Security Configuration and Hardening Guide

June 26, 2025

VMware Cloud Foundation 9.0.0
VMware vSphere Foundation 9.0.0
VMware vSAN 9.0.0

vmware by Broadcom

Table of Contents

Revision History

Date	Description of Change
June 26, 2025	Initial Release for GA (9.0.0).

Introduction

The VMware vSphere Security Configuration & Hardening Guide (SCG) is the baseline for hardening and auditing guidance for VMware Cloud Foundation and the components within. It has long served as guidance for virtualization administrators looking to protect their infrastructure.

Security is always a tradeoff, and turning on all security features, to their highest levels of security, often impedes day-to-day administration efforts. The goal of this guide is to be a core set of security best practices that inform administrators. It is not a catalogue of all available security controls, but instead a reasonable baseline on which to build.

Disclaimer

This kit is intended to provide general guidance for organizations that are considering Broadcom solutions. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided "AS IS." Broadcom makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.

This material is provided as is and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the copyright holder or contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage. The provider makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of this sample. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations. You acknowledge that there may be performance or other considerations, and that these examples may make assumptions which may not be valid in your environment or organization.

License

What is Included?

The Security Configuration & Hardening Guide includes two primary artifacts at this time:

- vmware-cloud-foundation-security-configuration-guide-90-guidance.pdf (this document)
- vmware-cloud-foundation-security-configuration-guide-90-controls.xlsx (spreadsheet with the security hardening baseline controls, discussion, and PowerCLI automation examples)
- vmware-cloud-foundation-security-configuration-guide-90-controls.csv (a version which is more conducive to GitHub's change tracking, in the hopes of solving the perpetual question of 'what changed?')

Spaces have been removed from filenames to ease downloading from GitHub. File names will no longer contain minor version numbers so that URLs remain stable.

Download the Latest Version

This guide was developed with VMware Cloud Foundation 9.0.0 and supersedes all earlier versions and guidance. We strongly encourage readers to stay current with patches and updates as a major part of a good security posture. The most up-to-date version of this document can be found at:

https://github.com/vmware/vcf-security-and-compliance-guidelines

That link also contains numerous additional resources to help your security and compliance efforts.

This guidance evolves; please check for the latest version before commencing security efforts.

Intended Audience

The audience for the vSphere Security Configuration Guide is VMware Cloud Foundation and VMware vSphere Foundation customers who have implemented this software directly. There are many engineered data center & hybrid cloud infrastructure products that implement VMware infrastructure products as part of their solutions. If this describes you, please check with those products' support before implementing these ideas.

This guidance evolves and will continue to expand to cover all VMware Cloud Foundation components, as well as to include compliance-oriented guidance aimed at assisting auditors. Additional guidance for US Department of Defense and related users can be found in our DISA STIG and DISA STIG Readiness Guides.

Third Party Identifiers & Mappings

This document includes regulatory compliance and security control identifiers from external sources as a convenience to end users. This does not constitute endorsement, in either direction.

There is not a one-to-one mapping of product capabilities to third-party controls. A product capability, or set of capabilities, may be applicable to multiple controls. Conversely, a control may be satisfied with the use of multiple capabilities.

Control identifier numbers have been included from the Secure Controls Framework, version 2025.1, under the terms of the Creative Commons Attribution-NoDerivatives 4.0 International Public License. No modifications have been made to the control identifier numbers under the terms of the license.

VMware Appliances

VMware appliances, such as the vCenter Server Appliance (VCSA), are tested and qualified in known configurations. Altering the configuration of appliances may affect support. Avoid upgrading the appliance virtual hardware versions except under the guidance of VMware Global Support Services.

The VMware vSphere Cluster Services VMs have been hardened with guidance present here and take advantage of vSphere default settings. If your security scanner identifies missing parameters check to ensure that they actually need to be set.

VM Hardware Versions

There are varying opinions within the greater VMware community about upgrading virtual machine hardware versions. Newer virtual machine hardware versions introduce new feature and guest OS support, better compatibility and performance with CPU vulnerability mitigations, better support for modern CPU security features, better security defaults, and so on.

Upgrading virtual machine hardware changes the virtual hardware presented to the guest operating system, just as if a boot device in a physical server was placed in a newer physical server. Changes like this can vary in risk, may require more than one reboot, and may require human interaction to complete.

Note that a virtual machine snapshot will capture the virtual hardware version. This means that reverting a snapshot taken before the upgrade will also revert the virtual hardware version. This makes virtual hardware version upgrades less risky and enables easier testing.

In general, Broadcom guidance is to:

- Run the latest version you are able, ideally the latest version available in the major vSphere version you run.
- Use VM Hardware 14 (vmx-14) or newer. Version 13 introduces important performance and security improvements for CPU vulnerability mitigations, and version 14 introduces support for vTPM.
- Take snapshots of virtual machines prior to upgrading, but do not forget to remove the snapshot later.
- When scheduling virtual hardware compatibility upgrades use the "Only upgrade after normal guest OS shutdown" to help ensure that a compatibility update does not complicate an unplanned incident or HA event.

Use Your Head!

This guide will be updated as necessary to improve clarity, correct problems, and reflect new and changed functionality. While many of the general information security principles are timeless, the technical guidance in this guide should not be applied to versions other than the version it was qualified on. **Even within the products, many security-related changes have serious consequences for performance, functionality, and usability and should be implemented carefully, with thorough testing, and staged rollouts.**

Power Off

All guidance in the Security Configuration Guide is meant to be applied to virtual machines in a powered off state, or hosts which have been placed in maintenance mode and are able to restart. **Changes to ESX have made it so that most advanced parameters cannot be set with virtual machines powered on**. This ensures that the running configuration of a virtual machine matches the reported configuration, but in practice may require organizational process changes. We encourage organizations to take advantage of product defaults to reduce the scope of work.

Code Examples & Tools

This Guide contains PowerCLI examples that standardize on formatting, such as:

- $VM is a string containing the virtual machine name,
- $ESXi is a string containing the ESXi host name,
- $VDS is a string containing the Distributed Virtual Switch name,
- $VDPG is a string containing the Distributed Virtual Switch port group name,

These code snippets can make changes that deeply affect operations and the responsibility for the impact of these changes is yours. Test these changes in a controlled, non-production environment first, and apply them to production environments

using staged rollout techniques. One easy way to build a test environment is to run ESXi inside a VM for non-production testing purposes, just as the VMware Hands-on Labs do.

VMware Cloud Foundation 9.0 represents a fundamental change in the structure of VCF, and as a result the Security Configuration & Hardening Guide does not currently include sample automation scripts for auditing & remediating environments. These will follow in a future release.

We regret that while we are happy to accept constructive feedback about the code examples, we cannot supply scripting support. There are options for scripting and automation support through VMware Professional Services. Please contact your Account Executive for more information. You might also check out the thriving community at developer.vmware.com.

Alternatively, the “Code Capture” and “API Explorer” features inside the vSphere Client’s Developer Center can be used to discover APIs, help script, and automate tasks. It isn’t perfect, but, in general, if you can do it inside the client, it will give you an example script to automate.

Feedback & Support

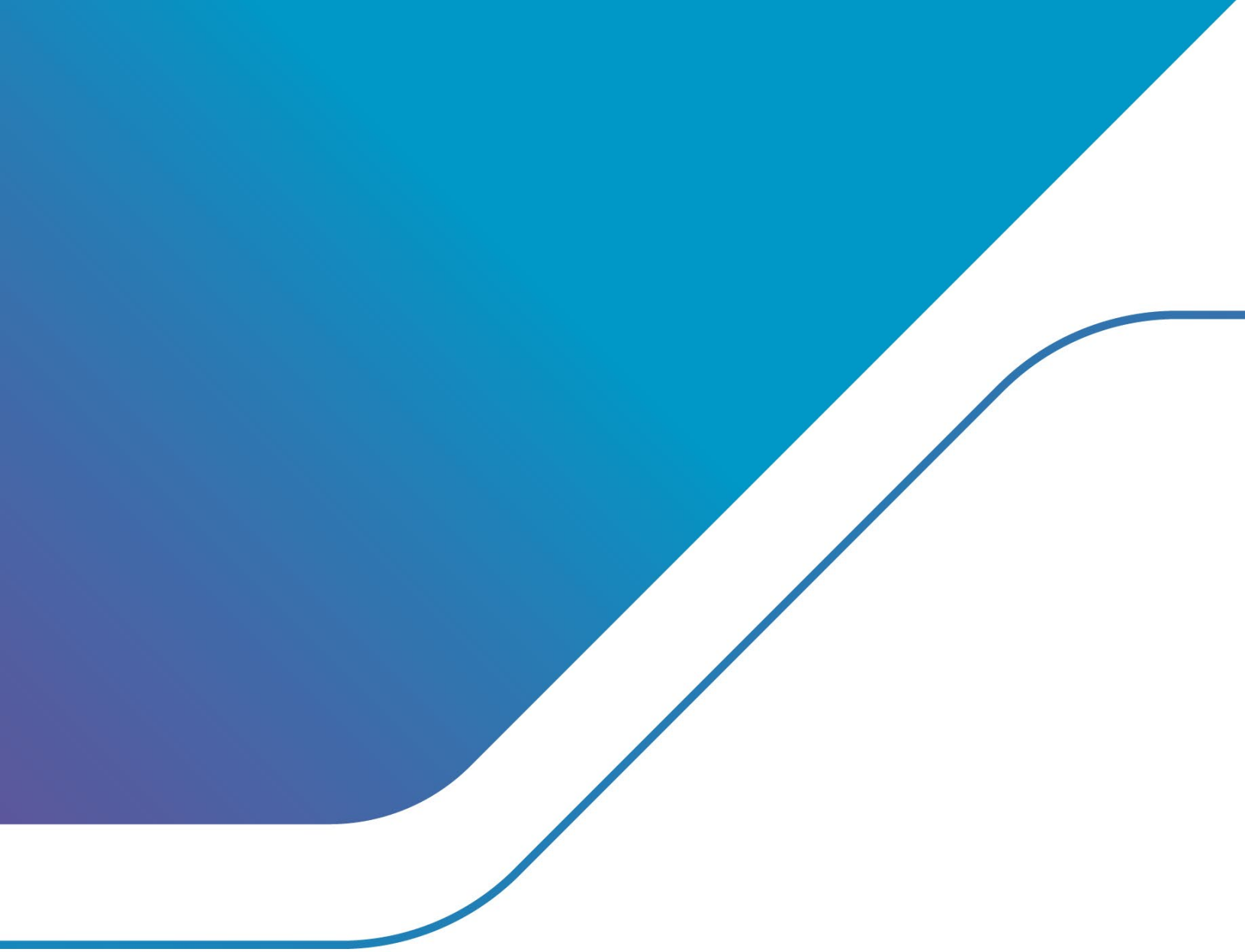
Please use the issue tracker in our GitHub repository to submit feedback:

https://github.com/vmware/vcf-security-and-compliance-guidelines/issues

For support, review the policy found at:

https://github.com/vmware/vcf-security-and-compliance-guidelines/blob/main/SUPPORT.md

Thank you.



vmware® by Broadcom