Installing Cisco Elastic Services Controller on Amazon Web Services

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

Prerequisites

Following are the prerequisites that you must complete before you start installing the ESC instance in AWS.

Note If the ESC AMI images are shared with your AWS account, you can ignore these prerequisites and directly use the AMI image for ESC installation.

Step 1 Configure AWS CLI . You can use pip to install AWS CLI. For more details, refer to the AWS documentation.

Step 2 Configure the credentials for AWS CLI based on your account information.

Step 3 Create a Amazon S3 Bucket. Use this for bucket for uploading ESC image.

Note You must have a role named vmimport that allows importing VM and you must attach an IAM policy to the role. For more information, refer to the documentation on the creation of S3 bucket in AWS.

Step 4 Extract the vmdk file from ESC ova file.

```
$ tar xvf ESC-<latest image file>.ova ESC-<latest image file>-disk1.vmdk
```

Installing the Elastic Services Controller Instance in AWS

Once you have completed the tasks specified in the prerequisites section, you can use the procedure below to deploy and launch ESC instance in AWS.

Step 1 **Upload and register ESC image.**

a) Upload the vmdk image to the S3 bucket.

```
aws s3 cp <esc-vmdk-file> s3://<S3 bucket name>/
```

b) Register the image.

```
aws ec2 import-image --description "<esc-vmdk-file>" --disk-containers file://containers.json
```

Step 2 **Create user data**.

a) Create a user for ESC VM. Without a user, you would not be able to access the VM. It is recommended to configure 'admin' user with sudo access and ssh key.

b) Create the esc-config.yaml in user-data using write_files command.

Each instance can have up to 15 interfaces, depending on the type of instances.

Note If you want to use two interfaces, ensure that you create the two network interfaces before hand. These interfaces on different subnets must belong to the same availability zone. Add the interface details in the 'Configure Instance Details' tab when launching the instance from AWS console.

c) Enable esc_service and start it.

Following is an example of a complete user data:

```
#cloud-config
# It is recommended to disable password authentication for ssh when ESC runs in public cloud such as
 AWS.
ssh_pwauth: False
users:
 - name: admin
   # Put admin in 'esc-user' group, otherwise some scripts of ESC might fail when running as admin.
   groups: esc-user
   gecos: User created by cloud-init
   # This is an example of the hashed password for 'admin'.
   passwd:
$6$rounds=656000$pswsUsR7Iz9NIfA4$7E1sEGV8rhDieNDhc824lYwL3cQ8Rsgp9Nds.OZBe9rG/DE56YWk0kDZoB.DsjATrj9pcBnAe.rSOpWll2r0N/

   # The public key for admin user. Replace it with your public key to login.
   ssh-authorized-keys:
     - ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCqGLe4EVVI/rQy4e4jZUEnc5PvYItc39x5fz9rRggZzpwYzKXSj+UnWQMgvkIai+
Mv5vTPiEYTSNZx9PmUKayZaLr/2GiLPmnPNEgyzvjD5v77vV3Ag7eHfLXKLYbu7ausYqFKEFbNgSTGC1PWhoz2geY4zNO9hS3eMhNvxNSLpbo3ftzamQoqtWSx2aRc81M/
piy6NcBzJ3JeH4rOk9bQ+QxRAYm3bOlq/qRfuoxmrsgd68xAIXeDWyGumEThXN9MDEcQMIWO54fiPQgkqKbZWztH2EBnE9/B6rZCRBUUvdoQhQt2L/
hbCZN1k+oqQ53rlG/BjT09CGfYbgoHq2v
   # false allows you to sudo with the password.
   lock-passwd: false
   homedir: /home/admin
   # sudo settings
   sudo: ALL=(ALL) ALL
write_files:
 - path: /etc/cloud/cloud.cfg.d/sys-cfg.yaml
   content: |
     network:
       version: 1
       config:
       # You must define the name server when you use the static IP address.
       - type: nameserver
         address:
         - 172.31.0.2
```

```
      # Define physical network interface
      - type: physical
        name: eth0
        subnets:
        # Define the static IP address
        - type: static
          address: 172.31.5.66
          netmask: 255.255.240.0
          # Define the routes
          routes:
          - gateway: 172.31.0.1
            # 0.0.0.0 means the default gateway
            network: 0.0.0.0
            netmask: 0.0.0.0
 # ESC service config file
 - path: /opt/cisco/esc/esc-config/esc-cfg.yaml
   content: |
     confd:
       # AAA users for ConfD
       init_aaa_users:
       # Public key for ConfD user 'admin'
      - key: c3NoLXJzYSBBQUFBQjNOemFDMXljMkVBQUFBREFRQUJBQUFCQVFDeFkwMzByaEMzSXlWekF2bStISVlmMmpkdm
RUZndTTEpCRjVPTjZoUEgvK2FBTkkzb0NCSmJndjhPdjRtVXUvYmlCYmsyS240QW52Ni9ROE1YWGducnZST241MlJuODN2ejRCWTAw
T1h2SzZrT2YrUnZkSDFtNjhscVlrWU9uZVErNEtOak5tQXRwV0huT0xCZE1mZ2pzTmF1SlF1QVJUMEtDS2VBS3k4aUVqSUZpZDhWZ3
NiSlA0aDNpTzdjcTkza0E1ZGFQb0xiNWRKRVp3ZW15WS9ENGp6ZnJUeDVKWFFuMy80SDdaQVZPaWcyNzBGUnlGVkZhNFl1VXNYcDk1d3
QveHdpc0RUREVCYTYydjkxQzdXamtaNy9rYkRlRW9VSU9OZExqdEdvbU84c2JRUUJoZHBVTTZlNXJkeUl2VzQ3YTZYOFA5N2lBR3JrQ09
qMWVHNkYgeGlhb3hpbnlAWElBT1hJTlktTS1SRVhXCg==
         # Note: 'admin' is the only user supported and you cannot change the name here.
         name: admin
         # Hashed password for admin user.
         passwd:
$6$rounds=656000$d4hZHtniblo4/b0m$fD3./1H3jcPlWAENviFlu70i5wKnH9DIasDwTkL.p70UFZlfalzD9O7utL1NdKXwudnNhxIOrvYagkBfq6AWh.

     # No specific settings for esc service. Leave it empty.
     esc_service: {}
runcmd:
 - [ cloud-init-per, once, escservicestart, sh, -c, "chkconfig esc_service on && service esc_service
 start"]
```

Following is an example to define two interfaces in user data:

```
 - path: /etc/cloud/cloud.cfg.d/sys-cfg.yaml
   content: |
     network:
       version: 1
       config:

       - type: physical
         name: eth0

         subnets:

         - type: static
           address: 172.31.5.66
           netmask: 255.255.240.0
           # Define the routes
           routes:
           - gateway: 172.31.0.1
             # 0.0.0.0 means the default gateway
             network: 0.0.0.0
             netmask: 0.0.0.0

       - type: physical
         name: eth1
```

```
subnets:

- type: static
  address: 172.31.51.220
  netmask: 255.255.240.0
```

Step 3 **Launch ESC VM in AWS**

Launch ESC VM using one of the following method:

- **From Portal**:
  1. Go to EC2 Management Console, IMAGES/AMIs. Select the image you imported and click **Launch**.
  2. Choose an instance type. Choose t2.xlarge as the instance type.
  3. Configure the Instance Details. Add details such as User Data, Storage, Tag name, and so on. While using two interfaces, create these network interfaces and them here.
  4. Configure a security group. Enable ssh only.
  5. Click **Launch**.
- **From Command Line**: Choose the image, subnet, security group and use the following command to instantiate ESC VM.

```
aws ec2 run-instances --subnet-id <subnet id> --image-id <image id> --security-group-ids <security
 group id> --count 1
--instance-type <instance> --key-name <key name>  --user-data <user data file location>
--associate-public-ip-address
```

Note ESC does not support HA installation on AWS.

What to do next

After you launch the ESC VM, check the status of the ESC service using the `$ sudo escadm status` command.