Security Configuration Guide for VMware vSphere 8 IA

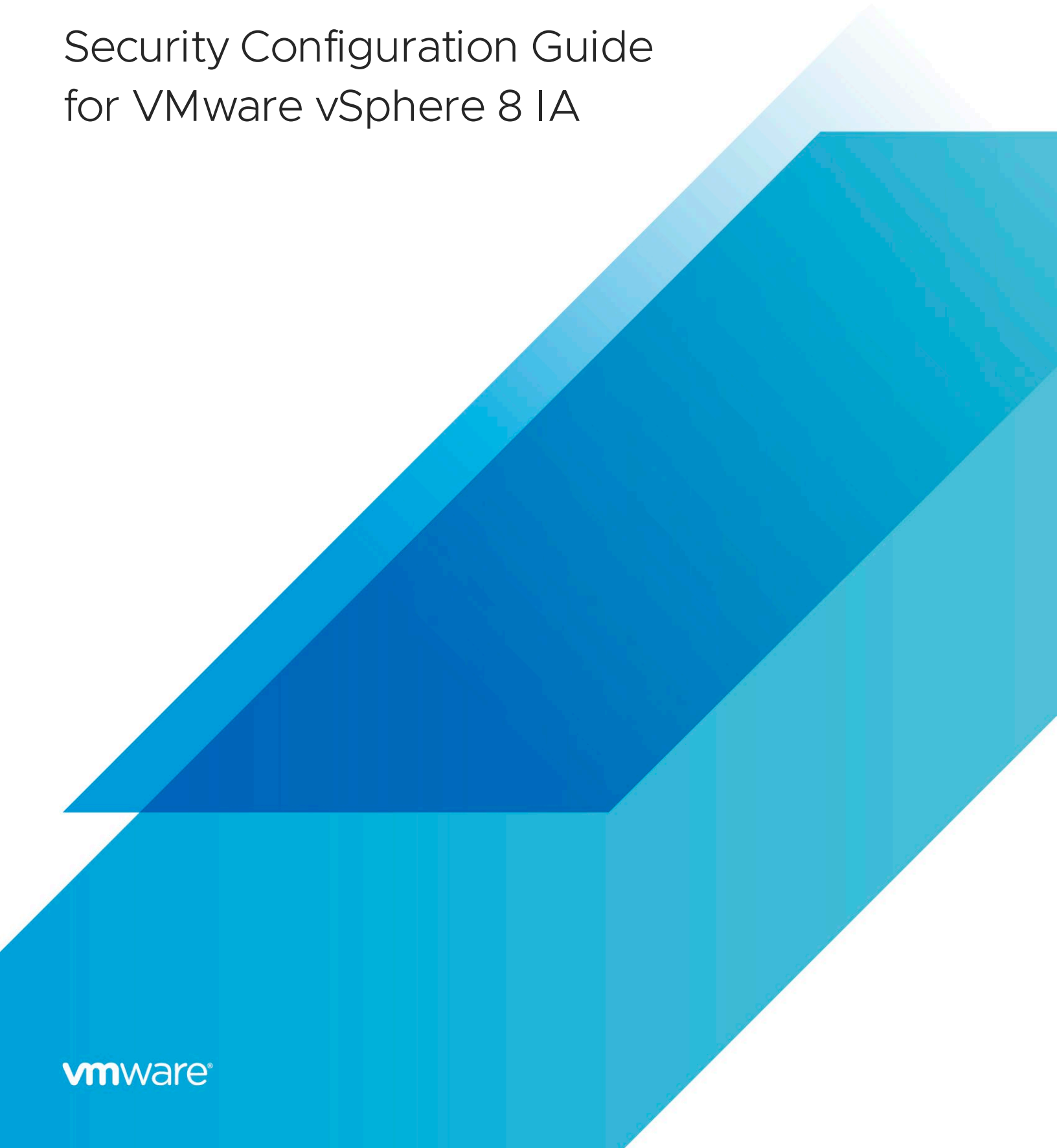

Table of Contents

Introduction 3
Disclaimer 3
What's New in vSphere Security Configuration Guide 7 Update 3 3
Intended Audience 4
VMware Appliances 4
Use Your Head! 4
Code Examples 5
Feedback 5
Download the Latest Version 5
Anatomy of this Guide 5
"Action Needed" Column 6
Special Thanks 6

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.

The vSphere Security Configuration Guide is intended to be a baseline set of security best practices that inform a vSphere Administrator's security efforts in a general way that examines the tradeoffs at hand. Turning on all security features to their highest levels can be detrimental, impeding day-to-day efforts by administrators to operate, patch, and monitor their environments. The Security Configuration Guide is not a catalogue of all available security controls, it is simply a reasonable baseline from which we can operate.

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.

What's New in vSphere Security Configuration Guide 8 IA

This release of the vSphere Security Configuration Guide is the first for vSphere 8, for the "Initial Availability" or IA release. It reflects new features and functionality present in the new major version. As future update releases are released for vSphere this guidance will also be updated.

This release of the vSphere 8 Security Configuration Guide builds on the latest guidance for vSphere 7, with similar changes to the format of the resources:

- A new "System Design" tab containing security controls that require deeper system design consideration and enablement. When seen through the core tenets of information security, all features of vSphere are security features. This release of the Security Configuration Guide begins to treat them as such.
- A new "Hardware Configuration" tab which has suggestions for configuring server hardware. This includes enablement of CPU security features, Trusted Platform Modules, security of hardware controllers, and more. Many hardware security functions are best configured before installation of ESXi, and this is intended to help encourage and guide those activities.
- A new "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.
- All new PowerCLI examples. See the section of this document entitled "Code Samples" for more information.
- Reflections of industry-standard best practices, including guidance about password expiration from NIST 800-63B and more.
- Wording changes across the whole guide. Many changes were made to improve clarity for users of the guide, from the headers of the columns to even what we use for "Yes" and "No."

This guide also departs from the traditional vSphere Security Configuration Guide in a few ways:

- The addition of compliance-oriented guidance such as login banners. While these are not strictly related to the security of the platform, there are important business reasons to use them.
- Stronger opinions on product defaults. In talking with customers about security they say that staffing and staff time continues to be a concern. By relying on the product defaults (many of which were updated in vSphere 8 to be secure by default) organizations can reduce the time they spend managing settings. You will see this reflected in the "Audit" guidance, where an undefined value can be accepted as valid.
- The removal of hardening guidance that does not apply to vSphere 8 or workloads running on vSphere 8. Third-party tools and resources that continue to check for unimplemented, irrelevant, and obsolete parameters should be updated.

Intended Audience

The audience for the vSphere Security Configuration Guide is VMware vSphere customers who have implemented vSphere 8 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 before implementing these ideas.

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 will 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.

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

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 8. 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 8. **Even within vSphere 8, 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

This Guide contains new PowerCLI examples that standardize on formatting. For example, $VM is a string containing the virtual machine name, and $ESXi is a string containing the ESXi host name.

The octothorpes (the '#' symbol) have been removed. This makes cutting & pasting potentially more dangerous but helps many people hoping to automate more things in their environment. Placing these in loops to operate on whole environments should be easy, but also can be dangerous, and is left as an exercise for you. Please always test these changes in a controlled, non-production environment first.

These code snippets can make changes that deeply affect operations and the responsibility for the impact of these changes is yours.

Important note: changes to vSphere have made it so that 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.

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, too, isn't perfect, but in general if you can do it inside the client, it will give you an example script to automate.

Feedback

Something wrong with this guide? Sorry about that. We strive for 100% accuracy, but it happens. Please visit:

https://via.vmware.com/scg

and use the Feedback mechanism on the page there to send us information. Thank you.

Download the Latest Version

This is Security Configuration Guide for VMware vSphere 8 version 800-20221031-01.

This guide was developed with VMware ESXi 8 build 20513097 and vCenter Server 8 build 20519528. 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.vmware.com/scg

Anatomy of this Guide

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

- Column Definitions, explaining the columns in the other tabs
- System Design, containing guidelines that should be implemented as part of the overall design of the environment.
- Hardware Configuration, containing guidelines for hardware configuration to support vSphere security features and functions.

- VMware ESXi, containing 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 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.
- Removed, 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, and not all columns are applicable to each entry.

"Action Needed" Column

The "Action Needed" column has been simplified:

- Modify, meaning that you should change that setting or feature.
- Audit, meaning that you should check that it is set correctly, or that it is unset and using the secure product default.

A valid course of action may also be removing the parameter and relying on the default.

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, Martin Philippi, Michael Banack, Michael MacFaden, Michael Eisler, Sam Subramanian, Nishant Arya, Swapneel Kekre, Jerry Breaud, Carlos Phoenix, Brian Armer, Chandra Prathuri, Paul Turner, Will Pien, Bo Fu, Bo Dong, Weiguo He, Lee Caswell, Lincoln Porter, Ryan Lakey, Ryan Johnson, Tanya McClymonds, Wayne Pauley, Dennis Moreau, Ravi Jagannathan, Carl Olafson, Andrew Sharpe, Colin Westwater, Marcel Daube, Markus Struck, 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

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