Cisco SD-WAN. Controllers onboarding.

- Post published:20/06/2019
- Post category:SD-WAN

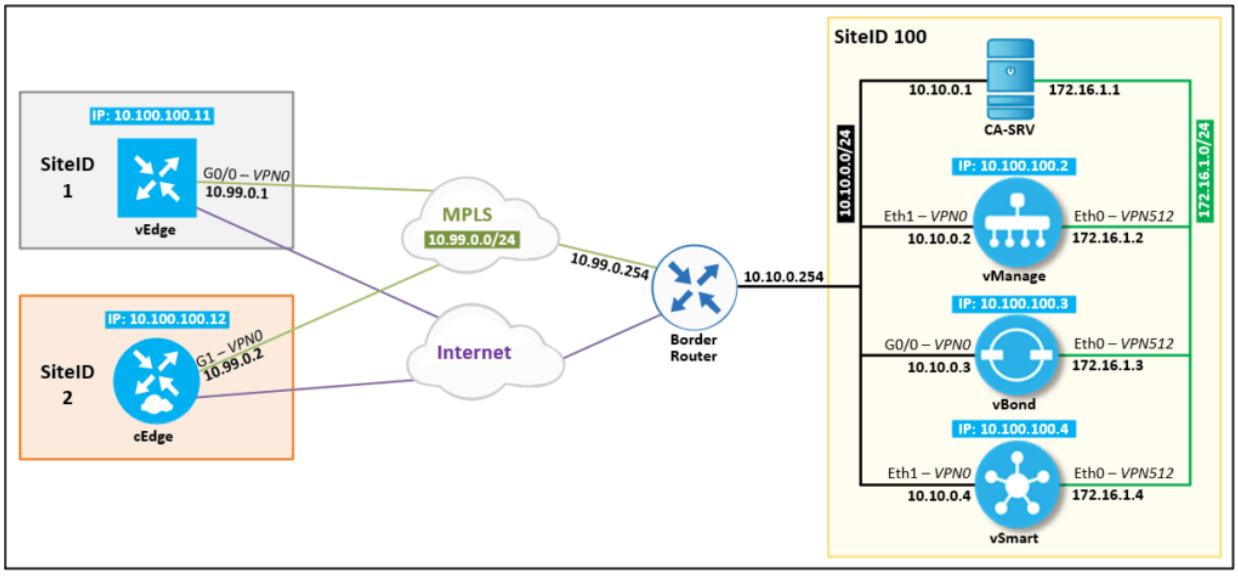
Building a SD-WAN lab leads to the need for onboarding, which is can be manual, mandatory for on-premise installations, or automated for cloud hosted deployments (AWS or Azure).

This post is the first one, i think there will be two in total, in which we download images, power-up lab and make basic configuration for devices.

First step in onboarding is downloading and installing required images from official site software.cisco.com. Software images can be downloaded from the Downloads Home/Routers/Software-Defined WAN (SD-WAN)/SD-WAN.
For this post i am using SD-WAN software version 19.1.0 with following image names:

- vManage: viptela-vmanage-19.1.0-genericx86-64.qcow2
- vBond and vEdge: viptela-edge-19.1.0-genericx86-64.qcow2
- vSmart: viptela-smart-19.1.0-genericx86-64.qcow2
- cEdge: csr1000v-ucmk9.16.11.1a-serial.qcow2

Because the lab purpose is to give an overview of onboarding of vDevices (vManager, vBond, vSmart, vEdge and cEdge), we use a simple topology, based on the following network diagram.



To be fast and effective, i use the best network simulation software, in my opinion, EVE-NG Pro. As usual, a guide for instalation and setup of Viptela images can be found in the How-To documentation area of EVE-NG website, for cEdge node installation follow steps described here. At the end of this document you can find download links for lab topology and node configurations. A Docker node (eve-gui-server) is used as a CA and for accessing web gui of vManage (users of EVE-NG Community Edition can use any other Linux node instead of Docker).

Basic configuration for vManage

After powering up vManage node in EVE-NG, we have to create and deploy a basic configuration that has to accomplish next requirements:

- Create a zone-based security, separating interfaces and VPNs in two categories, control (VPN 0) and management (VPN 512);
- Nodes connectivity, System IP, Site ID, Org-Name, vBond IP, Enterprise CA certificate.

We use the following, recommended, template:

```
system
 host-name vManage
 system-ip <vManage system IP>
 site-id   100
 admin-tech-on-failure
 organization-name "pocvlab sdwan"
 clock timezone Europe/Bucharest
 vbond <VPN0 VBOND IP>
!
vpn 0
 interface eth1
  ip address <VPN0 IP address/netmask>
  no shutdown
 ip route 0.0.0.0/0 <VPN0 gateway address>
!
vpn 512
 interface eth0
  ip address <VPN512 IP address/netmask>
  no shutdown
 ip route 0.0.0.0/0 <VPN512 gateway address>
!
ntp
 server 0.pool.ntp.org
  version 4
 exit
```

Be aware that organization-name must be consistent for all nodes, and must match exactly the value used in license. Check organization-name string that you plan to use, must be unique in Cisco database. You can check following steps from Cisco SD-WAN Edges licensing and onboarding, Add controller profile step.

Open web browser on Docker node and navigate to vManage web interface, authenticate using default username and password (admin/admin). Go to Administrator > Settings and verify that Organization Name is correctly displayed. Edit vBond settings and enter 10.10.0.3 in the IP address field.

If you don't configure vBond address under system settings, process of generating bootstrap config for vEdge node will not be successfull.

Basic configuration for vBond

vBond configuration has the next requirements:

- **Cannot be behind NAT**;
- Create a zone-based security, separating interfaces and VPNs in two categories, control (VPN 0) and management (VPN 512);
- Nodes connectivity, System IP, Site ID, Org-Name, vBond IP, Enterprise CA certificate.

Recommended template for this node is listed below. For the moment, tunnel-interface is disabled until the thrust chain between nodes is established:

```
system
 host-name vBond
 system-ip <vBond system IP>
 site-id 100
 organization-name "pocvlab sdwan"
 clock timezone Europe/Bucharest
 vbond <vBond VPN0 IP address> local vbond-only
!
vpn 0
 interface ge0/0
  ip address <VPN0 IP address/netmask>
  no tunnel-interface
  ipv6 dhcp-client
  no shutdown
 ip route 0.0.0.0/0 <VPN0 gateway address>
!
vpn 512
 interface eth0
  ip address <VPN512 IP address/netmask>
  no shutdown
 ip route 0.0.0.0/0 <VPN512 gateway address>
!
ntp
 server 0.pool.ntp.org
 version 4
exit
```

where `<vBond VPN0 IP address>` has to be equal with `<VPN0 IP address>`.

Basic configuration for vSmart Controller

Template for vSmart Controller is the next one:

```
system
 host-name               vSmart
 system-ip               <vSmart system IP>
 site-id                 100
 admin-tech-on-failure
 organization-name     "pocvlab sdwan"
 clock timezone Europe/Bucharest
 vbond <VPN0 VBOND IP>
!
vpn 0
 interface eth1
  ip address <VPN0 IP address/netmask>
```

```
  no tunnel-interface
  no shutdown
 ip route 0.0.0.0/0 <VPN0 gateway address>
!
vpn 512
 interface eth0
  ip address <VPN512 IP address/netmask>
  no shutdown
 ip route 0.0.0.0/0 <VPN512 gateway address>
!
ntp
 server 0.pool.ntp.org
  version 4
 exit
!
```

Verify connectivity to 10.10.0.2, 10.10.0.3, 10.10.0.254 and 10.10.0.1 using ping. It should be successful.

Before going further, check configuration on vManage, vBond and vSmart using `show control local-properties`. Verify that organizational name is correctly configured, site-id value assigned, system-ip uniquely configured, and vBond IP address correctly specified.

Root CA Certificate

To generate root CA certificate we use the following commands on Docker node (enter the same Organization Name used before when asked):

```
openssl genrsa -out CA.key 2048
openssl req -new -x509 -days 100 -key CA.key -out CA.crt
```

Now let's copy CA certificate to all three vDevices using scp:

```
scp CA.crt admin@172.16.1.2:
scp CA.crt admin@172.16.1.3:
scp CA.crt admin@172.16.1.4:
```

SSH into vManage and import the new Root-CA:

```
vManage# request root-cert-chain install /home/admin/CA.crt
Uploading root-ca-cert-chain via VPN 0
Copying ... /home/admin/CA.crt via VPN 0
Updating the root certificate chain..
Successfully installed the root certificate chain
```

Check if root CA is imported sucessful `using show certificate root-ca-cert`. Repeat the process on vBond and vSmart controllers.
On the Docker node, open Firefox and go to https://172.16.1.2/dataservice/system/device/sync/rootcertchain to resync vManage DB. You need to provide web user and password, which is admin/admin. The answer in JSON format should be: {"syncRootCertChain":"done"}.

From the vManage page (https://172.16.1.2), navigate to Configuration > Devices and then select Controllers in top left. Click Add Controller and select vBond from the list. Enter vBond VPN0 IP address, username and password (admin/admin). Deselect Generate CSR option and click Add. Repeat the process for the vSmart Controller.

Check on Administration > Settings page values for Organization Name and vBond ip address, should match the values used in basic configuration section. Change Controller Certificate Authorization to Enterprise Root certificate and import CA.crt.

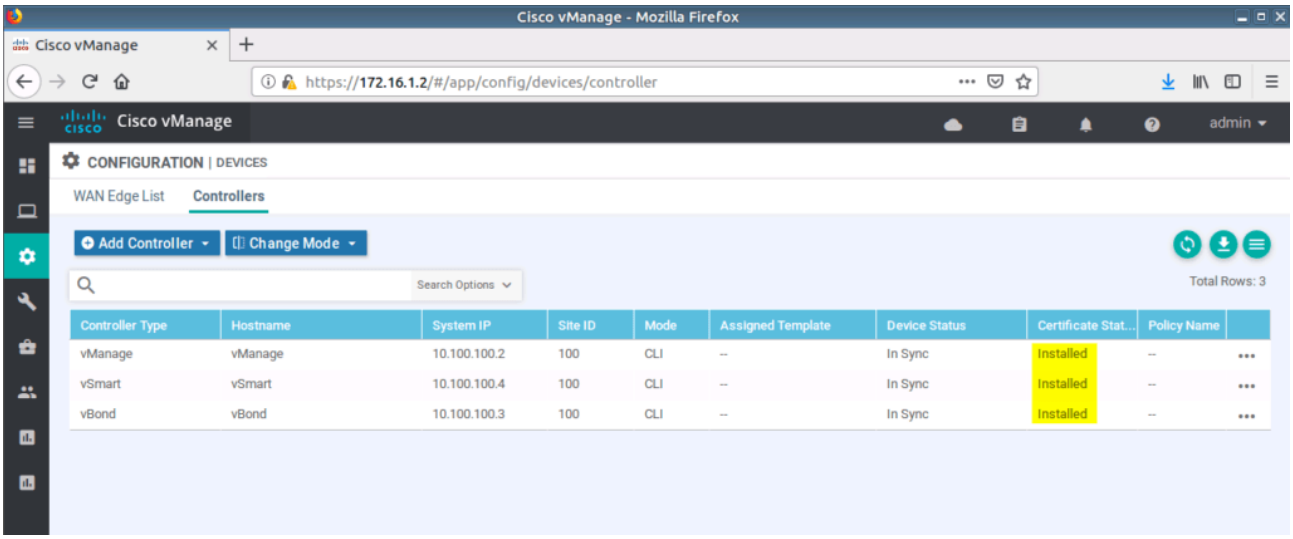
Navigate to Configuration > Certificates and then select Controllers in top left. In the right side for each device press on the three dots button to access Generate CSR option. Copy and paste the content in new file for each node, save files in /root directory as vManage, vBond.csr and vSmart.csr.

Sign CSRs using openssl:

```
openssl x509 -req -in vManage.csr -CA CA.crt -CAkey CA.key -CAcreateserial
-out vManage.crt -days 2000 -sha256
openssl x509 -req -in vBond.csr -CA CA.crt -CAkey CA.key -CAcreateserial -
out vBond.crt -days 2000 -sha256
openssl x509 -req -in vSmart.csr -CA CA.crt -CAkey CA.key -CAcreateserial
-out vSmart.crt -days 2000 -sha256
```

In the Configuration > Certificates > Controllers page, select vManage line and click Install Certificate, and install vManage.crt file. Repeat the process for vBond and vSmart.

Navigate to Configuration > Devices > Controllers, if the import of the certificate was sucessfull, you will see Certificate Installed status under all three controllers.



On the home dashboard, you notice that no control connection is established between nodes. One more step is needed, we have to configure `tunnel-interface` to VPN0 interface for each controller.

```
!vManage and vSmart
vpn 0
 interface eth1
```

```
  tunnel-interface
commit and-quit
!
!vBond
vpn 0
 interface ge0/0
  tunnel-interface
   encapsulation ipsec
commit and-quit
```

Check connection between vBond and the other two conntrollers, STATE of the connections should be UP:

```
vBond# show orchestrator connections
```

INSTANCE	PEER TYPE	PEER PROTOCOL	PEER SYSTEM IP	SITE ID	DOMAIN ID	PEER PRIVATE IP	PEER PRIVATE PORT	PEER PUBLIC IP	PEER PUBLIC PORT	REMOTE COLOR	STATE
0	vsmart	dtls	10.100.100.4	100	1	10.10.0.4	12346	10.10.0.4	12346	default	up
0	vsmart	dtls	10.100.100.4	100	1	10.10.0.4	12446	10.10.0.4	12446	default	up
0	vmanage	dtls	10.100.100.2	100	0	10.10.0.2	12346	10.10.0.2	12346	default	up
0	vmanage	dtls	10.100.100.2	100	0	10.10.0.2	12446	10.10.0.2	12446	default	up
0	vmanage	dtls	10.100.100.2	100	0	10.10.0.2	12546	10.10.0.2	12546	default	up
0	vmanage	dtls	10.100.100.2	100	0	10.10.0.2	12646	10.10.0.2	12646	default	up

In the next post we will see how we generate and install licenses for vEdge and cEdge and how the manual onboarding process works for these devices.

Lab Resources
EVE-NG Lab fileDownload
ViptelaNodesConfigDownload
Links
Viptela Overlay Network Bringup
Bringup Sequence of Events

SHARE IT NOWSHARE THIS CONTENT

- Opens in a new window
- Opens in a new window
- Opens in a new window

Read more articles

Next PostCisco SD-WAN. Edges licensing and onboarding.

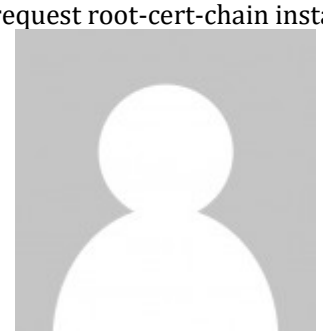
THIS POST HAS 21 COMMENTS

1. 

   NKK29 JUL 2019

   I got a question. I have generated CA.crt in docker, and i try below command as you mentioned, but it is no have this CA.crt, so update unsuccessful. When i use SCP in docker, it don't prompt me any error also. Need your advice.

vManage# request root-cert-chain install /home/admin/CA.crt

1. 

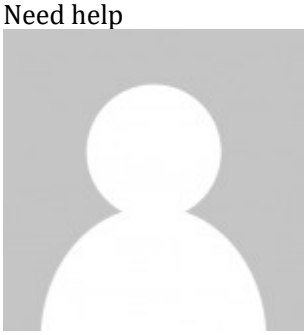
   alin.iorguta 29 JUL 2019

   Before using scp to copy CA.crt file to controllers, check if you have CA.crt in the current directory using ls command. Check if you can create a ssh session from docker to controllers (ssh admin@172.16.1.2 for example). Let me know what you find. Good Luck!

2. 

   NKK 10 AUG 2019

   resolved. i got the next problem when i add the controller (vbond and vsmart) in vManage. It prompt me error
   failed to add device
   java.net.SocketTimeoutException: connect timed out
   Need help

3. 

   NKK 12 AUG 2019

   java.net.SocketTimeoutException: connect timed out resolved. i remove the tunnel interface.

4. 

MSF 10 SEP 2019
When i load the certificate i get the following error
“Failed to decrypt serial number from certificate”
Need your advice

1. 
   Alin Iorguta 12 SEP 2019
   Please give me more information about the steps you have taken.
   Thx.

   1. 
      MSF 21 SEP 2019
      i got it resolved.thank

      1. 
         Suresh Kumar Vijayen 18 NOV 2019
         how do you resolved it?

5. 
   Adrian 27 SEP 2019

I'm testing the blog you've written.
I wonder if In Sync does not appear in Device Status after controller CA certification is completed.
The Certificate Status is all installed.

6. 

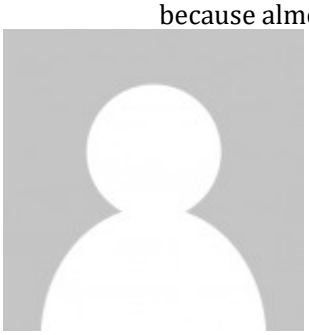
Sammt 2 OCT 2019

Thanks for amazing article. Please provide the password for EVE-NG lab file.
Thanks

   1. 

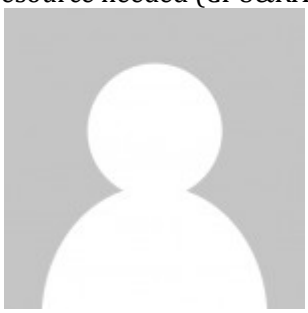
      alinux 2 OCT 2019

      Hi Sammt, thank you for the message. The lab file can be opened in EVE-NG Pro and can be used for all lab testing. Don't try to open the lab on Community edition because almost all nodes are not supported, for the moment.

7. 

mkav 15 OCT 2019

What is the resource needed (CPU&RAM&DISK) for this lab?

   1. 

      Alin Iorguta 15 OCT 2019

The resources are as follows: vManage-16GB/4CPU; vBond-2GB/2CPU; vSmart-2GB/2CPU; vEdge-2GB/1CPU; cEdge-4GB/2CPU and for disk you can count around 2,5GB per node.

8. 

Nik 1 NOV 2019

Great Post…
Is csr1000v-ucmk9.16.11.1a-serial.qcow2/csr1000v-ucmk9.16.11.1b-serial.qcow2 not compatible with viptela 18.4.302 qcow2 images ?
I successfully got vEdge to connect, however with csr, they register and then go down, After that I cannot log onto them using default username/password

1. 

Alin Iorguta 1 NOV 2019

Hi Nik,
please check if is not a resource allocation problem (at least 4GB RAM) for CSR, otherwise they should work.

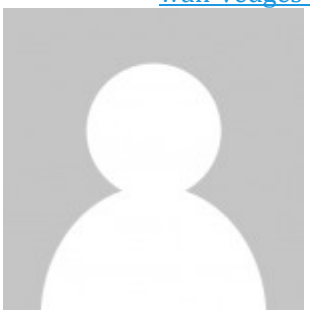
9. 

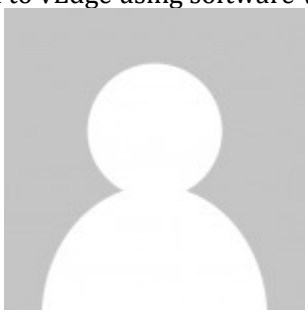
Nik 3 NOV 2019

Hi Alin
Thanks for your reply. CSR is UP but the control connection is not coming up
logs shows serial number is not accepted. I have checked valid-vedges in vbond and the chassis number is present.
But if i check on CSR, I see certificate not installed? root-chain certificate installed
cEdge# sh sdwan control local-properties
personality vedge
sp-organization-name lab sdwan
organization-name lab sdwan
root-ca-chain-status Installed

certificate-status Not-Installed
certificate-validity Not Applicable
certificate-not-valid-before Not Applicable
certificate-not-valid-after Not Applicable
cEdge#sh sdwan certificate serial
Certificate not yet installed … giving up.
Chassis number: CSR-78E1BD2C-3F37-18CA-AB60-9D57ACB4
Any idea why certificate status is not installed ?

1. 
   Alin Iorguta 4 NOV 2019
   Nik, prease see next post on how to onboard vedges. https://pocvlab.com/cisco-sd-wan-vedges-licensing-and-onboarding/

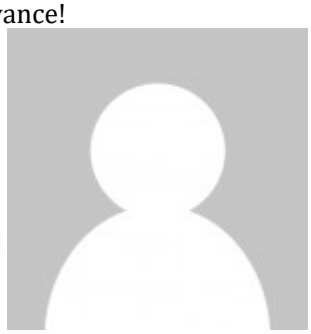
10. 
    OID 19 NOV 2019
    hallo all, why i cant login via username admin. after “System Initializing. Please wait to login…”
    Then “Login incorrect”
    im logging in to vEdge using software version viptela 18.4.303

    1. 
       Alin Iorguta 25 NOV 2019
       Hi,
       you have to wait a few minutes for the node to be ready to accept logins.

11. 

packetcaptur3 24 NOV 2019

Hi,
I just want to setup EVE-NG Viptela lab based on EVE-NG docs.
I can start for example vEdge and eve-ng shows that “vEdge: started”, but the icon remains gray so it does not start actually.
Do you have any idea why not starting devices properly?
Thanks in avance!

    1. 

    Alin Iorguta 25 NOV 2019

    Hello,
    first of all, you have to follow this guide for preparing Viptela images for EVE-NG.
    Second, you have to assure enough resources for vEdge (check Cisco SD-WAN recommendations) on EVE-NG host and don’t forget to enable Intel VT-x extensions on your host computer.