Installing and Deploying Avi Vantage for Cisco CSP

Avi Technical Reference (v20.1)

Installing and Deploying Avi Vantage for Cisco CSP

view online

Overview

Cisco Cloud Services Platform is a software and hardware platform for data center network functions virtualization (NFV). Avi Networks and Cisco partner to deliver a fully automated load balancing services on a turnkey NFV. This article explains how to install Avi Vantage on Cisco CSP.

Related reading: * Avi Vantage on Cisco CSP 2100 Sizing Guidelines * Avi Vantage on Cisco CSP 5000 Sizing Guidelines

Notes: 1. Avi Networks recommends running CSP v2.3.1 at a minimum. 2. Avi Networks recommends using VIRTIO as the disk type while configuring all Avi VNFs on CSP (Controllers and SEs). 3. Starting with Avi Vantage version 18.2.5, i40evf bonds are supported. This is supported only with CSP image version 2.4.1-185. 4. Starting with Avi Vantage version 18.2.9 and 20.1.1, 2.5.x /2.7.x version of CSP is supported.

CSP NIC Modes

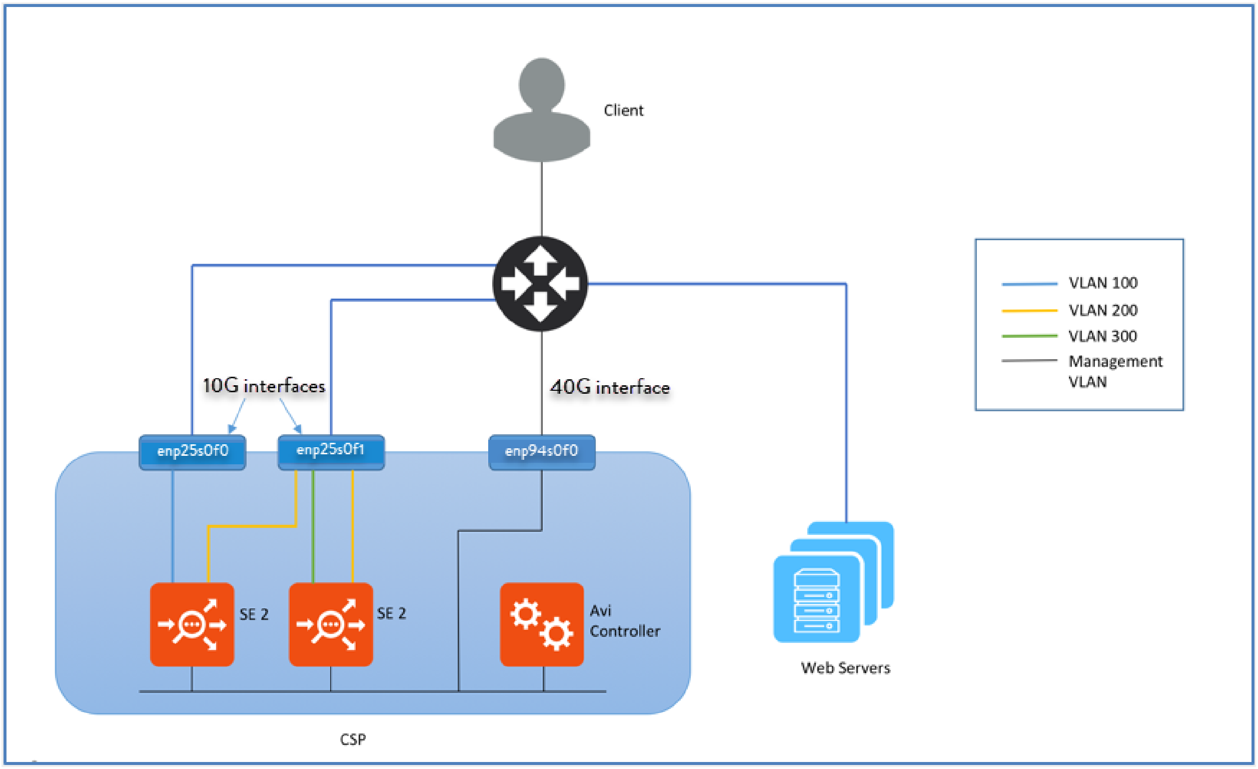
The following table explains three possible NIC mapping options on CSP and the corresponding performance implications:

```
<tr>
  <th>Mode
  </th>
  <th>Description
  </th>
  <th>Comments
  </th>
  <th>Drivers and Supported NICs<br>
  </th>
</tr>
<tr>
  <td>Access mode</td>
  <td>Traffic switched using OVS</td>
  <td>Allows physical NICs to be shared amongst VMs most generally. <br>
   Performance is generally lower due to soft switch overhead.</td>
  <td>NA
  </td>
</tr>
<tr>
  <td>Passthrough mode</td>
  <td>Physical NIC directly mapped to VM</td>
  <td>Physical NIC is dedicated to a VM.<br>
With 1x10 Gbps pNIC per VM, a maximum of 2 VMs or 4 VMs<br>can be created on a single CSP with 1 or 2 PCIe
dual-port<br>10-Gbps NIC cards. Provides the best performance.</td>
  <td>
ixgbe driver supports these NICs: 82599, X520, X540, X550, X552
<br><br>
i40e driver supports these NICs:<br>X710, XL710
  </td>
</tr>
<tr>
  <td>SR-IOV mode</td>
  <td>Virtual network functions<br>created from physical NIC</td>
  <td>Allows pNICs to be shared amongst VMs without sacrificing performance, as packets are switched in HW.<br>Maximum
  <td>
ixgbe-vf driver supports these NICs (and bonding): 82599, X520, X540, X550, X552<br><br>
i40e-vf driver supports these NICs (and bonding): X710, XL710
  </td>
</tr>
```

Topology

The topology explained below comprises of the Avi Controller and Avi Service Engines (SEs).
To leverage the DPDK capabilities of the physical NICs, the SEs should be connected to pNICs of the CSP in passthrough (PCIe) or SR-IOV mode. An instance is as given below: * 10 Gbps pNICs ? enp25s0f0 * 40 Gbps pNICs ? enp94s0f0

The SE can be connected to multiple VLANs on the pNICs? virtual functions (VF) in SR-IOV mode. The management network can be connected to the 10-Gbps pNIC.



Installing Avi Controller

Numad Service

The `numad` service needs to be disabled. CSP servers running versions 2.2.4 and above *may* have `numad` disabled by default.

numad is an user-level daemon that provides placement advice and process management for efficient CPU and memory utilization. On CSP servers, numad runs every 15 seconds and scans all candidate processes for optimization. The following are the required criteria for a candidate:
1. RAM usage greater than 300 MB. 2. CPU utilization greater than 50% of one core.

On CSP, numad takes each candidate process (which includes VNFs) and attempts to move either the process or its memory, so that they are on the same NUMA node (i.e., a physical CPU and its directly-attached RAM). On CSP servers, as it fails to move pages from memory, it takes about 10 to 30 seconds to move memory between NUMA nodes. This causes the VNFs processed by numad to hang during that duration. All processes, which includes even the VNFs, will become a candidate for numad after the holddown timer expires.

Note: Disabling numad is safe and has no adverse effects.

Avi SEs have high background CPU utilization, even when passing no traffic. This makes the Avi SE VNF a candidate for numad , which hangs the Avi SE VNF. This leads to various issues such as:
1. Heartbeat failures 2. BGP peer flapping 3. Inconsistent performance

Disabling numad service

1. Install Cisco CSP software.
2. Execute the following commands from CSP CLI:

```
avinet-3# config terminal
Entering configuration mode terminal
avinet-3(config)# cpupin enable
avinet-3(config)# end
Uncommitted changes found, commit them? [yes/no/CANCEL] yes
Commit complete.
avinet-3#
```

Notes: If the CSP server is running an older version than v2.2.4, contact Cisco support to disable numad.

Uploading Controller Image

1. Log on to the CSP dashboard on a browser.
2. Navigate to Configuration > Repository.
3. Click on the + sign, and browse to and select the Controller qcow2 image.
4. Click on Upload.

The Controller itself can have a day-zero YAML file before it is spun up. The YAML file needs to be imported into the repository prior to creating an image. Ensure you have VNC access to the console. In a large deployment, this might require additional firewall rules.

Note: A CSP cluster may have multiple copies (equal to the number of cluster hosts) of the same image/YAML file. Consequently, when any deletions are required, *all* copies should be deleted. Typically, you can change a key (such as auth token) with the same filename and re-upload.

Configuring Controller Metadata File

To configure the Controller management interface statically, the IP, netmask, and gateway information must be passed as a YAML file. The name of the metadata file must be in `avi_meta/*.yml` format.

For instance, create a text file with name `avi_meta_controller.yml` with contents as:

```
avi.mgmt-ip.CONTROLLER: "10.128.2.20"
avi.mgmt-mask.CONTROLLER: "255.255.255.0"
avi.default-gw.CONTROLLER: "10.128.2.1"
```

Here `avi.mgmt-ip.CONTROLLER` is the management IP for Avi controller, `avi.mgmt-mask.CONTROLLER` is the network mask and `avi.default-gw.CONTROLLER` is the gateway IP address for the management network. Make sure to replace the IP address in the example with correct ones for your network.

Upload this metadata file to CSP repository.

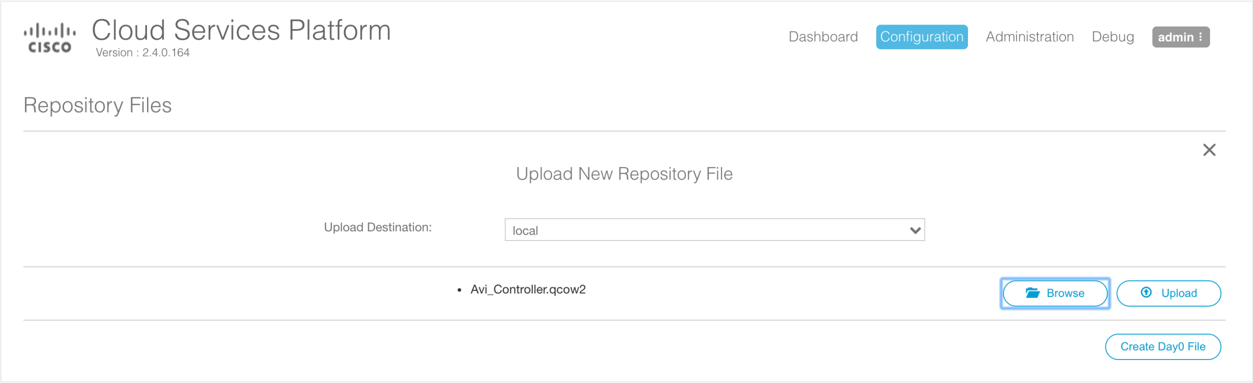
Deploying Avi Controller

This section describes how to deploy Avi Controller using both the CSP UI and the REST API.

Using CSP UI

Use the following steps to deploy the Avi Controller using the CSP UI:

1. Navigate to Configuration > Services.



Upload Destination: local

- Avi_Controller.qcow2

2. Click on +.

   Note: The disk size of any CSP image cannot be changed. To avoid deletion and recreation of the entire configuration, have an informed idea of deployment. Refer to System Requirements: Hardware and/or contact Avi for a recommendation.

3. Enter the Service Name.

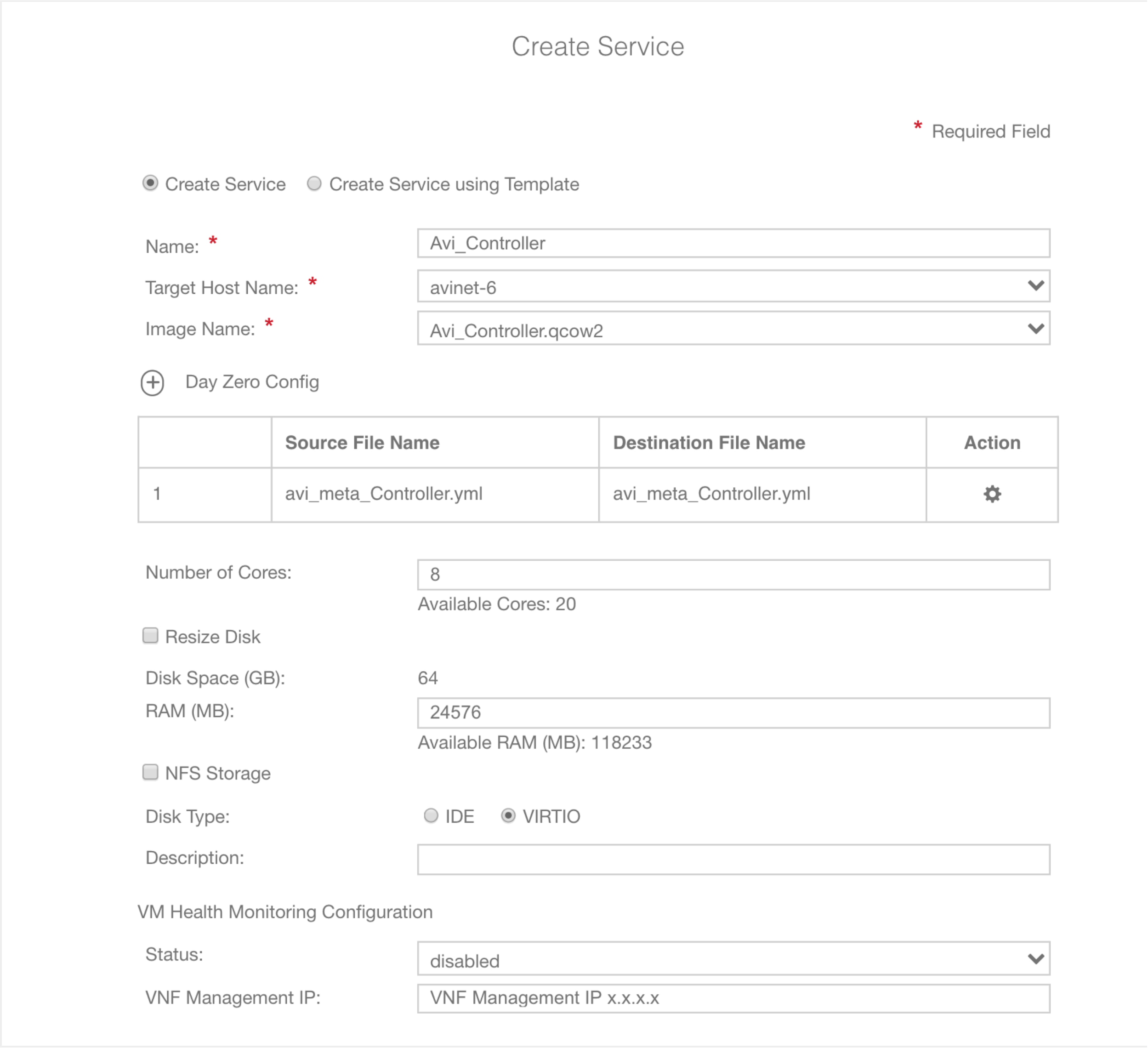
4. Click on Target Host Name and select the host from the list. In version CSP 2.1.0, on a CSP cluster, you can select the HA host name.

5. Leave the VNF Management IP field blank. This is set using the Day Zero Config.

6. Click on Image Name and select the controller.qcow2 image from the list.

7. Click on Day Zero Config dropdown and select the Controller metadata file.

8. Set the resource values for Disk, CPU and RAM (minimum values shown above).



Create Service

* Required Field

● Create Service ○ Create Service using Template

Name: * Avi_Controller

Target Host Name: * avinet-6

Image Name: * Avi_Controller.qcow2

⊕ Day Zero Config

	Source File Name	Destination File Name	Action
1	avi_meta_Controller.yml	avi_meta_Controller.yml	⚙

Number of Cores: 8
Available Cores: 20

□ Resize Disk

Disk Space (GB): 64

RAM (MB): 24576
Available RAM (MB): 118233

□ NFS Storage

Disk Type: ○ IDE ● VIRTIO

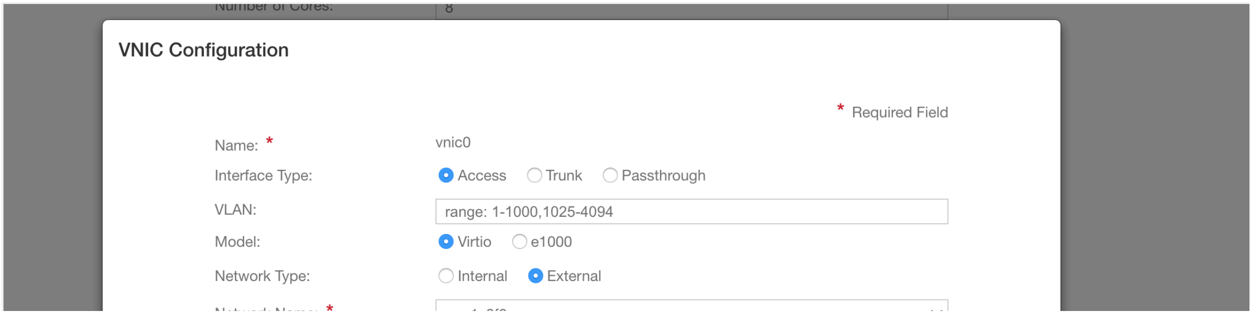
Description:

VM Health Monitoring Configuration

Status: disabled

VNF Management IP: VNF Management IP x.x.x.x

9. Click on + to add a vNIC and connect it to enp1s0f0 in access mode.



VNIC Configuration

* Required Field

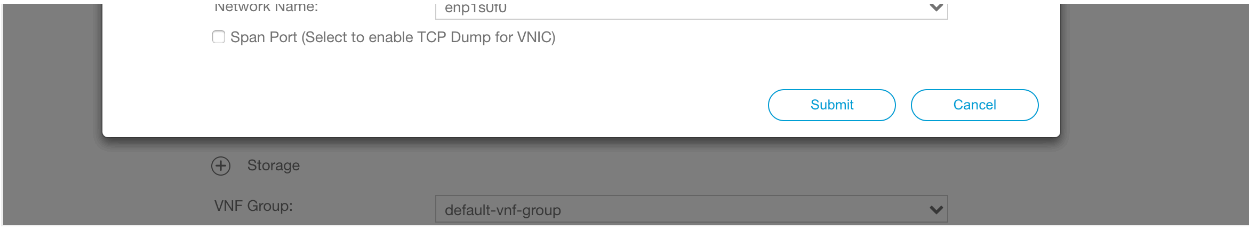
Name: * vnic0

Interface Type: ● Access ○ Trunk ○ Passthrough

VLAN: range: 1-1000,1025-4094

Model: ● Virtio ○ e1000

Network Type: ○ Internal ● External



Network Name: enp1s0f0

□ Span Port (Select to enable TCP Dump for VNIC)

VNF Group: default-vnf-group

Note: If the management network is on a different VLAN, specify the VLAN number in the VLAN field, and click on VLAN Tagged to enable tagging.

10. Specify a password for the console login using VNC, if required.
11. Click on Deploy.

Using REST API

CSP uses basic authentication for the REST API. Use the following `curl` command to create the Controller service:

```
curl -X POST --user admin:AviCsp@2100 -H "Content-Type: application/json" -d '{
   "service":{
     "name":"Controller",
     "power":"on",
     "iso_name":"controller.qcow2",
     "day0_filename":"avi_meta_controller.yml",
     "numcpu":8,
     "memory":24576,
     "vnics":{
       "vnic":[
         {
           "nic":"0",
           "type":"access",
           "tagged":"false",
           "network_name":"enp1s0f1"
         }
       ]
```

```
      }

    }

  }' -k "https://10.8.3.106/api/running/services/"
```

The CSP should reply with status code ?201 Created?.

To verify, get all installed services using following `curl` command:

```
curl -X GET --user username:password -H "Content-Type: application/json"  -k "https://10.8.3.106/api/running/services/s
```

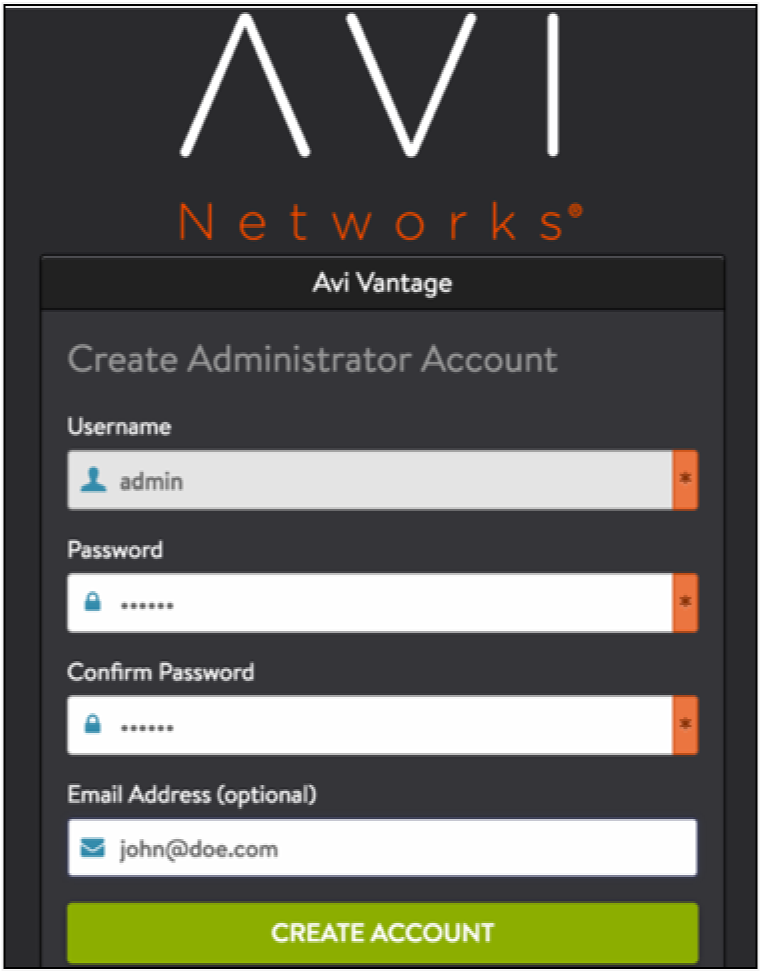
Response:

```
{
{

  "vsb:service": {

    "name": "Controller",

    "uuid": "368bf2e5-7590-4efc-b19b-2a501e616933",

    "memory": 24576,

    "numcpu": 8,

    "macid": 153,

    "disk_size": "64.0",

    "iso_name": "controller.qcow2",

    "power": "on",

    "day0_filename": "avi_meta_controller.yml",

    "vnics": {

      "vnic": [

        {

          "nic": 0

        }
      ]

    },

    "operations": {

      "export": "/api/running/services/service/Controller/_operations/export",

      "monitor": "/api/running/services/service/Controller/_operations/monitor"

    }

  }

}
```

Setting up Avi Controller

Use a browser to navigate to the Avi Controller IP address, and follow the below steps to perform the initial setup:

1. Configure an administrator password.



Avi Vantage

Create Administrator Account

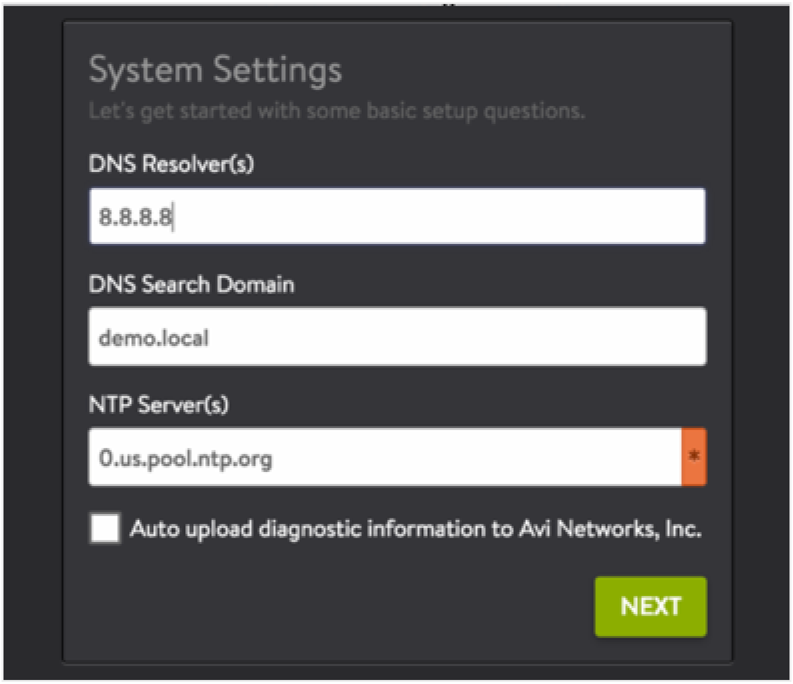
Username: admin

Password: ••••••

Confirm Password: ••••••

Email Address (optional): john@doe.com

2. Set DNS information.



System Settings

Let's get started with some basic setup questions.

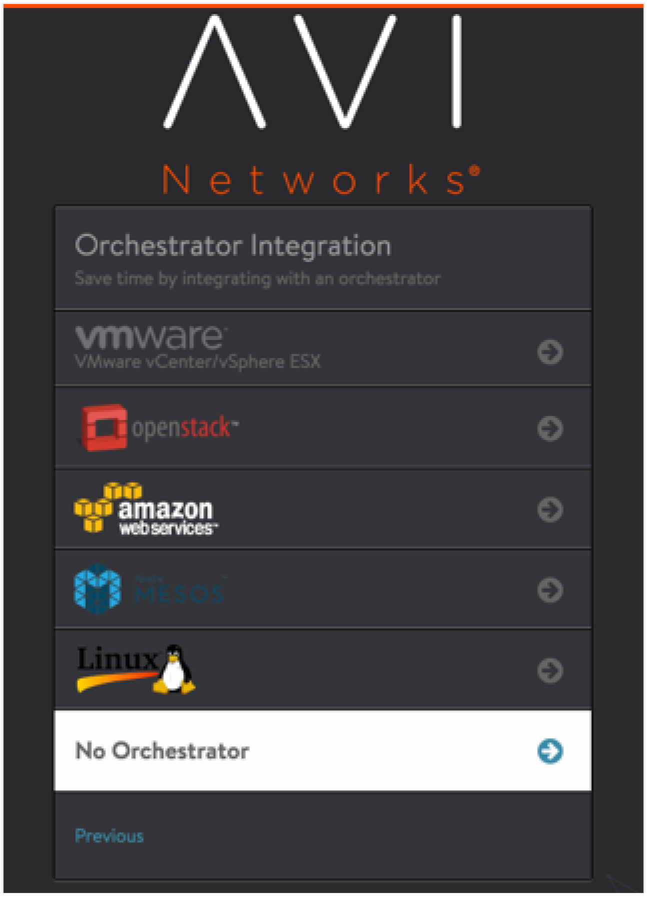
DNS Resolver(s): 8.8.8.8

DNS Search Domain: demo.local

NTP Server(s): 0.us.pool.ntp.org

□ Auto upload diagnostic information to Avi Networks, Inc.

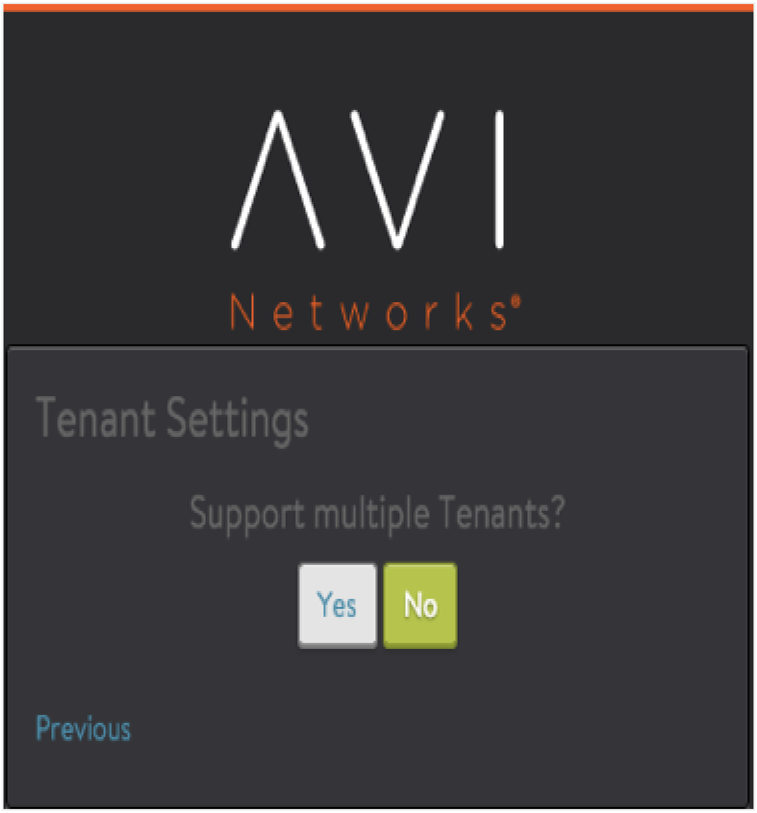
3. Select No Orchestrator.



Orchestrator Integration

Save time by integrating with an orchestrator

4. On the Tenant Settings wizard page, select the appropriate option. Refer to Tenants Versus SE Group Isolation.

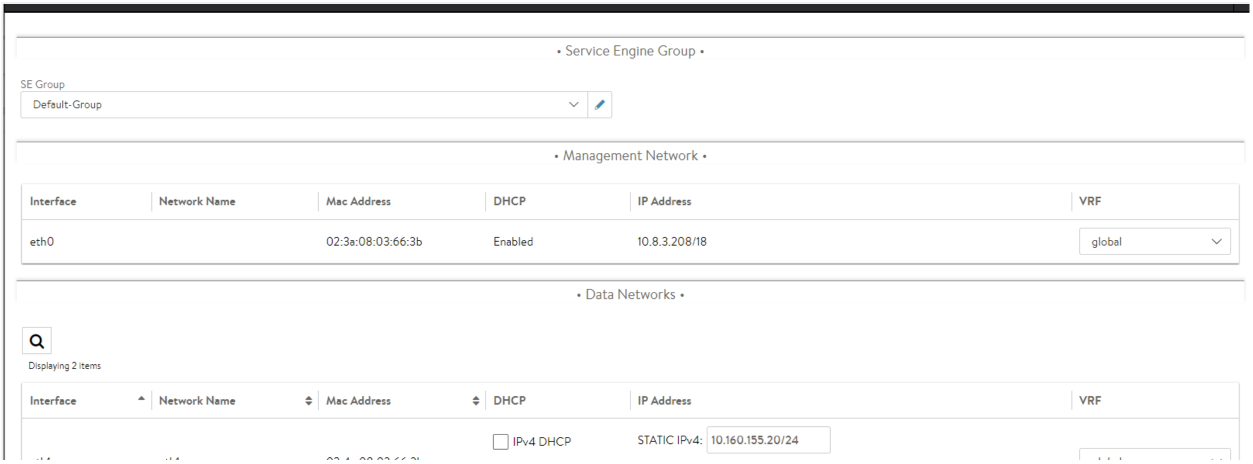


Deploying Avi Service Engine

This section walks through the workflow of deploying an Avi SE on CSP, with data NICs in SR-IOV passthrough mode.

Notes:

- Not every deployment will use SR-IOV, but if it is, it must be configured on the CSPs beforehand (for instance, numVFs).
- Starting with Avi Vantage version 18.1, Avi Vantage supports IPv6 for SE data interfaces.



• Service Engine Group •

SE Group: Default-Group

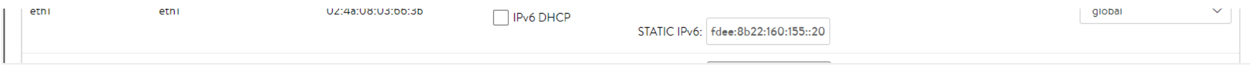
• Management Network •

Interface	Network Name	Mac Address	DHCP	IP Address	VRF
eth0		02:3a:08:03:66:3b	Enabled	10.8.3.208/18	global

• Data Networks •

Displaying 2 items

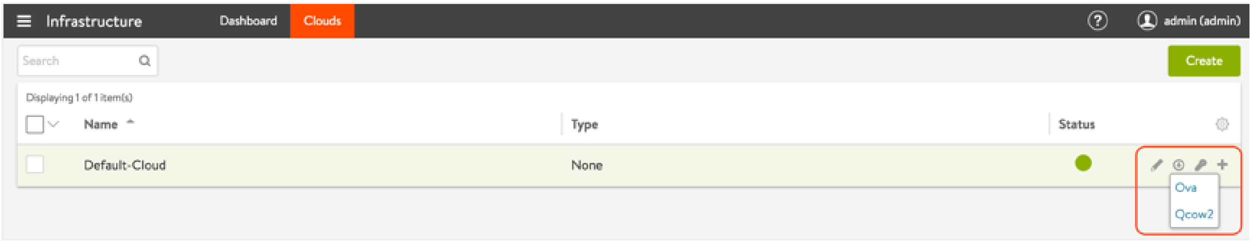
Interface	Network Name	Mac Address	DHCP	IP Address	VRF
			☐ IPv4 DHCP	STATIC IPv4: 10.160.155.20/24	



eth1 eth1 02:4a:08:03:66:3b ☐ IPv6 DHCP STATIC IPv6: fdee:8b22:160:155::20 global

Uploading SE Image

1. On the Avi Controller, navigate to Infrastructure > Clouds.
2. Click on the download icon on *Default Cloud* row and select Qcow2.



Displaying 1 of 1 item(s)

Name	Type	Status
Default-Cloud	None	●

3. Upload *se.qcow2* to the CSP repository.

Uploading SE Metadata File

To configure SE management interface statically, the IP, netmask and gateway information must be passed as a YAML file. The name of the metadata file must be in `avi_meta/*.yml` format.

For example, create a text file with name `avi_meta_se.yml` with contents as:

```
avi.mgmt-ip.SE: "10.128.2.18"
avi.mgmt-mask.SE: "255.255.255.0"
avi.default-gw.SE: "10.128.2.1"
AVICNTRL: "10.10.22.50"
AVICNTRL_AUTHTOKEN: "febab55d-995a-4523-8492-f798520d4515"
AVITENANT_UUID: 'tenant-f3fd4914-01e2-4fbf-b5bc-65b054700cee'
```

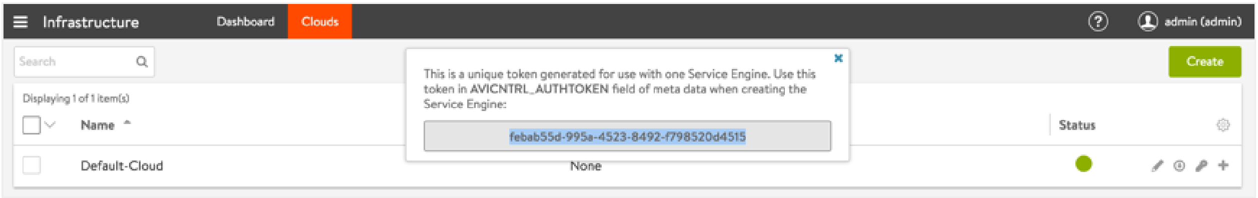
Here * `avi.mgmt-ip.SE` ? Management IP for Avi SE * `avi.mgmt-mask.SE` ? Network mask * `avi.default-gw.SE` ? Gateway IP address for the management network * `AVICNTRL` ? Management IP of the Avi Controller

Replace the IP address in the example with correct ones for your network.

`AVITENANT_UUID` (optional) is the UUID of the tenant on the Avi Controller to which the SE must connect. If this field is omitted, the SE will connect to the `admin` tenant by default.

`AVICNTRL_AUTHTOKEN` is the authentication token used to authenticate SE-to-Controller communication. Follow these steps to generate the authentication token: 1. Navigate to Infrastructure > Clouds.

2. Click on the key icon on the Default-Cloud row to view the authentication token key.



Displaying 1 of 1 item(s)

This is a unique token generated for use with one Service Engine. Use this token in AVICNTRL_AUTHTOKEN field of meta data when creating the Service Engine:

febab55d-995a-4523-8492-f798520d4515

Name	Type	Status
Default-Cloud	None	●

Note: The authentication token has a validity timeout of 1 hour by default.

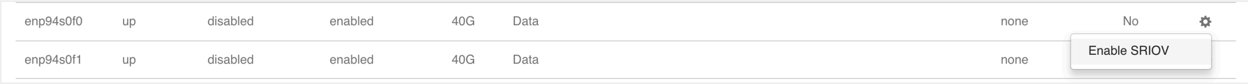
3. Copy the authentication token.

Upload this metadata file to the CSP repository.

Enabling SR-IOV

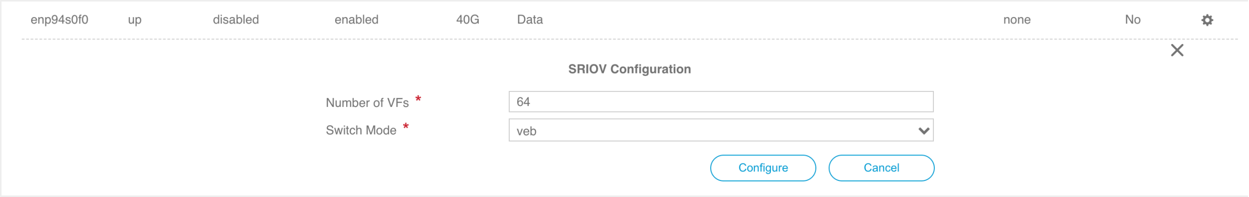
SR-IOV must be enabled on the CSP pNIC. Follow these steps to enable SR-IOV on `enp94s0f0`:

1. Navigate to Configuration > SRIOV Config. Click on the settings icon for the Enable SRIOV option.



enp94s0f0	up	disabled	enabled	40G	Data	none	No	⚙
enp94s0f1	up	disabled	enabled	40G	Data	none		

2. Under SRIOV Configuration, set the Number of VFs to a desired number and Switch Mode to *veb*.



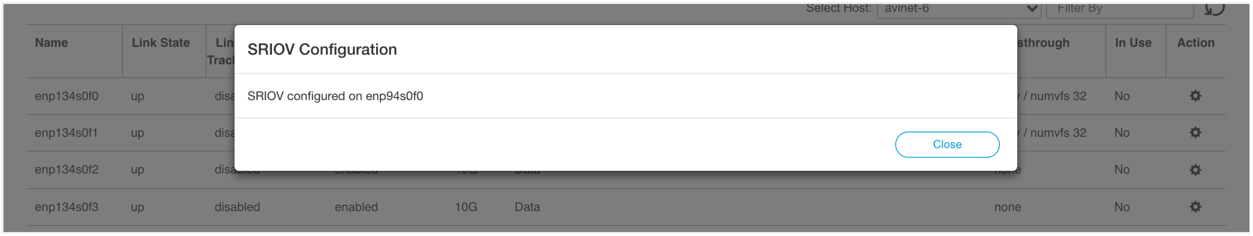
enp94s0f0	up	disabled	enabled	40G	Data	none	No	⚙

SRIOV Configuration

Number of VFs * 64

Switch Mode * veb

3. Confirm the SR-IOV configuration.



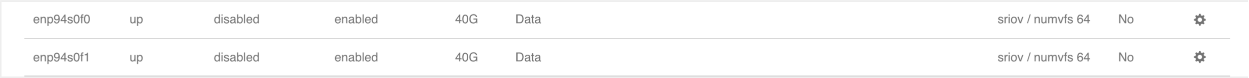
Select Host: avinet-6

SRIOV Configuration

SRIOV configured on enp94s0f0

Name	Link State	Lin Trac				sthrough	In Use	Action
enp134s0f0	up	disa				/ numvfs 32	No	⚙
enp134s0f1	up	disa				/ numvfs 32	No	⚙
enp134s0f2	up	disa					No	⚙
enp134s0f3	up	disabled	enabled	10G	Data	none	No	⚙

4. Repeat the above steps to configure `enp94s0f1` for SR-IOV if required.



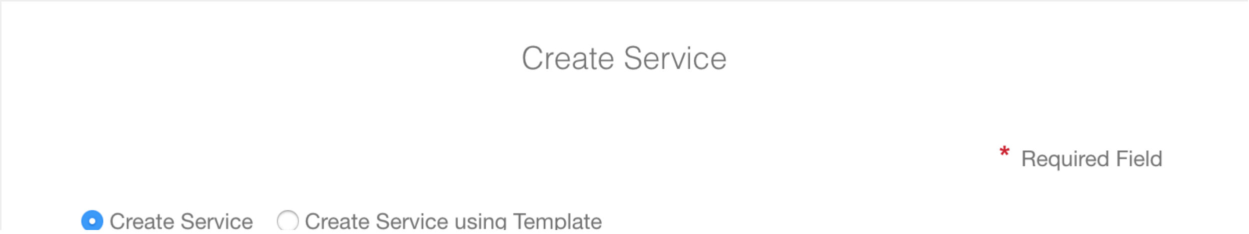
enp94s0f0	up	disabled	enabled	40G	Data	sriov / numvfs 64	No	⚙
enp94s0f1	up	disabled	enabled	40G	Data	sriov / numvfs 64	No	⚙

Deploying Service Engine in SR-IOV Mode

Follow these steps to deploy the Avi SE using the CSP UI:

1. Navigate to Configuration > Services.

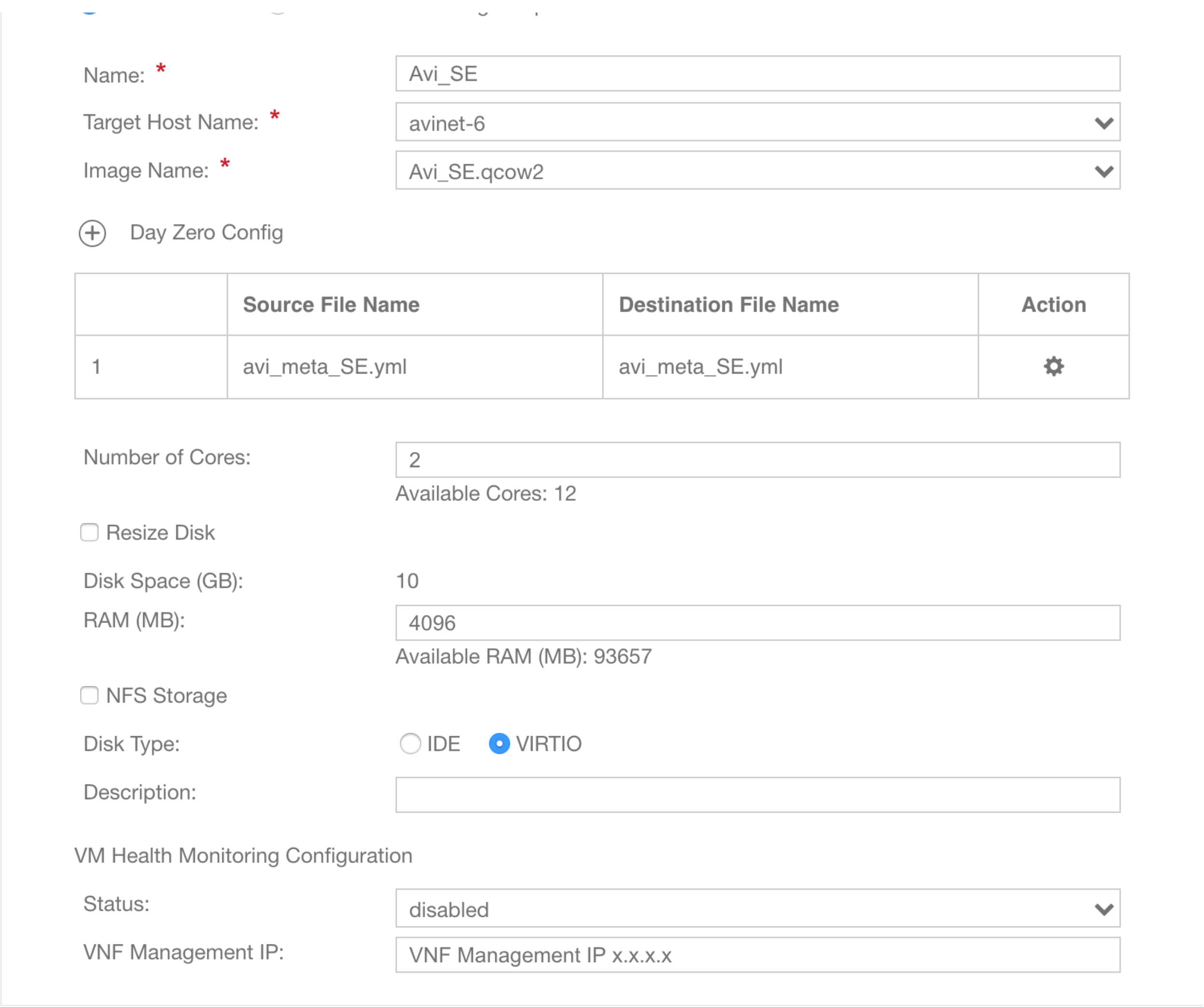
2. Click on +. Refer to System Requirements for recommendations on a minimum production SE configuration.



Create Service

* Required Field

● Create Service ○ Create Service using Template



Name: *	Avi_SE
Target Host Name: *	avinet-6
Image Name: *	Avi_SE.qcow2

	Source File Name	Destination File Name	Action
1	avi_meta_SE.yml	avi_meta_SE.yml	⚙

Number of Cores:	2 Available Cores: 12
□ Resize Disk	
Disk Space (GB):	10
RAM (MB):	4096 Available RAM (MB): 93657
□ NFS Storage	
Disk Type:	○ IDE ● VIRTIO
Description:	

VM Health Monitoring Configuration

Status:	disabled
VNF Management IP:	VNF Management IP x.x.x.x

3. Enter the Service Name.

4. Click on Target Host Name and select the host from the list.

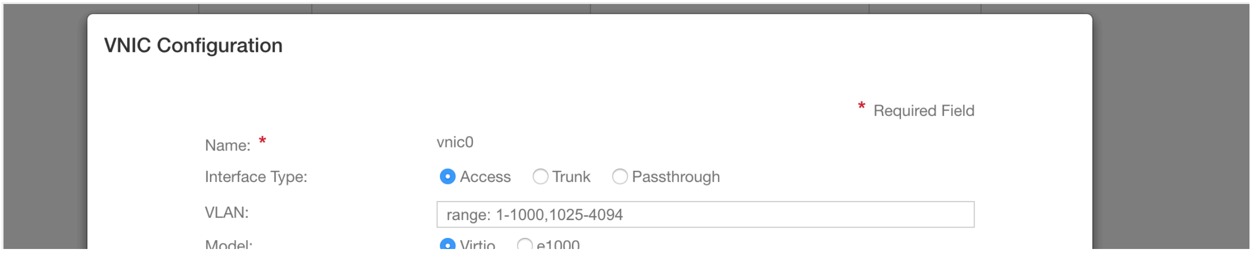
5. Leave the VNF Management IP field blank. This is set using the Day Zero Config.

6. Click on Image Name and select the se.qcow2 image from the list.

7. Click on Day Zero Config dropdown and select the SE metadata file.

8. Set the resource values for Disk, CPU and RAM (minimum values shown above).

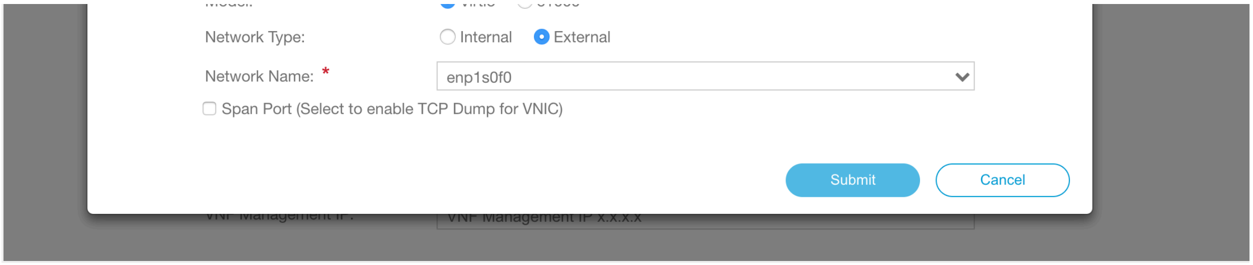
9. Click on + to add a vNIC and connect it to *enp1s0f0* in access mode.



VNIC Configuration

* Required Field

Name: *	vnic0
Interface Type:	● Access ○ Trunk ○ Passthrough
VLAN:	range: 1-1000,1025-4094
Model:	● Virtio ○ e1000



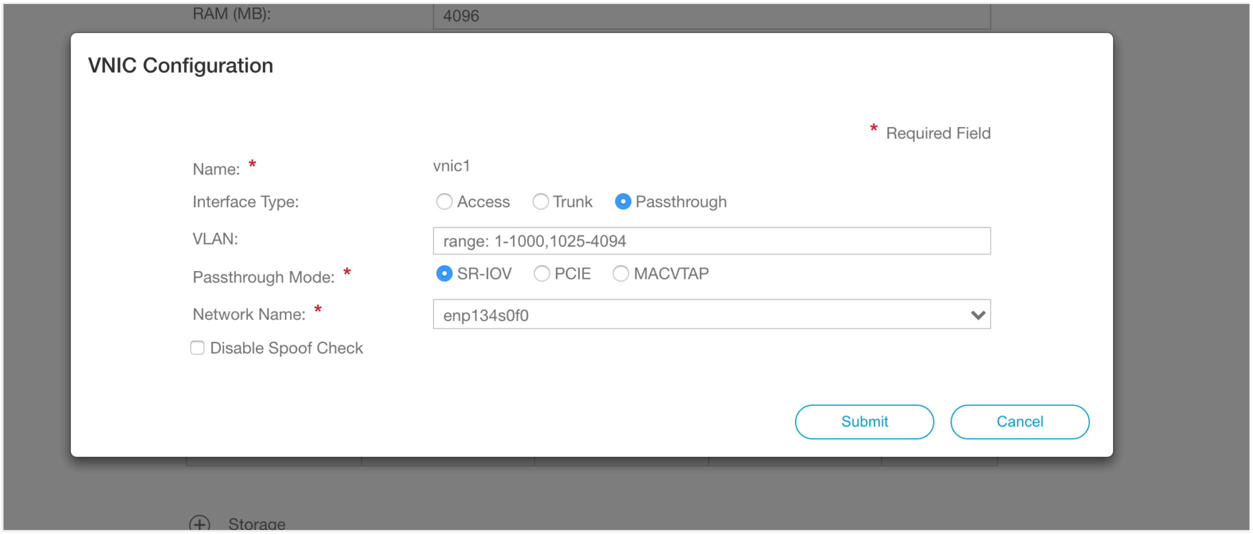
Network Type: ○ Internal ● External

Network Name: * enp1s0f0

□ Span Port (Select to enable TCP Dump for VNIC)

VNF Management IP: VNF Management IP x.x.x.x

10. Click on + to add a vNIC and connect it to *enp134s0f0* in SR-IOV mode.



RAM (MB): 4096

VNIC Configuration

* Required Field

Name: * vnic1

Interface Type: ○ Access ○ Trunk ● Passthrough

VLAN: range: 1-1000,1025-4094

Passthrough Mode: * ● SR-IOV ○ PCIE ○ MACVTAP

Network Name: * enp134s0f0

□ Disable Spoof Check

11. Specify a password for console login using VNC, if required.

12. Click on Deploy.

13. Verify the SE is able to connect to the Avi Controller by navigating to Infrastructure > Dashboard on the Avi Controller UI (this may take a few minutes).

Note: PF devices can be passed through to Service Engines. The method is the same as configuring a SR-IOV VF, with the exception that PCIE has to be selected for PF devices in the place of SR_IOV for VF devices.

CSP Ansible Roles

Refer to the links below for CSP related Ansible scripts: * https://github.com/avinetworks/ansible-role-avicontroller-csp * https://github.com/avinetworks/ansible-role-avise-csp

Related Articles

- Upgrading Avi Vantage Software
- Upgrades in an Avi GSLB Environment
- Deployment using Ansible scripts :
  - Avi Controller
  - Avi SE

Revision History

Edit Date	Applicable As Of Release	Summary
10Apr2018	All releases	Avi recommends CSP version 2.2.5 for CSP2100
30Apr2019	All releases	Avi recommends CSP version 2.3.1 for CSP5000