vSphere Certificate Management Questions & Answers

Table of contents

vSphere Certificate Management Questions & Answers

Questions & Answers

How and when is the VMware Certificate Authority (VMCA) root certificate generated?

There is not a default certificate or key pair for any component of vSphere. The necessary certificates and keys are generated when products are installed, using default parameters set by VMware Engineering.

Is the VMCA root certificate regenerated when vCenter Server is upgraded?

No, during an upgrade the existing certificates are copied over.

Can I change the names on the VMCA root certificate?

Yes, use certificate-manager to reissue the certificate with your own information, or import your own certificate and key pair.

Can I change the names on the certificates that the VMCA issues for ESXi hosts?

Yes, set the following advanced parameters in vCenter Server:

- vpxd.certmgmt.certs.cn.country
- vpxd.certmgmt.certs.cn.email
- vpxd.certmgmt.certs.cn.localityName
- vpxd.certmgmt.certs.cn.organizationalUnitName
- vpxd.certmgmt.certs.cn.organizationName
- vpxd.certmgmt.certs.cn.state

What is the validity period of certificates issued by the VMCA?

By default, two years, but it is configurable with the vCenter Server advanced parameter vpxd.certmgmt.certs.daysValid.

Can the VMCA be used to sign other certificates, like for a web site or a blog?

Technically, yes, and there are tools such as the VMCA Certificate Generator Fling that make that easier. However, the VMCA is purpose-built for vSphere, and its automation saves considerable effort by IT staff. It is not meant to be a general-purpose CA. Where there might be an issue, perhaps a simple agreement between an organization's vSphere administration team and PKI team that this won't be used except for vSphere implementations would suffice.

My organization's PKI team is concerned with intermediate/subordinate CA mode, as it may allow unauthorized staff to impersonate the organization.

Organizational PKI infrastructure has mitigating controls, such as Certificate Revocation Lists (CRLs), and can use intermediate CAs as protections.

Given the limited scope of who can access IT infrastructure management interfaces, some organizations' PKI teams have chosen to create a separate "infrastructure" CA for their IT admins, for use in these circumstances. It's the best of both worlds, as vSphere admins get time-saving automation and the PKI team gets the isolation they need.

How does the VMCA work with Enhanced Linked Mode?

It works well; each vCenter Server uses its own VMCA to manage certificates for attached hosts and solutions.

Can I use the same intermediate/subordinate CA certificate on multiple vCenter Servers?

Yes.

Can I set a passphrase on the keys?

No. Manual interaction like that, at scale, isn't desirable, and prevents the services your whole datacenter needs from starting automatically.

Where is the VMCA Certificate Revocation List (CRL)?

The VMCA is purpose-built for automating certificates inside vSphere. It is not a general-purpose CA and does not have a CRL.

Trust in vSphere is managed by the vSphere administrators, as part of the prompt to verify certificate thumbprints when connecting hosts and solutions. Revoke certificates by removing components from the cluster.

Is there support for Elliptical Curve (ECC) certificates and keys?

Not at this time. For feature and enhancement requests as well as roadmap information please work with your account team.

Can the VMCA proxy to an enterprise PKI infrastructure?

Not at this time. The SDDC Manager component of VMware Cloud Foundation can interact with external certificate authorities, though. For feature and enhancement requests as well as roadmap information please work with your account team.

Is there ACME support for interacting with an external certificate authority?

Not at this time. For feature and enhancement requests as well as roadmap information please work with your account team.

Can vCenter Server store private keys in an external KMS/HSM system?

Not at this time. This would create dependency loops for vSphere services and vSAN.

What order should the CA certificate chain be in?

Most specific to least specific, e.g. the CA root that signed the certificate at the top, then an intermediate, then the CA root.

My vCenter Server has multiple names, to which should I issue the certificate?

Issue the certificate to the one matching the DNS PTR record. All the others should be added to the Subject Alternate Name (SAN) fields in the certificate request. However, if you use SANs, list the Subject of the certificate as the first Subject Alternate Name, followed by the rest of the names.

Are there any large vSphere deployments using the VMCA in intermediate/subordinate CA mode?

Yes. Many. Even moderately sized deployments benefit greatly from the VMCA automation, and many large customers -- in regulated environments -- have become comfortable with the VMCA because of the massive staff time savings and reduction of human error across the board (vSphere admins, PKI staff, compliance auditors, and more). VMCA is a competitive advantage for those that use it.

How does vCenter Server store certificates and keys?

In the VMware Endpoint Certificate Store, or VECS. You can interact with VECS using a shell on the vCenter Server Appliance (VCSA) using the vecs-cli. For example, to list the different certificate stores use “/usr/lib/vmware-vmafd/bin/vecs-cli store list”

I had vCenter Server generate a CSR; how do I back up the private key it created?

Use the vecs-cli command:

/usr/lib/vmware-vmafd/bin/vecs-cli entry getcert --store MACHINE_SSL_CERT --alias __MACHINE_CERT

/usr/lib/vmware-vmafd/bin/vecs-cli entry getkey --store MACHINE_SSL_CERT --alias __MACHINE_CERT

Can I encrypt vCenter Server to protect the VMCA keys and certificates?

With certain system designs such as those that use vSphere Trust Authority, yes. Specific system design is beyond the scope of this FAQ.

Can I use wildcard certificates?

No. vSphere cares about the subject names as part of the trust that is established, and wildcards do not have specific names in their subject.

Will I get an alarm or notification when my certificates are expiring?

Yes, and that interval is configurable with the vpxd.certmgmt.certs.softThreshold and vpxd.certmgmt.certs.hardThreshold advanced vCenter Server parameters.

Are solution certificates still in use?

They are deprecated and will be removed in a future major version.

I need to shut particular ciphers off in TLS, how do I do that?

See KB 79476.

Once I've replaced my certificates what do I need to do?

Check all connected systems to ensure they work. This includes storage systems and VASA providers, backup systems, and monitoring applications.

What does VMware recommend for certificate management?

Every environment is different, and VMware cannot make a recommendation for you. Many small environments enjoy the hybrid mode, where only the vSphere Client certificate is changed. Many large environments appreciate the time savings of intermediate/subordinate CA mode.

Almost nobody thinks custom certificate replacements are worth the time spent. It wasn't so bad when certificate expirations were five years, but now that they are 397 days that is a lot of work.

We do recommend not making things harder than they need to be. We also recommend having conversations with each other, remembering you are on the same team. vSphere Admins have many other things to do than replacing certificates, and PKI folks and auditors worry about valid things that vSphere Admins have never thought about. Both perspectives are important.

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.

Additional Resources

Please visit the vSphere security resources at https://core.vmware.com/security.

Feedback

The purpose of this document is to answer questions that may fall outside the scope of product documentation and system design guidance. Your feedback is valuable. To comment on this document please use the feedback mechanisms on this page. Thank you.