Cisco SVO Admin Plane

This chapter describes the admin plane that used in Cisco NCS 2000 SVO and its related tasks.

Table 1: Feature History

Feature Name	Release Information	Feature Description
Admin Plane UI Enhancements	Cisco NCS 2000 Release 12.2	The following admin plane UI enhancements are done to improve the user experience: • Flexible memory reservation replaces memory profiles. This enhancement allows the user to assign desired memory for an SVO instance. • **IP Assignment Policy** page replaces IP Filtering page. This change enables the user to modify IP addresses in the allowed list and denied list. In case of conflicting entries, the allowed IP address is preferred. • **SVO Runtime Status** page simplifies troubleshooting and allows the user to extract detailed information about the runtime environment of both the local and remote SVO instances. • **Admin Plane Restart** button replaces Reset to Factory Default button in the **Utilities** page. This enhancement enables the user to restart the admin plane when required. • **Certificates** page is introduced to check the details of SVO admin plane. The **Renew Certificate** button can be used to extend the lifetime of self-signed admin plane certificates by five years.

Cisco SVO Admin Plane Overview

Cisco SVO admin plane is responsible for turning up the shelf virtualization orchestration services for the network elements (NE). It is a web user interface that facilitates the installation of the SVO software and configures the NE instances and orchestrates high availability (HA) services.

The admin plane is supported both on the external server and the SVO card. The admin plane allows you to create, update, manage, and delete SVO NE instances.

To achieve high availability for the exernal server, the SVO software is installed on two servers in local and remote locations. In the case of the SVO card, two SVO line cards are installed in two different chassis of the ROADM node. The two external servers or two SVO cards are connected by two intercommunication links—through the HA network (primary link) and through the devices network (secondary link). Both links are used for the communication between the admin planes. The primary link is also responsible for replicating all the configuration transactions that are performed on each active SVO instance to the related standby SVO instance.

All the networking configuration data required by the admin plane is present in a file shared by both the SVO cards or external servers. When creating a new SVO instance, you can configure the management interface address, while the other parameters are automatically selected by the admin plane based on the constraints defined in the configuration file.

The admin planes coordinate to automatically assign active and standby roles to the SVO instances. The admin planes can also perform an automatic switchover that promotes the standby instance to active when software or hardware faults affect the active instance.

The Cisco SVO admin plane allows you to:

- Create the super user for the SVO card model or the admin user for the external server model.

- Create, update, or delete SVO instances of type ROADM, OLA, DGE, or TXP. You can also view the details of the SVO instances.

Note The first SVO instance created on the SVO card is always a ROADM instance. Subsequent SVO instances can be OLA, DGE, or TXP.

- Control, monitor, and performs health checks of the SVO instances.

- Auto switch SVO instances during a software or hardware fault in the SVO cards or servers.

- Force a manual switch between the active and standby SVO instances.

- View parameters of the network configuration file.

- View a list of allowed and blocked IP addresses

- Troubleshoot using diagnostics. A zip file containing the log files from the admin plane can be downloaded.

- Reset the SVO card to factory defaults. This action erases all containers and configurations on the SVO card.

The following table highlights the differences between the two types of system installation.

SVO Card Model	External Server Model
The super user must be created to log in to the admin plane.	The admin user must be created to log in to the admin plane.
Only IPv4 addresses can be configured.	IPv4 or IPv6 addresses can be configured independently for the three networks (Management, HA, and Devices) during the installation.
Only one ROADM SVO instance can be created. Subsequent instances must be of type OLA, DGE, or TXP.	Any number of ROADM, OLA, DGE, or TXP SVO can be created.
The SVO card can be reset to its default values.	—

Network Configuration File

Network configuration file defines all the information that is related to the servers and the networking infrastructure that is required to set up the SVO functionalities. See Required Network Resources section to define the networks.

The *network.yml* configuration file starts with the **server-name** field. The **server-name** field refers to the **name** field of the server in which the installation executes.

The configuration files that are used for the installation in high availability networks on two servers or VMs contain different values in the **server-name** field for the respective servers.

The *network.yml* configuration file contains two main sections, one for each server or VM of the cluster.

For each server section, there are three fields:

- name—Server name (editable)

- mgmt-port—Not editable (value is 443)

- ha-agent-port—Not editable (value is 5480)

SVO network architecture is based on four networks. Each section in a *network.yml* file defines the following networks:

- **Management**—The management ports of the admin plane and SVO instances belong to this network.

- **High Availability**—This network is used for SVO database replication and communication between the admin planes.

- **Private HA Network**—This network is used only for communicating between the admin plane and the local SVO instances in certain processes such as node activation. It doesn't use external networking resources.

- **Devices**—This network is used for connecting the NCS 2000 devices. The devices must be reachable through this subnet. If the admin plane is unable to communicate with its peer server on the primary high availability network, it uses a link on this network as an alternative way to communicate.

The **Private HA Network** is local to the server or VM. The other three networks are exposed outwards and they must have three different subnets.

The following table describes the fields in the *network.yml* configuration files.

Field	Value	Editable	Description
server-name	—	Yes	Name of the server to which the file is applied.
name	management hanetwork haprivate devices	No	Name of the network
mgmt-port	443	No	Port that is used for admin plane web UI
ha-agent-port	5480	No	Port that is used for internal communication between the admin plane and SVO
host-nic-name	—	Yes	(Optional) Interface that is used in docker network **Note** Only in **management**, **hanetwork**, and **devices**
ha-port	10001 10002	Yes	Port used for admin plane high-availability on the specific network (primary path) **Note** Only in **HA** and **Devices.**
IPv4			
ip	—	Yes	Subnet
prefix	—	Yes	Mask
gateway	—	Yes	Gateway
host-nic	—	Yes	(Optional) IPv4 address that is assigned to the host interface **Note** Only in **management**, **hanetwork**, and **devices**
adminplane	—	Yes	IPv4 address that is assigned to the admin plane
IPv6: (Optional)			

Field	Value	Editable	Description
ip	—	Yes	Subnet
prefix	—	Yes	Mask
gateway	—	Yes	Gateway
host-nic	—	Yes	(Optional) IPv6 address that is assigned to the host interface **Note** Only in **management**, **hanetwork**, and **devices**
adminplane	—	Yes	IPv6 address that is assigned to the admin plane

The following sections contain one example of *network.yml* file for IPv4 configuration and one for IPv6 configuration.

To create the configuration file, use one of the following templates.

IPv4 Network YAML Configuration File Sample

```
server-name: VM1

servers:
  - name: VM1
    mgmt-port: 443
    ha-agent-port: 5480
    mgmt:
      name: management
      host-nic-name: ens192
      ipv4:
        ip: 10.58.233.0
        prefix: 24
        gateway: 10.58.233.1
        host-nic: 10.58.233.75
        adminplane: 10.58.233.76
    ha:
      name: hanetwork
      host-nic-name: ens224
      ha-port: 10001
      ipv4:
        ip: 192.168.1.0
        prefix: 24
        gateway: 192.168.1.1
        adminplane: 192.168.1.4
        host-nic: 192.168.1.2
    haprivate:
      name: haprivate
      ipv4:
        ip: 192.168.3.0
        prefix: 24
        gateway: 192.168.3.1
        adminplane: 192.168.3.2
    devices:
      name: devices
      host-nic-name: ens256
      ha-port: 10002
      ipv4:
        ip: 192.168.2.0
        prefix: 24
```

```
          gateway: 192.168.2.1
          adminplane: 192.168.2.4
          host-nic: 192.168.2.2

  - name: VM2
    mgmt-port: 443
    ha-agent-port: 5480
    mgmt:
      name: management
      host-nic-name: ens192
      ipv4:
        ip: 10.58.233.0
        prefix: 24
        gateway: 10.58.233.1
        host-nic: 10.58.233.77
        adminplane: 10.58.233.78
    ha:
      name: hanetwork
      host-nic-name: ens224
      ha-port: 10001
      ipv4:
        ip: 192.168.1.0
        prefix: 24
        gateway: 192.168.1.1
        adminplane: 192.168.1.5
        host-nic: 192.168.1.3
    haprivate:
      name: haprivate
      ipv4:
        ip: 192.168.3.0
        prefix: 24
        gateway: 192.168.3.1
        adminplane: 192.168.3.2
    devices:
      name: devices
      host-nic-name: ens256
      ha-port: 10002
      ipv4:
        ip: 192.168.2.0
        prefix: 24
        gateway: 192.168.2.1
        adminplane: 192.168.2.5
        host-nic: 192.168.2.3
```

IPv6 Network YAML Configuration File Sample

Networking infrastructure requires all the *network.yml* files with IPv6 section to have an IPv4 section.

In the following example, the IPv6 section has been configured for the three networks: management, high availability, and devices.

It is not mandatory that all networks must be configured in IPv6. Each network is independent of others.

Table 2: Network Types

Network Types	Description
Management	**Dual stack (IPv4+IPv6)**—User wants to use both IPv4 and IPv6 addresses. It is required that the same IPv4 subnet is used between the two servers **IPv6 only**—User wants to use only IPv6 addresses. Use different private IPv4 subnets between the two servers, to avoid any conflict In both scenarios, the IPv4 information are required by the networking infrastructure.
High availability and devices	When IPv6 information are available, IPv4 information are not used directly by the SVO application but are anyway required by the networking infrastructure. The suggestion is to use different private IPv4 subnets between the two servers, to avoid any conflict.
Private HA Network	It is a local network. You must use the IPv4 information as required by the networking infrastructure. There is no reason to add IPv6 section.

```
server-name: VM1

servers:
  - name: VM1
    mgmt-port: 443
    ha-agent-port: 5480
    mgmt:
      name: management
      host-nic-name: ens192
      ipv4:
        ip: 10.58.233.0
        prefix: 24
        gateway: 10.58.233.1
        adminplane: 10.58.233.72
      ipv6:
        ip: 2001:420:4491:2004::233:0
        prefix: 112
        gateway: 2001:420:4491:2004::233:2
        host-nic: 2001:420:4491:2004::233:70
        adminplane: 2001:420:4491:2004::233:72
    ha:
      name: hanetwork
      host-nic-name: ens224
      ha-port: 10001
      ipv4:
        ip: 192.168.80.0
        prefix: 24
        gateway: 192.168.80.1
        adminplane: 192.168.80.2
      ipv6:
        ip: 2001:db8:abc:111::0
        prefix: 64
```

```
              gateway: 2001:db8:abc:111::1
              adminplane: 2001:db8:abc:111::4
              host-nic: 2001:db8:abc:111::2
        haprivate:
          name: haprivate
          ipv4:
            ip: 192.168.3.0
            prefix: 24
            gateway: 192.168.3.1
            adminplane: 192.168.3.2
        devices:
          name: devices
          host-nic-name: ens256
          ha-port: 10002
          ipv4:
            ip: 192.168.81.0
            prefix: 24
            gateway: 192.168.81.1
            adminplane: 192.168.81.2
          ipv6:
            ip: 2001:db8:abc:222::0
            prefix: 64
            gateway: 2001:db8:abc:222::1
            adminplane: 2001:db8:abc:222::4
            host-nic: 2001:db8:abc:222::2

    - name: VM2
      mgmt-port: 443
      ha-agent-port: 5480
      mgmt:
        name: management
        host-nic-name: ens192
        ipv4:
          ip: 10.58.233.0
          prefix: 24
          gateway: 10.58.233.1
          adminplane: 10.58.233.73
        ipv6:
          ip: 2001:420:4491:2004::233:0
          prefix: 112
          gateway: 2001:420:4491:2004::233:2
          host-nic: 2001:420:4491:2004::233:71
          adminplane: 2001:420:4491:2004::233:73
      ha:
        name: hanetwork
        host-nic-name: ens224
        ha-port: 10001
        ipv4:
          ip: 192.168.83.0
          prefix: 24
          gateway: 192.168.83.1
          adminplane: 192.168.83.3
        ipv6:
          ip: 2001:db8:abc:111::0
          prefix: 64
          gateway: 2001:db8:abc:111::1
          adminplane: 2001:db8:abc:111::5
          host-nic: 2001:db8:abc:111::3
      haprivate:
        name: haprivate
        ipv4:
          ip: 192.168.3.0
          prefix: 24
          gateway: 192.168.3.1
```

```
      adminplane: 192.168.3.3
devices:
  name: devices
  host-nic-name: ens256
  ha-port: 10002
  ipv4:
    ip: 192.168.84.0
    prefix: 24
    gateway: 192.168.84.1
    adminplane: 192.168.84.3
  ipv6:
    ip: 2001:db8:abc:222::0
    prefix: 64
    gateway: 2001:db8:abc:222::1
    adminplane: 2001:db8:abc:222::5
    host-nic: 2001:db8:abc:222::3
```

Prepare the Network Configuration

Use this task to prepare the network configuration for the external server model or the SVO card model.

Before you begin

See Network Configuration File, on page 4.

Procedure

Step 1	Create a configuration file (*network.yml)* for each server with the networking configuration data. This file is uploaded during the installation.
Step 2	Cable and configure the related network interfaces (physical or virtual).
	Both the configuration files are identical and contain the data for both the servers in HA. The only difference is the *server-name* attribute that contains the name of the server to which the file is applied.

Recommended Hardware

The hardware recommendation is based on the Cisco UCS configuration with the VMWare ESXi-7.0U1c.

Note   In VMWare ESXi, configure the Security Policy of virtual switches as follow:

```
Allow promiscuous mode: yes
Allow forged transmits: yes
Allow MAC changes: yes
```

• Cisco UCS-C220-M5SX

• 32 CPUs (2x Intel Xeon Gold 5218 CPU @ 2.30GHz)

• 256GB RAM

• 2x 480GB SSD (Raid)

• MLOM NIC for additional network interfaces

Recommended Software

The following are the recommended OS versions.

• CentOS Linux release 7.9.2009 (Docker Engine 19.03.8)

• CentOS Linux release 8.3.2011 (Docker Engine 20.10.5)

Note   CentOS 7 active support ends in December 2024 (recommended)

CentOS 8 active support ends in December 2021

Recommended Resource for Virtual Machines

The following sections provide information on the resources that are required to define SVO instances.

In case of high availability, it is recommended to have the same resources on both the VMs.

CPU

• One virtual CPU for each ROADM node

• One virtual CPU for every three OLA, DGE, or TXP nodes

Memory

• 2 GB for admin plane

• 3 GB for each OLA, DGE, TXP, or ROADM with 2, 3 or 4 degrees

• 4 GB for each ROADM with 5, 6, 7 or 8 degrees

• 8 GB for each ROADM with more than 8 degrees

Disk Space

5 GB for each SVO instance

Required Network Resources

Network resources that must be planned in the design phase are related to three different subnets.

The following table describes the different networks.

Table 3: Network Type

Network	Network Type	Description
mgmt	Management network	Offers Netconf NBI and Web UIs for admin plane and SVO instances (used by users)
ha	High availability network	For data replication **Note** Used only between two servers or VMs
devices	Network to reach NCS 2000 devices	Communicate with NCS 2000 devices **Note** Used only between the servers or VMs and the NCS 2000 devices

The following figure illustrates the management of an NE before and after the introduction of SVO.

Figure 1: Network Element Before and After SVO

✎
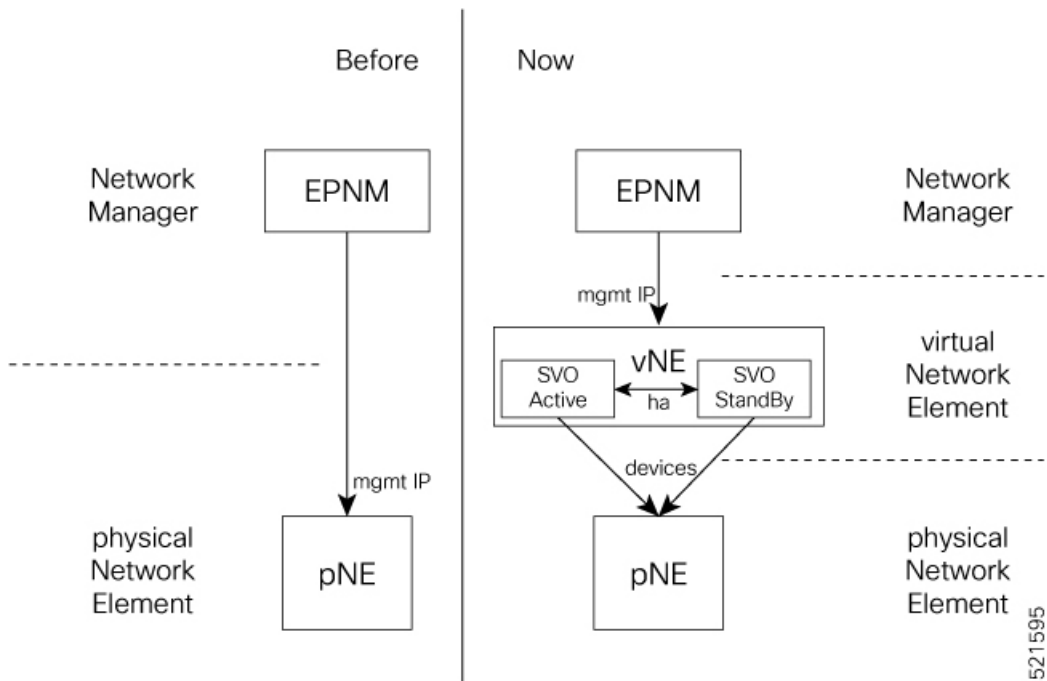
Note For each virtual NE, represented by a SVO instance, there is a single management IP address. The status of the management interface, Up or Down, is aligned with the status of the SVO, active or standby.

If SVO is active, the management interface is Up. If SVO is standby, the management interface is Down.

The status, active or standby, is orchestrated by admin plane.

In the following table, the data to define the size of the subnets to set up HA network and the description of each network and its usage.

Network	No. of IP Addresses	Description
management	One for each gateway Two for each host NIC Two for each admin plane One for each SVO instance	Must be the same subnet on both the servers or VMs. On this subnet, SVO software application offers Netconf NBI and Web UIs. When used from the customer DCN, this network becomes visible and routable in the customer DCN. Admin planes work in active/active status, that is, on each server or VM, when an admin plane is running, it is possible to connect to the Web UI through the management IP address (https://*mgmt-ip*). Each SVO instance works in active/standby status. The instances share the same management IP address. **Note** The network interface is Down on the standby side.
HA	One for each gateway Two for each host NIC Two for each admin plane Two for each SVO instance	In release 12.1, HA network must have the same subnet on both the servers or VMs. From release 12.2, HA network can have different and routable subnets. Allows data replication between active and standby SVO instances. It is the primary communication channel between admin planes.
Devices	One for each gateway Two for each host NIC Two for each admin plane Two for each SVO instance	In release 12.1, Devices network must have the same subnet on both the servers and the VMs. From release 12.2, the subnets can be different. Devices shall be routable towards NCS 2000 network. Used by SVO instances to communicate with NCS 2000 devices. It is the secondary communication channel between admin planes.

Install the External Server

Before you begin

You must complete the following recommendations:

- Recommended Hardware, on page 10
- Recommended Software, on page 11
- Recommended Resource for Virtual Machines, on page 11
- Required Network Resources, on page 11

Use this task to install the external server.

Procedure

Step 1   Create the network configuration. See Prepare the Network Configuration, on page 10.

Step 2   Obtain the admin plane (es-admin-plane) and SVO (svo-dos) docker images. Perform these steps:

- Get the `ncs2k-server-12.1.0_REL.tar` file and extract its contents.

```
> tar xvf ncs2k-server-12.1.0_REL.tar
> cd SIGNED_RPM; ls
NCS2K-S-1210.020K.2311.x86_64.rpm
es-admin-plane-12.1.0.B0582.x86_64.rpm
svo-dos-12.1.0.R0582.x86_64.rpm
> rpm2cpio es-admin-plane-12.1.0.B0582.x86_64.rpm | cpio -D <OUTDIR> -idmv
> rpm2cpio svo-dos-12.1.0.R0582.x86_64.rpm | cpio -D <OUTDIR> -idmv
```

- Load the admin plane and SVO images.

```
docker load -i es-admin-plane.tgz
docker load -i svo-dos.tgz
```

- Verify the images using the **docker images** command.

Step 3   Create the configuration folder */misc/disk1/data/adminplane*. The folder path need to used as a parameter the next step.

Step 4   Create a text file called *installer.properties* inside the configuration folder. Add the the following line to the file.

```
server.address=<adminplane-mgmt-ip>
installer.remote-connection=true
```

The `adminplane-mgmt-ip` is the IP address that is assigned to the admin plane in the management network.

Step 5   Create a docker network using any one of the following commands:

- **IPv4**

```
docker network create -d macvlan --attachable --subnet <subnet>/<mask> --gateway <gw>
-o parent=<mgmt-interface> management

docker create --name adminplane --network management --ip <adminplane-mgmt-ip> -m 2g
--memory-swap 2g --cap-add NET_ADMIN --restart
```

```
always -v /misc/disk1/data:/misc/disk1/data -v /var/run/docker.sock:/var/run/docker.sock
 -v /misc/disk1/data/adminplane:/opt/config es-admin-plane:<version>
```

- **IPv4 and IPv6**

```
docker network create -d macvlan --attachable --subnet <subnet>/<mask> --gateway <gw>
--ipv6 --subnet <ipv6-subnet>/<prefix> --gateway <ipv6-gw> -o parent=<mgmt-interface>
management
```

```
docker create --name adminplane --network management --ip <adminplane-mgmt-ip> --ip6
<adminplane-mgmt-ipv6> -m 2g --memory-swap 2g --cap-add NET_ADMIN --restart
always -v /misc/disk1/data:/misc/disk1/data -v /var/run/docker.sock:/var/run/docker.sock
 -v /misc/disk1/data/adminplane:/opt/config es-admin-plane:<version>
```

Step 6 Start the application using the following command:

```
docker start adminplane
```

Step 7 Run the SVO installation tool. See .

Run the SVO Installation Tool

Use this task to run the SVO installation tool for the external server model or the SVO card model.

Note In the SVO card model, the user created is the superuser in all the SVO instances created later.

Procedure

Step 1 Start the SVO installation tool using the IP address as follows:

- **External server model**—Use the management IP address, http://*adminplane-mgmt-ip*.

- **SVO card model**—Use the pre-defined IP address, http://192.168.0.66.

  Note The client must be connected to the SVO craft port using an ethernet cable.

Step 2 In the **Credentials** area, perform these steps:

 a. Enter a username in the **Username** field.

 b. Enter a password in the **Password** field.

    The password must be a minimum of eight characters, and it can be a maximum of 127 characters. The password must have at least one uppercase letter, one lowercase character, one number, and one special character.

 c. Retype the password in the **Retype Password** field.

Step 3 In the **Networks** area, perform these steps:

 a. Click **Browse** to select the *network.yml* configuration file **Configuration File** field.

For more information about the configuration file (*network.yml*), see Prepare the Network Configuration, on page 10.

Step 4   Click **Submit**.

The system creates the credentials, verifies the network configuration file and brings up the system. You are then directed to the Cisco SVO admin plane login page.

Log into the Cisco SVO Admin Plane

Use this task to log in to the Cisco SVO admin plane.

Procedure

Step 1   In the browser URL field, enter the IP address of the admin plane (https://*IP_address*/login).

The login page appears.

Step 2   Enter the username and password.

In an SVO card system, only the superuser is allowed to log in to the Cisco SVO admin plane.

Step 3   Click **Login**.

The SVO Instances page is displayed.

SVO Admin Plane Home Page

Side Menu Items

In the SVO Admin Plane home page, the menu items are present in the left panel. The menu items allow you to monitor and troubleshoot SVO instances, view certificates, and restart admin plane. The following list describes the menu items.

- **Instances**—Instances menu enables you to create, edit, and monitor SVO instances.
- **Diagnostics**—Diagnostics menu allows you to download log files to troubleshoot SVO instances.
- **Networks**—Networks menu enables you to configure networks and assign IP addresses.
- **Certificates**—Certificates menu enables you to view and renew the self-signed admin plane certificates.
- **Utilities**—Utilities menu allows you to restart the admin plane.

Bell Icon (HA Status)

The icon on the top right of the SVO home page indicates the status of high availability network (primary link) and devices network (secondary link). The icon statuses are:

- **Green**—Both the primary and secondary links are up. High availability is working successfully.

- **Yellow**—A warning that the primary link is up but the secondary link is down.

- **Red**—There are two cases:

  - **Small red icon**—The primary link is down but the admin planes are able to communicate because the secondary link is up.

  - **Large red icon**—Both the primary and secondary links are down and the server is functioning in standalone mode.

User Profile Icon

The user profile icon displays the username and the log out option for the user to exit the current SVO session.

SVO Instances

An SVO instance is a software virtualization of the physical NCS 2000 node that has been configured to manage. SVO instances are of types—ROADM, OLA, DGE, and TXP. In an SVO card model, you can configure a maximum of one ROADM SVO instance and up to 30 OLA DGE, or TXP SVO instances.

In an external server model, you can configure any number of ROADM, OLA, DGE, or TXP SVO instances.

You can create, update and delete SVO instances using the admin plane. Each SVO instance runs as an active instance on one server and as a standby instance on the other server. It is also possible to manually switch the roles of the SVO instance between active and standby.

The peer admin planes that are running on the local and remote server respectively have two intercommunication links, one through the HA network (primary link) and the other through the devices network (secondary link).

The table displays the SVO instances that were created. Each row has two entries relating to the local and remote SVO card or server. In each row, the first entry is the local instance and the second entry is the remote instance. The details are:

- **Name**—Name of the SVO instance.

- **IP Address**—The IP address of the SVO instance. It is IPv4 for the SVO card model, and IPv6 or IPv4 for the external server model.

- **SW version**—SW version on the server.

- **State**—State of the SVO instance.

- **App State**—State of the SVO application that is running on the SVO instance.

  - During a manual switching process, the **App State** field displays different statuses such as SWITCHING, SWITCH_DONE, or UP.

  - The **App State** field displays ACTIVATING or ACTIVATE_RESTART only after the SVO web UI has requested the admin plane to orchestrate the activation process.

- **Role** —Role of the SVO instance. The roles are ACTIVE, STANDBY, NONE, and UNKNOWN. In case of issues or specific SVO states, special tags are displayed such as NOT_RESPONDING, STARTING,STOPPED, or BAD_CLUSTER.

Note The green icon indicates the reachability of the SVO instance to the connected NCS 2000 device. If the active SVO instance is unable to reach the NCS 2000 device due to a network segregation, it performs an auto-switch.

- **Up Time**—Up time of the SVO instance.

- **Type**—Label for the SVO instance.

- **Action**—A set of actions can be performed on the SVO instance:

  - **Details of the SVO instance—**Click this icon to view the summary of the local and remote SVO instance.

  - **Edit SVO Instance**—Click this icon to edit the memory size of the SVO instance.

  - **Switch SVO Instance**—Click this icon to manually switch the SVO instance between servers.

Note A switch operation is possible only if both the SVO instances are up and running and the role of the instances are Active and Standby.

  - **Delete SVO Instance**—Click this icon to delete an SVO instance.

Note This icon is disabled when a switch operation is in progress.

Create an SVO Instance

Use this task to configure an SVO instance.

Before you begin

Log into the Cisco SVO Admin Plane, on page 16

Procedure

Step 1 Click the + button at the top-left of the SVO Instances page.

The SVO Instance Configuration page appears.

Step 2 In the **General Info** area, perform these steps:

a) Enter the name for the new SVO instance in the **Name** field.

The name is mandatory and must be unique among the SVO instances managed by the admin plane. It can contain a minimum of two characters and a maximum of 64 characters. It can include numbers, uppercase letters, lowercase letters, dashes (-), or underscores (_).

b) Choose the version from the **Software Version** drop-down list.

c) Choose the type of the SVO instance from the **TDM Terminology** drop-down list.

The two options are ANSI and ETSI.

d) Choose the label of the SVO instance from the **Type** drop-down list.

The four options are ROADM, OLA, DGE, and TXP. The type indicates the role of the SVO instance in the network.

> **Note**   When Type is selected, a default value for memory size is displayed in the **Reserved Memory GB** field.

e) Choose the memory size to be allocated to the SVO instance from the **Reserved Memory GB** field.

The user is allowed to reserve the SVO container memory in steps of 1GB. This value is visible and summarized at server level in the SVO instances table.

Step 3   In the **Admin User** area, perform these steps:

a) Enter the username in the **Username** field.

The values "admin," "oper," "private," or, "public" cannot be used as the admin username.

b) Enter the password in the **Password** field.

The password must be a minimum of eight characters. The password must contain at least an uppercase letter a number, and a special character. The special characters supported are ! $ % ^ ( ) [ ] _ - ~ { } . +

c) Enter the password again in the **Retype Password** field.

Step 4   In the **Management Network** area, the system suggests the management subnets to be used in the **IPv4 Address** or the **IPv6 Address** fields, depending on the type of addressing defined during the installation. The system checks for constraints defined in the network configuration file and ensures that the IP addresses that are assigned are not in use.

a) Enter the IPv4 Address in the **IPv4 Address** field in a SVO card model.

or

b) Enter the IPv4 or the IPv6 Address in the **IPv4 Address** or **IPv6 Address** field respectively in an external server model.

Step 5   Click **Create**.

Step 6   A message is displayed indicating the creation of the SVO instance.

Step 7   Click **OK**.

The SVO Instances page appears. The table displays the new SVO instance.

The SVO instance can now be accessed through a web browser.

View Details of an SVO Instance

Use this task to view the details of an SVO instance.

Note   This feature simplifies troubleshooting and allows extracting detailed information about the runtime environment of both local and remote SVO instances.

Before you begin

Log into the Cisco SVO Admin Plane, on page 16

Procedure

Step 1	Choose the SVO instance you want to view.
Step 2	Click **Details of SVO Instance**.
	The **SVO Instance Details** page is displayed.
Step 3	Click the heartbeat icon next to the desired instance.
	The **SVO Runtime Status** page is displayed.
Step 4	Expand the related sections to view the details of the SVO instances.
	The sections are NCS Status, HA Agent, and NCS Launcher.
Step 5	Click the hyperlink above the expandable sections to view the details in separate window as plain text.

Edit Reserved Memory of an SVO Instance

Use this task to edit the memory size of the SVO instance.

Before you begin

Log into the Cisco SVO Admin Plane, on page 16

Procedure

Step 1	Choose the SVO instance that you want to edit.
Step 2	Click **Edit SVO Instance**.
	The SVO Instance Edit page is displayed.
Step 3	Choose the memory size to allocate to the SVO instance from the **Reserved Memory GB** field.
Step 4	Click **Edit**.

Switch SVO Instances

Use this task to manually switch between active and standby SVO instances.

Before you begin

Procedure

Step 1   Choose the SVO instance you want to switch.

Step 2   Click **Switch SVO Instances**.

A dialog box is displayed asking for confirmation.

Step 3   Click **Confirm**.

During the switching process, the **App State** field displays different statuses such as SWITCHING, SWITCH_DONE, and UP. The **Role** field displays NONE, ACTIVE, and STANDBY.

Delete an SVO Instance

Use this task to delete an SVO instance.

Before you begin

Procedure

Step 1   Choose the SVO instance you want to delete.

Step 2   Click **Delete SVO Instances**.

A dialog box is displayed asking for confirmation of deletion.

Step 3   Click **Confirm**.

IP Assignment Policy

The IP Assignment Policy page displays two sets of IP addresses:

• Allowed List—Contains a list of available IP addresses.

• Denied List—Contains a list of blocked IP addresses.

The list of allowed and denied IP addresses displayed on this page are stored in two separate files on the file system of the local and remote server.

The IP lists are applicable only to the devices network. During the creation of the SVO instance, the denied list prevents the admin plane from selecting any IP address that is on the list for the IPv4 and IPv6 addresses whereas the allowed list permits the admin plane to select any IP address that is in the list.

The IP list can be modified on this page at runtime.

To view these IP addresses in the admin plane:

Before you begin

Procedure

Step 1   Click **Networks** in the left panel and choose **IP Assignment Policy**.

Step 2   Enter the needed IP addresses in the **Allowed IP addresses list** and **Denied IP addresses list** columns.

Step 3   Click **Apply**.

Note   If conflicting entries exist, the allowed IP address has the precedence.

Restart Admin Plane

Use this task to restart the SVO admin plane.

Before you begin

Procedure

Step 1   Click **Utilities** in the left panel.

The Utilities page appears.

Step 2   Click **Restart Admin Plane**.

All the SVO instances and configurations available on the SVO card are restarted.

A **Warning!** dialog box appears.

Step 3   Click **Confirm**.

Warning   Proceeding with confirmation may interrupt any running procedure.

View and Renew Certificate

Use this task to view and renew the certificates of the admin plane.

Lifetime of self-signed admin plane certificates can be extended by five years. In HA networks, the renewal must be run individually for each admin plane application.

Note The admin plane container must be restarted to renew the certificate. The operation is blocked if any orchestrated operation is running on the admin plane such as SW download.

Before you begin

Procedure

Step 1 Click **Certificates** in the left panel.

The **Certificates** page displays the certificate details.

Step 2 In case of renewal, click **Renew Certificate**.

Download Diagnostic Log Files

Use this task to download the diagnostic log files.

Before you begin

Procedure

Step 1 Click **Diagnostic** in the left panel.

The Diagnostic page appears.

Step 2 Click **Download Log Files**.

A zip file that contains the admin plane logs is downloaded.