

# VMware vSphere Certificate Management

Concepts, Introduction, and Q&A

Bob Plankers

Cloud Infrastructure Security & Compliance, VMware

June 2023



# Disclaimer

This document is intended to provide general guidance for organizations that are considering VMware solutions. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided “AS IS.”

VMware makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein.

Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.



# Agenda

Introduction to TLS, Certificates, and Trust

What do we think certificates really do for us?

Certificates Inside vSphere

How does vSphere consume certificates?

Resources

Links to Cloud Infrastructure security materials

Questions + Answers

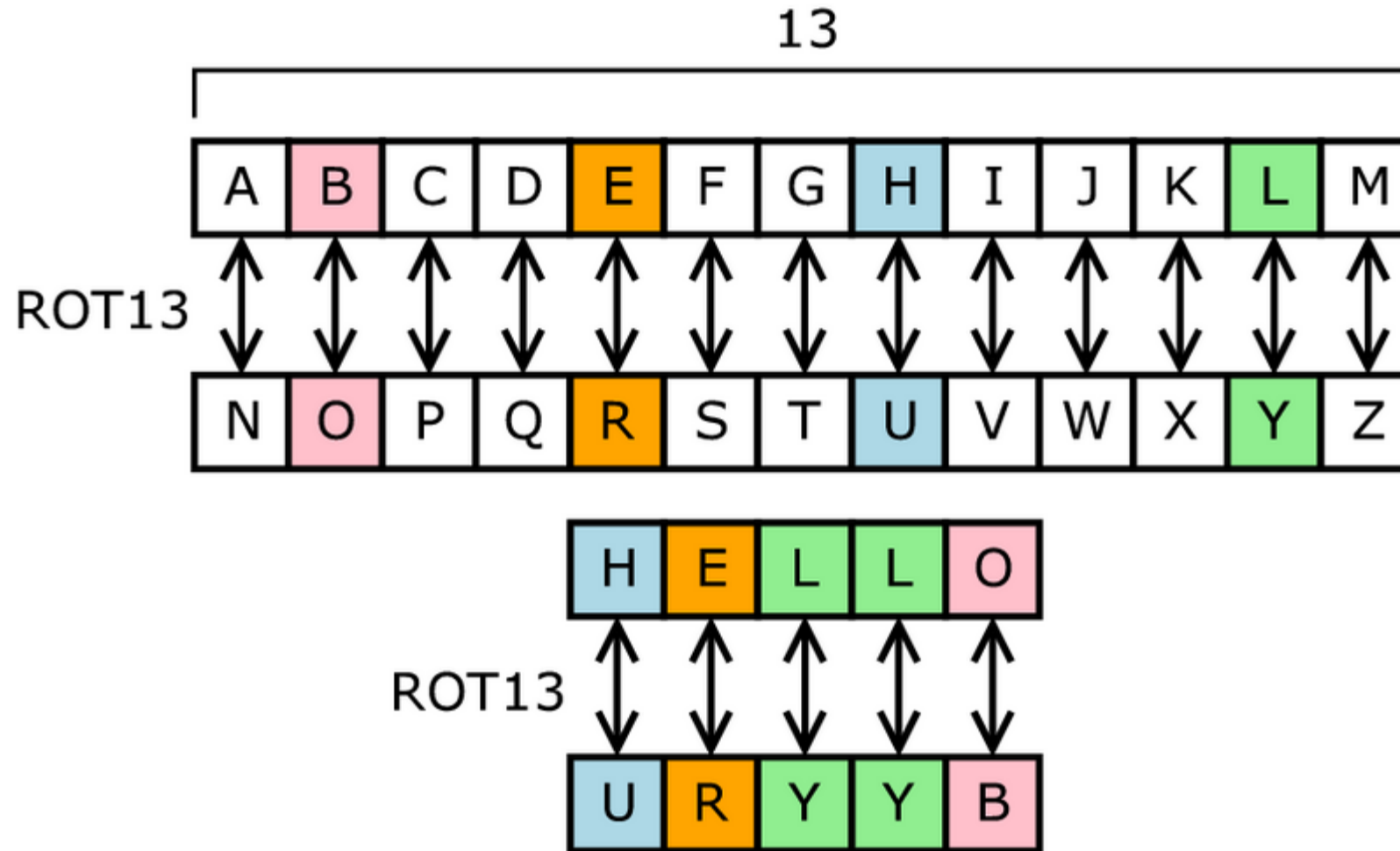
Real questions we get, and how we answer them

# Introduction to TLS, Certificates, and Trust



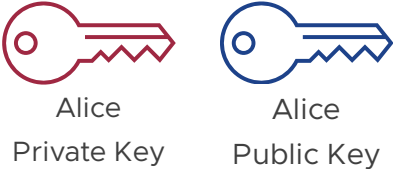
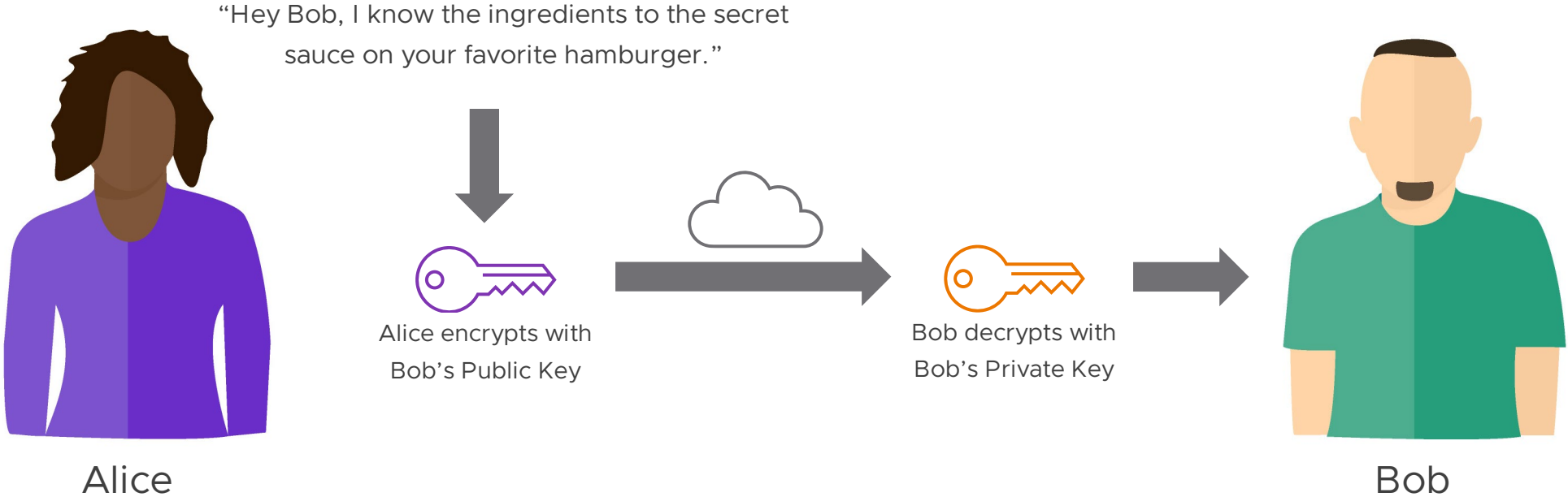
# How Do You Exchange Keys With Someone You Don't Know?

How do you agree on a secret?



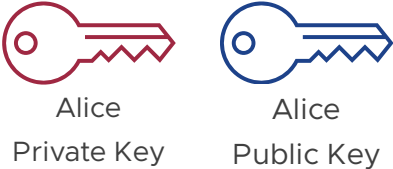
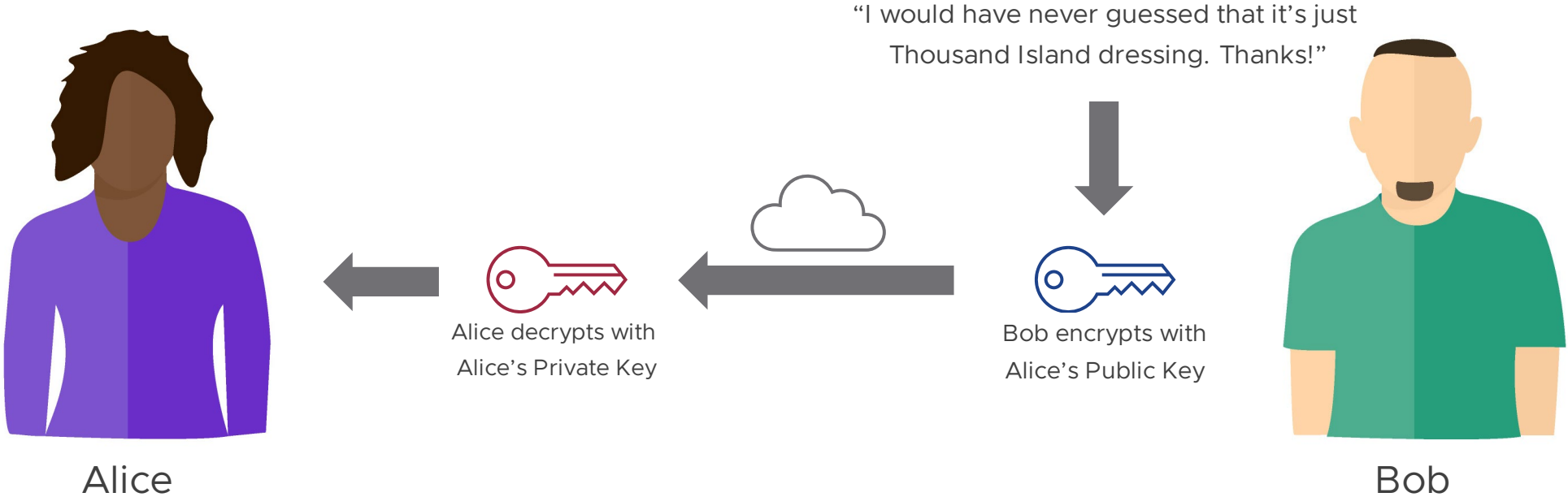
# Public-Key Cryptography

Secure Communications With Someone You Cannot Talk To First



# Public-Key Cryptography

Secure Communications With Someone You Cannot Talk To First



# Certificates Enable Transport Layer Security (TLS)

They contain the public key and other information to establish “trust”

Certificate

	*.vmware.com	DigiCert SHA2 Secure Server CA	DigiCert Global Root CA
<b>Subject Name</b>			
Country	US		
State/Province	California		
Locality	Palo Alto		
Organization	VMware, Inc.		
Common Name	*.vmware.com		
<b>Issuer Name</b>			
Country	US		
Organization	DigiCert Inc		
Common Name	DigiCert SHA2 Secure Server CA		
<b>Validity</b>			
Not Before	Tue, 29 Jun 2021 00:00:00 GMT		
Not After	Thu, 07 Jul 2022 23:59:59 GMT		

Domain name

Alternate names

Organization

Issuing Certificate Authority

Issue Date

Expiration Date

Public Key

Digital Signature by the Certificate Authority







# Let's Encrypt

Not  
"Let's Trust"




Opinion,  
not fact

### Connection is secure ✕

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.  
[Learn more](#)

 Flash	Ask (default) ▼
 Pop-ups and redirects	Allow ▼

---

-  Certificate (Valid)
-  Cookies (1 in use)
-  Site settings

Opinion,  
not fact

⚠ Not secure 192.168.20.254

**Your connection to this site is not secure** ✕

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. [Learn more](#)

⚙ Flash Ask (default) ▼

---

📄 Certificate (Invalid)

🍪 Cookies (0 in use)

⚙ Site settings

## QUESTION

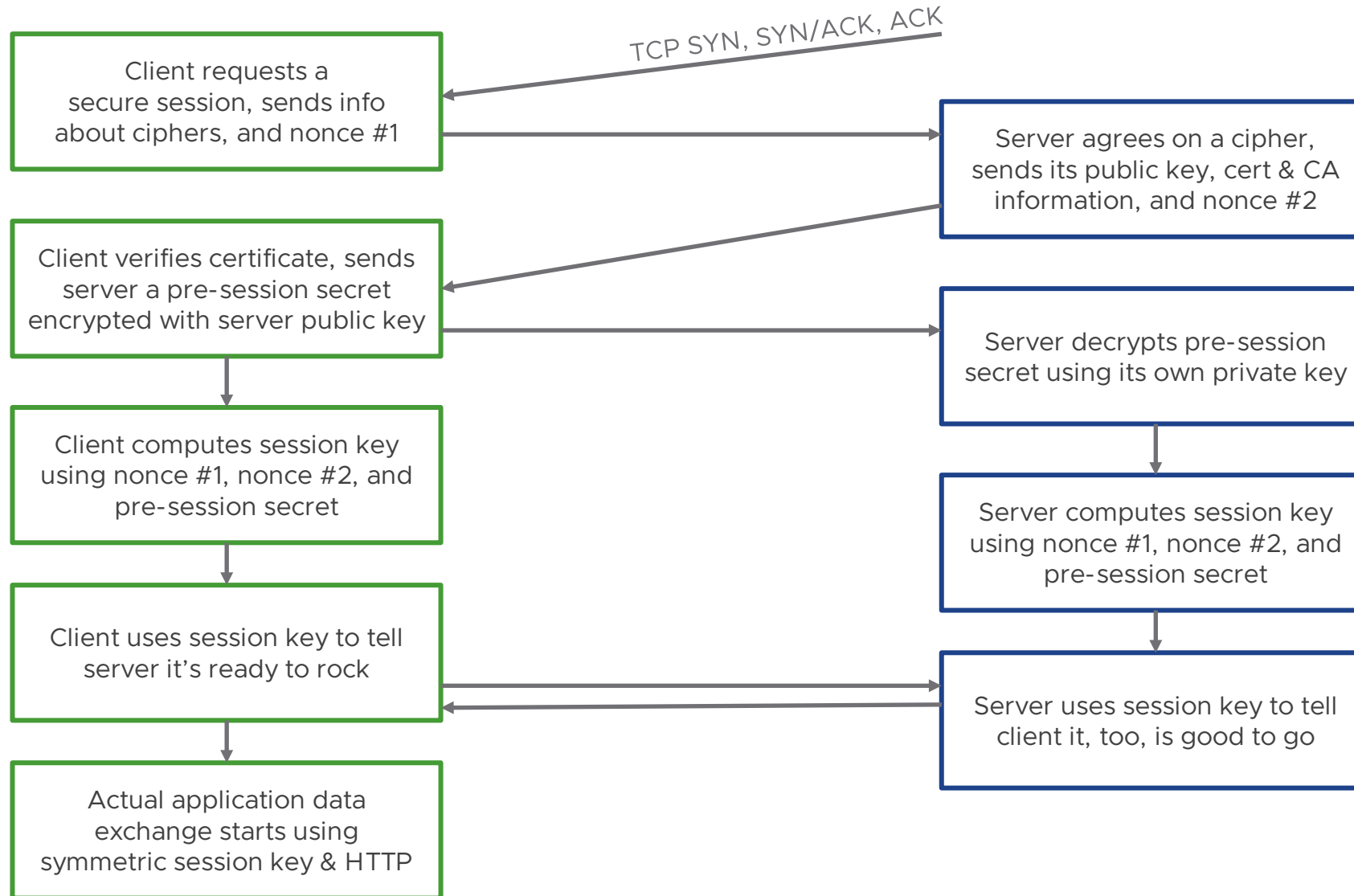
Actually... TLS doesn't use public keys for most of its transmissions, though.

---

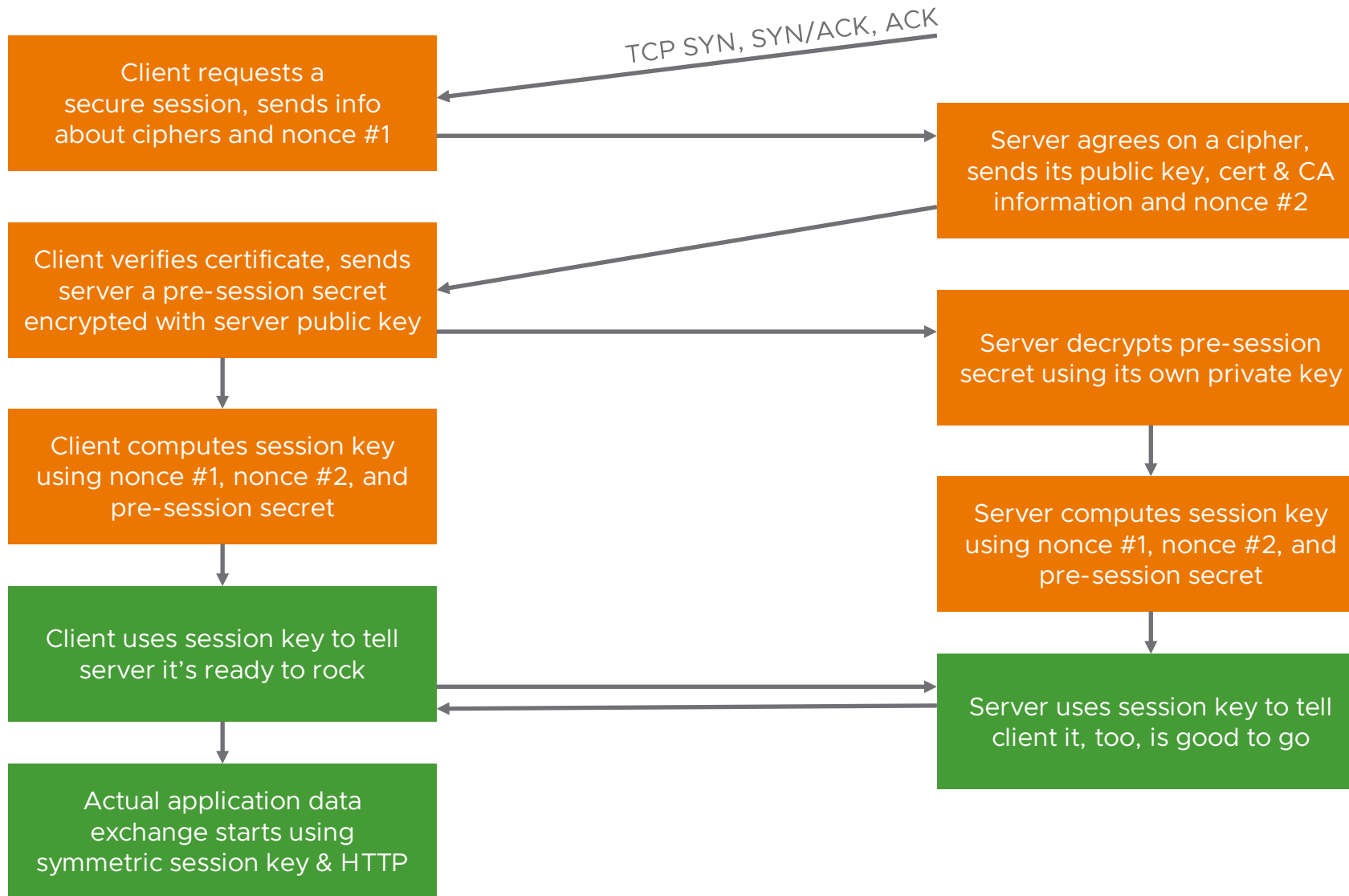
## ANSWER

Correct. Public key cryptography is extremely expensive in terms of computing power, so it is just used to exchange a one-time use symmetric key (a nonce). The nonce is then used as a session key for all the other encryption.

# How TLS Works



# High Computational Expense



Who, exactly, cares  
about trust at the  
infrastructure level?



# Who Cares About vSphere Certificates?

## Three Main Populations with Differing Motives

### Infrastructure Admins

---

They know network encryption is a good thing on its own

“NOT SECURE” can be a hint that something is wrong or misconfigured

Understand that padlocks & green status bars do not mean a system is secure

Have a lot to worry about beyond certificates, with limited lifespan



# Who Cares About vSphere Certificates?

## Three Main Populations with Differing Motives

### Infrastructure Admins

---

They know network encryption is a good thing on its own

“NOT SECURE” can be a hint that something is wrong or misconfigured

Understand that padlocks & green status bars do not mean a system is secure

Have a lot to worry about beyond certificates, with limited lifespan

### Infosec/Auditors/PKI

---

Recommend corporate policy to CISO/CIO & audit for compliance

Concerned with risk & “blast radius” of compromised crypto material

Generally, no direct stake in day-to-day infrastructure administration operations

Generally smaller understanding of vSphere, VMware Cloud, etc.

# Who Cares About vSphere Certificates?

## Three Main Populations with Differing Motives

### Infrastructure Admins

---

They know network encryption is a good thing on its own

“NOT SECURE” can be a hint that something is wrong or misconfigured

Understand that padlocks & green status bars do not mean a system is secure

Have a lot to worry about beyond certificates, with limited lifespan

### Infosec/Auditors/PKI

---

Recommend corporate policy to CISO/CIO & audit for compliance

Concerned with risk & “blast radius” of compromised crypto material

Generally, no direct stake in day-to-day infrastructure administration operations

Generally smaller understanding of vSphere, VMware Cloud, etc.

### Organization & Leadership

---

Cares deeply about risk, will heed scary stories from CISO

Wants to pass audits so they can keep taking credit cards & getting paid (or do health care, or generate power, or DoD, etc.)

Generally, has no need to access infrastructure management interfaces directly

# Certificates Inside VMware Cloud Infrastructure

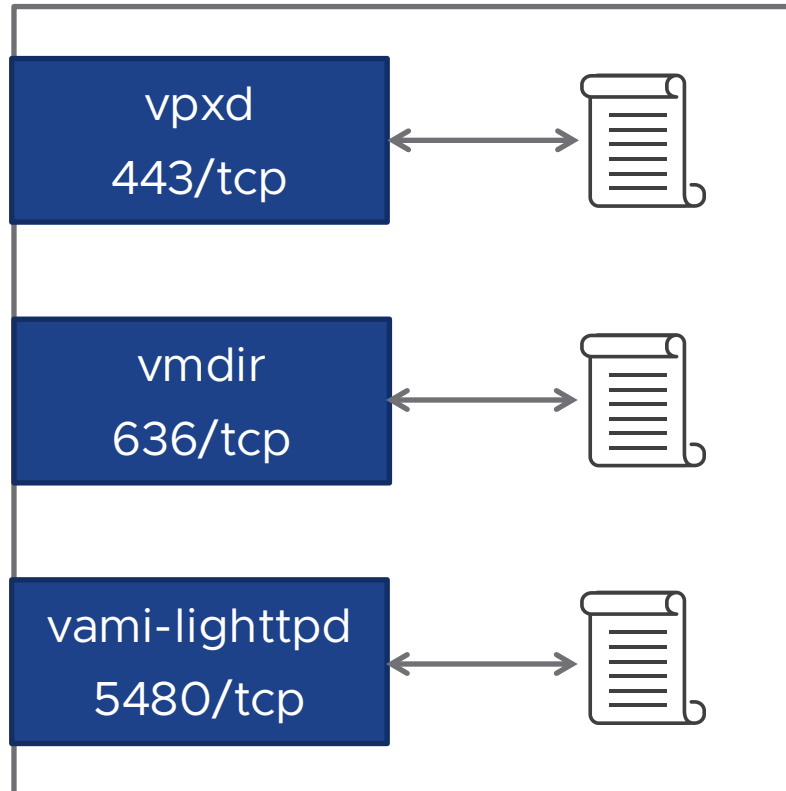


# VMware Certificate Authority (VMCA)



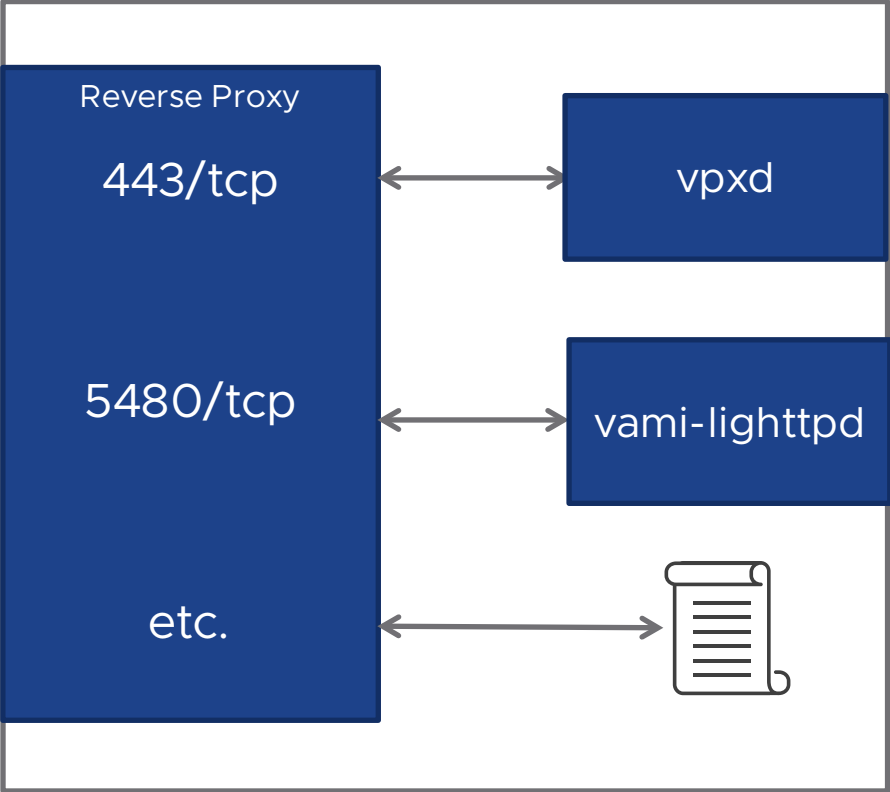
# Old Way: One Certificate Per Service in vSphere 6.x

No Wildcards



# Better: vSphere 7 Reverse Proxy Makes Life Easier

Still No Wildcards



# The Virtualization Admin Establishes Trust

Encryption is Automated; Trust is Not

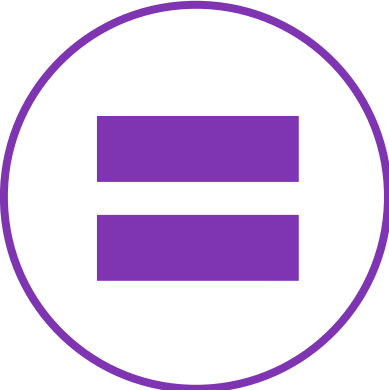
The screenshot shows the 'Add hosts' wizard in VMware vSphere. A 'Security Alert' dialog box is displayed in the foreground, asking the user to verify the SHA1 thumbprint of a certificate for one host. The dialog contains the following information:

The certificate on 1 host could not be verified. The SHA1 thumbprints of the certificate is listed below. To continue connecting, manually verify this certificate and accept the thumbprint below.

<input type="checkbox"/>	Hostname / IP Address	SHA1 Thumbprint
<input type="checkbox"/>	192.168.20.11	6D:03:11:B2:91:DA:7E:83:44:1A:39:4E:B1:BD:64:26:F8:E1:6E:FE

Buttons: CANCEL, OK

# VMCA Certificate Management Modes



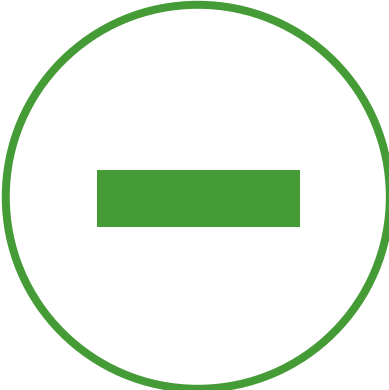
Fully Automated



Hybrid



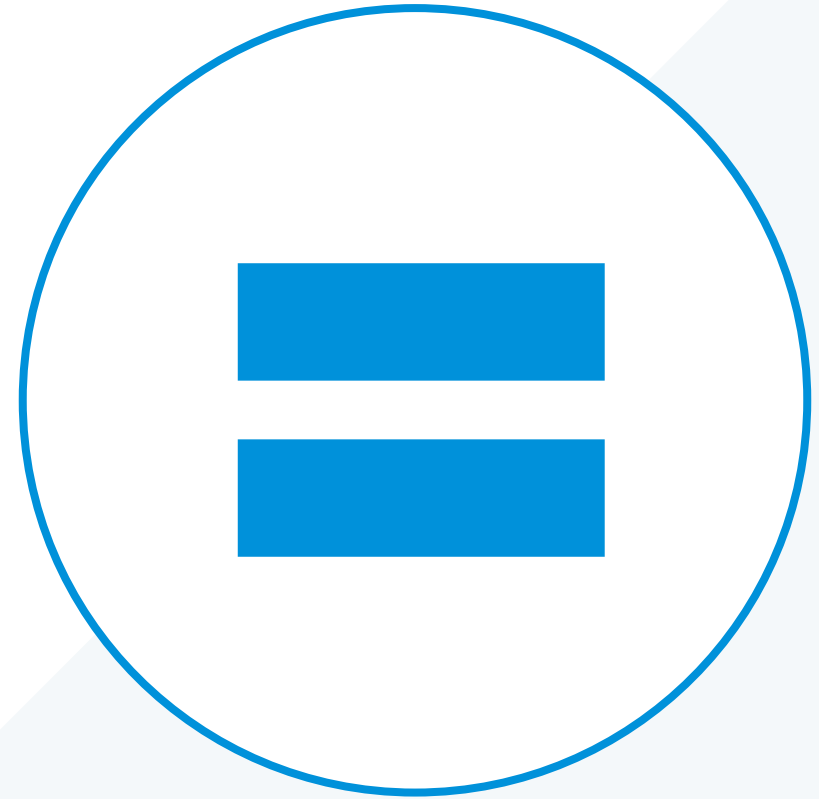
Subordinate CA



Fully Custom



# Fully Automated

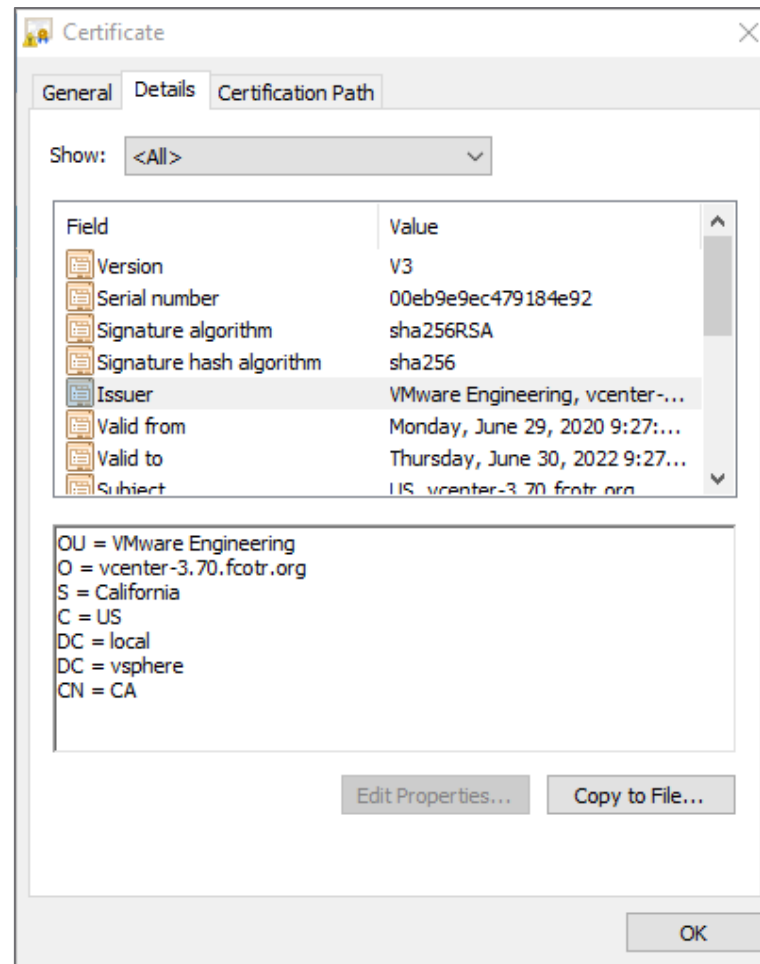


# Let vSphere Manage Its Own Certificates

VMCA Mode: Fully Automated (Default)

Uses the VMCA

No “default”  
certificate, CA  
root generated at  
vCenter Server  
install time



# Change the CA Root Certificate, Put In Your Own Information

VMCA Mode: Fully Automated (Default)

Uses the VMCA

No “default”  
certificate, CA  
root generated at  
vCenter Server  
install time

Root can be  
manually  
regenerated (#4)

```
OpenSSH SSH client
root@vcenter-1 [ ~ ]# /usr/lib/vmware-vmca/bin/certificate-manager

*** Welcome to the vSphere 8.0 Certificate Manager ***

-- Select Operation --

1. Replace Machine SSL certificate with Custom Certificate
2. Replace VMCA Root certificate with Custom Signing Certificate and replace all Certificates
3. Replace Machine SSL certificate with VMCA Certificate
4. Regenerate a new VMCA Root Certificate and replace all certificates
5. Replace Solution user certificates with Custom Certificate
NOTE: Solution user certs will be deprecated in a future release of vCenter. Refer to release notes for more details.
6. Replace Solution user certificates with VMCA certificates
7. Revert last performed operation by re-publishing old certificates
8. Reset all Certificates

Note : Use Ctrl-D to exit.
Option[1 to 8]:
```

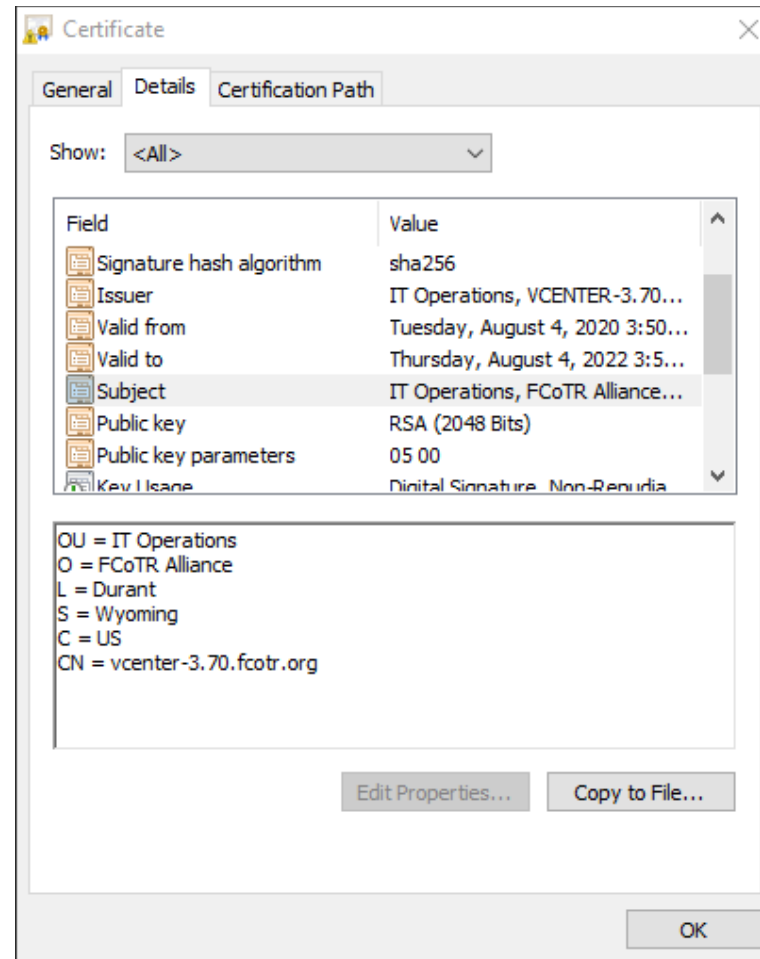
# Change the CA Root Certificate, Put In Your Own Information

VMCA Mode: Fully Automated (Default)

Uses the VMCA

No “default”  
certificate, CA  
root generated at  
vCenter Server  
install time

Root can be  
manually  
regenerated (#4)



# Download the VMCA Root CA Certificates

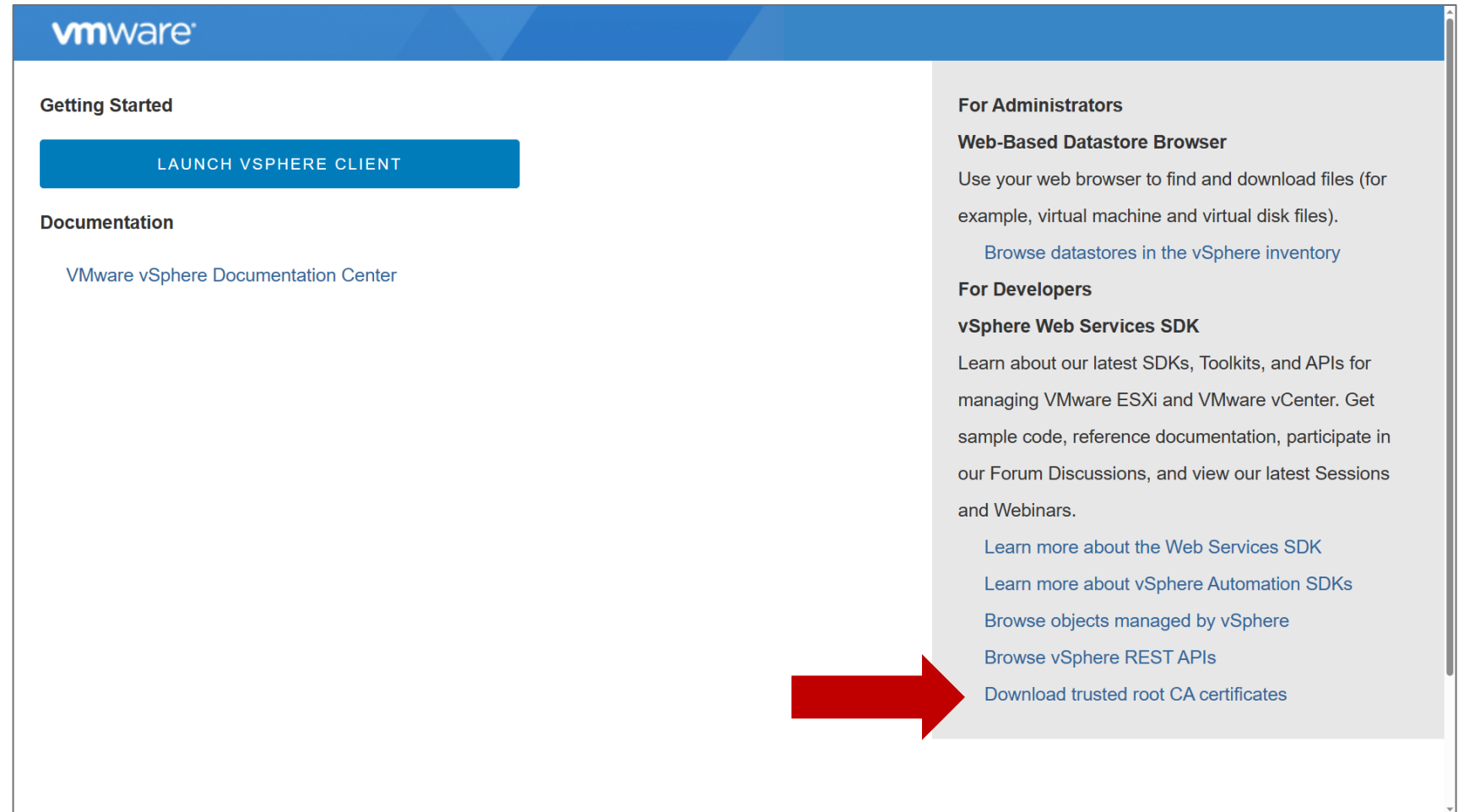
VMCA Mode: Fully Automated (Default)

Uses the VMCA

No “default”  
certificate, CA  
root generated at  
vCenter Server  
install time

Root can be  
manually  
regenerated (#4)

Absolute easiest  
but doesn't scale  
beyond a few vCs



The screenshot shows the VMware vSphere Client interface. At the top, the VMware logo is visible. Below it, the 'Getting Started' section contains a prominent blue button labeled 'LAUNCH VSPHERE CLIENT'. Underneath, the 'Documentation' section lists the 'VMware vSphere Documentation Center'. On the right side of the interface, there are three sections: 'For Administrators' with a sub-section 'Web-Based Datastore Browser', 'For Developers' with a sub-section 'vSphere Web Services SDK', and a list of links. A red arrow points to the link 'Download trusted root CA certificates' at the bottom of this list.

Hybrid



# A Trusted Client Certificate with Full Automation

VMCA Mode: Hybrid

```
OpenSSH SSH client
root@vcenter-1 [ ~ ]# /usr/lib/vmware-vmca/bin/certificate-manager

*** Welcome to the vSphere 8.0 Certificate Manager ***

-- Select Operation --

1. Replace Machine SSL certificate with Custom Certificate
2. Replace VMCA Root certificate with Custom Signing Certificate and replace all Certificates
3. Replace Machine SSL certificate with VMCA Certificate
4. Regenerate a new VMCA Root Certificate and replace all certificates
5. Replace Solution user certificates with Custom Certificate
NOTE: Solution user certs will be deprecated in a future release of vCenter. Refer to release notes for more details.
6. Replace Solution user certificates with VMCA certificates
7. Revert last performed operation by re-publishing old certificates
8. Reset all Certificates

Note : Use Ctrl-D to exit.
Option[1 to 8]:
```

Replace the vSphere Client certificate

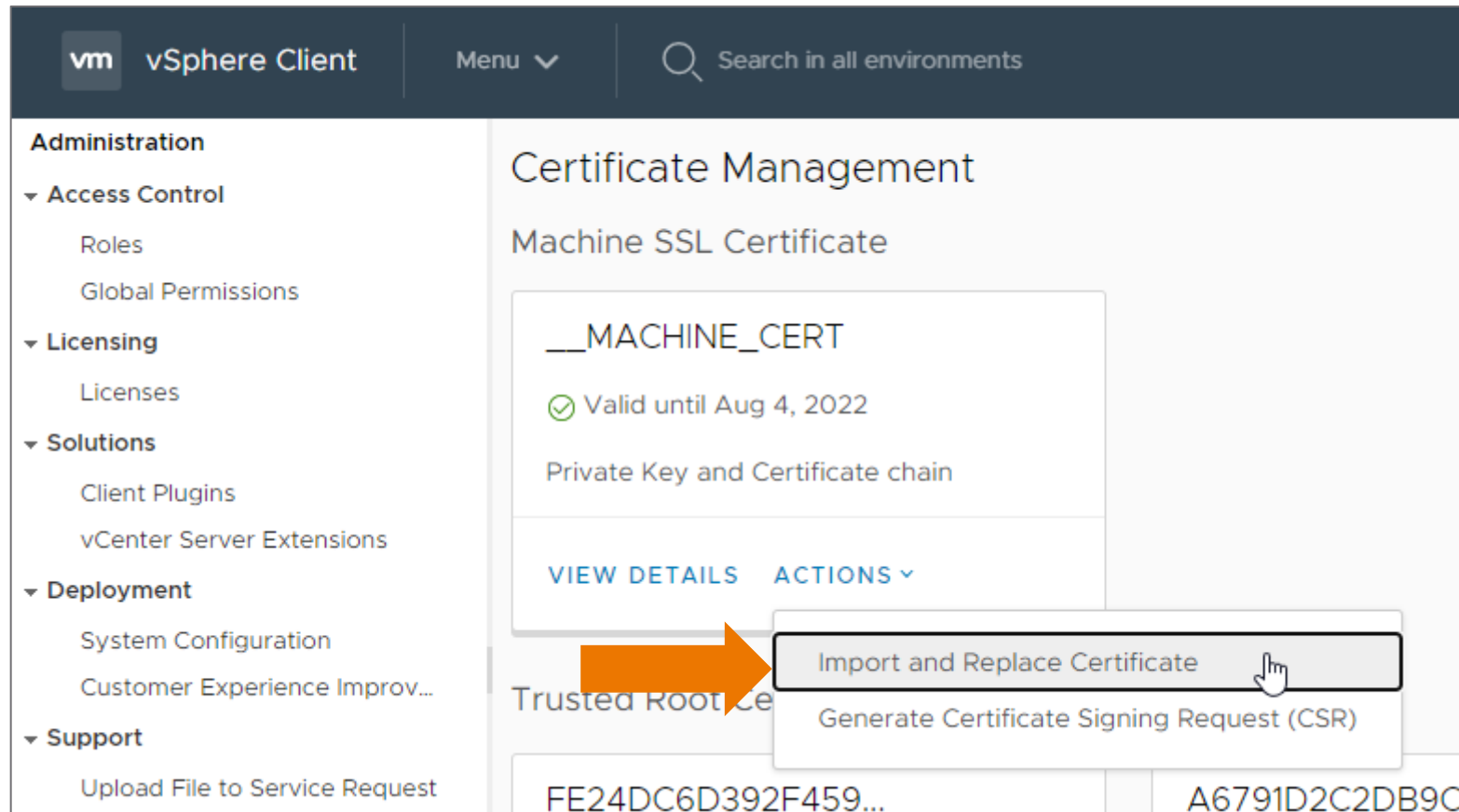
Can be done to any of the deployment models

Still doesn't scale very well

Can use CLI (#1)

# vSphere 7 Adds Nicer GUI Options

VMCA Mode: Hybrid



Same as fully automated, except you replace the vSphere Client “machine certificate”

Still doesn't scale very well

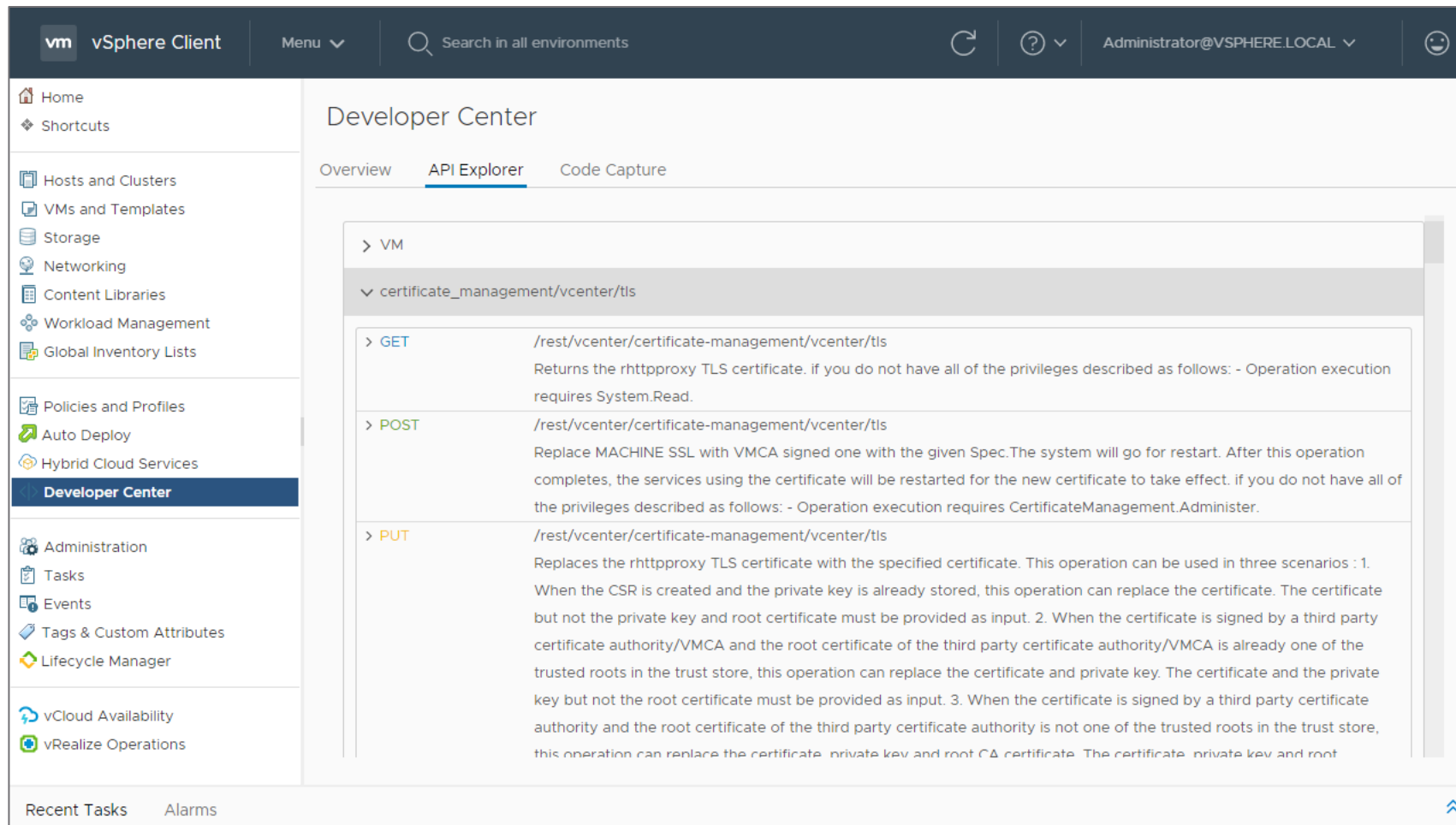
Can use CLI

Can use GUI



# vCenter Server 7 Adds APIs

## VMCA Mode: Hybrid



The screenshot shows the vSphere Client interface with the Developer Center API Explorer open. The API Explorer displays the following information:

- VM**
  - certificate\_management/vcenter/tls**
    - GET** `/rest/vcenter/certificate-management/vcenter/tls`  
Returns the rhttpproxy TLS certificate. if you do not have all of the privileges described as follows: - Operation execution requires System.Read.
    - POST** `/rest/vcenter/certificate-management/vcenter/tls`  
Replace MACHINE SSL with VMCA signed one with the given Spec.The system will go for restart. After this operation completes, the services using the certificate will be restarted for the new certificate to take effect. if you do not have all of the privileges described as follows: - Operation execution requires CertificateManagement.Administer.
    - PUT** `/rest/vcenter/certificate-management/vcenter/tls`  
Replaces the rhttpproxy TLS certificate with the specified certificate. This operation can be used in three scenarios : 1. When the CSR is created and the private key is already stored, this operation can replace the certificate. The certificate but not the private key and root certificate must be provided as input. 2. When the certificate is signed by a third party certificate authority/VMCA and the root certificate of the third party certificate authority/VMCA is already one of the trusted roots in the trust store, this operation can replace the certificate and private key. The certificate and the private key but not the root certificate must be provided as input. 3. When the certificate is signed by a third party certificate authority and the root certificate of the third party certificate authority is not one of the trusted roots in the trust store, this operation can replace the certificate, private key and root CA certificate. The certificate, private key and root

Same as fully automated, except you replace the vSphere Client “machine certificate”

Still doesn't scale very well

Can use CLI

Can use GUI

Can use API

# Tips For Using vSphere APIs to Replace Certificates

Little hints go a long way!

1. The specification is at:

[https://developer.vmware.com/apis/vsphere-automation/latest/vcenter/certificate\\_management/](https://developer.vmware.com/apis/vsphere-automation/latest/vcenter/certificate_management/)

2. Shell escapes for special characters will be your biggest enemy. API Explorer may not do it right for you because it doesn't know where you're pasting the example.
3. Use awk to turn the linefeeds into \n for the spec.  
Be careful not to remove the spaces in the -----BEGIN CERTIFICATE----- parts.

```
awk -vORS='\n' '1' file.pem
```

4. Get the session ID & sample from the API explorer but be careful with those because anyone with those is “you” according to vSphere. Don't check them into Git.
5. Make sure you're using good certificates, take snapshots of vCenter Server, test.

```
54
55
56 curl -X PUT 'https://vcenter-3.70.fcotr.org/rest/vcenter/certificate-management/vcenter/tls' -H 'vmware-api-session-id: db
57   "spec" : {
58     "cert" : "-----BEGIN CERTIFICATE-----\\nMIIGXjCCBEagAwIBAgICEA4wDQYJKoZIhvcNAQELBQAwZQxCzAJBgNVBAYTA1VT\\nMQswCQYD
59     "root_cert" : "-----BEGIN CERTIFICATE-----\\nMIIGFjCCA/6gAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwZ4xCzAJBgNVBAYTA1VT\\nMQs
60     "key" : "-----BEGIN RSA PRIVATE KEY-----\\nMIIEpAIBAAKCAQEAA2WlokrAcNsI3Cx58DI15ue9DmezHQgyHI3NQKn0Ea/cZ8EdZ\\nA2Dp0
61   }
62 }'
63
```



# Subordinate CA



# VMCA: Subordinate CA

Solving the scaling problem for large numbers of vSphere clusters

Set up using CLI  
(#2)

Solves scaling  
issues (trust one  
CA, not 200)

Enterprise PKI  
folks dislike it  
("blast radius")

...so use your own  
CA or have  
enterprise PKI  
build you one!

```
OpenSSH SSH client
root@vcenter-1 [ ~ ]# /usr/lib/vmware-vmca/bin/certificate-manager

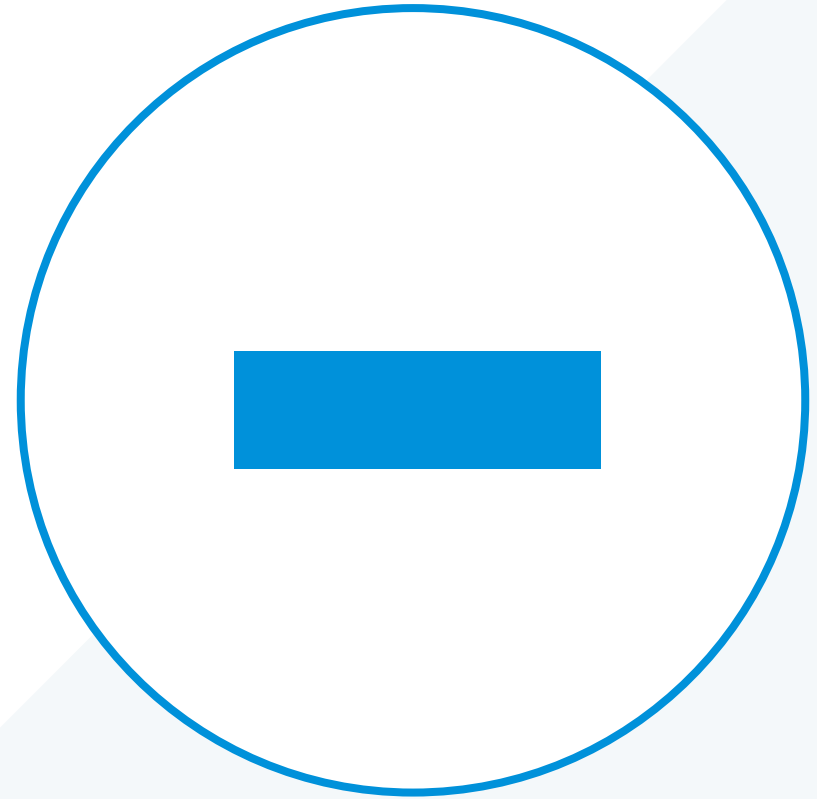
*** Welcome to the vSphere 8.0 Certificate Manager ***

-- Select Operation --

1. Replace Machine SSL certificate with Custom Certificate
2. Replace VMCA Root certificate with Custom Signing Certificate and replace all Certificates
3. Replace Machine SSL certificate with VMCA Certificate
4. Regenerate a new VMCA Root Certificate and replace all certificates
5. Replace Solution user certificates with Custom Certificate
NOTE: Solution user certs will be deprecated in a future release of vCenter. Refer to release notes for more details.
6. Replace Solution user certificates with VMCA certificates
7. Revert last performed operation by re-publishing old certificates
8. Reset all Certificates

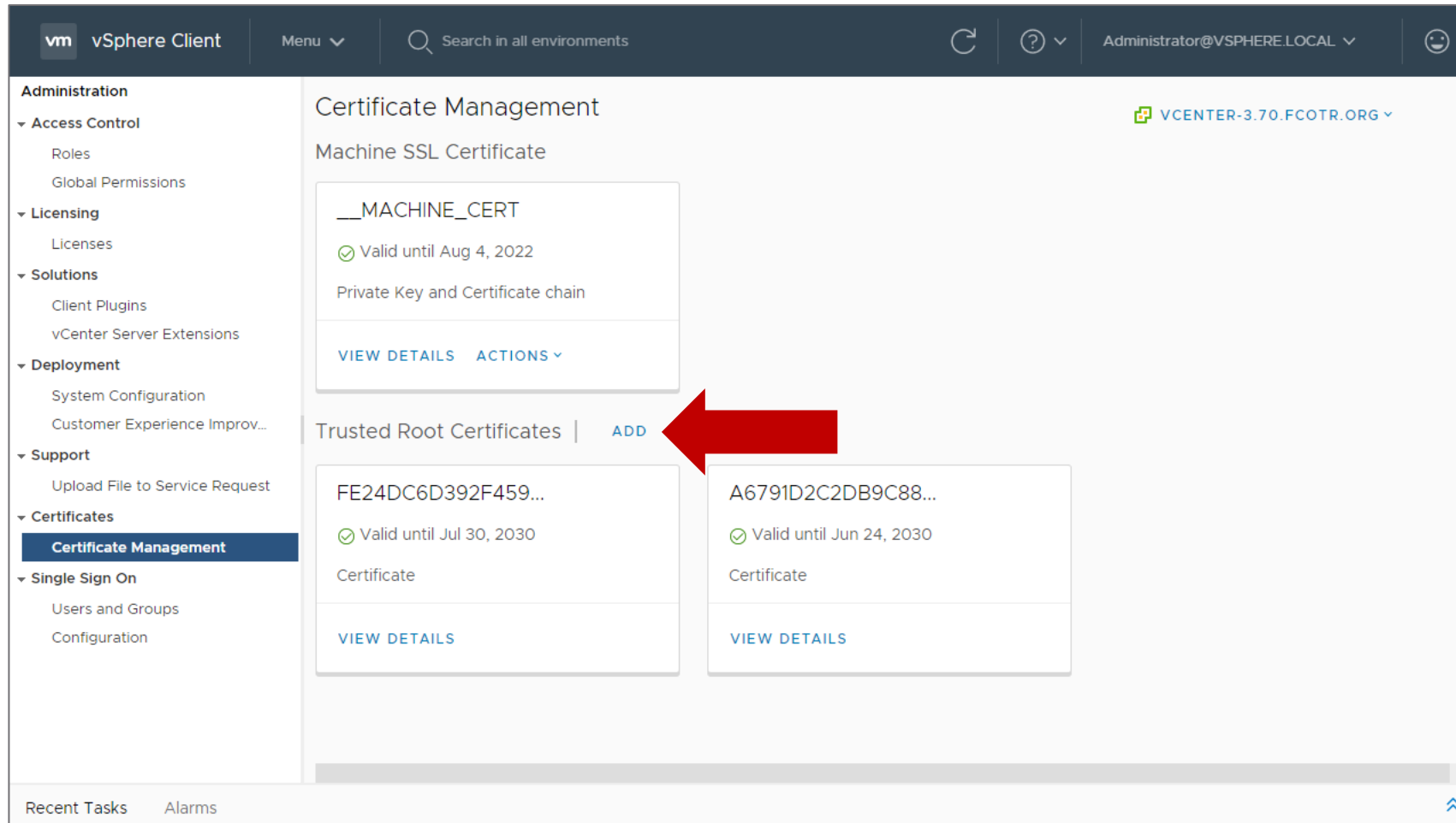
Note : Use Ctrl-D to exit.
Option[1 to 8]:
```

# Fully Custom



# VMCA: Fully Custom

Replace automation with humans or bespoke automation



The screenshot shows the vSphere Client interface for Certificate Management. The left sidebar contains a navigation menu with categories: Administration, Access Control, Licensing, Solutions, Deployment, Support, Certificates, and Single Sign On. The 'Certificates' category is expanded, and 'Certificate Management' is selected. The main content area is titled 'Certificate Management' and shows a 'Machine SSL Certificate' section with a card for '\_\_\_MACHINE\_CERT' (valid until Aug 4, 2022) and a 'Trusted Root Certificates' section with an 'ADD' button. A red arrow points to the 'ADD' button. Below the 'Trusted Root Certificates' section, two existing certificates are listed: 'FE24DC6D392F459...' (valid until Jul 30, 2030) and 'A6791D2C2DB9C88...' (valid until Jun 24, 2030). The top navigation bar includes the vSphere Client logo, a search bar, and the user 'Administrator@VSPHERE.LOCAL'.

Add CA root to trusted roots (follow docs or just do it as part of replacing the machine cert)

# VMCA: Fully Custom

Replace automation with humans or bespoke automation

The screenshot shows a web browser window displaying a VMware documentation page. The page title is "Replacing ESXi SSL Certificates and Keys" and it is for VMware vSphere 7.0. The page content includes a "Note" section and a "Note:" section. The "Note:" section states: "You can also use the `vim.CertificateManager` and `vim.host.CertificateManager` managed objects in the vSphere Web Services SDK. See the vSphere Web Services SDK documentation." The "Note" section states: "The default certificates are in the same location as the vSphere 5.5 certificates. You can replace the default certificates with trusted certificates in various ways." The "Note" section also states: "Replace VMCA-signed certificates with certificates from a trusted CA, either a commercial CA or an organizational CA, if your company policy requires it." The "Note" section also states: "By default, vSphere components use the VMCA-signed certificate and key that are created during installation. If you accidentally delete the VMCA-signed certificate, remove the host from its vCenter Server system, and add it back. When you add the host, vCenter Server requests a new certificate from VMCA and provisions the host with it." The "Note" section also states: "Your company's security policy might require that you replace the default ESXi SSL certificate with a third-party CA-signed certificate on each host." The page also features a sidebar with a navigation menu, a search bar, and social media sharing options.

Add CA root to trusted roots (follow docs or just do it as part of replacing the machine cert)

Replace ESXi certificates (shell, vifs, HTTPS PUT)

Restart the host

Reconnect the host



# VMCA: Fully Custom

vSAN is trickier because it needs to operate independently

The screenshot shows a web browser window displaying a VMware Knowledge Base article. The browser's address bar shows the URL <https://kb.vmware.com/s/article/56441>. The page header includes the VMware logo, 'Knowledge Base', and navigation links for Training, Community, Store, My VMware, and Tips on searching for a KB. A search bar is located below the header, with recent searches for '78221' and '78205'. The main content area features the article title 'Configuring Custom Certificates on ESXi hosts to authenticate vSAN hosts (56441)', last updated on 3/11/2019, and categories including Troubleshooting. The article is in English and has 2 likes. A 'Solution' section provides a five-step procedure for configuring custom certificates on ESXi hosts to authenticate vSAN hosts.

## Configuring Custom Certificates on ESXi hosts to authenticate vSAN hosts (56441)

Last Updated: 3/11/2019 Categories: Troubleshooting Language: English 2 likes subscribe

### Details

The KB outlines the steps to add custom certificate as the root CA to the ESXi trusted domain without bypassing the certificate based SSL authentication. The root CA can then be used to sign other intermediate CERTs and/or the host certificate file (i.e. private key – public key pair). Before making any changes you may like to validate with customer if they are using any third party trusted certificates.

### Solution

1. Set the vCenter Server to custom certificate mode by following the steps in the link outlined [here](#).
2. Ensure the custom Root certificate is retrieved in advance before proceeding.
3. Place the ESXi host in maintenance mode (Evacuate all data to other hosts)
4. Disconnect the ESXi host from the cluster.
5. SSH into the ESXi host

Additional Resources:

- KB • vSphere 7 Upgrade Best Practices (78205)
- Docs • vCenter Server Upgrade - VMware vSphere 7.0

Related Products:

- VMware vSAN

Related Versions:

- VMware vSAN 6.6.x

Actions:

- Copy link to clipboard

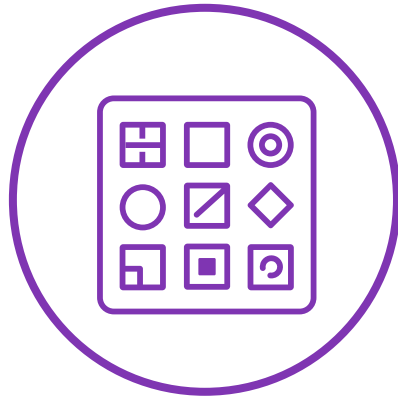
AdChoices

# Managing vSphere Certificates with PowerCLI

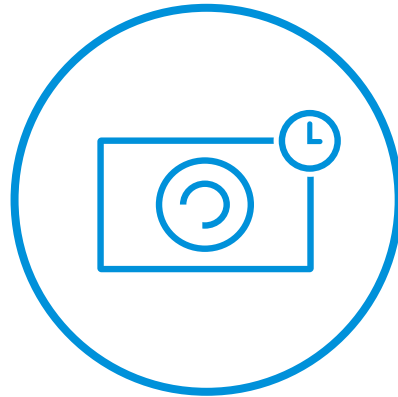
<https://blogs.vmware.com/PowerCLI/2022/02/managing-vsphere-certificates-with-powercli.html>



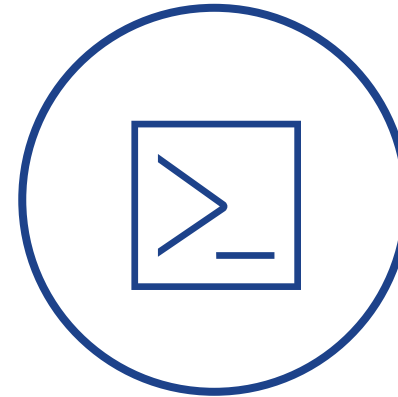
# General Thoughts on Getting Started



Nested ESXi  
for testing



Snapshots &  
backups



Linux helps  
(WSL2!)



Build your own  
CA for testing

# Build your own Certificate Authority

Great for testing and learning

1. Excellent Introduction:

<https://jamielinux.com/docs/openssl-certificate-authority/introduction.html>

2. How do I create a CSR with a Subject Alternate Name?

```
openssl req -config intermediate/openssl.cnf -key intermediate/private/$1.key.pem -  
new \  
-subj "/C=US/ST=Minnesota/L=Lake Wobegon/O=FCoTR Alliance/OU=R&D/CN=$1"  
\   
-addext "subjectAltName = DNS:$1" \  
-sha256 -out intermediate/csr/$1.csr.pem
```

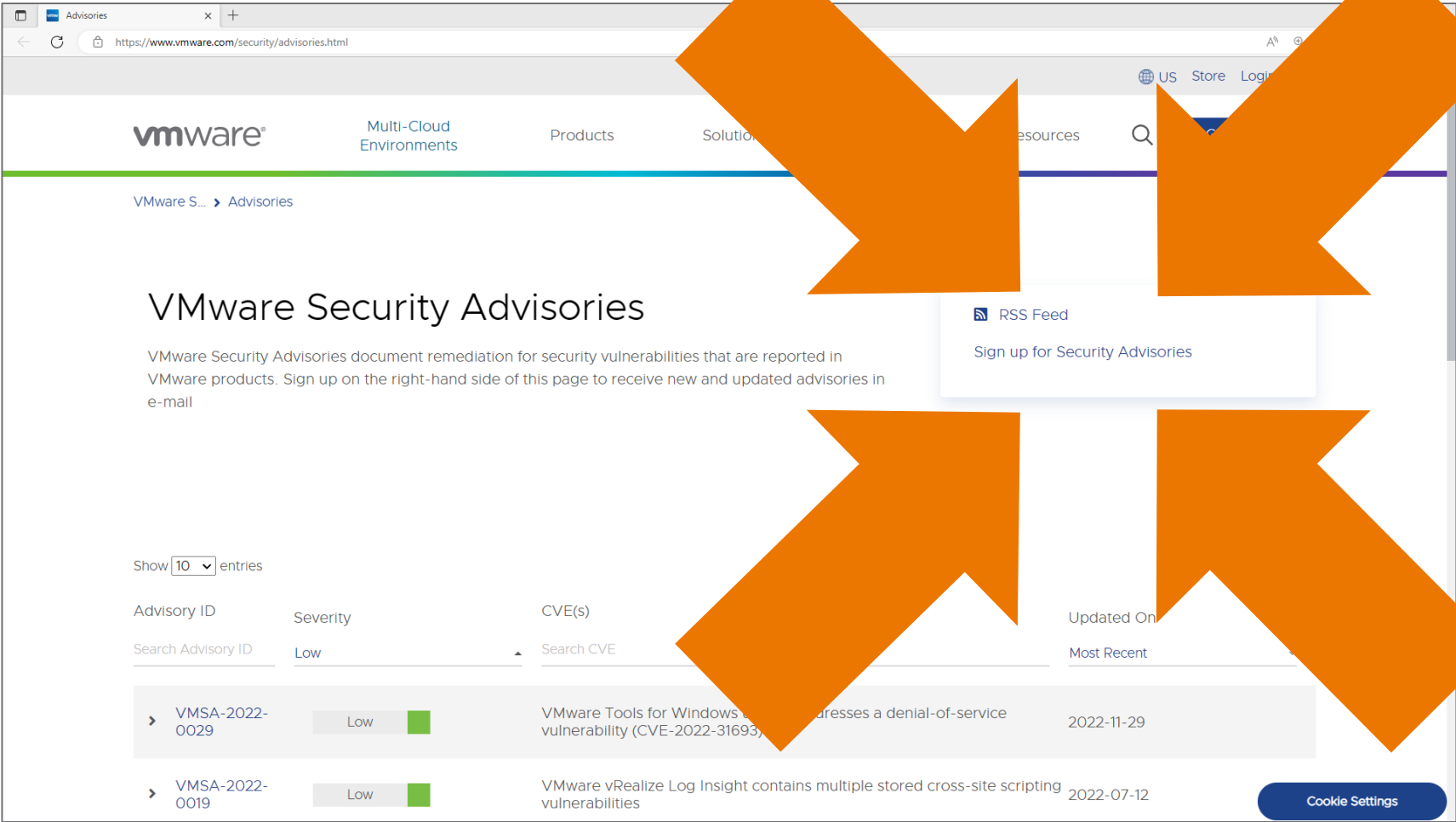
(where \$1 is a variable that contains the FQDN)

# Resources



# Sign Up For VMware Security Advisory (VMSA) Email

<https://www.vmware.com/security/advisories.html>



**VMSAs emailed  
the moment  
they are  
published**

**Just VMSAs;  
no marketing**

**Know before  
your Infosec  
people ask!**

**Prevention is a  
matter of time**

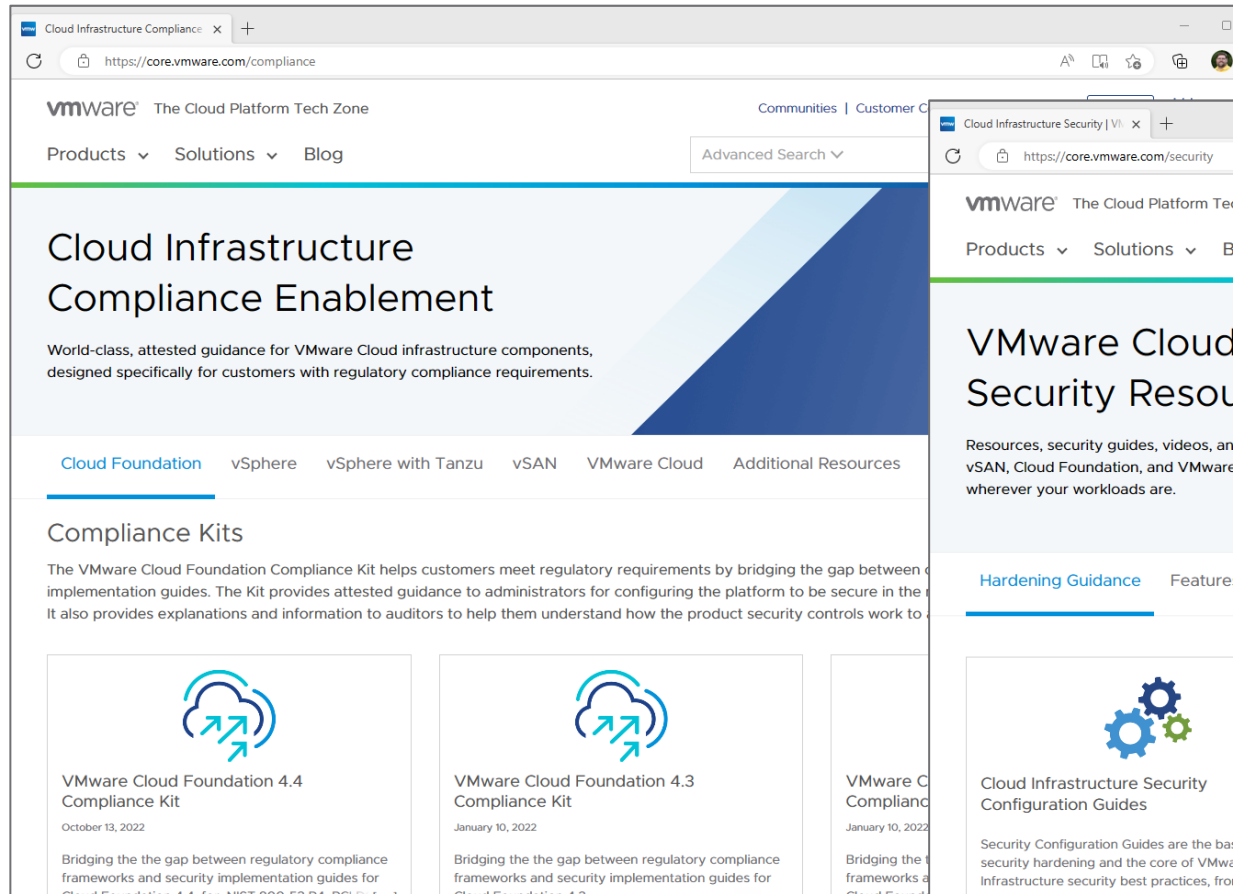
# VMware Cloud Infrastructure Security Configuration Guides

<https://via.vmw.com/scg>



# core.vmware.com

## Security & Compliance Resources for VMware Cloud Infrastructure



Cloud Infrastructure Compliance

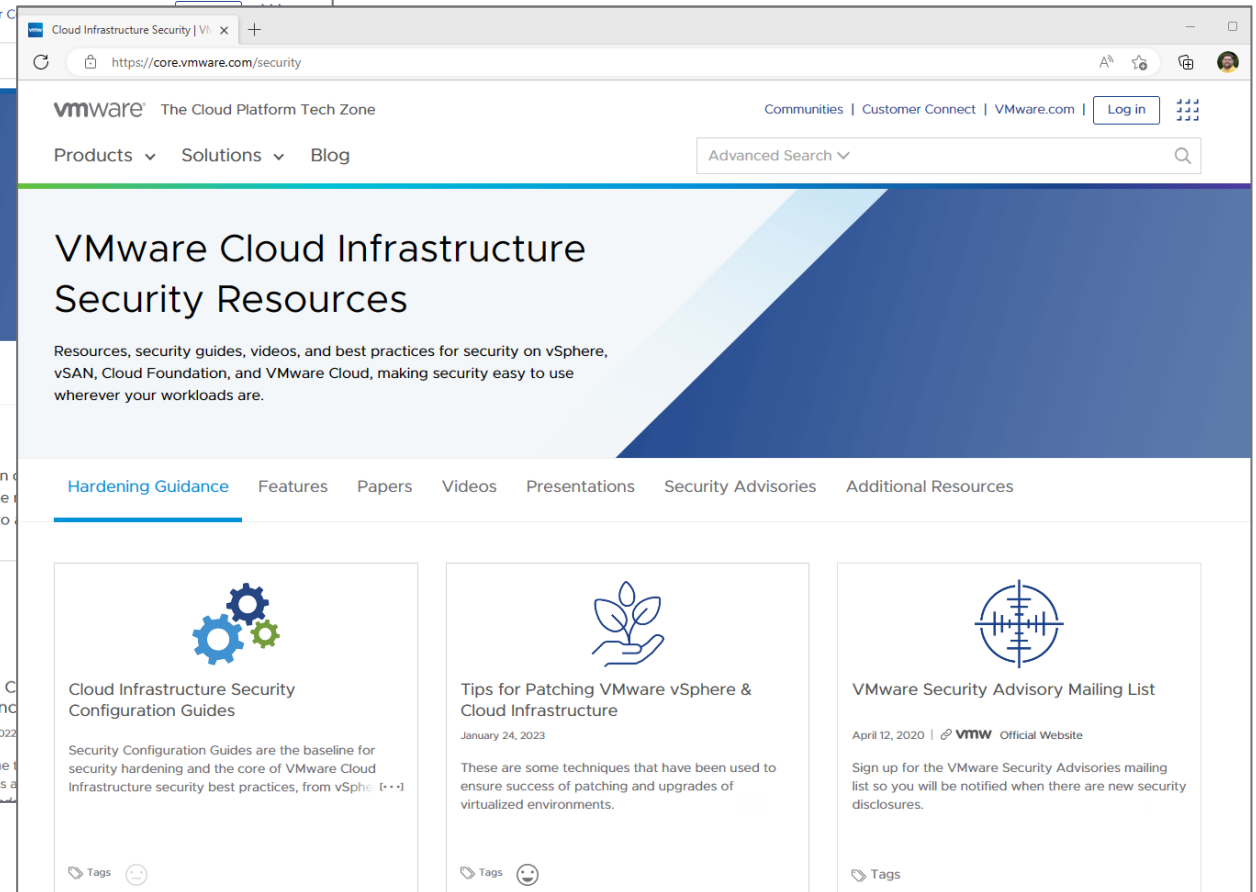
World-class, attested guidance for VMware Cloud infrastructure components, designed specifically for customers with regulatory compliance requirements.

Cloud Foundation | vSphere | vSphere with Tanzu | vSAN | VMware Cloud | Additional Resources

### 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 cloud. It also provides explanations and information to auditors to help them understand how the product security controls work to protect your data.

- VMware Cloud Foundation 4.4 Compliance Kit**  
October 13, 2022  
Bridging the gap between regulatory compliance frameworks and security implementation guides for VMware Cloud Foundation 4.4 for NIST 800-53, PCI DSS, and ISO 27001.
- VMware Cloud Foundation 4.3 Compliance Kit**  
January 10, 2022  
Bridging the gap between regulatory compliance frameworks and security implementation guides for VMware Cloud Foundation 4.3.
- VMware Cloud Foundation 4.2 Compliance Kit**  
January 10, 2022  
Bridging the gap between regulatory compliance frameworks and security implementation guides for VMware Cloud Foundation 4.2.



VMware Cloud Infrastructure Security Resources

Resources, security guides, videos, and best practices for security on vSphere, vSAN, Cloud Foundation, and VMware Cloud, making security easy to use wherever your workloads are.

Hardening Guidance | Features | Papers | Videos | Presentations | Security Advisories | Additional Resources

- Cloud Infrastructure Security Configuration Guides**  
Security Configuration Guides are the baseline for security hardening and the core of VMware Cloud Infrastructure security best practices, from vSphere 6.7 to VMware Cloud Foundation 4.4.
- Tips for Patching VMware vSphere & Cloud Infrastructure**  
January 24, 2023  
These are some techniques that have been used to ensure success of patching and upgrades of virtualized environments.
- VMware Security Advisory Mailing List**  
April 12, 2020 | VMware Official Website  
Sign up for the VMware Security Advisories mailing list so you will be notified when there are new security disclosures.



# Questions & Answers



## vSphere Certificate Questions & Answers (FAQ)

<https://via.vmw.com/cert-faq>

