Security Configuration and Hardening Guide

October 18, 2024

VMware ESXi 7.0.3
VMware vCenter 7.0.3

vmware by Broadcom

Table of Contents

Revision History

Date	Description of Change
October 31, 2022	Initial Release for vSphere 7 Update 3 (7.0.3): • A “System Design” tab containing security controls that require deeper system design consideration and enablement. • A “Hardware Configuration” tab which has guidance for configuring server hardware. • An “Implementation Priorities” column, a way to help organizations figure out what’s most important so they can do those things first. In general, we’d suggest doing the “P0” things first, “P1” second, and “P2” last. For more information see the “Column Definitions” tab in the spreadsheet. • Updated product defaults. • Updated to reflect industry best practices, such as guidance from NIST 800-63B.
September 25, 2023	Update to standardize & backport new guidance: • New format, single sheet for security controls, with filterable headings. • Product & Feature mappings to make it easier to consume as we add feature-specific data. • The addition of an “Advanced” implementation priority. This designation gives us the ability to denote new security controls that may have serious operational considerations but are interesting to organizations wishing to pursue deeper security. As these controls mature they will become P0. • Revision of control IDs, descriptions, and discussion to reflect VMware guidelines on use of language, and standardizing on more generic descriptions for commonality with forthcoming regulatory compliance guidance. We apologize to everyone that must update their downstream information. • Inheritance of some STIG controls. Most of these items are enabled by default anyhow, requiring only an audit to confirm. • Removal of the “Removed” tab to avoid confusion. See Appendix A for controls which have been removed. • Updated PowerCLI examples to correct compatibility with PowerCLI 13.0. • Updated Default and Suggested values to better reflect exactly what the product parameters are. • Updates Security.PasswordMaxDays and other password age parameters to “9999” to reflect limits in the UI, while still respecting the spirit of NIST 800-63B. • Host Image Profile Acceptance has returned to “PartnerSupported or Higher.” As long as you are not at CommunitySupported there will be cryptographic protections for ESXi VIBs. • Addition of many more logging parameters. Updated local log storage guidance for discussion about storing data on less-resilient SD and USB flash boot devices. • Addition of deeper guidance for VMware Tools. • Correction of Implementation Priority and Action Needed errata. • Correction of sched.mem.pshare.salt errata, the recommended guidance has been updated. • Addition of VMware.vSphere.SsoAdmin PowerCLI examples where available. • Addition of “Hardening” to the SCG name. While it will continue to be referred to as the SCG, its name is now the VMware vSphere Security Configuration & Hardening Guide. • Various PowerCLI example updates. Thank you to those who have submitted feedback. • Numerous minor updates for clarity. • Reference to product versions with the build version, such as 7.0.3, versus other names such as “Update 3.” • The tables have been fixed so that they sort all columns correctly & together. • Spreadsheets have been saved as “read only” to prevent inadvertent editing.

October 18, 2024	• Update to download URL, license, support, disclaimer, and feedback mechanisms. • Protected the workbook sheets (no password, unprotect with Review -> Unprotect Sheet). • Renaming of the documents to remove serial numbers, in favor of Git-based revision control.

Introduction

The VMware vSphere Security Configuration & Hardening Guide (SCG) is the baseline for hardening and auditing guidance for VMware vSphere itself. 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 Guide is a kit that includes several tools:

- VMware vSphere Security Configuration Guide 7 – Guidance.pdf (this document)
- VMware vSphere Security Configuration Guide 7 – Controls.xlsx (spreadsheet with the security hardening baseline controls, discussion, and PowerCLI automation examples for auditing and remediating vSphere objects).

Download the Latest Version

This guide was developed with VMware vSphere 7 Update 3 (7.0.3) 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.

Intended Audience

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

The information in this document has not been tested on newer versions of VMware vSphere. Please use product guidance which closely matches the version of the product you are using. Thank you.

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.

Use Your Head!

This guide may be updated as necessary to improve clarity, correct problems, and reflect new and changed functionality within the major version of vSphere 7. 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 vSphere 7, 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 vSphere 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

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. Paul R. Ehrlich once said that "To err is human, but to really foul things up you need a computer." Nothing has proven that more clearly than placing code samples such as these in loops and iterating across an entire environment. Please always 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.

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 community at developer.broadcom.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.

Appendix A: Removed Controls

The following controls have been removed from this guidance due to changes in industry best practice:

esxi-7.ad-enable: Use Active Directory for ESXi user authentication.

Centralized directories have been a popular target for attacks, and a common path for attackers to move laterally into infrastructure. As a result, VMware's guidance for use of those directories has changed. We no longer suggest joining infrastructure to general-purpose Active Directories in organizations, leaving authentication and authorization as a design decision for individual organizations and environments.

vcenter-7.vami-networking-settings: Remove unnecessary NICs.

This configuration is very uncommon and is difficult to check for programmatically in a meaningful manner. Moved the idea to the System Design group.

vcenter-7.vami-access-dcli: Limit access to vCenter Server by restricting DCLI.

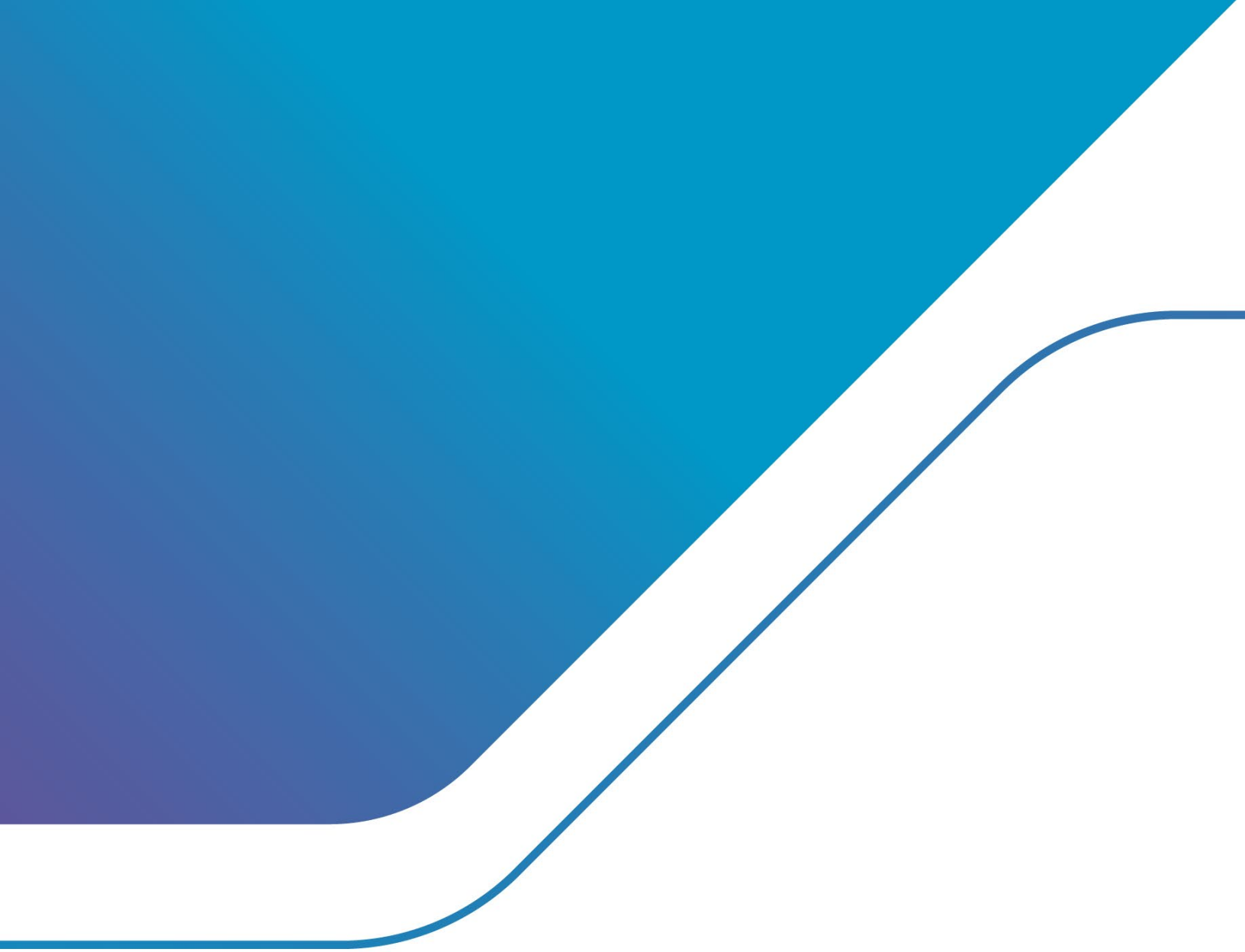
Was a wording error in the VAMI, the control alters the DCUI instead. VAMI was corrected in vSphere 7 Update 3.

vm-7.enable-vga-only-mode: Disable all but VGA mode on specific virtual machines.

Modern guest OSes often use graphics modes beyond VGA in their boot processes. Restricting access to those modes creates unnecessary friction for IT practitioners and limits access to diagnostic information. While there continues to be security merit to disabling 3D functionality when not needed, the return on investment of time and effort for this parameter is very low.

vm-7.isolation-bios-bbs-disable, vm-7.isolation-device-edit-disable, vm-7.isolation-ghi-host-shellAction-disable, vm-7.isolation-tools-dispTopoRequest-disable, vm-7.isolation-tools-getCreds-disable, vm-7.isolation-tools-ghi-autologon-disable, vm-7.isolation-tools-ghi-launchmenu-change, vm-7.isolation-tools-ghi-protocolhandler-info-disable, vm-7.isolation-tools-ghi-trayicon-disable, vm-7.isolation-tools-guestDnDVersionSet-disable, vm-7.isolation-tools-hgfsServerSet-disable, vm-7.isolation-tools-memSchedFakeSampleStats-disable, vm-7.isolation-tools-trashFolderState-disable, vm-7.isolation-tools-unityActive-disable, vm-7.isolation-tools-unity-disable, vm-7.isolation-tools-unityInterlockOperation-disable, vm-7.isolation-tools-unity-push-update-disable,vm-7.isolation-tools-unity-taskbar-disable, vm-7.isolation-tools-unity-windowContents-disable, vm-7.isolation-tools-vixMessage-disable,vm-7.RemoteDisplay-vnc-enabled, vm-7.isolation-tools-setGUIOptions-enable, vm-7.isolation-tools-vmxDnDVersionGet-disable

These parameters are unimplemented in vSphere 7 and newer. VMware does not recommend spending time implementing, maintaining, or auditing guidance that is not applicable to an environment. Some of these parameters do influence operations on VMware Workstation and VMware Fusion, however (such as the “Unity” parameters).



vmware® by Broadcom