VCFT1616LV

Hardening and Securing VMware Cloud Foundation

A Multi-Layered Approach

Bob Plankers
Security & Compliance Engineer, Broadcom

#vmwareexplore #VCFT1616LV

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Disclaimer

- Certain information in this presentation may outline Broadcom's general product direction.
- This presentation shall not serve to (i) affect the rights and/or obligations of Broadcom or its licensees under any existing or future license agreement or services agreement relating to any Broadcom software product; or (ii) amend any product documentation or specifications for any Broadcom software product.
- This presentation is based on current information and resource allocations and is subject to change or withdrawal by Broadcom at any time without notice.
- The development, release and timing of any features or functionality described in this presentation remain at Broadcom's sole discretion.
- Notwithstanding anything in this presentation to the contrary, upon the general availability of any future Broadcom product release referenced in this presentation, Broadcom may make such release available to new licensees in the form of a regularly scheduled major product release.
- Such release may be made available to licensees of the product who are active subscribers to Broadcom maintenance and support, on a when and if-available basis.
- The information in this presentation is not deemed to be incorporated into any contract.

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

CIA Triad: **Core Tenets** of Information Security

Confidentiality

Protecting systems & data from unauthorized people & groups

Integrity

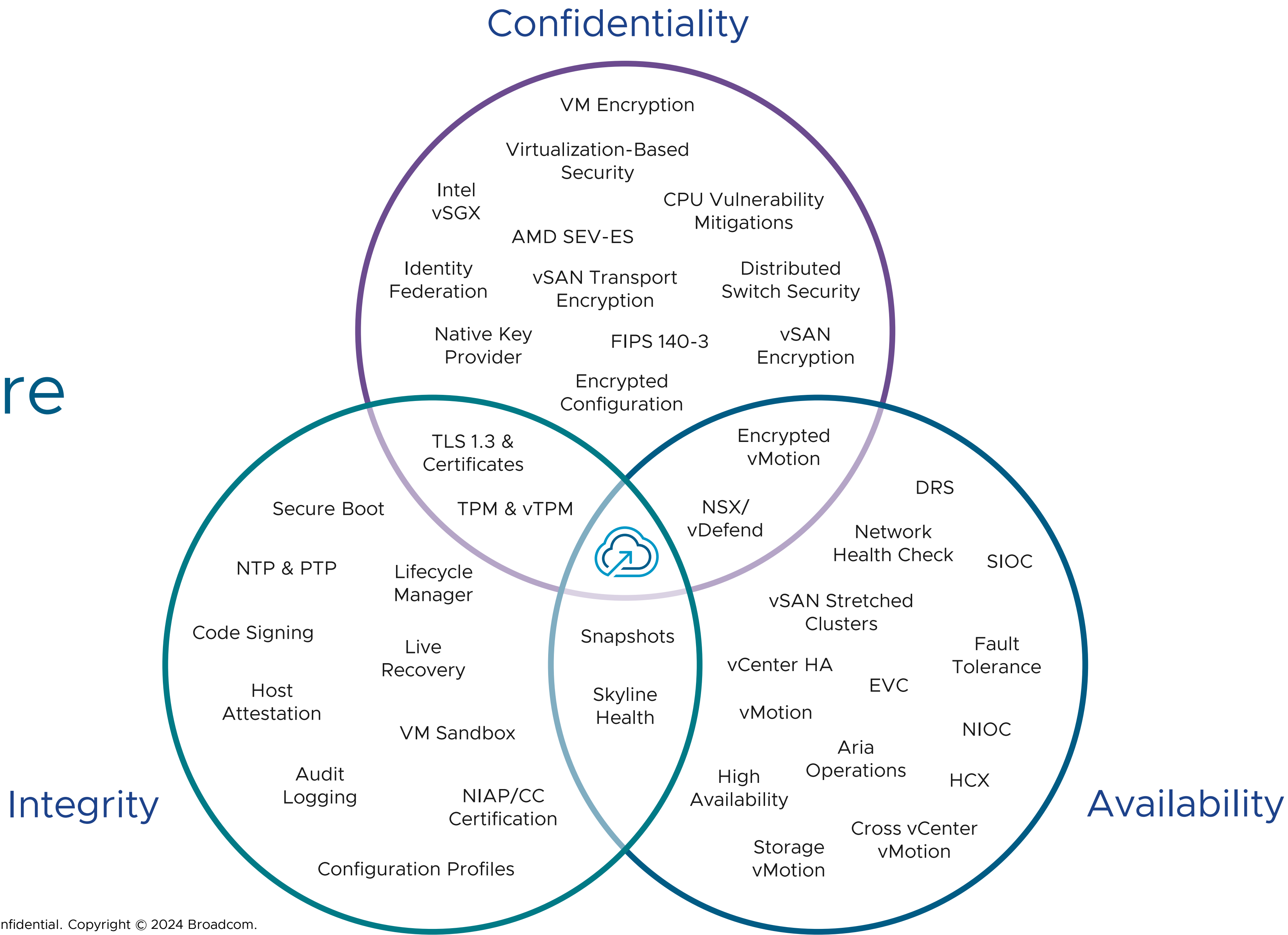
Preventing modification of data by unauthorized groups & systems

Availability

Ensuring that data is available to authorized parties when needed

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Every Feature is a Security Feature



Confidentiality

VM Encryption

Virtualization-Based Security

Intel vSGX

CPU Vulnerability Mitigations

AMD SEV-ES

Identity Federation

vSAN Transport Encryption

Distributed Switch Security

Native Key Provider

FIPS 140-3

vSAN Encryption

Encrypted Configuration

TLS 1.3 & Certificates

TPM & vTPM

Encrypted vMotion

NSX/ vDefend

Integrity

Secure Boot

NTP & PTP

Lifecycle Manager

Code Signing

Live Recovery

Host Attestation

VM Sandbox

Audit Logging

NIAP/CC Certification

Configuration Profiles

Snapshots

Skyline Health

Availability

DRS

Network Health Check

SIOC

vSAN Stretched Clusters

Fault Tolerance

vCenter HA

EVC

vMotion

NIOC

Aria Operations

High Availability

HCX

Cross vCenter vMotion

Storage vMotion

EXPLORE

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Introduction

Designing Hardened Systems

What is “Hardening?”

Designing Hardened Systems

1

Requirements

2

Threats

3

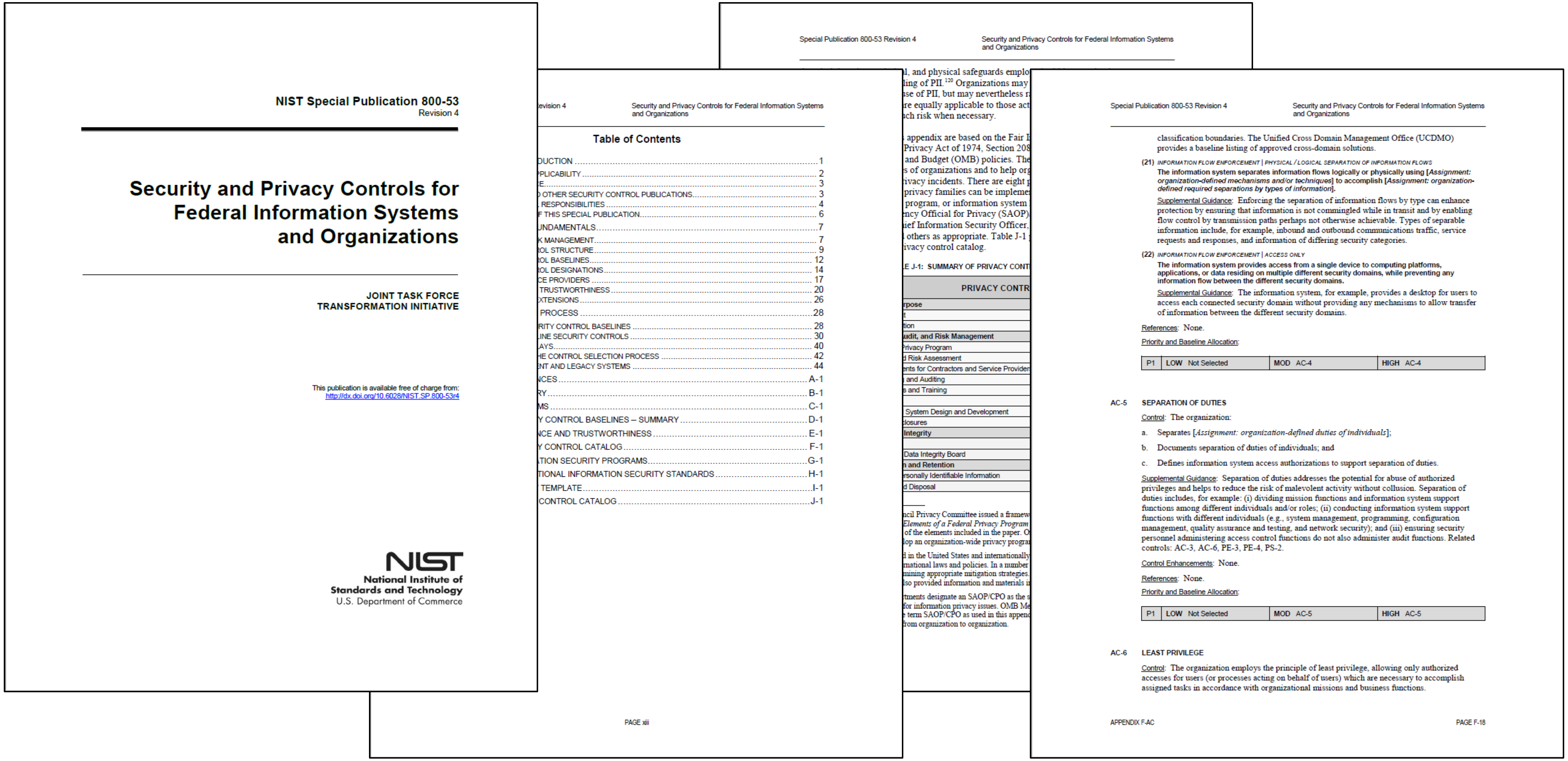
Technical Controls

4

System Design

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Regulatory Compliance Requirements?



NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

---

evision 4 Security and Privacy Controls for Federal Information Systems and Organizations

Table of Contents

DUCTION 1
PLICABILITY 2
E........ 3
OTHER SECURITY CONTROL PUBLICATIONS........ 3
RESPONSIBILITIES 4
F THIS SPECIAL PUBLICATION........ 6
UNDAMENTALS........ 7
K MANAGEMENT........ 7
OL STRUCTURE........ 9
OL BASELINES........ 12
OL DESIGNATIONS........ 14
CE PROVIDERS 17
TRUSTWORTHINESS 20
XTENSIONS........ 26
PROCESS 28
RITY CONTROL BASELINES 28
LINE SECURITY CONTROLS 30
AYS........ 40
HE CONTROL SELECTION PROCESS 42
NT AND LEGACY SYSTEMS 44
NCES A-1
RY........ B-1
MS C-1
Y CONTROL BASELINES – SUMMARY D-1
NCE AND TRUSTWORTHINESS E-1
Y CONTROL CATALOG F-1
TION SECURITY PROGRAMS........ G-1
TIONAL INFORMATION SECURITY STANDARDS H-1
TEMPLATE........ I-1
CONTROL CATALOG J-1

PAGE xiii

Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations

l, and physical safeguards emplo
ling of PII.[120] Organizations may
se of PII, but may nevertheless r
re equally applicable to those act
ch risk when necessary.

appendix are based on the Fair I
Privacy Act of 1974, Section 208
and Budget (OMB) policies. The
s of organizations and to help org
ivacy incidents. There are eight p
privacy families can be implemen
program, or information system
ncy Official for Privacy (SAOP),
ief Information Security Officer,
others as appropriate. Table J-1
ivacy control catalog.

E J-1: SUMMARY OF PRIVACY CONT

PRIVACY CONTR
rpose
t
tion
udit, and Risk Management
rivacy Program
d Risk Assessment
ents for Contractors and Service Provider
and Auditing
s and Training
System Design and Development
closures
Integrity
Data Integrity Board
n and Retention
rsonally Identifiable Information
d Disposal

---

ncil Privacy Committee issued a framew
Elements of a Federal Privacy Program
of the elements included in the paper. O
lop an organization-wide privacy progra

d in the United States and internationally
rnational laws and policies. In a number
mining appropriate mitigation strategies.
lso provided information and materials i

tments designate an SAOP/CPO as the s
for information privacy issues. OMB Me
term SAOP/CPO as used in this append
from organization to organization.

Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations

classification boundaries. The Unified Cross Domain Management Office (UCDMO) provides a baseline listing of approved cross-domain solutions.

(21) INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS

The information system separates information flows logically or physically using [*Assignment: organization-defined mechanisms and/or techniques*] to accomplish [*Assignment: organization-defined required separations by types of information*].

Supplemental Guidance: Enforcing the separation of information flows by type can enhance protection by ensuring that information is not commingled while in transit and by enabling flow control by transmission paths perhaps not otherwise achievable. Types of separable information include, for example, inbound and outbound communications traffic, service requests and responses, and information of differing security categories.

(22) INFORMATION FLOW ENFORCEMENT | ACCESS ONLY

The information system provides access from a single device to computing platforms, applications, or data residing on multiple different security domains, while preventing any information flow between the different security domains.

Supplemental Guidance: The information system, for example, provides a desktop for users to access each connected security domain without providing any mechanisms to allow transfer of information between the different security domains.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-4	HIGH AC-4

AC-5 SEPARATION OF DUTIES

Control: The organization:

a. Separates [*Assignment: organization-defined duties of individuals*];
b. Documents separation of duties of individuals; and
c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5

AC-6 LEAST PRIVILEGE

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

APPENDIX F-AC PAGE F-18

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

RPO & RTO?

Encryption?

Access Requirements?

Ability to Grow?

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

FY22 RISK AND VULNERABILITY ASSESSMENTS (RVA) RESULTS

MITRE ATT&CK™ TACTICS AND TECHNIQUES

The percent noted for each technique represents the success rate for that technique across 121 RVA assessments.

Mitigations reference CISA Cyber Performance Goals (CPGs). CPGs are a prioritized subset of IT and OT cybersecurity practices aimed at meaningfully reducing risks. CPGs are applicable across all Critical Infrastructure sectors.

UNITED STATES COAST GUARD CYBER COMMAND

FY22 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

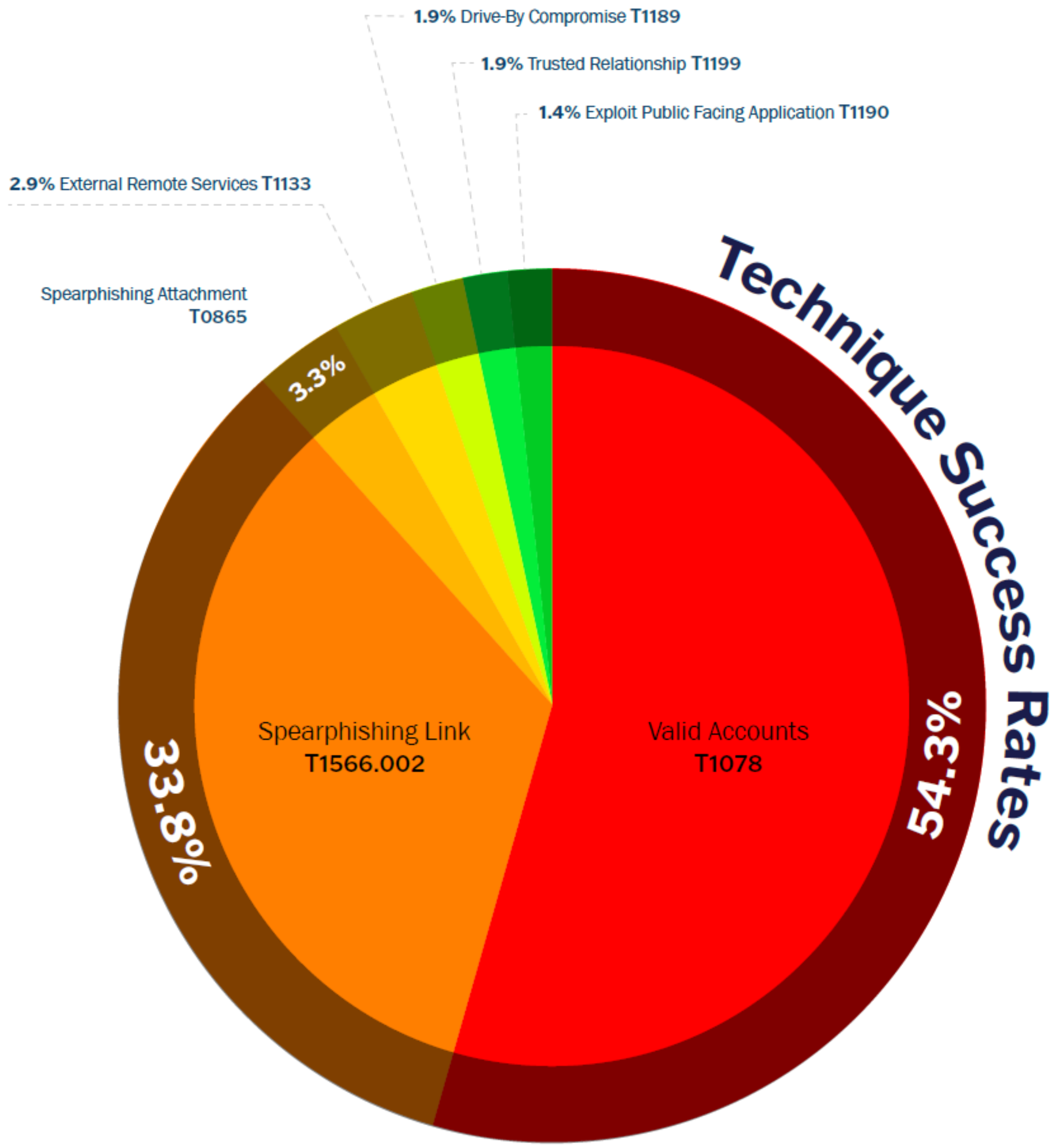
Initial Access

Threat actors attempt to obtain unauthorized initial access into a victim's network. Actors use techniques, such as valid accounts or spearphishing links, to gain this access. After obtaining initial access, actors can then execute other techniques to move about the network.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following Cyber Performance Goals (cisa.gov/cpg):

CPG 1.E Mitigating Known Vulnerabilities
CPG 2.A Changing Default Passwords
CPG 2.H Phishing-Resistant Multifactor Authentication
CPG 2.M Email Security
CPG 2.N Disable Macros by Default
CPG 2.W No Exploitable Services on the Internet



Shodan Maps Images Monitor Developer More...

SHODAN Explore Pricing

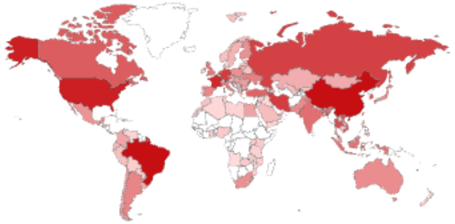
ESXi

Login

TOTAL RESULTS

19,411

TOP COUNTRIES



Brazil	**2,280**
China	**2,270**
United States	**1,716**
France	**1,458**
Germany	**995**

More...

TOP PORTS

View Report Browse Images View on Map

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using **InternetDB**

" + ID_EESX_Welcome + "

2023-08-03T02:34:10.805397

51.254.197.75
ns3044574.ip-51-254-197.eu
OVH SAS
France, Lille

eol-product

SSL Certificate

Issued By:
|- Organization:
VMware Installer

Issued To:
|- Common Name:
ns3044574.ip-51-254-197.eu

|- Organization:
VMware, Inc

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Date: Thu, 3 Aug 2023 02:34:10 GMT
Connection: Keep-Alive
Content-Type: text/html
X-Frame-Options: DENY
Content-Length: 5426


VMware ESXi:
  Full Name: VMware ESXi 6.0.0 build-3620759
  Name: VMware ESXi
  Version: 6.0.0
  Build: 3620759
  OS Type: vmnix-x86
  Product Line...
```

46.245.68.178

2023-08-03T03:50:48.592401

FY22 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Persistence

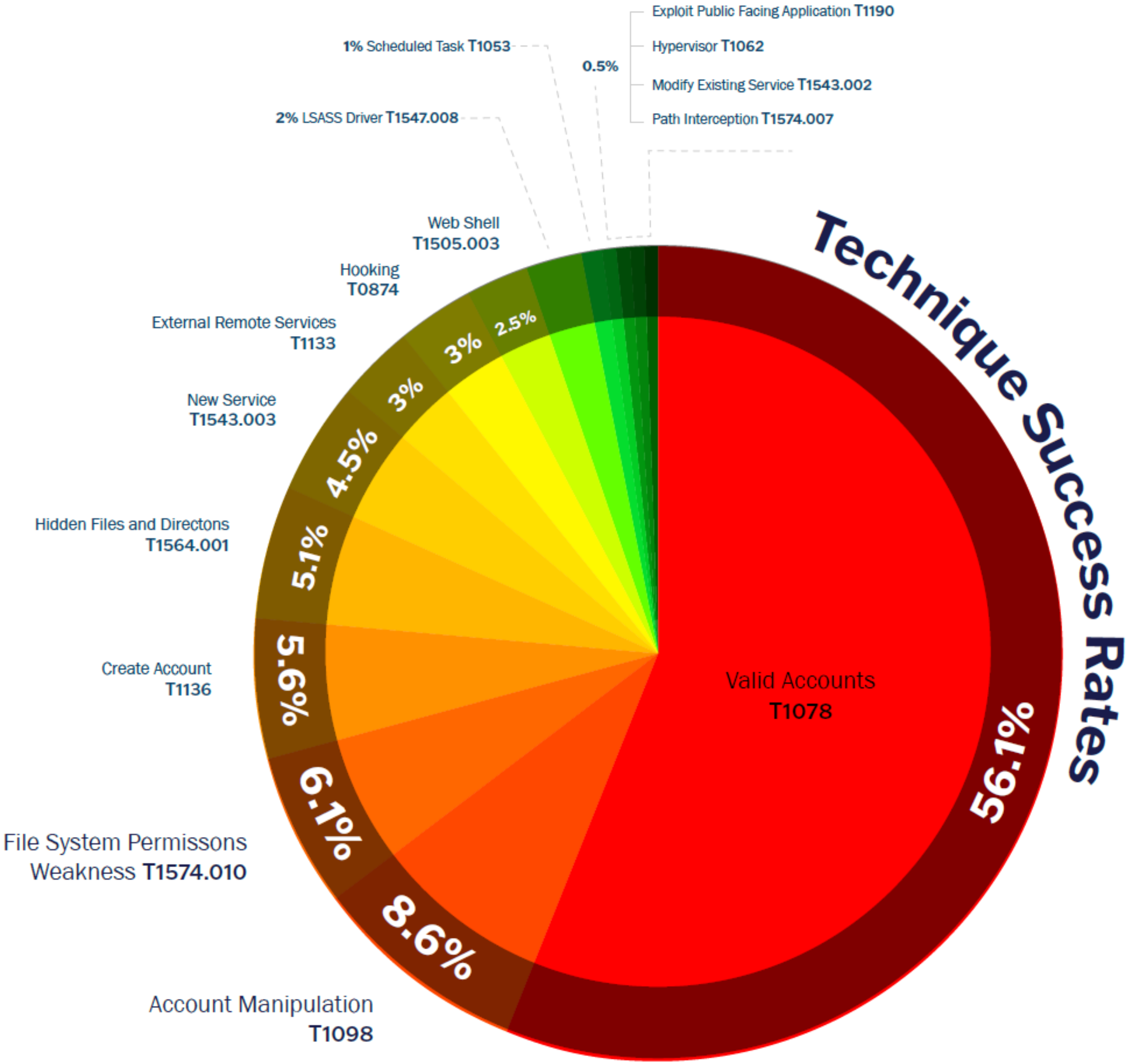
Threat actors maintain persistence or foothold in a network or system by changing credentials or modifying configuration files to maintain continued access. Threat actors may also monitor and manipulate reports observed in the Server Manager Performance Monitor to remain undetected.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following Cyber Performance Goals (cisa.gov/cpg):

CPG 2.H Phishing-Resistant Multifactor Authentication

CPG 2.T Log Collection



FY22 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

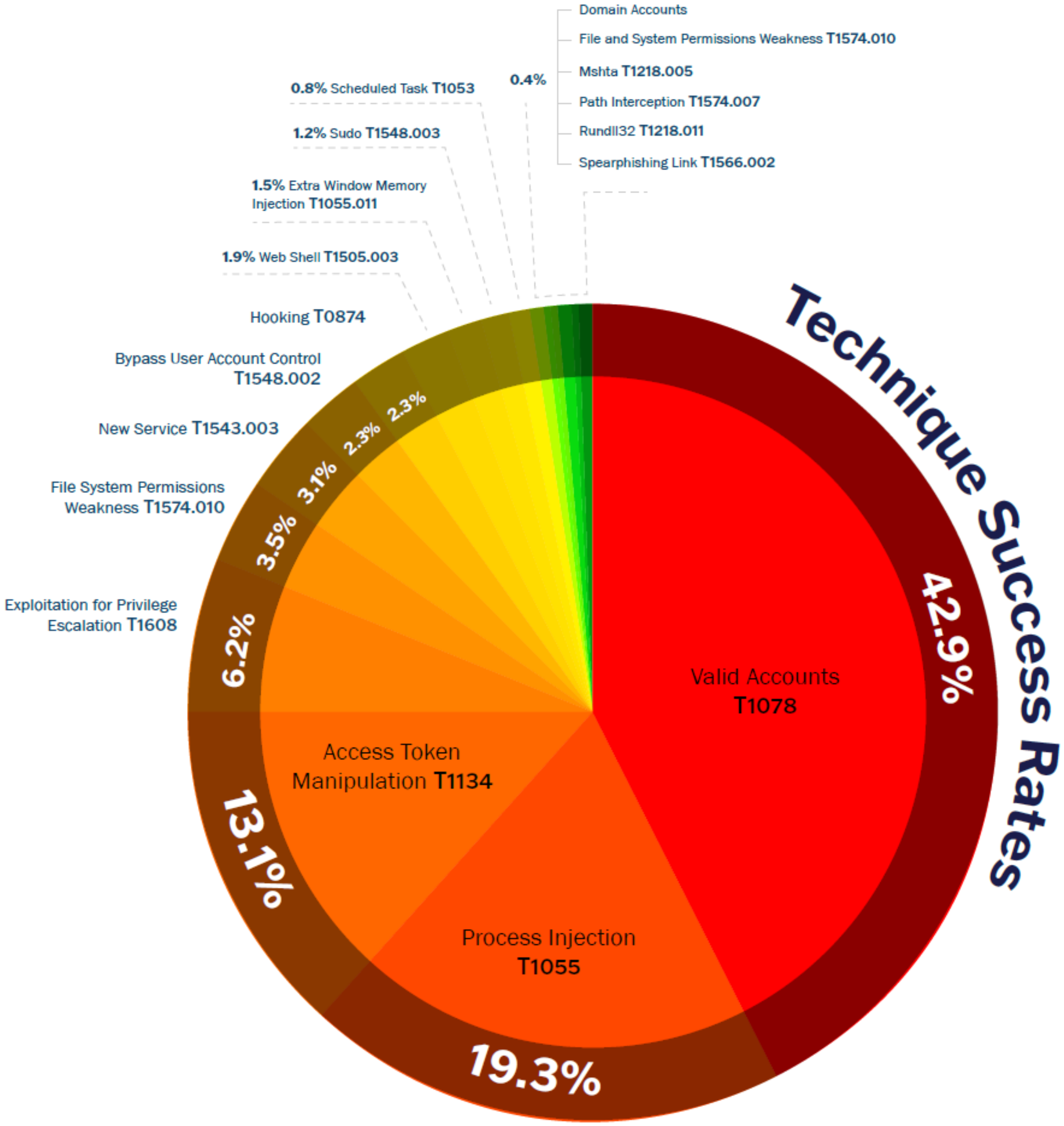
Privilege Escalation

Threat actors attempt to obtain escalated privileges to further compromise a network. Actors search systems for hard-coded or default credentials. When carrying out an attack, threat actors conduct extensive reconnaissance and credential harvesting to identify administrator accounts.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following Cyber Performance Goals (cisa.gov/cpg):

CPG 2.C Unique Credentials
CPG 2.L Secure Sensitive Data
CPG 3.A Detecting Relevant Threats and TTPs



Physical security?

Natural disasters?

Unique threats?

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Requirements + Threats + Technical Controls + System Design

Designing Hardened Systems

Technical Controls

Advanced parameters & specific settings

Easy to set and check

Security Configuration Guide,
DISA STIG & STIG Readiness Guides,
CIS Benchmark

Most settings are secure by default

Very binary (pass or fail, no in-between)

All technical, no people & process work

VCF.noBreaches = TRUE

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Requirements + Threats + Technical Controls + Design

Designing Hardened Systems

Technical Controls

Advanced parameters & specific settings

Easy to set and check

Security Configuration Guide,
DISA STIG & STIG Readiness Guides,
CIS Benchmark

Most settings are secure by default

Very binary (pass or fail, no in-between)

All technical, no people & process work

VCF.noBreaches = TRUE

System Design

Use features and functions to improve security

Not easy; needs to be done early

All organizations are different

Many features need to be enabled, because of…

Tradeoffs & “Compensating Controls”

Lots of people & process considerations

Where trust is established, or avoided

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Requirements + Threats + Technical Controls + Design

Designing Hardened Systems

Technical Controls

VMkernel.boot.execInstalledOnly = TRUE

vMotion Encryption = REQUIRED

vSAN Data-in-Transit = TRUE

etc. etc. x156

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Requirements + Threats + Technical Controls + Design

Designing Hardened Systems

Technical Controls

VMkernel.boot.execInstalledOnly = TRUE

vMotion Encryption = REQUIRED

vSAN Data-in-Transit = TRUE

etc. etc. x156

System Design

Do you have N+1 capacity so you can patch?

What key provider should you use?

How much performance change is there by enabling vSAN data-at-rest encryption?

What perimeter security controls do you have?

Secure Boot doesn’t allow use of %firstboot

What do you mean the Domain Admins have access to VCF?

…and so on.

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

EXPLORE

System Design Concepts

Designing Hardened Systems

Regulatory compliance isn't security.

Compliance is **always** a negotiation.

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Security **always** depends on context.

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

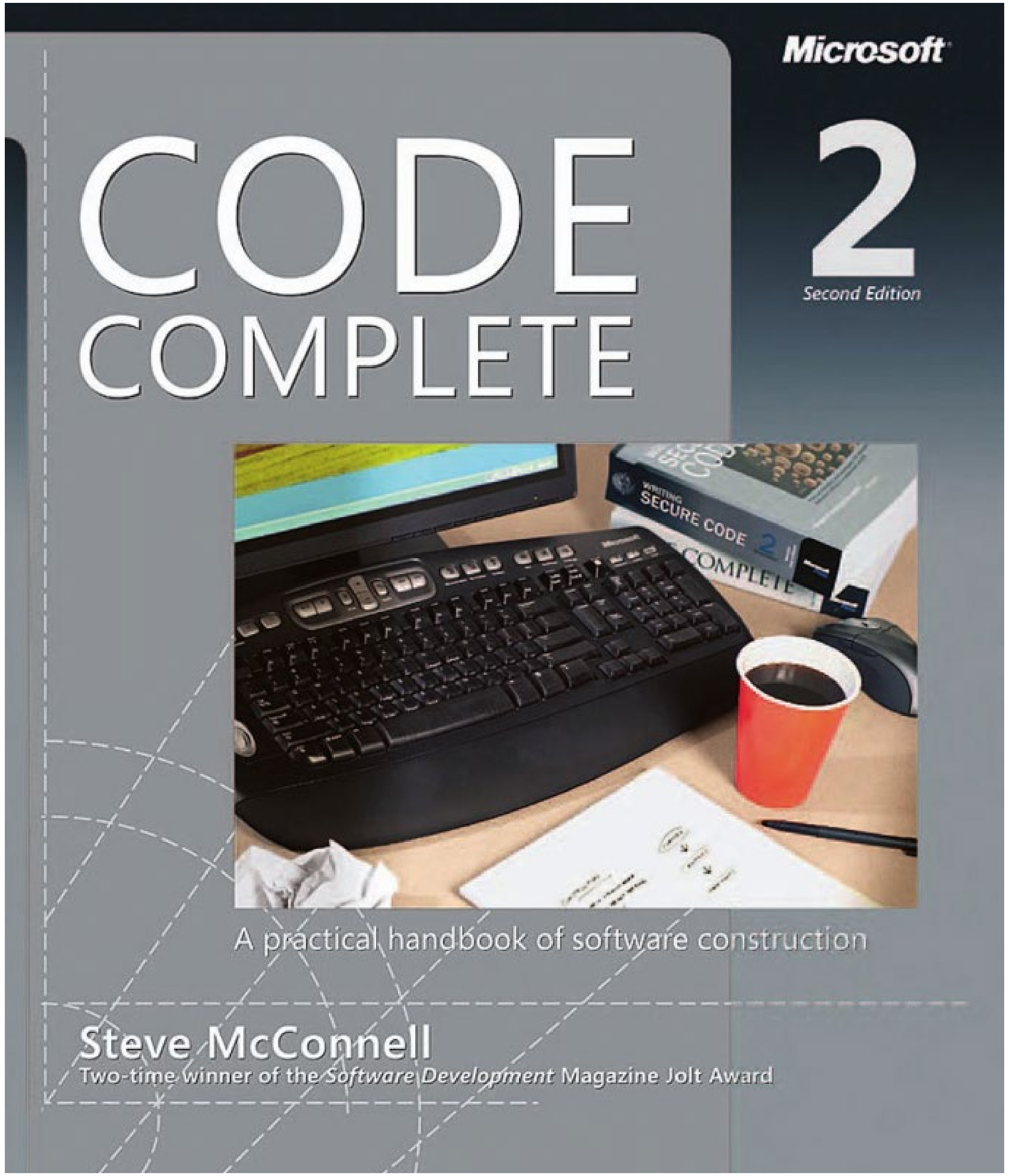
Security is **always** a tradeoff.

(Sometimes that tradeoff can be minimized, though)

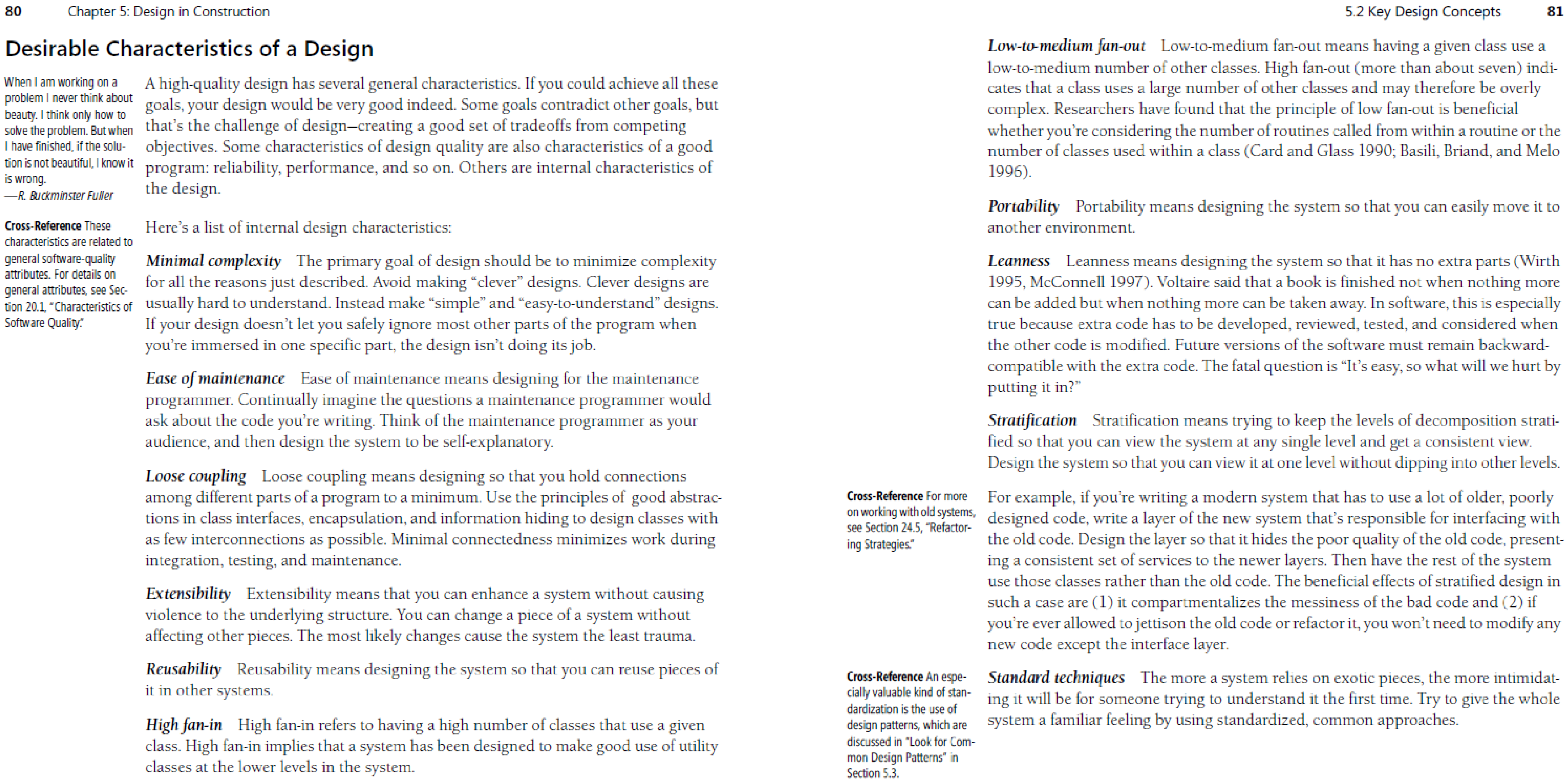
Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

“Zero Trust”

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.


Microsoft
CODE COMPLETE
2
Second Edition
WRITING SECURE CODE 2
COMPLETE
A practical handbook of software construction
Steve McConnell
Two-time winner of the Software Development Magazine Jolt Award

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



Desirable Characteristics of a Design

> When I am working on a problem I never think about beauty. I think only how to solve the problem. But when I have finished, if the solution is not beautiful, I know it is wrong.
> —*R. Buckminster Fuller*

A high-quality design has several general characteristics. If you could achieve all these goals, your design would be very good indeed. Some goals contradict other goals, but that's the challenge of design—creating a good set of tradeoffs from competing objectives. Some characteristics of design quality are also characteristics of a good program: reliability, performance, and so on. Others are internal characteristics of the design.

Cross-Reference These characteristics are related to general software-quality attributes. For details on general attributes, see Section 20.1, "Characteristics of Software Quality."

Here's a list of internal design characteristics:

Minimal complexity The primary goal of design should be to minimize complexity for all the reasons just described. Avoid making "clever" designs. Clever designs are usually hard to understand. Instead make "simple" and "easy-to-understand" designs. If your design doesn't let you safely ignore most other parts of the program when you're immersed in one specific part, the design isn't doing its job.

Ease of maintenance Ease of maintenance means designing for the maintenance programmer. Continually imagine the questions a maintenance programmer would ask about the code you're writing. Think of the maintenance programmer as your audience, and then design the system to be self-explanatory.

Loose coupling Loose coupling means designing so that you hold connections among different parts of a program to a minimum. Use the principles of good abstractions in class interfaces, encapsulation, and information hiding to design classes with as few interconnections as possible. Minimal connectedness minimizes work during integration, testing, and maintenance.

Extensibility Extensibility means that you can enhance a system without causing violence to the underlying structure. You can change a piece of a system without affecting other pieces. The most likely changes cause the system the least trauma.

Reusability Reusability means designing the system so that you can reuse pieces of it in other systems.

High fan-in High fan-in refers to having a high number of classes that use a given class. High fan-in implies that a system has been designed to make good use of utility classes at the lower levels in the system.

Low-to-medium fan-out Low-to-medium fan-out means having a given class use a low-to-medium number of other classes. High fan-out (more than about seven) indicates that a class uses a large number of other classes and may therefore be overly complex. Researchers have found that the principle of low fan-out is beneficial whether you're considering the number of routines called from within a routine or the number of classes used within a class (Card and Glass 1990; Basili, Briand, and Melo 1996).

Portability Portability means designing the system so that you can easily move it to another environment.

Leanness Leanness means designing the system so that it has no extra parts (Wirth 1995, McConnell 1997). Voltaire said that a book is finished not when nothing more can be added but when nothing more can be taken away. In software, this is especially true because extra code has to be developed, reviewed, tested, and considered when the other code is modified. Future versions of the software must remain backward-compatible with the extra code. The fatal question is "It's easy, so what will we hurt by putting it in?"

Stratification Stratification means trying to keep the levels of decomposition stratified so that you can view the system at any single level and get a consistent view. Design the system so that you can view it at one level without dipping into other levels.

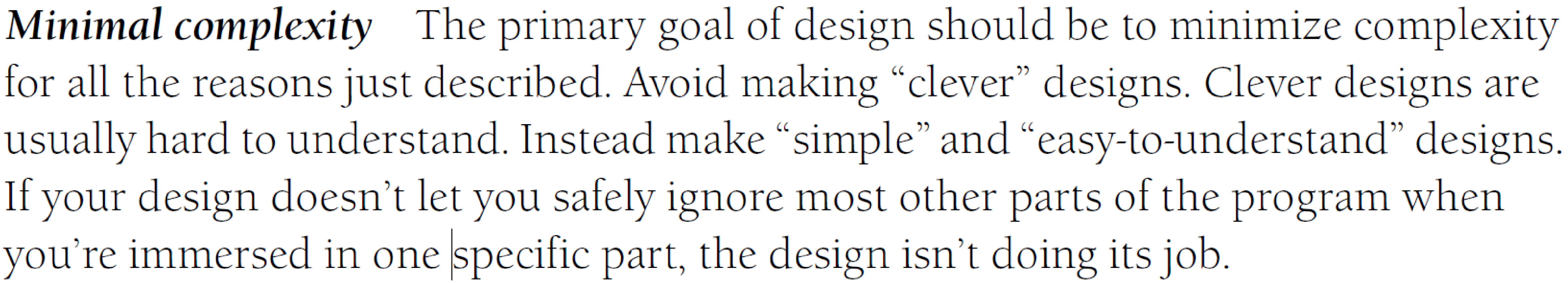
Cross-Reference For more on working with old systems, see Section 24.5, "Refactoring Strategies."

For example, if you're writing a modern system that has to use a lot of older, poorly designed code, write a layer of the new system that's responsible for interfacing with the old code. Design the layer so that it hides the poor quality of the old code, presenting a consistent set of services to the newer layers. Then have the rest of the system use those classes rather than the old code. The beneficial effects of stratified design in such a case are (1) it compartmentalizes the messiness of the bad code and (2) if you're ever allowed to jettison the old code or refactor it, you won't need to modify any new code except the interface layer.

Cross-Reference An especially valuable kind of standardization is the use of design patterns, which are discussed in "Look for Common Design Patterns" in Section 5.3.

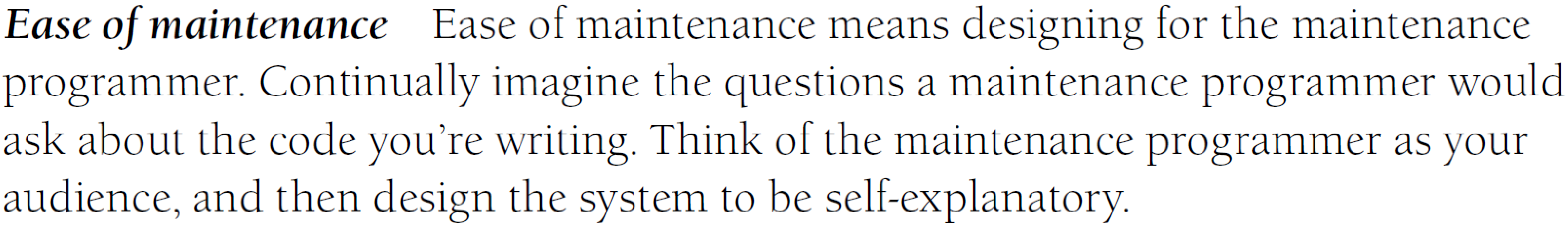
Standard techniques The more a system relies on exotic pieces, the more intimidating it will be for someone trying to understand it the first time. Try to give the whole system a familiar feeling by using standardized, common approaches.

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries



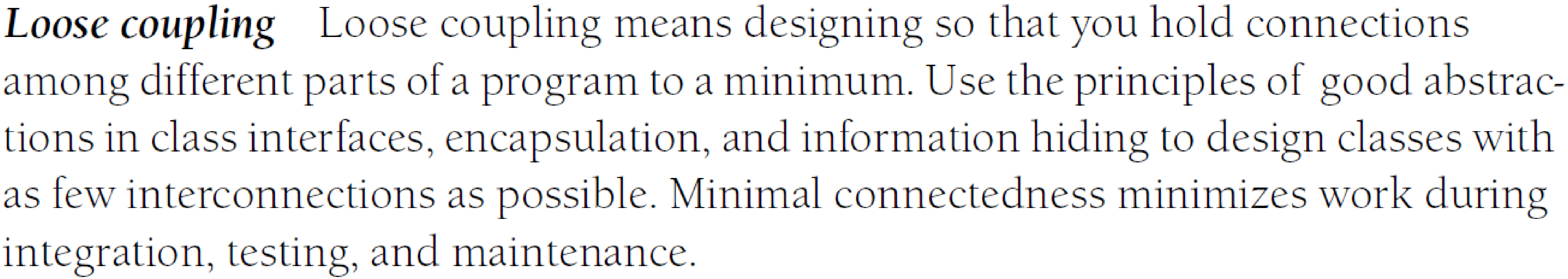
Minimal complexity The primary goal of design should be to minimize complexity for all the reasons just described. Avoid making "clever" designs. Clever designs are usually hard to understand. Instead make "simple" and "easy-to-understand" designs. If your design doesn't let you safely ignore most other parts of the program when you're immersed in one specific part, the design isn't doing its job.

EXPLORE
Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Ease of maintenance Ease of maintenance means designing for the maintenance programmer. Continually imagine the questions a maintenance programmer would ask about the code you're writing. Think of the maintenance programmer as your audience, and then design the system to be self-explanatory.

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



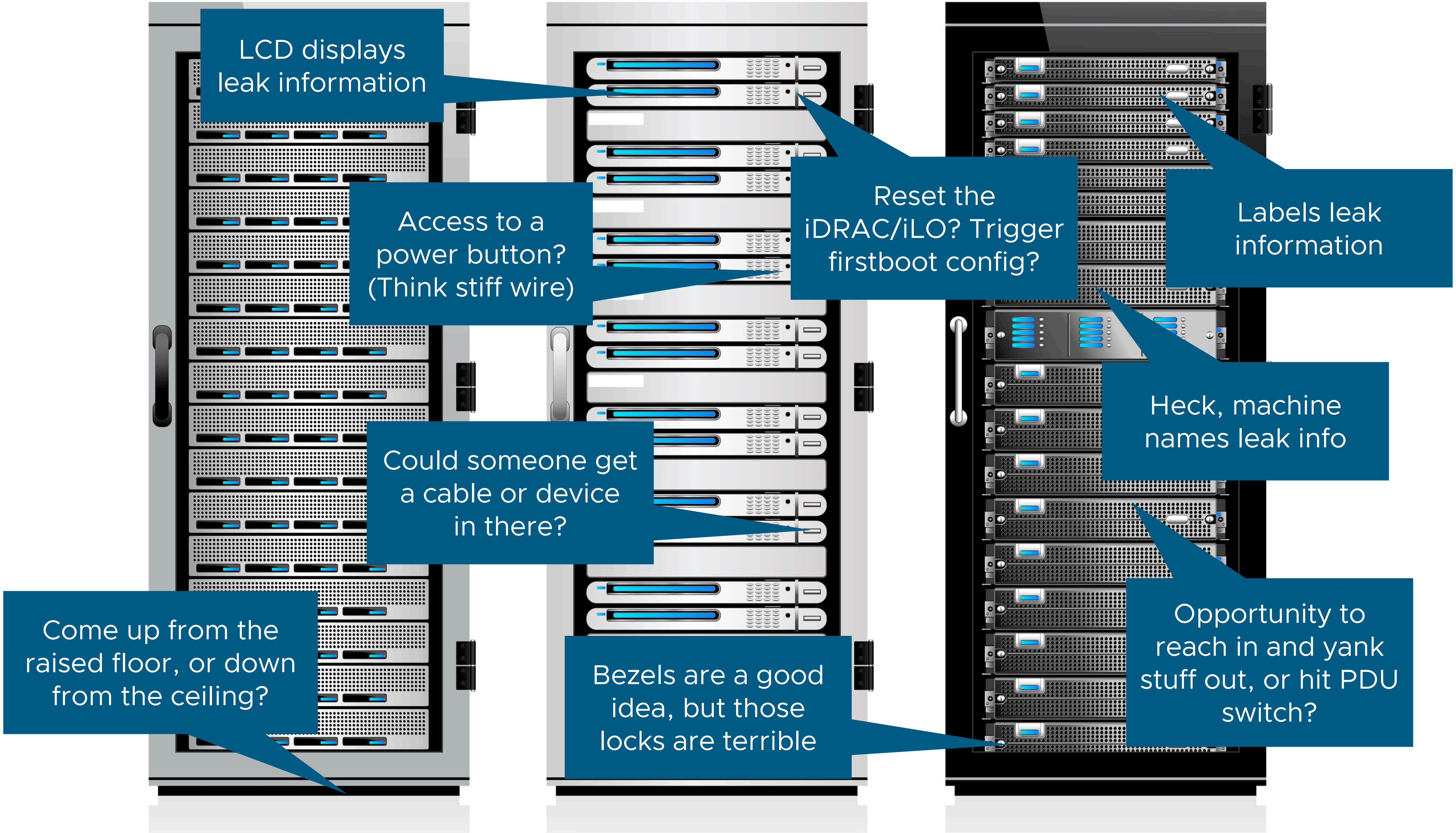
Loose coupling Loose coupling means designing so that you hold connections among different parts of a program to a minimum. Use the principles of good abstractions in class interfaces, encapsulation, and information hiding to design classes with as few interconnections as possible. Minimal connectedness minimizes work during integration, testing, and maintenance.

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

EXPLORE

Physical Environment

Designing Hardened Systems



LCD displays leak information

Access to a power button? (Think stiff wire)

Reset the iDRAC/iLO? Trigger firstboot config?

Labels leak information

Heck, machine names leak info

Could someone get a cable or device in there?

Come up from the raised floor, or down from the ceiling?

Bezels are a good idea, but those locks are terrible

Opportunity to reach in and yank stuff out, or hit PDU switch?

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

There is such a thing as too much security, though

(Fancy locks need power & network, for example)

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

EXPLORE

Server Hardware

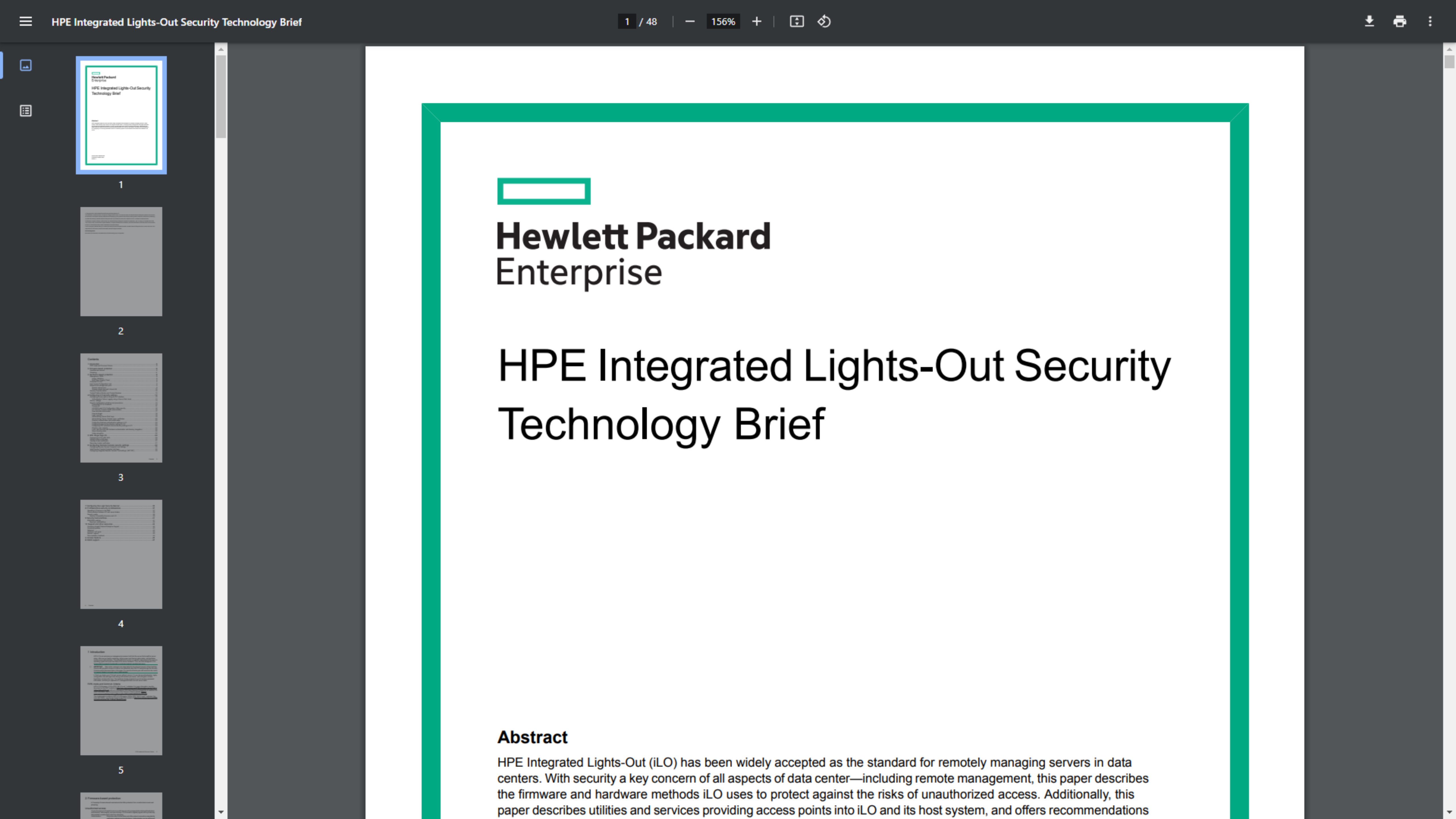
Designing Hardened Systems

Secure Hardware Underneath Everything

VMware Cloud Foundation Security & Compliance

Management Controllers

EXPLORE
Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



Hewlett Packard
Enterprise

HPE Integrated Lights-Out Security Technology Brief

Abstract

HPE Integrated Lights-Out (iLO) has been widely accepted as the standard for remotely managing servers in data centers. With security a key concern of all aspects of data center—including remote management, this paper describes the firmware and hardware methods iLO uses to protect against the risks of unauthorized access. Additionally, this paper describes utilities and services providing access points into iLO and its host system, and offers recommendations

Hardening Server Management Controllers for ESXi

VMware Cloud Foundation Security & Compliance

1. **Deactivate everything you are not actively using**: IPMI, VNC, Redfish, IPv6, SSH, Telnet, Remote Admin/RACADM, SNMP, Serial-over-LAN…

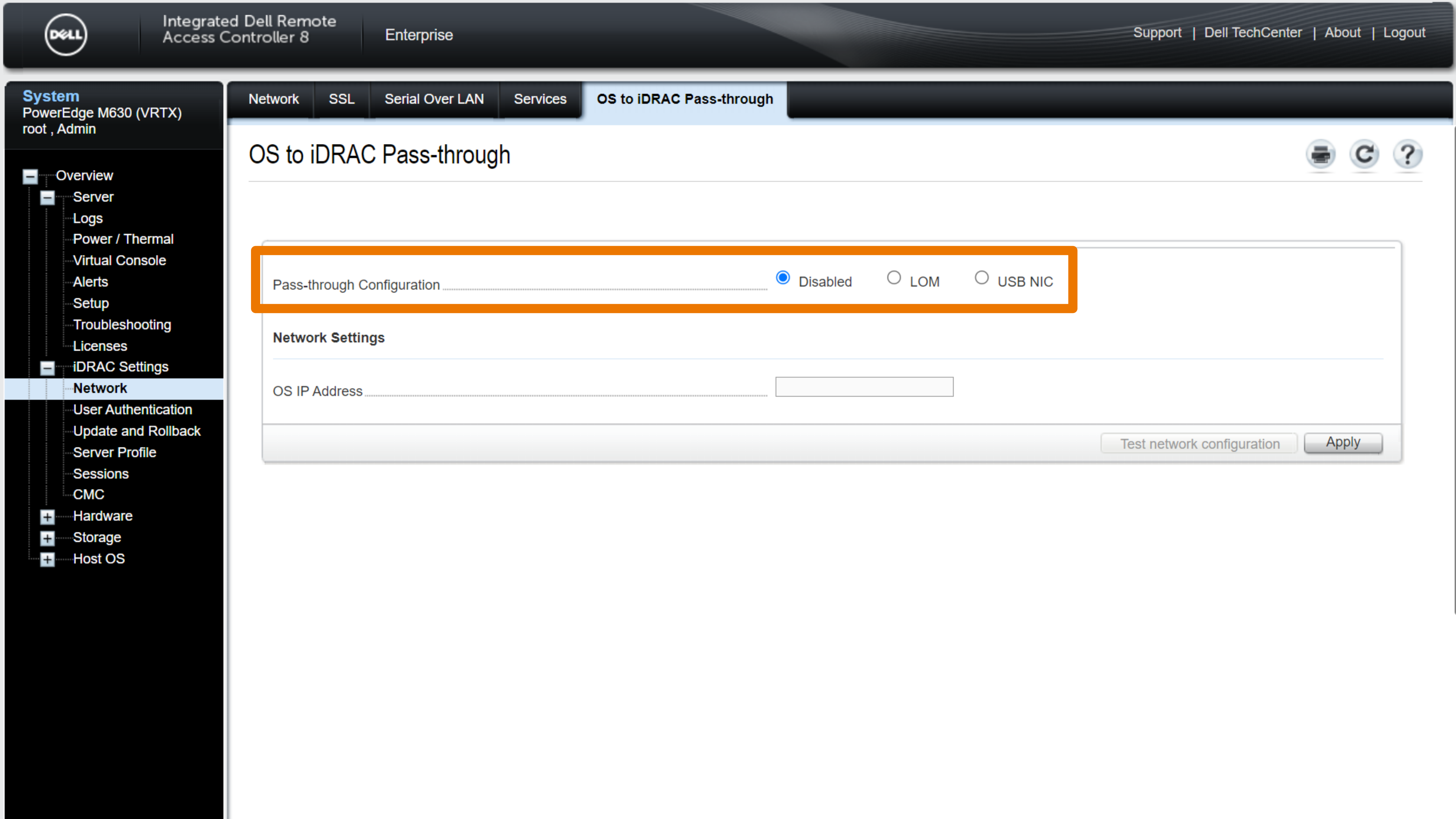
Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Hardening Server Management Controllers for ESXi

VMware Cloud Foundation Security & Compliance

1. Deactivate everything you are not actively using: IPMI, VNC, Redfish, IPv6, SSH, Telnet, Remote Admin/RACADM, SNMP, Serial-over-LAN…
2. **Deactivate the “OS Pass-through” or equivalent virtual NIC.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



OS to iDRAC Pass-through

Pass-through Configuration ● Disabled ○ LOM ○ USB NIC

Network Settings

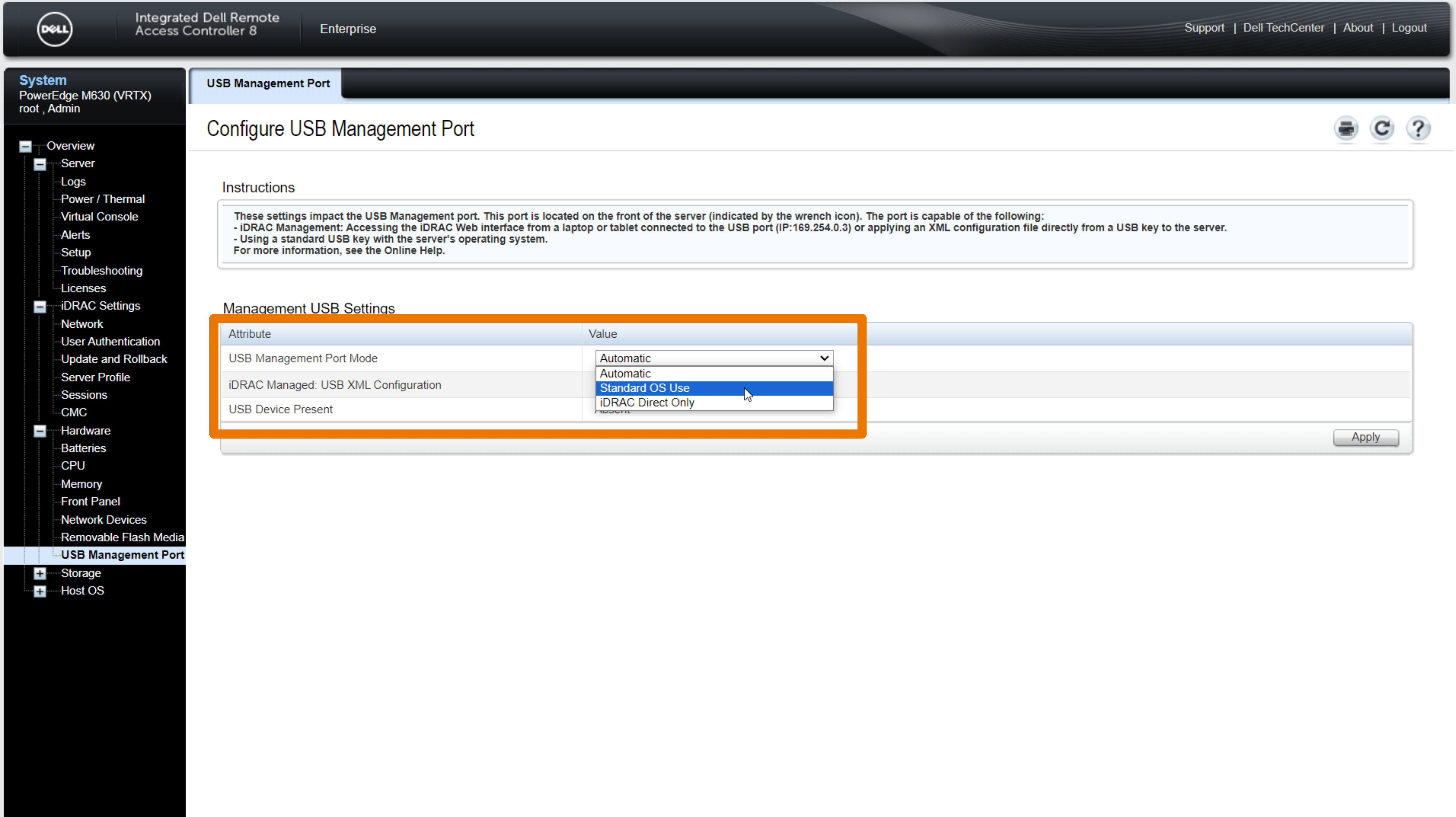
OS IP Address

Hardening Server Management Controllers for ESXi

VMware Cloud Foundation Security & Compliance

1. Deactivate everything you are not actively using: IPMI, VNC, Redfish, IPv6, SSH, Telnet, Remote Admin/RACADM, SNMP, Serial-over-LAN…
2. Deactivate the “OS Pass-through” or equivalent virtual NIC.
3. **Deactivate the USB configuration settings.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



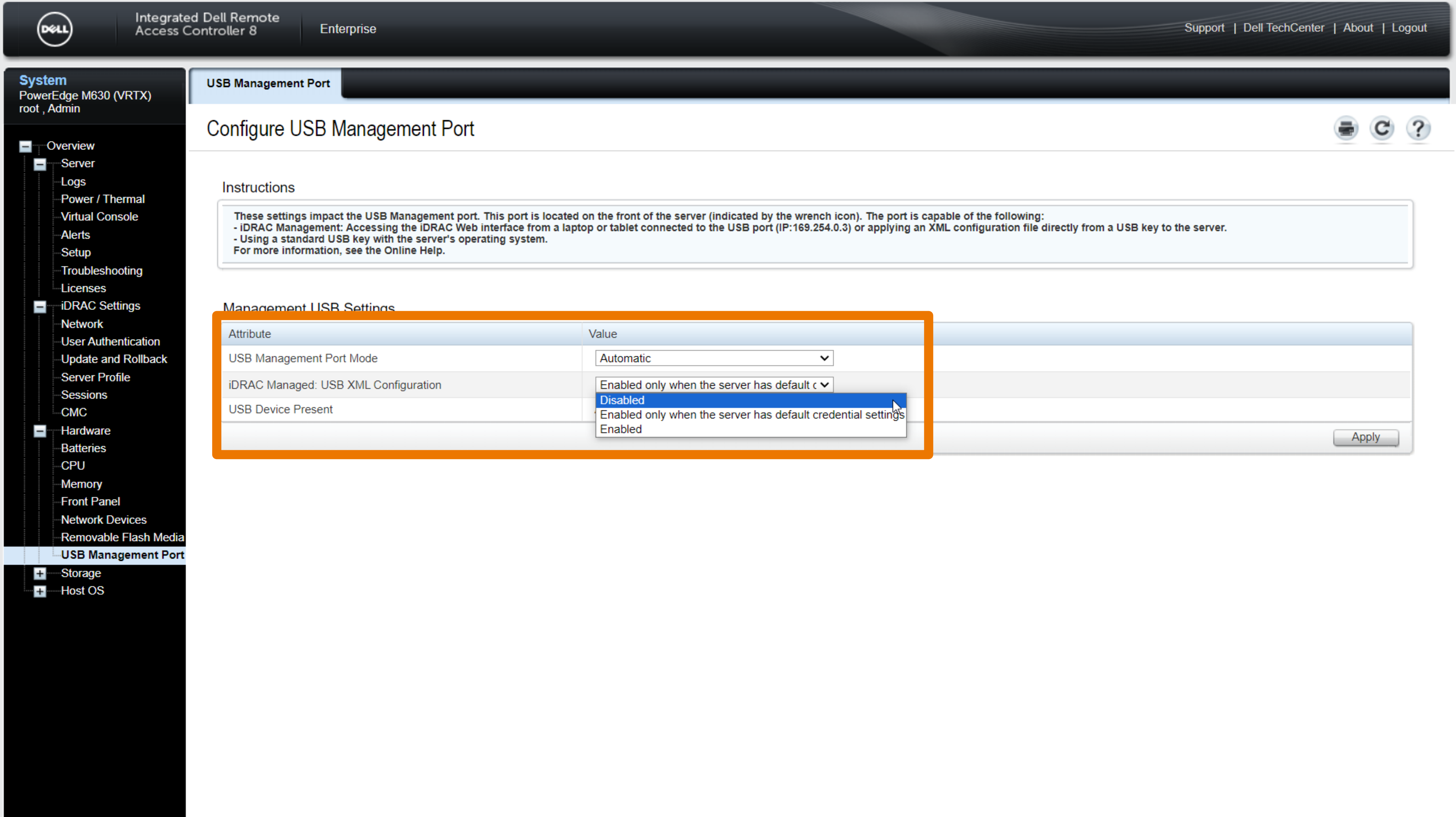
Configure USB Management Port

Instructions

These settings impact the USB Management port. This port is located on the front of the server (indicated by the wrench icon). The port is capable of the following:
- iDRAC Management: Accessing the iDRAC Web interface from a laptop or tablet connected to the USB port (IP:169.254.0.3) or applying an XML configuration file directly from a USB key to the server.
- Using a standard USB key with the server's operating system.
For more information, see the Online Help.

Management USB Settings

Attribute	Value
USB Management Port Mode	Automatic Automatic Standard OS Use iDRAC Direct Only
iDRAC Managed: USB XML Configuration	
USB Device Present	



Configure USB Management Port

Instructions

These settings impact the USB Management port. This port is located on the front of the server (indicated by the wrench icon). The port is capable of the following:
- iDRAC Management: Accessing the iDRAC Web interface from a laptop or tablet connected to the USB port (IP:169.254.0.3) or applying an XML configuration file directly from a USB key to the server.
- Using a standard USB key with the server's operating system.
For more information, see the Online Help.

Management USB Settings

Attribute	Value
USB Management Port Mode	Automatic
iDRAC Managed: USB XML Configuration	Enabled only when the server has default c
USB Device Present	

Hardening Server Management Controllers for ESXi

VMware Cloud Foundation Security & Compliance

1. Deactivate everything you are not actively using: IPMI, VNC, Redfish, IPv6, SSH, Telnet, Remote Admin/RACADM, SNMP, Serial-over-LAN…
2. Deactivate the “OS Pass-through” or equivalent virtual NIC.
3. Deactivate the USB configuration settings.
4. **Set NTP.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Hardening Server Management Controllers for ESXi

VMware Cloud Foundation Security & Compliance

1. Deactivate everything you are not actively using: IPMI, VNC, Redfish, IPv6, SSH, Telnet, Remote Admin/RACADM, SNMP, Serial-over-LAN…
2. Deactivate the “OS Pass-through” or equivalent virtual NIC.
3. Deactivate the USB configuration settings.
4. Set NTP.
5. **Set DNS.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Hardening Server Management Controllers for ESXi

VMware Cloud Foundation Security & Compliance

1. Deactivate everything you are not actively using: IPMI, VNC, Redfish, IPv6, SSH, Telnet, Remote Admin/RACADM, SNMP, Serial-over-LAN…
2. Deactivate the “OS Pass-through” or equivalent virtual NIC.
3. Deactivate the USB configuration settings.
4. Set NTP.
5. Set DNS.
6. **Forward logs to your syslog server, set up email alerts.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Hardening Server Management Controllers for ESXi

VMware Cloud Foundation Security & Compliance

1. Deactivate everything you are not actively using: IPMI, VNC, Redfish, IPv6, SSH, Telnet, Remote Admin/RACADM, SNMP, Serial-over-LAN…
2. Deactivate the “OS Pass-through” or equivalent virtual NIC.
3. Deactivate the USB configuration settings.
4. Set NTP.
5. Set DNS.
6. Forward logs to your syslog server, set up email alerts.
7. **Make good authentication choices (long passwords, vaulted).**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Hardening Server Management Controllers for ESXi

VMware Cloud Foundation Security & Compliance

1. Deactivate everything you are not actively using: IPMI, VNC, Redfish, IPv6, SSH, Telnet, Remote Admin/RACADM, SNMP, Serial-over-LAN…
2. Deactivate the “OS Pass-through” or equivalent virtual NIC.
3. Deactivate the USB configuration settings.
4. Set NTP.
5. Set DNS.
6. Forward logs to your syslog server, set up email alerts.
7. Make good authentication choices (long passwords, vaulted).
8. **Configure front-panel LCD displays & buttons wisely.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Secure Hardware Underneath Everything

VMware Cloud Foundation Security & Compliance

Management Controllers

UEFI Firmware Settings

EXPLORE
Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Legacy BIOS is **deprecated** in vSphere 8

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Servers are NOT delivered with optimal firmware configurations for ESXi

EXPLORE Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Hardening Server Hardware for ESXi

VMware Cloud Foundation Security & Compliance

1. **UEFI Secure Boot**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Hardening Server Hardware for ESXi

VMware Cloud Foundation Security & Compliance

1. UEFI Secure Boot
2. **Enable the Trusted Platform Module (SHA-256, TIS/FIFO)**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Trusted Platform Module 2.0: Hardware

Not required, yet. It’s inexpensive. Make sure it’s in **all new equipment**.

1. Secrets, slow random number generator, and permanent key as ID
2. Serial device that sits on the system board (think “modem” – not fast)
3. Belongs to ESXi - no workloads can touch it!
4. Stores encryption keys for ESXi Configuration Encryption
5. Doesn’t help if your whole server is stolen
6. Easily cleared later

EXPLORE Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Hardening Server Hardware for ESXi

VMware Cloud Foundation Security & Compliance

1. UEFI Secure Boot
2. Enable the Trusted Platform Module (SHA-256, TIS/FIFO)
3. **Enable Intel SGX or AMD SEV-ES**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Hardening Server Hardware for ESXi

VMware Cloud Foundation Security & Compliance

1. UEFI Secure Boot
2. Enable the Trusted Platform Module (SHA-256, TIS/FIFO)
3. Enable Intel SGX or AMD SEV-ES
4. **Enable Intel TXT**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Hardening Server Hardware for ESXi

VMware Cloud Foundation Security & Compliance

1. UEFI Secure Boot
2. Enable the Trusted Platform Module (SHA-256, TIS/FIFO)
3. Enable Intel SGX or AMD SEV-ES
4. Enable Intel TXT
5. **USB only for keyboards, or deactivated.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Hardening Server Hardware for ESXi

VMware Cloud Foundation Security & Compliance

1. UEFI Secure Boot
2. Enable the Trusted Platform Module (SHA-256, TIS/FIFO)
3. Enable Intel SGX or AMD SEV-ES
4. Enable Intel TXT
5. USB only for keyboards, or deactivated.
6. **Enable all the performance options that are shut off!**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Hardening Server Hardware for ESXi

VMware Cloud Foundation Security & Compliance

1. UEFI Secure Boot
2. Enable the Trusted Platform Module (SHA-256, TIS/FIFO)
3. Enable Intel SGX or AMD SEV-ES
4. Enable Intel TXT
5. USB only for keyboards, or deactivated.
6. Enable all the performance options that are shut off!
7. **Let ESXi control the CPU power states.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Secure Hardware Underneath Everything

VMware Cloud Foundation Security & Compliance

Management Controllers

UEFI Firmware Settings

Updating System Firmware

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Being Flexible With Hardware

Future-Proof Your Ability to Change Quickly

1. Multiple NICs
2. Empty DIMM Sockets
3. Empty Drive Bays
4. Reserve Capacity

EXPLORE
Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Isolation Techniques

Designing Hardened Systems

Isolation Decisions

VMware Cloud Foundation Security & Compliance

VLANs?

Separate NICs?

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Isolation Decisions

VMware Cloud Foundation Security & Compliance

VLANs?

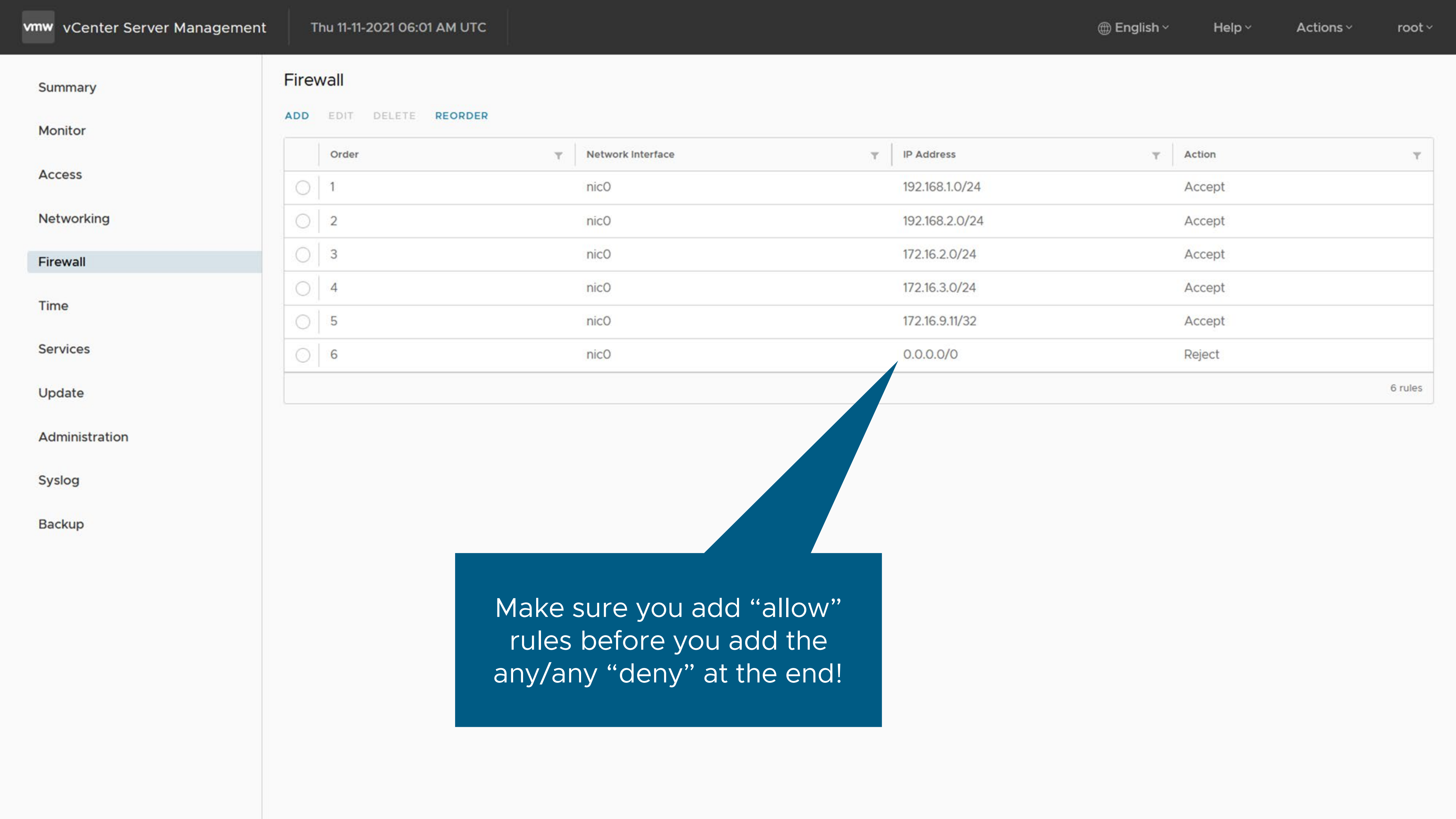
Separate NICs?

Firewalls?

ACLs?

VPNs?

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.



Firewall

	Order	Network Interface	IP Address	Action
○	1	nic0	192.168.1.0/24	Accept
○	2	nic0	192.168.2.0/24	Accept
○	3	nic0	172.16.2.0/24	Accept
○	4	nic0	172.16.3.0/24	Accept
○	5	nic0	172.16.9.11/32	Accept
○	6	nic0	0.0.0.0/0	Reject

6 rules

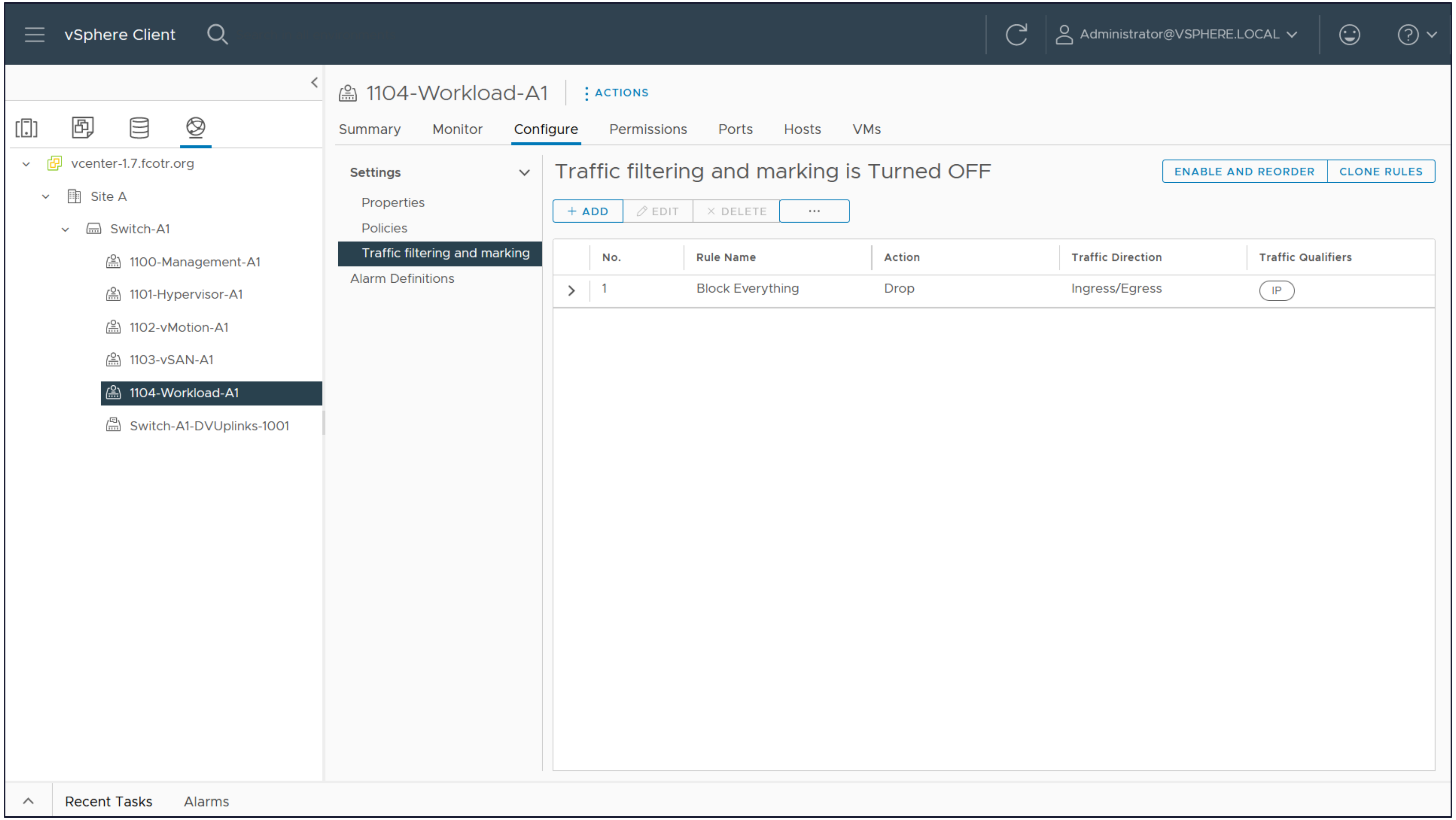
Make sure you add “allow” rules before you add the any/any “deny” at the end!

NSX Distributed Firewall can be applied to nearly everything, **except ESXi, vCenter, SDDC Manager, and NSX itself.**

(But you can use NSX Edge for that)

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Distributed Switch Traffic Filtering and Marking

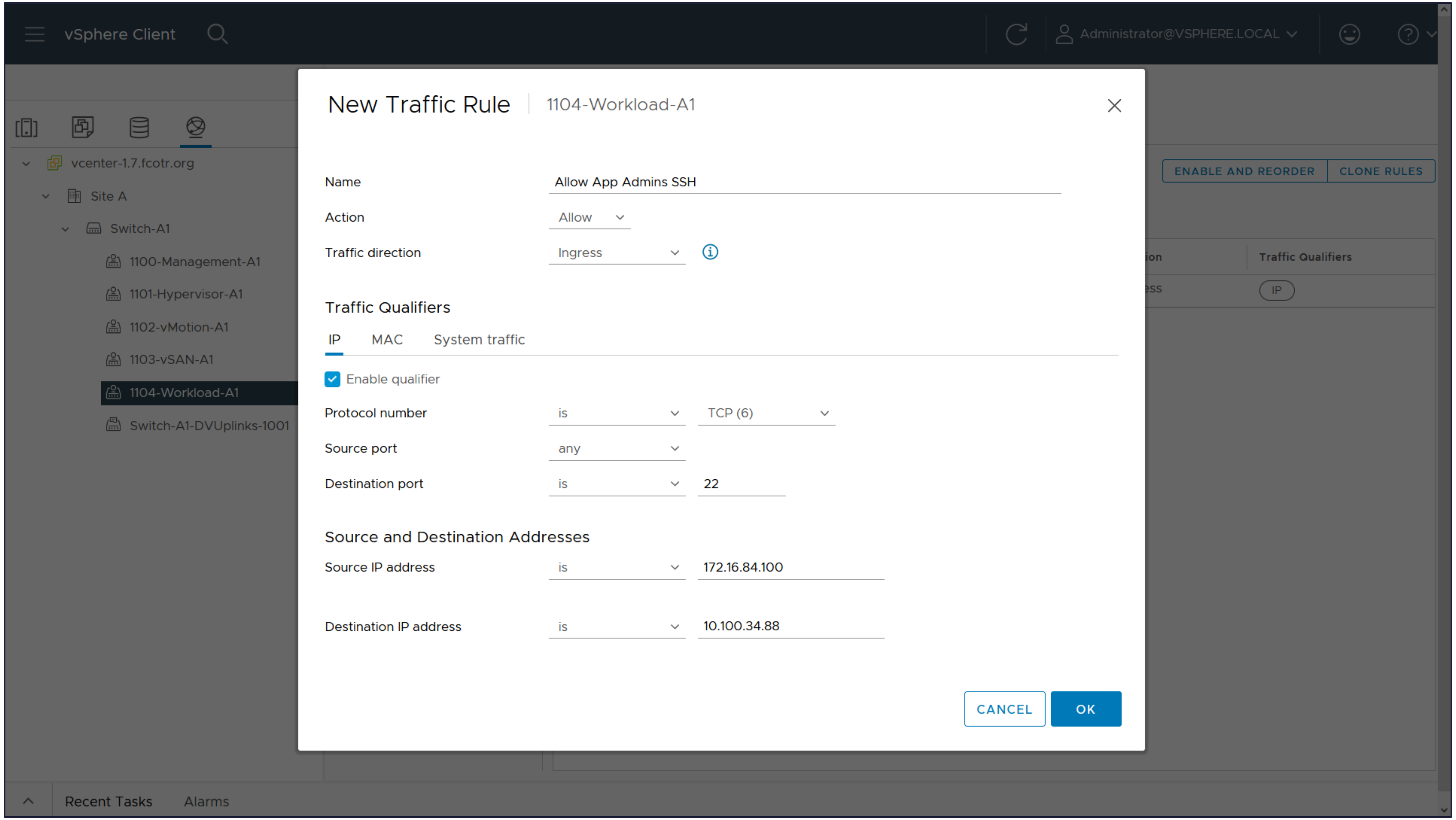


Traffic filtering and marking is Turned OFF

No.	Rule Name	Action	Traffic Direction	Traffic Qualifiers
1	Block Everything	Drop	Ingress/Egress	IP

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

More Like ACLs than a Modern Firewall



New Traffic Rule | 1104-Workload-A1

Name: Allow App Admins SSH

Action: Allow

Traffic direction: Ingress

Traffic Qualifiers

IP | MAC | System traffic

☑ Enable qualifier

Protocol number: is TCP (6)

Source port: any

Destination port: is 22

Source and Destination Addresses

Source IP address: is 172.16.84.100

Destination IP address: is 10.100.34.88

CANCEL | OK

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Isolation Decisions

VMware Cloud Foundation Security & Compliance

VLANs?

Separate NICs?

Firewalls?

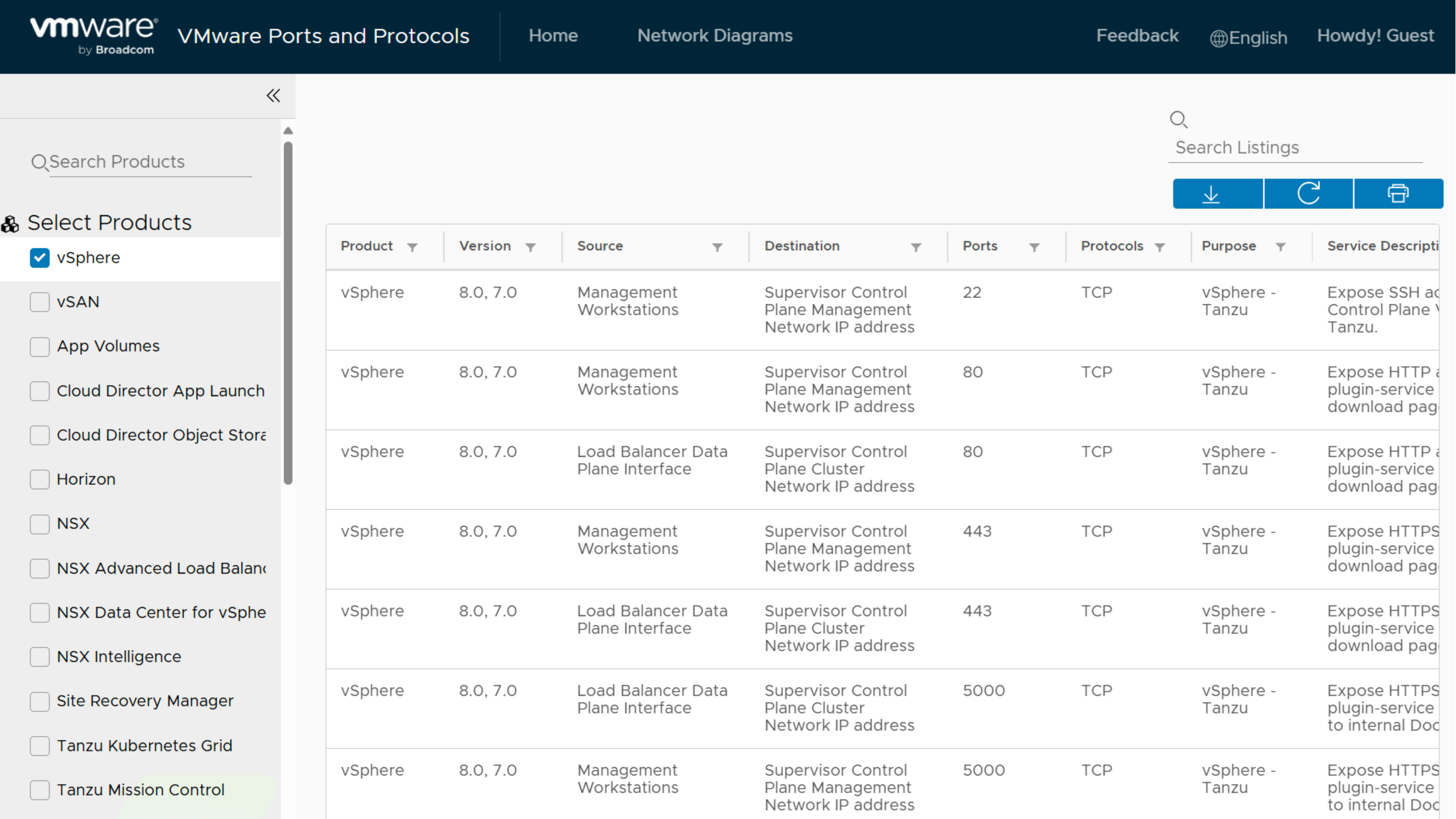
ACLs?

VPNs?

Ingress?

Egress?

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



Select Products

- ☑ vSphere
- ☐ vSAN
- ☐ App Volumes
- ☐ Cloud Director App Launch
- ☐ Cloud Director Object Stor
- ☐ Horizon
- ☐ NSX
- ☐ NSX Advanced Load Balan
- ☐ NSX Data Center for vSphe
- ☐ NSX Intelligence
- ☐ Site Recovery Manager
- ☐ Tanzu Kubernetes Grid
- ☐ Tanzu Mission Control

Product	Version	Source	Destination	Ports	Protocols	Purpose	Service Descripti
vSphere	8.0, 7.0	Management Workstations	Supervisor Control Plane Management Network IP address	22	TCP	vSphere - Tanzu	Expose SSH a Control Plane Tanzu.
vSphere	8.0, 7.0	Management Workstations	Supervisor Control Plane Management Network IP address	80	TCP	vSphere - Tanzu	Expose HTTP plugin-service download pag
vSphere	8.0, 7.0	Load Balancer Data Plane Interface	Supervisor Control Plane Cluster Network IP address	80	TCP	vSphere - Tanzu	Expose HTTP plugin-service download pag
vSphere	8.0, 7.0	Management Workstations	Supervisor Control Plane Management Network IP address	443	TCP	vSphere - Tanzu	Expose HTTPS plugin-service download pag
vSphere	8.0, 7.0	Load Balancer Data Plane Interface	Supervisor Control Plane Cluster Network IP address	443	TCP	vSphere - Tanzu	Expose HTTPS plugin-service download pag
vSphere	8.0, 7.0	Load Balancer Data Plane Interface	Supervisor Control Plane Cluster Network IP address	5000	TCP	vSphere - Tanzu	Expose HTTPS plugin-service to internal Do
vSphere	8.0, 7.0	Management Workstations	Supervisor Control Plane Management Network IP address	5000	TCP	vSphere - Tanzu	Expose HTTPS plugin-service to internal Do

Isolation Decisions

VMware Cloud Foundation Security & Compliance

VLANs?

Separate NICs?

Firewalls?

ACLs?

VPNs?

Ingress?

Egress?

Routed?

Unrouted?

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Should you put vCenter in/on the same network as ESXi management?

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Common Security Zones in a Deployment, Ignoring Workloads

VMware Cloud Foundation Security & Compliance

1. Pure Internal to Cluster
2. Access by Admins
3. Access by Non-Admins
4. Cluster-to-Cluster
5. Trusted Systems

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

EXPLORE

Access Control

Designing Hardened Systems

Access Control is **Everything**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Access Control
Includes Trust

EXPLORE Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Things Your Identity Provider Can Do To You

Not “Zero Trust” At All

- Change Group Membership
- Reset User Passwords
- Disable MFA and Other Controls
- Cover Their Tracks By Deleting Logs

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Potential Designs for Authentication

VMware Cloud Foundation Security & Compliance

Local Authentication

Centralized Authentication

Dedicated Authentication

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

How Do You Reduce Trust?

Reduce Overall Trust, Not Require More

VCF
Admins

IdP
Admins

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

How Do You Reduce Trust?

Reduce Overall Trust, Not Require More

VCF
Admins

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

vSphere Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. **Isolate from corporate/enterprise IdPs.**

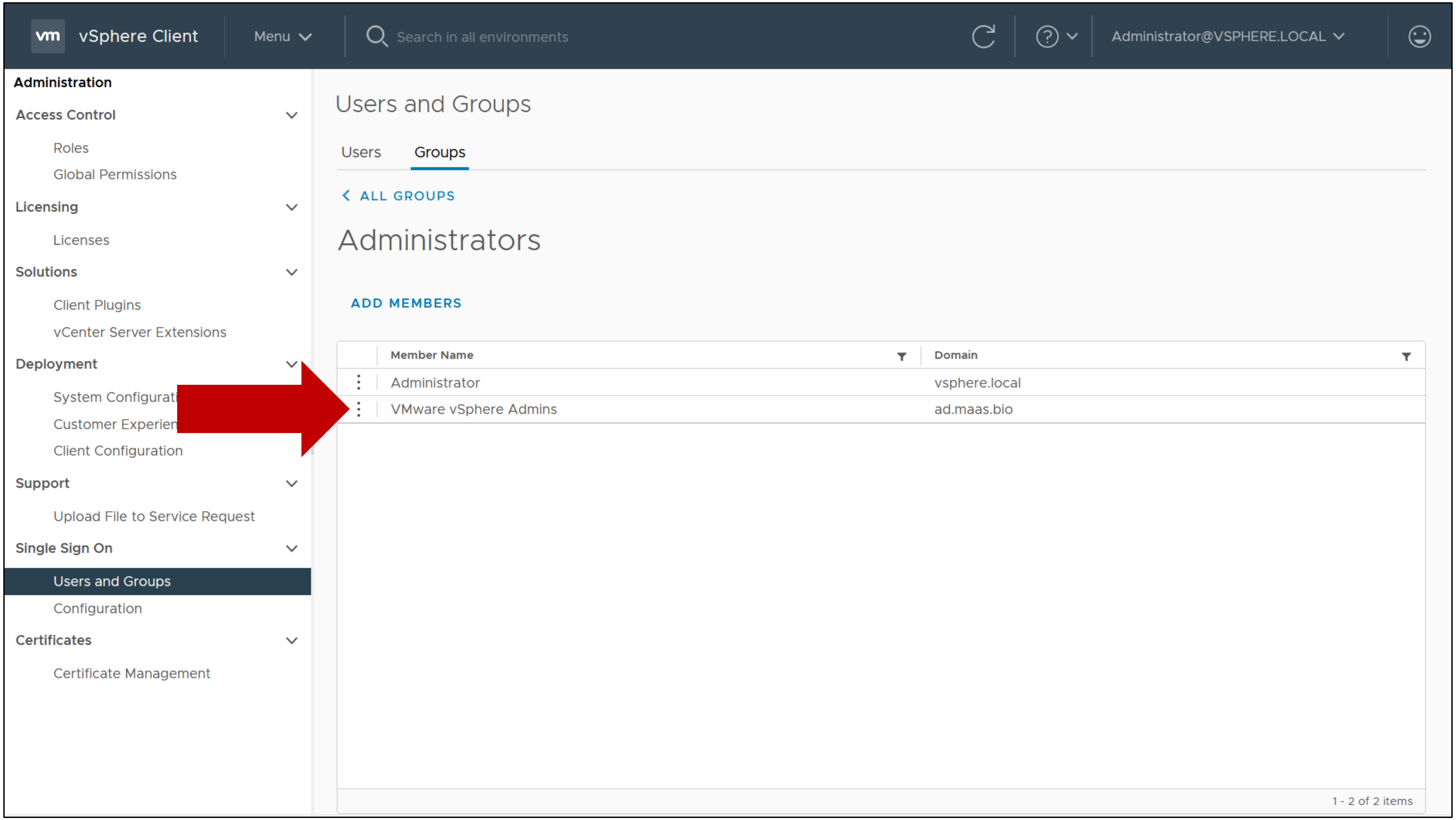
Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

vSphere Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from corporate/enterprise IdPs.
2. **If reasonable, do authorization inside vSphere/VCF, not inside your IdP.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



Users and Groups

Users | Groups

ALL GROUPS

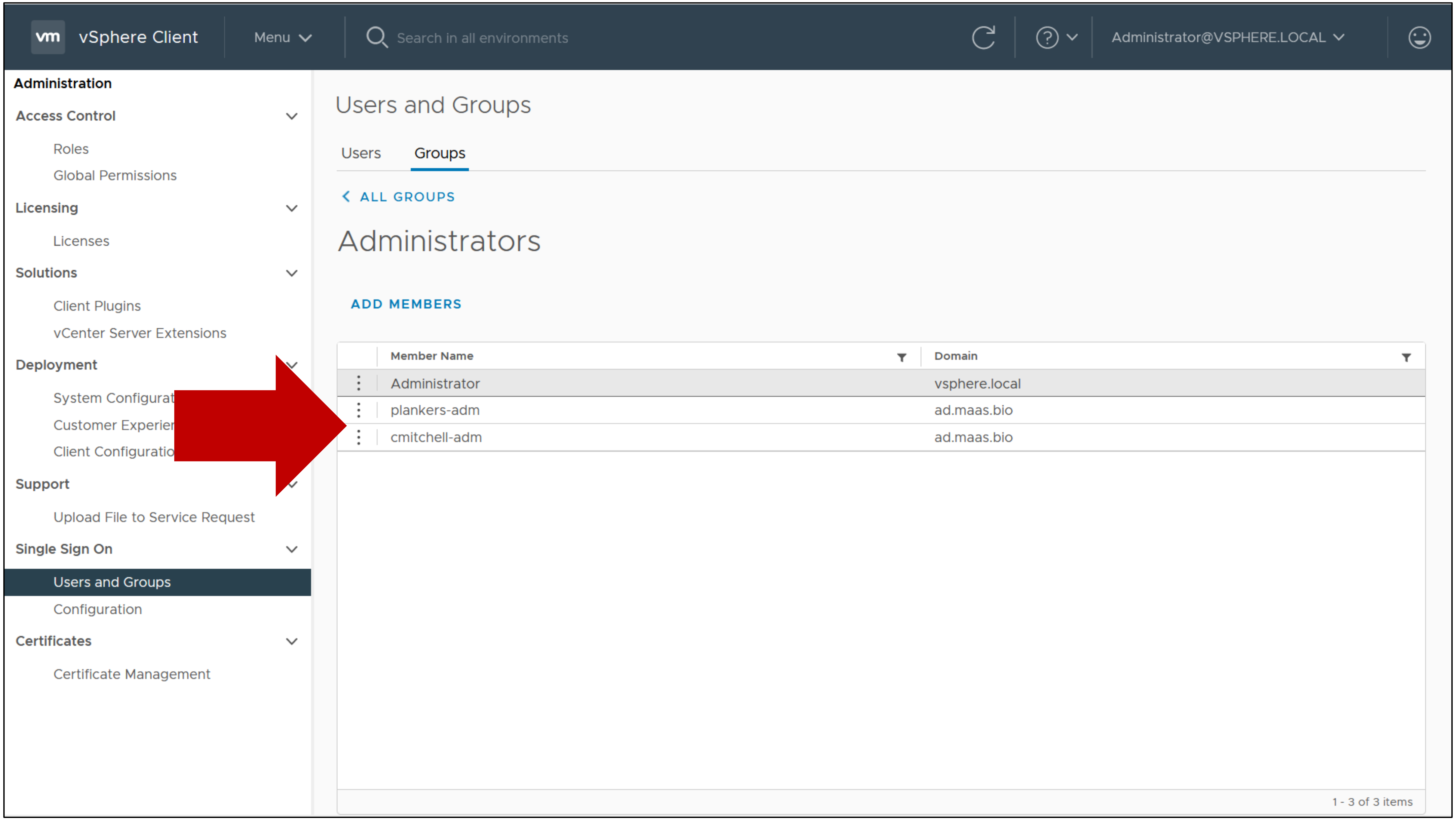
Administrators

ADD MEMBERS

Member Name	Domain
Administrator	vsphere.local
VMware vSphere Admins	ad.maas.bio

1 - 2 of 2 items

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



Administrators

Member Name	Domain
Administrator	vsphere.local
plankers-adm	ad.maas.bio
cmitchell-adm	ad.maas.bio

1 - 3 of 3 items

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

vSphere Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. **Use Identity Federation to introduce MFA.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Options For Enterprise Identity Federation in VCF

VMware Identity Broker (VIDB)

Microsoft AD over LDAPS

Microsoft ADFS

Okta Identity

Microsoft Entra ID

PingFederate is also available in VMware vSphere

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

panacea

[ˌpænəˈsiːə]

A panacea is a remedy, solution, or cure-all for all diseases, problems, or difficulties.

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

vSphere Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. Use Identity Federation to introduce MFA.
4. **Restrict access to vCenter Server to only those who absolutely need it.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

vCenter Server is for **vSphere Admins**

(Workload admins should RDP or SSH into their workloads directly)

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

vSphere Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. Use Identity Federation to introduce MFA.
4. Restrict access to vCenter Server to only those who absolutely need it.
5. **Severely restrict direct access to ESXi. Drive access through vCenter & RBAC model.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

vSphere Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. Use Identity Federation to introduce MFA..
4. Restrict access to vCenter Server to only those who absolutely need it.
5. Severely restrict direct access to ESXi. Drive access through vCenter & RBAC model.
6. **Also restrict access to other infrastructure systems' management interfaces.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

vSphere Authentication & Authorization Best Practices

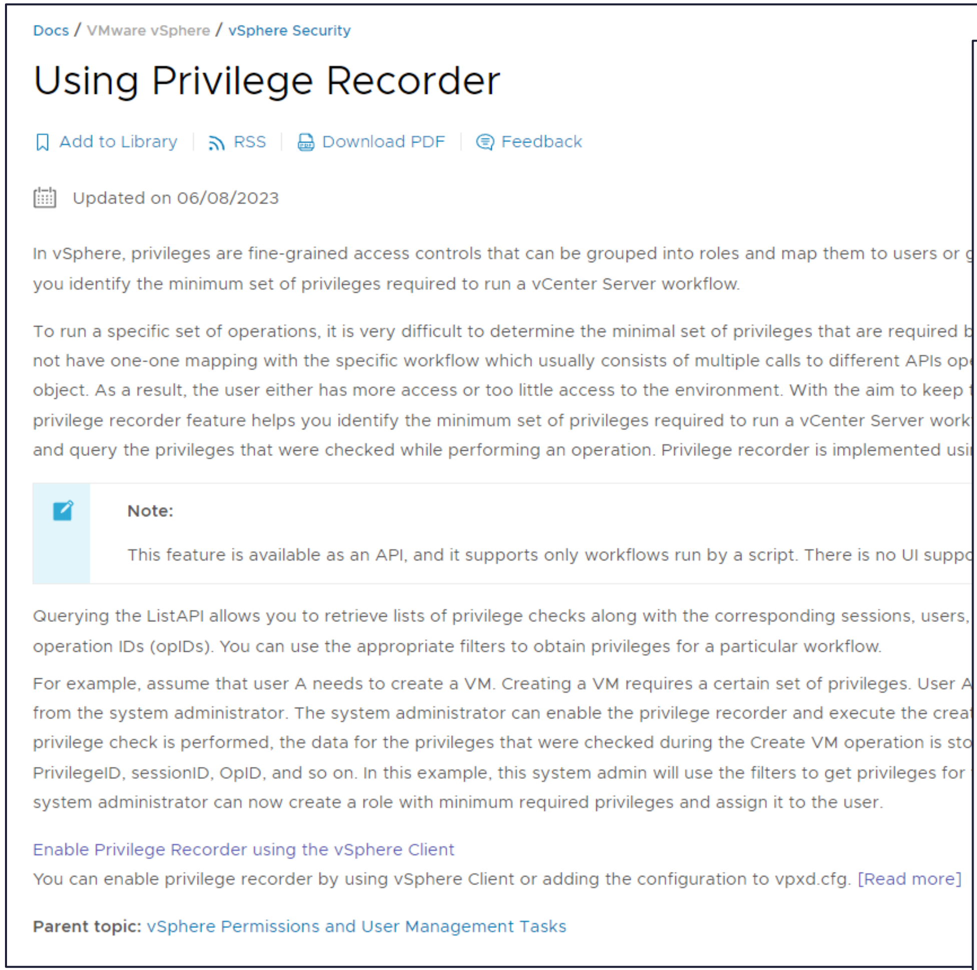
VMware Cloud Foundation Security & Compliance

1. Isolate from corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. Use Identity Federation to introduce MFA..
4. Restrict access to vCenter Server to only those who absolutely need it.
5. Severely restrict direct access to ESXi. Drive access through vCenter & RBAC model.
6. Severely restrict access to other infrastructure systems' management interfaces, too.
7. **Reduce permissions for service accounts to the minimum needed.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Know Exactly What Permissions Were Used

vSphere Privilege Recorder


Docs / VMware vSphere / vSphere Security

Using Privilege Recorder

Add to Library | RSS | Download PDF | Feedback

Updated on 06/08/2023

In vSphere, privileges are fine-grained access controls that can be grouped into roles and map them to users or g
you identify the minimum set of privileges required to run a vCenter Server workflow.

To run a specific set of operations, it is very difficult to determine the minimal set of privileges that are required b
not have one-one mapping with the specific workflow which usually consists of multiple calls to different APIs op
object. As a result, the user either has more access or too little access to the environment. With the aim to keep
privilege recorder feature helps you identify the minimum set of privileges required to run a vCenter Server work
and query the privileges that were checked while performing an operation. Privilege recorder is implemented usi

Note:

This feature is available as an API, and it supports only workflows run by a script. There is no UI suppo

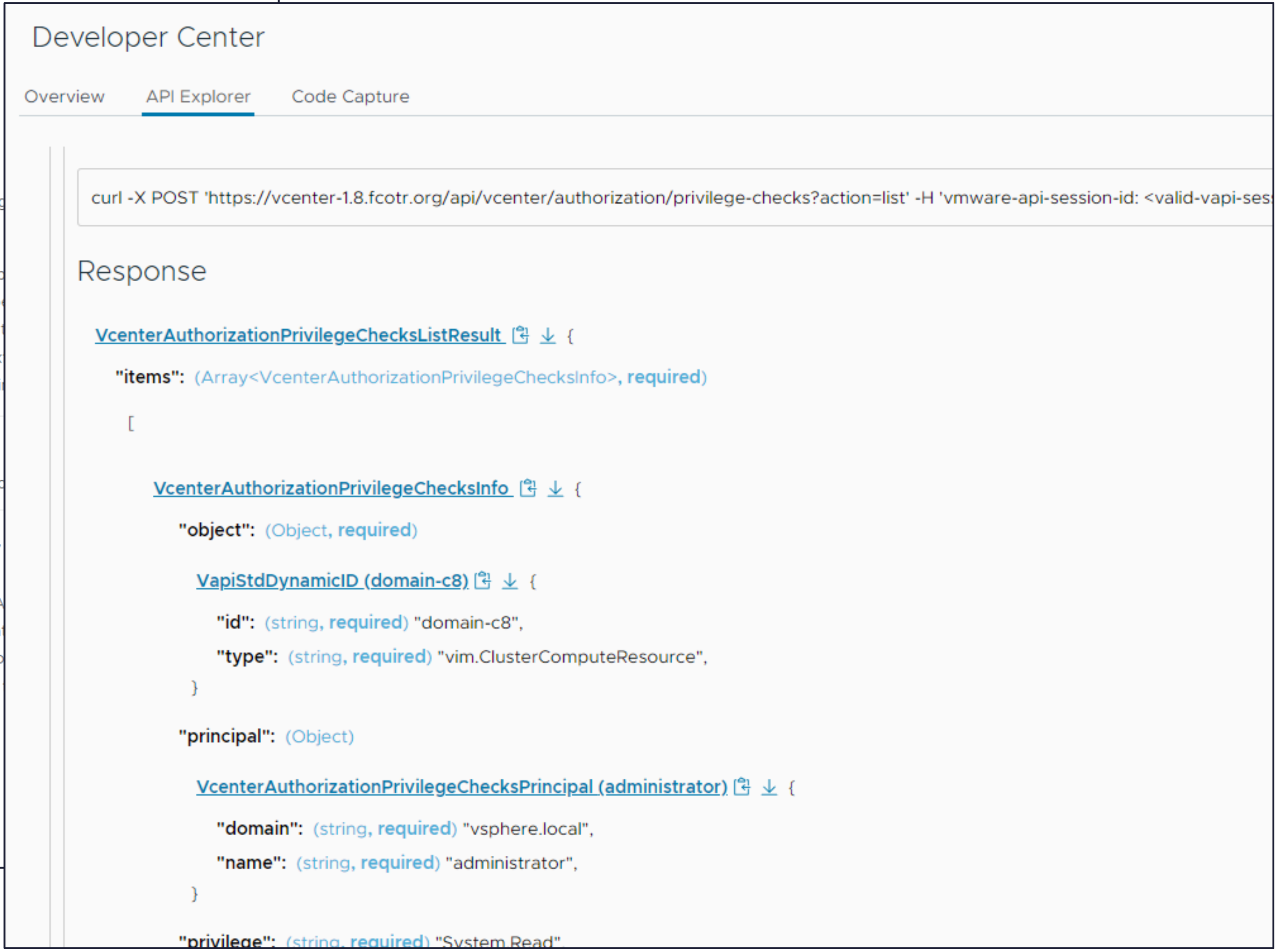
Querying the ListAPI allows you to retrieve lists of privilege checks along with the corresponding sessions, users,
operation IDs (opIDs). You can use the appropriate filters to obtain privileges for a particular workflow.

For example, assume that user A needs to create a VM. Creating a VM requires a certain set of privileges. User A
from the system administrator. The system administrator can enable the privilege recorder and execute the crea
privilege check is performed, the data for the privileges that were checked during the Create VM operation is sto
PrivilegeID, sessionID, OpID, and so on. In this example, this system admin will use the filters to get privileges for
system administrator can now create a role with minimum required privileges and assign it to the user.

Enable Privilege Recorder using the vSphere Client

You can enable privilege recorder by using vSphere Client or adding the configuration to vpxd.cfg. [Read more]

Parent topic: vSphere Permissions and User Management Tasks



```
curl -X POST 'https://vcenter-1.8.fcotr.org/api/vcenter/authorization/privilege-checks?action=list' -H 'vmware-api-session-id: <valid-vapi-ses
```

Response

```
VcenterAuthorizationPrivilegeChecksListResult {
  "items": (Array<VcenterAuthorizationPrivilegeChecksInfo>, required)
   [
      VcenterAuthorizationPrivilegeChecksInfo {
         "object": (Object, required)
           VapiStdDynamicID (domain-c8) {
              "id": (string, required) "domain-c8",
              "type": (string, required) "vim.ClusterComputeResource",
           }
         "principal": (Object)
           VcenterAuthorizationPrivilegeChecksPrincipal (administrator) {
              "domain": (string, required) "vsphere.local",
              "name": (string, required) "administrator",
           }
         "privilege": (string, required) "System.Read",
```

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

vSphere Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. Use Identity Federation to introduce MFA..
4. Restrict access to vCenter Server to only those who absolutely need it.
5. Severely restrict direct access to ESXi. Drive access through vCenter & RBAC model.
6. Severely restrict access to other infrastructure systems' management interfaces, too.
7. Reduce permissions for service accounts to the minimum needed.
8. **Enable IdP advanced features like conditional access, geographic location, phishing-resistant MFA (number matching), and device hygiene.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

vSphere Authentication & Authorization Best Practices

VMware Cloud Foundation Security & Compliance

1. Isolate from corporate/enterprise IdPs.
2. If reasonable, do authorization inside vSphere/VCF, not inside your IdP.
3. Use Identity Federation to introduce MFA..
4. Restrict access to vCenter Server to only those who absolutely need it.
5. Severely restrict direct access to ESXi. Drive access through vCenter & RBAC model
6. Severely restrict access to other infrastructure systems' management interfaces, too.
7. Reduce permissions for service accounts to the minimum needed.
8. Enable IdP advanced features like conditional access, geographic location, phishing-resistant MFA (number matching), and device hygiene.
9. **Ensure access logs are being retained in your IdP, for as long as possible.**

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

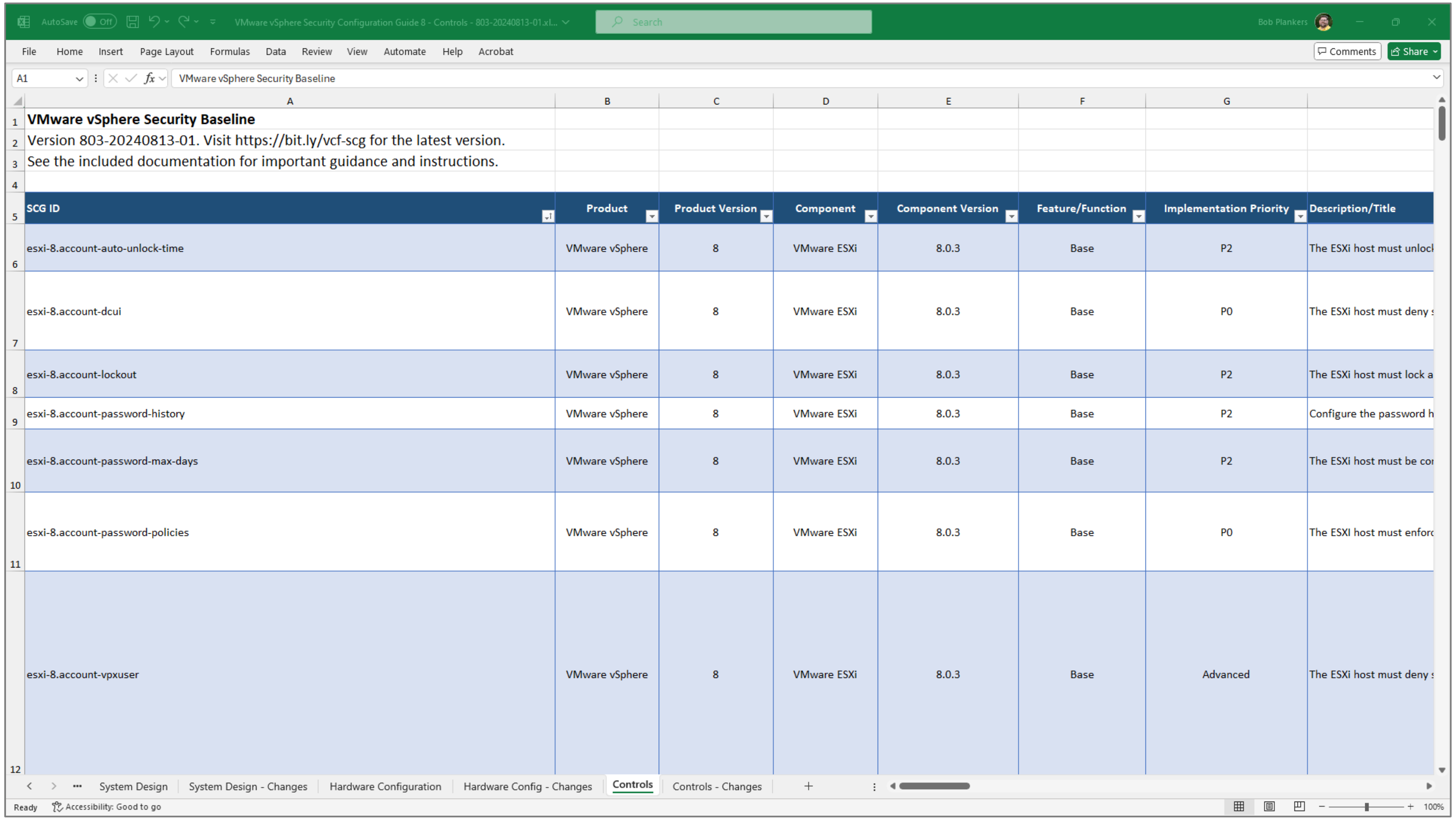
EXPLORE

Using Hardening Guidance

Designing Hardened Systems

“An Ounce of Prevention is Worth a Pound of Cure”

VMware Cloud Foundation Security & Compliance



VMware vSphere Security Baseline

Version 803-20240813-01. Visit https://bit.ly/vcf-scg for the latest version.

See the included documentation for important guidance and instructions.

SCG ID	Product	Product Version	Component	Component Version	Feature/Function	Implementation Priority	Description/Title
esxi-8.account-auto-unlock-time	VMware vSphere	8	VMware ESXi	8.0.3	Base	P2	The ESXi host must unloc
esxi-8.account-dcui	VMware vSphere	8	VMware ESXi	8.0.3	Base	P0	The ESXi host must deny
esxi-8.account-lockout	VMware vSphere	8	VMware ESXi	8.0.3	Base	P2	The ESXi host must lock a
esxi-8.account-password-history	VMware vSphere	8	VMware ESXi	8.0.3	Base	P2	Configure the password
esxi-8.account-password-max-days	VMware vSphere	8	VMware ESXi	8.0.3	Base	P2	The ESXi host must be co
esxi-8.account-password-policies	VMware vSphere	8	VMware ESXi	8.0.3	Base	P0	The ESXI host must enforc
esxi-8.account-vpxuser	VMware vSphere	8	VMware ESXi	8.0.3	Base	Advanced	The ESXi host must deny

Easy to understand hardening guidance

Now includes vSAN services

Maps differences to STIG and PCI

New scripts to audit and remediate!

EXPLORE

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Implementation Priority Helps Admins Prioritize

VMware Cloud Foundation Security & Compliance

P0

Do this first

Control does not have a secure default

P1

Do this second

Control is secure but default could be better

P2

Audit These

Default is secure but make sure it didn’t change

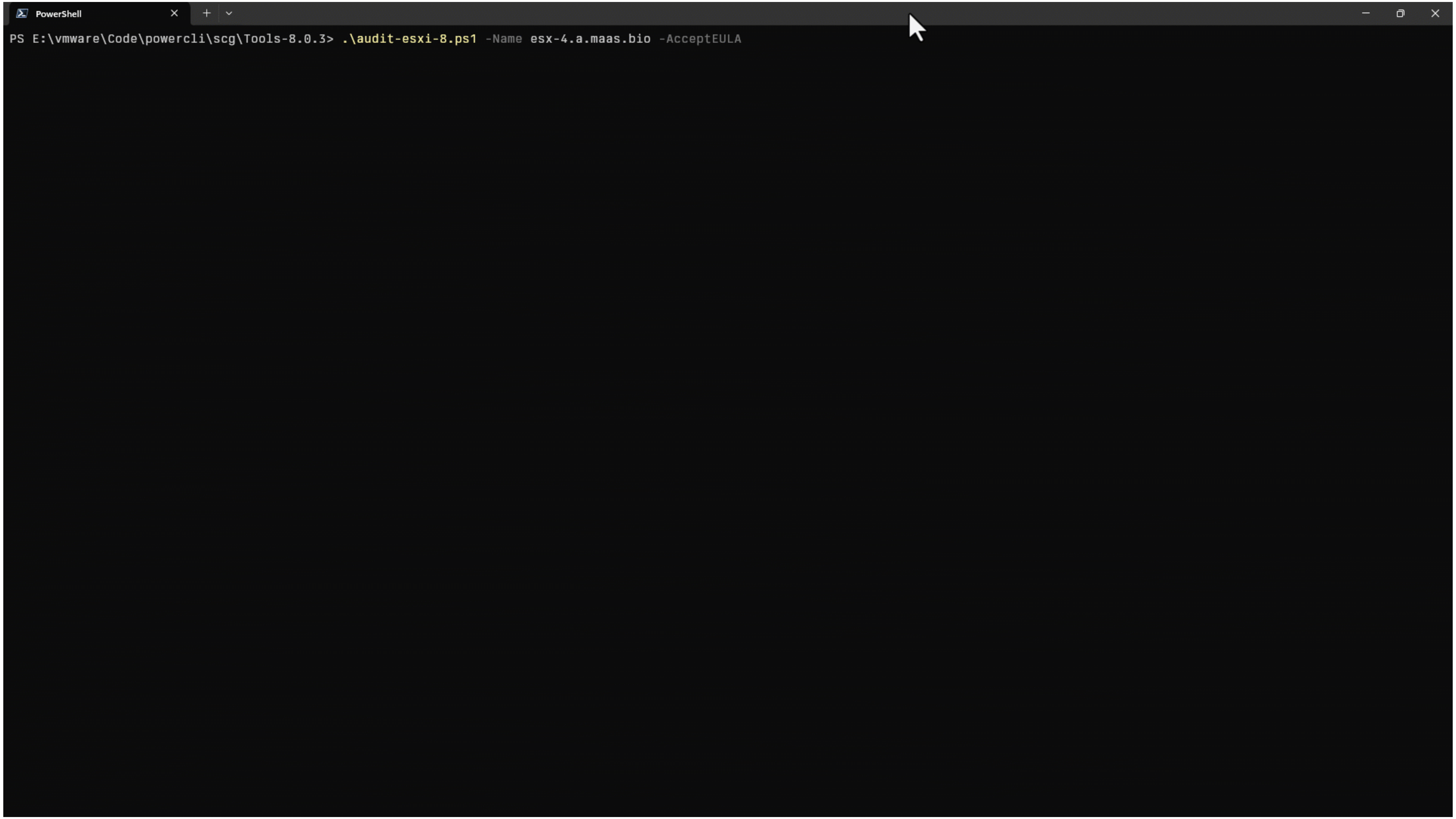
Advanced

Use Care

New and may have process or technology issues

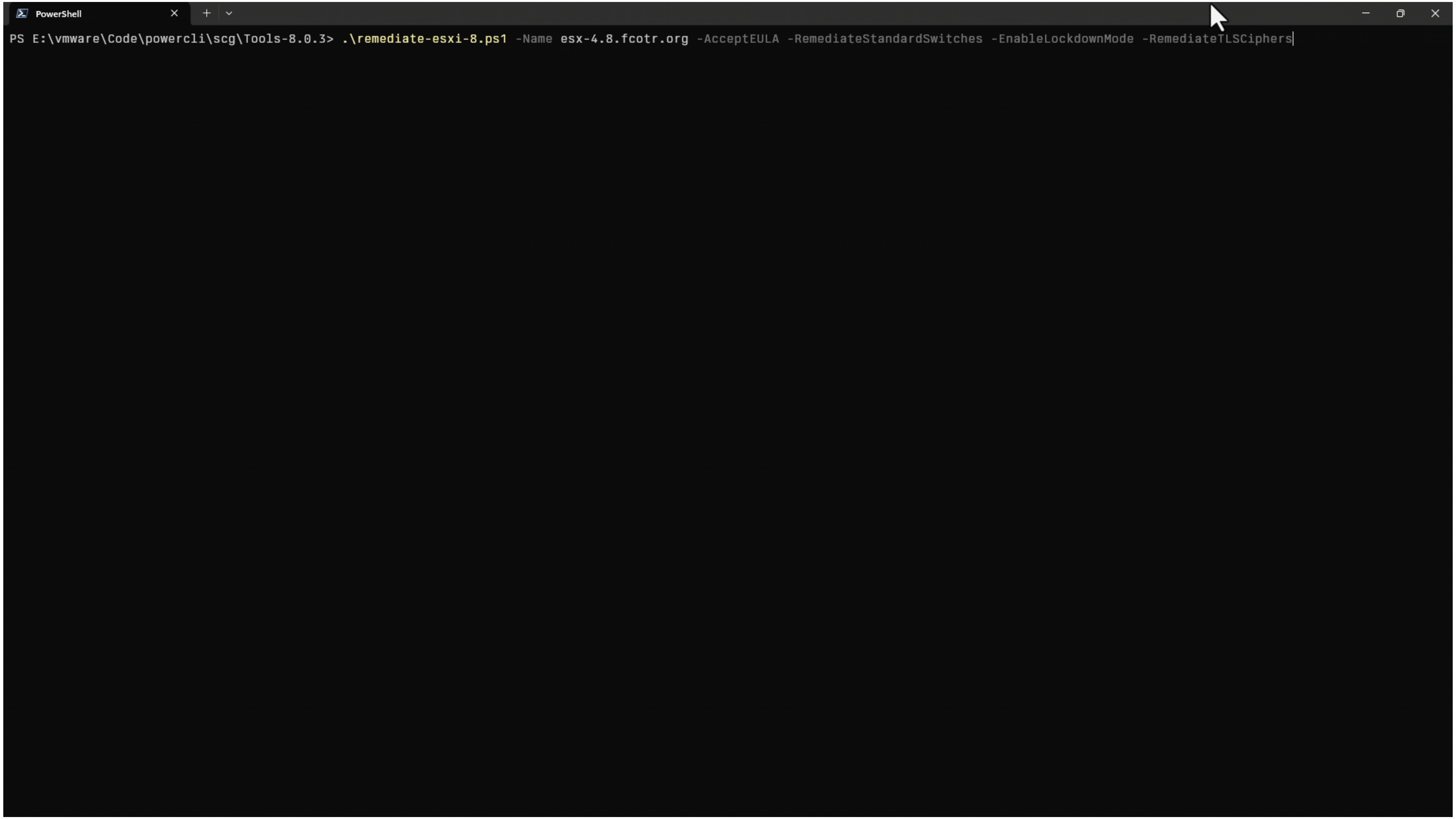
EXPLORE

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



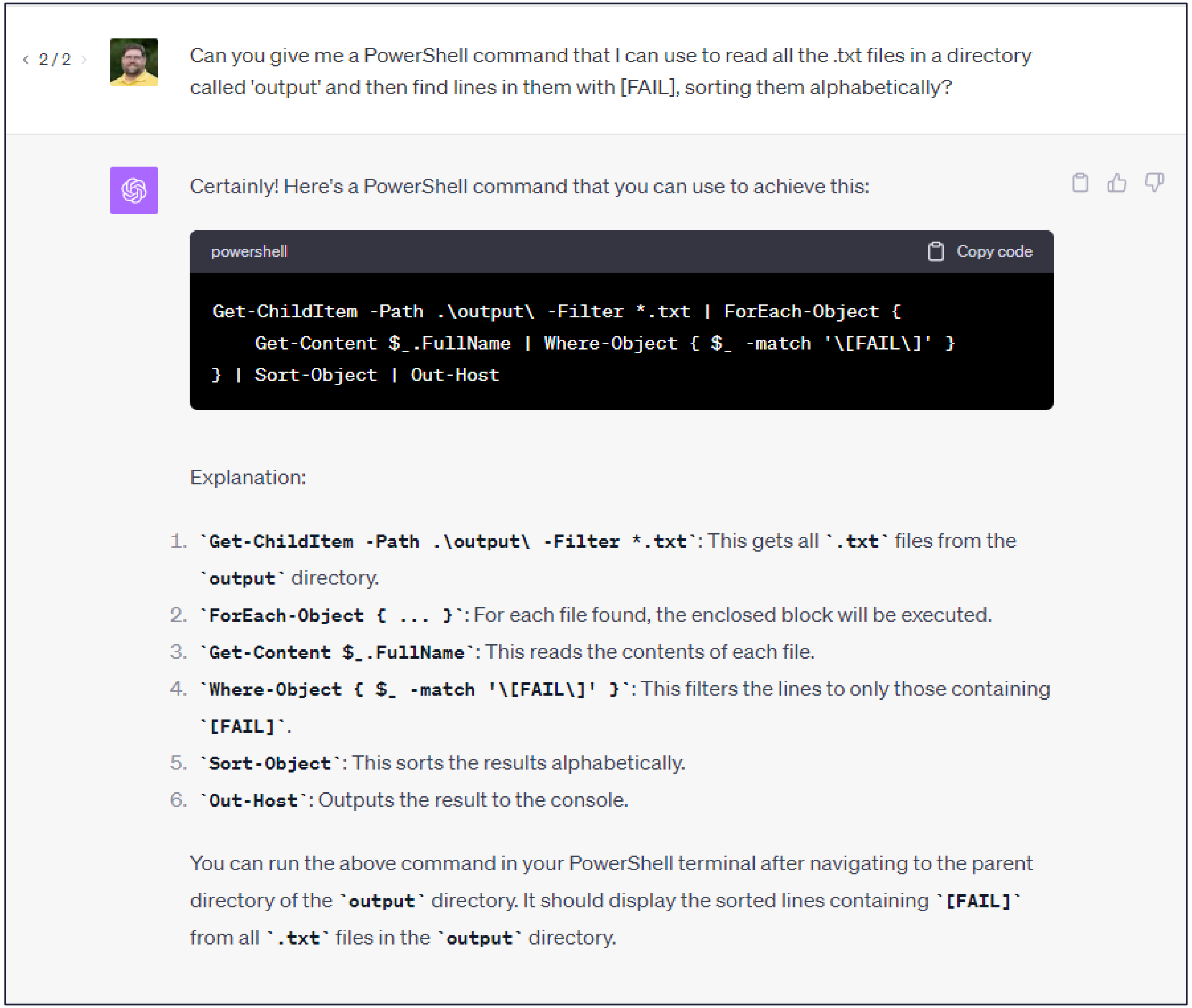
```
PS E:\vmware\Code\powercli\scg\Tools-8.0.3> .\audit-esxi-8.ps1 -Name esx-4.a.maas.bio -AcceptEULA
```

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



```
PS E:\vmware\Code\powercli\scg\Tools-8.0.3> .\remediate-esxi-8.ps1 -Name esx-4.8.fcotr.org -AcceptEULA -RemediateStandardSwitches -EnableLockdownMode -RemediateTLSCiphers
```

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



Can you give me a PowerShell command that I can use to read all the .txt files in a directory called 'output' and then find lines in them with [FAIL], sorting them alphabetically?

Certainly! Here's a PowerShell command that you can use to achieve this:

```powershell
Get-ChildItem -Path .\output\ -Filter *.txt | ForEach-Object {
    Get-Content $_.FullName | Where-Object { $_ -match '\[FAIL\]' }
} | Sort-Object | Out-Host
```

Explanation:

1. `Get-ChildItem -Path .\output\ -Filter *.txt`: This gets all `.txt` files from the `output` directory.
2. `ForEach-Object { ... }`: For each file found, the enclosed block will be executed.
3. `Get-Content $_.FullName`: This reads the contents of each file.
4. `Where-Object { $_ -match '\[FAIL\]' }`: This filters the lines to only those containing `[FAIL]`.
5. `Sort-Object`: This sorts the results alphabetically.
6. `Out-Host`: Outputs the result to the console.

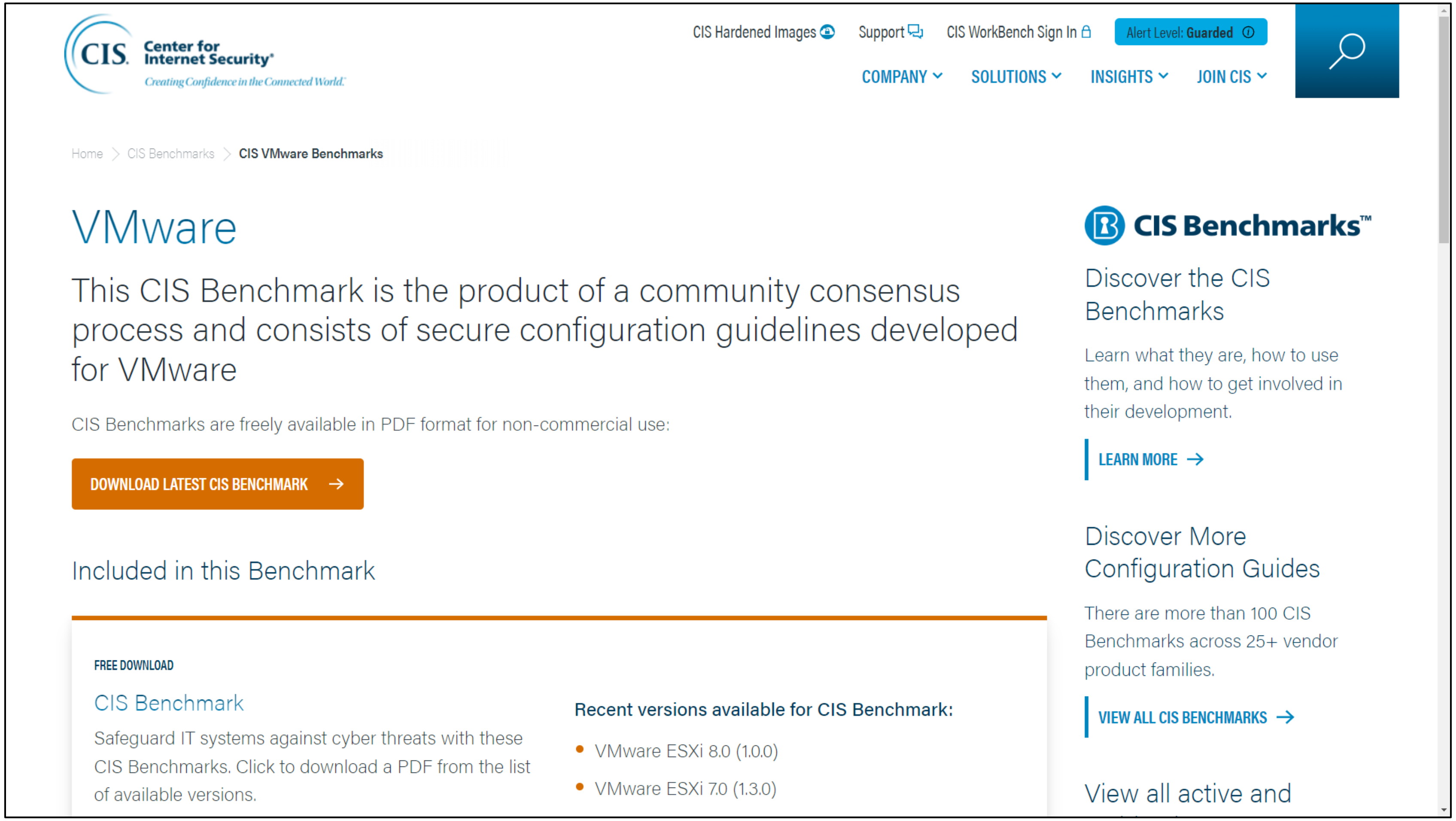
You can run the above command in your PowerShell terminal after navigating to the parent directory of the `output` directory. It should display the sorted lines containing `[FAIL]` from all `.txt` files in the `output` directory.

EXPLORE

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Center for Internet Security (CIS) Benchmark

VMware Cloud Foundation Security & Compliance



VMware

This CIS Benchmark is the product of a community consensus process and consists of secure configuration guidelines developed for VMware

CIS Benchmarks are freely available in PDF format for non-commercial use:

Included in this Benchmark

FREE DOWNLOAD

CIS Benchmark

Safeguard IT systems against cyber threats with these CIS Benchmarks. Click to download a PDF from the list of available versions.

Recent versions available for CIS Benchmark:

- VMware ESXi 8.0 (1.0.0)
- VMware ESXi 7.0 (1.3.0)

CIS Benchmarks™

Discover the CIS Benchmarks

Learn what they are, how to use them, and how to get involved in their development.

Discover More Configuration Guides

There are more than 100 CIS Benchmarks across 25+ vendor product families.

View all active and

ESXi 8 **synchronized with our guidance**

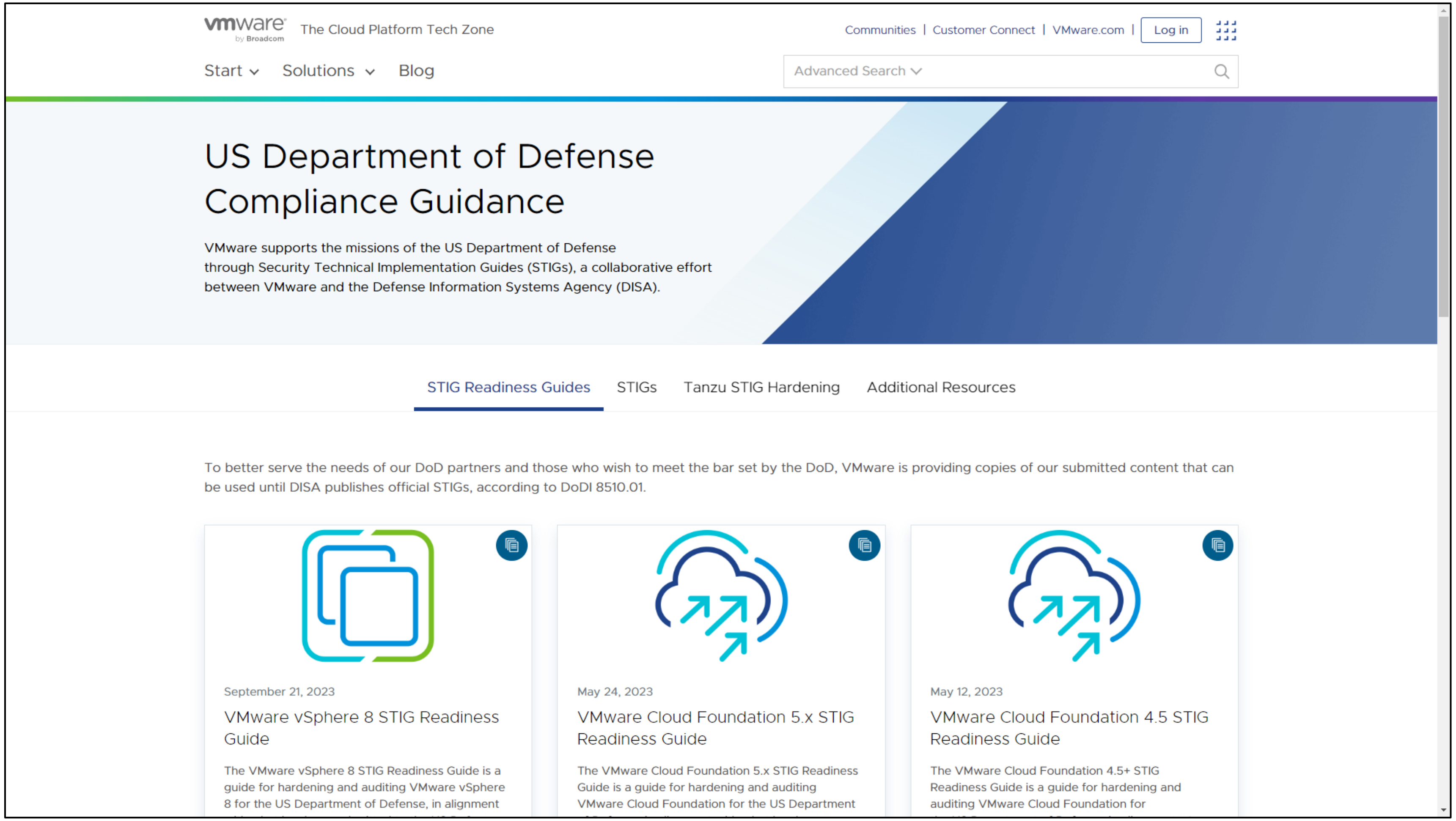
CIS Benchmark for ESXi 7 left as-is due to adoption

Only for VMware ESX! Does not include other components!

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

US Department of Defense Guidance (DISA STIG)

VMware Cloud Foundation Security & Compliance


vmware by Broadcom
The Cloud Platform Tech Zone
Communities | Customer Connect | VMware.com | Log in
Start
Solutions
Blog
Advanced Search

US Department of Defense Compliance Guidance

VMware supports the missions of the US Department of Defense through Security Technical Implementation Guides (STIGs), a collaborative effort between VMware and the Defense Information Systems Agency (DISA).

To better serve the needs of our DoD partners and those who wish to meet the bar set by the DoD, VMware is providing copies of our submitted content that can be used until DISA publishes official STIGs, according to DoDI 8510.01.

September 21, 2023

VMware vSphere 8 STIG Readiness Guide

The VMware vSphere 8 STIG Readiness Guide is a guide for hardening and auditing VMware vSphere 8 for the US Department of Defense, in alignment

May 24, 2023

VMware Cloud Foundation 5.x STIG Readiness Guide

The VMware Cloud Foundation 5.x STIG Readiness Guide is a guide for hardening and auditing VMware Cloud Foundation for the US Department

May 12, 2023

VMware Cloud Foundation 4.5 STIG Readiness Guide

The VMware Cloud Foundation 4.5+ STIG Readiness Guide is a guide for hardening and auditing VMware Cloud Foundation for

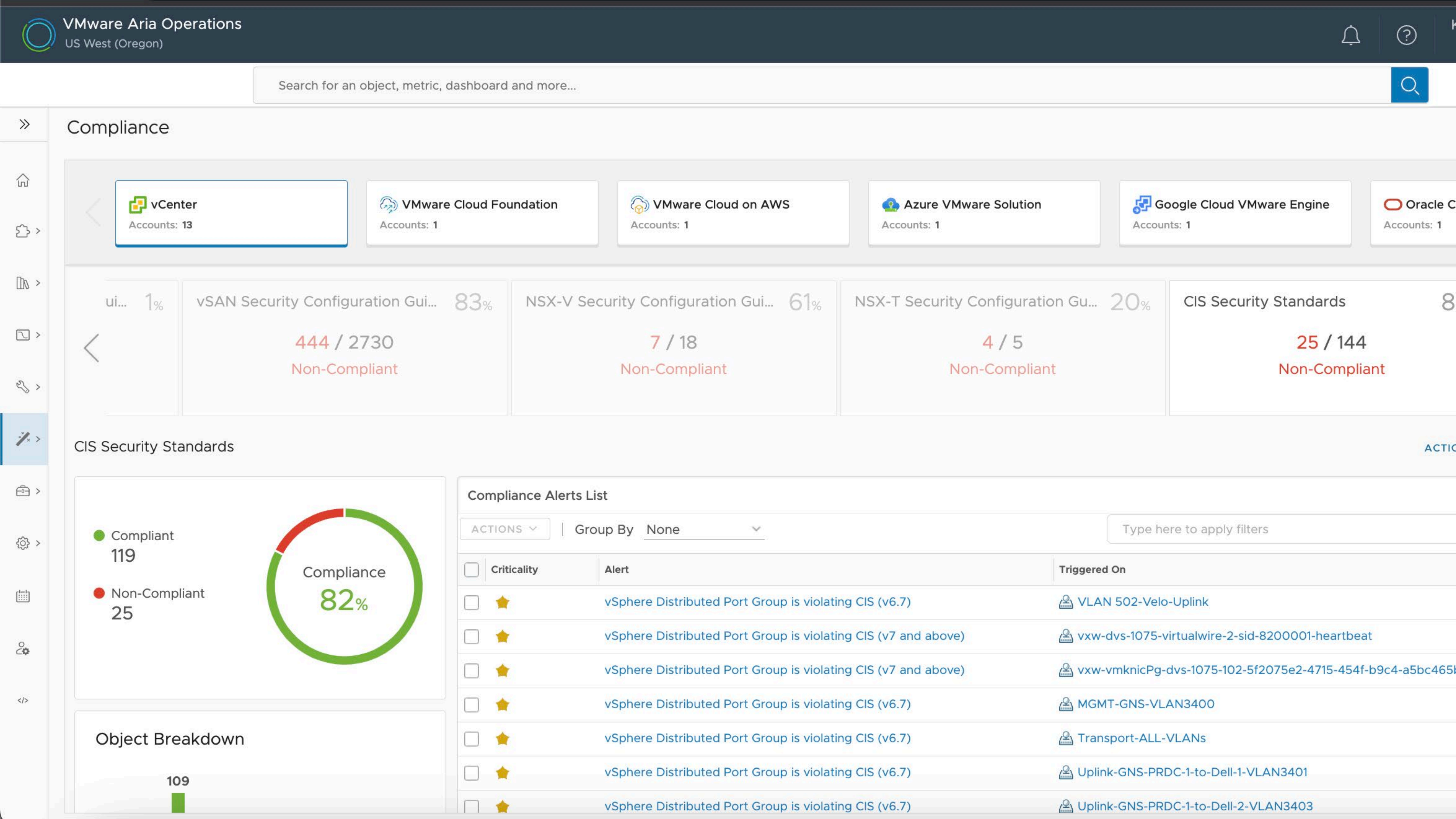
Intended for use by US DoD and affiliates

Official STIGs come from public.cyber.mil

Readiness Guides are materials that have or will be submitted

Need STIG Viewer to view

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



Compliance

Benchmark	%	Non-Compliant
ui...	1%	
vSAN Security Configuration Gui...	83%	444 / 2730 Non-Compliant
NSX-V Security Configuration Gui...	61%	7 / 18 Non-Compliant
NSX-T Security Configuration Gu...	20%	4 / 5 Non-Compliant
CIS Security Standards	8	25 / 144 Non-Compliant

CIS Security Standards

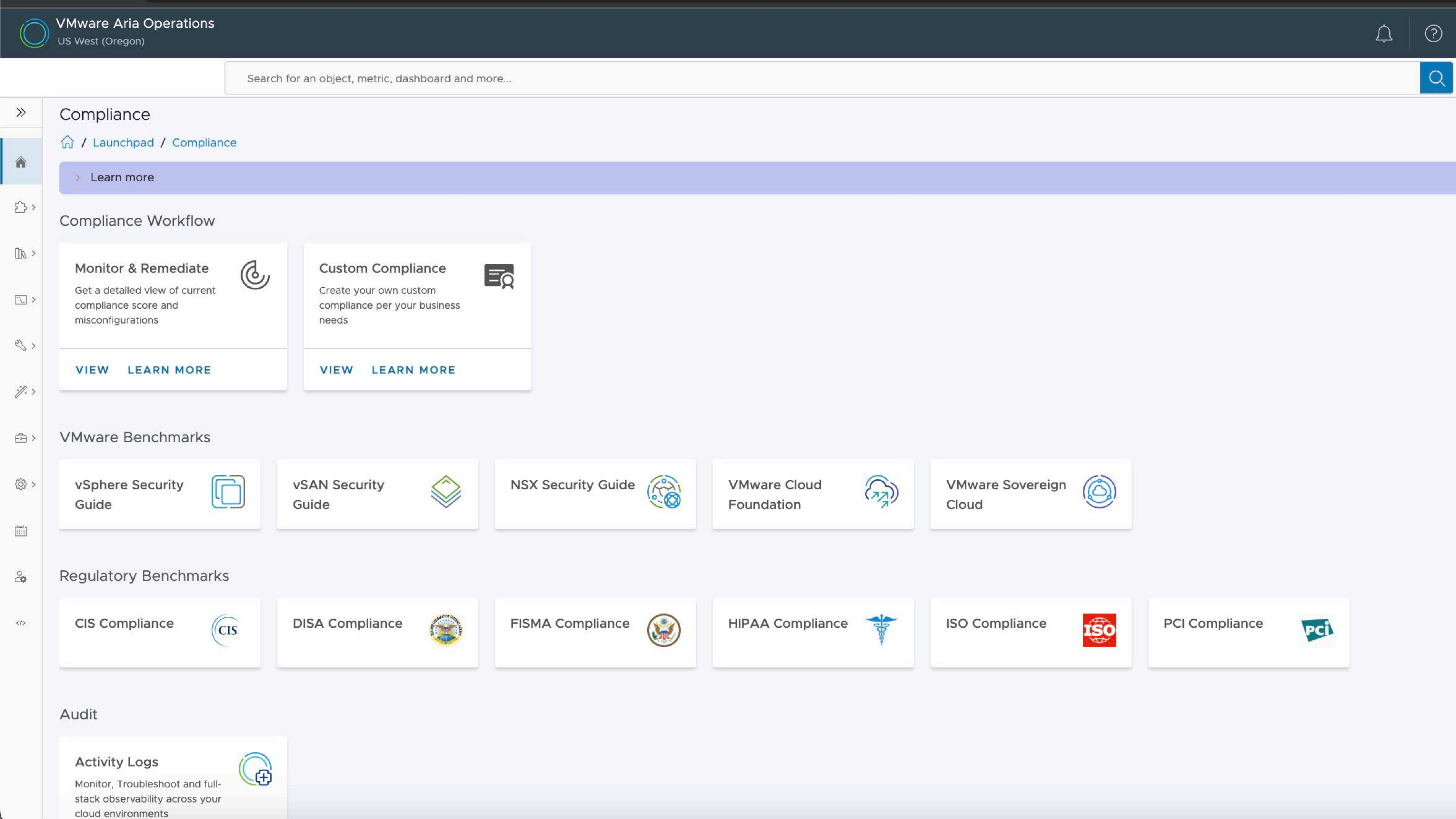
● Compliant
119

● Non-Compliant
25

Object Breakdown

Compliance Alerts List

☐	Criticality	Alert	Triggered On
☐	★	vSphere Distributed Port Group is violating CIS (v6.7)	VLAN 502-Velo-Uplink
☐	★	vSphere Distributed Port Group is violating CIS (v7 and above)	vxw-dvs-1075-virtualwire-2-sid-8200001-heartbeat
☐	★	vSphere Distributed Port Group is violating CIS (v7 and above)	vxw-vmknicPg-dvs-1075-102-5f2075e2-4715-454f-b9c4-a5bc465
☐	★	vSphere Distributed Port Group is violating CIS (v6.7)	MGMT-GNS-VLAN3400
☐	★	vSphere Distributed Port Group is violating CIS (v6.7)	Transport-ALL-VLANs
☐	★	vSphere Distributed Port Group is violating CIS (v6.7)	Uplink-GNS-PRDC-1-to-Dell-1-VLAN3401
☐	★	vSphere Distributed Port Group is violating CIS (v6.7)	Uplink-GNS-PRDC-1-to-Dell-2-VLAN3403



VMware Aria Operations
US West (Oregon)

Search for an object, metric, dashboard and more...

Compliance

Launchpad / Compliance

Learn more

Compliance Workflow

Monitor & Remediate
Get a detailed view of current compliance score and misconfigurations
VIEW LEARN MORE

Custom Compliance
Create your own custom compliance per your business needs
VIEW LEARN MORE

VMware Benchmarks

- vSphere Security Guide
- vSAN Security Guide
- NSX Security Guide
- VMware Cloud Foundation
- VMware Sovereign Cloud

Regulatory Benchmarks

- CIS Compliance
- DISA Compliance
- FISMA Compliance
- HIPAA Compliance
- ISO Compliance
- PCI Compliance

Audit

Activity Logs
Monitor, Troubleshoot and full-stack observability across your cloud environments

EXPLORE

Wrapping Up

Designing Hardened Systems

Keep it simple;
Complexity is our enemy

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Don’t tie things together unless you absolutely have to

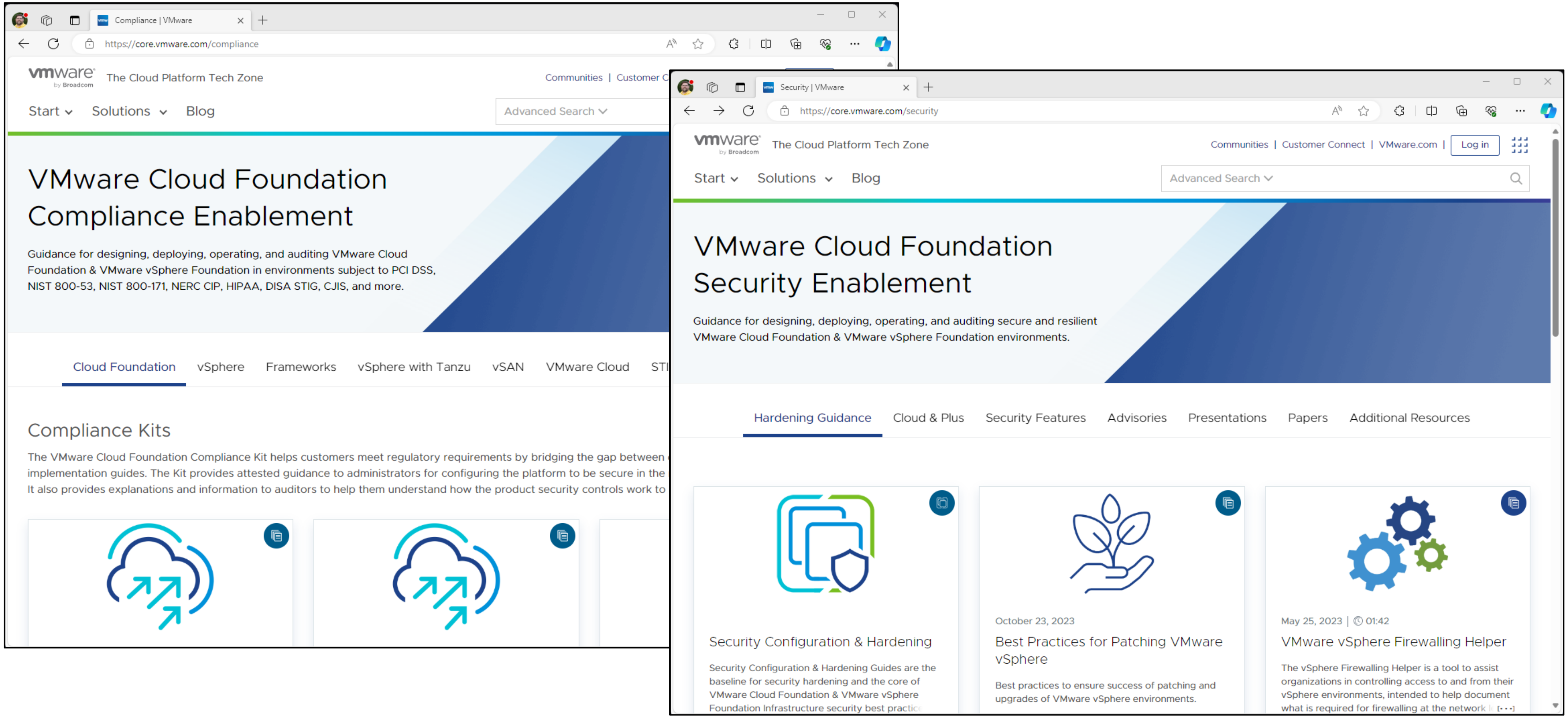
Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

“Baby steps”

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

https://bit.ly/vcf-security

Security & Compliance Resources for VMware Cloud Foundation



VMware Cloud Foundation Compliance Enablement

Guidance for designing, deploying, operating, and auditing VMware Cloud Foundation & VMware vSphere Foundation in environments subject to PCI DSS, NIST 800-53, NIST 800-171, NERC CIP, HIPAA, DISA STIG, CJIS, and more.

Compliance Kits

The VMware Cloud Foundation Compliance Kit helps customers meet regulatory requirements by bridging the gap between
implementation guides. The Kit provides attested guidance to administrators for configuring the platform to be secure in the
It also provides explanations and information to auditors to help them understand how the product security controls work to

VMware Cloud Foundation Security Enablement

Guidance for designing, deploying, operating, and auditing secure and resilient VMware Cloud Foundation & VMware vSphere Foundation environments.

Security Configuration & Hardening

Security Configuration & Hardening Guides are the baseline for security hardening and the core of VMware Cloud Foundation & VMware vSphere Foundation Infrastructure security best practic

October 23, 2023

Best Practices for Patching VMware vSphere

Best practices to ensure success of patching and upgrades of VMware vSphere environments.

May 25, 2023 | 01:42

VMware vSphere Firewalling Helper

The vSphere Firewalling Helper is a tool to assist organizations in controlling access to and from their vSphere environments, intended to help document what is required for firewalling at the network [...]

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

EXPLORE

Please take your survey.

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

EXPLORE

Thank you

Broadcom Proprietary and Confidential. Copyright © 2024 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.