Security Configuration Guide for VMware vSphere 6.5

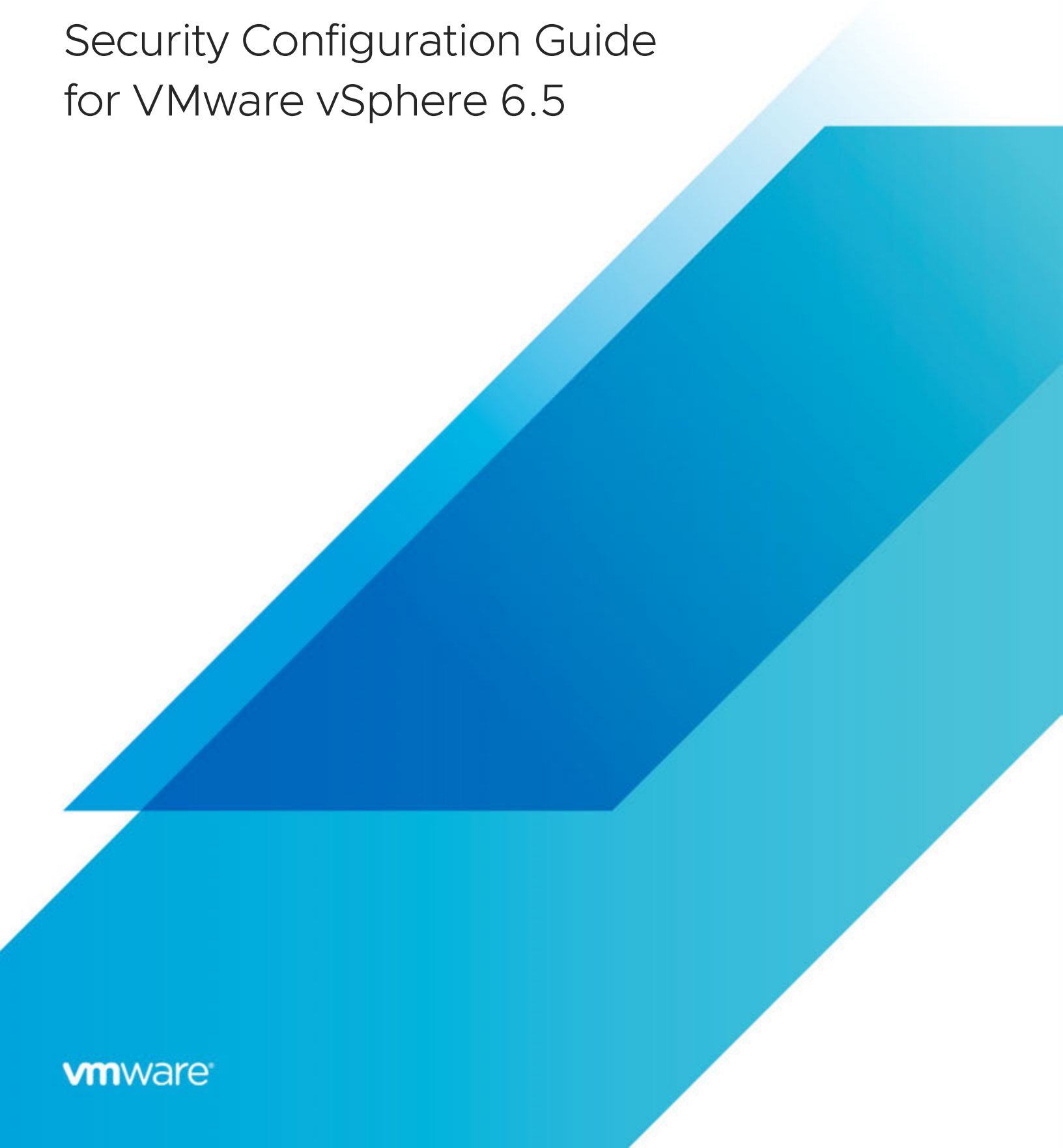

Table of Contents

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.

Intended Audience

The audience for the vSphere SCG is VMware vSphere customers who have implemented vSphere 6.5 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 6.5. 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 6.5. Even within vSphere 6.5, 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 scripting examples in the vSphere SCG 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.

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 "SCG65 Feedback" in the subject.

Download the Latest Version

This is Security Best Practices Guide for VMware vSphere 6.5 version 651-20170727-01.

The most up-to-date version of this document can be found at: *https://via.vmw.com/scg*

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

Date	Notes
February 10, 2021 651-20210210-01	Update to newer format with Guidance doc. • Introduced the “Deprecated” tab to track guidance that is obsolete. • svga.vgaOnly moved to Deprecated tab with explanation. • Introduced ESXi.disable-cim. • Introduced ESXi.disable-slp. • Minor wording changes and corrections for clarity

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: vmw-wp-temp-uslet-word-101-proof 6/20