PANDUIT
infrastructure for a connected world

Panduit Collector for Cisco Nexus Dashboard Installation Guide

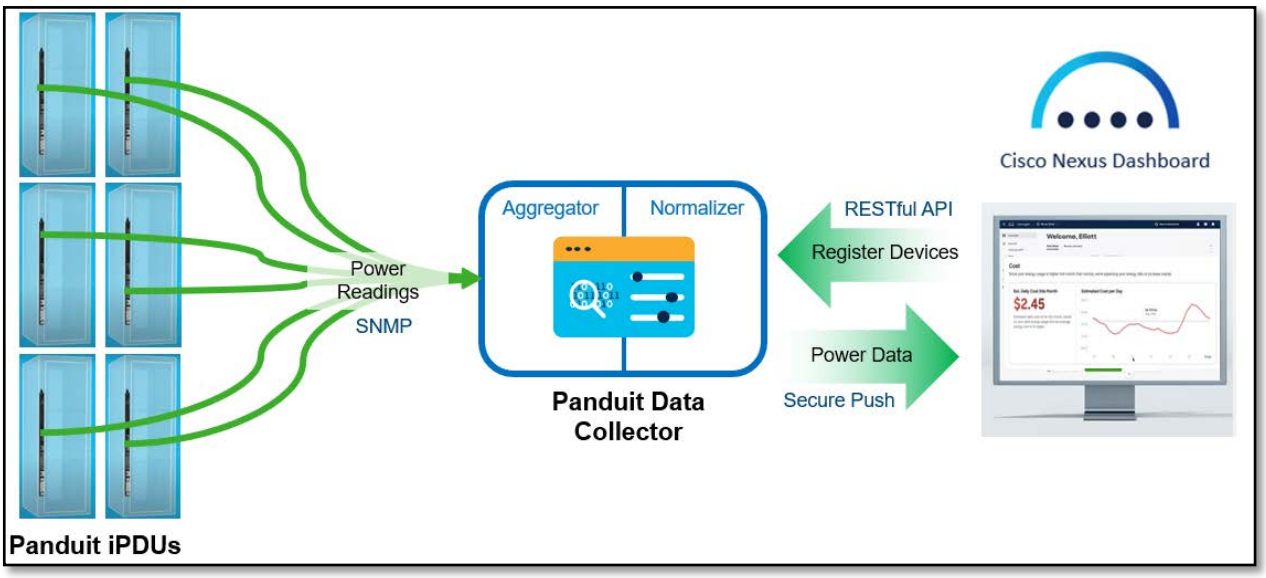
Version 1.2

Table of Contents

Panduit Data Collector

Panduit's intelligent Power Distribution Units (PDUs) are compatible with Cisco Nexus Dashboard software to enhance its insights related to Energy Savings and Sustainability.

The integration is available by using the Panduit Data Collector that collects and relays power data from the Panduit PDUs back to Nexus Dashboard through validated APIs. This simplifies the support of existing or new Panduit PDUs.

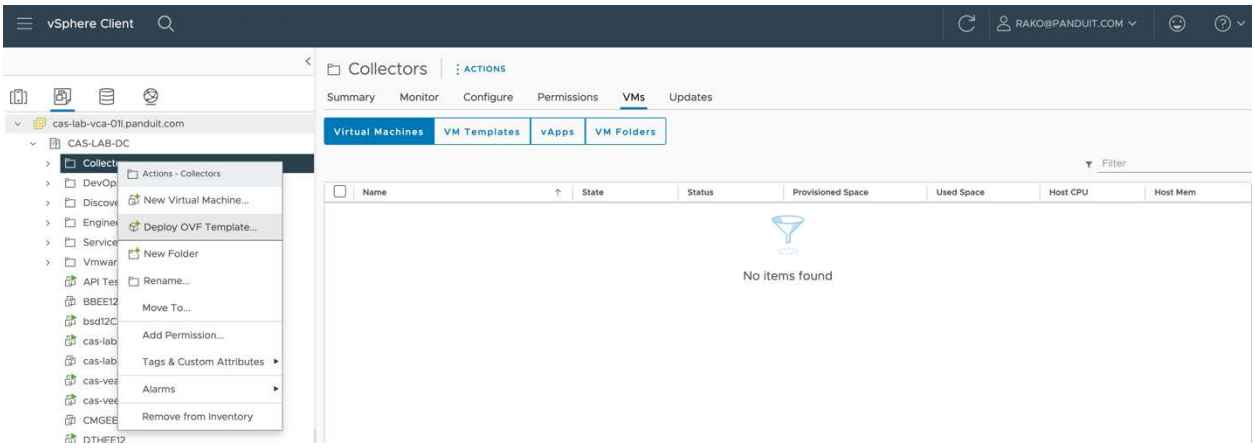


Data Collector Capacity

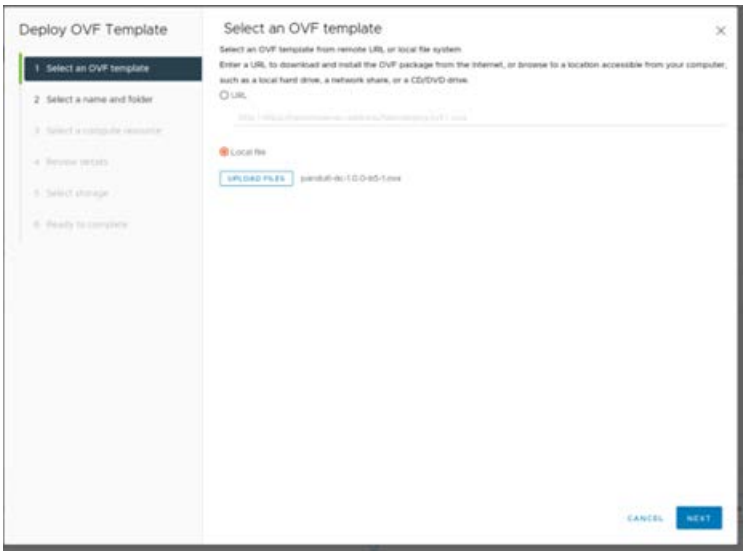
A single Data Collector is capable of processing data from up to 5,000 PDUs with a 15min polling rate.

Installation Option 1: OVA Image Files for VMware

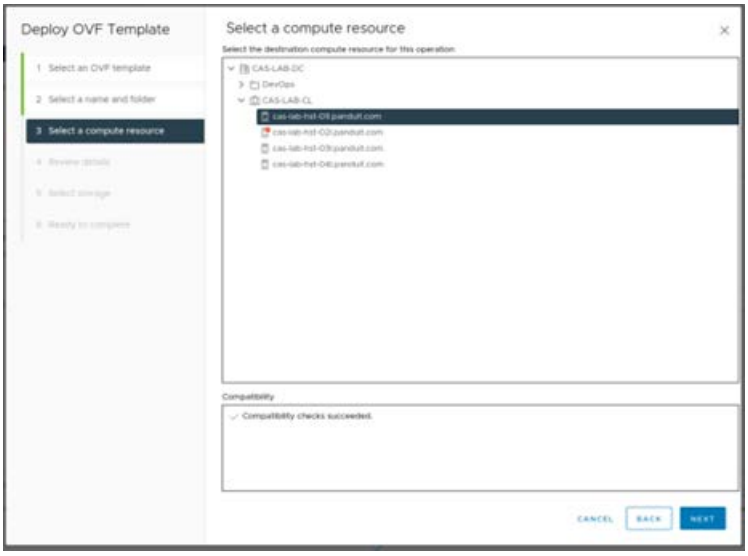
1. Go to [Panduit's download site](#).
2. Download the OVA image file.
3. Login to vSphere.
4. In vSphere, navigate to the folder where the Virtual Machine (VM) needs to be created.
5. Right click the folder and choose **Deploy OVF Template**.



6. In **Deploy OVF Template**:
    a. Select **Local File** and click **Upload Files**.

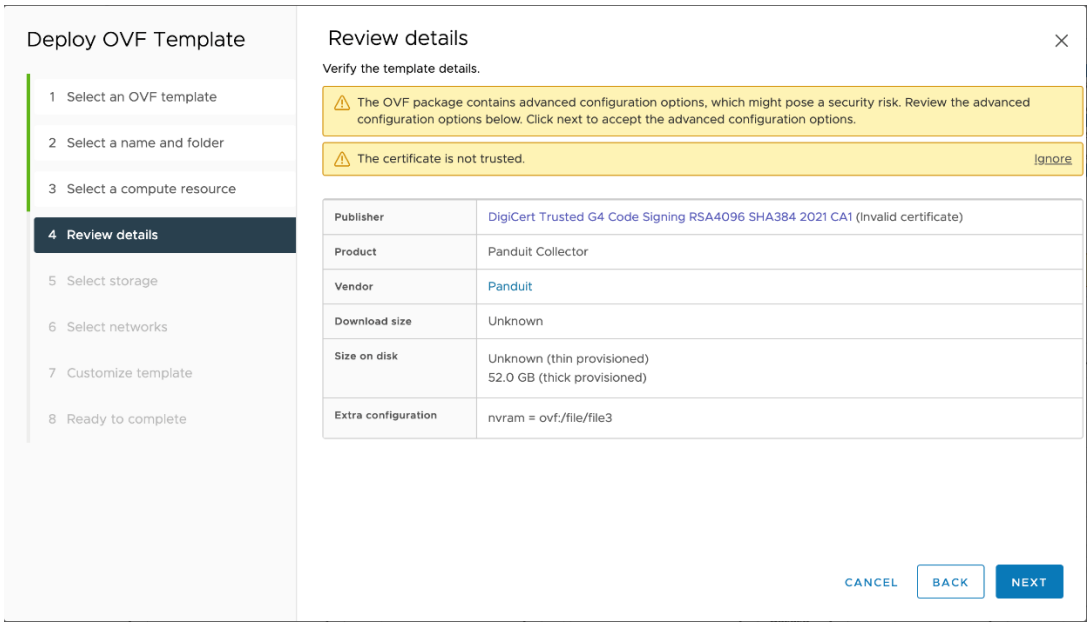


    b. In the **File** dialog select the ova file that was downloaded earlier.
    c. Click **Next**.
7. In **Select a name and folder**:
    a. Provide virtual machine name: **panduit-dc** (or any other name)
8. In **Select a compute resource**:
    a. Select a resource as per your setup. Please note that the following screenshot may not match your environment.



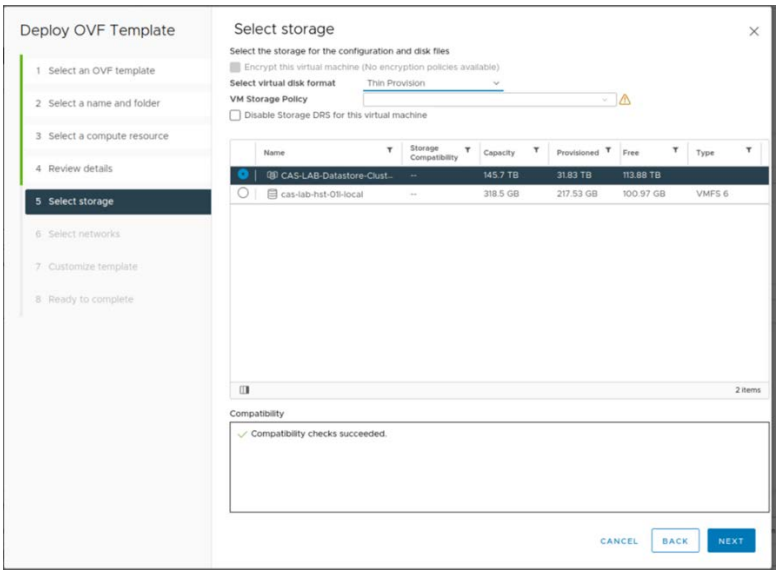
b. Click **Next**.

9. In the **Review details** page:
   a. Review the details.



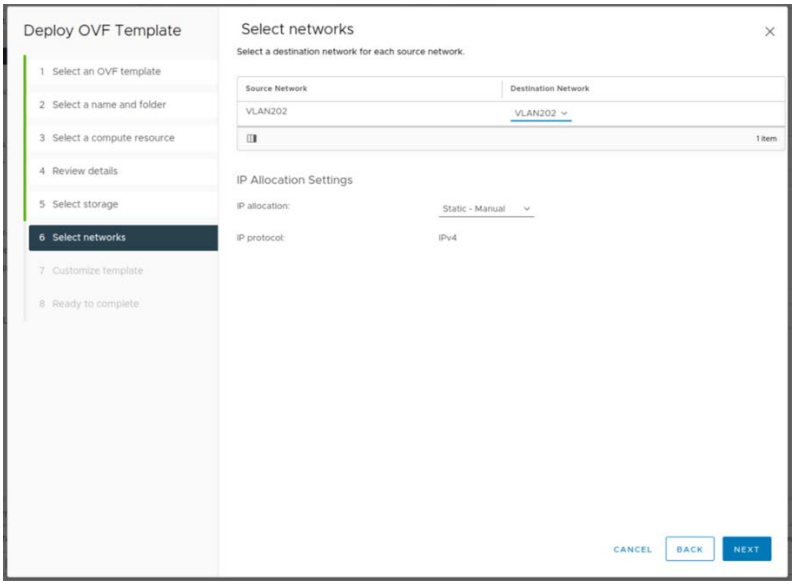
   b. To Avoid the “Certificate is not trusted” warning, see Appendix A: Removing the Certificate Warning.

10. In the **Select storage** page:
    a. Select your storage as per your environment.



b. Click **Next**.

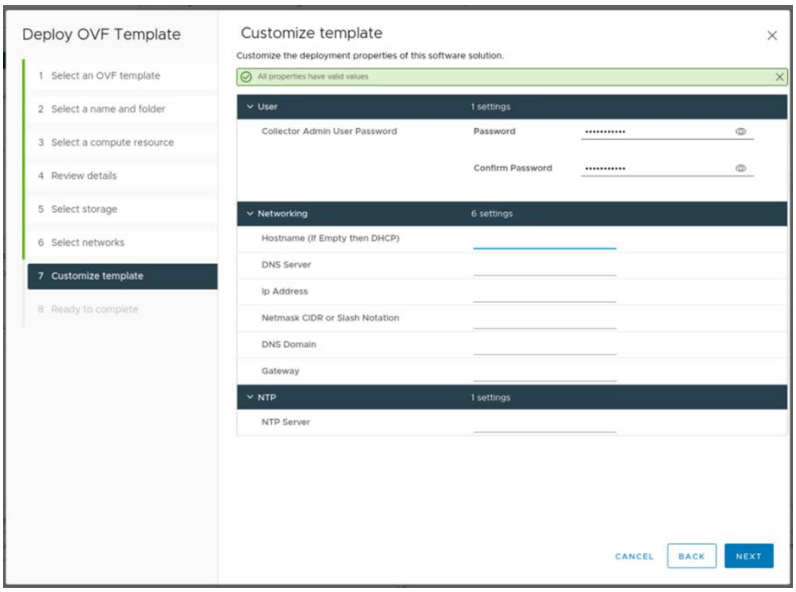
11. In **Select networks:**
    a. Select your **Destination vlan** as per your environment.
    b. Leave the defaults in IP Allocation Settings. We will change this in the next page.



c. Click **Next**.

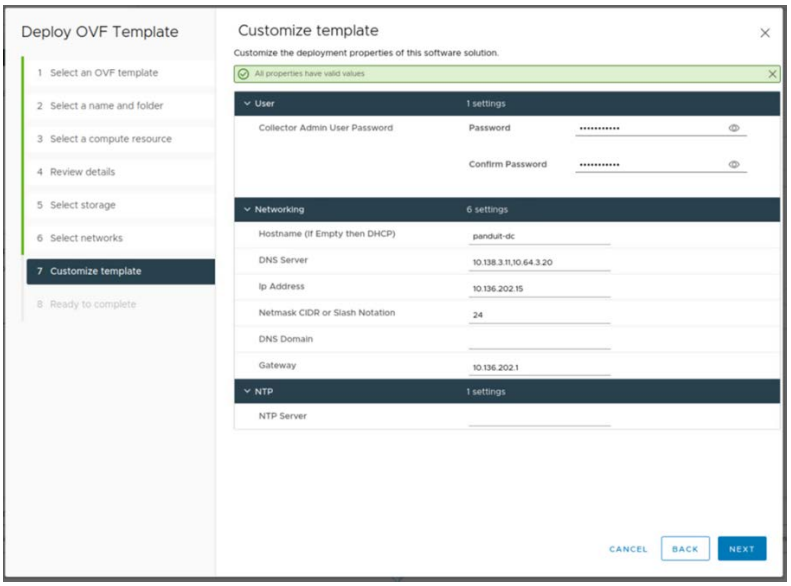
12. In the **Customize template** page:
    a. You will see three sections – User, Networking and NTP.
    b. User section:
        i. Provide the admin password and confirm the password for the collector in the User section. This password needs to be stored in a secure place because it will be used in the Nexus Dashboard.
    c. Network Section:

i. This section needs to be populated only when a static IP needs to be assigned. If you are using DHCP, then the Network section needs to be empty as shown below.



ii. For assigning static IP (only), you need to populate the following mandatory fields for the network to come up in the VM:

1. Hostname – Any unique hostname – Example: **panduit-dc**.
2. DNS Server – DNS server information. Example: 10.138.3.11 (for single DNS) or 10.138.3.11,10.64.3.20 (for multiple DNS servers).
3. IP Address – IP you wish to assign. Example: 10.136.202.15.
4. Subnet Netmask CIDR in slash notation.
   For 255.255.255.0 use 24
   For 255.255.255.128 use 25
   For 255.255.255.192 use 26
5. Gateway – Enter Gateway – Example: 10.136.202.1.

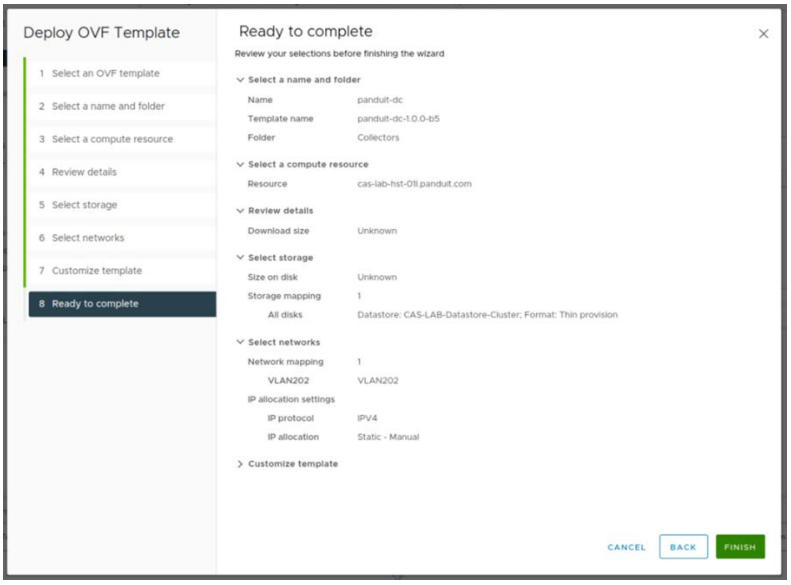


iii. DNS Domain is a non-mandatory field.

d. NTP
   i. This is a non-mandatory field
   ii. Provide the NTP server you wish to be part of the time synchronization of the VM. Example: **time.google.com**.

e. Click **Next**.

13. In the **Ready to complete** page:
    a. Review and click **Finish** to start the import process.



14. Once the import is complete, the new VM based on the OVA file will be created.

15. Power on the new VM for the collector to start. You can login to the VM using SSH with username as **panduit** and password as **panduit#1**.
16. You will be asked to change the default password during the first-time login via SSH.

Installation Option 2: Linux Installer

The collector can be installed on the Ubuntu Linux server. These are the Linux requirements.

Linux Environment Dependencies

- whiptail (for the whiptail command)
- docker-ce (for the docker command)
- docker-compose-plugin (for the docker compose command)
- Root access
- Docker hub registry access

Minimum Requirements for a Linux (AMD64/X86_64)

- 4 CPU cores
- 8 GB of RAM
- 50 GB of free space in the /opt partition or where the /opt directory resides
- Ubuntu Server LTS 22.04

Minimum Requirements for a Linux (RPI ARM64) Data Collector Device

- Raspberry Pi 4 Model B (8GB)
- 50 GB of free space (note: you must be using an SSD drive)
- Ubuntu Server LTS 22.04

Installation can begin once the pre-requisites are met.

1. Download the Linux Installer files from Panduit's download site.
2. Copy the installer file, installer signature, and public certificate to the Linux host.
3. Extract public key from the downloaded public certificate.

```
ubuntu> openssl x509 -pubkey -noout -in
panduit_public_cert.pem  > panduit_public_key.pem
```

4. Verify the Linux Installer.

```
ubuntu> openssl dgst -sha256 -verify panduit_public_key.pem -
signature panduit-dc-installer-linux-<version>.tar.gz.sig
panduit-dc-installer-linux-<version>.tar.gz

Verified OK
```

5. Check for “Verified OK” message.
6. Untar the Linux Installer.
   a. `ubuntu>tar -xvzf panduit-dc-<version>.tz`
7. Change to **panduit-dc directory**.

    a. `ubuntu>cd panduit-dc`
8. List the files in the directory. You will see one file (anduit-dc-install.sh) and one folder (components).
    a. `ubuntu>ls`
       `components  panduit-dc-install.sh`
9. Execute the **panduit-dc-install.sh**.
    a. `ubuntu>sudo ./panduit-dc-install.sh`
10. You will be prompted for admin user password. The password should:
    a. Have a minimum length of 8 characters
    b. Have at least one uppercase letter
    c. Have at least one lowercase letter
    d. Have at least one digit
11. The installer exits if you entered a password that does not match the criteria. You need to run the installer again from step 6 to continue.
12. If the password is valid then in the next screen re-confirm the password.
13. The installer will download all the appropriate containers to the Linux host and will start the collector.
14. If the installer was successful, then you will see an “Installation is done” message.

Upgrading Panduit Collector Software

Follow the instructions below to update the Panduit Collector software after it was installed through an OVA image or a Linux Installer. Note that this method only updates the Panduit collector software stack and not the Linux host or the Virtual Machine. In addition, it also does not affect the application's current state. All the registered devices and their configuration will remain intact after the upgrade.

1. Login to Panduit collector host via ssh.
    a. You can login to the VM using SSH with default credentials for the first time (panduit/ panduit#1)
2. Navigate to /opt/panduit/scripts folder.
    a. panduit@panduit-dc>cd /opt/panduit/scripts
3. Execute the upgrade script
    a. panduit@panduit-dc>sudo ./upgrade.sh
    b. It checks for connectivity to Docker hub
    c. Removes current Panduit collector images
    d. Retrieves the most recent collector images
4. Once the process finished you will see "Upgrade Complete" message

Troubleshooting

Issue 1: Network Issue on OVA based Virtual Machine:

1. Login to Panduit collector host via ssh.
    a. You can login to the VM using SSH with default credentials for the first time (panduit/ panduit#1)
2. Open the network configuration file.
    a. panduit@panduit-dc >sudo vi /etc/netplan/00-installer-config.yaml
3. Edit this file to suit your environment (DHCP or Static IP)
4. For DHCP the configuration should look like:

```
network:
  ethernets:
    ens160:
      dhcp4: true
      dhcp-identifier: mac
      optional: true
  version: 2
  renderer: networkd
```

5. For static IP setting the configuration should like the following:

```
network:
  ethernets:
    ens160:
      dhcp4: false
      addresses:
        - 10.136.205.15/24
      routes:
        - to: default
          via: 10.136.205.1
      nameservers:
        addresses: [10.138.3.11]

  version: 2
  renderer: networkd
```

   You need to replace IP (10.136.205.15), netmask (/24), default route (10.136.205.1) and the name server (10.138.3.11) with your network information.

6. Apply the netplan configuration once the configuration file is updated and saved
    a. panduit@panduit-dc >sudo netplan apply
7. Verify that your VM's network issue has been fixed

Issue 2: Log Files for Troubleshooting Panduit Collector

1. To access the Panduit collector log files, login to Panduit collector host via ssh.
    a. You can login to the VM using SSH with default credentials for the first time (panduit/ panduit#1)
2. The log files are located in /opt/panduit/logs directory
    a. panduit@panduit-dc >cd /opt/panduit/logs
3. There are two log files: PanduitNormalizer.log & PanduitCollector.log
4. Panduit collector logs error and other information into these two log files which can be helpful in troubleshooting.

Appendix A: Removing the Certificate Warning

To Avoid the “Certificate is not trusted” warning, import the Digi Cert’s Root and Intermediate certificate into vSphere.

The Certificates can be downloaded from Digi Cert’s web site:
https://www.digicert.com/kb/digicert-root-certificates.htm#roots

Note: Search using the specific Serial# listed below for the correct certificates in the Digi Cert’s website as there are many Root and Intermediate certificates listed there.

Digi Cert Root Certificate:

DigiCert Trusted Root G4
Valid until: 15/Jan/2038
Serial #: 05:9B:1B:57:9E:8E:21:32:E2:39:07:BD:A7:77:75:5C
SHA1 Fingerprint: DD:FB:16:CD:49:31:C9:73:A2:03:7D:3F:C8:3A:4D:7D:77:5D:05:E4
SHA256
Fingerprint: 55:2F:7B:DC:F1:A7:AF:9E:6C:E6:72:01:7F:4F:12:AB:F7:72:40:C7:8E:76:1A:C2:03:D1:D9:D2:0A:C8:99:88

Digi Cert Intermediate Certificate:

DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1
Issuer: DigiCert Trusted Root G4
Valid until: 28/Apr/2036
Serial #: 08:AD:40:B2:60:D2:9C:4C:9F:5E:CD:A9:BD:93:AE:D9
SHA1 Fingerprint: 7B:0F:36:0B:77:5F:76:C9:4A:12:CA:48:44:5A:A2:D2:A8:75:70:1C
SHA256
Fingerprint: 46:01:1E:de:1C:14:7E:B2:BC:73:1A:53:9B:7C:04:7B:7E:E9:3E:48:B9:D3:C3:BA:71:0C:E1:32:BB:DF:AC:6B

Download both the Root and Intermediate certificates into vSphere: