



Security Configuration and Hardening Guide

January 7, 2026

VMware Cloud Foundation 9.0.1
VMware vSphere Foundation 9.0.1
VMware vSAN 9.0.1

Contents

Revision History	3
Introduction	4
Disclaimer	4
License	4
VMware ESXi versus VMware ESX	4
Downloading the Latest Version	5
Using Git to Download the Guide	5
Using Subversion (svn) to Download the Guide	5
What is Included?	6
Intended Audience.....	6
Third Party Identifiers & Mappings	6
VMware Appliances	6
Use Your Head!.....	7
Power Off	7
VM Hardware Versions.....	7
Code Examples & Tools	7
Feedback & Support	8
Appendix A: Sample Audit and Remediation Scripts.....	9
License and Disclaimer	9
Support	9
Usage Warning	9
Nested Test Environments	10
Audit & Remediation Coverage	10
Interaction with DISA STIG and Regulatory Compliance Guidance	10
How to Use These Tools	10
Sample Script Command Reference	13

Revision History

Date	Description of Change
June 26, 2025	<ul style="list-style-type: none"> Initial Release for GA (9.0.0).
June 28, 2025	<ul style="list-style-type: none"> Updates to restore missing PowerCLI commands. Updates to correct several control defaults, and their subsequent priorities. Consolidation of ESX SSH configuration parameters into a single control, <code>esx-9.ssh-configuration</code>. Addition of <code>esx-9.account-password-history</code>. Addition of <code>esx-9.memory-tiering-encryption</code>. Addition of <code>vcenter-9.smtp</code>.
August 22, 2025	<ul style="list-style-type: none"> Change of recommendation for <code>esx-9.log-level-global</code> (<code>syslog.global.logLevel</code>) 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. Inclusion of PCI DSS 4.0.1 control mappings. Continued improvements to Secure Controls Framework mappings. Clarification and improvements to control descriptions.
August 23, 2025	<ul style="list-style-type: none"> Rerelease to correct formatting and data alignment error.
September 4, 2025	<ul style="list-style-type: none"> Modifications to <code>esx-9.log-level-global</code> priority and related columns.
January 7, 2026	<ul style="list-style-type: none"> Updates to the Secure Controls Framework mappings. Updates to the PCI DSS 4.0.1 mappings. Modification to <code>esx-9.api-soap-timeout</code> recommendation to match common timeout value of 600 seconds. Correction of find & replace errors for <code>UserVars.ESXiShellInteractiveTimeout</code>, <code>UserVars.ESXiShellTimeout</code>, due to renaming of ESXi in VMware Cloud Foundation 9.0. Updates to various descriptions, titles, discussions, and functional impacts. Added PowerCLI commands for auditing <code>vcenter-9.vami-password-max-age</code> and <code>vcenter-9.vami-firewall-restrict-access</code> Inclusion of sample audit and remediation scripts. See Appendix A.

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

Copyright (c) CA, Inc. All rights reserved.

You are hereby granted a non-exclusive, worldwide, royalty-free license under CA, Inc.’s copyrights to use, copy, modify, and distribute this software in source code or binary form for use in connection with CA, Inc. products.

This copyright notice shall be included in all copies or substantial portions of the software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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 9.0 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/9.0
```

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/cloud-foundation/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/9.0
```

What is Included?

The Security Configuration & Hardening Guide includes two primary artifacts at this time:

- vmware-cloud-foundation-security-configuration-guide-90-guidance.pdf (this document)
- vmware-cloud-foundation-security-configuration-guide-90-controls.xlsx (spreadsheet with the security hardening baseline controls, discussion, and PowerCLI automation examples)
- vmware-cloud-foundation-security-configuration-guide-90-controls.csv (a version which is more conducive to GitHub's change tracking, in the hopes of solving the perpetual question of 'what changed?')
- 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 Cloud Foundation and VMware vSphere Foundation customers who have implemented this software directly. There are many engineered data center & hybrid cloud infrastructure products that implement VMware infrastructure products as part of their solutions. If this describes you, please check with those products' support before implementing these ideas.

This guidance evolves and will continue to expand to cover all VMware Cloud Foundation components, as well as to include compliance-oriented guidance aimed at assisting auditors. Additional guidance for US Department of Defense and related users can be found in our DISA STIG and DISA STIG Readiness Guides.

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.

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 ESX 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 A.

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: 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

Copyright (c) CA, Inc. All rights reserved.

You are hereby granted a non-exclusive, worldwide, royalty-free license under CA, Inc.'s copyrights to use, copy, modify, and distribute this software in source code or binary form for use in connection with CA, Inc. products.

This copyright notice shall be included in all copies or substantial portions of the software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

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 ESX 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 ESX 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 ESX 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-esx-9.ps1 -Name esx-01a.vcf.lab
```

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

```
.\audit-vm-9.ps1 -Name TESTVM
```

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

```
.\audit-vcenter-9.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-esx-9.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, ESX, 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-9.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-esx-9.ps1

Assesses a particular ESX 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-9.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-9.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-esx-9.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-9.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.

