NIST SPECIAL PUBLICATION 1800-19C

Trusted Cloud:

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

Volume C:
How-to Guides

Michael Bartock
Murugiah Souppaya
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

DISCLAIMER

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

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

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

FEEDBACK

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

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

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

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

NIST CYBERSECURITY PRACTICE GUIDES

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

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

ABSTRACT

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

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

KEYWORDS

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

ACKNOWLEDGMENTS

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

Technology Partner/Collaborator	Build Involvement
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

DOCUMENT CONVENTIONS

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

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

CALL FOR PATENT CLAIMS

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

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

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

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

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

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

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

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

Contents

Appendices

List of Figures

List of Tables

1 Introduction

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

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

1.1 Practice Guide Structure

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

This guide contains three volumes:

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

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

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

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

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

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

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

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

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

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

1.2 Build Overview

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

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

1.3 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	file names and path names; references to documents that are not hyperlinks; new terms; and placeholders	For language use and style guidance, see the *NCCoE Style Guide*.
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	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
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.

1.4 Logical Architecture Summary

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

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

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

The ICSV instance consists of the following components:

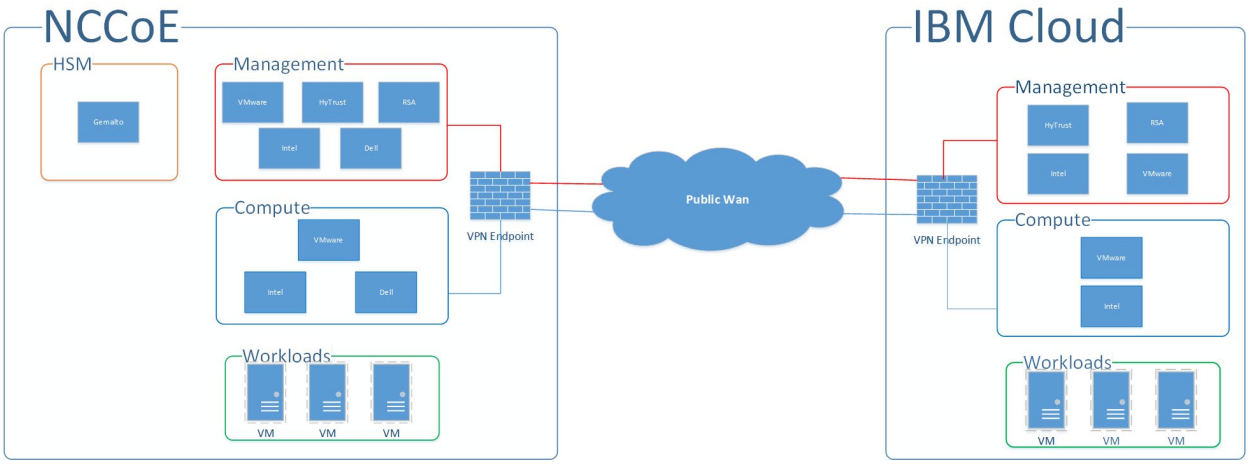
- IBM-provisioned servers with Intel processors
- compute, storage, network virtualization with VMware components
- asset tagging and policy enforcement, and workload and storage encryption with HyTrust components

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

Figure 1-1 shows the high-level architecture. It depicts the four main components that comprise the build:

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

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.

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

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

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

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

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

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

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

1. Set the hostname:

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

2. Configure password policies:

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

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

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

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

c. Enable password with highest privileges:

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

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

```
fips mode enable
```

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

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

4. Enable SSH server:

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

5. Disable telnet server:

```
no ip telnet server enable
```

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

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

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

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

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

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

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

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

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

10. Define the IPv4 static route:

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

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

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

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

12. Configure Media Access Control (MAC) settings:

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

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

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

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

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

15. Configure the login banner text:

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

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

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

17. Disable Support Assist:

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

18. Configure redundancy:

```
redundancy auto-synchronize full
```

19. Configure the loopback interface for management traffic:

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

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

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

21. Enter the clock timezone for your system:

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

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

```
no ip source-route
```

23. Configure reload behavior:

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

24. Enable login statistics:

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

25. Configure the management interface:

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

```
 no shutdown
!
```

2.2.1 Functionality and interoperability (layer 3 access)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2.2 VLANs

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

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

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

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

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

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

2.3 Dell PowerEdge Hardening

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

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

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

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

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

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

2.4 Avamar Security Hardening

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

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

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

3 Gemalto Product Installation and Configuration Guide

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

3.1 Gemalto Luna 6 Initialization

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

1. Set the time zone to US Eastern:

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

2. Set the date/time format:

```
syscont time HH:MM YYYMMDD
```

3. Set the hostname:

```
net hostname TCHSM
```

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

```
net dns add nameserver 172.16.1.11
```

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

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

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

1. Generate the certificate:

```
sysconf regenCert
```

2. Bind the cert to eth0:

```
ntls bind eth0
```

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

```
ntls show
```

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

1. Initialize the HSM and set the login timeout:

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

2. Next, log in as Security Officer:

```
hsm init -label NCCoE_Lab
```

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

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

3.2 Create HSM Partition

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

1. `hsm login`
2. Create the HSM partition to be used for KeyControl:

```
partition create -partition HyTrust_KeyControl
```

3. Set the password for the newly created partition:

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

4. Allow activation:

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

5. Allow auto-activation:

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

6. Activate the newly created partition:

```
partition activate -partition HyTrust_KeyControl
```

7. Show partition serial number for high availability:

```
partition show
```

4 HyTrust Product Installation and Configuration Guide

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

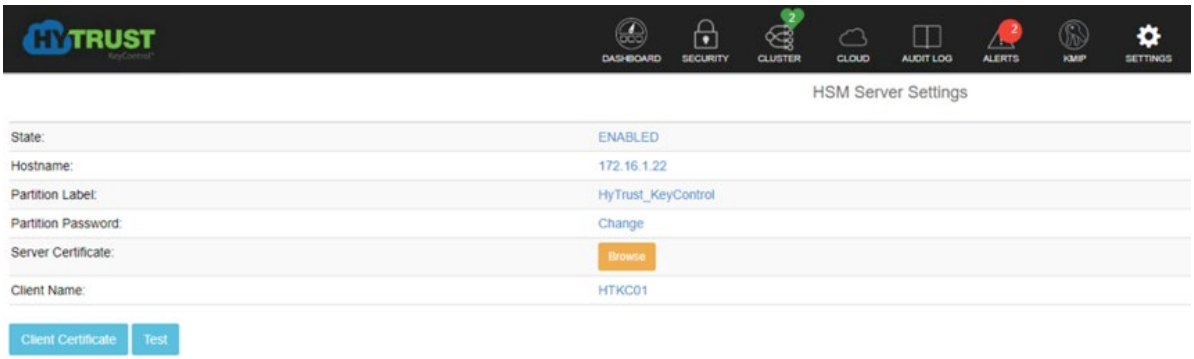
4.1 HyTrust KeyControl Setup

First, follow the directions on these pages:

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

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

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



4.2 HyTrust DataControl Setup

Follow the directions on these pages:

1. Creating a Cloud VM Set
2. Installing Policy Agent on Windows
3. Registering the Policy Agent Using the HyTrust Policy Agent GUI
4. Encrypting a Disk Using the WebGUI

4.3 HyTrust CloudControl Appliance Setup

Follow the directions on these pages:

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

6. Adding Hosts to CloudControl
    a. Protected Hosts
    b. Adding a Host
7. Configuring Managed Hosts
8. Enabling a Good Known Host
9. Verifying and Updating Host Trust (and Host Icons Used in CloudControl)

For more information on PolicyTags provisioning and evaluation, see the "PolicyTags Provisioning" section in chapter 6 of the Administration Guide for HyTrust CloudControl.

4.3.1 Provisioning PolicyTags

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

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

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

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

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

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

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

5. Repeat this for each Trusted host.

4.3.1.2 Generate esxcli Commands

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

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

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

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

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

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

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

   Example:

   ```
   export--2018-08-27T23-44-43Z/6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-
   dc27fe259e1a/system--6aa6af76-14f6-42e8-b452-dc27fe259e1a.der
   export--2018-08-27T23-44-43Z/6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-
   dc27fe259e1a/system--6aa6af76-14f6-42e8-b452-dc27fe259e1a.sha1.bin
   export--2018-08-27T23-44-43Z/6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-
   dc27fe259e1a/system--6aa6af76-14f6-42e8-b452-dc27fe259e1a.sha256.bin
   export--2018-08-27T23-44-43Z/6aa6af76/14f6/42e8/b452/6aa6af76-14f6-42e8-b452-
   dc27fe259e1a/system--6aa6af76-14f6-42e8-b452-dc27fe259e1a.metadata.txt
   export--2018-08-27T23-44-43Z/dddfda66/314e/4378/8f4d/dddfda66-314e-4378-8f4d-
   060b5d885038/system--dddfda66-314e-4378-8f4d-060b5d885038.der
   export--2018-08-27T23-44-43Z/dddfda66/314e/4378/8f4d/dddfda66-314e-4378-8f4d-
   060b5d885038/system--dddfda66-314e-4378-8f4d-060b5d885038.sha1.bin
   export--2018-08-27T23-44-43Z/dddfda66/314e/4378/8f4d/dddfda66-314e-4378-8f4d-
   060b5d885038/system--dddfda66-314e-4378-8f4d-060b5d885038.sha256.bin
   export--2018-08-27T23-44-43Z/dddfda66/314e/4378/8f4d/dddfda66-314e-4378-8f4d-
   060b5d885038/system--dddfda66-314e-4378-8f4d-060b5d885038.metadata.txt
   ```

3. Navigate to the extracted directory, for example:

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

4. At the prompt, type the following command:

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

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

   ```
   "subject" : "4c4c4544-0032-3010-8035-b5c04f333832",
   "id" : "6aa6af76-14f6-42e8-b452-dc27fe259e1a"
   ```

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

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

This returns the `esxcli` command.

Example:

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

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

4.3.1.3 Run esxcli Commands

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

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

   Example:

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

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

4.3.2 Policy Interaction

See the Policy Interaction webpage for more information on how policy enforcement works.

4.4 HyTrust CloudAdvisor Appliance Setup

Follow the directions on these pages:

1. Deploying CloudAdvisor
2. Configuring the CloudAdvisor Virtual Appliance
3. Setting Up CloudAdvisor
4. Adding VMs to Inventory

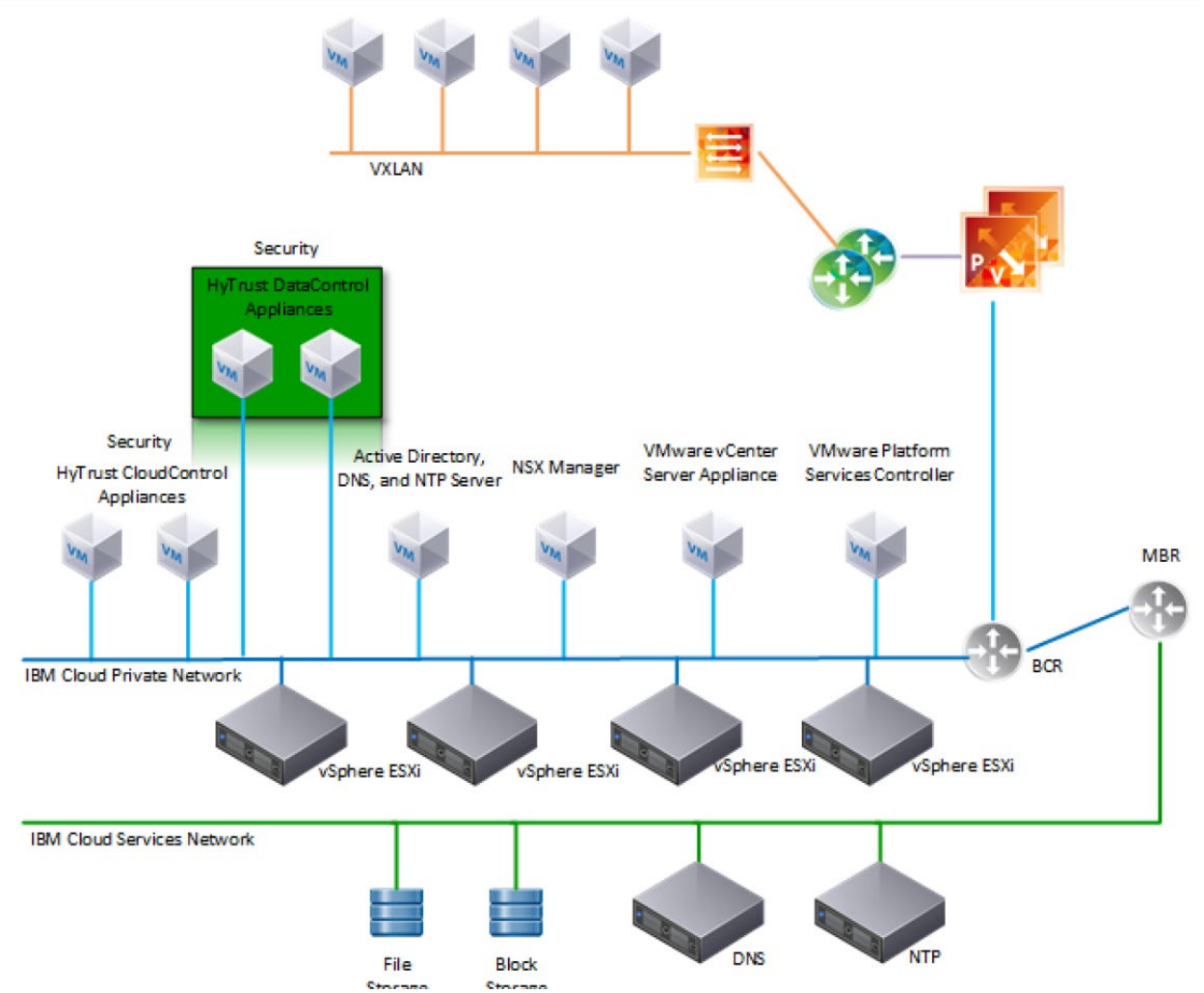
5 IBM Product Installation and Configuration Guide

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

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

5.1 ICSV Deployment

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



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

5.1.1 Pre-deployment

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

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

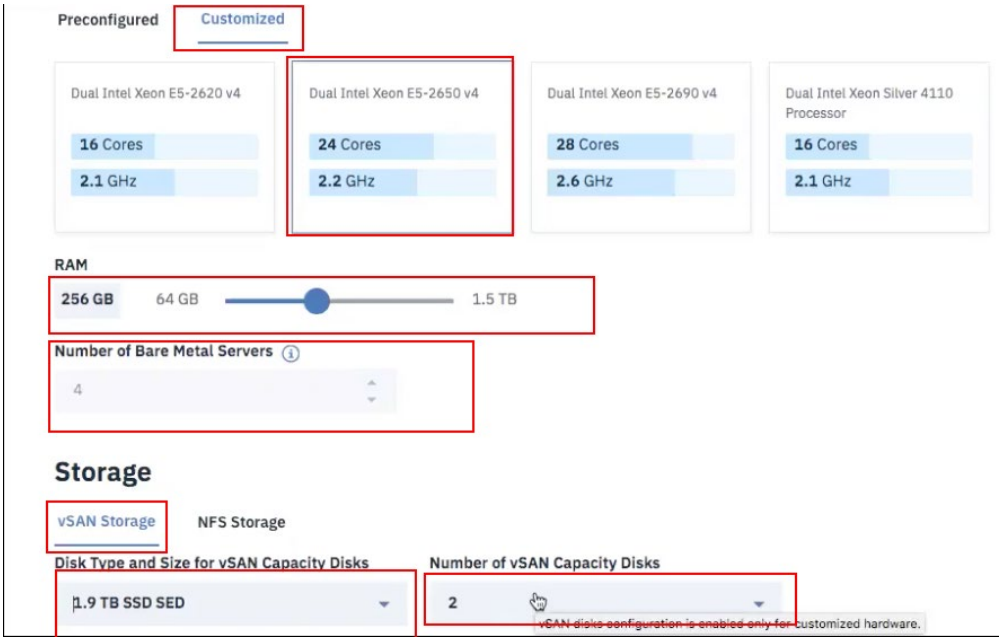
Client Input Variables	Choices	Example Values
Intel core base	2.1, 2.2, 2.3 GHz	2.2 GHz
RAM	64 GB-1.5 TB	256 GB
Data center location	Dallas, DC, Boulder, etc.	Dallas
Data storage	NFS or VSAN	VSAN
Size of each data storage	1, 2, 4, 8, 12 TB	2 TB
Performance of file shares	2, 4, 10 IOPS/GB	NA
NFS version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

5.1.2 Automation deployment

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

1. Log into the IBM Cloud infrastructure customer portal at https://console.ng.bluemix.net/catalog/.

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



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

5.1.3 Post-deployment

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

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_ESXMAdmin	default	ASC_ESXMAdmin
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_ESXMAdmin	default	ASC_ESXMAdmin
ASC_NetworkAdmin	default	ASC_NetworkAdmin
ASC_PolicyAdmin	default	ASC_PolicyAdmin
ASC_RoleAdmin	default	ASC_RoleAdmin
ASC_StorageAdmin	default	ASC_StorageAdmin
ASC_SuperAdmin	default	ASC_SuperAdmin
ASC_ThirdParty	default	ASC_ThirdParty
ASC_UCSLogin	default	ASC_UCSLogin
ASC_VIAdmin	default	ASC_VIAdmin
ASC_VMPowerUser	default	ASC_VMPowerUser
ASC_VMUser	default	ASC_VMUser

5.2 Enable Hardware Root of Trust on ICSV Servers

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

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

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

5.2.2 Enable TPM/TXT on SuperMicro hosts

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

    < Start of ticket description >

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

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

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

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

Please let me know when you have done this successfully.

< End of ticket description >

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

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

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

5.2.3 Enable TPM/TXT in IBM Cloud

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

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

5.2.4 Validate the TPM/TXT is enabled

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

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

   This should show if the TPM library was loaded.

2. Other commands to check are:

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

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

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

   ```
   esxcli hardware trustedboot get
   ```

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

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

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

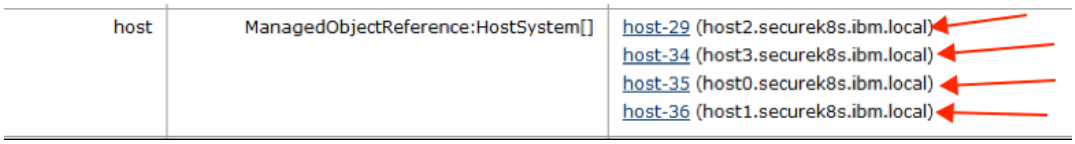
licenseManager	ManagedObjectReference:LicenseManager	LicenseManager
localizationManager	ManagedObjectReference:LocalizationManager	LocalizationManager
overheadMemoryManager	ManagedObjectReference:OverheadMemoryManager	OverheadMemoryManger
ovfManager	ManagedObjectReference:OvfManager	OvfManager
perfManager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

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

d. Search for **group-h4 (host)** and click on it.

e. Search for **domain-c7 (SDDC-Cluster)** and click on it.

f. Search for **host,** and you will see all the hosts listed with their host names.



g. Click on the host that you need to validate. In our demo, we are checking **host1.securek8s.ibm.local**.

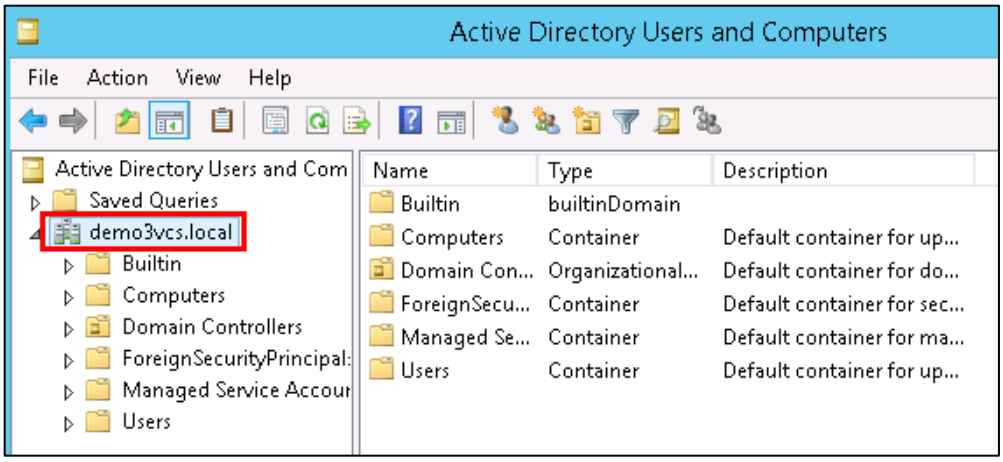
h. Search for method **QueryTpmAttestationReport** and click on it to invoke the method.

i. Click on **Invoke Method**.

5.2.6 Set up Active Directory users and groups

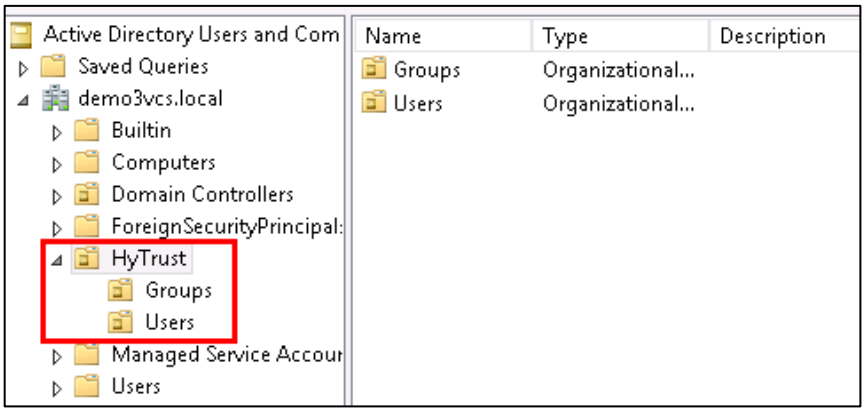
In this part of the setup, you will create several new organizational units. Remember that this procedure uses a Windows 2012 server and Microsoft AD to illustrate the steps. Your environment and your specific steps might be different. This section assumes actions are being performed from the ICSV Microsoft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

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



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

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

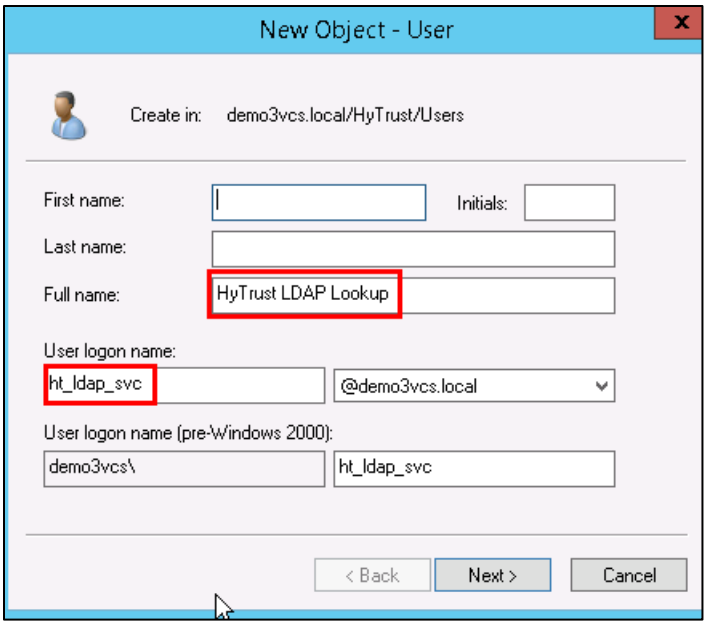


6. Add two users to the **Users** group. To do this, right-click on the **HyTrust/Users** organizational unit and select **New -> User**.

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

   Full name: **HyTrust LDAP Lookup**

   User logon name: **ht_ldap_svc**



8. Click **Next** to go to the user password screen. It asks you to establish a password and some password options for the user. Enter or verify these fields:

    a. Enter and confirm a password for the user. The password needs to have at least one upper case letter, otherwise the user will not be created. Note the password in the deployment spreadsheet.

    b. Uncheck this option: **User must change password at next logon**.

    c. Check this option: **Password never expires**.

    d. Click **Next**.

    e. Verify the information and finish.

9. The second user will be used as the service account when HTCC interacts with vCenter. You could use the **Administrator@vsphere.local** account, but best practice is to create a specific service account in AD and use that. Create the second user (in the same way as the first user) with the following values:

    Full name: **HyTrust VCenter svc account**

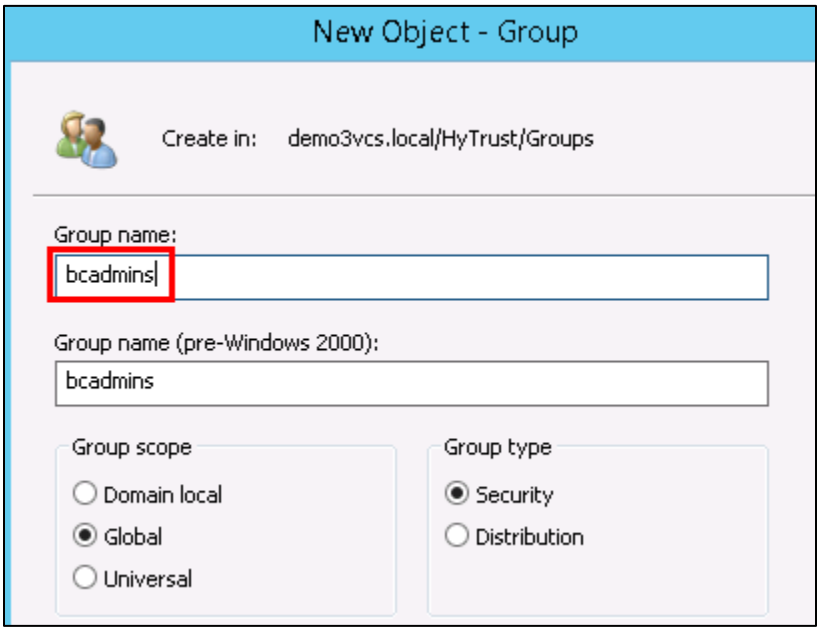
    User logon name: **ht_vcenter_svc**

    Ensure that the password never expires.

10. You will now create two subgroups under **Groups**.

a. First, right-click on the **Groups** organizational unit and select **New -> Group**.

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



c. Right-click again on the **Groups** organizational unit and select **New -> Group**.

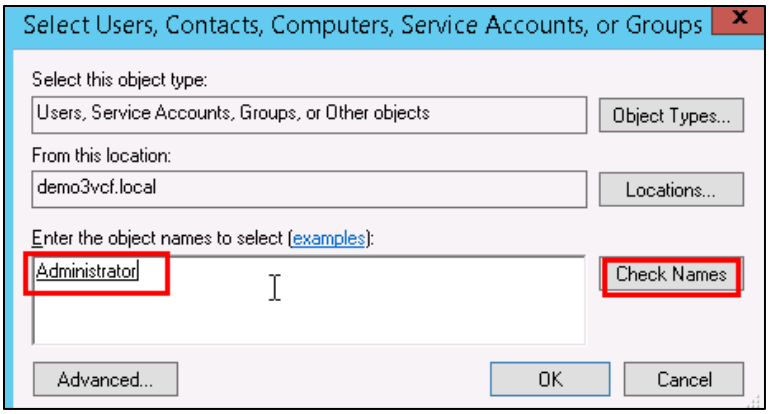
d. When prompted, enter a name for this group: **ht_superadmin_users** and press **OK**. Later, you will tell HTCC to use this group to specify administrative users of HTCC.

11. You will now add members to the **superadmin** group.

a. To do this, right-click on the **ht_superadmin_users** group, and select **Properties**.

b. In the pop-up window, select the **Members** tab, then click **Add**.

c. In the next pop-up screen, enter an object name **Administrator**, and click on **Check Names**. If no error is returned, click **OK**.



12. Close the AD control panel.

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

5.2.7 Join vCenter to the AD domain

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

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

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

   If the output indicates it's already joined, you can skip the rest of this section (5.2.7).
3. If it's not already joined, run the following command to join it:

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

   Example:

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

   Output:

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

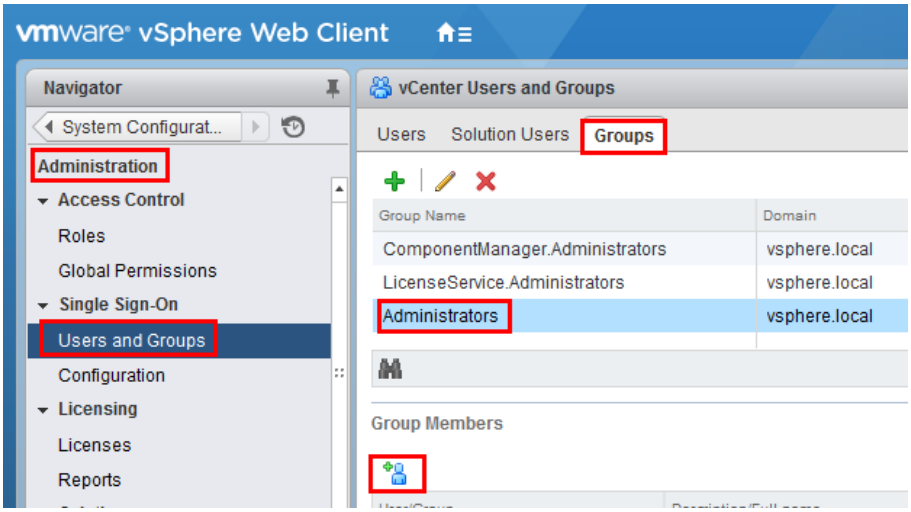
   Then reboot.
4. SSH into PSC again and verify that the join has succeeded by issuing the following command:

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

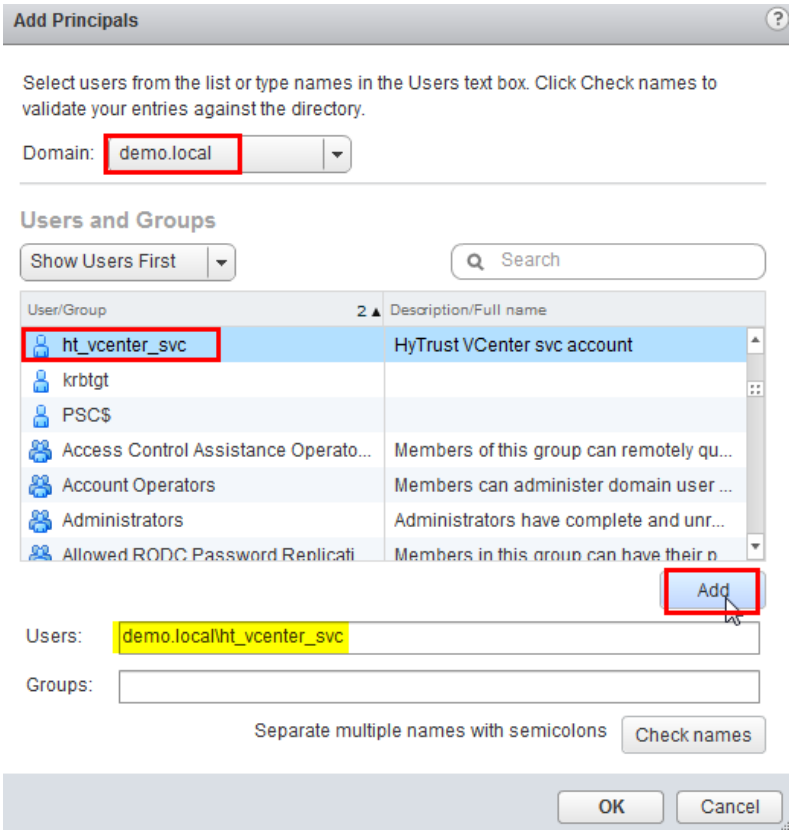
5.2.8 Add AD HyTrust-vCenter service user to vCenter as Administrator

This is for both the VCS and VCF instances.

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



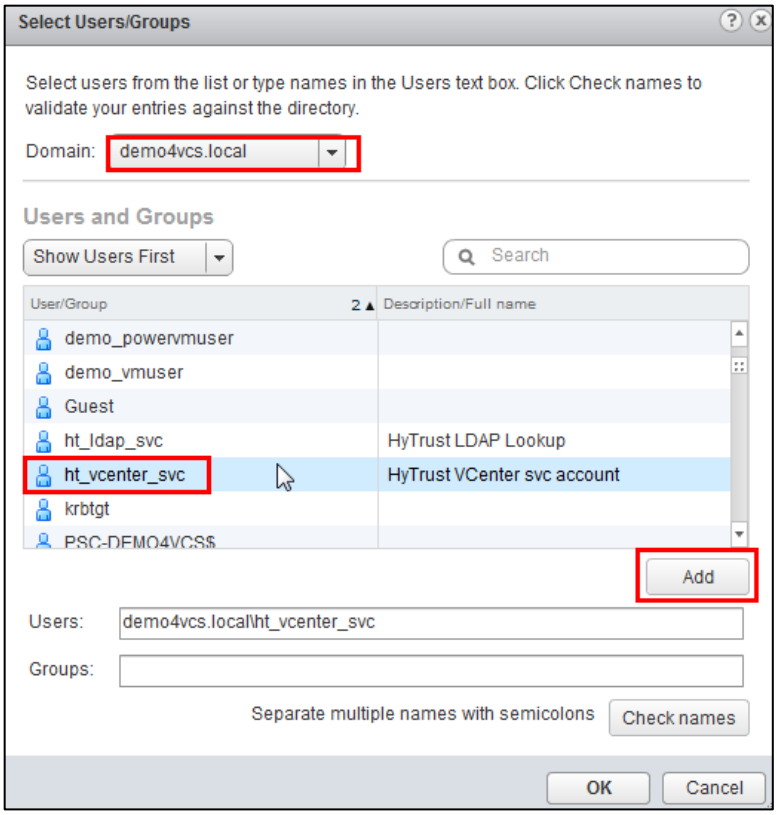
2. In the **Add Principals** panel, select the Windows AD Domain (**demo.local** in our example), scroll down and select the user **ht_vcenter_svc** user (that was created in Windows AD), and click on the **Add** button. That user should appear in the Users list. Then press the **OK** button.



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

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

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



5.2.10 Configure HTCC for AD authentication

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

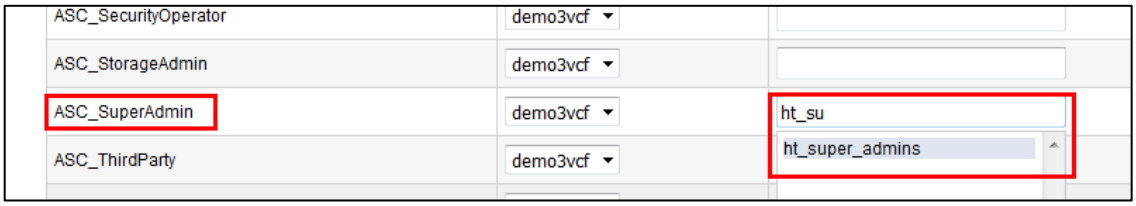
By default, HTCC is set to use a demo userid/password authentication. Once you change to AD authentication, you cannot revert back to the demo authentication.

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

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

To set up HTCC authentication, follow these steps:

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



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

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

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

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

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

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

Next, follow the directions at Enabling a Good Known Host, then Verifying and Updating Host Trust.

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

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

d. Verify that the PolicyTags have been provisioned. If the tag icon next to the host being provisioned is blue, then the PolicyTags assigned to the host are provisioned. If the tag icon is yellow, then the PolicyTags assigned to the host are not provisioned.

e. Note: If the provisioning process was not successful, you may have to clear the TPM once again and repeat the process.

f. After the PolicyTag provisioning is successful, you can remove the hosts from maintenance mode.

6 Intel Product Installation and Configuration Guide

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

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

7 RSA Product Installation and Configuration Guide

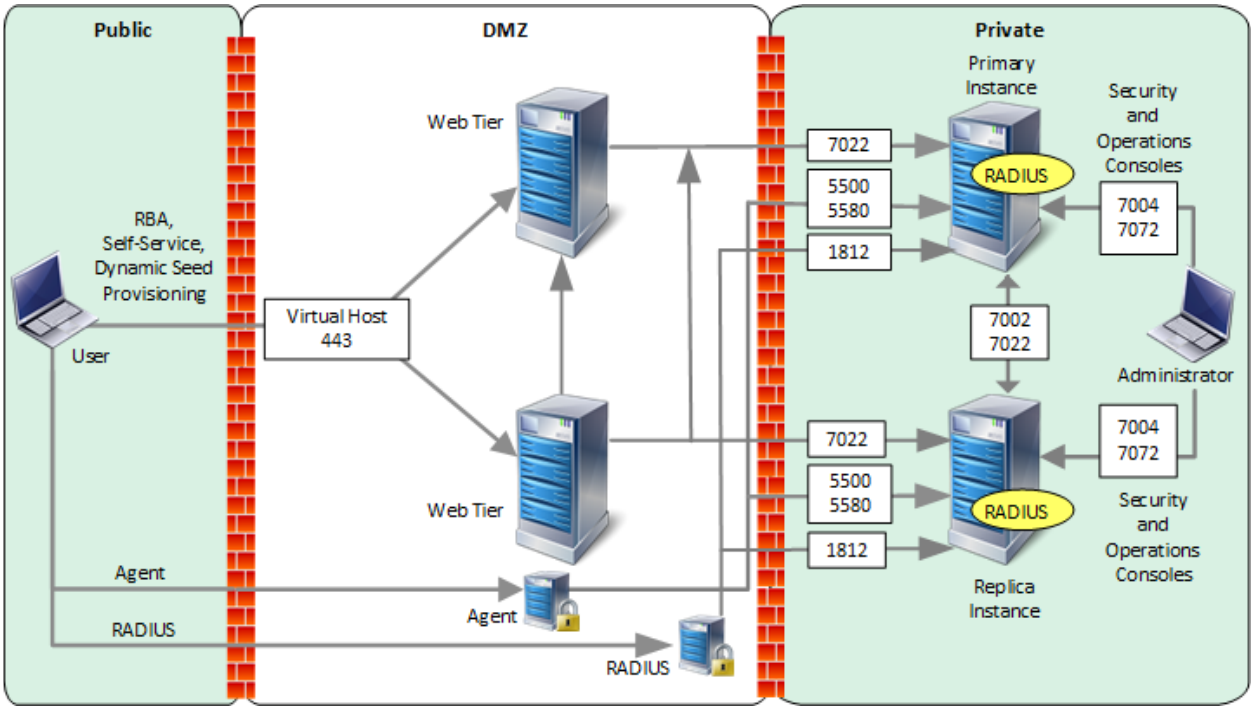
This section covers the installation and configuration of the RSA products used to build the example solution.

7.1 RSA SecurID

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

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

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**.

d. Enter **RSA Log Capture** as the name of the Role.

e. Choose **All Privileges** > **Global** > **Diagnostics** as the only privilege for this role.

2. Create a local ESXi user as follows:

a. From the Left navigation pane, click on the ESXI host, then click the **Users** or **Local Users & Groups** tab. The name of the tab depends on the credentials you used to log onto the ESXi host.

b. Right-click on the **Users** tab, then click **Add.**

c. Enter **rsa-vcenter-logs** in the **Login** field, and choose a strong password.

3. Assign the role to the local user as follows:

a. From the Left navigation pane, click on the ESXI host, then click the **Permissions** tab.

b. Right-click in the **Permissions** table, then click **Add Permission**.

c. In the dialog box, under the **Assigned Role** drop-down menu, choose **RSA Log Capture**.

d. Under **Users and Groups**, click **Add**.... The **Select Users and Groups** dialog box is displayed.

e. In the dialog box, leave the Domain value as (server), and select the **rsa-vcenter-logs** user.

f. Click **Add**, then click **OK**.

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

7.2.2 Configure the RSA NetWitness Log Collector for VMware Collection

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

8 VMware Product Installation and Configuration Guide

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

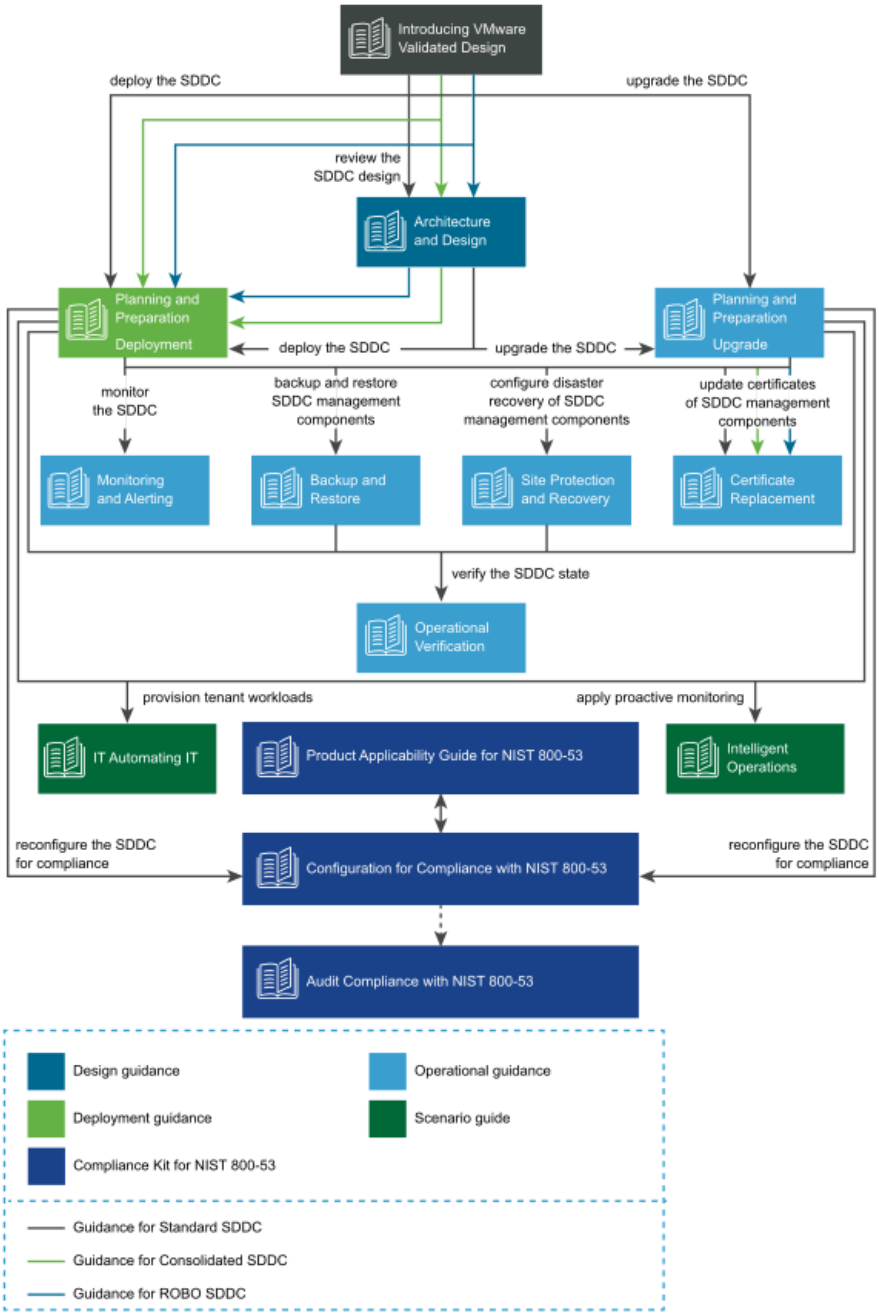
8.1 Prerequisites

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

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

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

Figure 8-1: Map of VVD Documentation



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

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

8.2 Installation and Configuration

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

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

8.3 Configuration Customization Supporting the Use Cases and Security Capabilities

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

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

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

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

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

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

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

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

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

iii. **Minimum Length** should be set to **15**.

iv. **Upper-case Characters** should be set to **1**.

v. **Lower-case Characters** should be set to **1**.

vi. **Numeric Characters** should be set to **1**.

vii. **Special Characters** should be set to **1.**

3. Configure the lockout policies.

    a. On the **Policies** tab, click **Lockout Policy** and click **Edit**.

    b. In the **Edit Lockout Policy** dialog box, for **Maximum Number of Failed Login Attempts**, enter **3**.

    c. For **Interval Between Failures**, enter **900**.

    d. For **Unlock Time**, enter **0** and then click **OK**.

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

1. In a web browser, log in to vCenter Server by using the vSphere Web Client.

2. Enable **Host Encryption Mode** on the **sfo01m01esx01.sfo01.rainpole.local** host.

    a. From the **Home** menu of the vSphere Web Client, select **Hosts and Clusters**.

    b. Under the **sfo01-m01dc data center**, select the **sfo01m01esx01.sfo01.rainpole.local** host and click the **Configure** tab.

    c. Under **System**, click **Security profile**.

    d. Under **Host Encryption Mode**, click **Edit**.

    e. In the **Set Encryption Mode** dialog box, from the **Encryption Mode** drop-down menu, select **Enabled** and click **OK**.

    f. Repeat the procedure for all remaining hosts in Region A.

3. Enable VM encryption on all the VMs and virtual disks.

    a. From the **Home** menu of the vSphere Web Client, select **VMs and Templates**.

    b. Under the **sfo01-m01dc data center**, expand the **sfo01-m01fd-bcdr** folder, right-click the **sfo01m01vc01 VM** and select **VM Policies**, then **Edit VM Storage Policies**.

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

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

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

1. Update the "Ciphers" directive with the following command:

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

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

```
service sshd restart
```

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

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

8.4 Operation, Monitoring, and Maintenance

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

8.4.1 Operation

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

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

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

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

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

8.4.2 Monitoring

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

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

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

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

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

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

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

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

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

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

8.4.3 Maintenance

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

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

SDDC Layer	Product Name	Product Version in VVD 4.3	Product Version in VVD 5.0.1	Operation Type
Operations Management	vRealize Suite Lifecycle Manager	1.2	2.0.0 Patch 2	Upgrade
	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 - Before you begin any upgrade process, review all the release notes.
1752 - Consider that the SDDC design and implementation may be affected by security features that
1753 are enabled. Ensure interoperability testing is performed before and after making security
1754 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.

- Perform a backup copy of your current certificates before you start the upgrade process. If you need to request a new certificate, ensure you follow the procedures in this document for VVD 4.3 and this document for VVD 5.1.

The following is a tip for updating the SDDC:

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

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

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

8.5 Product Configuration Overview

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

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

- VMware vRealize Automation 7.x Lighttpd
- VMware vRealize Automation 7.x SLES
- VMware vRealize Automation 7.x tc Server
- VMware vRealize Operations Manager 6.x Application
- VMware vRealize Operations Manager 6.x SLES
- VMware vRealize Operations Manager 6.x tc Server
- VMware vRealize – Cassandra

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

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

Appendix A Security Configuration Settings

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

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84401-9	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-84402-7	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-84403-5	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-84404-3	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	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84405-0	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-84406-8	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-84407-6	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-84408-4	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-84409-2	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	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84410-0	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-84411-8	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-84412-6	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-84413-4	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-84414-2	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	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84415-9	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-84416-7	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-84417-5	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-84418-3	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-84419-1	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	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84420-9	NIST800 53-VI-ESXi-CFG-00020	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 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.	aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc, aes256-cbc
CCE-84421-7	NIST800 53-VI-ESXi-CFG-00022	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Security.PasswordQualityControl` If Security.PasswordQualityControl is not set to "`similar=deny retry=3 min=disabled,disabled,disabled,disabled,15`", this is a finding.	similar=deny re-try=3 min=disa-bled,disabled,disa-bled,disabled,15
CCE-84422-5	NIST800 53-VI-ESXi-CFG-00028	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-VMHostFirewallException | Where {$_.Name -eq 'SSH Server' -and $_.Enabled -eq $true} \| Select Name,Enabled,@{N="AllIPEnabled";E={$_.ExtensionData.AllowedHosts.AllIP}}` If for an enabled service "`Allow connections from any IP address`" is selected, this is a finding.	AllIPEnabled: False
CCE-84423-3	NIST800 53-VI-ESXi-CFG-00030	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name UserVars.SuppressShellWarning` If UserVars.SuppressShellWarning is not set to 0, this is a finding.	0
CCE-84424-1	NIST800 53-VI-ESXi-	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command:	lockdownNormal

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
	CFG-00031			`Get-VMHost | Select Name,@{N="Lockdown";E={$_.Extensiondata.Config.LockdownMode}}` If Lockdown Mode is disabled, this is a finding. For environments that do not use vCenter server to manage ESXi, this is not applicable.	
CCE-84425-8	NIST800 53-VI-ESXi-CFG-00034	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Security.AccountLockFailures` If Security.AccountLockFailures is not set to 3, this is a finding.	3
CCE-84426-6	NIST800 53-VI-ESXi-CFG-00038	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeOut` If UserVars.ESXiShellInteractiveTimeOut is not set to 600, this is a finding.	600
CCE-84427-4	NIST800 53-VI-ESXi-CFG-00039	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name UserVars.ESXiShellTimeOut` If UserVars.ESXiShellTimeOut is not set to 600, this is a finding.	600
CCE-84428-2	NIST800 53-VI-ESXi-CFG-00043	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Net.BlockGuestBPDU` If Net.BlockGuestBPDU is not set to 1, this is a finding.	1
CCE-84429-0	NIST800 53-VI-ESXi-	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following commands:	TRUE

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
	CFG-00056			`$esxcli = Get-EsxCli` `$esxcli.system.coredump.network.get()` If there is no active core dump partition or the network core dump collector is not configured and enabled, this is a finding.	
CCE-84430-8	NIST800 53-VI-ESXi-CFG-00106	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHostFirewallDefaultPolicy` If the Incoming or Outgoing policies are True, this is a finding.	FALSE
CCE-84431-6	NIST800 53-VI-ESXi-CFG-00107	Enhanced	ESXi	Log in to the host and run the following command: `# ls -la /etc/ssh/keys-root/authorized_keys` If the *authorized_keys* file exists, this is a finding.	File should not exist
CCE-84432-4	NIST800 53-VI-ESXi-CFG-00108	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHostSnmp | Select *` or From a console or ssh session run the following command: `esxcli system snmp get` 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 `esxcli` command.	FALSE

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84433-2	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-84434-0	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-84435-7	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 {$_.Label -eq "SSH"}` If the ESXi SSH service is running, this is a finding.	Policy: Off and Running: False
CCE-84436-5	NIST800 53-VI-ESXi-CFG-00112	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-VMHostService | Where {$_.Label -eq "ESXi Shell"}` If the ESXi Shell service is running, this is a finding.	Policy: Off and Running: False
CCE-84437-3	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	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84438-1	NIST80053-VI-ESXi-CFG-00114	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-VMHostAuthentication` 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 Directory Services Type is not set to “Active Directory”, this is a finding.	sfo01.rainpole.local
CCE-84439-9	NIST80053-VI-ESXi-CFG-00115	Built-in	ESXi	From a PowerCLI command prompt, while connected to vCenter run the following command: `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}}` Verify if "`JoinADEnabled`" is "`True`“ then "`JoinDomainMethod`" should be "`FixedCAMConfigOption`". 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 vSphere Authentication Proxy is not used to join hosts to an Active Directory domain, this is a finding.	JoinADEnabled: True, JoinDomain-Method: Fixed-CAMConfigOption

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84440-7	NIST800 53-VI-ESXi-CFG-00116	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-VMHostAuthentication` 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 the Directory Services Type is not set to “Active Directory”, this is a finding.	sfo01.rainpole.local
CCE-84441-5	NIST800 53-VI-ESXi-CFG-00117	Built-in	ESXi	From a PowerCLI command prompt, while connected to vCenter run the following command: `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}}` Verify if "`JoinADEnabled`" is "`True`“ then "`JoinDomainMethod`" should be "`FixedCAMConfigOption`". 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 vSphere Authentication Proxy is not used to join hosts to an Active Directory domain, this is a finding.	sfo01.rainpole.local

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84442-3	NIST80053-VI-ESXi-CFG-00118	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-VMHostAuthentication` 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 Directory Services Type is not set to “Active Directory”, this is a finding.	sfo01.rainpole.local
CCE-84443-1	NIST80053-VI-ESXi-CFG-00119	Built-in	ESXi	From a PowerCLI command prompt, while connected to vCenter run the following command: `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}}` Verify if "`JoinADEnabled`" is "`True`“ then "`JoinDomainMethod`" should be "`FixedCAMConfigOption`". 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 vSphere Authentication Proxy is not used to join hosts to an Active Directory domain, this is a finding.	sfo01.rainpole.local

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84444-9	NIST800 53-VI-ESXi-CFG-00120	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-VMHostAuthentication` 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 Directory Services Type is not set to “Active Directory”, this is a finding.	sfo01.rainpole.local
CCE-84445-6	NIST800 53-VI-ESXi-CFG-00121	Built-in	ESXi	From a PowerCLI command prompt, while connected to vCenter run the following command: `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}}` Verify if "`JoinADEnabled`" is "`True`“ then "`JoinDomainMethod`" should be "`FixedCAMConfigOption`". 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 vSphere Authentication Proxy is not used to join hosts to an Active Directory domain, this is a finding.	sfo01.rainpole.local

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84446-4	NIST80053-VI-ESXi-CFG-00122	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Annotations.WelcomeMessage` 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.	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.

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84447-2	NIST80053-VI-ESXi-CFG-00123	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Config.Etc.issue` If the Config.Etc.issue setting (*/etc/issue* file) does not contain the logon banner exactly as shown in the parameter value, this is a finding.	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.

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84448-0	NIST80053-VI-ESXi-CFG-00124	Enhanced	ESXi	Connect via SSH and run the following command: `# grep -i "^Banner" /etc/ssh/sshd_config` If there is no output or the output is not exactly "`Banner /etc/issue`", this is a finding.	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.

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84449-8	NIST800 53-VI-ESXi-CFG-00125	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following script: `$vmhost = Get-VMHost \| Get-View` `$lockdown = Get-View $vmhost.ConfigManager.HostAccessManager` `$lockdown.QueryLockdownExceptions()` If the exception users list contains accounts that do not require special permissions, this is a finding. Note: This list is not intended for system administrator accounts but for special circumstances such as a service account.	Remove unnecessary users from the exception user list
CCE-84450-6	NIST800 53-VI-ESXi-CFG-00127	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Annotations.WelcomeMessage` 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.	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-84451-4	NIST800 53-VI-ESXi-CFG-00129	Enhanced	ESXi	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. 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. If the ESXi host does not have the latest patches, this is a finding. If the ESXi host is not on a supported release, this is a finding.	Apply latest patches and updates
CCE-84452-2	NIST800 53-VI-ESXi-CFG-00134	Enhanced	ESXi	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: `# sha1sum <filename>.iso` 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.	Compare the SHA1 sum output with the value posted on the VMware Web site. SHA1 hash should match.
CCE-84453-0	NIST800 53-VI-ESXi-CFG-00135	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logHost` 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	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84454-8	NIST800 53-VI-ESXi-CFG-00136	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logDir` If LocalLogOutputIsPersistent is not set to true, this is a finding.	[] /scratch/log
CCE-84455-5	NIST800 53-VI-ESXi-CFG-00137	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.plugins.hostsvc.esxAdminsGroup` 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-84456-3	NIST800 53-VI-ESXi-CFG-00138	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Mem.ShareForceSalting` If Mem.ShareForceSalting is not set to 2, this is a finding.	2
CCE-84457-1	NIST800 53-VI-ESXi-CFG-00139	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHostFirewallDefaultPolicy` If the Incoming or Outgoing policies are True, this is a finding.	N/A
CCE-84458-9	NIST800 53-VI-ESXi-	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logHost`	udp://sfo01vrli01.sfo01.rainpole.local:514

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
	CFG-00141			If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.	
CCE-84459-7	NIST800 53-VI-ESXi-CFG-00142	Enhanced	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.plugins.hostsvc.esxAdminsGroup` 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-84460-5	NIST800 53-VI-ESXi-CFG-00143	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logHost` If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.	udp://sfo01vrli01.sfo01.rainpole.local:514
CCE-84461-3	NIST800 53-VI-ESXi-CFG-00145	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-VMHostNTPServer` `Get-VMHost | Get-VMHostService | Where {$_.Label -eq "NTP Daemon"}` If the NTP service is not configured with authoritative DoD time sources and the service is not configured to start and stop with the host and is running, this is a finding.	ntp.lax01.rainpole.local, ntp.sfo01.rainpole.local
CCE-84462-1	NIST800 53-VI-ESXi-CFG-00157	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: `$esxcli = Get-EsxCli` `$esxcli.software.acceptance.get()` If the acceptance level is CommunitySupported, this is a finding.	PartnerSupported

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84463-9	NIST800 53-VI-ESXi-CFG-00158	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: `$esxcli = Get-EsxCli` `$esxcli.software.acceptance.get()` If the acceptance level is CommunitySupported, this is a finding.	PartnerSupported
CCE-84464-7	NIST800 53-VI-ESXi-CFG-00159	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: `$esxcli = Get-EsxCli` `$esxcli.software.acceptance.get()` If the acceptance level is CommunitySupported, this is a finding.	PartnerSupported
CCE-84465-4	NIST800 53-VI-ESXi-CFG-00160	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: `$esxcli = Get-EsxCli` `$esxcli.software.acceptance.get()` If the acceptance level is CommunitySupported, this is a finding.	PartnerSupported
CCE-84466-2	NIST800 53-VI-ESXi-CFG-00161	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: `Get-VDSwitch | Get-VDSecurityPolicy` `Get-VDPortGroup | Get-VDSecurityPolicy` If Forged Transmits is set to accept, this is a finding.	FALSE
CCE-84467-0	NIST800 53-VI-ESXi-CFG-00162	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: `Get-VDSwitch | Get-VDSecurityPolicy` `Get-VDPortGroup | Get-VDSecurityPolicy` If MAC Address Changes is set to accept, this is a finding.	FALSE

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84468-8	NIST800 53-VI-ESXi-CFG-00163	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name DCUI.Access` If DCUI.Access is not restricted to root, this is a finding. Note: This list is only for local user accounts and should only contain the root user.	root
CCE-84469-6	NIST800 53-VI-ESXi-CFG-00164	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logHost` If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.	udp://sfo01vrli01.sfo01.rainpole.lo-cal:514
CCE-84470-4	NIST800 53-VI-ESXi-CFG-00165	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Security.AccountUnlockTime` If Security.AccountUnlockTime is not set to 900, this is a finding.	900
CCE-84471-2	NIST800 53-VI-ESXi-CFG-00166	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.plugins.solo.enableMob` If Config.HostAgent.plugins.solo.enableMob is not set to false, this is a finding.	FALSE
CCE-84472-0	NIST800 53-VI-ESXi-CFG-00167	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.plugins.hostsvc.esxAdminsGroup` 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.	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-84473-8	NIST800 53-VI-ESXi-CFG-00168	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name UserVars.DcuiTimeOut` If UserVars.DcuiTimeOut is not set to 600, this is a finding.	600
CCE-84474-6	NIST800 53-VI-ESXi-CFG-00169	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Net.DVFilterBindIpAddress` If Net.DVFilterBindIpAddress is not blank and security appliances are not in use on the host, this is a finding.	""
CCE-84475-3	NIST800 53-VI-ESXi-CFG-00170	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logHost` If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.	udp://sfo01vrli01.sfo01.rainpole.local:514
CCE-84476-1	NIST800 53-VI-ESXi-CFG-00171	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name UserVars.DcuiTimeOut` If UserVars.DcuiTimeOut is not set to 600, this is a finding.	600
CCE-84477-9	NIST800 53-VI-ESXi-	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logHost` 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	Prod-uct	Audit Procedure	Recommended Parameter Value
	CFG-00172				
CCE-84478-7	NIST800 53-VI-ESXi-CFG-00173	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.plugins.hostsvc.esxAdminsGroup` 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 the Config.HostAgent.plugins.hostsvc.esxAdminsGroup keyword is set to “ESX Admins”, this is a finding.	ug-SDDC-Admins
CCE-84479-5	NIST800 53-VI-ESXi-CFG-00174	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logHost` If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.	udp://sfo01vrli01.sfo01.rainpole.local:514
CCE-84480-3	NIST800 53-VI-ESXi-CFG-00175	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.plugins.hostsvc.esxAdminsGroup` 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 ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84481-1	NIST800 53-VI-ESXi-CFG-00176	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logHost` If Syslog.global.logHost is not set to a site-specific syslog server, this is a finding.	udp://sfo01vrli01.sfo01.rainpole.local:514
CCE-84482-9	NIST800 53-VI-ESXi-CFG-00177	Built-in	ESXi	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. 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. 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. 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. For environments that do not use vCenter Server to manage ESXi, this is not applicable.	vMotion VMKernel Port group should be in a dedicated VLAN. The check for this will be unique per environment.
CCE-84483-7	NIST800 53-VI-ESXi-CFG-00178	Built-in	ESXi	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. 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. If the network segment is routed, except to networks where other management-related entities are located such as vCenter, this is a finding. If production virtual machine traffic is routed to this network, this is a finding.	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	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84484-5	NIST800 53-VI-ESXi-CFG-00179	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.log.level` If Config.HostAgent.log.level is not set to info, this is a finding. Note: Verbose logging level is acceptable for troubleshooting purposes.	info
CCE-84485-2	NIST800 53-VI-ESXi-CFG-00180	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.log.level` If Config.HostAgent.log.level is not set to info, this is a finding. Note: Verbose logging level is acceptable for troubleshooting purposes.	info
CCE-84486-0	NIST800 53-VI-ESXi-CFG-00181	Built-in	ESXi	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. If any VMkernel is used for more than one type of management traffic, this is a finding.	N/A
CCE-84487-8	NIST800 53-VI-ESXi-CFG-00182	Built-in	ESXi	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. If any system TCP/IP stack is configured and not in use by a VMkernel adapter, this is a finding.	N/A
CCE-84488-6	NIST800 53-VI-ESXi-CFG-00192	Built-in	ESXi	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-VMHostNTPServer` `Get-VMHost | Get-VMHostService | Where {$_.Label -eq "NTP Daemon"}` 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.	Policy :On and Running: True

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84489-4	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-84501-6	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-84502-4	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-84503-2	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-84504-0	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-84505-7	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-84506-5	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-84507-3	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-84508-1	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-84509-9	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-84510-7	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-84511-5	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-84512-3	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-84513-1	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-84514-9	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-84515-6	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-84516-4	NIST800 53-VI-NET-CFG-00296	Built-in	NSX	If the controller network is not deployed on a network that is not configured for or connected to other types of traffic, this is a finding.	Procedural (Dependent on Customer Configurations)
CCE-84517-2	NIST800 53-VI-NET-CFG-00297	Built-in	NSX	Run this Rest API call to get the properties of the controller node: `https://<nsxmgr>/api/2.0/vdn/controller/node` Response: `<controllerNodeConfig>` `<ipSecEnabled>true</ipSecEnabled >` `</controllerNodeConfig>` If ipSecEnabled is not true, this is a finding.	<ipSecEnabled>true</ipSecEnabled >

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84518-0	NIST800 53-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	NIST800 53-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	NIST800 53-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	NIST800 53-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	NIST800 53-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	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84523-0	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-84524-8	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-84525-5	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-84526-3	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-84527-1	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	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84528-9	NIST800 53-VI-NET-CFG-00316	Built-in	NSX	Log on to vSphere Web Client with credentials authorized for administration. Navigate and select **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-84529-7	NIST800 53-VI-NET-CFG-00317	Built-in	NSX	Log into NSX Manager with built-in administrator account “admin” and default manufacturer password “default”. If the NSX Manager accepts the default password, this is a finding.	Non-default pass-word
CCE-84530-5	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-84531-3	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-84532-1	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-84533-9	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-84534-7	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-84535-4	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-84536-2	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-84537-0	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	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84538-8	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-84539-6	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-84540-4	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-84541-2	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-84542-0	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-84301-1	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-84302-9	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-84303-7	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: `Get-VM | Where {$_.ExtensionData.Config.Hardware.Device.DeviceInfo.Label -match ""parallel""}` If a virtual machine has a parallel device present, this is a finding.	Disconnect unauthorized parallel devices
CCE-84304-5	NIST800 53-VI-ESXI-CFG-00066	Built-in	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: `Get-VM | Where {$_.ExtensionData.Config.Hardware.Device.DeviceInfo.Label -match ""serial""}` If a virtual machine has a serial device present, this is a finding.	Disconnect unauthorized serial devices
CCE-84305-2	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: `Get-VM | Get-UsbDevice` 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-84306-0	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name sched.mem.pshare.salt` If sched.mem.pshare.salt exists, this is a finding.	Remove the advanced setting sched.mem.pshare.salt
CCE-84307-8	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.copy.disable` If isolation.tools.copy.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84308-6	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.dnd.disable` If isolation.tools.dnd.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84309-4	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.setGUIOptions.enable` If isolation.tools.setGUIOptions.enable does not exist or is not set to false, this is a finding.	FALSE
CCE-84310-2	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.paste.disable` If isolation.tools.paste.disable does not exist or is not set to true, this is a finding.	TRUE

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84311-0	NIST800 53-VI-ESXI-CFG-00074	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.diskShrink.disable` If isolation.tools.diskShrink.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84312-8	NIST800 53-VI-ESXI-CFG-00075	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.diskWiper.disable` If isolation.tools.diskWiper.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84313-6	NIST800 53-VI-ESXI-CFG-00076	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.hgfsServerSet.disable` If isolation.tools.hgfsServerSet.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84314-4	NIST800 53-VI-ESXI-CFG-00077	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.ghi.autologon.disable` If isolation.tools.ghi.autologon.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84315-1	NIST800 53-VI-ESXI-CFG-00078	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.bios.bbs.disable` If isolation.bios.bbs.disable does not exist or is not set to true, this is a finding.	TRUE

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84316-9	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.getCreds.disable` If isolation.tools.getCreds.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84317-7	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.ghi.launchmenu.change` If isolation.tools.ghi.launchmenu.change does not exist or is not set to true, this is a finding.	TRUE
CCE-84318-5	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.memSchedFakeSampleStats.disable` If isolation.tools.memSchedFakeSampleStats.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84319-3	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.ghi.protocolhandler.info.disable` If isolation.tools.ghi.protocolhandler.info.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84320-1	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.ghi.host.shellAction.disable` If isolation.ghi.host.shellAction.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-84321-9	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.dispTopoRequest.disable` If isolation.tools.dispTopoRequest.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84322-7	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.trashFolderState.disable` If isolation.tools.trashFolderState.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84323-5	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.ghi.trayicon.disable` If isolation.tools.ghi.trayicon.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84324-3	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.unity.disable` If isolation.tools.unity.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84325-0	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.unityInterlockOperation.disable` If isolation.tools.unityInterlockOperation.disable does not exist or is not set to true, this is a finding.	TRUE

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84326-8	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.unity.push.update.disable` If isolation.tools.unity.push.update.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84327-6	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.unity.taskbar.disable` If isolation.tools.unity.taskbar.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84328-4	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.unityActive.disable` If isolation.tools.unityActive.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84329-2	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.unity.windowContents.disable` If isolation.tools.unity.windowContents.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84330-0	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.vmxDnDVersionGet.disable` 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-84331-8	NIST800 53-VI-ESXI-CFG-00094	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.guestDnDVersionSet.disable` If isolation.tools.guestDnDVersionSet.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84332-6	NIST800 53-VI-ESXI-CFG-00095	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.vixMessage.disable` If isolation.tools.vixMessage.disable does not exist or is not set to true, this is a finding.	TRUE
CCE-84333-4	NIST800 53-VI-ESXI-CFG-00096	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: `Get-VM "VM Name" | Get-AdvancedSetting -Name RemoteDisplay.maxConnections` If RemoteDisplay.maxConnections does not exist or is not set to 1, this is a finding.	1
CCE-84334-2	NIST800 53-VI-ESXI-CFG-00097	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: `Get-VM "VM Name" | Get-AdvancedSetting -Name RemoteDisplay.vnc.enabled` If RemoteDisplay.vnc.enabled does not exist or is not set to false, this is a finding.	FALSE
CCE-84335-9	NIST800 53-VI-ESXI-CFG-00098	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the ESXi host or vCenter server run the following command: `Get-VM "VM Name" | Get-AdvancedSetting -Name isolation.tools.autoInstall.disable` If isolation.tools.autoInstall.disable does not exist or is not set to true, this is a finding.	TRUE

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84336-7	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-84337-5	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-84338-3	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-84339-1	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-84340-9	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-84341-7	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: `Get-VM | Get-FloppyDrive | Select Parent, Name, ConnectionState` If a virtual machine has a floppy drive present, this is a finding.	Disconnect unauthorized floppy devices
CCE-84342-5	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: `Get-VM | Get-CDDrive | Where {$_.extensiondata.connectable.connected -eq $true} | Select Parent,Name` If a virtual machine has a CD/DVD drive connected other than temporarily, this is a finding.	Disconnect unauthorized CD/DVD drives
CCE-84343-3	NIST800 53-VI-ESXI-CFG-00185	Built-in	vCenter	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VirtualPortGroup | Select Name, VLanID` If any port group is configured with VLAN 4095 and is not documented as a needed exception, this is a finding.	Not 4095
CCE-84344-1	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-84345-8	NIST800 53-VI-NET-CFG-00341	Built-in	vCenter	If the vCenter server is not joined to an Active Directory domain and not configured for Single Sign-On Identity Source of the Active Directory domain, and Active Directory/CAC/PIV certificate-based accounts are not used for daily operations of the vCenter server, this is a finding.	Procedural (Dependent on Customer Configurations)

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84347-4	NIST800 53-VI-VC-CFG-00402	Built-in	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following command: `Get-VDPortgroup | select Name, VlanConfiguration` If any port group is configured with VLAN 4095 and is not documented as a needed exception, this is a finding.	Not 4095
CCE-84348-2	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-84349-0	NIST800 53-VI-VC-CFG-00404	Built-in	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following command: `Get-AdvancedSetting -Entity <vcenter server name> -Name config.log.level` If the level is not set to info, this is a finding.	info
CCE-84350-8	NIST800 53-VI-VC-CFG-00405	Built-in	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following commands: `Get-VDSwitch | Get-VDSecurityPolicy` `Get-VDPortgroup | Get-VDSecurityPolicy` If the Promiscuous Mode policy is set to accept, this is a finding.	reject
CCE-84351-6	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-84352-4	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	Prod-uct	Audit Procedure	Recommended Parameter Value
	VC-CFG-00407			`Get-VDSwitch | Get-VDSecurityPolicy` `Get-VDPortgroup | Get-VDSecurityPolicy` If the MAC Address Changes policy is set to accept, this is a finding.	
CCE-84353-2	NIST800 53-VI-VC-CFG-00408	Built-in	vCenter	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-84354-0	NIST800 53-VI-VC-CFG-00409	Built-in	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following command: `Get-VDSwitch | select Name,@{N="NIOC Enabled";E={$_.ExtensionData.config.NetworkResourceManagementEnabled}}` If Network I/O Control is disabled, this is a finding.	enabled
CCE-84355-7	NIST800 53-VI-VC-CFG-00410	Enhanced	vCenter	From the vSphere Web Client go to **Administration** >> **Single Sign-On** >> **Configuration** >> **Policies** >> **Password Policy**. If the Minimum Length is not set to at least 15, this is a finding.	15
CCE-84356-5	NIST800 53-VI-VC-CFG-00411	Enhanced	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following commands: `$vds = Get-VDSwitch` `$vds.ExtensionData.Config.HealthCheckConfig` If the health check feature is enabled on distributed switches and is not on temporarily for troubleshooting purposes, this is a finding.	FALSE
CCE-84357-3	NIST800 53-VI-VC-CFG-00412	Enhanced	vCenter	From the vSphere Client, select the vCenter server at the top of the hierarchy and go to **Alarms** >> **Definitions**. or From a PowerCLI command prompt, while connected to the vCenter server run the following command:	Procedural

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
				`Get-AlarmDefinition | Where {$_.ExtensionData.Info.Expression.Expression.EventTypeId -eq "vim.event.PermissionUpdatedEvent"} \| Select Name,Enabled,@{N="EventTypeId";E={$_.ExtensionData.Info.Expression.Expression.EventTypeId}}` If there is not an alarm created to alert on permission update events, this is a finding.	
CCE-84358-1	NIST800 53-VI-VC-CFG-00413	Built-in	vCenter	From the vSphere Web Client go to **Administration** >> **Single Sign-On** >> **Configuration** >> **Policies** >> **Password Policy**. If Lower-Case Characters is not set to at least 1, this is a finding.	1
CCE-84359-9	NIST800 53-VI-VC-CFG-00414	Enhanced	vCenter	From the vSphere Client, select the vCenter server at the top of the hierarchy and go to **Alarms** >> **Definitions**. or From a PowerCLI command prompt, while connected to the vCenter server run the following command: `Get-AlarmDefinition | Where {$_.ExtensionData.Info.Expression.Expression.EventTypeId -eq "vim.event.PermissionAddedEvent"} \| Select Name,Enabled,@{N="EventTypeId";E={$_.ExtensionData.Info.Expression.Expression.EventTypeId}}` If there is not an alarm created to alert on permission addition events, this is a finding.	Procedural
CCE-84360-7	NIST800 53-VI-VC-CFG-00415	Built-in	vCenter	From the vSphere Web Client, go to **Administration** >> **Access Control** >> **Roles**. or From a PowerCLI command prompt, while connected to the vCenter server run the following command: `Get-VIPermission | Sort Role | Select Role,Principal,Entity,Propagate,IsGroup | FT -Auto` Application service account and user required privileges should be documented. If any user or service account has more privileges than required, this is a finding.	Procedural (Dependent on Customer Configurations)

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84361-5	NIST800 53-VI-VC-CFG-00416	Enhanced	vCenter	From the vSphere Client, select the vCenter server at the top of the hierarchy and go to **Alarms** >> **Definitions**. or From a PowerCLI command prompt, while connected to the vCenter server run the following command: `Get-AlarmDefinition | Where {$_.ExtensionData.Info.Expression.Expression.EventTypeId -eq "vim.event.PermissionRemovedEvent"} \| Select Name,Enabled,@{N="EventTypeId";E={$_.ExtensionData.Info.Expression.Expression.EventTypeId}}` If there is not an alarm to alert on permission deletion events, this is a finding.	Procedural
CCE-84362-3	NIST800 53-VI-VC-CFG-00417	Built-in	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following command: `Get-VDPortgroup | Select Name,VirtualSwitch,@{N="NetFlowEnabled";E={$_.Extensiondata.Config.defaultPortConfig.ipfixEnabled.Value}}` If NetFlow is configured and the collector IP is not known and is not enabled temporarily for troubleshooting purposes, this is a finding.	Known Ips
CCE-84363-1	NIST800 53-VI-VC-CFG-00418	Enhanced	vCenter	If no clusters are enabled for VSAN, this is not applicable. From the vSphere Web Client go to **Host and Clusters** >> Select a vCenter Server >> **Configure** >> **vSAN** >> **Internet Connectivity** >> **Status**. If a proxy is not configured, this is a finding.	Procedural
CCE-84364-9	NIST800 53-VI-VC-CFG-00419	Built-in	vCenter	From a PowerCLI command prompt, while connected to the vCenter server run the following command: `Get-VIPermission | Sort Role | Select Role,Principal,Entity,Propagate,IsGroup | FT -Auto` Application service account and user required privileges should be documented. If any user or service account has more privileges than required, this is a finding.	Procedural (Dependent on Customer Configurations)

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84365-6	NIST800 53-VI-VC-CFG-00420	Built-in	vCenter	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. or From a PowerCLI command prompt, while connected to the vCenter server run the following command: `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"` `}` If VSAN is enabled and the datastore is named "vsanDatastore", this is a finding.	No name with "vsanDatastore"
CCE-84366-4	NIST800 53-VI-VC-CFG-00421	Enhanced	vCenter	From the vSphere Web Client, go to **Administration** >> **Single Sign-On** >> **Configuration** >> **Policies** >> **Password Policy**. If Maximum Lifetime is not set to 60, this is a finding.	60
CCE-84367-2	NIST800 53-VI-VC-CFG-00422	Enhanced	vCenter	On the system where vCenter is installed, locate the *webclient.properties* file. */etc/vmware/vsphere-client/* and */etc/vmware/vsphere-ui/* If session.timeout is not set to 10 (minutes), this is a finding.	10
CCE-84368-0	NIST800 53-VI-VC-CFG-00427	Enhanced	vCenter	`Get-AdvancedSetting -Entity <vcenter server name> -Name config.vpxd.hostPasswordLength`	32

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84369-8	NIST800 53-VI-VC-CFG-00428	Built-in	vCenter	From the vSphere Web Client, go to **vCenter Inventory Lists** >> **vCenter Servers** >> Select your vCenter Server >> **Settings** >> **Advanced System Settings**. or From a PowerCLI command prompt, while connected to the vCenter server run the following command: `Get-AdvancedSetting -Entity <vcenter server name> -Name VirtualCenter.VimPasswordExpirationInDays` If VirtualCenter.VimPasswordExpirationInDays is set to a value other than 30 or does not exist, this is a finding.	FALSE
CCE-84370-6	NIST800 53-VI-VC-CFG-00429	Built-in	vCenter	Check the following conditions: 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. 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". If "Direct connection to Internet" is configured, this is a finding. If all of the above conditions are not met, this is a finding.	Procedural
CCE-84371-4	NIST800 53-VI-VC-CFG-00432	Built-in	vCenter	From the vSphere Web Client, go to **Administration** >> **Single Sign-On** >> **Configuration** >> **Policies** >> **Password Policy**. If Special Characters is not set to at least 1, this is a finding.	1
CCE-84372-2	NIST800 53-VI-	Built-in	vCenter	From the vSphere Web Client, go to **Administration** >> **Single Sign-On** >> **Configuration** >> **Policies** >> **Password Policy**. If Numeric Characters is not set to at least 1, this is a finding.	1

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
	VC-CFG-00433				
CCE-84373-0	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-84374-8	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-84375-5	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-84376-3	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: `Get-AdvancedSetting -Entity <vcenter server name> -Name config.nfc.useSSL` If config.nfc.useSSL is not set to true, this is a finding.	TRUE
CCE-84377-1	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	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84378-9	NIST800 53-VI-VC-CFG-00440	Enhanced	vCenter	From the vSphere Web Client, go to **Networking** >> Select a distributed port group >> **Manage** >> **Settings** >> **Properties**. View the Override port policies. or From a PowerCLI command prompt, while connected to the vCenter server run the following command: `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` 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. This does not apply to the reset port configuration on disconnect policy. If any port level overrides are enabled and not documented, this is a finding.	disabled
CCE-84379-7	NIST800 53-VI-VC-CFG-00442	Enhanced	vCenter	From the vSphere Client, select the vCenter server at the top of the hierarchy and go to **Alarms** >> **Definitions**. or	Enabled

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
				From a PowerCLI command prompt, while connected to the vCenter server run the following command: `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}}` If there is no alarm created to alert if an ESXi host can no longer reach its syslog server, this is a finding.	
CCE-84380-5	NIST800 53-VI-VC-CFG-00445	Built-in	vCenter	If IP-based storage is not used, this is not applicable. 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. From the vSphere Client, select **Networks** >> **Distributed Port Groups** and review the VLANs associated with any IP-based storage VMkernels. If any IP-based storage networks are not isolated from other traffic types, this is a finding.	Unique IP Addresses
CCE-84381-3	NIST800 53-VI-VC-CFG-00447	Built-in	vCenter	Log in to the vCenter server and view the local administrators group membership. If the local administrators group contains users and/or groups that are not vCenter Administrators such as “Domain Admins”, this is a finding.	Only necessary users and groups
CCE-84382-1	NIST800 53-VI-VC-CFG-00450	Built-in	vCenter	From the vSphere Client, go to **Home** >> **Networking**. Select a distributed port group, click **Edit**, then go to **Security**. or From a PowerCLI command prompt, while connected to the vCenter server run the following commands: `Get-VDSwitch | Get-VDSecurityPolicy` `Get-VDPortgroup | ?{$_.IsUplink -eq $false} | Get-VDSecurityPolicy` If the Forged Transmits policy is set to accept for a non-uplink port, this is a finding.	reject

CCE ID	Configuration(s)	Built-In/ Enhanced	Product	Audit Procedure	Recommended Parameter Value
CCE-84383-9	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-84384-7	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-84385-4	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name svga.vgaonly` If svga.vgaonly does not exist or is not set to false, this is a finding.	TRUE
CCE-84386-2	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: `Get-VM "VM Name" | Get-AdvancedSetting -Name pciPassthru*.present` If pciPassthru*.present does not exist or is not set to false, this is a finding.	FALSE
CCE-84601-4	NIST800 53-VI-Storage-SDS-CFG-00178	Enhanced	vSAN	From a PowerCLI command prompt, while connected to the vCenter server run the following command: `Get-VIPermission | Where {$_.Role -eq "Admin"} | Select Role,Principal,Entity,Propagate,IsGroup | FT -Auto` If there are any users other than Solution Users with the Administrator role that are not explicitly designated for cryptographic operations, this is a finding.	No Cryptography Administrator
CCE-84602-2	NIST800 53-VI-Storage-SDS-	Built-in	vSAN	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: `Get-VMHost | Get-VMHostNTPServer` `Get-VMHost | Get-VMHostService | Where {$_.Label -eq "NTP Daemon"}`	Correct date and timestamp

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	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	NIST800 53-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	NIST800 53-VI-Storage-SDS-CFG-00182	Built-in	vSAN	From a PowerCLI command prompt, while connected to the ESXi host run the following command: `Get-VMHost | Get-AdvancedSetting -Name UserVars.HostClientSessionTimeout` If UserVars.HostClientSessionTimeout is not set to 900, this is a finding.	900
CCE-84605-5	NIST800 53-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	NIST800 53-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 Up-grades

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

CCE ID	Configuration(s)	Built-In/ Enhanced	Prod-uct	Audit Procedure	Recommended Parameter Value
CCE-84611-3	NIST800 53-VI-Storage-SDS-CFG-00179	Enhanced	vSAN	From a PowerCLI command prompt, while connected to the ESXi host run the following commands: `$esxcli = Get-EsxCli` `$esxcli.system.coredump.network.get()` If there is no active core dump partition or the network core dump collector is not configured and enabled, this is a finding.	TRUE
CCE-84612-1	NIST800 53-VI-Storage-SDS-CFG-00186	Enhanced	vSAN	Make sure you have sufficient capacity in the management vSAN cluster for the management virtual machines. If you do not have sufficient capacity, this is a finding.	Procedural

1799

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

Appendix C Glossary

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

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 *trusted pool*.