Installing Cisco Elastic Services Controller on Cisco Cloud Services Platform 2100

This chapter describes how to install Cisco Elastic Services Controller on CSP 2100 and includes the following sections:

Prerequisites

Following are the prerequisites that you require before you start installing the ESC instance in CSP 2100.

- Virtual CPUs 4 (minimum)
- Memory 8 GB
- Disk size 30 GB

Installing the Elastic Services Controller Instance in CSP 2100

Once you have completed the tasks specified in the prerequisites section, you can use the following procedure to deploy and launch ESC instance in CSP 2100. Following are the three deployment alternatives available for CSP 2100.

- ESC with Single and Dual Interfaces
- ESC HA Active/Standby Installation

For list of variables used in the CSP 2100 sample files, see List of Variables Used in CSP 2100 Sample Files, on page 10.

ESC with Single and Dual Interface

To install ESC in CSP, you must create the user-data in the following format as the day0 configuration file:

A sample for single interface describing the day zero file as config drive and user data is as follows:

```
#cloud-config
users:
 - name: admin          # The user's login name
   gecos: admin         # The user name's real name
   groups: esc-user     # add admin to group esc-user
   passwd: $6$saltsalt$9PDBehueUG4XTLEj6BFZA5MDGh/XeQ6QPbf9HYLU3RifHj1
                        # The hash -- not the password itself -- of the password you want
                       #           to use for this user. You can generate a safe hash via:

                        #               mkpasswd --method=SHA-512 --rounds=4096
   lock-passwd: false   # Defaults to true. Lock the password to disable password login
                        # Set to false if you want to password login
   homedir: /home/admin # Optional. Set to the local path you want to use. Defaults to
/home/<username>
   sudo: ALL=(ALL) ALL  # Defaults to none. Set to the sudo string you want to use

ssh_pwauth: True        # Defaults to False. Set to True if you want to enable password
authentication for sshd.
write_files:
# ESC Configuration
- path: /opt/cisco/esc/esc-config/esc-config.yaml
  content: |
    resources:
      confd:
        init_aaa_users:
        - key: c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUF
          passwd: $6$rounds=4096$adWFd7LUn2PEUPWtWPl5tCD7pO9bae672T1
        option: start-phase0
      escmanager:
        open_ports:
        - '8080'
        - '8443'
        url:
        - http://0.0.0.0:8080/ESCManager
        - https://0.0.0.0:8443/ESCManager
      esc_service:
        type: group
# Params
- path: /opt/cisco/esc/esc-config/esc_params.conf
  content: |
    default.active_vim=CSP
    default.enable_cascade_deletion=true
# Networking
- path: /etc/sysconfig/network-scripts/ifcfg-eth0
  content: |
    DEVICE="eth0"
    BOOTPROTO="none"
    ONBOOT="yes"
    TYPE="Ethernet"
    USERCTL="yes"
    IPADDR="VAR_NETWORK0_IPADDR"
    NETMASK="VAR_NETWORK0_NETMASK"
    GATEWAY="VAR_NETWORK0_GATEWAY"
    DEFROUTE="yes"
    NM_CONTROLLED="no"
    IPV6INIT="no"
    IPV4_FAILURE_FATAL="yes"
bootcmd:
- [ cloud-init-per, once, disable_ipv6_eth0, sh, -c, "echo net.ipv6.conf.eth0.disable_ipv6
 = 1 >> /etc/sysctl.conf"]
- [ cloud-init-per, once, update_host_name, sh, -c, "echo VAR_LOCAL_HOSTNAME >> /etc/hostname
 && hostnamectl set-hostname VAR_LOCAL_HOSTNAME"]
- [ cloud-init-per, once, update_hosts, sh, -c, "echo 127.0.0.1 VAR_LOCAL_HOSTNAME >>
/etc/hosts"]
```

```
- [ cloud-init-per, once, add_name_server, sh, -c, "echo nameserver VAR_NAMESERVER_IP >>
/etc/resolv.conf"]
- [ cloud-init-per, once, add_ntp_server, sh, -c, "echo server VAR_NTP_SERVER iburst >>
/etc/ntp.conf"]
- [ cloud-init-per, once, enable_ecdsa-sha2-nistp521, sh, -c, "/usr/bin/ssh-keygen -f
/etc/ssh/ssh_host_ecdsa_521_key -t ecdsa -b 521 -N ''"]
- [ cloud-init-per, once, enable_ecdsa-sha2-nistp384, sh, -c, "/usr/bin/ssh-keygen -f
/etc/ssh/ssh_host_ecdsa_384_key -t ecdsa -b 384 -N ''"]
- [ cloud-init-per, once, enable_ssh_rsa, sh, -c, "sed -i '/ssh_host_rsa_key/s/^#//g'
/etc/ssh/sshd_config"]
runcmd:
- [ cloud-init-per, once, apply_network_config, sh, -c, "systemctl restart network"]
- [ cloud-init-per, once, stop_chronyd, sh, -c, "systemctl stop chronyd;systemctl disable
chronyd"]
- [ cloud-init-per, once, start_ntp, sh, -c, "systemctl enable ntpd;systemctl start ntpd"]
- [ cloud-init-per, once, set_timezone, sh, -c, "timedatectl set-timezone VAR_TIMEZONE"]
- [ cloud-init-per, once, confd_keygen_root, sh, -c, "/usr/bin/escadm confd keygen --user
root"]
- [ cloud-init-per, once, confd_keygen_admin, sh, -c, "/usr/bin/escadm confd keygen --user
 admin"]
- [ cloud-init-per, once, esc_service_start, sh, -c, "chkconfig esc_service on && service
esc_service start"] # You must include this line
```

A sample for dual interfaces describing the day zero file as config drive and user data is as follows:

You can configure an ethernet-based physical network device with a static IPv4 in ESC .

```
#cloud-config
users:
 - name: admin          # The user's login name
   gecos: admin         # The user name's real name
   groups: esc-user     # add admin to group esc-user
   passwd: $6$saltsalt$9PDBehueUG4XTLEj6BFZA5MDGh/XeQ6QPbf9HYLU3RifHj1
                        # The hash -- not the password itself -- of the password you want
                       #           to use for this user. You can generate a safe hash via:

                        #               mkpasswd --method=SHA-512 --rounds=4096
   lock-passwd: false   # Defaults to true. Lock the password to disable password login
                        # Set to false if you want to password login
   homedir: /home/admin # Optional. Set to the local path you want to use. Defaults to
/home/<username>
   sudo: ALL=(ALL) ALL  # Defaults to none. Set to the sudo string you want to use

ssh_pwauth: True        # Defaults to False. Set to True if you want to enable password
authentication for sshd.
write_files:
# ESC Configuration
- path: /opt/cisco/esc/esc-config/esc-config.yaml
  content: |
    resources:
      confd:
        init_aaa_users:
        - key: c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUF
          passwd: $6$rounds=4096$adWFd7LUn2PEUPWtWPl5tCD7pO9bae672T1
        option: start-phase0
      escmanager:
        open_ports:
        - '8080'
        - '8443'
        url:
        - http://0.0.0.0:8080/ESCManager
        - https://0.0.0.0:8443/ESCManager
      esc_service:
        type: group
# Params
```

```
- path: /opt/cisco/esc/esc-config/esc_params.conf
  content: |
    default.active_vim=CSP
    default.enable_cascade_deletion=true
# Networking
- path: /etc/sysconfig/network-scripts/ifcfg-eth0
  content: |
    DEVICE="eth0"
    BOOTPROTO="none"
    ONBOOT="yes"
    TYPE="Ethernet"
    USERCTL="yes"
    IPADDR="VAR_NETWORK0_IPADDR"
    NETMASK="VAR_NETWORK0_NETMASK"
    GATEWAY="VAR_NETWORK0_GATEWAY"
    DEFROUTE="yes"
    NM_CONTROLLED="no"
    IPV6INIT="no"
    IPV4_FAILURE_FATAL="yes"
- path: /etc/sysconfig/network-scripts/ifcfg-eth1
  content: |
    DEVICE="eth1"
    BOOTPROTO="none"
    ONBOOT="yes"
    TYPE="Ethernet"
    USERCTL="yes"
    IPADDR="VAR_NETWORK1_IPADDR"
    NETMASK="VAR_NETWORK1_NETMASK"
    GATEWAY="VAR_NETWORK1_GATEWAY"
    DEFROUTE="no"
    NM_CONTROLLED="no"
    IPV6INIT="no"
    IPV4_FAILURE_FATAL="yes"
bootcmd:
- [ cloud-init-per, once, disable_ipv6_eth0, sh, -c, "echo net.ipv6.conf.eth0.disable_ipv6
 = 1 >> /etc/sysctl.conf"]
- [ cloud-init-per, once, update_host_name, sh, -c, "echo VAR_LOCAL_HOSTNAME >> /etc/hostname
 && hostnamectl set-hostname VAR_LOCAL_HOSTNAME"]
- [ cloud-init-per, once, update_hosts, sh, -c, "echo 127.0.0.1 VAR_LOCAL_HOSTNAME >>
/etc/hosts"]
- [ cloud-init-per, once, add_name_server, sh, -c, "echo nameserver VAR_NAMESERVER_IP >>
/etc/resolv.conf"]
- [ cloud-init-per, once, add_ntp_server, sh, -c, "echo server VAR_NTP_SERVER iburst >>
/etc/ntp.conf"]
- [ cloud-init-per, once, enable_ecdsa-sha2-nistp521, sh, -c, "/usr/bin/ssh-keygen -f
/etc/ssh/ssh_host_ecdsa_521_key -t ecdsa -b 521 -N ''"]
- [ cloud-init-per, once, enable_ecdsa-sha2-nistp384, sh, -c, "/usr/bin/ssh-keygen -f
/etc/ssh/ssh_host_ecdsa_384_key -t ecdsa -b 384 -N ''"]
- [ cloud-init-per, once, enable_ssh_rsa, sh, -c, "sed -i '/ssh_host_rsa_key/s/^#//g'
/etc/ssh/sshd_config"]
runcmd:
- [ cloud-init-per, once, apply_network_config, sh, -c, "systemctl restart network"]
- [ cloud-init-per, once, stop_chronyd, sh, -c, "systemctl stop chronyd;systemctl disable
chronyd"]
- [ cloud-init-per, once, start_ntp, sh, -c, "systemctl enable ntpd;systemctl start ntpd"]
- [ cloud-init-per, once, set_timezone, sh, -c, "timedatectl set-timezone VAR_TIMEZONE"]
- [ cloud-init-per, once, confd_keygen_root, sh, -c, "/usr/bin/escadm confd keygen --user
root"]
- [ cloud-init-per, once, confd_keygen_admin, sh, -c, "/usr/bin/escadm confd keygen --user
 admin"]
- [ cloud-init-per, once, esc_service_start, sh, -c, "chkconfig esc_service on && service
esc_service start"] # You must include this line
```

Creating ESC passwords to use in Day0 Files

When using the Cloud-Init day0 file to deploy an ESC instance, the passwords must be passed in as a hash, and not a plain text.

To create a hashed password, use the mkpasswd tool. The following example shows how to use the mkpasswd tool to create a hashed password.

```
~$ mkpasswd --method=SHA-512 --rounds=4096
Password:
$6$rounds=4096$Yo11pRsFO$iT5SGMJ6z8WEnmj8TKMdInblgWeb/UChmrsQs3aspx8j.yUuuhxKk2XScOkerWWxpqD5F0sLfC5kzT5t2xGkL1
```

Procedure

Step 1 **Upload user-data file to CSP**

To deploy ESC, the user-data file must be first uploaded to the CSP node.

Note The path to upload images and day0 files is: /osp/repository

```
scp user-data-esc admin@<CSP_IP_ADDRESS>:/osp/repository
```

Step 2 **Deploying ESC VM**

You must edit configuration to be sent to the CSP node hosting the ESC VM.

Following is the deployment datamodel for single interface. For dual interface, you have two interfaces.`<name>ESC-SA-2-IF</name>`

```
<?xml version="1.0"?>
<services xmlns="http://www.cisco.com/ns/test/service">
  <service>
    <name>VAR_SERVICE_NAME</name>
    <memory>8192</memory> <!-- minimum 8G -->
    <numcpu>4</numcpu> <!-- minimum 4 -->
    <disk_size>30.0</disk_size> <!-- minimum 30G -->
    <disk-resize>true</disk-resize>
    <iso_name>ESC-5_0_0_xxx</iso_name> <!-- the name of the ESC image already on the CSP
-->
    <power>on</power>
    <ip>172.20.117.40</ip>
    <!-- add the ip for display in the CSP web/console interfaces -->
    <vnc_password>password1</vnc_password>
    <!-- to secure the VNC console session -->
    <vnics>
      <!-- This interface aligns with eth0 in the user-data file -->
      <vnic>
        <nic>0</nic>
        <vlan>1</vlan>
        <tagged>false</tagged>
        <type>access</type>
        <passthrough_mode>none</passthrough_mode>
        <model>virtio</model>
        <network_name>VAR_NETWORK0_NAME</network_name>
      </vnic>
      <!-- This interface aligns with eth1 in the user-data file -->
      <!-- If not using 2 interfaces, this vnic block can be removed -->
      <vnic>
        <nic>1</nic>
        <vlan>1</vlan>
        <tagged>false</tagged>
        <type>access</type>
        <passthrough_mode>none</passthrough_mode>
        <model>virtio</model>
```

```
        <network_name>VAR_NETWORK1_NAME</network_name>
      </vnic>
    </vnics>
    <disk_type>ide</disk_type>
    <day0_filename>user-data-esc</day0_filename> <!-- this name MUST match the name of the
 file that was copied to the CSP -->
    <day0-dest-filename>user-data</day0-dest-filename>  <!-- mandatory value -->
    <day0-volume-id>cidata</day0-volume-id>  <!-- mandatory value -->
  </service>
</services>
```

Step 3 **Sending Configuration**

Use a netconf-console (shipped with ConfD) to deploy ESC on a CSP node.

```
$ netconf-console --port=2022 --host=<CSP_IP_ADDRESS> --user=CSP_ADMIN_USERNAME
--password=CSP_ADMIN_PASSWORD --edit-config=deployESCHA1.xml
```

If HA, repeat the command with the configuration for the second ESC.

Step 4 **Configuring the VIM Connector**

After ESC has booted, configure the VIM Connectors.

When installing ESC in CSP, no VIM connectors are added by default. To manage VNFs, you must create the VIM connector.

Step 5 **Adding the VIM Connectors**

For more information on configuring VIM connectors after installation, and managing VIM connectors, see Managing VIM Connectors in the *Cisco Elastic Services Controller User Guide*.

ESC HA Active/Standby Installation

To install ESC in CSP, you must create the user-data in the following format as the day0 configuration file. For HA, you must define one file for each VM.

For creating ESC passwords to use in Day0 Files, see the **Creating ESC passwords to use in Day0 Files** section.

A sample for ESC HA Active/Standby installation on node 1 describing the day zero file as config drive and user data is as follows:

```
user-data sample - HA Node 1
#cloud-config
users:
 - name: admin          # The user's login name
   gecos: admin         # The user name's real name
   groups: esc-user     # add admin to group esc-user
   passwd: $6$saltsalt$9PDBehueUG4XTLEj6BFZA5MDGh/XeQ6QPbf9HYLU3RifHj1
                        # The hash -- not the password itself -- of the password you want
                       #           to use for this user. You can generate a safe hash via:

                        #               mkpasswd --method=SHA-512 --rounds=4096
   lock-passwd: false   # Defaults to true. Lock the password to disable password login
                        # Set to false if you want to password login
   homedir: /home/admin # Optional. Set to the local path you want to use. Defaults to
/home/<username>
   sudo: ALL=(ALL) ALL  # Defaults to none. Set to the sudo string you want to use
```

```
ssh_pwauth: True        # Defaults to False. Set to True if you want to enable password
authentication for sshd.

write_files:
# ESC Configuration
- path: /opt/cisco/esc/esc-config/esc-cfg.yaml
  content: |
    ha:
      vri: VAR_NETWORK0_KADVRI
      mode: drbd
      vip: VAR_NETWORK0_KADVIP
      vif: eth0
      nodes:
      - ipaddr: VAR_NETWORK0_IPADDR
      - ipaddr: VAR_NETWORK0_IPADDR2
    confd:
      init_aaa_users:
      - name: admin
        passwd: $6$rounds=4096$adWFd7LUn2PEUPWtWPl5tCD7pO9bae672T1
      escmanager:
        open_ports:
        - '8080'
        - '8443'
        url:
        - http://0.0.0.0:8080/ESCManager
        - https://0.0.0.0:8443/ESCManager
    esc_service: {}
# Params
- path: /opt/cisco/esc/esc-config/esc_params.conf
  content: |
    default.active_vim=CSP
    default.enable_cascade_deletion=true
# Networking
- path: /etc/sysconfig/network-scripts/ifcfg-eth0
  content: |
    DEVICE="eth0"
    BOOTPROTO="none"
    ONBOOT="yes"
    TYPE="Ethernet"
    USERCTL="yes"
    IPADDR="VAR_NETWORK0_IPADDR"
    NETMASK="VAR_NETWORK0_NETMASK"
    GATEWAY="VAR_NETWORK0_GATEWAY"
    DEFROUTE="yes"
    IPV6INIT="no"
    IPV4_FAILURE_FATAL="yes"
bootcmd:
- [ cloud-init-per, once, disable_ipv6_eth0, sh, -c, "echo net.ipv6.conf.eth0.disable_ipv6
 = 1 >> /etc/sysctl.conf"]
- [ cloud-init-per, once, update_host_name, sh, -c, "echo VAR_LOCAL_HOSTNAME >> /etc/hostname
 && hostnamectl set-hostname VAR_LOCAL_HOSTNAME"]
- [ cloud-init-per, once, update_hosts, sh, -c, "echo 127.0.0.1 VAR_LOCAL_HOSTNAME >>
/etc/hosts"]
- [ cloud-init-per, once, add_name_server, sh, -c, "echo nameserver VAR_NAMESERVER_IP >>
/etc/resolv.conf"]
- [ cloud-init-per, once, add_ntp_server, sh, -c, "echo server VAR_NTP_SERVER iburst >>
/etc/ntp.conf"]
- [ cloud-init-per, once, enable_ecdsa-sha2-nistp521, sh, -c, "/usr/bin/ssh-keygen -f
/etc/ssh/ssh_host_ecdsa_521_key -t ecdsa -b 521 -N ''"]
- [ cloud-init-per, once, enable_ecdsa-sha2-nistp384, sh, -c, "/usr/bin/ssh-keygen -f
/etc/ssh/ssh_host_ecdsa_384_key -t ecdsa -b 384 -N ''"]
- [ cloud-init-per, once, enable_ssh_rsa, sh, -c, "sed -i '/ssh_host_rsa_key/s/^#//g'
/etc/ssh/sshd_config"]
runcmd:
```

```
- [ cloud-init-per, once, apply_network_config, sh, -c, "systemctl restart network"]
- [ cloud-init-per, once, stop_chronyd, sh, -c, "systemctl stop chronyd;systemctl disable
chronyd"]
- [ cloud-init-per, once, start_ntp, sh, -c, "systemctl enable ntpd;systemctl start ntpd"]
- [ cloud-init-per, once, set_timezone, sh, -c, "timedatectl set-timezone VAR_TIMEZONE"]
- [ cloud-init-per, once, confd_keygen_root, sh, -c, "/usr/bin/escadm confd keygen --user
root"]
- [ cloud-init-per, once, confd_keygen_admin, sh, -c, "/usr/bin/escadm confd keygen --user
 admin"]
- [ cloud-init-per, once, esc_service_start, sh, -c, "chkconfig esc_service on && service
esc_service start"] # You must include this line
```

Procedure

Step 1 **Uploading user-data file to CSP**

To deploy ESC, the user-data file must be first uploaded to the CSP node.

Note The path to upload images and day0 files is: /osp/repository

```
scp user-data-esc-ha-1 CSP_ADMIN_USERNAME@<CSP_IP_ADDRESS>:/osp/repository

scp user-data-esc-ha-2 CSP_ADMIN_USERNAME@<CSP_IP_ADDRESS>:/osp/repository
```

Step 2 **Deploying ESC VM**

You must edit configuration to be sent to the CSP node hosting the ESC VM.

Following is the deployment datamodel for ESC HA Active/Standby on node 1 :

```
deployESC-HA-1.xml
<?xml version="1.0"?>
<services xmlns="http://www.cisco.com/ns/test/service">
  <service>
    <name>VAR_SERVICE_NAME</name>
    <memory>8192</memory> <!-- minimum 8G -->
    <numcpu>4</numcpu> <!-- minimum 4 -->
    <disk_size>30.0</disk_size> <!-- minimum 30G -->
    <disk-resize>true</disk-resize>
    <iso_name>ESC-5_0_0_xxx</iso_name> <!-- the name of the ESC image already on the CSP
-->
    <power>on</power>
    <ip>172.20.117.40</ip>
    <!-- add the ip for display in the CSP web/console interfaces -->
    <vnc_password>password1</vnc_password>
    <!-- to secure the VNC console session -->
    <vnics>
      <!-- This interface aligns with eth0 in the user-data file -->
      <vnic>
        <nic>0</nic>
        <vlan>1</vlan>
        <tagged>false</tagged>
        <type>access</type>
        <passthrough_mode>none</passthrough_mode>
        <model>virtio</model>
        <network_name>VAR_NETWORK0_NAME</network_name>
      </vnic>
      <!-- This interface aligns with eth1 in the user-data file -->
      <!-- If not using 2 interfaces, this vnic block can be removed -->
      <vnic>
        <nic>1</nic>
        <vlan>1</vlan>
```

```
        <tagged>false</tagged>
        <type>access</type>
        <passthrough_mode>none</passthrough_mode>
        <model>virtio</model>
        <network_name>VAR_NETWORK1_NAME</network_name>
      </vnic>
    </vnics>
    <disk_type>ide</disk_type>
    <day0_filename>user-data-esc</day0_filename> <!-- this name MUST match the name of the
 file that was copied to the CSP -->
    <day0-dest-filename>user-data</day0-dest-filename>  <!-- mandatory value -->
    <day0-volume-id>cidata</day0-volume-id>  <!-- mandatory value -->
  </service>
</services>
```

Following is the deployment datamodel for ESC in HA Active/Standby on node 2 :

```
deployESC-HA-2.xml
deployESC-HA-1.xml
<?xml version="1.0"?>
<services xmlns="http://www.cisco.com/ns/test/service">
  <service>
    <name>VAR_SERVICE_NAME</name>
    <memory>8192</memory> <!-- minimum 8G -->
    <numcpu>4</numcpu> <!-- minimum 4 -->
    <disk_size>30.0</disk_size> <!-- minimum 30G -->
    <disk-resize>true</disk-resize>
    <iso_name>ESC-5_0_0_xxx</iso_name> <!-- the name of the ESC image already on the CSP
-->
    <power>on</power>
    <ip>172.20.117.40</ip>
    <!-- add the ip for display in the CSP web/console interfaces -->
    <vnc_password>password1</vnc_password>
    <!-- to secure the VNC console session -->
    <vnics>
      <!-- This interface aligns with eth0 in the user-data file -->
      <vnic>
        <nic>0</nic>
        <vlan>1</vlan>
        <tagged>false</tagged>
        <type>access</type>
        <passthrough_mode>none</passthrough_mode>
        <model>virtio</model>
        <network_name>VAR_NETWORK0_NAME</network_name>
      </vnic>
      <!-- This interface aligns with eth1 in the user-data file -->
      <!-- If not using 2 interfaces, this vnic block can be removed -->
      <vnic>
        <nic>1</nic>
        <vlan>1</vlan>
        <tagged>false</tagged>
        <type>access</type>
        <passthrough_mode>none</passthrough_mode>
        <model>virtio</model>
        <network_name>VAR_NETWORK1_NAME</network_name>
      </vnic>
    </vnics>
    <disk_type>ide</disk_type>
    <day0_filename>user-data-esc</day0_filename> <!-- this name MUST match the name of the
 file that was copied to the CSP -->
    <day0-dest-filename>user-data</day0-dest-filename>  <!-- mandatory value -->
    <day0-volume-id>cidata</day0-volume-id>  <!-- mandatory value -->
  </service>
</services>
```

Step 3 **Sending Configuration**

Use a netconf-console (shipped with ConfD) to deploy ESC on a CSP node.

```
$ netconf-console --port=2022 --host=<CSP_IP_ADDRESS> --user=<CSP_ADMIN_USERNAME>
--password=<CSP_ADMIN_PASSWORD> --edit-config=deployESC-HA-1.xml

$ netconf-console --port=2022 --host=<CSP_IP_ADDRESS> --user=<CSP_ADMIN_USERNAME>
--password=<CSP_ADMIN_PASSWORD> --edit-config=deployESC-HA-2.xml
```

Step 4 **Configuring the VIM Connector**

After ESC has booted, configure the VIM Connectors.

When installing ESC in CSP, no VIM connectors are added by default. To manage VNFs, you must create the VIM connector.

Step 5 **Adding the VIM Connectors**

For more information on configuring VIM connectors after installation, and managing VIM connectors, see Managing VIM Connectors in the *Cisco Elastic Services Controller User Guide*.

List of Variables Used in CSP 2100 Sample Files

To create the user-data file, to configure the ESC you must have values ready for the following list of variables used in the sample files:

Table 1: List of Variables

Variable Name	Purpose
VAR_TIMEZONE	The timezone for the ESC clock to use
VAR_SERVICE_NAME	The name of the ESC service on the CSP
VAR_NTP_SERVER	The IP address of an NTP server
VAR_NETWORK1_NETMASK	The netmask for the eth1 interface (Dual Interface ESC)
VAR_NETWORK1_NAME	The name of the network on the CSP where ESC's eth1 interface exists (Dual Interface ESC)
VAR_NETWORK1_IPADDR	The IP address for the eth1 interface (Dual Interface ESC)
VAR_NETWORK1_GATEWAY	The gateway for the eth1 interface (Dual Interface ESC)
VAR_NETWORK0_NETMASK	The netmask for the eth0 interface
VAR_NETWORK0_NAME	The name of the network on the CSP where ESC's eth0 interface exists

Variable Name	Purpose
VAR_NETWORK0_KADVRI	The VRRP ID used for HA. Must be unique in the subnet for the HA pair and the same value used on both ESCs Range is from 1 to 254
VAR_NETWORK0_KADVIP	The VIP for the HA pair that connects to the current Active ESC
VAR_NETWORK0_IPADDR2	The IP address for the other ESC's eth0 interface
VAR_NETWORK0_IPADDR	The IP address for ESC (eth0 interface)
VAR_NETWORK0_GATEWAY	The gateway for the eth0 interface
VAR_NAMESERVER_IP	The IP address of a DNS server
VAR_LOCAL_HOSTNAME	The hostname for ESC
CSP_IP_ADDRESS	IP address of the CSP 2100 to be used