

# NIST SPECIAL PUBLICATION 1800-19

---

## Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments

---

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)

Michael Bartock  
Donna Dodson\*  
Murugiah Souppaya  
Daniel Carroll  
Robert Masten  
Gina Scinta  
Paul Massis  
Hemma Prafullchandra\*  
Jason Malnar  
Harmeet Singh  
Rajeev Ghandi

Laura E. Storey  
Raghuram Yeluri  
Tim Shea  
Michael Dalton  
Rocky Weber  
Karen Scarfone  
Anthony Dukes  
Jeff Haskins  
Carlos Phoenix  
Brenda Swarts

*\*Former employee; all work for this publication was done while at employer*

April 2022

FINAL

This publication is available free of charge from <https://doi.org/10.6028/NIST.SP.1800-19>

The draft publication is available free of charge from  
<https://www.nccoe.nist.gov/publications/practice-guide/trusted-cloud-vmware-hybrid-cloud-iaas-environments-nist-sp-1800-19-draft>



# Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments

*Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B); and How-To Guides (C)*

Michael Bartock  
Donna Dodson\*  
Murugiah Souppaya  
*NIST*

Daniel Carroll  
Robert Masten  
*Dell/EMC*

Gina Scinta  
Paul Massis  
*Gemalto*

Hemma Prafullchandra\*  
Jason Malnar  
*HyTrust*

Harmeet Singh  
Rajeev Ghandi  
Laura E. Storey  
*IBM*

Raghuram Yeluri  
*Intel*

Tim Shea  
Michael Dalton  
Rocky Weber  
*RSA*

Karen Scarfone  
*Scarfone Cybersecurity*

Anthony Dukes  
Jeff Haskins  
Carlos Phoenix  
Brenda Swarts  
*VMware*

*\*Former employee; all work for this publication was done while at employer*

FINAL

April 2022



U.S. Department of Commerce  
*Gina M. Raimondo, Secretary*

National Institute of Standards and Technology  
*Laurie E. Locascio, NIST Director and Undersecretary of Commerce for Standards and Technology*

# Trusted Cloud:

## Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments

---

### Volume A: Executive Summary

**Donna Dodson\***  
NIST

**Daniel Carroll**  
Dell/EMC

**Gina Scinta**  
Gemalto

**Hemma  
Prafullchandra\***  
HyTrust

**Harmeet Singh**  
IBM

**Raghuram Yeluri**  
Intel

**Tim Shea**  
RSA

**Carlos Phoenix**  
VMware

*\*Former employee; all work for this publication done while at employer.*

April 2022

FINAL

This publication is available free of charge from <https://doi.org/10.6028/NIST.SP.1800-19>

The draft publication is available free of charge from  
<https://www.nccoe.nist.gov/projects/trusted-cloud-vmware-hybrid-cloud-iaas-environments>

# Executive Summary

Organizations can take advantage of cloud services to increase their security, privacy, efficiency, responsiveness, innovation, and competitiveness. The core concerns about cloud technology adoption are protecting information and virtual assets in the cloud and having sufficient visibility to conduct oversight and ensure compliance with applicable laws and business practices. This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates how organizations can address these concerns by implementing what are known as trusted compute pools. Through these pools, organizations can safeguard the security and privacy of their applications and data being run within a cloud or being transferred between a private cloud and a hybrid or public cloud.

## CHALLENGE

In cloud environments, workloads are constantly being spun up, scaled out, moved around, and shut down. Organizations often find adopting cloud technologies is not a good business proposition because they encounter one or more of the following issues:

1. Cannot maintain consistent security and privacy protections for information—applications, data, and related metadata—across platforms, even for a single class of information.
2. Do not have the flexibility to be able to dictate how different information is protected, such as providing stronger protection for more sensitive information in a multi-tenancy environment.
3. Cannot retain visibility into how their information is protected to ensure consistent compliance with legal and business requirements.

Many organizations, especially those in regulated sectors like finance and healthcare, face additional challenges because security and privacy laws vary around the world. Laws for protecting information the organization collects, processes, transmits, or stores may vary depending on whose information it is, what kind of information it is, and where it is located. Cloud technologies may silently move an organization's data from one jurisdiction to another. Because laws in some jurisdictions may conflict with an organization's own policies or the laws in another jurisdiction, an organization may decide it needs to restrict which on-premises private or hybrid/public cloud servers it uses based on their geolocations to avoid compliance issues.








### This practice guide can help your organization:

- understand how trusted cloud technologies can reduce your risk and satisfy your existing system security and privacy requirements
- gain the ability to determine each cloud workload's security posture at any time through continuous monitoring, regardless of the cloud infrastructure or server
- modernize your legacy on-premises infrastructure by moving existing workloads to the cloud while maintaining the same security and compliance outcomes

## SOLUTION

Organizations need to be able to monitor, track, apply, and enforce their security and privacy policies on their cloud workloads based on business requirements in a consistent, repeatable, and automated way. Building on previous NIST work documented in [NIST Internal Report \(IR\) 7904, Trusted Geolocation in the Cloud: Proof of Concept Implementation](#), the National Cybersecurity Center of Excellence (NCCoE) has developed a trusted cloud solution that demonstrates how trusted compute pools leveraging hardware roots of trust can provide the necessary security capabilities. These capabilities not only provide assurance that cloud workloads are running on trusted hardware and in a trusted geolocation or logical boundary, but also improve the protections for the data in the workloads and data flows between workloads.

The example solution uses technologies and security capabilities (shown below) from our project collaborators. The technologies used in the solution support security and privacy standards and guidelines including the NIST Cybersecurity Framework, among others.

Collaborator	Security Capability or Component
	Server, storage, and networking hardware
	Hardware security module (HSM) for storing keys
	Asset tag and policy enforcement, workload and storage encryption, and data scanning
	Public cloud environment with IBM-provisioned servers
	Intel processors in the Dell EMC servers
	Multifactor authentication, network traffic monitoring, and dashboard and reporting
	Compute, storage, and network virtualization capabilities

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

## HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

**Business decision makers, including chief information security and technology officers** can use this part of the guide, *NIST SP 1800-19A: Executive Summary*, to understand the drivers for the guide, the

cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

**Technology, security, and privacy program managers** who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-19B: Approach, Architecture, and Security Characteristics*, which describes what we built and why, including the risk analysis performed and the security/privacy control mappings.

**IT professionals** who want to implement an approach like this can make use of *NIST SP 1800-19C: How-To Guides*, which provides specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

## SHARE YOUR FEEDBACK

You can view or download the guide at <https://www.nccoe.nist.gov/projects/trusted-cloud-vmware-hybrid-cloud-iaas-environments>. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at [trusted-cloud-nccoe@nist.gov](mailto:trusted-cloud-nccoe@nist.gov).

---

## COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

# Trusted Cloud:

## Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments

---

### Volume B:

#### Approach, Architecture, and Security Characteristics

**Michael Bartock**

**Murugiah Souppaya**

Computer Security Division  
Information Technology  
Laboratory

**Hemma Prafullchandra\***

**Jason Malnar**

HyTrust  
Mountain View, California

**Tim Shea**

**Michael Dalton**

RSA  
Bedford, Massachusetts

**Daniel Carroll**

**Robert Masten**

Dell/EMC  
Hopkinton, Massachusetts

**Harmeet Singh**

IBM  
Armonk, New York

**Karen Scarfone**

Scarfone Cybersecurity  
Clifton, Virginia

**Gina Scinta**

**Paul Massis**

Gemalto  
Austin, Texas

**Raghuram Yeluri**

Intel  
Santa Clara, California

**Anthony Dukes**

**Carlos Phoenix**

**Brenda Swarts**

VMware  
Palo Alto, California

*\*Former employee; all work for this publication done while at employer.*

April 2022

FINAL

This publication is available free of charge from <https://doi.org/10.6028/NIST.SP.1800-19>

The draft publication is available free of charge from <https://www.nccoe.nist.gov/projects/trusted-cloud-vmware-hybrid-cloud-iaas-environments>

## DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk through outreach and application of standards and best practices, it is the stakeholder's responsibility to fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise, and the impact should the threat be realized before adopting cybersecurity measures such as this recommendation.

National Institute of Standards and Technology Special Publication 1800-19B, Natl. Inst. Stand. Technol. Spec. Publ. 1800-19B, 55 pages, (April 2022), CODEN: NSPUE2

## FEEDBACK

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at [trusted-cloud-nccoe@nist.gov](mailto:trusted-cloud-nccoe@nist.gov).

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence  
National Institute of Standards and Technology  
100 Bureau Drive  
Mailstop 2002  
Gaithersburg, MD 20899  
Email: [nccoe@nist.gov](mailto:nccoe@nist.gov)



## NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit <https://www.nccoe.nist.gov/>. To learn more about NIST, visit <https://www.nist.gov>.

## NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

## ABSTRACT

A *cloud workload* is an abstraction of the actual instance of a functional application that is virtualized or containerized to include compute, storage, and network resources. Organizations need to be able to monitor, track, apply, and enforce their security and privacy policies on their cloud workloads, based on business requirements, in a consistent, repeatable, and automated way. The goal of this project is to develop a trusted cloud solution that will demonstrate how trusted compute pools leveraging hardware roots of trust can provide the necessary security capabilities. These capabilities not only provide assurance that cloud workloads are running on trusted hardware and in a trusted geolocation or logical boundary, but also improve the protections for the data in the workloads and in the data flows between workloads. The example solution leverages modern commercial off-the-shelf technology and cloud services to address lifting and shifting a typical multi-tier application between an organization-controlled private cloud and a hybrid/public cloud over the internet.

## KEYWORDS

*cloud technology; compliance; cybersecurity; privacy; trusted compute pools*

## ACKNOWLEDGMENTS

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
<a href="#">Dell EMC</a>	Server, storage, and networking hardware
<a href="#">Gemalto (A Thales Company)</a>	Hardware security module (HSM) for storing keys
<a href="#">HyTrust (An Entrust Company)</a>	Asset tagging and policy enforcement, workload and storage encryption, and data scanning
<a href="#">IBM</a>	Public cloud environment with IBM-provisioned servers
<a href="#">Intel</a>	Intel processors in the Dell EMC servers
<a href="#">RSA</a>	Multifactor authentication, network traffic monitoring, and dashboard and reporting
<a href="#">VMware</a>	Compute, storage, and network virtualization capabilities

## DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

## PATENT DISCLOSURE NOTICE

*NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to*

*respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.*

*As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.*

*No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.*

## Contents

<b>1</b>	<b>Summary .....</b>	<b>1</b>
1.1	Challenge .....	1
1.2	Solution.....	2
1.3	Benefits.....	2
<b>2</b>	<b>How to Use This Guide .....</b>	<b>3</b>
2.1	Typographical Conventions.....	4
<b>3</b>	<b>Approach .....</b>	<b>5</b>
3.1	Audience .....	5
3.2	Scope .....	6
3.3	Assumptions .....	6
3.4	Risk Assessment.....	6
3.4.1	Threats .....	7
3.4.2	Vulnerabilities .....	10
3.4.3	Risk .....	10
<b>4</b>	<b>Architecture.....</b>	<b>10</b>
4.1	Architecture Components.....	11
4.2	Technologies.....	12
4.2.1	Dell EMC.....	12
4.2.2	Gemalto .....	13
4.2.3	HyTrust.....	13
4.2.4	IBM.....	15
4.2.5	Intel .....	15
4.2.6	RSA .....	16
4.2.7	VMware.....	17
4.2.8	Products and Technologies Summary.....	19
4.3	NCCoE Cloud Solution Architecture .....	24
4.3.1	VMware Cluster Architectures.....	25

4.3.2	RSA Cluster Architecture.....	29
4.3.3	HSM Architecture.....	29
4.3.4	HyTrust Architecture.....	30
4.3.5	Dell Leaf and Spine Switch Architecture .....	32
4.4	IBM Cloud Solution Architecture .....	33
<b>5</b>	<b>Security Characteristics Analysis .....</b>	<b>34</b>
5.1	Assumptions and Limitations .....	34
5.2	Demonstration of the Capabilities .....	35
5.2.1	Use Case Scenario 1: Demonstrate Control and Visibility for the Trusted Hybrid Cloud Environment .....	35
5.2.2	Use Case Scenario 2: Demonstrate Control of Workloads and Data Security .....	37
5.2.3	Use Case Scenario 3: Demonstrate a Workload Security Policy in a Hybrid Cloud ....	41
5.2.4	Use Case Scenario 4: Demonstrate Recovery From an Unexpected Infrastructure Outage.....	42
5.2.5	Use Case Scenario 5: Demonstrate Providing Visibility into Network Traffic Patterns.....	43
5.2.6	Use Case Scenario 6: Demonstrate Application Zero Trust .....	43
<b>Appendix A</b>	<b>Mappings .....</b>	<b>45</b>
<b>Appendix B</b>	<b>List of Acronyms.....</b>	<b>49</b>
<b>Appendix C</b>	<b>Glossary .....</b>	<b>53</b>
<b>Appendix D</b>	<b>References .....</b>	<b>54</b>

## List of Figures

Figure 4-1	High-Level Solution Architecture.....	11
Figure 4-2	High-Level NCCoE Cloud Architecture .....	25
Figure 4-3	VMware Management Cluster Architecture.....	27
Figure 4-4	VMware Compute Cluster Architecture .....	28
Figure 4-5	RSA Cluster .....	29
Figure 4-6	HSM Architecture in the NCCoE Cloud .....	30

Figure 4-7 HyTrust Architecture in the NCCoE Cloud .....	31
Figure 4-8 HTKC Node Deployments .....	32
Figure 4-9 NCCoE Layer 3 Leaf – Spine Logical Network Diagram .....	33
Figure 4-10 IBM Cloud Architecture.....	34
Figure 5-1 Example of Secure Configuration Scan Results .....	36
Figure 5-2 Examples of Trusted Compute Nodes .....	37
Figure 5-3 Example of Decrypted Workload .....	38
Figure 5-4 Example of Workload on Untagged Server .....	39
Figure 5-5 Example of Workload that Cannot Be Decrypted .....	39
Figure 5-6 Example of Workload Migrated to Trusted and Tagged Server .....	40
Figure 5-7 Example of Workload Running on Trusted and Tagged Server.....	41

## List of Tables

Table 3-1 Common Threats Associated with Hybrid Cloud Usage .....	7
Table 4-1 Products and Technologies Summary.....	20
Table A-1 List of NIST SP 800-53 Revision 5 Controls Addressed by Solution .....	45
Table A-2 List of NIST Cybersecurity Framework Subcategories Addressed by Solution .....	47

# 1 Summary

Building on previous work documented in National Institute of Standards and Technology (NIST) Internal Report (NISTIR) 7904, *Trusted Geolocation in the Cloud: Proof of Concept Implementation* [\[1\]](#), the goal of the project is to expand upon the security capabilities provided by trusted compute pools in a hybrid cloud model, including the following capabilities:

- single pane of glass for the management and monitoring of cloud workloads, including software configurations and vulnerabilities
- data protection and encryption key management enforcement focused on trust-based and geolocation-based/resource pools, and secure migration of cloud workloads
- key management and keystore controlled by the organization, not the cloud service provider
- persistent data flow segmentation before and after the trust-based and geolocation-based/resource pools secure migration
- industry sector and/or organizational business compliance enforcement for regulated workloads between the on-premises private and hybrid/public clouds

These additional capabilities not only provide assurance that cloud workloads are running on trusted hardware and in a trusted geolocation or logical boundary, but also improve the protections for the data in the workloads and in the data flows between workloads.

## 1.1 Challenge

Cloud services can provide organizations, including federal agencies, with the opportunity to increase the flexibility, availability, resiliency, and scalability of cloud services, which the organizations can, in turn, use to increase security, privacy, efficiency, responsiveness, innovation, and competitiveness. However, many organizations, especially those in regulated sectors like finance and healthcare, face additional security and privacy challenges when adopting cloud services.

Cloud platform hardware and software are evolving to take advantage of the latest hardware and software features, and there are hundreds or thousands of virtualized or containerized workloads that are spun up, scaled out, moved around, and shut down at any instant, based on business requirements. In such environments, organizations want to be able to monitor, track, apply, and enforce policies on the workloads, based on business requirements, in a consistent, repeatable, and automated way. In other words, organizations want to maintain consistent security protections and to have visibility and control for their workloads across on-premises private clouds and third-party hybrid/public clouds in order to meet their security and compliance requirements.

This is further complicated by organizations' need to comply with security and privacy laws applicable to the information that they collect, transmit, or hold, which may change depending on whose information it is (e.g., European citizens under the General Data Protection Regulation), what kind of information it is

(e.g., health information compared to financial information), and in what state or country the information is located. Additionally, an organization must be able to meet its own policies by implementing appropriate controls dictated by its risk-based decisions about the necessary security and privacy of its information.

Because laws in one location may conflict with an organization's policies or mandates, an organization may decide that it needs to restrict the type of cloud servers it uses, based on the state or country. Thus, the core impediments to broader adoption of cloud technologies are the abilities of an organization to protect its information and virtual assets in the cloud, and to have sufficient visibility into that information so that it can conduct oversight and ensure that it and its cloud provider are complying with applicable laws and business practices.

In addition, there are technical challenges and architectural decisions that have to be made when connecting two disparate clouds. An important consideration revolves around the type of wide area network connecting the on-premises private cloud and the hybrid/public cloud, because it may impact the latency of the workloads and the security posture of the management plane across the two infrastructures.

## 1.2 Solution

The project involves collaborating with industry partners to design, engineer, and build solutions leveraging commercial off-the-shelf technology and cloud services to deliver a trusted cloud implementation. This implementation will allow organizations in regulated industries to leverage the flexibility, availability, resiliency, and scalability of cloud services while complying with applicable requirements, such as the Federal Information Security Modernization Act (FISMA), the Payment Card Industry Data Security Standard (PCI DSS), and the Health Insurance Portability and Accountability Act (HIPAA), as well as industry-neutral voluntary frameworks like the NIST Cybersecurity Framework. The technology stack includes modern hardware and software that can be leveraged to support the described use cases and ease the adoption of cloud technology.

The example implementation is for a hybrid cloud use case, enabling an organization to lift and shift a typical multi-tier application between a private cloud stack located in the National Cybersecurity Center of Excellence (NCCoE) data center and the IBM public cloud over the public internet.

## 1.3 Benefits

- Organizations will be able to maintain consistent security and privacy protections for information across cloud platforms; dictate how different information is protected, such as having stronger protection for more-sensitive information; and retain visibility into how their information is protected, to ensure consistent compliance with legal and business requirements.



- Technical staff will learn how to utilize commercial off-the-shelf technology and cloud services to achieve trusted cloud implementations that protect cloud workloads and support compliance initiatives.
- Senior management and information security officers will be motivated to use trusted cloud technologies.

## 2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate the trusted compute pools in a hybrid cloud model that provide expanded security capabilities. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST Special Publication (SP) 1800-19A: *Executive Summary*
- NIST SP 1800-19B: *Approach, Architecture, and Security Characteristics* – what we built and why **(you are here)**
- NIST SP 1800-19C: *How-To Guides* – instructions for building the example solution

Depending on your role in your organization, you might use this guide in different ways:

**Business decision makers, including chief security and technology officers**, will be interested in the *Executive Summary, NIST SP 1800-19A*, which describes the following topics:

- challenges enterprises face in protecting cloud workloads in hybrid cloud models
- example solution built at the NCCoE
- benefits of adopting the example solution

**Technology or security program managers** who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this part of the guide, *NIST SP 1800-19B*, which describes what we did and why. The following sections will be of particular interest:

- [Section 3.4.3](#), Risk, provides a description of the risk analysis we performed
- [Appendix A](#), Mappings, maps the security characteristics of this example solution to cybersecurity standards and best practices

You might share the *Executive Summary, NIST SP 1800-19A*, with your leadership team members to help them understand the importance of adopting standards-based trusted compute pools in a hybrid cloud model that provide expanded security capabilities.

**Information technology (IT) professionals** who want to implement an approach like this will find the whole practice guide useful. You can use the how-to portion of the guide, *NIST SP 1800-19C*, to replicate

all or parts of the build created in our lab. The how-to portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products together in our environment to create an example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a trusted cloud implementation leveraging commercial off-the-shelf technology. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. [Section 4.2](#), Technologies, lists the products we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to [trusted-cloud-nccoe@nist.gov](mailto:trusted-cloud-nccoe@nist.gov).

## 2.1 Typographical Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the <i>NCCoE Style Guide</i> .
<b>Bold</b>	names of menus, options, command buttons, and fields	Choose <b>File &gt; Edit</b> .
Monospace	command-line input, on-screen computer output, sample code examples, and status codes	<code>mkdir</code>
<b>Monospace Bold</b>	command-line user input contrasted with computer output	<b><code>service sshd start</code></b>
<a href="#">blue text</a>	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at <a href="https://www.nccoe.nist.gov">https://www.nccoe.nist.gov</a> .

## 3 Approach

The NCCoE invited technology providers to participate in demonstrating a proposed approach for implementing trusted resource pools leveraging commercial off-the-shelf technology and cloud services to aggregate trusted systems and segregate them from untrusted resources. This would result in the separation of higher-value, more-sensitive workloads from commodity application and data workloads in an infrastructure as a service (IaaS) deployment model. In this project, the example implementation involves securely migrating—“lifting and shifting”—a multi-tier application from an organization-controlled private cloud to a hybrid/public cloud over the internet. The implementation automatically, and with assurance, restricts cloud workloads to servers meeting selected characteristics. It also provides the ability to determine the security posture of a cloud workload at any time through continuous monitoring, no matter the cloud or the cloud server.

The NCCoE prepared a Federal Register notice [\[2\]](#) seeking technology providers to provide products and/or expertise to compose prototypes that include commodity servers with hardware cryptographic modules; commodity network switches; hypervisors; operating systems (OSs); application containers; attestation servers; orchestration and management servers; database servers; directory servers; software-defined networks; data encryption and key management servers; and cloud services. Cooperative Research and Development Agreements (CRADAs) were established with qualified respondents, and “build teams” were assembled.

The following actions were performed by the build teams:

- fleshing out the initial architecture and composing the collaborators’ components into demonstration prototypes
- documenting the architecture and design implementation, including the steps taken to install and configure each component of the demonstration environment
- conducting security and functional testing of the demonstration environment, and then conducting and documenting the results of a risk assessment and a security characteristics analysis
- working with industry collaborators to suggest future considerations

### 3.1 Audience

This guide is intended for cloud computing practitioners, system integrators, IT managers, security managers, IT architects, and others interested in practical, effective implementations of trusted cloud technologies that can reduce risk and satisfy existing system security requirements.

## 3.2 Scope

The scope of this project is the usage of hybrid/public clouds and on-premises private clouds to securely host an organization's own workloads in an IaaS deployment model. The project is intended to be particularly useful to organizations in regulated industries, but it should be of use to organizations in any industry and sector.

## 3.3 Assumptions

This project is guided by the following assumptions:

- Organizations implementing this solution are responsible for providing core infrastructure services, including Microsoft Active Directory, certificate services, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Network Time Protocol (NTP), Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), and logging services.
- Organizations should already have their physical infrastructure configured to be fault tolerant.
- Organizations should work with their cloud service provider, legal team, and others as needed to have the necessary agreements in place regarding responsibilities.
- Federal agencies will need to choose hybrid/public clouds that are Federal Risk and Authorization Management Program (FedRAMP) certified. Other industry sectors should follow their sector-specific cloud service certification program.
- Organizations will need to implement and manage all security controls that their cloud service provider is not formally responsible for implementing and maintaining on their behalf.
- Organizations will need to ensure that the VMware Validated Design meets their requirements for availability, manageability, performance, recoverability, and security.
- Organizations will need to ensure that they have identified all applicable compliance requirements.
- Organizations should have trained and qualified staff to architect, secure, and operate the solution stack.

## 3.4 Risk Assessment

[NIST SP 800-30 Revision 1, \*Guide for Conducting Risk Assessments\*](#), states that risk is “a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.” The guide further defines risk assessment as “the process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.” [\[3\]](#)

The NCCoE recommends that any discussion of risk management, particularly at the enterprise level, begin with a comprehensive review of NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations [4] for the United States (U.S.) government public sector; private-sector risk management frameworks (RMFs), such as International Organization for Standardization (ISO) 31000 [5], Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management – Integrating with Strategy and Performance (2017) [6], and Factor Analysis of Information Risk (FAIR) [7]; or sector-agnostic frameworks, such as the NIST Cybersecurity Framework [8]—material that is available to the public. The [Risk Management Framework \(RMF\)](#) guidance, as a whole, proved to be invaluable in giving us a baseline to assess risks, from which we developed the project, the security characteristics of the build, and this guide.

### 3.4.1 Threats

[Table 3-1](#) lists examples of common threats associated with the hybrid cloud usage scenario of this project, where two clouds under the control of different providers are linked together so that workloads can be moved between them. This list of threats is not meant to be comprehensive.

**Table 3-1 Common Threats Associated with Hybrid Cloud Usage**

Threat/Attack Type	Example	Addressed by Solution
<b>Threats Against Cloud Infrastructure</b>		
Physical threat against data center (e.g., natural disaster, cooling system failure)	A regional power outage necessitates shutting down servers at one data center location.	Have adequate environmental controls in place for the data center, such as backup power, heating and cooling mechanisms, and fire detection and suppression systems. Be prepared to automatically shift workloads to another suitable location at any time. The enterprise data center infrastructure team or cloud service operators are responsible for providing these mechanisms.
Tampering with server firmware (e.g., Basic Input/Output System [BIOS])	An unapproved change management control or a malicious insider gains physical access to a server in the data center and alters its BIOS configuration to disable its security protections.	Use physical security controls to restrict data center access to authorized personnel only. Monitor data center access at all times. Detect changes by taking an integrity measurement of the BIOS at boot and comparing it with a previous measurement taken in a “clean room” environment and configured as a good known BIOS.

Threat/Attack Type	Example	Addressed by Solution
<b>Threats Against Cloud Management</b>		
Tampering with a virtual machine manager (VMM)	An unapproved change management control, a malicious insider, or an external attacker with stolen administrator credentials reuses them to gain access to the VMM and install malicious code.	Detect changes to the VMM by taking an integrity measurement of the kernel and specific vSphere Installation Bundles (VIBs) at boot and comparing it with previous measurements taken in a “clean room” environment and configured as a good known host (GKH).
Unauthorized administrator-level or service-level access	An external attacker steals an administrator account password and reuses it to gain access to a file.	Enforce strong authentication, including two-factor authentication with a cryptographic token, for all administrative and service access to cloud workloads, VMMs, and other management systems. Allow only administrators to manage the systems they have a need to administer by enforcing least privilege and separation of duties. Monitor the use of administrator and service credentials at all times, log all access attempts, and alert when suspicious activity is observed.
Administrative changes (accidental or malicious) that are destructive	An administrator accidentally deletes a virtualized domain controller.	Enforce secondary approval workflow for specific assets and/or administrative operations to implement the “four-eyes” principle for highly sensitive systems and/or operations.
Intentional or accidental configuration changes that violate hardening best practices	Upgrading an authorized application inadvertently wipes out existing application configuration settings.	Continuously monitor all configuration changes on all components. Run regularly scheduled assessments and remediations with customized hardening templates to remain in compliance with configuration hardening best practices.
Unauthorized access to secret cryptographic keys	An attacker takes advantage of a weak key management protocol implementation to intercept unprotected keys being distributed to virtual machines (VMs).	Provide Federal Information Processing Standard (FIPS) 140-validated, Key Management Interoperability Protocol (KMIP)-compliant key management services for cryptographic functions that operate in a hardware security module (HSM) to safeguard sensitive key materials.

Threat/Attack Type	Example	Addressed by Solution
<b>Threats Against Cloud Workload Storage, Execution, and Use</b>		
Running a cloud workload within an untrusted environment or location	A cloud administrator may respond to an impending maintenance disruption by moving workloads to cloud servers in other locations.	Allow cloud workloads to execute only on a physical server that is known to be good (i.e., not tampered with) and is within an authorized geolocation.
Unauthorized access from one workload to another within a cloud	A user of one workload connects to another organization's workload and exploits vulnerabilities in it to gain unauthorized access.	Establish network boundaries through dedicated virtual local area networks (VLANs) leveraging automated access control lists (ACLs). Use Institute of Electrical and Electronics Engineers (IEEE) 802.1Q VLAN tagging for network traffic within the cloud data center so that only traffic tagged with a server's unique VLAN identifier is routed to or from that server.
Unauthorized movement within the cloud environment from a compromised cloud workload (e.g., lateral movement)	A cloud workload is compromised, and the attacker has full privileged access to the system. The attacker tries to move laterally to discover sensitive resources and escalate privileges to gain greater access to the environment.	Use software-defined technology and user privilege segmentation to allowlist the network communications and access rights.
Intentional or accidental exposure of sensitive data	An administrator copies a cloud workload file to an unauthorized location.	Encrypt cloud workloads at rest. Use end-to-end encryption with mutual authentication when moving a workload from one location to another.
Unauthorized access to files containing sensitive data	A malicious insider misuses OS access to copy a file.	Scan filesystems for sensitive data, categorize the discovered files, monitor all access to those files, and report on that access. Enforce access controls that prevent different cloud provider administrators of workloads from accessing sensitive applications and data drives.

### 3.4.2 Vulnerabilities

The primary areas of concern are software flaws and misconfigurations at all levels of the architecture: low-level services (compute, storage, network), VMMs, OSs, and applications, including cloud workload management, VMM management, and other management tools. Related to these concerns is the need to ensure that the same security policies are being enforced within both clouds for the workloads to eliminate some vulnerabilities and mitigate others.

Some examples of vulnerabilities that might be particularly impactful if exploited are listed below:

- cryptographic keys being stored or transmitted without being strongly encrypted
- cloud workloads being migrated without performing mutual authentication of the clouds or verifying the integrity of the migrated workload
- weak administrator or service account credentials that are highly susceptible to theft and unauthorized reuse
- access controls that do not enforce the principles of least privilege and separation of duties

### 3.4.3 Risk

The proposed solution implements several layers of controls to protect workloads while they reside within clouds and while they are migrated from one cloud to another. The cloud workloads are still vulnerable. For example, an unknown software flaw in a cloud workload's software, or in the VMM underlying that workload, could be exploited, potentially compromising the workload itself. There are always residual risks for cloud workloads. The proposed solution includes only technical controls; therefore, risk involving the solution's physical environment, people (e.g., users, administrators), processes, and other non-technical items will also need to be addressed.

## 4 Architecture

At a high level, the trusted cloud architecture has three main pieces: a private cloud hosted at the NCCoE, an instance of the public IBM Cloud Secure Virtualization (ICSV), and an Internet Protocol Security (IPsec) virtual private network (VPN) that connects the two clouds to form a hybrid cloud. [Figure 4-1](#) provides a simplified diagram of the architecture.

The private on-premises cloud at the NCCoE consists of the following components:

- HSM for storing keys by Gemalto
- server, storage, and networking hardware by Dell EMC
- Intel processors in the Dell EMC servers
- compute, storage, and network virtualization capabilities by VMware



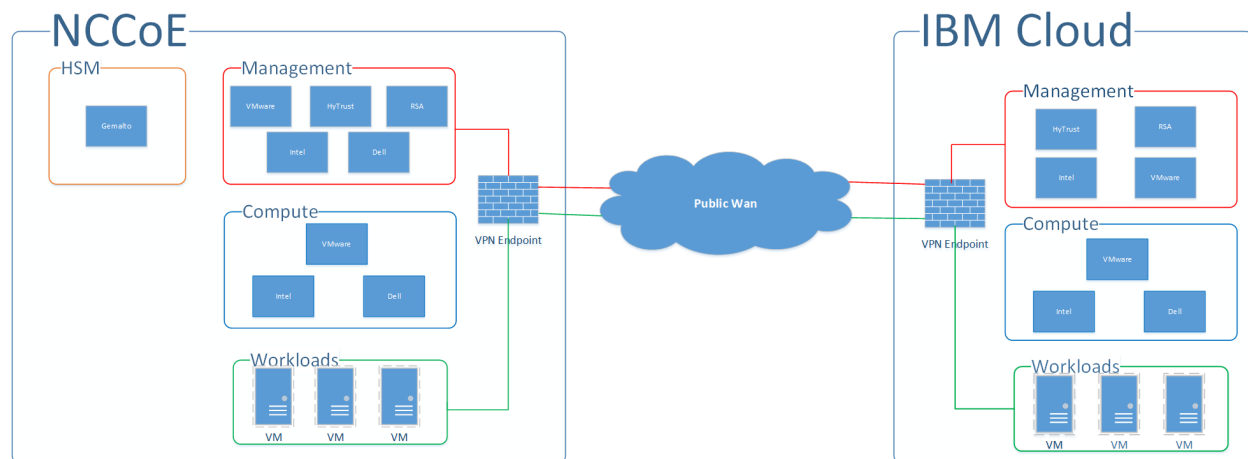
- asset tagging and policy enforcement, workload and storage encryption, and data scanning by HyTrust
- multifactor authentication, network traffic monitoring, and dashboard and reporting by RSA

The ICSV instance consists of the following components:

- IBM-provisioned servers with Intel processors
- compute, storage, network virtualization with VMware components
- asset tagging and policy enforcement, and workload and storage encryption with HyTrust components

The IPSec VPN established between the two clouds allows them to be part of the same management domain so that each component can be managed and utilized in the same fashion, which creates one hybrid cloud. The workloads can be shifted or live-migrated between the two sites.

Figure 4-1 High-Level Solution Architecture



## 4.1 Architecture Components

Within the high-level architecture, there are four main components that comprise the trusted cloud build:

- **HSM component:** This build utilizes HSMs to store sensitive keys within the environment. One set of HSMs is used for the domain's root and issuing Transport Layer Security (TLS) certificate authorities (CAs), while another HSM is used to protect keys that are used to encrypt workloads. The HSM component is deployed in the private cloud at the NCCoE, and network access is strictly limited to only the machines that need to communicate with it.
- **Management component:** The identical functional management components are instantiated across the NCCoE private cloud and the ICSV public cloud instance. The single management

console is used to operate the virtual infrastructure hosting the tenant workloads. At a minimum, each management component consists of hardware utilizing Intel processors, VMware running the virtualization stack, HyTrust providing the asset tagging policy enforcement aspect, and RSA providing network-visibility, dashboard, and reporting capabilities. The management components on each site are connected through the IPsec VPN to represent one logical management element.

- **Compute component:** Both sites of the hybrid cloud include similar compute components. The compute components host the tenant workload VMs. Asset tagging is provisioned on the compute servers so that policy can be assigned and enforced to ensure that tenant workloads reside on servers that meet specific regulatory compliance requirements. At a minimum, each compute component consists of hardware utilizing Intel processors and VMware running the virtualization stack. The compute components on each site are connected through the IPsec VPN so that workloads can be migrated between the two sites.
- **Workload component:** Both sites of the hybrid cloud have similar workload components. The workload components include VMs, data storage, and networks owned and operated by the tenant and data owner. Policies are applied to the workloads to ensure that they can run only on servers that meet specific requirements, such as asset tag policies.

## 4.2 Technologies

We built the proposed solution by using products from vendors who have established CRADAs with the NCCoE for this project. The NCCoE does not endorse or recommend these products. Each organization should determine if these products, or other products on the market with similar capabilities, best meet your own requirements and integrate well with your existing IT system infrastructure.

The following subsections describe the vendors and products that we used for our example solution.

### 4.2.1 Dell EMC

Dell EMC has developed a keen focus on building security into the product design versus bolting on security after release. For this solution, Dell EMC provided enterprise and in-rack networking solutions, Dell PowerEdge Servers to provide compute capabilities, and Dell EMC Unity unified storage for the primary storage solutions.

Dell Networking solutions utilizing the OS9 OS and the Dell PowerEdge servers have gone through rigorous testing and approval processes to be published on the Defense Information Systems Agency (DISA) Approved Products List. This includes the inclusion of the Integrated Dell Remote Access Controller, Lifecycle Controller, and connectivity to the OpenManage solution. This capability allows for enterprise standardization of platform and switch configurations to enable NIST SP 800-53 security controls [\[9\]](#).

Dell EMC Unity provides a robust unified storage solution with built-in security configuration that allows for a simple enablement of platform hardening to meet DISA Security Technical Implementation Guide (STIG) standards. The Dell EMC Unity solution OS is based on a derivative of SUSE Linux 12. Dell EMC, in collaboration with DISA, performed extensive testing and development to ensure that Dell EMC Unity meets the high standards that DISA has established for its Approved Product Listing.

Dell EMC provided implementation and consulting services to ensure that these components of the overall solution were implemented to meet the proof-of-concept guidelines for a highly secured infrastructure.

#### 4.2.2 Gemalto

Gemalto's Enterprise and Cybersecurity business unit focuses on providing solutions for the encryption of data at rest and data in motion, secure storage and management of encryption keys through the use of HSMs and centralized key management, and controlling access by using multifactor authentication and identity access management across cloud, virtual, and on-premises environments.

SafeNet Hardware Security Modules provide the highest level of security by always storing cryptographic keys in hardware. SafeNet HSMs provide a secure cryptographic foundation, as the keys never leave the intrusion-resistant, tamper-evident, FIPS-validated appliance. Because all cryptographic operations occur within the HSM, strong access controls prevent unauthorized users from accessing sensitive cryptographic material.

The SafeNet Luna Universal Serial Bus (USB) HSM is a small form-factor USB-attached HSM that is used as a root of trust for storing root cryptographic keys in an offline key storage device.

The SafeNet Luna Network HSM (Versions 6 and 7) is a network-attached HSM protecting encryption keys used by applications in on-premises, virtual, and cloud environments. The HSM has more than 400 integrations. For this project, SafeNet Luna Network HSM 7 is the root of trust for Microsoft Active Directory Certificate Services (ADCS) used to issue TLS certificates. SafeNet Luna Network HSM 6 is integrated as the root of trust for HyTrust KeyControl (HTKC) via the KMIP key management service.

The SafeNet Backup HSM ensures that sensitive cryptographic material remains strongly protected in hardware, even when not being used. You can back up and duplicate keys securely to the SafeNet Backup HSM for safekeeping in case of emergency, failure, or disaster.

#### 4.2.3 HyTrust

HyTrust helps make cloud infrastructure more trustworthy for those organizations pursuing a multi-cloud approach by delivering a critical set of capabilities required to proactively secure workloads wherever they reside. The HyTrust Cloud Security Policy Framework (CloudSPF) allows organizations to automate the creation, application, and enforcement of security and compliance policies for private, hybrid, and public cloud workloads, including three critical attributes of the workload—people, data,

and infrastructure. HyTrust CloudSPF is supported by a portfolio of five solutions that deliver the functionality needed to enable policy-driven security and automated compliance of workloads in multi-cloud environments—including securing data and ensuring data privacy, preventing privileged admin misuse, automating compliance tasks, securing multi-tenant environments, and more. The five solutions are as follows:

- **HyTrust CloudControl (HTCC):** Workload Security Policy Enforcement and Compliance: Key capabilities help organizations protect their virtualized infrastructures with authentication, authorization, and auditing. Better visibility and control simplify compliance and accelerate further virtualization and data center transformation. CloudControl functionality includes two-factor authentication, secondary approval workflows, advanced role-based and object-based access controls, audit-quality logging, and hypervisor hardening.
- **HyTrust DataControl (HTDC):** Workload Encryption and Integrated Key Management: Provides strong data-at-rest encryption for workloads in any cloud, along with easy-to-deploy key management that organizations control—whether workloads are running in a private cloud powered by vSphere or in a hybrid/public cloud like IBM Cloud, Microsoft Azure, or Amazon Web Services (AWS)—throughout the entire workload life cycle. DataControl also supports the highest levels of availability by offering the ability to rekey workloads without taking applications offline.
- **HyTrust KeyControl (HTKC):** Workload Encryption Key Management: Simplifies the process of key management for workloads that do not require sophisticated policy-based key management, but that need to scale to enterprise-level performance. Organizations retain full ownership of encryption keys with policy-based controls to protect data and to meet compliance requirements. KeyControl works with both DataControl and third-party encryption solutions, such as VMware vSphere VM Encryption and vSAN.
- **HyTrust CloudAdvisor (HTCA):** Data Discovery and Classification Across Virtual Machines and Backups: Provides complete visibility into data stored within each workload and associates this information with whomever is interacting with it and when. CloudAdvisor defines policies to automatically discover the data that is valuable; detect anomalous user access behaviors; and defend an organization against careless exposure, data loss, malicious users, and regulatory noncompliance.
- **HyTrust BoundaryControl (HTBC):** Workload Placement Policies, Data Geo-Fencing, and Location-Aware Encryption: Enables administrators to set policies so that workloads can run only on proven, trusted hosts that are physically located within the defined parameters. BoundaryControl's foundation is rooted in Intel Trusted Execution Technology (Intel TXT), which provides processor-level attestation of the hardware, BIOS, and hypervisor. Administrators can also assign labels that bind workloads to run only in predefined locations. Also, encryption policies can be applied to ensure that data is never decrypted outside the defined parameters/boundary.

#### 4.2.4 IBM

ICSV combines the power of IBM Cloud bare-metal servers, VMware virtualization and management applications (IBM Cloud for VMware – vCenter Server [vCS]), HyTrust security virtual appliances (HTCC/HTDC), Intel TXT, and Intel Trusted Platform Module (TPM). This service provides enhanced security capabilities, utilizing automation from deployment to ongoing management.

ICSV allows clients to set, apply, and automate the enforcement of workload governance policies to meet their security needs for critical workloads and to support regulatory or industry compliance requirements through continuous monitoring and real-time reporting. ICSV gives clients visibility of physical servers across any virtualized infrastructure, so that they can ensure that only authorized servers in authorized locations handle sensitive workloads. In turn, clients can better enforce only authorized administrator actions and can help make sure that all requested actions—whether approved or denied—are logged for reporting and compliance. With this type of control and visibility, clients can more effectively reduce risk and increase security, allowing them to address in-house security needs as well as compliance requirements for mission-critical business operations. This means that they can now take full advantage of the benefits of cloud computing while maintaining the strongest levels of data protection, visibility, and auditing necessary to protect the business.

IBM Cloud bare-metal servers function as the hardware foundation of this solution. The IBM Cloud service allows customers to provision bare-metal servers according to their needs. In contrast to environments with typical cloud-based VMs, customers have control over these bare-metal servers. Customers can specify the servers' OS, security configuration, and other configuration aspects, including modifying server BIOS settings and deploying various hypervisors. The bare-metal servers are built with Intel Xeon processors, which come equipped with Intel TXT and TPM technologies that enable trusted compute pools (via HTCC) for workloads and data. The servers also take advantage of Intel technologies, such as Intel Advanced Encryption Standard – New Instructions (Intel AES-NI), and other cryptographic technologies to enhance and accelerate encryption (via HTDC).

The ICSV solution complements the IBM Cloud for VMware – vCS offering by providing security services. ICSV takes advantage of the infrastructure automation jointly developed by IBM and VMware. This advanced automation supports the deployment and integration of Intel and HyTrust technologies with the vCS from VMware, so that IBM clients can continue to use familiar tools to manage their workloads without having to retool or refactor applications. IBM Cloud for VMware – vCS provides the virtualization of compute, storage, and networking, providing a software-defined data center.

#### 4.2.5 Intel

The Intel Data Center Group (DCG) is at the heart of Intel's transformation from a personal computer (PC) company to a company that runs the cloud and billions of smart, connected computing devices. The data center is the underpinning for every data-driven service, from artificial intelligence to 5G to high-performance computing, and DCG delivers the products and technologies—spanning software,

processors, storage, input/output (I/O), security and networking solutions—that fuel cloud, communications, enterprise, and government data centers around the world.

Intel TXT provides hardware-based security technologies that address the increasing and evolving security threats across physical and virtual infrastructures by complementing runtime protections, such as anti-virus software. Intel TXT also can play a role in meeting government and industry regulations and data protection standards by providing a hardware-based method of verification that is useful in compliance efforts. Intel TXT is specifically designed to harden platforms from the emerging threats of hypervisor attacks, BIOS, or other firmware attacks; malicious rootkit installations; or other software-based attacks. Intel TXT increases protection by allowing greater control of the launch stack through a Measured Launch Environment (MLE) and enabling isolation in the boot process. More specifically, it extends the Virtual Machine Extensions (VMX) environment of Intel Virtualization Technology (Intel VT), permitting a verifiably secure installation, launch, and use of a hypervisor or OS.

Intel Cloud Integrity Technology (Intel CIT) extends a hardware-based root of trust up through the cloud solution stack to ensure the privacy and integrity of cloud platforms and workloads. Intel CIT secures cloud-based workloads through workload placement, encryption, and launch control bound to the hardware-rooted chain of trust. By using Intel TXT to measure server firmware and software components during system launch, server configurations can be verified against tampering. Extending this chain of trust, additional software components, hypervisors, VMs, and containers can be similarly attested and verified. By encrypting workload images and tying the decryption key to server hardware using a TPM, final control over where a VM may or may not launch is given to the customer, preventing unauthorized access and enabling data sovereignty. Intel CIT is the foundational technology leveraged by HyTrust to provide boundary and data-control capabilities.

#### 4.2.6 RSA

RSA, a Dell Technologies business, offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage digital risk and protect what matters most. RSA's award-winning cybersecurity solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies to thrive in an uncertain, high-risk world.

The RSA NetWitness Platform is an evolved Security Information and Event Management (SIEM) and threat-defense solution engineered to immediately identify high-risk threats on devices, in the cloud, and across your virtual enterprise. It automates security processes to reduce attacker dwell time and make analysts more efficient and effective.

The RSA SecurID Suite is an advanced multifactor authentication and identity governance solution. It applies risk analytics and business context to provide users with convenient, secure access to any application from any device, and to simplify day-to-day identity governance for administrators.

The RSA Archer Suite is a comprehensive, integrated risk-management solution designed to empower organizations of all sizes to manage multiple dimensions of risk on a single, configurable, and integrated platform. It features a wide variety of use cases for IT risk management, operational risk management, and much more.

#### 4.2.7 VMware

VMware, Inc., a subsidiary of Dell Technologies, provides virtualization and cloud-infrastructure solutions enabling businesses to transform the way they build, deliver, and consume IT resources. VMware is an industry-leading virtualization software company empowering organizations to innovate by streamlining IT operations and modernizing the data center into an on-demand service by pooling IT assets and automating services. VMware products allow customers to manage IT resources across private, hybrid, and public clouds. VMware offers services to its customers, including modernizing data centers, integrating public clouds, empowering digital workspaces, and transforming security.

VMware Validated Design (VVD) 4.2 is a family of solutions for data center designs that span compute, storage, networking, and management, serving as a blueprint for your software-defined data center (SDDC) implementations. VVDs are designed by experts and are continuously improved based on feedback from real deployments. The design is continuously validated for scale and interoperability, ensuring that it remains valid. The VVD is a comprehensive design that includes a fully functional SDDC while remaining hardware agnostic. Each VVD comes with its own reference design, deployment, operations, and upgrade guides: *Architecture and Design: VMware Validated Design for Management and Workload Consolidation 4.2* [\[10\]](#), *Deployment for Region A: VMware Validated Design for Software-Defined Data Center 4.2* [\[11\]](#), *Operational Verification: VMware Validated Design for Software-Defined Data Center 4.2* [\[12\]](#), and *Planning and Preparation: VMware Validated Design for Software-Defined Data Center 4.2* [\[13\]](#).

The standard VVD for an SDDC is a design for a production-ready SDDC that can be single-region or dual-region. Each region is deployed on two workload domains, management and shared edge and compute. VMs are separated into a minimum of two vSphere clusters, one for management VMs and one for customer VMs. Each of these clusters has a minimum of four ESXi hosts and is managed by a dedicated vCS. Additional compute hosts or clusters can be added to scale the solution as needed.

The standard VVD for an SDDC consists of the following VMware products:

- VMware vSphere virtualizes and aggregates the underlying physical hardware resources across multiple systems and provides pools of virtual resources to the data center. VMware vSphere includes the following components:
  - VMware ESXi is a type-1 hypervisor that enables a virtualization layer run on physical servers that abstracts processor, memory, storage, and resources into multiple VMs.



- The Platform Services Controller (PSC) Appliance provides common infrastructure services to the vSphere environment. Services include licensing, certificate management, and authentication with vCenter Single Sign-On.
- VMware vCS Appliance is a management application that allows for the management of VMs and ESXi hosts centrally. The vSphere Web Client is used to access the vCS.
- vSAN is fully integrated hypervisor-converged storage software. vSAN creates a cluster of server hard-disk drives and solid-state drives, and presents a flash-optimized, highly-resilient, shared storage data store to ESXi hosts and VMs. vSAN allows you to control capacity, performance, and availability, on a per-VM basis, through the use of storage policies.
- NSX for vSphere (NSX-V) creates a network virtualization layer. All virtual networks are created on top of this layer, which is an abstraction between the physical and virtual networks. Network virtualization services include logical switches, logical routers, logical firewalls, and other components. This design includes the following components:
  - NSX Manager provides the centralized management plane for NSX-V and has a one-to-one mapping to vCS workloads.
  - The NSX Virtual Switch is based on the vSphere Distributed Switch (VDS), with additional components to enable rich services. The add-on NSX components include kernel modules (VIBs) that run within the hypervisor kernel and that provide services, such as distributed logical routers (DLRs), distributed firewalls (DFWs), and Virtual Extensible Local Area Network (VXLAN) capabilities.
  - NSX logical switches create logically abstracted segments to which tenant VMs can be connected. NSX logical switches provide the ability to spin up isolated logical networks with the same flexibility and agility that exist with VMs. Endpoints, both virtual and physical, can connect to logical segments and establish connectivity independently from their physical location in the data center network.
  - The universal distributed logical router (UDLR) in NSX-V is optimized for forwarding in the virtualized space (between VMs, on VXLAN-backed or VLAN-backed port groups).
  - VXLAN Tunnel Endpoints (VTEPs) are instantiated within the VDS to which the ESXi hosts that are prepared for NSX-V are connected. VTEPs are responsible for encapsulating VXLAN traffic as frames in User Datagram Protocol (UDP) packets and for the corresponding decapsulation. VTEPs exchange packets with other VTEPs.
  - The primary function of the NSX Edge Services Gateway (ESG) is north-south communication, but it also offers support for Layer 2; Layer 3; perimeter firewall; load balancing; and other services, such as Secure Sockets Layer (SSL) VPN and DHCP relay.
- vRealize Operations Manager (vROPS) tracks and analyzes the operation of multiple data sources in the SDDC by using specialized analytic algorithms. These algorithms help vROPS learn



and predict the behavior of every object that it monitors. Users access this information by using views, reports, and dashboards.

- vRealize Log Insight (vRLI) provides real-time log management and log analysis with machine-learning-based intelligent grouping, high-performance searching, and troubleshooting across physical, virtual, and cloud environments.
- vRealize Automation (vRA) provides the self-service provisioning, IT services delivery, and life-cycle management of cloud services across a wide range of multivendor, virtual, physical, and cloud platforms, through a flexible and robust distributed architecture.
- vRealize Orchestrator (vRO) provides the automation of complex tasks by allowing for a quick and easy design and deployment of scalable workflows. It automates management and operational tasks across both VMware and third-party applications, such as service desks, change management, and IT asset management systems.
- vRealize Business for Cloud (vRB) automates cloud costing, consumption analysis, and comparison, delivering the insight that you need for efficiently deploying and managing cloud environments. vRB tracks and manages the costs of private and public cloud resources from a single dashboard.
- VMware Site Recovery Manager (optional, depends on failover site) is disaster-recovery software that enables application availability and mobility across sites with policy-based management, non-disruptive testing, and automated orchestration. Site Recovery Manager administrators perform frequent non-disruptive testing to ensure IT disaster-recovery predictability and compliance. Site Recovery Manager enables fast and reliable recovery by using fully automated workflows.
- vSphere Replication (vR) (optional, depends on failover site) is a hypervisor-based, asynchronous replication solution for vSphere VMs. It is fully integrated with the VMware vCS and the vSphere Web Client. vR delivers flexible, reliable, and cost-efficient replication to enable data protection and disaster recovery for VMs.

#### 4.2.8 Products and Technologies Summary

[Table 4-1](#) lists all of the products and technologies that we incorporated in the proposed solution, and maps each of them to the Cybersecurity Framework subcategories and the NIST SP 800-53 Revision 4 controls that the proposed solution helps address. Note that this is **not** a listing of every subcategory or control that each product supports, uses for its own internal purposes, etc., but is a listing of those that are being offered by the solution. For example, a component might be designed based on the principle of least privilege for its internal functioning, but this component is not used to enforce the principle of least privilege on access to cloud workloads for the solution.

From the time the initial implementation of the proposed solution began to the time the build was completed, numerous components of the proposed solution were upgraded, some more than once. For brevity, [Table 4-1](#) only lists the current version of each component as of when the build was completed.

Note: the first entry in the table on the public cloud hosting component does not contain information on the Cybersecurity Framework subcategories and the NIST SP 800-53 Revision 4 controls that the public cloud hosting helps address. That information is contained in the IBM Federal Cloud FedRAMP report, but because that report contains sensitive information, it is not directly available. Organizations wanting access to that report would need to have the necessary agreements in place with IBM first.

**Table 4-1 Products and Technologies Summary**

Component	Product	Version	Function	Cybersecurity Framework Subcategories	SP 800-53r4 Controls
Public Cloud Hosting	IBM Cloud and ICSV	Not applicable (N/A)	Provides IaaS capabilities for public cloud hosting at the FedRAMP moderate level.	Refer to the IBM Federal Cloud FedRAMP report.	Refer to the IBM Federal Cloud FedRAMP report.
Logging	vRLI	4.5.1	Provides real-time log management and log analysis with machine-learning-based intelligent grouping, high-performance searching, and troubleshooting across physical, virtual, and cloud environments.	PR.PT-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, DE.CM-1, DE.CM-7	AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-10, AU-11, AU-12
Operations Management	vROPS	6.6.1	Tracks and analyzes the operation of multiple data sources in the SDDC by using specialized analytic algorithms. These algorithms help vROPS learn and predict the behavior of every object that it monitors. Users access this information by views, reports, and dashboards.	PR.PT-1	AU-2, AU-6, AU-7, AU-8, AU-9

Component	Product	Version	Function	Cybersecurity Framework Subcategories	SP 800-53r4 Controls
Cloud Management	vRB	7.3.1	Automates tracking and managing cloud costing, and resource consumption analysis and comparison.	N/A	N/A
Cloud Management	vRA	7.3	Provides a secure web portal where authorized administrators, developers, and business users can request new IT services and manage specific cloud and IT resources, while ensuring compliance with business policies.	PR.AC-3, PR.MA-1	AC-17, AC-20, MA-2, MA-3, MA-4, MA-5, MA-6, SC-15
Cloud Management	vRO	7.3	Provides the capability to develop complex automation tasks, as well as access and launch workflows from the VMware vSphere client, various components of vRealize Suite, or other triggering mechanisms.	PR.MA-1	MA-2, MA-3, MA-4, MA-5, MA-6
Virtual Infrastructure Management	vSphere vCS	6.5u1	Provides a centralized and extensible platform for managing the virtual infrastructure (VMware vSphere environments).	PR.MA-1	MA-2, MA-3, MA-4, MA-5, MA-6
Virtual Infrastructure Management	vSphere Update Manager (VUM)	6.5u1	Provides centralized, automated patch and version management for VMware ESXi hosts, appliances, and VMs.	PR.IP-3, PR.IP-12	CM-3, CM-4, RA-3, RA-5, SI-2

Component	Product	Version	Function	Cybersecurity Framework Subcategories	SP 800-53r4 Controls
Virtual Infrastructure Networking	NSX-V	6.4	Creates a network virtualization layer. All virtual networks are created on top of this layer, which is an abstraction between the physical and virtual networks.	PR.AC-5, PR.PT-4	AC-4, SC-7
Virtual Infrastructure Storage	vSAN	6.6.1	Delivers flash-optimized, secure shared storage for virtualized workloads.	PR.DS-1, PR.DS-2	SC-8, SC-28
Virtual Infrastructure Security	PSC	6.5u1	Controls infrastructure security functions, such as vCenter Single Sign-On, licensing, certificate management, and server reservation.	ID.AM-2, PR.AC-7, PR.DS-3, PR.MA-1	CM-8, IA-2, IA-3, IA-4, IA-5, MA-2, MA-3
Virtual Infrastructure Hypervisor	vSphere ESXi	6.5u1	Enterprise-class, type-1 hypervisor for deploying and servicing VMs.	PR.MA-1	MA-2, MA-3, MA-4
Virtual Infrastructure Data Synchronization	Site Recovery Manager (SRM)	6.5.1	Disaster recovery solution for vSphere VMs that automates the disaster recovery process and helps manage the synchronization of data between protected and recovery sites.	PR.IP-4, PR.IP-9	CP-9, CP-10
Virtual Infrastructure VM Replication	vR	6.5.1	Hypervisor-based, asynchronous replication solution for vSphere VMs.	N/A	N/A

Component	Product	Version	Function	Cybersecurity Framework Subcategories	SP 800-53r4 Controls
Governance, Risk, and Compliance (GRC)	RSA Archer Suite	6.X	Governance and risk management workflow and dashboard.	PR.PT-1, DE.CM-1	AU-6, AU-7, CA-7, CM-3, SI-4
Logging	RSA NetWitness Suite	11.x	Compliance reporting.	PR.PT-1	AU-6, AU-7
Authentication	RSA SecurID Suite	N/A	Strong authentication for administrative access.	PR.AC-1, PR.AC-6, PR.AC-7	IA-2, IA-4, IA-5, IA-7
Networking Switch	Dell Networking S4048-ON Switch	OS9+	Leaf and spine switches for network architecture.	N/A	N/A
Networking Switch	Dell Networking S3048-ON Switch	OS9+	In-band management network.	N/A	N/A
Storage Device	Dell EMC Unity	4.3.1	Unified storage solution.	N/A	N/A
Backup Solution	Data Domain Virtual Edition (DD VE)	4.0	Solution backup capabilities.	N/A	N/A
Compute	Dell PowerEdge Server	R730	Compute nodes for the solution.	N/A	N/A
Compute	Dell PowerEdge Server	R730	Compute nodes for the solution.	N/A	N/A
Physical Layer	Top-of-rack (TOR) Switches	N/A	Dell TOR switch.	N/A	N/A

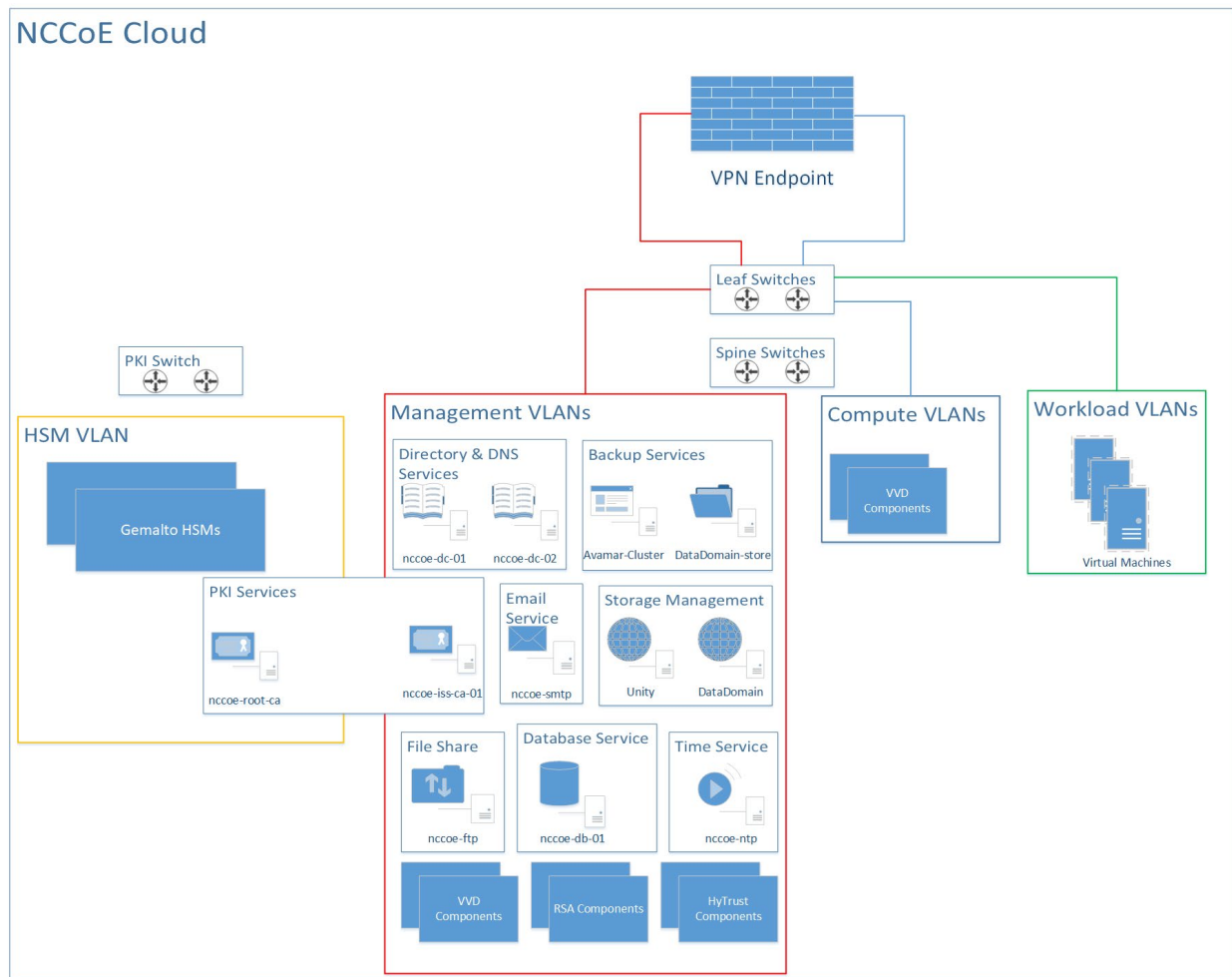
Component	Product	Version	Function	Cybersecurity Framework Subcategories	SP 800-53r4 Controls
Physical Layer	Conventional Storage	N/A	Unity Storage.	N/A	N/A
Business Continuity Layer	Backup	N/A	Avamar.	PR.IP-4	CP-9, CP-10
HSM – Network Attached	Gemalto SafeNet Luna Network HSM 6	FW 6.10.9 SW 6.2.2	Network-attached HSM root of trust for HTKC.	PR.AC-1, PR.DS-1, PR.DS-6	IA-5, IA-7, SA-18, SC-12, SC-13
HSM – Network Attached	Gemalto SafeNet Luna Network HSM 7	FW 7.0.1 SW 7.2.0-220	Network-attached HSM root of trust for Microsoft ADCS.	PR.AC-1, PR.DS-1, PR.DS-6	IA-5, IA-7, SA-18, SC-12, SC-13
HSM – USB Attached	Gemalto SafeNet Luna USB HSM	FW 6.10.9	USB HSM integrated with offline Microsoft Root CA.	PR.AC-1, PR.DS-1, PR.DS-6	IA-5, IA-7, SA-18, SC-12, SC-13

### 4.3 NCCoE Cloud Solution Architecture

[Figure 4-2](#) expands the high-level solution architecture first illustrated in [Figure 4-1](#). The following subsections provide additional details on the following parts of this architecture:

- VMware cluster architectures ([Section 4.3.1](#))
- RSA cluster architecture ([Section 4.3.2](#))
- HSM architecture ([Section 4.3.3](#))
- HyTrust architecture ([Section 4.3.4](#))
- Dell leaf and spine switch architecture ([Section 4.3.5](#))

**Figure 4-2 High-Level NCCoE Cloud Architecture**



### 4.3.1 VMware Cluster Architectures

The diagrams of the VMware management cluster architecture ([Figure 4-3](#)) and compute cluster architecture ([Figure 4-4](#)) are based on several assumptions about the data centers in which the VVD would be implemented, including the following:

- use of the leaf-spine architecture
- use of Border Gateway Protocol (BGP) routing
- availability of dedicated VLANs
- ability to configure jumbo frames
- Network File System (NFS) storage availability

- use of vSAN Ready Nodes (optional)
- availability of existing data-center services, such as Active Directory, DNS, SMTP, and NTP

The components described below are included in the VVD for an SDDC.

vSphere provides a powerful, flexible, and secure foundation for the SDDC. The vSphere solution includes the vCS and the PSC to provide a centralized platform for managing the virtual infrastructure. Within the VVD, PSC high availability is achieved by utilizing load balancers across multiple appliances. Additionally, dedicated vCSs are deployed to manage clusters designated for infrastructure management workloads and for compute or customer workloads. Optionally, VMware vSAN is defined within the VVD to pool together storage devices across the vSphere cluster to create a distributed shared datastore.

The VVD includes VMware NSX to virtualize the network; this solution abstracts the network from the underlying physical infrastructure. The VVD NSX solution ensures a highly available solution by utilizing both equal-cost multi-path (ECMP)-enabled and high-availability-enabled appliances. ESGs configured to utilize the BGP routing protocol are configured as ECMP pairs and act as the north-south boundary. Routing within the logical space, east-west, is provided by high-availability-enabled distributed logical routers. In this solution, VXLAN overlays the existing Layer 3 network infrastructure, addressing scalability problems associated with cloud computing environments.

vRLI provides deep operational visibility and faster troubleshooting across physical, virtual, and cloud environments. In this solution, vRLI is designed to provide a highly available solution for each site where logs can be forwarded to a remote site for retention.

vROPS provides administrators with the ability to efficiently manage capacity and performance while also gaining visibility across the virtual infrastructure. vROPS in the VVD is designed to provide high availability while also ensuring that remote data centers are monitored. Within this design, in case of a disaster, it is possible to failover the necessary vROPS components while leaving remote collectors at their designated data centers.

vRA provides a portal where authorized individuals can request new IT services and manage cloud and IT workloads. Requests for IT services, including infrastructure, applications, desktops, and many others, are processed through a common service catalog to provide a consistent user experience despite the underlying heterogeneous infrastructure. In this design, the “Large” reference architecture for vRA is followed, allowing for high availability and scalability up to 50,000 managed machines. The vRA solution includes embedded VMware Identity Manager and embedded vRO.

vRB automates cloud cost management, consumption metering, and cloud comparison, delivering cost visibility. vRB is integrated with vRA, providing cost information for the solution and pricing information per blueprint. vRB is architected to include a remote collector at each site while the vRB appliance remains in proximity to the vRA solution. vRB is protected by vSphere High Availability.



Figure 4-3 VMware Management Cluster Architecture

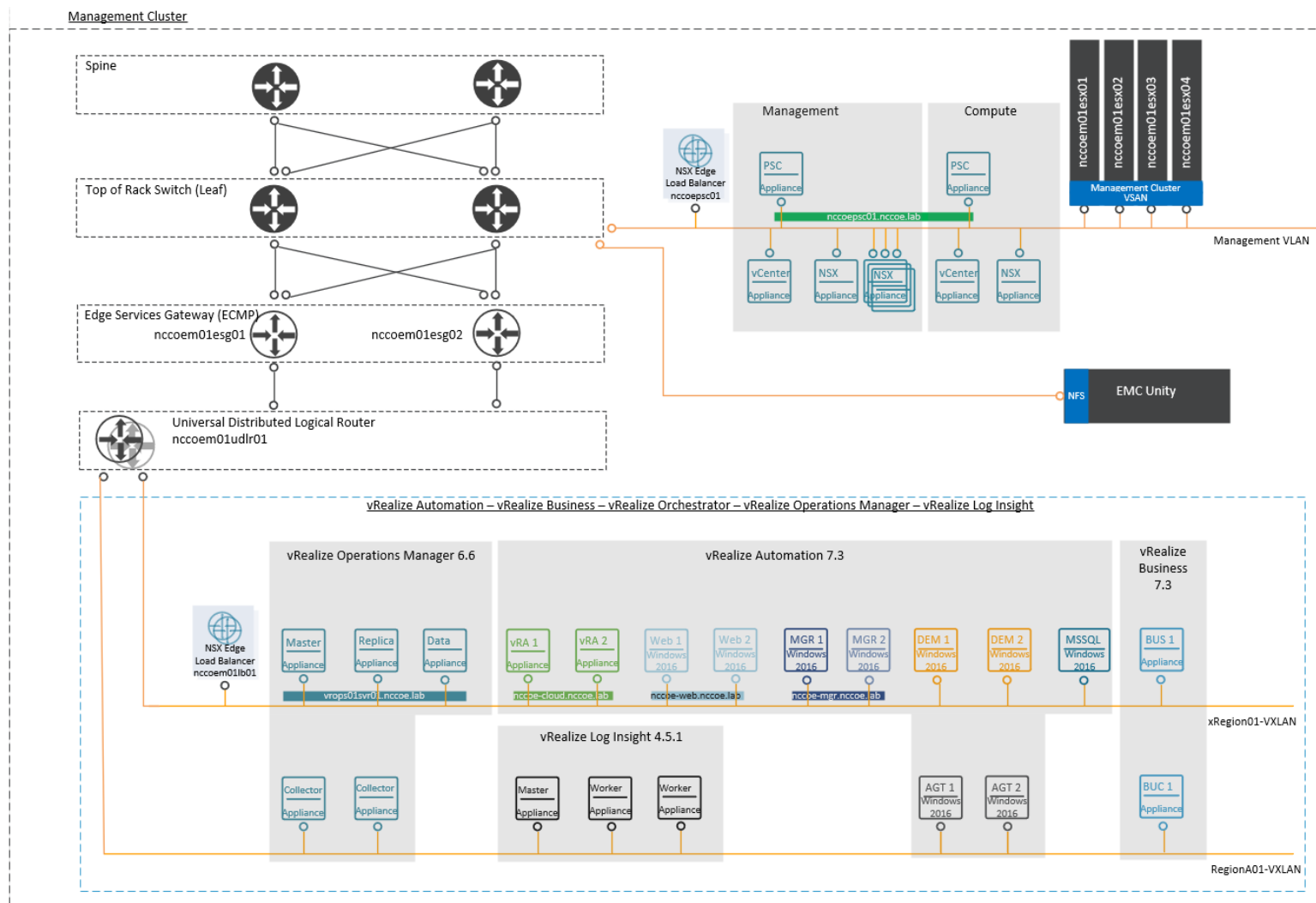
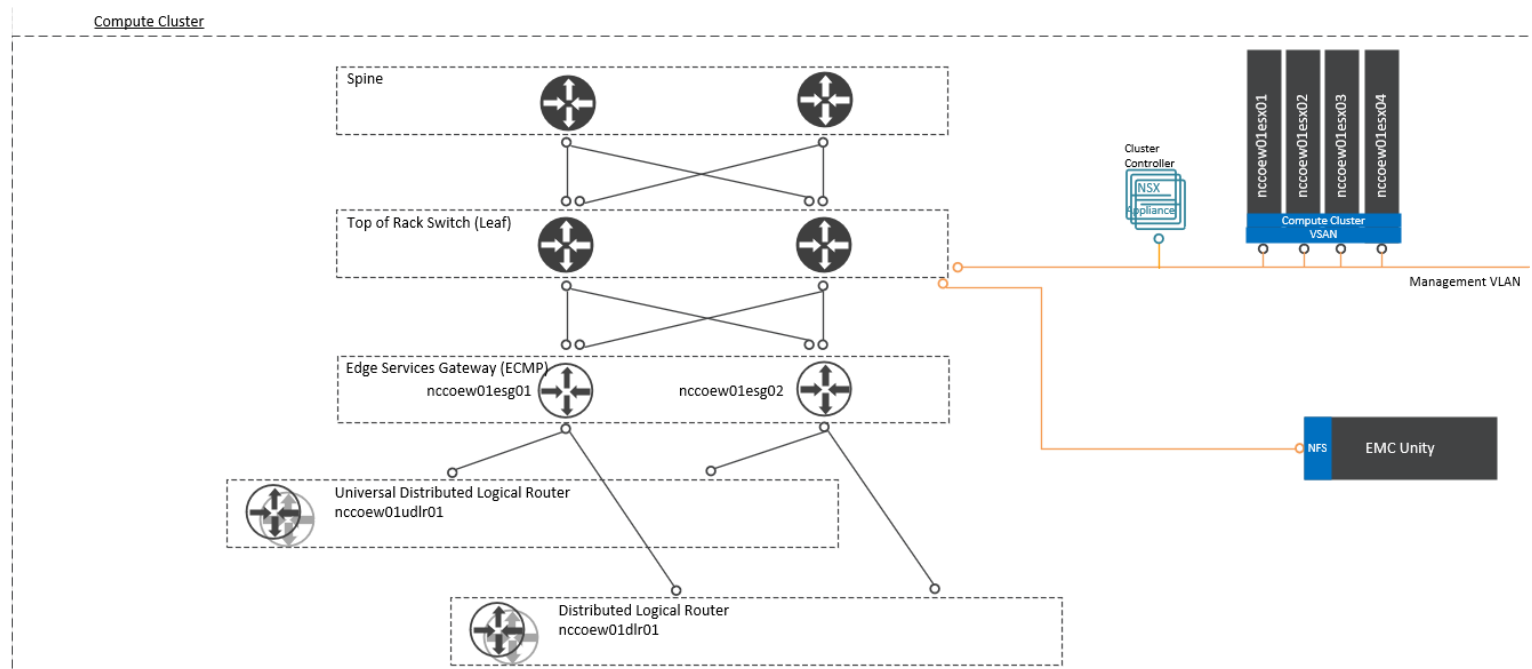


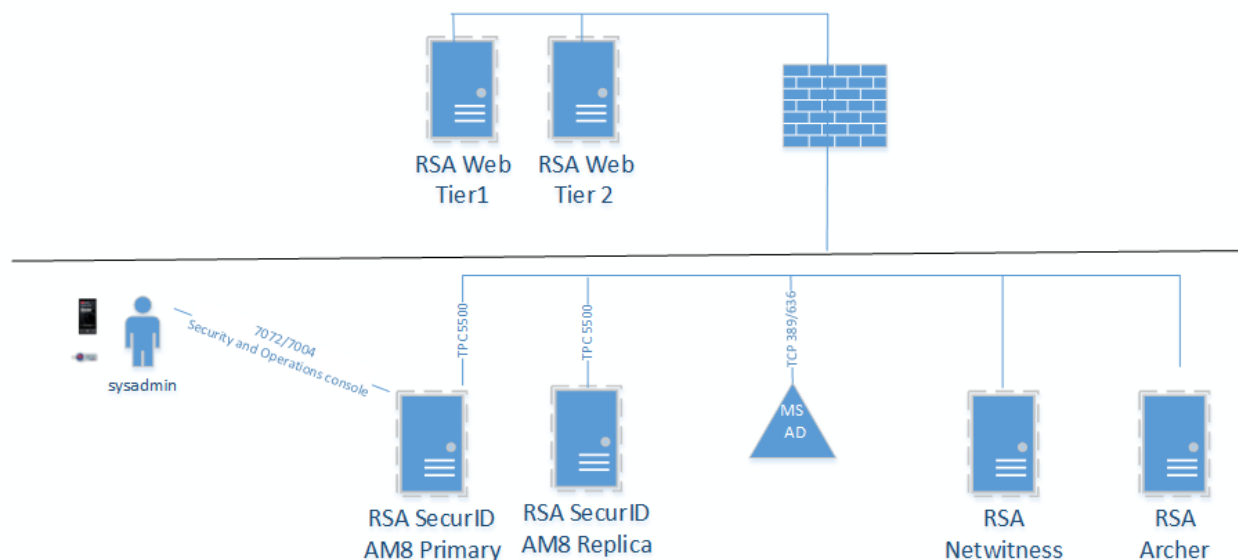
Figure 4-4 VMware Compute Cluster Architecture



### 4.3.2 RSA Cluster Architecture

[Figure 4-5](#) depicts the architecture of the RSA cluster. Within this cluster, the RSA SecurID Suite provides strong authentication for administrator access to critical trusted cloud infrastructure components. RSA NetWitness collects, analyzes, reports on, and stores log data from a variety of sources to support security policy and regulatory compliance requirements across the trusted cloud deployment. Finally, the RSA Archer risk management solution instantiates compliance with applicable requirements, such as FISMA, PCI DSS, and HIPAA, as well as industry-neutral voluntary frameworks like the NIST Cybersecurity Framework, for this trusted cloud deployment.

**Figure 4-5 RSA Cluster**



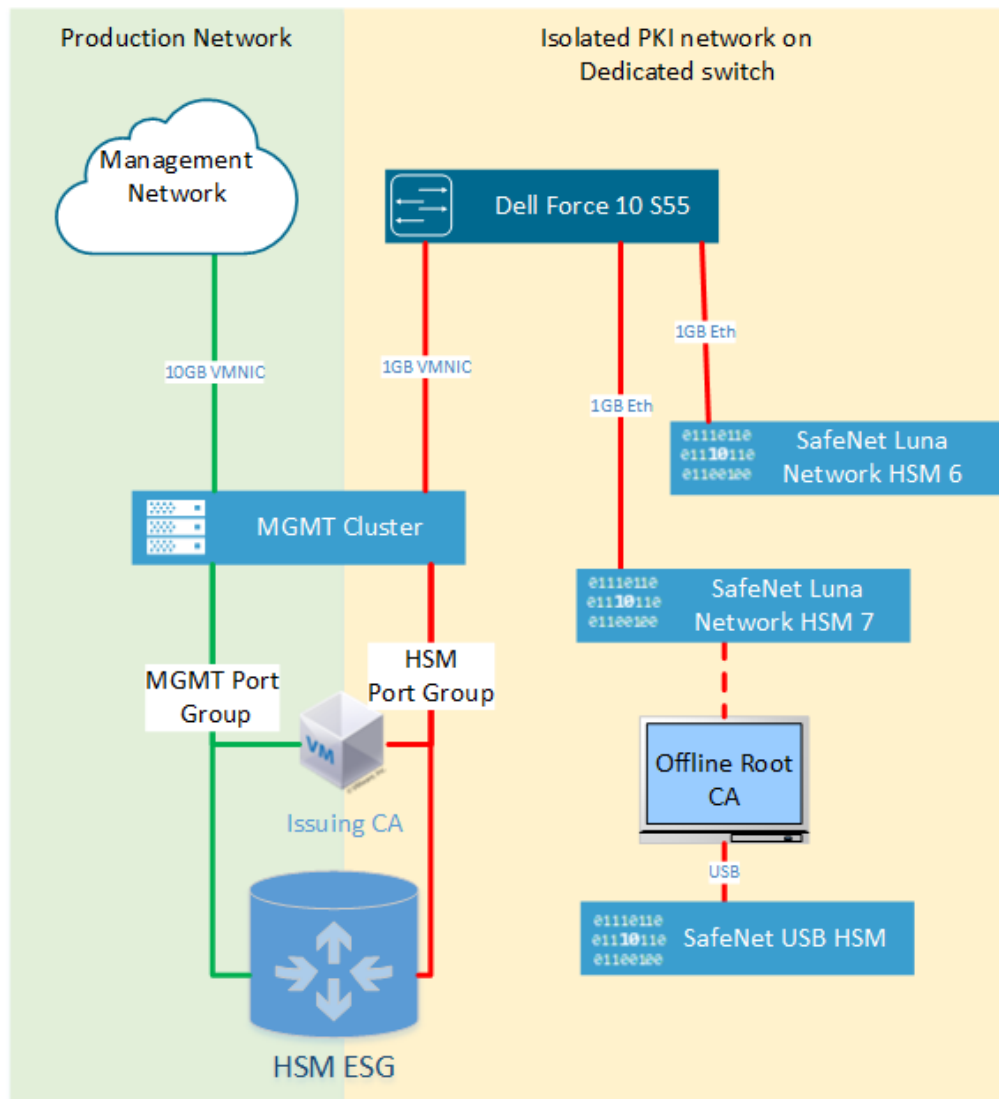
### 4.3.3 HSM Architecture

[Figure 4-6](#) shows the HSM architecture in the NCCoE cloud. The following components are of the greatest interest:

- The SafeNet USB HSM is a small form-factor physical device connected via USB to the Microsoft Root CA Server. To sign and issue a new Issuing CA certificate, the SafeNet USB HSM must be connected directly to the Root CA. Because the SafeNet USB HSM is primarily used to protect the Root CA's keys, it is typically stored securely in a vault. The SafeNet USB HSM is backed up (i.e., cloned) to a secondary SafeNet USB HSM for redundancy.
- SafeNet Luna Network HSM 7 is a network-attached HSM that is tightly integrated with the Microsoft Issuing CA that is located on a VM in the management cluster as a root of trust for FIPS 140-2 Level 3 Compliance.

- SafeNet Luna Network HSM 6 is a network-attached HSM integrated with HTKC as a root of trust for FIPS 140-2 Level 3 Compliance.

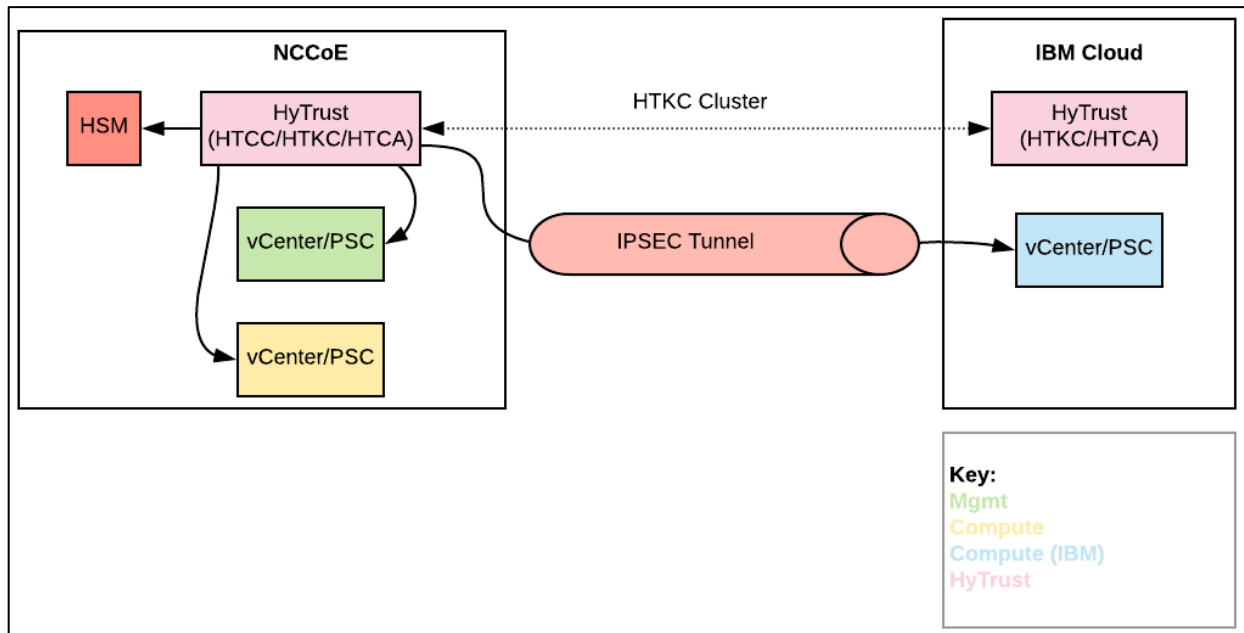
Figure 4-6 HSM Architecture in the NCCoE Cloud



#### 4.3.4 HyTrust Architecture

The NCCoE trusted cloud includes several HyTrust security components, including encryption and key management, data discovery and classification, and advanced security for vSphere. From a placement standpoint, the locations of the HyTrust appliances are shown in [Figure 4-7](#).

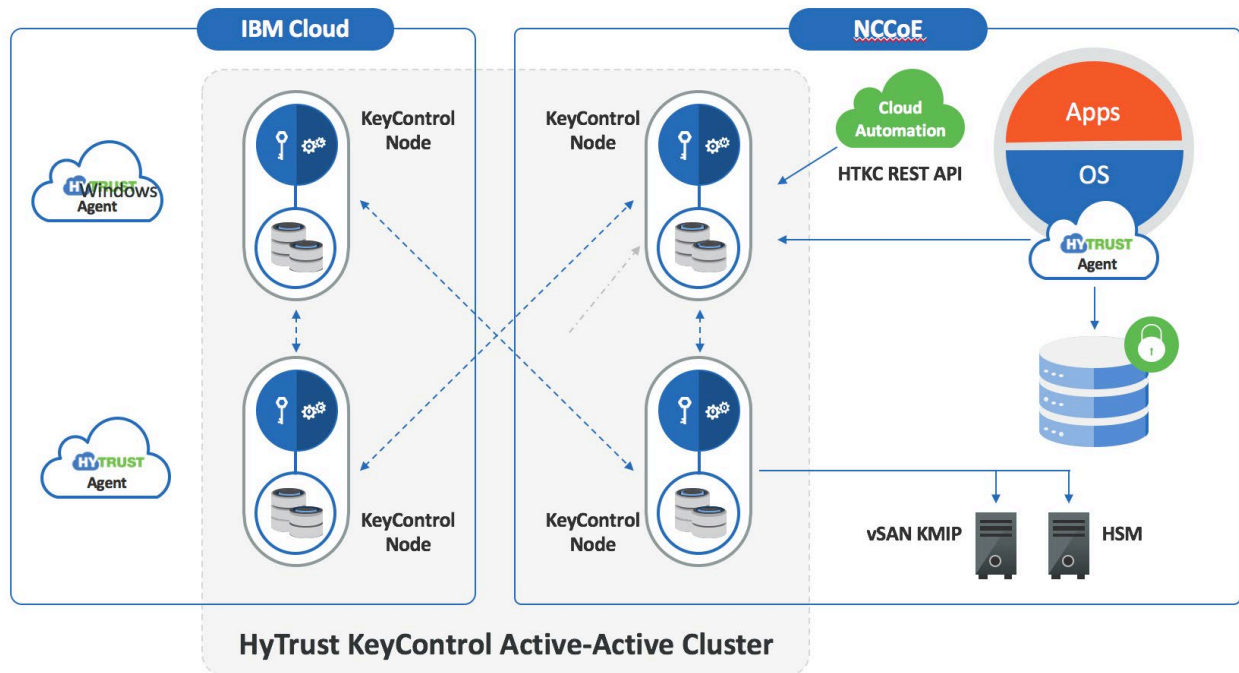
Figure 4-7 HyTrust Architecture in the NCCoE Cloud



The following items explain where each type of HyTrust appliance is located within the architecture and what functions it is providing:

- HTCC provides advanced security features to vSphere. Additionally, HTCC Compliance is used to verify the compliance of ESXi hosts. Users access vSphere via the “Published IP [Internet Protocol]” (PIP) via the HTCC transparent proxy. Approved actions are passed through to vSphere via a service account. Finally, HTCC conducts trust attestation for Intel TXT/TPM to provide hardware verification for HTBC. HTCC will be placed in the NCCoE management cluster. HTCC will be configured with two virtual appliances in an active/passive cluster. That HTCC cluster will service all three vSphere implementations.
- HTKC provides key management to both HTDC in-guest encryption agents and vSANs for storage-level encryption. HTKC leverages the NCCoE SafeNet Luna HSM for hardware administration key storage. HTKC is configured as a trusted key management service in vCenter to provide key management to vSAN. Two HTKC nodes will be placed in the NCCoE management cluster, and two HTKC nodes will be placed in the IBM Cloud, with all four nodes in the same fully active cluster. [Figure 4-8](#) depicts this cluster.
- HTCA will be placed in the NCCoE management cluster and the IBM Cloud. There will be one HTCA node per location, and the nodes will not be clustered.

Figure 4-8 HTKC Node Deployments



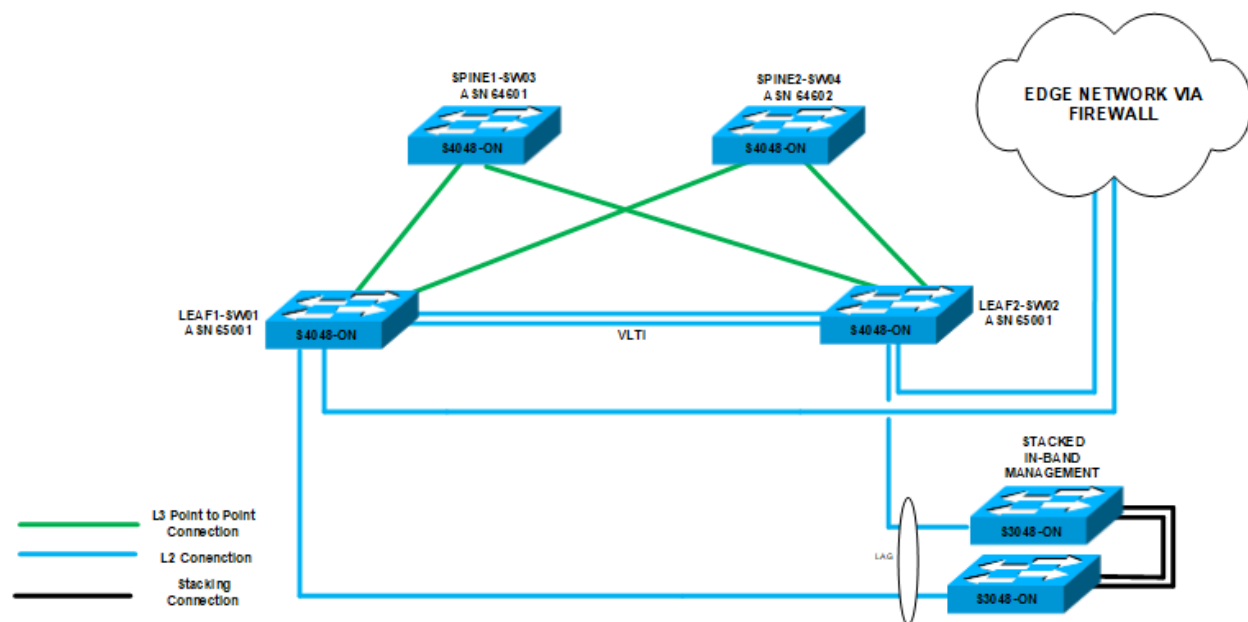
#### 4.3.5 Dell Leaf and Spine Switch Architecture

The core physical networking required for the components within the NCCoE cloud is comprised of four Dell S4048-ON switches and two Dell S3048-ON switches, as shown in [Figure 4-9](#). The Dell S4048-ON switches are configured in a typical leaf-spine topology, with 40-gigabit (GB) interfaces for the interconnections between the switches. The spine switches are in place to handle any east-west traffic that may happen with the data center, while the leaf switches are in place to handle traffic for adjacent servers, as well as northbound traffic out of the NCCoE Cloud.

All of the Dell PowerEdge R740xd servers that comprise the ESXi servers have redundant 10 GB links connected to each of the leaf servers for direct communication with each other. The leaf switches have a Virtual Link Tunnel interconnect (VLTi) between them to provide Layer 2 aggregation between the two switches. The BGP is also enabled on the leaf switches so that they can share routes with the spine switches, and also allow the VMware NSX components to pair with them so that the leaf switches can receive routing information from NSX. The two Dell S3048-ON switches are stacked together by 10 GB interfaces so that they appear as one logical unit. The Dell S3048-ON switches also each use a 10 GB Link Aggregate (LAG) connection as an uplink to the leaf switches. The uplink from the two Dell S3048-ON switches to the leaf switches is necessary because the two Dell S3048-ON switches are mainly 1 GB Ethernet ports supporting components in the environment that have only 1 GB Ethernet connections

and that need to communicate with devices that use 10 GB Enhanced Small Form-Factor Pluggable (SFP+) connections.

**Figure 4-9 NCCoE Layer 3 Leaf – Spine Logical Network Diagram**

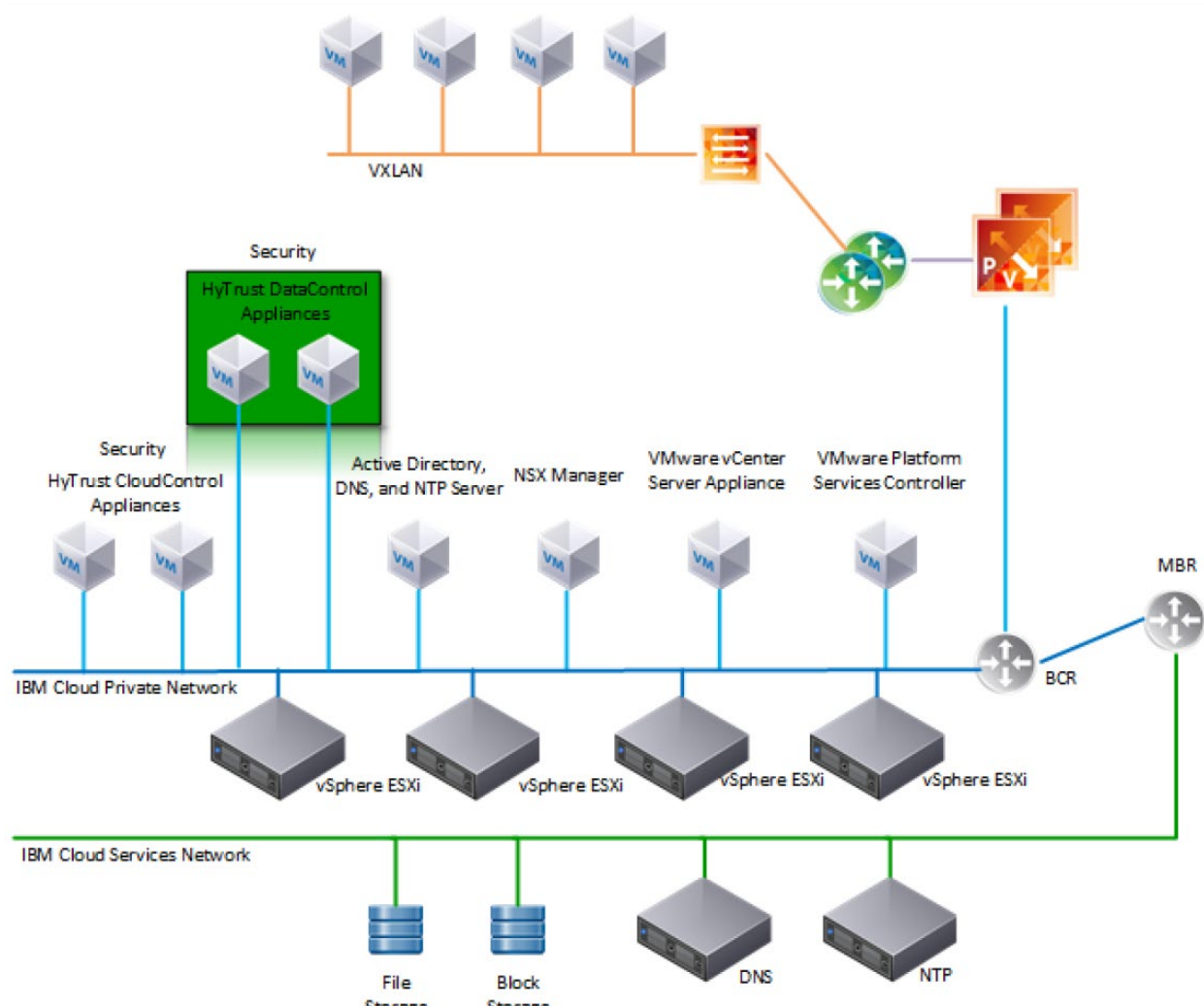


## 4.4 IBM Cloud Solution Architecture

ICSV is deployed on the IBM Cloud infrastructure according to a VMware, HyTrust, IBM, and Intel-validated design reference architecture. The architecture depicted in [Figure 4-10](#) is hosted on a minimum of four bare-metal servers with Intel TXT enabled. VMware vCS is used for hypervisors with VMware vSphere stack as a service. The VMware environment is built on top of bare-metal servers and vSAN storage, and it includes the automatic deployment and configuration of an easy-to-manage logical edge firewall that is powered by VMware NSX. This provides full native access to the entire VMware stack, including the vSphere 6.5 Enterprise Plus edition; the NSX for Service Providers edition; and the centralized platform for management, vCS. The solution, coupled with Windows Active Directory, HTCC, and HTDC, provides a solid foundation to address security and compliance concerns. The entire environment can be provisioned in a matter of hours, and the elastic bare-metal infrastructure can rapidly scale out its compute capacity when needed.

See [Section 4.3](#) for more information on the architecture of the solution components from VMware, HyTrust, and others. Because some of the same components are used for both clouds to extend the management plane across the infrastructure, details of those components are omitted from this section to avoid duplication.

Figure 4-10 IBM Cloud Architecture



## 5 Security Characteristics Analysis

The purpose of the security characteristics analysis is to understand the extent to which the project meets its objective of demonstrating a trusted cloud implementation leveraging commercial off-the-shelf technology. In addition, it seeks to understand the security benefits and drawbacks of the example solution.

### 5.1 Assumptions and Limitations

The security characteristics analysis has the following limitations:



- It is neither a comprehensive test of all security components nor a red-team exercise.
- It cannot identify all weaknesses.
- It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these devices would reveal only weaknesses in implementation that would not be relevant to those adopting this reference architecture.

## 5.2 Demonstration of the Capabilities

The analysis is based on defining a set of use case scenarios for the example solution, and then demonstrating the security capabilities that can be achieved with the example solution for each use case scenario. Each demonstration was documented, including the basic steps performed and the security capabilities achieved.

### 5.2.1 Use Case Scenario 1: Demonstrate Control and Visibility for the Trusted Hybrid Cloud Environment

The business problem is needing to have a well-secured cloud environment to reduce the risk of a compromise of that environment.

Assumptions for the trusted hybrid cloud environment (steps taken before the demonstrations occur) are as follows:

1. The cryptographic, compute, storage, and network hardware components are secured and hardened.
2. The VVD and the IBM Cloud for VMware – vCS have been instantiated on IBM Cloud stacks through automation scripts.
3. The cryptographic network is separated and isolated from the management cluster and the tenant workloads cluster.
4. The user accounts are isolated and secured based on defined functional roles following the principle of least privilege.
5. The core components of the VVD and vCS, third-party software components, and all core services are secured and hardened using recommended practices, such as vendor-developed or community-developed secure configuration guides or DISA STIGs.
6. RSA NetWitness Logs is installed on the virtual machine or dedicated hardware.
7. RSA Archer Suite and the Public Sector Use Cases (Assessment & Authorization [A&A], Continuous Monitoring) are installed.
8. Logs from core services are being forwarded to RSA NetWitness Logs.
9. One or more industry-standard cloud service provider certifications, such as ISO, PCI, Cloud Security Alliance (CSA), Service Organization Control (SOC), HIPAA, and FedRAMP, are leveraged.

## Capability demonstrations:

1. Show the configuration of the hardware components, including the HSM, the compute node, the storage device, and the network switches.
2. Show the VVD and vCS stacks in vCenter (e.g., vSAN is encrypted).
3. Show the backup solution for the resiliency and recovery of workloads in a disaster-recovery scenario.
4. Show the three isolation domains, including the cryptographic, management, and tenant workloads in NSX.
5. Show multifactor authentication with an RSA SecurID token and the Active Directory domain groups and access rights structure.
6. Scan and show the secure configuration of VMware software components, such as ESXi, NSX, and Windows domain controller, by using CloudControl and a Windows configuration scanner.  
[Figure 5-1](#) shows an example of results from a secure configuration scan.

**Figure 5-1 Example of Secure Configuration Scan Results**

Hosts	Host Type	Patch Level	Label	Last Run Template	Last Run	Compliance
10.121.71.133	ESXi Host	VMware ESXi 6.5.0 build-7967591	PIL	N/A	Never	0%
10.121.71.135	ESXi Host			N/A	N/A	0%
192.168.4.105	VMware NSX	6.4.0.7564187		N/A	Never	0%
192.168.4.106	VMware NSX	6.4.0.7564187		N/A	Never	0%
cloud-vcenter.icsv.nccoe.lab	vCenter	6.5.0 build-6816762		N/A	N/A	
cloud-vcenter.icsv.nccoe.lab	vSphere Web Client Server			N/A	N/A	
comp-nccoe-esxi-01.nccoe.lab	ESXi Host	VMware ESXi 6.5.0 build-7388607		VMware 6.0 ESXi_Custom_Template	08/23/2018 12:14:24 PM	100%
comp-nccoe-esxi-02.nccoe.lab	ESXi Host	VMware ESXi 6.5.0 build-7388607	TRUSTED, PIL	VMware 6.0 ESXi_Custom_Template	08/23/2018 12:14:24 PM	100%
comp-nccoe-esxi-03.nccoe.lab	ESXi Host	VMware ESXi 6.5.0 build-7388607	TRUSTED, PIL	VMware 6.0 ESXi_Custom_Template	08/24/2018 10:25:14 AM	100%
comp-nccoe-esxi-04.nccoe.lab	ESXi Host	VMware ESXi 6.5.0 build-7388607	TRUSTED, PIL	VMware 6.0 ESXi_Custom_Template	08/23/2018 12:14:24 PM	100%

7. Scan and show any software vulnerabilities of an ESXi node and a Microsoft workload.
8. Show the IBM FedRAMP report.
9. Show the configuration of the log collector for ingesting and enriching VMware ESXi logs.
10. Show the logs and alerts (if any) in the Analyst UI.
11. Show the ability to raise an Incident from RSA NetWitness Logs to RSA Archer Suite.
12. Show the configuration of the Archer Public Sector Use Cases to accept and/or ingest information from various components about risks in the trusted hybrid cloud environment.
13. Show the analyst interface and outputs of Archer Public Sector Use Cases in recording compliance and enabling risk mitigation activities.

The potential benefits of this are reducing the risk that workloads running in that cloud environment are compromised, and identifying potential security issues more quickly.

### 5.2.2 Use Case Scenario 2: Demonstrate Control of Workloads and Data Security

The business problem is needing to protect workloads so they only execute on authorized compute nodes.

Assumptions for the trusted hybrid cloud environment (steps taken before the demonstrations occur) are as follows:

1. Workloads are encrypted and are running on a trusted compute node with a specific asset tag (PCI or HIPAA) within a mixed cluster.
2. Secondary approval is enforced for highly sensitive systems and/or operations.

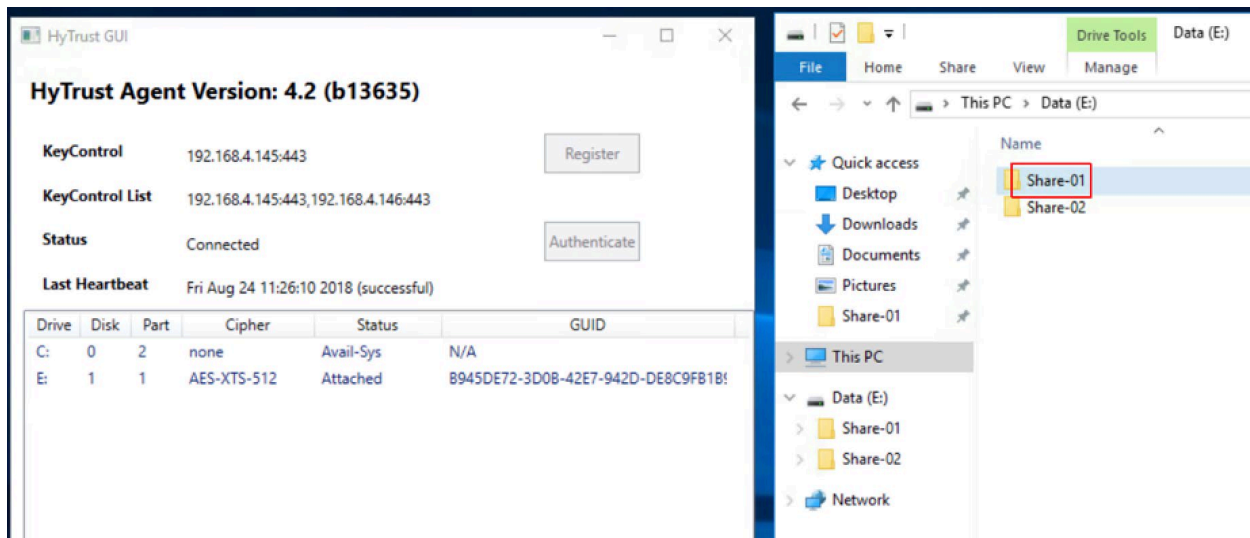
Capability demonstrations:

1. Show that the workload on the trusted compute node is decrypted, as it matches the trust and asset tag policy. [Figure 5-2](#) shows examples of nodes with their labels (e.g., TRUSTED, PII). [Figure 5-3](#) shows verification that a workload on one of the nodes has been decrypted.

Figure 5-2 Examples of Trusted Compute Nodes

<a href="#">comp-nccoe-esxi-01.nccoe.lab</a> 	ESXi Host	VMware ESXi 6.5.0 build-7388607	
<a href="#">comp-nccoe-esxi-02.nccoe.lab</a>  	ESXi Host	VMware ESXi 6.5.0 build-7388607	TRUSTED, PII
<a href="#">comp-nccoe-esxi-03.nccoe.lab</a>  	ESXi Host	VMware ESXi 6.5.0 build-7388607	TRUSTED, PII
<a href="#">comp-nccoe-esxi-04.nccoe.lab</a>  	ESXi Host	VMware ESXi 6.5.0 build-7388607	TRUSTED, PII

Figure 5-3 Example of Decrypted Workload



2. Migrate the workload to a compute node without the same asset tag policy, and show that the workload cannot be decrypted on the untrusted compute node. [Figure 5-4](#) presents an example of a workload running on a server that does not have any tags. [Figure 5-5](#) shows that the same workload cannot be decrypted because the server on which it runs lacks the necessary tags.

Figure 5-4 Example of Workload on Untagged Server

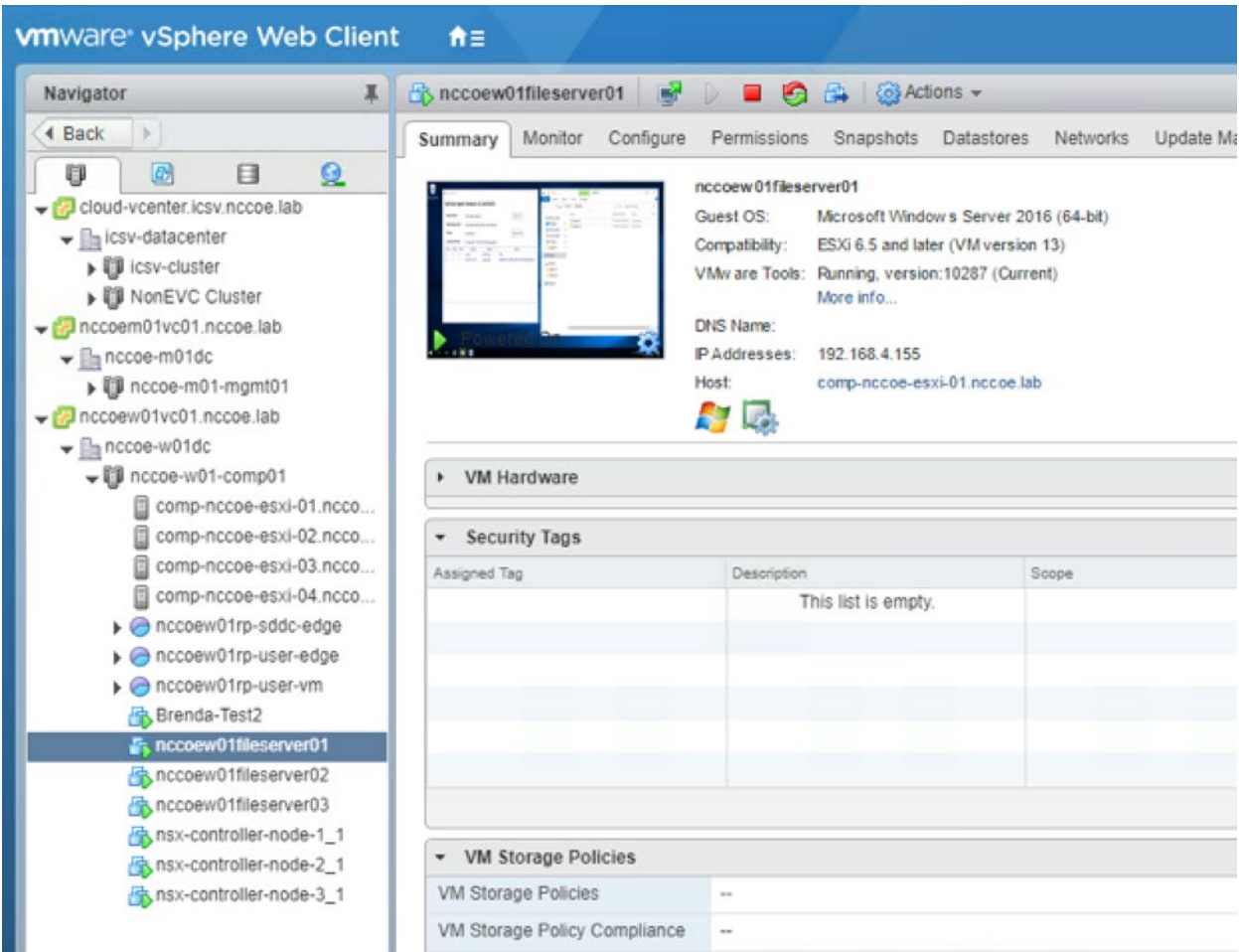


Figure 5-5 Example of Workload that Cannot Be Decrypted



- 3. Migrate the workload back to a trusted compute node, and show that the workload can be decrypted and that the data can be accessed on the trusted compute node. [Figure 5-6](#) shows that the workload has been migrated to a trusted and tagged server. [Figure 5-7](#) shows that the workload can decrypt its data again because it is running on a trusted and tagged server.

Figure 5-6 Example of Workload Migrated to Trusted and Tagged Server

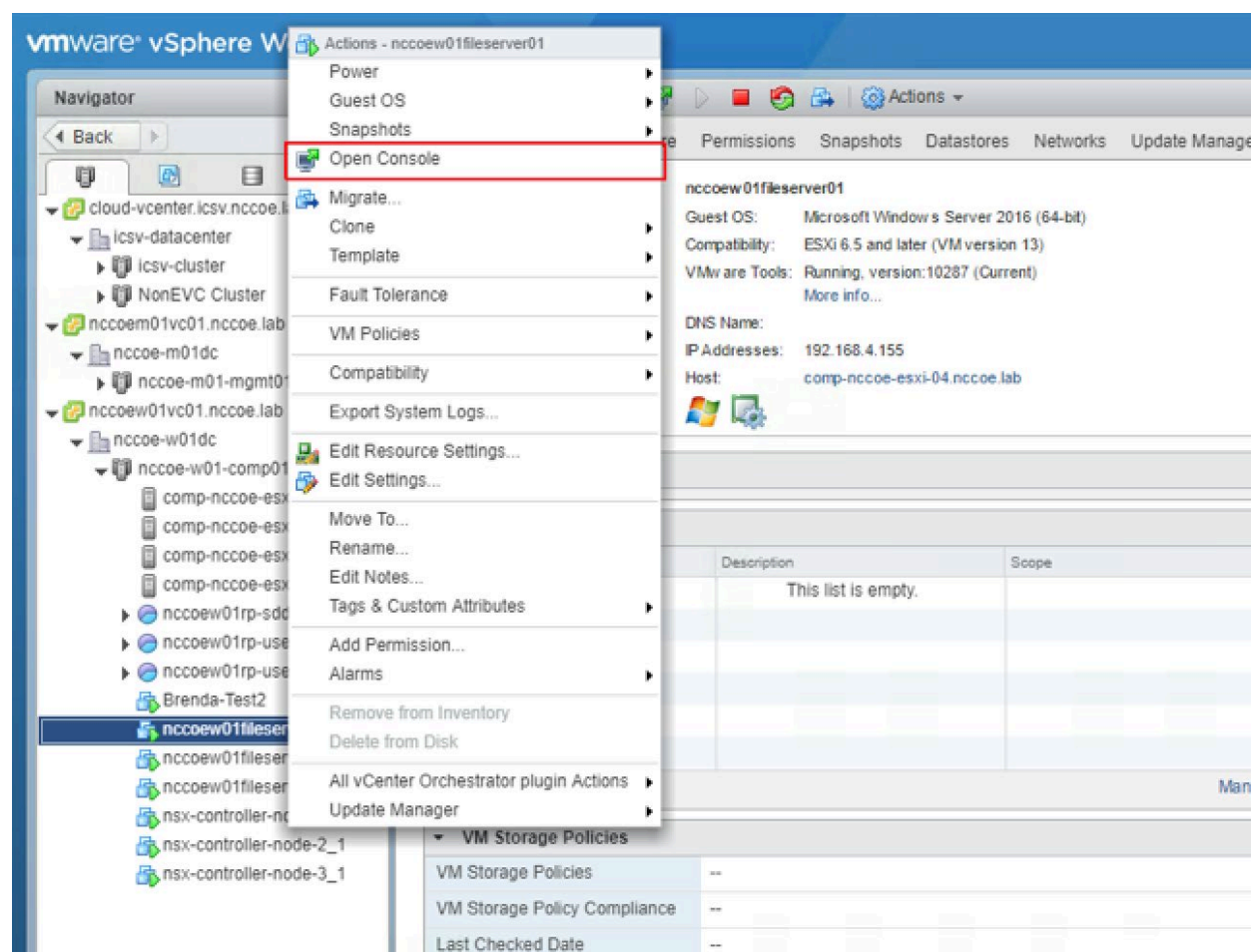
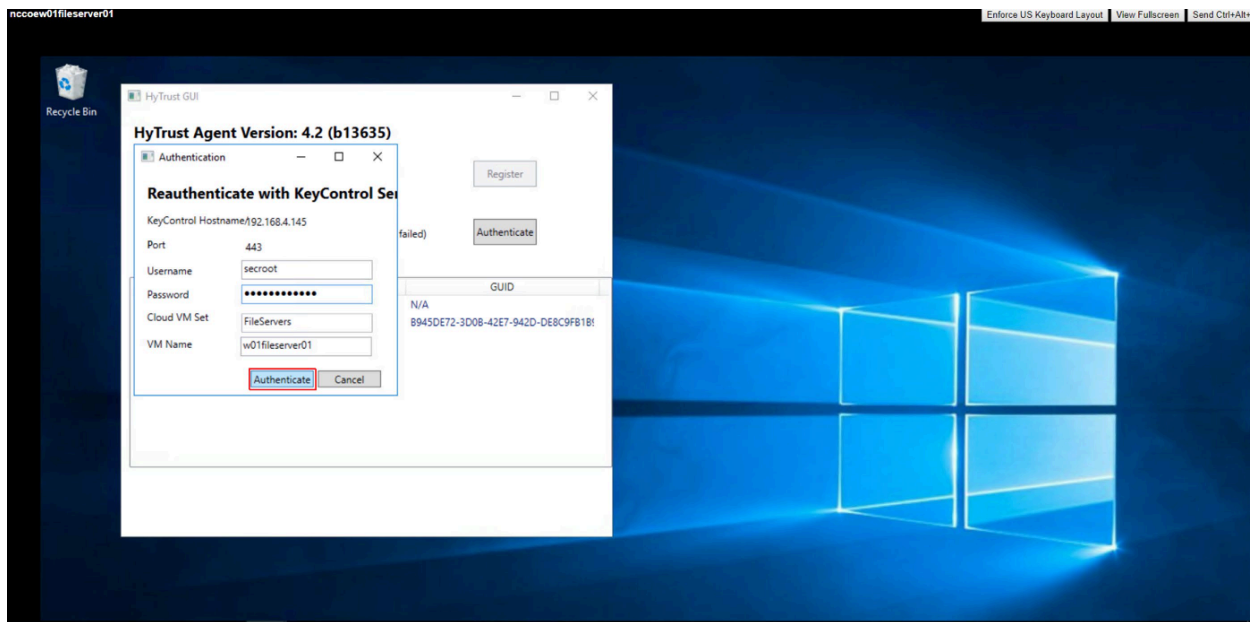


Figure 5-7 Example of Workload Running on Trusted and Tagged Server



4. Show that two individuals are required to authorize the deletion of a high-value asset.
5. Scan and classify data based on a data classification schema, such as personally identifiable information.

The potential benefit of this is reducing the risk that workloads are compromised.

### 5.2.3 Use Case Scenario 3: Demonstrate a Workload Security Policy in a Hybrid Cloud

There are two business problems addressed. The first is needing to move workloads (VMs and data) from one trusted compute node to a second one without any degradation of security posture or any loss of information in order to perform scheduled maintenance on the first trusted compute node. An example of a reason for scheduled maintenance is to patch or upgrade the hypervisor. The second is ensuring scripts, configurations, and other files or settings with hard-coded IP addresses or domain names continue to work even when workloads containing them are migrated from one cloud to another.

Assumptions for the trusted hybrid cloud environment (steps taken before the demonstrations occur) are as follows:

1. The trusted on-premises environment has been instantiated.
2. A secure connection has been established between the on-premises environment and the public cloud instance.



3. The security capabilities from the on-premises environment have been extended to the public cloud instance by integrating it into the on-premises management plane.
4. A three-tier web application is running in the on-premises environment with a specified security policy (e.g., data protection, network segmentation, compliance requirements).

Capability demonstrations:

1. Show that the three-tier web application's security policy is enforced within the on-premises environment.
2. Show that the three-tier web application can be migrated from the on-premises environment to the public cloud instance.
3. Show that the workload continues to operate normally after migration and its security posture is not negatively impacted by running the scripts with hard-coded IP addresses and domain names.
4. Show that the three-tier web application's security policy is persistent after the migration to the public cloud instance.

The potential benefits of this are reducing the risk that workloads are compromised and reducing the risk that operations are interrupted because of a workload migration.

#### 5.2.4 Use Case Scenario 4: Demonstrate Recovery From an Unexpected Infrastructure Outage

The business problem is needing to quickly restore operations for a three-tier application when an unexpected infrastructure outage occurs at the site where the application is hosted, while also ensuring there is no degradation of security posture for the application when it is restored at another site. This allows the application to continue functioning while the outage at the first site is addressed.

Assumptions for the trusted hybrid cloud environment (steps taken before the demonstrations occur) are as follows:

1. When the outage started, the workloads were encrypted and were running on a trusted compute node with a specific asset tag (PCI or HIPAA) within a mixed cluster.
2. The outage has made all three tiers of the application unavailable at the original site, and on-premises recovery is not possible until the outage has been resolved.
3. A second trusted compute node within a different data center acting as a disaster recovery site is authorized to run the same types of workloads as the first trusted compute node.
4. Secondary approval is enforced for highly sensitive systems and/or operations.

Capability demonstrations:

1. Show that the three tiers of the application are present at the disaster recovery site and that each tier is up to date.



2. Show that Fault Tolerance (FT) was regularly backing up data from the original site to the disaster recovery site until shortly before the outage occurred.
3. Show that the workloads on the trusted compute node at the disaster recovery site can be decrypted, as they match the trust and asset tag policy.
4. Show that the NSX Universal Distributed Firewall rules are present and enforced at the receiving end (the disaster recovery site) to enable updating the workloads and data on the trusted compute node.

The potential benefit of this is to minimize disruption from unscheduled outages, which means operations should be restored more quickly.

Note that this demonstration is simple, with static content. The intent is that this demonstration could be extended to a more complex scenario, such as applications with dynamic content where the application developers need to decide how the application should handle failures, including possibly retaining state when a failure occurs and maintaining persistent connections.

### 5.2.5 Use Case Scenario 5: Demonstrate Providing Visibility into Network Traffic Patterns

The business problem is needing to have visibility into network traffic flow patterns so abnormal patterns can be identified and investigated.

Assumptions for the trusted hybrid cloud environment (steps taken before the demonstrations occur) are as follows:

1. Logging has been enabled at ESXi Hosts, NSX Managers, NSX Controllers, Edge Service Gateways, Control VMs, and DFWS, including tunnels.
2. NetWitness is ready and available to collect and store logs from other hosts.

Capability demonstrations:

1. Show that authorized administrators can see a vRLI custom dashboard for traffic flows indicating what is talking to what, both physical and virtual.
2. Show that the traffic flows include source, destination, ports, and protocol.
3. Show that the traffic flows from all the devices logging the flows are transferred to NetWitness.

The potential benefit of this is to identify suspicious activity, such as large data bursts, that may indicate exfiltration of sensitive data or other security problems.

### 5.2.6 Use Case Scenario 6: Demonstrate Application Zero Trust

The business problem is preventing unauthorized communications with a particular application.

Assumptions for the trusted hybrid cloud environment (steps taken before the demonstrations occur) are as follows:

1. An application is executing within a workload running on a trusted compute node.
2. The infrastructure supporting the application has been allowlisted through DFW.

Capability demonstrations:

1. Show that communications from the allowlisted infrastructure components are permitted.
2. Show that communications from anywhere other than the allowlisted infrastructure components are denied and such communications flagged or alerted on.

The potential benefit of this is to prevent attackers and other unauthorized parties from accessing the application and using it or compromising it.

## Appendix A Mappings

The tables in this appendix include all the NIST SP 800-53 Revision 5 controls ([Table A-1](#)) and NIST Cybersecurity Framework subcategories ([Table A-2](#)) listed in [Section 4.2.8](#)—those provided by individual components of the solution—and also list additional subcategories and controls provided by the solution as a whole, not an individual component.

**Table A-1 List of NIST SP 800-53 Revision 5 Controls Addressed by Solution**

ID	Control Description
<b>Access Control (AC)</b>	
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-17	Remote Access
AC-20	Use of External Information Systems
<b>Audit and Accountability (AU)</b>	
AU-2	Audit Events
AU-3	Content of Audit Records
AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failures
AU-6	Audit Review, Analysis, and Reporting
AU-7	Audit Reduction and Report Generation
AU-8	Time Stamps
AU-9	Protection of Audit Information
AU-10	Non-Repudiation
AU-11	Audit Record Retention
AU-12	Audit Generation
<b>Security Assessment and Authorization (CA)</b>	
CA-7	Continuous Monitoring
<b>Configuration Management (CM)</b>	
CM-3	Configuration Change Control
CM-4	Security Impact Analysis
CM-8	Information System Component Inventory

ID	Control Description
CM-9	Configuration Management Plan
CM-10	Software Usage Restrictions
<b>Identification and Authentication (IA)</b>	
IA-2	Identification and Authentication (Organizational Users)
IA-3	Device Identification and Authentication
IA-4	Identifier Management
IA-5	Authenticator Management
IA-7	Cryptographic Module Authentication
<b>Maintenance (MA)</b>	
MA-2	Controlled Maintenance
MA-3	Maintenance Tools
MA-4	Nonlocal Maintenance
MA-5	Maintenance Personnel
MA-6	Timely Maintenance
<b>Risk Assessment (RA)</b>	
RA-3	Risk Assessment
RA-5	Vulnerability Scanning
<b>System and Services Acquisition (SA)</b>	
SA-18	Tamper Resistance and Detection
<b>System and Communications Protection (SC)</b>	
SC-2	Application Partitioning
SC-3	Security Function Isolation
SC-7	Boundary Protection
SC-8	Transmission Confidentiality and Integrity
SC-12	Cryptographic Key Establishment and Management
SC-13	Cryptographic Protection
SC-15	Collaborative Computing Devices
SC-16	Transmission of Security Attributes
SC-28	Protection of Information at Rest

ID	Control Description
<b>System and Information Integrity (SI)</b>	
SI-2	Flaw Remediation
SI-4	Information System Monitoring
SI-7	Software, Firmware, and Information Integrity

**Table A-2 List of NIST Cybersecurity Framework Subcategories Addressed by Solution**

Cyber-security Framework Subcategory Identifier	Cybersecurity Framework Subcategory Name
<b>Identify (ID)</b>	
ID.AM-2	Software platforms and applications within the organization are inventoried.
<b>Protect (PR)</b>	
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.
PR.AC-3	Remote access is managed.
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation).
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions.
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the privacy risks and other organizational risks).
PR.DS-1	Data-at-rest is protected.
PR.DS-2	Data-in-transit is protected.
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition.
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity.
PR.IP-3	Configuration change control processes are in place.
PR.IP-4	Backups of information are conducted, maintained, and tested.
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.
PR.IP-12	A vulnerability management plan is developed and implemented.

Cyber-security Framework Subcategory Identifier	Cybersecurity Framework Subcategory Name
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.
PR.PT-4	Communications and control networks are protected.
<b>Detect (DE)</b>	
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed.
DE.AE-2	Detected events are analyzed to understand attack targets and methods.
DE.AE-3	Event data are collected and correlated from multiple sources and sensors.
DE.AE-4	Impact of events is determined.
DE.AE-5	Incident alert thresholds are established.
DE.CM-1	The network is monitored to detect potential cybersecurity events.
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed.

## Appendix B List of Acronyms

<b>A&amp;A</b>	Assessment & Authorization
<b>ACL</b>	Access Control List
<b>ADCS</b>	Active Directory Certificate Services
<b>AWS</b>	Amazon Web Services
<b>BGP</b>	Border Gateway Protocol
<b>BIOS</b>	Basic Input/Output System
<b>CA</b>	Certificate Authority
<b>CloudSPF</b>	Cloud Security Policy Framework
<b>COSO</b>	Committee of Sponsoring Organizations of the Treadway Commission
<b>CRADA</b>	Cooperative Research and Development Agreement
<b>CSA</b>	Cloud Security Alliance
<b>DCG</b>	Data Center Group
<b>DD VE</b>	Data Domain Virtual Edition
<b>DFW</b>	Distributed Firewall
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DISA</b>	Defense Information Systems Agency
<b>DLR</b>	Distributed Logical Router
<b>DNS</b>	Domain Name System
<b>ECMP</b>	Equal-Cost Multi-Path
<b>ESG</b>	Edge Services Gateway
<b>FAIR</b>	Factor Analysis of Information Risk
<b>FedRAMP</b>	Federal Risk and Authorization Management Program
<b>FIPS</b>	Federal Information Processing Standard
<b>FISMA</b>	Federal Information Security Modernization Act
<b>FOIA</b>	Freedom of Information Act

<b>FT</b>	Fault Tolerance
<b>GB</b>	Gigabyte
<b>Gb</b>	Gigabit
<b>GKH</b>	Good Known Host
<b>GRC</b>	Governance, Risk, and Compliance
<b>HIPAA</b>	Health Insurance Portability and Accountability Act
<b>HSM</b>	Hardware Security Module
<b>HTBC</b>	HyTrust BoundaryControl
<b>HTCA</b>	HyTrust CloudAdvisor
<b>HTCC</b>	HyTrust CloudControl
<b>HTDC</b>	HyTrust DataControl
<b>HTKC</b>	HyTrust KeyControl
<b>I/O</b>	Input/Output
<b>IaaS</b>	Infrastructure as a Service
<b>ICSV</b>	IBM Cloud Secure Virtualization
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>Intel AES-NI</b>	Intel Advanced Encryption Standard – New Instructions
<b>Intel CIT</b>	Intel Cloud Integrity Technology
<b>Intel TPM</b>	Intel Trusted Platform Module
<b>Intel TXT</b>	Intel Trusted Execution Technology
<b>Intel VT</b>	Intel Virtualization Technology
<b>IPsec</b>	Internet Protocol Security
<b>ISO</b>	International Organization for Standardization
<b>IT</b>	Information Technology
<b>KMIP</b>	Key Management Interoperability Protocol
<b>LAG</b>	Link Aggregate
<b>MLE</b>	Measured Launch Environment



<b>N/A</b>	Not Applicable
<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NFS</b>	Network File System
<b>NIST</b>	National Institute of Standards and Technology
<b>NISTIR</b>	National Institute of Standards and Technology Internal Report
<b>NSX-V</b>	NSX for vSphere
<b>NTP</b>	Network Time Protocol
<b>OS</b>	Operating System
<b>PC</b>	Personal Computer
<b>PCI DSS</b>	Payment Card Industry Data Security Standard
<b>PIP</b>	Published Internet Protocol
<b>PSC</b>	Platform Services Controller
<b>RMF</b>	Risk Management Framework
<b>SDDC</b>	Software-Defined Data Center
<b>SFP+</b>	Enhanced Small Form-Factor Pluggable
<b>SIEM</b>	Security Information and Event Management
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SNMP</b>	Simple Network Management Protocol
<b>SOC</b>	Service Organization Control
<b>SP</b>	Special Publication
<b>SRM</b>	Site Recovery Manager
<b>SSL</b>	Secure Sockets Layer
<b>STIG</b>	Security Technical Implementation Guide
<b>TLS</b>	Transport Layer Security
<b>TOR</b>	Top-of-Rack
<b>U.S.</b>	United States

<b>UDLR</b>	Universal Distributed Logical Router
<b>UDP</b>	User Datagram Protocol
<b>USB</b>	Universal Serial Bus
<b>vCS</b>	vCenter Server
<b>VDS</b>	vSphere Distributed Switch
<b>VIB</b>	vSphere Installation Bundle
<b>VLAN</b>	Virtual Local Area Network
<b>VLTi</b>	Virtual Link Tunnel Interconnect
<b>VM</b>	Virtual Machine
<b>VMM</b>	Virtual Machine Manager
<b>VMX</b>	Virtual Machine Extensions
<b>VPN</b>	Virtual Private Network
<b>vR</b>	vSphere Replication
<b>vRA</b>	vRealize Automation
<b>vRB</b>	vRealize Business for Cloud
<b>vRLI</b>	vRealize Log Insight
<b>vRO</b>	vRealize Orchestrator
<b>vROPS</b>	vRealize Operations Manager
<b>VTEP</b>	VXLAN Tunnel Endpoint
<b>VUM</b>	vSphere Update Manager
<b>VVD</b>	VMware Validated Design
<b>VXLAN</b>	Virtual Extensible Local Area Network

## Appendix C Glossary

All significant technical terms used within this document are defined in other key documents, particularly NISTIR 7904, *Trusted Geolocation in the Cloud: Proof of Concept Implementation* [\[1\]](#). As a convenience to the reader, terms critical to understanding this volume are provided in this glossary.

<b>Attestation</b>	The process of providing a digital signature for a set of measurements securely stored in hardware, and then having the requester validate the signature and the set of measurements.
<b>Cloud workload</b>	A logical bundle of software and data that is present in, and processed by, a cloud computing technology.
<b>Geolocation</b>	Determining the approximate physical location of an object, such as a cloud computing server.
<b>Hardware root of trust</b>	An inherently trusted combination of hardware and firmware that maintains the integrity of information.
<b>Trusted compute pool</b>	A physical or logical grouping of computing hardware in a data center that is tagged with specific and varying security policies. Within a trusted compute pool, the access and execution of applications and workloads are monitored, controlled, audited, etc. Also known as a <i>trusted pool</i> .

## Appendix D References

- [1] M. Bartock et al., *Trusted geolocation in the cloud: Proof of concept implementation*, NIST Internal Report 7904, Gaithersburg, MD, Dec. 2015, 59 pp.  
Available: <https://doi.org/10.6028/NIST.IR.7904>.
- [2] “National Cybersecurity Center of Excellence (NCCoE) trusted geolocation in the cloud building block,” *Federal Register*, vol. 82, no. 90, May 11, 2017, pp. 21979-21980.  
Available: <https://www.govinfo.gov/content/pkg/FR-2017-05-11/pdf/2017-09502.pdf>.
- [3] Joint Task Force, *Guide for Conducting Risk Assessments*, NIST SP 800-30 Revision 1, Gaithersburg, MD, Sep. 2012, 95 pp. Available: <https://doi.org/10.6028/NIST.SP.800-30r1>.
- [4] Joint Task Force, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST SP 800-37 Revision 2, Gaithersburg, MD, Dec. 2019, 183 pp. Available: <https://doi.org/10.6028/NIST.SP.800-37r2>.
- [5] *Risk management – Guidelines*, ISO 31000:2018, Feb. 2018. Available: <https://www.iso.org/iso-31000-risk-management.html>.
- [6] COSO, “Enterprise risk management – Integrating with strategy and performance,” COSO, Jun. 2017. Available: <https://www.coso.org/Pages/erm.aspx>.
- [7] J. Freund and J. Jones, *Measuring and Managing Information Risk: A FAIR Approach*. Oxford, England: Butterworth-Heinemann, 2014.
- [8] NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, Gaithersburg, MD, Apr. 16, 2018, 55 pp. Available: <https://doi.org/10.6028/NIST.CSWP.04162018>.
- [9] Joint Task Force Transformation Initiative, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Revision 4, Gaithersburg, MD, Apr. 2013, 462 pp. Available: <https://doi.org/10.6028/NIST.SP.800-53r4>.
- [10] VMware, “Architecture and design: VMware validated design for management and workload consolidation 4.2,” VMware, Palo Alto, CA, Mar. 27, 2018.  
Available: <https://docs.vmware.com/en/VMware-Validated-Design/4.2/vmware-validated-design-42-sddc-consolidated-architecture-design.pdf>.
- [11] VMware, “Deployment for region A: VMware validated design for software-defined data center 4.2,” VMware, Palo Alto, CA, Feb. 13, 2018. Available: <https://docs.vmware.com/en/VMware-Validated-Design/4.2/vmware-validated-design-42-sddc-regiona-deployment.pdf>.

- [12] VMware, “Operational verification: VMware validated design for software-defined data center 4.2,” VMware, Palo Alto, CA, Mar.27, 2018. Available: <https://docs.vmware.com/en/VMware-Validated-Design/4.2/vmware-validated-design-42-sddc-operational-verification.pdf>.
- [13] VMware, “Planning and preparation: VMware validated design for software-defined data center 4.2,” VMware, Palo Alto, CA, Feb. 13, 2018. Available: <https://docs.vmware.com/en/VMware-Validated-Design/4.2/vmware-validated-design-42-sddc-planning-preparation.pdf>.

## NIST SPECIAL PUBLICATION 1800-19C

---

# Trusted Cloud:

## Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments

---

### Volume C: How-to Guides

**Michael Bartock**  
**Murugiah Souppaya**  
NIST

**Daniel Carroll**  
**Robert Masten**  
Dell/EMC

**Gina Scinta**  
**Paul Massis**  
Gemalto

**Harmeet Singh**  
**Rajeev Ghandi**  
**Laura E. Storey**  
IBM

**Raghuram Yeluri**  
Intel

**Michael Dalton**  
**Rocky Weber**  
RSA

**Karen Scarfone**  
Scarfone Cybersecurity

**Anthony Dukes**  
**Jeff Haskins**  
**Carlos Phoenix**  
**Brenda Swarts**  
VMware

April 2022

FINAL

This publication is available free of charge from <https://doi.org/10.6028/NIST.SP.1800-19>

The draft publication is available free of charge from  
<https://www.nccoe.nist.gov/projects/trusted-cloud-vmware-hybrid-cloud-iaas-environments>



## DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk through outreach and application of standards and best practices, it is the stakeholder's responsibility to fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise, and the impact should the threat be realized before adopting cybersecurity measures such as this recommendation.

National Institute of Standards and Technology Special Publication 1800-19C, Natl. Inst. Stand. Technol. Spec. Publ. 1800-19C, 125 pages, (April 2022), CODEN: NSPUE2

## FEEDBACK

As a private-public partnership, we are always seeking feedback on our practice guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at [trusted-cloud-nccoe@nist.gov](mailto:trusted-cloud-nccoe@nist.gov).

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence  
National Institute of Standards and Technology  
100 Bureau Drive  
Mailstop 2002  
Gaithersburg, MD 20899  
Email: [nccoe@nist.gov](mailto:nccoe@nist.gov)

## NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

To learn more about the NCCoE, visit <https://www.nccoe.nist.gov/>. To learn more about NIST, visit <https://www.nist.gov>.

## NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

## ABSTRACT

A *cloud workload* is an abstraction of the actual instance of a functional application that is virtualized or containerized to include compute, storage, and network resources. Organizations need to be able to monitor, track, apply, and enforce their security and privacy policies on their cloud workloads, based on business requirements, in a consistent, repeatable, and automated way. The goal of this project is to develop a trusted cloud solution that will demonstrate how trusted compute pools leveraging hardware roots of trust can provide the necessary security capabilities. These capabilities not only provide assurance that cloud workloads are running on trusted hardware and in a trusted geolocation or logical boundary, but also improve the protections for the data in the workloads and in the data flows between



workloads. The example solution leverages modern commercial off-the-shelf technology and cloud services to address lifting and shifting a typical multi-tier application between an organization-controlled private cloud and a hybrid/public cloud over the internet.

## KEYWORDS

*cloud technology; compliance; cybersecurity; privacy; trusted compute pools*

## ACKNOWLEDGMENTS

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Technology Partner/Collaborator	Build Involvement
<a href="#">Dell EMC</a>	Server, storage, and networking hardware
<a href="#">Gemalto (A Thales Company)</a>	Hardware security module (HSM) for storing keys
<a href="#">HyTrust (An Entrust Company)</a>	Asset tagging and policy enforcement, workload and storage encryption, and data scanning
<a href="#">IBM</a>	Public cloud environment with IBM-provisioned servers
<a href="#">Intel</a>	Intel processors in the Dell EMC servers
<a href="#">RSA</a>	Multifactor authentication, network traffic monitoring, and dashboard and reporting
<a href="#">VMware</a>	Compute, storage, and network virtualization capabilities

## DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms

“may” and “need not” indicate a course of action permissible within the limits of the publication. The terms “can” and “cannot” indicate a possibility and capability, whether material, physical, or causal.

## **PATENT DISCLOSURE NOTICE**

*NOTICE: The Information Technology Laboratory (ITL) has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.*

*As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.*

*No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.*

## Contents

<b>1</b>	<b>Introduction.....</b>	<b>1</b>
1.1	Practice Guide Structure.....	1
1.2	Build Overview.....	2
1.3	Typographic Conventions .....	3
1.4	Logical Architecture Summary .....	3
<b>2</b>	<b>Dell EMC Product Installation and Configuration Guide .....</b>	<b>5</b>
2.1	Dell EMC Unity Hardening Guidance .....	5
2.2	Dell Networking S4048-ON, S3048-ON, OS9 Hardening .....	6
2.2.1	Functionality and interoperability (layer 3 access).....	11
2.2.2	VLANs.....	16
2.3	Dell PowerEdge Hardening .....	20
2.4	Avamar Security Hardening .....	20
<b>3</b>	<b>Gemalto Product Installation and Configuration Guide .....</b>	<b>21</b>
3.1	Gemalto Luna 6 Initialization .....	21
3.2	Create HSM Partition .....	22
<b>4</b>	<b>HyTrust Product Installation and Configuration Guide .....</b>	<b>23</b>
4.1	HyTrust KeyControl Setup.....	23
4.2	HyTrust DataControl Setup .....	24
4.3	HyTrust CloudControl Appliance Setup.....	24
4.3.1	Provisioning PolicyTags.....	25
4.3.2	Policy Interaction .....	27
4.4	HyTrust CloudAdvisor Appliance Setup.....	27
<b>5</b>	<b>IBM Product Installation and Configuration Guide.....</b>	<b>27</b>
5.1	ICSV Deployment .....	28
5.1.1	Pre-deployment .....	29
5.1.2	Automation deployment .....	31

5.1.3	Post-deployment .....	33
5.2	Enable Hardware Root of Trust on ICSV Servers .....	37
5.2.1	Enable Managed Object Browser (MOB) for each ESXi Server .....	37
5.2.2	Enable TPM/TXT on SuperMicro hosts .....	37
5.2.3	Enable TPM/TXT in IBM Cloud .....	38
5.2.4	Validate the TPM/TXT is enabled .....	39
5.2.5	Check the vCenter MOB to see if the TPM/TXT is enabled .....	39
5.2.6	Set up Active Directory users and groups .....	40
5.2.7	Join vCenter to the AD domain .....	44
5.2.8	Add AD HyTrust-vCenter service user to vCenter as Administrator .....	45
5.2.9	Add AD HyTrust-vCenter service user to vCenter Global Permissions .....	46
5.2.10	Configure HTCC for AD authentication .....	47
5.3	Add Hosts to HTCC and Enable Good Known Host (GKH) .....	48
<b>6</b>	<b>Intel Product Installation and Configuration Guide .....</b>	<b>50</b>
<b>7</b>	<b>RSA Product Installation and Configuration Guide .....</b>	<b>50</b>
7.1	RSA SecurID .....	50
7.2	RSA NetWitness .....	51
7.2.1	Configure the VMware ESX/ESXi Event Source .....	51
7.2.2	Configure the RSA NetWitness Log Collector for VMware Collection .....	52
<b>8</b>	<b>VMware Product Installation and Configuration Guide .....</b>	<b>52</b>
8.1	Prerequisites .....	53
8.2	Installation and Configuration .....	55
8.3	Configuration Customization Supporting the Use Cases and Security Capabilities ....	55
8.3.1	Example VVD 5.0.1 Configuration: Configure the Password and Policy Lockout Setting in vCenter Server in Region A .....	56
8.3.2	Example VVD 5.0.1 Configuration: Configure Encryption Management in Region A .....	57
8.3.3	Example vRealize Automation DISA STIG Configuration: Configure SLES for vRealize to protect the confidentiality and integrity of transmitted information .....	58
8.3.4	Example vRealize Operations Manager DISA STIG Configuration: Configure the vRealize Operations server session timeout .....	58

8.4	Operation, Monitoring, and Maintenance .....	58
8.4.1	Operation.....	58
8.4.2	Monitoring .....	59
8.4.3	Maintenance .....	60
8.5	Product Configuration Overview .....	62
<b>Appendix A Security Configuration Settings.....</b>		<b>65</b>
<b>Appendix B List of Acronyms .....</b>		<b>121</b>
<b>Appendix C Glossary .....</b>		<b>125</b>

## List of Figures

Figure 1-1: High-Level Solution Architecture .....	5
Figure 5-1: Reference Architecture for ICSV.....	29
Figure 7-1: RSA Authentication Manager Deployment Architecture .....	51
Figure 8-1: Map of VVD Documentation.....	54

## List of Tables

Table 5-1: Example of IBM Cloud Contact Information Template.....	30
Table 5-2: ICSV Requirement & Deployment Template .....	30
Table 5-3: Examples of HTCC Configuration Parameters .....	34
Table 5-4: Examples of Additional HTCC Configuration Parameters .....	35
Table 8-1: Summary of VVD Version and Associated Bill of Materials (Product Versions) .....	60
Table 8-2: Configuration Items Without Control Mappings.....	63

# 1 Introduction

The following volumes of this guide show information technology (IT) professionals and security engineers how we implemented this example solution. We cover all of the products employed in this reference design. We do not re-create the product manufacturers' documentation, which is presumed to be widely available. Rather, these volumes show how we incorporated the products together in our environment.

*Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.*

## 1.1 Practice Guide Structure

This National Institute of Standards and Technology (NIST) Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate a trusted cloud solution using trusted compute pools leveraging hardware roots of trust to provide the necessary security capabilities. This reference design is modular and can be deployed in whole or in part.

This guide contains three volumes:

- NIST SP 1800-19A: *Executive Summary*
- NIST SP 1800-19B: *Approach, Architecture, and Security Characteristics* – what we built and why
- NIST SP 1800-19C: *How-To Guides* – instructions for building the example solution (**you are here**)

Depending on your role in your organization, you might use this guide in different ways:

**Business decision makers, including chief security and technology officers**, will be interested in the *Executive Summary*, NIST SP 1800-19A, which describes the following topics:

- challenges that enterprises face in protecting cloud workloads in hybrid cloud models
- example solution built at the NCCoE
- benefits of adopting the example solution

**Technology or security program managers** who are concerned with how to identify, understand, assess, and mitigate risk will be interested in *NIST SP 1800-19B*, which describes what we did and why. The following sections will be of particular interest:

- Section 3.4.3, Risk, describes the risk analysis we performed.
- Appendix A, Mappings, maps the security characteristics of this example solution to cybersecurity standards and best practices.

You might share the *Executive Summary, NIST SP 1800-19A*, with your leadership team members to help them understand the importance of adopting standards-based trusted compute pools in a hybrid cloud model that provide expanded security capabilities.

**IT professionals** who want to implement an approach like this will find the whole practice guide useful. You can use this How-To portion of the guide, *NIST SP 1800-19C*, to replicate all or parts of the build created in our lab. This How-To portion of the guide provides specific product installation, configuration, and integration instructions for implementing the example solution.

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a trusted cloud implementation leveraging commercial off-the-shelf technology. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and best practices. Section 4.2, Technologies, in *NIST SP 1800-19B* lists the products that we used and maps them to the cybersecurity controls provided by this reference solution.

A NIST Cybersecurity Practice Guide does not describe “the” solution, but a possible solution. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to [trusted-cloud-nccoe@nist.gov](mailto:trusted-cloud-nccoe@nist.gov).

## 1.2 Build Overview

The NCCoE worked with its build team partners to create a lab demonstration environment that includes all of the architectural components and functionality described in Section 4 of *NIST SP 1800-19B*. The following use case scenarios were demonstrated in the lab environment:

1. Demonstrate control and visibility for the trusted hybrid cloud environment
2. Demonstrate control of workloads and data security
3. Demonstrate a workload security policy in a hybrid cloud
4. Demonstrate recovery from an unexpected infrastructure outage
5. Demonstrate providing visibility into network traffic patterns
6. Demonstrate application zero trust

## 1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
<i>Italics</i>	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the <i>NCCoE Style Guide</i> .
<b>Bold</b>	names of menus, options, command buttons, and fields	Choose <b>File &gt; Edit</b> .
Monospace	command-line input, onscreen computer output, sample code examples, and status codes	<code>mkdir</code>
<b>Monospace Bold</b>	command-line user input contrasted with computer output	<b><code>service sshd start</code></b>
<a href="#">blue text</a>	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at <a href="https://www.nccoe.nist.gov">https://www.nccoe.nist.gov</a> .

## 1.4 Logical Architecture Summary

At a high level, the trusted cloud architecture has three main pieces: a private cloud hosted at the NCCoE, an instance of the public IBM Cloud Secure Virtualization (ICSV), and an Internet Protocol Security (IPsec) virtual private network (VPN) that connects the two clouds to form a hybrid cloud.

The private on-premises cloud at the NCCoE consists of the following components:

- Hardware Security Module (HSM) for storing keys by Gemalto
- server, storage, and networking hardware by Dell EMC
- Intel processors in the Dell EMC servers
- compute, storage, and network virtualization capabilities by VMware
- asset tagging and policy enforcement, workload and storage encryption, and data scanning by HyTrust
- multifactor authentication, network traffic monitoring, and dashboard and reporting by RSA



The ICSV instance consists of the following components:

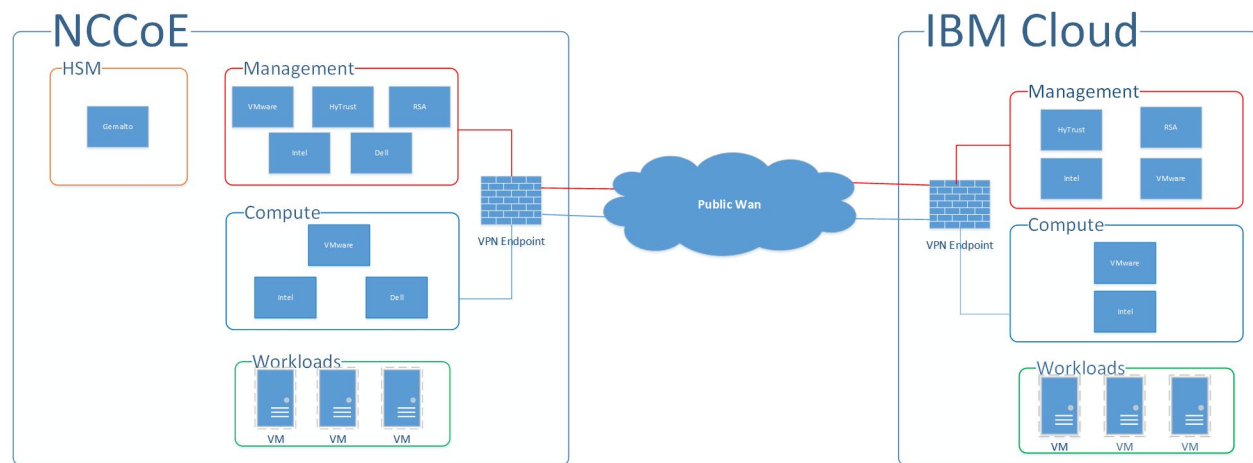
- IBM-provisioned servers with Intel processors
- compute, storage, network virtualization with VMware components
- asset tagging and policy enforcement, and workload and storage encryption with HyTrust components

The IPsec VPN established between the two clouds allows them to be part of the same management domain, so that each component can be managed and utilized in the same fashion, which creates one hybrid cloud. The workloads can be shifted or live-migrated between the two sites.

[Figure 1-1](#) shows the high-level architecture. It depicts the four main components that comprise the build:

- **HSM component:** This build utilizes HSMs to store sensitive keys within the environment.
- **Management component:** Identical functional management components are instantiated within each cloud instance. At a minimum, each management component includes VMware running the virtualization stack, HyTrust providing the asset tagging policy enforcement aspect, and RSA providing network-visibility, dashboard, and reporting capabilities. The management components are connected through the VPN to represent one logical management element.
- **Compute component:** The compute components host the tenant workload virtual machines (VMs). Asset tagging is provisioned on the compute servers so that policy can be assigned and enforced to ensure that tenant workloads reside on servers that meet specific regulatory compliance requirements.
- **Workload component:** The workload components include VMs, data storage, and networks owned and operated by the tenant and data owner. Policies are applied to the workloads to ensure that they can run only on servers that meet specific requirements, such as asset tag policies.

Figure 1-1: High-Level Solution Architecture



## 2 Dell EMC Product Installation and Configuration Guide

This section lists all prerequisites that must be met before the Dell EMC product installation and configuration can take place. This includes dependencies on any other parts of the example solution. It is recommended to download the latest security and hardening documentation from the Dell Technologies support site for the following products:

- Dell PowerEdge R740xD
- Dell EMC Unity
- Dell Networking S3048/4048-ON Networking
- Dell Avamar
- Dell Data Domain

This section explains how to install and configure the Dell EMC products and hardening guides. It points to existing documentation whenever possible, so this document only includes supplemental information, such as configuration settings recommended for the example solution that differ from the defaults.

### 2.1 Dell EMC Unity Hardening Guidance

Dell EMC utilizes a derivative of SUSE Linux 12 for its embedded operating system (OS) to manage the hardware and provide storage device services. Dell EMC Unity has a simple command-line capability to enable security hardening that meets the guidelines of the SUSE Linux 12 Security Technical Implementation Guide (STIG). Some of the hardening steps to meet STIG requirements are turned on by running service scripts.

Dell EMC Unity Data at Rest Encryption (D@RE) protects against unauthorized access to lost, stolen, or failed drives by ensuring all sensitive user data on the system is encrypted as it is written to disk. It does this through hardware-based encryption modules located in the serial attached SCSI (SAS) controllers and 12 gigabits per second (Gb/s) SAS IO modules which encrypt data as it is written to the back-end drives, and decrypt data as it is retrieved from these drives.

To enable and configure D@RE, first read the [Dell EMC Unity: Data at Rest Encryption paper](#) and follow the instructions in these sections:

- Enabling D@RE
- Enabling External Key Management
- Keystore Backup
- Audit Log and Checksum Retrieval

Next, configure the storage system to enable Federal Information Processing Standards (FIPS) 140-2 mode for the Transport Layer Security (TLS) modules that encrypt client management traffic. Directions for doing so are in the “Management support for FIPS 140-2” section of Chapter 4 of the [Dell EMC Unity Family Security Configuration Guide](#). Finally, to enable STIG mode on the Dell EMC Unity system (for physical deployments only), follow the three steps, in order, for hardening your storage system in the “Manage STIG mode” section of Chapter 8 in the same Security Configuration Guide.

## 2.2 Dell Networking S4048-ON, S3048-ON, OS9 Hardening

This section provides example configurations for release 9.14(1.0) on the S3048-ON and shows how to configure the Dell EMC Networking system in accordance with applicable DISA STIGs and DoD Unified Capabilities Requirements (UCR) 2013 Errata-1. For more information on configuring the S3048-ON, see the [Dell EMC Configuration Guide for the S3048-ON System](#).

Configure the following features in the specified order. After you configure these features, configure the Functionality and Interoperability (Layer 2 Access) or Functionality and Interoperability (Layer 3 Access) features. For information about using the command line interface (CLI), see the Configuration Fundamentals and Getting Started sections in the Dell Networking Configuration Guide for your platform, or use the [Dell Command Line Reference Guide for the S3048-ON System](#). To access all documentation for release 9.14, go to <https://www.dell.com/support/home/en-us/product-support/product/dell-emc-os-9/docs>.

1. Set the hostname:  

```
hostname NCCOE-S4048-01
```
2. Configure password policies:

- a. Define the minimum security policy to create passwords. Ensure that the password attributes match your organization's security policy.

```
password-attributes min-length 15 character-restriction lower 2
character-restriction upper 2 character-restriction numeric 2 character-
restriction special 2
```

- b. Set up the login lockout period to match your organization's security policy:

```
password-attributes lockout-period 15
```

- c. Enable password with highest privileges:

```
enable password level 15 <clear-text password>
```

3. To enable FIPS cryptography mode, enter this command:

```
fips mode enable
```

**Note:** Enable FIPS mode before you configure the features below. If you do not, the system will clear some of the configuration, and you must reconfigure some of the features.

**Note:** If the system fails to transition to FIPS mode, the system is not in a compliant state.

4. Enable SSH server:

```
ip ssh server cipher aes128-ctr aes192-ctr aes256-ctr
ip ssh server enable
ip ssh server mac hmac-sha1 hmac-sha2-256
```

5. Disable telnet server:

```
no ip telnet server enable
```

6. Define content addressable memory (CAM) allocation and optimization. CAM is a type of memory that stores information in the form of a lookup table. These CAM settings are required to configure a conformant IPv4 and IPv6 solution.

```
cam-acl 12acl 2 ipv4acl 2 ipv6acl 4 ipv4qos 2 12qoa 1 12pt 0 ipmacacl 0 vman-
qos cfmact 0 fedgova1
```

7. Enforce authentication and authorization of users connecting to system through the console or SSH, and then set the timer for terminating a session after 10 minutes of inactivity.

```
login authentication ucraaa_console
exec-timeout 10 0
authorization exec ucraaa_console
line vty 0
login authentication ucraaa_vty
exec-timeout 10 0
authorization exec ucraaa_vty
line vty 1
login authentication ucraaa_vty
```

```

exec-timeout 10 0
authorization exec ucraaa_vty
line vty 2
login authentication ucraaa_vty
exec-timeout 10 0
authorization exec ucraaa_vty
line vty 3
login authentication ucraaa_vty
exec-timeout 10 0
authorization exec ucraaa_vty
line vty 4
login authentication ucraaa_vty
exec-timeout 10 0
authorization exec ucraaa_vty
line vty 5
login authentication ucraaa_vty
exec-timeout 10 0
authorization exec ucraaa_vty
line vty 6
login authentication ucraaa_vty
exec-timeout 10 0
authorization exec ucraaa_vty
line vty 7
login authentication ucraaa_vty
exec-timeout 10 0
authorization exec ucraaa_vty
line vty 8
login authentication ucraaa_vty
exec-timeout 10 0
authorization exec ucraaa_vty
line vty 9
login authentication ucraaa_vty
exec-timeout 10 0
authorization exec ucraaa_vty

```

**8. Define a role-based user supplying an encrypted password:**

```
username admin password 7 888dc89d1f1bca2882895c1658f993e7 privilege 15
```

**9. Limit open Transmission Control Protocol (TCP) connections by defining the wait duration for TCP connections as nine seconds:**

```
ip tcp reduced-syn-ack-wait
```

**10. Define the IPv4 static route:**

```
ip route 0.0.0.0/0 192.168.101.1
```

**11. Configure IPv4 Open Shortest Path First (OSPF) routes:**

```

router ospf 101
router-id 192.168.101.3
network 192.168.101.0/24 area 101

```

```
area 101 nssa default-information-originate
redistribute bgp 65001
```

## 12. Configure Media Access Control (MAC) settings:

```
mac-address-table station-move refresh-arp
mac-address-table agint-time 1000000
```

## 13. Configure system and audit log settings, such as syslog version, buffer size, logging server, and coredump destination:

```
service timestamps log datetime localtime msec show-timezone
service timestamps debug datetime localtime msec show-timezone
!
logging coredump stack-unit 1
logging coredump stack-unit 2
logging coredump stack-unit 3
logging coredump stack-unit 4
logging coredump stack-unit 5
logging coredump stack-unit 6
!
```

## 14. Set up the Network Time Protocol (NTP):

```
ntp server 192.168.4.10
ntp server 192.168.4.11
```

## 15. Configure the login banner text:

```
banner login ^CYou are accessing a U.S. Government (USG) Information System
(IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent
to the following conditions:
-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement
(LE), and counterintelligence (CI) investigations.
-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are subject
to routine monitoring, interception, and search, and may be disclosed or used
for any USG-authorized purpose.
-This IS includes security measures (e.g., authentication and access controls)
to protect USG interests--not for your personal benefit or privacy.
-Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or services
by attorneys, psychotherapists, or clergy, and their assistants. Such
communications and work product are private and confidential.^C
```

## 16. Configure the switch to securely bring the software image to its flash drive. Define where to upgrade the software image to (flash drive) and where to boot the software image from.

```
boot system stack-unit 1 primary system://B
boot system stack-unit 1 secondary system://B
boot system stack-unit 1 default system://A
!
```

**17. Disable Support Assist:**

```
eula-consent support-assist reject
```

**18. Configure redundancy:**

```
redundancy auto-synchronize full
```

**19. Configure the loopback interface for management traffic:**

```
interface Loopback 0
description NCCOE-S4048-02
ip address 10.0.2.2/32
no shutdown
!
```

**20. Enter the File Transfer Protocol (FTP) source interface, for example Loopback 1:**

```
ip ftp source-interface loopback 1
```

**21. Enter the clock timezone for your system:**

```
clock timezone Eastern -5
clock summer-time Eastern recurring 2 Sun Mar 02:00 1 Sun Nov 02:00
!
```

**22. To disable IP source routing, enter the following command:**

```
no ip source-route
```

**23. Configure reload behavior:**

```
reload-type
boot-type normal-reload
config-scr-download enable
vendor-class-identifier " "
!
```

**24. Enable login statistics:**

```
login concurrent-session limit 3
login statistics enable
!
```

**25. Configure the management interface:**

```
interface ManagementEthernet 1/1
description OOB_MGMT
ip address 10.10.10.11/24
```

```
no shutdown
!
```

### 2.2.1 Functionality and interoperability (layer 3 access)

This section describes how to configure functionality and interoperability using Layer 2. The example configurations shown in the following sections are based on the requirements in UCR 2013 Errata 1. Your site needs to update the configurations as the UCR requirements periodically change.

1. Configure the Link Layer Discovery Protocol (LLDP):

```
protocol lldp
advertise dot1-tlv port-vlan-id
advertise dot3-tlv max-frame-size
advertise management-tlv management-address system-capabilities system-
description system-name
advertise interface-port-desc
!
```

2. The following configurations create aggregated links and were applied to interfaces to enable link aggregation control protocol (LACP). The aggregated links were then subscribed to virtual local area networks (VLANs). For complete information about this feature, see the Port Channel Interfaces and Link Aggregation Control Protocol (LACP) sections in the Dell Networking Configuration Guide and the Dell Networking Command Line Reference Guide.

```
interface Port-channel 64
description LAG to IB-MGMT switches
no ip address
switchport
vlt-peer-lag port-channel 64
no shutdown
!
interface Port-channel 67
no ip address
mtu 9216
portmode hybrid
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
lacp fast-switchover
vlt-peer-lag port-channel 67
no shutdown
!
interface Port-channel 68
no ip address
mtu 9216
portmode hybrid
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
```



```

lacp fast-switchover
vlt-peer-lag port-channel 68
no shutdown
!
interface Port-channel 127
description VLTi
no ip address
channel-member fortyGigE 1/51,1/52
no shutdown
!

```

3. Apply input and output policies to physical interfaces. The following are the configurations in the NCCoE lab and can be run on the switch CLI as written to duplicate:

```

interface TenGigabitEthernet 1/1
description mgt-nccoe-esxi-01
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/2
description mgt-nccoe-esxi-02
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/3
description mgt-nccoe-esxi-03
no ip address
_ mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/4
description mgt-nccoe-esxi-04
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/5
description mgt-nccoe-esxi-01

```

```

no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/6
description mgt-nccoe-esxi-02
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/7
description mgt-nccoe-esxi-03
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/8
description mgt-nccoe-esxi-04
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/9
description comp-nccoe-esxi-01
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/10
description comp-nccoe-esxi-02
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!

```

```

interface TenGigabitEthernet 1/11
description comp-nccoe-esxi-03
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/12
description comp-nccoe-esxi-04
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/13
description comp-nccoe-esxi-01
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/14
description comp-nccoe-esxi-02
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/15
description comp-nccoe-esxi-03
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
no shutdown
!
interface TenGigabitEthernet 1/16
description comp-nccoe-esxi-04
no ip address
mtu 9216
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation

```

```

no shutdown
!
interface TenGigabitEthernet 1/31
description TO-UNITY-ARRAY
no ip address
mtu 9216
!
port-channel-protocol LACP
port-channel 68 mode active
no shutdown
!
interface TenGigabitEthernet 1/32
description TO-UNITY-ARRAY
no ip address
mtu 9216
!
port-channel-protocol LACP
port-channel 67 mode active
no shutdown
!
interface TenGigabitEthernet 1/47
description NorthBound Firewall X5
no ip address
switchport
no shutdown
!
interface TenGigabitEthernet 1/48
description IB-MGMT Switch Stack Port 49
no ip address
!
port-channel-protocol LACP
port-channel 64 mode active
no shutdown
interface fortyGigE 1/51
description VLTi
no ip address
no shutdown
!
interface fortyGigE 1/52
description VLTi
no ip address
no shutdown
!
interface fortyGigE 1/53
description to Spine Switch 4 Port 54
ip address 192.168.1.1/31
no shutdown
!
interface fortyGigE 1/54
description to Spine Switch 3 Port 54
ip address 192.168.2.1/31
no shutdown

```

```

!
interface Port-channel 64
description LAG to IB-MGMT Switches
no ip address
switchport
vlt-peer-lag port-channel 64
no shutdown
!
interface Port-channel 67
no ip address
mtu 9216
portmode hybrid
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
lacp fast-switchover
vlt-peer-lag port-channel 67
no shutdown
!
interface Port-channel 68
no ip address
mtu 9216
portmode hybrid
switchport
spanning-tree rstp edge-port bpduguard shutdown-on-violation
spanning-tree 0 portfast bpduguard shutdown-on-violation
lacp fast-switchover
vlt-peer-lag port-channel 68
no shutdown
!
interface Port-channel 127
description VLTi
no ip address
channel-member fortyGigE 1/51,1/52
no shutdown
!
interface Port-channel 128
no ip address
shutdown
!

Honor 802.1p markings on incoming traffic and assign them to a default queue
service-class dynamic dot1p

Include overhead fields in rate-metering calculations
qos-rate-adjust 20

```

## 2.2.2 VLANs

Define the network-specific VLAN interfaces. For complete information about this feature, see the Virtual LANs (VLANs) section in the Dell Networking Configuration Guide and the Dell Networking

Command Line Reference Guide. The following are the configurations in the NCCoE lab and can be run on the switch CLI as written to duplicate:

```
interface Vlan 1
!untagged Port-channel 67-68,127
!
interface Vlan 101
ip address 192.168.101.3/24
untagged TenGigabitEthernet 1/47
!
vrrp-group 101
virtual-address 192.168.101.2
no shutdown
!
interface Vlan 103
no ip address
shutdown
!
interface Vlan 104
description nccoe-m01-vds01-managemnt
ip address 192.168.4.252/24
tagged TenGigabitEthernet 1/1-1/16,1/21
tagged Port-channel 64,127
!
vrrp-group 104
priority 254
virtual-address 192.168.4.254
no shutdown
!
interface Vlan 110
description nccoe-m01-vds01-nfs
ip address 192.168.10.252/24
tagged TenGigabitEthernet 1/1-1/16,1/21
tagged Port-channel 67-68,127
!
vrrp-group 110
priority 254
virtual-address 192.168.10.254
no shutdown
!
interface Vlan 120
description nccoe-m01-vds01-vmotion
ip address 192.168.20.252/24
tagged TenGigabitEthernet 1/1-1/8
tagged Port-channel 127
!
vrrp-group 120
priority 254
virtual-address 192.168.20.254
no shutdown
!
interface Vlan 130
```

```

description nccoe-m01-vds01-vsan
ip address 192.168.30.252/24
tagged TenGigabitEthernet 1/1-1/8
tagged Port-channel 127
!
vrrp-group 130
priority 254
virtual-address 192.168.30.254
no shutdown
!
interface Vlan 140
description nccoe-m01-vds01-replication
ip address 192.168.40.252/24
tagged TenGigabitEthernet 1/1-1/8
tagged Port-channel 127
!
vrrp-group 140
priority 254
virtual-address 192.168.40.254
no shutdown
!
interface Vlan 150
description VTEP VLAN
ip address 192.168.50.252/24
tagged TenGigabitEthernet 1/1-1/16
tagged Port-channel 127
!
vrrp-group 150
priority 254
virtual-address 192.168.50.254
no shutdown
!
interface Vlan 160
description nccoe-m01-vds01-uplink01
ip address 192.168.60.252/24
tagged TenGigabitEthernet 1/1-1/16
!
vrrp-group 160
priority 254
virtual-address 192.168.60.254
no shutdown
!
interface Vlan 180
description nccoe-m01-vds01-ext-management
no ip address
tagged TenGigabitEthernet 1/1-1/16
tagged Port-channel 127
no shutdown
!
interface Vlan 210
description nccoe-w01-vds01-nfs
ip address 192.168.210.252/24

```

```

tagged TenGigabitEthernet 1/1-1/16
tagged Port-channel 127
!
vrrp-group 210
priority 254
virtual-address 192.168.210.254
no shutdown
!
interface Vlan 220
description nccoe-w01-vds01-vmotion
ip address 192.168.220.252/24
tagged TenGigabitEthernet 1/9-1/16
tagged Port-channel 127
!
vrrp-group 220
priority 254
virtual-address 192.168.220.254
no shutdown
!
interface Vlan 230
description nccoe-w01-vds01-vsan
ip address 192.168.230.252/24
tagged TenGigabitEthernet 1/9-1/16
tagged Port-channel 127
!
vrrp-group 230
priority 254
virtual-address 192.168.230.254
no shutdown
!
interface Vlan 240
description VTEP VLAN
ip address 192.168.240.252/24
tagged TenGigabitEthernet 1/1-1/16
tagged Port-channel 127
!
vrrp-group 240
priority 254
virtual-address 192.168.240.254
no shutdown
!
interface Vlan 1000
description collapsed leaf edge bgp peering network
ip address 192.168.100.1/24
no shutdown
!
interface Vlan 1110
description nccoe-w01-vds01-uplink01
ip address 192.168.110.252/24
tagged TenGigabitEthernet 1/1-1/16
!
vrrp-group 111

```



```
priority 254
virtual-address 192.168.110.254
no shutdown
!
```

## 2.3 Dell PowerEdge Hardening

Unified Extensible Firmware Interface (UEFI) Secure Boot is a technology that secures the boot process by verifying if the drivers and OS loaders are signed by the key that is authorized by the firmware. When enabled, Secure Boot makes sure that:

- the BIOS boot option is disabled;
- only UEFI-based OSs are supported for OS deployment in all management applications; and
- only authenticated EFI images and OS loaders are started from UEFI firmware.

You can enable or disable the Secure Boot attribute locally or remotely using Dell EMC management applications. Lifecycle Controller supports deploying an OS with the Secure Boot option only in the UEFI boot mode.

There are two BIOS attributes that are associated with Secure Boot:

- **Secure Boot** — Displays if the **Secure Boot** is enabled or disabled.
- **Secure Boot Policy** — Allows you to specify the policy or digital signature that the BIOS uses to authenticate. The policy can be classified as:
  - **Standard** — The BIOS uses the default set of certificates to validate the drivers and OS loaders during the boot process.
  - **Custom** — The BIOS uses the specific set of certificates that you import or delete from the standard certificates to validate the drivers and OS loaders during the boot process.

**Note:** The secure boot policy settings made in the BIOS can also be changed on the Lifecycle Controller graphical user interface (GUI).

## 2.4 Avamar Security Hardening

Avamar servers running the SUSE Linux Enterprise Server (SLES) OS can implement various server security hardening features. These features are primarily targeted at customers needing to comply with DoD STIGs for Unix requirements. The following are specific steps to harden different components and services on the Avamar server. All come from Chapter 7 of the [Dell EMC Avamar Product Security Guide](#).

1. Disabling Samba (under “Level-1 security hardening”)
2. Preventing unauthorized access to GRUB configuration (under “Level-1 security hardening”)
3. Preventing the OS from loading USB storage (under “Level-1 security hardening”)

4. Updating OpenSSH (under “Level-3 security hardening”)
5. Disabling RPC (under “Level-3 security hardening”)
6. Configuring the firewall to block access to port 9443 (under “Level-3 security hardening”)
7. Changing file permissions (under “Level-3 security hardening”)

## 3 Gemalto Product Installation and Configuration Guide

This section describes the steps and commands to configure the Gemalto Luna 6 HSM and create partitions on it for networked servers to use.

### 3.1 Gemalto Luna 6 Initialization

The following commands are for initializing the system and configuring the Luna HSM networking. When the system is logged into for the first time, the default user is `admin` and the password is `PASSWORD`. A prompt is immediately presented upon successful login to change the default password. Once the password is changed, run the following commands for configuration purposes:

1. Set the time zone to US Eastern:

```
sysconf timezone set US/Eastern
```

2. Set the date/time format:

```
syscont time HH:MM YYMMDD
```

3. Set the hostname:

```
net hostname TCHSM
```

4. Set the Domain Name System (DNS) server:

```
net dns add nameserver 172.16.1.11
```

5. Set the network interface card (NIC) configuration for eth0 on the HSM:

```
net interface -device eth0 -ip 172.16.1.22 -netmask 255.255.255.0 -gateway  
172.16.1.254
```

Perform the following steps to generate and use a new HSM server certificate:

1. Generate the certificate:

```
sysconf regenCert
```

2. Bind the cert to eth0:

```
ntls bind eth0
```

3. Verify the status of Network Trust Links (NTLS):

```
ntls show
```

The following commands initialize the HSM and set up policies for logging in and which algorithms it can use:

1. Initialize the HSM and set the login timeout:

```
hsm PED timeout set -type -seconds 300
```

2. Next, log in as Security Officer:

```
hsm init -label NCCoE_Lab
```

3. Policy 12 controls non-FIPS compliant algorithms. Setting the value to zero disables any non-FIPS compliant algorithms:

```
hsm changePolicy -policy 12 -v 0
```

## 3.2 Create HSM Partition

The following steps create the individual partition in the HSM that will be used for the HyTrust KeyControl cluster to use as its key management system (KMS):

1. `hsm login`

2. Create the HSM partition to be used for KeyControl:

```
partition create -partition HyTrust_KeyControl
```

3. Set the password for the newly created partition:

```
partition changePW -partition HyTrust_KeyControl -newpw <new password> -oldpw  
<old password>
```

4. Allow activation:

```
partition changePolicy -partition HyTrust_KeyControl -policy 22 -v 1
```

5. Allow auto-activation:

```
partition changePolicy -partition HyTrust_KeyControl -policy 23 -v 1
```

6. Activate the newly created partition:

```
partition activate -partition HyTrust_KeyControl
```

7. Show partition serial number for high availability:

```
partition show
```

## 4 HyTrust Product Installation and Configuration Guide

This build implemented the HyTrust KeyControl, DataControl, CloudControl, and CloudAdvisor appliances. The following subsections show how the installation and configurations were performed, as well as how they were integrated with other components in the build.

### 4.1 HyTrust KeyControl Setup

First, follow the directions on these pages:

1. [Installing KeyControl from an OVA Template \(note: OVA stands for open virtual appliance\)](#)
2. [Configuring the First KeyControl Node \(OVA Install\)](#)
3. [Adding a New KeyControl Node to an Existing Cluster \(OVA Install\)](#)

Next, in order to use the Gemalto Luna HSM as the KMS server to protect its keys, there must be connectivity between KeyControl and the HSM. To configure the HSM in KeyControls:

1. Log in to the web user interface (UI) and click the **SETTINGS** button.
2. Once in the **Settings** menu, click on the “**HSM Server Settings**” link to configure the HSM.
3. Enter in the following information for the Gemalto Luna HSM:
  - hostname or IP address
  - partition label that was created in the Gemalto steps
  - partition password
  - server certificate file
  - client name for this KeyControl server
4. When the information is entered correctly and the KeyControl server can communicate with and authenticate to the Gemalto HSM, the state will show as “**ENABLED**”.

State:	ENABLED
Hostname:	172.16.1.22
Partition Label:	HyTrust_KeyControl
Partition Password:	Change
Server Certificate:	<a href="#">Browse</a>
Client Name:	HTKC01

[Client Certificate](#) [Test](#)

## 4.2 HyTrust DataControl Setup

Follow the directions on these pages:

1. [Creating a Cloud VM Set](#)
2. [Installing \[the Policy Agent\] Interactively on Windows](#)
3. [Registering the Policy Agent Using the HyTrust Policy Agent GUI](#)
4. [Encrypting a Disk Using the webGUI](#)

## 4.3 HyTrust CloudControl Appliance Setup

Follow the directions on these pages:

1. [Overview](#)
2. [Installing from an OVA File](#)
3. [Configuring the Management Interface](#)
4. [Configuring the Management Console](#)
5. Configuring High Availability
  - a. [HA Overview](#)
  - b. [High Availability Configuration Modes](#)
  - c. [High Availability Considerations and Limitations](#)
  - d. [High Availability Setup and Configuration](#)
  - e. [Default Configuration](#)

6. Adding Hosts to CloudControl
  - a. [Protected Hosts](#)
  - b. [Adding a Host](#)
7. [Configuring Managed Hosts](#)
8. [Enabling a Good Known Host](#)
9. [Verify and Update Host Trust](#) (and [Host Icons Used in CloudControl](#))

For more information on PolicyTags provisioning and evaluation, see the “PolicyTags Provisioning” section in chapter 6 of the [Administration Guide for HyTrust CloudControl](#).

### 4.3.1 Provisioning PolicyTags

To provision the PolicyTags, you need to perform the following tasks:

1. Collect the UUID (Universally Unique Identifier) information for each Trusted host.
2. Generate and run the `esxcli` commands for hardware provisioning for each Trusted host.
3. Verify that the PolicyTags are provisioned.

#### 4.3.1.1 Collect UUIDs of Good Known Hosts (GKHs) and Trusted Hosts

The UUID information for the GKHs and Trusted hosts can be collected from the vCenter Managed Object Browser (MOB). You will need to obtain the UUID for each GKH and Trusted host.

1. Log into the vCenter Managed Object Browser at `https://<VSPHERE_URL>/mob`.
2. Perform the following series of page selections to reach the host page for each of your Intel TXT-enabled hosts:

Managed Object ID (page)	NAME (selection row)	VALUE (link to select)
ServiceInstance	Content	content
content	rootFolder	group-d#
group-d#	childEntity	datacenter-#
datacenter-#	hostFolder	group-h#
group-h#	childEntity	domain-c#
domain-c#	host	host-## (Intel TXT host)

3. On the **Hosts** page, click **Summary**.
4. On the **Summary** page, click **Hardware**. The **Hardware** page contains the UUID information.

5. Repeat this for each Trusted host.

#### 4.3.1.2 Generate *esxcli* Commands

Use the CloudControl cli to generate *esxcli* commands that can be used for hardware provisioning.

1. Log into CloudControl as the *ascadminuser*, and run the following command:

```
asc tas --export-certs
```

This generates a file in */tmp* in the following format: *export--xxxx-xx-xxx.tgz*

2. Navigate to the */tmp* folder and extract the file using the following command:

```
tar -xvf export--xxxx-xx-xxx.tgz
```

The extraction process lists several files, including the *sha1.bin* for each Trusted ESXi host.

Example:

```
export--2018-08-27T23-44-43Z/6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-dc27fe259e1a/system--6aa6af76-14f6-42e8-b452-dc27fe259e1a.der
```

```
export--2018-08-27T23-44-43Z/6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-dc27fe259e1a/system--6aa6af76-14f6-42e8-b452-dc27fe259e1a.sha1.bin
```

```
export--2018-08-27T23-44-43Z/6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-dc27fe259e1a/system--6aa6af76-14f6-42e8-b452-dc27fe259e1a.sha256.bin
```

```
export--2018-08-27T23-44-43Z/6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-dc27fe259e1a/system--6aa6af76-14f6-42e8-b452-dc27fe259e1a.metadata.txt
```

```
export--2018-08-27T23-44-43Z/dddafa66/314e/4378/8f4d/dddafa66-314e-4378-8f4d-060b5d885038/system--dddafa66-314e-4378-8f4d-060b5d885038.der
```

```
export--2018-08-27T23-44-43Z/dddafa66/314e/4378/8f4d/dddafa66-314e-4378-8f4d-060b5d885038/system--dddafa66-314e-4378-8f4d-060b5d885038.sha1.bin
```

```
export--2018-08-27T23-44-43Z/dddafa66/314e/4378/8f4d/dddafa66-314e-4378-8f4d-060b5d885038/system--dddafa66-314e-4378-8f4d-060b5d885038.sha256.bin
```

```
export--2018-08-27T23-44-43Z/dddafa66/314e/4378/8f4d/dddafa66-314e-4378-8f4d-060b5d885038/system--dddafa66-314e-4378-8f4d-060b5d885038.metadata.txt
```

3. Navigate to the extracted directory, for example:

```
cd /tmp/export--xxxx-xx-xxx
```

4. At the prompt, type the following command:

```
grep -E -- '(id|subject)' : ' json.dump | grep -A1 '<Trusted-Host-UUID> '
```

This command returns the “subject” and the “id.” Example:

```
"subject" : "4c4c4544-0032-3010-8035-b5c04f333832",
```

```
"id" : "6aa6af76-14f6-42e8-b452-dc27fe259e1a"
```

5. Run the following *hexdump* command for each Trusted host, where *<sha1.bin file path>* matches the “id” for the specific host:

```
hexdump -e '"esxcli hardware tpm tag set --data=" 20/1 "%1.2x" ";\n"' <sha1.bin  
file path>
```

This returns the `esxcli` command.

Example:

```
hexdump -e '"esxcli hardware tpm tag set --data=" 20/1 "%1.2x" ";\n"  
6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-dc27fe259e1a/system--6aa6af76-  
14f6-42e8-b452-dc27fe259e1a.sha1.bin  
  
esxcli hardware tpm tag set --data=46f048ce41afdfa686e4c00f9fd67a2b71d1c749;
```

#### 4.3.1.3 Run `esxcli` Commands

Run the `esxcli` commands for each Trusted host to provision the hardware tags.

1. Put the Trusted host into maintenance mode.
2. Log in to the ESXi host as `root`.
3. Run the specific `esxcli` command for the Trusted host. The command is part of the `hexdump` output.

Example:

```
esxcli hardware tpm tag set --data=46f048ce41afdfa686e4c00f9fd67a2b71d1c749;
```

4. Restart the ESXi host. The host should still be in maintenance mode.

#### 4.3.2 Policy Interaction

See the [Policy Interaction webpage](#) for more information on how policy enforcement works.

### 4.4 HyTrust CloudAdvisor Appliance Setup

Follow the directions on these pages:

1. [Deploying CloudAdvisor](#)
2. [Configuring the CloudAdvisor Virtual Appliance](#)
3. [Setting Up CloudAdvisor](#)
4. [Adding VMs to Inventory](#)

## 5 IBM Product Installation and Configuration Guide

This section covers all the aspects of installing and configuring the IBM products used to build the example solution. Note that the information in this section reflects product and service names, features, options, and configurations as of when the build was performed. The IBM products in this section are

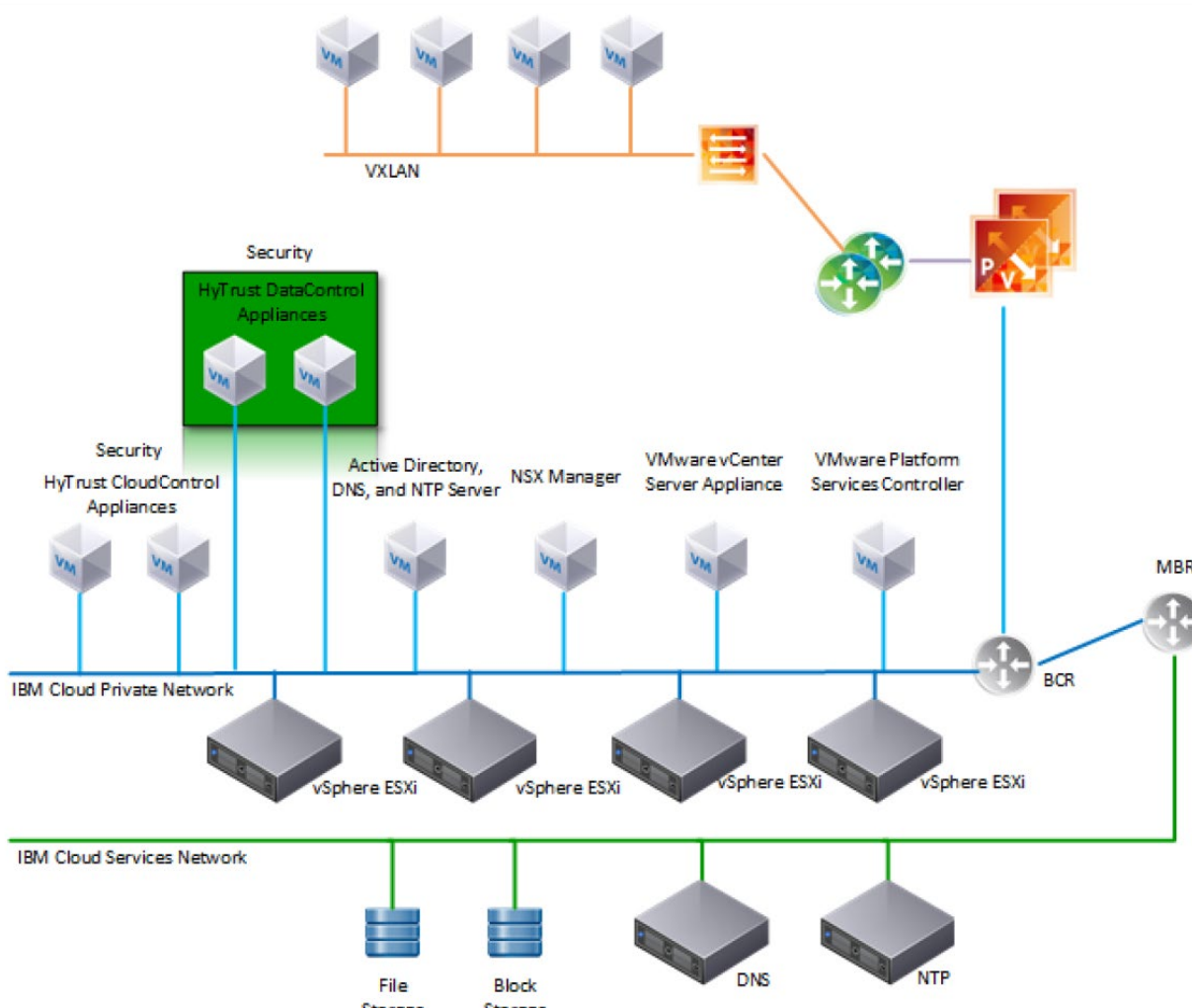


cloud-based with web-based documentation, and they do not use versioning conventions, so it is not possible to reference the documentation that was used during this build. As of this writing, the latest information from IBM is available through the IBM Cloud for VMware Solutions site at <https://www.ibm.com/cloud/vmware>.

## 5.1 ICSV Deployment

IBM Cloud Secure Virtualization (ICSV) combines the power of IBM Cloud, VMware Cloud Foundation, HyTrust security software, and Intel TXT-enabled hardware to protect virtualized workloads. ICSV is deployed on the IBM Cloud infrastructure according to a VMware, HyTrust, IBM, and Intel-validated design reference architecture. IBM Cloud Secure Virtualization is initially deployed as a four-node cluster within the choice of clients of available IBM Cloud Data Centers worldwide. [Figure 5-1](#) displays a reference architecture for ICSV that shows the separation between IBM Cloud services, ICSV provisioned infrastructure, and tenant VMs. ICSV utilizes the IBM Cloud Services Network to enable provisioning the IBM Cloud Private Network to a customer, which in turn protects the virtualized workloads.

Figure 5-1: Reference Architecture for ICSV



To deploy the ICSV reference architecture stack, IBM has streamlined the process in three phases for the customer.

### 5.1.1 Pre-deployment

This phase starts after the customer has agreed to purchase the ICSV stack in the IBM cloud and has identified the use cases using a workshop or IBM Garage methodology. For the NCCoE project, we had a good understanding of the use case and the capabilities provided by ICSV. To achieve success in all three phases, the IBM Services team filled out [Table 5-1](#) and [Table 5-2](#). The information provided in each table helped us with decisions in later steps.

**Table 5-1: Example of IBM Cloud Contact Information Template**

	Name	Email Address	Phone Number
Client Sponsor			
Client Technical Lead			
Client Oversight			
Client Sales Engineer			
IBM Account Exec			
IBM Sales Contact			
IBM OM Contact			
IBM Program Manager (PM)			
IBM Consultant			
Other IBMers			
Vendors info (if applicable)			

**Table 5-2: ICSV Requirement & Deployment Template**

Client Input Variables	Choices	Example Values
SoftLayer user id		<user_name> from IAAS
SoftLayer API key		<user_key> from IAAS
Deployment - VMware Cloud Foundation (VCF) or vCenter Server (VCS)	VCF or VCS	VCS
VCS deployment details		
Instance name	-	TrustedCld
# of hosts (min. 3)	3 to 20	4
Instance	Primary or Secondary	Primary
Host configuration	Small, Medium, Large, Custom	Custom
Cores	16, 24, 28, 36	24

Client Input Variables	Choices	Example Values
Intel core base	2.1, 2.2, 2.3 GHz	2.2 GHz
RAM	64 GB-1.5 TB	256 GB
Data center location	Dallas, DC, Boulder, etc.	Dallas
Data storage	NFS or VSAN	VSAN
Size of each data storage	1, 2, 4, 8, 12 TB	2 TB
Performance of file shares	2, 4, 10 IOPS/GB	NA
NFS version - v3.0 or v4.1 for shared drives		NA
Windows AD	VSI OR VM	VM
Host prefix	-	Esxi0
Domain name (used in Windows AD)	-	nccoe.lab
Sub domain (used by VM)	-	icsv
VM License	BYO or Purchase	Purchase
VM Vcenter Server License	-	Standard
VM vSphere License	-	Enterprise Plus
VM NSX License	-	Enterprise
Services to be added		
Veeam	Yes / No	No
F5	Yes / No	No
Fortinet Security Appliance	Yes / No	No
Fortinet Virtual Appliance	Yes / No	No
Zerto version 5.0	Yes / No	No
HyTrust DataControl	Yes / No	Yes
HyTrust CloudControl	Yes / No	Yes
IBM Spectrum Protect Plus	Yes / No	No

### 5.1.2 Automation deployment

The following are steps for ordering an ICSV instance through the IBM portal.

1. Log into the IBM Cloud infrastructure customer portal at <https://cloud.ibm.com/login>.

2. From the top left corner, select the “Hamburger” menu, then select **VMware** from the drop-down menu on the left side.
3. Click on **Settings** and make sure the correct application programming interface (API) key is entered before provisioning the solution.
4. On the **IBM Cloud for VMware Solutions** screen, select **VMware vCenter Server on IBM Cloud**.
5. On the next screen, select **vCenter Server** and click the **Create** button.
6. In the next window, type in the **Instance Name** and make sure **Primary Instance** is highlighted for Instance type. For the **Licensing** options, select **Include with purchase** for all of them. For the **NSX License**, select **Enterprise** from the drop-down menu.
7. Under **Bare Metal Server**:
  - a. For the **Data Center Location**, open the drop-down menu for **NA South** and select **DAL09**.
  - b. Select **Customized** since our workload needs a virtual storage area network (VSAN), which requires a minimum of a four-node cluster.
8. Under **Storage**:
  - a. Select **vSan Storage**.
  - b. Set the **Disk Type and Size** for vSAN Capacity Disks to **1.9 TB SSD SED**.
  - c. Select **2** from the drop-down menu for the **Number of vSAN Capacity Disks**.
  - d. For **vSAN License**, select **Include with purchase** and then choose **Enterprise** from the drop-down menu.

Preconfigured **Customized**

Dual Intel Xeon E5-2620 v4  
16 Cores  
2.1 GHz

**Dual Intel Xeon E5-2650 v4**  
24 Cores  
2.2 GHz

Dual Intel Xeon E5-2690 v4  
28 Cores  
2.6 GHz

Dual Intel Xeon Silver 4110 Processor  
16 Cores  
2.1 GHz

RAM  
256 GB 64 GB 1.5 TB

Number of Bare Metal Servers ①  
4

**Storage**

**vSAN Storage** NFS Storage

Disk Type and Size for vSAN Capacity Disks  
1.9 TB SSD SED

Number of vSAN Capacity Disks  
2

vSAN disks configuration is enabled only for customized hardware.

9. For the **Network Interface**, enter the following:
  - a. Hostname Prefix: `esxi`
  - b. Subdomain Label: `icsv`
  - c. Domain Name: `nccoe.lab`
10. Select **Order New VLANs**.
11. Under **DNS Configuration**, select **Two highly available dedicated Windows Server VMs on the management cluster**.
12. Under Services, remove **Veeam on IBM Cloud 9.5** and select **HyTrust CloudControl on IBM Cloud 5.3** and **HyTrust DataControl on IBM Cloud 4.1**.
13. Click on the **Provision** button in the bottom right-hand corner. This will begin the provisioning process for the selected topology. It can take roughly 24 hours to complete the automation deployment. Once deployment has completed, you should receive an email notification.

### 5.1.3 Post-deployment

This information is needed to set up HyTrust CloudControl (HTCC) to interact with Windows AD and vCenter. The IBM Service team will set up HTCC so it is ready for HyTrust configuration based on the use cases required by the client. [Table 5-3](#) shows examples of HTCC configuration parameters.

**Table 5-3: Examples of HTCC Configuration Parameters**

Client Input Variables	Choices	Example Values
SMTP Server - for email notifications	Point to company or enable third party sendgrid	sendgrid
SNMP Server		
NTP Server (provided by SL)	Use default (10.0.77.54), unless specified	10.0.77.54 (time.service.networklayer.com)
<b>Windows AD Groups and Users</b>		
Group / Users		
HTCC Super Admin group	ht_superadmin_users	ht_superadmin_users
User in: ht_superadmin_users (Full Admin)	Administrator	Administrator
User: ht_ldap_svc HTCC to AD login user	ht_ldap_svc unless specified by client	ht_ldap_svc
User: ht_vcenter_svc HTCC to vCenter login user	ht_vcenter_svc unless specified by client	ht_vcenter_svc
<b>H/W Policy tags</b>		
Country (from BMXI portal, as displayed)	Country name	USA
State/Province	State or province name	DAL
Physical Data Center (PDC)	Location (IBM Cloud Data Center name as displayed)	DAL09
Region	Region where data center is located	South West
Classification (User ID-Client name)	Custom	

The IBM services team gathers information from the client, such as the examples in [Table 5-4](#), after understanding the use cases. The information will be used to configure HyTrust, VMware, and Intel TPM/TXT to enforce workload rules and policy. Once post-deployment is completed, the IBM services team will perform a verification test and deliver the asset to the client.

**Table 5-4: Examples of Additional HTCC Configuration Parameters**

Client Input Variables	Choices	Example Values
SMTP Server - for email notifications	Point to company or enable third party sendgrid	sendgrid
SNMP Server	?	?
HyTrust H/W TPM Policy Tags		
HTCC Compliance Templates - Custom		
Name		Based on PCI, NIST, ...
HTCC Scheduled Events		
Name		Template or Label
HTCC Policy Labels		
Name		Template
HTCC Roles		
Default Roles		
<b>Users</b>		
ASC_ARCAdmin	default	ASC_ARCAdmin
ASC_ARCAssessor	default	ASC_ARCAssessor
ASC_ApplAdmin	default	ASC_ApplAdmin
ASC_BackupAdmin	default	ASC_BackupAdmin
ASC_BasicLogin	default	ASC_BasicLogin
ASC_CoreApplAdmin	default	ASC_CoreApplAdmin
ASC_DCAdmin	default	ASC_DCAdmin
ASC_ESXMAAdmin	default	ASC_ESXMAAdmin
ASC_NetworkAdmin	default	ASC_NetworkAdmin
ASC_PolicyAdmin	default	ASC_PolicyAdmin
ASC_RoleAdmin	default	ASC_RoleAdmin



Client Input Variables	Choices	Example Values
ASC_StorageAdmin	default	ASC_StorageAdmin
ASC_SuperAdmin	default	ASC_SuperAdmin
ASC_ThirdParty	default	ASC_ThirdParty
ASC_UCSLogin	default	ASC_UCSLogin
ASC_VIAdmin	default	ASC_VIAdmin
ASC_VMPowerUser	default	ASC_VMPowerUser
ASC_VMUser	default	ASC_VMUser
<b>Groups</b>		
ASC_ARCAdmin	default	ASC_ARCAdmin
ASC_ARCAssessor	default	ASC_ARCAssessor
ASC_ApplAdmin	default	ASC_ApplAdmin
ASC_BackupAdmin	default	ASC_BackupAdmin
ASC_BasicLogin	default	ASC_BasicLogin
ASC_CoreApplAdmin	default	ASC_CoreApplAdmin
ASC_DCAdmin	default	ASC_DCAdmin
ASC_ESXMAdmin	default	ASC_ESXMAdmin
ASC_NetworkAdmin	default	ASC_NetworkAdmin
ASC_PolicyAdmin	default	ASC_PolicyAdmin
ASC_RoleAdmin	default	ASC_RoleAdmin
ASC_StorageAdmin	default	ASC_StorageAdmin
ASC_SuperAdmin	default	ASC_SuperAdmin
ASC_ThirdParty	default	ASC_ThirdParty
ASC_UCSLogin	default	ASC_UCSLogin
ASC_VIAdmin	default	ASC_VIAdmin
ASC_VMPowerUser	default	ASC_VMPowerUser
ASC_VMUser	default	ASC_VMUser

## 5.2 Enable Hardware Root of Trust on ICSV Servers

In order to leverage the ICSV instance for hardware roots of trust, steps must be taken to enable these features within the server BIOS, as well as ensuring features in the VMware products are enabled to access and leverage these measurements.

### 5.2.1 Enable Managed Object Browser (MOB) for each ESXi Server

1. Open the vSphere Client and navigate to the relevant host.
2. Click on the **Configure** tab.
3. On the left-hand side under **Software**, click on **System**, then **Advanced System Settings**.
4. Click on the **Edit** button.
5. Modify or add the configuration to enable MOB: **Config.HostAgent.plugins.solo.enableMob** (set value to **True**).
6. To confirm that MOB has been enabled on the host, open *http://x.x.x.x/mob*, where x.x.x.x is the IP address of the ESX Server.

### 5.2.2 Enable TPM/TXT on SuperMicro hosts

1. From the vCenter console, enter the ESX host(s) in maintenance mode.
2. Log into your IBM Cloud console and open a support ticket. In the ticket, specify the following:
  - a. ESX host(s) you want them to work on. You can have support work on multiple hosts as long as you have the minimum running as required by your instance—minimum of three hosts for instances that have VSAN, otherwise two hosts.
  - b. Enter ticket description as follows:

< Start of ticket description >

*We need your assistance to enable TPM/TXT in the BIOS for this IBM Cloud Secure Virtualization (ICSV) instance.*

*Please enable the TPM/TXT flags in the BIOS, following the steps in the exact order specified:*

1. *Reboot the following host(s) specified below and enter into the BIOS – <provide the list of hosts again here for clarity.>*

2. Go to Advanced 'Trusted Computing'. *If TPM cannot be cleared in the **Pending Operations** option, then reboot to the BIOS and **enable TPM only**. You will need this to clear TPM in the next reboot. **Press F4 to save and exit**.*
3. *On reboot, again go to the BIOS and go to Advanced 'Trusted Computing'. **Clear TXT**. This will clear TPM and TXT. **Press F4 to save and exit**.*
4. *On reboot go to the BIOS and **enable TPM only**. **Press F4 to save and exit**. **Do not enable TPM and TXT in the same reboot. They have to be enabled in sequence**.*
5. *On reboot, again go to the BIOS and now **enable TXT**. The TPM should have been enabled from last step. **Press F4 to save and exit**.*
6. *Let the reboot continue to boot to ESX.*

*Please let me know when you have done this successfully.*

< End of ticket description >

- c. Once the support person returns the ticket with the task completed, continue with the tasks below.
3. From the vCenter console, exit maintenance mode. You may need to connect the ESX hosts again if the host got disconnected.
4. From the vSphere web client or vSphere client, disconnect the host and then connect the host back. This is needed to have the ESXi host re-read the TPM settings.
5. Check the vCenter MOB to check if TPM/TXT is enabled.

At a minimum, there must be three hosts up in instances that have VSAN. So make sure you only work on hosts that will ensure this requirement is met. Ideally, work on one host at a time.

### 5.2.3 Enable TPM/TXT in IBM Cloud

1. Through vCenter, place the ESXi host in maintenance mode.
2. Reboot the ESXi server by pressing the **F12** key in the iKVM viewer.
3. Once the server reboots, access the BIOS. Disable the **TPM Provision Support**, the **TXT Support**, and the **TPM State**, then **Save & Exit**.
4. Reboot the server all the way to the ESXi OS level.
5. Reboot the server again using the **F12** key.
6. Make sure the OS is not loaded, and access the BIOS. Set the **TPM State** to **Enabled**, then **Save & Exit**.

7. Let the system boot up, but access the BIOS before the OS is loaded. If the system boots the OS, you will have to do the above steps again.
8. Enable **TXT Support** in the BIOS, then **Save & Exit**.
9. Boot the server to OS hypervisor level.

#### 5.2.4 Validate the TPM/TXT is enabled

1. SSH into the ESX host as `root` and run the following command:

```
zcat /var/log/boot.gz | grep -I tpm
```

This should show if the TPM library was loaded.

2. Other commands to check are:

```
vmkload_mod -l | grep tpm
```

```
grep -i tpm /var/log/hostd.log | less -S
```

3. As a root user, run the following command:

```
esxcli hardware trustedboot get
```

It should show two answers, and both should be **true**.

#### 5.2.5 Check the vCenter MOB to see if the TPM/TXT is enabled

1. Open a browser with <https://<vCenter-console-IP address>/mob> to access the vCenter MOB (do not use the individual ESXi host MOB). Authenticate using the vCenter credential.
2. Click on different resources of the MOB in the steps shown below:
  - a. Click on **content**.
  - b. Search for **group-d1 (Datacenters)** and click on it.

licenseManager	ManagedObjectReference:LicenseManager	<a href="#">LicenseManager</a>
localizationManager	ManagedObjectReference:LocalizationManager	<a href="#">LocalizationManager</a>
overheadMemoryManager	ManagedObjectReference:OverheadMemoryManager	<a href="#">OverheadMemoryManger</a>
ovfManager	ManagedObjectReference:OvfManager	<a href="#">OvfManager</a>
perfManager	ManagedObjectReference:PerformanceManager	<a href="#">PerfMgr</a>
propertyCollector	ManagedObjectReference:PropertyCollector	<a href="#">propertyCollector</a>
rootFolder	ManagedObjectReference:Folder	<a href="#">group-d1 (Datacenters)</a>
scheduledTaskManager	ManagedObjectReference:ScheduledTaskManager	<a href="#">ScheduledTaskManager</a>

- c. Find **datacenter-2 (SDDC-Datacenter)** and click on it.

- d. Search for **group-h4 (host)** and click on it.
- e. Search for **domain-c7 (SDDC-Cluster)** and click on it.
- f. Search for **host**, and you will see all the hosts listed with their host names.

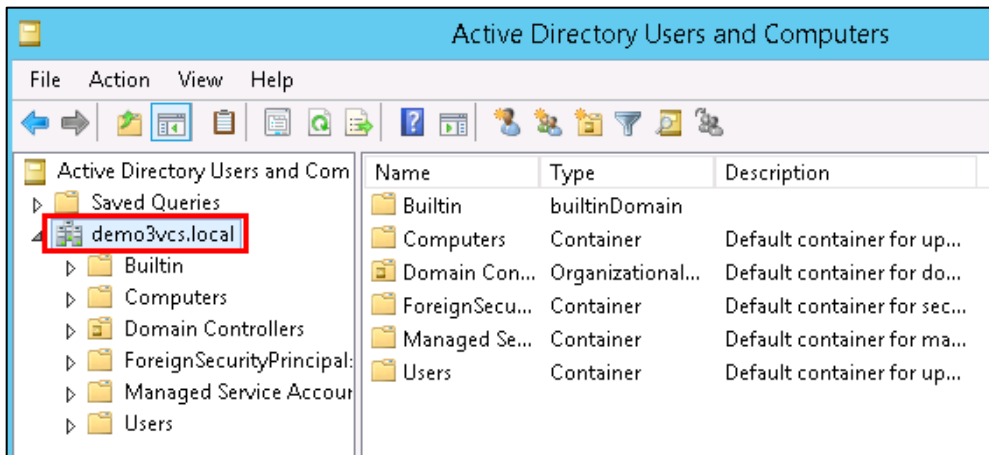
host	ManagedObjectReference:HostSystem[]	<a href="#">host-29 (host2.securek8s.ibm.local)</a> <a href="#">host-34 (host3.securek8s.ibm.local)</a> <a href="#">host-35 (host0.securek8s.ibm.local)</a> <a href="#">host-36 (host1.securek8s.ibm.local)</a>
------	-------------------------------------	---

- g. Click on the host that you need to validate. In our demo, we are checking **host1.securek8s.ibm.local**.
- h. Search for method **QueryTpmAttestationReport** and click on it to invoke the method.
- i. Click on **Invoke Method**.

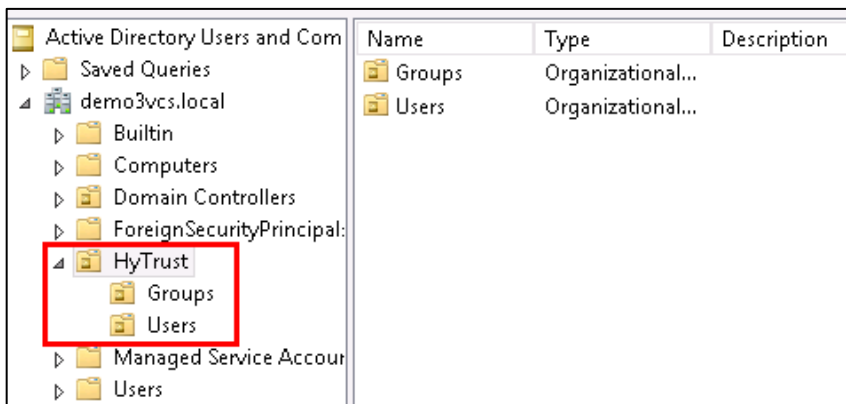
## 5.2.6 Set up Active Directory users and groups

In this part of the setup, you will create several new organizational units. Remember that this procedure uses a Windows 2012 server and Microsoft AD to illustrate the steps. Your environment and your specific steps might be different. This section assumes actions are being performed from the ICSV Microsoft AD server. Alternatively, you can follow these steps to set up AD. Note that the values in the screen shots will be different than your values.

1. In Windows Server, start the Server Manager, if not already started.
2. From the **Server Manager** window, select **Tools -> Active Directory Users and Computers**.
3. Right-click on your domain that has been created based on the instance name you provided by Windows AD deployment (for VCS) or during VCF deployment creation. For our demo, it is **demo3VCS.local**. Select **New -> Organizational Unit**. You should create the new **OU**.



4. Enter **HyTrust** as the name of the new unit. Right-click on the **HyTrust** organizational unit, select **New -> Organizational Unit**, and give the name of **Groups**.
5. Right-click again on the **HyTrust** organizational unit, select **New -> Organizational Unit**, and give the name of **Users**. This group will be used to allow a user to communicate between HTCC and AD. The directory hierarchy should now look similar to this:



6. Add two users to the **Users** group. To do this, right-click on the **HyTrust/Users** organizational unit and select **New -> User**.
7. The first user is the primary user account that will be used to communicate between HTCC and AD. In the pop-up screen for users, enter user information as appropriate. The screen might look like this:

Full name: **HyTrust LDAP Lookup**

User logon name: **ht\_ldap\_svc**

New Object - User

Create in: demo3vcs.local/HyTrust/Users

First name:  Initials:

Last name:

Full name: **HyTrust LDAP Lookup**

User logon name: **ht\_ldap\_svc** @demo3vcs.local

User logon name (pre-Windows 2000): demo3vcs\ ht\_ldap\_svc

< Back Next > Cancel

8. Click **Next** to go to the user password screen. It asks you to establish a password and some password options for the user. Enter or verify these fields:
  - a. Enter and confirm a password for the user. The password needs to have at least one upper case letter, otherwise the user will not be created. Note the password in the deployment spreadsheet.
  - b. Uncheck this option: **User must change password at next logon.**
  - c. Check this option: **Password never expires.**
  - d. Click **Next**.
  - e. Verify the information and finish.
9. The second user will be used as the service account when HTCC interacts with vCenter. You could use the **Administrator@vsphere.local** account, but best practice is to create a specific service account in AD and use that. Create the second user (in the same way as the first user) with the following values:
 

Full name: **HyTrust VCenter svc account**

User logon name: **ht\_vcenter\_svc**

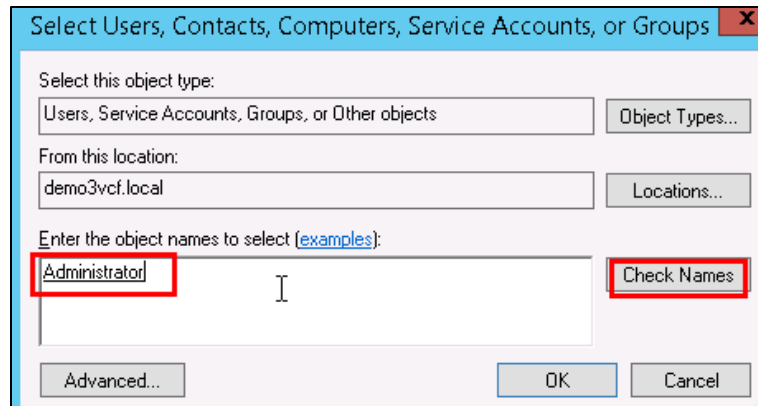
Ensure that the password never expires.
10. You will now create two subgroups under **Groups**.

- a. First, right-click on the **Groups** organizational unit and select **New -> Group**.
- b. When prompted, enter a name for the new group: **bcadmins**. Later, you will tell HTDC to use this group when communicating with HTCC to verify boundary checks. Keep the rest of the options (Group scope and type) the default values as shown below. Press **OK** to create the group.

The screenshot shows the 'New Object - Group' dialog box. At the top, it says 'Create in: demo3vcs.local/HyTrust/Groups'. Below that, the 'Group name' field is filled with 'bcadmins' and is highlighted with a red rectangle. The 'Group name (pre-Windows 2000)' field is also filled with 'bcadmins'. In the 'Group scope' section, the 'Global' radio button is selected. In the 'Group type' section, the 'Security' radio button is selected.

- c. Right-click again on the **Groups** organizational unit and select **New -> Group**.
  - d. When prompted, enter a name for this group: **ht\_superadmin\_users** and press **OK**. Later, you will tell HTCC to use this group to specify administrative users of HTCC.
11. You will now add members to the **superadmin** group.
- a. To do this, right-click on the **ht\_superadmin\_users** group, and select **Properties**.
  - b. In the pop-up window, select the **Members** tab, then click **Add**.
  - c. In the next pop-up screen, enter an object name **Administrator**, and click on **Check Names**. If no error is returned, click **OK**.





12. Close the AD control panel.

You are now ready to set up HTCC authentication to work with AD, as described in the next procedure.

### 5.2.7 Join vCenter to the AD domain

We need to integrate the AD domain into vCenter so that we can later give the AD HyTrust service account vCenter permissions. You first have to join the vCenter to the AD domain, and then add the AD user to vCenter. Note that this is already done for VCS and VCF. However, you may want to check using the instructions below.

1. To check if vCenter is already joined to the AD domain, SSH into PSC.
2. Run the following command:

```
/opt/likewise/bin/domainjoin-cli query
```

If the output indicates it's already joined, you can skip the rest of this section (5.2.7).

3. If it's not already joined, run the following command to join it:

```
/opt/likewise/bin/domainjoin-cli join <domain-name> <AD Administrator user>
<password>
```

Example:

```
/opt/likewise/bin/domainjoin-cli join demo3vcs.local Administrator Passw0rd
```

Output:

```
Joining to AD Domain:  demo3vcs.local
With Computer DNS Name:  psc.demo3vcs.local
SUCCESS
```

Then reboot.

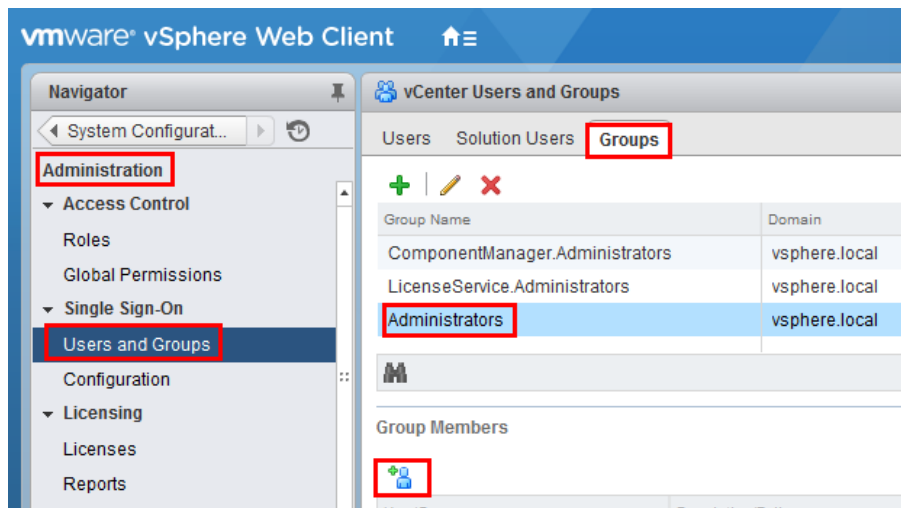
4. SSH into PSC again and verify that the join has succeeded by issuing the following command:

```
/opt/likewise/bin/domainjoin-cli query
```

## 5.2.8 Add AD HyTrust-vCenter service user to vCenter as Administrator

This is for both the VCS and VCF instances.

1. In the vSphere Web Client, go to **Administration** and then **Users and Groups**. Click on **Groups**, then **Administrators**, and select the Group Members **Add** icon.



2. In the **Add Principals** panel, select the Windows AD Domain (**demo.local** in our example), scroll down and select the user **ht\_vcenter\_svc** user (that was created in Windows AD), and click on the **Add** button. That user should appear in the Users list. Then press the **OK** button.

**Add Principals** ?

Select users from the list or type names in the Users text box. Click Check names to validate your entries against the directory.

Domain: **demo.local**

---

**Users and Groups**

Show Users First Search

User/Group	Description/Full name
<b>ht_vcenter_svc</b>	HyTrust vCenter svc account
krbtgt	
PSC\$	
Access Control Assistance Operato...	Members of this group can remotely qu...
Account Operators	Members can administer domain user ...
Administrators	Administrators have complete and unr...
Allowed RODC Password Replicati...	Members in this group can have their p...

**Add**

Users: **demo.local\ht\_vcenter\_svc**

Groups:

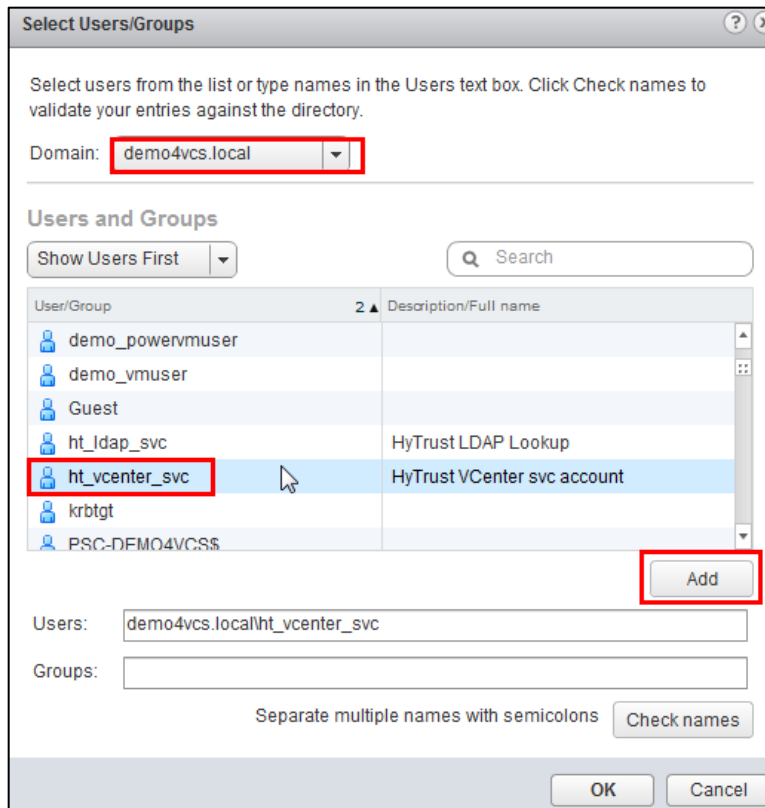
Separate multiple names with semicolons Check names

OK Cancel

You have successfully added the Windows AD HyTrust vCenter LDAP id as part of the Administrator group. This id will be used for all interaction between HTCC and vCenter, when the vCenter is added to HTCC.

## 5.2.9 Add AD HyTrust-vCenter service user to vCenter Global Permissions

1. Go to the vCenter web client. Under **Administration**, click on **Global Permissions**.
2. Add the AD user for the HyTrust-vCenter service, **ht\_vcenter\_svc**, and give it Administration permission.



### 5.2.10 Configure HTCC for AD authentication

HTCC requires a directory services solution. In this deployment solution, HTCC authentication will be set up to work with Microsoft AD. Before you configure HTCC to use AD, you must define two groups and one user. You can do this via existing AD entries or create entries just for HTCC (as is the case in our implementation).

By default, HTCC is set to use a demo userid/password authentication. Once you change to AD authentication, you cannot revert back to the demo authentication.

If AD is configured with TLS, the AD server's certificate must be imported into HTCC. To configure HTCC with an AD server with TLS configuration, refer to the [HTCC Administration Guide](#) for the following steps:

1. To import AD Server certificate into HTCC, refer to the HTCC Administration Guide section titled "Installing a Third-Party Root Certificate."
2. Configure AD with TLS in HTCC. Refer to the HTCC Administration Guide section titled "Integrating the Appliance with Active Directory."

To set up HTCC authentication, follow these steps:

1. Log onto the HTCC web console, using URL `https://<HTCC-Virtual-IP>/asc` with the default username of `superadminuser` and the password `Pa$$w0rd123!`
2. From the HTCC dashboard, select the **Configuration** menu, and then **Authentication**.
3. Change the **Authentication Server Type** to **Directory Service** and accept your changes.
4. You should see a screen for configuring the service account. Make sure that the default domain name is the one you used to deploy the instance. In our demo, it's **demo3vcf.local**. In the service account name field, enter the username (**ht\_ldap\_svc**) and password that you used during the AD setup steps.
5. Click **Next**, and you will see the domain listed. Click **Next** again.
6. You should now see the **Role-Group Mapping** page. Look under the **ASC\_SuperAdmin** section entry. Confirm that your AD domain is listed in the selected pull-down entry. In the group name field, enter the admin group name, **ht\_superadmin\_users**, that you created earlier in the initial AD setup. HTCC will attempt to perform predictive searches to allow for name completion.

ASC_SecurityOperator	demo3vcf	
ASC_StorageAdmin	demo3vcf	
ASC_SuperAdmin	demo3vcf	ht_su ht_superadmins
ASC_ThirdParty	demo3vcf	

7. Click **Next** and review the summary. If it is correct, finish. If AD is working correctly, the web interface will automatically log you out.
8. Log back in using the **Administrator** user and password of your Windows AD/DNS Server (which is the domain controller). Recall that we had added **Administrator** to the **ht\_superadmin\_users** group in Windows AD.

At this point, AD should be correctly set up for deployment. You are ready to set up the trust attestation service.

### 5.3 Add Hosts to HTCC and Enable Good Known Host (GKH)

You will add hosts in vCenter and then enable the Good Known Host (GKH) values to make them Trusted.

First, since all the hosts are managed by vCenter (as compared to standalone ESX hosts), you will add vCenter as the host—that will automatically detect the NSX server and the ESX hosts, and add them to HTCC. The high-level steps are:

1. In HTCC, add vCenter as the host. For vCenter, use the same AD LDAP used for the HTCC vCenter AD ID, **ht\_vcenter\_svc@ibm.local** (change the domain name based on what you have). While you can use **Administrator@vsphere.local**, best practice suggests you use the AD ID.
2. For all the ESX hosts that are detected, add their user IDs/passwords and **Publish IPs**.
3. If the vCenter and ESX host patch levels are not one of the valid patches supported by HTCC, add the patch level to HTCC so it recognizes them as valid hosts.

Next, follow the directions at [Enabling a Good Known Host](#), then [Verify and Update Host Trust](#).

Finally, to define, assign, and provision PolicyTags, follow these steps:

1. [Define PolicyTags in CloudControl](#).
2. Assign PolicyTags to hosts. Important: We recommend that you put your host in maintenance mode before assigning PolicyTags, especially if you are modifying existing PolicyTag assignments which may be in use by your existing compliance rules. Do not remove the host from maintenance mode until you have verified that the new PolicyTag assignment has been correctly provisioned.
  - a. Select **Compliance > Hosts**.
  - b. On the **Hosts** page, check the checkbox for the Intel TXT-enabled host and click **Edit**.
  - c. On the **Edit Hosts** page, select the **PolicyTag** tab.
  - d. Select the appropriate **PolicyTag** value for one or more of the fields listed in Step 1.
  - e. Click **OK**.
  - f. CloudControl displays a JGrowl error message that prompts users to PXE boot the host(s) to activate the PolicyTag assignment.
3. Follow all of the PolicyTags provisioning directions in [Section 4.3.1](#).
4. Verify the provisioning using these steps:
  - a. Open CloudControl and select **Compliance > Hosts**.
  - b. Select the host that you just updated and click **Update Trust**.
  - c. Select **Policy > Resources**.

- d. Verify that the PolicyTags have been provisioned. If the tag icon next to the host being provisioned is blue, then the PolicyTags assigned to the host are provisioned. If the tag icon is yellow, then the PolicyTags assigned to the host are not provisioned. If the provisioning process was not successful, you may have to clear the TPM once again and repeat the process.
- e. After the PolicyTag provisioning is successful, you can remove the hosts from maintenance mode.

## 6 Intel Product Installation and Configuration Guide

Intel TXT provides hardware-based security technologies that address the increasing and evolving security threats across physical and virtual infrastructures by complementing runtime protections. Intel TXT increases protection by allowing greater control of the launch stack through a Measured Launch Environment (MLE) and enabling isolation in the boot process. More specifically, it extends the Virtual Machine Extensions (VMX) environment of Intel Virtualization Technology (Intel VT), permitting a verifiably secure installation, launch, and use of a hypervisor or OS. These measured values in the boot process are extended to and stored in a TPM on the server.

To enable Intel TXT and the necessary TPM in the server BIOS, follow the steps in [Section 5.2.3](#). The steps in [Section 5.2.4](#) can be followed to verify that each Dell ESXi host has successfully enabled the TPM and Intel TXT. The steps in [Section 5.2.5](#) can be followed to verify that the Dell ESXi hosts' TPM values are successfully read by the vCenter Server.

## 7 RSA Product Installation and Configuration Guide

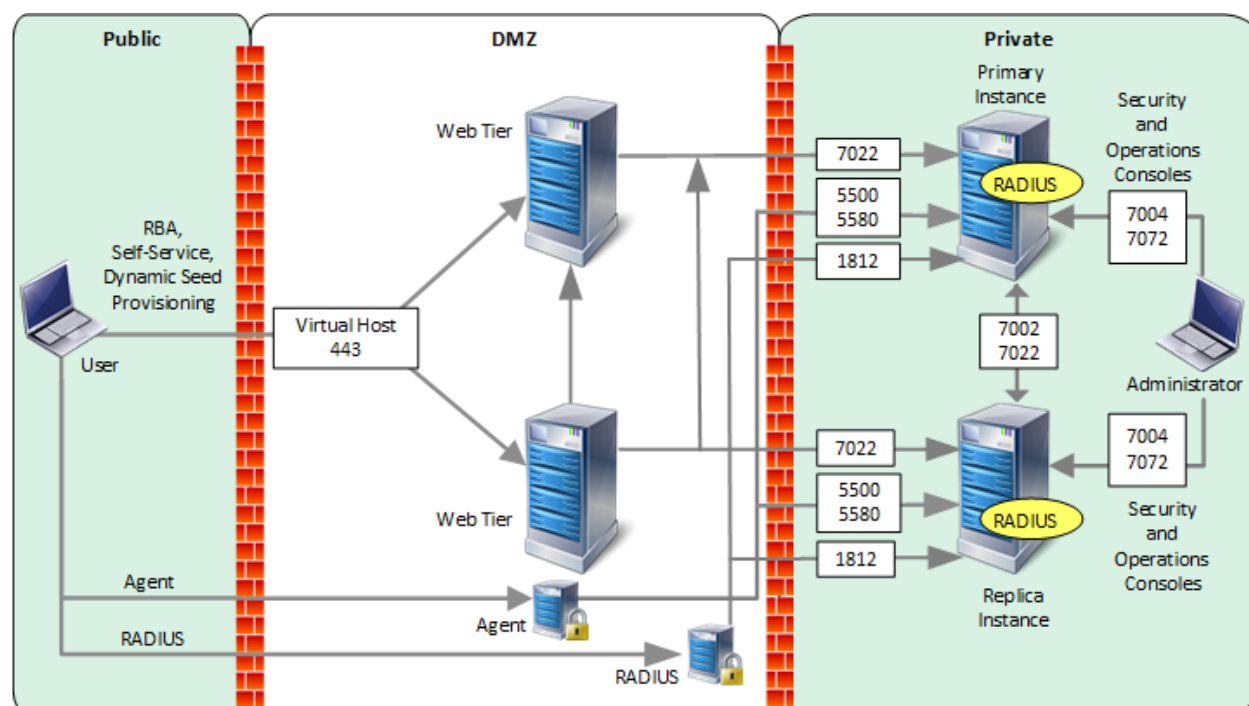
This section covers the installation and configuration of the RSA products used to build the example solution.

### 7.1 RSA SecurID

RSA Authentication Manager is the authentication, administration, and database management component of RSA SecurID, which provides strong authentication of users accessing valuable network resources. Refer to [RSA Authentication Manager 8.4 VMware Virtual Appliance Getting Started](#) for installation instructions. Another source of information is [Getting Started with RSA Authentication Manager](#).

[Figure 7-1](#) represents a common RSA Authentication Manager deployment with primary and replica instances, web tiers, and a load balancer. An external firewall protects the primary and replica instances, and another external firewall protects the DMZ.

Figure 7-1: RSA Authentication Manager Deployment Architecture



## 7.2 RSA NetWitness

To install and configure virtual hosts for RSA NetWitness Platform 11.4, follow the instructions in the [Virtual Host Installation Guide](#). Start by reading the “Basic Virtual Deployment” section, then reading and following the steps in the “Install NetWitness Platform Virtual Host in Virtual Environment” section (except you can skip Step 1b).

The rest of this section explains how to configure NetWitness for VMware log collection from an ESX host.

### 7.2.1 Configure the VMware ESX/ESXi Event Source

This section describes how to create a least privilege user to extract logs from an ESX/ESXi host. You first create a role, then you create the user, and finally, you assign the role to the user.

1. Create a role as follows:
  - a. Log onto the ESXi host using the vSphere Client, with administrative privileges.
  - b. Click on **Administration > Roles**.
  - c. Click on **Add Role**.



- d. Enter **RSA Log Capture** as the name of the Role.
  - e. Choose **All Privileges > Global > Diagnostics** as the only privilege for this role.
- 2. Create a local ESXi user as follows:
  - a. From the Left navigation pane, click on the ESXi host, then click the **Users or Local Users & Groups** tab. The name of the tab depends on the credentials you used to log onto the ESXi host.
  - b. Right-click on the **Users** tab, then click **Add**.
  - c. Enter **rsa-vcenter-logs** in the **Login** field, and choose a strong password.
- 3. Assign the role to the local user as follows:
  - a. From the Left navigation pane, click on the ESXi host, then click the **Permissions** tab.
  - b. Right-click in the **Permissions** table, then click **Add Permission**.
  - c. In the dialog box, under the **Assigned Role** drop-down menu, choose **RSA Log Capture**.
  - d. Under **Users and Groups**, click **Add....** The **Select Users and Groups** dialog box is displayed.
  - e. In the dialog box, leave the Domain value as (server), and select the **rsa-vcenter-logs** user.
  - f. Click **Add**, then click **OK**.

This completes the process of adding a least privilege user. When you configure the Log Collector for VMware collection in RSA NetWitness Suite, make sure to enter the credentials for this user in the **Add Source** dialog box.

### 7.2.2 Configure the RSA NetWitness Log Collector for VMware Collection

To configure the RSA NetWitness Log Collection for VMware Collection, go to page 105 in the [Log Collection Configuration Guide for RSA NetWitness Platform 11.4](#), and follow the instructions in the section titled “Configure VMware Event Sources in NetWitness Platform.”

## 8 VMware Product Installation and Configuration Guide

This section covers all the aspects of installing and configuring the VMware products used to build the example solution.

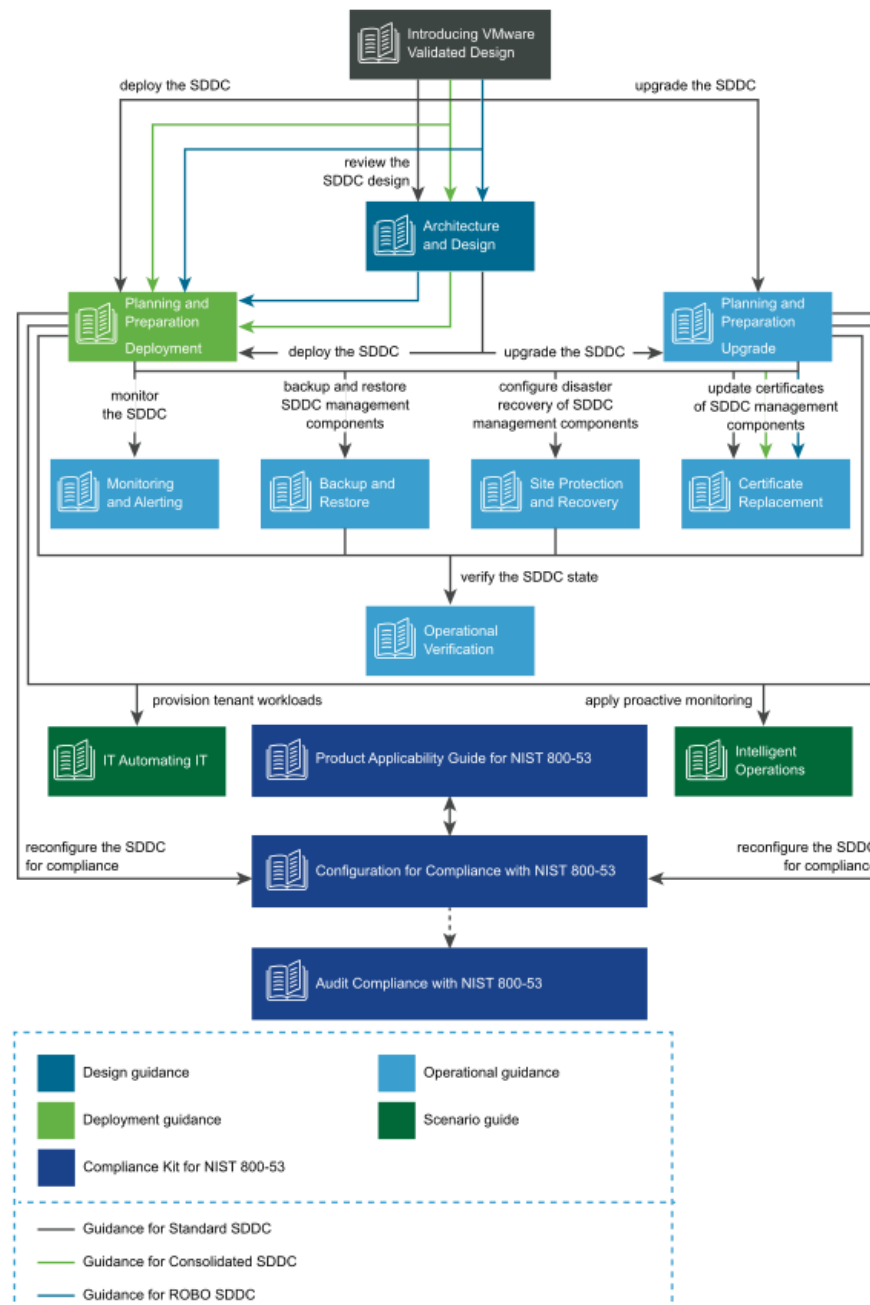
## 8.1 Prerequisites

The VMware Validated Design (VVD) is a blueprint for a Software Defined Data Center (SDDC). A Standard deployment model was used. In order to prepare for the implementation of the VVD, review the following documentation. It outlines the preparation and planning phases, contains logical design architectures and design decisions related to the implementation, and assists with the end-to-end process of deploying a VVD:

- [VMware Validated Design Documentation](#)
- *Documentation Structure and Audience* ([VVD 4.3](#), [VVD 5.0.1](#)), see [Figure 8-1](#).
  - Architecture and Design
  - Planning and Preparation Deployment
  - Planning and Preparation Upgrade
  - Monitoring and Alerting
  - Backup and Restore
  - Site Protection and Recovery
  - Certificate Replacement
  - Operational Verification
  - IT Automating IT
  - Intelligent Operations
  - Security and Compliance Configuration for NIST 800-53:
    - [Introduction to Security and Compliance](#)
    - [Product Applicability Guide for NIST 800-53](#)
    - [Configuration for Compliance with NIST 800-53](#)
    - [Audit Compliance with NIST 800-53](#)
- *Introducing VMware Validated Design for Software-Defined Data Center* ([VVD 4.3](#), [VVD 5.0.1](#))
- *Design Objectives of VMware Validated Designs* ([VVD 4.3](#), [VVD 5.0.1](#))
- *Overview of Standard SDDC* ([VVD 4.3](#), [VVD 5.0.1](#))
- *VMware Validated Design Architecture and Design* ([VVD 4.3](#), [VVD 5.0.1](#))
- *VMware Validated Design Planning and Preparation* ([VVD 4.3](#), [VVD 5.0.1](#))
- *VMware Validated Design for Software-Defined Data Center Release Notes* ([VVD 4.3](#), [VVD 5.0](#), [VVD 5.0.1](#))

To visualize how the VVD works in conjunction with the Compliance Kit for NIST 800-53, [Figure 8-1](#) provides an overview of the documentation structure. The VMware Validated Design Compliance Kit enhances the documentation of the VVD for SDDC and must be applied after the SDDC is deployed.

**Figure 8-1: Map of VVD Documentation**



To reconfigure your SDDC for compliance with NIST SP 800-53 (<https://doi.org/10.6028/NIST.SP.800-53r4>), you must download and license additional VMware and third-party software.

The VVD coupled with *Security and Compliance Configuration for NIST 800-53* uses scripts and commands based on VMware PowerCLI to reconfigure the SDDC. You must prepare a host with a supported OS for running Microsoft PowerShell, set up Microsoft PowerShell, and install the latest version of VMware PowerCLI. The host must have connectivity to the ESXi management network in the management cluster.

## 8.2 Installation and Configuration

Review the following documentation for the complete guide concerning the installation and configuration for the VVD for an SDDC for a Standard Deployment:

- Deployment for Region A ([VVD 4.3](#), [VVD 5.0.1](#))
- Deployment for Region B ([VVD 4.3](#), [VVD 5.0.1](#))

## 8.3 Configuration Customization Supporting the Use Cases and Security Capabilities

After deployment of a Standard VVD, the enhancements outlined in this publication should be applied. The security configurations and controls outlined in this section were implemented on a number of VVD versions, beginning with VVD 4.2 and then VVD 4.3. In addition to this lab, a separate project to publish the security configurations as a Compliance Kit that works as an enhancement to the VVD was published to VVD version 5.0.1. Changes between VVD 4.2, 4.3, 5.0.1, and even the most current version as of this writing, 5.1, are unlikely to have a significant impact to the configuration guidance.

Although this document outlines a specific version of the VVD, the Compliance Kit has been developed to support VVD 4.3, 5.0.1, 5.1, and future VVD releases. This section discusses the [VMware Validated Design 5.0.1 Compliance Kit for NIST 800-53](#) and provides supplemental information detailing the resources that are included within the kit because the kit was not formally published for VVD 4.2 or 4.3, even though it was tested based on these versions. The VVD 5.0.1 Compliance Kit contains a number of files, including:

- *Introduction to Security and Compliance*
- *Product Applicability Guide*
- *Configuration Guide*
- *Audit Guide*
- *Audit Guide Appendix*

The configuration procedures included within the kit are in two groups:

- **Built-In Controls:** Security controls based on compliance requirements are included in the VVD for SDDC. These may require configuration and adjustment, but by design the capabilities are included in the VVD for SDDC.
- **Enhanced Controls:** Additional guidance on a per regulation or standard basis includes a set of capabilities that can be added to the VVD for SDDC.

Over time, we expect a significant number of enhancement VVD controls to be incorporated into the VVD for SDDC. The enhancement guide always contains some number of NIST controls that are applicable to NIST SP 800-53 but are not included in the VVD for SDDC implementation. Each procedure documented in the *Configuration Guide* includes the NIST SP 800-53 control(s) that are associated with each. Two examples sampled from the *Configuration Guide* are included in [Section 8.3.1](#) and [Section 8.3.2](#).

Although the compliance kit was designed under VVD 5.0.1, the procedures and information included within the following sections are applicable to future releases of VVD, including VVD 5.1 and 5.1.1. Please note that while future iterations of the compliance kit will include configurations across all products, version 5.0.1 only corresponds to the following products: vCenter, ESXi, NSX for vSphere (NSX-V), and vSAN.

The following products are part of the VVD Bill of Materials, but not included in the current iteration of the Compliance Kit: vRealize, vRealize Automation (vRA), vRealize Operations Manager (vROPS), and vRealize Log Insight (vRLI). The documentation surrounding the configuration of these products does exist and is sourced from their respective *DISA Security Technical Implementation Guides*, which can be reviewed at <https://public.cyber.mil/stigs/downloads>. There are two examples for these configurations sampled from the *Configuration Guide* ([Section 8.3.3](#) and [Section 8.3.4](#)).

### 8.3.1 Example VVD 5.0.1 Configuration: Configure the Password and Policy Lockout Setting in vCenter Server in Region A

1. In a web browser, log into vCenter by using the vSphere Web Client.
2. Configure the password policies.
  - a. From the **Home** menu of the vSphere Web Client, click **Administration**.
  - b. In the Navigator, under **Single Sign-On**, click **Configuration**.
  - c. On the **Policies** tab, under **Password Policy**, click **Edit**.
  - d. In the **Edit Password Policies** dialog box, configure the password policies and click **OK**.
    - i. **Maximum Lifetime** should be set to **60**.

- ii. **Restrict Reuse** should be set to **5**.
  - iii. **Minimum Length** should be set to **15**.
  - iv. **Upper-case Characters** should be set to **1**.
  - v. **Lower-case Characters** should be set to **1**.
  - vi. **Numeric Characters** should be set to **1**.
  - vii. **Special Characters** should be set to **1**.
- 3. Configure the lockout policies.
  - a. On the **Policies** tab, click **Lockout Policy** and click **Edit**.
  - b. In the **Edit Lockout Policy** dialog box, for **Maximum Number of Failed Login Attempts**, enter **3**.
  - c. For **Interval Between Failures**, enter **900**.
  - d. For **Unlock Time**, enter **0** and then click **OK**.

### 8.3.2 Example VVD 5.0.1 Configuration: Configure Encryption Management in Region A

- 1. In a web browser, log in to vCenter Server by using the vSphere Web Client.
- 2. Enable **Host Encryption Mode** on the **sfo01m01esx01.sfo01.rainpole.local** host.
  - a. From the **Home** menu of the vSphere Web Client, select **Hosts and Clusters**.
  - b. Under the **sfo01-m01dc data center**, select the **sfo01m01esx01.sfo01.rainpole.local** host and click the **Configure** tab.
  - c. Under **System**, click **Security profile**.
  - d. Under **Host Encryption Mode**, click **Edit**.
  - e. In the **Set Encryption Mode** dialog box, from the **Encryption Mode** drop-down menu, select **Enabled** and click **OK**.
  - f. Repeat the procedure for all remaining hosts in Region A.
- 3. Enable VM encryption on all the VMs and virtual disks.
  - a. From the **Home** menu of the vSphere Web Client, select **VMs and Templates**.

- b. Under the **sfo01-m01dc data center**, expand the **sfo01-m01fd-bcdr** folder, right-click the **sfo01m01vc01 VM** and select **VM Policies**, then **Edit VM Storage Policies**.
- c. From the **VM Storage Policy** drop-down menu, select **VM Encryption Policy**, click **Apply to all**, and click **OK**.
- d. Repeat the procedure to reconfigure the remaining VMs in Region A.

### 8.3.3 Example vRealize Automation DISA STIG Configuration: Configure SLES for vRealize to protect the confidentiality and integrity of transmitted information

1. Update the “Ciphers” directive with the following command:

```
sed -i "/^[^#]*Ciphers/ c\Ciphers aes256-ctr,aes128-ctr" /etc/ssh/sshd_config
```

2. Save and close the file.
3. Restart the sshd process:

```
service sshd restart
```

### 8.3.4 Example vRealize Operations Manager DISA STIG Configuration: Configure the vRealize Operations server session timeout

1. Log on to the admin UI as the administrator.
2. Navigate to **Global Settings**.
3. Select **Edit Global Settings**.
4. Set the **Session Timeout** setting to **15** minutes.
5. Select **OK**.

## 8.4 Operation, Monitoring, and Maintenance

This section explains how to operate, monitor, and maintain various VMware products. It points to existing documentation whenever possible, so this document only includes supplemental information, such as backup and recovery processes, and specific monitoring practices recommended for the example solution.

### 8.4.1 Operation

This section discusses the basic operation of the VVD 5.0.1 for an SDDC, in addition to any relevant products associated with such operations.

vSphere vCenter Server (vCS) Appliance is a management application that allows for the management of VMs and ESXi hosts centrally. The vSphere Web Client is used to access the vCS.

vRealize Operations Manager (vROPS) tracks and analyzes the operation of multiple data sources in the SDDC by using specialized analytic algorithms. The algorithms help vROPS learn and predict the behavior of every object that it monitors. Users access this information by views, reports, and dashboards.

vRealize Automation (vRA) provides a secure web portal where authorized administrators, developers, and business owners can request new IT services and manage specific cloud and IT resources, while ensuring compliance with business policies.

Please review the following for further information and discussion pertaining to the operational standards of the VVD 5.0.1 for an SDDC: [VMware Validated Design Documentation](#), [VMware Validated Design 5.0.1 Compliance Kit for NIST 800-53](#), and *NIST SP 1800-19B*.

## 8.4.2 Monitoring

This section outlines monitoring and alerting functionalities and best practices pertaining to VVD.

Use the vRealize Log Insight (vRLI) event signature engine to monitor key events and to send filtered or tagged events to one or more remote destinations. You can use a set of alerts to send to vROPS and through SMTP for operations team notification. The use of vRLI allows you to monitor the SDDC and provide troubleshooting and cause analysis, which can reduce operating costs.

With the integration between vRLI and vROPS, you can implement the following cross-product event tracking:

- Send alerts from vRLI to vROPS, which maps them to the target objects.
- Launch in context from a vROPS object to the objects logs in vRLI.
- Launch in context from a vRLI event to the objects in vROPS.

Use applications in vROPS to group monitoring data about the virtual machines of the SDDC management components.

vROPS builds an application to determine how your environment is affected when one or more components experience problems. You can also monitor the overall health and performance of the application.

vROPS collects data from the components in the application and displays the results in a summary dashboard with a real-time analysis for any or all the components.

Ensuring that your backup solution is configured to trigger an email alert generation showing the status of your backup jobs is a recommended practice within the SDDC. This should be included in daily



monitoring activities to ensure that all management objects within the SDDC have successful backup images. The following can be done to enable broad monitoring using vROPS:

1. Create applications in vROPS to group the monitoring data
  - a. about the VMs of vRealize Suite Lifecycle Manager
  - b. about the VMs of vRLI
  - c. about the VMs of VMware Site Recovery Manager
  - d. about the VMs of VMware vSphere Replication (vR)
  - e. for the VMs of vROPS
  - f. collected from your vSphere Storage APIs for Data Protection (VADP)-based backup solution VMs
  - g. about the VMs of VMware vSphere Update Manager Download Service (UMDS)
2. Create email notifications in vROPS so it informs the SDDC operators of issues in the main monitoring parameters of the environment.
3. Configure vROPS to send email notifications about important alerts in the SDDC.

Please review the [Monitoring and Alerting](#) documentation for more information regarding the monitoring of the VVD 4.3 deployment, and the [VVD for SDDC 5.0.1 release notes](#) for more information on monitoring for VVD 5.0.1 deployments.

### 8.4.3 Maintenance

This section outlines the steps to perform an SDDC upgrade that follows a defined upgrade path. The NCCoE project started with VVD version 4.3 and upgraded to 5.0.1. [Table 8-1](#) provides a summary of the system requirements and upgrade sequence associated with the Bill of Materials (BOM) or product versions associated with each VVD version. This upgrade path is functional and defined by layers in which the components are upgraded or updated. It is important to note that functional and scalability tests for individual patches and express patches are not required for an environment.

**Table 8-1: Summary of VVD Version and Associated Bill of Materials (Product Versions)**

SDDC Layer	Product Name	Product Version in VVD 4.3	Product Version in VVD 5.0.1	Operation Type
Operations Management	vRealize Suite Lifecycle Manager	1.2	2.0.0 Patch 2	Upgrade

SDDC Layer	Product Name	Product Version in VVD 4.3	Product Version in VVD 5.0.1	Operation Type
	vRealize Log Insight	4.6	4.7	Upgrade
	vRealize Log Insight Agent	4.6	4.7	Upgrade
	vRealize Operations Manager	6.7	7.0	Upgrade
Cloud Management	vRealize Business for Cloud	7.4	7.5	Upgrade
	vRealize Automation with Embedded vRealize Orchestrator	7.4	7.5	Upgrade
Business Continuity	Site Recovery Manager	6.5.1.1	8.1.1	Upgrade
	vSphere Replication	6.5.1.3	8.1.1	Upgrade
	Backup solution based on VMware vSphere Storage APIs for Data Protection	Compatible Version	Compatible Version	Vendor Specific
Virtual Infrastructure	NSX Data Center for vSphere	6.4.1	6.4.4	Update
	Platform Services Controller	6.5 Update 2	6.7 Update 1	Upgrade
	vCenter Server	6.5 Update 2	6.7 Update 1	Upgrade
	vSphere Update Manager Download Service	6.5 Update 2	6.7 Update 1	Upgrade
	ESXi	6.5 Update 2	6.7 Update 1	Upgrade
	vSAN	6.6.1 Update 2	6.7 Update 1	Upgrade

The following are tips for upgrading the SDDC:

- Before you begin any upgrade process, review all the release notes.
- Consider that the SDDC design and implementation may be affected by security features that are enabled. Ensure interoperability testing is performed before and after making security changes, as well as when introducing new features, functionality, and bug fixes.
- The environment within the NCCoE lab varies from the conventional VVD deployment because for the NCCoE, additional integration with vendors is included, e.g., integration between HyTrust components and Key Management Server (KMS) and the VVD.

- Note that if a distributed environment is used, ensure there is replication by using the `vdcrepadmin` command line interface between the platform services controller (PSC) and the vCenter environments. This can be checked by following the instructions in [VMware Knowledge Base article 2127057](#).
- Perform a backup copy of your current certificates before you start the upgrade process. If you need to request a new certificate, ensure you follow the procedures in [this document for VVD 4.3](#) and [this document for VVD 5.1](#).

The following is a tip for updating the SDDC:

- Ensure an operational verification test is performed before and after performing an update. In most cases, updates should not impact the SDDC design and implementation (updates could include patches and bug fixes).

Updates that are not validated by VVD should be approached with caution.

- Scalability and functionality tests for individual patches, express patches, and hot fixes are not typically performed using the VVD. If a patch must be applied to your environment, follow the VMware published practices and VMware Knowledge Base articles for the specific patch. If an issue occurs during or after the process of applying a patch, contact VMware Technical Support.
- For further information and instruction regarding an update, please see the documentation for VVD 4.3 or VVD 5.0.

## 8.5 Product Configuration Overview

This section contains [Table 8-2](#), which details all configurations for each product, their corresponding enhanced or built-in label, and their mapped NIST SP 800-53 Revision 4 controls (which are defined at <https://doi.org/10.6028/NIST.SP.800-53r4>). The labels are derived from the compliance kit with the exception of the vRA and vROPS items, which are sourced directly from their corresponding DISA STIGs.

There are only a small number of vROPS and vRA DISA STIGs included in the following table, which means it does not include all available configurations. For the entire compilation of vROPS and vRA DISA STIGs, please review the following links:

- [VMware vRealize Automation 7.x Lighttpd](#)
- [VMware vRealize Automation 7.x SLES](#)
- [VMware vRealize Automation 7.x tc Server](#)
- [VMware vRealize Operations Manager 6.x Application](#)
- [VMware vRealize Operations Manager 6.x SLES](#)
- [VMware vRealize Operations Manager 6.x tc Server](#)
- [VMware vRealize – Cassandra](#)

There are a few notable items for which there are no NIST control mappings; rather, they are identified as “VMware Best Practices”. These items are not sourced from any existing DISA STIGs, hardening guides, or other compliance frameworks. Their implementation is strongly recommended.

**Table 8-2: Configuration Items Without Control Mappings**

Product Name	Configuration Label	Enhanced or Built-in	NIST SP 800-53 Rev. 4 Controls
ESXi	NIST80053-VI-ESXI-CFG-00048	Enhanced	AC-12
ESXi	NIST80053-VI-ESXI-CFG-00146	Built-In	AC-14a, AC-14b
ESXi	NIST80053-VI-ESXI-CFG-00031	Enhanced	AC-17
ESXi	NIST80053-VI-ESXI-CFG-00165	Built-In	AC-7
ESXi	NIST80053-VI-ESXI-CFG-00002	Enhanced	AC-8
NSX	NIST80053-VI-NET-CFG-00343	Built-In	CM-7
NSX	NIST80053-VI-NET-CFG-00344	Built-In	CM-7
NSX	NIST80053-VI-NET-CFG-00372	Enhanced	CP-9
NSX	NIST80053-VI-NET-CFG-00374	Enhanced	CP-9
NSX	NIST80053-VI-NET-CFG-00312	Built-In	IA-5
vCenter	NIST80053-VI-VC-CFG-00453	Built-In	VMware Best Practice only. No specific UCF_NIST_800_53_R4_High control is associated with this capability.
vCenter	NIST80053-VI-VC-CFG-00465	Built-In	VMware Best Practice only. No specific UCF_NIST_800_53_R4_High control is associated with this capability.
vCenter	NIST80053-VI-VC-CFG-00442	Enhanced	AU-5(2)
vCenter	NIST80053-VI-VC-CFG-00461	Built-In	AU-9, AU-6a, AU-2d, AC-6(9)
vCenter	NIST80053-VI-VC-CFG-00460	Built-In	AU-9, AU-7b, AU-7a, AU-7(1), AU-6a, AU-12c, AU-12a, AC-6(9)
vRA	VRAU-TC-000710	Enhanced	AC-17 (1)
vRA	VRAU-VA-000010	Enhanced	AC-17 (2)
vRA	VRAU-HA-000140	Enhanced	CM-7a
vRA	VRAU-LI-000215	Enhanced	CM-7a
vRA	VRAU-SL-000360	Enhanced	IA-5 (1) (b)
vRA	VRAU-VI-000240	Enhanced	IA-5 (1) (c)
vRA	VRAU-AP-000265	Enhanced	IA-7

Product Name	Configuration Label	Enhanced or Built-in	NIST SP 800-53 Rev. 4 Controls
vRA	VRAU-PG-000470	Enhanced	SC-13
vROPS	VROM-CS-000005	Enhanced	AC-3
vROPS	VROM-PG-000220	Enhanced	IA-7
vROPS	VROM-SL-001240	Enhanced	SC-13
vROPS	VROM-TC-000505	Enhanced	SC-2
vSAN	NIST80053-VI-Storage-SDS-CFG-00182	Built-In	AC-11a
vSAN	NIST80053-VI-Storage-SDS-CFG-00186	Enhanced	AU-4
vSAN	NIST80053-VI-Storage-SDS-CFG-00180	Built-In	AU-8b, AU-8a, AU-8(1)(b), AU-8(1)(a)
vSAN	NIST80053-VI-Storage-SDS-CFG-00181	Built-In	AU-9, AU-7b, AU-7a, AU-7(1), AU-6a, AU-12c, AU-12a, AC-6(9)
vSAN	NIST80053-VI-Storage-SDS-CFG-00183	Enhanced	SC-13, MP-5(4), AU-9(3)
vSphere	NIST80053-VI-VSPHERE-CFG-00571	Enhanced	CM-6
vSphere	NIST80053-VI-VSPHERE-CFG-00563	Enhanced	IA-2

## Appendix A Security Configuration Settings

This appendix captures the security configuration settings (Common Configuration Enumerations [CCEs]). The following table lists the VMware products and their associated security configurations.

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8440 1-9	NIST800 53-VI-ESXi-CFG-00001	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^Ciphers" /etc/ssh/sshd_config If there is no output or the output is not "Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc" or a subset of this list, ciphers that are not FIPS-approved are in use, so this is a finding.	aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc
CCE-8440 2-7	NIST800 53-VI-ESXi-CFG-00002	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^Protocol" /etc/ssh/sshd_config If there is no output or the output is not exactly "Protocol 2", this is a finding.	2
CCE-8440 3-5	NIST800 53-VI-ESXi-CFG-00003	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^IgnoreRhosts" /etc/ssh/sshd_config If there is no output or the output is not exactly "IgnoreRhosts yes", this is a finding.	yes
CCE-8440 4-3	NIST800 53-VI-ESXi-CFG-00004	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^HostbasedAuthentication" /etc/ssh/sshd_config If there is no output or the output is not exactly "HostbasedAuthentication no", this is a finding.	no

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8440-5-0	NIST800-53-VI-ESXi-CFG-00005	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^PermitRootLogin" /etc/ssh/sshd_config If there is no output or the output is not exactly "PermitRootLogin no", this is a finding.	no
CCE-8440-6-8	NIST800-53-VI-ESXi-CFG-00006	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^PermitEmptyPasswords" /etc/ssh/sshd_config If there is no output or the output is not exactly "PermitEmptyPasswords no", this is a finding.	no
CCE-8440-7-6	NIST800-53-VI-ESXi-CFG-00007	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^PermitUserEnvironment" /etc/ssh/sshd_config If there is no output or the output is not exactly "PermitUserEnvironment no", this is a finding.	no
CCE-8440-8-4	NIST800-53-VI-ESXi-CFG-00008	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^MACs" /etc/ssh/sshd_config If there is no output or the output is not exactly "MACs hmac-sha1,hmac-sha2-256,hmac-sha2-512", this is a finding.	hmac-sha1,hmac-sha2-256,hmac-sha2-512
CCE-8440-9-2	NIST800-53-VI-ESXi-CFG-00009	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^GSSAPIAuthentication" /etc/ssh/sshd_config If there is no output or the output is not exactly "GSSAPIAuthentication no", this is a finding.	no

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8441-0-0	NIST800-53-VI-ESXi-CFG-00010	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^KerberosAuthentication" /etc/ssh/sshd_config If there is no output or the output is not exactly "KerberosAuthentication no", this is a finding.	no
CCE-8441-1-8	NIST800-53-VI-ESXi-CFG-00011	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^StrictModes" /etc/ssh/sshd_config If there is no output or the output is not exactly "StrictModes yes", this is a finding.	yes
CCE-8441-2-6	NIST800-53-VI-ESXi-CFG-00012	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^Compression" /etc/ssh/sshd_config If there is no output or the output is not exactly "Compression no", this is a finding.	no
CCE-8441-3-4	NIST800-53-VI-ESXi-CFG-00013	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^GatewayPorts" /etc/ssh/sshd_config If there is no output or the output is not exactly "GatewayPorts no", this is a finding.	no
CCE-8441-4-2	NIST800-53-VI-ESXi-CFG-00014	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^X11Forwarding" /etc/ssh/sshd_config If there is no output or the output is not exactly "X11Forwarding no", this is a finding.	no



CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8441-5-9	NIST800-53-VI-ESXi-CFG-00015	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^AcceptEnv" /etc/ssh/sshd_config If there is no output or the output is not exactly "AcceptEnv", this is a finding.	AcceptEnv
CCE-8441-6-7	NIST800-53-VI-ESXi-CFG-00016	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^PermitTunnel" /etc/ssh/sshd_config If there is no output or the output is not exactly "PermitTunnel no", this is a finding.	no
CCE-8441-7-5	NIST800-53-VI-ESXi-CFG-00017	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^ClientAliveCountMax" /etc/ssh/sshd_config If there is no output or the output is not exactly "ClientAliveCountMax 3", this is a finding.	3
CCE-8441-8-3	NIST800-53-VI-ESXi-CFG-00018	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^ClientAliveInterval" /etc/ssh/sshd_config If there is no output or the output is not exactly "ClientAliveInterval 200", this is a finding.	200
CCE-8441-9-1	NIST800-53-VI-ESXi-CFG-00019	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^MaxSessions" /etc/ssh/sshd_config If there is no output or the output is not exactly "MaxSessions 1", this is a finding.	1

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8442-0-9	NIST800-53-VI-ESXi-CFG-00020	Enhanced	ESXi	<p>Connect via SSH and run the following command:</p> <pre># grep -i "^Ciphers" /etc/ssh/sshd_config</pre> <p>If there is no output or the output is not exactly "Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc", ciphers that are not FIPS-approved may be used, so this is a finding.</p>	aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc
CCE-8442-1-7	NIST800-53-VI-ESXi-CFG-00022	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Security.PasswordQualityControl</pre> <p>If Security.PasswordQualityControl is not set to "similar=deny retry=3 min=disabled,disabled,disabled,disabled,15", this is a finding.</p>	similar=deny retry=3 min=disabled,disabled,disabled,disabled,15
CCE-8442-2-5	NIST800-53-VI-ESXi-CFG-00028	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-VMHostFirewallException   Where {\$_.Name -eq 'SSH Server' -and \$_.Enabled -eq \$true}   Select Name, Enabled, @{N="AllIPEnabled";E={\$_.ExtensionData.AllowedHosts.AllIP}}</pre> <p>If for an enabled service "Allow connections from any IP address" is selected, this is a finding.</p>	AllIPEnabled: False
CCE-8442-3-3	NIST800-53-VI-ESXi-CFG-00030	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name UserVars.SuppressShellWarning</pre> <p>If UserVars.SuppressShellWarning is not set to 0, this is a finding.</p>	0
CCE-8442-4-1	NIST800-53-VI-ESXi-	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p>	lockdownNormal

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
	CFG-00031			<pre>Get-VMHost   Select Name,@{N="Lockdown";E={\$_.Extensiondata.Config.LockdownMode}}</pre> <p>If Lockdown Mode is disabled, this is a finding.</p> <p>For environments that do not use vCenter server to manage ESXi, this is not applicable.</p>	
CCE-8442 5-8	NIST800 53-VI-ESXi-CFG-00034	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Security.AccountLockFailures</pre> <p>If Security.AccountLockFailures is not set to 3, this is a finding.</p>	3
CCE-8442 6-6	NIST800 53-VI-ESXi-CFG-00038	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeout</pre> <p>If UserVars.ESXiShellInteractiveTimeout is not set to 600, this is a finding.</p>	600
CCE-8442 7-4	NIST800 53-VI-ESXi-CFG-00039	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name UserVars.ESXiShellTimeout</pre> <p>If UserVars.ESXiShellTimeout is not set to 600, this is a finding.</p>	600
CCE-8442 8-2	NIST800 53-VI-ESXi-CFG-00043	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Net.BlockGuestBPDU</pre> <p>If Net.BlockGuestBPDU is not set to 1, this is a finding.</p>	1
CCE-8442 9-0	NIST800 53-VI-ESXi-	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following commands:</p>	TRUE

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
	CFG-00056			<pre>\$esxcli = Get-ESxCli</pre> <pre>\$esxcli.system.coredump.network.get()</pre> <p>If there is no active core dump partition or the network core dump collector is not configured and enabled, this is a finding.</p>	
CCE-8443 0-8	NIST800 53-VI-ESXi-CFG-00106	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHostFirewallDefaultPolicy</pre> <p>If the Incoming or Outgoing policies are True, this is a finding.</p>	FALSE
CCE-8443 1-6	NIST800 53-VI-ESXi-CFG-00107	Enhanced	ESXi	<p>Log in to the host and run the following command:</p> <pre># ls -la /etc/ssh/keys-root/authorized_keys</pre> <p>If the <i>authorized_keys</i> file exists, this is a finding.</p>	File should not exist
CCE-8443 2-4	NIST800 53-VI-ESXi-CFG-00108	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHostSnmpp   Select *</pre> <p>or</p> <p>From a console or ssh session run the following command:</p> <pre>esxcli system snmp get</pre> <p>If SNMP is not in use and is enabled, this is a finding.</p> <p>If SNMP is enabled and “read only communities” is set to public, this is a finding.</p> <p>If SNMP is enabled and is not using v3 targets, this is a finding.</p> <p>Note: SNMP v3 targets can only be viewed and configured from the <i>esxcli</i> command.</p>	FALSE

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8443-3-2	NIST800-53-VI-ESXi-CFG-00109	Enhanced	ESXi	Connect via SSH and run the following command: # grep -i "^password" /etc/pam.d/passwd   grep sufficient If the remember setting is not set or is not "remember=5", this is a finding.	remember=5
CCE-8443-4-0	NIST800-53-VI-ESXi-CFG-00110	Built-in	ESXi	Run the following command: # grep -i "^password" /etc/pam.d/passwd   grep sufficient If sha512 is not listed, this is a finding.	sha512
CCE-8443-5-7	NIST800-53-VI-ESXi-CFG-00111	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: Get-VMHost   Get-VMHostService   Where {\$_.Label -eq "SSH"} If the ESXi SSH service is running, this is a finding.	Policy: Off and Running: False
CCE-8443-6-5	NIST800-53-VI-ESXi-CFG-00112	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: Get-VMHost   Get-VMHostService   Where {\$_.Label -eq "ESXi Shell"} If the ESXi Shell service is running, this is a finding.	Policy: Off and Running: False
CCE-8443-7-3	NIST800-53-VI-ESXi-CFG-00113	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: Get-VMHost   Get-VMHostService   Where {\$_.Label -eq "SSH"} If the ESXi SSH service is running, this is a finding.	Policy: Off and Running: False

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8443 8-1	NIST800 53-VI-ESXi-CFG-00114	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-VMHostAuthentication</pre> <p>For systems that do not use Active Directory and have no local user accounts, other than root, dcui, and/or vpxuser, this is not applicable.</p> <p>For systems that do not use Active Directory and do have local user accounts, other than root, dcui, and/or vpxuser, this is a finding.</p> <p>If Directory Services Type is not set to "Active Directory", this is a finding.</p>	sfo01.rainpole.local
CCE-8443 9-9	NIST800 53-VI-ESXi-CFG-00115	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to vCenter run the following command:</p> <pre>Get-VMHost   Select Name, ` @{N="HostProfile";E={\$_   Get-VMHostProfile}}, ` @{N="JoinADEnabled";E=({\$_   Get-VmHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory.Enabled}}, ` @{N="JoinDomainMethod";E=({(\$_   Get-VMHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory   Select -ExpandProperty Policy   Where {\$_ .Id -eq "JoinDomainMethodPolicy"}}).Policyoption.Id}}</pre> <p>Verify if "JoinADEnabled" is "True" then "JoinDomainMethod" should be "FixedCAMConfigOption".</p> <p>For systems that do not use Active Directory and have no local user accounts, other than root, dcui, and/or vpxuser, this is not applicable.</p> <p>For systems that do not use Active Directory and do have local user accounts, other than root, dcui, and/or vpxuser, this is a finding.</p> <p>If vSphere Authentication Proxy is not used to join hosts to an Active Directory domain, this is a finding.</p>	JoinADEnabled: True, JoinDomainMethod: Fixed-CAMConfigOption

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8444 0-7	NIST800 53-VI-ESXi-CFG-00116	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-VMHostAuthentication</pre> <p>For systems that do not use Active Directory and have no local user accounts, other than root, dcui, and/or vpxuser, this is not applicable.</p> <p>For systems that do not use Active Directory and do have local user accounts, other than root, dcui, and/or vpxuser, this is a finding.</p> <p>If the Directory Services Type is not set to "Active Directory", this is a finding.</p>	sfo01.rainpole.local
CCE-8444 1-5	NIST800 53-VI-ESXi-CFG-00117	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to vCenter run the following command:</p> <pre>Get-VMHost   Select Name, ` @{N="HostProfile";E={\$_   Get-VMHostProfile}}, ` @{N="JoinADEnabled";E=({\$_   Get-VmHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory.Enabled}}, ` @{N="JoinDomainMethod";E=({(\$_   Get-VMHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory   Select -ExpandProperty Policy   Where {\$_ .Id -eq "JoinDomainMethodPolicy"}}).Policyoption.Id}}</pre> <p>Verify if "JoinADEnabled" is "True" then "JoinDomainMethod" should be "FixedCAMConfigOption".</p> <p>For systems that do not use Active Directory and have no local user accounts, other than root, dcui, and/or vpxuser, this is not applicable.</p> <p>For systems that do not use Active Directory and do have local user accounts, other than root, dcui, and/or vpxuser, this is a finding.</p> <p>If vSphere Authentication Proxy is not used to join hosts to an Active Directory domain, this is a finding.</p>	sfo01.rainpole.local

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8444-2-3	NIST800-53-VI-ESXi-CFG-00118	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-VMHostAuthentication</pre> <p>For systems that do not use Active Directory and have no local user accounts, other than root, dcui, and/or vpxuser, this is not applicable.</p> <p>For systems that do not use Active Directory and do have local user accounts, other than root, dcui, and/or vpxuser, this is a finding.</p> <p>If Directory Services Type is not set to "Active Directory", this is a finding.</p>	sfo01.rainpole.local
CCE-8444-3-1	NIST800-53-VI-ESXi-CFG-00119	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to vCenter run the following command:</p> <pre>Get-VMHost   Select Name, ` @{N="HostProfile";E={\$_   Get-VMHostProfile}}, ` @{N="JoinADEnabled";E=({\$_   Get-VmHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory.Enabled}}, ` @{N="JoinDomainMethod";E=({(\$_   Get-VMHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory   Select -ExpandProperty Policy   Where {\$_ .Id -eq "JoinDomainMethodPolicy"}}).Policyoption.Id}}</pre> <p>Verify if "JoinADEnabled" is "True" then "JoinDomainMethod" should be "FixedCAMConfigOption".</p> <p>For systems that do not use Active Directory and have no local user accounts, other than root, dcui, and/or vpxuser, this is not applicable.</p> <p>For systems that do not use Active Directory and do have local user accounts, other than root, dcui, and/or vpxuser, this is a finding.</p> <p>If vSphere Authentication Proxy is not used to join hosts to an Active Directory domain, this is a finding.</p>	sfo01.rainpole.local



CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8444-4-9	NIST800-53-VI-ESXi-CFG-00120	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-VMHostAuthentication</pre> <p>For systems that do not use Active Directory and have no local user accounts, other than root, dcui, and/or vpxuser, this is not applicable.</p> <p>For systems that do not use Active Directory and do have local user accounts, other than root, dcui, and/or vpxuser, this is a finding.</p> <p>If Directory Services Type is not set to "Active Directory", this is a finding.</p>	sfo01.rainpole.local
CCE-8444-5-6	NIST800-53-VI-ESXi-CFG-00121	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to vCenter run the following command:</p> <pre>Get-VMHost   Select Name, ` @{N="HostProfile";E={\$_   Get-VMHostProfile}}, ` @{N="JoinADEnabled";E=({\$_   Get-VmHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory.Enabled}}, ` @{N="JoinDomainMethod";E=({(\$_   Get-VMHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory   Select -ExpandProperty Policy   Where {\$_ .Id -eq "JoinDomainMethodPolicy"}) .Policyoption.Id}}</pre> <p>Verify if "JoinADEnabled" is "True" then "JoinDomainMethod" should be "FixedCAMConfigOption".</p> <p>For systems that do not use Active Directory and have no local user accounts, other than root, dcui, and/or vpxuser, this is not applicable.</p> <p>For systems that do not use Active Directory and do have local user accounts, other than root, dcui, and/or vpxuser, this is a finding.</p> <p>If vSphere Authentication Proxy is not used to join hosts to an Active Directory domain, this is a finding.</p>	sfo01.rainpole.local

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8444 6-4	NIST800 53-VI- ESXi- CFG- 00122	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Annotations.WelcomeMessage</pre> <p>Check for the login banner text (mentioned in the parameter value) based on the character limitations imposed by the system. An exact match of the text is required. If this banner is not displayed, this is a finding.</p>	<p>This system is for the use of authorized users only. Individuals using this computer system without authority or in excess of their authority are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.</p>

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8444 7-2	NIST800-53-VI-ESXi-CFG-00123	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Config.Etc.issue</pre> <p>If the Config.Etc.issue setting (<i>/etc/issue</i> file) does not contain the logon banner exactly as shown in the parameter value, this is a finding.</p>	<p>This system is for the use of authorized users only. Individuals using this computer system without authority or in excess of their authority are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.</p>

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84448-0	NIST80053-VI-ESXi-CFG-00124	Enhanced	ESXi	<p>Connect via SSH and run the following command:</p> <pre># grep -i "^Banner" /etc/ssh/sshd_config</pre> <p>If there is no output or the output is not exactly "Banner /etc/issue", this is a finding.</p>	<p>This system is for the use of authorized users only. Individuals using this computer system without authority or in excess of their authority are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.</p>

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8444-9-8	NIST800-53-VI-ESXi-CFG-00125	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following script:</p> <pre>\$vmhost = Get-VMHost   Get-View \$lockdown = Get-View \$vmhost.ConfigManager.HostAccessManager \$lockdown.QueryLockdownExceptions()</pre> <p>If the exception users list contains accounts that do not require special permissions, this is a finding.</p> <p>Note: This list is not intended for system administrator accounts but for special circumstances such as a service account.</p>	Remove unnecessary users from the exception user list
CCE-8445-0-6	NIST800-53-VI-ESXi-CFG-00127	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Annotations.WelcomeMessage</pre> <p>Check for the login banner text (mentioned in the parameter value) based on the character limitations imposed by the system. An exact match of the text is required. If this banner is not displayed, this is a finding.</p>	This system is for the use of authorized users only. Individuals using this computer system without authority or in excess of their authority are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
					activity, system personnel may provide the evidence of such monitoring to law enforcement officials.
CCE-8445 1-4	NIST800 53-VI-ESXi-CFG-00129	Enhanced	ESXi	<p>If vCenter Update Manager is used on the network, it can scan all hosts for missing patches. From the vSphere Client, go to <b>Hosts and Clusters</b> &gt;&gt; <b>Update Manager</b> tab, and select <b>Scan</b> to view all hosts' compliance status.</p> <p>If vCenter Update Manager is not used, a host's compliance status must be manually determined by the build number. VMware KB 1014508 can be used to correlate patches with build numbers.</p> <p>If the ESXi host does not have the latest patches, this is a finding.</p> <p>If the ESXi host is not on a supported release, this is a finding.</p>	Apply latest patches and updates
CCE-8445 2-2	NIST800 53-VI-ESXi-CFG-00134	Enhanced	ESXi	<p>The downloaded ISO, offline bundle, or patch hash must be verified against the vendor's checksum to ensure the integrity and authenticity of the files. See the typical command line example for the sha1 hash check:</p> <pre># sha1sum &lt;filename&gt;.iso</pre> <p>If any of the system's downloaded ISO, offline bundle, or system patch hashes cannot be verified against the vendor's checksum, this is a finding.</p>	Compare the SHA1 sum output with the value posted on the VMware Web site. They should match.
CCE-8445 3-0	NIST800 53-VI-ESXi-CFG-00135	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Syslog.global.logHost</pre> <p>If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.</p>	udp://sfo01vrli01.sfo01.rainpole.local:514

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8445-4-8	NIST800-53-VI-ESXi-CFG-00136	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: <code>Get-VMHost   Get-AdvancedSetting -Name Syslog.global.logDir</code> If LocalLogOutputIsPersistent is not set to true, this is a finding.	[] /scratch/log
CCE-8445-5-5	NIST800-53-VI-ESXi-CFG-00137	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: <code>Get-VMHost   Get-AdvancedSetting -Name Config.HostAgent.plugins.hostsvc.esxAdminsGroup</code> For systems that do not use Active Directory and have no local user accounts, other than root, dcui, and/or vpxuser, this is not applicable. For systems that do not use Active Directory and do have local user accounts, other than root, dcui, and/or vpxuser, this is a finding. If Config.HostAgent.plugins.hostsvc.esxAdminsGroup is set to "ESX Admins", this is a finding.	ug-SDDC-Admins
CCE-8445-6-3	NIST800-53-VI-ESXi-CFG-00138	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: <code>Get-VMHost   Get-AdvancedSetting -Name Mem.ShareForceSalting</code> If Mem.ShareForceSalting is not set to 2, this is a finding.	2
CCE-8445-7-1	NIST800-53-VI-ESXi-CFG-00139	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: <code>Get-VMHostFirewallDefaultPolicy</code> If the Incoming or Outgoing policies are True, this is a finding.	N/A
CCE-8445-8-9	NIST800-53-VI-ESXi-	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: <code>Get-VMHost   Get-AdvancedSetting -Name Syslog.global.logHost</code>	udp://sfo01vrli01.sfo01.rainpole.local:514

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
	CFG-00141			If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.	
CCE-84459-7	NIST80053-VI-ESXi-CFG-00142	Enhanced	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Config.HostAgent.plugins.hostsvc.esxAdminsGroup</pre> <p>For systems that do not use Active Directory and have no local user accounts, other than root, dcui, and/or vpxuser, this is not applicable.</p> <p>For systems that do not use Active Directory and do have local user accounts, other than root, dcui, and/or vpxuser, this is a finding.</p> <p>If Config.HostAgent.plugins.hostsvc.esxAdminsGroup is set to "ESX Admins", this is a finding.</p>	ug-SDDC-Admins
CCE-84460-5	NIST80053-VI-ESXi-CFG-00143	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Syslog.global.logHost</pre> <p>If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.</p>	udp://sfo01vrli01.sfo01.rainpole.local:514
CCE-84461-3	NIST80053-VI-ESXi-CFG-00145	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-VMHostNTPServer Get-VMHost   Get-VMHostService   Where {\$_.Label -eq "NTP Daemon"}</pre> <p>If the NTP service is not configured with authoritative DoD time sources and the service is not configured to start and stop with the host and is running, this is a finding.</p>	ntp.lax01.rainpole.local, ntp.sfo01.rainpole.local
CCE-84462-1	NIST80053-VI-ESXi-CFG-00157	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following commands:</p> <pre>\$esxcli = Get-EsxCli \$esxcli.software.acceptance.get()</pre> <p>If the acceptance level is CommunitySupported, this is a finding.</p>	PartnerSupported



CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8446-3-9	NIST800-53-VI-ESXi-CFG-00158	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: <pre>\$esxcli = Get-ESxCli \$esxcli.software.acceptance.get()</pre> If the acceptance level is CommunitySupported, this is a finding.	PartnerSupported
CCE-8446-4-7	NIST800-53-VI-ESXi-CFG-00159	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: <pre>\$esxcli = Get-ESxCli \$esxcli.software.acceptance.get()</pre> If the acceptance level is CommunitySupported, this is a finding.	PartnerSupported
CCE-8446-5-4	NIST800-53-VI-ESXi-CFG-00160	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: <pre>\$esxcli = Get-ESxCli \$esxcli.software.acceptance.get()</pre> If the acceptance level is CommunitySupported, this is a finding.	PartnerSupported
CCE-8446-6-2	NIST800-53-VI-ESXi-CFG-00161	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: <pre>Get-VDSwitch   Get-VDSecurityPolicy Get-VDPortGroup   Get-VDSecurityPolicy</pre> If Forged Transmits is set to accept, this is a finding.	FALSE
CCE-8446-7-0	NIST800-53-VI-ESXi-CFG-00162	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: <pre>Get-VDSwitch   Get-VDSecurityPolicy Get-VDPortGroup   Get-VDSecurityPolicy</pre> If MAC Address Changes is set to accept, this is a finding.	FALSE

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8446-8-8	NIST800-53-VI-ESXi-CFG-00163	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name DCUI.Access</pre> <p>If DCUI.Access is not restricted to root, this is a finding.</p> <p>Note: This list is only for local user accounts and should only contain the root user.</p>	root
CCE-8446-9-6	NIST800-53-VI-ESXi-CFG-00164	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Syslog.global.logHost</pre> <p>If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.</p>	udp://sfo01vrli01.sfo01.rainpole.local:514
CCE-8447-0-4	NIST800-53-VI-ESXi-CFG-00165	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Security.AccountUnlockTime</pre> <p>If Security.AccountUnlockTime is not set to 900, this is a finding.</p>	900
CCE-8447-1-2	NIST800-53-VI-ESXi-CFG-00166	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Config.HostAgent.plugins.solo.enableMob</pre> <p>If Config.HostAgent.plugins.solo.enableMob is not set to false, this is a finding.</p>	FALSE
CCE-8447-2-0	NIST800-53-VI-ESXi-CFG-00167	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Config.HostAgent.plugins.hostsvc.esxAdminsGroup</pre> <p>For systems that do not use Active Directory and have no local user accounts, other than root, dcui, and/or vpxuser, this is not applicable.</p>	ug-SDDC-Admins

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
				For systems that do not use Active Directory and do have local user accounts, other than root, dcui, and/or vpxuser, this is a finding. If Config.HostAgent.plugins.hostsvc.esxAdminsGroup is set to "ESX Admins", this is a finding.	
CCE-8447 3-8	NIST800 53-VI-ESXi-CFG-00168	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: <code>Get-VMHost   Get-AdvancedSetting -Name UserVars.DcuiTimeOut</code> If UserVars.DcuiTimeOut is not set to 600, this is a finding.	600
CCE-8447 4-6	NIST800 53-VI-ESXi-CFG-00169	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: <code>Get-VMHost   Get-AdvancedSetting -Name Net.DVFilterBindIpAddress</code> If Net.DVFilterBindIpAddress is not blank and security appliances are not in use on the host, this is a finding.	""
CCE-8447 5-3	NIST800 53-VI-ESXi-CFG-00170	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: <code>Get-VMHost   Get-AdvancedSetting -Name Syslog.global.logHost</code> If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.	udp://sfo01vrli01.sfo01.rainpole.local:514
CCE-8447 6-1	NIST800 53-VI-ESXi-CFG-00171	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: <code>Get-VMHost   Get-AdvancedSetting -Name UserVars.DcuiTimeOut</code> If UserVars.DcuiTimeOut is not set to 600, this is a finding.	600
CCE-8447 7-9	NIST800 53-VI-ESXi-	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: <code>Get-VMHost   Get-AdvancedSetting -Name Syslog.global.logHost</code> If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.	udp://sfo01vrli01.sfo01.rainpole.local:514

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
	CFG-00172				
CCE-84478-7	NIST80053-VI-ESXi-CFG-00173	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Config.HostAgent.plugins.hostsvc.esxAdminsGroup</pre> <p>For systems that do not use Active Directory and have no local user accounts, other than root, dcui, and/or vpxuser, this is not applicable.</p> <p>For systems that do not use Active Directory and do have local user accounts, other than root, dcui, and/or vpxuser, this is a finding.</p> <p>If the Config.HostAgent.plugins.hostsvc.esxAdminsGroup keyword is set to “ESX Admins”, this is a finding.</p>	ug-SDDC-Admins
CCE-84479-5	NIST80053-VI-ESXi-CFG-00174	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Syslog.global.logHost</pre> <p>If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.</p>	udp://sfo01vrli01.sfo01.rainpole.local:514
CCE-84480-3	NIST80053-VI-ESXi-CFG-00175	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Config.HostAgent.plugins.hostsvc.esxAdminsGroup</pre> <p>For systems that do not use Active Directory and have no local user accounts, other than root, dcui, and/or vpxuser, this is not applicable.</p> <p>For systems that do not use Active Directory and do have local user accounts, other than root, dcui, and/or vpxuser, this is a finding.</p> <p>If Config.HostAgent.plugins.hostsvc.esxAdminsGroup is set to “ESX Admins”, this is a finding.</p>	ug-SDDC-Admins

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8448 1-1	NIST800 53-VI-ESXi-CFG-00176	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Syslog.global.logHost</pre> <p>If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.</p>	udp://sfo01vrli01.sfo01.rainpole.local:514
CCE-8448 2-9	NIST800 53-VI-ESXi-CFG-00177	Built-in	ESXi	<p>The vMotion VMkernel port group should be in a dedicated VLAN that can be on a common standard or distributed virtual switch as long as the vMotion VLAN is not shared by any other function and it is not routed to anything but ESXi hosts. The check for this will be unique per environment.</p> <p>From the vSphere Client, select the ESXi host and go to <b>Configure &gt; Networking &gt; VMKernel adapters</b>. Review the VLANs associated with the vMotion VMkernel(s) and verify they are dedicated for that purpose and logically separated from other functions.</p> <p>If long distance or cross vCenter vMotion is used, the vMotion network can be routable but must be accessible to only the intended ESXi hosts.</p> <p>If the vMotion port group is not on an isolated VLAN and/or is routable to systems other than ESXi hosts, this is a finding.</p> <p>For environments that do not use vCenter Server to manage ESXi, this is not applicable.</p>	vMotion VMKernel Port group should be in a dedicated VLAN. The check for this will be unique per environment.
CCE-8448 3-7	NIST800 53-VI-ESXi-CFG-00178	Built-in	ESXi	<p>The Management VMkernel port group should be in a dedicated VLAN that can be on a common standard or distributed virtual switch as long as the Management VLAN is not shared by any other function and it is not routed to anything other than management related functions such as vCenter. The check for this will be unique per environment.</p> <p>From the vSphere Client, select the ESXi host and go to <b>Configure &gt; Networking &gt; VMKernel adapters</b>. Review the VLANs associated with the Management VMkernel and verify they are dedicated for that purpose and logically separated from other functions.</p> <p>If the network segment is routed, except to networks where other management-related entities are located such as vCenter, this is a finding.</p> <p>If production virtual machine traffic is routed to this network, this is a finding.</p>	Management VMKernel Port group should be in a dedicated VLAN. The check for this will be unique per environment

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8448-4-5	NIST800-53-VI-ESXi-CFG-00179	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Config.HostAgent.log.level</pre> <p>If Config.HostAgent.log.level is not set to info, this is a finding.</p> <p>Note: Verbose logging level is acceptable for troubleshooting purposes.</p>	info
CCE-8448-5-2	NIST800-53-VI-ESXi-CFG-00180	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Config.HostAgent.log.level</pre> <p>If Config.HostAgent.log.level is not set to info, this is a finding.</p> <p>Note: Verbose logging level is acceptable for troubleshooting purposes.</p>	info
CCE-8448-6-0	NIST800-53-VI-ESXi-CFG-00181	Built-in	ESXi	<p>From the vSphere Client, select the ESXi Host and go to <b>Configure &gt;&gt; Networking &gt;&gt; VMkernel adapters</b>. Review each VMkernel adapter that is defined and ensure it is enabled for only one type of management traffic.</p> <p>If any VMkernel is used for more than one type of management traffic, this is a finding.</p>	N/A
CCE-8448-7-8	NIST800-53-VI-ESXi-CFG-00182	Built-in	ESXi	<p>From the vSphere Client, select the ESXi Host and go to <b>Configure &gt;&gt; Networking &gt;&gt; TCP/IP Configuration</b>. Review the default system TCP/IP stacks and verify they are configured with the appropriate IP address information.</p> <p>If any system TCP/IP stack is configured and not in use by a VMkernel adapter, this is a finding.</p>	N/A
CCE-8448-8-6	NIST800-53-VI-ESXi-CFG-00192	Built-in	ESXi	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-VMHostNTPServer Get-VMHost   Get-VMHostService   Where {\$_.Label -eq "NTP Daemon"}</pre> <p>If the NTP service is not configured with authoritative DoD time sources and the service is not configured to start and stop with the host and is running, this is a finding.</p>	Policy: On and Running: True

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8448-9-4	NIST800-53-VI-ESXi-CFG-00184	Built-in	ESXi	This check refers to an entity outside the physical scope of the ESXi server system. The configuration of upstream physical switches must be documented to ensure that spanning tree protocol is disabled and/or portfast is configured for all physical ports connected to ESXi hosts. Inspect the documentation and verify that the documentation is updated on a regular basis and/or whenever modifications are made to either ESXi hosts or the upstream physical switches. Alternatively, log in to the physical switch and verify that spanning tree protocol is disabled and/or portfast is configured for all physical ports connected to ESXi hosts. If the physical switch's spanning tree protocol is not disabled or portfast is not configured for all physical ports connected to ESXi hosts, this is a finding.	N/A
CCE-8450-1-6	NIST800-53-VI-NET-CFG-00251	Built-in	NSX	From the vSphere Web Client, go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Policies &gt;&gt; Password Policy</b> .	NSX Manager Appliance - NSX Domain Service Account - Password (Dependent on Customer Configurations)
CCE-8450-2-4	NIST800-53-VI-NET-CFG-00252	Built-in	NSX	From the vSphere Web Client, go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Policies &gt;&gt; Password Policy</b> .	Border Gateway Protocol Password (Dependent on Customer Configurations)
CCE-8450-3-2	NIST800-53-VI-NET-CFG-00253	Built-in	NSX	From the vSphere Web Client, go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Policies &gt;&gt; Password Policy</b> .	Universal Distributed Logical Router Password (Dependent on Customer Configurations)

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84504-0	NIST80053-VI-NET-CFG-00281	Built-in	NSX	Log on to NSX Manager Virtual Appliance, then go to <b>Backup &amp; Restore</b> . If “Audit Logs” or “System Events” are excluded (by default they are NOT excluded), this is a finding.	Audit Logs and System Events are not excluded
CCE-84505-7	NIST80053-VI-NET-CFG-00282	Built-in	NSX	Log on to NSX Manager Virtual Appliance, then go to <b>Manage Appliance Settings</b> and look under <b>General Network Settings</b> . If IPv6 is configured, this is a finding.	IPv6 should be disabled
CCE-84506-5	NIST80053-VI-NET-CFG-00283	Built-in	NSX	Log on to NSX Manager Virtual Appliance, then go to <b>Manage Appliance Settings</b> and look under <b>DNS Servers</b> . If IPv6 DNS is configured, this is a finding.	IPv6 DNS should be disabled
CCE-84507-3	NIST80053-VI-NET-CFG-00285	Built-in	NSX	Log on to NSX Manager Virtual Appliance, then go to <b>Manage Appliance Settings</b> and look under <b>Time Settings</b> . If any of the NTP Servers are not authorized or trusted, this is a finding.	1) Use at least three NTP servers from outside time sources -OR- 2) Configure a few local NTP servers on a trusted network that in turn obtain their time from at least three outside time sources



CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8450-8-1	NIST800-53-VI-NET-CFG-00286	Built-in	NSX	Log on to NSX Manager Virtual Appliance and go to <b>Manage Appliance Settings</b> . Verify syslog server configuration.	Remote syslog server is configured
CCE-8450-9-9	NIST800-53-VI-NET-CFG-00287	Built-in	NSX	Log on to NSX Manager Virtual Appliance, then go to <b>Manage Appliance Settings --&gt; SSL Certificates</b> . Click on the certificate and verify certificate details.	1) Appropriate issuer 2) Correct certificate type 3) RSA algorithm 4) 2048-bit keys or higher
CCE-8451-0-7	NIST800-53-VI-NET-CFG-00288	Built-in	NSX	Access the deployment and try to reach NSX Manager on the standard network. NSX Manager should only be reachable using isolation mechanisms.	Procedural
CCE-8451-1-5	NIST800-53-VI-NET-CFG-00289	Built-in	NSX	Log in to the VMware vSphere environment and inspect which users have access permissions to NSX Manager Virtual Appliance.  If any user other than the intended administrator has access or is able to carry out any administrative actions, this is a finding.	Procedural
CCE-8451-2-3	NIST800-53-VI-NET-CFG-00290	Built-in	NSX	Log in to the SFTP server and navigate to the backup directory.  If the backup directory can be read from or written to by users other than the backup user, this is a finding.	No read or write permissions on backup directory

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84513-1	NIST800-53-VI-NET-CFG-00291	Built-in	NSX	Log on to NSX Manager Virtual Appliance, then go to <b>Manage Appliance Settings</b> and look under <b>General network settings</b> . If IPv4 DNS is not authorized or secure, this is a finding.	IPv4 DNS is authorized and secure
CCE-84514-9	NIST800-53-VI-NET-CFG-00294	Built-in	NSX	Log on to NSX Manager Virtual Appliance, then look under <b>Backup &amp; Restore</b> . Verify “FTP Server settings”.	FTP Server settings (Dependent on Customer Configurations)
CCE-84515-6	NIST800-53-VI-NET-CFG-00295	Built-in	NSX	After downloading the media, use the SHA1 sum value to verify the integrity of the download. Compare the SHA1 hash output with the value posted on the VMware secure website. If the hash output does not match the website value, this is a finding.	SHA1 hash should match
CCE-84516-4	NIST800-53-VI-NET-CFG-00296	Built-in	NSX	If the controller network is not deployed on a network that is not configured for or connected to other types of traffic, this is a finding.	Procedural (Dependent on Customer Configurations)
CCE-84517-2	NIST800-53-VI-NET-CFG-00297	Built-in	NSX	Run this REST API call to get the properties of the controller node: <code>https://&lt;nsxmgr&gt;/api/2.0/vdn/controller/node</code> <b>Response:</b> <controllerNodeConfig> <ipSecEnabled>true</ipSecEnabled> </controllerNodeConfig> If ipSecEnabled is not true, this is a finding.	<ipSecEnabled>true</ipSecEnabled>

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84518-0	NIST80053-VI-NET-CFG-00300	Built-in	NSX	Thoroughly review the deployment. If the virtual network is not isolated, this is a finding.	Procedural (Dependent on Customer Configurations)
CCE-84519-8	NIST80053-VI-NET-CFG-00301	Built-in	NSX	Do a thorough check on the infrastructure design and deployment network diagram. If there are any non-hypervisors on the logical network data plane or if any untrusted hypervisors are used, this is a finding.	Procedural (Dependent on Customer Configurations)
CCE-84520-6	NIST80053-VI-NET-CFG-00302	Built-in	NSX	Use the vSphere Web Client to connect to the vCenter Server. As administrator, go to <b>Home &gt; Inventory &gt; Networking</b> . Select “DSwitch” for distributed portgroups. Select each dvPortgroup connected to active VMs requiring securing. Go to tab <b>Summary &gt; Edit Settings &gt; Policies &gt; Security</b> . If Forged Transmits is not set to Reject, this is a finding.	Reject
CCE-84521-4	NIST80053-VI-NET-CFG-00303	Built-in	NSX	Use the vSphere Web Client to connect to the vCenter Server. As administrator, go to <b>Home &gt; Inventory &gt; Networking</b> . Select “DSwitch” for distributed portgroups. Select each dvPortgroup connected to active VMs requiring securing. Go to tab <b>Summary &gt; Edit Settings &gt; Policies &gt; Security</b> . If Mac Address Changes is not set to Reject, this is a finding.	Reject
CCE-84522-2	NIST80053-VI-NET-CFG-00304	Built-in	NSX	Use the vSphere Web Client to connect to the vCenter Server. As administrator, go to <b>Home &gt; Inventory &gt; Networking</b> . Select “DSwitch” for distributed portgroups. Select each dvPortgroup connected to active VMs requiring securing. Go to tab <b>Summary &gt; Edit Settings &gt; Policies &gt; Security</b> . If Promiscuous Mode is not set to Reject, this is a finding.	Reject

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84523-0	NIST80053-VI-NET-CFG-00306	Built-in	NSX	Log in to VMware vSphere Web Client. Navigate to <b>Networking and Security --&gt; Installation and Upgrade</b> . Go to the “Host Preparation” tab. Under the “VXLAN” column, select “View Configuration”. If VMKNic Teaming Policy is not set to “Load Balance - SRCID”, this is a finding.	Load Balance - SRCID
CCE-84524-8	NIST80053-VI-NET-CFG-00308	Built-in	NSX	Log into the vCenter web interface with credentials authorized for administration. Navigate to <b>Networking and Security &gt;&gt; Firewall</b> . Expand “Default Section Layer 3” in Configuration. If the action for the Default Rule is “Allow”, this is a finding.	Denied
CCE-84525-5	NIST80053-VI-NET-CFG-00311	Built-in	NSX	Log on to vSphere Web Client with credentials authorized for administration. Navigate and select <b>Networking and Security &gt;&gt; Users and Domains</b> . View each role and verify the users and/or groups assigned to it.	Procedural
CCE-84526-3	NIST80053-VI-NET-CFG-00312	Built-in	NSX	From the vSphere Web Client, go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Configuration &gt;&gt; Policies &gt;&gt; Password Policy</b> . View the values of the password format requirements. If Numeric Characters is not set to at least 1, this is a finding.	1
CCE-84527-1	NIST80053-VI-NET-CFG-00313	Built-in	NSX	From the vSphere Web Client, go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Configuration &gt;&gt; Policies &gt;&gt; Password Policy</b> . View the values of the password format requirements. If Special Characters is not set to at least 1, this is a finding.	1

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84528-9	NIST800-53-VI-NET-CFG-00316	Built-in	NSX	Log on to vSphere Web Client with credentials authorized for administration. Navigate and select <b>Networking and Security &gt;&gt; Users and Domains</b> . View each role and verify the users and/or groups assigned to it. If any user or service account has more privileges than required, this is a finding.	Procedural
CCE-84529-7	NIST800-53-VI-NET-CFG-00317	Built-in	NSX	Log into NSX Manager with built-in administrator account “admin” and default manufacturer password “default”. If the NSX Manager accepts the default password, this is a finding.	Non-default password
CCE-84530-5	NIST800-53-VI-NET-CFG-00318	Built-in	NSX	Log into vSphere Web Client with credentials authorized for administration. Navigate to <b>Networking and Security &gt;&gt; Firewall</b> . Expand rule sections as necessary to view rules. If there are no rules configured to enforce authorizations, this is a finding.	Procedural
CCE-84531-3	NIST800-53-VI-NET-CFG-00321	Built-in	NSX	From the vSphere Web Client, go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Configuration &gt;&gt; Policies &gt;&gt; Password Policy</b> . View the values of the password format requirements. If Lower-Case Characters is not set to at least 1, this is a finding.	1
CCE-84532-1	NIST800-53-VI-NET-CFG-00322	Built-in	NSX	From the vSphere Web Client, go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Configuration &gt;&gt; Policies &gt;&gt; Password Policy</b> . If Upper-Case Characters is not set to at least 1, this is a finding.	1

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84533-9	NIST80053-VI-NET-CFG-00323	Enhanced	NSX	Log into vSphere Web Client with credentials authorized for administration. Navigate and select <b>Networking and Security</b> >> <b>Firewall</b> tab to display a list of firewall rules deployed across the NSX environment. Click on the dropdown arrow to expand each firewall rule's section. For each rule, select the pencil icon in the "Action" column. If the "Log" option has not been enabled for all rules, this is a finding.	Log
CCE-84534-7	NIST80053-VI-NET-CFG-00324	Enhanced	NSX	Log into vSphere Web Client with credentials authorized for administration. Navigate and select <b>Networking and Security</b> >> <b>SpoofGuard</b> . Check the Default policy of each NSX Manager. If the mode is disabled, this is a finding.	Enabled
CCE-84535-4	NIST80053-VI-NET-CFG-00328	Built-in	NSX	Log onto vSphere Web Client with credentials authorized for administration. Navigate and select <b>Networking and Security</b> >> and select the <b>NSX Edges</b> tab on the left-side menu. Double-click the Edge ID. Navigate to <b>Manage</b> >> <b>Verify</b> the configurations under <b>Settings, Firewall, Routing, Bridging, and DHCP Relay</b> are enabled only as necessary for the deployment. If unnecessary services are enabled, this is a finding.	Enabled
CCE-84536-2	NIST80053-VI-NET-CFG-00329	Built-in	NSX	If the built-in SSO administrator account is used for daily operations or there is no policy restricting its use, this is a finding.	Procedural (Dependent on Customer Configurations)
CCE-84537-0	NIST80053-VI-NET-CFG-00330	Built-in	NSX	From the vSphere Web Client, go to <b>Administration</b> >> <b>Single Sign-On</b> >> <b>Configuration</b> >> <b>Policies</b> >> <b>Password Policy</b> . If Restrict Reuse is not set to "5" or more, this is a finding.	5

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8453-8-8	NIST800-53-VI-NET-CFG-00340	Built-in	NSX	Go to the vSphere Web Client URL <i>https://client-hostname/vsphere-client</i> and verify the CA certificate is signed by an approved service provider. If a public key certificate from an appropriate certificate policy through an approved service provider is not used, this is a finding.	Procedural
CCE-8453-9-6	NIST800-53-VI-NET-CFG-00343	Built-in	NSX	Log into vSphere Web Client with credentials authorized for administration. Navigate and select <b>Networking and Security</b> >> <b>Firewall</b> . If there are services enabled that should not be, this is a finding.	Procedural
CCE-8454-0-4	NIST800-53-VI-NET-CFG-00344	Built-in	NSX	Log into vSphere Web Client with credentials authorized for administration. Navigate and select <b>Networking and Security</b> >> <b>Firewall</b> . If ports, protocols, and/or services are not disabled or restricted as required by the PPSM, this is a finding.	Procedural
CCE-8454-1-2	NIST800-53-VI-NET-CFG-00360	Built-in	NSX	Log onto vSphere Web Client with credentials authorized for administration. Navigate and select <b>Networking and Security</b> >> and select the <b>NSX Edges</b> tab on the left-side menu. Double-click the EdgeID. Click on the <b>Configure</b> tab on the top of the new screen, then <b>Interfaces</b> . Check the "Connection Status" column for the associated interface. If any inactive router interfaces are not disabled, this is a finding.	Procedural
CCE-8454-2-0	NIST800-53-VI-NET-CFG-00372	Built-in	NSX	Log on to NSX Manager with credentials authorized for administration. Navigate and select <b>Backup and Restore</b> >> <b>Backup History</b> . If backups are not being sent to a centralized location when changes occur or weekly, whichever is sooner, this is a finding.	Procedural

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8430 1-1	NIST800 53-VI-VC-CFG-00060	Enhanced	vCenter	<p>Ask the system administrator if hardened, patched templates are used for VM creation with properly configured OS deployments, including applications both dependent and non-dependent on VM-specific configurations.</p> <p>If hardened, patched templates are not used for VM creation, this is a finding. The system must use templates to deploy VMs whenever possible.</p>	Hardened virtual machine templates to use for OS deployments
CCE-8430 2-9	NIST800 53-VI-ESXI-CFG-00061	Enhanced	vCenter	<p>On the Home page of the vSphere Client, select <b>Menu &gt; Administration</b> and click <b>Roles</b>. Select the VC from the Roles provider drop-down menu. Select the Virtual machine user (sample) role and click <b>Privileges</b>.</p> <p>If the Console Interaction privilege is assigned to the role, this is a finding. If SSH and/or terminal management services are exclusively used to perform management tasks, this is not a finding.</p>	Disable Console Interaction privilege
CCE-8430 3-7	NIST800 53-VI-ESXI-CFG-00065	Built-in	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM   Where {\$_.ExtensionData.Config.Hardware.Device.DeviceInfo.Label -match "parallel"}</pre> <p>If a virtual machine has a parallel device present, this is a finding.</p>	Disconnect unauthorized parallel devices
CCE-8430 4-5	NIST800 53-VI-ESXI-CFG-00066	Built-in	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM   Where {\$_.ExtensionData.Config.Hardware.Device.DeviceInfo.Label -match "serial"}</pre> <p>If a virtual machine has a serial device present, this is a finding.</p>	Disconnect unauthorized serial devices
CCE-8430 5-2	NIST800 53-VI-ESXI-CFG-00067	Built-in	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM   Get-UsbDevice</pre> <p>If a virtual machine has any USB devices or USB controllers present, this is a finding.</p>	No USB device present



CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84306-0	NIST80053-VI-ESXI-CFG-00068	Built-in	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name sched.mem.pshare.salt If sched.mem.pshare.salt exists, this is a finding.	Remove the advanced setting sched.mem.pshare.salt
CCE-84307-8	NIST80053-VI-ESXI-CFG-00070	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.copy.disable If isolation.tools.copy.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84308-6	NIST80053-VI-ESXI-CFG-00071	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.dnd.disable If isolation.tools.dnd.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84309-4	NIST80053-VI-ESXI-CFG-00072	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.setGUIOptions.enable If isolation.tools.setGUIOptions.enable does not exist or is not set to false, this is a finding.	FALSE
CCE-84310-2	NIST80053-VI-ESXI-CFG-00073	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.paste.disable If isolation.tools.paste.disable does not exist or is not set to true, this is a finding.	TRUE

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8431-1-0	NIST800-53-VI-ESXI-CFG-00074	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.diskShrink.disable If isolation.tools.diskShrink.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8431-2-8	NIST800-53-VI-ESXI-CFG-00075	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.diskWiper.disable If isolation.tools.diskWiper.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8431-3-6	NIST800-53-VI-ESXI-CFG-00076	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.hgfsServerSet.disable If isolation.tools.hgfsServerSet.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8431-4-4	NIST800-53-VI-ESXI-CFG-00077	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.ghi.autologon.disable If isolation.tools.ghi.autologon.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8431-5-1	NIST800-53-VI-ESXI-CFG-00078	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.bios.bbs.disable If isolation.bios.bbs.disable does not exist or is not set to true, this is a finding.	TRUE

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84316-9	NIST800-53-VI-ESXI-CFG-00079	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.getCreds.disable</pre> <p>If isolation.tools.getCreds.disable does not exist or is not set to true, this is a finding.</p>	TRUE
CCE-84317-7	NIST800-53-VI-ESXI-CFG-00080	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.ghi.launchmenu.change</pre> <p>If isolation.tools.ghi.launchmenu.change does not exist or is not set to true, this is a finding.</p>	TRUE
CCE-84318-5	NIST800-53-VI-ESXI-CFG-00081	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.memSchedFakeSampleStats.disable</pre> <p>If isolation.tools.memSchedFakeSampleStats.disable does not exist or is not set to true, this is a finding.</p>	TRUE
CCE-84319-3	NIST800-53-VI-ESXI-CFG-00082	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.ghi.protocolhandler.info.disable</pre> <p>If isolation.tools.ghi.protocolhandler.info.disable does not exist or is not set to true, this is a finding.</p>	TRUE
CCE-84320-1	NIST800-53-VI-ESXI-CFG-00083	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.ghi.host.shellAction.disable</pre> <p>If isolation.ghi.host.shellAction.disable does not exist or is not set to true, this is a finding.</p>	TRUE

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8432-1-9	NIST800-53-VI-ESXI-CFG-00084	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.dispTopoRequest.disable</pre> <p>If isolation.tools.dispTopoRequest.disable does not exist or is not set to true, this is a finding.</p>	TRUE
CCE-8432-2-7	NIST800-53-VI-ESXI-CFG-00085	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.trashFolderState.disable</pre> <p>If isolation.tools.trashFolderState.disable does not exist or is not set to true, this is a finding.</p>	TRUE
CCE-8432-3-5	NIST800-53-VI-ESXI-CFG-00086	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.ghi.trayicon.disable</pre> <p>If isolation.tools.ghi.trayicon.disable does not exist or is not set to true, this is a finding.</p>	TRUE
CCE-8432-4-3	NIST800-53-VI-ESXI-CFG-00087	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.unity.disable</pre> <p>If isolation.tools.unity.disable does not exist or is not set to true, this is a finding.</p>	TRUE
CCE-8432-5-0	NIST800-53-VI-ESXI-CFG-00088	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.unityInterlockOperation.disable</pre> <p>If isolation.tools.unityInterlockOperation.disable does not exist or is not set to true, this is a finding.</p>	TRUE

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8432-6-8	NIST800-53-VI-ESXI-CFG-00089	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.unity.push.update.disable</pre> <p>If isolation.tools.unity.push.update.disable does not exist or is not set to true, this is a finding.</p>	TRUE
CCE-8432-7-6	NIST800-53-VI-ESXI-CFG-00090	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.unity.taskbar.disable</pre> <p>If isolation.tools.unity.taskbar.disable does not exist or is not set to true, this is a finding.</p>	TRUE
CCE-8432-8-4	NIST800-53-VI-ESXI-CFG-00091	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.unityActive.disable</pre> <p>If isolation.tools.unityActive.disable does not exist or is not set to true, this is a finding.</p>	TRUE
CCE-8432-9-2	NIST800-53-VI-ESXI-CFG-00092	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.unity.windowContents.disable</pre> <p>If isolation.tools.unity.windowContents.disable does not exist or is not set to true, this is a finding.</p>	TRUE
CCE-8433-0-0	NIST800-53-VI-ESXI-CFG-00093	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command:</p> <pre>Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.vmxDnDVersionGet.disable</pre> <p>If isolation.tools.vmxDnDVersionGet.disable does not exist or is not set to true, this is a finding.</p>	TRUE

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8433-1-8	NIST800-53-VI-ESXI-CFG-00094	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.guestDnDVersionSet.disable If isolation.tools.guestDnDVersionSet.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8433-2-6	NIST800-53-VI-ESXI-CFG-00095	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.vixMessage.disable If isolation.tools.vixMessage.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8433-3-4	NIST800-53-VI-ESXI-CFG-00096	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name RemoteDisplay.maxConnections If RemoteDisplay.maxConnections does not exist or is not set to 1, this is a finding.	1
CCE-8433-4-2	NIST800-53-VI-ESXI-CFG-00097	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name RemoteDisplay.vnc.enabled If RemoteDisplay.vnc.enabled does not exist or is not set to false, this is a finding.	FALSE
CCE-8433-5-9	NIST800-53-VI-ESXI-CFG-00098	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.tools.autoInstall.disable If isolation.tools.autoInstall.disable does not exist or is not set to true, this is a finding.	TRUE

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8433-6-7	NIST800-53-VI-ESXI-CFG-00099	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name tools.setinfo.sizeLimit If tools.setinfo.sizeLimit does not exist or is not set to 1048576, this is a finding.	1048576
CCE-8433-7-5	NIST800-53-VI-ESXI-CFG-00100	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.device.edit.disable If isolation.device.edit.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8433-8-3	NIST800-53-VI-ESXI-CFG-00101	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name isolation.device.connectable.disable If isolation.device.connectable.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8433-9-1	NIST800-53-VI-ESXI-CFG-00102	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-AdvancedSetting -Name tools.guestlib.enableHostInfo If tools.guestlib.enableHostInfo does not exist or is not set to false, this is a finding.	FALSE
CCE-8434-0-9	NIST800-53-VI-ESXI-CFG-00154	Built-in	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: Get-VM "VM Name"   Get-HardDisk   Select Parent, Name, Filename, DiskType, Persistence   FT -AutoSize If the virtual machine has attached disks that are in independent nonpersistent mode, this is a finding.	Persistent

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8434-1-7	NIST800-53-VI-ESXI-CFG-00155	Built-in	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <code>Get-VM   Get-FloppyDrive   Select Parent, Name, ConnectionState</code> If a virtual machine has a floppy drive present, this is a finding.	Disconnect unauthorized floppy devices
CCE-8434-2-5	NIST800-53-VI-ESXI-CFG-00156	Built-in	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <code>Get-VM   Get-CDDrive   Where {\$_.extensiondata.connectable.connected -eq \$true}   Select Parent,Name</code> If a virtual machine has a CD/DVD drive connected other than temporarily, this is a finding.	Disconnect unauthorized CD/DVD drives
CCE-8434-3-3	NIST800-53-VI-ESXI-CFG-00185	Built-in	vCenter	From a PowerCLI command prompt, while connected to the ESXi host run the following command: <code>Get-VirtualPortGroup   Select Name, VlanID</code> If any port group is configured with VLAN 4095 and is not documented as a needed exception, this is a finding.	Not 4095
CCE-8434-4-1	NIST800-53-VI-NET-CFG-00341	Built-in	vCenter	If the vCenter server is not joined to an Active Directory domain and not configured for Single Sign-On Identity Source of the Active Directory domain, and Active Directory/CAC/PIV certificate-based accounts are not used for daily operations of the vCenter server, this is a finding.	Procedural (Dependent on Customer Configurations)
CCE-8434-5-8	NIST800-53-VI-NET-CFG-00341	Built-in	vCenter	If the vCenter server is not joined to an Active Directory domain and not configured for Single Sign-On Identity Source of the Active Directory domain, and Active Directory/CAC/PIV certificate-based accounts are not used for daily operations of the vCenter server, this is a finding.	Procedural (Dependent on Customer Configurations)



CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84347-4	NIST80053-VI-VC-CFG-00402	Built-in	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following command: <code>Get-VDPortgroup   select Name, VlanConfiguration</code> If any port group is configured with VLAN 4095 and is not documented as a needed exception, this is a finding.	Not 4095
CCE-84348-2	NIST80053-VI-VC-CFG-00403	Built-in	vCenter	From the vSphere Web Client go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Configuration &gt;&gt; Policies &gt;&gt; Password Policy</b> . If Restrict Reuse is not set to 5 or more, this is a finding.	5
CCE-84349-0	NIST80053-VI-VC-CFG-00404	Built-in	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following command: <code>Get-AdvancedSetting -Entity &lt;vcenter server name&gt; -Name config.log.level</code> If the level is not set to info, this is a finding.	info
CCE-84350-8	NIST80053-VI-VC-CFG-00405	Built-in	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following commands: <code>Get-VDSwitch   Get-VDSecurityPolicy</code> <code>Get-VDPortgroup   Get-VDSecurityPolicy</code> If the Promiscuous Mode policy is set to accept, this is a finding.	reject
CCE-84351-6	NIST80053-VI-VC-CFG-00406	Built-in	vCenter	From the vSphere Web Client go to <b>Administration &gt;&gt; Client Plug-Ins</b> . View the Installed/Available Plug-ins list and verify they are all identified as authorized VMware, 3rd party (Partner), and/or site-specific (locally developed and site) approved plug-ins. If any Installed/Available plug-ins in the viewable list cannot be verified as vSphere Client plug-ins and/or authorized extensions from trusted sources, this is a finding.	Authorized extensions from Trusted Sources
CCE-84352-4	NIST80053-VI-	Built-in	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following commands:	reject

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
	VC-CFG-00407			Get-VDSwitch   Get-VDSecurityPolicy Get-VDPortgroup   Get-VDSecurityPolicy If the MAC Address Changes policy is set to accept, this is a finding.	
CCE-8435-3-2	NIST800-53-VI-VC-CFG-00408	Built-in	vCenter	From the vSphere Web Client go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Configuration &gt;&gt; Policies &gt;&gt; Password Policy</b> . If Upper-Case Characters is not set to at least 1, this is a finding.	1
CCE-8435-4-0	NIST800-53-VI-VC-CFG-00409	Built-in	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following command: Get-VDSwitch   select Name,@{N="NIOC Enabled";E={\$_.ExtensionData.config.NetworkResourceManagementEnabled}} If Network I/O Control is disabled, this is a finding.	enabled
CCE-8435-5-7	NIST800-53-VI-VC-CFG-00410	Enhanced	vCenter	From the vSphere Web Client go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Configuration &gt;&gt; Policies &gt;&gt; Password Policy</b> . If the Minimum Length is not set to at least 15, this is a finding.	15
CCE-8435-6-5	NIST800-53-VI-VC-CFG-00411	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following commands: \$vds = Get-VDSwitch \$vds.ExtensionData.Config.HealthCheckConfig If the health check feature is enabled on distributed switches and is not on temporarily for troubleshooting purposes, this is a finding.	FALSE
CCE-8435-7-3	NIST800-53-VI-VC-CFG-00412	Enhanced	vCenter	From the vSphere Client, select the vCenter server at the top of the hierarchy and go to <b>Alarms &gt;&gt; Definitions</b> . or From a PowerCLI command prompt, while connected to the vCenter server run the following command:	Procedural

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
				<pre>Get-AlarmDefinition   Where {\$_ .ExtensionData.Info.Expression.Expression.EventTypeId -eq "vim.event.PermissionUpdatedEvent"}   Select Name,Enabled,@{N="EventTypeId";E={\$_ .ExtensionData.Info.Expression.Expr ession.EventTypeId}}</pre> <p>If there is not an alarm created to alert on permission update events, this is a finding.</p>	
CCE-8435-8-1	NIST800-53-VI-VC-CFG-00413	Built-in	vCenter	<p>From the vSphere Web Client go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Configuration &gt;&gt; Policies &gt;&gt; Password Policy</b>.</p> <p>If Lower-Case Characters is not set to at least 1, this is a finding.</p>	1
CCE-8435-9-9	NIST800-53-VI-VC-CFG-00414	Enhanced	vCenter	<p>From the vSphere Client, select the vCenter server at the top of the hierarchy and go to <b>Alarms &gt;&gt; Definitions</b>.</p> <p>or</p> <p>From a PowerCLI command prompt, while connected to the vCenter server run the following command:</p> <pre>Get-AlarmDefinition   Where {\$_ .ExtensionData.Info.Expression.Expression.EventTypeId -eq "vim.event.PermissionAddedEvent"}   Select Name,Enabled,@{N="EventTypeId";E={\$_ .ExtensionData.Info.Expression.Expr ession.EventTypeId}}</pre> <p>If there is not an alarm created to alert on permission addition events, this is a finding.</p>	Procedural
CCE-8436-0-7	NIST800-53-VI-VC-CFG-00415	Built-in	vCenter	<p>From the vSphere Web Client, go to <b>Administration &gt;&gt; Access Control &gt;&gt; Roles</b>.</p> <p>or</p> <p>From a PowerCLI command prompt, while connected to the vCenter server run the following command:</p> <pre>Get-VIPermission   Sort Role   Select Role,Principal,Entity,Propagate,IsGroup   FT -Auto</pre> <p>Application service account and user required privileges should be documented.</p> <p>If any user or service account has more privileges than required, this is a finding.</p>	Procedural (Dependent on Customer Configurations)

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8436-1-5	NIST800-53-VI-VC-CFG-00416	Enhanced	vCenter	<p>From the vSphere Client, select the vCenter server at the top of the hierarchy and go to <b>Alarms &gt;&gt; Definitions</b>.</p> <p>or</p> <p>From a PowerCLI command prompt, while connected to the vCenter server run the following command:</p> <pre>Get-AlarmDefinition   Where {\$_ .ExtensionData.Info.Expression.EventTypeId -eq "vim.event.PermissionRemovedEvent"}   Select Name,Enabled,@{N="EventTypeId";E={\$_ .ExtensionData.Info.Expression.EventTypeId}}</pre> <p>If there is not an alarm to alert on permission deletion events, this is a finding.</p>	Procedural
CCE-8436-2-3	NIST800-53-VI-VC-CFG-00417	Built-in	vCenter	<p>From a PowerCLI command prompt, while connected to the vCenter server run the following command:</p> <pre>Get-VDPortgroup   Select Name,VirtualSwitch,@{N="NetFlowEnabled";E={\$_ .Extensiondata.Config.defaultPortConfig.ipfixEnabled.Value}}</pre> <p>If NetFlow is configured and the collector IP is not known and is not enabled temporarily for troubleshooting purposes, this is a finding.</p>	Known IPs
CCE-8436-3-1	NIST800-53-VI-VC-CFG-00418	Enhanced	vCenter	<p>If no clusters are enabled for VSAN, this is not applicable.</p> <p>From the vSphere Web Client go to <b>Host and Clusters &gt;&gt; Select a vCenter Server &gt;&gt; Configure &gt;&gt; vSAN &gt;&gt; Internet Connectivity &gt;&gt; Status</b>.</p> <p>If a proxy is not configured, this is a finding.</p>	Procedural
CCE-8436-4-9	NIST800-53-VI-VC-CFG-00419	Built-in	vCenter	<p>From a PowerCLI command prompt, while connected to the vCenter server run the following command:</p> <pre>Get-VIPermission   Sort Role   Select Role,Principal,Entity,Propagate,IsGroup   FT -Auto</pre> <p>Application service account and user required privileges should be documented.</p> <p>If any user or service account has more privileges than required, this is a finding.</p>	Procedural (Dependent on Customer Configurations)

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8436-5-6	NIST800-53-VI-VC-CFG-00420	Built-in	vCenter	<p>From the vSphere Web Client, go to <b>Host and Clusters</b> &gt;&gt; Select a Cluster &gt;&gt; <b>Related Objects</b> &gt;&gt; <b>Datastores</b>. Review the datastores. Identify any datastores with “vsan” as the datastore type.</p> <p>or</p> <p>From a PowerCLI command prompt, while connected to the vCenter server run the following command:</p> <pre>If(\$(Get-Cluster   where {\$_.VsanEnabled}   Measure).Count -gt 0){ Write-Host "VSAN Enabled Cluster found" Get-Cluster   where {\$_.VsanEnabled}   Get-Datastore   where {\$_.type -match "vsan"} } else{ Write-Host "VSAN is not enabled, this finding is not applicable" }</pre> <p>If VSAN is enabled and the datastore is named “vsanDatastore”, this is a finding.</p>	No name with “vsanDatastore”
CCE-8436-6-4	NIST800-53-VI-VC-CFG-00421	Enhanced	vCenter	<p>From the vSphere Web Client, go to <b>Administration</b> &gt;&gt; <b>Single Sign-On</b> &gt;&gt; <b>Configuration</b> &gt;&gt; <b>Policies</b> &gt;&gt; <b>Password Policy</b>.</p> <p>If Maximum Lifetime is not set to 60, this is a finding.</p>	60
CCE-8436-7-2	NIST800-53-VI-VC-CFG-00422	Enhanced	vCenter	<p>On the system where vCenter is installed, locate the <i>webclient.properties</i> file.</p> <p><i>/etc/vmware/vsphere-client/</i> and <i>/etc/vmware/vsphere-ui/</i></p> <p>If session.timeout is not set to 10 (minutes), this is a finding.</p>	10
CCE-8436-8-0	NIST800-53-VI-VC-CFG-00427	Enhanced	vCenter	<pre>Get-AdvancedSetting -Entity &lt;vcenter server name&gt; -Name config.vpxd.hostPasswordLength</pre>	32

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84369-8	NIST80053-VI-VC-CFG-00428	Built-in	vCenter	<p>From the vSphere Web Client, go to <b>vCenter Inventory Lists &gt;&gt; vCenter Servers &gt;&gt;</b> Select your vCenter Server &gt;&gt; <b>Settings &gt;&gt; Advanced System Settings</b>.</p> <p>or</p> <p>From a PowerCLI command prompt, while connected to the vCenter server run the following command:</p> <pre>Get-AdvancedSetting -Entity &lt;vcenter server name&gt; -Name VirtualCenter.VimPasswordExpirationInDays</pre> <p>If VirtualCenter.VimPasswordExpirationInDays is set to a value other than 30 or does not exist, this is a finding.</p>	FALSE
CCE-84370-6	NIST80053-VI-VC-CFG-00429	Built-in	vCenter	<p>Check the following conditions:</p> <ol style="list-style-type: none"> <li>1. The Update Manager must be configured to use the Update Manager Download Server.</li> <li>2. The use of physical media to transfer update files to the Update Manager server (air-gap model example: separate Update Manager Download Server which may source vendor patches externally via the internet versus an internal source) must be enforced with site policies.</li> </ol> <p>To verify download settings, from the vSphere Client/vCenter Server system, click <b>Update Manager</b>. Select a Host and then click the <b>Settings</b> tab. In the <b>Download Settings</b> tab, find "Direct connection to Internet."</p> <p>If "Direct connection to Internet" is configured, this is a finding.</p> <p>If all of the above conditions are not met, this is a finding.</p>	Procedural
CCE-84371-4	NIST80053-VI-VC-CFG-00432	Built-in	vCenter	<p>From the vSphere Web Client, go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Configuration &gt;&gt; Policies &gt;&gt; Password Policy</b>.</p> <p>If Special Characters is not set to at least 1, this is a finding.</p>	1
CCE-84372-2	NIST80053-VI-	Built-in	vCenter	<p>From the vSphere Web Client, go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Configuration &gt;&gt; Policies &gt;&gt; Password Policy</b>.</p> <p>If Numeric Characters is not set to at least 1, this is a finding.</p>	1

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
	VC-CFG-00433				
CCE-8437-3-0	NIST800-53-VI-VC-CFG-00434	Enhanced	vCenter	From the vSphere Web Client, go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Configuration &gt;&gt; Policies &gt;&gt; Lockout Policy</b> . If the Time interval between failures is not set to at least 900, this is a finding.	900
CCE-8437-4-8	NIST800-53-VI-VC-CFG-00435	Enhanced	vCenter	From the vSphere Web Client, go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Configuration &gt;&gt; Policies &gt;&gt; Lockout Policy</b> . If the Unlock time is not set to 0, this is a finding.	0
CCE-8437-5-5	NIST800-53-VI-VC-CFG-00436	Enhanced	vCenter	From the vSphere Web Client, go to <b>Administration &gt;&gt; Single Sign-On &gt;&gt; Configuration &gt;&gt; Policies &gt;&gt; Lockout Policy</b> . If the Maximum number of failed login attempts is not set to 3, this is a finding.	3
CCE-8437-6-3	NIST800-53-VI-VC-CFG-00437	Enhanced	vCenter	From the vSphere Web Client go to <b>vCenter Inventory Lists &gt;&gt; vCenter Servers &gt;&gt; Select your vCenter Server &gt;&gt; Settings &gt;&gt; Advanced Settings</b> . or From a PowerCLI command prompt, while connected to the vCenter server run the following command: <code>Get-AdvancedSetting -Entity &lt;vcenter server name&gt; -Name config.nfc.useSSL</code> If config.nfc.useSSL is not set to true, this is a finding.	TRUE
CCE-8437-7-1	NIST800-53-VI-VC-CFG-00439	Built-in	vCenter	If the built-in SSO administrator account is used for daily operations or there is no policy restricting its use, this is a finding.	Procedural

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84378-9	NIST800-53-VI-VC-CFG-00440	Enhanced	vCenter	<p>From the vSphere Web Client, go to <b>Networking</b> &gt;&gt; Select a distributed port group &gt;&gt; <b>Manage</b> &gt;&gt; <b>Settings</b> &gt;&gt; <b>Properties</b>. View the Override port policies.</p> <p>or</p> <p>From a PowerCLI command prompt, while connected to the vCenter server run the following command:</p> <pre>Get-VDPortgroup   Get-View   Select Name, @{N="VlanOverrideAllowed";E={\$_.Config.Policy.VlanOverrideAllowed}}, @{N="UplinkTeamingOverrideAllowed";E={\$_.Config.Policy.UplinkTeamingOverrideAllowed}}, @{N="SecurityPolicyOverrideAllowed";E={\$_.Config.Policy.SecurityPolicyOverrideAllowed}}, @{N="IpfixOverrideAllowed";E={\$_.Config.Policy.IpfixOverrideAllowed}}, @{N="BlockOverrideAllowed";E={\$_.Config.Policy.BlockOverrideAllowed}}, @{N="ShapingOverrideAllowed";E={\$_.Config.Policy.ShapingOverrideAllowed}}, @{N="VendorConfigOverrideAllowed";E={\$_.Config.Policy.VendorConfigOverrideAllowed}}, @{N="TrafficFilterOverrideAllowed";E={\$_.Config.Policy.TrafficFilterOverrideAllowed}}, @{N="PortConfigResetAtDisconnect";E={\$_.Config.Policy.PortConfigResetAtDisconnect}}   Sort Name</pre> <p>Note: This was broken up into multiple lines for readability. Either paste as is into a PowerShell script or combine into one line and run.</p> <p>This does not apply to the reset port configuration on disconnect policy.</p> <p>If any port-level overrides are enabled and not documented, this is a finding.</p>	disabled
CCE-84379-7	NIST800-53-VI-VC-CFG-00442	Enhanced	vCenter	<p>From the vSphere Client, select the vCenter server at the top of the hierarchy and go to <b>Alarms</b> &gt;&gt; <b>Definitions</b>.</p> <p>or</p>	Enabled



CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
				<p>From a PowerCLI command prompt, while connected to the vCenter server run the following command:</p> <pre>Get-AlarmDefinition   Where {\$_ .ExtensionData.Info.Expression.Expression.EventTypeId -eq "esx.problem.vmsyslogd.remote.failure"}   Select Name,Enabled,@{N="EventTypeId";E={\$_ .ExtensionData.Info.Expression.Expression.EventTypeId}}</pre> <p>If there is no alarm created to alert if an ESXi host can no longer reach its syslog server, this is a finding.</p>	
CCE-8438-0-5	NIST800-53-VI-VC-CFG-00445	Built-in	vCenter	<p>If IP-based storage is not used, this is not applicable.</p> <p>IP-based storage (iSCSI, NFS, VSAN) VMkernel port groups must be in a dedicated VLAN that can be on a common standard or distributed virtual switch that is logically separated from other traffic types. The check for this will be unique per environment.</p> <p>From the vSphere Client, select <b>Networks</b> &gt;&gt; <b>Distributed Port Groups</b> and review the VLANs associated with any IP-based storage VMkernels.</p> <p>If any IP-based storage networks are not isolated from other traffic types, this is a finding.</p>	Unique IP addresses
CCE-8438-1-3	NIST800-53-VI-VC-CFG-00447	Built-in	vCenter	<p>Log in to the vCenter server and view the local administrators group membership.</p> <p>If the local administrators group contains users and/or groups that are not vCenter Administrators such as "Domain Admins", this is a finding.</p>	Only necessary users and groups
CCE-8438-2-1	NIST800-53-VI-VC-CFG-00450	Built-in	vCenter	<p>From the vSphere Client, go to <b>Home</b> &gt;&gt; <b>Networking</b>. Select a distributed port group, click <b>Edit</b>, then go to <b>Security</b>.</p> <p>or</p> <p>From a PowerCLI command prompt, while connected to the vCenter server run the following commands:</p> <pre>Get-VDSwitch   Get-VDSecurityPolicy Get-VDPortgroup   ?{\$_ .IsUplink -eq \$false}   Get-VDSecurityPolicy</pre> <p>If the Forged Transmits policy is set to accept for a non-uplink port, this is a finding.</p>	reject

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8438-3-9	NIST800-53-VI-VC-CFG-00455	Enhanced	vCenter	If the vSphere Storage API - Data Protection (VADP) solution is not configured for performing backup and restore of the management components, this is a finding.	vSphere Storage API - Data Protection (VADP)
CCE-8438-4-7	NIST800-53-VI-VC-CFG-00497	Built-in	vCenter	On the Edit port group - VM Network window, check for input 1611 for VLAN ID. If the vlan is 1611, this is a finding.	Not 1611
CCE-8438-5-4	NIST800-53-VI-VC-CFG-00555	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <code>Get-VM "VM Name"   Get-AdvancedSetting -Name svga.vgaonly</code> If svga.vgaonly does not exist or is not set to true, this is a finding.	TRUE
CCE-8438-6-2	NIST800-53-VI-VC-CFG-00561	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <code>Get-VM "VM Name"   Get-AdvancedSetting -Name pciPassthru*.present</code> If pciPassthru*.present does not exist or is not set to false, this is a finding.	FALSE
CCE-8460-1-4	NIST800-53-VI-Storage-SDS-CFG-00178	Enhanced	vSAN	From a PowerCLI command prompt, while connected to the vCenter server run the following command: <code>Get-VIPermission   Where {\$_.Role -eq "Admin"}   Select Role,Principal,Entity,Propagate,IsGroup   FT -Auto</code> If there are any users other than Solution Users with the Administrator role that are not explicitly designated for cryptographic operations, this is a finding.	No Cryptography Administrator
CCE-8460-2-2	NIST800-53-VI-Storage-SDS-	Built-in	vSAN	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: <code>Get-VMHost   Get-VMHostNTPServer</code> <code>Get-VMHost   Get-VMHostService   Where {\$_.Label -eq "NTP Daemon"}</code>	Correct date and timestamp

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
	CFG-00180			If the NTP service is not configured with authoritative DoD time sources and the service is not configured to start and stop with the host and is running, this is a finding.	
CCE-84603-0	NIST80053-VI-Storage-SDS-CFG-00181	Built-in	vSAN	Log in to the vRealize Log Insight user interface. Click the configuration drop-down menu icon and select <b>Content Packs</b> . Under Content Pack Marketplace, select <b>Marketplace</b> . If the VMware - vSAN content pack does not appear in the Installed Content Packs list, this is a finding.	VMware - vSAN
CCE-84604-8	NIST80053-VI-Storage-SDS-CFG-00182	Built-in	vSAN	From a PowerCLI command prompt, while connected to the ESXi host run the following command: <code>Get-VMHost   Get-AdvancedSetting -Name UserVars.HostClientSessionTimeout</code> If UserVars.HostClientSessionTimeout is not set to 900, this is a finding.	900
CCE-84605-5	NIST80053-VI-Storage-SDS-CFG-00183	Enhanced	vSAN	From the vSphere client, select the cluster. Click the Configure tab and under <b>vSAN</b> , click <b>Services</b> . If Encryption is not enabled or the KMS cluster is not configured, this is a finding.	Enabled
CCE-84606-3	NIST80053-VI-Storage-SDS-CFG-00184	Built-in	vSAN	Perform a compliance check on the inventory objects to make sure that you have all the latest security patches and updates applied. Use the vSphere Client to log in to a vCenter Server Appliance or to a vCenter Server system with which Update Manager is registered. If all the latest security patches and updates are not applied, this is a finding.	Up-to-date patches and upgrades

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84607-1	NIST800-53-VI-Storage-SDS-CFG-00185	Built-in	vSAN	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following command:</p> <pre>Get-VMHost   Get-AdvancedSetting -Name Syslog.global.logHost</pre> <p>If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.</p>	udp://sfo01vrli01.sfo01.rainpole.local:514
CCE-84608-9	NIST800-53-VI-Storage-SDS-CFG-00204	Enhanced	vSAN	<p>From a PowerCLI command prompt, while connected to the vCenter server run the following command:</p> <pre>Get-VIPermission   Where {\$_.Role -eq "Admin"}   Select Role,Principal,Entity,Propagate,IsGroup   FT -Auto</pre> <p>If there are any users other than Solution Users with the Administrator role that are not explicitly designated for cryptographic operations, this is a finding.</p>	No Cryptography Administrator
CCE-84609-7	NIST800-53-VI-Storage-SDS-CFG-00207	Enhanced	vSAN	<p>If VSAN Health Check is installed:</p> <p>From the vSphere Client, go to <b>Host and Clusters</b>. Select a vCenter Server and go to <b>Configure &gt; vSAN &gt; Internet Connectivity &gt; Status</b>.</p> <p>If “Enable Internet access for this cluster” is enabled and a proxy is not configured, this is a finding.</p>	Proxy should be configured
CCE-84610-5	NIST800-53-VI-Storage-SDS-CFG-00208	Built-in	vSAN	<p>From a PowerCLI command prompt, while connected to the vCenter server run the following command:</p> <pre>If(\$(Get-Cluster   where {\$_.VsanEnabled}   Measure).Count -gt 0){ Write-Host "VSAN Enabled Cluster found" Get-Cluster   where {\$_.VsanEnabled}   Get-Datastore   where {\$_.type -match "vsan"} } else{ Write-Host "VSAN is not enabled, this finding is not applicable" }</pre> <p>If VSAN is enabled and the datastore is named “vsanDatastore”, this is a finding.</p>	Datastore name is unique

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8461 1-3	NIST800 53-VI-Storage-SDS-CFG-00179	Enhanced	vSAN	<p>From a PowerCLI command prompt, while connected to the ESXi host run the following commands:</p> <pre>\$esxcli = Get-EsxCli \$esxcli.system.coredump.network.get()</pre> <p>If there is no active core dump partition or the network core dump collector is not configured and enabled, this is a finding.</p>	TRUE
CCE-8461 2-1	NIST800 53-VI-Storage-SDS-CFG-00186	Enhanced	vSAN	<p>Make sure you have sufficient capacity in the management vSAN cluster for the management virtual machines.</p> <p>If you do not have sufficient capacity, this is a finding.</p>	Procedural

## Appendix B List of Acronyms

<b>AD</b>	Active Directory
<b>API</b>	Application Programming Interface
<b>BIOS</b>	Basic Input/Output System
<b>BOM</b>	Bill of Materials
<b>CA</b>	Certificate Authority
<b>CAC</b>	Common Access Card
<b>CAM</b>	Content Addressable Memory
<b>CCE</b>	Common Configuration Enumeration
<b>CLI</b>	Command Line Interface
<b>CRADA</b>	Cooperative Research and Development Agreement
<b>D@RE</b>	(Dell EMC Unity) Data at Rest Encryption
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DISA</b>	Defense Information Systems Agency
<b>DNS</b>	Domain Name System
<b>DoD</b>	Department of Defense
<b>EFI</b>	Extensible Firmware Interface
<b>FIPS</b>	Federal Information Processing Standards
<b>FTP</b>	File Transfer Protocol
<b>GB</b>	Gigabyte
<b>Gb/s</b>	Gigabits per Second
<b>GHz</b>	Gigahertz
<b>GKH</b>	Good Known Host
<b>GUI</b>	Graphical User Interface
<b>HSM</b>	Hardware Security Module
<b>HTCC</b>	HyTrust CloudControl
<b>IaaS</b>	Infrastructure as a Service
<b>ICSV</b>	IBM Cloud Secure Virtualization
<b>IOPS</b>	Input/Output Operations per Second
<b>IP</b>	Internet Protocol
<b>IPsec</b>	Internet Protocol Security
<b>IT</b>	Information Technology

<b>KMS</b>	Key Management System
<b>LACP</b>	Link Aggregation Control Protocol
<b>LLDP</b>	Link Layer Discovery Protocol
<b>MAC</b>	Media Access Control
<b>MLE</b>	Measured Launch Environment
<b>MOB</b>	(vCenter) Managed Object Browser
<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NFS</b>	Network File System
<b>NIC</b>	Network Interface Card
<b>NIST</b>	National Institute of Standards and Technology
<b>NISTIR</b>	National Institute of Standards and Technology Internal Report
<b>NSX-V</b>	NSX for vSphere
<b>NTLS</b>	Network Trust Links
<b>NTP</b>	Network Time Protocol
<b>OS</b>	Operating System
<b>OSPF</b>	Open Shortest Path First
<b>OU</b>	Organizational Unit
<b>OVA</b>	Open Virtual Appliance
<b>PDC</b>	Physical Data Center
<b>PIV</b>	Personal Identity Verification
<b>PSC</b>	Platform Services Controller
<b>PXE</b>	Preboot Execution Environment
<b>RAM</b>	Random Access Memory
<b>RPC</b>	Remote Procedure Call
<b>SAS</b>	Serial Attached SCSI
<b>SCSI</b>	Small Computer System Interface
<b>SDDC</b>	Software Defined Data Center
<b>SED</b>	Self-Encrypting Drive
<b>SFTP</b>	Secure File Transfer Protocol
<b>SHA</b>	Secure Hash Algorithm
<b>SLES</b>	SUSE Linux Enterprise Server
<b>SMTP</b>	Simple Mail Transfer Protocol

<b>SNMP</b>	Simple Network Management Protocol
<b>SP</b>	Special Publication, Storage Processor
<b>SSD</b>	Solid State Drive
<b>SSH</b>	Secure Shell
<b>SSO</b>	Single Sign-On
<b>STIG</b>	Security Technical Implementation Guide
<b>TB</b>	Terabyte
<b>TCP</b>	Transmission Control Protocol
<b>TLS</b>	Transport Layer Security
<b>TPM</b>	Trusted Platform Module
<b>TXT</b>	(Intel) Trusted Execution Technology
<b>UCR</b>	Unified Capabilities Requirements
<b>UEFI</b>	Unified Extensible Firmware Interface
<b>UI</b>	User Interface
<b>UMDS</b>	Update Manager Download Service
<b>URL</b>	Uniform Resource Locator
<b>USB</b>	Universal Serial Bus
<b>UUID</b>	Universally Unique Identifier
<b>VADP</b>	vSphere Storage APIs for Data Protection
<b>VCF</b>	VMware Cloud Foundation
<b>VCS</b>	vCenter Server
<b>VLAN</b>	Virtual Local Area Network
<b>VM</b>	Virtual Machine
<b>VMX</b>	Virtual Machine Extensions
<b>VPN</b>	Virtual Private Network
<b>vR</b>	vSphere Replication
<b>vRA</b>	vRealize Automation
<b>vRLI</b>	vRealize Log Insight
<b>vROPS</b>	vRealize Operations Manager
<b>VSAN</b>	Virtual Storage Area Network
<b>VSI</b>	Virtual Storage Integrator
<b>VT</b>	(Intel) Virtualization Technology



**VVD**

VMware Validated Design

## Appendix C Glossary

All significant technical terms used within this document are defined in other key documents, particularly National Institute of Standards and Technology Internal Report (NISTIR) 7904, *Trusted Geolocation in the Cloud: Proof of Concept Implementation*. As a convenience to the reader, terms critical to understanding this volume are provided in this glossary.

<b>Cloud workload</b>	A logical bundle of software and data that is present in, and processed by, a cloud computing technology.
<b>Geolocation</b>	Determining the approximate physical location of an object, such as a cloud computing server.
<b>Hardware root of trust</b>	An inherently trusted combination of hardware and firmware that maintains the integrity of information.
<b>Trusted compute pool</b>	A physical or logical grouping of computing hardware in a data center that is tagged with specific and varying security policies. Within a trusted compute pool, the access and execution of applications and workloads are monitored, controlled, audited, etc. Also known as a <i>trusted pool</i> .