Appendix E: Sample Payloads for Creating Cisco SD-WAN Control Plane on Openstack

This appendix contains the sample JSON configuration files for adding VIM and control plane payloads in the provider and tenant network. The authentication certificate is a part of the control plane deployment activity in vManage and sample JSON files are given for both enterprise and symantec certificate based on the network.

This appendix covers these section:

Adding VIM Payload in Provider Network

This is the sample JSON file for adding VIM payload in the provider network.

Note:

- Ensure that the names used in "dtlsNetName"(VPN0) and "mgmtNetName"(VPN512) are from the provider network, that is already created in the OpenStack cloud.
- The VPN512 network should be reachable from MSX for the deployment of the control plane.
- The VPN0 network should be reachable from vEdge for the deployment of vEdge on the deployed control plane.

Provider Network.json

```
#Provider
{
"tenantID": "TestTenant",
"vim":
{
"type": "openstack",
"openstack":
{
```

```
"username": "username",
"password": "password",
"authURL": "URL",
"projectName": "admin",
"projectID": Project ID,
"domainName": "Default",
"region": "RegionOne",
"extNetName": "external",
"networkType": "provider",
"network":
{
"dtlsNetName": "Vnf-outside",
"mgmtNetName": "external"
}
}
}
}
```

Adding VIM Payload in Tenant Network

This is the sample JSON file for adding VIM payload in tenant network.

Note:

- Ensure that the names used in "dtlsNetName"(VPN0) and "mgmtNetName"(VPN512) are not repeated on the openstack cloud.
- The subnet used in "dtlsSubnet"(VPN0) and "mgmtSubnet"(VPN512) for the 'create control plane' payload should not be repeated on the openstack cloud. You can provide two subnets in this payload.
- The VPN512 network has floating IPs that should be reachable from MSX for the deployment of the control plane.
- The VPN0 network has floating IPs that should be reachable from vEdge for the deployment of vEdge on the deployed control plane.

Tenant Network.json

```
{
"tenantID": "TestTenant",
"vim": {
"type": "openstack",
"openstack": {
"username": "username",
"password": "password",
"authURL": "url",
"projectName": "admin",
"projectID": "Project ID",
"domainName": "Default",
"region": "RegionOne",
"extNetName": "external",
"networkType": "tenant",
"network": {
"dtlsNetName": "Test-Dtls",
"mgmtNetName": "Test-Mgmt"
}
}
}
}
```

Adding Control Plane Payload with Enterprise Certificate in Provider Network

This is the sample JSON file for adding control plane payload with enterprise certificate in provider network.

Provider Network with EnterpriseCA.json

```
{
"tenantID": "TestTenant",
"controlPlane": {
"vimID": "vimID",
"vmanage": {
"flavor": "viptela-vmanage-vm",
"image": "viptela-vmanage-19.1.0-genericx86-64.qcow2",
"hostname": "TestManage01",
"systemID": "system ID",
"day0": "vmanage-fip.j2",
"vpn0": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"},
"vpn512": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
}
},
"vbond": {
"flavor": "viptela-vbond-vm",
"image": "viptela-edge-19.1.0-genericx86-64.qcow2",
"hostname": "TestBond01",
"systemID": "system ID",
"day0": "vbond-fip-3.j2",
"vpn0": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
},
"vpn512": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
}
},
"vsmart": {
"flavor": "viptela-vsmart-vm",
"image": "viptela-smart-19.1.0-genericx86-64.qcow2",
"hostname": "TestSmart01",
"systemID": "system ID",
"day0": "vsmart-fip.j2",
"vpn0": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
},
"vpn512": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
}
},
"credentials": {
"username": "username",
"password": "password"
},
"org": "vmsoverlay1",
"siteID": "site ID",
"ntpServer": "ntp.esl.cisco.com",
"dnsServer": "dns serverIP address",
"createCA": true
}
}
```

Adding Control Plane Payload with Symantec Certificate in Provider Network

This is the sample JSON file for adding control plane payload with symantec certificate in provider network.

Provider Network with Symantec.json

```
{
"tenantID": "TestTenant",
"controlPlane": {
"vimID": "vim ID",
"vmanage": {
"flavor": "viptela-vmanage-vm",
"image": "viptela-vmanage-19.1.0-genericx86-64.qcow2",
"hostname": "TestManage01",
"systemID": "system ID",
"day0": "vmanage-fip-noCA.j2",
"vpn0": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
},
"vpn512": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
}
},
"vbond": {
"flavor": "viptela-vbond-vm",
"image": "viptela-edge-19.1.0-genericx86-64.qcow2",
"hostname": "TestBond01",
"systemID": "system ID",
"day0": "vbond-fip-3-noCA.j2",
"vpn0": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
},
"vpn512": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
}
},
"vsmart": {
"flavor": "viptela-vsmart-vm",
"image": "viptela-smart-19.1.0-genericx86-64.qcow2",
"hostname": "TestSmart01",
"systemID": "system ID",
"day0": "vsmart-fip-noCA.j2",
"vpn0": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
},
"vpn512": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
}
},
"credentials": {
"username": "username",
"password": "password"
},
"org": "vmsoverlay1",
"siteID": "site ID",
"ntpServer": "ntp.esl.cisco.com",
"dnsServer": "IP address",
"createCA": false
}
}
```

Adding Control Plane Payload with Enterprise Certificate in Tenant Network

This is the sample JSON file for adding control plane payload with enterprise certificate in tenant network.

Tenant Network with EnterpriseCA.json

```
{
"tenantID": "TestTenant",
"controlPlane": {
"vimID": "vim ID",
"vmanage": {
"flavor": "viptela-vmanage-vm",
"image": "viptela-vmanage-19.1.0-genericx86-64.qcow2",
"hostname": "TestManage10",
"systemID": "system ID",
"day0": "vmanage-fip.j2",
"vpn0": {
"subnetMaskBits": "24"
},
"vpn512": {
"subnetMaskBits": "24"
}
},
"vbond": {
"flavor": "viptela-vbond-vm",
"image": "viptela-edge-19.1.0-genericx86-64.qcow2",
"hostname": "TestBond10",
"systemID": "50.0.1.11",
"day0": "vbond-fip-3.j2",
"vpn0": {
"subnetMaskBits": "24"
},
"vpn512": {
"subnetMaskBits": "24"
}
},
"vsmart": {
"flavor": "viptela-vsmart-vm",
"image": "viptela-smart-19.1.0-genericx86-64.qcow2",
"hostname": "TestSmart10",
"systemID": "system ID",
"day0": "vsmart-fip.j2",
"vpn0": {
"subnetMaskBits": "24"
},
"vpn512": {
"subnetMaskBits": "24"
}
},
"credentials": {
"username": "username",
"password": "password"
},
"org": "vmsoverlay1",
"siteID": "site ID",
"ntpServer": "ntp.esl.cisco.com",
"dnsServer": "IP address",
"createCA": true,
"dtlsSubnet": "IP address",
"mgmtSubnet": "IP address"
}
}
```

Adding Control Plane Payload with Symantec Certificate on Tenant Network

This is the sample JSON file for adding control plane payload with symantec certificate on tenant network.

Tenant Network with Symantec.json

```
{
"tenantID": "TestTenant",
"controlPlane": {
"vimID": "vim ID",
"vmanage": {
"flavor": "viptela-vmanage-vm",
"image": "viptela-vmanage-19.1.0-genericx86-64.qcow2",
"hostname": "TestManage10",
"systemID": "system ID",
"day0": "vmanage-fip-noCA.j2",
"vpn0": {
"subnetMaskBits": "24"
},
"vpn512": {
```

```
"subnetMaskBits": "24"
}
},
"vbond": {
"flavor": "viptela-vbond-vm",
"image": "viptela-edge-19.1.0-genericx86-64.qcow2",
"hostname": "TestBond10",
"systemID": "system ID",
"day0": "vbond-fip-3-noCA.j2",
"vpn0": {
"subnetMaskBits": "24"
},
"vpn512": {
"subnetMaskBits": "24"
}
},
"vsmart": {
"flavor": "viptela-vsmart-vm",
"image": "viptela-smart-19.1.0-genericx86-64.qcow2",
"hostname": "TestSmart10",
"systemID": "system ID",
"day0": "vsmart-fip-noCA.j2",
"vpn0": {
"subnetMaskBits": "24"
},
"vpn512": {
"subnetMaskBits": "24"
}
},
"credentials": {
"username": "username",
"password": "password"
},
"org": "vmsoverlay1",
"siteID": "site ID",
"ntpServer": "ntp.esl.cisco.com",
"dnsServer": "IP address",
"createCA": false,
"dtlsSubnet": "IP address",
"mgmtSubnet": "IP address"
}
}
```