Security Configuration Guide for VMware vSphere 7

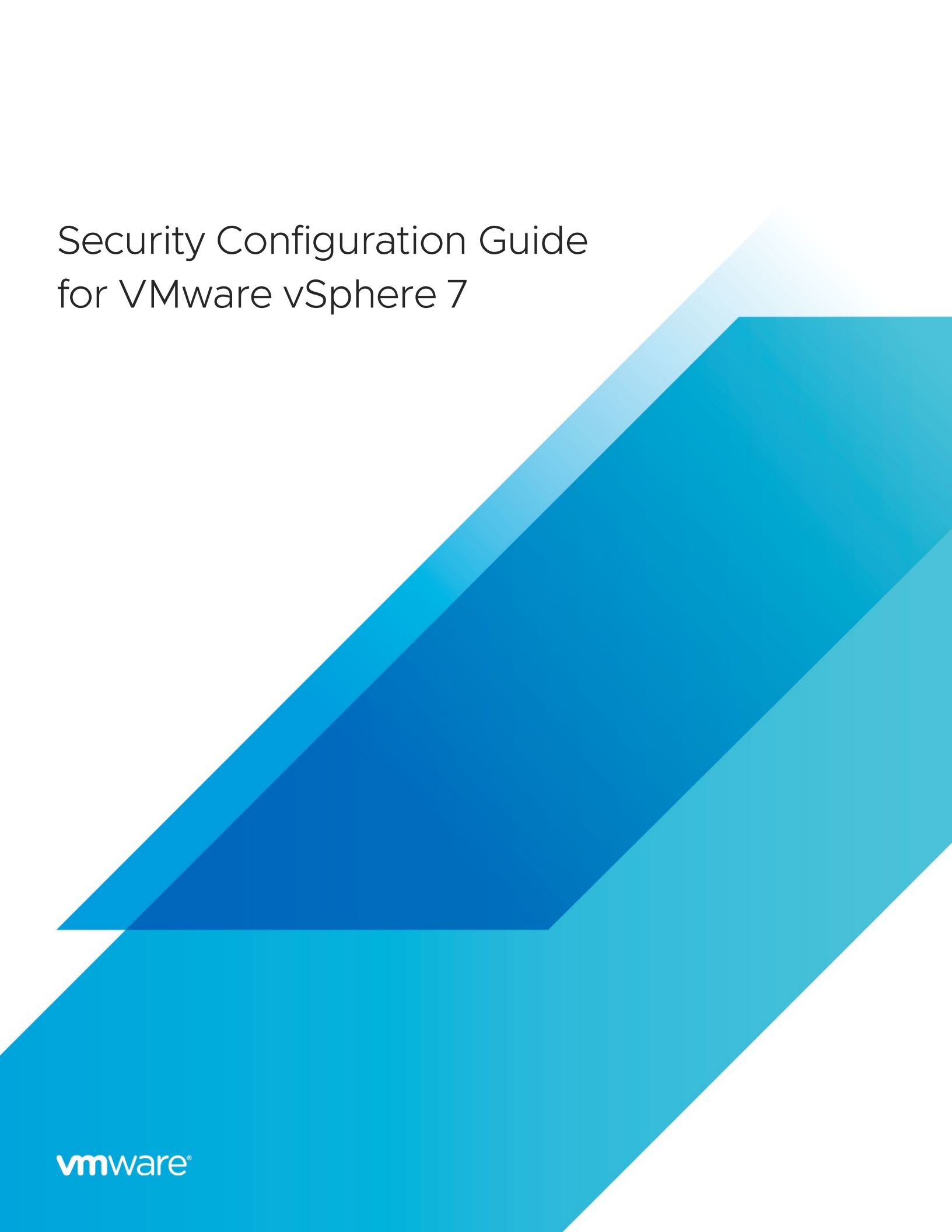

Table of Contents

Introduction

The vSphere Security Configuration Guide (SCG) is the baseline for hardening and auditing guidance for VMware vSphere itself. Started more than a decade ago, it has long served as guidance for vSphere Administrators looking to protect their infrastructure.

In the world of security there are compliance frameworks and implementation guides. Compliance frameworks, like NIST 800-53, PCI DSS, CMMC, and the like often specify what security goals we need to achieve, but they do not tell us how. In contrast, implementation guides are sets of specific technical controls, intended for a specific audience or application. These tell us how to do something, but not why. In an ideal world these two come together as a matched set, as they do in the VMware Compliance Kits for NIST 800-53 and PCI DSS, to bridge the gap between implementation & audit.

Implementation guides tend to be inflexible; you implement them the way they say or else! Should a vSphere Administrator who wants security guidance adopt an implementation guide that isn't specifically for them? For example, a DISA STIG is intended for use by agencies of the United States' federal government and has guidance specific to federal standards. Security is always a tradeoff against something else, primarily usability, but often performance, staff time, and expense, too. Too much security is costly in terms of opportunity cost. Too little is costly in terms of security incidents and liability. Compliance frameworks are helpful in determining a balance, but in lieu of that how does a vSphere Administrator and their organization choose to trade usability, staff time, and budget?

This is where the vSphere SCG fits in. The vSphere Security Configuration Guide is intended to be a baseline set of security best practices that inform a vSphere Administrator's security efforts but does so in a general way that examines the tradeoffs at hand. It has numerous "controls" but no scoring and no risk profiles or levels. Does other security guidance have those things? Yes, and they need to. DISA needs to be able to score their agencies against their own standards, and a compliance auditor needs to be able to determine if an organization has correctly implemented security processes. The SCG's goal, though, is to be guidance that reflects that security is a process, not just a particular set of tools, products, or security "nerd knobs" on a spreadsheet, and to meet organizations where they are to find the balance they need.

What's New in vSphere SCG

The vSphere Security Configuration Guide 7 is the first major update in a few years and reflects a changed landscape, both within VMware and in information security in general.

First, this version is a transition to a new model that, in the future, will be aligned to our compliance efforts. As much as we vSphere Administrators like to try to avoid compliance it is here to stay, and we have found that much of the friction around compliance is caused by gaps in understanding during the audit process. By aligning to NIST 800-53 and using our patented processes for mapping those controls into NIST 800-171, CMMC, PCI DSS, ISO 27001, NERC CIP, and other compliance standards, we can reduce duplicate efforts and create better guidance that helps fill the gaps in understanding and gets you to a secure state faster.

Second, this update reflects the core tenets of information security: confidentiality, integrity, and availability. This is called the CIA triad and it reflects that security is woven into all aspects of IT. Our guidance needs to reflect that, too. Security isn't just keeping our data safe in place, it's keeping it safe in use, and making sure that our systems are usable when we need them to be. Threats like CPU & hardware vulnerabilities and ransomware were unrealized when vSphere 6.7 was released, but they are major considerations now which everyone needs to take very seriously. To these ends we are "doubling down" on ideas like reducing attack surface, disabling SSH (and leaving it that way), automating with PowerCLI & APIs, patching at all levels, and isolation among

systems. Acknowledging this new reality, prior vSphere SCG guidance that encouraged other behaviors has been removed in this release.

Last, the release of VMware vSphere 7 in April 2020 brought new technologies, but also new release processes, too. Moving forward we hope to release updates to vSphere on more regular intervals. The intention is to update the SCG at those intervals as well, correcting errors and omissions that we find, introducing automation, and adjusting the guidance to reflect changing defaults in vSphere. The vSphere SCG isn't just for customers, we also use it as a benchmark for how well we are meeting our goals of making vSphere secure by default and making security features easy to use. You will see that some of the SCG guidance reflects that and offers vSphere Administrators the option of relying on the new defaults in order to reduce the customizations that need to be managed.

Intended Audience

The audience for the vSphere SCG is VMware vSphere customers who have implemented vSphere 7 directly. There are many engineered data center & hybrid cloud infrastructure products, like VMware Cloud Foundation, VMware Cloud, Dell EMC VxRail, and such that implement vSphere as part of their solutions. If this is how you consume vSphere you should check with those products' support for guidance on security first, before implementing these ideas. Some of the vSphere SCG's recommendations are likely to be safe to implement, but others may interfere with operations of those solutions.

VMware Appliances

VMware appliances, such as vCenter Server, are tested and qualified in known configurations. Take care if you choose to alter those, as it may impact support. In particular, avoid upgrading the appliance virtual hardware versions except under the guidance of VMware Global Support Services, and if you do please understand the risks and take precautions using backups and snapshots.

There are ongoing efforts to standardize security guidance & implementations within VMware and the SCG is a part of that. Future product releases will bring the defaults forward, as old product versions become unsupported.

Use Your Head!

This guide will 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 vSphere 7. 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.

A wonderful way to test functional changes to vSphere is by taking a page from the VMware Hands-on Labs: use nested virtualization. While it isn't supported for production use, ESXi can be installed inside ESXi. You can give it virtual TPMs, enable secure boot, configure vSAN, and do most everything you can do on hardware. Install a test vCenter Server and you're set. The advantage is that you can also take a snapshot of it (though we recommend it all be off when you do, for cluster consistency) so if you do something dangerous you can revert the snapshot and keep testing.

Code Examples

The PowerCLI examples in the vSphere SCG have all been prefaced with "#" to make them comments, so they cannot be pasted into PowerCLI directly. It might be annoying, but this is for safety. These code snippets can make changes that deeply impact operations and the responsibility for the impact of these changes is with you if you execute them in your environments. Heed the guidance above, test first.

We regret that while we are happy to accept constructive feedback about the code examples, we cannot provide 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 code.vmware.com.

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

Disclaimer

This set of documents is intended to provide general guidance for organizations that are considering VMware solutions to help them address compliance requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide regulatory advice and is provided "AS IS." VMware 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 regulatory compliance requirements.

Feedback

See an error, something is unclear, or there is a potential improvement? We strive for 100% accuracy, but it happens. We at VMware enjoy feedback and discussions with customers and the community. Whether it is this guide, an issue with a product, or an improvement that would make your life better please say something. For issues with this guide in particular please email Bob Plankers, rplankers@vmware.com, and include "SCG7 Feedback" in the subject.

vSphere 7 Update 1 and later releases integrate a feedback mechanism directly into the vSphere Client. Something in the product bothering you? Don't keep it a secret; please use the feedback system and tell us so that we can fix it.

Download the Latest Version

This is Security Configuration Guide for VMware vSphere 7 version 701-20210210-01.

This guide was developed with VMware ESXi 7 build 17551050 and vCenter Server build 17327586. 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://via.vmw.com/scg*

Anatomy of this Guide

Included with this document is a Microsoft Excel spreadsheet with four tabs:

- VMware ESXi, containing a table with guidelines that apply specifically to VMware ESXi. These include ESXi-centric features like the vSphere Standard Switch, the Host Client, etc.
- VMware vCenter Server, containing a table with guidelines specific to the vCenter Server VAMI and features enabled through vCenter Server, such as the vSphere Distributed Switch.
- Virtual Machines, containing a table of guidelines that refer mainly to the "outside" of a virtual machine. In many cases this is a judgement call but, in general, if it is an advanced setting to be applied to the VM it is here.
- In-Guest, containing a table of guidelines that, if implemented, need to be coordinated with the guest OS more closely.
- Deprecated, containing a table of guidance that is no longer applicable or desired.

These tables are all sortable and filterable depending on your needs. Not all tables contain the same columns.

"Action Needed" Column

The tables of guidelines all have an "Action Needed" column. The guidance is:

- Add: you will need to add a parameter to implement the guidance.
- Audit: check this to see if it is correct, fix it if not.
- Audit or Remove: the default behavior of vSphere 7 is what this guidance recommends, so after checking it to find deviations you can remove the parameter completely if you wish to use the defaults.
- Modify: the parameter or setting should already exist and will need to be modified.

How to Use This Guide

One of the nice things about the vSphere Security Configuration Guide is that you can choose how you use it. Ideally, implementation of these ideas begins as a discussion with your fellow vSphere Administrators, organizational management, and admins responsible for workloads. It should not be used directly as a checklist, as not every entry in it will apply to your organization.

The vSphere SCG does show opinions at times, but it does not indicate priorities. Indeed, prioritization of improvements will depend on your own organization. All of these suggestions are easy to implement in a brand-new deployment, but a working environment won't be as easy to change. Do what you can, prioritize according to your perceived gaps. Security is a process, after all.

If you'd like a suggestion for a starting point, patching & updates would be one of our top priorities, along with disablement of SSH and good authentication practices.

Other Tools & Automation

Other organizations take the vSphere SCG and incorporate it into their own tools and guidance. This often turns the SCG into an implementation guide or type of compliance artifact, which it is not intended to be. There are many excellent, flexible tools for helping audit security. Please take care and ask questions when presented with them.

If you need compliance guidance please check out the VMware Compliance Kits, found at: *https://core.vmware.com/compliance*

Special Thanks

Special thanks for contributions & feedback go to Mike Foley for his years of work defining this space, democratizing security information, and driving security forward within VMware, along with Adam Eckerle, Ken Werneburg, Niels Hagoort, Nigel Hickey, Kev Johnson, David Stamen, Myles Gray, Michael West, Justin Murray, Jim Brogan, Jatin Purohit, Aditya Sahu, Glenn Sizemore, Joe Sciallo, Amy Waller, Ken Drori, David Dunn, Barry Gerhardt, Edward Hawkins, Kevin Christopher, Jesse Pool, Manoj Mulpuru, Sam Subramanian, Nishant Arya, Swapneel Kekre, Jerry Breaud, Carlos Phoenix, Brian Armer, Chandra Prathuri, Paul Turner, Weiguo He, Lee Caswell, Lincoln Porter, Ryan Lakey, Ryan Johnson, Tanya McClymonds, Wayne Pauley, Dennis Moreau, Ravi Jagannathan, Carl Olafson, and countless others throughout the greater VMware community whose encouragement, questions, comments, and works big and small provided the foundation for this.

As always, thank you for being our customers, and for working hard to improve security.

- Bob Plankers

Changelog

February 10, 2021 701-20210210-01	Updated with cumulative feedback. • Corrected errors in the PowerCLI guidance for auditing VMs (Get-VM vs. Get-VMHost) • Introduced the “Deprecated” tab to track guidance that is obsolete. • svga.vgaOnly moved to Deprecated tab with explanation. • Updated guidance for esxi-7.disable-cim. • Introduced esxi-7.disable-slp • Introduced esxi-7.network-isolation-vmotion, esxi-7.network-isolation-vsan, esxi-7.network-isolation-hardware-management, and vcenter-7.network-isolation-management to reflect system design guidance for defense-in-depth. • Introduced esxi-7.supported and vcenter-7.supported to resolve a loophole many compliance frameworks have closed, where an organization can meet the letter of “running all available patches” but not have any patches available because the software has exceeded its support lifespan. • Introduced esxi-7.hardware-tpm as guidance to acquire and enable hardware Trusted Platform Modules. This is an important and inexpensive component that enables very advanced security features and should be included in all server hardware purchases moving forward. • Reinstated vm-7.pci-passthrough with updated guidance. • Introduced vcenter-7.vami-access-dcli. • Minor wording changes and corrections for clarity

October 6, 2020 701-20201006-01	Initial Release. • The esxcli and vcli examples from previous guides have been removed, as we discourage use of SSH as a management interface. • DISA STIG ID has been removed pending release of new STIGs under the new DISA processes. • Documentation & API references have become more dynamic, please use docs.vmware.com and code.vmware.com directly to find API calls. Alternatively, the “Code Capture” and “API Explorer” features inside the vSphere Client’s Developer Center can be used to discover APIs and help automate. • VM hardware version guidance is tricky. We’d love it if you came up to VM Hardware 18 but understand the process. Please make sure you’re up to version 11, though. • We took an intentionally light stance with CPU vulnerabilities. They aren’t just technical issues, but discussions of risk, budgets, performance, and architectures. Hopefully the approach we took with checking for suppressed warnings and emphasizing patching leaves room for flexibility. • Mention of strict lockdown mode is just a reference in the guideline about normal lockdown mode. Strict lockdown mode has serious operational implications. Many customers use the SCG as a straight checklist and having a line item for strict lockdown that contradicted normal lockdown caused implementation issues. • A few other controls were removed because they did not represent best practices, they added complications, or in most cases were covered by other controls. If there was doubt we evaluated it by looking at the friction it would cause a vSphere Administrator for the return on time investment, and whether it made sense for every vSphere installation on our planet. • All of the guidance in the vSphere SCG is to be applied through PowerCLI, the vSphere Client, or the Host Client. There is only one control, ESXi Secure Boot, that may require SSH to check enablement and compatibility. If you do that, please disable SSH afterwards.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com