SHADOWSOFT

RHEL DISA STIG AWS Marketplace AMI Offering Product Page

What is DISA STIG?

The U.S. Department of Defense (DoD) established the Defense Information Systems Agency (DISA) to provide IT and communication support. DISA created Security Technical Implementation Guides (STIGs) STIGs - **a series of cybersecurity requirements for IT products deployed within DoD** - to define how all network devices, software, databases and operating systems must be secured.

How did we harden the image?

DISA STIG demands **370+ configuration requirements** be met to secure information for all DoD related entities. Our software engineers modified the default configuration of the base minimal RHEL 8.6 image to meet DISA STIG regulations satisfying an OpenSCAP scan.

Why use a RHEL DISA STIG image?

The purpose of DISA STIG is to **reduce the risk of cyberattacks on DoD infrastructure**. All DoD agencies or related entities that accept, store, transmit, or process data must be STIG compliant and this image is pre-configured to meet STIG requirements to reduce your risk of attacks by malicious state and non-state actors.

Use Cases for RHEL DISA STIG image?

- Drastically reduce effort in configuring system to meet DISA compliance requirements
- Reduce surface attack vector when using RHEL

Compliance and Scoring

The target system did not satisfy the conditions of 48 rules! Please review rule results and consider applying remediation.

Rule results

306 passed | 48 failed | 7

Severity of failed rules

10 low | 34 medium | 4 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	82.163025	100.000000	82.16%