



Managing Backup and Restore Operations

The following topics describe Cisco NFVI management node backup and restore operations.

- [Managing Backup and Restore Operations, on page 1](#)
- [Restoring the Management Node, on page 3](#)
- [Management Node Auto-backup, on page 5](#)

Managing Backup and Restore Operations

The management node hosts critical services such as Cisco VIM REST API, Cobbler for PXE, ELK for Logging/Kibana dashboard, and VMTP for cloud validation in Cisco VIM.

The management node is not redundant during the initial Cisco VIM offering, hence it is recommended to take backup of the management node. Using the saved management node information, you can restore the management node if you are facing any issues with the platform.

Backing up the Management Node

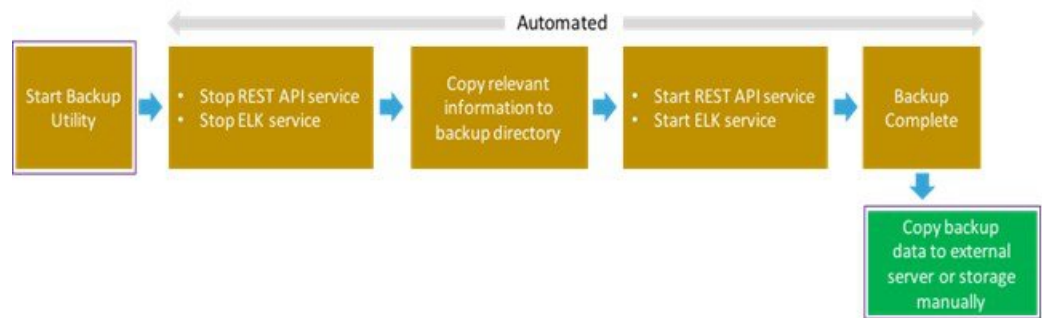
An administrator must maintain the number of back up snapshots on the management node. The backup of the management node is possible only after complete deployment of at least one Cisco VIM. Two copies of backup directories are maintained at the management node itself and the older copy will be overwritten when a next backup is performed.

During the backup operation, activities such as pod management, software update or upgrade, and addition or deletion or replacement of nodes cannot be performed.

The REST API and ELK services are stopped during the backup operation, the OpenStack logs are cached on the control, compute, and storage nodes till the restoration of the management node is completed.

As part of the backup operation, two files are created: `.backup_files` and `.backup_hash`. `.backup_files` is a list of files that are backed up, while the second one is the hash. These two files are placed under the backup directory `/var/cisco/backup_<tag>_<date-time>` at the management node and also at the `/var/cisco/` directory of all three controllers. These two files are used during the restore validation. When user attempt to restore from a particular backup, these two files within this backup are compared to those at the controllers. If there is any discrepancy, the restore validation will fail and user will be prompted to either terminate the restore operation or continue despite the validation failure. Only one copy of the `.backup_files` and `.backup_hash` are kept at the controllers, that is every time a new backup is created, these two files are overwritten with the most recent ones. Hence the restore validation will only pass when the latest backup is used for restore.

Figure 1: Cisco NFVI Management Node Backup Operation

**Before you begin**

- Save the management node information (for example, IP address of the management node) for use during the restore operation.
- Ensure that you have the br_mgmt and br_api IP addresses and respective network information.

Step 1 Launch a SSH session to the Cisco NFVI management node.

Step 2 Navigate to the <installer-ws>/tools/mgmt/ directory.

Step 3 Execute **mgmt_node_backup.py**.

What to do next

The backup operation takes approximately 30 minutes and creates the backup_<tag>_<date-time> directory in the /var/cisco/ path.

Copy the directory to a remote server to recover the management node using rsync.

For example, to copy the backup directory to the remote server 20.0.0.5 /var/cisco/directory , execute the following command sequence:

```
rsync -e ssh -rtvpX --numeric-ids /var/cisco/backup_2017-01-09_14-04-38
root@20.0.0.5:/var/cisco/
```



Note On the remote server, protect the backup directory for any unauthorized access as the backup files may contain sensitive information

At the remote server, change directory to where the backup directory is copied to; in this example /var/cisco/backup_<tag>_<date-time>/.

To verify if the backup is not corrupted or modified, execute **./check_integrity**.

Check_integrity depends on the following packages, they should be installed on the server where check_integrity is executed.

```
python-prettytable
python-jinja2
```

```
python-babel
python-markupsafe
python-setuptools
pytz
```

Backup with Forwarding ELK logs to External Syslog Server

When the feature Forwarding ELK logs to External Syslog Server is enabled, during the backup process, in both the auto-backup and manual backup, the ELK logs are not collected. For manual backups, user can override by appending the `-a` or `--add-elk` option to the backup command. The `-s` or `--skip-elk` option is to skip the ELK logs collection regardless of the forwarding feature is enabled or not.

```
# cd installer/tools/mgmt
# ./mgmt_node_backup.py --help
Usage: ./mgmt_node_backup.py [options]
Options:
  -h, --help            show this help message and exit
  -s, --skip-elk        do not collect ELK logs during backup
  -a, --add-elk         force to also collect ELK logs on backup
```

Restoring the Management Node

As an administrator, you have to re-image the management node with the same ISO version when the backup is performed, before initiating the restore operation. Restore will fail when there is a version mismatch.

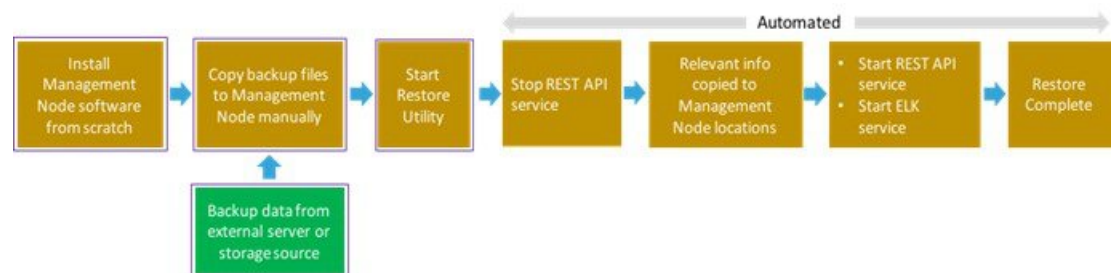


Note Version checking is available only for offline installation.

As part of the restore operation, system checks for management node's IP address information to match the prior configuration. Logs are cached on the control, compute and storage nodes from the moment of the management node fails until its restoration.

If you are using Cisco VIM Insight (in Tech Preview), in the same management node, you will have to re-bootstrap it for installation. During installation, RBAC and Pod registration information will be lost, hence it is advised to make a note of the RBAC and Pod information.

Figure 2: Cisco NFVI Management Node Restore Operation



Before you begin

Ensure that you have the `br_mgmt` and `br_api` IP addresses of the failed management node.

- Step 1** Re-image the management node with the ISO version with which you want to restore the node, and with the same IP address that is used before the failure of the node.
- Step 2** Navigate to /var/cisco/directory at the remote server where the backup directory is copied during the backup operation. Execute `./check_integrity` to verify if the backup is not corrupted or modified.
- Step 3** Copy the backup file to the /var/cisco/directory of the re-imaged management node.
- For example, to copy the backup directory from the remote host 20.0.0.5 to the management node /var/cisco/directory, execute the following command sequence:
- ```
rsync -e ssh -rtvpX --numeric-ids root@20.0.0.5:/var/cisco/backup_2017-01-09_14-04-38 /var/cisco/
```
- Step 4** Navigate to the backup directory and execute the following command to verify if the backup is not corrupted or modified.
- ```
# cd /var/cisco/backup_<date-time>
# ./check-integrity
```
- Step 5** In /var/cisco/backup_<date-time> directory, execute the following command:
- ```
/var/cisco/backup_<date-time> # ./restore
```
- The restore operation takes around 45 minutes.
- Step 6** Before restoration, the restore script performs validation of the backup directory. If validation fails, restore operation will be halted and an error message will be displayed. The script will also verify the last performed backup directory in the Management Node, and if any defects are detected, the user needs to confirm to proceed with restore operation.

```
...
2017-02-02 21:25:23 INFO Starting Cisco VIM restore...
2017-02-02 21:25:23 INFO Cisco VIM restore: estimated run time is approx. 45 mins...
2017-02-02 21:25:23 INFO Please see progress log for restore at
/var/log/mercury/installer/restore_2017-02-02_21:25:23.log
2017-02-02 21:25:27 ERROR Error: Backup id is not the one expected
Error: Found hashID file only in controller(s): j10-controller-2, j10-controller-3
Management backup files are ok (as per j10-controller-2)
Management backup files are ok (as per j10-controller-3)
The management node changed after the last backup was stored. Do you still want to proceed restoring
this management node? [Y/n] y
2017-02-02 22:17:55 INFO Workspace restored to /root/installer-6518
2017-02-02 22:17:55 INFO Cisco VIM restore: Executing restore playbook ...
2017-02-02 22:18:47 INFO Cisco VIM restore: Executing bootstrap playbook ...
```

**Note** The default behavior is to continue by keying **Return** or **Y**. Keying **N** will abort the restore operation.

```
...
2017-02-02 21:25:23 INFO Starting Cisco VIM restore...
2017-02-02 21:25:23 INFO Cisco VIM restore: estimated run time is approx. 45 mins...
2017-02-02 21:25:23 INFO Please see progress log for restore at
/var/log/mercury/installer/restore_2017-02-02_21:25:23.log
2017-02-02 21:25:27 ERROR Error: Backup id is not the one expected
Error: Found hashID file only in controller(s): j10-controller-2, j10-controller-3
Management backup files are ok (as per j10-controller-2)
Management backup files are ok (as per j10-controller-3)
The management node changed after the last backup was stored. Do you still want to proceed restoring
this management node? [Y/n] n
Aborting the restore operation as per user request
```

Once restore operation ends, several health check points will be automatically executed and the summary of results for that particular cloud reachability will be display.

- Step 7** User can run the following checks manually to verify the status of the restore:

- Check the status of the REST API server:

```
cd installer-<tagid>/tools
#./restapi.py -a status
Status of the REST API Server: active (running) since Thu 2016-08-18 09:15:39 UTC; 9h ago
REST API launch directory: /root/installer-<tagid>/
```

- Check the setup\_data and runtime consistency of the management node:

```
cd installer-<tagid>/; ./ciscovimclient/ciscovim run --perform 1,3 -y
```

- Execute the cloud sanity command:

```
cd installer-<tagid>/tools
./cloud_sanity.py -c all
```

## Management Node Auto-backup

After the successful completion of certain Pod management operations, a backup of the management node is performed automatically. Only one copy of the auto-backup directory is kept at /var/cisco/ at any given time. The directory format is autobackup\_<tag>\_<timestamp>

Below is a list of operations:

- Fresh install of Cisco VIM
- Commit an update
- Replace controller
- Add or Remove compute nodes
- Add or Remove storage node
- Reconfigure
- NFVIMON

Enabling or disabling the variable auto-backup, is defined in the setup\_data.yaml file. It is enabled by default.

Add the following setup-data.yaml file snippet:

```
#####
AutoBackup configuration
#####
#Default is True
#autobackup: True or False
```

The following tables shows when an auto-backup is performed during update or rollback or commit.

| POD operation | Auto-backup performed |
|---------------|-----------------------|
| Update        | No                    |
| Rollback      | No                    |
| Commit        | Yes                   |

|                                |    |
|--------------------------------|----|
| Update fail with auto rollback | No |
|--------------------------------|----|

After successful auto-backup directory creation, user can copy it to an external server for later restoration as mentioned in [Restoring the Management Node](#).

During the auto backup, if **Forwarding ELK logs to External Syslog server** option is enabled, the ElasticSearch database will not be maintained and the ELK logs will not be recovered after restoring the management node.