Security Configuration and Hardening Sample Tools

October 18, 2024

VMware ESXi 8.0.3
VMware vCenter 8.0.3

vmware by Broadcom

Table of Contents

Revision History

See the main vSphere Security Configuration & Hardening Guide (SCG) for information about revisions to guidance itself.

Date	Description of Change
October 5, 2023	• Initial Release of vSphere Security Configuration & Hardening Sample Tools.
August 1, 2024	• Comprehensive update to the SCG Sample Tools, including remediation scripts and logging capabilities.
October 18, 2024	• Update to download URL, license, support, disclaimer, and feedback mechanisms

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

Introduction

The VMware vSphere Security Configuration & Hardening Guide (SCG) has been the foundation for VMware vSphere hardening and auditing for the better part of two decades. Starting with vSphere 8.0.2, the SCG introduced sample scripts to automate auditing. 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.
- **Ability to Customize**: The scripts can be easily modified by end users to suit their needs. For example, if an organization requires a different login timeout value than the security baseline one only needs to edit the scripts to make the change.
- **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, while 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.

Feedback & 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.

Please use the issue tracker in our GitHub repository to submit feedback:

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.

Usage Warning

The audit scripts read from the environment, and attempt to minimize the number of queries to a vCenter Server. This improves execution speed and reduces overall load in a large 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 PowerCLI 13.3.0 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 VMware.PowerCLI -MinimumVersion 13.3.0 -Scope AllUsers
Install-Module -Name VMware.vSphere.SsoAdmin -MinimumVersion 1.3.9 -Scope AllUsers
```

These tools assume, and check for, VMware vCenter Server 8.0.3 and VMware ESXi 8.0.3. Using these tools against a different environment will have untested results. If you wish to subvert the safety checks, each script has a "-NoSafetyChecks" flag you can use. See below for more information.

Some users have reported that PowerCLI is not detected correctly by these scripts. This may be the case if you have installed a newer version of PowerShell than the version shipped with your operating system, or have manually installed the modules. In these cases you might choose to use -NoSafetyChecks, or simply edit the scripts themselves to comment the section out.

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 vcenter-1.8.fcotr.org
Connect-CisServer -User username@vsphere.local -Server vcenter-1.8.fcotr.org
Connect-SsoAdminServer -User username@vsphere.local -Server vcenter-1.8.fcotr.org
```

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

```
.\connect.ps1 -vCenter vcenter-1.8.fcotr.org -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-1.8.fcotr.org
```

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. Your mileage will vary.

"`-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.

"`-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.

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

Filtering with Select-String

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-4.8.fcotr.org -OutputFileName esx-4.txt -AcceptEULA
Get-Content "esx-4.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 Server. 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 actually 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.

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.

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-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.”

remediate-esxi-8.ps1

Remediate a 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

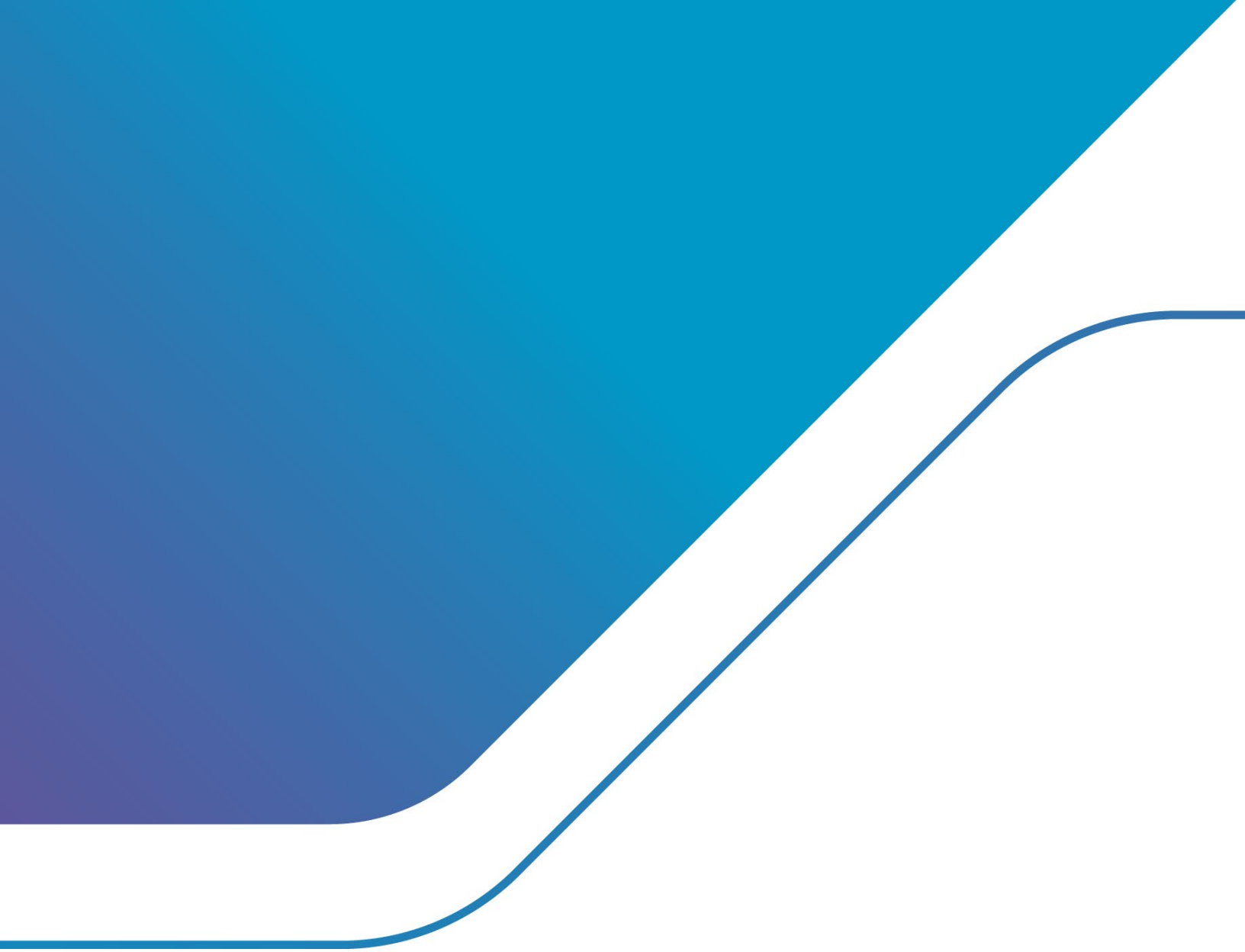
-Name <string>: Name of the virtual machine object to be audited. Required.

-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.



vmware® by Broadcom