

NFVIS host management

Objective

The NFVIS host system provides a set of commands to manage power states, maintain file systems, and perform secure data transfers. These operations are performed directly on the NFVIS host to ensure system stability and efficient data management.

- Power management, on page 1
- Secure copy, on page 2
- Reset factory default, on page 3
- Banner and message-of-the-day, on page 4
- Set the system time manually or configure NTP, on page 5
- Back up and restore VMs before an NFVIS factory reset, on page 6
- NFVIS backup and restore restrictions, on page 6
- NFVIS backup and restore behavior, on page 7
- NFVIS factory reset data retention, on page 11

Power management

Objective

Use these commands to control the power state of the NFVIS host. A notification and syslog entry are generated for each operation to indicate that the action was performed.

Power management

Action	Command
Power cycle the system	`nfvis# hostaction powercycle`
Reboot the system	`nfvis# hostaction reboot`
Shut down the system	`nfvis# hostaction shutdown`

Secure copy

Objective

The secure copy (`scp`) command allows only the admin user to securely copy files from NFVIS to an external system, or from an external system to NFVIS. For example, this command can be used to copy an upgrade package to NFVIS.

SCP syntax and usage notes

Syntax: **scp***sourcedestination*

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

SCP between two NFVIS devices is not supported.

Examples

Objective

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

SCP file transfer examples

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

The following example shows how to secure copy from techsupport as source:

```
nfvis# scp logs:nfvis_techsupport.tar.gz user@203.0.113.2:/Users/user/Desktop/copie
```

Reset factory default

Procedure

Reset factory default.

Factory default reset allows you to restore the host server to its original configuration state for troubleshooting purposes.

Factory default reset is available on all NFVIS supported hardware platforms. You can reset the host server to factory default with three different options that provide varying levels of data preservation.

Before you begin

Contact Cisco Technical Support before performing factory default reset.

Follow these steps to reset to factory default:

Reset NFVIS to factory default

The system resets to factory default configuration based on the selected option and reboots successfully.

Procedure

Step 1 Choose the appropriate factory default reset option based on your requirements.

Table 1: Factory default reset options

Option	Description
Reset all	Deletes VMs and volumes, files including logs, images, and certificates. Erases all configuration. Connectivity will be lost, and the admin password will be changed to factory default password.
Reset all-except-images	Delete VMs and volumes, files including logs, user uploaded files and certificates. Erases all configuration except registered images. Connectivity will be lost, and the admin password will be changed to factory default password.
Reset all-except-images-connectivity	Deletes VMs and volumes, files including logs and certificates. Erases all configuration except images, network, and connectivity.

Note Factory default reset must be used only for troubleshooting purpose. We recommend you contact Cisco Technical Support before performing factory default reset. This feature will reboot the system. Do not perform any operations until the system reboots successfully.

Step 2 Enter the factory default reset command with your chosen option.

Example:

```
nfvis#factory-default-resetall|all-except-images|all-except-images-connectivity
```

Step 3 Enter Yes when prompted with the factory default warning message or no to cancel.

The system resets to factory default configuration based on the selected option and reboots successfully.

Banner and message-of-the-day

Objective

Configure custom banners and messages to provide information to users when they access the Cisco NFVIS portal.

Banner types and messages of the day

Cisco 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.

Configure the banner and message of the day

Procedure

Enter global configuration mode and configure the banner and message.

```
nfvis# configure terminal
nfvis# banner-motd banner "This is a banner" motd "This is the message of the day"
nfvis# 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.

The custom banner is displayed on the login page and the message of the day appears on the portal's home page after users log in.

Set the system time manually or configure NTP

Procedure

Step 1 Set the system time manually.

This task allows you to configure the system time on Cisco NFVIS either manually or by synchronizing with an external NTP server to ensure accurate timekeeping.

Accurate system time is essential for logging, security, and synchronization with other network devices. You can set the time manually for isolated systems or use NTP for automatic synchronization with time servers.

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

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

Step 2 Set the system time using NTP IPv4.

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

Step 3 Verify the system time configuration using the show system time command in privileged EXEC mode.

```
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 is not displayed in the table.

The system time is configured either manually or synchronized with NTP servers. The verification command displays the current time configuration and NTP server status.

Back up and restore VMs before an NFVIS factory reset

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.

Note To backup and restore a single VM, use **vmExportAction** (for VM backup) and **vmImportAction** (for VM restore) APIs.

To avoid losing VMs during a host restore because of insufficient disk space, complete these steps.

Procedure

Step 1 Stop the VMs that are associated with Cisco NFVIS.

Step 2 Perform individual image backups of the VMs using the **vmExportAction** command.

Step 3 After the backups succeed, delete the VMs and their images from Cisco NFVIS.

Step 4 After deleting the VMs and images, perform a host-level backup with the configuration-only option by using **hostaction backup configuration-only file-path** *extdatastore2:sample-dir/sample* .

Step 5 Copy the backup files to a file server.

Step 6 Perform a factory reset by using the **factory-default-reset** command.

Step 7 Copy the backup from the file server to NFVIS, and restore the host-level backup file by using **hostaction restore file-path** *extdatastore2:sample-dir/sample.bkup* .

Step 8 If the restore fails because of disk storage issues, restore the configuration-only backup. After the restore succeeds, restore the VMs and their images by using **vmImportAction importPath** */mnt/extdatastore1/tiny_backup.vmbkp* .

NFVIS backup and restore restrictions

Observe these restrictions when you back up or restore NFVIS:

- The backup includes all deployed VMs and the registered images except uploaded files.
- VM restore using **hostaction restore** and **vmImportAction** requires original registered image to be on the system, on the same datastore. Missing registered image or image registered in a different datastore results in VM restore failure.
- The time required to back up a VM depends on the selected backup option.
- You can either backup all the VMs or none.

- The final backup is a compressed file which requires temporary disk space to create the VM backup file. If the system has only one datastore, the maximum deployment backups in a single file is around one-third to half of the datastore disk space. If the deployments occupies more disk space, use **vmExportAction** to backup an individual VM instead of relying on host backup for all VM deployments.
- NFVIS only supports backup or restore on the same release.

NFVIS backup and restore behavior

Objective

This reference describes how NFVIS backup and restore options affect configurations, VMs, and images.

Backup commands and status

The following examples shows backup options and status:

```
nfvis# hostaction backup configuration-and-vms file-path intdatastore:sample
nfvis# hostaction backup configuration-only file-path extdatastore2:sample-dir/sample
nfvis# show hostaction backup status
hostaction backup status 2020-07-16T07:02:44-00:00
destination intdatastore:backup_20200704.bkup
status      BACKUP-SUCCESS
size        "2798.0 MB"
components FIREWALL
  status      BACKUP-SUCCESS
  last update 2020-07-16T07:07:38-00:00
  size        "20.49 MB"
  details     ""
components Linux
  status      BACKUP-SUCCESS
  last update 2020-07-16T07:07:36-00:00
  size        "0.01 MB"
  details     ""
components NFS
  status      BACKUP-SUCCESS
  last update 2020-07-16T07:06:44-00:00
  size        "0.01 MB"
```

```
  details     ""
components NFVIS
  status      BACKUP-SUCCESS
  last update 2020-07-16T07:02:48-00:00
  size        "0.72 MB"
  details     ""
components ROUTER
  status      BACKUP-SUCCESS
  last update 2020-07-16T07:07:35-00:00
  size        "579.89 MB"
  details     ""
components VM_Images_Flavors
  status      BACKUP-SUCCESS
  last update 2020-07-16T07:06:45-00:00
  size        "2197.73 MB"
  details     ""
```

Restore options and outcomes

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

The restore is based on the system condition created during backup.

Condition	Restore configuration-only	Restore configuration-and-vms
Restore system configurations	Yes	Yes
Restore upgrade configurations	yes, requires same upgrade files in system if the host backup was taken has such upgrade files. No, if host where backup was taken did not have any upgrade files registered. Restore will fail.	Yes, requires same upgrade files in system if the host backup was taken has such upgrade files. No, if host where backup was taken did not have any upgrade files registered. Restore will fail.

Condition	Restore configuration-only	Restore configuration-and-vms
Restore registered images and flavors	Yes, if images sources are still available (URL link is still valid, or uploaded files are still in the same locations). No, if images sources are not available (URL link is invalid, upload files are deleted or moved to new location). The restore process will fail.	Yes, restore from backup file.
Restore deployments	No	Yes, restore from backup file.

Note This means if there are upgrade files registered in the NFVIS. The backup create on this host will contain those information. If using this backup on new host or same host after factory-default-reset, the restore will fail.

Condition	dpdk-disabled while backup	dpdk-enable while backup
dpdk-disabled while restore	Yes (system is dpdk-disabled)	Yes (system will beconverted to dpdk enabled, and VM vnic will be convereted inf needed)
dpdk-enabled while restore	No support	Yes (system is dpdk-enabled)

Note In **hostaction restore** process, the full file name (with .bkup extension) is required in the CLI.

```
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
```

Use the **show hostaction restore-status** command to view the status of the overall restore process and each components like system, image and flavors, vm and so on.

The following is an example of the show command output after the restore process is complete:

```
nfvis# show hostaction restore-status

hostaction restore-status 2020-07-16T07:18:54-00:00

source intdatastore:backup_20200704.bkup

status RESTORE-SUCCESS

components FIREWALL.vmbkp
```

```
  status      RESTORE-SUCCESS
  last update 2020-07-16T07:26:34-00:00
  details     ""
components Linux.vmbkp
  status      RESTORE-SUCCESS
  last update 2020-07-16T07:26:03-00:00
  details     ""
components NFS.vmbkp
  status      RESTORE-SUCCESS
  last update 2020-07-16T07:25:36-00:00
  details     ""
components NFVIS
  status      RESTORE-SUCCESS
  last update 2020-07-16T07:22:03-00:00
  details     ""
components ROUTER.vmbkp
  status      RESTORE-SUCCESS
  last update 2020-07-16T07:26:55-00:00
  details     ""
components VM_Images_Flavors
  status      RESTORE-SUCCESS
  last update 2020-07-16T07:26:01-00:00
  details     ""
components intdatastore:backup_20200704.bkup
  status      VERIFICATION-SUCCESS
  last update 2020-07-16T07:18:54-00:00
  details     ""
```

You can backup registered images and flavors into backup package and restore these images and flavors into the system. The new system does not require a pre-registered image before system restore. If the system has existing images, flavors or deployments, the system restore erases them all and restores from its own backup.

NFVIS factory reset data retention

Objective

This reference lists data retained or deleted by each NFVIS factory-default-reset option.

Backup, restore, and factory-default-reset

You can copy backup file to intdatastore/ if there is sufficient storage space. If the backup is larger than free disk space in intdatastore/, you can copy to a remote server like scp or NFVIS web portal.

The following table lists the data erased and retained upon using NFVIS factory default reset options:

Data	factory-default-reset all	factory-default-reset all-except-images	factory-default-reset all-except-images-connectivity
files under intdatastore	Retain	Retain	Retain
files under intdatastore/uploads/	Delete	Delete	Delete
files under extdatastore${1,2}	Delete	Retain	Retain
files under extdatastore${1,2}/uploads/	Delete	Delete	Delete
files under USB	Retain	Retain	Retain
files under NFS mounted datastore	Retain	Retain	Retain
Deployments	Delete	Delete	Delete
Registered Images and Flavors	Delete	Retain	Retain

Failure to restore

NFVIS configurations fail to restore if there is no sufficient disk space. Restore requires temporary disk space to save un-compressed files. You can move, copy or upload the backup file to a larger datastore and run system restore.

```
nfvis# show hostaction restore-status

    hostaction restore-status 2020-07-16T21:29:08-00:00

    source intdatastore:encs07-configVms-dpdk-2020-07101600.bkup

    status RESTORE-ERROR

    components intdatastore:encs07-configVms-dpdk-2020-07101600.bkup

      status      VERIFICATION-ERROR
```

```
last update 2020-07-16T21:49:18-00:00

details     "Backup package could not be inflated. No space left on device"
```

The application communication fails. You can see this error after the first restore attempt has failed, and when you try to restore for the second time. You can reboot NFVIS before you attempt restore again.

```
nfvis# hostaction restore file-path extdatastore2:backup_20200704.bkup
Error: application communication failure
```