



# Installing and Deploying Avi Vantage for Cisco CSP-2100

Avi Technical Reference (v17.2)

# Installing and Deploying Avi Vantage for Cisco CSP-2100 [view online](#)

This article describes how to install Avi Vantage on the Cisco CSP 2100 platform.

Related reading: [Avi Vantage on Cisco CSP 2100 Sizing Guidelines](#)

## Notes:

1. *Avi Networks recommends running CSP version v2.2.5 at a minimum.*
2. *Avi Networks recommends using VIRTIO as the disk type when configuring all Avi VNFs on CSP (Controllers and SEs)*

## Networking Interfaces of CSP 2100

The following table shows the names of physical interfaces (pNICs) on the CSP 2100, along with their supported speeds.

Name	Speed
enp1s0f0	1 Gbps
enp1s0f1	1 Gbps
enp4s0f0	1 Gbps
enp4s0f1	1 Gbps
enp4s0f2	1 Gbps
enp4s0f3	1 Gbps
enp7s0f0	10 Gbps
enp7s0f1	10 Gbps

The pNIC named enp1s0f0 can be connected to the management network. This provides access to the CSP dashboard. The 10-Gbps interfaces (enp7s0f0 and enp7s0f1) can be used as data NICs and must be connected to the corresponding data VLANs or trunk links.

**Note:** For VLAN trunking, the maximum number of VLANs that can be added to SRIOV VF NICs created from a single PF is 64.

## CSP NIC Modes

The following table explains 3 possible NIC mapping options on CSP and the corresponding performance implications.

```
<tr>
  <th>Mode
</th>
  <th>Explanation
</th>
  <th>Comments
</th>
  <th>Drivers and Supported NICs<br>
```

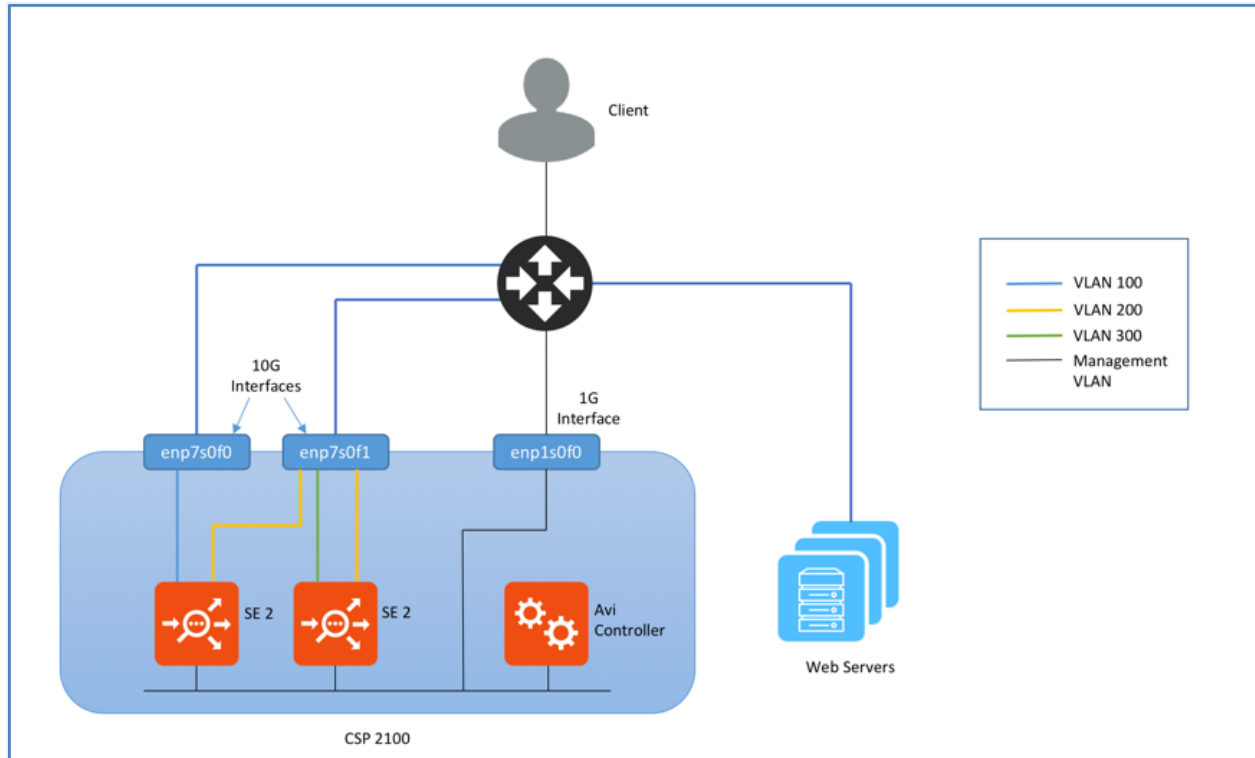
```

</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>but performance is generally lower due to soft s
  <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 best performance.</td>
  <td>
  ixgbe-vf driver supports these NICs: 82599, X520, X540, X550, X552
  <br><br>
  i40e-vf 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, since packets are switched in HW.<br>Maxim
  <td>
  ixgbe-vf driver supports these NICs (and bonding): 82599, X520, X540, X550, X552<br><br>
  i40e-vf driver supports these NICs (bonding not supported): X710, XL710
  </td>
</tr>

```

## Topology

The topology shown below consists of an Avi Controller and Avi Service Engines (SEs). To leverage the DPDK capabilities of the physical NICs, the SEs should be connected to the 10-Gbps enp7s0fx pNICs of the CSP 2100 in passthrough (PCIe) or SR-IOV mode. 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 1-Gbps pNIC.



## Installing The Avi Controller

### A Note on `numad` Service

#### Summary

The `numad` service needs to be disabled. CSP servers running versions 2.2.4 and above *may* have `numad` disabled by default, but it's wise to check, and then take action if need be.

#### What is `numad`?

`numad` is a user-level daemon that provides placement advice and process management for efficient use of CPUs and memory. On CSP servers `numad` runs every 15 seconds, and scans all processes for candidates for optimization. To be a candidate, the criteria are:

1. There is more than 300 Mbytes of RAM usage.
2. CPU utilization is greater than 50% of one core.

#### What issue is `numad` causing on CSP?

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, it is taking between 10 and 30 seconds to try to move memory between NUMA nodes. This is because it fails to move some pages from memory. This causes the VNFs which are being processed by `numad` to hang for that duration. All processes (which includes VNFs) will become a candidate for `numad` again once the holddown timer expires. Hence, this can cause repeated instability.

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

### How Avi is affected:

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

### To disable `numad`:

1. Install Cisco CSP software.
2. From the CSP CLI execute the following commands:

```
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: To disable `numad` if the CSP server is running a older version than v2.2.4, contact Cisco support.*

### Upload the Avi Controller Image

1. Log on to the CSP dashboard using a browser.
2. Navigate to Configuration > Repository.
3. Click on + sign, and browse to and select the Controller qcow2 image.
4. Click 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 image creation. Ensure you have VNC access to the console. In a large deployment, this *might* require additional firewall rules.

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

### Avi 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/*.yaml` format.

For example, create a text file with name `avi_meta_controller.yaml` 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 as shown in 3.1.

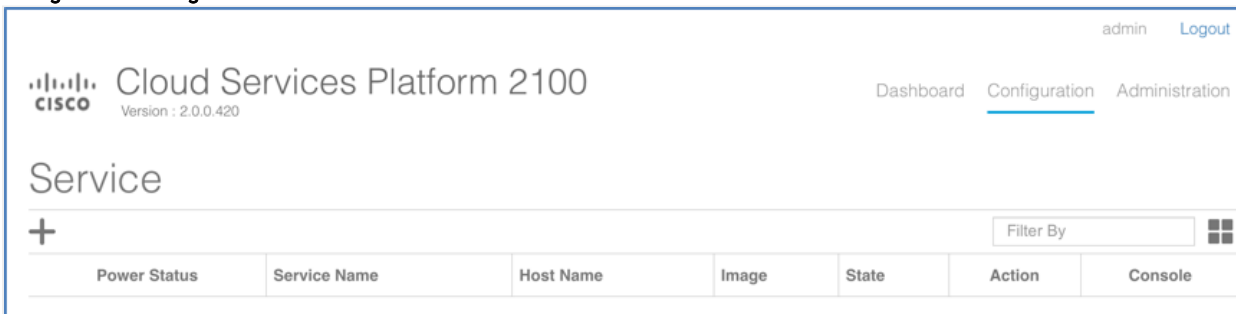
## Deploy the Avi Controller

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

### Deploy Using CSP UI

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

1. Navigate to Configuration > Services.



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.

Create Service
  Create Service using Template

Name: \*

Target Host Name: \*

VNF Management IP:

Image Name: \*

Day Zero Config

	Source File Name	Destination File Name	Action
1	avi_meta_data_ctr.yml	avi_meta_data_ctr.yml	

Number of Cores:   
 Available Cores: 16

Do you want to resize disk?

Disk Space (GB):   
 Available Disk Space (GB): 2563 | Minimum Disk Size (GB) : 64

RAM (MB):	<input type="text" value="18432"/>
	Available RAM (MB): 196302
<input type="checkbox"/> NFS Storage	
Disk Type:	<input type="radio"/> IDE <input checked="" type="radio"/> VIRTIO

- Enter ?Avi Controller? in the Service Name field and press enter.
- 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.
- Leave the VNF Management IP field blank. This is set using the Day Zero Config.
- Click on Image Name and select the controller.qcow2 image from the list.
- Click on Day Zero Config dropdown and select the Controller metadata file.
- Set the resource values for Disk, CPU and RAM (minimum values shown above)
- Click on + to add a vNIC and connect it to enp1s0f0 in access mode.

Name: *	<input type="text" value="vnic0"/>
VLAN Type:	<input checked="" type="radio"/> Access <input type="radio"/> Trunk <input type="radio"/> Passthrough
VLAN:	<input type="text" value="range 1-1000,1025-4094"/>
VLAN Tagged:	<input type="radio"/> True <input checked="" type="radio"/> False
Native VLAN:	<input type="text" value="range 0-4095"/>
Model:	<input type="radio"/> Virtio <input checked="" type="radio"/> e1000
Network Type:	<input type="radio"/> Internal <input checked="" type="radio"/> External
Network Name: *	<input type="text" value="enp1s0f0"/>

**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.

- (optional) Specify a password for console login using VNC.
- Click Deploy.

## 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 csp-username:csp-password -H "Content-Type: application/json" -d '{
  "service":{
    "disk_size": "64",
    "name": "Controller",
    "power": "on",
    "iso_name": "controller.qcow2",
    "day0_filename": "avi_meta_controller.yml",
    "numcpu": 6,
    "memory": 18432,
    "vnics": {
      "vnic": {
        {
```

```

        "nic": "0",
        "type": "access",
        "tagged": "false",
        "network_name": "enpl1s0f0"
    }
  ]
}
}
}' "https://

<csp-ip>
  /api/running/services/"
</csp-ip>

```

The CSP should reply with status code 201 Created?

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

```
curl -X GET --user csp-username:csp-password -H "Content-Type: application/json" "https://10.128.2.16/api/running/servi
```

Response:

```

{
  "service": [
    {
      "disk_size": "64.0",
      "name": "Controller-16-2",
      "power": "on",
      "iso_name": "controller.qcow2",
      "day0_filename": "avi_meta_controller.yml",
      "numcpu": 6,
      "macid": 65,
      "memory": 18432,
      "vnics": {
        "vnic": [
          {
            "nic": 0
          }
        ]
      },
      "uuid": "d8b977fe-42e7-48dd-a6a4-79f4ab5a8f0f"
    }
  ]
}

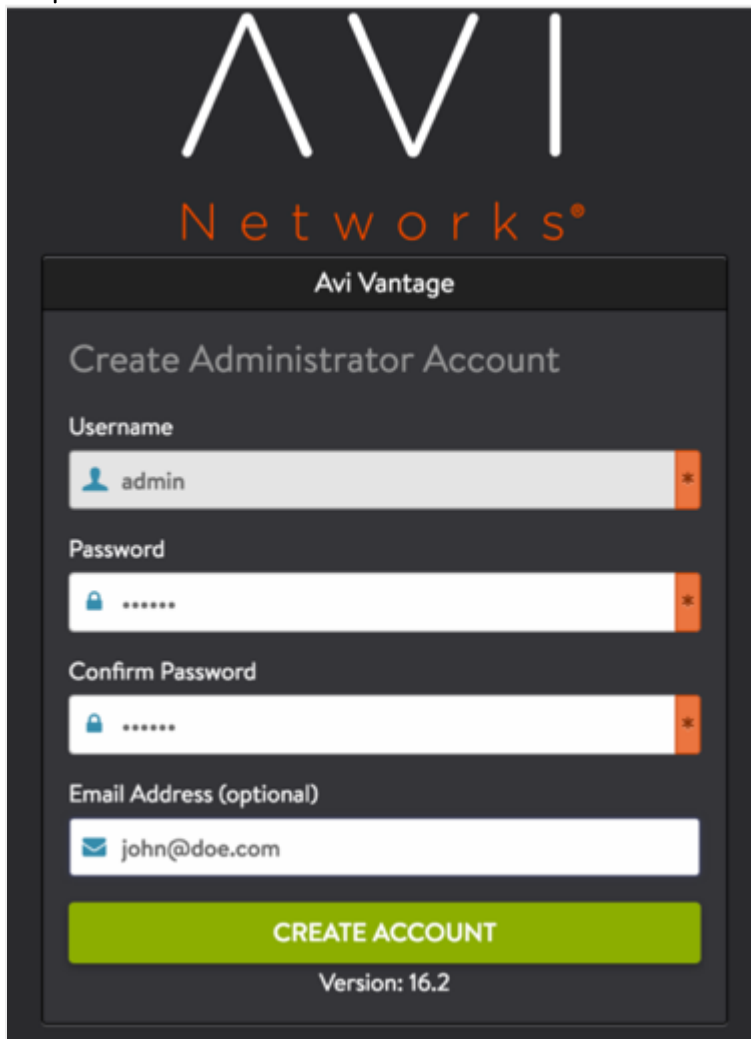
```



## Initial Setup of Avi Controller

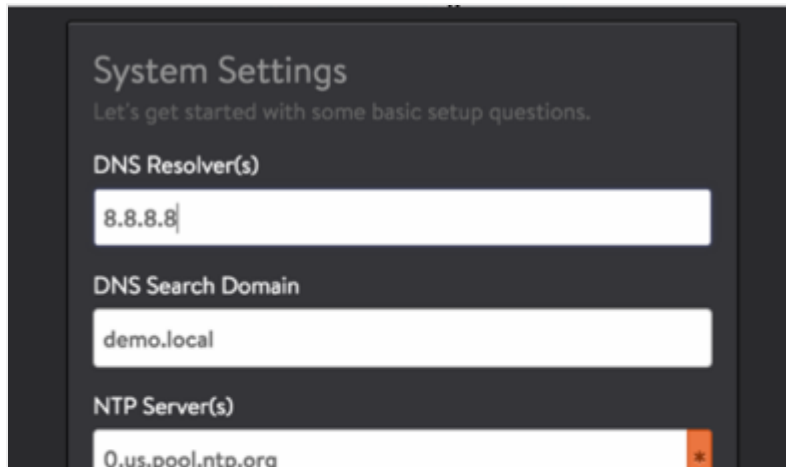
Use a browser to navigate to the Avi Controller IP address, and follow the below steps to perform initial setup:

1. Configure an administrator password.

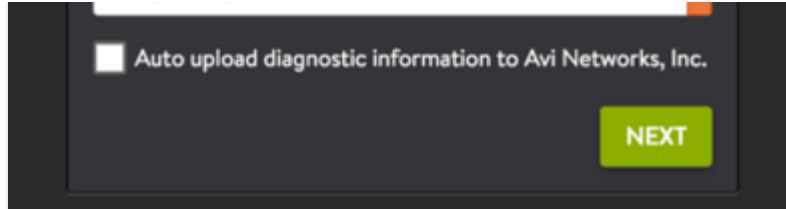


The screenshot shows the 'Create Administrator Account' form in the Avi Vantage interface. At the top, the Avi Networks logo is displayed. Below it, the text 'Avi Vantage' is centered. The form title is 'Create Administrator Account'. It contains four input fields: 'Username' with the value 'admin', 'Password' with masked characters '\*\*\*\*\*', 'Confirm Password' with masked characters '\*\*\*\*\*', and 'Email Address (optional)' with the value 'john@doe.com'. A green 'CREATE ACCOUNT' button is at the bottom, with 'Version: 16.2' displayed below it.

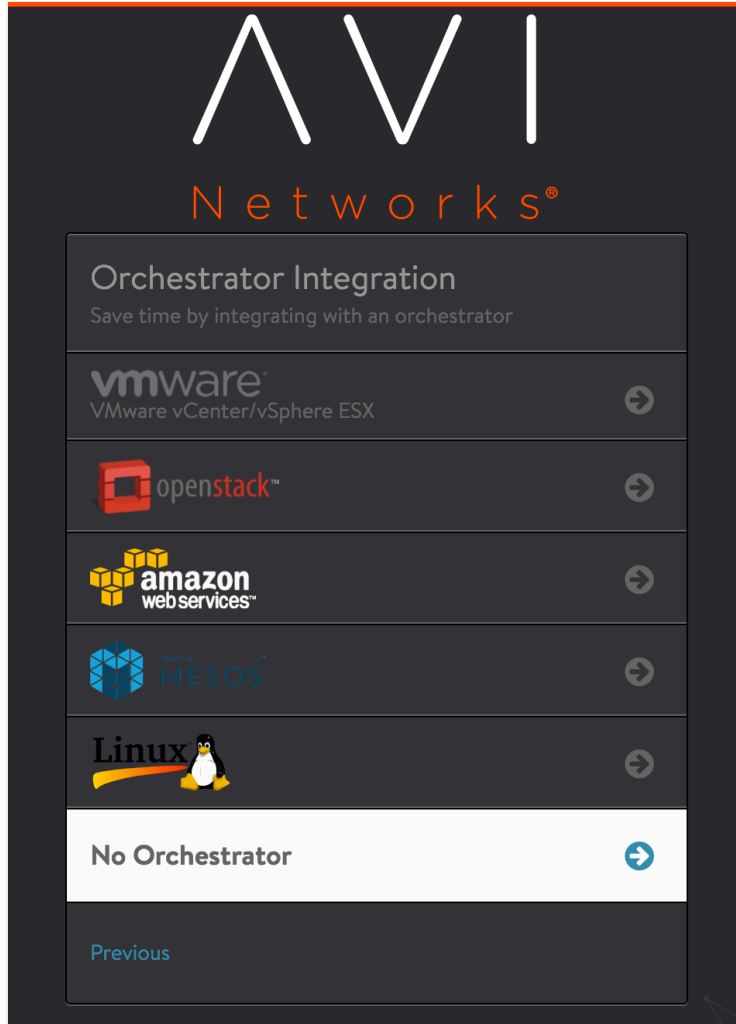
2. Set DNS information.



The screenshot shows the 'System Settings' form in the Avi Vantage interface. The title is 'System Settings' with the subtitle 'Let's get started with some basic setup questions.' Below this, there are three input fields: 'DNS Resolver(s)' with the value '8.8.8.8', 'DNS Search Domain' with the value 'demo.local', and 'NTP Server(s)' with the value '0.us.pool.ntp.org'. A small orange asterisk icon is visible to the right of the NTP Server(s) field.

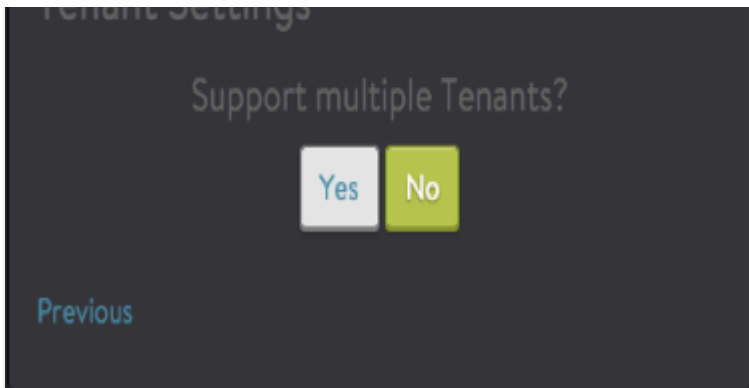


3. Select No Orchestrator.



4. On the Tenant Settings wizard page, select the appropriate option. Refer to [Tenants Versus SE Group Isolation](#).





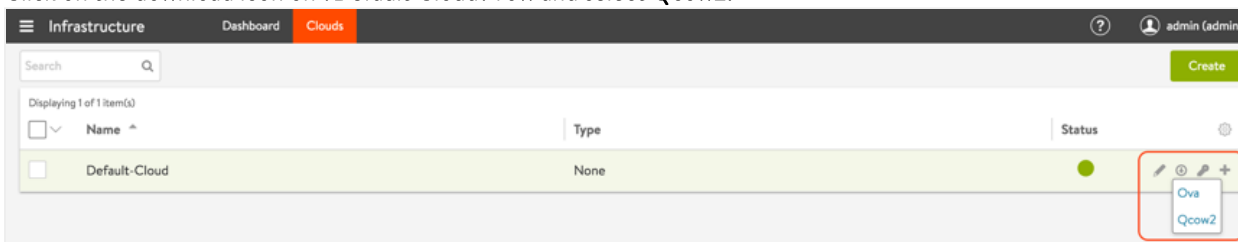
## Deploy Avi SE

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

**Note:** Not every deployment will use SR-IOV, but if it is, it must be configured on the CSPs beforehand (e.g., numVFs). A figure appearing in the Enable SR-IOV section of this article shows the number of VFs and the switch mode being set.

### Upload SE image

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



3. Upload the se.qcow2 to the CSP repository ([steps to upload](#)).

### Upload 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/\*.yaml format.

For example, create a text file with name avi\_meta\_se.yaml with contents as:

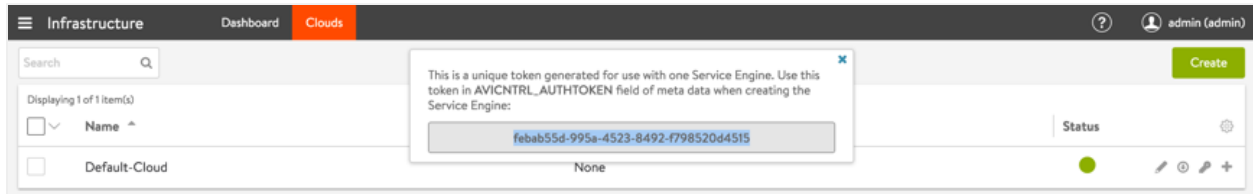
```
avi.mgmt-ip.SE: "10.128.2.18"
avi.mgmt-mask.SE: "255.255.255.0"
avi.default-gw.SE: "10.128.2.1"
AVICNTRL: "10.10.22.50"
AVICNTRL_AUTHTOKEN: "febab55d-995a-4523-8492-f798520d4515"
AVITENANT_UUID: 'tenant-f3fd4914-01e2-4fbf-b5bc-65b054700cee'
```

Here avi.mgmt-ip.SE is the management IP for Avi SE, avi.mgmt-mask.SE is the network mask and avi.default-gw.SE is the gateway IP address for the management network. AVICNTRL is the management IP of the Avi Controller. Make sure to 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.



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 ([steps to upload](#)).

## Enable SR-IOV

SR-IOV must be enabled on the CSP pNIC. Follow these steps to enable SR-IOV on `enp7s0f0`:

1. Navigate to Configuration > SRIOV Config
2. Click on the settings icon



for `enp7s0f0`.

3. Set the ?Number of VFs? to the desired number.
4. Set the ?Switch Mode? to `veb`.

### SRIOV Configuration

Number of VFs \*

Switch Mode \*

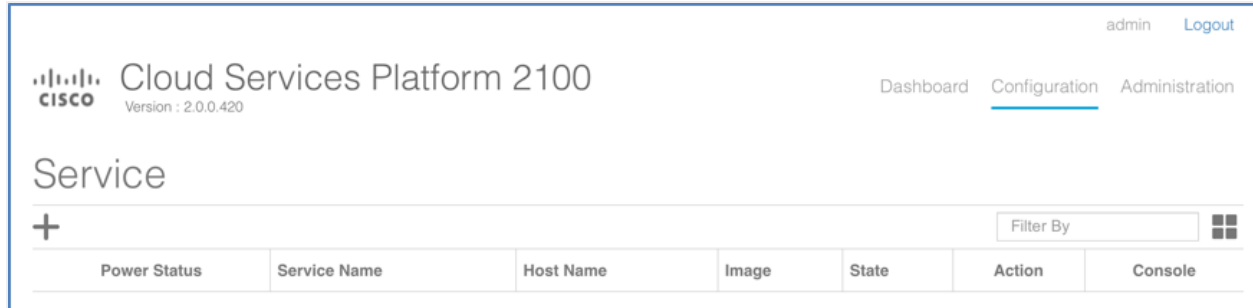
Note: In above example 8 VFs (virtual functions) are configured on the pNIC. The user should configure this number

5. Repeat the above steps to configure `enps0f1` for SR-IOV if required.

## Deploy Avi SE 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: Hardware](#) for recommendations on a minimum production SE configuration.

Create Service
  Create Service using Template

Name: \*

Target Host Name: \*

VNF Management IP:

Image Name: \*

Day Zero Config

	Source File Name	Destination File Name	Action
1	avi_meta_data_se-1.yml	avi_meta_data_se-1.yml	

Number of Cores:   
 Available Cores: 16

Do you want to resize disk?

Disk Space (GB):   
 Available Disk Space (GB): 2563 | Minimum Disk Size (GB) : 10

RAM (MB):   
 Available RAM (MB): 196302

NFS Storage

Disk Type:  IDE  VIRTIO

3. Enter ?Avi SE1? in the Service Name field and press enter.
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.

Name: *	<input type="text" value="vnic0"/>
VLAN Type:	<input checked="" type="radio"/> Access <input type="radio"/> Trunk <input type="radio"/> Passthrough
VLAN:	<input type="text" value="range 1-1000,1025-4094"/>
VLAN Tagged:	<input type="radio"/> True <input checked="" type="radio"/> False
Native VLAN:	<input type="text" value="range 0-4095"/>
Model:	<input type="radio"/> Virtio <input checked="" type="radio"/> e1000
Network Type:	<input type="radio"/> Internal <input checked="" type="radio"/> External
Network Name: *	<input type="text" value="enp1s0f0"/> ▼

10. Click on + to add a vNIC and connect it to enp7s0f0 in SR-IOV mode.

Name: *	<input type="text" value="vnic1"/>
VLAN Type:	<input type="radio"/> Access <input type="radio"/> Trunk <input checked="" type="radio"/> Passthrough
VLAN:	<input type="text" value="200"/>
Passthrough Mode: *	<input checked="" type="radio"/> SR-IOV <input type="radio"/> PCIE <input type="radio"/> MACVTAP
Network Name: *	<input type="text" value="enp7s0f0"/> ▼

11. (optional) Specify a password for console login using VNC.
12. Click Deploy.
13. Verify the SE is able to connect to the Avi Controller by navigating to Infrastructure > Dashboard on Avi Controller UI (this may take a few minutes).

**Related Articles:**

- [Upgrading Avi Vantage Software](#)
- [Upgrades in an Avi GSLB Environment](#)

**Revision History**

Applicable	Summary
Edit Date	As Of Release
10Apr2018	All releases
	As of 2Apr2018, Avi recommends CSP version 2.2.5