Introducing Security and Compliance for VMware Cloud Foundation 4.3

10 JAN 2022

VMware Cloud Foundation 4.3

VMware Cloud Foundation 4.3.1

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2021-2022 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

About Introducing Security and Compliance for VMware Cloud Foundation 4.3

The *Introducing Security and Compliance for VMware Cloud Foundation* document provides general guidance for organizations that are considering VMware solutions to help them address on-premise compliance requirements. This document is a building block of the *Compliance Kit for VMware Cloud Foundation*.

Legal Disclaimer This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address on-premise compliance requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide regulatory advice and is provided "AS IS". VMware makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements.

Intended Audience

Introducing Security and Compliance for VMware Cloud Foundation is intended for cloud architects, infrastructure administrators, and cloud administrators. Familiarity with VMware software is required. This guide introduces security and compliance as it relates to the VMware Cloud Foundation.

Required VMware Software

The *Introducing Security and Compliance for VMware Cloud Foundation* document builds on top of VMware Cloud Foundation and is specific to the standard architecture model of VMware Cloud Foundation.

The products included in this compliance kit cover selected products from the VMware Cloud Foundation 4.2 bill-of-materials:

- VMware ESXi™
- VMware vCenter Server®
- VMware vSAN™
- VMware NSX-T™ Data Center
- VMware Cloud Foundation™ SDDC Manager™

See *VMware Cloud Foundation Release Notes* for more information about supported product versions.

Security by Design

1

Security and compliance guidance includes both default configurations in the VMware Cloud Foundation and non-default configurations that can be implemented post-deployment.

The *Compliance Kit for VMware Cloud Foundation* views configurations from two personas. System administrators and implementation teams for VMware Cloud Foundation use the *Security and Compliance Configuration for VMware Cloud Foundation* to assess and implement non-default configurations. Default configurations that address compliance are not subject of the configuration guide because they do not require additional configuration. In some cases, default configurations must be evaluated to ensure the default parameter aligns with the policy and procedures of your organization. Guidance for auditors who evaluate a VMware Cloud Foundation environment can use the *VMware Cloud Foundation Audit Guide* and the associated *VMware Cloud Foundation Audit Guide Appendix* to evaluate both default and non-default configurations.

Default configurations

Security configurations based on compliance requirements that are configured by default in VMware Cloud Foundation. According to the different regulatory requirements, the parameter values might require changes, but by secure design these configurations are included in the current implementation.

Non-default configurations

Additional input by the organization is required to identify, select, and set configurations based on a target regulation.

Security Architecture

2

Security in VMware Cloud Foundation is evaluated with a clear objective to balance best practices with usability and performance.

For VMware Cloud Foundation implementations, post-deployment, security must be handed over to a dedicated team to augment and monitor the security posture. Attack vectors and compliance guidelines are constantly evolving so the information provided is often used to establish a baseline, not an absolute, or complete picture.

NIST 800-53 Revision 4,risk rating Moderate, forms the security baseline used to evaluate VMware Cloud Foundation. NIST 800-53 is the baseline because of its vast array of controls and because it is often used by other regulations as part of their reference framework.

NIST is a risk-based framework, which requires each organization to assess their own risk posture and identify applicable controls. The *Compliance Kit for VMware Cloud Foundation* does not remove this step. The VMware Cloud Foundation security design and compliance mappings inform the reader of both design decisions and security configurations.

The VMware Cloud Foundation security design is not enough on its own. Each organization must have a series of supporting security architecture, technology, processes, and people to evaluate. Applications, workload domains, software-defined networking topology, customer data, privacy, and myriad other factors must be evaluated as part of the overall security architecture.

Super users of the system inherit various technologies and typically work with security specialists to implement controls effectively. VMware Cloud Foundation has evaluated many design decisions that are incorporated with the overall design as outlined by VMware Validated Design architecture guides.

Subsequent deployments benefit from post-implementation security health checks to enhance the organizations security posture as it relates to the VMware Validated Design used in conjunction with VMware Cloud Foundation.

Security Principles

3

Across all regulations or standards, security principles dictate the mindset for applying security controls in VMware Cloud Foundation.

The security concepts are treated as guiding principles to develop a secure VMware Cloud Foundation environment that leverages capabilities available across all products. These principles do not only result in the configurations identified in this guidance but are also inherent in product capabilities. Organizations that leverage these guidelines can expand these capabilities across the Software-Defined Data Center to include people, process, and technology controls. Each organization must tailor these principles and prioritize how they approach them.

Separation of duties

- Assign roles to users to separate conflicts of duty
- Roles can be customized and further tailored as needed.
- Restrict the use of super users
- Create service accounts where possible
- Create separate accounts for system-to-system communication
- Separate production from development environments
- Evaluate access to create, edit, or delete permissions
- Assign only read-only access where possible

Least privilege

- Disable unused services
- Do not grant or retain permissions longer than needed

Confidentiality - Integrity - Availability (CIA)

- Protect the data and the assets used to access it
- Confidentiality applies to the authorization to access the data
- Integrity applies to the authorization to modify the data
- Availability applies to the accessibility to access the data

Defense in depth

- Do not allow lateral movement
- Isolate environments
- Patch systems
- Implement layered security

Zero trust

- Implicit access denial regardless of origin
- Treat internal network as a potential threat vector
- Access is restricted via a trust broker
- Applications are hidden from discovery

Secure Software Development Life-Cycle (SDLC)

- VMware performs static code analysis
- VMware performs penetration testing
- VMware performs vulnerability scan
- Align development with VMware internal vSECR software development security guidelines/procedures

Data in transit protection

- Encryption of virtual machines during migration between hosts
- Use of encrypted mechanism when a super user is interacting with server consoles

Data at rest protection

- Encryption of virtual machines while powered off (at rest)

Trusted Computing Base (TCB)

- Architecture view that brings together the collection of all the hardware, software, and firmware components (including the security kernel and reference monitor)
- Brings a unified security policy and baseline consistent across various layers, abstractions, and detailed components to meet security requirements.

Governance, Risk, and Compliance and Mapping

4

This guidance describes the security configurations that can support Governance, Risk, and Compliance (GRC) considerations. Due to the variety of compliance standards and different organizational business needs, due care should be taken to identify and map VMware Cloud Foundation configurations against a targeted regulation.

Where possible, examples of audit artifacts are included as evidence in the *VMware Cloud Foundation Audit Guide Appendix*, focused on compliance and producing evidence to meet controls. To map configurations across regulatory standards, we use a third-party tool produced by the Unified Compliance Framework (UCF). This removes a subjective, manual control cross-walk approach and replaces it with a repeatable and data driven methodology. The crosswalk or reference across regulatory standards is not a mapping matrix, but instead utilizes the UCF as a shared library of controls tied to the underlying citation text within each standard. This removes the subjective mapping and replaces it with a programmatic, software-driven mapping engine.

In some cases, the regulation may be too generic or too vague, which can reduce the mapping efficacy. In these cases, an additional review is performed to isolate new citation text and then included in the engine through the corresponding and newly identified UCF control. No mapping is provided with an accompany UCF control and accompanying citation text for each regulation. If no mapping is identified, the mapping uses `VMware Best Practice` text to clarify that mapping was not found but to keep up with the security principles, the configuration is recommended.

The compliance mapping is a subject of expansion, as more security controls are evaluated, including additional compliance domains and regulations.

The top ten compliance and regulatory standards mapping are included:

- NIST 800-53 R4 (Moderate)
- PCI DSS 3.2.1
- DISA STIG
- FedRAMP
- HIPAA
- FBI CJIS
- NERC CIP
- NIST 800-171 / CMMC

- ISO27001:2013 / GDPR
- SOC 2 (across all five Trust Service Principles)

For guidance on each standard, refer to the *VMware Cloud Foundation Audit Guide Appendix*.

Control Definition

Controls are designed to mitigate risk. These are derived by using a Risk Framework, such as the *Guide for Applying the Risk Management Framework to Federal Information Systems* published by NIST, publication number 800-37. NIST 800-53 R4 control catalog is used to develop a baseline of controls compared to the software-defined data center technical and security configurations. These security configurations must be evaluated and considered against the risk management framework used by your organization. Other frameworks such as ISO27001 can be coupled with its Annex A, ISO27002, or ISO27005 to evaluate controls to mitigate risk.

Cybersecurity Considerations

It is the responsibility of each security, compliance, and audit teams in your organization to verify that configurations meet their compliance requirements. The attack vectors and compliance guidelines are constantly evolving, which requires constant monitoring and risk management processes.

Business Impact Assessment

Measuring risk and evaluating scope may require performing a business impact assessment. This analysis can inform IT security and audit professionals the areas of the Software-Defined Data Center that require more controls, tightened access restrictions, micro-segmentation, enhanced disaster recovery, and additional monitoring.

Compliance Kit for VMware Cloud Foundation

5

The compliance kits is a solution that builds on top of VMware Cloud Foundation and leverages security fundamentals. The kit address the top ten most frequently requested compliance standards, regulations, and frameworks.

The compliance kit is designed and validated to tailor security configurations without impacting the ability of VMware Cloud Foundation to meet its design objectives. The kit can assist organizations to secure information systems in a compliance context.

This guidance has been validated and tested against certain product versions. Changes between subsequent releases of VMware Cloud Foundation are designed for stability and optimal upgrade experience. Guidance provided by the *Compliance Kit for VMware Cloud Foundation* is for a specific VMware Cloud Foundation release, but can still be used until a subsequent kit release is available. This guidance is not backward-compatible and must not be trimmed down into component products. In many cases, the Software-Defined Data Center stack provided by VMware Cloud Foundation requires to avoid some security configurations that could be implemented within individual component product implementations.

Compliance Kit for VMware Cloud Foundation Structure

The compliance kit consists of documents specific to the standard architecture model of VMware Cloud Foundation.

Document Name	Document Description	Intended Audience
Security and Compliance Configuration for VMware Cloud Foundation	Non-default configurations can be performed post deployment of VMware Cloud Foundation for Standard Architecture.	■ System Integrator ■ Cloud Administrator ■ Infrastructure Administrator

VMware Cloud Foundation Audit Guide	Procedures to validate both default and non-default configurations with a preface composed by an independent, third-party auditor introducing the audit content and its applicability to control testing of a Software-Defined Data Center.	■ Security Professional ■ Auditor
VMware Cloud Foundation Audit Guide Appendix	Includes actual configuration values for the different compliance standards. Use in conjunction with the configuration guide to adjust values configured in the procedures to a desired compliance standard. Includes audit procedures for auditors examining an environment for compliance readiness.	■ System Integrator ■ Cloud Administrator ■ Infrastructure Administrator ■ Security Professional ■ Auditor

The compliance kit is designed to work holistically. Each document supports the overall blueprint and builds trust across multiple persona that may interact with the life cycle of a system operating within a compliance context: architect, system administrator, system integrator, security professional, and auditor.

Introducing Security and Compliance for VMware Cloud Foundation outlines security and compliance concepts used in the development of the VMware Cloud Foundation, Compliance Kit. For example, considerations such as governance, risk, and compliance, separation of duties, and security architecture to name a few.

The *Security and Compliance Configuration Guide for VMware Cloud Foundation* outlines the steps to implement non-default configurations. Default configurations are confirmed and excluded from the configuration guide as part of the VMware Cloud Foundation post deployment steps. You must perform the procedures from the guide to ensure that the SDDC performance is not compromised.

The Audit Guide supports the post-implementation process and audit process. It includes procedures to validate both default and non-default configurations. The preface to the Audit Guide is composed by an independent third-party auditor evaluating VMware Cloud Foundation, compliance kit and attests to its ability to address compliance requirements. It includes concepts required to audit a virtualized environment and tips on how to audit a Software-Defined Data Center. In the*VMware Cloud Foundation Audit Guide Appendix*, mappings between configurations and compliance controls provide a comprehensive inventory of configurations designated as default or non-default.

VMware Cloud Foundation Compliance Kit

Compliance kits apply to core products in VMware Cloud Foundation:

- VMware ESXi™
- VMware vCenter Server®
- VMware vSAN™
- VMware NSX-T™ Data Center
- VMware Cloud Foundation™ SDDC Manager

Default Access Controls Configured in VMware Cloud Foundation

6

Each product can support a range of settings that must be evaluated and if necessary, modified to meet security and compliance requirements.

Frequently requested access control settings are listed with the default values in VMware Cloud Foundation 4.2. Configurations with a value of 0 are disabled.

For the recommended parameters, review the desired regulatory standard or framework in the *VMware Cloud Foundation Audit Guide Appendix*. This appendix lists the top 4 standards: NIST 800-53 R4 (Moderate), PCI DSS 3.2.1, NIST 800-171 / CMMC, ISO27001:2013 / GDPR.

The default settings are not the recommended values. This is the default out-of-the-box state of access controls in VMware Cloud Foundation.

Table 6-1. Default Access Control Parameters in VMware Cloud Foundation

Product	Configuration ID	Configuration Description	Default Setting
NSX-T Data Center	VI-NET-CFG-1416	Configure NSX-T Manager to terminate idle sessions after a certain period of time.	1800 seconds
NSX-T Data Center	VI-NET-CFG-1417	Configure NSX-T Manager to block any login attempts after consecutive invalid login attempts for a certain period.	900 seconds
NSX-T Data Center	VI-NET-CFG-1418	Configure NSX-T Manager to block further login attempts after a number of consecutive failed login attempts.	5 attempts
NSX-T Data Center	VI-NET-CFG-1419	Configure NSX-T Manager locked accounts to automatically get unlocked after a period of time following the last failed login attempt.	900 seconds
NSX-T Data Center	VI-NET-CFG-1421	Configure a minimum password length for NSX-T Manager accounts.	12 characters

Table 6-1. Default Access Control Parameters in VMware Cloud Foundation (continued)

Product	Configuration ID	Configuration Description	Default Setting
ESXi	VI-ESXI-CFG-00034	Set the maximum number of failed login attempts before an account is locked.	5 attempts
ESXi	VI-ESXI-CFG-00038	Configure the inactivity timeout to automatically terminate idle shell sessions.	0 seconds (automatic termination is disabled)
ESXi	VI-ESXI-CFG-00109	Configure the password history to restrict the reuse of a certain number of previous passwords.	0 passwords (password history is disabled)
ESXi	VI-ESXI-CFG-00165	Configure a time for automatic unlock of a locked user account.	900 seconds
ESXi	VI-ESXI-CFG-00564	Configure the inactivity timeout to automatically terminate idle Host Client sessions.	900 seconds
ESXi	VI-ESXI-CFG-00168	Configure the inactivity timeout to automatically terminate idle DCUI sessions.	600 seconds
vCenter Server	VI-VC-CFG-00403	Configure the password history to restrict the reuse of a certain number of previous passwords.	5 passwords
vCenter Server	VI-VC-CFG-00421	Configure vCenter Server to enforce a maximum password lifetime restriction.	90 days
vCenter Server	VI-VC-CFG-00422	Configure the inactivity timeout to automatically terminate vSphere Client sessions.	120 minutes
vCenter Server	VI-VC-CFG-00428	Configure vCenter Server to rotate the vpxuser auto-password periodically.	30 days
vCenter Server	VI-VC-CFG-00427	Configure a minimum password length for the vpxuser account.	32 characters
vCenter Server	VI-VC-CFG-00410	Configure the minimum number of characters for password length for any vCenter Server user.	8 characters

Table 6-1. Default Access Control Parameters in VMware Cloud Foundation (continued)

Product	Configuration ID	Configuration Description	Default Setting
vCenter Server	VI-VC-CFG-00408	Configure the minimum number of uppercase characters in the password for any vCenter Server user.	1 character
vCenter Server	VI-VC-CFG-00413	Configure the minimum number of lowercase characters in the password for any vCenter Server user.	1 character
vCenter Server	VI-VC-CFG-00433	Configure the minimum number of numeric characters in the password for any vCenter Server user.	1 character
vCenter Server	VI-VC-CFG-00432	Configure the minimum number of special characters in the password for any vCenter Server user.	1 character
vCenter Server	VI-VC-CFG-00436	Limit the maximum number of failed login attempts for vCenter Server users.	5 attempts
vCenter Server	VI-VC-CFG-00434	Configure the number of failed login attempts in a period of time before an account gets locked.	180 seconds
vCenter Server	VI-VC-CFG-00435	Configure a timer for automatic account unlock for accounts locked after failed login attempts.	300 seconds
vCenter Server	VI-VC-CFG-00096	Disable console connection sharing on the virtual machine.	1 (disabled)