VMware NSX 4.x STIG Readiness Guide Overview

Version 1 Release 1

vmware

Table of contents

Overview

VMware is a trusted partner in highly secure, mission critical systems around the world, including the US Department of Defense (DoD). In the DoD, all IT systems must adhere to the rigorous Risk Management Framework (RMF) as defined in DoDI 8510.01. A critical component of RMF is the mandatory implementation of Security Technical Implementation Guides (STIGs) and Security Requirements Guidelines (SRGs) as maintained by the Defense Information Systems Agency (DISA). Where a product specific STIG is not available, the relevant SRGs must be used instead.

DoDI 8510.01

"STIGs are product-specific and document applicable DoD policies and security requirements, as well as best practices and configuration guidelines. STIGs are associated with security controls through CCIs, which are decompositions of NIST SP 800-53 security controls into single, actionable, measurable items. SRGs are developed by DISA to provide general security compliance guidelines and serve as source guidance documents for STIGs. When a STIG is not available for a product, an SRG may be used."

To better serve the needs of our DoD partners, and those who wish to meet the bar set by the DoD, VMware is providing SRG content that is the source material for an existing STIG, the basis for a future or in-process STIG, or that can be used in the absence of a DISA published STIG.

What does STIG Readiness mean?

VMware has published several STIGs with DISA and as such, we are very familiar with the SRGs and what it takes to meet DISA's stringent requirements for risk acceptance and publication. "STIG Readiness" means that we are doing the same level of work as we would do with DISA but self-publishing the content to make it available and usable as soon as possible. The quality is high enough, in our experience, that should a given "STIG Ready" product be put through the DISA process, we are confident that there would be minimal content changes before publication.

This project represents VMware's effort to document our compliance against the SRG requirements and nothing more. A published STIG is our eventual goal, in most cases, but this content should not be viewed to be "as good as a STIG". A DISA published STIG includes technical validation, review of requirement fulfillment, accuracy and style, risk acceptance and is digitally signed by the RME and posted on cyber.mil. Except for products that already have published STIGs, there is no explicit or implied DISA approval of the provided content. We also make no guarantee that any STIG(s) will be published from this content in the future.

Support

As previously stated, this content is produced by VMware without any DISA ownership. As such, any technical issues must not be directed to DISA.

Other Considerations

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 as such ensure all steps are taken to back systems up before implementation.

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. Furthermore, VMware implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is intended for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level because some of the settings may not be able to be configured in environments outside the DoD architecture.

Product Summary

VMware NSX is the network virtualization and security platform that enables VMware's cloud networking solution with a software-defined approach to networking that extends across data centers, clouds, and application frameworks. With NSX, networking and security are brought closer to the application wherever it's running, from virtual machines (VMs) to containers to physical servers. Like the operational model of VMs, networks can be provisioned and managed independent of underlying hardware. NSX reproduces the entire network model in software, enabling any network topology—from simple to complex multitier networks—to be created and provisioned in seconds. Users can create multiple virtual networks with diverse requirements, leveraging a combination of the services offered via NSX or from a broad ecosystem of third-party integrations—ranging from next-generation firewalls to performance management solutions—to build inherently more agile and secure environments. These services can then be extended to a variety of endpoints within and across clouds.

NSX is an implementation of a software-defined network. It provides network services such as switching, routing, load balancing, firewalls, and VPN. In a vSphere environment, an NSX deployment consists of the following components:

- vCenter Server (VC) - It provides NSX with access to the environment and objects it manages, such as virtual distributed switches and VMs. In NSX, a VC is called a compute manager. NSX supports multiple compute managers.
- ESXi hosts - After NSX modules are installed on an ESXi host, it is called a host transport node. Network services for VMs running on the host can be provided by NSX.
- NSX Edge nodes - VMs that provide network services to all the NSX components. Also known as edge transport nodes.
- NSX Managers - VMs that provide a browser-based GUI for administering the NSX environment.

NSX has the following logical network components:

- Segment - A logical switch that can connect VMs to gateways and a tier-0 gateway to a physical router.
- Tier-1 gateway - A logical router that routes traffic between segments.
- Tier-0 gateway - A logical router that connects tier-1 gateways to a physical router so that segments have external connectivity.

Applicability

The content contained within this guidance was intended for the following product and versions:

- VMware NSX 4.1

Application of this guidance to product versions outside of those listed is not supported.

Frequently Asked Questions

What do the severity codes mean?

As stated in the DISA Security Requirements Guides:

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.

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.

Most of the severity codes in the associated guides are CAT IIs. During STIG development DISA modifies severity codes on a per product and context specific basis.

How do I view a STIG?

STIGs are delivered as an XML file that follows the XCCDF schema as defined by NIST. These XML files can be imported into a tool called STIG viewer which is available from DISA for download here: https://public.cyber.mil/stigs/srg-stig-tools/

Can I import the XCCDF files into STIG Viewer?

Yes, the XCCDF files can be imported into STIG Viewer and then used to create STIG Checklists as necessary. They can alternatively be viewed by opening the XML file in Internet Explorer.

Are there any scripts or tools to help audit and remediate these controls?

Yes, there are example scripts and playbooks to aid in these tasks available in the GitHub repo linked below. Please carefully examine and test before running these in a production environment.

https://github.com/vmware/dod-compliance-and-automation/

What requirements were considered when developing this content?

All technical NIST SP 800-53 requirements and applicable SRGs were considered while developing this content. Requirements that are applicable and configurable will be included in the final content.