DRIVENETS®

DNOR Architecture and Commissioning Guide

Contents

About DNOR

DriveNets Orchestration system (DNOR) is a comprehensive management suite for planning, operating, and troubleshooting DriveNets Network Cloud. DNOR is designed to address disaggregated network management challenges and provide a unique automation toolset to orchestrate next-generation hyper-scalable networks in a simple and user-friendly manner. DNOR offers Zero Touch Provisioning for Network Cloud deployment, configuration provisioning, and life cycle management operations such as software version control. In addition, DNOR provides Network Cloud inventory and topology views that enable in-depth visibility of the Network Cloud building blocks. DNOR's service assurance capabilities such as: fault management and analytics, performance monitoring, network KPI management, and auto-healing enable the detection and correction of problems in an automated fashion contributing to reductions in OpEx. DNOR's cloud-native micro-service based architecture enables support for any Network Cloud scale. DNOR provides northbound APIs that allow easy integration with third-party orchestration systems, OSS/BSS, and Inventory management systems.

DNOR's main features are:

- **NCE management**: Enables you to create, edit, upgrade, or delete NCEs. Update NCCs and view NCE configuration and update the In-band and Out-of-band configuration.
- **Stacks & Packages**: Repository of software images used to upgrade DNOS software on the NCEs. After the images have been added to the repository, an NCE can be upgraded from NCE Management.
- **Site management**: Enables you to create and delete sites.
- **Zero-touch provisioning**: Install equipment in your network automatically, without manual intervention.
- **Cluster view**: DNOR automatically discovers the NCE nodes based on the NCC configuration and physical connections.
- **DNOR redundancy**: When two DNORs are used, one serves as the active DNOR while the other is in standby. DNOR automatically detects the presence of its mate and allows you to monitor the synchronization status and manually switchover to the redundant DNOR at the click of a button.
- **Fault management**: Fault management systems (e.g. Syslog server), DNOR provides a live display of alerts for every NCE in the DriveNets Network Cloud architecture.
- **NCE upgrade**: With DNOR, you can upgrade the DNOS software version of any DriveNets NCE. Select from the versions that are available for upgrade and monitor the success of the upgrade process.

- **Hardware inventory**: detailed hardware information of all NCEs in your network, such as location, model, and device status.
- **Physical topology**: Provides a live view of the nodes, their states, formation, and internal port connectivity. Physical topology also enables you to drill down into the node to view the internal node states such as CPU and memory use, internal temperature, PSU, and the software versions installed on the node.
- **Message center**: Presents system notifications.
- **System Configuration**: Manage your redundant DNOR servers, viewing the last time they were synchronized, and their status. Configure log retention policies, timeout policies, and user access policies.

DNOR Installation

Make sure all of the prerequisites are installed / complete prior to the DNOR installation. During installation DNOR validates that the Docker and jq prerequisites are installed, and prompts for the user to run installation commands to install them from the installation package.

You must install the primary DNOR server first, then secondary, and finally, the tertiary server. When adding the tertiary server, the primary and secondary servers must be running. DNOR can be installed on a physical server or as a virtual machine.

You can install DNOR on a laptop. For further instructions, see DNOR Installation on a Laptop.

The default user, Superadmin cannot be deleted. It is recommended that once DNOR is installed, the default password is changed. To change a password, see Change the Default User Password in Initial Configuration.

Installation Prerequisites

- Ubuntu 20.04
- Host IP address configured on the host.
- IPv4/IPv6 stack enabled in Ubuntu. (This is enabled by default)
- Docker 19.03.2 (Installed as part of the DNOR package)
- jq (Installed as part of the DNOR package)
- Curl
- wget
- NTP client configured on the host. No specific client or configuration is required.
- IP or FQDN of your primary, secondary and tertiary DNOR servers.
- Hardware according to the System Requirements.

To install DNOR on the host:

1. Log in to the host using SSH and the host IP.

2. Run the wget command to download the dnor_[version].tar package to a local directory:
   wget "[url_of_package_server]" -O /local_directory/dnor_[version].tar

   If you reinstall DNOR, you must download the file to the same local directory so that DNOR can reference the settings within the configuration file.

3. Extract the .tar file. A directory named deploy is created within the local directory:
   tar xvf dnor_[version].tar

4. Navigate to the deploy directory:
   cd /local_directory/deploy/

5. Create a configuration file, based on the configuration template:
   cp dnor.cfg.template dnor.cfg

6. Open the configuration file, in an editor and enter the configuration information:
   vi dnor.cfg

   a. name - enter a name for the server you want to install, e.g dn123.

      Each DNOR server in a cluster must have a unique name.

   b. addr - enter the IP address or FQDN of the DNOR server you want to install.

      Use the same address type on all DNOR servers, do not mix IP with FQDN.

   c. role - enter the role (Primary, Secondary, or Tertiary) of the DNOR server .

   d. keepalive_token - enter a complex password for keepalive authentication, for example 'B}w4k2@5-31g,Od6qJ6[R}5~P41e8Ukm#g'. The same password must be added to the dnor.cfg file on all DNOR servers. The keepalive authentication makes sure that only the DNOR servers with the same keepalive token password can send messages to each other.

      If you leave this field blank during the installation of DNOR on the primary server a complex password is generated automatically. Once the installation has completed, open dnor.cfg and copy the password to use in the dnor.cfg file of the secondary and tertiary DNOR servers. You cannot leave this field blank on the secondary and tertiary DNOR servers.

Never use the same password on different DNOR clusters.

e. primary_addr, secondary_addr, tertiary_addr - enter the IP addresses of the other DNOR servers. When installing a secondary server, but you are not installing a tertiary server, leave the tertiary field blank.

Do not enter an IP addresses in these fields when installing the primary server. You must enter the primary server IP address when installing the secondary server. You must enter the primary and secondary server IP addresses when installing the tertiary server.

Example dnor.cfg file for a primary DNOR server.

```
## Configuration file of DNOR

# DO NOT MODIFY
_version=1.0.1

# DNOR name (label). Make sure to use a unique name per VM/server
name=dnor1

# DNOR FQDN or IPv4 addr. Should be reachable from other DNOR servers
# DO NOT use localhost or 127.0.0.1
addr=dnor1.server.com

# Role of the current node: primary/secondary/teritary
# Required for the first install only.
role=primary

# Auth token for keepalive service
# If no token defined on the first install of 'primary' server, it will be generated automatically
# User then should make sure to copy an exactly the same token to 'secondary' and 'tertiary' configuration files
keepalive_token='6pwbB8pzxD'

# Cluster members
# Can be empty for the first member in the cluster (primary)
# The "tertiary" can be empty for the "secondary" if no "tertiary" exists.
# When configuring "tertiary", both "primary" and "secondary" are mandatory
primary_addr=
secondary_addr=
tertiary_addr=
```

7. Run the command to install DNOR:
   sudo ./install

Repeat the steps above to install the secondary and tertiary DNOR servers.

During the installation of the secondary and tertiary servers:

- Both servers must be running the same DNOR version as the active DNOR.

- Both servers must be able to communicate with the active server.
- The tertiary server must also be able to communicate with the secondary server.

Installation Verification

Verify that the services are up and running, run the following command in the DNOR server. Verify for each service that its status is: **1/1**. Any required service that is not running is displayed as **0/1**. Any service not required is displayed as **0/0**.

> The cold-standby DNOR server does not run all services. To verify that the correct services are up and running, make sure the services: DNOR_keepalive, DNOR_nginx, and DNOR_redis-master have a status of **1/1**.

docker service ls

ID	NAME	MODE	REPLICAS	IMAGE	PORTS
lqtuk28xl6cn	DNOR_curator	global	1/1	dnor-registry.dev.drivenets.net/elk-curator:e4aead6d61	
nbr9efqdqjyh	DNOR_dn-aaa	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2258->2222/tcp, *:9258->9229/tcp
qzkgm9zrorx8	DNOR_dn-backup-and-restore	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2234->2222/tcp, *:9234->9229/tcp
x3cpqbgs9m35	DNOR_dn-cli-management	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2277->2222/tcp, *:9277->9229/tcp
t2811hrj7bx8	DNOR_dn-clusters-connectivity	replicated	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2248->2222/tcp, *:9248->9229/tcp
j7dwuqdspzo1	DNOR_dn-clusters-detailed-view	replicated	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2247->2222/tcp, *:9247->9229/tcp
zbpz80cu7cur	DNOR_dn-clusters-info	replicated	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2246->2222/tcp, *:9246->9229/tcp
jbuahrmngxzc	DNOR_dn-clusters-physical-topology	replicated	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2244->2222/tcp, *:9244->9229/tcp
z4yfsbknelr8	DNOR_dn-clusters-ports-data-topology	replicated	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2245->2222/tcp, *:9245->9229/tcp
65s6sc9f4kmq	DNOR_dn-clusters-upgrade	replicated	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2261->2222/tcp, *:9261->9229/tcp
va83terfjfcv	DNOR_dn-comparison	replicated	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2265->2222/tcp, *:9264->9229/tcp
zicmw3i4l0ee	DNOR_dn-dnor-management	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2233->2222/tcp, *:9233->9229/tcp
qfnv12bgwrma	DNOR_dn-external-request	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2255->2222/tcp, *:9255->9229/tcp
9qknswvsdtu6	DNOR_dn-gpg-cipher	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2250->2222/tcp, *:9250->9229/tcp
9x39j1fpnr3p	DNOR_dn-grpc-client	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2243->2222/tcp, *:9243->9229/tcp
3z3kx5307d9t	DNOR_dn-image-management	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2257->2222/tcp, *:9257->9229/tcp
lne82qye1ki8	DNOR_dn-interfaces-counters	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2241->2222/tcp, *:9241->9229/tcp
90apr17b8o46	DNOR_dn-lock-manager	replicated	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2253->2222/tcp, *:9253->9229/tcp
s0v3bhwikkjy	DNOR_dn-log-analyzer	global	1/1	dnor-registry.dev.drivenets.net/dn-log-analyzer:c9bd3bca58	
2hnslpbxoa3t	DNOR_dn-main-pages	replicated	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2254->2222/tcp, *:9254->9229/tcp
yyn9m34j1x7f	DNOR_dn-monitoring	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2276->2222/tcp, *:9276->9229/tcp
noyucj8ooop2	DNOR_dn-nce-management	replicated	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2252->2222/tcp, *:9252->9229/tcp
crcftzjzdihy	DNOR_dn-netconf	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2262->2222/tcp, *:9262->9229/tcp
a0a0d97ao2xa	DNOR_dn-notifier	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2232->2222/tcp, *:9232->9229/tcp
ki5707ig88ey	DNOR_dn-performance-monitor	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2235->2222/tcp, *:9235->9229/tcp
tr417dji1y41	DNOR_dn-rabbit	global	1/1	dnor-registry.dev.drivenets.net/rabbitmq:3.7.28-19215c5b92	*:5672->5672/tcp
5etdlg0esp60	DNOR_dn-redundancy	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2237->2222/tcp, *:9237->9229/tcp
n5rx1giae38y	DNOR_dn-scheduler	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2229->2222/tcp, *:9229->9229/tcp
z5q1jrv8zm14	DNOR_dn-self-signed-certificate	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2251->2222/tcp, *:9251->9229/tcp
9l4ygjbdkamy	DNOR_dn-settings	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2230->2222/tcp, *:9230->9229/tcp
vnnc0akflwgj	DNOR_dn-simulator	global	0/0	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2256->2222/tcp, *:9256->9229/tcp
y8eleh05jb8j	DNOR_dn-statistics-metadata	replicated	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2242->2222/tcp, *:9242->9229/tcp
rdh9w9wcm5y4	DNOR_dn-storage	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2263->2222/tcp, *:9263->9229/tcp
w5mnx6ud9why	DNOR_dn-sys-log-event	replicated	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2236->2222/tcp, *:9236->9229/tcp
4zabykx3rt2c	DNOR_dn-system-details	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2259->2222/tcp, *:9259->9229/tcp
u84u2e57h41t	DNOR_dn-users	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2231->2222/tcp, *:9231->9229/tcp
76jelsha5pwz	DNOR_dn-web	global	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2264->2222/tcp
yc5n4hw9326o	DNOR_dn-yangs-version-control	replicated	1/1	dnor-registry.dev.drivenets.net/dn-web:dev.15.0.0.78-a0fea3b4fb	*:2249->2222/tcp, *:9249->9229/tcp
l6ylkxa6qjik	DNOR_elk	global	1/1	dnor-registry.dev.drivenets.net/elk:6.7.0-e4aead6d61	*:9200->9200/tcp
swttu8dh0qc2	DNOR_etcd-cluster	global	1/1	dnor-registry.dev.drivenets.net/etcd-python:3.4.13-e4aead6d61	
whsp43fn7xc9	DNOR_etcd-local	global	1/1	dnor-registry.dev.drivenets.net/etcd-python:3.4.13-e4aead6d61	
a1x07rrlmdva	DNOR_haproxy	global	1/1	dnor-registry.dev.drivenets.net/haproxy-patroni:2.2.9-e4aead6d61	*:5433->5433/tcp, *:5436->5436/tcp
9u5ixfhl2euh	DNOR_keepalive	global	1/1	dnor-registry.dev.drivenets.net/keepalive:7f01e6f9c6	
ugf5kk2n4e8t	DNOR_mon-cadvisor	global	1/1	dnor-registry.dev.drivenets.net/google-cadvisor:v0.37.0	
0u0xor200qs0	DNOR_mon-elasticsearch-exporter	global	1/1	dnor-registry.dev.drivenets.net/elasticsearch-exporter:1.1.0	
rgum5l97gndz	DNOR_mon-nodeexporter	global	1/1	dnor-registry.dev.drivenets.net/prom-node-exporter:v1.0.1	
i7802y54jfuj	DNOR_mon-postgres-exporter	global	1/1	dnor-registry.dev.drivenets.net/postgres-exporter:96adf3	
of3souesgxmp	DNOR_mon-prometheus	global	1/1	dnor-registry.dev.drivenets.net/prom-prometheus:v2.24.0	
vs34qut44zm1	DNOR_mon-prometheus-pushgw	global	1/1	dnor-registry.dev.drivenets.net/prom-pushgateway:v1.3.1	
t512hn7p6qif	DNOR_mon-rabbit-exporter	global	1/1	dnor-registry.dev.drivenets.net/rabbitmq-exporter:2c7926	
da7yvv7w42ez	DNOR_mon-redis-exporter	global	1/1	dnor-registry.dev.drivenets.net/redis-exporter:v1.6.1	
m1oqg9er6pry	DNOR_mon-telegraf	global	1/1	dnor-registry.dev.drivenets.net/telegraf:1.19.3	
lacuwf9ipcd5	DNOR_nginx	global	1/1	dnor-registry.dev.drivenets.net/nginx:1.18.0-6e6a3b9eef	
l2bk781kee7s	DNOR_patroni	global	1/1	dnor-registry.dev.drivenets.net/patroni:e4aead6d61	
jd18c4439dgf	DNOR_patroni-tsdb	global	1/1	dnor-registry.dev.drivenets.net/patroni-tsdb:94aaae420c	
bexp64sytn2o	DNOR_promscale	global	1/1	dnor-registry.dev.drivenets.net/timescale-promscale:0.5.1	*:9201->9201/tcp
95sdr0ejf3fh	DNOR_redis-master	global	1/1	dnor-registry.dev.drivenets.net/redis:6.0.9-466da5	

Validate DNOR Role and State

Once DNOR is installed, you can validate the server role, either primary, secondary, or tertiary and its state and status which are determined by the keepalive service. Possible states include:

- Active - Main DNOR server.
- Standby - Second server in the redundancy architecture. Automatically takes over if the active DNOR server fails.
- Cold-Standby - Third server in the redundancy architecture. Can be manually promoted if one of the two other instances fail.
- Fault - Server is in error state.

Possible statuses include:

- Up - Server is up and running.
- Down - Server is unreachable or powered off.
- Fault - Server database is down or invalid and can’t be fixed automatically.
- Versions mismatch - Server is running a different version from the current server.
- In Progress - Changing state, for example from hot-standby to cold standby.

To display the DNOR server role and state, do these steps:

1. Log in to the host using SSH and the host IP.
2. Run the command:
   /opt/drivenets/scripts/dnor_status
   Example output:
   /opt/drivenets/scripts/dnor_status
   {
   "DNOR_VERSION": "15.0.0.69-45df244d19",
   "DNOR_ROLE": "SECONDARY",
   "DNOR_KEEPALIVE": "STANDBY"
   }

Certificate Installation

Once DNOR is running, you must install a certificate to ensure communication is encrypted and secure. To install a certificate on DNOR:

1. Log in to the host using SSH and the host IP.
2. Copy the certificate and its private key to:
   /opt/drivenets/scripts/
3. Run the command:
   sudo /opt/drivenets/scripts/update_certs crt /opt/drivenets/scripts/cert.pem /opt/drivenets/scripts/privkey.pem

   You must perform the certificate installation on each DNOR server if running in a redundant scheme.

Certificate Reset

You can reset the HTTPS certificate to a self-signed certificate if there is a fault with the certificate. For example, this can occur if the certificate has an invalid domain name, which can block access to the DNOR GUI. To reset the certificate to a self-signed certificate, do these steps:

1. Log in to the host using SSH and the host IP.
2. Run the command:
   sudo /opt/drivenets/scripts/update_certs reset

   You must perform the certificate reset on each DNOR server if running in a redundant scheme.

DNOR Installation on a Laptop

There are situations when a mobile DNOR installation is useful. For example, maybe you want to deploy an NCE at a new site, but the main DNOR server isn't ready or there are connectivity issues to the main DNOR server. In these cases, an engineer can visit the site to perform DNOS life-cycle functions such as deploy, upgrade, or delete upgrade NCEs. The engineer uses DNOR installed on a laptop and an out-of-band connection. Once the NCEs are running and connectivity to the main DNOR is available, the engineer can configure the NCCs with the main DNORs IP address and the NCEs will be managed by the main DNOR server.

Laptop System Requirements

Requirements	Size
RAM	16GB
Disk	400GB SSD
CPU	Intel Core i5 or equivalent.
Host Operating System	Windows, MacOS, Linux, Solaris. For more information see virtualbox.org
One Virtual Machine	VirtualBox 7.0.6 and higher
Guest OS (Operating System Hosting DNOR)	**Ubuntu 20.04 LTS** *Currently Ubuntu 22.04 LTS is not supported*
Laptop resources dedicated to Ubuntu VM	At least 8 cores for VM At least 128 GB disk space At least 8GB RAM

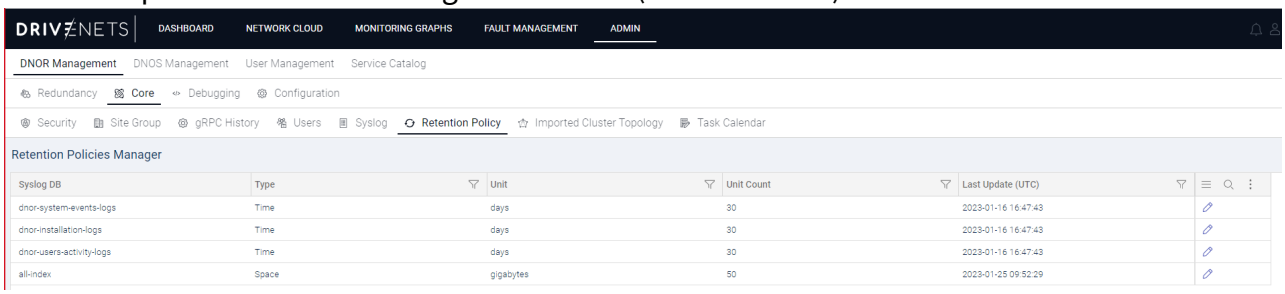
Prerequisites

- VirtualBox VM is installed on the host Operating System.

DNOR Laptop Limitations

The installation of DNOR onto a laptop has the following limitations:

- Manages two NCEs.
- No redundancy, as it is a single DNOR server.
- Fault management information configured for one month (default).
- Traffic statistics information configured for one month (default).
- Syslog collection information configured for one month (default).
- All-index space information configured to 50Gb (default 100Gb).



- DNOR/NCE tech-support generation should be limited to three files created per system (more than three files may cause an issue with storage capacity).
- Configuration backup should be limited to four files (default) per NCE being created (above four files may cause an issue with storage capacity).

Virtual Machine Installation

To run DNOR on a laptop requires the use of a virtual machine. In the procedure below DriveNets use VirtualBox.

1. Download and install the latest version of VirtualBox from https://www.virtualbox.org/wiki/Downloads
2. Download and install Ubuntu 20.04 LTS .ISO from https://releases.ubuntu.com/.
3. Click New from the Create Virtual Machine window.
4. Enter a name for your virtual machine.
5. Select the Ubuntu ISO image file.
6. Click Next.
7. Enter a username and password for the Guest OS installation.
8. Click Next.
9. Select Hardware resources for the guest operating system.
10. Click Next.
11. Create a Virtual Storage.
12. Click Next.
13. Configure the Static IP address reachable to NCEs (Firewall/Ports/etc.) - SCREENSHOT WILL BE PROVIDED BY HAJ
14. Validate the configuration in the Summary and click Finish to create the guest.

DNOR Installation Prerequisites

- Host IP address configured on the host.
- IPv4/IPv6 stack enabled in Ubuntu. (This is enabled by default)
- Docker (Installed as part of the DNOR package)
- jq (Installed as part of the DNOR package)
- Curl
- wget
- NTP client configured on the host (optional). If you choose not to configure NTP, you are required to maintain the same time between DNOR and the NCE. No specific client or configuration is required.

DNOR Installation

1. Log into the Ubuntu virtualbox.

2. Download the dnor_[version].tar package and insert it into the virtualbox storage.

3. Extract the .tar file. A directory named deploy is created within the local directory:
   tar xvf dnor_[version].tar

4. Navigate to the deploy directory:
   cd /local_directory/deploy/

5. Create a configuration file, based on the configuration template:
   cp dnor.cfg.template dnor.cfg
6. Open the configuration file in an editor and enter the configuration information:
   vi dnor.cfg
   a. name - enter a name for the server you want to install, e.g dn123.
   b. addr - enter the IP address of the DNOR server you want to install.
   c. role - enter the role of the DNOR server as Primary.
   d. keepalive_token - generated automatically during the initial installation.
   e. primary_addr - Do not enter any IP information. Leave this blank.
   Example dnor.cfg file for a primary DNOR server.

```
## Configuration file of DNOR
# DO NOT MODIFY!
_version=1.0.1

# DNOR name (label).
Make sure to use a unique name per VM/server
name=dnor1
# DNOR IPv4 addr. Should be reachable from other DNOR servers
# DO NOT use localhost or 127.0.0.1
addr=164.1.1.1

# Role of the current node: primary
# Required for the first install only.
role=primary

# Auth token for keepalive service
# Token will be generated automatically
keepalive_token='6fRDbh2xx'
```

7. Run the command to install DNOR:
   sudo ./install

Connect the DNOR Server to the NCE

When a DHCP server is available:

- USB to ethernet adapter (if the laptop has an Ethernet port you do not need an adapter) + 5m CAT6E cable - Connect directly to the NCC management port in a cluster formation or an IPMI port for a standalone NCE formation. Follow this procedure to configure the NCC and add the DNOR server IP address.

When no DHCP server is available:

- USB to console adapter + 5m CAT6E cable - Standalone formations - connect directly to the NCP console to configure a static IP address of the NCC management port. Follow this procedure to configure the NCC and add the DNOR server IP address.
- USB to ethernet adapter (if the laptop has an Ethernet port you do not need an adapter) + 5m CAT6E cable - Cluster formations - connect directly to the NCC using the iLO/iDRAC port in a cluster formation to configure a static IP address of the NCC Or follow this procedure to configure the NCC and add the DNOR server IP address.

Upload Software to DNOR

Before an upgrade or deploy life-cycle function can be performed you must create a software stack.

Import a Package

User role:

This process is not traffic affecting.

To add a package to DNOR to be used to create a stack, do these steps:

1. Select Admin from the Main menu.
2. Select DNOS Management > Core >Stacks & Packages from the menu.
3. Click Actions 

.
4. Select Import Package.
5. Select either:
   a. Select Files (checked by default) - to browse to the package location and upload them.
   b. Provide URL - to provide one or more URLs where the packages reside to upload them.
6. The Create new stack from the imported package, option is checked by default. It displays the original bundle as delivered by DriveNets. This option retains the entire bundle in a DNOR stack.
7. Click Import.

Create a Stack

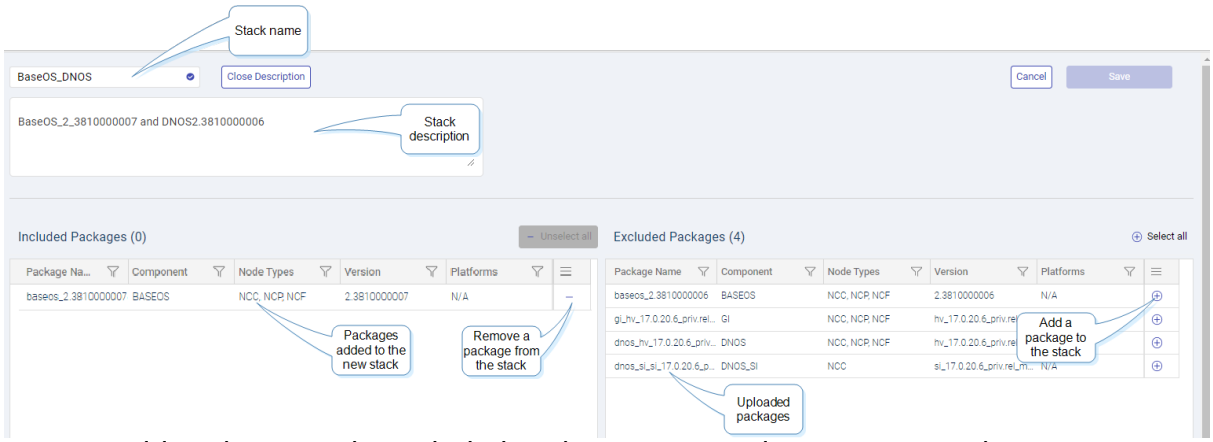
User role:

This process is not traffic affecting.

Stacks are formed from an imported package or packages. DNOR uses a Stack to deploy and upgrade NCEs. To create a Stack from a previously uploaded package, do these steps:

To save space on the nodes, if you use bundle_<version>_full.tar as the source file, create a stack which includes only the packages you want to install on the NCE.

1. Select Admin from the Main menu.
2. Select DNOS Management > Core > Stacks & Packages from the menu.
   a. Click Actions Actions .
   b. Select Add Stack. The package selector is displayed.
   c. Enter a name for the Stack.



   d. Use + to add packages to the Included Packages pane and - to remove packages.
   e. Click Save to create the Stack.

DNORUpgrade

The DNOR upgrade process maintains existing data such as statistical counters, syslog, and configuration data in a snapshot. DNOR uses a multi-node redundancy scheme to improve business continuity as two instances are running in an active-standby configuration whilst a third cold-standby server is ready to be promoted if one of the two other instances fail. Prior to the upgrade process starting DNOR saves the DNOR configuration in /opt/db-backup/upgrade/. The configuration file includes:

- NCE configuration
- DNOS management configuration, such as security settings, self-signed certificate, and GNMI settings

- DNOR management configuration, such as site, user management, AAA configuration, security, and Syslog settings

The configuration does not include:

- DNOS images
- Alarms
- Syslog files
- Statistics
- Tech support files
- Previously backup configuration files

You cannot upgrade from DNOR versions v14.2 and earlier to v15.1 and above.

DNOR can be upgraded from DNOR 15.1 to the latest version.

It is recommended to copy the configuration from /opt/db-backup/upgrade/ to another location should you need to restore DNOR.

Upgrade Multi-Node Redundant Architecture

When upgrading, you must first update the active node, then the hot-standby, and finally the cold-standby. When performing this procedure on the active DNOR, make sure a switchover is not triggered.

The upgrade procedure removes DNOR's log files that have not been modified in the last 10 days.

To upgrade DNOR on the host:

1. From the active DNOR select Admin>DNOR Management>Redundancy.
2. Click Change to Cold Standby to disable the hot standby server.
3. Log in to the host of the active DNOR using SSH and the host IP.

   To upgrade DNOR you must upgrade the active server, then the hot-standby and finally the cold-standby DNOR servers. When repeating the procedure to upgrade the hot-standby and cold-standby DNOR servers, log into the host of those servers.
4. Run the wget command to download the dnor_[version].tar package to a local directory:
   wget "[url_of_package_server]" -O /local_directory/dnor_[version].tar

You must download the file to the same local directory used for installation so that DNOR can reference the settings within the configuration file.

5. Extract the .tar file.
   tar xvf dnor_[version].tar
6. Navigate to the deploy directory:
   cd deploy

   The settings within the configuration file are retained.

7. Run the command to install DNOR:
   sudo ./install

Repeat the steps 3-7 above to update the hot-standby and cold-standby DNOR servers.

DNOR Restore

Using a copy of the DNOR configuration backup file, you can restore DNOR to the configuration at the time of the backup. The restore must be performed on the same version of DNOR that created the backup. In addition, prior to an upgrade DNOR automatically creates a backup file. The backup files both include the NCE configuration, DNOS and DNOR settings. Depending on the use case, you can use one of these files to restore the configuration if you decide to revert to an earlier DNOR version.

The two backup files are saved in different locations. When a backup of DNOR is performed from DNOR Management > Backup and Restore, the backup file is saved to /opt/db-backup. When an upgrade is performed a backup is automatically saved to /opt/db-backup/upgrade.

There are three restore use cases.

1. You want to restore the DNOR version and configuration to the state prior to an upgrade. This step requires you to uninstall DNOR, install the earlier version, and restore the configuration database. Start here, Restore DNOR Version and then Restore from the Upgrade Backup File.
2. You want to restore the DNOR version and configuration to the state saved to a backup file. This step requires you to uninstall DNOR, install the earlier version, and restore the configuration database. Start here, Restore DNOR Version and then Restore from the Backup and Restore File using the DNOR Interface.

3. You want to restore a DNOR configuration file onto a new DNOR installation. The backup was created using the Backup and Restore feature.

1. Log in to the active DNOR server using SSH and the host IP.

2. Copy the file to the new server, run the command:

scp <local_path> <dnor username@dnor_ip_address:/opt/db-backup>
Example:
scp c:\users\desktop\backupfile jbloggs@10.10.0.2:/opt/db-backup

3. Upload the DNOS images on the newly installed DNOR server. To display the images that must be uploaded navigate to Network Cloud > Reports > Discovered NCEs and check the Conflict List column for " NCE DNOS image [DNOS version] does not exist".
4. Restore from the Backup and Restore File using the DNOR Interface.

The restore must be performed on the same version of DNOR that created the backup file.

When restoring a DNOR configuration, any changes made to the DNOR after the configuration backup file was created will be lost.

Restore DNOR Version

To uninstall DNOR and reinstall the version used by the backup file.

1. Log in to the each DNOR server using SSH and the host IP.
2. Uninstall DNOR. Run the command:
sudo ./uninstall

The uninstall process does not remove configuration files, but it is recommended to copy the configuration files to a local machine before uninstalling DNOR.

3. After DNOR has been uninstalled. Navigate to the configuration file location:
   a. Configuration files generated using DNOR Management > Backup and Restore are stored in `/opt/db-backup`.
   b. Configuration files created prior to an upgrade are stored in `/opt/db-backup/upgrade`.
4. Extract the .tar file.
tar xvf dnor_[version].tar
5. Navigate to the deploy directory:
cd deploy
6. Run the command to restore the DNOR version:
sudo ./install

Perform the steps above on each DNOR server.

Before proceeding, make sure that other than the active DNOR server, the newly installed DNOR servers are in cold-standby mode.

You must upload the DNOS images on the newly installed DNOR server. To display the images that must be uploaded navigate to Network Cloud > Reports > Discovered NCEs and check the Conflict List column for " NCE DNOS image [DNOS version] does not exist".

Restore from the Upgrade Backup File

To restore the database schema for the DNOR version from the backup taken during the upgrade process.

Only perform the database restore on the active DNOR server.

1. Log in to the host of the active DNOR using SSH and the host IP.

   Any data changes from the time the snapshot was taken (during the upgrade) to the time the database is restored will be lost.

2. Restore the database:
   /opt/drivenets/scripts/dnor_db -r /opt/db-backup/upgrade/{dnor_config_file_name}.gz
   Example to restore a DNOR 14.0.1.6 database file:
   /opt/drivenets/scripts/dnor_db -r /opt/db-backup/upgrade/14.0.1.6-c30fc07903.gz

Once complete, if applicable, change one of the cold-standby DNOR servers to hot-standby, where it will synchronize the new database schema.

Restore from the Backup and Restore File using the DNOR Interface.

To restore the database schema from the backup taken during the back and restore process.

1. Enter the URL of the DNOR server into a Chrome browser.
2. Navigate to Admin > DNOR Management > Backup and Restore. The backup files previously created by DNOR are not displayed.
3. Click Backup to create a new backup file.
4. Select Restore on the new backup file.
5. Click Yes to continue. The previously created DNOR backup files are displayed.
6. Select Restore on the configuration file to restore the database.

These steps are only required after reinstalling DNOR, otherwise you only need to perform steps 4 and 5, see DNOR Operation Guide Backup and Restore for more information.

DNOR Uninstall

To uninstall DNOR version 11.5.1 and newer, do these steps:

1. Log in to the DNOR host OS using SSH and the host IP.
2. Navigate to the deploy directory:
   cd /local_directory/deploy/
3. Run the command to uninstall DNOR:
   sudo ./uninstall

Initial Configuration

After installation, DNOR is ready for use. The following paragraphs describe the initial steps you must perform to configure DNOR. For details on operating DNOR, see the DNOR Web UI user guide.

The default user, Superadmin cannot be deleted. It is recommended that once DNOR is installed, the default password is changed. To change a password, see Change the Default User Password

Log in to DNOR

User role:

1. Enter the DNOR server address https://<server host/ip> into your browser.
2. Enter the default Superadmin user name and password. See User Management.

Change the Default DNOR User Password

User role:

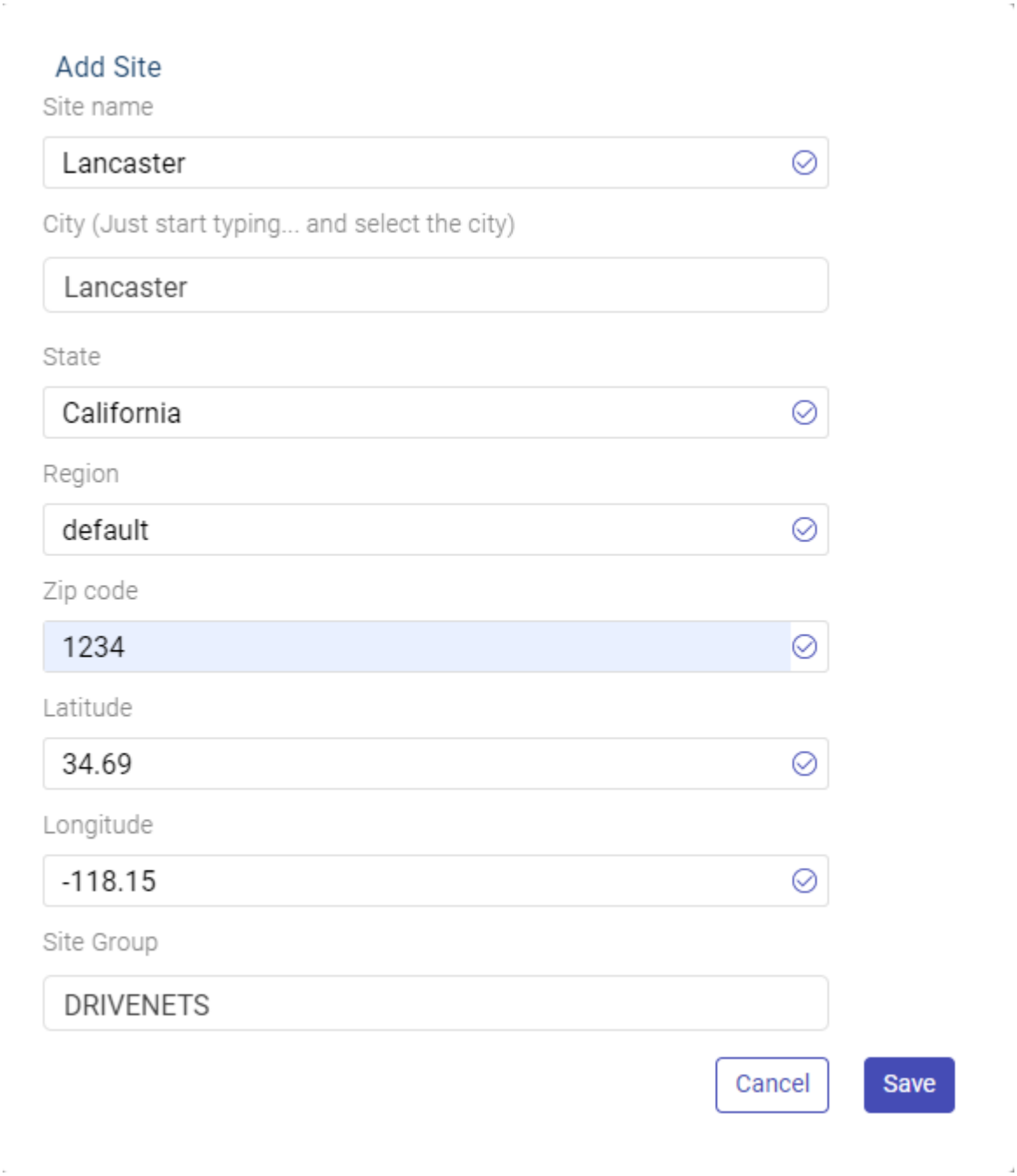
1. Select DNOR Users from the User Management menu.
2. Click the More menu (⋮) of the user you want to change the password.
3. Select Reset Password.
4. Enter the new password twice to confirm they match.
5. Click Change.

Create a Site

User role:

Sites enables the management of the NCEs into logical geographic areas, to create a site. Sites are placed within Regions. The hierarchical structure of the logical areas are Region, Site, and then NCE.

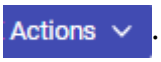
1. Click Network Cloud, from the Main menu.
2. Click Actions  underneath NCE Management.
3. Select Add New Site from the drop-down menu.
4. Enter a name for the site.
5. Enter a city, auto-complete provides a list of cities based on the city name entered. Select the city from the drop-down list. The longitude, latitude and state fields auto-complete based on the city selected.
6. Enter a region. This is a geographical area used to divide your network logically. Enter default to allocate the site to the default region.
7. Enter a Zip code.
8. Enter a Site Group to associate with this site. For more information on Site Groups see Site Group.
9. Click Save to create the site.



Import a Package

User role:

To add a package to DNOR to be used to create a stack, do these steps:

1. Select Admin from the Main menu.
2. Select DNOS Management > Core >Stacks & Packages from the menu.
3. Click Actions 

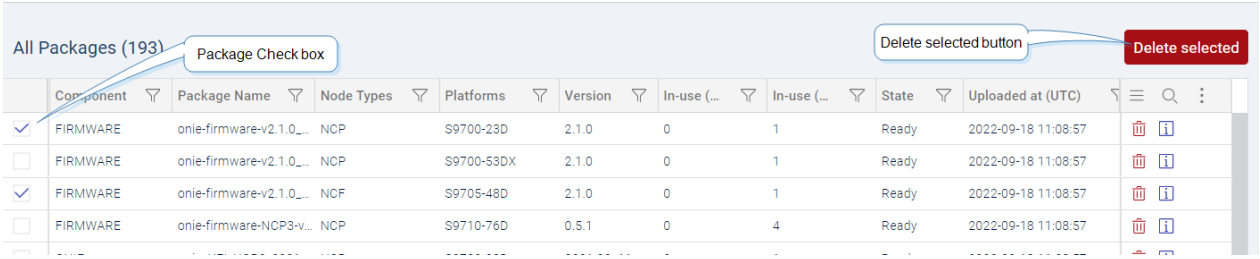
.
4. Select Import Package.
5. Select either:
   a. Select Files (checked by default) - to browse to the package location and upload them.
   b. Provide URL - to provide one or more URLs where the packages reside to upload them.
6. The Create new stack from the imported package, option is checked by default. It displays the original bundle as delivered by DriveNets. This option retains the entire bundle in a DNOR stack.
7. Click Import.

Delete Packages

User role:

To delete one or more packages from a stack, do these steps:

1. Select Admin from the Main menu.
2. Select DNOS Management > Core > Stacks & Packages from the menu.
3. Check the box/es next to the package/s to be deleted. The Delete selected button will appear.



4. Click Delete selected . Re-enter Superadmin Credentials.
5. Click Import Proceed. The package/s will be removed.

If the selected packages are included in a stack, they will be deleted by this action.

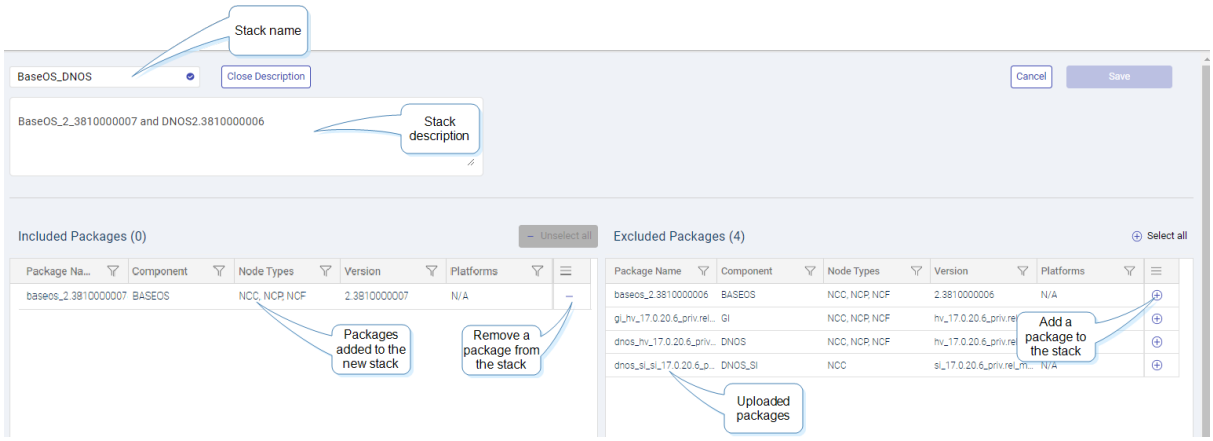
Create a Stack

User role:

Stacks are formed from an imported package or packages. DNOR uses a Stack to deploy and upgrade NCEs. To create a Stack from a previously uploaded package, do these steps:

To save space on the nodes, if you use bundle_<version>_full.tar as the source file, create a stack which includes only the packages you want to install on the NCE.

1. Select Admin from the Main menu.
2. Select DNOS Management > Core > Stacks & Packages from the menu.
   a. Click Actions Actions .
   b. Select Add Stack. The package selector is displayed.
   c. Enter a name for the Stack.



   d. Use + to add packages to the Included Packages pane and - to remove packages.

e. Click Save to create the Stack.

Add an NCE (Network Cloud Element)

User role:

When an NCE is created the profile must include the following:

- NCE name
- DNOS stack
- OOB management IP address for the cluster. (if DHCP is used this is not required)
- NCE formation, either standalone, SA-40C, SA-10CD, SA-36CD-S, or a cluster, CL-16, CL-32, CL-48, CL-51, CL-64, CL-76, CL-96, CL-192 or CL-768.
- The NCC serial number. You can add one NCC per NCE. In a cluster formation, if two NCCs are physically connected, DNOR uses of them to create the active NCC is first, then the second NCC is deployed.

When an NCE cluster or NCP (in the case of a standalone NCE being formed) is connected to the network, the NCC calls to DNOR. DNOR checks through the profiles to find a profile that matches an NCC serial number. When an NCC with a matching serial number is located, DNOS is automatically installed. The NCC then downloads from DNOR the software stack, which contains all of the software packages required to form the NCE.

On a standalone router, the NCC runs within the NCP, and an external NCC is not used. Before the NCE installation process begins, DNOR checks that there is connectivity to the active NCC. DNOR also makes sure the ports are open for connectivity between DNOR and DNOS. If no profile is found for the NCC, the device is displayed in the Discovered NCCs report as unprovisioned. This process can be monitored from the Monitoring tab in NCE Management > NCE Toolbox. The following table describes the system states.

Status	Description
Not Deployed	DNOR is communicating with the NCC, but DNOS has not been deployed.
Deployment	The NCE is being deployed for the first time.

Status	Description
Running	The NCE is running. An NCE is considered running when: • At least one NCC is registered to DNOR. • The NCC is running the docker stack. • DNOS using gNMI is responding to DNOR.
Upgrade	The NCE is being upgraded.
Revert	Revert to the Stack in the displayed in the Revert column in Stack Comparison.
Deletion	NCE is being deleted.
Deployment - Waiting For Equipment	The Create NCE form has been completed, but the equipment has not been physically connected.
Communication Error - Application Out Of Band	A problem with the connectivity between DNOR and the agent on the NCC.

Make sure the packages you want to use to create an NCE are uploaded to DNOR and compiled to form a Stack. For more information see Stacks & Packages.

Make sure the site you want to assign the NCE has already been created. See Create a Site in NCE Management Actions

You can edit an NCE Configuration whilst it is in a *Waiting for Equipment* state. After this stage to change a configuration you must delete the NCE and recreate it.

1. Click Network Cloud from the Main menu.

2. Click Actions  underneath NCE Management.

3. Select Add New NCE from the drop-down menu. The New NCE Profile window is displayed.

   You must complete all fields except the optional Configuration File and OOB IPv6. A blue check-mark () is displayed when the input field fulfills the input criteria.

4. Enter a name for the new NCE.

   The name must be between 4-32 characters. Use letters, numbers or dashes (-).

5. Select the NCE system formation type, either standalone, SA-40C, SA-10CD, SA-36CD-S, or a cluster, CL-16, CL-32, CL-48, CL-51, CL-64, CL-76, CL-96, CL-192 or CL-768.

   When creating a standalone system the NCP fabric ports are disabled, with the exception of SA-36CD.

   For information on the Network Cloud model names, see Supported Hardware in the Documentation Portal.

6. Select the Stack to deploy the new NCE.

   If the Stack does not exist, click Edit () to create the Stack.

7. Add the NCC serial number if the NCC has not been discovered by DNOR or select an NCC from the drop-down list.

   An NCE in a standalone formation only requires one NCC whereas an NCE in a cluster formation can have a second NCC connected for redundancy. When the second NCC is physically connected to an existing NCE it is automatically updated and added to the NCE cluster.

8. Enter the new NCE's network configuration:

   Once the NCE is created you cannot change the OOB IP address function between static IP address allocation and Acquire.

a. Select Out-of-Band Virtual IPv4.

b. Select either:

   i. Static IP from the drop-down list to configure static IPv4 addresses.

   ii. Enter an IP address, subnet mask and default gateway in the x.x.x.x/x format.
   or

   iii. Acquired to enable DNOR to acquire the IP address that the NCE is using after the NCE is created, for example the NCE may use a DHCP issued IP address. Once the NCE has been created, the Out-of-Band configuration will display the NCE IP addresses.

After an NCE is created you cannot change the OOB IP address options between Static IP and Acquire.

If the NCE IP address is updated, either due to a new DHCP address allocation or a static IP address is added on the NCE, the DNOR VIP Out-of-Band configuration is updated to reflect the new NCE IP address.

This IP address is also required for a Standalone configuration and must be different to the configured mgmt-ncc0 IP address (the IP address assigned to the mgmt-ncc0 interface).

c. Select Out-of-Band Virtual IPv6.

d. Select either:

   i. Static IP from the drop-down list to configure static IPv6 addresses.

   ii. Enter an IP address, subnet mask and default gateway in the x:x::x:x/x format.
   or

   iii. Acquired to enable DNOR to acquire the IP address that the NCE is using after the NCE is created, for example the NCE may use a DHCP issued IP address. Once the NCE has been created, the Out-of-Band configuration will display the NCE IP addresses.

After an NCE is created you cannot change the OOB IP address options between Static IP and Acquire.

If the NCE IP address is updated, either due to a new DHCP address allocation or a static IP address is added on the NCE, the DNOR VIP Out-of-Band configuration is updated to reflect the new NCE IP address.

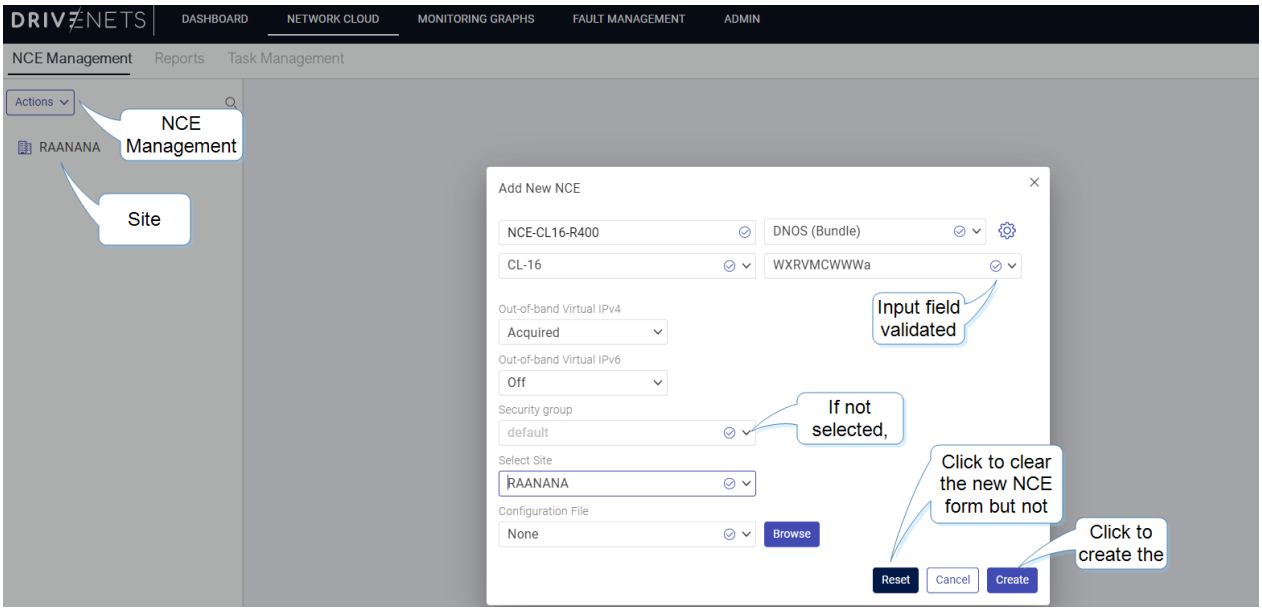
or

iv. Off the default value, to not use IPv6 addresses.

9. Select a security group to add the new NCE to. If no security group is selected, the NCE is added to the default security group. Security groups enable you to manage multiple NCEs with the same account credentials. A security group contains a list of NCEs, an NCE local user, and an optional AAA user which DNOR uses to communicate with the NCEs. When a new NCE is deployed, initially the default security group is used for communication. If communication with the new NCE fails, the selected security group is used instead. Security groups are configured in User Management.
10. Select a site to assign the NCE from the drop-down list.
11. Optional: Select a previously saved DNOS configuration file to be used as a template. This is applied as a configuration commit to the NCE once the new NCE is created. If the commit fails, the Activity Log displays the failed step. A commit failure does not cause the entire deployment to fail.

When using the DNOS configuration file as a template to create a new NCE you must remove router specific configuration settings such as NCE name or IP address before the new NCE is created.

12. Click Create to create the NCE. You can monitor the NCE creation progress from the Maintenance tab.



When the NCE creation is complete, the hardware components that make the NCE are displayed in the Components tab.

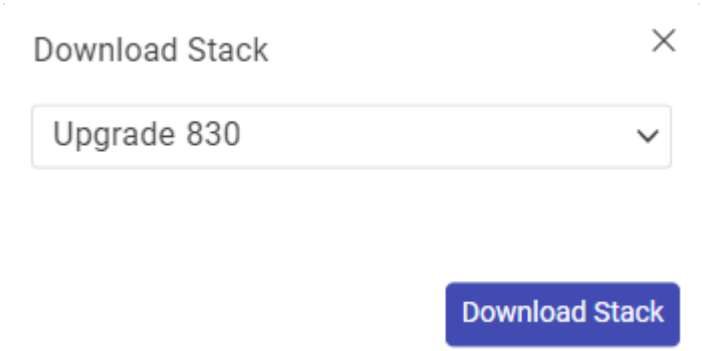
Download the Stack to the NCC

User role:

To download the Stack to the NCC, do these steps:

1. Click Network Cloud from the Main menu. The NCE Management window is displayed.
2. Expand the site which contains the NCE you want to upgrade.
3. Click NCE Actions 

.
4. Select Download Stack. The Download window is displayed.
5. Select the Stack to download from the dropdown menu.



6. Click Download Stack.
7. Enter a Superadmin level user name and password to authorize the download.
8. Click Download.
9. Click the Maintenance tab of the NCE Toolbox to monitor the process. See Monitoring

Set Storage Use

It is recommended to configure the DNOR log and image management based on the available storage. For example, for 10 NCEs, DNOR requires 512GB of storage, and the following configuration:

1. Admin > DNOR Management > Core > Retention Policy

Syslog Database Name	Configuration
dnor-system-events-logs	30 days
dnor-installation-logs	30 days
dnor-users-activity-logs	30 days
all-index	110 Gigabytes

For more information see Retention Policy in the DNOR User Guide.

2. Admin > DNOR Management > Configuration > Statistics Configuration.
   Keep the default settings:

Retention Setting	Default
Chunk size per worker tick	1000
Realtime retention period (minutes)	3
Minute retention period (hours)	3
Hour retention period (days)	3
Day retention period (months)	3
Week retention period (years)	3

For more information see Statistics Configuration in the DNOR User Guide.

It is recommended to follow Security Hardening in the Network Cloud Cluster Deployment guide.

Change History

Date	SW Ver.	Doc Rev.	Change	Affected Topics
29 December, 2022	17.2	1.0	Install DNOR on a laptop	DNOR Installation on a Laptop