Security Technical Implementation Guide (STIG) provides technical requirements for securing an RKE2 platform version 1.23.6+rke2r2. RKE2, also known as RKE Government, is Rancher's next-generation Kubernetes distribution. It is a fully conformant Kubernetes distribution that focuses on security and compliance within the U.S. Federal Government.

To meet these goals, RKE2 does the following:

- Provides defaults and configuration options that allow clusters to pass the CIS Kubernetes Benchmark v1.5 or v1.6 with minimal operator intervention.
- Enables FIPS 140-2 compliance.
- Regularly scans components for CVEs using Trivy in the build pipeline.

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 to optimize for edge deployments, but RKE1 and RKE2 can stay closely aligned with upstream. 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."

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that DISA "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked Controlled Unclassified Information (CUI) will be available for items that did not meet requirements. This report will be available to component authorizing official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For all STIG requirements that pertain to a graphical user interface (GUI), the STIG check and fix assume an organization has implemented the TOSS 4 default, GNOME Shell GUI. If an organization is not using the default GUI, it is the responsibility of the organization to implement the security feature using their chosen GUI.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

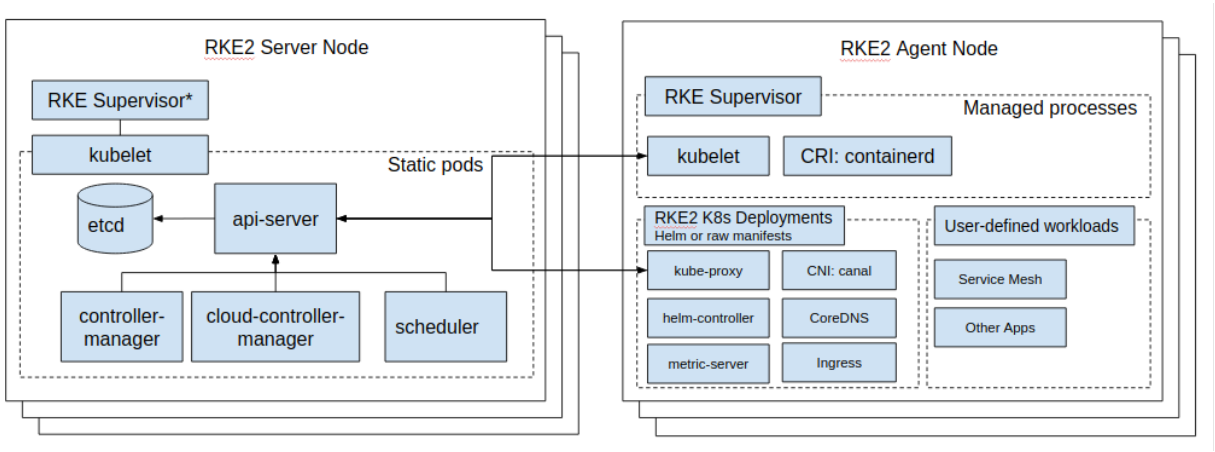
- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DODI 8100.04.

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

RKE2 takes lessons learned from developing and maintaining lightweight Kubernetes distribution and K3s and applies them to build an enterprise-ready distribution with K3s ease-of-use. RKE2 is, at its simplest, a single binary to be installed and configured on all nodes expected to participate in the Kubernetes cluster. Once started, RKE2 is then able to bootstrap and supervise role-appropriate agents per node while sourcing needed content from the network.

Figure 2-1: RKE2 Architecture



3. CONCEPTS AND TERMINOLOGY CONVENTIONS

The approach for RKE2 is to take lessons learned from developing and maintaining lightweight Kubernetes distribution, K3s, and apply them to build an enterprise-ready distribution with K3s ease-of-use.

3.1 Control Plane Services

- API Server.
- Controller Manager.
- Kubelet.
- Scheduler.
- Proxy.

3.2 Ingress

RKE2 ships with NGNIX as its default ingress provider. As of v1.21+, this component is FIPS compliant. There are two primary subcomponents for NGINX ingress:

- Controller: Responsible for monitoring/updating Kubernetes resources and configuring the server accordingly.
- Server: Responsible for accepting and routing traffic.

The controller is written in Go and compiled using a FIPS compatible Go compiler. The server is written in C and also requires OpenSSL to function properly. It leverages a FIPS-validated version of OpenSSL to achieve FIPS compliance.

4. GENERAL SECURITY REQUIREMENTS

4.1 Host Operating System

This STIG assumes the STIGs for the applicable underlying layers have been completed using the Red Hat Enterprise Linux (RHEL) 8 operating system with the applicable STIG applied.

The operating system is the foundation for Rancher Government Solutions Multi-Cluster Manager (RGS MCM). By not securing the operating system properly, RGS MCM can become a front end for a nefarious user to gain access to an organization's networked resources.