RANCHER GOVERNMENT SOLUTIONS MULTI-CLUSTER MANAGER (RGS MCM) SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 1

30 March 2022

Developed by Rancher Government Solutions and DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any non-federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The Rancher Government Solutions Multi-Cluster Manager (RGS MCM) Security Technical Implementation Guide (STIG) provides technical requirements for securing basic Kubernetes platforms managed by RGS MCM. There are many capabilities and configurations shared between the underlying Kubernetes cluster and RGS MCM. The shared capabilities and configurations are better applied at the Kubernetes layer and may be considered out-of-scope for this STIG.

RGS MCM's main use case is managing multiple clusters. Best practice of applying security features at this layer through RGS MCM, such as global role-based access control (RBAC), are applicable to this STIG as these can provide security features at the global, multi-cluster level.

The Kubernetes cluster runs on top of other components. These components, such as a runtime and a container network interface (CNI), act differently depending on the software (runtime examples are Docker and ContainerD) or the plugin (CNI plugin examples are Flannel, Calico, and Canal) installed. The component also determines what additional security can be implemented for Kubernetes, for example, the CNI installed can determine the type of network policies if they can be implemented. Because of the differences in capabilities, features of Kubernetes components are outside the scope of the RGS MCM STIG, but the components need to be secured. To secure the components outside the scope of this document, use the specific vendor STIG or technology Security Requirements Guide (SRG).

Services provided specifically by the underlying Kubernetes distribution are also outside the scope of this document and one must follow the appropriate vendor-specific STIG, if one exists. If a vendor-specific STIG does not exist, the more generic technology SRG must be used. Services must also follow any guidance that pertains to the way the services are implemented.

This STIG assumes that only out-of-the-box components of RGS MCM are being used and no special configuration is being provided to swap out any bundled components. This STIG requires that all applicable underlying security controls have been met. A typical stack that Rancher runs on top of consists of infrastructure, hypervisor, operating system, container runtime, and Kubernetes distribution. Proper hardening of the surrounding environment is independent of RGS MCM but ensures overall security stature.

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

	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 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) containing DoD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5   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.

1.6 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 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.

1.7 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

RGS MCM is designed to be extremely flexible and can be conceptualized as a window into the powerful potential of the underlying Kubernetes distribution. Rancher is a container management platform, not a container orchestration platform, with many components that can be customized based on organizational needs. This document will not attempt to cover everything Rancher can configure.

Figure 2-1: RGS MCM Architecture
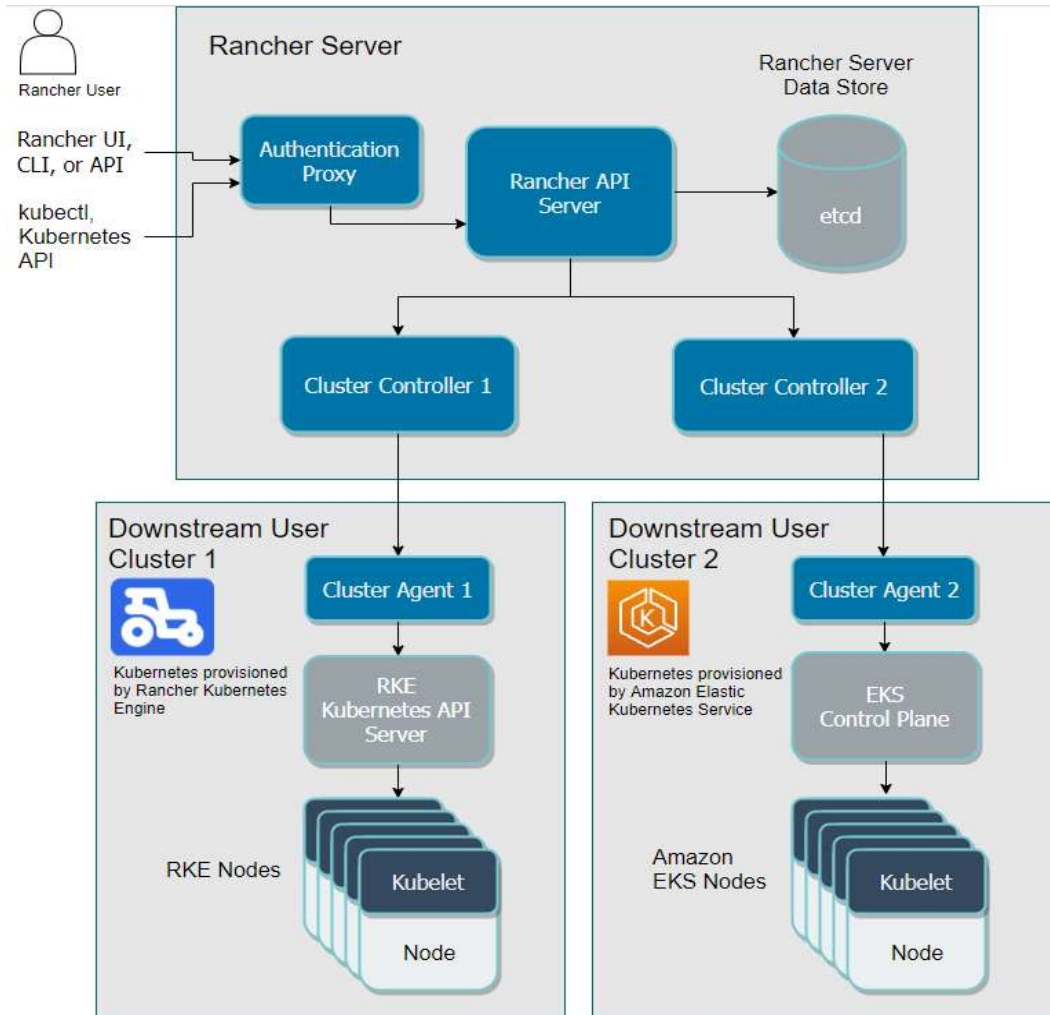
3.   CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1   RGS MCM Installation Overview

RGS MCM is installed and upgraded using a Kubernetes package manager called Helm (https://helm.sh/). Helm packages, known as "charts", allow for declarative configuration of Rancher MCM deployments and provide upgrade features. It is important to install RGS MCM using the most current, and therefore secure, Helm configuration possible (https://rancher.com/docs/rancher/v2.6/en/installation/install-rancher-on-k8s/chart-options/), regularly updating, and version controlling.

3.2   Downstream Deployment Strategies and Types

There are many strategies that can be used when registering downstream clusters. The best method relies completely on the use case and limitations of the operating environment.

3.2.1   Hub & Spoke Strategy

It is advantageous to use one deployment of RGS MCM to manage many clusters across multiple regions. For example, if only one method of authentication or a centralized authentication method is desired for many independent clusters, using a Hub and Spoke is the best practice.

Figure 3-1: Hub & Spoke Strategy
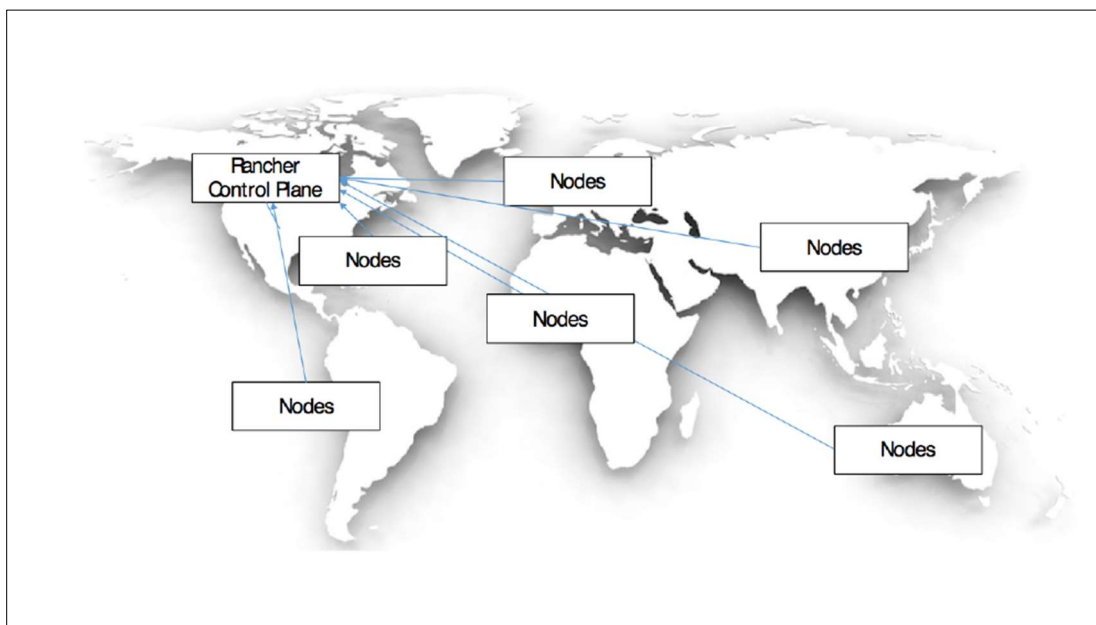
3.2.2   Regional Strategy

When different users and authentication strategies exist across regions, a regional strategy might be preferred. This is also something to consider when multiple environment types are required,

such as development, test, and production environments, in which there is a requirement for separation. This is also a common strategy when clusters span classification domains.

Figure 3-2: Regional Strategy
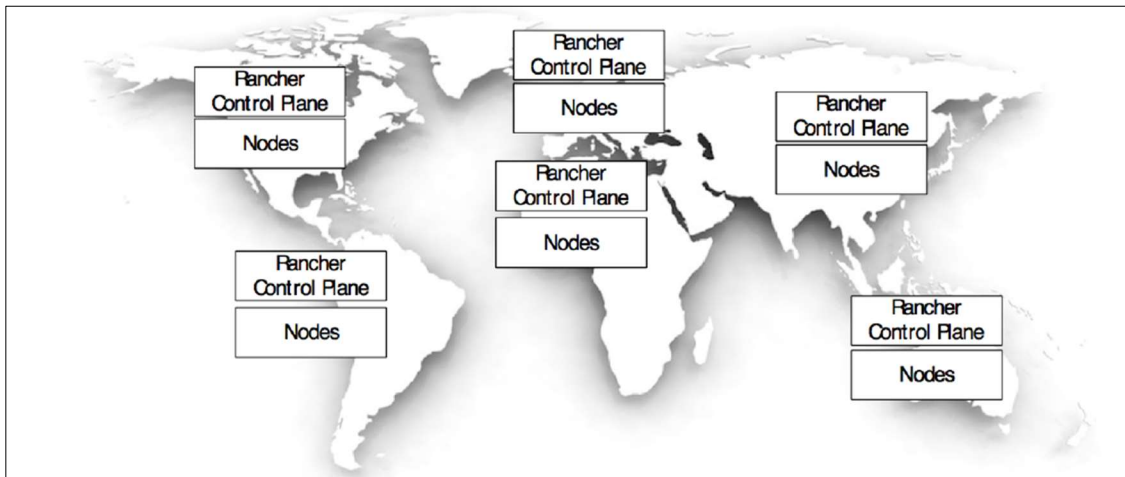
3.3 Terminology

3.3.1 Rancher Control Plane

The Rancher Control Plane, sometimes called the Management Plane or Local Cluster, is a deployment of RGS MCM that has other clusters registered to it. The Rancher Control Plane is installed on top of a Kubernetes Distribution, such as RKE2, using Helm. This RGS MCM deployment serves as the central management point of all the clusters it manages.

3.3.2 Local Cluster

The default name of the cluster where Rancher runs. This cluster-friendly name can be changed, but the name in the API cannot be changed. When a user installs RGS MCM on a cluster, that cluster is automatically designated as the Local cluster.

3.3.3 Downstream Cluster

Downstream clusters are clusters registered to Rancher that fall under Rancher's control anywhere other than the Local cluster. These clusters are separate Kubernetes clusters with their own Kubernetes control plane components. Rancher manages these using Cattle cluster-agents and node-agents.

3.3.4 Helm

Helm is a Kubernetes configuration and package manager that helps launch complex Kubernetes objects with simple parameters using YAML templating. This tool is used to install and upgrade RGS MCM on top of a Kubernetes cluster.

3.3.5   Cluster and Node Agents

Cluster and Node agents are deployments in downstream clusters that proxy cluster operations from the local cluster/RGS MCM Control Plane and the downstream clusters.

3.3.6   Node Drivers

RGS MCM has the capability of managing hypervisor infrastructure (such as AWS and ESXI) by spinning up virtual machines (VMs). RGS MCM uses the Node Driver tool behind the scenes to drive this provisioning process. Clusters provisioned in this manner are considered out-of-scope for this STIG.

4. GENERAL SECURITY REQUIREMENTS

RGS MCM security goes beyond configuration settings. To secure RGS MCM properly, consideration must be given to the services being hosted, who the user community is, what type of data is being accessed, and where RGS MCM will reside. By not looking beyond the application itself, security flaws in the implementation can lead to the compromise of user personally identifiable information (PII), organization-sensitive data and processes, and the compromise of access to other systems and applications within the organization with a trusted relationship to RGS MCM services.

4.1   Hosting Operating Systems

The operating system is the foundation for 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.

This STIG assumes the STIGs for the applicable underlying layers have been completed using RHEL 8 OS with the applicable STIG applied and RKE2 with the generic container platform SRG applied (until a final version of the STIG for RKE2 is released).

4.2   Kubernetes

Rancher needs to be installed on top of an already functioning and hardened Kubernetes distribution and operating system. This STIG assumes these STIGs for the applicable underlying layers have been completed using RHEL 8 OS with the applicable STIG applied and RKE2 with the generic container platform SRG applied (until a final version of the STIG for RKE2 is released).

4.3   Downstream Stream Clusters Deployment Strategy

Clusters created through Rancher's Node-Drivers are considered out-of-scope for this STIG. Currently the best way to register clusters to Rancher is to set them up independently, apply all applicable STIGs, and then register to RGS MCM.

4.4   User Management

One of the most powerful features of RGS MCM is its ability to aggregate Kubernetes and API user management across multiple clusters using a single Identity Provider (IDP). It is extremely important this third-party IDP tool is set up properly. If a vendor-specific STIG does not exist, the more generic technology SRG must be used.

Local auth users should not be present in RGS MCM. All users should be managed by the IDP and only the "Default Admin" should be tied to a local auth user for emergency backup purposes. Credentials for this user must be protected.

Defining user roles properly is essential to securing the Kubernetes cluster. Too often, all the operating system users are given the same roles. Giving users more privileges than necessary allows a user to escalate their privileges and make cluster changes, which is an administrator function. It is crucial to look at the roles the organization wants to implement for privileged users and give users only the roles required for carrying out their duties. The definition and duties of each role should be completed before any user accounts are created and RGS MCM is deployed.

This STIG was baselined using KeyCloak as the third-party OpenID Connect identity provider.

4.5   Storage at Rest and In-Flight

One of the most important aspects of any platform is storage. Keeping data encrypted at rest and while in transit using the most modern methodologies should be extremely high in priority when planning a container platform. While RGS MCM makes it easy to integrate storage solutions, the security hardening of these tools is out-of-scope of this STIG.

RGS MCM can manage all workloads deployed in Kubernetes so it can be used to check and fix all workloads and their TLS settings if configurable at the pod or container level. It is important to ensure all network communication settings are configured to use approved modern standards.

4.6   Security Scans

RGS MCM has an add-on feature called the CIS Scanner that can scan clusters for security compliance. These scans are not STIG related and do not check for STIG requirements. These scan profiles can be customized and run on a period schedule with alerting features. It is recommended to set this up to check for some common security controls.

4.7   Other Major Platform Components

There are many additional components of a highly functioning and secure platform. RGS MCM makes deploying and configuring these tools much faster and easier, however configuring, and securing them is out of scope for this STIG.

Audit and application log aggregation is a major component that can be invaluable when a problem strikes. RGS MCM facilitates launching and configuring log aggregation tools but applying security controls to these tools is out-of-scope for this STIG.

Monitoring your workloads can aide in preventing DoS attacks and general outages by viewing system performance over time. RGS MCM facilitates launching and configuring monitoring tools but applying security controls to these tools is out-of-scope for this STIG.

4.8   Conclusion

RGS MCM provides a means to manage anything in Kubernetes, however, it is not Kubernetes itself. It is also not an operating system. RGS MCM depends heavily on these underlying systems to provide many security features. Due to the nature of any heavily abstracted environment, everything depends on its underlying sub-systems. It is important that all pieces of the software stack be individually analyzed, and security controls applied according to best practices and industry standards.