SDDC Certificate Tool

User Guide

Table of Contents

Summary

Replacing SSL certificates across VMware products is a manual and time-consuming process. The SDDC Certificate Tool automates this workflow and makes it easy to keep certificates across your SDDC up to date. It will replace all certificates in the supported products and reestablish trust between the components.

Supported Products:

- VMware Platform Services Controller (PSC)
- VMware vCenter Server (VC)
- VMware NSX for vSphere (NSX)
- vRealize Log Insight (vRLI)
- vRealize Operations Manager (vROps)
- vRealize Automation (vRA)
- vRealize Business for Cloud (vRB)

System Requirements

- Linux server running Java 1.8+
- Certificate Files in x509 format (.cer)
- Certificate Chain in x509 format (.cer)

Supported VMware products:

Product	Minimum Version	Maximum Version
VMware Platform Services Controller (PSC)	6.0 U2	6.7
VMware vCenter Server (VC)	6.0 U2	6.7
VMware NSX for vSphere (NSX)	6.2.4	6.4.1
vRealize Log Insight (vRLI)	3.6	4.6
vRealize Operations Manager (vROps)	6.3	6.7
vRealize Automation (vRA)	7.4	7.4
vRealize Business for Cloud (vRB)	7.1	7.4

Instructions

Installation

To run CertReplace you will need Linux host with Java Version 1.8 or higher. PhotonOS is the suggested distribution.

1. Download and install PhotonOS: https://github.com/vmware/photon/wiki/Downloading-Photon-OS

2. Download the SDDC Certificate Tool RPM and transfer it to the created PhotonOS VM.
3. Install Java 1.8.
   `tdnf install openjdk8`
4. Browse to the directory where you transferred the SDDC Certificate Tool and install the RPM.
   `rpm -ivh cert-mgmt-1.0.0-8986031.noarch.rpm`
5. The SDDC Certificate Tool will be installed at `/opt/vmware/cert-mgmt/`.

Workflows

There are two workflows described in these instructions. The simple workflow is if you already have signed certificates from a trusted Certificate Authority (CA) and simply want to use the tool to replace certificates. The advanced workflow is if you would like the SDDC Certificate Tool to generate Certificate Signing Requests (CSRs) for the VMware appliances, send the CSRs to a trusted CA for certificate generation, and finally replace the certificates.

The steps to perform the simple workflow are:

1. Copy certificate, private keys, and the root chain to a Linux server.
2. Download and extract the SDDC Certificate Tool.
3. Edit the configuration file to include hostnames, account credentials, and location of the certificate files.
4. Run SDDC Certificate Tool to replace certificates.

Additional details are in the Simple Workflow section.

The advanced workflow steps are:

1. Download and extract the SDDC Certificate Tool.
2. Edit the Configuration JSON file with hostnames and passwords.
3. Use SDDC Certificate Tool to Generate Certificate Signing Requests (CSRs).
4. Use generated CSRs to receive signed certificates from Certificate Authority and copy it to the Linux server.
5. Edit the configuration JSON file to include locations of the certificates.
6. Run SDDC Certificate Tool to replace certificates.

Additional details are in the Advanced Workflow section.

Configuration File

The first step is to create a configuration file to match your environment. Check the sample configuration files in `/opt/vmware/cert-mgmt/config/` directory for further configuration templates. This file is a JSON with multiple VMware product components. This is a sample PSC configuration with a description below.

Note, including passwords in the JSON configuration file is optional for security reasons. Remove the `password` line in the JSON. If you choose this method, use the `passwordEntry` command line argument:

```
java -jar lib/certreplace-*.jar -config config/config.json -createlocalcsr -passwordEntry
```

This will prompt you for all passwords initially and can optionally save them in an encrypted file for reuse later. To save the passwords for reuse, see Save Passwords in an Encrypted file.

Sample JSON

This is an example JSON configuration file showing specifics of a vCenter Server and the descriptions of the keys.

```
{
   "default":{
      "csrspec":"output/csrspec/default.txt"
   },
   "vcenters":[
      {
         "host":{
            "hostname":"sfo01m01vc01.rainpole.local",
            "osadmin":{
               "username":"root",
               "password":"VMware1!"
            }
         },
         "admin":{
            "username":"administrator@vsphere.local",
            "password":"VMware1!"
         },
         "serviceaccounts":[
            {
               "credential":{
                  "username":"svc-vrops@rainpole.local",
                  "password":"VMware1!"
               },
               "description":"Example service account for vCenter to access vROps"
            }
         ],
         "newsslcert":true,
         "sslcert":{
            "csrspec":"output/csrspec/sfo01m01vc01.txt",
            "privatekey":"SignedByMSCACerts/sfo01m01vc01/sfo01m01vc01.key",
            "password":"VMware1!",
            "signedcert":"SignedByMSCACerts/sfo01m01vc01/sfo01m01vc01.1.cer",
            "cachain":"SignedByMSCACerts/RootCA/Root64.cer"
         }
      }
   ]
}
```

Configuration File Samples

The `/opt/vmware/cert-mgmt/config` folder includes a few sample configuration files:

File	Description
config-all-products.json	All supported products supported by SDDC Certificate Tool with CSR generation code.
config-csr.json	Two-member external PSC and one vCenter that need CSR generation and replacement.
embedded-psc-vcenter.json	Embedded PSC and vCenter instance that requires a certificate replacement.

nsx+vc.json	NSX and VC with Embedded PSC but only the certificate on NSX needs replacement.
psc+vc.json	Two-member external PSC with one vCenter that all require replacement.

JSON Key Description

Keys	Description
default	Config file location for common entries across all of your certificate signing requests such as OU, LOC, CN, etc. This is not required if CertReplace is not going generate CSRs.
pscs/ vcenters/ nsxmanagers/etc.	Identifies which product it is. There is a section for each product, see the sample configuration file for all of the products that are supported.
host	The hostname and appliance root username and passwords are needed here.
admin	The administrator account's username and password are needed here.
serviceaccounts	If you are using service accounts to connect to other appliances in your SDDC, you will need to include those here.
newsslcert	This specifies if you would the SSL certificate of this component replaced with a true or false. If this is true, the sslcert section is mandatory.
sslcert	The file location of the csrspec, private key, password, signed certificate, and the certificate authority chain file. The csrspec file has hostnames and SAN that will be included in the certificate and needs to be edited. See the included files for a sample.

Simple Workflow

This workflow is if you already have signed certificates that you want to replace it on the VMware components.

1. Copy signed certificates, private keys, and the certificate authority chain from your Certificate Signing Authority to a Linux server. A private folder is recommended to safeguard the private keys.
2. Download and extract the SDDC Certificate Tool to the `/opt/vmware/cert-mgmt/` folder.
3. Follow a configuration template and edit it to match your environment. Follow the examples at `/opt/vmware/cert-mgmt/config` and the Configuration File section for a detailed look.
4. Run Certificate Replacement command.
   ```
   java -jar lib/certreplace-*.jar -c config/config.json -replacecert -passwordEntry
   ```

If there are any errors in the configuration file, they will be shown and certificate replacement will only proceed once all errors have been fixed.

Advanced Workflow

This workflow increases the level of security by creating certificate signing requests on the VMware product appliances. The private keys will stay on the appliances and will not need to be copied anywhere.

1. Download and extract the SDDC Certificate Tool to the `/opt/vmware/cert-mgmt/` folder.
2. Follow a configuration template and edit it to match your environment. Follow the examples at `/opt/vmware/cert-mgmt/config/config-csr.json` and the Configuration File section for a detailed look.
3. Use SDDC Certificate Tool to Generate Certificate Signing Requests (CSRs).
   ```
   java -jar lib/certreplace-*.jar -config config/config.json -createcsr -passwordEntry
   ```
   See the Creating Certificate Signing Requests section for more details.
4. Use generated CSRs placed in `/opt/vmware/cert-mgmt/output/csrs/` to receive signed certificates from Certificate Authority and copy it to the Linux server. If you are using a Microsoft Certificate Authority, you can use the CertGenVVD Powershell script. See Request Signed Certificates for all VMware Components for more information.
5. Edit the configuration JSON file to include locations of the certificates. Follow `/opt/vmware/cert-mgmt/config/config-csr.json` as a reference.
6. Run CertReplace to replace certificates.
   ```
   java -jar lib/certreplace-*.jar -c config/config.json -replacecert -passwordEntry
   ```

Creating Certificate Signing Requests

A Certificate Signing Request (CSR) needs to be created for each VMware component. There are a few ways to do this with our tool once the configuration file is complete. The CSRs will then need to be sent a Certificate Authority to receive a signed certificate. You can do this manually or use CertGen.

You will need to edit the files in `/opt/vmware/cert-mgmt/output/csrspec` to match your environment. The `default.txt` file contains all common elements across the SDDC. Each other component has its own file with a unique CN and SANs. See the files in this folder for samples.

Generate CSRs on each product appliance

CSRs can be generated on each product appliance specified in the configuration file. This will increase the security since private keys will stay on the appliance not be transferred through the network.

Example Usage:

```
java -jar lib/certreplace-*.jar -config config/config.json -createcsr -
passwordEntry
```

This will store all of the CSR files in the `/opt/vmware/cert-mgmt/output/csrs`.

Generate CSRs locally on the host

If you prefer to generate CSRs on the host where you are running the certreplace tool, run:

```
java -jar lib/certreplace-*.jar -config config/config.json -createlocalcsr -
passwordEntry
```

Request Signed Certificates for all VMware Components

The next step is to take the CSRs and send it to a Certificate Authority (CA) to get it signed. You can use any third-party CA. For a Microsoft Certificate Authority, you can use CertGenVVD to do this.

Using the CSRs generated, run:

```
.\CertGenVVD-3.0.1.ps1 –CSR -extra
```

Refer to the CertGen KB article for more information.

Save Passwords in an Encrypted file

If you prefer to not save your passwords in the configuration file, use the passwordEntry command line argument.

```
java -jar lib/certreplace-*.jar -c config/config.json -replacecert \
       -passwordEntry
```

If a password is not in the configuration file, you will be prompted for the password. After all passwords have been entered, you can optionally save the passwords in an encrypted file for reuse next time with a master password.

```
java -jar lib/certreplace-*.jar -c config/config.json -replacecert \
       -passwordEntry -passwdFile /opt/vmware/cert-mgmt/config/passwords.secure
```

Command Line Arguments

Argument	Description
-config	Configuration file path
-passwordEntry	Require all passwords to be input from the user if not specified in JSON file. More details in Save Passwords in an Encrypted file
-passwdFile	File path to save encrypted credentials. This is recommended to not have to enter in the credentials multiple times.
-replacecert	Replace certificates across the SDDC stack

-createcsr	Create certificate signing requests in product appliances
-createlocalcsr	Create certificate signing requests on this host
-cleanup	Cleanup temporary files in both localhost and product appliances
-help	Display command line arguments and details.