

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
Murugiah Souppaya
Donna Dodson
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
Carlos Phoenix
Anthony Dukes
Jeff Haskins
Brenda Swarts

DRAFT

This publication is available free of charge from
<https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud>

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
Murugiah Souppaya
Donna Dodson*
*Computer Security
Division
Information Technology
Laboratory*

Daniel Carroll
Robert Masten
*Dell/EMC
Hopkinton, Massachusetts*

Gina Scinta
Paul Massis
*Gemalto
Austin, Texas*

Hemma Prafullchandra*
Jason Malnar
*HyTrust
Mountain View, California*

Harmeet Singh
Rajeev Ghandi
Laura E. Storey
*IBM
Armonk, New York*

Raghuram Yeluri
*Intel
Santa Clara, California*

Tim Shea
Michael Dalton
Rocky Weber
*RSA
Bedford, Massachusetts*

Karen Scarfone
*Scarfone Cybersecurity
Clifton, Virginia*

Carlos Phoenix
Anthony Dukes
Jeff Haskins
Brenda Swarts
*VMware
Palo Alto, California*

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

DRAFT

October 2021



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

National Institute of Standards and Technology
*James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for
Standards and Technology & Director, National Institute of Standards and Technology*

DRAFT

NIST SPECIAL PUBLICATION 1800-19A

Trusted Cloud:

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

Volume A: Executive Summary

Donna Dodson*

Computer Security Division
Information Technology Laboratory

Harmeet Singh

IBM
Armonk, New York

Daniel Carroll

Dell/EMC
Hopkinton, Massachusetts

Raghuram Yeluri

Intel
Santa Clara, California

Gina Scinta

Gemalto
Austin, Texas

Tim Shea

RSA
Bedford, Massachusetts

Hemma Prafullchandra*

HyTrust
Mountain View, California

Carlos Phoenix

VMware
Palo Alto, California

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

October 2021

DRAFT

This publication is available free of charge from:

<https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud>



Executive Summary

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

9 CHALLENGE

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

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

19 Many organizations, especially those in regulated sectors like finance and healthcare, face additional
20 challenges because security and privacy laws vary around the world. Laws for protecting information the
21 organization collects, processes, transmits, or stores may vary depending on whose information it is,
22 what kind of information it is, and where it is located. Cloud technologies may silently move an
23 organization's data from one jurisdiction to another. Because laws in some jurisdictions may conflict
24 with an organization's own policies or local laws and regulations, an organization may decide it needs to
25 restrict which on-premises private or hybrid/public cloud servers it uses based on their geolocations to
26 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

27 SOLUTION

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

37 The example solution uses technologies and security capabilities (shown below) from our project
 38 collaborators. The technologies used in the solution support security and privacy standards and
 39 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

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

46 HOW TO USE THIS GUIDE

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

48 **Business decision makers, including chief information security and technology officers** can use this
49 part of the guide, *NIST SP 1800-19A: Executive Summary*, to understand the drivers for the guide, the
50 cybersecurity challenge we address, our approach to solving this challenge, and how the solution could
51 benefit your organization.

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

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

59 SHARE YOUR FEEDBACK

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

66 To provide comments or to learn more by arranging a demonstration of this example implementation,
67 contact the NCCoE at trusted-cloud-nccoe@nist.gov.

68 COLLABORATORS

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

74 Certain commercial entities, equipment, products, or materials may be identified by name or company
75 logo or other insignia in order to acknowledge their participation in this collaboration or to describe an
76 experimental procedure or concept adequately. Such identification is not intended to imply special
77 status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it
78 intended to imply that the entities, equipment, products, or materials are necessarily the best available
79 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

October 2021

DRAFT

This publication is available free of charge from:
<https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud>

1 **DISCLAIMER**

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

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

13 National Institute of Standards and Technology Special Publication 1800-19B, Natl. Inst. Stand. Technol.
14 Spec. Publ. 1800-19B, 55 pages, (October 2021), CODEN: NSPUE2

15 **FEEDBACK**

16 You can improve this document by contributing feedback.

17 Comments on this publication may be submitted to: trusted-cloud-nccoe@nist.gov.

18 Public comment period: October 27, 2021 through December 6, 2021

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

20 National Cybersecurity Center of Excellence
21 National Institute of Standards and Technology
22 100 Bureau Drive
23 Mailstop 2002
24 Gaithersburg, MD 20899
25 Email: nccoe@nist.gov

26 NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

42 NIST CYBERSECURITY PRACTICE GUIDES

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

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

52 ABSTRACT

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

64 KEYWORDS

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

66 ACKNOWLEDGMENTS

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

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

71 DOCUMENT CONVENTIONS

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

79 CALL FOR PATENT CLAIMS

80 This public review includes a call for information on essential patent claims (claims whose use would be
 81 required for compliance with the guidance or requirements in this Information Technology Laboratory
 82 (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication
 83 or by reference to another publication. This call also includes disclosure, where known, of the existence

DRAFT

84 of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant
85 unexpired U.S. or foreign patents.

86 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in writ-
87 ten or electronic form, either:

88 a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not
89 currently intend holding any essential patent claim(s); or

90 b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring
91 to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft
92 publication either:

- 93 1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination;
94 or
95 2. without compensation and under reasonable terms and conditions that are demonstrably free
96 of any unfair discrimination.

97 Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its
98 behalf) will include in any documents transferring ownership of patents subject to the assurance, provi-
99 sions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that
100 the transferee will similarly include appropriate provisions in the event of future transfers with the goal
101 of binding each successor-in-interest.

102 The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of
103 whether such provisions are included in the relevant transfer documents.

104 Such statements should be addressed to: trusted-cloud-nccoe@nist.gov

105 **Contents**

106 **1 Summary..... 1**

107 1.1 Challenge..... 1

108 1.2 Solution..... 2

109 1.3 Benefits..... 2

110 **2 How to Use This Guide 3**

111 2.1 Typographical Conventions..... 4

112 **3 Approach 5**

113 3.1 Audience..... 6

114 3.2 Scope 6

115 3.3 Assumptions 6

116 3.4 Risk Assessment 6

117 3.4.1 Threats 7

118 3.4.2 Vulnerabilities 10

119 3.4.3 Risk 10

120 **4 Architecture 10**

121 4.1 Architecture Components 12

122 4.2 Technologies..... 12

123 4.2.1 Dell EMC..... 13

124 4.2.2 Gemalto 13

125 4.2.3 HyTrust..... 14

126 4.2.4 IBM..... 15

127 4.2.5 Intel 16

128 4.2.6 RSA 17

129 4.2.7 VMware..... 17

130 4.2.8 Products and Technologies Summary..... 20

131 4.3 NCCoE Cloud Solution Architecture 24

132 4.3.1 VMware Cluster Architectures..... 25

133	4.3.2	RSA Cluster Architecture.....	29
134	4.3.3	HSM Architecture.....	29
135	4.3.4	HyTrust Architecture.....	31
136	4.3.5	Dell Leaf and Spine Switch Architecture.....	32
137	4.4	IBM Cloud Solution Architecture.....	33
138	5	Security Characteristics Analysis	34
139	5.1	Assumptions and Limitations	35
140	5.2	Demonstration of the Capabilities	35
141	5.2.1	Use Case Scenario 1: Demonstrate Control and Visibility for the Trusted Hybrid Cloud Environment	35
142			
143	5.2.2	Use Case Scenario 2: Demonstrate Control of Workloads and Data Security	37
144	5.2.3	Use Case Scenario 3: Demonstrate a Workload Security Policy in a Hybrid Cloud	41
145	5.2.4	Use Case Scenario 4: Demonstrate Recovery From an Unexpected Infrastructure Outage.....	42
146			
147	5.2.5	Use Case Scenario 5: Demonstrate Providing Visibility into Network Traffic Patterns.....	43
148			
149	5.2.6	Use Case Scenario 6: Demonstrate Application Zero Trust	43
150	Appendix A	Mappings	45
151	Appendix B	List of Acronyms.....	49
152	Appendix C	Glossary	53
153	Appendix D	References	54
154			
155		List of Figures	
156	Figure 4-1	High-Level Solution Architecture	11
157	Figure 4-2	High-Level NCCoE Cloud Architecture	25
158	Figure 4-3	VMware Management Cluster Architecture.....	27
159	Figure 4-4	VMware Compute Cluster Architecture	28
160	Figure 4-5	RSA Cluster	29
161	Figure 4-6	HSM Architecture in the NCCoE Cloud	30

162 **Figure 4-7 HyTrust Architecture in the NCCoE Cloud**.....31

163 **Figure 4-8 HTKC Node Deployments**32

164 **Figure 4-9 NCCoE Layer 3 Leaf – Spine Logical Network Diagram**.....33

165 **Figure 4-10 IBM Cloud Architecture**34

166 **Figure 5-1 Example of Secure Configuration Scan Results**36

167 **Figure 5-2 Examples of Trusted Compute Nodes**37

168 **Figure 5-3 Example of Decrypted Workload**38

169 **Figure 5-4 Example of Workload on Untagged Server**39

170 **Figure 5-5 Example of Workload that Cannot Be Decrypted**.....39

171 **Figure 5-6 Example of Workload Migrated to Trusted and Tagged Server**40

172 **Figure 5-7 Example of Workload Running on Trusted and Tagged Server**41

173 **List of Tables**

174 **Table 3-1 Common Threats Associated with Hybrid Cloud Usage**.....7

175 **Table 4-1 Products and Technologies Summary**.....20

176 **Table A-1 List of NIST SP 800-53 Revision 5 Controls Addressed by Solution**.....45

177 **Table A-2 List of NIST Cybersecurity Framework Subcategories Addressed by Solution**47

178 1 Summary

179 Building on previous work documented in National Institute of Standards and Technology (NIST)
180 Interagency Report (NISTIR) 7904, *Trusted Geolocation in the Cloud: Proof of Concept Implementation*
181 [\[1\]](#), the goal of the project is to expand upon the security capabilities provided by trusted compute pools
182 in a hybrid cloud model, including the following capabilities:

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

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

195 1.1 Challenge

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

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

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

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

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

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

227 **1.2 Solution**

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

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

240 **1.3 Benefits**

- 241
 - 242
 - 243
 - 244
 - 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.

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

250 2 How to Use This Guide

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

255 This guide contains three volumes:

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

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

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

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

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

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

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

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

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

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

290 A NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a
 291 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and
 292 success stories will improve subsequent versions of this guide. Please contribute your thoughts to
 293 trusted-cloud-nccoe@nist.gov.

294 2.1 Typographical Conventions

295 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> .
Bold	names of menus, options, command buttons, and fields	Choose File > Edit .
Monospace	command-line input, on-screen computer output, sample code examples, and status codes	<code>mkdir</code>

Typeface/Symbol	Meaning	Example
Monospace Bold	command-line user input contrasted with computer output	<code>service sshd start</code>
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST’s NCCoE are available at https://www.nccoe.nist.gov .

296 3 Approach

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

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

314 The following actions have been, or will be, were performed by the build teams:

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

323 3.1 Audience

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

327 3.2 Scope

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

332 3.3 Assumptions

333 This project is guided by the following assumptions:

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

352 3.4 Risk Assessment

353 [NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*](#), states that risk is “a measure of the
354 extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

355 (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of
 356 occurrence.” The guide further defines risk assessment as “the process of identifying, estimating, and
 357 prioritizing risks to organizational operations (including mission, functions, image, reputation),
 358 organizational assets, individuals, other organizations, and the Nation, resulting from the operation of
 359 an information system. Part of risk management incorporates threat and vulnerability analyses, and
 360 considers mitigations provided by security controls planned or in place.” [3]

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

3.4.1 Threats

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

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

Threat/Attack Type	Example	Addressed by Solution
Threats Against Cloud Infrastructure		
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.

Threat/Attack Type	Example	Addressed by Solution
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.
Threats Against Cloud Management		
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.

Threat/Attack Type	Example	Addressed by Solution
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) 140-2-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.
Threats Against Cloud Workload Storage, Execution, and Use		
Running a cloud workload within an untrusted environment or location	A cloud administrator may respond to an impending maintenance disruption by moving cloud 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 cloud workload to another within a cloud	A user of one cloud workload connects to another organization's cloud 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.

Threat/Attack Type	Example	Addressed by Solution
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 cloud workloads from accessing sensitive applications and data drives.

3.4.2 Vulnerabilities

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

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

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

3.4.3 Risk

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

394 4 Architecture

395 At a high level, the trusted cloud architecture has three main pieces: a private cloud hosted at the
 396 NCCoE, an instance of the public IBM Cloud Secure Virtualization (ICSV), and an Internet Protocol

397 Security (IPsec) virtual private network (VPN) that connects the two clouds to form a hybrid cloud.

398 [Figure 4-1](#) provides a simplified diagram of the architecture.

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

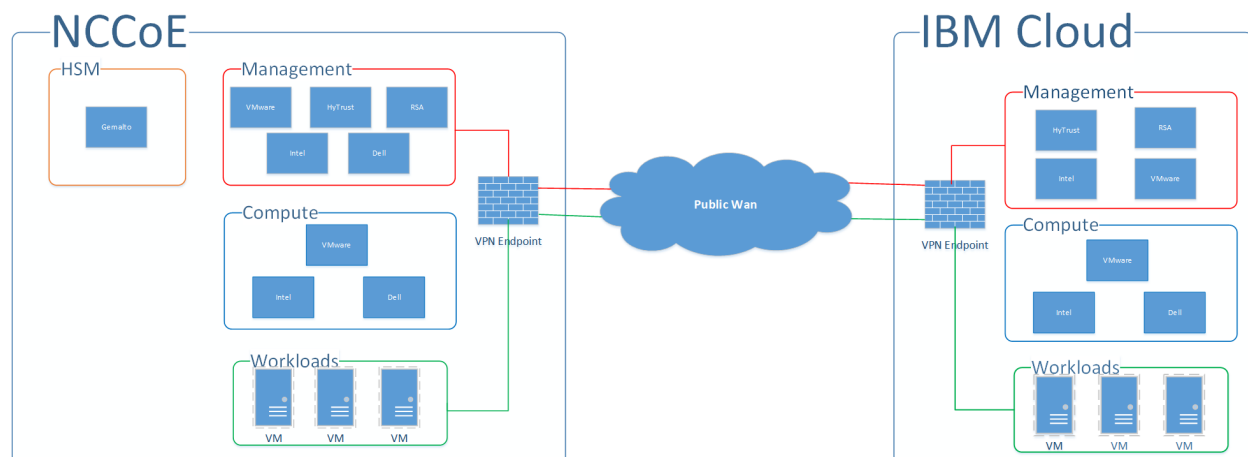
- 400 ▪ HSM for storing keys by Gemalto
- 401 ▪ server, storage, and networking hardware by Dell EMC
- 402 ▪ Intel processors in the Dell EMC servers
- 403 ▪ compute, storage, and network virtualization capabilities by VMware
- 404 ▪ asset tagging and policy enforcement, workload and storage encryption, and data scanning by HyTrust
- 405 ▪ multifactor authentication, network traffic monitoring, and dashboard and reporting by RSA
- 406 ▪ multifactor authentication, network traffic monitoring, and dashboard and reporting by RSA

407 The ICSV instance consists of the following components:

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

412 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.

415 **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

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

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

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

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

4.2.2 Gemalto

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

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

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

478 The SafeNet Luna Network HSM (Versions 6 and 7) is a network-attached HSM protecting encryption
479 keys used by applications in on-premises, virtual, and cloud environments. The HSM has more than 400
480 integrations. For this project, SafeNet Luna Network HSM 7 is the root of trust for Microsoft Active

481 Directory Certificate Services (ADCS) used to issue TLS certificates. SafeNet Luna Network HSM 6 is
482 integrated as the root of trust for HyTrust KeyControl (HTKC) via the KMIP key management service.

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

4.2.3 HyTrust

486 HyTrust helps make cloud infrastructure more trustworthy for those organizations pursuing a multi-
487 cloud approach, by delivering a critical set of capabilities required to proactively secure workloads
488 wherever they reside. The HyTrust Cloud Security Policy Framework (CloudSPF) allows organizations to
489 automate the creation, application, and enforcement of security and compliance policies for private,
490 hybrid, and public cloud workloads, including three critical attributes of the workload—people, data,
491 and infrastructure. HyTrust CloudSPF is supported by a portfolio of five solutions that deliver the
492 functionality needed to enable policy-driven security and automated compliance of workloads in multi-
493 cloud environments—including securing data and ensuring data privacy, preventing privileged admin
494 misuse, automating compliance tasks, securing multi-tenant environments, and more. The five solutions
495 are as follows:

- 496 ▪ **HyTrust CloudControl (HTCC):** Workload Security Policy Enforcement and Compliance: Key
497 capabilities help organizations protect their virtualized infrastructures with authentication,
498 authorization, and auditing. Better visibility and control simplify compliance and accelerate
499 further virtualization and data center transformation. CloudControl functionality includes two-
500 factor authentication, secondary approval workflows, advanced role-based and object-based
501 access controls, audit-quality logging, and hypervisor hardening.
- 502 ▪ **HyTrust DataControl (HTDC):** Workload Encryption and Integrated Key Management: Provides
503 strong data-at-rest encryption for workloads in any cloud, along with easy-to-deploy key
504 management that organizations control—whether workloads are running in a private cloud
505 powered by vSphere or in a hybrid/public cloud like IBM Cloud, Microsoft Azure, or Amazon
506 Web Services (AWS)—throughout the entire workload life cycle. DataControl also supports the
507 highest levels of availability by offering the ability to rekey workloads without taking
508 applications offline.
- 509 ▪ **HyTrust KeyControl (HTKC):** Workload Encryption Key Management: Simplifies the process of
510 key management for workloads that do not require sophisticated policy-based key
511 management, but that need to scale to enterprise-level performance. Organizations retain full
512 ownership of encryption keys with policy-based controls to protect data and to meet
513 compliance requirements. KeyControl works with both DataControl and third-party encryption
514 solutions, such as VMware vSphere VM Encryption and vSAN.
- 515 ▪ **HyTrust CloudAdvisor (HTCA):** Data Discovery and Classification Across Virtual Machines and
516 Backups: Provides complete visibility into data stored within each workload and associates this

517 information with whomever is interacting with it and when. CloudAdvisor defines policies to
518 automatically discover the data that is valuable; detect anomalous user access behaviors; and
519 defend an organization against careless exposure, data loss, malicious users, and regulatory
520 noncompliance.

521 ▪ **HyTrust BoundaryControl (HTBC):** Workload Placement Policies, Data Geo-Fencing, and
522 Location-Aware Encryption: Enables administrators to set policies so that workloads can run
523 only on proven, trusted hosts that are physically located within the defined parameters.
524 BoundaryControl's foundation is rooted in Intel Trusted Execution Technology (Intel TXT), which
525 provides processor-level attestation of the hardware, BIOS, and hypervisor. Administrators can
526 also assign labels that bind workloads to run only in predefined locations. Also, encryption
527 policies can be applied to ensure that data is never decrypted outside the defined
528 parameters/boundary.

4.2.4 IBM

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

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

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

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

4.2.5 Intel

559 The Intel Data Center Group (DCG) is at the heart of Intel’s transformation from a personal computer
560 (PC) company to a company that runs the cloud and billions of smart, connected computing devices. The
561 data center is the underpinning for every data-driven service, from artificial intelligence to 5G to high-
562 performance computing, and DCG delivers the products and technologies—spanning software,
563 processors, storage, input/output (I/O), security and networking solutions—that fuel cloud,
564 communications, enterprise, and government data centers around the world.

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

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

4.2.6 RSA

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

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

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

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

4.2.7 VMware

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

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

618 *Data Center 4.2* [\[12\]](#), and *Planning and Preparation: VMware Validated Design for Software-Defined*
619 *Data Center 4.2* [\[13\]](#).

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

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

- 626 ▪ VMware vSphere virtualizes and aggregates the underlying physical hardware resources across
627 multiple systems and provides pools of virtual resources to the data center. VMware vSphere
628 includes the following components:
 - 629 • VMware ESXi is a type-1 hypervisor that enables a virtualization layer run on physical servers
630 that abstracts processor, memory, storage, and resources into multiple VMs.
 - 631 • The Platform Services Controller (PSC) Appliance provides common infrastructure services
632 to the vSphere environment. Services include licensing, certificate management, and
633 authentication with vCenter Single Sign-On.
 - 634 • VMware vCS Appliance is a management application that allows for the management of
635 VMs and ESXi hosts centrally. The vSphere Web Client is used to access the vCS.
 - 636 • vSAN is fully integrated hypervisor-converged storage software. vSAN creates a cluster of
637 server hard-disk drives and solid-state drives, and presents a flash-optimized, highly-
638 resilient, shared storage data store to ESXi hosts and VMs. vSAN allows you to control the
639 capacity, performance, and availability, on a per-VM basis, through the use of storage
640 policies.
- 641 ▪ NSX for vSphere (NSX-V) creates a network virtualization layer. All virtual networks are created
642 on top of this layer, which is an abstraction between the physical and virtual networks. Network
643 virtualization services include logical switches, logical routers, logical firewalls, and other
644 components. This design includes the following components:
 - 645 • NSX Manager provides the centralized management plane for NSX-V and has a one-to-one
646 mapping to vCS workloads.
 - 647 • The NSX Virtual Switch is based on the vSphere Distributed Switch (VDS), with additional
648 components to enable rich services. The add-on NSX components include kernel modules
649 (VIBs) that run within the hypervisor kernel and that provide services, such as distributed
650 logical routers (DLRs), distributed firewalls (DFWs), and Virtual Extensible Local Area
651 Network (VXLAN) capabilities.
 - 652 • NSX logical switches create logically abstracted segments to which tenant VMs can be
653 connected. NSX logical switches provide the ability to spin up isolated logical networks with

- 654 the same flexibility and agility that exist with VMs. Endpoints, both virtual and physical, can
655 connect to logical segments and establish connectivity independently from their physical
656 location in the data center network.
- 657 • The universal distributed logical router (UDLR) in NSX-V is optimized for forwarding in the
658 virtualized space (between VMs, on VXLAN-backed or VLAN-backed port groups).
 - 659 • VXLAN Tunnel Endpoints (VTEPs) are instantiated within the VDS to which the ESXi hosts
660 that are prepared for NSX-V are connected. VTEPs are responsible for encapsulating VXLAN
661 traffic as frames in User Datagram Protocol (UDP) packets and for the corresponding
662 decapsulation. VTEPs exchange packets with other VTEPs.
 - 663 • The primary function of the NSX Edge Services Gateway (ESG) is north-south
664 communication, but it also offers support for Layer 2; Layer 3; perimeter firewall; load
665 balancing; and other services, such as Secure Sockets Layer (SSL) VPN and DHCP relay.
- 666 ■ vRealize Operations Manager (vROPS) tracks and analyzes the operation of multiple data
667 sources in the SDDC by using specialized analytic algorithms. These algorithms help vROPS learn
668 and predict the behavior of every object that it monitors. Users access this information by using
669 views, reports, and dashboards.
 - 670 ■ vRealize Log Insight (vRLI) provides real-time log management and log analysis with machine-
671 learning-based intelligent grouping, high-performance searching, and troubleshooting across
672 physical, virtual, and cloud environments.
 - 673 ■ vRealize Automation (vRA) provides the self-service provisioning, IT services delivery, and life-
674 cycle management of cloud services across a wide range of multivendor, virtual, physical, and
675 cloud platforms, through a flexible and robust distributed architecture.
 - 676 ■ vRealize Orchestrator (vRO) provides the automation of complex tasks by allowing for a quick
677 and easy design and deployment of scalable workflows. It automates management and
678 operational tasks across both VMware and third-party applications, such as service desks,
679 change management, and IT asset management systems.
 - 680 ■ vRealize Business for Cloud (vRB) automates cloud costing, consumption analysis, and
681 comparison, delivering the insight that you need for efficiently deploying and managing cloud
682 environments. vRB tracks and manages the costs of private and public cloud resources from a
683 single dashboard.
 - 684 ■ VMware Site Recovery Manager (optional, depends on failover site) is disaster-recovery
685 software that enables application availability and mobility across sites with policy-based
686 management, non-disruptive testing, and automated orchestration. Site Recovery Manager
687 administrators perform frequent non-disruptive testing to ensure IT disaster-recovery
688 predictability and compliance. Site Recovery Manager enables fast and reliable recovery by
689 using fully automated workflows.
 - 690 ■ vSphere Replication (vR) (optional, depends on failover site) is a hypervisor-based, asynchronous
691 replication solution for vSphere VMs. It is fully integrated with the VMware vCS and the vSphere

692 Web Client. vR delivers flexible, reliable, and cost-efficient replication to enable data protection
693 and disaster recovery for VMs.

4.2.8 Products and Technologies Summary

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

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

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

709 **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.

Component	Product	Version	Function	Cybersecurity Framework Subcategories	SP 800-53r4 Controls
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
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

Component	Product	Version	Function	Cybersecurity Framework Subcategories	SP 800-53r4 Controls
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
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

Component	Product	Version	Function	Cybersecurity Framework Subcategories	SP 800-53r4 Controls
Virtual Infrastructure Data Synchronization	Site Recovery Manager (SRM)	6.5.1	A 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	A hypervisor-based, asynchronous replication solution for vSphere VMs.	N/A	N/A
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

Component	Product	Version	Function	Cybersecurity Framework Subcategories	SP 800-53r4 Controls
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
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

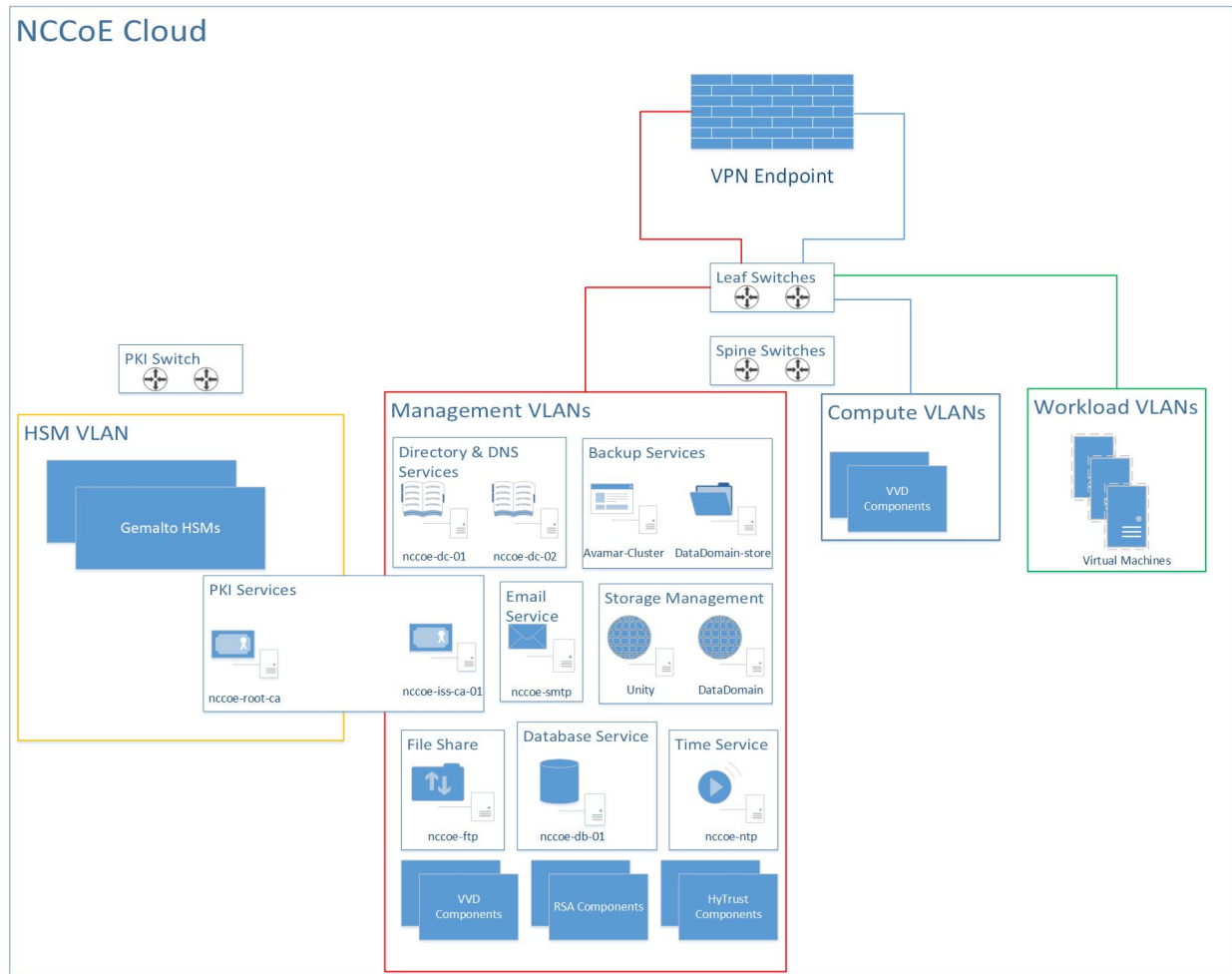
710 4.3 NCCoE Cloud Solution Architecture

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

- 713 ▪ VMware cluster architectures ([Section 4.3.1](#))
- 714 ▪ RSA cluster architecture ([Section 4.3.2](#))
- 715 ▪ HSM architecture ([Section 4.3.3](#))
- 716 ▪ HyTrust architecture ([Section 4.3.4](#))

- 717 ▪ Dell leaf and spine switch architecture ([Section 4.3.5](#))

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



4.3.1 VMware Cluster Architectures

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

- 722 ▪ use of the leaf-spine architecture
- 723 ▪ use of Border Gateway Protocol (BGP) routing
- 724 ▪ availability of dedicated VLANs
- 725 ▪ ability to configure jumbo frames

- 726 ▪ Network File System (NFS) storage availability
- 727 ▪ use of vSAN Ready Nodes (optional)
- 728 ▪ availability of existing data-center services, such as Active Directory, DNS, SMTP, and NTP

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

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

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

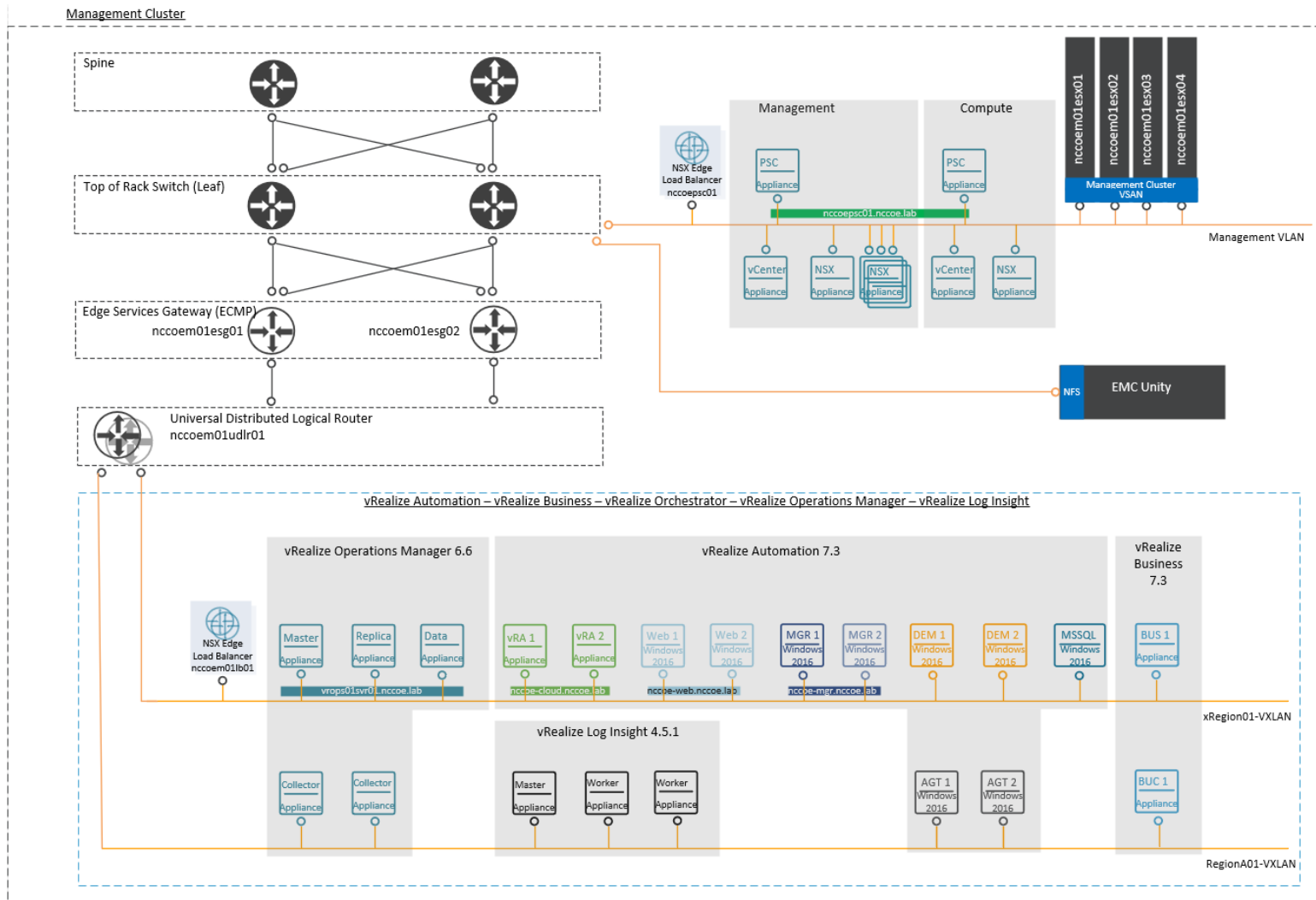
743 vRLI provides deep operational visibility and faster troubleshooting across physical, virtual, and cloud
744 environments. In this solution, vRLI is designed to provide a highly available solution for each site where
745 logs can be forwarded to a remote site for retention.

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

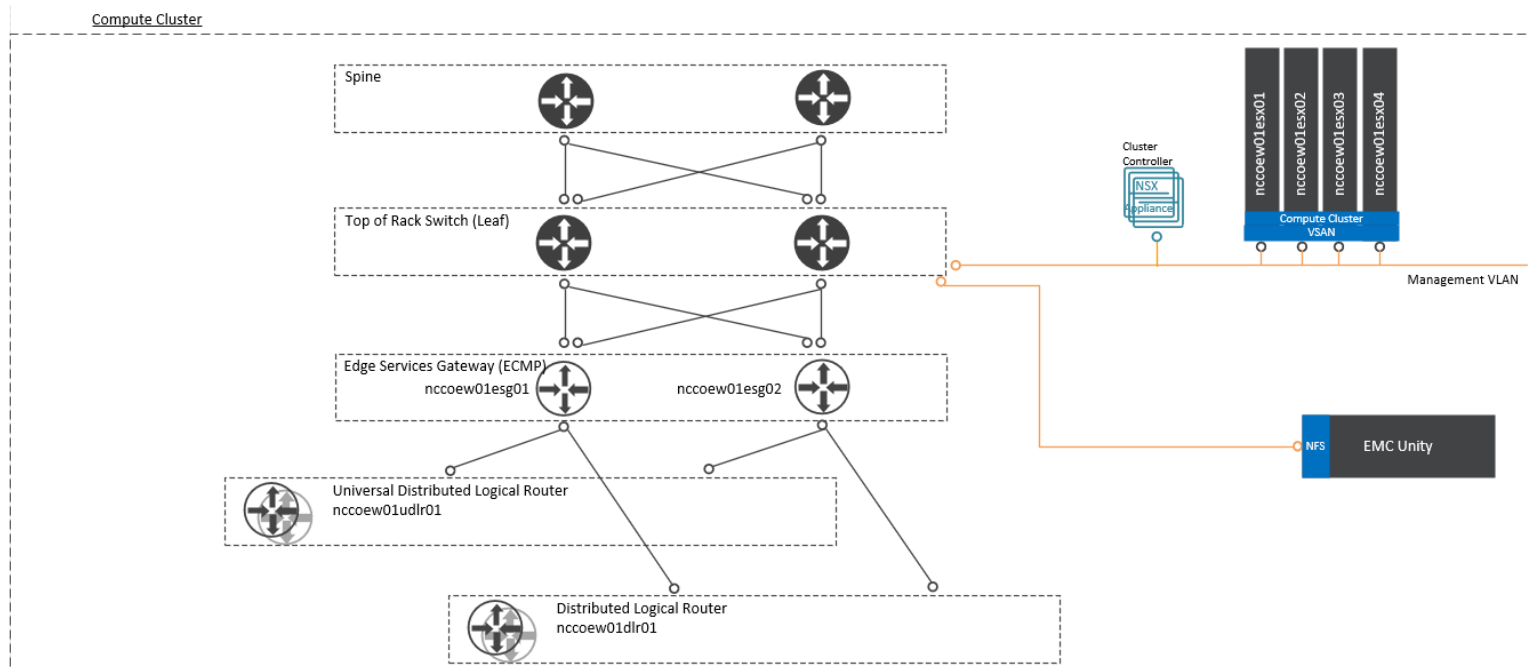
751 vRA provides a portal where authorized individuals can request new IT services and manage cloud and IT
752 workloads. Requests for IT services, including infrastructure, applications, desktops, and many others,
753 are processed through a common service catalog to provide a consistent user experience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

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

761 Figure 4-3 VMware Management Cluster Architecture



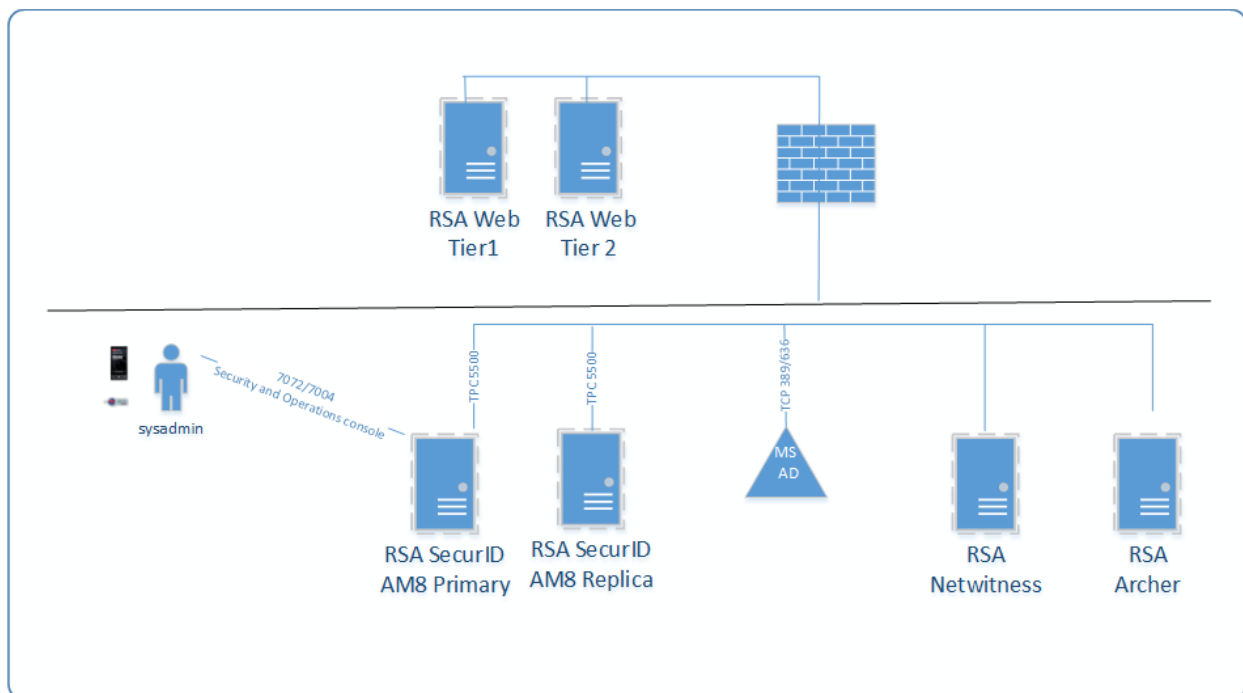
762 Figure 4-4 VMware Compute Cluster Architecture



4.3.2 RSA Cluster Architecture

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

770 **Figure 4-5 RSA Cluster**



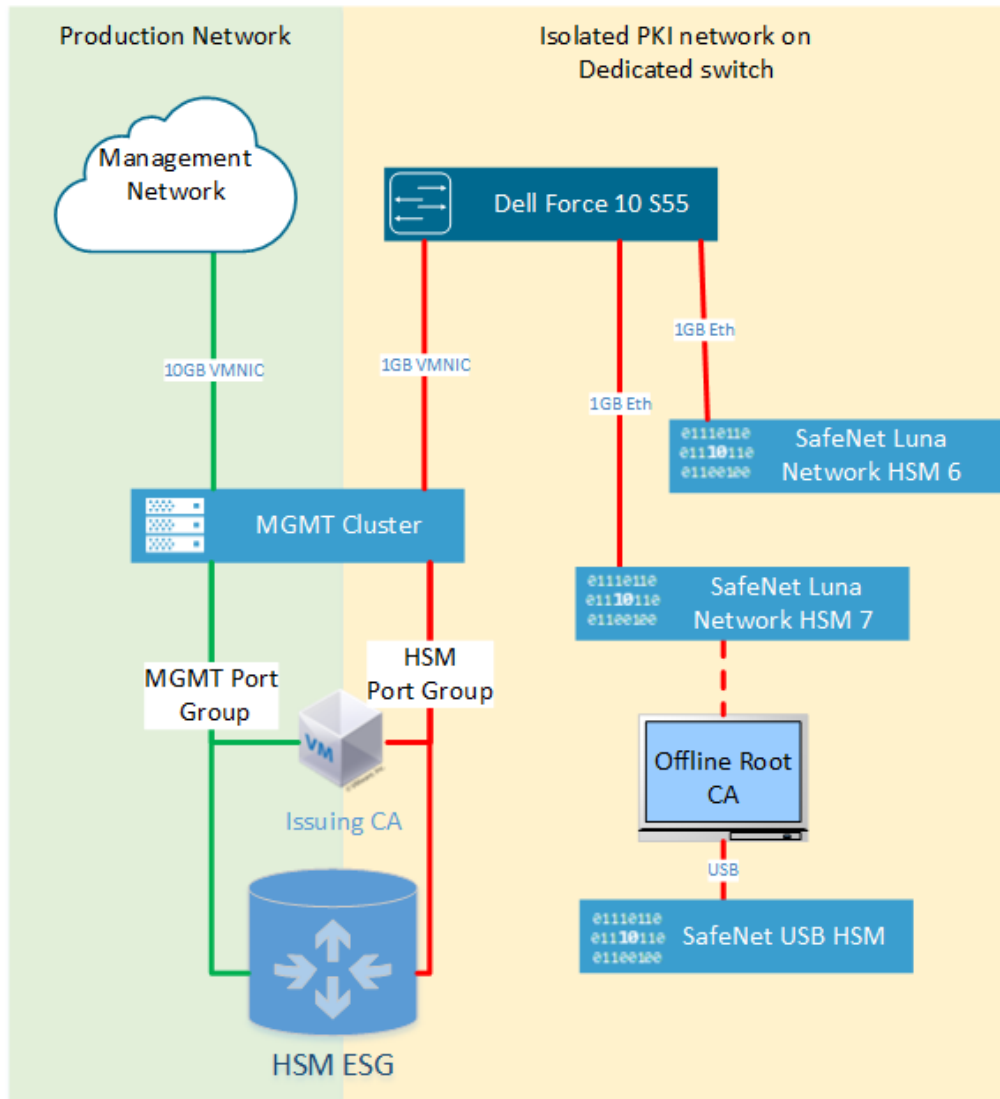
4.3.3 HSM Architecture

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

- 773 ▪ The SafeNet USB HSM is a small form-factor physical device connected via USB to the Microsoft
 774 Root CA Server. To sign and issue a new Issuing CA certificate, the SafeNet USB HSM must be
 775 connected directly to the Root CA. Because the SafeNet USB HSM is primarily used to protect
 776 the Root CA's keys, it is typically stored securely in a vault. The SafeNet USB HSM is backed up
 777 (i.e., cloned) to a secondary SafeNet USB HSM for redundancy.

- 778 ▪ SafeNet Luna Network HSM 7 is a network-attached HSM that is tightly integrated with the
779 Microsoft Issuing CA that is located on a VM in the management cluster as a root of trust for
780 FIPS 140-2 Level 3 Compliance.
- 781 ▪ SafeNet Luna Network HSM 6 is a network-attached HSM integrated with HTKC as a root of trust
782 for FIPS 140-2 Level 3 Compliance.

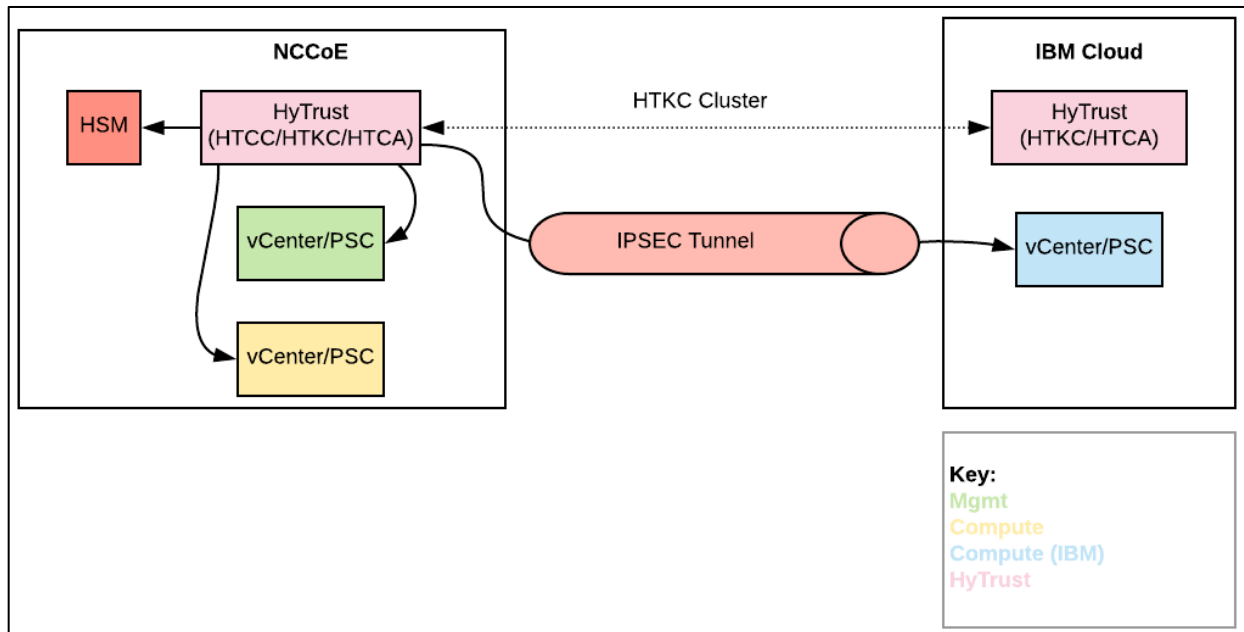
783 **Figure 4-6 HSM Architecture in the NCCoE Cloud**



4.3.4 HyTrust Architecture

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

787 **Figure 4-7 HyTrust Architecture in the NCCoE Cloud**

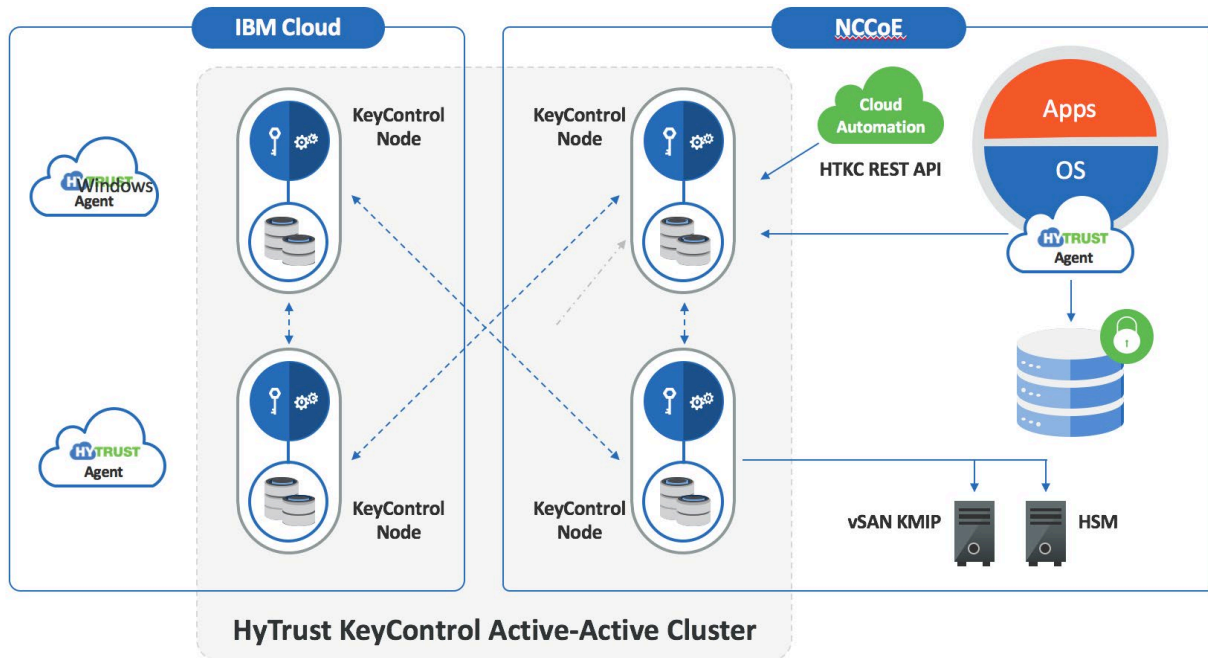


788 The following items explain where each type of HyTrust appliance is located within the architecture and
 789 what functions it is providing:

- 790 ■ HTCC provides advanced security features to vSphere. Additionally, HTCC Compliance is used to
 791 verify the compliance of ESXi hosts. Users access vSphere via the “Published IP [Internet
 792 Protocol]” (PIP) via the HTCC transparent proxy. Approved actions are passed through to
 793 vSphere via a service account. Finally, HTCC conducts trust attestation for Intel TXT/TPM, to
 794 provide hardware verification for HTBC. HTCC will be placed in the NCCoE management cluster.
 795 HTCC will be configured with two virtual appliances in an active/passive cluster. That HTCC
 796 cluster will service all three vSphere implementations.
- 797 ■ HTKC provides key management to both HTDC in-guest encryption agents and vSANs for
 798 storage-level encryption. HTKC leverages the NCCoE SafeNet Luna HSM for hardware
 799 administration key storage. HTKC is configured as a trusted key management service in vCenter
 800 to provide key management to vSAN. Two HTKC nodes will be placed in the NCCoE management
 801 cluster, and two HTKC nodes will be placed in the IBM Cloud, with all four nodes in the same
 802 fully active cluster. [Figure 4-8](#) depicts this cluster.

- 803 ▪ HTCA will be placed in the NCCoE management cluster and the IBM Cloud. There will be one
804 HTCA node per location, and the nodes will not be clustered.

805 **Figure 4-8 HTKC Node Deployments**



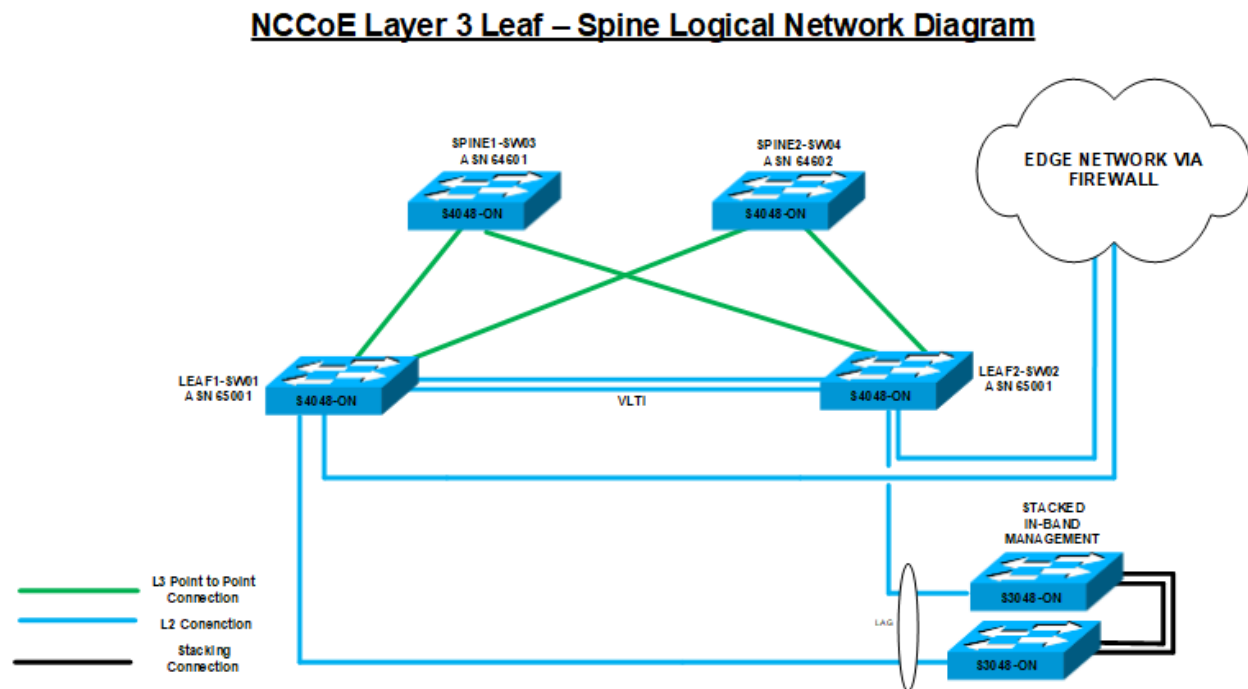
4.3.5 Dell Leaf and Spine Switch Architecture

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

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

821 Ethernet ports supporting components in the environment that have only 1 GB Ethernet connections
 822 and that need to communicate with devices that use 10 GB Enhanced Small Form-Factor Pluggable
 823 (SFP+) connections.

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



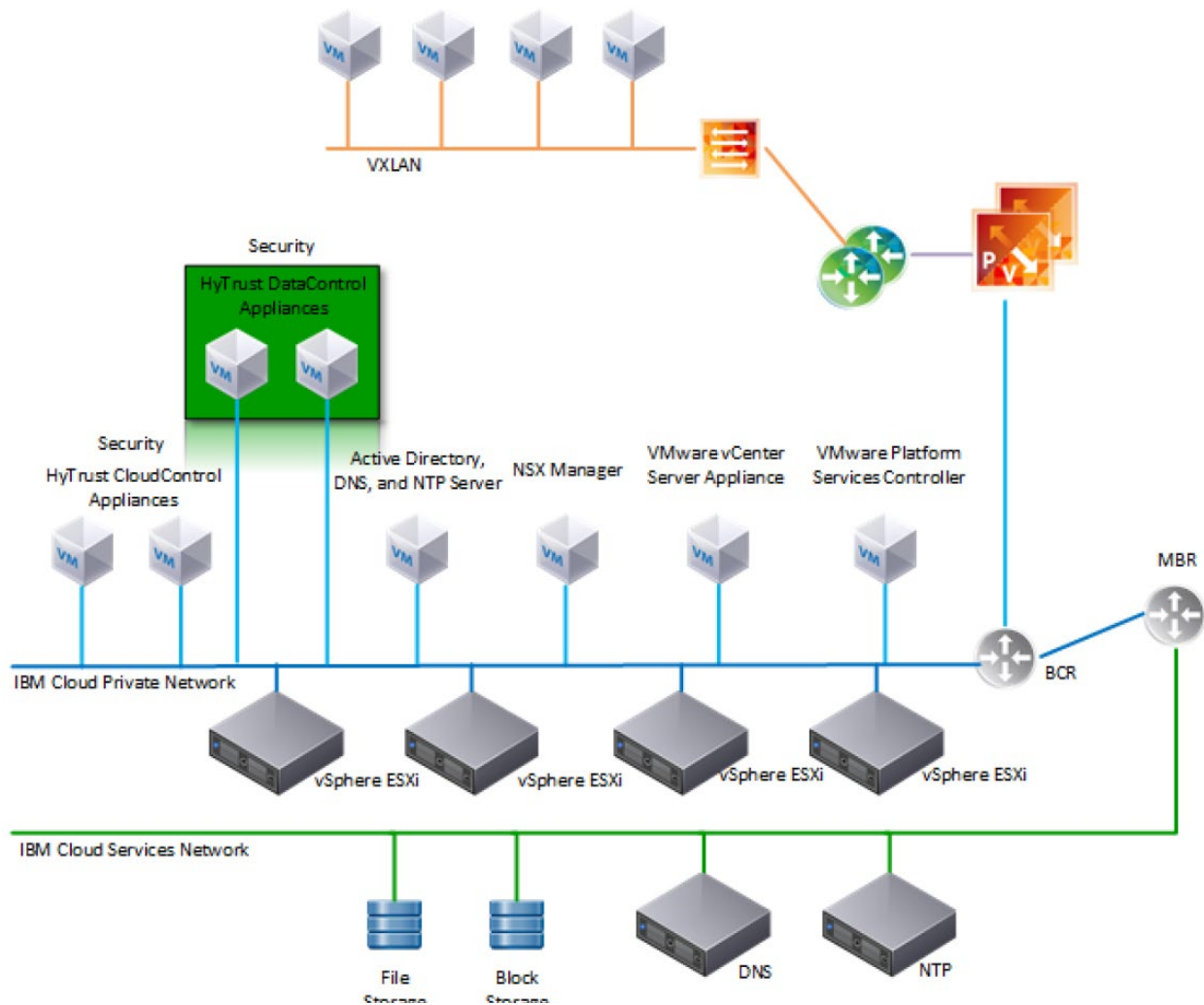
825 **4.4 IBM Cloud Solution Architecture**

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

837 See [Section 4.3](#) for more information on the architecture of the solution components from VMware,
 838 HyTrust, and others. Because some of the same components are used for both clouds to extend the

839 management plane across the infrastructure, details of those components are omitted from this section
840 to avoid duplication.

841 Figure 4-10 IBM Cloud Architecture



842 5 Security Characteristics Analysis

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

847 5.1 Assumptions and Limitations

848 The security characteristics analysis has the following limitations:

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

854 5.2 Demonstration of the Capabilities

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

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

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

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

- 863 1. The cryptographic, compute, storage, and network hardware components are secured and
864 hardened.
- 865 2. The VVD and the IBM Cloud for VMware – vCS have been instantiated on IBM Cloud stacks
866 through automation scripts.
- 867 3. The crypto network is separated and isolated from the management cluster and the tenant
868 workloads cluster.
- 869 4. The user accounts are isolated and secured based on defined functional roles following the
870 principle of least privilege.
- 871 5. The core components of the VVD and vCS, third-party software components, and all core
872 services are secured and hardened using recommended practices, such as vendor-developed or
873 community-developed secure configuration guides or DISA STIGs.
- 874 6. RSA NetWitness Logs is installed on the virtual machine or dedicated hardware.
- 875 7. RSA Archer Suite and the Public Sector Use Cases (Assessment & Authorization [A&A],
876 Continuous Monitoring) are installed.

- 877 8. Logs from core services are being forwarded to RSA NetWitness Logs.
- 878 9. One or more industry-standard cloud service provider certifications, such as ISO, PCI, Cloud
- 879 Security Alliance (CSA), Service Organization Control (SOC), HIPAA, and FedRAMP, are leveraged.
- 880 Capability demonstrations:
- 881 1. Show the configuration of the hardware components, including the HSM, the compute node, the
- 882 storage device, and the network switches.
- 883 2. Show the VVD and vCS stacks in vCenter (e.g., vSAN is encrypted).
- 884 3. Show the backup solution for the resiliency and recovery of workloads in a disaster-recovery
- 885 scenario.
- 886 4. Show the three isolation domains, including the cryptographic, management, and tenant
- 887 workloads in NSX.
- 888 5. Show multifactor authentication with an RSA SecurID token and the Active Directory domain
- 889 groups and access rights structure.
- 890 6. Scan and show the secure configuration of VMware software components, such as ESXi, NSX,
- 891 and Windows domain controller, by using CloudControl and a Windows configuration scanner.
- 892 Figure 5-1 shows an example of results from a secure configuration scan.

893 **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	PII	N/A	Never	0%
10.121.71.135	ESXi Host			N/A	N/A	0%
192.168.4.105	VMware NSX	6.4.0.7554187		N/A	Never	0%
192.168.4.106	VMware NSX	6.4.0.7554187		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, PII	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, PII	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, PII	VMware 6.0 ESXi_Custom_Template	08/23/2018 12:14:24 PM	100%

- 894 7. Scan and show any software vulnerabilities of an ESXi node and a Microsoft workload.
- 895 8. Show the IBM FedRAMP report.
- 896 9. Show the configuration of the log collector for ingesting and enriching VMware ESXi logs.
- 897 10. Show the logs and alerts (if any) in the Analyst UI.
- 898 11. Show the ability to raise an Incident from RSA NetWitness Logs to RSA Archer Suite.
- 899 12. Show the configuration of the Archer Public Sector Use Cases to accept and/or ingest
- 900 information from various components about risks in the trusted hybrid cloud environment.

901 13. Show the analyst interface and outputs of Archer Public Sector Use Cases in recording
 902 compliance and enabling risk mitigation activities.

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

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

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

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

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

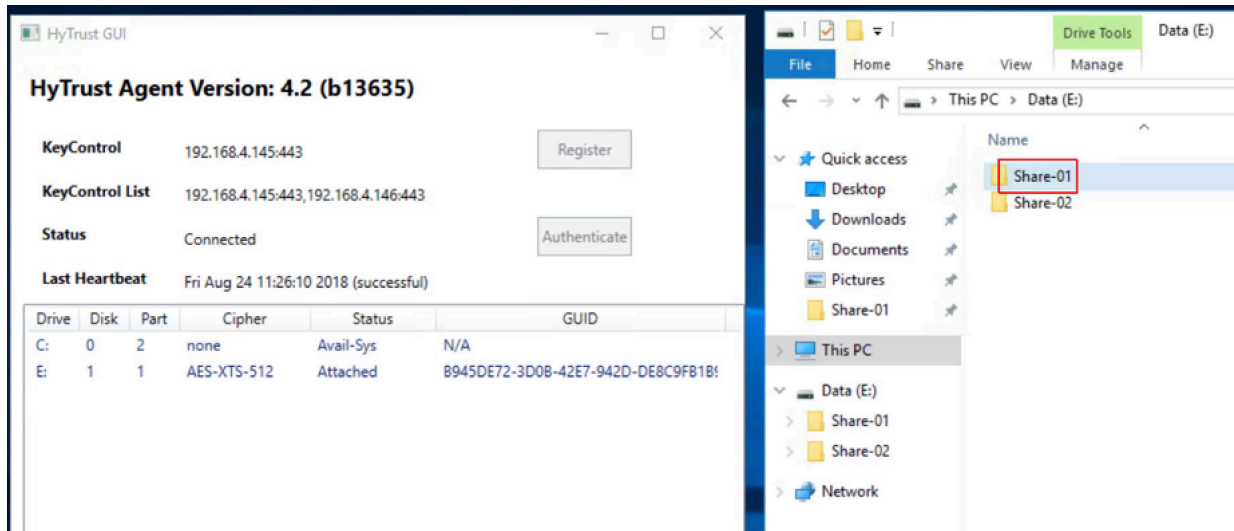
912 Capability demonstrations:

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

916 **Figure 5-2 Examples of Trusted Compute Nodes**

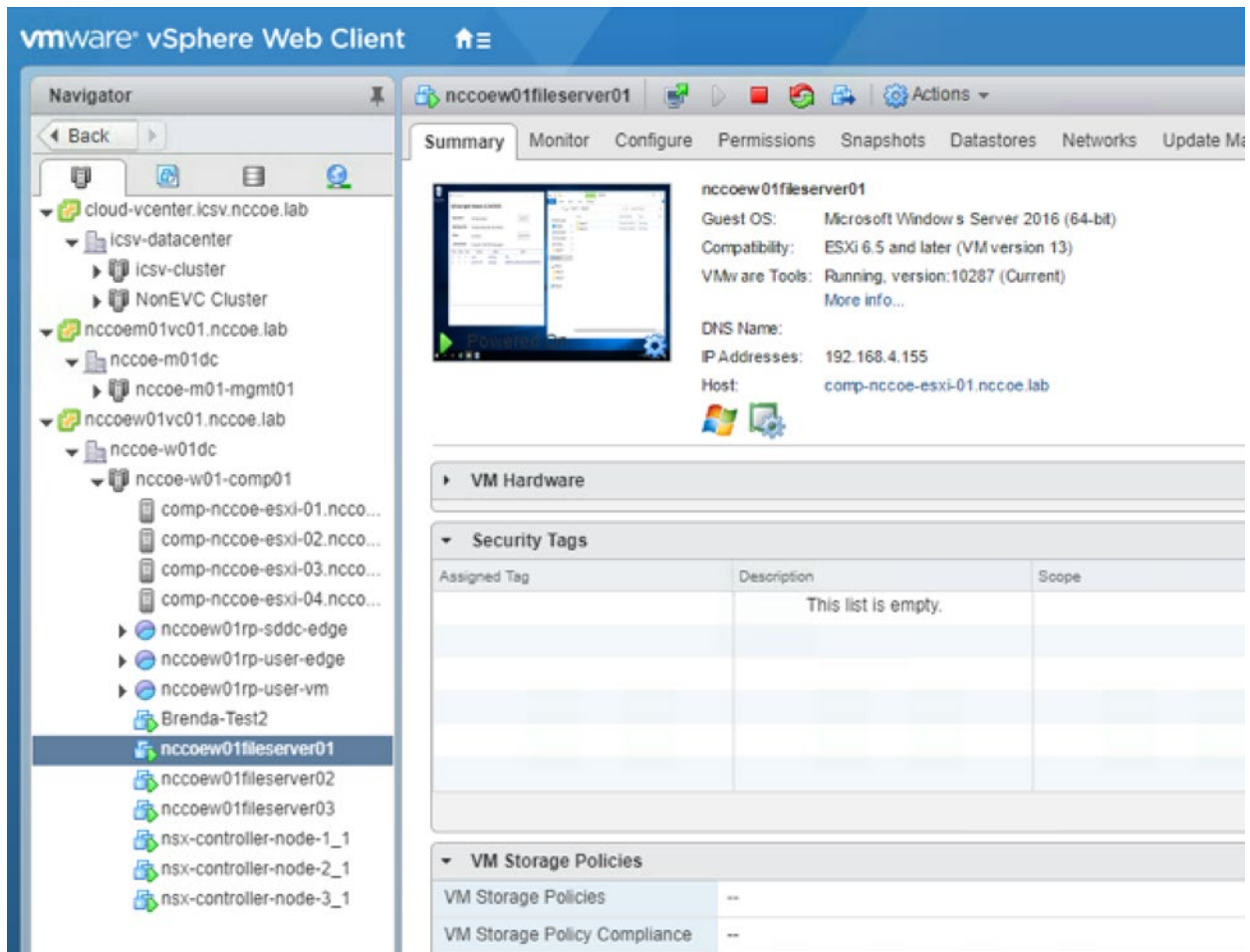
comp-nccoe-esxi-01.nccoe.lab 	ESXi Host	VMware ESXi 6.5.0 build-7388607	
comp-nccoe-esxi-02.nccoe.lab  	ESXi Host	VMware ESXi 6.5.0 build-7388607	TRUSTED, PII
comp-nccoe-esxi-03.nccoe.lab  	ESXi Host	VMware ESXi 6.5.0 build-7388607	TRUSTED, PII
comp-nccoe-esxi-04.nccoe.lab  	ESXi Host	VMware ESXi 6.5.0 build-7388607	TRUSTED, PII

917 Figure 5-3 Example of Decrypted Workload



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

922 Figure 5-4 Example of Workload on Untagged Server

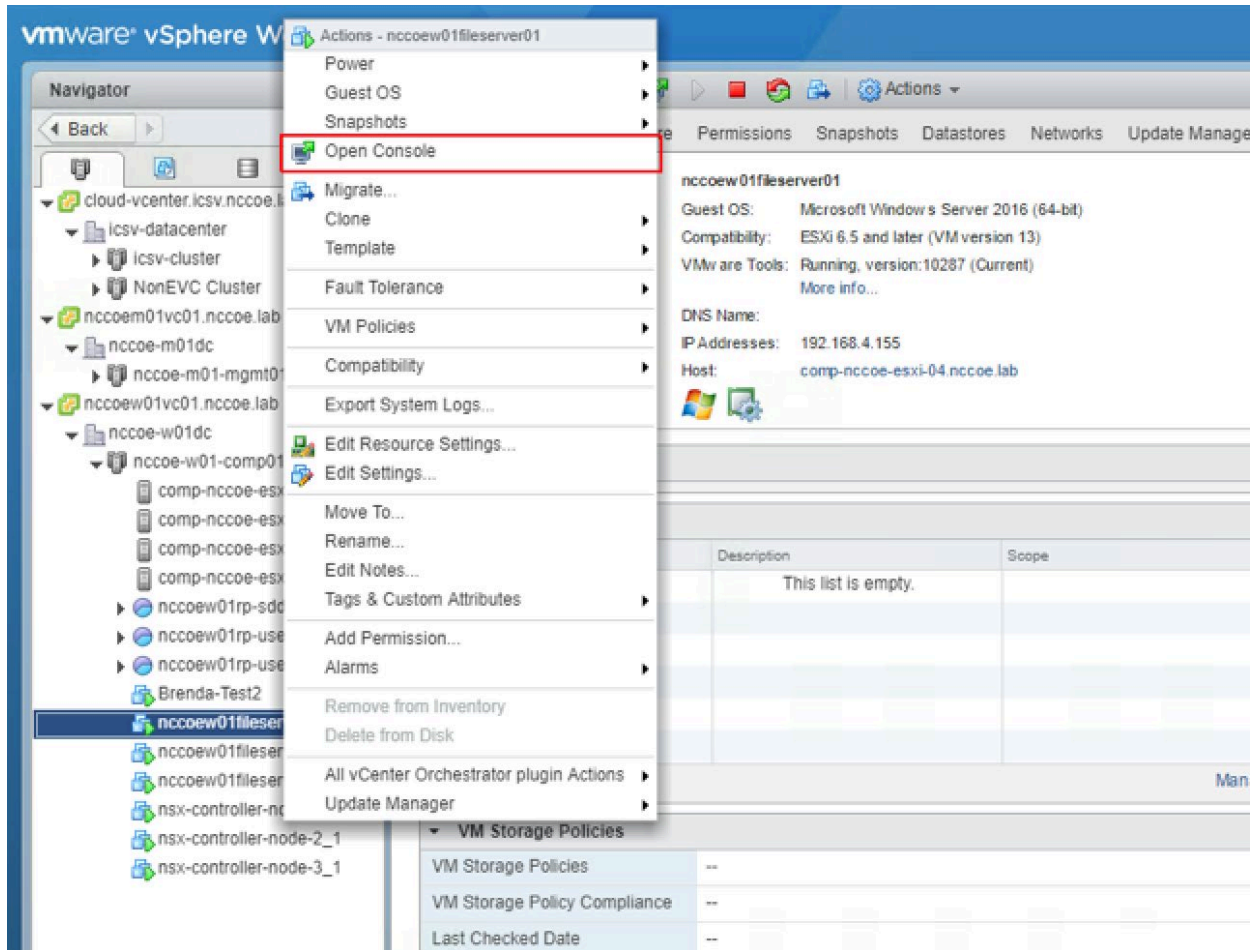


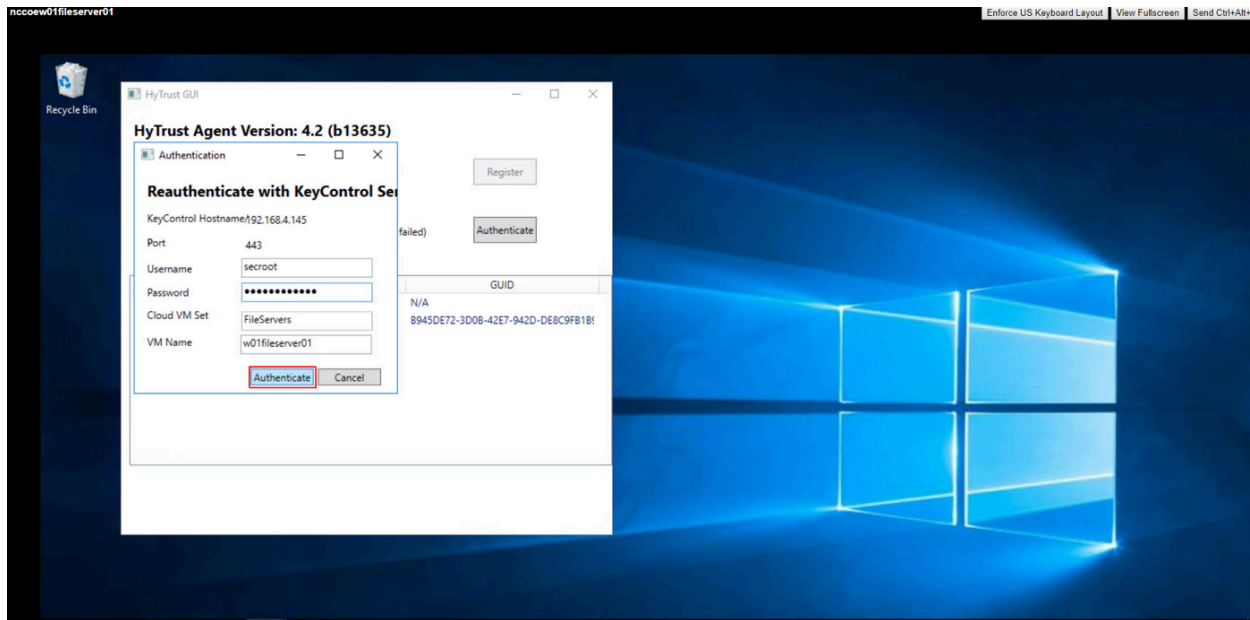
923 Figure 5-5 Example of Workload that Cannot Be Decrypted



- 924
- 925 3. Migrate the workload back to a trusted compute node, and show that the workload can be
- 926 decrypted and that the data can be accessed on the trusted compute node. [Figure 5-6](#) shows
- 927 that the workload has been migrated to a trusted and tagged server. [Figure 5-7](#) shows that the
- 928 workload can decrypt its data again because it is running on a trusted and tagged server.

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



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

- 931 4. Show that two individuals are required to authorize the deletion of a high-value asset.
- 932 5. Scan and classify data based on a data classification schema, such as personally identifiable
- 933 information.
- 934 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

935 There are two business problems addressed. The first is needing to move workloads (VMs and data)

936 from one trusted compute node to a second one without any degradation of security posture or any loss

937 of information, in order to perform scheduled maintenance on the first trusted compute node. An

938 example of a reason for scheduled maintenance is to patch or upgrade the hypervisor. The second is

939 ensuring scripts, configurations, and other files or settings with hard-coded IP addresses or domain

940 names continue to work even when workloads containing them are migrated from one cloud to

941 another.

942 Assumptions for the trusted hybrid cloud environment (steps taken before the demonstrations occur)

943 are as follows:

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

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

951 Capability demonstrations:

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

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

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

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

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

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

975 Capability demonstrations:

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

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

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

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

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

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

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

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

998 Capability demonstrations:

- 999 1. Show that authorized administrators can see a vRLI custom dashboard for traffic flows indicating
1000 what is talking to what, both physical and virtual.
- 1001 2. Show that the traffic flows include source, destination, ports, and protocol.
- 1002 3. Show that the traffic flows from all the devices logging the flows are transferred to NetWitness.

1003 The potential benefit of this is to identify suspicious activity, such as large data bursts, that may indicate
1004 exfiltration of sensitive data or other security problems.

5.2.6 Use Case Scenario 6: Demonstrate Application Zero Trust

1005 The business problem is preventing unauthorized communications with a particular application.

1006 Assumptions for the trusted hybrid cloud environment (steps taken before the demonstrations occur)
1007 are as follows:

- 1008 1. An application is executing within a workload running on a trusted compute node.
- 1009 2. The infrastructure supporting the application has been allowlisted through DFW.

1010 Capability demonstrations:

- 1011 1. Show that communications from the allowlisted infrastructure components are permitted.
- 1012 2. Show that communications from anywhere other than the allowlisted infrastructure
1013 components are denied, and such communications flagged or alerted on.

1014 The potential benefit of this is to prevent attackers and other unauthorized parties from accessing the
1015 application and using it or compromising it.

1016 Appendix A Mappings

1017 The tables in this appendix include all the NIST Cybersecurity Framework subcategories and NIST SP 800-
 1018 53 Revision 5 controls listed in [Section 4.2.8](#)—those provided by individual components of the
 1019 solution—and also list additional subcategories and controls provided by the solution as a whole, not an
 1020 individual component.

1021 **Table A-1 List of NIST SP 800-53 Revision 5 Controls Addressed by Solution**

ID	Control Description
Access Control (AC)	
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-17	Remote Access
AC-20	Use of External Information Systems
Audit and Accountability (AU)	
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
Security Assessment and Authorization (CA)	
CA-7	Continuous Monitoring
Configuration Management (CM)	
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
Identification and Authentication (IA)	
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
Maintenance (MA)	
MA-2	Controlled Maintenance
MA-3	Maintenance Tools
MA-4	Nonlocal Maintenance
MA-5	Maintenance Personnel
MA-6	Timely Maintenance
Risk Assessment (RA)	
RA-3	Risk Assessment
RA-5	Vulnerability Scanning
System and Services Acquisition (SA)	
SA-18	Tamper Resistance and Detection
System and Communications Protection (SC)	
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
System and Information Integrity (SI)	
SI-2	Flaw Remediation
SI-4	Information System Monitoring
SI-7	Software, Firmware, and Information Integrity

1022 Table A-2 List of NIST Cybersecurity Framework Subcategories Addressed by Solution

Cyber-security Framework Subcategory Identifier	Cybersecurity Framework Subcategory Name
Identify (ID)	
ID.AM-2	Software platforms and applications within the organization are inventoried.
Protect (PR)	
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.
Detect (DE)	
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.

1023 **Appendix B List of Acronyms**

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

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

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

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

1024 **Appendix C** **Glossary**

1025 All significant technical terms used within this document are defined in other key documents,
1026 particularly NISTIR 7904, *Trusted Geolocation in the Cloud: Proof of Concept Implementation* [\[1\]](#). As a
1027 convenience to the reader, terms critical to understanding this volume are provided in this glossary.

Attestation	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.
Cloud workload	A logical bundle of software and data that is present in, and processed by, a cloud computing technology.
Geolocation	Determining the approximate physical location of an object, such as a cloud computing server.
Hardware root of trust	An inherently trusted combination of hardware and firmware that maintains the integrity of information.
Trusted compute pool	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> .

1028 Appendix D References

- 1029 [1] M. Bartock et al., “Trusted geolocation in the cloud: Proof of concept implementation,” NIST,
1030 Gaithersburg, MD, NISTIR 7904, Dec. 2015. Available: <https://doi.org/10.6028/NIST.IR.7904>.
- 1031 [2] NIST, “National Cybersecurity Center of Excellence (NCCoE) trusted geolocation in the cloud
1032 building block,” *Federal Register*, vol. 82, no. 90, pp. 21979-21980, May 11, 2017.
1033 Available: <https://www.gpo.gov/fdsys/pkg/FR-2017-05-11/pdf/2017-09502.pdf>.
- 1034 [3] Joint Task Force, “Guide for conducting risk assessments,” NIST, Gaithersburg, MD, NIST SP 800-
1035 30 Revision 1, Sep. 2012. Available: <https://doi.org/10.6028/NIST.SP.800-30r1>.
- 1036 [4] Joint Task Force, “Risk Management Framework for Information Systems and Organizations: A
1037 System Life Cycle Approach for Security and Privacy,” NIST, Gaithersburg, MD, NIST SP 800-37
1038 Revision 2, Dec. 2019. Available: <https://doi.org/10.6028/NIST.SP.800-37r2>.
- 1039 [5] *Risk management – Guidelines*, ISO Standard 31000:2018, Feb. 2018.
1040 Available: <https://www.iso.org/iso-31000-risk-management.html>.
- 1041 [6] COSO, “Enterprise risk management – Integrating with strategy and performance,” COSO, Jun.
1042 2017. Available: <https://www.coso.org/Pages/erm.aspx>.
- 1043 [7] J. Freund and J. Jones, *Measuring and Managing Information Risk: A FAIR Approach*. Oxford,
1044 England: Butterworth-Heinemann, 2014.
- 1045 [8] NIST, “Framework for improving critical infrastructure cybersecurity,” NIST, Gaithersburg, MD,
1046 Apr. 16, 2018, Version 1.1. Available: <https://doi.org/10.6028/NIST.CSWP.04162018>.
- 1047 [9] Joint Task Force Transformation Initiative, “Security and privacy controls for federal information
1048 systems and organizations,” NIST, Gaithersburg, MD, NIST SP 800-53 Revision 4, Apr. 2013.
1049 Available: <https://doi.org/10.6028/NIST.SP.800-53r4>.
- 1050 [10] VMware, “Architecture and design: VMware validated design for management and workload
1051 consolidation 4.2,” VMware, Palo Alto, CA, Mar. 27, 2018.
1052 Available: <https://docs.vmware.com/en/VMware-Validated-Design/4.2/vmware-validated-design-42-sddc-consolidated-architecture-design.pdf>.
1053
- 1054 [11] VMware, “Deployment for region A: VMware validated design for software-defined data center
1055 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>.
1056
- 1057 [12] VMware, “Operational verification: VMware validated design for software-defined data center
1058 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>.
1059

- 1060 [13] VMware, "Planning and preparation: VMware validated design for software-defined data center
1061 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>.
1062

Trusted Cloud:

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

Volume C: How-to Guides

Michael Bartock
Murugiah Souppaya
Computer Security Division
Information Technology
Laboratory

Daniel Carroll
Robert Masten
Dell/EMC
Hopkinton, Massachusetts

Gina Scinta
Paul Massis
Gemalto
Austin, Texas

Harmeet Singh
Rajeev Ghandi
Laura E. Storey
IBM
Armonk, New York

Raghuram Yeluri
Intel
Santa Clara, California

Michael Dalton
Rocky Weber
RSA
Bedford, Massachusetts

Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

Anthony Dukes
Jeff Haskins
Carlos Phoenix
Brenda Swarts
VMware
Palo Alto, California

October 2021

DRAFT

This publication is available free of charge from:
<https://www.nccoe.nist.gov/projects/building-blocks/trusted-cloud>

1 **DISCLAIMER**

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

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

13 National Institute of Standards and Technology Special Publication 1800-19C, Natl. Inst. Stand. Technol.
14 Spec. Publ. 1800-19C, 124 pages, (October 2021), CODEN: NSPUE2

15 **FEEDBACK**

16 You can improve this guide by contributing feedback. As you review and adopt this solution for your
17 own organization, we ask you and your colleagues to share your experience and advice with us.

18 Comments on this publication may be submitted to: trusted-cloud-nccoe@nist.gov.

19 Public comment period: October 27, 2021 through December 6, 2021

20 All comments are subject to release under the Freedom of Information Act.

21 National Cybersecurity Center of Excellence
22 National Institute of Standards and Technology
23 100 Bureau Drive
24 Mailstop 2002
25 Gaithersburg, MD 20899
26 Email: nccoe@nist.gov

27 NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

43 NIST CYBERSECURITY PRACTICE GUIDES

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

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

53 ABSTRACT

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

63 services to address lifting and shifting a typical multi-tier application between an organization-
64 controlled private cloud and a hybrid/public cloud over the internet.

65 **KEYWORDS**

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

67 **ACKNOWLEDGMENTS**

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

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

72 **DOCUMENT CONVENTIONS**

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

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

80 **CALL FOR PATENT CLAIMS**

81 This public review includes a call for information on essential patent claims (claims whose use would be
82 required for compliance with the guidance or requirements in this Information Technology Laboratory
83 (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication
84 or by reference to another publication. This call also includes disclosure, where known, of the existence
85 of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant
86 unexpired U.S. or foreign patents.

87 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in writ-
88 ten or electronic form, either:

89 a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not
90 currently intend holding any essential patent claim(s); or

91 b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring
92 to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft
93 publication either:

- 94 1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination;
95 or
- 96 2. without compensation and under reasonable terms and conditions that are demonstrably free
97 of any unfair discrimination.

98 Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its
99 behalf) will include in any documents transferring ownership of patents subject to the assurance, provi-
100 sions sufficient to ensure that the commitments in the assurance are binding on the transferee, and
101 that the transferee will similarly include appropriate provisions in the event of future transfers with the
102 goal of binding each successor-in-interest.

103 The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of
104 whether such provisions are included in the relevant transfer documents.

105 Such statements should be addressed to: trusted-cloud-nccoe@nist.gov

106 **Contents**

107 **1 Introduction 1**

108 1.1 Practice Guide Structure 1

109 1.2 Build Overview 2

110 1.3 Typographic Conventions..... 3

111 1.4 Logical Architecture Summary 3

112 **2 Dell EMC Product Installation and Configuration Guide 5**

113 2.1 Dell EMC Unity Hardening Guidance 5

114 2.2 Dell Networking S4048-ON, S3048-ON, OS9 Hardening..... 6

115 2.2.1 Functionality and interoperability (layer 3 access)..... 11

116 2.2.2 VLANs..... 16

117 2.3 Dell PowerEdge Hardening..... 20

118 2.4 Avamar Security Hardening..... 20

119 **3 Gemalto Product Installation and Configuration Guide 21**

120 3.1 Gemalto Luna 6 Initialization 21

121 3.2 Create HSM Partition 22

122 **4 HyTrust Product Installation and Configuration Guide..... 23**

123 4.1 HyTrust KeyControl Setup 23

124 4.2 HyTrust DataControl Setup 24

125 4.3 HyTrust CloudControl Appliance Setup..... 24

126 4.3.1 Provisioning PolicyTags..... 25

127 4.3.2 Policy Interaction 27

128 4.4 HyTrust CloudAdvisor Appliance Setup..... 27

129 **5 IBM Product Installation and Configuration Guide 27**

130 5.1 ICSV Deployment..... 28

131 5.1.1 Pre-deployment 29

132 5.1.2 Automation deployment 31

133	5.1.3	Post-deployment	33
134	5.2	Enable Hardware Root of Trust on ICSV Servers.....	37
135	5.2.1	Enable Managed Object Browser (MOB) for each ESXi Server.....	37
136	5.2.2	Enable TPM/TXT on SuperMicro hosts	37
137	5.2.3	Enable TPM/TXT in IBM Cloud	38
138	5.2.4	Validate the TPM/TXT is enabled	39
139	5.2.5	Check the vCenter MOB to see if the TPM/TXT is enabled	39
140	5.2.6	Set up Active Directory users and groups.....	40
141	5.2.7	Join vCenter to the AD domain.....	44
142	5.2.8	Add AD HyTrust-vCenter service user to vCenter as Administrator.....	45
143	5.2.9	Add AD HyTrust-vCenter service user to vCenter Global Permissions	46
144	5.2.10	Configure HTCC for AD authentication	47
145	5.3	Add Hosts to HTCC and Enable Good Known Host (GKH).....	48
146	6	Intel Product Installation and Configuration Guide.....	50
147	7	RSA Product Installation and Configuration Guide.....	50
148	7.1	RSA SecurID	50
149	7.2	RSA NetWitness.....	51
150	7.2.1	Configure the VMware ESX/ESXi Event Source	51
151	7.2.2	Configure the RSA NetWitness Log Collector for VMware Collection.....	52
152	8	VMware Product Installation and Configuration Guide	52
153	8.1	Prerequisites.....	53
154	8.2	Installation and Configuration.....	55
155	8.3	Configuration Customization Supporting the Use Cases and Security Capabilities....	55
156	8.3.1	Example VVD 5.0.1 Configuration: Configure the Password and Policy Lockout Setting in vCenter Server in Region A	56
157			
158	8.3.2	Example VVD 5.0.1 Configuration: Configure Encryption Management in Region A	57
159			
160	8.3.3	Example vRealize Automation DISA STIG Configuration: Configure SLES for vRealize to protect the confidentiality and integrity of transmitted information.....	58
161			
162	8.3.4	Example vRealize Operations Manager DISA STIG Configuration: Configure the vRealize Operations server session timeout.....	58
163			

164 8.4 Operation, Monitoring, and Maintenance..... 58
165 8.4.1 Operation.....58
166 8.4.2 Monitoring.....59
167 8.4.3 Maintenance.....60
168 8.5 Product Configuration Overview..... 62

169

170 Appendices

171 Appendix A Security Configuration Settings 65
172 Appendix B List of Acronyms 121
173 Appendix C Glossary 124

174

175 List of Figures

176 Figure 1-1: High-Level Solution Architecture 5
177 Figure 7-1: RSA Authentication Manager Deployment Architecture..... 51
178 Figure 8-1: Map of VVD Documentation 54

179

180 List of Tables

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

187 1 Introduction

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

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

195 1.1 Practice Guide Structure

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

200 This guide contains three volumes:

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

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

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

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

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

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

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

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

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

233 A NIST Cybersecurity Practice Guide does not describe “the” solution, but a possible solution. This is a
234 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and
235 success stories will improve subsequent versions of this guide. Please contribute your thoughts to
236 trusted-cloud-nccoe@nist.gov.

237 **1.2 Build Overview**

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

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

247 1.3 Typographic Conventions

248 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> .
Bold	names of menus, options, command buttons, and fields	Choose File > Edit .
Monospace	command-line input, onscreen computer output, sample code examples, and status codes	<code>mkdir</code>
Monospace Bold	command-line user input contrasted with computer output	<code>service sshd start</code>
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's NCCoE are available at https://www.nccoe.nist.gov .

249 1.4 Logical Architecture Summary

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

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

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

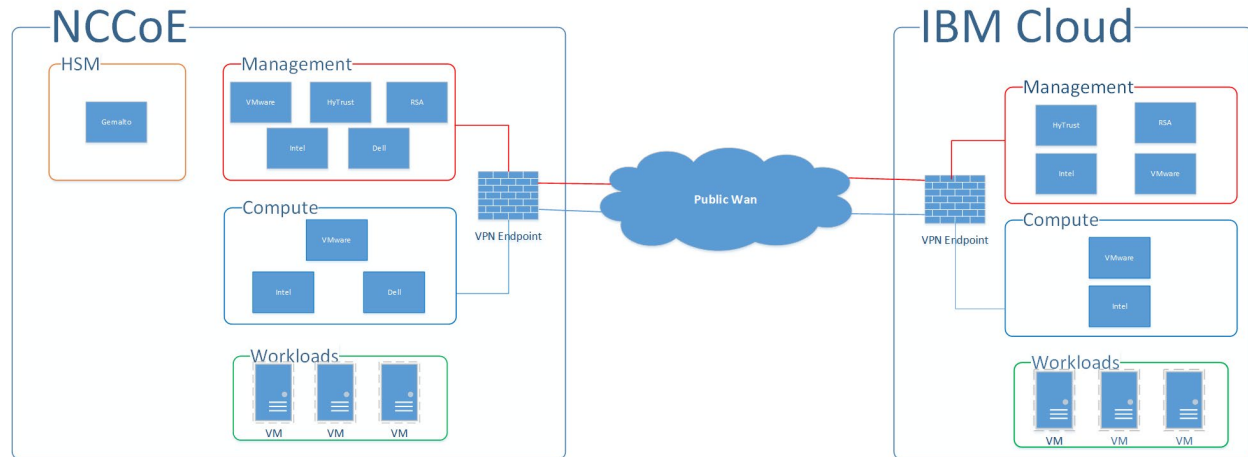
261 The ICSV instance consists of the following components:

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

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

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

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

285 **Figure 1-1: High-Level Solution Architecture**

286 **2 Dell EMC Product Installation and Configuration Guide**

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

- 291 ▪ Dell PowerEdge R740xD
- 292 ▪ Dell EMC Unity
- 293 ▪ Dell Networking S3048/4048-ON Networking
- 294 ▪ Dell Avamar
- 295 ▪ Dell Data Domain

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

300 **2.1 Dell EMC Unity Hardening Guidance**

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

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

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

- 313 ▪ Enabling D@RE
- 314 ▪ Enabling External Key Management
- 315 ▪ Keystore Backup
- 316 ▪ Audit Log and Checksum Retrieval

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

323 **2.2 Dell Networking S4048-ON, S3048-ON, OS9 Hardening**

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

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

335 1. Set the hostname:

```
336             hostname NCCOE-S4048-01
```

337 2. Configure password policies:

- 338 a. Define the minimum security policy to create passwords. Ensure that the password
 339 attributes match your organization's security policy.
- ```
340 password-attributes min-length 15 character-restriction lower 2
341 character-restriction upper 2 character-restriction numeric 2 character-
342 restriction special 2
```
- 343 b. Set up the login lockout period to match your organization's security policy.
- ```
344 password-attributes lockout-period 15
```
- 345 c. Enable password with highest privileges:
- ```
346 enable password level 15 <clear-text password>
```
- 347 3. To enable FIPS cryptography mode, enter this command:
- ```
348 fips mode enable
```
- 349 Note: Enable FIPS mode before you configure the features below. If you do not, the system will
 350 clear some of the configuration, and you must reconfigure some of the features.
- 351 Note: If the system fails to transition to FIPS mode, the system is not in a compliant state.
- 352 4. Enable SSH server:
- ```
353 ip ssh server cipher aes128-ctr aes192-ctr aes256-ctr
354 ip ssh server enable
355 ip ssh server mac hmac-sha1 hmac-sha2-256
```
- 356 5. Disable telnet server:
- ```
357 no ip telnet server enable
```
- 358 6. Define content addressable memory (CAM) allocation and optimization. CAM is a type of
 359 memory that stores information in the form of a lookup table. These CAM settings are required
 360 to configure a conformant IPv4 and IPv6 solution.
- ```
361 cam-acl 12acl 2 ipv4acl 2 ipv6acl 4 ipv4qos 2 12qoa 1 12pt 0 ipmacacl 0 vman-
362 qos cfmacl 0 fedgova1
```
- 363 7. Enforce authentication and authorization of users connecting to system through the console or  
 364 SSH, and then set the timer for terminating a session after 10 minutes of inactivity.
- ```
365 login authentication ucraaa_console
366 exec-timeout 10 0
367 authorization exec ucraaa_console
368 line vty 0
369 login authentication ucraaa_vty
370 exec-timeout 10 0
371 authorization exec ucraaa_vty
372 line vty 1
373 login authentication ucraaa_vty
```

```
374     exec-timeout 10 0
375     authorization exec ucraaa_vty
376     line vty 2
377         login authentication ucraaa_vty
378         exec-timeout 10 0
379         authorization exec ucraaa_vty
380     line vty 3
381         login authentication ucraaa_vty
382         exec-timeout 10 0
383         authorization exec ucraaa_vty
384     line vty 4
385         login authentication ucraaa_vty
386         exec-timeout 10 0
387         authorization exec ucraaa_vty
388     line vty 5
389         login authentication ucraaa_vty
390         exec-timeout 10 0
391         authorization exec ucraaa_vty
392     line vty 6
393         login authentication ucraaa_vty
394         exec-timeout 10 0
395         authorization exec ucraaa_vty
396     line vty 7
397         login authentication ucraaa_vty
398         exec-timeout 10 0
399         authorization exec ucraaa_vty
400     line vty 8
401         login authentication ucraaa_vty
402         exec-timeout 10 0
403         authorization exec ucraaa_vty
404     line vty 9
405         login authentication ucraaa_vty
406         exec-timeout 10 0
407         authorization exec ucraaa_vty
```

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

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

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

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

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

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

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

```
416     router ospf 101
417         router-id 192.168.101.3
418         network 192.168.101.0/24 area 101
```

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

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

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

424 13. Configure system and audit log settings, such as syslog version, buffer size, logging server, and 425 coredump destination:

```
426     service timestamps log datetime localtime msec show-timezone
427     service timestamps debug datetime localtime msec show-timezone
428     !
429     logging coredump stack-unit 1
430     logging coredump stack-unit 2
431     logging coredump stack-unit 3
432     logging coredump stack-unit 4
433     logging coredump stack-unit 5
434     logging coredump stack-unit 6
435     !
```

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

```
437     ntp server 192.168.4.10
438     ntp server 192.168.4.11
```

439 15. Configure the login banner text:

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

460 16. Configure the switch to securely bring the software image to its flash drive. Define where to up- 461 grade the software image to (flash drive) and where to boot the software image from.

```
462     boot system stack-unit 1 primary system://B
463     boot system stack-unit 1 secondary system://B
464     boot system stack-unit 1 default system://A
465     !
```

466 **17. Disable Support Assist:**

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

468 **18. Configure redundancy:**

```
469     redundancy auto-synchronize full
```

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

```
471     interface Loopback 0
472     description NCCOE-S4048-02
473     ip address 10.0.2.2/32
474     no shutdown
475     !
```

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

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

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

```
479     clock timezone Eastern -5
480     clock summer-time Eastern recurring 2 Sun Mar 02:00 1 Sun Nov 02:00
481     !
```

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

```
483     no ip source-route
```

484 **23. Configure reload behavior:**

```
485     reload-type
486     boot-type normal-reload
487     config-scr-download enable
488     vendor-class-identifier "    "
489     !
```

490 **24. Enable login statistics:**

```
491     login concurrent-session limit 3
492     login statistics enable
493     !
```

494 **25. Configure the management interface:**

```
495     interface ManagementEthernet 1/1
496     description OOB_MGMT
497     ip address 10.10.10.11/24
```

```

498         no shutdown
499         !

```

500 2.2.1 Functionality and interoperability (layer 3 access)

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

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

```

505     protocol lldp
506     advertise dot1-tlv port-vlan-id
507     advertise dot3-tlv max-frame-size
508     advertise management-tlv management-address system-capabilities system-
509     description system-name
510     advertise interface-port-desc
511     !

```

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

```

517     interface Port-channel 64
518     description LAG to IB-MGMT switches
519     no ip address
520     switchport
521     vlt-peer-lag port-channel 64
522     no shutdown
523     !
524     interface Port-channel 67
525     no ip address
526     mtu 9216
527     portmode hybrid
528     switchport
529     spanning-tree rstp edge-port bpduguard shutdown-on-violation
530     spanning-tree 0 portfast bpduguard shutdown-on-violation
531     lacp fast-switchover
532     vlt-peer-lag port-channel 67
533     no shutdown
534     !
535     interface Port-channel 68
536     no ip address
537     mtu 9216
538     portmode hybrid
539     switchport
540     spanning-tree rstp edge-port bpduguard shutdown-on-violation
541     spanning-tree 0 portfast bpduguard shutdown-on-violation

```



```

542     lacp fast-switchover
543     vlt-peer-lag port-channel 68
544     no shutdown
545     !
546     interface Port-channel 127
547         description VLTi
548         no ip address
549         channel-member fortyGigE 1/51,1/52
550         no shutdown
551     !

```

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

```

554     interface TenGigabitEthernet 1/1
555         description mgt-nccoe-esxi-01
556         no ip address
557         mtu 9216
558         switchport
559         spanning-tree rstp edge-port bpduguard shutdown-on-violation
560         spanning-tree 0 portfast bpduguard shutdown-on-violation
561         no shutdown
562     !
563     interface TenGigabitEthernet 1/2
564         description mgt-nccoe-esxi-02
565         no ip address
566         mtu 9216
567         switchport
568         spanning-tree rstp edge-port bpduguard shutdown-on-violation
569         spanning-tree 0 portfast bpduguard shutdown-on-violation
570         no shutdown
571     !
572     interface TenGigabitEthernet 1/3
573         description mgt-nccoe-esxi-03
574         no ip address
575         _ mtu 9216
576         _ switchport
577         spanning-tree rstp edge-port bpduguard shutdown-on-violation
578         spanning-tree 0 portfast bpduguard shutdown-on-violation
579         no shutdown
580     !
581     interface TenGigabitEthernet 1/4
582         description mgt-nccoe-esxi-04
583         no ip address
584         mtu 9216
585         switchport
586         spanning-tree rstp edge-port bpduguard shutdown-on-violation
587         spanning-tree 0 portfast bpduguard shutdown-on-violation
588         no shutdown
589     !
590     interface TenGigabitEthernet 1/5
591         description mgt-nccoe-esxi-01

```

```
592     no ip address
593     mtu 9216
594     switchport
595     spanning-tree rstp edge-port bpduguard shutdown-on-violation
596     spanning-tree 0 portfast bpduguard shutdown-on-violation
597     no shutdown
598     !
599 interface TenGigabitEthernet 1/6
600     description mgt-nccoe-esxi-02
601     no ip address
602     mtu 9216
603     switchport
604     spanning-tree rstp edge-port bpduguard shutdown-on-violation
605     spanning-tree 0 portfast bpduguard shutdown-on-violation
606     no shutdown
607     !
608 interface TenGigabitEthernet 1/7
609     description mgt-nccoe-esxi-03
610     no ip address
611     mtu 9216
612     switchport
613     spanning-tree rstp edge-port bpduguard shutdown-on-violation
614     spanning-tree 0 portfast bpduguard shutdown-on-violation
615     no shutdown
616     !
617 interface TenGigabitEthernet 1/8
618     description mgt-nccoe-esxi-04
619     no ip address
620     mtu 9216
621     switchport
622     spanning-tree rstp edge-port bpduguard shutdown-on-violation
623     spanning-tree 0 portfast bpduguard shutdown-on-violation
624     no shutdown
625     !
626 interface TenGigabitEthernet 1/9
627     description comp-nccoe-esxi-01
628     no ip address
629     mtu 9216
630     switchport
631     spanning-tree rstp edge-port bpduguard shutdown-on-violation
632     spanning-tree 0 portfast bpduguard shutdown-on-violation
633     no shutdown
634     !
635 interface TenGigabitEthernet 1/10
636     description comp-nccoe-esxi-02
637     no ip address
638     mtu 9216
639     switchport
640     spanning-tree rstp edge-port bpduguard shutdown-on-violation
641     spanning-tree 0 portfast bpduguard shutdown-on-violation
642     no shutdown
643     !
```

```
644 interface TenGigabitEthernet 1/11
645 description comp-nccoe-esxi-03
646 no ip address
647 mtu 9216
648 switchport
649 spanning-tree rstp edge-port bpduguard shutdown-on-violation
650 spanning-tree 0 portfast bpduguard shutdown-on-violation
651 no shutdown
652 !
653 interface TenGigabitEthernet 1/12
654 description comp-nccoe-esxi-04
655 no ip address
656 mtu 9216
657 switchport
658 spanning-tree rstp edge-port bpduguard shutdown-on-violation
659 spanning-tree 0 portfast bpduguard shutdown-on-violation
660 no shutdown
661 !
662 interface TenGigabitEthernet 1/13
663 description comp-nccoe-esxi-01
664 no ip address
665 mtu 9216
666 switchport
667 spanning-tree rstp edge-port bpduguard shutdown-on-violation
668 spanning-tree 0 portfast bpduguard shutdown-on-violation
669 no shutdown
670 !
671 interface TenGigabitEthernet 1/14
672 description comp-nccoe-esxi-02
673 no ip address
674 mtu 9216
675 switchport
676 spanning-tree rstp edge-port bpduguard shutdown-on-violation
677 spanning-tree 0 portfast bpduguard shutdown-on-violation
678 no shutdown
679 !
680 interface TenGigabitEthernet 1/15
681 description comp-nccoe-esxi-03
682 no ip address
683 mtu 9216
684 switchport
685 spanning-tree rstp edge-port bpduguard shutdown-on-violation
686 spanning-tree 0 portfast bpduguard shutdown-on-violation
687 no shutdown
688 !
689 interface TenGigabitEthernet 1/16
690 description comp-nccoe-esxi-04
691 no ip address
692 mtu 9216
693 switchport
694 spanning-tree rstp edge-port bpduguard shutdown-on-violation
695 spanning-tree 0 portfast bpduguard shutdown-on-violation
```

```
696         no shutdown
697         !
698     interface TenGigabitEthernet 1/31
699         description TO-UNITY-ARRAY
700         no ip address
701         mtu 9216
702         !
703         port-channel-protocol LACP
704         port-channel 68 mode active
705         no shutdown
706         !
707     interface TenGigabitEthernet 1/32
708         description TO-UNITY-ARRAY
709         no ip address
710         mtu 9216
711         !
712         port-channel-protocol LACP
713         port-channel 67 mode active
714         no shutdown
715         !
716     interface TenGigabitEthernet 1/47
717         description NorthBound Firewall X5
718         no ip address
719         switchport
720         no shutdown
721         !
722     interface TenGigabitEthernet 1/48
723         description IB-MGMT Switch Stack Port 49
724         no ip address
725         !
726         port-channel-protocol LACP
727         port-channel 64 mode active
728         no shutdown
729     interface fortyGigE 1/51
730         description VLTi
731         no ip address
732         no shutdown
733         !
734     interface fortyGigE 1/52
735         description VLTi
736         no ip address
737         no shutdown
738         !
739     interface fortyGigE 1/53
740         description to Spine Switch 4 Port 54
741         ip address 192.168.1.1/31
742         no shutdown
743         !
744     interface fortyGigE 1/54
745         description to Spine Switch 3 Port 54
746         ip address 192.168.2.1/31
747         no shutdown
```

```

748      !
749      interface Port-channel 64
750          description LAG to IB-MGMT Switches
751          no ip address
752          switchport
753          vlt-peer-lag port-channel 64
754          no shutdown
755      !
756      interface Port-channel 67
757          no ip address
758          mtu 9216
759          portmode hybrid
760          switchport
761          spanning-tree rstp edge-port bpduguard shutdown-on-violation
762          spanning-tree 0 portfast bpduguard shutdown-on-violation
763          lacp fast-switchover
764          vlt-peer-lag port-channel 67
765          no shutdown
766      !
767      interface Port-channel 68
768          no ip address
769          mtu 9216
770          portmode hybrid
771          switchport
772          spanning-tree rstp edge-port bpduguard shutdown-on-violation
773          spanning-tree 0 portfast bpduguard shutdown-on-violation
774          lacp fast-switchover
775          vlt-peer-lag port-channel 68
776          no shutdown
777      !
778      interface Port-channel 127
779          description VLTi
780          no ip address
781          channel-member fortyGigE 1/51,1/52
782          no shutdown
783      !
784      interface Port-channel 128
785          no ip address
786          shutdown
787      !
788
789      Honor 802.1p markings on incoming traffic and assign them to a default queue
790      service-class dynamic dot1p
791
792      Include overhead fields in rate-metering calculations
793      qos-rate-adjust 20

```

794 2.2.2 VLANs

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

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

```
799     interface Vlan 1
800     !untagged Port-channel 67-68,127
801     !
802     interface Vlan 101
803     ip address 192.168.101.3/24
804     untagged TenGigabitEthernet 1/47
805     !
806     vrrp-group 101
807     virtual-address 192.168.101.2
808     no shutdown
809     !
810     interface Vlan 103
811     no ip address
812     shutdown
813     !
814     interface Vlan 104
815     description nccoe-m01-vds01-managemnt
816     ip address 192.168.4.252/24
817     tagged TenGigabitEthernet 1/1-1/16,1/21
818     tagged Port-channel 64,127
819     !
820     vrrp-group 104
821     priority 254
822     virtual-address 192.168.4.254
823     no shutdown
824     !
825     interface Vlan 110
826     description nccoe-m01-vds01-nfs
827     ip address 192.168.10.252/24
828     tagged TenGigabitEthernet 1/1-1/16,1/21
829     tagged Port-channel 67-68,127
830     !
831     vrrp-group 110
832     priority 254
833     virtual-address 192.168.10.254
834     no shutdown
835     !
836     interface Vlan 120
837     description nccoe-m01-vds01-vmotion
838     ip address 192.168.20.252/24
839     tagged TenGigabitEthernet 1/1-1/8
840     tagged Port-channel 127
841     !
842     vrrp-group 120
843     priority 254
844     virtual-address 192.168.20.254
845     no shutdown
846     !
847     interface Vlan 130
```

```
848     description nccoe-m01-vds01-vsan
849     ip address 192.168.30.252/24
850     tagged TenGigabitEthernet 1/1-1/8
851     tagged Port-channel 127
852     !
853     vrrp-group 130
854         priority 254
855         virtual-address 192.168.30.254
856     no shutdown
857     !
858     interface Vlan 140
859         description nccoe-m01-vds01-replication
860         ip address 192.168.40.252/24
861         tagged TenGigabitEthernet 1/1-1/8
862         tagged Port-channel 127
863         !
864         vrrp-group 140
865             priority 254
866             virtual-address 192.168.40.254
867         no shutdown
868         !
869     interface Vlan 150
870         description VTEP VLAN
871         ip address 192.168.50.252/24
872         tagged TenGigabitEthernet 1/1-1/16
873         tagged Port-channel 127
874         !
875         vrrp-group 150
876             priority 254
877             virtual-address 192.168.50.254
878         no shutdown
879         !
880     interface Vlan 160
881         description nccoe-m01-vds01-uplink01
882         ip address 192.168.60.252/24
883         tagged TenGigabitEthernet 1/1-1/16
884         !
885         vrrp-group 160
886             priority 254
887             virtual-address 192.168.60.254
888         no shutdown
889         !
890     interface Vlan 180
891         description nccoe-m01-vds01-ext-management
892         no ip address
893         tagged TenGigabitEthernet 1/1-1/16
894         tagged Port-channel 127
895         no shutdown
896         !
897     interface Vlan 210
898         description nccoe-w01-vds01-nfs
899         ip address 192.168.210.252/24
```

```
900     tagged TenGigabitEthernet 1/1-1/16
901     tagged Port-channel 127
902     !
903     vrrp-group 210
904         priority 254
905         virtual-address 192.168.210.254
906     no shutdown
907     !
908     interface Vlan 220
909         description nccoe-w01-vds01-vmotion
910         ip address 192.168.220.252/24
911         tagged TenGigabitEthernet 1/9-1/16
912         tagged Port-channel 127
913     !
914     vrrp-group 220
915         priority 254
916         virtual-address 192.168.220.254
917     no shutdown
918     !
919     interface Vlan 230
920         description nccoe-w01-vds01-vsan
921         ip address 192.168.230.252/24
922         tagged TenGigabitEthernet 1/9-1/16
923         tagged Port-channel 127
924     !
925     vrrp-group 230
926         priority 254
927         virtual-address 192.168.230.254
928     no shutdown
929     !
930     interface Vlan 240
931         description VTEP VLAN
932         ip address 192.168.240.252/24
933         tagged TenGigabitEthernet 1/1-1/16
934         tagged Port-channel 127
935     !
936     vrrp-group 240
937         priority 254
938         virtual-address 192.168.240.254
939     no shutdown
940     !
941     interface Vlan 1000
942         description collapsed leaf edge bgp peering network
943         ip address 192.168.100.1/24
944     no shutdown
945     !
946     interface Vlan 1110
947         description nccoe-w01-vds01-uplink01
948         ip address 192.168.110.252/24
949         tagged TenGigabitEthernet 1/1-1/16
950     !
951     vrrp-group 111
```



```

952     priority 254
953     virtual-address 192.168.110.254
954     no shutdown
955     !

```

956 2.3 Dell PowerEdge Hardening

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

- 960 ■ BIOS boot option is disabled.
- 961 ■ Only UEFI-based OSES are supported for OS deployment in all management applications.
- 962 ■ Only authenticated EFI images and OS loaders are started from UEFI firmware.

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

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

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

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

976 2.4 Avamar Security Hardening

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

- 982 1. Disabling Samba (under “Level-1 security hardening”)
- 983 2. Preventing unauthorized access to GRUB configuration (under “Level-1 security hardening”)

- 984 3. Preventing the OS from loading USB storage (under “Level-1 security hardening”)
- 985 4. Updating OpenSSH (under “Level-3 security hardening”)
- 986 5. Disabling RPC (under “Level-3 security hardening”)
- 987 6. Configuring the firewall to block access to port 9443 (under “Level-3 security hardening”)
- 988 7. Changing file permissions (under “Level-3 security hardening”)

989 3 Gemalto Product Installation and Configuration Guide

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

992 3.1 Gemalto Luna 6 Initialization

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

- 997 1. Set the time zone to US Eastern:

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

- 999 2. Set the date/time format:

```
1000 syscont time HH:MM YYMMDD
```

- 1001 3. Set the hostname:

```
1002 net hostname TCHSM
```

- 1003 4. Set the Domain Name System (DNS) server:

```
1004 net dns add nameserver 172.16.1.11
```

- 1005 5. Set the network interface card (NIC) configuration for eth0 on the HSM:

```
1006 net interface -device eth0 -ip 172.16.1.22 -netmask 255.255.255.0 -gateway  
1007 172.16.1.254
```

1008 Perform the following steps to generate and use a new HSM server certificate:

- 1009 1. Generate the certificate:

```
1010 sysconf regenCert
```

- 1011 2. Bind the cert to eth0:

```
1012 ntlm bind eth0
```

1013 3. Verify the status of Network Trust Links (NTLS):

1014 `ntls show`

1015 The following commands initialize the HSM and set up policies for logging in and which algorithms it can
1016 use:

1017 1. Initialize the HSM and set the login timeout:

1018 `hsm PED timeout set -type -seconds 300`

1019 2. Next, log in as Security Officer:

1020 `hsm init -label NCCoE_Lab`

1021 3. Policy 12 controls non-FIPS compliant algorithms. Setting the value to zero disables any non-FIPS
1022 compliant algorithms:

1023 `hsm changePolicy -policy 12 -v 0`

1024 3.2 Create HSM Partition

1025 The following steps create the individual partition in the HSM that will be used for the HyTrust
1026 KeyControl cluster to use as its key management system (KMS):

1027 1. `hsm login`

1028 2. Create the HSM partition to be used for KeyControl:

1029 `partition create -partition HyTrust_KeyControl`

1030 3. Set the password for the newly created partition:

1031 `partition changePW -partition HyTrust_KeyControl -newpw <new password> -oldpw`
1032 `<old password>`

1033 4. Allow activation:

1034 `partition changePolicy -partition HyTrust_KeyControl -policy 22 -v 1`

1035 5. Allow auto-activation:

1036 `partition changePolicy -partition HyTrust_KeyControl -policy 23 -v 1`

1037 6. Activate the newly created partition:

1038 `partition activate -partition HyTrust_KeyControl`

1039 7. Show partition serial number for high availability:

1040 `partition show`

1041 4 HyTrust Product Installation and Configuration Guide

1042 This build implemented the HyTrust KeyControl, DataControl, CloudControl, and CloudAdvisor
1043 appliances. The following subsections show how the installation and configurations were performed, as
1044 well as how they were integrated with other components in the build.

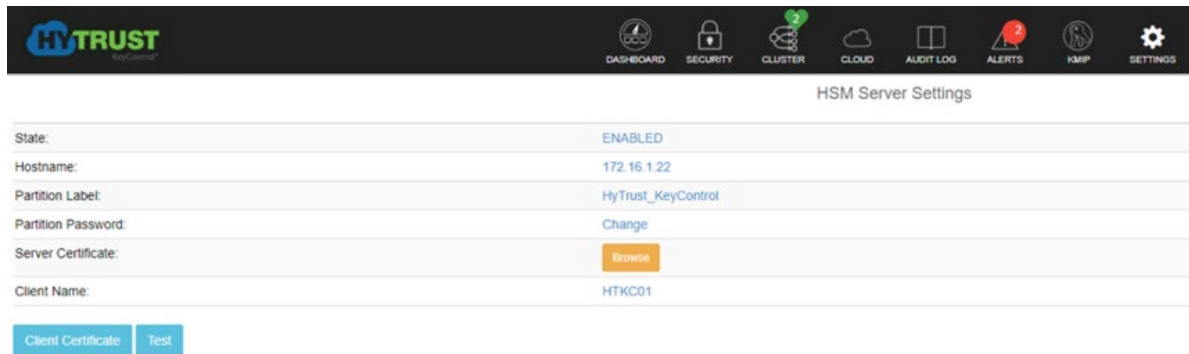
1045 4.1 HyTrust KeyControl Setup

1046 First, follow the directions on these pages:

- 1047 1. [Installing KeyControl from an OVA Template \(note: OVA stands for open virtual appliance\)](#)
- 1048 2. [Configuring the First KeyControl Node \(OVA Install\)](#)
- 1049 3. [Adding a New KeyControl Node to an Existing Cluster \(OVA Install\)](#)

1050 Next, in order to use the Gemalto Luna HSM as the KMS server to protect its keys, there must be
1051 connectivity between KeyControl and the HSM. To configure the HSM in KeyControls:

- 1052 1. Log in to the web user interface (UI) and click the **SETTINGS** button.
- 1053 2. Once in the **Settings** menu, click on the “**HSM Server Settings**” link to configure the HSM.
- 1054 3. Enter in the following information for the Gemalto Luna HSM:
 - 1055 • hostname or IP address
 - 1056 • partition label that was created in the Gemalto steps
 - 1057 • partition password
 - 1058 • server certificate file
 - 1059 • client name for this KeyControl server
- 1060 4. When the information is entered correctly, and the KeyControl server can communicate with
1061 and authenticate to the Gemalto HSM, the state will show as “**ENABLED**”.



1062 4.2 HyTrust DataControl Setup

1063 Follow the directions on these pages:

- 1064 1. [Creating a Cloud VM Set](#)
- 1065 2. [Installing Policy Agent on Windows](#)
- 1066 3. [Registering the Policy Agent Using the HyTrust Policy Agent GUI](#)
- 1067 4. [Encrypting a Disk Using the WebGUI](#)

1068 4.3 HyTrust CloudControl Appliance Setup

1069 Follow the directions on these pages:

- 1070 1. [Overview](#)
- 1071 2. [Installing from an OVA File](#)
- 1072 3. [Configuring the Management Interface](#)
- 1073 4. [Configuring the Management Console](#)
- 1074 5. Configuring High Availability
 - 1075 a. [HA Overview](#)
 - 1076 b. [High Availability Configuration Modes](#)
 - 1077 c. [High Availability Considerations and Limitations](#)
 - 1078 d. [High Availability Setup and Configuration](#)
 - 1079 e. [Default Configuration](#)

- 1080 6. Adding Hosts to CloudControl
- 1081 a. [Protected Hosts](#)
- 1082 b. [Adding a Host](#)
- 1083 7. [Configuring Managed Hosts](#)
- 1084 8. [Enabling a Good Known Host](#)
- 1085 9. [Verifying and Updating Host Trust](#) (and [Host Icons Used in CloudControl](#))

1086 For more information on PolicyTags provisioning and evaluation, see the “PolicyTags Provisioning”
 1087 section in chapter 6 of the [Administration Guide for HyTrust CloudControl](#).

1088 4.3.1 Provisioning PolicyTags

1089 To provision the PolicyTags, you need to perform the following tasks:

- 1090 1. Collect the UUID (Universally Unique Identifier) information for each Trusted host.
- 1091 2. Generate and run the `esxcli` commands for hardware provisioning for each Trusted host.
- 1092 3. Verify that the PolicyTags are provisioned.

1093 4.3.1.1 Collect UUIDs of Good Known Hosts (GKHs) and Trusted Hosts

1094 The UUID information for the GKHs and Trusted hosts can be collected from the vCenter Managed
 1095 Object Browser (MOB). You will need to obtain the UUID for each GKH and Trusted host.

- 1096 1. Log into the vCenter Managed Object Browser at `https://<VSPHERE_URL>/mob`.
- 1097 2. Perform the following series of page selections to reach the host page for each of your Intel TXT-
 1098 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)

- 1099 3. On the **Hosts** page, click **Summary**.
- 1100 4. On the **Summary** page, click **Hardware**. The **Hardware** page contains the UUID information.

1101 5. Repeat this for each Trusted host.

1102 4.3.1.2 *Generate esxcli Commands*

1103 Use the CloudControl cli to generate `esxcli` commands that can be used for hardware provisioning.

1104 1. Log into CloudControl as the `ascadminuser`, and run the following command:

1105 `asc tas --export-certs`

1106 This generates a file in `/tmp` in the following format: `export--xxxx-xx-xxx.tgz`

1107 2. Navigate to the `/tmp` folder and extract the file using the following command:

1108 `tar -xvf export--xxxx-xx-xxx.tgz`

1109 The extraction process lists several files, including the `sha1.bin` for each Trusted ESXi host.

1110 Example:

1111 `export--2018-08-27T23-44-43Z/6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-`
1112 `dc27fe259e1a/system--6aa6af76-14f6-42e8-b452-dc27fe259e1a.der`

1113 `export--2018-08-27T23-44-43Z/6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-`
1114 `dc27fe259e1a/system--6aa6af76-14f6-42e8-b452-dc27fe259e1a.sha1.bin`

1115 `export--2018-08-27T23-44-43Z/6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-`
1116 `dc27fe259e1a/system--6aa6af76-14f6-42e8-b452-dc27fe259e1a.sha256.bin`

1117 `export--2018-08-27T23-44-43Z/6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-`
1118 `dc27fe259e1a/system--6aa6af76-14f6-42e8-b452-dc27fe259e1a.metadata.txt`

1119 `export--2018-08-27T23-44-43Z/dddafa66/314e/4378/8f4d/dddafa66-314e-4378-8f4d-`
1120 `060b5d885038/system--dddafa66-314e-4378-8f4d-060b5d885038.der`

1121 `export--2018-08-27T23-44-43Z/dddafa66/314e/4378/8f4d/dddafa66-314e-4378-8f4d-`
1122 `060b5d885038/system--dddafa66-314e-4378-8f4d-060b5d885038.sha1.bin`

1123 `export--2018-08-27T23-44-43Z/dddafa66/314e/4378/8f4d/dddafa66-314e-4378-8f4d-`
1124 `060b5d885038/system--dddafa66-314e-4378-8f4d-060b5d885038.sha256.bin`

1125 `export--2018-08-27T23-44-43Z/dddafa66/314e/4378/8f4d/dddafa66-314e-4378-8f4d-`
1126 `060b5d885038/system--dddafa66-314e-4378-8f4d-060b5d885038.metadata.txt`

1127 3. Navigate to the extracted directory, for example:

1128 `cd /tmp/export--xxxx-xx-xxx`

1129 4. At the prompt, type the following command:

1130 `grep -E -- '(id|subject)' : ' json.dump | grep -A1 '<Trusted-Host-UUID> '`

1131 This command returns the “subject” and the “id.” Example:

1132 `"subject" : "4c4c4544-0032-3010-8035-b5c04f333832",`

1133 `"id" : "6aa6af76-14f6-42e8-b452-dc27fe259e1a"`

1134 5. Run the following `hexdump` command for each Trusted host, where `<sha1.bin file path>` matches
1135 the “id” for the specific host:

1136 `hexdump -e '"esxcli hardware tpm tag set --data=" 20/1 "%1.2x" ";\n"' <sha1.bin`
 1137 `file path>`

1138 This returns the `esxcli` command.

1139 Example:

1140 `hexdump -e '"esxcli hardware tpm tag set --data=" 20/1 "%1.2x" ";\n"'`
 1141 `6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-dc27fe259e1a/system--6aa6af76-`
 1142 `14f6-42e8-b452-dc27fe259e1a.sha1.bin`

1143 `esxcli hardware tpm tag set --data=46f048ce41afdfa686e4c00f9fd67a2b71d1c749;`

1144 [4.3.1.3 Run esxcli Commands](#)

1145 Run the `esxcli` commands for each Trusted host to provision the hardware tags.

- 1146 1. Put the Trusted host into maintenance mode.
- 1147 2. Log in to the ESXi host as `root`.
- 1148 3. Run the specific `esxcli` command for the Trusted host. The command is part of the `hexdump`
 1149 output.

1150 Example:

1151 `esxcli hardware tpm tag set --data=46f048ce41afdfa686e4c00f9fd67a2b71d1c749;`

- 1152 4. Restart the ESXi host. The host should still be in maintenance mode.

1153 [4.3.2 Policy Interaction](#)

1154 See the [Policy Interaction webpage](#) for more information on how policy enforcement works.

1155 [4.4 HyTrust CloudAdvisor Appliance Setup](#)

1156 Follow the directions on these pages:

- 1157 1. [Deploying CloudAdvisor](#)
- 1158 2. [Configuring the CloudAdvisor Virtual Appliance](#)
- 1159 3. [Setting Up CloudAdvisor](#)
- 1160 4. [Adding VMs to Inventory](#)

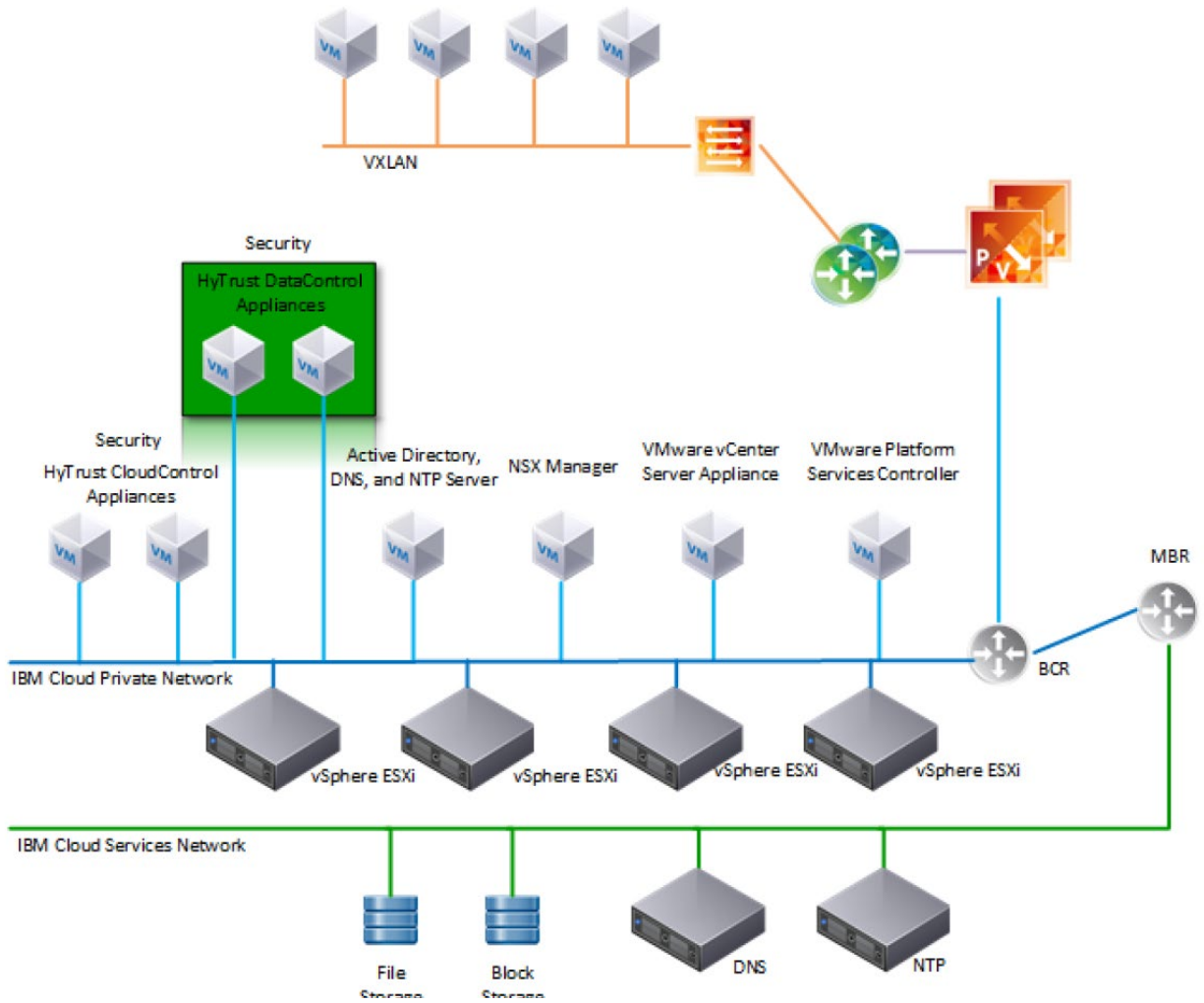
1161 [5 IBM Product Installation and Configuration Guide](#)

1162 This section covers all the aspects of installing and configuring the IBM products used to build the
 1163 example solution. Note that the information in this section reflects product and service names, features,
 1164 options, and configurations as of when the build was performed. The IBM products in this section are

1165 cloud-based with web-based documentation, and they do not use versioning conventions, so it is not
1166 possible to reference the documentation that was used during this build. As of this writing, the latest
1167 information from IBM is available through the IBM Cloud for VMware Solutions site at
1168 <https://www.ibm.com/cloud/vmware>.

1169 **5.1 ICSV Deployment**

1170 IBM Cloud Secure Virtualization (ICSV) combines the power of IBM Cloud, VMware Cloud Foundation,
1171 HyTrust security software, and Intel TXT-enabled hardware to protect virtualized workloads. ICSV is
1172 deployed on the IBM Cloud infrastructure according to a VMware, HyTrust, IBM, and Intel-validated
1173 design reference architecture. IBM Cloud Secure Virtualization is initially deployed as a four-node cluster
1174 within the choice of clients of available IBM Cloud Data Centers worldwide. Below is a reference
1175 architecture for ICSV that shows the separation between IBM Cloud services, ICSV provisioned
1176 infrastructure, and tenant VMs. ICSV utilizes the IBM Cloud Services Network to enable provisioning the
1177 IBM Cloud Private Network to a customer, which in turn protects the virtualized workloads.



1178 To deploy the ICSV reference architecture stack, IBM has streamlined the process in three phases for the
 1179 customer.

1180 5.1.1 Pre-deployment

1181 This phase starts after the customer has agreed to purchase the ICSV stack in the IBM cloud and has
 1182 identified the use cases using a workshop or IBM Garage methodology. For the NCCoE project, we had a
 1183 good understanding of the use case and the capabilities provided by ICSV. To achieve success in all three
 1184 phases, the IBM Services team filled out [Table 5-1](#) and [Table 5-2](#). The information provided in each table
 1185 helped us with decisions in later steps.

1186 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)			

1187 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

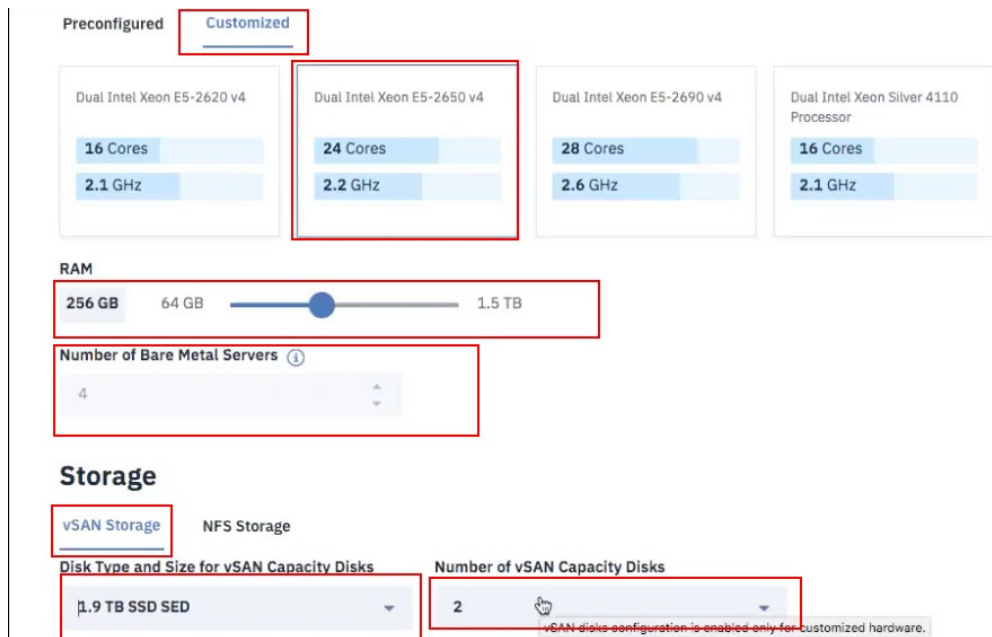
Client Input Variables	Choices	Example Values
Intel core base	2.1, 2.2, 2.3 GHz	2.2 GHz
RAM	64 GB-1.5 TB	256 GB
Data center location	Dallas, DC, Boulder, etc.	Dallas
Data storage	NFS or VSAN	VSAN
Size of each data storage	1, 2, 4, 8, 12 TB	2 TB
Performance of file shares	2, 4, 10 IOPS/GB	NA
NFS version - 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

1188 5.1.2 Automation deployment

1189 The following are steps for ordering an ICSV instance through the IBM portal.

- 1190 1. Log into the IBM Cloud infrastructure customer portal at <https://console.ng.bluemix.net/cata->
- 1191 [log/](https://console.ng.bluemix.net/cata-log/).

- 1192 2. From the top left corner, select the “Hamburger” menu, then select **VMware** from the drop-
1193 down menu on the left side.
- 1194 3. Click on **Settings** and make sure the correct application programming interface (API) key is en-
1195 tered before provisioning the solution.
- 1196 4. On the **IBM Cloud for VMware Solutions** screen, select **VMware vCenter Server on IBM Cloud**.
- 1197 5. On the next screen, select **vCenter Server** and click the **Create** button.
- 1198 6. In the next window, type in the **Instance Name** and make sure **Primary Instance** is highlighted
1199 for Instance type. For the **Licensing** options, select **Include with purchase** for all of them. For the
1200 **NSX License**, select **Enterprise** from the drop-down menu.
- 1201 7. Under **Bare Metal Server**:
- 1202 a. For the **Data Center Location**, open the drop-down menu for **NA South** and select
1203 **DAL09**.
- 1204 b. Select **Customized** since our workload needs a virtual storage area network (VSAN),
1205 which requires a minimum of a four-node cluster.
- 1206 8. Under **Storage**:
- 1207 a. Select **vSan Storage**.
- 1208 b. Set the **Disk Type and Size** for vSAN Capacity Disks to **1.9 TB SSD SED**.
- 1209 c. Select **2** from the drop-down menu for the **Number of vSAN Capacity Disks**.
- 1210 d. For **vSAN License**, select **Include with purchase** and then choose **Enterprise** from the
1211 drop-down menu.



- 1212 9. For the **Network Interface**, enter the following:
- 1213 a. Hostname Prefix: `esxi`
- 1214 b. Subdomain Label: `icsv`
- 1215 c. Domain Name: `nccoe.lab`
- 1216 10. Select **Order New VLANs**.
- 1217 11. Under **DNS Configuration**, select **Two highly available dedicated Windows Server VMs on the**
- 1218 **management cluster**.
- 1219 12. Under Services, remove **Veem on IBM Cloud 9.5** and select **HyTrust CloudControl on IBM**
- 1220 **Cloud 5.3** and **HyTrust DataControl on IBM Cloud 4.1**.
- 1221 13. Click on the **Provision** button in the bottom right-hand corner. This will begin the provisioning
- 1222 process for the selected topology. It can take roughly 24 hours to complete the automation de-
- 1223 ployment. Once deployment has completed, you should receive an email notification.

1224 5.1.3 Post-deployment

1225 This information is needed to set up HyTrust CloudControl (HTCC) to interact with Windows AD and

1226 vCenter. The IBM Service team will set up HTCC so it is ready for HyTrust configuration based on the use

1227 cases required by the client. Table 5-3 shows examples of HTCC configuration parameters.

1228 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)
Windows AD Groups and Users		
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
H/W Policy tags		
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	

1229 The IBM services team gathers information from the client, such as the examples in Table 5-4, after
1230 understanding the use cases. The information will be used to configure HyTrust, VMware, and Intel
1231 TPM/TXT to enforce workload rules and policy. Once post-deployment is completed, the IBM services
1232 team will perform a verification test and deliver the asset to the client.

1233 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		
Users		
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
Groups		
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
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

1234 5.2 Enable Hardware Root of Trust on ICSV Servers

1235 In order to leverage the ICSV instance for hardware roots of trust, steps must be taken to enable these
 1236 features within the server BIOS, as well as ensuring features in the VMware products are enabled to
 1237 access and leverage these measurements.

1238 5.2.1 Enable Managed Object Browser (MOB) for each ESXi Server

- 1239 1. Open the vSphere Client and navigate to the relevant host.
- 1240 2. Click on the **Configure** tab.
- 1241 3. On the left-hand side under **Software**, click on **System**, then **Advanced System Settings**.
- 1242 4. Click on the **Edit** button.
- 1243 5. Modify or add the configuration to enable MOB: **Config.HostAgent.plugins.solo.enableMob** (set
 1244 value to **True**).
- 1245 6. To confirm that MOB has been enabled on the host, open *http://x.x.x.x/mob*, where x.x.x.x is
 1246 the IP address of the ESX Server.

1247 5.2.2 Enable TPM/TXT on SuperMicro hosts

- 1248 1. From the vCenter console, enter the ESX host(s) in maintenance mode.
- 1249 2. Log into your IBM Cloud console and open a support ticket. In the ticket, specify the following:
 - 1250 a. ESX host(s) you want them to work on. You can have support work on multiple hosts as
 1251 long as you have the minimum running as required by your instance—minimum of three
 1252 hosts for instances that have VSAN, otherwise two hosts.
 - 1253 b. Enter ticket description as follows:

1254 < Start of ticket description >

1255 *We need your assistance to enable TPM/TXT in the BIOS for this IBM Cloud Secure*
 1256 *Virtualization (ICSV) instance.*

1257 *Please enable the TPM/TXT flags in the BIOS, following the steps in the exact order*
 1258 *specified:*

 - 1259 1. *Reboot the following host(s) specified below and enter into BIOS – <provide the list*
 1260 *of hosts again here for clarity.>*

- 1261 2. Go to Advanced 'Trusted Computing'. *If TPM cannot be cleared in the **Pending***
 1262 ***Operations** option, then reboot to BIOS and **enable TPM only**. You will need this to*
 1263 *clear TPM in the next reboot. **Press F4 to save and exit**.*
 1264 3. *On reboot, again go to BIOS and go to Advanced 'Trusted Computing'. **Clear TXT**.*
 1265 *This will clear TPM and TXT. **Press F4 to save and exit**.*
 1266 4. *On reboot go to BIOS and **enable TPM only**. **Press F4 to save and exit**. **Do not***
 1267 ***enable TPM and TXT in the same reboot. They have to be enabled in sequence**.*
 1268 5. *On reboot, again go to BIOS and now **enable TXT**. The TPM should have been*
 1269 *enabled from last step. **Press F4 to save and exit**.*
 1270 6. *Let the reboot continue to boot to ESX.*

1271 *Please let me know when you have done this successfully.*

1272 < End of ticket description >

1273 c. Once the support person returns the ticket with the task completed, continue with the
 1274 tasks below.

1275 3. From the vCenter console, exit maintenance mode. You may need to connect the ESX hosts
 1276 again if the host got disconnected.

1277 4. From the vSphere web client or vSphere client, disconnect the host and then connect the host
 1278 back. This is needed to have the ESXi host re-read the TPM settings.

1279 5. Check the vCenter MOB to check if TPM/TXT is enabled.

1280 At a minimum, there must be three hosts up in instances that have VSAN. So make sure you only work
 1281 on hosts that will ensure this requirement is met. Ideally, work on one host at a time.

1282 5.2.3 Enable TPM/TXT in IBM Cloud

1283 1. Through vCenter, place the ESXi host in maintenance mode.

1284 2. Reboot the ESXi server by pressing the **F12** key in the iKVM viewer.

1285 3. Once the server reboots, access the BIOS. Disable the **TPM Provision Support**, the **TXT Support**,
 1286 and the **TPM State**, then **Save & Exit**.

1287 4. Reboot the server all the way to the ESXi OS level.

1288 5. Reboot the server again using the **F12** key.

1289 6. Make sure the OS is not loaded, and access the BIOS. Set the **TPM State** to **Enabled**, then **Save &**
 1290 **Exit**.

- 1291 7. Let the system boot up, but access the BIOS before the OS is loaded. If the system boots the OS,
- 1292 you will have to do the above steps again.
- 1293 8. Enable **TXT Support** in the BIOS, then **Save & Exit**.
- 1294 9. Boot the server to OS hypervisor level.

5.2.4 Validate the TPM/TXT is enabled

- 1296 1. SSH into the ESX host as `root` and run the following command:

```
1297 zcat /var/log/boot.gz | grep -I tpm
```

1298 This should show if the TPM library was loaded.

- 1299 2. Other commands to check are:

```
1300 vmkload_mod -l | grep tpm
```

```
1301 grep -i tpm /var/log/hostd.log | less -S
```

- 1302 3. As a root user, run the following command:

```
1303 esxcli hardware trustedboot get
```

1304 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

- 1306 1. Open a browser with `https://<vCenter-console-IP address>/mob` to bring the vCenter MOB (do
- 1307 not use the individual ESXi host MOB). Authenticate using the vCenter credential.
- 1308 2. Click on different resources of the MOB in the steps shown below:
- 1309 a. Click on **content**.
- 1310 b. Search for **group-d1 (Datacenters)** and click on it.

licenseManager	ManagedObjectReference:LicenseManager	LicenseManager
localizationManager	ManagedObjectReference:LocalizationManager	LocalizationManager
overheadMemoryManager	ManagedObjectReference:OverheadMemoryManager	OverheadMemoryManger
ovfManager	ManagedObjectReference:OvfManager	OvfManager
perfManager	ManagedObjectReference:PerformanceManager	PerfMgr
propertyCollector	ManagedObjectReference:PropertyCollector	propertyCollector
rootFolder	ManagedObjectReference:Folder	group-d1 (Datacenters)
scheduledTaskManager	ManagedObjectReference:ScheduledTaskManager	ScheduledTaskManager

- 1311 c. Find **datacenter-2 (SDDC-Datacenter)** and click on it.

- 1312 d. Search for **group-h4 (host)** and click on it.
- 1313 e. Search for **domain-c7 (SDDC-Cluster)** and click on it.
- 1314 f. Search for **host**, and you will see all the hosts listed with their host names.

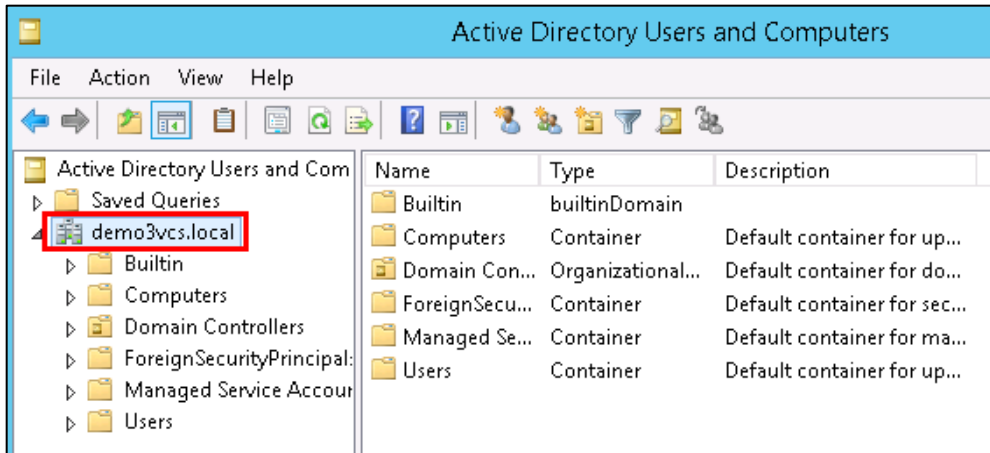
host	ManagedObjectReference:HostSystem[]	host-29 (host2.securek8s.ibm.local)  host-34 (host3.securek8s.ibm.local)  host-35 (host0.securek8s.ibm.local)  host-36 (host1.securek8s.ibm.local) 
------	-------------------------------------	--

- 1315 g. Click on the host that you need to validate. In our demo, we are checking **host1.se-**
- 1316 **ecurek8s.ibm.local**.
- 1317 h. Search for method **QueryTpmAttestationReport** and click on it to invoke the method.
- 1318 i. Click on **Invoke Method**.

1319 5.2.6 Set up Active Directory users and groups

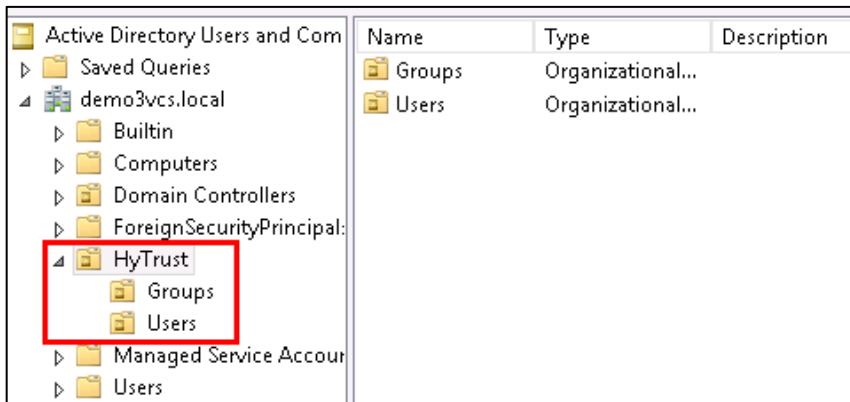
1320 In this part of the setup, you will create several new organizational units. Remember that this procedure
 1321 uses a Windows 2012 server and Microsoft AD to illustrate the steps. Your environment and your
 1322 specific steps might be different. This section assumes actions are being performed from the ICSV
 1323 Microsoft AD server. Alternatively, you can follow these steps to set up AD. Note that the values in the
 1324 screen shots will be different than your values.

- 1325 1. In Windows Server, start the Server Manager, if not already started.
- 1326 2. From the **Server Manager** window, select **Tools -> Active Directory Users and Computers**.
- 1327 3. Right-click on your domain that has been created based on the instance name you provided by
 1328 Windows AD deployment (for VCS) or during VCF deployment creation. For our demo, it is
 1329 **demo3VCS.local**. Select **New -> Organizational Unit**. You should create the new **OU**.



1330 4. Enter **HyTrust** as the name of the new unit. Right-click on the **HyTrust** organizational unit, select
 1331 **New -> Organizational Unit**, and give the name of **Groups**.

1332 5. Right-click again on the **HyTrust** organizational unit, select **New -> Organizational Unit**, and give
 1333 the name of **Users**. This group will be used to allow a user to communicate between HTCC and
 1334 AD. The directory hierarchy should now look similar to this:



1335 6. Add two users to the **Users** group. To do this, right-click on the **HyTrust/Users** organizational
 1336 unit and select **New -> User**.

1337 7. The first user is the primary user account that will be used to communicate between HTCC and
 1338 AD. In the pop-up screen for users, enter user information as appropriate. The screen might look
 1339 like this:

1340 Full name: **HyTrust LDAP Lookup**

1341 User logon name: **ht_ldap_svc**

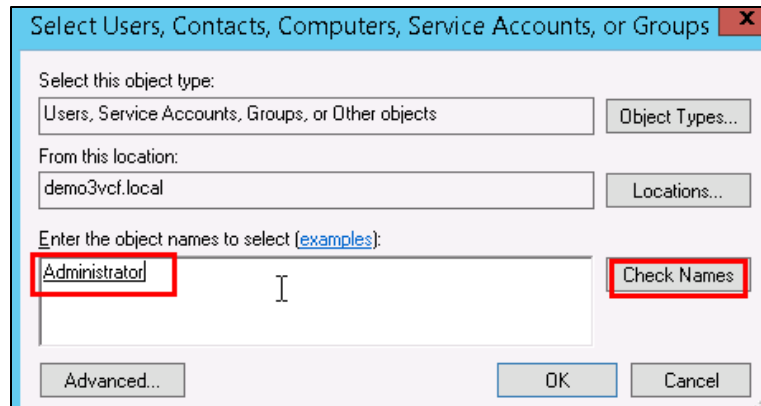
The screenshot shows the 'New Object - User' dialog box. The 'Create in' path is 'demo3vcs.local/HyTrust/Users'. The 'Full name' field is filled with 'HyTrust LDAP Lookup'. The 'User logon name' field is filled with 'ht_ldap_svc'. The domain dropdown is set to '@demo3vcs.local'. The 'User logon name (pre-Windows 2000)' field is filled with 'demo3vcs\' and 'ht_ldap_svc'. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom.

- 1342 8. Click **Next** to go to the user password screen. It asks you to establish a password and some pass-
 1343 word options for the user. Enter or verify these fields:
- 1344 a. Enter and confirm a password for the user. The password needs to have at least one up-
 1345 per case letter, otherwise the user will not be created. Note the password in the deploy-
 1346 ment spreadsheet.
- 1347 b. Uncheck this option: **User must change password at next logon.**
- 1348 c. Check this option: **Password never expires.**
- 1349 d. Click **Next.**
- 1350 e. Verify the information and finish.
- 1351 9. The second user will be used as the service account when HTCC interacts with vCenter. You
 1352 could use the **Administrator@vsphere.local** account, but best practice is to create a specific ser-
 1353 vice account in AD and use that. Create the second user (in the same way as the first user) with
 1354 the following values:
- 1355 Full name: **HyTrust VCenter svc account**
- 1356 User logon name: **ht_vcenter_svc**
- 1357 Ensure that the password never expires.
- 1358 10. You will now create two subgroups under **Groups.**

- 1359 a. First, right-click on the **Groups** organizational unit and select **New -> Group**.
- 1360 b. When prompted, enter a name for the new group: **bcadmins**. Later, you will tell HTDC to
- 1361 use this group when communicating with HTCC to verify boundary checks. Keep the rest
- 1362 of the options (Group scope and type) the default values as shown below. Press **OK** to
- 1363 create the group.

The screenshot shows a dialog box titled "New Object - Group". At the top, it says "Create in: demo3vcs.local/HyTrust/Groups". Below that, there are two text input fields. The first is labeled "Group name:" and contains the text "bcadmins", which is enclosed in a red rectangular box. The second is labeled "Group name (pre-Windows 2000):" and also contains "bcadmins". Below these fields are two sections of radio buttons. The "Group scope" section has three options: "Domain local" (unselected), "Global" (selected), and "Universal" (unselected). The "Group type" section has two options: "Security" (selected) and "Distribution" (unselected).

- 1364 c. Right-click again on the **Groups** organizational unit and select **New -> Group**.
- 1365 d. When prompted, enter a name for this group: **ht_superuser_admin_users** and press **OK**.
- 1366 Later, you will tell HTCC to use this group to specify administrative users of HTCC.
- 1367 11. You will now add members to the **superadmin** group.
- 1368 a. To do this, right-click on the **ht_superuser_admin_users** group, and select **Properties**.
- 1369 b. In the pop-up window, select the **Members** tab, then click **Add**.
- 1370 c. In the next pop-up screen, enter an object name **Administrator**, and click on **Check**
- 1371 **Names**. If no error is returned, click **OK**.



1372 12. Close the AD control panel.

1373 You are now ready to set up HTCC authentication to work with AD, as described in the next procedure.

1374 5.2.7 Join vCenter to the AD domain

1375 We need to integrate the AD domain into vCenter so that we can later give the AD HyTrust service
 1376 account vCenter permissions. You first have to join the vCenter to the AD domain, and then add the AD
 1377 user to vCenter. Note that this is already done for VCS and VCF. However, you may want to check using
 1378 the instructions below.

1379 1. To check if vCenter is already joined to the AD domain, SSH into PSC.

1380 2. Run the following command:

1381 `/opt/likewise/bin/domainjoin-cli query`

1382 If the output indicates it's already joined, you can skip the rest of this section (5.2.7).

1383 3. If it's not already joined, run the following command to join it:

1384 `/opt/likewise/bin/domainjoin-cli join <domain-name> <AD Administrator user>`
 1385 `<password>`

1386 Example:

1387 `/opt/likewise/bin/domainjoin-cli join demo3vcs.local Administrator Passw0rd`

1388 Output:

1389 `Joining to AD Domain: demo3vcs.local`
 1390 `With Computer DNS Name: psc.demo3vcs.local`
 1391 `SUCCESS`

1392 Then reboot.

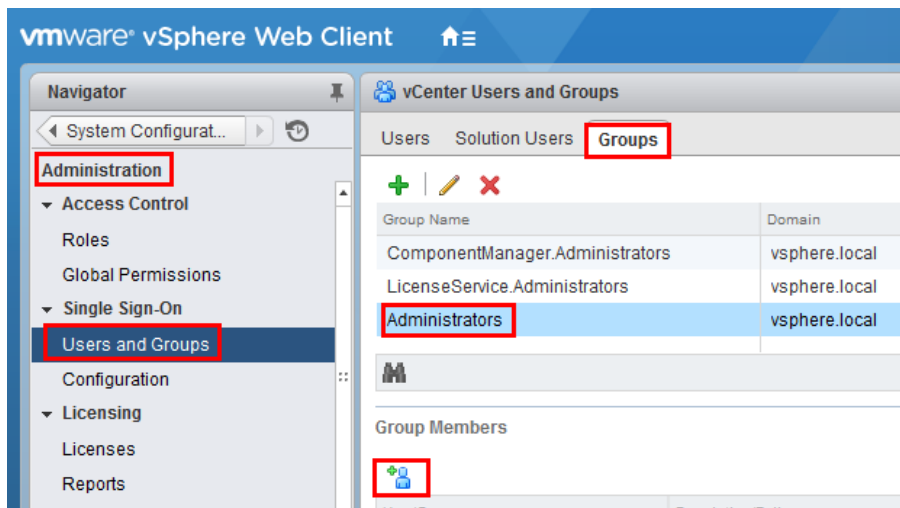
1393 4. SSH into PSC again and verify that the join has succeeded by issuing the following command:

1394 `/opt/likewise/bin/domainjoin-cli query`

1395 5.2.8 Add AD HyTrust-vCenter service user to vCenter as Administrator

1396 This is for both the VCS and VCF instances.

- 1397 1. In the vSphere Web Client, go to **Administration** and then **Users and Groups**. Click on **Groups**,
1398 then **Administrators**, and select the Group Members **Add** icon.



- 1399 2. In the **Add Principals** panel, select the Windows AD Domain (**demo.local** in our example), scroll
1400 down and select the user **ht_vcenter_svc** user (that was created in Windows AD), and click on
1401 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
ht_vcenter_svc	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:

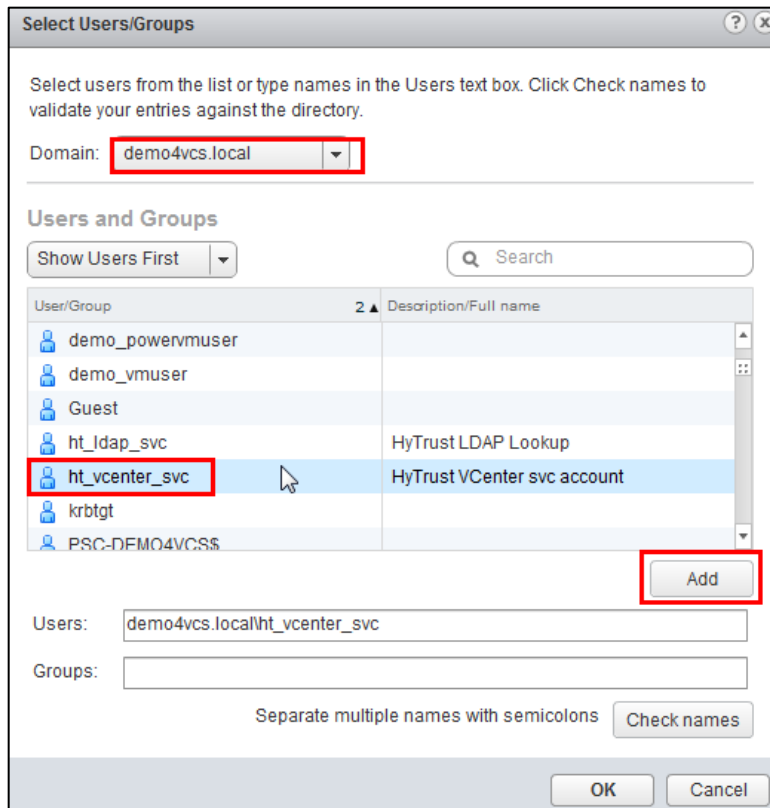
Separate multiple names with semicolons Check names

OK Cancel

1402 You have successfully added the Windows AD HyTrust vCenter LDAP id as part of the Administrator
 1403 group. This id will be used for all interaction between HTCC and vCenter, when the vCenter is added to
 1404 HTCC.

1405 5.2.9 Add AD HyTrust-vCenter service user to vCenter Global Permissions

- 1406 1. Go to the vCenter web client. Under **Administration**, click on **Global Permissions**.
- 1407 2. Add the AD user for the HyTrust-vCenter service, **ht_vcenter_svc**, and give it Administration per-
 1408 mission.



1409 5.2.10 Configure HTCC for AD authentication

1410 HTCC requires a directory services solution. In this deployment solution, HTCC authentication will be set
 1411 up to work with Microsoft AD. Before you configure HTCC to use AD, you must define two groups and
 1412 one user. You can do this via existing AD entries or create entries just for HTCC (as is the case in our
 1413 implementation).

1414 By default, HTCC is set to use a demo userid/password authentication. Once you change to AD
 1415 authentication, you cannot revert back to the demo authentication.

1416 If AD is configured with TLS, the AD server's certificate must be imported into HTCC. To configure HTCC
 1417 with an AD server with TLS configuration, refer to the [HTCC Administration Guide](#) for the following
 1418 steps:

- 1419 1. To import AD Server certificate into HTCC, refer to the HTCC Administration Guide section titled
 1420 "Installing a Third-Party Root Certificate."
- 1421 2. Configure AD with TLS in HTCC. Refer to the HTCC Administration Guide section titled "Integrat-
 1422 ing the Appliance with Active Directory."

1423 To set up HTCC authentication, follow these steps:

- 1424 1. Log onto the HTCC web console, using URL *https://<HTCC-Virtual-IP>/asc* with the default
1425 username of `superadminuser` and the password `Pa$$w0rd123!`
- 1426 2. From the HTCC dashboard, select the **Configuration** menu, and then **Authentication**.
- 1427 3. Change the **Authentication Server Type** to **Directory Service** and accept your changes.
- 1428 4. You should see a screen for configuring the service account. Make sure that the default domain
1429 name is the one you used to deploy the instance. In our demo, it's **demo3vcf.local**. In the ser-
1430 vice account name field, enter the username (**ht_ldap_svc**) and password that you used during
1431 the AD setup steps.
- 1432 5. Click **Next**, and you will see the domain listed. Click **Next** again.
- 1433 6. You should now see the **Role-Group Mapping** page. Look under the **ASC_SuperAdmin** section
1434 entry. Confirm that your AD domain is listed in the selected pull-down entry. In the group name
1435 field, enter the admin group name, **ht_superadmin_users**, that you created earlier in the initial
1436 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
ASC_ThirdParty	demo3vcf	ht_super_admins

- 1437 7. Click **Next** and review the summary. If it is correct, finish. If AD is working correctly, the web in-
1438 terface will automatically log you out.
- 1439 8. Log back in using the **Administrator** user and password of your Windows AD/DNS Server (which
1440 is the domain controller). Recall that we had added **Administrator** to the **ht_superadmin_users**
1441 group in Windows AD.

1442 At this point, AD should be correctly set up for deployment. You are ready to set up the trust attestation
1443 service.

1444 5.3 Add Hosts to HTCC and Enable Good Known Host (GKH)

1445 You will add hosts in vCenter and then enable the Good Known Host (GKH) values to make them
1446 Trusted.

1447 First, since all the hosts are managed by vCenter (as compared to standalone ESX hosts), you will add
1448 vCenter as the host—that will automatically detect the NSX server and the ESX hosts, and add them to
1449 HTCC. The high-level steps are:

- 1450 1. In HTCC, add vCenter as the host. For vCenter, use the same AD LDAP used for the HTCC vCenter
1451 AD id, **ht_vcenter_svc@ibm.local** (change the domain name based on what you have). While
1452 you can use **Administrator@vsphere.local**, best practice suggests you use the AD id.
- 1453 2. For all the ESX hosts that are detected, add their user ids/passwords and **Publish IPs**.
- 1454 3. If the vCenter and ESX host patch levels are not one of the valid patches supported by HTCC, add
1455 the patch level to HTCC so it recognizes them as valid hosts.

1456 Next, follow the directions at [Enabling a Good Known Host](#), then [Verifying and Updating Host Trust](#).

1457 Finally, to define, assign, and provision PolicyTags, follow these steps:

- 1458 1. [Define PolicyTags in CloudControl](#).
- 1459 2. Assign PolicyTags to hosts. Important: We recommend that you put your host in maintenance
1460 mode before assigning PolicyTags, especially if you are modifying existing PolicyTag assignments
1461 which may be in use by your existing compliance rules. Do not remove the host from mainte-
1462 nance mode until you have verified that the new PolicyTag assignment has been correctly provi-
1463 sioned.
 - 1464 a. Select **Compliance > Hosts**.
 - 1465 b. On the **Hosts** page, check the checkbox for the Intel TXT-enabled host and click **Edit**.
 - 1466 c. On the **Edit Hosts** page, select the **PolicyTag** tab.
 - 1467 d. Select the appropriate **PolicyTag** value for one or more of the fields listed in Section 1.
 - 1468 e. Click **OK**.
 - 1469 f. CloudControl displays a JGrowl error message that prompts users to PXE boot the
1470 host(s) to activate the PolicyTag assignment.
- 1471 3. Follow all of the PolicyTags provisioning directions in Section [4.3.1](#).
- 1472 4. Verify the provisioning using these steps:
 - 1473 a. Open CloudControl and select **Compliance > Hosts**.
 - 1474 b. Select the host that you just updated and click **Update Trust**.
 - 1475 c. Select **Policy > Resources**.

- 1476 d. Verify that the PolicyTags have been provisioned. If the tag icon next to the host being
1477 provisioned is blue, then the PolicyTags assigned to the host are provisioned. If the tag
1478 icon is yellow, then the PolicyTags assigned to the host are not provisioned.
- 1479 e. Note: If the provisioning process was not successful, you may have to clear the TPM
1480 once again and repeat the process.
- 1481 f. After the PolicyTag provisioning is successful, you can remove the hosts from mainte-
1482 nance mode.

1483 6 Intel Product Installation and Configuration Guide

1484 Intel TXT provides hardware-based security technologies that address the increasing and evolving
1485 security threats across physical and virtual infrastructures by complementing runtime protections. Intel
1486 TXT increases protection by allowing greater control of the launch stack through a Measured Launch
1487 Environment (MLE) and enabling isolation in the boot process. More specifically, it extends the Virtual
1488 Machine Extensions (VMX) environment of Intel Virtualization Technology (Intel VT), permitting a
1489 verifiably secure installation, launch, and use of a hypervisor or OS. These measured values in the boot
1490 process are extended to and stored in a TPM on the server.

1491 To enable Intel TXT and the necessary TPM in server BIOS, follow the steps in Section 5.2.3. The steps in
1492 Section 5.2.4 can be followed to verify that that each Dell ESXi host has successfully enabled the TPM
1493 and Intel TXT. The steps in Section 5.2.5 can be followed to verify that the Dell ESXi hosts' TPM values
1494 are successfully read by the vCenter Server.

1495 7 RSA Product Installation and Configuration Guide

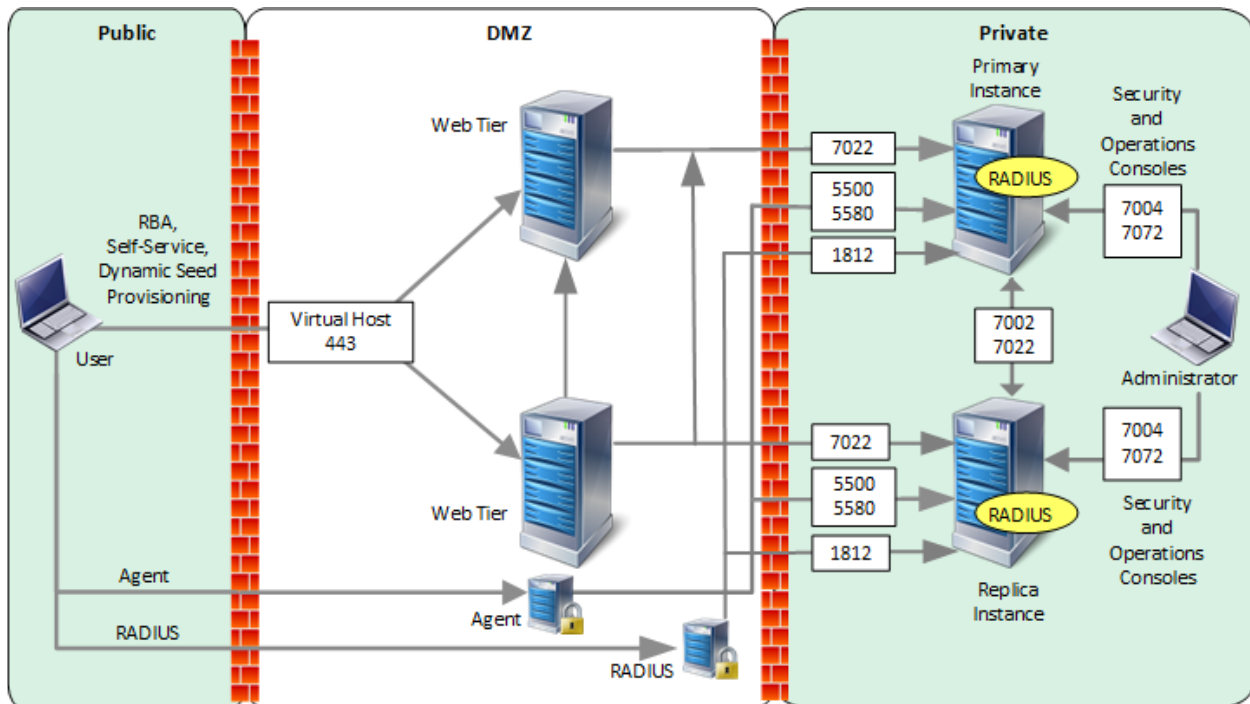
1496 This section covers the installation and configuration of the RSA products used to build the example
1497 solution.

1498 7.1 RSA SecurID

1499 RSA Authentication Manager is the authentication, administration, and database management
1500 component of RSA SecurID, which provides strong authentication of users accessing valuable network
1501 resources. Refer to [RSA Authentication Manager 8.4 VMware Virtual Appliance Getting Started](#) for
1502 installation instructions. Another source of information is [Getting Started with RSA Authentication
1503 Manager](#).

1504 Figure 7-1 represents a common RSA Authentication Manager deployment with primary and replica
1505 instances, web tiers, and a load balancer. An external firewall protects the primary and replica instances,
1506 and another external firewall protects the DMZ.

1507 Figure 7-1: RSA Authentication Manager Deployment Architecture

1508

7.2 RSA NetWitness

1509 To install and configure virtual hosts for RSA NetWitness Platform 11.4, follow the instructions in the
 1510 [Virtual Host Installation Guide](#). Start by reading the “Basic Virtual Deployment” section, then reading
 1511 and following the steps in the “Install NetWitness Platform Virtual Host in Virtual Environment” section
 1512 (except you can skip Step 1b).

1513 The rest of this section explains how to configure NetWitness for VMware log collection from an ESX
 1514 host.

1515

7.2.1 Configure the VMware ESX/ESXi Event Source

1516 This section describes how to create a least privilege User to extract logs from an ESX/ESXi host. You first
 1517 create a role, then you create the user, and finally, you assign the role to the user.

- 1518 1. Create a role as follows:
 - 1519 a. Log onto the ESXi host using the vSphere Client, with administrative privileges.
 - 1520 b. Click on **Administration > Roles**.
 - 1521 c. Click on **Add Role**.

- 1522 d. Enter **RSA Log Capture** as the name of the Role.
- 1523 e. Choose **All Privileges > Global > Diagnostics** as the only privilege for this role.
- 1524 2. Create a local ESXi user as follows:
- 1525 a. From the Left navigation pane, click on the ESXi host, then click the **Users or Local Users**
- 1526 **& Groups** tab. The name of the tab depends on the credentials you used to log onto the
- 1527 ESXi host.
- 1528 b. Right-click on the **Users** tab, then click **Add**.
- 1529 c. Enter **rsa-vcenter-logs** in the **Login** field, and choose a strong password.
- 1530 3. Assign the role to the local user as follows:
- 1531 a. From the Left navigation pane, click on the ESXi host, then click the **Permissions** tab.
- 1532 b. Right-click in the **Permissions** table, then click **Add Permission**.
- 1533 c. In the dialog box, under the **Assigned Role** drop-down menu, choose **RSA Log Capture**.
- 1534 d. Under **Users and Groups**, click **Add...** The **Select Users and Groups** dialog box is displayed.
- 1535
- 1536 e. In the dialog box, leave the Domain value as (server), and select the **rsa-vcenter-logs**
- 1537 user.
- 1538 f. Click **Add**, then click **OK**.

1539 This completes the process of adding a least privilege user. When you configure the Log Collector for

1540 VMware collection in RSA NetWitness Suite, make sure to enter the credentials for this user in the **Add**

1541 **Source** dialog box.

1542 7.2.2 Configure the RSA NetWitness Log Collector for VMware Collection

1543 To configure the RSA NetWitness Log Collection for VMware Collection, go to page 105 in the [Log](#)

1544 [Collection Configuration Guide for RSA NetWitness Platform 11.4](#), and follow the instructions in the

1545 section titled “Configure VMware Event Sources in NetWitness Platform.”

1546 8 VMware Product Installation and Configuration Guide

1547 This section covers all the aspects of installing and configuring the VMware products used to build the

1548 example solution.

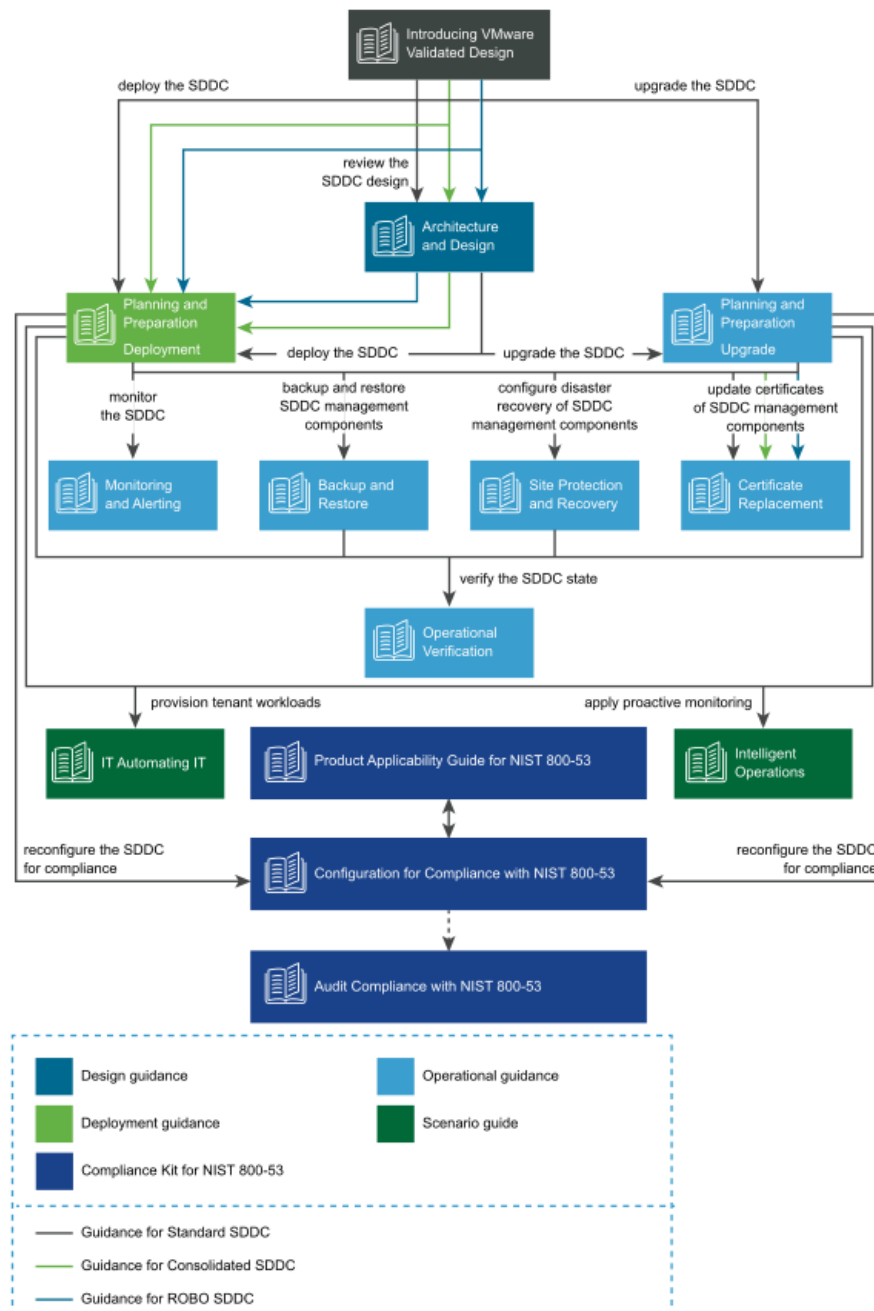
1549 8.1 Prerequisites

1550 The VMware Validated Design (VVD) is a blueprint for a Software Defined Data Center (SDDC). A
1551 Standard deployment model was used. In order to prepare for the implementation of the VVD, review
1552 the following documentation. It outlines the preparation and planning phases, contains logical design
1553 architectures and design decisions related to the implementation, and assists with the end-to-end
1554 process of deploying a VVD:

- 1555 ▪ [VMware Validated Design Documentation](#)
- 1556 ▪ *Documentation Structure and Audience* ([VVD 4.3](#), [VVD 5.0.1](#)), see [Figure 8-1](#)
 - 1557 • Architecture and Design
 - 1558 • Planning and Preparation Deployment
 - 1559 • Planning and Preparation Upgrade
 - 1560 • Monitoring and Alerting
 - 1561 • Backup and Restore
 - 1562 • Site Protection and Recovery
 - 1563 • Certificate Replacement
 - 1564 • Operational Verification
 - 1565 • IT Automating IT
 - 1566 • Intelligent Operations
 - 1567 • Security and Compliance Configuration for NIST 800-53:
 - 1568 ▪ [Introduction to Security and Compliance](#)
 - 1569 ▪ [Product Applicability Guide for NIST 800-53](#)
 - 1570 ▪ [Configuration for Compliance with NIST 800-53](#)
 - 1571 ▪ [Audit Compliance with NIST 800-53](#)
- 1572 ▪ *Introducing VMware Validated Design for Software-Defined Data Center* ([VVD 4.3](#), [VVD 5.0.1](#))
- 1573 ▪ *Design Objectives of VMware Validated Designs* ([VVD 4.3](#), [VVD 5.0.1](#))
- 1574 ▪ *Overview of Standard SDDC* ([VVD 4.3](#), [VVD 5.0.1](#))
- 1575 ▪ *VMware Validated Design Architecture and Design* ([VVD 4.3](#), [VVD 5.0.1](#))
- 1576 ▪ *VMware Validated Design Planning and Preparation* ([VVD 4.3](#), [VVD 5.0.1](#))
- 1577 ▪ *VMware Validated Design for Software-Defined Data Center Release Notes* ([VVD 4.3](#), [VVD 5.0](#),
1578 [VVD 5.0.1](#))

1579 To visualize how the VVD works in conjunction with the Compliance Kit for NIST 800-53, Figure 8-1
 1580 provides an overview of the documentation structure. The VMware Validated Design Compliance Kit
 1581 enhances the documentation of the VVD for SDDC and must be applied after the SDDC is deployed.

1582 **Figure 8-1: Map of VVD Documentation**



1583 To reconfigure your SDDC for compliance with NIST SP 800-53 ([https://doi.org/10.6028/NIST.SP.800-](https://doi.org/10.6028/NIST.SP.800-53r4)
1584 [53r4](https://doi.org/10.6028/NIST.SP.800-53r4)), you must download and license additional VMware and third-party software.

1585 The VVD coupled with *Security and Compliance Configuration for NIST 800-53* uses scripts and
1586 commands based on VMware PowerCLI to reconfigure the SDDC. You must prepare a host with a
1587 supported OS for running Microsoft PowerShell, set up Microsoft PowerShell, and install the latest
1588 version of VMware PowerCLI. The host must have connectivity to the ESXi management network in the
1589 management cluster.

1590 8.2 Installation and Configuration

1591 Review the following documentation for the complete guide concerning the installation and
1592 configuration for the VVD for an SDDC for a Standard Deployment:

- 1593 ▪ Deployment for Region A ([VVD 4.3](#), [VVD 5.0.1](#))
- 1594 ▪ Deployment for Region B ([VVD 4.3](#), [VVD 5.0.1](#))

1595 8.3 Configuration Customization Supporting the Use Cases and Security 1596 Capabilities

1597 After deployment of a Standard VVD, the enhancements outlined in this publication should be applied.
1598 The security configurations and controls outlined in this section were implemented on a number of VVD
1599 versions, beginning with VVD 4.2 and then VVD 4.3. In addition to this lab, a separate project to publish
1600 the security configurations as a Compliance Kit that works as an enhancement to the VVD was published
1601 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
1602 writing, 5.1, are unlikely to have a significant impact to the configuration guidance.

1603 Although this document outlines a specific version of the VVD, the Compliance Kit has been developed
1604 to support VVD 4.3, 5.0.1, 5.1, and future VVD releases. This section discusses the [VMware Validated
1605 Design 5.0.1 Compliance Kit for NIST 800-53](#) and provides supplemental information detailing the
1606 resources that are included within the kit because the kit was not formally published for VVD 4.2 or 4.3,
1607 even though it was tested based on these versions. The VVD 5.0.1 Compliance Kit contains a number of
1608 files, including:

- 1609 ▪ *Introduction to Security and Compliance*
- 1610 ▪ *Product Applicability Guide*
- 1611 ▪ *Configuration Guide*
- 1612 ▪ *Audit Guide*
- 1613 ▪ *Audit Guide Appendix*

1614 The configuration procedures included within the kit are in two groups:

- 1615 ▪ **Built-In Controls:** Security controls based on compliance requirements are included in the VVD
1616 for SDDC. These may require configuration and adjustment, but by design the capabilities are
1617 included in the VVD for SDDC.
- 1618 ▪ **Enhanced Controls:** Additional guidance on a per regulation or standard basis includes a set of
1619 capabilities that can be added to the VVD for SDDC.

1620 Over time, we expect a significant number of enhancement VVD controls to be incorporated into the
1621 VVD for SDDC. The enhancement guide always contains some number of NIST controls that are
1622 applicable to NIST SP 800-53 but are not included in the VVD for SDDC implementation. Each procedure
1623 documented in the *Configuration Guide* includes the NIST SP 800-53 control(s) that are associated with
1624 each. Two examples sampled from the *Configuration Guide* are included in Sections [8.3.1](#) and [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.

1625 The following products are part of the VVD Bill of Materials, but not included in the current iteration of
1626 the Compliance Kit: vRealize, vRealize Automation (vRA), vRealize Operations Manager (vROPS), and
1627 vRealize Log Insight (vRLI). The documentation surrounding the configuration of these products does
1628 exist and is sourced from their respective *DISA Security Technical Implementation Guides*, which can be
1629 reviewed at <https://public.cyber.mil/stigs/downloads>. There are two examples for these configurations
1630 sampled from the *Configuration Guide* (Sections [8.3.3](#) and [8.3.4](#)).

1631 [8.3.1 Example VVD 5.0.1 Configuration: Configure the Password and Policy](#) 1632 [Lockout Setting in vCenter Server in Region A](#)

- 1633 1. In a web browser, log into vCenter by using the vSphere Web Client.
- 1634 2. Configure the password policies.
 - 1635 a. From the **Home** menu of the vSphere Web Client, click **Administration**.
 - 1636 b. In the Navigator, under **Single Sign-On**, click **Configuration**.
 - 1637 c. On the **Policies** tab, under **Password Policy**, click **Edit**.
 - 1638 d. In the **Edit Password Policies** dialog box, configure the password policies and click **OK**.
 - 1639 i. **Maximum Lifetime** should be set to **60**.
 - 1640 ii. **Restrict Reuse** should be set to **5**.

- 1641 iii. **Minimum Length** should be set to **15**.
- 1642 iv. **Upper-case Characters** should be set to **1**.
- 1643 v. **Lower-case Characters** should be set to **1**.
- 1644 vi. **Numeric Characters** should be set to **1**.
- 1645 vii. **Special Characters** should be set to **1**.
- 1646 3. Configure the lockout policies.
- 1647 a. On the **Policies** tab, click **Lockout Policy** and click **Edit**.
- 1648 b. In the **Edit Lockout Policy** dialog box, for **Maximum Number of Failed Login Attempts**,
1649 enter **3**.
- 1650 c. For **Interval Between Failures**, enter **900**.
- 1651 d. For **Unlock Time**, enter **0** and then click **OK**.

1652 8.3.2 Example VVD 5.0.1 Configuration: Configure Encryption Management in 1653 Region A

- 1654 1. In a web browser, log in to vCenter Server by using the vSphere Web Client.
- 1655 2. Enable **Host Encryption Mode** on the **sfo01m01esx01.sfo01.rainpole.local** host.
- 1656 a. From the **Home** menu of the vSphere Web Client, select **Hosts and Clusters**.
- 1657 b. Under the **sfo01-m01dc data center**, select the **sfo01m01esx01.sfo01.rainpole.local**
1658 host and click the **Configure** tab.
- 1659 c. Under **System**, click **Security profile**.
- 1660 d. Under **Host Encryption Mode**, click **Edit**.
- 1661 e. In the **Set Encryption Mode** dialog box, from the **Encryption Mode** drop-down menu,
1662 select **Enabled** and click **OK**.
- 1663 f. Repeat the procedure for all remaining hosts in Region A.
- 1664 3. Enable VM encryption on all the VMs and virtual disks.
- 1665 a. From the **Home** menu of the vSphere Web Client, select **VMs and Templates**.
- 1666 b. Under the **sfo01-m01dc data center**, expand the **sfo01-m01fd-bcdr** folder, right-click
1667 the **sfo01m01vc01 VM** and select **VM Policies**, then **Edit VM Storage Policies**.

1668 c. From the **VM Storage Policy** drop-down menu, select **VM Encryption Policy**, click **Apply**
1669 **to all**, and click **OK**.

1670 d. Repeat the procedure to reconfigure the remaining VMs in Region A.

1671 8.3.3 Example vRealize Automation DISA STIG Configuration: Configure SLES for 1672 vRealize to protect the confidentiality and integrity of transmitted 1673 information

1674 1. Update the “Ciphers” directive with the following command:

```
1675 sed -i "/^[^#]*Ciphers/ c\Ciphers aes256-ctr,aes128-ctr" /etc/ssh/sshd_config
```

1676 2. Save and close the file.

1677 3. Restart the sshd process:

```
1678 service sshd restart
```

1679 8.3.4 Example vRealize Operations Manager DISA STIG Configuration: Configure 1680 the vRealize Operations server session timeout

1681 1. Log on to the admin UI as the administrator.

1682 2. Navigate to **Global Settings**.

1683 3. Select **Edit Global Settings**.

1684 4. Set the **Session Timeout** setting to **15** minutes.

1685 5. Select **OK**.

1686 8.4 Operation, Monitoring, and Maintenance

1687 This section explains how to operate, monitor, and maintain various VMware products. It points to
1688 existing documentation whenever possible, so this document only includes supplemental information,
1689 such as backup and recovery processes, and specific monitoring practices recommended for the
1690 example solution.

1691 8.4.1 Operation

1692 This section discusses the basic operation of the VVD 5.0.1 for an SDDC, in addition to any relevant
1693 products associated with such operations.

1694 vSphere vCenter Server (vCS) Appliance is a management application that allows for the management of
1695 VMs and ESXi hosts centrally. The vSphere Web Client is used to access the vCS.

1696 vRealize Operations Manager (vROPS) tracks and analyzes the operation of multiple data sources in the
1697 SDDC by using specialized analytic algorithms. The algorithms help vROPS learn and predict the behavior
1698 of every object that it monitors. Users access this information by views, reports, and dashboards.

1699 vRealize Automation (vRA) provides a secure web portal where authorized administrators, developers,
1700 and business owners can request new IT services and manage specific cloud and IT resources, while
1701 ensuring compliance with business policies.

1702 Please review the following for further information and discussion pertaining to the operational
1703 standards of the VVD 5.0.1 for an SDDC: [VMware Validated Design Documentation](#), [VMware Validated](#)
1704 [Design 5.0.1 Compliance Kit for NIST 800-53](#), and [NIST SP 1800-19B](#).

1705 8.4.2 Monitoring

1706 This section outlines monitoring and alerting functionalities and best practices pertaining to VVD.

1707 Use the vRealize Log Insight (vRLI) event signature engine to monitor key events and to send filtered or
1708 tagged events to one or more remote destinations. You can use a set of alerts to send to vROPS and
1709 through SMTP for operations team notification. The use of vRLI allows you to monitor the SDDC and
1710 provide troubleshooting and cause analysis, which can reduce operating costs.

1711 With the integration between vRLI and vROPS, you can implement the following cross-product event
1712 tracking:

- 1713 ▪ Send alerts from vRLI to vROPS, which maps them to the target objects.
- 1714 ▪ Launch in context from a vROPS object to the objects logs in vRLI.
- 1715 ▪ Launch in context from a vRLI event to the objects in vROPS.

1716 Use applications in vROPS to group monitoring data about the virtual machines of the SDDC
1717 management components.

1718 vROPS builds an application to determine how your environment is affected when one or more
1719 components experience problems. You can also monitor the overall health and performance of the
1720 application.

1721 vROPS collects data from the components in the application and displays the results in a summary
1722 dashboard with a real-time analysis for any or all the components.

1723 Ensuring that your backup solution is configured to trigger an email alert generation showing the status
1724 of your backup jobs is a recommended practice within the SDDC. This should be included in daily
1725 monitoring activities to ensure that all management objects within the SDDC have successful backup
1726 images. The following can be done to enable broad monitoring using vROPS:

- 1727 1. Create applications in vROPS to group the monitoring data
- 1728 a. about the VMs of vRealize Suite Lifecycle Manager
- 1729 b. about the VMs of vRLI
- 1730 c. about the VMs of VMware Site Recovery Manager
- 1731 d. about the VMs of VMware vSphere Replication (vR)
- 1732 e. for the VMs of vROPS
- 1733 f. collected from your vSphere Storage APIs for Data Protection (VADP)-based backup so-
- 1734 lution VMs
- 1735 g. about the VMs of VMware vSphere Update Manager Download Service (UMDS)
- 1736 2. Create email notifications in vROPS so it informs the SDDC operators of issues in the main moni-
- 1737 toring parameters of the environment.
- 1738 3. Configure vROPS to send email notifications about important alerts in the SDDC.
- 1739 Please review the [Monitoring and Alerting](#) documentation for more information regarding the
- 1740 monitoring of the VVD 4.3 deployment, and the [VVD for SDDC 5.0.1 release notes](#) for more information
- 1741 on monitoring for VVD 5.0.1 deployments.

1742 8.4.3 Maintenance

1743 This section outlines the steps to perform an SDDC upgrade that follows a defined upgrade path. The

1744 NCCoE project started with VVD version 4.3 and upgraded to 5.0.1. Table 8-1 provides a summary of the

1745 system requirements and upgrade sequence associated with the Bill of Materials (BOM) or product

1746 versions associated with each VVD version. This upgrade path is functional and defined by layers in

1747 which the components are upgraded or updated. It is important to note that functional and scalability

1748 tests for individual patches and express patches are not required for an environment.

1749 **Table 8-1: Summary of VVD Version and Associated Bill of Materials (Product Versions)**

SDDC Layer	Product Name	Product Ver- sion in VVD 4.3	Product Ver- sion in VVD 5.0.1	Operation Type
Operations Man- agement	vRealize Suite Lifecycle Manager	1.2	2.0.0 Patch 2	Upgrade
	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

SDDC Layer	Product Name	Product Version in VVD 4.3	Product Version in VVD 5.0.1	Operation Type
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

1750 The following are tips for upgrading the SDDC:

- 1751
- 1752 ■ Before you begin any upgrade process, review all the release notes.
 - 1753 ■ Consider that the SDDC design and implementation may be affected by security features that
 - 1754 are enabled. Ensure interoperability testing is performed before and after making security changes, as well as when introducing new features, functionality, and bug fixes.
 - 1755 ■ The environment within the NCCoE lab varies from the conventional VVD deployment because
 - 1756 for the NCCoE, additional integration with vendors is included, e.g., integration between HyTrust
 - 1757 components and Key Management Server (KMS) and the VVD.
 - 1758 ■ Note that if a distributed environment is used, ensure there is replication by using the
 - 1759 *vdcrepadmin* command line interface between the platform services controller (PSC) and the
 - 1760 vCenter environments. This can be checked by following the instructions in [VMware Knowledge](#)
 - 1761 [Base article 2127057](#).

- 1762 ▪ Perform a backup copy of your current certificates before you start the upgrade process. If you
 1763 need to request a new certificate, ensure you follow the procedures in [this document for VVD](#)
 1764 [4.3](#) and [this document for VVD 5.1](#).

1765 The following is a tip for updating the SDDC:

- 1766 ▪ Ensure an operational verification test is performed before and after performing an update. In
 1767 most cases, updates should not impact the SDDC design and implementation (updates could
 1768 include patches and bug fixes).

1769 Updates that are not validated by VVD should be approached with caution.

- 1770 ▪ Scalability and functionality tests for individual patches, express patches, and hot fixes are not
 1771 typically performed using the VVD. If a patch must be applied to your environment, follow the
 1772 VMware published practices and VMware Knowledge Base articles for the specific patch. If an
 1773 issue occurs during or after the process of applying a patch, contact VMware Technical Support.
- 1774 ▪ For further information and instruction regarding an update, please see the documentation for
 1775 [VVD 4.3](#) or [VVD 5.0](#).

1776 8.5 Product Configuration Overview

1777 This section contains Table 8-2, which details all configurations for each product, their corresponding
 1778 enhanced or built-in label, and their mapped NIST SP 800-53 Revision 4 controls (which are defined at
 1779 <https://doi.org/10.6028/NIST.SP.800-53r4>). The labels are derived from the compliance kit with the
 1780 exception of the vRA and vROPS items, which are sourced directly from their corresponding DISA STIGs.

1781 There are only a small number of vROPS and vRA DISA STIGs included in the following table, which
 1782 means it does not include all available configurations. For the entire compilation of vROPS and vRA DISA
 1783 STIGs, please review the following links:

- 1784 ▪ [VMware vRealize Automation 7.x Lighttpd](#)
- 1785 ▪ [VMware vRealize Automation 7.x SLES](#)
- 1786 ▪ [VMware vRealize Automation 7.x tc Server](#)
- 1787 ▪ [VMware vRealize Operations Manager 6.x Application](#)
- 1788 ▪ [VMware vRealize Operations Manager 6.x SLES](#)
- 1789 ▪ [VMware vRealize Operations Manager 6.x tc Server](#)
- 1790 ▪ [VMware vRealize – Cassandra](#)

1791 There are a few notable items for which there are no NIST control mappings; rather, they are identified
 1792 as “VMware Best Practices”. These items are not sourced from any existing DISA STIGs, hardening
 1793 guides, or other compliance frameworks. Their implementation is strongly recommended.

1794 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
vRA	VRAU-PG-000470	Enhanced	SC-13
vROPS	VROM-CS-000005	Enhanced	AC-3
vROPS	VROM-PG-000220	Enhanced	IA-7

Product Name	Configuration Label	Enhanced or Built-in	NIST SP 800-53 Rev. 4 Controls
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

1795

1796 Appendix A Security Configuration Settings

1797 This appendix captures the security configuration settings (Common Configuration Enumerations [CCEs]). The following table lists the VMware
1798 products and their associated security configurations.

CCE ID	Configur- ation(s)	Built-In/ Enhanced	Prod- uct	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. 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. If SNMP is enabled and “read only communities” is set to public, this is a finding. If SNMP is enabled and is not using v3 targets, this is a finding. Note: SNMP v3 targets can only be viewed and configured from the <code>esxcli</code> 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: FixedCAMConfigOption

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 personal 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 8-0	NIST800 53-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 personal 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 personal 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 Hosts and Clusters >> Update Manager tab, and select Scan 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 <filename>.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. SHA1 hash 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: <pre>Get-VMHost Get-AdvancedSetting -Name Syslog.global.logDir</pre> 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: <pre>Get-VMHost Get-AdvancedSetting -Name Config.HostAgent.plugins.hostsvc.esxAdminsGroup</pre> 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: <pre>Get-VMHost Get-AdvancedSetting -Name Mem.ShareForceSalting</pre> 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: <pre>Get-VMHostFirewallDefaultPolicy</pre> 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: <pre>Get-VMHost Get-AdvancedSetting -Name Syslog.global.logHost</pre>	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-8445-9-7	NIST800-53-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-8446-0-5	NIST800-53-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-8446-1-3	NIST800-53-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-8446-2-1	NIST800-53-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-8447-8-7	NIST800-53-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-8447-9-5	NIST800-53-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-8448-0-3	NIST800-53-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 Configure > Networking > VMKernel adapters. 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 Configure > Networking > VMKernel adapters. 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 Configure >> Networking >> VMkernel adapters. 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 Configure >> Networking >> TCP/IP Configuration. 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 Administration >> Single Sign-On >> Policies >> Password Policy .	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 Administration >> Single Sign-On >> Policies >> Password Policy .	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 Administration >> Single Sign-On >> Policies >> Password Policy .	Universal Distributed Logical Router Password (Dependent on Customer Configurations)

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8450-4-0	NIST800-53-VI-NET-CFG-00281	Built-in	NSX	Log on to NSX Manager Virtual Appliance, then go to Backup & Restore . 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-8450-5-7	NIST800-53-VI-NET-CFG-00282	Built-in	NSX	Log on to NSX Manager Virtual Appliance, then go to Manage Appliance Settings and look under General Network Settings . If IPv6 is configured, this is a finding.	IPv6 should be disabled
CCE-8450-6-5	NIST800-53-VI-NET-CFG-00283	Built-in	NSX	Log on to NSX Manager Virtual Appliance, then go to Manage Appliance Settings and look under DNS Servers . If IPv6 DNS is configured, this is a finding.	IPv6 DNS should be disabled
CCE-8450-7-3	NIST800-53-VI-NET-CFG-00285	Built-in	NSX	Log on to NSX Manager Virtual Appliance, then go to Manage Appliance Settings and look under Time Settings . If any 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 Manage Appliance Settings . 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 Manage Appliance Settings --> SSL Certificates . Click on the certificate and verify certificate details.	1) Appropriate Issuer 2) Correct certificate Type 3) RSA Algorithm 4) 2048 bits keys or higher
CCE-8451-0-7	NIST800-53-VI-NET-CFG-00288	Built-in	NSX	Assess the deployment and try to reach NSX manager being on standard network. The NSX manager should only be reachable using isolation mechanisms.	No read or write permissions on backup directory
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 backup directory. If the backup directory can be read 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-8451-3-1	NIST800-53-VI-NET-CFG-00291	Built-in	NSX	Log on to NSX Manager Virtual Appliance, then go to Manage Appliance Settings and look under General network settings . If IPv4 DNS is not authorized or secure, this is a finding.	IPv4 DNS is authorized and secure
CCE-8451-4-9	NIST800-53-VI-NET-CFG-00294	Built-in	NSX	Log on to NSX Manager Virtual Appliance, then look under Backup & Restore . Verify “FTP Server settings”.	FTP Server settings (Dependent on Customer Configurations)
CCE-8451-5-6	NIST800-53-VI-NET-CFG-00295	Built-in	NSX	After downloading the media, use the MD5/SHA1 sum value to verify the integrity of the download. Compare the MD5/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 or MD5 hash should match
CCE-8451-6-4	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-8451-7-2	NIST800-53-VI-NET-CFG-00297	Built-in	NSX	Run this Rest API call to get the properties of the controller node: <code>https://<nsxmgr>/api/2.0/vdn/controller/node</code> Response: <code><controllerNodeConfig></code> <code><ipSecEnabled>true</ipSecEnabled ></code> <code></controllerNodeConfig></code> If ipSecEnabled is not true, this is a finding.	<code><ipSecEnabled>true</ipSecEnabled ></code>

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 Home > Inventory > Networking . Select “DSwitch” for distributed portgroups. Select each dvPortgroup connected to active VMs requiring securing. Go to tab Summary > Edit Settings > Policies > Security . 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 Home > Inventory > Networking . Select “DSwitch” for distributed portgroups. Select each dvPortgroup connected to active VMs requiring securing. Go to tab Summary > Edit Settings > Policies > Security . 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 Home > Inventory > Networking . Select “DSwitch” for distributed portgroups. Select each dvPortgroup connected to active VMs requiring securing. Go to tab Summary > Edit Settings > Policies > Security . 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-8452-3-0	NIST800-53-VI-NET-CFG-00306	Built-in	NSX	Log in to VMware vSphere Web Client. Navigate to Networking and Security --> Installation and Upgrade . 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-8452-4-8	NIST800-53-VI-NET-CFG-00308	Built-in	NSX	Log into the vCenter web interface with credentials authorized for administration. Navigate to Networking and Security >> Firewall . Expand “Default Section Layer 3” in Configuration. If the action for the Default Rule is “Allow”, this is a finding.	Denied
CCE-8452-5-5	NIST800-53-VI-NET-CFG-00311	Built-in	NSX	Log on to vSphere Web Client with credentials authorized for administration. Navigate and select Networking and Security >> Users and Domains . View each role and verify the users and/or groups assigned to it.	Procedural
CCE-8452-6-3	NIST800-53-VI-NET-CFG-00312	Built-in	NSX	From the vSphere Web Client, go to Administration >> Single Sign-On >> Configuration >> Policies >> Password Policy . View the values of the password format requirements. If Numeric Characters is not set to at least 1, this is a finding.	1
CCE-8452-7-1	NIST800-53-VI-NET-CFG-00313	Built-in	NSX	From the vSphere Web Client, go to Administration >> Single Sign-On >> Configuration >> Policies >> Password Policy . 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-8452-8-9	NIST800-53-VI-NET-CFG-00316	Built-in	NSX	Log on to vSphere Web Client with credentials authorized for administration. Navigate and select Networking and Security >> Users and Domains . 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-8452-9-7	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-8453-0-5	NIST800-53-VI-NET-CFG-00318	Built-in	NSX	Log into vSphere Web Client with credentials authorized for administration. Navigate to Networking and Security >> Firewall . Expand rule sections as necessary to view rules. If there are no rules configured to enforce authorizations, this is a finding.	Procedural
CCE-8453-1-3	NIST800-53-VI-NET-CFG-00321	Built-in	NSX	From the vSphere Web Client, go to Administration >> Single Sign-On >> Configuration >> Policies >> Password Policy . 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-8453-2-1	NIST800-53-VI-NET-CFG-00322	Built-in	NSX	From the vSphere Web Client, go to Administration >> Single Sign-On >> Configuration >> Policies >> Password Policy . 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-8453-3-9	NIST800-53-VI-NET-CFG-00323	Enhanced	NSX	Log into vSphere Web Client with credentials authorized for administration. Navigate and select Networking and Security >> Firewall 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-8453-4-7	NIST800-53-VI-NET-CFG-00324	Enhanced	NSX	Log into vSphere Web Client with credentials authorized for administration. Navigate and select Networking and Security >> SpoofGuard . Check the Default policy of each NSX Manager. If the mode is disabled, this is a finding.	Enabled
CCE-8453-5-4	NIST800-53-VI-NET-CFG-00328	Built-in	NSX	Log onto vSphere Web Client with credentials authorized for administration. Navigate and select Networking and Security >> select the NSX Edges tab on the left-side menu. Double-click the Edge ID. Navigate to Manage >> Verify the configurations under Settings, Firewall, Routing, Bridging, and DHCP Relay are enabled only as necessary to the deployment. If unnecessary services are enabled, this is a finding.	Enabled
CCE-8453-6-2	NIST800-53-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-8453-7-0	NIST800-53-VI-NET-CFG-00330	Built-in	NSX	From the vSphere Web Client, go to Administration >> Single Sign-On >> Configuration >> Policies >> Password Policy . 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 https://client-hostname/vsphere-client 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 Networking and Security >> Firewall . 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 Networking and Security >> Firewall . 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 Networking and Security >> NSX Edges tab on the left-side menu. Double-click the EdgeID. Click on the Configure tab on the top of the new screen, then Interfaces >> 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 Backup and Restore >> Backup History . 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	Ask the system administrator if hardened, patched templates are used for VM creation, properly configured OS deployments, including applications both dependent and non-dependent on VM-specific configurations. If hardened, patched templates are not used for VM creation, this is a finding. The system must use templates to deploy VMs whenever possible.	Hardened virtual machine templates to use for OS deployments.
CCE-8430-2-9	NIST800-53-VI-ESXI-CFG-00061	Enhanced	vCenter	On the Home page of the vSphere Client, select Menu > Administration and click Roles . Select the VC from the Roles provider drop-down menu. Select the Virtual machine user (sample) role and click Privileges . 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.	Disable Console interaction privilege
CCE-8430-3-7	NIST800-53-VI-ESXI-CFG-00065	Built-in	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM Where {\$_ .ExtensionData.Config.Hardware.Device.DeviceInfo.Label -match "parallel"}</pre> If a virtual machine has a parallel device present, this is a finding.	Disconnect unauthorized parallel devices
CCE-8430-4-5	NIST800-53-VI-ESXI-CFG-00066	Built-in	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM Where {\$_ .ExtensionData.Config.Hardware.Device.DeviceInfo.Label -match "serial"}</pre> If a virtual machine has a serial device present, this is a finding.	Disconnect unauthorized serial devices
CCE-8430-5-2	NIST800-53-VI-ESXI-CFG-00067	Built-in	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM Get-UsbDevice</pre> If a virtual machine has any USB devices or USB controllers present, this is a finding.	No USB device present

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-8430-6-0	NIST800-53-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: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name sched.mem.pshare.salt</pre> If sched.mem.pshare.salt exists, this is a finding.	Remove the advanced setting sched.mem.pshare.salt
CCE-8430-7-8	NIST800-53-VI-ESXI-CFG-00070	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.copy.disable</pre> If isolation.tools.copy.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8430-8-6	NIST800-53-VI-ESXI-CFG-00071	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.dnd.disable</pre> If isolation.tools.dnd.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8430-9-4	NIST800-53-VI-ESXI-CFG-00072	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.setGUIOptions.enable</pre> If isolation.tools.setGUIOptions.enable does not exist or is not set to false, this is a finding.	FALSE
CCE-8431-0-2	NIST800-53-VI-ESXI-CFG-00073	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.paste.disable</pre> 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: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.diskShrink.disable</pre> 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: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.diskWiper.disable</pre> 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: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.hgfsServerSet.disable</pre> 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: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.ghi.autologon.disable</pre> 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: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.bios.bbs.disable</pre> 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-8431-6-9	NIST800-53-VI-ESXI-CFG-00079	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.getCreds.disable</pre> If <code>isolation.tools.getCreds.disable</code> does not exist or is not set to true, this is a finding.	TRUE
CCE-8431-7-7	NIST800-53-VI-ESXI-CFG-00080	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.ghi.launchmenu.change</pre> If <code>isolation.tools.ghi.launchmenu.change</code> does not exist or is not set to true, this is a finding.	TRUE
CCE-8431-8-5	NIST800-53-VI-ESXI-CFG-00081	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.memSchedFakeSampleStats.disable</pre> If <code>isolation.tools.memSchedFakeSampleStats.disable</code> does not exist or is not set to true, this is a finding.	TRUE
CCE-8431-9-3	NIST800-53-VI-ESXI-CFG-00082	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.ghi.protocolhandler.info.disable</pre> If <code>isolation.tools.ghi.protocolhandler.info.disable</code> does not exist or is not set to true, this is a finding.	TRUE
CCE-8432-0-1	NIST800-53-VI-ESXI-CFG-00083	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.ghi.host.shellAction.disable</pre> If <code>isolation.ghi.host.shellAction.disable</code> 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-8432-1-9	NIST800-53-VI-ESXI-CFG-00084	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.dispTopoRequest.disable</pre> If <code>isolation.tools.dispTopoRequest.disable</code> does not exist or is not set to true, this is a finding.	TRUE
CCE-8432-2-7	NIST800-53-VI-ESXI-CFG-00085	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.trashFolderState.disable</pre> If <code>isolation.tools.trashFolderState.disable</code> does not exist or is not set to true, this is a finding.	TRUE
CCE-8432-3-5	NIST800-53-VI-ESXI-CFG-00086	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.ghi.trayicon.disable</pre> If <code>isolation.tools.ghi.trayicon.disable</code> does not exist or is not set to true, this is a finding.	TRUE
CCE-8432-4-3	NIST800-53-VI-ESXI-CFG-00087	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.unity.disable</pre> If <code>isolation.tools.unity.disable</code> does not exist or is not set to true, this is a finding.	TRUE
CCE-8432-5-0	NIST800-53-VI-ESXI-CFG-00088	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.unityInterlockOperation.disable</pre> If <code>isolation.tools.unityInterlockOperation.disable</code> 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-8432-6-8	NIST800-53-VI-ESXI-CFG-00089	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.unity.push.update.disable</pre> If isolation.tools.unity.push.update.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8432-7-6	NIST800-53-VI-ESXI-CFG-00090	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.unity.taskbar.disable</pre> If isolation.tools.unity.taskbar.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8432-8-4	NIST800-53-VI-ESXI-CFG-00091	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.unityActive.disable</pre> If isolation.tools.unityActive.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8432-9-2	NIST800-53-VI-ESXI-CFG-00092	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.unity.windowContents.disable</pre> If isolation.tools.unity.windowContents.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-8433-0-0	NIST800-53-VI-ESXI-CFG-00093	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.vmxDnDVersionGet.disable</pre> If isolation.tools.vmxDnDVersionGet.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-8433-1-8	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: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.guestDnDVersionSet.disable</pre> 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: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.vixMessage.disable</pre> 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: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name RemoteDisplay.maxConnections</pre> 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: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name RemoteDisplay.vnc.enabled</pre> 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: <pre>Get-VM "VM Name" Get-AdvancedSetting -Name isolation.tools.autoInstall.disable</pre> 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-8434-7-4	NIST800-53-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-8434-8-2	NIST800-53-VI-VC-CFG-00403	Built-in	vCenter	From the vSphere Web Client go to Administration >> Single Sign-On >> Configuration >> Policies >> Password Policy . If Restrict Reuse is not set to 5 or more, this is a finding.	5
CCE-8434-9-0	NIST800-53-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 <vcenter server name> -Name config.log.level</code> If the level is not set to info, this is a finding.	info
CCE-8435-0-8	NIST800-53-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-8435-1-6	NIST800-53-VI-VC-CFG-00406	Built-in	vCenter	From the vSphere Web Client go to Administration >> Client Plug-Ins . 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.	N/A
CCE-8435-2-4	NIST800-53-VI-	Built-in	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following commands:	Authorized extensions from Trusted Sources

CCE ID	Configuration(s)	Built-In/Enhanced	Product	Audit Procedure	Recommended Parameter Value
	VC-CFG-00407			<pre>Get-VDSwitch Get-VDSecurityPolicy Get-VDPortgroup Get-VDSecurityPolicy</pre> <p>If the MAC Address Changes policy is set to accept, this is a finding.</p>	
CCE-8435-3-2	NIST800-53-VI-VC-CFG-00408	Built-in	vCenter	<p>From the vSphere Web Client go to Administration >> Single Sign-On >> Configuration >> Policies >> Password Policy.</p> <p>If Upper-Case Characters is not set to at least 1, this is a finding.</p>	1
CCE-8435-4-0	NIST800-53-VI-VC-CFG-00409	Built-in	vCenter	<p>From a PowerCLI command prompt, while connected to the vCenter server run the following command:</p> <pre>Get-VDSwitch select Name,@{N="NIOCEnabled";E={\$_.ExtensionData.config.NetworkResourceManagementEnabled}}</pre> <p>If Network I/O Control is disabled, this is a finding.</p>	enabled
CCE-8435-5-7	NIST800-53-VI-VC-CFG-00410	Enhanced	vCenter	<p>From the vSphere Web Client go to Administration >> Single Sign-On >> Configuration >> Policies >> Password Policy.</p> <p>If the Minimum Length is not set to at least 15, this is a finding.</p>	15
CCE-8435-6-5	NIST800-53-VI-VC-CFG-00411	Enhanced	vCenter	<p>From a PowerCLI command prompt, while connected to the vCenter server run the following commands:</p> <pre>\$vds = Get-VDSwitch \$vds.ExtensionData.Config.HealthCheckConfig</pre> <p>If the health check feature is enabled on distributed switches and is not on temporarily for troubleshooting purposes, this is a finding.</p>	FALSE
CCE-8435-7-3	NIST800-53-VI-VC-CFG-00412	Enhanced	vCenter	<p>From the vSphere Client, select the vCenter server at the top of the hierarchy and go to Alarms >> Definitions.</p> <p>or</p> <p>From a PowerCLI command prompt, while connected to the vCenter server run the following command:</p>	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 Administration >> Single Sign-On >> Configuration >> Policies >> Password Policy.</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 Alarms >> Definitions.</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 Administration >> Access Control >> Roles.</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 Alarms >> Definitions.</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.PermissionRemovedEvent"} Select Name,Enabled,@{N="EventTypeId";E={\$_ .ExtensionData.Info.Expression.Expr ession.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.defa ultPortConfig.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 Host and Clusters >> Select a vCenter Server >> Configure >> vSAN >> Internet Connectivity >> Status.</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 Host and Clusters >> Select a Cluster >> Related Objects >> Datastores. 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 Administration >> Single Sign-On >> Configuration >> Policies >> Password Policy.</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 <vcenter server name> -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 vCenter Inventory Lists >> vCenter Servers >> Select your vCenter Server >> Settings >> Advanced System Settings.</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 <vcenter server name> -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"> 1. The Update Manager must be configured to use the Update Manager Download Server. 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. <p>To verify download settings, from the vSphere Client/vCenter Server system, click Update Manager. Select a Host and then click the Settings tab. In the Download Settings 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 Administration >> Single Sign-On >> Configuration >> Policies >> Password Policy.</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 Administration >> Single Sign-On >> Configuration >> Policies >> Password Policy.</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 Administration >> Single Sign-On >> Configuration >> Policies >> Lockout Policy . 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 Administration >> Single Sign-On >> Configuration >> Policies >> Lockout Policy . 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 Administration >> Single Sign-On >> Configuration >> Policies >> Lockout Policy . 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 vCenter Inventory Lists >> vCenter Servers >> Select your vCenter Server >> Settings >> Advanced Settings . or From a PowerCLI command prompt, while connected to the vCenter server run the following command: <code>Get-AdvancedSetting -Entity <vcenter server name> -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-8437-8-9	NIST800-53-VI-VC-CFG-00440	Enhanced	vCenter	<p>From the vSphere Web Client, go to Networking >> Select a distributed port group >> Manage >> Settings >> Properties. 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-8437-9-7	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 Alarms >> Definitions.</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 Networks >> Distributed Port Groups 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 Home >> Networking. Select a distributed port group, click Edit, then go to Security.</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 <code>svga.vgaonly</code> does not exist or is not set to false, 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 <code>pciPassthru*.present</code> 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 Content Packs . Under Content Pack Marketplace, select Marketplace . 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 vSAN , click Services . 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-8460-7-1	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-8460-8-9	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-8460-9-7	NIST800-53-VI-Storage-SDS-CFG-00207	Enhanced	vSAN	<p>If vSAN Health Check is installed:</p> <p>From the vSphere Client, go to Host and Clusters. Select a vCenter Server and go to Configure > vSAN > Internet Connectivity > Status.</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-8461-0-5	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

1799

1800 **Appendix B List of Acronyms**

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

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

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

1801 **Appendix C** **Glossary**

1802 All significant technical terms used within this document are defined in other key documents,
1803 particularly National Institute of Standards and Technology Interagency Report (NISTIR) 7904, *Trusted*
1804 *Geolocation in the Cloud: Proof of Concept Implementation*. As a convenience to the reader, terms
1805 critical to understanding this volume are provided in this glossary.

Cloud workload	A logical bundle of software and data that is present in, and processed by, a cloud computing technology.
Geolocation	Determining the approximate physical location of an object, such as a cloud computing server.
Hardware root of trust	An inherently trusted combination of hardware and firmware that maintains the integrity of information.
Trusted compute pool	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> .