Setting Up System Configuration

Default System Configuration on the Cisco ENCS

The diagram below illustrates the default network configuration of Cisco Enterprise NFVIS with the Cisco ENCS.

Figure 1: Default Network Configuration of Cisco Enterprise NFVIS with the Cisco ENCS 5400
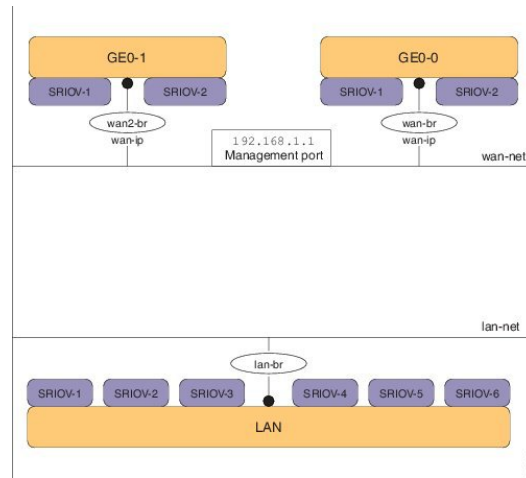
Figure 2: Default Network Configuration of Cisco Enterprise NFVIS with the Cisco ENCS 5100
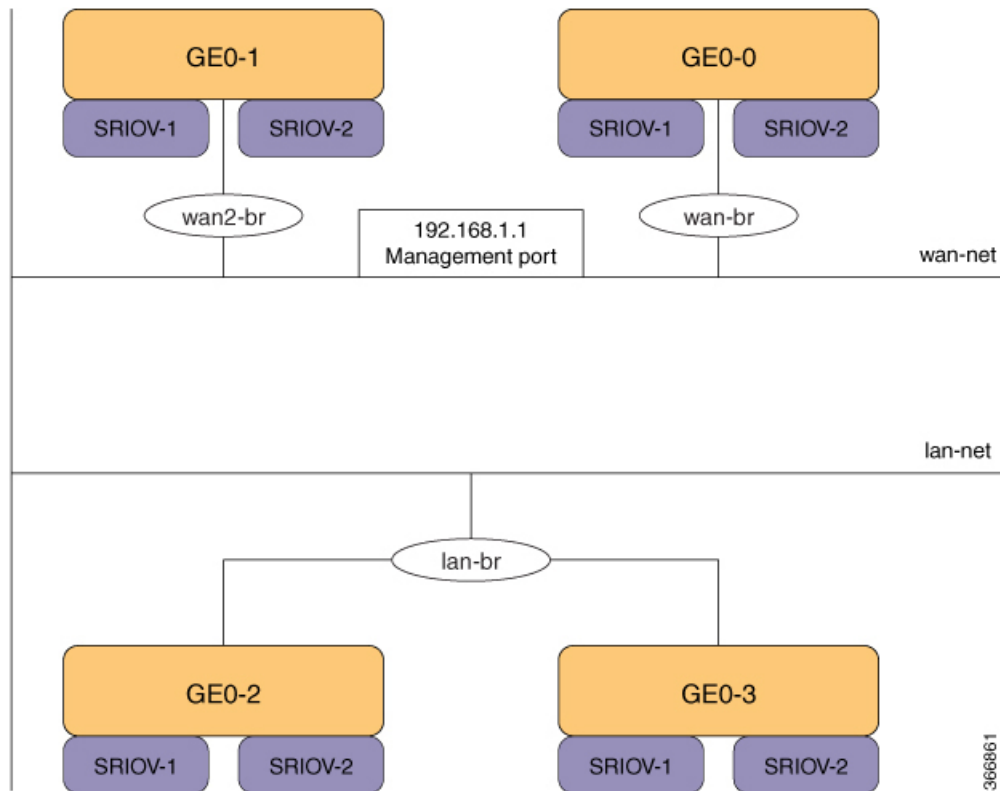
- LAN ports—Eight physical Gigabit Ethernet ports for inbound and outbound traffic.

- WAN port—You can use one of the dual media Ethernet ports (wan-br and wan2-br) for DHCP connection.

- Bridges—They form a Layer 2 domain between virtual network interface controllers (vNICs) of VMs. A vNIC is used by a virtual machine to provide virtual network interfaces by defining a range of MAC addresses. The default management IP address (192.168.1.1) for the NFVIS host is configured on the management port. Multiple VMs can use the same LAN port for local connectivity.

• Network—It is a segment Layer 2 bridge domain where only the specific VLAN traffic is allowed.

• Reserved VLANs in the LAN network on the ENCS 5400 platform—The VLAN range 2350-2449 is reserved for internal use and should not be used on the external switch ports and for virtual machines in the LAN ports". Note that this limitation doesn't apply to the WAN ports.

• Internal 192.168.10.00/24 and 192.168.50.0/24 networks—The IP subnet 192.168.10.0/24 and 192.168.50.0/24 are used for the ENCS-5400 internal networks. A user should not use this IP subnet on the NFVIS management network. In the future NFVIS releases, this internal subnet will be isolated so that users can use this for NFVIS management.

Note The following networks and bridges are automatically configured. You can configure more as required.

• A LAN network (lan-net) and a LAN bridge (lan-br)

• A WAN network (wan-net) and a WAN bridge (wan-br)

wan2-net and wan2-br are the default configurations for ENCS 5400 and ENCS 5100.

The default networks and bridges cannot be deleted.

Default System Configuration on the Cisco UCS C220 M4 Server and Cisco CSP 2100

Configuring the networks in Cisco Enterprise NFVIS allows inbound and outbound traffic and VMs to be service chained. The following diagram illustrates the default network configuration:

Figure 3: Default Network Configuration with Cisco UCS C220 M4 and Cisco CSP 2100
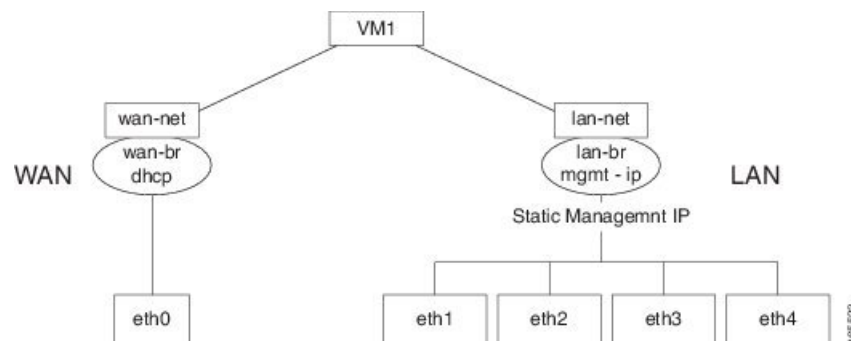
The following networks and bridges are created by default, and cannot be deleted. You can configure more as required.

• A LAN network (lan-net) and a LAN bridge (lan-br)—The default static management IP address (192.168.1.1) for the NFVIS host is configured on the LAN bridge. All other ports for inbound and outbound traffic are associated with the LAN bridge. Any LAN port can be used to access the default static IP address. By default, the hostname is set to "nfvis".

- A WAN network (wan-net) and a WAN bridge (wan-br)—This is created with the "eth0" port, and is configured to enable the DHCP connection.

By default, the first port on the device is associated with the WAN bridge. All the other ports on the device are associated with the LAN bridge.

For more details about the initial setup, see the Installing the Server chapter in the *Cisco UCS C220 M4 Server Installation and Service Guide* or *Cisco Cloud Services Platform 2100 Hardware Installation Guide*.

Default System Configuration on the Cisco UCS E-Series Servers

Figure 4: Default Network Configuration with a Cisco UCS E-Series Server

The following networks and bridges are created by default, and cannot be deleted. You can configure more as required.

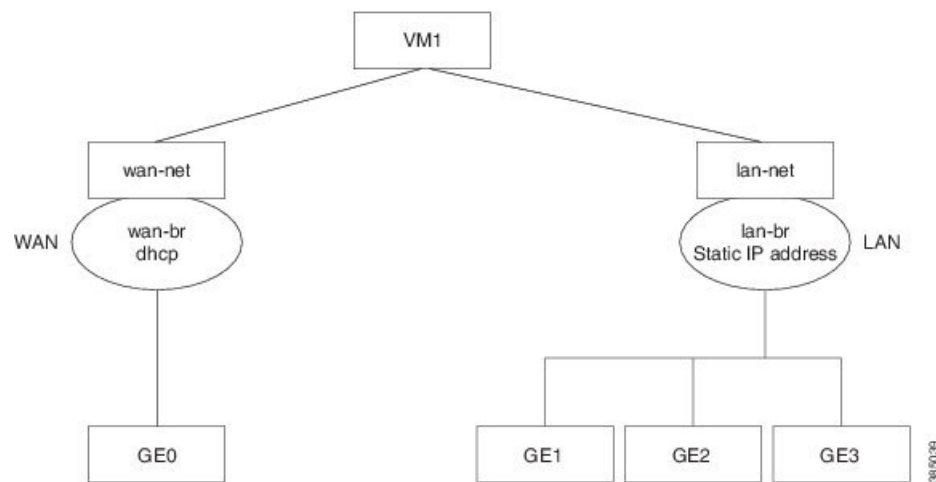- A LAN network (lan-net) and a LAN bridge (lan-br)—The default static management IP address (192.168.1.1) for the NFVIS host is configured on the LAN bridge. All other ports for inbound and outbound traffic are associated with the LAN bridge. By default, the hostname is set to "nfvis".
- A WAN network (wan-net) and a WAN bridge (wan-br)— The physical WAN ports are on the Cisco ISR module. They are not externally available on the Cisco UCS E server. The WAN traffic comes from the ISR WAN ports, and goes through the backplane to the Cisco UCS-E server. The backplane has one internal WAN interface (GE0) to establish connection with the Cisco UCS-E server. By default, the "GE0" interface is enabled for the DHCP connection.

For more details on the initial setup, see the Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine.

Setting Up Initial Configuration

For initial login, use **admin** as the default user name, and **Admin123#** as the default password. Immediately after the initial login, the system prompts you to change the default password. You must set a strong password as per the on-screen instructions to proceed with the application. All other operations are blocked until default password is changed. API will return 401 unauthorized error if the default password is not reset.

If wan-br and wan2-br has not obtained IP addresses through DHCP, the zero touch deployment is terminated. To manually apply the IP configurations answer 'y' and the system proceeds with dhclient on wan-br until the configurations are changed. For dhclient to continue to request IP address for PnP flow on both WAN interfaces answer 'n'.

You must follow the rules to create a strong password:

- Must contain at least one upper case and one lower case letter.

- Must contain at least one number and one special character (# _ - * ?).

- Must contain seven characters or greater. Length should be between 7 and 128 characters.

You can change the default password in three ways:

- Using the Cisco Enterprise NFVIS portal.

- Using the CLI—When you first log into Cisco Enterprise NFVIS through SSH, the system will prompt you to change the password.

- Using PnP (for details, see the Cisco Network Plug-n-Play Support).

- Using console - After the initial login using the default password, you are prompted to change the default password.

```
NFVIS Version: 3.10.0-9

Copyright (c) 2015-2018 by Cisco Systems, Inc.
Cisco, Cisco Systems, and Cisco Systems logo are registered trademarks of Cisco
Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

The copyrights to certain works contained in this software are owned by other
third parties and used and distributed under third party license agreements.
Certain components of this software are licensed under the GNU GPL 2.0, GPL 3.0,
LGPL 2.1, LGPL 3.0 and AGPL 3.0.

nfvis login: console (automatic login)

login:
login:
login:
login:
login: admin

Cisco Network Function Virtualization Infrastructure Software (NFVIS)

NFVIS Version: 3.10.0-9

Copyright (c) 2015-2018 by Cisco Systems, Inc.
Cisco, Cisco Systems, and Cisco Systems logo are registered trademarks of Cisco
Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

The copyrights to certain works contained in this software are owned by other
third parties and used and distributed under third party license agreements.
Certain components of this software are licensed under the GNU GPL 2.0, GPL 3.0,
LGPL 2.1, LGPL 3.0 and AGPL 3.0.

admin@localhost's password:

admin connected from ::1 using ssh on nfvis
nfvis# show version
```

Note To commit the target configuration to the active (running) configuration, use the **commit** command in any configuration mode in Cisco Enterprise NFVIS Release 3.5.1 and later. Changes made during a configuration session are inactive until the **commit** command is entered. By default, the commit operation is pseudo-atomic, meaning that all changes must succeed for the entire commit operation to succeed.

Connecting to the System

Using IPv4

The three interfaces that connect the user to the system are the WAN and WAN2 interfaces and the management interface. By default, the WAN interface has the DHCP configuration and the management interface is configured with the static IP address 192.168.1.1. If the system has a DHCP server connected to the WAN interface, the WAN interface will receive the IP address from this server. You can use this IP address to connect to the system.

You can connect to the server locally (with an Ethernet cable) using the static management IP address; to connect to the box remotely using a static IP address, the default gateway needs to be configured.

You can connect to the system in the following three ways:

- Using the local portal—After the initial login, you are prompted to change the default password.

- Using the KVM console—After the initial login using the default password, you are prompted to change the default password.

- Using PnP—After the initial provisioning through PnP, the configuration file pushed by the PNP server must include the new password for the default user (admin).

Using IPv6

IPv6 can be configured in static, DHCP stateful and Stateless Autoconfiguration (SLAAC) mode. By default, DHCP IPv6 stateful is configured on the WAN interface. If DHCP stateful is not enabled on the network, the router advertisement (RA) flag decides which state the network stays in. If the RA shows Managed (M) flag, then the network stays in DHCP mode, even if there is no DHCP server in the network. If the RA shows Other (O) flag, then the network switches from DHCP server to SLAAC mode.

SLAAC provides ipv6 address and default gateway. Stateless dhcp is enabled in the SLAAC mode. If the server has dns and domain configured, then SLAAC also provides those values via stateless dhcp.

Performing Static Configuration without DHCP

Note Starting from NFVIS 3.10.1 release, for ENCS 5400 and ENCS 5100, wan2-br obtains an IP address from DHCP. To configure default gateway, first use **no bridges bridge wan2-br dhcp** command.

If you want to disable DHCP and use static configuration, initial configuration is done by setting the WAN IP address and/or management IP address, and the default gateway. You can also configure a static IP on a created bridge.

To perform initial configuration on the system without using DHCP:

```
configure terminal
```

```
system settings mgmt ip address 192.168.1.2 255.255.255.0
bridges bridge wan-br ip address 209.165.201.22 255.255.255.0
system settings default-gw 209.165.201.1
commit
```

Note When an interface is configured with a static IP address, DHCP is automatically disabled on that interface.

Now you can either use the management IP or WAN IP to access the portal.

To configure static IPv6 on the WAN interface:

```
configure terminal
system settings mgmt ipv6 address 2001:DB8:1:1::72/64
bridges bridge wan-br ipv6 address 2001:DB8:1:1::75/64
system settings default-gw-ipv6 2001:DB8:1:1::76
commit
```

Note When an interface is configured with a static IPv6 address, DHCP IPv6 is automatically disabled on that interface. There are three options for IPv6 - static, DHCP and SLAAC, out of which only one can be enabled at a time.

Configuring DHCP on the WAN or Management Interface

Note Starting from NFVIS 3.10.1, you can configure DHCP on any bridge. You can only have one DHCP bridge or management interface active at a time, and cannot have DHCP and default gateway configured at the same time.

You can configure DHCP either on the WAN interface or the management interface; you cannot configure DHCP on both the interfaces simultaneously.

To configure DHCP on any one of the interfaces (WAN or management), delete the default gateway.

To configure DHCP on the management interface:

```
configure terminal
no system settings default-gw
system settings mgmt dhcp
commit
exit
hostaction mgmt-dhcp-renew
```

To configure DHCP IPv6 on the management interface:

```
configure terminal
no system settings default-gw-ipv6
system settings mgmt dhcp-ipv6
commit
exit
hostaction mgmt-dhcp-renew
```

To configure DHCP on the WAN interface:

```
configure terminal
no system settings default-gw
system settings wan dhcp
commit
exit
hostaction wan-dhcp-renew
```

Note Starting from NFVIS 3.10.1, you can configure DHCP IPv6 on any bridge. You can only have one DHCP IPv6 bridge or management interface active at a time, and cannot have DHCP IPv6 and default gateway IPv6 or SLAAC IPv6 configured at the same time.

To configure DHCP IPv6 on the WAN interface:

```
configure terminal
no system settings default-gw-ipv6
system settings wan dhcp-ipv6
commit
exit
hostaction wan-dhcp-renew
```

Configuring SLAAC on the WAN or Management Interface

Note Starting from NFVIS 3.10.1, you can configure SLAAC IPv6 on any bridge. You can only have one SLAAC IPv6 bridge or management interface active at a time, and cannot have SLAAC IPv6 and default gateway IPv6 or DHCP IPv6 configured at the same time.

To configure SLAAC IPv6 on the WAN interface:

```
configure terminal
system settings wan slaac-ipv6
commit
```

To configure SLAAC IPv6 on the management interface:

```
configure terminal
system settings mgmt slaac-ipv6
commit
```

Verifying Initial Configuration

The **show system settings-native** command is used to verify initial configuration. Use **show bridge-settings** and **show bridge-settings** *bridge_name* commands to verify the configuration for any bridge on the system.

Extract from the output of the **show system settings-native** command when both WAN and management interfaces have a static configuration:

```
system settings-native mgmt ip-info interface lan-br
system settings-native mgmt ip-info ipv4_address 192.168.1.2
system settings-native mgmt ip-info netmask 255.255.255.0
```

```
!
!
!
system settings-native mgmt dhcp disabled
system settings-native wan ip-info interface wan-br
system settings-native wan ip-info ipv4_address 209.165.201.22
system settings-native wan ip-info netmask 255.255.255.0
!
!
!
system settings-native wan dhcp disabled
!
!
system settings-native gateway ipv4_address 209.165.201.1
system settings-native gateway interface wan-br
```

Extract from the output of the **show system settings-native** command when the management interface has a DHCP configuration and the WAN interface has a static configuration:

```
system settings-native mgmt ip-info interface MGMT
system settings-native mgmt ip-info ipv4_address 192.168.1.2
system settings-native mgmt ip-info netmask 255.255.255.0
!
!
!
system settings-native mgmt dhcp enabled
system settings-native wan ip-info interface wan-br
system settings-native wan ip-info ipv4_address 209.165.201.22
system settings-native wan ip-info netmask 255.255.255.0
!
!
!
system settings-native wan dhcp disabled
```

Extract from the output of the **show system settings-native** command when the WAN interface has a DHCP configuration and the management interface has a static configuration:

```
system settings-native mgmt ip-info interface lan-br
system settings-native mgmt ip-info ipv4_address 209.165.201.2
system settings-native mgmt ip-info netmask 255.255.255.0
!
!
!
system settings-native mgmt dhcp disabled
system settings-native wan ip-info interface wan-br
system settings-native wan ip-info ipv4_address 209.165.201.22
system settings-native wan ip-info netmask 255.255.255.0
!
!
!
system settings-native wan dhcp enabled
```

Related APIs and Commands

APIs	Commands
• /api/operational/system/settings-native • /api/config/system/settings • /api/operational/bridge-settings • /api/config/bridges/bridge/	• system settings hostname • system settings default-gw • system settings mgmt ip address • system settings mgmt dhcp • system settings wan ip address • system settings wan dhcp • hostaction wan-dhcp-renew • hostaction mgmt-dhcp-renew • bridges bridge wan-br ip address • bridges bridge wan-br dhcp • bridges bridge wan2-br ip address • bridges bridge wan2-br dhcp • bridges bridge user-br ip address • bridges bridge user-br dhcp • hostaction bridge-dhcp-renew bridge wan-br • hostaction bridge-dhcp-renew bridge wan2-br • hostaction bridge-dhcp-renew bridge user-br

Configuring VLAN for NFVIS Management Traffic

A VLAN is a method of creating independent logical networks within a physical network. VLAN tagging is the practice of inserting a VLAN ID into a packet header in order to identify which VLAN the packet belongs to.

You can configure a VLAN tag on the WAN bridge (wan-br) interface to isolate Cisco Enterprise NFVIS management traffic from VM traffic. You can also configure VLAN on any bridge on the system (wan2-br for ENCS5400 or ENCS 5100, and user-br for all systems)

By default, Wan bridge and LAN bridge are in trunk mode and allows all VLANs. When you configure native VLAN, you must also configure all the allowed VLANs at the same time. The native VLAN becomes the only allowed VLAN if you do not configure all the VLANs. If you want a network that allows only one VLAN, then create another network on top of wan-net and lan-net and make it access network.

Note   You cannot have the same VLAN configured for the NFVIS management and VM traffc.

For more details on the VLAN configuration, see the Understanding and Configuring VLANs module in the Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide.

To configure a VLAN:

```
configure terminal
bridges bridge wan-br vlan 120
commit
```

Verifying VLAN Configuration

Run the **show bridge-settings wan-br vlan** command to verify the VLAN configuration as shown below:

```
nfvis# show bridge-settings wan-br vlan
bridges bridge wan-br vlan 120
```

VLAN APIs and Commands

VLAN APIs	VLAN Commands
• /api/config/bridges/bridge/wan-br/vlan • /api/config/bridges/bridge/wan2-br/vlan • /api/config/bridges/bridge/user-br/vlan • /api/operational/bridge-settings/bridge/wan-br/vlan • /api/operational/bridge-settings/bridge/wan2-br/vlan • /api/operational/bridge-settings/bridge/user-br/vlan	• bridges bridge wan2-br vlan • bridges bridge user-br vlan • show bridge-settings wan-br vlan • show bridge-settings wan2-br vlan • show bridge-settings user-br vlan • show bridge-settings vlan

Configuring System Routes

In addition to the default routes in the system, you can configure additional system routes. This configuration is specifically useful when certain destinations are not reachable through the default routes.

While you can create a route just by providing the destination and prefix length, a valid route requires that you specify either a device or a gateway or both.

To configure additional system routes:

```
configure terminal
system routes route  209.165.201.1 dev lan-br
commit
```

Verifying the System Routes Configuration

To verify the system routes configuration, use the **show system routes** command as shown below:

```
nfvis# show system routes
DESTINATION   PREFIXLEN   STATUS
--------------------------------
209.165.201.1   12 -
209.165.201.2   12 -
209.165.201.3   24 -
```

System Routes APIs and Commands

System Routes APIs	System Routes Commands
• /api/config/system/routes • /api/config/system/routes/route/<host destination,netmask>	• system routes route • show system routes

User Roles and Authentication

Role based access enables the administrator to manage different levles of access to the system's compute, storage, database, and application services. It uses the access control concepts such as users, groups, and rules, which you can apply to individual API calls. You can also keep a log of all user activities.

Table 1: Supported User Roles and Privileges

User Role	Privilege
Administrators	Owns everything, can perform all tasks including changing of user roles, but cannot delete basic infrastructure. Admin's role cannot be changed; it is always "administrators".
Operators	Start and stop a VM, and view all information
Auditors	Read-only permission

Rules for User Passwords

The user passwords must meet the following requirements:

• Must have at least seven characters length or the minimum required length configured by the admin user.

• Must not have more than 128 characters.

• Must contain a digit.

• Must contain one of the following special characters: hash (#), underscore (_), hyphen (-), asterisk (*), and question mark (?).

• Must contain an uppercase character and a lowercase character.

• Must not be same as last five passwords.

Creating Users and Assigning Roles

The administrator can create users and define user roles as required. You can assign a user to a particular user group. For example, the user "test1" can be added to the user group "administrators".

Note   All user groups are created by the system. You cannot create or modify a user group.

To create a user:

```
configure terminal
rbac authentication users create-user name test1 password Test1_pass role administrators
commit
```

To delete a user:

```
configure terminal
rbac authentication users delete-user name test1
commit
```

Note   To change the password, use the **rbac authentication users user change-password** command in global configuartion mode. To change the user role, use the **rbac authentication users user change-role** command in global configuration mode.

User Management APIs and Commands

User Management APIs	User Management Commands
• /api/operations/rbac/authentication/users /user/<user-name>/change-password • /api/operations/rbac/authentication/users/user /oper/change-role • /api/config/rbac/authentication/users/user?deep	• rbac authentication users • rbac authentication users user change-password • rbac authentication users user change-role

Configuring Minimum Length for Passwords

The admin user can configure the minimum length required for passwords of all users. The minimum length must be between 7 to 128 characters. By default, the minimum length required for passwords is set to 7 characters.

```
configure terminal
rbac authentication min-pwd-length 10
commit
```

Minimum Password Length APIs and Commands

APIs	Commands
/api/config/rbac/authentication/	rbac authentication min-pwd-length

Configuring Password Lifetime

The admin user can configure minimum and maximum lifetime values for passwords of all users and enforce a rule to check these values. The default minimum lifetime value is set to 1 day and the default maximum lifetime value is set to 60 days.

When a minimum lifetime value is configured, the user cannot change the password until the specified number of days have passed. Similarly, when a maximum lifetime value is configured, a user must change the password before the specified number of days pass. If a user does not change the password and the specified number of days have passed, a notification is sent to the user.

Note The minimum and maximum lifetime values and the rule to check for these values are not applied to the admin user.

```
configure terminal
rbac authentication password-lifetime enforce true min-days 2 max-days 30
commit
```

Password Lifetime APIs and Commands

APIs	Commands
/api/config/rbac/authentication/password-lifetime/	rbac authentication password-lifetime

Deactivating Inactive User Accounts

The admin user can configure the number of days after which an unused user account is marked as inactive and enforce a rule to check the configured inactivity period. When marked as inactive, the user cannot login to the system. To allow the user to login to the system, the admin user can activate the user account by using the **rbac authentication users user** *username* **activate** command.

Note The inactivity period and the rule to check the inactivity period are not applied to the admin user.

```
configure terminal
rbac authentication account-inactivity enforce true inactivity-days 2
commit
```

Deactivate Inactive User Accounts APIs and Commands

APIs	Commands
/api/config/rbac/authentication/account-inactivity/	rbac authentication account-inactivity

Activating an Inactive User Account

The admin user can activate the account of an inactive user.

```
configure terminal
rbac authentication users user guest_user activate
commit
```

Activate Inactive User Account APIs and Commands

APIs	Commands
/api/operations/rbac/authentication/users/user/username/activate	rbac authentication users user activate

Certification

Generate Sign-Request

```
nfvis(config)# system certificate signing-request ?

Possible completions:

  common-name            country-code

  locality               organization

  organization-unit-name  state
```

The .csr file will be saved in /data/intdatastore/download/nfvis.csr

Use the scp command to download the file.

Install CA Sign Certificate

After CA sign in, the user needs to use the scp command to upload the file into nfvis.

```
nfvis(config)# system certificate install-cert path file:///<full path of the file>
```

The path needs to start with "file://"

Switch Certificate

```
nfvis(config)# system certificate use-cert cert-type ca-signed
```

nginx process restarts after the switch.

The users cannot access the log files. The log files are added to all the user actions and the user can download and view some of the logs from portal. A notification is generated when the log files reach 75% capacity.

Secure Copy Command

The secure copy (**scp**) command allows only the admin user to secure copy a file from the Cisco NFVIS to an external system or from an external system to Cisco NFVIS. The **scp** command is:

scp *source* *destination*

Note For detailed information about how to use the **scp** command to copy to or from supported locations, see the **scp** section in Cisco Enterprise Network Function Virtualization Infrastructure Software Command Reference.

Examples

The following example copies the sample.txt file from intdatastore to an external system.

```
nfvis# scp intdatastore:sample.txt user@203.0.113.2:/Users/user/Desktop/sample.txt
```

The following example copies the test.txt file from an external system to intdatastore.

```
nfvis# scp user@203.0.113.2:/Users/user/Desktop/test.txt intdatastore:test_file.txt
```

The following example copies the test.txt file from an external system to USB.

```
nfvis# scp user@203.0.113.2:/user/Desktop/my_test.txt usb:usb1/test.txt
```

The following example copies the sample.txt file to an NFS location.

```
nfvis# scp user@203.0.113.2:/user/Desktop/sample.txt nfs:nfs_test/sample.txt
```

The following example copies the sample.txt file from an external system with IPv6 address.

```
nfvis# scp user@[2001:DB8:0:ABCD::1]:/user/Desktop/sample.txt intdatastore:sample.txt
```

The following example copies the nfvis_scp.log file to an external system.

```
nfvis# scp logs:nfvis_scp.log user@203.0.113.2:/Users/user/Desktop/copied_nfvis_scp.log
```

Configuring the IP Receive ACL

To filter out unwanted traffic, you can configure ip-receive-acl to block or allow certain traffic based on the IP address and service ports.

To configure the source network for Access Control List (ACL) access to the management interface:

```
configure terminal
system setting ip-receive-acl 198.0.2.0/24
commit
```

Verifying the Trusted IP Connection

Use the **show running-config system settings ip-receive-ac** command to display the configured source network for ACL access to the management interface

```
nfvis# show running-config system settings ip-receive-ac
system settings ip-receive-acl 198.51.100.11/24
service
[ ssh https scpd]
action accept
priority 100
```

Port 22222 and Management Interface ACL

Management interface ACL provides the Access Control List (ACL) to restrict the traffic through the management interface for setting up different ACL of subnet inside a big subnet. From 3.7.1 release, port 22222 is closed by default on an NFVIS system.

To open port 22222:

```
configure terminal
system settings ip-receive-acl 0.0.0.0/0 service scpd priority 2 action accept
commit
```

Note Priority can be set to any number, as long as there is no other ACL that drops packets from same IP with lower priority number.

Use **no system settings ip-receive-acl** to close port 22222. When an entry is deleted from **ip-receive-acl**, all configurations to that source are deleted since the source IP address is the key. To delete one service, configure other services again.

Note From 3.8.1 release, only an admin user can use the scp command on this port to upload or download only from restricted folders like /data/intdatastore/.

Use the **show running-config system settings ip-receive-acl** command to verify the interface configuration:

```
nfvis# show running-config system settings ip-receive-acl

system settings ip-receive-acl 10.156.0.0/16

 service   [ ssh https scpd ]

 action    accept

 priority 100

!
```

Configuring Your Banner and Message of the Day

Cisco Enterprise NFVIS supports two types of banners: system-defined and user-defined banners. You cannot edit or delete the system-defined banner, which provides copyright information about the application. Banners are displayed on the login page of the portal.

You can post messages using the Message of the Day option. The message is displayed on the portal's home page when you log into the portal.

To configure your banner and message:

```
configure terminal
banner-motd banner "This is a banner" motd "This is the message of the day"
commit
```

Note Currently, you can create banners and messages in English only. You can view the system-defined banner using the **show banner-motd** command. This command does not display the user-defined banner or message.

Banner and Message APIs and Commands

Banner and Message APIs	Banner and Message Commands
• /api/config/banner-motd • /api/operational/banner-motd	• banner-motd • show banner-motd

Setting the System Time Manually or With NTP

You can configure the Cisco Enterprise NFVIS system time manually or synchronise with an external time server using Network Time Protocol (NTP).

To set the system time manually:

```
configure terminal
system set-manual-time 2017-01-01T00:00:00
commit
```

Note NTP is automatically disabled when the time clock is set manually.

To set the system time using NTP IPv4:

```
configure terminal
system time  ntp preferred_server 209.165.201.20 backup_server 1.ntp.esl.cisco.com
commit
```

To set the system time using NTP IPv6:

```
configure terminal
system time  ntp-ipv6 2001:420:30d:201:ffff:ffff:fff4:35
commit
```

Verifying the System Time Configuration

To verify all system time configuration details, use the **show system time** command in privileged EXEC mode as shown below:

```
nfvis# show system time

system time current-time 2017-01-01T17:35:39+00:00

system time current-timezone "UTC (UTC, +0000)"
```

REMOTE	REFID	ST	T	WHEN	POLL	REACH	DELAY	OFFSET	JITTER
*calo-timeserver	.GPS.	1	u	4	64	1	69.423	2749736	0.000

```
* sys.peer and synced, o pps.peer, # selected, + candidate,

- outlyer, . excess, x falseticker, space reject
```

If the NTP server is invalid, it will not be displayed in the table. Also, when an NTP server is queried, if a response is not received before the timeout, the NTP server will also not be displayed in the table.

System Time APIs and Commands

APIs	Commands
• /api/operations/system/set-manual-time • /api/config/system/time/ntp/preferred_server • /api/config/system/time/ntp/backup_server • /api/config/system/time/timezone • /api/operational/system/time?deep	• system time • show system time • system set-manual-time

Enabling or Disabling the Portal Access

The Cisco Enterprise NFVIS portal access is enabled by default. You can disable the access if required.

To disable the portal access:

```
configure terminal
system portal access disabled
commit
```

Note   You can enable the portal access using the **enable** keyword with the **system portal access** command.

Verifying the Portal Access

Use the **show system portal status** command to verify the portal access status as shown below:

```
nfvis# show system portal status
system portal status "access disabled"
```

Portal Access APIs and Commands

Portal Access APIs	Portal Access Commands
• /api/config/system/portal • /api/operational/system/portal/status	• system portal access • show system portal status

Configuring System Logs

You can view system logs for troubleshooting purpose. There are two log types and five log levels. The two log types are configuration and operational.

The INFO and WARNING log levels are set by default respectively for the configuration and operational log types. You can change them as required. However, the change to the log level is not persisted across a reboot. After a reboot, the default log levels are used.

The following table explains the log levels:

Log Level	Purpose
DEBUG	Information, typically of interest only when diagnosing problems.
INFO	Confirmation that things are working as expected.
WARNING	An indication that something unexpected happened, or indicative of some problem in the near future (for example, 'disk space low'). The software application is still working as expected.
ERROR	Due to a serious problem, the software application is not able to perform some function.
CRITICAL	A serious error, indicating that the program itself may not be ble to continue running.

You can configure system logs using the **system set-log** command in global configuration or privileged EXEC mode:

```
system set-log level error logtype configuration
```

Verifying the System Log Configuration

To verify the system log configuration, use the **show system logging-level** command as shown below:

```
nfvis# show system logging-level
system logging-level configuration error
system logging-level operational warning
```

System Log APIs and Commands

System Log APIs	System Log Commands
• /api/operations/system/set-log • /api/operational/system/logging-level	• system set-log logtype [all/configuration/operational] level [critical/debug/error/info/warning] • show system logging-level

Network File System Support

The Network File System (NFS) is an application where the user can view, store and update the files on a remote device. NFS allows the user to mount all or a part of a file system on a server. NFS uses Remote Procedure Calls (RPC) to route requests between the users and servers.

NFS Mount and Unmount

To mount NFS:

```
configure terminal
system storage nfs_storage
nfs
100
10.29.173.131
/export/vm/amol
commit
```

To unmount NFS use **no system storage nfs_storage** command.

Image Registration on NFS

Images in tar.gz, ISO and qcow2 format, remote images and images on mounted NFS can be registered on NFS.

To register tar.gz images on NFS:

```
configure terminal
vm_lifecycle images image myas10 src file:///data/mount/nfs_storage/repository/asav961.tar.gz
properties property placement value nfs_storage
commit
```

Similar configuration can be used for the various images formats.

To unregister an image from NFS use **no vm_lifecycle images** command.

Deploy VM on NFS

To deploy a VM on NFS, under deployment vm group use **placement type zone_host host nfs_storage** command.

Secure Boot of host

✎

Note This feature is supported only on ENCS 5400. Upgrade BIOS to version 2.6 for this feature. The secure boot feature is only available for release 3.9.1 fresh install.

The secure boot feature prevents malicious software applications and unauthorized operating systems from loading into the system during the system start up process. If secure boot feature is enabled, only the authorized software applications boots up from the device. Each device has keys that allow software with the correct signature to boot up on the device.

This feature ensures that the software applications that boot up on the device are certified by Cisco. The NFVIS 3.9.1 image is signed with Cisco key. If secure boot is enabled the signature is verified during the device boot up. If the verification fails, the image does not boot up.

Secure boot is disabled by default and to enable it you must change firmware configurations from CIMC. Secure boot needs to boot from a separate UEFI partition.

To enable secure boot:

1. Get into CIMC and use **show bios detail** command to view the BIOS version.

```
ENCS# scope bios
ENCS/bios # show detail
BIOS:
    BIOS Version: " ENCS54_2.6 (Build Date: 07/12/2018)"
    Boot Order: EFI
    FW Update/Recovery Status: Done, OK
    Active BIOS on next reboot: main
    UEFI Secure Boot: disabled
ENCS/bios #
```

2. enable secure boot.

```
ENCS/bios # set secure-boot enable
Setting Value : enable
Commit Pending.
ENCS/bios *# commit
ENCS/bios # show detail
BIOS:
    BIOS Version: "ENCS54_2.6 (Build Date: 07/12/2018)"
    Boot Order: EFI
    FW Update/Recovery Status: None, OK
    Active BIOS on next reboot: main
    UEFI Secure Boot: enabled
ENCS/bios #
```

Legacy boot, UEFI boot and UEFI secure boot are the three boot modes. Secure boot can only be used on a disk that has UEFI partition.

You can configure boot order from CIMC command or portal or from BIOS setup menu. With CIMC you can only configure legacy boot order. BootOrderRules are by default set to Strict and so boot order follows the CIMC configuration. Since CIMC cannot be used to configure UEFI boot order, the BootOrderRules setting must be changed to Loose when secure boot is enabled.

If BootOrderRules is set to Loose, the boot order will follow the BIOS setup menu. When an operating system is installed in secure boot mode, the new UEFI boot option for the OS automatically appears at the top of the BIOS menu boot order list, to boot the installed operating system.

To set BootOrderRule to Loose:

```
ENCS/bios # scope advanced
ENCS/bios/advanced # set BootOrderRules Loose
ENCS/bios/advanced *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N]y
```

CIMC Control

On ENCS 5400, NFVIS administrators have authoritative control of the device. This includes capability to change the IP address used to reach the CIMC and modifying the CIMC and BIOS passwords

CIMC Access using NFVIS

Note CIMC access using NFVIS is supported only on ENCS 5400.

When CIMC access is enabled on NFVIS, there is a potential risk of unauthorized ISRv to gain access to the host CIMC and switch management console. You must have authorization from CID or Consent token to gain root access.

To access CIMC using NFVIS WAN or management interface IP address, use the **system settings cimc-access enable** command. Once you configure CIMC access on NFVIS, the stand alone CIMC access using CIMC IP address is disabled and you will be able to access CIMC using NFVIS management interface IP address. The configurations remain on the device even after the device reboot.

When the CIMC access is configured, it enables a few ports to access services like SSH, SNMP, HTTP and HTTPs into the CIMC.

The following port numbers are being used for forwarding services to CIMC:

- 20226 for SNMP
- 20227 for SSH
- 20228 for HTTP
- 20229 for HTTPS

If you are unable to access CIMC using NFVIS, check the show log nfvis_config.log file.

Use **system settings cimc-access disable** to disable this feature.

BIOS-CIMC Update

Starting from 3.8.1 release, for ENCS 5400 router, if existing BIOS/CIMC version is lower than the bundled image in 3.8.1 NFVIS package, it is updated automatically during the NFVIS upgrade or installation. Also the CPU microcode is upgraded. The upgrade time takes longer than the previous releases and the upgrade will be done automatically, and you cannot stop the process once it is initiated.

For ENCS 5100 router, BIOS will be upgraded automatically to a new version but you need to boot up the server manually after the upgrade.

NFVIS Password Recovery

1. Load the NFVIS 3.9.1 image, using the CIMC KVM console.

2. Select Troubleshooting from the Boot Selection menu.

3. Select Rescue a NFVIS Password.

4. Select Continue.

5. Press Return to get a shell.

6. Run the **chroot /mnt/sysimage** command.

7. Run the **./nfvis_password_reset** command to reset the password to admin.

8. Confirm the change in password and enter Exit twice.

   Remove the CD-ROM and reboot NFVIS.

9. Login to NFVIS with the default credentials admin/Admin123#.

   After login to NFVIS, enter a new password at prompt.

10. Connect to NFVIS with the new password.

Note   You can update and recover NFVIS 3.8.1 and older passwords using NFVIS 3.9.1.

DPDK Support on NFVIS

The Data Plane Development Kit (DPDK) is a set of data plane libraries and network interface controller drivers for fast packet processing.

DPDK Support for NFVIS 3.10.x

DPDK support is enabled only on ENCS 5400 from NFVIS 3.10.1 release. To enable DPDK use **system settings dpdk enable** command. Once DPDK is enabled it cannot be disabled. You can use **factory-default-reset all-except-images-connectivity** to disable DPDK.

To enable DPDK support:

```
configure terminal
system settings dpdk enable
commit
```

DPDK can be enabled if:

- No VMs are deployed.

- There are no other bridges created other than the default bridge which is wan-br, wan2-br or lan-br.

- The default bridges are not modified.

DPDK mode is enabled on a bridge, if the bridge is created as part of a network or bridge api without any NIC ports. NIC ports can also be added later to the bridge, if no VMs are deployed on the network associated to the bridge. If a NIC port is added to the bridge, the bridge will switch to non-dpdk mode. Once a bridge enters non-dpdk mode, it will not switch back to DPDK mode again. NFVIS supports DPDK for the interface with virtio driver only.

Note NFVIS 3.10.x release does not support **tcpdump packetcapture** command on DPDK enabled bridge.

If DPDK is enabled, all VMs deployed will have DPDK and HugePage support. The default hugepage size is 2MB. After DPDK is enabled the system reserves 512 hugepages for Openvswitch operations. Hugepages for VM are allocated dynamically. If the system is not able to allocate HugePages for a newly deployed VM, the VM will boot up in error state. Memory Fragmentation is the main reason why HugePage allocation fails. In this case a reboot can help solve the issue.

Note DPDK support is only enabled on the bridges without NIC ports.

For a system without Hyper-threading one additional core is reserved by the system and for a system with Hyper-threading two additional logical cores are reserved by the system.

NFVIS does not support changing Hyper-thread option such as disabling after DPDK is enabled with Hyper-thread. The system can be unstable if you change Hyper-thread setting after DPDK is enabled.

DPDK VM Migration for NFVIS 3.11.x

Enhancements to DPDK Support in NFVIS 3.12.x

Service Bridge DPDK Support for New Platforms

Starting from NFVIS 3.12.1 DPDK support is added for service bridges on UCS-C M5, UCS-E M3 and CSP 5000 series. Only the service bridge is supported and the default wan bridge and lan bridge do not support DPDK feature. DPDK is supported on service bridge with or without any pnic. The configuration for service bridge without any pnic is the same as ENCS platform on NFVIS 3.11.1 release, all service bridges will become dpdk-capable after DPDK is enabled. NFVIS system does not require reboot after DPDK is enabled.

DPDK and SR-IOV cannot co-exist on the pnic used for DPDK-capable bridge. The configuration for service bridge with pnic is as followed:

1. (Optional) If pnic ethX-Y is still attached to lan-br, remove it from lan-br.

```
configure terminal
bridges bridge lan-br
no port ethX-Y
commit
```

2. Remove SR-IOV networks associated with ethX-Y (usually ethX-Y-SRIOV-*).

```
configure terminal
no networks network ethX-Y-SRIOV-1
no networks network ethX-Y-SRIOV-2
...
commit
```

3. Disable ethX-Y SRIOV configuration.

```
configure terminal
pnic ethX-Y
no sriov
nnumvf 0
commit
```

4. Create service bridge with port ethX-Y.

```
configure terminal
bridges bridge service-br port ethX-Y
networks network service-net bridge service-br
commit
```

5. Enable system-wide DPDK setting.

```
configure terminal
system settings dpdk enable
commit
```

Note

- You can also enable DPDK before creating service bridge with port ethX-Y.

- Except ENCS 5400 platform, all default bridges (lan-br, wan-br, wan-br2) does not enter DPDK-mode after DPDK is enabled system-wide.

- If you do not remove SR-IOV configuration from pnic ethX-Y, and ethX-Y is a port of service bridge, this service bridge cannot enter DPDK-mode after DPDK is enabled system-wide. If you have to use pnic ethX-Y in DPDK bridge, after removing SR-IOV configuration from ethX-Y, delete old bridge and create new bridge and attach ethX-Y to the new bridge.

Migration for VMs with PNIC associated to DPDK bridge

If DPDK is enabled, all VMs deployed will have DPDK and HugePage support. The default hugepage size is 2MB. After DPDK is enabled, the system will reserve additional 512~2048 contiguous hugepages for DPDK operations. Though hugepages for VM are allocated dynamically, it will cause memory fragmentation and the main reason DPDK enabling process will fail. In this case, a system reboot might help to solve the issue.

If system can find enough hugepages for DPDK process, not only service bridges will enter DPDK-mode, all VMs' vnic attached to those bridges will be migrated from virtio to dpdk type (dpdkvhostuserclient):

```
nfvis# support ovs vsctl show | begin service-br
    Bridge service-br
        Port "vnic2"
            Interface "vnic2"
                type: dpdkvhostuserclient
                options: {vhost-server-path="/run/vhostfd/vnic2"}
        Port service-br
            Interface service-br
                type: internal

nfvis# support virsh dumpxml ROUTER | begin interface | until serial
    <interface type='network'>
      <mac address='52:54:00:ae:14:57'/>
      <source network='wan-net'/>
      <target dev='vnic1'/>
      <model type='virtio'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
    </interface>
    <interface type='vhostuser'>
      <mac address='52:54:00:3d:ee:1a'/>
      <source type='unix' path='/run/vhostfd/vnic2' mode='server'/>
      <target dev='vnic2'/>
      <model type='virtio'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
    </interface>
```

DPDK and Factory Reset

The three commonly-used factory reset configurations disable DPDK.

Factory-default-reset configuration	DPDK enabled	Networks kept	Deployment deleted	Registered image deleted
all	No	No	Yes	Yes
all-except-images	No	No	Yes	No
all-except-images -connectivity	No	Yes	Yes	No

Frequently Seen Failures

- Error when DPDK is enabled.

    - When enabling DPDK, lack of system memory results in an error. Ensure that you have 4 GB contiguous HugePages to enable DPDK. You can also reboot the system.

    - DPDK requires one physical core from each socket. A multi-sockets system (like UCS-C or CSP) can encounter deployments that occupy all cores on one socket and DPDK can fail to enable. Power-off some VM (resource-locking VMs likes ISRv/ASAv/vWAAS) and enable VM after DPDK is enabled successfully.

- If the system is not able to allocate HugePages for a newly deployed VM, the VM will boot up in error state.

Import and Export NFVIS VM

Starting from NFVIS 3.10.1 release, you can backup or export (vmExportAction) and restore or import (vmImportAction) VMs. To backup or restore the whole NFVIS system, refer Backup and Restore NFVIS and VM Configurations.

VM Export and Import Limitations

- The imported VM cannot change datastore.

- The original registered image must exist.

- The OVS network name must be identical to the one used by original deployment.

- NFVIS does not check the disk space before exporting or importing a VM.

- The VM has larger disk footprint compared to original deployment after exporting or importing.

To export a VM ensure that:

- VM is in powered off state.

- Backup file is saved in any NFVIS datastores or USB.

- Provide a backup name for NFVIS to append .vmbkp extension to the backup name.

You can only create and save a VM backup to datastores. The backup file has .bkup extension. To verify the backup:

```
nfvis# show system file-list disk local | display xpath | include backup

/system/file-list/disk/local[si-no='84']/name tiny_backup.vmbkp
nfvis# show system file-list disk local 84
SI NO  NAME                PATH            SIZE  TYPE               DATE MODIFIED
--------------------------------------------------------------------------------------
84     tiny_backup.vmbkp  /mnt/extdatastore1  17M   VM Backup Package  2019-01-31 19:31:32
```

To import a VM ensure that:

- The Backup file is placed under NFVIS datastores or USB.

- The registered image used by the original deployed VM is in the same datastore, with same properties.

- The Original deployed VM does not exist on the system.

- OVS network used by the original deployment should exist.

- Restored VM is created with the same datastore with same deployment properties.

- The full path name to backup file is used (for example, /mnt/extdatastore1/backup.vmbkp, not extdatastore1:backup)

```
nfvis# vmImportAction importPath /mnt/extdatastore1/tiny_backup.vmbkp
System message at 2019-01-31 19:53:32...
```

```
Commit performed by admin via ssh using maapi.
```

The following examples show export failures:

- Original deployment is not deleted

```
nfvis# vmImportAction importPath /mnt/extdatastore1/tiny_backup.vmbkp
Error: Exception from action callback: Deployment Configuration :
'SystemAdminTenantIdtiny' already exists , can not be imported/restored due to conflict!
```

- 2. OVS network used by original deployment is deleted.

```
nfvis# vmImportAction importPath /mnt/extdatastore1/tiny_backup.vmbkp
Error: Exception from action callback: Restoration Request rejected, see logs for root
 cause
```

Backup and Restore NFVIS and VM Configurations

Starting from NFVIS 3.10.1 release, you can backup and restore NFVIS configurations and VMs. You can also restore a backup from one NFVIS device to another if they are running on the same version of NFVIS and have the same platform.

Note To backup or restore a single VM, use vmImportAction and vmBackupAction APIs.

To backup and save NFVIS and all VM configurations use configuration-only option. To backup and save VM disks, NFVIS and VM configurations use configuration-and-vms option.

You can only create a backup to datastore or uploads directory. The backup file has *.bkup* extension.

The following examples shows the backup options:

```
nfvis# hostaction backup configuration-and-vms file-path intdatastore:sample.bkup
```

```
nfvis# hostaction backup configuration-only file-path extdatastore2:sample-dir/sample.bkup
```

The following example shows the backup stored on a USB:

```
nfvis# hostaction backup configuration-only file-path usb:usb1/sample.bkup
```

Use **hostaction backup force-stop** command to stop the running backup.

To restore a previous backup on same NFVIS setup or on a new NFVIS setup use except-connectivity option which preserves connectivity of the NFVIS and restores everything else from backup.

```
nfvis# hostaction restore file-path intdatastore:sample.bkup
```

The following example shows how to restore a backup on a different NFVIS device:

```
nfvis# hostaction restore except-connectivity file-path extdatastore2:sample-dir/sample.bkup
```

Backup, Restore and Factory-Default-Reset

To restore the system after factory-default-reset using backup or restore, check:

- Backup file location:

    - The system backup bundle is saved under */datastore/uploads/* by default.

    - Factory-default-reset cleans up all files under */datastore/uploads/*, but leave files under */datastore/* intact.

    - To restore the system from backup bundle after factory-default-reset, if the backup bundle is saved on any other location, the minimum requirement is to have a connection to the NFVIS to upload the backup bundle.

- VM restoration if system backup contains VM backups:

    - VM restoration requires the original image or template registered in NFVIS.

    - Factory-default-reset all clean ups all registered images and uploaded files. You need to configure minimum setup, like host connection and upload registered images to the same datastore.

To save backup bundle from factory-default-reset:

- Save the backup bundle in remote locations. Then restore the connectivity and upload the backup bundle after reset.

- Save backup bundle in local */datastore/* and not in */datastore/uploads/*:

```
# Backup & Restore on the same NFVIS box without NFS & USB
# [[ BACKUP ]]
# before executing factory-default-reset

nfvis# nfvis# hostaction backup configuration-only file-path
extdatastore1:configBackup-01.bkup
nfvis# system file-copy source /mnt/extdatastore1/uploads/configBackup-01.bkup destination
 /mnt/extdatastore2/

# after factory-default-reset all-except-images or all-except-images-connnectivity,
# file /mnt/extdatastore1/uploads/configBackup-01.bkup will be deleted
# but /mnt/extdatastore2/configBackup-01.bkup won't.

# [[RESTORE]]
# after NFVIS rebooted and login to console, copy file to uploads/ directory

nfvis# system file-copy source /mnt/extdatastore2/configBackup-01.bkup destination
/mnt/extdatastore2/uploads/
nfvis# hostaction restore file-path extdatastore2:configBackup-01.bkup
```

For VM restoration:

- Use all-except-images and all-except-images-connectivity to keep registered images intact.

- Save the configurations of existing image registrations before running factory-default-reset all. Save the customized flavors or profiles if you have them which can be used as reference after factory-default-reset all.

Dynamic SR-IOV

Dynamic SR-IOV allows you to enable or disable SR-IOV on a Physical Network Interface Controller (PNIC). You can disable SR-IOV on any PNIC to 0 and enable SR-IOV by setting a value between 1 to maximum virtual functions (maxvfs) supported on PNICs. You can also create and delete SR-IOV networks based on the number of virtual functions (numvfs) set on that PNIC while enabling SR-IOV. Existing fresh installation behavior has not changed. Each PNIC has default number of VFs created and Default SRIOV networks are created. User can use CLI, API or GUI to Enable/Disable SR-IOV on a PNIC or to Create/Delete SR-IOV networks

Restrictions or Limitations

- The supported platforms are CSP-2100, CSP-5000, UCSc-C220-M5X and UCS-E-M3.

- Dynamic SR-IOV is not supported on certain PNICs:

  - PNIC with driver i40e

  - PNIC that does not support SRIOV

- Only switch mode VEB is supported for NFVIS 3.12.1 release.

- Resizing the number of virtual functions is not supported. SR-IOV should be disabled and then enabled with desired number of virtual functions.

Disable SR-IOV on a PNIC

All SR-IOV networks for a PNIC must be deleted. PNIC should not be attached to a bridge.

```
configure terminal
no pnic eth0-1 sriov
commit
```

Enable SR-IOV on a PNIC

To enable SR-IOV on a PNIC, it has to support SR-IOV, numvfs field should be less than maximum supported VFs (maxvfs) on a PNIC and PNIC should not be attached to a bridge.

```
configure terminal
pnic eth0-1 sriov numvfs 20
commit
```

To display SR-IOV state of all PNICs use **show pnic sriov** command. To display SR-IOV state of individual PNIC use **show pnic eth0-1 sriov** command.

Creation of SR-IOV Networks

To create SR-IOV networks, PNIC must have SRIOV enabled and configured with numvfs. The SRIOV network name must have the following format: <pnic_name>-SRIOV-<num> with <pnic_name> as a valid PNIC name and <num> must be greater than 0 and less than numvfs.

To create SR-IOV network in trunk mode:

```
configure terminal
networks network eth0-1-SRIOV-1 sriov true
commit
```

To create SR-IOV network in access mode:

```
configure terminal
networks network eth0-1-SRIOV-1 sriov true trunk false vlan 30
commit
```

Delete SR-IOV Networks

To delete SR-IOV networks VM should not be attached to the network.

```
configure terminal
no networks network eth0-1-SRIOV-1
commit
```

To verify the system networks use **show system networks** command.