System Access Configuration

Host system requirements

These resources are required for a standalone Cisco NFVIS.

Table 1: CPU allocation

Total Cores	NFVIS 4.10.x and later Releases
16 or less	1 + (1 core per socket applicable to DPDK systems)
More than 16	2 cores in NUMA-0 1 core in NUMA-1 (if Multi-NUMA node system*) (1 core per socket applicable to DPDK systems)

Total Cores	NFVIS 4.10.x and later Releases
* Indicates that Multi-NUMA node systems require an additional CPU core system reserved. This additional core is helpful in processing the cross NUMA nodes, indirectly improving the performance of Cisco NFVIS functions on the system cores.	

Note

- If hyper-threading is enabled on the device, each core reflects two logical CPUs.

Table 2: Memory allocation

Reserved System Memory	Up to 16 GB	Up to 32 GB	Up to 64 GB	Up to 128 GB	Greater than 128 GB	Greater than 256 GB
Reserved for NFVIS	For UCSC-M6 : 7 GB/ 8 GB*	For UCSC-M6 : 11 GB/ 12 GB*	For UCSC-M6 : 11 GB/ 12 GB*	For UCSC-M6 : 11 GB/ 12 GB*	For UCSC-M6 : 11 GB/ 13 GB*	For UCSC-M6 : 16 GB/ 20 GB*
* Indicates the memory allocation is applicable only for Multi-NUMA node systems. In case of single node systems, the memory allocation values without * is applicable.						

Total System Memory	Additional memory required for DPDK support per NUMA node
Upto 63 GB	1
64 GB - 127 GB	2
128 GB - 256 GB	4

Requirements: system setting hostname

You must adhere to the following rules for hostname on NFVIS:

- Must contain minimum length of 2 and maximum length of 255.
- Must begin with a letter or digit and can contain alphabets, numbers and hyphen.
- Must not be deleted.
- The hostname range is from 1 to 58. The hostname range must contain a letter or a digit, it may contain alphabets, numbers, and hyphens.

Access NFVIS

This task enables you to gain initial access to the NFVIS system and configure network connectivity for ongoing management operations.

NFVIS provides multiple access methods including portal, CLI, console, and PNP. The system requires immediate password change after first login for security purposes. Network connectivity can be established through WAN, WAN2, and management interfaces with support for both IPv4 and IPv6 configurations.

Before you begin

Ensure physical connectivity to the NFVIS system through one of the available interfaces.

Follow these steps to access NFVIS and configure initial connectivity:

Procedure

Step 1 Log in using the default credentials.

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 returns 401 unauthorized error if the default password is not reset.

If WAN-br or wan2-br have 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 DHCP assignment on WAN-br until the configurations are changed. For DHCP assignment to continue to request IP address for PNP flow on both WAN interfaces answer 'n'.

Step 2 Create a strong password that meets the security requirements.

You must adhere to these 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 NFVIS portal.
- Using the CLI (When you first log into Cisco 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).

Example:

```
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


NFVIS Version: 3.12.3

Copyright (c) 2015-2020 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.

login: admin
NFVIS service is OK
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
admin@localhost's password:


Cisco Network Function Virtualization Infrastructure Software (NFVIS)

NFVIS Version: 3.12.3-RC8

Copyright (c) 2015-2020 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 connected from ::1 using ssh on nfvis
admin logged with default credentials
Setting admin password will disable zero touch deployment behaviors.
Do you wish to proceed? [y or n]y
Please provide a password which satisfies the following criteria:
        1.At least one lowercase character
        2.At least one uppercase character
        3.At least one number
        4.At least one special character from # _ - * ?
        5.Length should be between 7 and 128 characters
Please reset the password :
Please reenter the password :


 Resetting admin password


New admin password is set

nfvis#
System message at 2020-01-08 03:10:10...
Commit performed by system via system using system.
nfvis#
```

Step 3 Connect 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 DHCP configuration and the management interface is configured with a static IP address of 192.168.1.1. If the system has a DHCP server connected to the WAN interface, the WAN interface is assigned an 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. However, to be able to use a static IP address to remotely connect to a server, the default gateway needs to be configured first.

You can connect to the system in these 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).

Step 4 Perform static configuration without DHCP if needed.

Step 5 Verify the initial configuration.

Use the **show system settings-native** command 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.

Example:

```
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
```

Here is an 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
```

You have successfully accessed NFVIS, changed the default password, and configured network connectivity. The system is now ready for management operations through your chosen access method.

VLAN configuration for NFVIS management traffic

A VLAN is a logical network segmentation technology that

- creates independent logical networks within a physical network
- uses VLAN tagging to insert a VLAN ID into a packet header to identify which VLAN the packet belongs to, and
- enables isolation of Cisco NFVIS management traffic from VM traffic when configured on bridge interfaces.

VLAN configuration details

You can configure a VLAN tag on these bridge interfaces:

- WAN bridge (WAN-br) interface to isolate Cisco NFVIS management traffic from VM traffic
- wan2-br for ENCS5400 or ENCS 5100

- user-br for all systems

By default, WAN bridges and LAN bridges 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.

Configure the IP receive ACL

This task configures the IP receive ACL to filter out unwanted traffic by allowing or blocking traffic based on IP addresses and service ports.

Use the IP receive ACL feature to control access to the management interface by specifying which source networks are permitted to connect.

Before you begin

Follow these steps to configure the IP receive ACL:

Procedure

Step 1 Configure the source network for Access Control List (ACL) access.

Example:

```
configure terminal
system settings ip-receive-acl 198.0.2.0/24
action accept priority 10
commit
```

Step 2 Verify the trusted IP connection using the **show running-config system settings IP-receive-ACL** command.

This command displays the configured source network for ACL access to the management interface.

Example:

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

The IP receive ACL is configured and the trusted IP connection settings are verified. Traffic from the specified source network is now allowed based on the configured ACL rules.

Configure port 22222 and management interface ACL

Use this task to configure an IP receive Access Control List (ACL) to filter traffic. This allows you to block or allow specific traffic based on IP addresses and service ports to enhance network security.

The IP receive ACL enables you to control access to the management interface. Note that port 22222, used for the SCP server, is closed by default. You must explicitly open this port if you need to SCP files into NFVIS from an external server.

Note The SCP command cannot be used to copy files between two NFVIS devices.

Procedure

Step 1 Configure the source network for ACL access.

Follow these steps to define the source network allowed to access the management interface:

```
configure terminal
system settings ip-receive-acl 198.0.2.0/24
action accept priority 10
commit
```

Step 2 Open port 22222 for SCP access.

If you need to SCP files from an external server, follow these steps to open the port:

Example:

```
config terminal
system settings ip-receive-acl address/mask_len service scpd priority 2 action accept
commit
```

Note
The ACL is identified by the address. If you remove this ACL, all other ACLs sharing the same address are also removed. You must reconfigure those ACLs if necessary.

Step 3 Verify the interface configuration using the **show running-config system settings ip-receive-ACL** command.

Example:

```
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

!
```

Port 22222 is now open and configured for SCP file transfer from external servers to the NFVIS system.

Configure secondary IP address and source interface

Configure secondary IP addresses and source interfaces to enable multiple IP addresses per interface and control packet source addressing on NFVIS.

The Cisco NFVIS supports multiple IP addresses per interface. You can configure a secondary IP address on the WAN interface, as an additional IP address to reach the software. Set the external routes for secondary IP address to reach the NFVIS. Routers configured with secondary addresses can route between the different subnets attached to the same physical interface.

The Source Interface feature lets you assign an IP address to a source interface. The IP address configured is used for packets generated by the NFVIS. The packets generated use the default route.

To access secondary IP address through ISRv, the WAN physical port is removed from WAN-br similar to single IP address.

Before you begin

- The IP address must be one of the IP addresses configured in system settings.
- The source interface IP address can be one of the following:
  - mgmt
  - WAN
  - WAN Secondary IP
  - WAN2 IP or IP configured on any bridge
- Source-interface configuration must be applied if the WAN IP is static.
- For DHCP, source interface IP address is accepted but cannot be applied. The configuration takes effect once you switch from DHCP to static.

Procedure

Step 1 Configure Secondary IP Address:

Example:

```
nfvis(config)# system settings wan secondary ip address 1.1.2.3 255.255.255.0
```

Step 2 Configure source Interface:

Example:

```
nfvis(config)# system settings source-interface
1.1.2.3
```

The secondary IP address and source interface are configured. The secondary IP address and source interface related errors are logged in **`show log nfvis_config.log`** file.

Users, roles, and authentication

Configure local user account management

Configure role-based access control to enable administrators to manage different levels of access to the system's compute, storage, database, and application services using access control concepts such as users, groups, and rules.

Role based access enables the administrator to manage different levels 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 3: Supported user roles and privileges

User Role	Privilege
Administrators	Owns everything, can perform all tasks including changing user roles, but cannot delete basic infrastructure. An admin's role can't be changed
Operators	Start, stop, and delete a VM. Clear logs and view all information
Auditors	Read-only permission and can't perform any tasks

Before you begin

The user passwords must meet these 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 (*), or question mark (?).
- Must contain an uppercase character and a lowercase character.
- Must not be the same as last five passwords.

Procedure

Step 1 Create a user and assign a role.

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".

Example:

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

Step 2 Delete a user if needed.

Example:

```
rbac authentication users delete-user name test1
```

Note
To change the password, use the **rbac authentication users user test1 change-password new-password newPassword old-password oldPassword** command. To change the user role to administrators, operators or auditors, use the **rbac authentication users user test1 change-role new-role newRole old-role oldRole** command.

Step 3 Configure the 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.

Example:

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

Step 4 Configure password lifetime values.

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.

Example:

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

Step 5 Configure automatic deactivation of 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.

Example:

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

Step 6 Activate an inactive user account when needed.

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

Example:

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

Local user account management is configured with role-based access control, password requirements, and account lifecycle management policies.

User and role management in the NFVIS portal

User and role management in the NFVIS portal is a graphical interface that

- provides an intuitive alternative to command-line operations for managing user accounts and roles
- enables administrators to create, modify, and delete user accounts, and
- allows assignment of specific roles to define user access levels within the system.

Create new users

Create new user accounts in NFVIS portal to provide controlled access to system resources based on assigned roles and permissions.

Use this procedure when you need to grant access to the NFVIS system for new team members or when setting up role-based access control for different user types.

Before you begin

Log in to the NFVIS portal as an administrator.

Follow these steps to create a new user account through the NFVIS portal:

Procedure

Step 1 Navigate to **Configuration** > **Host** > **Security** > **Users and Roles**.

Step 2 From the **Users and Roles** page, click the **+** icon to create a new user.

Step 3 Enter the following details:

Field	Description
Name	Enter the unique login name for the new user account..

Field	Description
Role	Select the predefined role that defines the user's permissions and access level within the NFVIS system. Options typically include: • Administrator: Full access to configure, update, or delete resources, and manage user roles. • Operator: Can view, start, stop, and delete Virtual Machines (VMs). • Auditor: Read-only access to system information.
Password	Enter the password for the new user account. This must comply with the configured strong password policies (e.g., minimum length, complexity requirements including uppercase, lowercase, numbers, and special characters).
Confirm Password	Re-enter the password exactly as entered in the **Password** field to confirm accuracy and prevent typing errors.
Group	Choose a user group to assign this user to. User groups are used for granular role-based access control (RBAC) and can define specific access policies for sets of users or resources.
Preferred Language	Choose the default language for a user's NFVIS portal interface: • English • Japanese When this user logs in, the NFVIS portal will be displayed in the language chosen here.

Step 4 Click **Submit** to create the new user account with the specified details and save the configuration.

- Click **Cancel** to discard any entered information and return to the previous screen without creating the user.
- Click **Reset** to clear all fields on the form, allowing you to re-enter information.

The new user account is created with the specified role, permissions, and configuration settings. The user can now log in to the NFVIS portal using the assigned credentials.

Modify users

Modify user account details such as role, password, group, and preferred language to maintain proper access control and user management.

User accounts may need to be updated periodically to reflect changes in user roles, security requirements, or personal preferences. This task allows administrators to modify existing user accounts through the NFVIS portal interface.

Before you begin

Log in to the NFVIS portal as an administrator.

Follow these steps to modify a user account through the NFVIS portal:

Procedure

Step 1 Navigate to **Configuration** > **Host** > **Security** > **Users and Roles**.

Step 2 From the **Users and Roles** page, click the edit icon to modify an existing user account.

When modifying a user account, you can update details such as their Role, password, Group, and Preferred Language.

Step 3 Click **Submit** to apply the changes and save the updated configuration.

Click **Cancel** to discard any changes and return to the previous screen without modifying the user.

Click **Reset** to clear all fields on the form, allowing you to re-enter information.

The user account is successfully updated with the new configuration details, and the changes are saved in the system.

Delete users

Delete user accounts to remove access and manage security within the NFVIS portal.

Use this procedure when you need to remove user accounts from the NFVIS system through the portal interface.

Before you begin

Log in to the NFVIS portal as an administrator.

Follow these steps to delete users through the NFVIS portal:

Procedure

Step 1 Navigate to **Configuration** > **Host** > **Security** > **Users and Roles**.

Step 2 From the **Users and Roles** page, identify the user account you want to delete and click the Delete icon associated with it.

A confirmation message is displayed to confirm the deletion of the user account.

Step 3 In the confirmation dialog, use the following options:

- Delete: Click this button to proceed with the permanent deletion of the selected user account(s).
- Cancel: Click this button to abort the deletion process and return to the "Users and Roles" page without removing the user(s).

The selected user account is permanently deleted from the NFVIS system.

Change language preferences in the NFVIS portal

Configure the NFVIS portal interface language to support user interaction in their preferred language (English or Japanese).

Cisco NFVIS portal now supports both English and Japanese languages, providing users with the flexibility to interact with the interface in their preferred language.

Users can adjust their language preferences through two ways methods within the NFVIS portal:

- From the current user session, using the **Settings** icon.
- From the Users and Roles page. For more information on setting the default language for user accounts, see *Create New Users*.

Before you begin

Follow these steps to change the language for your current portal session:

Procedure

Step 1 Log in to the NFVIS portal

Step 2 Click the user profile icon.

Step 3 From the drop-down menu, choose **Language Preferences**

Step 4 Choose your desired language (English or Japanese) from the available options.

Once a language is chosen, the portal interface will immediately update to the chosen language, and a confirmation notification will appear. This change applies only to your current session.

The portal interface displays in your selected language for the current session.

User groups

Granular Role-Based access control

Restrictions for granular Role-Based access control

When configuring granular role-based access control, observe these restrictions to ensure proper system operation:

- A group can only be associated with one policy, either the `resource-access-control` policy or the `local-authentication-only` policy.
- One user can be assigned to one group only.
- A VM can only belong to one group.

Granular role-based access control

Granular Role-Based Access Control (Granular RBAC) is a security feature that

- restricts VM management to a particular set of users
- enables system administrators to define resource groups and assign VNFs and system resources to these groups, and
- allows user assignment to resource groups for access to associated VNFs.

Resource management components

The system administrator can define a set of resource groups, and assign VNFs and system resources such as VMs, disk files, and system level configurations to these defined groups. When you create a user, you can assign that user to one of the resource groups, and this enables the user to access the associated VNFs.

Roles

The three roles defined by the system are:

- Administrator: An administrator user has complete access to configure, update or delete a resource.
- Operator: An operator user can only view and operate a resource.
- Auditor: An auditor user can only view a resource and cannot perform any action on it.

Note All three roles have a read-access to all host level configurations, VMs, and images.

Users

A user is an account that

- is created with a role definition that is consistent across all groups
- has read access to NFVIS configurations, filesystems, logs, VMs and images
- can be a member of only one group, and
- may have remote authentication mapping for TACACS and RADIUS based on privilege level.

Admin user characteristics

The admin user is a special user account with unique properties:

- The admin user cannot be deleted or modified.
- The admin user permanently has the administrator role in the default global group.
- The admin user functions as a member of every group and can execute administrative privileges for every group.
- The admin user cannot be assigned to a specific user group.

Groups

A group is a collection of users that

- provides access control to resources based on membership

- defines resource assignment boundaries where a resource can belong to one specific group, and
- ensures all members have access to the resources assigned to that group, with privileges defined by the user's role.

Group types and characteristics

The global group is a special group assigned to users who are not members of any other group. A user in the global group can access all resources on the system, at the privilege level.

Resources can be assigned to the global group or a specific group.

When creating a group, the `resource-access-control` policy should be enabled, to have resource restrictions.

For more details on Granular RBAC feature capabilities, see Appendix.

Create groups and assign local users to the groups

This task allows you to establish role-based access control by creating groups and assigning local users to them, enabling organized user management and policy enforcement.

Groups provide a way to organize users and apply policies for role-based access control (RBAC). You can create groups with or without specific policies and then assign local users to these groups to manage their access permissions.

Procedure

Step 1 Create a group with or without a policy.

Example:

```
nfvis(config)# aaa groups group rac_group policy resource-access-control
nfvis(config-policy-resource-access-control)# commit
Commit complete.
```

Step 2 Create a local user and assign them to a group.

Example:

```
nfvis# rbac authentication users create-user name local_admin_3 password Cisco123\# role administrators
 group rac_group
```

Step 3 View a list of RBAC users with role and group information.

Example:

```
nfvis# show running-config rbac authentication users
rbac authentication users user admin
 role administrators
!
rbac authentication users user local_admin_1
 role administrators
!
rbac authentication users user local_admin_2
 role administrators
!
rbac authentication users user local_admin_3
 role administrators
 groups group rac_group
```

```
 !
!
rbac authentication users user local_oper_1
 role operators
!
rbac authentication users user local_test_1
 role operators
!
```

The groups are created and local users are assigned to them. You can verify the configuration by viewing the RBAC users with their associated roles and groups.

Assign remote users to the group

Assign remote users to a resource control group so they can manage deployments based on their defined role in the remote server.

NFVIS depends on a remote server for user authentication and authorization. When remote users login to NFVIS, they can only manage the deployment that belongs to its own resource control group, based on their defined role in the remote server. Any remote user that is not mentioned in the resource group, is treated as a global group user and that user can operate the system and manage the deployments based on their defined role.

Procedure

Assign remote users to the group using the following commands:

Example:

```
nfvis(config)# aaa groups group tac_group user remote_admin1
nfvis(config-user-remote_admin1)# user remote_admin2
nfvis(config-user-remote_admin2)# user remote_operator3
nfvis(config-user-remote_operator3)# policy resource-access-control
nfvis(config-policy-resource-access-control)# commit
Commit complete.
nfvis(config-policy-resource-access-control)# end
nfvis# show running-config aaa groups group tac_group
aaa groups group tac_group
policy resource-access-control
!
user remote_admin1
!
user remote_admin2
!
user remote_operator3
!
!
nfvis#
nfvis# show rbac authentication users
NAME
-------
admin
```

Note

In the above example, `remote_admin1`, `remote_admin2`, and `remote_operator3` are TACACS+/RADIUS users.

Remote users are successfully assigned to the resource control group and can manage deployments according to their defined roles.

Configure local authentication for a specific group of users

This task enables you to create a group and add specific users to it, allowing these users to bypass the default authentication order and only go through local authentication instead of the default TACACS then local authentication sequence.

Typically, users who need authentication go through the default authentication order. The default order involves external authentication through TACACS as the first step, and local authentication as the second step. The local authentication for a specific group of users feature enables you to create a group and add specific users to it, allowing these users to bypass the default authentication order. The users in this group skip the external TACACS authentication and only go through local authentication. For this group to function as expected, assign the 'local-authentication-only' policy to the group.

Restrictions for local authentication for a specific group of users:

- One user can be assigned to a maximum of one group.
- If a local user assigned to the local authentication group has the same user name as a remote (TACACS+/RADIUS) user, then only the local user's credentials are taken into consideration. The remote user's credentials are considered even if the local user's authentication fails.

Procedure

Step 1 Create a group with the local-authentication-only policy.

Example:

```
nfvis#(config) aaa groups group [ group-name ] policy local-authentication-only
```

Step 2 Assign a user to the group using one of these methods:

- Assign an existing user to the group:

  ```
  nfvis# rbac authentication users user <username> assign-group [ group-name ]
  ```

- Create a new user and assign to the group simultaneously:

  ```
  nfvis# rbac authentication users create-user name <username> password <password> role <role>
  group [ group-name ]
  ```

To remove a user from a group, use:

```
nfvis# rbac authentication users user <username> remove-group [ group-name ]
```

The group is created with the local-authentication-only policy, and the specified users are assigned to the group. These users will now bypass external TACACS authentication and only go through local authentication.

RADIUS support

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a distributed client-server system that

- secures networks against unauthorized access
- uses Cisco routers as RADIUS clients that send authentication requests to a central RADIUS server containing all user authentication and network service access information, and
- operates as a fully open protocol distributed in source code format that can be modified to work with any security system currently available on the market.

RADIUS implementation details

Cisco supports RADIUS under its AAA security paradigm. RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Note You can configure upto four RADIUS servers. When multiple RADIUS servers are configured, if the first server is unreachable, NFVIS tries the next server in the order it is configured.

How RADIUS authentication works

Summary

The key components involved in RADIUS authentication are:

- User: Provides credentials and receives authentication responses
- Access server: Prompts for credentials and relays authentication requests
- RADIUS server: Validates credentials and provides authorization data

Workflow

These stages describe how RADIUS authentication works:

1. The user is prompted to enter the username and PASSWORD.
2. The username and encrypted PASSWORD are sent over the network to the RADIUS server.
3. The user receives one of these responses from the RADIUS server:
   - ACCEPT—The user is authenticated.
   - CHALLENGE—A CHALLENGE is issued by the RADIUS server. The CHALLENGE collects additional data from the user.
   - CHANGE PASSWORD—A request is issued by the RADIUS server, asking the user to select a new PASSWORD.

- REJECT—The user is not authenticated and is prompted to reenter the username and PASSWORD, or access is denied.

Result

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of services that the user can access, including connections such as Telnet, rlogin, or local-area transport (LAT), and services such as PPP, Serial Line Protocol (SLIP), or EXEC services, and connection parameters, including the host or client IP address, access list, and user timeouts.

Configure RADIUS

This task configures RADIUS authentication to enable secure client-server communication with encrypted secret key support.

RADIUS secret encryption is supported on NFVIS. You can configure either secret key or encrypted secret key at a given time. Use encrypted secret if special characters are used in secret. NFVIS encrypts both shared-secret and encrypted-shared-secret configurations and supports both TLS and non-TLS client-server communication for RADIUS.

- Secret length must be between 1 and 127 characters.
- Secret must only contain characters from the set: [-_a-zA-Z0-9 ./\<>%!*$€#{}()+@]*

Procedure

Step 1 Configure RADIUS support using one of the following methods:

- For non-TLS RADIUS configuration, use these commands:

```
configure terminal
radius-server host 1.2.3.4
shared-secret abc
admin-priv 15
oper-priv 11
commit
```

- For TLS RADIUS configuration, use these commands:

```
configure terminal
radius-server host 1.2.3.4
shared-secret efkbkuabcwuabvauvvwqbd
use-tls true
pskidentity identity
admin-priv 15
oper-priv 11
commit
```

Step 2 Verify the RADIUS configuration using the **show running-config RADIUS-server** command.

Example:

```
nfvis# show running-config radius-server radius-server host 1.2.3.4
shared-secret $8$lZwgccBvs9x1oQpx6f1s8/JkZ4rLdQ95VMUjRrhD9Z8=
```

```
admin-priv    15
oper-priv     11
```

The shared secret is displayed in encrypted form.

RADIUS authentication is successfully configured with encrypted secret key support for secure client-server communication.

TACACS+ support

TACACS+

TACACS+ is a security application that

- provides centralized validation of users attempting to gain access to a router or network access server
- maintains services in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation, and
- requires TACACS+ server configuration before the configured TACACS+ features on your network access server are available.

TACACS+ server configuration requirements

On the TACACS+ server, ensure you configure Cisco attribute-value (AV) pair privilege level (priv-lvl) for Cisco NFVIS as a service for the minimum privilege level of administrators and operators.

Note You can configure upto four TACACS+ servers. When multiple TACACS+ servers are configured, if the first server is unreachable, NFVIS tries the next server in the order it is configured.

How TACACS operates

Summary

The key components involved in TACACS operation are:

- User: Attempts to log in to NFVIS using credentials
- NFVIS: Sends user credentials to TACACS+ server and processes responses
- TACACS+ server: Authenticates users and provides authorization responses

Workflow

The TACACS operation involves these stages:

1. When the user tries to log in, NFVIS sends user credential to TACACS+ server.
2. NFVIS will eventually receive one of the following responses from the TACACS+ server:

- ACCEPT—The user is authenticated and service can begin. If NFVIS is configured to require authorization, authorization begins at this time.
- REJECT—The user is not authenticated. The user can be denied access or is prompted to retry the login sequence, depending on the TACACS+ server.
- ERROR—An ERROR occurred at some time during authentication with the server or in the network connection between the server and NFVIS. If an ERROR response is received, NFVIS typically tries to use an alternative method for authenticating the user.
- CONTINUE—The user is prompted for additional authentication information.

After authentication, NFVIS will send authorization request to TACACS+ server.

3. Based on authorization result, NFVIS will assign user's role.

Configure a TACACS+ server

Configure TACACS+ server authentication to enable centralized user authentication and authorization with customizable privilege levels for different user roles.

TACACS+ secret encryption is supported. You can only configure either secret key or encrypted secret key at a given time. Encrypted secret key can contain special characters but secret key cannot. The following pattern is supported for encryped-shared-key: [-_a-zA-Z0-9./\\<>%!*$€#{}()+].

NFVIS encrypts both shared-secret and encrypted-shared-secret configurations.

NFVIS supports both TLS and non-TLS client-server communication for TACACS+.

The following constraints apply:

- Secret length must be between 1 and 127 characters.
- Secret must only contain characters from the set: [-_a-zA-Z0-9 ./\<>%!*$€#{}()+@]*

Procedure

Step 1 Configure TACACS+ without TLS.

Example:

```
configure terminal
tacacs-server host 1.2.3.4
shared-secret asdfghh
admin-priv 14
oper-priv 9
commit
```

In this configuration, privilege level 14 is assigned to the administrator role, and privilege level 9 is assigned to the operator role. This means a user with privilge level 14 or higher will have all admin privileges when the user logs into the system, and a user with privilege level 9 or higher will have all privileges of an operator at the time of login.

Step 2 Configure TACACS+ with TLS.

Example:

```
configure terminal
tacacs-server host 1.2.3.4
```

```
shared-secret mfqwudvkdwnbkyuDLndkw
use-tls true
pskidentity identity
admin-priv 14
oper-priv 9
commit
```

Step 3 Verify the TACACS+ configuration.

Example:

```
nfvis# show running-config tacacs-server
tacacs-server host 1.2.3.4
shared-secret $8$JkMZFgA3DkbjAHOrmdBr3U2cLg2qY1FuHAIJiIp7nSw=
admin-priv    14
oper-priv     9
```

Use the **show running-config TACACS-server** command to verify the configuration. The shared secret is displayed in encrypted form.

The TACACS+ server is configured with the specified host, shared secret, and privilege levels. Users can now authenticate through the TACACS+ server with appropriate role-based privileges.

Default authentication order

Default authentication order is a security mechanism that

- supports both TACACS+ and RADIUS but allows only one authentication method to be enabled at a time
- requires method lists to be defined for TACACS+ and RADIUS authentication through AAA commands, and
- uses local authentication as fallback when TACACS+ or RADIUS is not accessible.

Authentication configuration

After you have identified the TACACS+ and RADIUS server and defined an associated TACACS+ and RADIUS authentication key, you must define method lists for TACACS+ and RADIUS authentication. Because TACACS+ and RADIUS authentication is operated through AAA, you need to issue the AAA authentication command, specifying TACACS+ or RADIUS as the authentication method.

```
nfvis(config)# aaa authentication ?
Possible completions:
  radius   Use RADIUS for AAA
  tacacs   Use TACACS+ for AAA
  users    List of local users
```

Note

- Only when TACACS+ or RADIUS is enabled, it can be used for authentication.
- When TACACS+ or RADIUS is not accessible, local authentication is used. It is recommended to use **AAA authentication TACACS local** command to authenticate using local database. Local authentication is disabled if the connection between TACACS+ or RADIUS and NFVIS is restored.
- If the same username is registered for both local authentication and authentication through RADIUS or TACACS+, RADIUS or TACACS+ is chosen as the authentication method.
- It is recommended to configure Syslog so that it is easier to debug if TACACS+ or RADIUS does not work as expected.

All login attempts will be logged in syslogs in the local *nfvis_syslog.log*, *NFVIS-ext-auth.log* files and in remote syslog servers.

User specific authentication order

The system follows this authentication sequence for user-specific authentication:

- If the user is part of the local database, local authentication is executed and the user is permitted or denied access.
- If the user is not part of the local database, TACACS+ is used for authentication.
- If the same user is part of both the databases (local and TACACS+), the user can login with either the local password or the TACACS+ password. However, registering the same user in both the databases is not recommended.

Networking

Bridges

A bridge is a network connectivity component that

- enables NFVIS connectivity through IPv4 or IPv6 configurations such as Static IP, DHCP, SLAAC, or VLAN
- can have a port or port channel associated with it, and
- provides default LAN and WAN connectivity on NFVIS installations.

Bridge configuration information

The IP configuration on bridges and the **show bridge-settings** command were added in NFVIS 3.10.1 release.

NFVIS is installed with LAN and WAN bridges by default. A service bridge can also be created. On all NFVIS systems, LAN-br and WAN-br are generated by default and populated with the appropriate ports for that system. On ENCS 5000 series platforms, wan2-br is also generated by default for the dual WAN initialization.

The default LAN bridge is configured with a static IP address 192.168.1.1 and the WAN bridges uses DHCP for initial NFVIS connectivity.

IPv4 bridge configuration:

- If the system has a DHCP server connected to a bridge with DHCP configured, the bridge receives the IP address from the server. You can use this IP address to connect to the system.
- You can also connect to the server locally with an ethernet cable using a static IP address. To connect to the device remotely using a static IP address, you must configure the default gateway or setup an appropriate static route.
- DHCP and a default gateway cannot be configured on NFVIS simultaneously. NFVIS only supports one system level default gateway. If DHCP is configured, the default gateway is assigned to the system through the DHCP server. Also, only one bridge can be configured with DHCP at any time.

IPv6 bridge configuration:

- IPv6 can be configured in static, DHCP stateful, and Stateless Auto configuration (SLAAC) modes. 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 the Managed (M) flag, then the network stays in DHCP mode, even if there is no DHCP server in the network. If the RA shows the Other (O) flag, then the network switches from DHCP server to SLAAC mode.
- SLAAC provides IPv6 address and a default gateway. Stateless DHCP is enabled in the SLAAC mode. If the server has DNS and domain configured, then SLAAC also provides those values through stateless DHCP.
- Similar to IPv4, IPv6 DHCP and IPv6 default gateway cannot be configured on the system simultaneously, nor can stateful and stateless IPv6 DHCP. Also, only one bridge can be configured with either stateful or stateless IPv6 DHCP at any time.

Create bridges

This task allows you to create and configure a new bridge in the system.

Use this procedure when you need to establish a new bridge configuration for network connectivity.

Procedure

Step 1 Configure a new bridge.

Example:

```
configure terminal
bridges bridge my-br
commit
```

Step 2 Verify the bridge generation using the **show bridge-settings** command.

Example:

```
nfvis# show bridge-settings my-br ip-info interface
ip-info interface my-br
```

The bridge is successfully created and configured. The verification command displays the bridge settings and interface information.

Configure bridge port

Configure a bridge port to establish the connection between a bridge and a physical interface or port channel.

A bridge can be tied to a physical interface by applying the port configuration. A bridge can have as many ports as are available, however a port must be unique to at most one bridge. If a port channel is applied to a bridge, it must be the only port configuration on that bridge.

Procedure

Step 1 Configure a port on a bridge.

Example:

```
configure terminal
bridges bridge my-br port eth3
commit
```

Step 2 Configure a port channel on a bridge.

Example:

```
configure terminal
bridges bridge my-br port pc1
commit
```

Step 3 Verify the port settings applied to a bridge using the **support ovs vsctl** command.

Example:

```
nfvis# support ovs vsctl list-ports my-br
eth3
```

The same command can be used to verify the port channel settings applied to a bridge:

```
nfvis# support ovs vsctl list-ports my-br
bond-pc1
```

The bridge port is configured and can be verified using the support ovs vsctl command to display the configured ports.

Configure bridge IP connectivity

This task enables you to establish network connectivity for bridges by configuring IP addressing methods, VLAN isolation, and MAC learning parameters on Cisco NFVIS systems.

Bridge IP connectivity configuration is essential for proper network operation in NFVIS environments. You can configure different connectivity options including DHCP for automatic IP assignment, static IP for fixed addressing, VLAN tagging for traffic isolation, and MAC aging time for optimal MAC address table management.

Before you begin

Follow these steps to configure bridge IP connectivity:

Procedure

Step 1 Configure DHCP on the bridge if automatic IP assignment is required.

DHCP configuration can be applied to any bridge if no other bridge on the system has DHCP configured, and default gateway is not applied under system settings. DHCP configuration on a bridge automatically triggers a DHCP renew request from the bridge. For an additional DHCP renew trigger, use the **hostaction bridge-DHCP-renew** command.

Example:

```
configure terminal
bridges bridge my-br dhcp
commit
```

To verify the DHCP settings applied to a bridge, use the **show bridge-settings <br_name> DHCP** command.

```
nfvis# show bridge-settings my-br dhcp

dhcp enabled
dhcp offer                          true
dhcp interface                      my-br
dhcp fixed_address                  10.10.10.14
dhcp subnet_mask                     255.255.255.128
dhcp gateway                         10.10.10.1
dhcp lease_time                      7200
dhcp message_type                      5
dhcp name_servers                     NA
dhcp server_identifier               10.10.10.1
dhcp renewal_time                    3600
dhcp rebinding_time                    6300
dhcp vendor_encapsulated_options     NA
dhcp domain_name                       NA
dhcp renew                       2019-12-11T13:28:29-00:00
dhcp rebind                      2019-12-11T14:17:12-00:00
dhcp expire                      2019-12-11T14:32:12-00:00
```

Step 2 Configure a static IP address on the bridge if fixed IP assignment is required.

An IPv4 address and subnet can be configured on any bridge which does not have DHCP configured. To enable routing outside of the subnet, apply the default gateway under system settings or confirgure system routes.

Example:

```
configure terminal
```

```
bridges bridge my-br ip address 172.25.220.124 255.255.255.0
commit
```

To verify the IPv4 settings applied to a bridge, use the **show bridge-settings <br_name> ip_info** command.

```
nfvis# show bridge-settings my-br ip_info
ip-info interface                        my-br
ip-info ipv4_address                     172.25.220.124
ip-info netmask                          255.255.255.0
ip-info link-local ipv6 address          fe80::4e00:82ff:fead:e802
ip-info link-local ipv6 prefixlen        64
ip-info global ipv6                     address::
ip-info global ipv6 prefix               len0
ip-info mac_address                      4c:00:82:ad:e8:02
ip-info mtu                             9216
ip-info txqueuelen                      1000
```

Step 3 Configure VLAN tagging on the bridge to isolate 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 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.

Example:

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

To verify the VLAN settings applied to a bridge, use the **show bridge-settings my-br VLAN** command.

```
nfvis# show bridge-settings my-br vlan
vlan tag 10
```

Step 4 Configure MAC aging time on the bridge to optimize MAC address table management.

MAC aging time specifies the time at which a MAC address entry ages out of the MAC address table. The max-aging-time specifies the maximum number of seconds to retain a MAC learning entry for which no packets have been seen. The default value is 300 seconds.

Example:

```
configure terminal
bridges bridge my-br mac-aging-time 600
commit
```

To verify the MAC aging time settings applied to a bridge, use the **show bridge-settings <br_name> MAC-aging-time** command.

```
nfvis# show bridge-settings my-br mac-aging-time
mac-aging-time 600
```

The bridge is configured with the appropriate IP connectivity settings including DHCP or static IP addressing, VLAN tagging for traffic isolation, and optimized MAC aging time for efficient network operation.

Physical network interface cards

Configure LLDP

LLDP enables network devices to advertise their identity, capabilities, and neighbors, allowing connected devices to see each other as neighbors.

LLDP is supported on NFVIS. The Link Layer Discovery Protocol (LLDP) is used by network devices for advertising their identity, capabilities, and neighbors. You can configure LLDP on a PNIC which is not a port channel or a DPDK port. By default, LLDP is disabled for all PNICs.

LLDP information is sent by devices from each of their interfaces at a fixed interval, in the form of an Ethernet frame. Each frame contains one LLDP Data Unit (LLDPDU). Each LLDPDU is a sequence of type-length-value (TLV) structures.

LLDP is enabled in transmit and receive mode. The LLDP agent can transmit the local system capabilities and status information and receive the remote system's capabilities and status information.

If LLDP is enabled on two connected devices, they can see each other as neighbors.

Note LLDP packets are not propagated to VMs. LLDP cannot be enabled on port channel or DPDK ports.

Procedure

Step 1 To enable LLDP on a PNIC:

Example:

```
configure terminal
pnic eth0 lldp enabled
commit
```

Step 2 To disable LLDP on a PNIC:

Example:

```
configure terminal
pnic eth0 lldp disabled
commit
```

Step 3 Use the **show LLDP neighbors** command to display the peer information:

Example:

```
nfvis# show lldp neighbors eth0
------------------------------------------------------------
DEVICE
NAME ID      HOLDTIME  CAPS  PLATFORM  PORTID  DESCRIPTION

------------------------------------------------------------
eth0 Switch1623 120 Bridge, Router Cisco IOS Software, Catalyst L3 Switch Software
(CAT3K_CAA-UNIVERSALK9-M), Version 15.0(1)EX3, RELEASE SOFTWARE (fc2)Ifname:
Gi1/0/4GigabitEthernet1/0/4
```

Step 4 Use the **show LLDP stats** command to display the tx and rx information:

Example:

```
nfvis# show lldp stats eth0
-------------------------------------------------------------------
TX      DISCARD  ERROR  RX      DISCARDED  UNREC
NAME    FRAMES  RX       RX     FRAMES    TLVS       TLVS   AGEOUTS
-------------------------------------------------------------------
eth0    23      0        0       19667     0         0         0
```

LLDP is configured on the specified PNIC, enabling the device to exchange identity and capability information with connected neighbors.

Configure the administrative status of a port

Configure the administrative status of a port to control its operational state.

Administrative status provides a mechanism for configuring the administrative status of a port. It can be set to up or down and the default setting is on.

Note Administrative status cannot be enabled on port channel.

Procedure

Step 1 Configure the admin status on a pnic for a VM.

Example:

```
configure terminal
pnic GE0-1 admin status down
commit
```

Step 2 Verify the admin status configuration.

Use the **show pnic** command to verify the admin status configuration. Use the **show pnic link_state** command to verify the admin state configuration.

Example:

```
nfvis# show pnic GE0-1 link_state
link_state down
```

Note
Speed and duplex values in **show pnic** and **ethtool** outputs may differ depending on the peer device's interface speed and duplex settings.

The administrative status of the port has been configured and verified. The port's operational state is now controlled according to the specified administrative setting.

Configure speed, duplex and autonegotiation

This task enables you to configure speed and duplex settings on Physical Network Interface Cards (PNICs) to control autonegotiation behavior and ensure optimal network connectivity.

NFVIS supports autonegotiation by default on all PNICs. Speed and duplex are set to *auto* mode to indicate autonegotiation is enabled.

Autonegotiation allows a PNIC to communicate with the device on the other end of the link to determine the optimal duplex mode and speed for the connection. Autonegotiation can be turned off by configuring speed and duplex. Supported Ethernet speed is 10 Mbps, 100 Mbps, and 1G and 10 G.

Duplex mode displays the data flow on the interface. Duplex mode on an interface can be full or half duplex. A half-duplex interface can only transmit or receive data at any given time and a full-duplex interface can send and receive data simultaneously.

When autonegotiation is enabled on a port, it does not automatically determine the configuration of the port on the other side of the ethernet cable to match it. Autonegotiation only works if it is enabled on both sides of the link. If one side of a link has auto-negotiation enabled, and the other side of the link does not, then autonegotiation cannot determine the speed and duplex configurations of the other side. If autonegotiation is enabled on the other side of the link, the two devices decide together on the best speed and duplex mode. Each interface advertises the speed and duplex mode at which it can operate, and the best match is selected. Higher speed and full duplex is the preferred mode.

If one side of a link does not have autonegotiation enabled, then the speed and duplex on both sides must match so that the data can transmit without collisions. Autonegotiation fails on 10/100 links, if one side of the link has been set to 100/full, and the other side has been set to autonegotiation which is 100/half.

Procedure

Step 1 To disable autonegotiation on a PNIC, configure speed and duplex:

Example:

```
configure terminal
pnic GE0-0 speed 100 duplex full
commit
```

Step 2 To enable autonegotiation on a PNIC:

Example:

```
configure terminal
pnic GE0-0 speed auto duplex auto
commit
```

Step 3 To configure speed and duplex with non auto values:

Example:

```
configure terminal
pnic GE0-0 speed 100 duplex full
commit
```

Step 4 Use the **show PNIC GE0-0 operational-speed**, **show PNIC GE0-0 operational-duplex** and **show PNIC GE0-0 autoneg** to verify the configurations.

Example:

```
nfvis# show pnic GE0-0 operational-speed
operational-speed 100

nfvis# show pnic GE0-0 operational-duplex
operational-duplex full

nfvis# show pnic GE0-0 autoneg
autoneg off
```

Step 5 To verify the PNIC speed and duplex configurations, use the **show notification stream NFVIS Event** command.

Example:

```
notification
event Time 2019-12-16T22:52:49.238604+00:00
nfvisEvent
    user_id admin
    config_change true
    transaction_id 0
    status FAILURE
    status_code 0
    status_message Pnic GE0-1 speed did not update successfully
    details NA
    event_type PNIC_SPEED_UPDATE
    severity INFO
    host_name nfvis
    !
!
notification
event Time 2019-12-16T22:53:05.01598+00:00
nfvisEvent
    user_id admin
    config_change true
    transaction_id 0
    status SUCCESS
    status_code 0
    status_message Pnic GE0-1 duplex updated successfully:full
    details NA
    event_type PNIC_DUPLEX_UPDATE
    severity INFO
    host_name nfvis
    !
!
```

The PNIC speed and duplex settings are configured according to your requirements, and autonegotiation is either enabled or disabled as specified.

Port Channels

Port channels

A port channel is a logical link that

- combines individual links into a group to provide the aggregate bandwidth of up to eight physical links
- increases bandwidth and redundancy and load balances traffic between the member ports, and
- switches traffic from a failed port to the remaining member ports when a member port fails.

Port channel configuration requirements

Port channel configuration has these requirements:

- Port channels must have at least two ports and can be configured using static mode or Link Access Control Protocol (LACP).
- Configuration changes that are applied to the port channel are applied to each member port of the port channel.
- A port channel can also be added to a bridge. When a port channel has two or more than two members and the port channel is added to a bridge, a bond is created.
- A port can be a member of only one port channel and all the ports in a port channel must be compatible.
- Each port must use the same speed and operate in full-duplex mode.

Note

- The Physical Network Interface Controllers (PNICs) added to the port channel should be uniform. For example, all the PNICs associated with the port channel must have SRIOV VFs or they should not have SRIOV VFs.
- The Data Plane Development Kit (DPDK) can be associated only with port channels that have no SRIOV VFs attached to them. When a port channel is attached to a bridge and if the port channel has SRIOV VFs attached, the bridge gets automatically downgraded to a non-DPDK bridge.

Port channel bond modes include:

- **`active-backup`**: In this mode, one of the ports in the aggregated link is active and all others ports are in the standby mode.
- **`balance-slb`**: In this mode, load balancing of traffic is done based on the source MAC address and VLAN.
- **`balance-tcp`**: In this mode, 5-tuple (source and destination IP, source and destination port, protocol) is used to balance traffic across the ports in an aggregated link.

Port channel LACP modes include:

- **`off`**: Indicates that no mode is applicable.
- **`active`**: Indicates that the port initiates transmission of LACP packets.

- **passive**: Indicates that the port only responds to the LACP packets that it receives but does not initiate the LACP negotiation.

Configure a port channel

Port channels provide link aggregation to increase bandwidth and provide redundancy between network devices. This task allows you to create and manage port channels for optimal network performance.

Port channels combine multiple physical interfaces into a single logical interface. You can add ports to existing port channels and integrate them into bridge configurations for enhanced network connectivity.

Procedure

Step 1 Create a port channel.

Example:

```
configure terminal
pnic egroup type port_channel lacp_type active bond_mode balance-tcp trunks 10,20
commit
```

Note
Ensure to commit the changes.

Step 2 Add ports to the port channel.

You can add a port to a new port channel or a port channel that already contains ports. Adding GE0-0 and GE0-1 to egroup:

Example:

```
configure terminal
pnic GE0-0 member_of egroup
commit
```

Note
Ensure to commit the changes.

Example:

```
configure terminal
pnic GE0-1 member_of egroup
commit
```

Note
Ensure to commit the changes.

Step 3 Add the port channel to a bridge.

You can add a port channel to a new bridge or an existing bridge. When a port channel is added to a bridge, a bond is added for the port channel.

Example:

```
configure terminal
bridges bridge test-br port egroup
commit
```

Note

Ensure to commit the changes.

Step 4 Verify port channel configurations using the **show port-channel** command.

Example:

```
nfvis# show port-channel

----bond-egroup----
bond_mode: balance-tcp
bond may use recirculation: yes, Recirc-ID : 1
bond-hash-basis: 0
updelay: 0 ms
downdelay: 0 ms
next rebalance: 6921 ms
lacp_status: negotiated >>>this should be negotiated to indicate port channel is active
lacp_fallback_ab: false
active slave mac: 38:90:a5:1b:fe:0d(GE0-1)>>should indicate active slave mac address

slave GE0-0: enabled
may_enable: true

slave GE0-1: enabled
active slave >>>active slaveport should show active
may_enable: true
```

The port channel is successfully configured with the specified ports and added to the bridge. The verification output displays the port channel status, including LACP negotiation status and active slave information.

What to do next

Before deleting a port channel, you must remove all members assigned to the port channel. If the port channel is configured on the bridge, you must remove the port channel from the bridge.

Enable promiscuous mode

NFVIS allows enabling promiscuous mode on interfaces. Enabling promiscuous mode on an interface can be used to monitor all incoming packets on the interface.

When an interface is connected to a bridge, NFVIS enables promiscuous mode on the interface.

Procedure

Step 1 Enable promiscuous mode on the interface.

Example:

```
nfvis# config terminal
nfvis(config)# pnic GE0-0 promiscuous enabled
nfvis(config-pnic-GE0-0)# commit
```

Step 2 Verify that promiscuous mode has been enabled.

Use the **show pnic GE0-0 operational-promiscuous** command to verify if promiscuous mode has been enabled.

Promiscuous mode is enabled on the interface, allowing monitoring of all incoming packets.

Configure dynamic SR-IOV

Configure dynamic SR-IOV to control SR-IOV functionality on Physical Network Interface Controllers, allowing you to enable or disable SR-IOV and manage SR-IOV networks based on virtual function requirements.

Dynamic Single-root input/output virtualization (SR-IOV) allows you to enable or disable SR-IOV on a Physical Network Interface Controller (PNIC). To disable SR-IOV on a PNIC, set the SR-IOV value to 0. To enable SR-IOV on a PNIC, set the SR-IOV value between 1 and the maximum number of virtual functions (maxvfs) supported on that PNIC. 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. The existing fresh installation behavior has not changed. Each PNIC has a number of VFs and SR-IOV networks created by default. You can use CLI, API, or the GUI to enable and disable SR-IOV on a PNIC and to create and delete SR-IOV networks.

Note The number of SR-IOV networks, numvfs or inusevfs, created per PNIC on fresh installation of NFVIS depends on the link speed of that particular PNIC.

Procedure

Step 1 Disable SR-IOV on a PNIC by ensuring all SR-IOV networks on the PNIC are deleted and the PNIC is not attached to a bridge.

Example:

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

Step 2 Enable SR-IOV on a PNIC by ensuring the PNIC supports SR-IOV, the numvfs field is populated with a value less than the maximum number of virtual functions supported, and the PNIC is not attached to a bridge.

Example:

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

To display the SR-IOV status of all PNICs, use the **show PNIC SRIOV** command. To display the SR-IOV state of an individual PNIC use the **show PNIC eth0-1 SRIOV** command.

Step 3 Create SR-IOV networks when the PNIC has SR-IOV enabled and configured with numvfs, using the format <pnic_name>-SRIOV-<num> where <num> is greater than 0 and less than the number of VFs.

To create an SR-IOV network in trunk mode:

Example:

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

To create an SR-IOV network in access mode:

Example:

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

Step 4 Delete SR-IOV networks by ensuring no VMs are attached to the network.

Example:

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

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

SR-IOV is successfully configured on the PNIC with the appropriate virtual functions and networks created or deleted as specified.

System routes

A system route is a static routing configuration that

- directs traffic that should not go through the default gateway
- provides connectivity when certain destinations are not reachable through the default routes, and
- updates the system routing table when configured.

System route configuration requirements

You can create a route by providing the destination and prefix length, but a valid route requires a specified device, a gateway or both. The gateway input represents the address of the nexthop router in the address family. The dev input is the name of the outbound interface for the static route.

Configure system routes

Configure additional static routes to enable network connectivity to specific destinations through designated gateways or devices.

System routes define how network traffic is directed to different destinations. Static routes provide explicit control over routing decisions for specific network segments.

Procedure

Step 1 Configure the system routes using the following commands:

Example:

```
configure terminal
system routes route 172.25.222.024 gateway 172.25.221.1
system routes route 172.25.223.024 dev wan-br
commit
```

Step 2 Verify the system routes configuration using the **show system routes** command.

Example:

```
nfvis# show system routes

DESTINATION    PREFIXLEN       STATUS
---------------------------------------
172.25.222.0      24           Success
172.25.223.0      24           Success
```

The system routes are configured and verified. The output displays the configured destinations with their prefix lengths and successful status.

Troubleshoot system route configuration errors

To troubleshoot errors in configured routes, use the **show system routes** command to identify the failed route. This example shows common failures with system routes:

```
nfvis# show system routes

DESTINATION      PREFIXLEN       STATUS
-----------------------------------------
172.25.222.0        24          Failure(1)
172.25.223.1        24          Failure(2)
```

You can find the cause for each error in the *nfvos-confd* log.

Network unreachable error:

```
Failure 1) result=RTNETLINK answers: Network is unreachable
```

This example indicates that the failure is caused because the network is unreachable. To resolve this issue you can either reconfigure the route with a reachable gateway or identify network connectivity issue.

Invalid argument error:

```
Failure 2)result=RTNETLINK answers: Invalid argument
```

This failure is caused due to a mismatch between the subnet address and the prefix length. To resolve this issue you can reconfigure the route with the correct subnet address (in this case 172.25.223.0 for prefix length of 24).

Cisco network Plug-n-Play support

Cisco Network Plug-n-Play support is a provisioning solution that

- provides a simple, secure, unified, and integrated offering for enterprise network customers to ease new branch or campus device rollouts
- enables provisioning updates to an existing network, and
- delivers a unified approach to provision enterprise networks comprising Cisco routers, switches, and wireless devices with a near zero touch deployment experience.

Cisco network plug and play client capabilities

You can use the Cisco Network Plug and Play client to:

- Auto discover the server
- Provide device information to the server
- Bulk provisioning of user credentials

You can change the default user name and password of the devices using the Cisco Network PnP client. The Cisco Network PnP server sends the configuration file to Cisco Network PnP clients residing on multiple devices in the network, and the new configuration is automatically applied to all the devices.

Note For bulk provisioning of user credentials, ensure that you have the necessary configuration file uploaded to the Cisco APIC-EM. These are the supported configuration formats:

Configuration file formats - Sample 1

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <rbac xmlns="http://www.cisco.com/nfv/rbac">
    <authentication>
      <users>
        <user>
          <name>admin</name>
          <password>Cisco123#</password>
          <role>administrators</role>
        </user>
        <user>
          <name>test1</name>
          <password>Test1239#</password>
          <role>administrators</role>
        </user>
        <user>
          <name>test2</name>
          <password>Test2985#</password>
          <role>operators</role>
        </user>
      </users>
    </authentication>
  </rbac>
</config>
```

Configuration file formats - Sample 2

If you use format 2, the system will internally convert this format into format 1.

```
<aaa xmlns="http://tail-f.com/ns/aaa/1.1">
    <authentication>
      <users>
        <user>
          <name>admin</name>
          <password>User123#</password>
        </user>
      </users>
    </authentication>
</aaa>
```

PnP discovery methods

A PnP discovery method is a network discovery mechanism that

- enables Cisco Network PnP agents to locate and connect to the PnP server in Cisco APIC-EM
- activates automatically when a device powers on for the first time without a startup configuration file, and
- provides multiple fallback options to ensure successful server discovery.

Discovery method types

When a device is powered on for the first time, the Cisco Network PnP agent discovery process, which is embedded in the device, starts in the absence of the startup configuration file, and discovers the IP address of the Cisco Network PnP server located in the Cisco APIC-EM. The Cisco Network PnP agent uses these discovery methods:

- Static IP address—The IP address of the Cisco Network PnP server is specified using the **set pnp static IP-address** command.
- DHCP with option 43—The Cisco PnP agent automatically discovers the IP address of the Cisco Network PnP server specified in the DHCP option 43 string. For more details on how to configure DHCP for PnP server auto-discovery, see the Solution Guide for Cisco Network Plug and Play
- Domain Name System (DNS) lookup—If DHCP discovery fails to get the IP address of the PnP server, for example, because option 43 is not configured, the Cisco Plug and Play Agent falls back on a DNS lookup method. Based on the network domain name returned by the DHCP server, it constructs a fully qualified domain name (FQDN) for the PnP server, using the preset hostname "pnpserver". For more details on how to configure DNS for PnP server auto-discovery, see the Solution Guide for Cisco Network Plug and Play.

Note DNS FQDN Only lookup method is supported since 3.10.1 release.

- Cloud Redirection—This method uses the Cisco Cloud Device Redirect tool available in the Cisco Software Central.The Cisco Plug and Play Agent falls back on the Cloud Redirection method if DNS lookup is not successful.

Configure PnP discovery methods

Configure PnP discovery methods to enable device provisioning and management through static configuration with specific IP addresses or FQDN, or automatic discovery through DHCP, DNS, and CCO methods.

PnP discovery enables automatic device provisioning in network environments. You can configure discovery methods using static mode with specific IP addresses, IPv6 addresses, or FQDN, or use automatic mode that leverages DHCP, DNS, and CCO services for device discovery.

Procedure

Step 1 Enable static mode for PnP discovery using IPv4.

Example:

```
configure terminal
pnp automatic dhcp disable dhcp-ipv6 disable dns disable dns-ipv6 disable cco disable cco-ipv6 disable
pnp static ip-address 192.0.2.8 port 80 transport http
commit
pnp action command restart
```

Step 2 Enable static mode for PnP discovery using IPv6.

Example:

```
configure terminal
pnp automatic dhcp disable dhcp-ipv6 disable dns disable dns-ipv6 disable cco disable cco-ipv6 disable
pnp static ipv6-address 0:0:0:0:0:ffff:c000:208 port 80 transport http
commit
pnp action command restart
```

Note
Either IPv4 or IPv6 can be enabled at a time.

Step 3 Enable static mode for PnP discovery using FQDN.

Example:

```
configure terminal
pnp static ip-address apic-em-fqdn.cisco.com port 80 transport http
commit
```

Note
In FQDN support for PnP, domain names can be specified as an input. FQDN that is configured with IPv6 on a DNS server is not supported.

Step 4 Enable automatic mode for PnP discovery using IPv4.

Example:

```
configure terminal
pnp automatic dhcp enable
pnp automatic dns enable
pnp automatic cco enable
```

```
pnp automatic timeout 100
commit
```

Note
By default, the automatic discovery mode for DHCP, DNS, and CCO is enabled. You can enable or disable the options as required. For example, you can enable all options or keep one enabled, and the rest disabled.

Step 5 Enable automatic mode for PnP discovery using IPv6.

Example:

```
configure terminal
pnp automatic dhcp-ipv6 enable
pnp automatic dns-ipv6 enable
pnp automatic cco-ipv6 enable
pnp automatic timeout 30
commit
```

Note
You cannot disable both static and automatic PnP discovery modes at the same time. You must restart PnP action every time you make changes to the PnP discovery configuration. You can do this using the **pnp action command restart**.

Step 6 Verify the PnP status using the **show pnp** command in privileged EXEC mode.

Example:

```
nfvis# show pnp
pnp status response "PnP Agent is running\n"
pnp status ip-address 192.0.2.8
pnp status ipv6-address ""
pnp status port 80
pnp status transport http
pnp status cafile ""
pnp status created_by user
pnp status dhcp_opt43 0
pnp status dns_discovery 0
pnp status cco_discovery 0
pnp status dhcp-ipv6 0
pnp status dns-ipv6 0
pnp status cco-ipv6 0
pnp status timeout 100
nfvis#
```

FQDN

```
nfvis# show pnp
pnp status response "PnP Agent is running\nserver-connection\n    status: Success\n    time: 06:23:11
 Jun 17\ndevice-info\n    status: Success\n    time: 06:23:06 Jun 17\nbackoff\n    status: Success\n
    time: 06:23:11 Jun 17\ncertificate-install\n    status: Success\n    time: 06:21:38 Jun
17\ncli-exec\n    status: Success\n    time: 06:22:50 Jun 17\ntopology\n    status: Success\n
time: 06:23:00 Jun 17\n"
pnp status ip-address apic-em-fqdn.cisco.com
pnp status ipv6-address ""
pnp status port 443
pnp status transport https
pnp status cafile /etc/pnp/certs/trustpoint/pnplabel
pnp status created_by user
pnp status dhcp_opt43 0
pnp status dns_discovery 0
pnp status cco_discovery 0
pnp status dhcp-ipv6 0
pnp status dns-ipv6 0
```

```
pnp status cco-ipv6 0
pnp status timeout 0
nfvis#
```

The following sample output shows that the static discovery mode is disabled, and the automatic discovery mode is enabled for DHCP, DNS, and CCO:

DHCP:

```
nfvis# show pnp
pnp status response "PnP Agent is running\nserver-connection\n    status: Success\n    time: 05:05:59
 Jun 17\ninterface-info\n    status: Success\n    time: 05:05:56 Jun 17\ndevice-info\n    status:
Success\n    time: 05:05:38 Jun 17\nbackoff\n    status: Success\n    time: 05:05:59 Jun
17\ncapability\n    status: Success\n    time: 05:05:44 Jun 17\ncertificate-install\n    status:
Success\n    time: 05:01:19 Jun 17\ncli-exec\n    status: Success\n    time: 04:58:29 Jun 17\ntopology\n
    status: Success\n    time: 05:05:49 Jun 17\n"
pnp status ip-address 192.0.2.8
pnp status ipv6-address ""
pnp status port 443
pnp status transport https
pnp status cafile /etc/pnp/certs/trustpoint/pnplabel
pnp status created_by dhcp_discovery
pnp status dhcp_opt43 1
pnp status dns_discovery 1
pnp status cco_discovery 1
pnp status dhcp-ipv6 1
pnp status dns-ipv6 1
pnp status cco-ipv6 1
pnp status timeout 60
```

DNS:

```
nfvis# show pnp
pnp status response "PnP Agent is running\nserver-connection\n    status: Success\n    time: 05:13:55
 Jun 17\ndevice-info\n    status: Success\n    time: 05:13:49 Jun 17\nbackoff\n    status: Success\n
    time: 05:13:55 Jun 17\ncertificate-install\n    status: Success\n    time: 05:12:26 Jun
17\ncli-exec\n    status: Success\n    time: 05:13:34 Jun 17\ntopology\n    status: Success\n
time: 05:13:45 Jun 17\n"
pnp status ip-address pnpserver.apic-em-fqdn.cisco.com
pnp status ipv6-address ""
pnp status port 443
pnp status transport https
pnp status cafile /etc/pnp/certs/trustpoint/pnplabel
pnp status created_by dns_discovery
pnp status dhcp_opt43 1
pnp status dns_discovery 1
pnp status cco_discovery 1
pnp status dhcp-ipv6 1
pnp status dns-ipv6 1
pnp status cco-ipv6 1
pnp status timeout 60
```

CCO:

```
nfvis# show pnp
pnp status response "PnP Agent is running\nserver-connection\n    status: Success\n    time: 05:24:25
 Jun 17\ninterface-info\n    status: Success\n    time: 05:23:13 Jun 17\ndevice-info\n    status:
Success\n    time: 05:23:01 Jun 17\nbackoff\n    status: Success\n    time: 05:24:25 Jun
17\ncapability\n    status: Success\n    time: 05:23:06 Jun 17\nredirection\n    status: Success\n
   time: 05:09:43 Jun 17\ncli-exec\n    status: Success\n    time: 05:09:53 Jun
17\ncertificate-install\n    status: Success\n    time: 05:18:43 Jun 17\ntopology\n    status:
Success\n    time: 05:23:10 Jun 17\n"
pnp status ip-address 192.0.2.8
pnp status ipv6-address ""
pnp status port 443
pnp status transport https
```

```
pnp status cafile /etc/pnp/certs/trustpoint/pnplabel
pnp status created_by cco_discovery
pnp status dhcp_opt43 1
pnp status dns_discovery 1
pnp status cco_discovery 1
pnp status dhcp-ipv6 1
pnp status dns-ipv6 1
pnp status cco-ipv6 1
pnp status timeout 60
```

The output displays the current PnP configuration status, showing whether static or automatic discovery modes are enabled and the specific parameters configured for each method.

PnP discovery methods are configured according to your network requirements. The device can now discover and connect to the PnP server using the specified method (static IP/IPv6/FQDN or automatic DHCP/DNS/CCO discovery).

PnP Root Certificate and Static Configuration

This reference provides the technical specifications, file requirements, and command syntax for uploading PnP root certificates and configuring static PnP settings on the NFVIS host.

A certificate can be used as a PnP root certificate through Command Line Interface (CLI). The following command is used to upload a certificate:

```
system certificate input filepath <filepath> pem-data <certificate contents>
```

- The file containing the certificate information is created inside /data/intdatastore/uploads directory.
- The certificate should be in PEM encoding. Any invalid content or format is rejected with an error message.
- Multiple certificates can also be added to form a certificate chain and they should be separated by a new line.
- The certificate content must have:
  - Maximum size of base64 content in each certificate limited to 6144 bytes,
  - Maximum number of certificates allowed in a certificate chain input as 10.
- For both single certificate and a chain of certificates, the input should end with a new line.
- If a file with the same name as the certificate file name already exists inside /data/intdatastore/uploads directory, the user gets an appropriate error message.

The following are examples to show how to upload certificates:

```
nfvis# system certificate input filepath intdatastore:uploads/apic_em_oneline_02.pem pem-data
 "-----BEGIN
[redacted]
 CERTIFICATE-----\n-----BEGIN
[redacted]
 CERTIFICATE-----\n"
nfvis#
```

```
nfvis# system certificate input filepath
Value for 'filepath' (<string>): intdatastore:uploads/test_cert.pem
Value for 'pem-data' (<string>):
[Multiline mode, exit with ctrl-D.]
> -----BEGIN CERTIFICATE-----
> MIIDvzCCAqegAwIBAgIUKBZWJ4U2c1gBYJFBFWNlNQSVd2MwDQYJKoZIhvcNAQEL
> BQAwgYgxLTArBgNVBAMTJDEyYjQ0ZDhmLWRhZWItNGIxNi1iYWZhLWRiYTQxZGRk
> MWY3MzELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExEDAOBgNVBAcT
> B1Nhbkpvc2UxEzARBgNVBAsTCkFQSUNFTS1TRE4xDjAMBgNVBAoTBUNpc2NvMB4X
> DTE4MDcyMTIwNDMyN1oXDTIzMDcyMDIwNDMyN1owXjEVMBMGA1UEAxMMMTcyLjI1
> LjIxNy44MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQswCQYDVQQGEwJVUzEOMAwGA1UE
> ChMFQ2lzY28xEzARBgNVBAsTCkFQSUNFTS1TRE4wggEiMA0GCSqGSIb3DQEBAQUA
> A4IBDwAwggEKAoIBAQDD616jSBX+DfxI5kGT3JCmcIgOHYDDhJJd1L8qhxDAOM7P
> qLjLEdUCOTap8Lu/dKpVClN+hE0LNr9HyQSZ7Mn8+UrM7wQqTKEA6p3dw323wWbp
> ia/XSgByznj4JEY3xW8/trKGkoxfZ7D2JA/cLTf7hK3v44Nev4ONdKtnwNXV32ms
> E7Mpx/Wb/110hYn37DJ9sN5+o34F1KkF1quaXPOgmQA8PMH2Y1LMOh/Z3g3afali
> uOsbPpeGxawEWgfc5pK5EJbziWy1JUSh/c2DaqrfvnKnlprM/HfjZLgzit9FnLyL
> 0lxW54U77AMDRcNALtSq0G3YDX12pdb+ateFWznFAgMBAAGjSjBIMAkGA1UdEwQC
> MAAwCwYDVR0PBAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAP
> BgNVHREECDAGhwSsGdkIMA0GCSqGSIb3DQEBCwUAA4IBAQAiD3XiYgUTFK0MuxuB
> DYanVIuAPBImqULdidh3uDlnoTUlzDFU+feYug+XHjAPk7rczZ1Yoc5Hvo90/gQU
> WQUd9TftJygftRn4vG4MMb4fjDPqoh7rxj0P51NRJIA64ro6/gvbQn+T70a62/Wt
> sDGIdXhp8MUTzA/R99vxYUS9YfTMFVAEv5KAW9ZRwC+CTPT+YeN0B+iNO3cXmZ3A
> C0YDXgN27yfF/+1Lna1aOMCTXdTFzNCplOIhhWKulM74Re9QN0Lwvkt9PDim3rX+
> GaDvd4nINMcIXRXy40ieQOOv0W9xnYnvgFD3xjhKQhzDEXX1BStXVJwaqAwWlDlY
> 8EdE
> -----END CERTIFICATE-----
> -----BEGIN CERTIFICATE-----
> MIIDrzCCApegAwIBAgIGCMgojJNOMA0GCSqGSIb3DQEBCwUAMIGIMS0wKwYDVQQD
> EyQxMmI0NGQ4Zi1kYWViLTRiMTYtYmFmYS1kYmE0MWRkZDFmNzMxCzAJBgNVBAYT
> AlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRAwDgYDVQQHEwdTYW5Kb3NlMRMwEQYD
> VQQLEwpBUElDRU0tU0ROMQ4wDAYDVQQKEwVDaXNjbzAeFw0xODA3MjEyMDQzMjVa
> Fw00ODA3MTMyMDQzMjVaMIGIMS0wKwYDVQQDEyQxMmI0NGQ4Zi1kYWViLTRiMTYt
> YmFmYS1kYmE0MWRkZDFmNzMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9y
> bmlhMRAwDgYDVQQHEwdTYW5Kb3NlMRMwEQYDVQQLEwpBUElDRU0tU0ROMQ4wDAYD
> VQQKEwVDaXNjbzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALd/HK9i
> 6H45KJ42G3awGiehp5ZJWeUNqbmnkD0eiR6PNJIVNGBGMV3k+SW0kIfTjxIDkqSc
> K+K5tfEtTRc0R+WmgtdT+asDhPOmfmL73POqIXLr2RE98J0FLkcdhpRU2K1/tDu3
> 4+7WBA1OT/uIb9LVkVrk1pwolVKAWfgwBgCfmLmebtNfvexI3hvk2awcl4fmVb+d
> CMGVXHBw+yQW2AE3RH66VebS/E6bc3ifAvXHlWYWMt/tPRQRftH+0ZrgXt/dar5o
> 24Qq8taPwY1UIse41Nnnp1Q+FuoE9elLVmLidVaJ7qraDw5Yi6ZSQNGud813lU8s
> 6RtbNS48SSB3U0MCAwEAAaMdMBswDAYDVR0TBAUwAwEB/zALBgNVHQ8EBAMCAQYw
> DQYJKoZIhvcNAQELBQADggEBAHUddWTSeJR7QLxud9aaoIYzbL8lwJx7Ot49K5So
> RrymEKbrUSGtZaBp+hdam3l2ByDS44OmwDolelMsdIN61hV5o8DgpaJLwMhoY8gS
> HXyUTdpiLQD6RoxNWim6wGJGDTiMZFYaiaz5oFeazzOG7D8qu9agQ+/7Ky0RVkUK
> 6IoZZPSQ4BgBnsKg3OdBSPUWSIB7+rMz6ww5ELNOBIDo+yo0wCNgvmy19QgabM0/
> 5SJc2pMyidQy2yj3h1+DpMlZ6nWPqF+9IZlzoErKYABySH/Stho4l2kMXY5libCi
> AEqsyhYpxeO9S466uzcujQwJFARog2GGO0vJEDICqKm+lDI=
> -----END CERTIFICATE-----
>
nfvis#


nfvis#
nfvis# system certificate input filepath intdatastore:uploads/pnp_cert7.pem
Value for 'pem-data' (<string>):
[Multiline mode, exit with ctrl-D.]
> -----BEGIN CERTIFICATE-----
> MIICLDCCAdKgAwIBAgIBADAKBggqhkjOPQQDAjB9MQswCQYDVQQGEwJCRTEPMA0G
> A1UEChMGR251VExTMSUwIwYDVQQLExxHbnVUTFMgY2VydGlmaWNhdGUgYXV0aG9y
> aXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAjBgNVBAMTHEdudVRMUyBjZXJ0aWZpY2F0
> ZSBhdXRob3JpdHkwHhcNMTEwNTIzMjAzODIxWhcNMTIxMjIyMDc0MTUxWjB9MQsw
> CQYDVQQGEwJCRTEPMA0GA1UEChMGR251VExTMSUwIwYDVQQLExxHbnVUTFMgY2Vy
> dGlmaWNhdGUgYXV0aG9yaXR5MQ8wDQYDVQQIEwZMZXV2ZW4xJTAjBgNVBAMTHEdu
```

```
> dVRMUyBjZXJ0aWZpY2F0ZSBhdXRob3JpdHkwWTATBgcqhkjOPQIBBggqhkjOPQMB
> BwNCAARS2I0jiuNn14Y2sSALCX3IybqiIJUvxUpj+oNfzngvj/Niyv2394BWnW4X
> uQ4RTEiywK87WRcWMGgJB5kX/t2no0MwQTAPBgNVHRMBAf8EBTADAQH/MA8GA1Ud
> DwEB/wQFAwMHBgAwHQYDVR0OBBYEFPC0gf6YEr+1KLlkQAPLzB9mTigDMAoGCCqG
> SM49BAMCA0gAMEUCIDGuwD1KPyG+hRf88MeyMQcqOFZD0TbVleF+UsAGQ4enAiEA
> l4wOuDwKQa+upc8GftXE2C//4mKANBC6It01gUaTIpo=
> -----END CERTIFICATE-----
>
nfvis# config
Entering configuration mode terminal
nfvis(config)# pnp automatic cco disable
nfvis(config)# pnp automatic cco-ipv6 disable
nfvis(config)# pnp automatic dns disable
nfvis(config)# pnp automatic dns-ipv6 disable
nfvis(config)# pnp automatic dhcp disable
nfvis(config)# pnp automatic dhcp-ipv6 disable
nfvis(config)# commit
Commit complete.
nfvis(config)# pnp static ip-address 10.0.0.7 port 443 transport https cafile
/data/intdatastore/uploads/pnp_cert7.pem
nfvis(config)# commit
Commit complete.
nfvis(config)# end
nfvis# exit
```

DPDK support on NFVIS

DPDK support on NFVIS is a network performance feature that

- increases network throughput by allowing applications to pull data directly from the Network Interface Card (NIC) without involving the kernel
- delivers high-performance user-space network I/O by allowing network traffic to bypass NFVIS kernel and directly reach deployed VNFs and service chains, and
- reserves additional cores and memory to enhance system performance.

DPDK support features

DPDK support on NFVIS includes:

- Upgrading existing bridges to enable DPDK
- Upgrading virtual NICs attached to VNFs to enable DPDK
- Upgrading physical NICs to enable DPDK

Once DPDK support is successfully enabled, you can disable DPDK only by resetting NFVIS to factory settings.

DPDK restrictions include:

- You must enable DPDK using the **system settings DPDK enable** command before you commit any other configurations.
- DPDK is not supported on wan-br or wan2-br on any NFVIS platform.
- SR-IOV interfaces and DPDK support: To enable DPDK, every device driver must be supported by DPDK. NFVIS does not support SR-IOV interface upgrade to enable DPDK because SR-IOV device

drivers are not supported by DPDK. If any SR-IOV network has been configured on an interface, that interface will not support DPDK. Also if an SR-IOV interface is attached to a bridge, the bridge does not support DPDK and if a bridge supports DPDK, no SR-IOV interface can be attached to it.

- VNF downtime: When DPDK support is enabled on a system, NFVIS upgrades virtual NICs attached to the VNFs. The VNFs are powered down causing a downtime for the VNF service for a short duration of time. After the upgrade is complete, all VNFs are powered up again.

DPDK support system requirements include:

DPDK support optimizes the performance by utilizing additional resources such as CPU and memory. If NFVIS is not able to acquire additional processing or memory, DPDK support can not be enabled.

Enabling DPDK support requires an additional core from each socket available in the system. Depending upon the number of sockets present in the system, NFVIS acquires an additional core for DPDK support.

DPDK operational status values are:

Table 4: DPDK status values

DPDK Status	Description
disabled	The system is not using DPDK.
enabled	DPDK support is successfully enabled on the system. Additional CPU and memory resources are reserved for DPDK.
enabling	The system is in the process of enabling DPDK.
error	The system is unable to acquire the required resources to support DPDK. All of the resources that were acquired by DPDK are released again.

Configuring DPDK support takes up to a minute and network changes can be observed during the process. NFVIS provides an operational status for DPDK support which indicates if DPDK support is enabled or not.

If DPDK status is in error state, DPDK support can be manually disabled. Before enabling DPDK again, reboot the system to defragment the system memory and increase the chance of resource allocation for a successful configuration.

After enabling DPDK, physical NICs configured with SR-IOV will not be able to interact with DPDK bridges. To add a physical NIC to a DPDK bridge, all SR-IOV networks created on the interface should be removed first. NFVIS will not allow adding an SR-IOV configured interface to a DPDK bridge. For more information, see #unique_139.

DPDK configuration examples

To enable DPDK support:

```
config terminal
system setting dpdk enable
commit
```

To display the operational status that indicates DPDK support, use **show system native settings** command.

```
nfvis# show system settings-native dpdk-status
system settings-native dpdk-status enabled
```

If NFVIS is unable to acquire sufficient resources, it shows an error state, and DPDK configuration can be removed. After removing the configuration, DPDK can be enabled again.

```
nfvis# show system settings-native dpdk-status
system settings-native dpdk-status error

config terminal
no system settings dpdk
commit

nfvis# show system setting-native dpdk-status
system settings-native dpdk-status disabled
```

Storage access

Configure network file system support

Configure Network File System (NFS) to enable file access on remote devices using Remote Procedure Calls (RPC) to route requests between users and servers.

Network File System (NFS) is an application where you can view, store, and update the files on a remote device. NFS allows you 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.

Procedure

Step 1 Mount NFS storage on the system.

Example:

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

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

Step 2 Register images on NFS.

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

To register tar.gz images on NFS:

Example:

```
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.

Step 3 Deploy a VM on NFS.

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

NFS is configured and ready for file operations, image registration, and VM deployment on the mounted storage.

Host System Operations

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

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.

Table 5: Power Management

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

System File Management

Use these commands to list, copy, and delete files within the NFVIS environment.

List System Files

To view a list of files on the system, use the `show system file-list` command.

```
nfvis# show system file-list [disk [local | nfs | usb] ]
```

Table 6: System Files

Disk Type	Files
local	Files present in the internal datastore and external datastores

Disk Type	Files
nfs	Files on NFS
usb	Files on the mounted USB drive

Copy System Files

To copy a file from the USB drive to the /data/intdatastore/uploads directory, use the `system file-copy` command. To copy a VM image from the USB drive:

```
configure terminal
system usb-mount mount active
system file-copy usb file name usb1/package/isrv-universalk9.16.03.01.tar.gz
commit
```

The `system file-copy` command can also be used to copy a file from the given source path to the given destination path.

The allowed directories for source path and destination path are:

- /data/intdatastore
- /mnt/extdatastore1
- /mnt/extdatastore2
- /mnt/extdatastore3
- /data/mount

```
nfvis# system file-copy source <path-to-source-file> destination <path-to-destination-file>
```

Delete System Files

The `system file-delete` command is used to delete a file from one of these directories: /data/intdatastore, /mnt/extdatastore1, /mnt/extdatastore2, /mnt/extdatastore3, /mnt-usb/ or /data/mount.

```
nfvis# system file-delete file name
/data/intdatastore/uploads/isrv-universalk9.16.03.01.tar.gz
```

Secure Copy (SCP)

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.

Syntax: **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 Network Function Virtualization Infrastructure Software Command Reference.

SCP between two NFVIS devices is not supported.

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
```

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
```

Backup and Restore NFVIS and VM Configurations

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 and restore a single VM, use vmExportAction (for VM backup) and vmImportAction (for VM restore) APIs.
- Perform the following hostaction backup that avoids loss of VMs during hostaction restore due to insufficient disk space:
  1. Stop the functioning of the VMs that are associated with Cisco NFVIS.
  2. Perform individual image backups of the VMs using the **vmExportAction** command.
  3. Once the backup is successful, delete the VMs and the images from Cisco NFVIS.
  4. When you delete the VMs and the images, perform a host level backup with configurations-only option using the command **hostaction backup configuration-only file-path** *extdatastore2:sample-dir/sample* .
  5. Copy the backup files to a file server.
  6. Perform a factory reset using the **factory-default-reset** command.
  7. Paste the backup copied to a file server and restore the host level backup file using the **hostaction restore** *file-path extdatastore2:sample-dir/sample.bkup* command.
  8. When the restore fails due to disk storage issues, restore the configurations-only backup. When the restore is successful, restore the VMs and their images using the **vmImportAction** *importPath /mnt/extdatastore1/tiny_backup.vmbkp* command.

Restrictions for Backup and Restore on 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 taken to backup a VM depends on the option you choose:
  - *configuration-only* - within 1 min.
  - *configuration-and-vms* - depends on the number of VM deployments on your system, system disk write speed, and compress the VM disks into one bundle.
- 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. For example, backup created in Cisco NFVIS release 4.1.1 cannot be used to restore on Cisco NFVIS release 4.2.1.

Feature Comparison Table for Backup and Restore

Backup using hostaction backup:

Feature	NFVIS 26.2.1 Release
Default file location for backup	/data/intdatastore/backup.bkup /mnt/extdatastore1/backup.bkup /mnt/extdatastore2/backup.bkup /mnt/extdatastore3/backup.bkup
VM backup format	Diff disk backup
Registered Image and Flavors	Yes
Status monitoring	Yes
Check disk space before backup	Yes

Restore using hostaction restore:

Feature	NFVIS 26.2.1 Release
Default file location for backup	/data/intdatastore/backup.bkup /mnt/extdatastore1/backup.bkup /mnt/extdatastore2/backup.bkup /mnt/extdatastore3/backup.bkup
Restore images and flavors	Yes
Unique Mac Uid for VM	Yes
Status monitoring	Yes
SNMP v3 user/passphrase restore (with uniqMacUid)	If system engine ID is the same as backup, restore all v3 users. If system engine ID is different from backup, ignore v3 users restoration.
SNMP engine ID restore on different system	Engine ID changed to same as backup bundle

VM backup using vmExportAction:

Feature	NFVIS 26.2.1 Release
VM backup format	Diff disk backup

Backup and Restore

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 and save into datastore, or mounted USB storage device. Without specifying, the backup file will have *.bkup* extension.

Action	Backup configuration-only	Backup configuration-and-vms
Save system configurations	Yes	Yes
Save system upgrade configurations	Yes	Yes
Save system upgrade file	No	No
Save images and flavors configurations	Yes	Yes
Save image disks	No	Yes
Save deployments configurations	Yes	Yes
Save deployments disks	No	Yes

The following examples shows the backup options:

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

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

The following example shows the backup stored on a USB:

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

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

Use the **show hostaction backup status** command to view the status of the overall backup 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 backup process is complete:

```
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     ""
nfvis#
```

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. Restoree 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.
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)

Condition	dpdk-disabled while backup	dpdk-enable while backup
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     ""
nfvis#
```

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.

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 fails 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"
nfvis#
```

- 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
```

Reset to 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:

Procedure

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

Table 7: 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.

Configure banner, message of the day and system time

Configure your banner and message of the day

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

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.

Procedure

Enter global configuration mode and configure the banner and message:

Example:

```
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.

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 with NTP

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.

Procedure

Step 1 Set the system time manually.

Example:

```
configure terminal
```

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

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

Step 2 Set the system time using NTP IPv4.

Example:

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

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

Example:

```
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.

Configure DNS name servers

DNS name servers are used for domain name resolution. Configuring them allows the system to resolve domain names to IP addresses.

DNS name servers configured using the **system settings name-server** command is prepended to DNS name servers provided by a DHCP server automatically. To view the list of configured name servers, use the **show system settings-native DNS** command.

Procedure

Step 1 Configure name servers.

Example:

```
config terminal
system settings name-server 209.165.201.24 209.165.201.23 2001:420:30d:201:ffff:ffff:fff4:36
commit
```

Step 2 To update name servers, first unconfigure existing name servers and then configure new ones.

Example:

```
config terminal
no system settings name-server
system settings name-server 209.165.201.23 2001:420:30d:201:ffff:ffff:fff4:33 209.165.201.27
commit
```

Step 3 To unconfigure name servers, use the no form of the command.

Example:

```
config terminal
no system settings name-server
commit
```

The DNS name servers are configured and will be used for domain name resolution. The configured servers are prepended to any DHCP-provided DNS servers.

Configure the IP host

Use this task to specify static mapping between hostnames and IP addresses on the NFVIS host. This configuration allows you to resolve hostnames locally without relying on external DNS services.

Procedure

Step 1 Enter configuration mode

Example:

```
configure terminal
```

Step 2 Configure the IP host mapping.

Define the hostname and its associated IP addresses.

```
ip host test2.com 2.2.2.3 2.2.2.1
```

Step 3 Commit the configuration

```
commit
```

The static mapping between the hostname and the specified IP addresses is saved to the system configuration.