Compliance & Vulnerability Scanning Frequently Asked Questions

VMware Compliance

Table of contents

Compliance & Vulnerability Scanning Frequently Asked Questions

Introduction

Many customers employ security & compliance scanning tools to assist them during audits of their environments. This is a collection of common questions posed to VMware about this process.

Questions

Can VMware recommend a vulnerability scanning tool?

VMware cannot make a recommendation for a particular scanning tool. While we do not support scanning tools directly, we do support use of approved APIs and clients. We do recommend choosing a solution that specifically lists vSphere as a supported scanning target because it shows that the maker of the tool understands how vSphere is delivered.

My scanning tool is asking me whether ESXi is Linux or UNIX. Which one should I pick?

VMware ESXi is its own operating system and is neither Linux nor UNIX. If your tool does not specifically support VMware vSphere components, you should avoid using it on your environment or use network-based scanning only. Scanning VMware ESXi as a Linux or UNIX host will, at best, result in false positives and lost staff time interpreting the false positives.

What is the best way to scan ESXi via SSH?

SSH and command shells (ESXi Shell) on vSphere components, like ESXi and vCenter Server, are maintenance & support tools designed for use only in temporary circumstances, at the guidance and instruction of VMware Global Support Services (GSS) staff. ESXi ships with SSH & the ESXi Shell disabled and off and raises alarms in vCenter Server if it is enabled and running. Neither are intended to be operational on the host.

There are no customer-serviceable or replaceable components inside ESXi. ESXi is delivered and maintained as a single software image, similar to how a network switch firmware is delivered, and altering permissions or software inside that image may affect availability and support.

We strongly recommend SSH be left disabled, and that scanning tools examine the version information to determine if an update is available.

What distribution of Linux do vCenter Server, SDDC Manager, and other appliances use?

While it is true that VMware virtual appliances are built on Linux, they are not general-purpose computing devices. Altering them in any way outside the guidance of VMware Global Support Services is unsupported. They are meant to be updated through the official APIs and interfaces.

As such, it is better to treat the appliances more like network switch firmware, where the OS would be “VMware vCenter Server” instead of a Linux distribution. This helps change managers and other organizational processes and staff understand that these appliances cannot be managed like other Linux systems.

My scanner says it found issues. How do I fix those?

VMware tracks all software installed and in use as part of our products. If a security or functional issue is reported to an external project VMware will assess its impact according to the VMware Security Response Policy. If needed, a subsequent update to the product will be made available through the supported update mechanisms according to the response policy schedule.

Changes made to file permissions or software components without the explicit guidance of VMware Global Support Services are not supported and may affect availability, serviceability, and supportability of your infrastructure. VMware is committed to the security and stability of our products and customers, and if there are issues or concerns, please begin by opening a support case with VMware Global Support Services.

My scanning tool discovered permission problems when scanning ESXi. How do I fix those?

ESXi is not Linux or UNIX and does not follow the permission models of those operating systems. Because SSH and the ESXi Shell are intended for maintenance only, and ESXi is not a traditional multiuser OS, all users logging into ESXi via those mechanisms intentionally have administrator/root-level permissions.

ESXi 7 and newer reads its operating system image into a RAMdisk at system boot. Changes made directly to configuration files will not persist between reboots.

My scanning tool discovered a vulnerability in an appliance component, and I replaced the package with one from another Linux distribution. Now things don’t work right. How do I fix this?

Changing components manually is not supported and can lead to serious availability and functional problems. Please open a support case with VMware Global Support Services for assistance.

If I shouldn’t use SSH how will I configure my ESXi host?

There are a variety of supported methods for configuring ESXi and vCenter Server, through the GUI interfaces and through API &

CLI interfaces. Host Profiles, Configuration Manager, PowerCLI, and the esxcli are common mechanisms for doing so. The code.vmware.com site has many examples and options in numerous scripting and programming languages. By interacting with ESXi via vCenter Server you also take advantage of the fully featured role-based access control (RBAC) in vCenter Server.

Can I disable SSH if it is enabled?

Yes, and we recommend doing so because it improves security and reduces audit scope. Please consult the vSphere documentation and Security Configuration Guide for your version.

Are there any problems with network-based scanning?

vSphere is a very robust and mature infrastructure product and can withstand routine network scanning. It is recommended that you test your scanner on a test environment first (nested ESXi is a great way to test), then on a subset of production hosts (maintenance mode), before scanning everything. This builds confidence and lets you assess the results more quickly.

My scanning tool discovered issues with TLS. How do I fix this?

TLS 1.2 is the default in VMware vSphere 6.7 and newer, and we recommend upgrading to take advantage of that and many other default security & functional improvements, both in vSphere and in vSAN.

Is there a way to limit users logging in to ESXi?

Yes, consult the product documentation around the DCUI.Access advanced option and Lockdown Mode. We recommend limiting ESXi shell access only to staff that are directly involved with support of the underlying hardware, but also taking care to mind dependencies so that systems can be brought online by the support team if an incident is occurring. In most cases it is recommended that staff interact with ESXi through vCenter Server where the robust role-based access control (RBAC) model can be applied.

Are there default accounts created on vCenter Server or ESXi?

Yes, the administrator@vsphere.local (or the domain you specify) account is created as part of the installation of vCenter Server, with a password that is specified at the time of installation.

Similarly, ESXi creates the 'root' account with a password specified at installation.

ESXi has additional accounts called ‘vpxuser’ and ‘dcui’ account for privilege separation for the console application. Appliances such as the vCenter Server Appliance will also have additional accounts for privilege separation and least privilege.

If you do inspect /etc/passwd and /etc/shadow you will note that any Linux system default accounts and any additional accounts that support vCenter Server are set to prevent logins, with the passwords locked and shells set to /sbin/nologin or /bin/false.

My compliance folks are insisting that they be granted SSH access to vSphere. What do I tell them?

SSH is a troubleshooting and support interface, not enabled as part of the default installation of the product, and not intended to be enabled unless troubleshooting is occurring. Because of the intentional permission model of the ESXi Shell, there is no way to limit what a scanner can access when logged in directly, which is a violation of the least-privilege principle.

There are no user-serviceable components accessible via SSH. You cannot replace individual components and remain supported, and so vCenter Server and ESXi must be evaluated as a whole unit.

In general, environments should be scanned as they are. Enabling SSH decreases security, and vendor best practices and product documentation unequivocally state that SSH be disabled to reduce attack surface and management complexity.

Granting access to a scanner tends to find issues that aren’t issues, wasting staff time and increasing billable hours by auditors, with zero net gain in security. It is paradoxical for a security auditor and/or information security professional to insist on drastically reducing security, especially since their audit will then list the results as findings that need to be fixed. The findings are only the result of their requests and would not be present otherwise.

This is no different than scanning a storage array’s controller, where the storage array vendor does not permit access even though it may be running SSH for support.

If we still want to scan vCenter Server and/or ESXi via SSH, what's the best way?

We always recommend customers have a test environment. It is easy to deploy a secondary, non-production copy of vCenter Server, as well as to install ESXi inside a virtual machine (nested ESXi). If you must scan in this fashion this is how we would do it, to reduce the likelihood of operational & support incidents in your production environments. Use the same software build versions as what you have deployed, in representative configurations. If you shut the nested test environment down you can safely snapshot it, providing flexibility for reverting changes during testing.

Please note that while nested vSphere is possible, and is how the Hands-on Labs works, it is not supported by VMware Global Support Services. There are many community resources for creating these types of environments.