



Cisco Elastic Services Controller の Cisco Cloud Services Platform 2100 へのインストール

この章では、CSP 2100 に Cisco Elastic Services Controller をインストールする手順について説明します。この章は次のセクションで構成されています。

- [前提条件 \(1 ページ\)](#)
- [Elastic Services Controller インスタンスの CSP 2100 へのインストール \(1 ページ\)](#)
- [CSP 2100 のサンプルファイルで使用される変数リスト \(11 ページ\)](#)

前提条件

CSP 2100 で ESC インスタンスのインストールを開始するための前提条件は、次のとおりです。

- 仮想 CPU : 4 基 (最小)
- メモリ : 8 GB
- ディスクサイズ : 30 GB

Elastic Services Controller インスタンスの CSP 2100 へのインストール

前提条件のセクションに記載されたタスクを完了すると、次の手順を使用して、CSP 2100 で ESC インスタンスを展開および起動できます。次に、CSP 2100 で使用可能な別の展開方法を 3 つ示します。

- シングルインターフェイスとデュアルインターフェイスを使用した ESC
- ESC HA アクティブ/スタンバイのインストール

CSP2100 のサンプルファイルで使用される変数のリストについては、[CSP2100 のサンプルファイルで使用される変数リスト \(11 ページ\)](#) を参照してください。

シングルインターフェイスとデュアルインターフェイスを使用した ESC

CSP に ESC をインストールするには、day0 設定ファイルとして次の形式でユーザデータを作成する必要があります。

day0 ファイルを設定ドライブおよびユーザデータとして記述するシングルインターフェイスの例を次に示します。

```
#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$adWfd7LUn2PEUPWtWP15tCD7pO9bae672T1
            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

```

day0 ファイルを設定ドライブおよびユーザデータとして記述するデュアルインターフェイスの例を次に示します。

ESC では、静的 IPv4 を使用してイーサネットベースの物理ネットワークデバイスを設定できます。

```

#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$adWfD7LUn2PEUPWtWP15tCD7pO9bae672T1
            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

```

day0 ファイルで使用する ESC パスワードの作成

Cloud-Init day0 ファイルを使用して ESC インスタンスを展開する場合、パスワードは、プレーンテキストではなくハッシュとして渡す必要があります。

ハッシュ化されたパスワードを作成するには、mkpasswd ツールを使用します。次に、mkpasswd ツールを使用して、ハッシュ化されたパスワードを作成する例を示します。

```

~$ mkpasswd --method=SHA-512 --rounds=4096
Password:
$6$rounds=4096$Yo11pRsFO$itT5SGMJ6z8WErmj8TRMdInblgWeb/UChmrsQs3aspx8j.yUuuhxKk2XScOkerWwXpqD5F0sLfC5kzT5t2xGkL1

```

手順

ステップ 1 CSP へのユーザデータファイルのアップロード

ESC を展開するには、ユーザデータファイルをまず CSP ノードにアップロードする必要があります。

(注) イメージと day0 ファイルをアップロードするパスは、次のとおりです。/osp/repository

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

ステップ 2 ESC VM の展開

ESC VM をホストする CSP ノードに送信されるように設定を編集する必要があります。

次に、シングルインターフェイス用の展開データモデルを示します。デュアルインターフェイスの場合は、2つのインターフェイスがあります。<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 -->
  </service>
</services>

```

```

<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>

```

ステップ 3 設定の送信

(ConfD 付属の) Netconf コンソールを使用して、CSP ノードで ESC を展開します。

```
$ netconf-console --port=2022 --host=<CSP_IP_ADDRESS> --user=CSP_ADMIN_USERNAME
--password=CSP_ADMIN_PASSWORD --edit-config=deployESCH1.xml
```

HA の場合は、2 番目の ESC の設定を使用してコマンドを繰り返します。

ステップ 4 VIM コネクタの設定

ESC が起動したら、VIM コネクタを設定します。

CSP に ESC をインストールする場合、デフォルトでは VIM コネクタは追加されません。VNF を管理するには、VIM コネクタを作成する必要があります。

ステップ 5 VIM コネクタの追加

インストール後の VIM コネクタの設定、および VIM コネクタの管理の詳細については、『*Cisco Elastic Services Controller User Guide*』の「Managing VIM Connectors」を参照してください。

ESC HA アクティブ/スタンバイのインストール

CSP に ESC をインストールするには、day0 設定ファイルとして次の形式でユーザデータを作成する必要があります。HA の場合は、VM ごとに1つのファイルを作成する必要があります。

day0 ファイルで使用する ESC パスワードの作成については、「**day0 ファイルで使用する ESC パスワードの作成**」のセクションを参照してください。

次に、設定ドライブおよびユーザデータとして day0 ファイルを記述するノード 1 に ESC HA アクティブ/スタンバイをインストールする例を示します。

```
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$adWfD7LUn2PEUPWtWP15tCD7pO9bae672T1
      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

```

手順

ステップ 1 CSP へのユーザデータファイルのアップロード

ESC を展開するには、ユーザデータファイルをまず CSP ノードにアップロードする必要があります。

(注) イメージと day0 ファイルをアップロードするパスは、次のとおりです。/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
```

ステップ 2 ESC VM の展開

ESC VM をホストする CSP ノードに送信されるように設定を編集する必要があります。

次に、ノード 1 での ESC HA アクティブ/スタンバイの展開データモデルを示します。

```

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>

```

次に、ノード 2 での ESC HA アクティブ/スタンバイの展開データモデルを示します。

```

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>

```

ステップ 3 設定の送信

(ConfD 付属の) Netconf コンソールを使用して、CSP ノードで ESC を展開します。

```
$ 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
```

ステップ 4 VIM コネクタの設定

ESC が起動したら、VIM コネクタを設定します。

CSP に ESC をインストールする場合、デフォルトでは VIM コネクタは追加されません。VNF を管理するには、VIM コネクタを作成する必要があります。

ステップ 5 VIM コネクタの追加

インストール後の VIM コネクタの設定、および VIM コネクタの管理の詳細については、『Cisco Elastic Services Controller User Guide』の「Managing VIM Connectors」を参照してください。

CSP 2100 のサンプルファイルで使用する変数リスト

ユーザデータファイルを作成する場合や ESC を設定する場合、サンプルファイルで使用されている次の変数リストの値を準備する必要があります。

表 1: 変数リスト

変数名	目的
VAR_TIMEZONE	ESC クロックで使用されるタイムゾーン
VAR_SERVICE_NAME	CSP の ESC サービス名
VAR_NTP_SERVER	NTP サーバの IP アドレス
VAR_NETWORK1_NETMASK	eth1 インターフェイスのネットマスク (デュアルインターフェイス ESC)
VAR_NETWORK1_NAME	ESC の eth1 インターフェイスが存在する CSP 上のネットワーク名 (デュアルインターフェイス ESC)
VAR_NETWORK1_IPADDR	eth1 インターフェイスの IP アドレス (デュアルインターフェイス ESC)
VAR_NETWORK1_GATEWAY	eth1 インターフェイスのゲートウェイ (デュアルインターフェイス ESC)
VAR_NETWORK0_NETMASK	eth0 インターフェイスのネットマスク
VAR_NETWORK0_NAME	ESC の eth0 インターフェイスが存在する CSP 上のネットワーク名
VAR_NETWORK0_KADVRI	HA に使用される VRRP ID。HA ペアのサブネット内で一意である必要があり、両方の ESC で使用されているものと同じ値である必要があります。 範囲は 1 ~ 254 です。
VAR_NETWORK0_KADVIP	現在のアクティブ ESC に接続する HA ペアの VIP
VAR_NETWORK0_IPADDR2	他の ESC の eth0 インターフェイスに割り当てられた IP アドレス
VAR_NETWORK0_IPADDR	ESC の IP アドレス (eth0 インターフェイス)
VAR_NETWORK0_GATEWAY	eth0 インターフェイスのゲートウェイ

変数名	目的
VAR_NAMESERVER_IP	DNS サーバの IP アドレス
VAR_LOCAL_HOSTNAME	ESC のホスト名
CSP_IP_ADDRESS	使用する CSP 2100 の IP アドレス