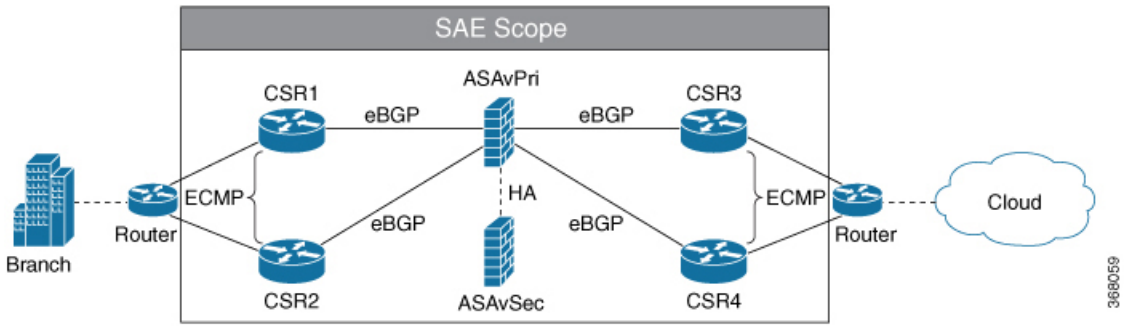
Deploy SAE

The steps to deploy SAE using the SAE core function pack are shown using a service chain example. The overall deployment procedure remains the same for different service chains with varying VNFs.

Service Chain Example: This chapter describes how to deploy a full service chain that uses CSRs as both–the consumer and the provider side endpoint gateways; and connects them through two ASAv VNFs: one as active and the other as a stand-by VNF. A single network service descriptor (NSD) is created for the entire service chain and consists of four CSRv VNFs and and two ASAv VNFs.



The procedure assumes that Nexus 9000 leaf switches are connected as a VPC switch pair.

The VNFs in the example are SR-IOV VNFs, which means that they are connected to SR-IOV interfaces on the CSP devices.

The following topics show a complete example of deploying SAE for the service chain described above.

- Verify Prerequisites, on page 1
- Create SAE Site, on page 2
- Design Your Services, on page 7
- Deploy Service Chain, on page 10

Verify Prerequisites

Ensure that the following prerequisites are met before proceeding to the next step.

- All switches are booted, and the users are configured with the required privileges.
- All CSP devices are booted.
- CSP devices and Nexus 9000 switches are wired according to the prescribed physical topology.

- The switches and CSP are configured to enable link discovery using LLDP.
- The switches are configured as a Virtual Port Channel (VPC) pair.
- Management ports of all CSPs are connected to redundant L3 networks and the correct IP addresses are assigned.
- Ensure that you have the pNIC information for your CSP devices. For more information, click here.
- The status of LLDP neigbors and VPC configuration on your Nexus 9000 switches have been verified. For more information, click here.
- The VNF images used in the example are uploaded to the CSP repository.
- The required routing configuration is done to enable management connectivity between the NSO server and all the devices.
- NTP server is ready for use and configured on devices used in the topology being used.
- All platform versions and requirements are verified.
- NSO has been installed. See Cisco Network Services Orchestrator (NSO) Solutions for more information.
- ESC has been installed. See Cisco Elastic Services Controller 4.3 User Guide for more details.
- SAE core function pack has been installed. See Cisco SAE Core Function Pack Installation Guide for details.

Create SAE Site

Step 1: Create authgroups for switches and CSP devices

The following example shows how to create authgroups for your CSP devices and switches. Replace the variables values such as passwords and IP addresses with values specific to your environment.

1. Create a file called AUTHGROUP.cli with the following content.

```
devices {
  authgroups {
        group SWITCH_AUTHGROUP {
                default-map {
                        remote-name     admin;
                        remote-password password123;
                }
        }
        group CSP_AUTHGROUP {
                default-map {
                        remote-name               admin;
                        remote-password           password123;
                        remote-secondary-password password567;
                }
        }
    }
}
```

2. Log in to NCS CLI and load merge the file you created in the previous step as shown below.

```
ncs_cli -u admin
configure
```

```
load merge AUTHGROUP.cli
commit
```

Step 2: Create resource pools

In this step, you will create the following respurce pools.

- **IP address pool:** SAE core function pack assigns IP addresses to virtual links between VNFs from this pool.
- **VLAN Pool:** The VLAN range that is allocated for service chains.
- **Management IP Pool:**The subnet or range of IP addresses.

The following example shows how to create resource pools. Ensure that you replace the values for IP_DATA_POOL, IP_MGMT_POOL with values specific to your environment.

1. Create a file called RESOURCE_POOL.cli with the following content.

```
resource-pools {
        id-pool VLAN_POOL {
                range {
                        start 101;
                        end   1000;
                }
        }
        id-pool default-as-pool {
                range {
                        start 4200000000;
                        end   4294967294;
                }
        }
        ip-address-pool IP_DATA_POOL {
                subnet X.X.X.X;
        }
        ip-address-pool IP_MGMT_POOL {
                subnet X.X.X.X;
        }
}
```

2. Log in to NCS CLI and load merge the file you created in the previous step as shown below.

```
ncs_cli -u admin
configure
load merge RESOURCE_POOL.cli
commit
```

Step 3: Create SAE catalog

The following example shows how to create your SAE catalog. Replace the name for CSP type with the corresponding name in your environment.

1. Create a file called CATALOG.cli with the following content.

```
sae-catalog SAE_CATALOG {
   csp CSP2100_SH {
   }
}
```

2. Log in to NCS CLI and load merge the file you created in the previous step as shown below.

```
ncs_cli -u admin
configure
load merge CATALOG.cli
commit
```

Step 4: Create SAE provider

The following example shows how to create an SAE provider and tenant for your site. You can replace the provider and tenant names with suitable names for your environment.

1. Create a file called PROVIDER.cli with the following content.

```
sae-provider SAE_PROVIDER {
    sae-provider-catalog SAE_CATALOG;
    sae-tenant SAE_TENANT;
}
```

2. Log in to NCS CLI and load merge the file you created in the previous step as shown below.

```
ncs_cli -u admin
configure
load merge PROVIDER.cli
commit
```

Step 5: Create SAE site

The following example shows how to create an SAE site and tenant for your site. Replace all variable values like site name, server name, etc. with values specific to your environment.

1. Create a file called SITE.cli with the following content.

```
sae-site SANJOSE  {
    sae-provider SAE_PROVIDER;
    sae-tenant   SAE_TENANT;
        vnf-mgmt-resources {
            vnf-mgmt-netmask X.X.X.X;
            vnf-mgmt-vlan    X;
            vnf-mgmt-gateway X.X.X.X;
        }
    var NTP_SERVER {
        val ntp.esl.cisco.com;
    }
    var DOMAIN_NAME {
        val cisco.com;
    }
    var NAME_SERVER1 {
        val X.X.X.X;
    }
    var NAME_SERVER2 {
        val X.X.X.X;
    }
    var PROXY_SERVER {
        val X.X.X.X;
    }
    var PORT {
        val 80;
    }
    var LICENSE_TOKEN {
        val FIX_ME;
    }
    resource-pools {
```

```
            as-pool          default-as-pool;
            mgmt-ip-pool     IP_MGMT_POOL;
            internal-ip-pool IP_DATA_POOL;
        }
        infrastructure {
            switching {
                type    n9k-switch-pair;
                bgp-asn 100;
            }
            compute-clusters Cluster1 {
                vlan-pool VLAN_POOL;
            }
        }
    }
```

2. Log in to NCS CLI and load merge the file you created in the previous step as shown below.

```
ncs_cli -u admin
configure
load merge SITE.cli
commit
```

Step 6: Create Inventory Discovery File

Create a file called discovery.cfg in your home directory with the following content.

```
{
    "site"              :       "SANJOSE",
    "cluster"           :       "CLUSTER1",
    "cspType"           :       "CSP2100_SH",
    "switch_seed_address":       "X.X.X.X",
    "rest_username"     :       "admin",
    "rest_password"     :       "Cisco123#",
    "csp_authgroup"     :       "CSP_AUTHGROUP",
    "n9k_authgroup"     :       "SWITCH_AUTHGROUP"
}
```

Ensure that your inventory discovery file includes the following information specific to your environment.

- `cspType` is the category defined in the Create Catalog step above.
- `csp_authgroup` and `n9k_authgroup` represent the authgroups you created in Step 1 of Create Site.
- `rest_username` and `rest_password` represent the rest API credentials of Nexus 9000 switches.

Step 7: Run the inventory discovery file to populate site infrastructure

The following example shows how to populate your site infrastructure by running the inventory discovery file you created in the previous step.

```
ncs_cli -u admin
admin@ncs>request discovery_action discover configFile /home/sae/discovery.cfg
```

Step 8: Add authgroups for VNFs used in your service chain

The following example shows how to create authgroups for the VNFs being used in the example service chain—CSR and ASA.

1. Create a file called VNF_AUTHGROUPS.cli with the following content.

```
devices authgroups {
    group CSR_AUTHGROUP {
```

```
            default-map {
               remote-name               admin;
               remote-password           password111;
               remote-secondary-password password222;
               }
            }
        group asa_authgroup {
        default-map {
               remote-name               admin;
               remote-password           password333;
               remote-secondary-password password444;
               }
        }
        group ESC_AUTHGROUP {
        default-map {
                    remote-name     admin;
                    remote-password password555;
                    }
            }
    }
```

2. Log in to NCS CLI and load merge the file you created in the previous step as shown below.

```
ncs_cli -u admin
configure
load merge VNF_AUTHGROUPS.cli
commit
```

Step 9: Bring up ESC and Create VNF Site Manager

Create only one VNF manager per SAE site.

```
ncs_cli -u admin
configure

---Bring up ESC---

set devices device ESC-0 authgroup ESC_AUTHGROUP address X.X.X.X port 830 state admin-state
 unlocked
set devices device ESC-0 device-type netconf ned-id netconf
set devices device ESC-0 trace pretty
commit

---Fetch SSH key and sync from ESC---

request devices fetch-ssh-host-keys
commit

---Sync from ESC0---

request devices sync-from device
commit

devices global-settings connect-timeout 3600 read-timeout 3600 write-timeout 3600
devices global-settings trace raw
commit
```

Step 10: Verify the list of devices onboarded on NSO device tree

```
show devices list

NAME     ADDRESS    DESCRIPTION  NED ID     ADMIN STATE
-------------------------------------------------------
```

```
CSP-1    X.X.X.X   -           netconf    unlocked
CSP-2    X.X.X.X   -           netconf    unlocked
ESC-0    X.X.X.x   -           netconf    unlocked
N9K-1    X.X.X.X   -           cisco-nx   unlocked
N9K-2    X.X.X.X   -           cisco-nx   unlocked
```

Design Your Services

Note All the configuration examples are representative only. The variables in your configuration such as: IP addresses, passwords, license information etc. would differ based on your environment and specifications.

All the sample configuration used in this service chain example can be downloaded here.

Configure and Deploy VNFD

Create VNFD for CSR

Note You can download the zipped folder containing all the configuration files for VNFs, VNFDs, and NSDs here.

Step 1: Create a file called V_CSR.cli with content from this location.

Step 2: Log in to NCS CLI and load merge the file you created in step 1 as shown below.

```
ncs_cli -C -u admin
configure
load merge V_CSR.cli
commit
top
```

Create VNFD for ASA

Step 1: Create a file called V_ASA.cli with content from this location.

Step 2: Log in to NCS CLI by running the command and load merge the file you created in step 1 as shown below.

```
ncs_cli -C -u admin
configure
load merge V_ASA.cli
commit
top
```

Configure VNFD Deployment For Primary Consumer CSR

1. Create a text file called VD_CSR_PC.txt with content from this location.
2. With sudo privilege, copy the file to /opt/cisco/nso/day0.
3. Create a text file called VD_CSR_PC.cli in your SAE catalog with content from this location.
4. Log in to NCS CLI and load merge the file you created in step 3 as shown below.

```
ncs_cli -C -u admin
configure
load merge VD_CSR_PC.cli
commit
top
```

Configure VNFD Deployment For Secondary Consumer CSR

1. Create a text file called VD_CSR_SC.txt with content from this location.
2. With sudo privilege, copy the file to /opt/cisco/nso/day0.
3. Create a text file called VD_CSR_SC.cli, with content from this location.
4. Log in to NCS CLI and load merge the file you created in step 3 as shown below.

```
ncs_cli -C -u admin
configure
load merge VD_CSR_SC.cli
commit
top
```

Configure VNFD Deployment For Primary Provider CSR

1. Create a text file called VD_CSR_PP.txt for day-0 VNF with content from this location.
2. With sudo privilege, copy the file to /opt/cisco/nso/day0.
3. Create a text file called VD_CSR_PP.cli in your SAE catalog with content from this location.
4. Log in to NCS CLI and load merge the file you created in step 3 as shown below.

```
ncs_cli -C -u admin
configure
load merge VD_CSR_PP.cli
commit
top
```

Configure VNFD Deployment For Secondary Provider CSR

Create day-0 VNF for your secondary provider CSR

1. Create a text file called VD_CSR_SP.txt for day-0 VNF with content from this location.
2. With sudo privilege, copy the file to /opt/cisco/nso/day0.
3. Create a text file called VD_CSR_SP.cli in your SAE catalog with content from this location.
4. Log in to NCS CLI and load merge the file you created in step 3 as shown below.

```
ncs_cli -C -u admin
configure
load merge VD_CSR_SP.cli
commit
top
```

Configure VNFD Deployment For Primary ASA

1. Create a text file called VD_ASA_PM.txt with content from this location.

2. With sudo privilege, copy the file to /opt/cisco/nso/day0.
3. Create a text file called VD_ASA_PM.cli in your SAE catalog with content from this location.
4. Log in to NCS CLI and load merge the file you created in step 3 as shown below.

```
ncs_cli -C -u admin
configure
load merge VD_ASA_PM.cli
commit
top
```

Configure VNFD Deployment For Secondary ASA

Create day-0 VNF for your secondary ASA.

1. Create a text file called VD_ASA_SM.txt for day-0 VNF with content from this location.
2. With sudo privilege, copy the file to /opt/cisco/nso/day0.
3. Create a text file called VD_ASA_SM.cli in your SAE catalog with content from this location.
4. Log in to NCS CLI and load merge the file you created in step 3 as shown below.

```
ncs_cli -C -u admin
configure
load merge VD_ASA_SM.cli
commit
top
```

Configure and Deploy NSD

Note You can download the zipped folder containing all the text files referenced in this document here.

Create NSD for CSR_ASA_CSR

Step 1: Create a file called N_CSR_ASA_CSR_E2E.cli with content from the following location: https://github.com/Cisco-SAE/CSRv_ECMP-ASAv_HA-CSRv_ECMP/blob/master/N_CSR_ASA_CSR_E2E.cli.

The preceeding NSD includes six VNF profiles. The NSD includes the following Service Access Point Descriptors (SAPD).

- FACING_CONSUMER_SAPD INSIDE: Represents the consumer endpoint and indicates traffic flow from the consumer endpoint gateway.
- MANAGEMENT: Represents VNF management.
- FACING_CONSUMER_SAPD OUTSIDE: Represents the provider endpoint and indicates traffic flow from the provider endpoint gateway.
- software-image-descriptor image: Represents the file on the web server.

Step 2: Log in to NCS CLI and load merge the file you created in step 1 as shown below.

```
ncs_cli -C -u admin
configure
load merge N_CSR_ASA_CSR_E2E.cli
commit
top
```

Configure NSD Deployment For VNFs

In this step, you will create an NSD deployment for the consumer CSR, the provider CSR, and the ASA, that form part of your service design.

1. Create a text file called ND_CSR_ASA_CSR_E2E .cli with content from the following location: https://github.com/Cisco-SAE/CSRv_ECMP-ASAv_HA-CSRv_ECMP/blob/master/ND_CSR_ASA_CSR_E2E.cli.

Note The names of the VNFDs and NSDs referenced in the text file above should match the VNFD and NSD names created in the preceding sections.

2. Log in to NCS CLI and load merge the file you created in step 1 as shown below.

```
ncs_cli -C -u admin
configure
load merge ND_CSR_ASA_CSR_E2E .cli
commit
top
```

Deploy Service Chain

Configure External Endpoints

The following example show how to configure external endpoints using pre-allocated resources such as IP address, gateways, netmasks, and VLANs.

Note All the configuration examples are representative only and are specific to the service chain example being used in this chapter. The variables in your configuration such as: IP addresses, passwords, license information etc. would differ based on your environment and specifications.

1. Create a text file called EEP_CSR_ASA_CSR.cli with content from the this location.
2. Login to NCS CLI and load merge the file you created in step 1 as shown below.

```
ncs_cli -C -u admin
configure
load merge EEP_CSR_ASA_CSR.cli
commit
top
```

Deploy Full Service Chain (CSR-ASA-CSR)

1. Create a text file called E2E_1_CSR_ASA_CSR.cli with content from this location.

2. Login to NCS CLI and load merge the file you created in step 1 as shown below.

```
ncs_cli -C -u admin
configure
load merge E2E_CSR_ASA_CSR.cli
commit
```