Security Configuration and Hardening Guide

January 7, 2026

VMware ESXi 8.0.3
VMware vCenter 8.0.3
VMware vSAN 8.0.3

vmware by Broadcom

Contents

Revision History

Date	Description of Change
October 10, 2022	Initial Release for IA (8.0.0): • 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.
June 13, 2023	Major update for vSphere 8 Update 1 (8.0.1): • New format, single sheet for security controls, with filterable headings. • Inclusion of a second worksheet tab – “Changes Highlighted” – making it easier to see what changed since the last revision. Updated cells appear in yellow. The background table formatting continues to alternate blue & white and does not convey meaning. • 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. • Addition of mappings to DISA STIG. This is not comprehensive, as DISA has more stringent requirements, but where there is baseline overlap with the STIG it is noted. • Inheritance of some STIG controls. Most notably there are FIPS controls now present in the baseline. We weigh this heavily, because not all organizations require FIPS. However, FIPS support is in many ways synonymous with better TLS cipher suites, which are desirable. 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. • Updated PowerCLI examples to correct compatibility with PowerCLI 13.0. • Updated Default and Suggested values to better reflect exactly what the product parameters are. • Updated Security.PasswordHistory guidance to reflect an improved product default of “5” older passwords. • 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. • Spreadsheets have been saved as “read only” to prevent inadvertent editing.

September 21, 2023	Update for VMware vSphere 8 Update 2 (8.0.2): • Addition of Solution mapping information, to make it easier to handle VMware product groupings like VMware vSphere (which is a combination of VMware vCenter Server, VMware ESXi, and other components) or VMware Cloud Foundation. • Synchronization of control titles and recommended values, where feasible, with DISA STIG guidance and downstream regulatory compliance guidance. • Expansion of feature-specific guidance. For example, our guidance still recommends not enabling SSH on ESXi, but if you do there are additional controls that should be audited. Auditors who use this guidance should first survey the environment for use of specific features covered by this guide. • Addition of controls present in DISA STIG and downstream regulatory compliance guidance. • Addition of DISA STIG Suggested Values. The DISA STIG, delivered from public.cyber.mil, should always be considered the reference if there is a discrepancy between the guides. • Addition of VMware Configuration ID mappings, to help align downstream regulatory compliance guidance. • Addition of VCF Compatibility information, denoting parameters that should be used with care in a VMware Cloud Foundation environment. • Reintroduction of esxi-8.timekeeping-services, ensuring that timekeeping services such as NTP or PTP are enabled and running, separate from the configuration controls. In general, the approach moving forward is to have one programmatically auditable setting per control. • Reintroduction of esxi-8.ad-auth-proxy. • 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 8.0.2, versus other names such as "Update 2." • The tables have been fixed so that they sort all columns correctly & together.
September 25, 2023	Minor updates to synchronize 8.0.2 guidance with current 7.0.3 guidance where applicable: • Implementation priority for esxi-8.lockdown-dcui-access & esxi-8.lockdown-exception-users changed to P2 (default configuration is secure). • Implementation priority for vcenter-8.etc-issue changed to P1 to match other login banner guidance (product is secure by default but setting could be improved by the administrator). • Implementation priority for vcenter-8.vami-administration-password-expiration changes to P0 (product default needs to be examined and/or changed). • Feature/component for guest-8.secure-boot changed to Virtual Machine. • Slight wording change to esxi-8.hw-virtual-nic to clarify that it is a virtual NIC between ESXi and the management controller, not the out-of-band management controller NIC. • The Table of Contents page numbers were not accurate in the 802-20230921-01 release.
October 5, 2023	• Introduction of PowerCLI-based auditing tools (see "Tools" directory and PDF). • Addition of a column to show whether the auditing tools check the control. • esxi-8.memeagerzero changed to P0 to reflect threat landscape. • vcenter-8.administration-sso-lockout-policy-unlock-time changed to P0 to reflect threat landscape. • vcenter-8.etc-issue changed to P1 to synchronize with other banners' priorities. • vcenter-8.vami-administration-password-expiration corrected to P0. • vm-8.deactivate-non-essential-3d-features and vm-8.vmrc-lock defaults corrected for VM Hardware 21 (vmx-21). Older versions of VM Hardware may have other defaults and require auditing. • vcenter-8.network-restrict-discovery-protocol values adjusted to reflect PowerCLI output. • Numerous PowerCLI auditing examples updated to improve formatting and specificity of output. • Assignment of the Apache License, Version 2.0.

August 13, 2024	• Comprehensive revision of auditing tools, and addition of sample remediation scripts. See “Tools” directory and PDF for more information. • Addition of a column to show whether the sample tools remediate the control. • Update of the permalink to https://bit.ly/vcf-scg • Addition of “Changes” tabs to highlight updates to the guidance. • Spreadsheets are no longer read-only, but the sheets are protected. Use “Review -> Unprotect Sheet” to make them editable. There is no password. • Addition of design-8.boot-device to help guide users towards persistent boot volumes which ease logging. • Addition of design-8.native-key-provider to help users understand the tradeoffs between key providers when it comes to physical security. • Addition of design-8.network-isolation-vsan-icsci-target to guide users towards isolation for vSAN iSCSI services. • hw-8.hardware-tpm updated with new PowerCLI assessment capabilities. • Addition of esxi-8.key-persistence. • Separation of functionality between esxi-8.secureboot and a new control, esxi-8.secureboot-enforcement. • Addition of esxi-8.tls-profile. • Deprecation of esxi-8.tls-protocols, largely obsolete now with the new TLS profiles. This control will be removed in a future SCG release. • Modification of esxi-8.tpm-configuration to apply to the “TPM” feature, in an attempt to indicate that it only applies to hosts with TPM capabilities (which is recommended). • Addition of vcenter-8.network-mac-learning. • Addition of vcenter-8.tls-profile. • Addition of vcenter-8.vami-firewall-restrict-access. • Addition of vm-8.efi-boot-types. • Addition of vsan-8.data-at-rest, vsan-8.data-in-transit, vsan-8.file-services-access-control-nfs, vsan-8.file-services-authentication-smb, vsan-8.force-provisioning, vsan-8.iscsi-mutual-chap, vsan-8.object-checksum, vsan-8.operations-reserve. • Updates to numerous PowerCLI examples. • Addition of a column that indicates DISA STIG recommended values. • Addition of a column that indicates whether DISA STIG recommended values exceed that of the SCG. • Addition of a column that indicates PCI DSS 4.0 recommended values. • Addition of a column that indicates whether PCI DSS 4.0 recommended values exceed that of the SCG. • Updates to values in the “VCF Compatible” column.
September 4, 2025	• Change of recommendation for esxi-8.log-level-global (syslog.global.logLevel) to the default of “error.” With the addition of the audit logging subsystem it is no longer necessary to increase the verbosity of all logging to see security audit events. This change should also have a positive effect on log collection and storage volume and performance. Because this control has been part of VMware product security guidance for many years it will remain in this edition of this guidance to help publicize the update. • Changes to GitHub filenames to ease linking and downloading, as well as adopting VCF 9.0 style version control to monitor changes via commit history.
January 7, 2026	• Modification to esxi-8.api-soap-timeout recommendation to match common timeout value of 600 seconds. • Added PowerCLI commands for auditing vcenter-8.vami-administration-password-expiration, vcenter-8.vami-backup, and vcenter-8.vami-firewall-restrict-access. • Merged sample scripts with main Security Configuration Guide to manage together. See Appendix B. • Significant updates to the sample scripts. • General updates to text in the accompanying documentation.

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

VMware ESXi versus VMware ESX

With the release of VMware Cloud Foundation 9.0 the name of the VMware Hypervisor was changed from ESXi back to ESX. Documents such as this, which use information that span a range of release versions, may use the names ESXi and ESX interchangeably, or refer to the hypervisor solely as ESX for simplicity. Unless you are running VMware vSphere 4.1, please consider both ESXi and ESX to be the same, and use the product version to determine applicability to your environment.

If you are running VMware vSphere 4.1, or any version which has passed the End of General Support deadline, please know that Broadcom has resources available to assist you in migrating smoothly to the latest version.

Downloading the Latest Version

This guide was developed with VMware vSphere 8 Update 3 (8.0.3) 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

A shortened version of that URL exists as:

https://brcm.tech/vcf-scg

These links also contain numerous additional resources to help your security and compliance efforts.

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

Using Git to Download the Guide

The VMware VCF Security and Compliance Guidelines GitHub repository is a monolithic repository that contains multiple distinct projects and components related to infrastructure security and regulatory compliance. While that's helpful as a single place to visit to find materials, it can be overwhelming if you just need one particular thing, or even a group of files like what comprise the SCG. Complicating things further, with our use of GitHub we have stopped producing single Zip files to download, as binary files such as those are not compatible with how Git is meant to be used.

However, you can use the "sparse-checkout" function of Git to download just the directories you would like. For example, to check out only the VMware vSphere 8.0 hardening guidance you might use:

```
git clone --filter=blob:none --sparse https://github.com/vmware/vcf-security-and-compliance-guidelines.git
cd vcf-security-and-compliance-guidelines
git sparse-checkout set security-configuration-hardening-guide/vsphere/8.0
```

In the future, to retrieve the latest versions from the main repository, issue the command:

```
git pull
```

To add more directories from the repository, issue a command like:

```
git sparse-checkout add security-configuration-hardening-guide/vsphere/9.0
```

To see what is included in your copy of the repository you can issue the command:

```
git sparse-checkout list
```

Using Subversion (svn) to Download the Guide

GitHub also supports the older Subversion version control protocols which can be used to download directories without additional version control information. For example:

```
svn export https://github.com/vmware/vcf-security-and-compliance-guidelines/trunk/security-configuration-hardening-guide/vsphere/8.0
```

What is Included?

The Security Configuration & Hardening Guide is a kit that includes several artifacts:

- vmware-cloud-foundation-security-configuration-guide-8-guidance.pdf (this document)
- vmware-vsphere-security-configuration-guide-8-controls.xlsx (spreadsheet with the security hardening baseline controls, discussion, and PowerCLI automation examples for auditing and remediating vSphere objects)
- vmware-vsphere-security-configuration-guide-8-controls.csv (CSV version of the hardening controls)
- A “tools” directory with sample auditing and remediation scripts, based in VMware PowerCLI (PowerShell)

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.

Intended Audience

The audience for the vSphere Security Configuration Guide is VMware vSphere customers who have implemented vSphere 8.0.3 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.

If you desire VCF 5.2 guidance, use the DISA STIG for VMware Cloud Foundation 5.2, and only choose the product controls which can be set without editing components inside the virtual appliances.

Additionally the “VCF Compatible” column in this guidance indicates whether a control is compatible with VCF.

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 2025.4, 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. If you do decide to upgrade an appliance, ensure that you have a backup and/or a snapshot that you can revert to or restore if problems arise.

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 need to be set.

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.

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.

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.

This guide includes sample automation scripts for auditing & remediating certain components. Please see Appendix B.

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.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 pertaining to this Guide:

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-8.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-8.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-8.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-8.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-8.isolation-bios-bbs-disable, vm-8.isolation-device-edit-disable, vm-8.isolation-ghi-host-shellAction-disable, vm-8.isolation-tools-dispTopoRequest-disable, vm-8.isolation-tools-getCreds-disable, vm-8.isolation-tools-ghi-autologon-disable, vm-8.isolation-tools-ghi-launchmenu-change, vm-8.isolation-tools-ghi-protocolhandler-info-disable, vm-8.isolation-tools-ghi-trayicon-disable, vm-8.isolation-tools-guestDnDVersionSet-disable, vm-8.isolation-tools-hgfsServerSet-disable, vm-8.isolation-tools-memSchedFakeSampleStats-disable, vm-8.isolation-tools-trashFolderState-disable, vm-8.isolation-tools-unityActive-disable, vm-8.isolation-tools-unity-disable, vm-8.isolation-tools-unityInterlockOperation-disable, vm-8.isolation-tools-unity-push-update-disable,vm-8.isolation-tools-unity-taskbar-disable, vm-8.isolation-tools-unity-windowContents-disable, vm-8.isolation-tools-vixMessage-disable,vm-8.RemoteDisplay-vnc-enabled, vm-8.isolation-tools-setGUIOptions-enable, vm-8.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).

Appendix B: Sample Audit and Remediation Scripts

This guide includes sample scripts to model audit and remediation tasks at scale. The scripts serve three main purposes:

- **Ease of Use for Beginners**: These scripts act as a steppingstone for those new to scripting, while also having an important purpose. Using the readily available VMware PowerCLI cmdlets with PowerShell makes vSphere automation straightforward. The scripts prioritize readability over programmatic elegance to ensure they align closely with SCG examples and can be easily modified by administrators as needed.
- **Simplicity & Integration**: Adhering to the UNIX philosophy of doing one thing and doing it well, these scripts each have a single purpose, and can be used in conjunction with inherent features of PowerShell. For instance, use of the Select-String command for pattern matching, such as for finding audit lines containing the labels [PASS] and [FAIL]. Extensive examples are provided below.
- **Generating Audit Records**: The output is structured to provide audit details like dates, times, hostnames, and current configurations. This allows the scripts to capture a snapshot of an environment, aiding regulatory compliance, and also allowing administrators to demonstrate progress.

While these tools offer significant advantages, they aren't a one-size-fits-all solution. They can't assess design nuances, firewall configurations, patch levels, and more. There are also a number of controls that do not have programmatic methods of assessment, either. Nevertheless, these samples might decrease the manual effort tied to the SCG's controls.

License and Disclaimer

Support

While we are happy to accept constructive feedback about the code examples and tools, we cannot supply direct support for them, through the author or via VMware Global Support Services. 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.

Usage Warning

The audit scripts are set up to minimize the number of queries to a vCenter Server, to improve execution speed and to reduce overall load in a large environment. However, there still may be impact to a busy environment.

The sample remediation scripts **will change environments in ways that cause operational issues, require restarts, and might otherwise impact a running environment**. As such, you need to edit the script to remove the "Exit" commands that end the script. If you are not comfortable with this, you should not proceed. You can always remediate manually.

By changing the scripts you acknowledge and accept all risk associated with these sample tools.

Do not use the remediation scripts in production environments without careful consideration and testing.

Nested Test Environments

A great way to build familiarity with security and compliance controls in the SCG is with a nested test environment. You can run ESXi as a virtual machine on ESXi itself, and paired with a separate copy of vCenter Server you have a great (and snapshot-able) test environment. You can even configure vSAN. There are many community resources available for nested environments, use your favorite search engine to find them.

Audit & Remediation Coverage

Not all security controls are accessible programmatically. Not all security controls can be safely remediated programmatically, either. Where this is the case, it is denoted in the spreadsheet attached to the Security Configuration Guide itself. These are sample scripts and the authoritative reference is the Security Configuration Guide.

Additionally, these tools cannot audit and remediate design decisions, such as evaluating the trust you may have established between your identity provider and your infrastructure systems. For a comprehensive evaluation reach out to your account executive and VMware Professional Services.

Interaction with DISA STIG and Regulatory Compliance Guidance

These sample tools are built around the hardening guidance for VMware ESXi and VMware vCenter found in the Security Configuration & Hardening Guide in this kit. The US Department of Defense, and various regulatory compliance frameworks, may have other requirements that are out of scope for these samples. The beauty of these samples, though, is that you can feel free to adjust the parameters in the scripts as you see fit.

The Security Configuration & Hardening Guide has started to indicate differences between DISA STIG and PCI DSS 4.0 compliance requirements in the rightmost columns. Check it out.

How to Use These Tools

Step 0: Software Requirements

These scripts are built on VMware PowerCLI. They require VMware VCF PowerCLI 9.0.0 or newer. Installation instructions for PowerCLI can be found at https://developer.broadcom.com/powercli but it can be as simple as opening a relatively recent version of PowerShell (such as version 5.1 on a default Windows 10 desktop) and typing:

```
Set-PSRepository -Name PSGallery -InstallationPolicy Trusted
Install-Module -Name VCF.PowerCLI -MinimumVersion 9.0.0 -Scope AllUsers
Install-Module -Name VMware.vSphere.SsoAdmin -MinimumVersion 1.4.0 -Scope AllUsers
```

These tools assume the version of the products associated with this guide. Using these tools against a different environment will have untested results.

Earlier versions of these scripts checked versions of VCF components, and versions of PowerCLI. These checks were unreliable and presented problems for a number of users, especially where PowerCLI modules were installed manually, or where environments had mixed versions. As such, the checks have been removed, and now rely on your judgment.

Many organizations treat PowerShell and PowerCLI as a threat and block it on desktops. While it is true that attackers could use PowerShell, it is also a tremendous way for legitimate administrators to do work quickly, and that work helps secure environments from the threats that the organizations are concerned with. We encourage the information security staff inside organizations to work with VCF and vSphere administrators to find a way to allow this behavior on the select desktops or systems VCF administrators use to manage their environments.

Step 1: Connection Requirements

These tools are built to connect to a VMware vCenter Server. You may be able to connect directly to an ESXi host but it is untested. There are two methods for connecting. First, you can use the following commands to do so, substituting the correct values for User, Server, and perhaps Password (see below):

```
Connect-VIServer -User username@vsphere.local -Server vc-mgmt-a.vcf.lab
Connect-CisServer -User username@vsphere.local -Server vc-mgmt-a.vcf.lab
Connect-SsoAdminServer -User username@vsphere.local -Server vc-mgmt-a.vcf.lab
```

Second, you can use the included connect.ps1 script:

```
.\connect.ps1 -vCenter vc-mgmt-a.vcf.lab -User username@vsphere.local
```

This script will prompt for a password, collected from the console and masked with asterisks (*).

While it may be tempting to automate these connection strings, **under no circumstances do we recommend storing account logon information in a script**. Doing so is a leading cause of unauthorized access, breaches, and eventual situations like ransomware. Properly storing account information for automated tools depends heavily on your own environment and is out of scope for this document.

Step 2: Run The Tools

Change into the directory with the scripts and issue a command like:

```
.\audit-esxi-8.ps1 -Name esx-01a.vcf.lab
```

Replacing the value after "-Name" with a valid hostname in your environment. Similarly:

```
.\audit-vm-8.ps1 -Name TESTVM
```

However, the vCenter auditing script does not require a name, since you're already connected:

```
.\audit-vcenter-8.ps1
```

Running the tools individually gives you an idea of what the output will look like and will help expose any issues with their execution.

More information about the flags available for the scripts is below.

Step 3: Troubleshoot & Customize

Each script has additional flags you can use as needed:

"-NoSafetyChecks" which allows the script to run unhindered. Currently the only safety checks are to confirm that you are only attached to one vCenter, and that you have ESXi hosts attached to the vCenter.

"-NoSafetyChecksExceptAppliances" which allows audit-vm-8.ps1 to skip all checks except the ones for VMware appliances, like the vCenter Server Appliance, vCLS VMs, vSphere Cloud Gateway, and so on. Changing settings on those appliances is unsupported as per VMware Global Support Services policy.

"-AcceptEULA" will suppress the disclaimer, should you desire that (you could also edit the script to remove it).

"-OutputFileName" will log to a filename you specify. It will create the file or append to an existing one.

There are other flags to control the remediation scripts as well, documented below.

Step 4: Read the Output

Each line from the script will begin with the name of the object being examined, and then have a label:

[INFO] – Informational output, such as date, time, and target of the scan.

[WARNING] – A result that requires additional review.

[ERROR] – The script has an error and exited.

[EULA] – Disclaimer and risk acceptance, can be acknowledged with -AcceptEULA.

[PASS] – The control being tested passed the check. This does not mean it is secure, it means the check passed.

[FAIL] – The control being tested did not pass the check. This does not mean it is insecure, it means the check failed.

[UPDATE] – The remediation script was able to update this parameter. You should check it again with the audit script.

Each line will have the current configured value in parentheses at the end of the line.

No audit is perfect. Failures may simply indicate that something needs to be checked manually. For example, physical NICs connected to access ports will fail the check for default VLANs, even though they are not on a trunk and therefore not vulnerable to that type of problem.

Step 5: Use PowerShell to Search the Results

The previous version of these sample scripts allowed for direct filtering of output, but due to changes how they print text we need to use two steps: run the audit and write to a file, then use Select-String on the file:

```
.\audit-esxi-8.ps1 -Name esx-01a.vcf.lab -OutputFileName esx-01a.txt -AcceptEULA
Get-Content “esx-01a.txt” | Select-String -Pattern "\[FAIL\]|\[INFO\]"
```

This will return the lines that require further checking, labeled with [FAIL].

Characters like brackets ([or]) are special characters to PowerShell and require “escaping” or making the shell understand not to interpret them. The backslash (\) is what does that. The vertical pipe (|) symbol in the pattern means “or.” A tremendous use of modern Large Language Model (LLM) AIs is to ask them for help constructing patterns such as these. For instance, a statement like “Please give me the correct pattern for use with Select-String in PowerShell to find lines that contain [INFO], [PASS], and [FAIL]” will return a useful example.

Step 6: Remediate

There are three sample remediation scripts, for VMs, ESXi, and vCenter. Each has different flags to help control some behavior that may be disruptive.

To reiterate, these sample remediation scripts supplied here **will change environments in ways that cause operational issues, require restarts, and might otherwise impact the running environment**. As such, you need to edit the script to remove the "Exit" commands that end the script. If you are not comfortable with this, you should not proceed.

By changing the scripts you acknowledge and accept all risk associated with these sample tools. Do not use the remediation scripts in production environments without careful consideration and testing.

See the "Reference" section for parameters and syntax.

Step 7: Customize

Every environment has audit findings that are not actionable but continue to appear in reports. A good example here might be "unnecessary hardware" where a particular device, such as an XHCI controller, might be flagged but it is required for proper operation of the guest OS on your virtual machines. These scripts are set up in a way where you should be able to easily find and edit those out if they are truly false positives.

Similarly, you could filter them after the fact with Select-String commands.

Sample Script Command Reference

audit-vm-8.ps1

Assesses a particular virtual machine for compliance with the VMware Security Configuration Guide.

Parameters

-Name <string>: Name of the virtual machine object to be audited. Required.

-OutputFileName <filename>: Name of a file to receive the logged output from the audit. Optional.

-AcceptEULA: Accepts the disclaimer and the license for this tool to avoid the need for user input. Optional.

-NoSafetyChecks: Skip safety checks on software versions and VMware appliances. Optional.

-NoSafetyChecksExceptAppliances: Skip software version safety checks but do not audit VMware appliances. Optional.

audit-esxi-8.ps1

Assesses a particular ESXi host for compliance with the VMware Security Configuration Guide.

Parameters

-Name <string>: Name of the host to be audited. Required.

-OutputFileName <filename>: Name of a file to receive the logged output from the audit. Optional.

-AcceptEULA: Accepts the disclaimer and the license for this tool to avoid the need for user input. Optional.

-NoSafetyChecks: Skip safety checks on software versions. Optional.

audit-vcenter-8.ps1

Assesses a particular vCenter Server for compliance with the VMware Security Configuration Guide.

Parameters

-Name <string>: Name of the vCenter Server to be audited. Required.

-OutputFileName <filename>: Name of a file to receive the logged output from the audit. Optional.

-AcceptEULA: Accepts the disclaimer and the license for this tool to avoid the need for user input. Optional.

-NoSafetyChecks: Skip safety checks on software versions. Optional.

audit-all.ps1

Recursively assesses VMs, hosts, and vCenter for compliance with the VMware Security Configuration Guide.

Parameters

-OutputDirName <directory name>: Name of an empty directory to receive the logged output from the audit. Required.

-AcceptEULA: Accepts the disclaimer and the license for this tool to avoid the need for user input. Optional.

-NoSafetyChecks: Skip safety checks on software versions. Optional.

remediate-vm-8.ps1

Remediate a virtual machine against the VMware Security Configuration Guide.

Parameters

-Name <string>: Name of the virtual machine object to be audited. Required.

-OutputFileName <filename>: Name of a file to receive the logged output from the script. Optional.

-AcceptEULA: Accepts the disclaimer and the license for this tool to avoid the need for user input. Optional.

-NoSafetyChecks: Skip safety checks on software versions and VMware appliances. Optional.

-NoSafetyChecksExceptAppliances: Skip software version safety checks but do not audit VMware appliances. Optional.

-RemoveExtraDevices: When specified, will remove virtual CD/DVD, AHCI controller, USB & XHCI, parallel & serial port, floppy drive, and sound card devices from the virtual machine. This may negatively impact the function of the VM. Take a snapshot and ensure you also have a proper backup.

-UpdateHardwareVersion: When specified, updates the virtual machine hardware version to 21. There may be compatibility considerations for your guest operating system when doing this. Take a snapshot and ensure you also have a proper backup.

-TakeSnapshot: When specified, take a snapshot prior to making changes to the virtual machine. The snapshot name will be “Security Configuration Guide Remediation.”

connect.ps1

An example script for connecting to vCenter Server.

Parameters

-vCenter <string>: Name of the vCenter Server to connect to. Required.

-User <string>: Username to use when connecting to the named vCenter Server. Required.

remediate-esxi-8.ps1

Remediate an ESXi host against the VMware Security Configuration Guide.

Parameters

-Name <string>: Name of the virtual machine object to be audited. Required.

-OutputFileName <filename>: Name of a file to receive the logged output from the script. Optional.

-AcceptEULA: Accepts the disclaimer and the license for this tool to avoid the need for user input. Optional.

-NoSafetyChecks: Skip safety checks on software versions and VMware appliances. Optional.

-RemediateStandardSwitches: When specified, update standard virtual switches and their port groups against the recommended settings. This may have negative effects on workload connectivity.

-EnableLockdownMode: When specified, enable ESXi lockdown mode. This may have negative effects on the ability to connect directly to the host to manage it.

-RemediateTLSCiphers: When specified, enable TLS 1.3 and the NIST_2024 limited set of ciphers. This will require a host reboot, which you will need to orchestrate yourself.

remediate-vcenter-8.ps1

Remediate a vCenter Server against the VMware Security Configuration Guide.

Parameters

-Name <string>: Name of the virtual machine object to be audited. Required.

-OutputFileName <filename>: Name of a file to receive the logged output from the audit. Optional.

-AcceptEULA: Accepts the disclaimer and the license for this tool to avoid the need for user input. Optional.

-NoSafetyChecks: Skip safety checks on software versions and VMware appliances. Optional.

-RemediateDistributedSwitches: When specified, update distributed virtual switches and their port groups against the recommended settings. This may have negative effects on workload connectivity.