

User Guide

for Lenovo ThinkAgile Network Controller 1.0



Note: Before using this information and the product it supports, read the general information in the *Safety information and Environmental Notices* and *User Guide* documents on the *Lenovo Documentation CD*, and the *Warranty Information* document that comes with the product.

First Edition (November 2017)

© Copyright Lenovo 2017

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant a General Services Administration "GSA" contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Lenovo and the Lenovo logo are trademarks of Lenovo in the United States, other countries, or both.

Contents

Preface5
Who Should Use This Guide	6
What You'll Find in This Guide.	7
Typographic Conventions	8
 Chapter 1. Getting Started9
Supported Platforms and System Requirements10
Supported Platforms10
System Requirements10
Installing and Upgrading ThinkAgile Network Controller11
 Chapter 2. Configuring ThinkAgile Network Controller12
Creating a Virtual Network in TNC13
Creating a Floating IP Address Pool.16
Using Security Groups with Virtual Machines (Instances)17
Security Groups Overview17
Creating Security Groups and Adding Rules17
Configuring IPv6 Networks in TNC.18
IPv6 Networks Overview18
Creating IPv6 Virtual Networks in TNC19
Configuring EVPN and VXLAN20
Configuring the VXLAN Identifier Mode.20
Configuring Forwarding21
Configuring the VXLAN Identifier22
Configuring Encapsulation Methods.23
Configuring DNS Servers25
DNS Overview25
Configuring DNS Using the Interface25
Configuring Static Routes with Services28
Configuring Static Routes for Service Instances28
Configuring Static Routes as Host Routes33
Configuring Metadata Service34
Configuring Service Chaining35
Service Chaining Overview.35
Load Balance Service Chain Example35
Configuring Source Network Address Translation (SNAT).39
SNAT Overview39
Associating a Floating IP to a VM40
Multicast Support.42
All-Broadcast/Limited-Broadcast and Link-Local Multicast42
All-Broadcast/Limited-Broadcast Example42
Link-Local Multicast Example.42
Host Broadcast43
TNC Analytics Application Programming Interfaces (APIs) and User-Visible Entities (UVEs)44

Chapter 3. Monitoring the System	45
Infrastructure menu	46
Infrastructure>Dashboard	47
Networking menu	48
Networking>Dashboard	49
TNC Commands	51
Viewing Node Status	51
Syntax	51
Privilege level	51
Sample Output	51
Viewing Version Information.	52
Syntax	52
Privilege level	52
Sample Output	52
 Appendix A. Getting help and technical assistance.	 53
 Appendix B. Notices	 55
Trademarks	56

Preface

Lenovo ThinkAgile Network Controller is a SDN solution from Lenovo which provides network virtualization with service chaining capability to offer flexibility, agility and scalability needed for modern cloud data centers.

Lenovo ThinkAgile Network Controller is based on the OpenContrail R3.2 release.

This release supplement provides the latest information regarding Lenovo ThinkAgile Network Controller 1.0 (referred to as TNC throughout this document).

Who Should Use This Guide

This guide is intended for network installers and system administrators engaged in configuring and maintaining a network. The administrator should be familiar with Ethernet concepts, IP addressing, and virtualization.

What You'll Find in This Guide

This guide will help you plan, implement, and administer the Lenovo ThinkAgile Network Controller 1.0. Where possible, each section provides feature overviews, usage examples, and configuration instructions. The following material is included:

- [“Getting Started” on page 9](#)
- [“Configuring ThinkAgile Network Controller” on page 12](#)
- [“Monitoring the System” on page 45](#)

Typographic Conventions

The following table describes the typographic styles used in this book.

Table 1. *Typographic Conventions*

Typeface or Symbol	Meaning	Example
ABC123	This type is used for names of commands, files, and directories used within the text. It also depicts on-screen computer output and prompts.	View the readme.txt file. NE10032#
ABC123	This bold type appears in command Example. It shows text that must be typed in exactly as shown.	NE10032# sys
<ABC123>	This italicized type appears in command Example as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets. This also shows book titles, special terms, or words to be emphasized.	To establish a Telnet session, enter: NE10032# telnet <IP address> Read your <i>User's Guide</i> thoroughly.
{ }	Command items shown inside brackets are mandatory and cannot be excluded. Do not type the brackets.	NE10032# ls {-a}
[]	Command items shown inside brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	NE10032# ls [-a]
	The vertical bar () is used in command example to separate choices where multiple options exist. Select only one of the listed options. Do not type the vertical bar.	NE10032# set {left right}
AaBbCc123	This block type depicts menus, buttons, and other controls that appear in Web browsers and other graphical interfaces.	Click the <Save> button.

Chapter 1. Getting Started

This chapter discusses the following topics:

- [“Supported Platforms and System Requirements” on page 10](#)
- [“Installing and Upgrading ThinkAgile Network Controller” on page 11](#)

Supported Platforms and System Requirements

Supported Platforms

Lenovo ThinkAgile Network Controller supports the following platforms and operating system versions:

Table 2. *Supported Platforms*

OpenStack Release	Operating System
OpenStack Newton	Red Hat RHEL 7.3 Linux

System Requirements

Lenovo ThinkAgile Network Controller solution requires three servers with the following minimum system requirements:

- 256 GB memory
- 500 GB hard drive
- 16 CPU cores
- Two Intel Ethernet ports (82599 or newer)

In the PoC environment, Lenovo ThinkAgile Network Controller can support the following minimum requirements:

- 32 GB RAM
- 350 GB hard drive
- 8 CPU cores
- Two Intel Ethernet ports (82599 or newer), or E1000/VXNET3 compatible vNICs in the virtual environment

Installing and Upgrading ThinkAgile Network Controller

The Lenovo ThinkAgile Network Controller is installed on multiple servers. The base software image is installed on all servers to be used and provisioning scripts are run to launch role-based components of the software.

Note: A similar procedure is used to upgrade an existing software version to a newer one.

The role-based components are the following:

- *cfgm*: TNC configuration manager (config-node)
- *openstack*: OpenStack services such as Nova, Quantum etc
- *collector*: Monitoring and analytics services
- *compute*: vRouter service and tenant virtual machines (VMs) launcher
- *control*: Control plane service
- *database*: Analytics and configuration database services
- *webui*: Administrator web-based user interface service

Note: Usually, the roles are run on multiple servers. A single node can have multiple roles. For testing purposes, the roles can also run on a single server.

Chapter 2. Configuring ThinkAgile Network Controller

This chapter provides configuration background and examples for using the TNC to perform network virtualization functions. The following topics are addressed in this chapter:

- [“Creating a Virtual Network in TNC” on page 13](#)
- [“Creating a Floating IP Address Pool” on page 16](#)
- [“Using Security Groups with Virtual Machines \(Instances\)” on page 17](#)
- [“Configuring IPv6 Networks in TNC” on page 18](#)
- [“Configuring EVPN and VXLAN” on page 20](#)
- [“Configuring DNS Servers” on page 25](#)
- [“Configuring Static Routes with Services” on page 28](#)
- [“Configuring Metadata Service” on page 34](#)
- [“Configuring Service Chaining” on page 35](#)
- [“Configuring Source Network Address Translation \(SNAT\)” on page 39](#)
- [“Multicast Support” on page 42](#)
- [“TNC Analytics Application Programming Interfaces \(APIs\) and User-Visible Entities \(UVEs\)” on page 44](#)

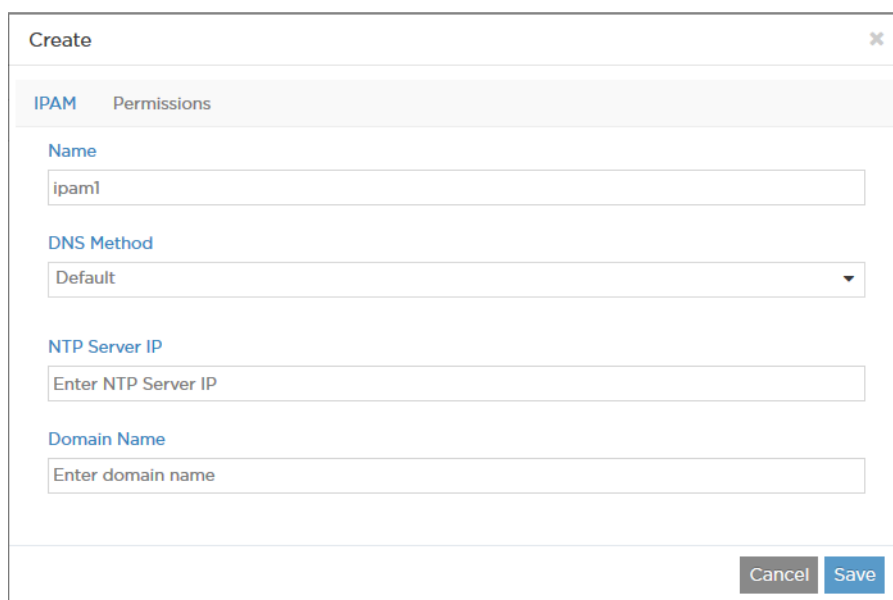
Creating a Virtual Network in TNC

TNC offers the possibility to create networks and network policies in the configuration part of the GUI and to associate policies with each network.

To create a virtual network, use the following procedure:

1. When creating a virtual network, you can either use the default IP Address Management (IPAM) or create an IPAM inside your project. To create an IPAM, navigate to **Configure > Networking > IP Address Management** and click the **Create** button. The *Create IPAM* window is displayed (see [Figure 1 on page 13](#)).

Figure 1. Create IPAM Window



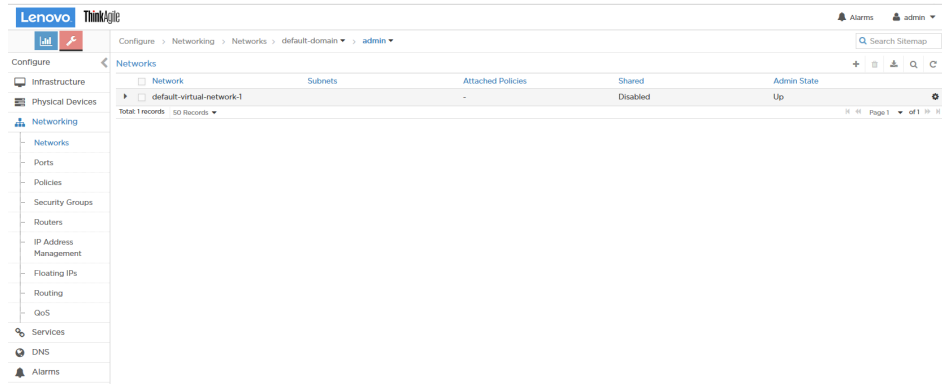
2. Complete the fields in the *Create IPAM* window.

Table 3. Create IPAM field descriptions

Field	Description
<i>Name</i>	The name of the new IPAM.
<i>DNS Method</i>	The domain name server method. One of the following: <ul style="list-style-type: none">● Default● Virtual DNS● Tenant● None
<i>NTP Server IP</i>	The IP address of an NTP server to be used for this IPAM.
<i>Domain Name</i>	The domain name to be used for this IPAM.

3. Navigate to **Configure > Networking > Networks**. The *Configure Networks* page is displayed (see [Figure 2 on page 14](#)).

Figure 2. Configure Networks Page



4. Verify that your project is displayed as active in the upper-right field, and then click the **+** icon. The *Create Network* window is displayed (see [Figure 3 on page 14](#)).

Figure 3. Create Network Window

5. Complete the fields in the *Create Network* window with the relevant network name, network policy and IP options.

Field	Description
<i>Name</i>	The name of the virtual network.
<i>Network Policy(s)</i>	Select from the drop-down list of available policies the policy to be applied to this network. You can select more than one policy by clicking each one.

Field	Description
<i>Subnets</i>	Manage subnets for this virtual network. Click the + icon to open fields for IPAM, CIDR, Allocation Pools, Gateway, DNS, and DHCP. Select the IPAM to be added from a drop down list in the IPAM field. Complete the remaining fields as necessary. You can add multiple subnets to a network. When finished, click the + icon to add the selections into the columns below the fields or click the - icon to remove the selections.
<i>Host Routes</i>	Add or remove host routes for this network. Click the + icon to open fields where you can enter the Route Prefix and the Next Hop. Click the + icon to add the information, or click the - icon to remove the information.
<i>Advanced Options</i>	Add or remove advanced options, including identifying the Admin State to be Up or Down, to identify the network as Shared or External, to add DNS servers, or to define a VxLAN Identifier.
<i>DNS Server(s)</i>	Add one or more DNS servers to be used by instances that belong to this network.
<i>Floating IP Pools</i>	Identify and manage the Floating IP address pools for this virtual network. Click the + icon to open fields where you can enter the Pool Name and Projects. Click the + icon to add the information, or click the - icon to remove the information.
<i>Route Target(s)</i>	Move the scroll bar down to access this area, then specify one or more route targets for this virtual network. Click the + icon to open fields where you can enter route target identifiers. Click the + icon to add the information, or click the - icon to remove the information.
<i>Export Route Target(s)</i>	Enter the route target identifiers that will be exported.
<i>Import Route Target(s)</i>	Enter the route target identifiers that will be imported.

- To save your network, click the **Save** button, or click **Cancel** to discard your work and start over.

Creating a Floating IP Address Pool

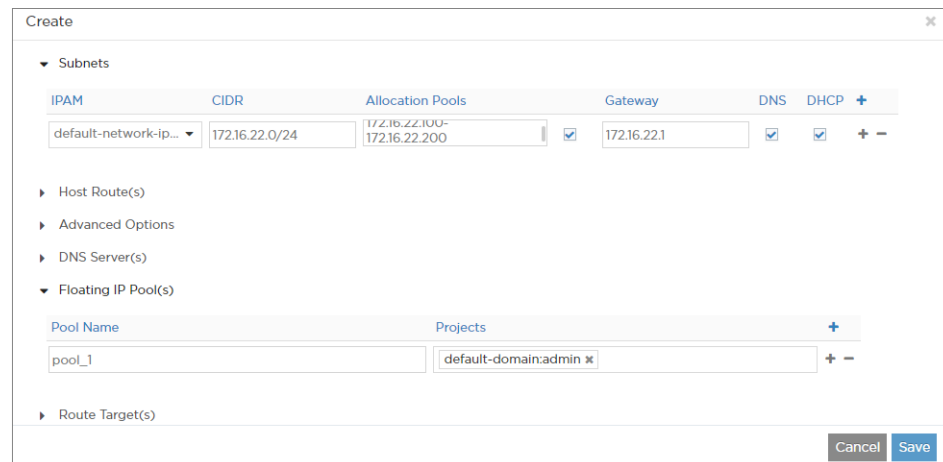
A floating IP address is an IP address that can be dynamically assigned to a running virtual instance, so that the instance can be accessed from the public network on the floating IP address.

Note: Make sure to configure floating IP address pools in project networks in TNC before assigning floating IP addresses from the pool to virtual machine instances.

To do this, follow the procedure below:

1. Select **Configure > Networking > Networks**.
Note: Make sure your project is the active project in the upper right.
2. Choose the network you want to associate with a floating IP pool. In the **Action** column, click the action icon and select **Edit**. The *Edit Network* window for the selected network is displayed (see [Figure 4 on page 16](#)).

Figure 4. Edit Network Window



The screenshot shows the 'Create' window for editing a network. The window has a title bar with 'Create' and a close button. The main content area is divided into several sections. The 'Subnets' section is expanded, showing a table with columns for IPAM, CIDR, Allocation Pools, Gateway, DNS, and DHCP. The table has one row with the following values: IPAM: default-network-ip..., CIDR: 172.16.22.0/24, Allocation Pools: 172.16.22.100-172.16.22.200, Gateway: 172.16.22.1, DNS: checked, DHCP: checked. Below the table are expandable sections for Host Route(s), Advanced Options, DNS Server(s), and Floating IP Pool(s). The Floating IP Pool(s) section is expanded, showing a table with columns for Pool Name and Projects. The Pool Name field contains 'pool_1' and the Projects field contains 'default-domain:admin'. At the bottom right of the window are 'Cancel' and 'Save' buttons.

3. In the **Floating IP Pools** section, click the **Pool Name** field and enter a name for your floating IP pool. Click the **+** icon to add the IP pool to the table below the field.
4. Click **Save** to create the floating IP address pool, or click **Cancel** to remove your work and start over.

Using Security Groups with Virtual Machines (Instances)

Security Groups Overview

A security group provides a set of security rules. Security groups and security group rules allow administrators to specify the type of traffic that is allowed to pass through a port. When a virtual machine (VM) is created in a virtual network (VN), a security group can be associated with the VM when it is launched. If a security group is not specified, a port is associated with a default security group. The default security group allows both ingress and egress traffic. Security rules can be added to the default security group to change the traffic behavior.

Creating Security Groups and Adding Rules

1. Select **Configure > Networking** and click the **Security Groups** button.

Figure 5. Edit Security Window

Direction	Ether Type	Address	Protocol	Port Range	
Egress	IPv4	0.0.0.0/0	ANY	0 - 65535	+ -
Egress	IPv6	:::/0	ANY	0 - 65535	+ -

2. When an instance is launched, you may associate a security group through the OpenStack application.

Configuring IPv6 Networks in TNC

IPv6 Networks Overview

TNC supports a series of features for IPv6 networks and overlay.

Note: The underlay network must be IPv4.

The table below offers an overview of the IPv6 supported/unsupported features:

Table 4. *IPv6 supported/unsupported features*

Feature	Supported
Virtual machines with IPv6 and IPv4 interfaces	YES
Virtual machines with IPv6-only interfaces	YES
DHCPv6 and neighbor discovery	YES
Security groups	YES
IPv6 flow set up, tear down, and aging	YES
Flow set up and tear down based on TCP state machine	YES
Protocol-based flow aging	YES
Fat flow	YES
Allowed address pair configuration with IPv6 addresses	YES
IPv6 service chaining	YES
Equal Cost Multi-Path (ECMP)	YES
Virtual Domain Name Services (vDNS), name-to-IPv6 address resolution	YES
User-Visible Entities (UVEs)	YES
Source Network Address Translation (SNAT)	NO
Load Balancing as a Service (LBaaS)	NO
IPv6 fragmentation	NO
Floating IP	NO
Link-local and metadata services	NO
Diagnostics for IPv6	NO

Creating IPv6 Virtual Networks in TNC

To create IPv6 networks, navigate to **Configure > Networking > Networks**. The *Configure Networks* page is displayed (see [Figure 6 on page 19](#)).

For further details on the fields, please refer to [“Creating a Virtual Network in TNC” on page 13](#).

Figure 6. Configure Networks Window

Edit

Network Permissions

Name

net-1

Network Policy(s)

Select Network Policies

Subnets

IPAM	CIDR	Allocation Pools		Gateway	DNS	DHCP	
default-network-ip...	20.0.0.0/24	20.0.0.100-20.0.0.200	<input checked="" type="checkbox"/>	20.0.0.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	+ -
default-network-ip...	2001::0/64	2001::10-2001::ff	<input checked="" type="checkbox"/>	2001::1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	+ -

Host Route(s)

Cancel Save

Configuring EVPN and VXLAN

TNC supports Ethernet VPNs (EVPN) and Virtual Extensible Local Area Networks (VXLAN).

Note: In TNC, EVPN is enabled by default.

TNC supports the following forwarding modes:

- Fallback bridging: IPv4 traffic lookup is performed using the IP FIB. All non-IPv4 traffic is directed to a MAC FIB.
- Layer 2 only: all traffic is forwarded using a MAC FIB lookup.

You can configure the forwarding mode individually on each virtual network.

The following table summarizes the traffic and encapsulation types supported for EVPN.

Table 5. *Traffic and Encapsulation Types*

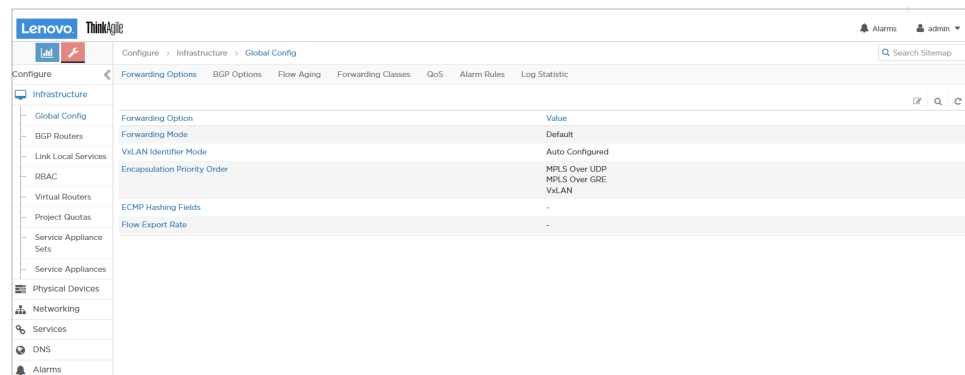
Traffic Type	Encapsulation		
	MPLS-GRE	MPLS-UDP	VXLAN
IP unicast	Yes	Yes	No
IP-BUM	Yes	Yes	No
non IP unicast	Yes	Yes	Yes
non IP-BUM	Yes	Yes	No

Configuring the VXLAN Identifier Mode

To configure the global VXLAN identifier mode, follow the procedure below:

1. Navigate to **Configure > Infrastructure > Global Config**. The *Global Configuration* page is displayed (see [Figure 7 on page 20](#)).

Figure 7. Global Configuration Page



2. Click the **Edit** icon. The *Edit Forwarding Options* window is displayed (see [Figure 8 on page 21](#)).

Figure 8. Edit Forwarding Options Window

Edit Forwarding Options

Forwarding Mode: Default

Flow Export Rate: Flow export rate in number

Vxlan Network Identifier Mode: ☒ Auto Configured ☐ User Configured

Encapsulation Priority Order: +

MPLS Over UDP: + -

MPLS Over GRE: + -

VxLAN: + -

ECMP Hashing Fields: source-ip x destination-ip x ip-protocol x source-port x destination-port x

Cancel Save

3. Select one of the following:
 - **Auto Configured:** The VXLAN identifier is automatically assigned to the virtual network.
 - **User Configured-** You must provide the VXLAN identifier for the virtual network

Note: When **User Configured** is selected, if an identifier is not provided, VXLAN encapsulation is not used and the mode falls back to MPLS.

Configuring Forwarding

In TNC, the default forwarding mode is enabled for fallback bridging (IP FIB and MAC FIB).

To change the forwarding mode, follow the procedure below:

1. From the TNC Web UI, navigate to **Configure > Networking > Networks**.
2. Select the virtual network that you want to change the forwarding mode for.

3. Click the gear icon and select **Edit**. The *Edit Network* window is displayed (see [Figure 9 on page 22](#)).

Figure 9. Edit Network Window

Edit Forwarding Options

Forwarding Mode
Default

Flow Export Rate
Flow export rate in number

Vxlan Network Identifier Mode
☐ Auto Configured ☒ User Configured

Encapsulation Priority Order +

VxLAN + -

MPLS Over GRE + -

MPLS Over UDP + -

ECMP Hashing Fields

source-ip x destination-ip x ip-protocol x source-port x
destination-port x

Cancel Save

4. Under the **Advanced Options** select one of the following forwarding modes:
 - **Default:** Enables the default forwarding mode.
 - **L2 and L3:** Enables IP and MAC FIB (fallback bridging).
 - **L2 Only:** Enables only MAC FIB.
 - **L3 Only:** Enables IP only.

Configuring the VXLAN Identifier

To configure the global VXLAN identifier, follow the procedure below:

Note: The VXLAN identifier can be set only if the VXLAN network identifier mode is set to **User Configured**.

1. From the TNC Web UI, navigate to **Configure > Networking > Networks**.
2. Select the virtual network you want to change the forwarding mode for.

- Click the gear icon and select **Edit**. The *Edit* window is displayed (see [Figure 10 on page 23](#)).

Figure 10. Edit Network Window for VXLAN Identifier

The 'Edit' window displays the following configuration options:

- Subnets**
- Host Route(s)**
- Advanced Options**
 - Admin State:** Up
 - ☐ Shared
 - ☐ External
 - ☐ Allow Transit
 - ☐ Mirroring
 - ☐ Flood Unknown
 - ☒ Reverse Path Forwarding
 - ☐ Multiple Service Chains
- Forwarding Mode:** L2 and L3
- VxLAN Identifier:** 1 - 16777215
- Extend to Physical Router(s):** Select Physical Router(s)
- Static Route(s):** Select Static Route(s)

Buttons: Cancel, Save

- Type the VXLAN identifier.
- Click **Save**.

Configuring Encapsulation Methods

- From the TNC Web UI, navigate to **Configure > Infrastructure > Global Config**.
- Click the **Edit** icon. The *Edit Forwarding Options* window is displayed (see [Figure 11 on page 23](#)).

Figure 11. Edit Forwarding Options Window

The 'Edit Forwarding Options' window displays the following configuration options:

- Forwarding Mode:** Default
- Flow Export Rate:** Flow export rate in number
- Vxlan Network Identifier Mode:**
 - ☐ Auto Configured
 - ☒ User Configured
- Encapsulation Priority Order:**
 - VxLAN
 - MPLS Over GRE
 - MPLS Over UDP
- ECMP Hashing Fields:**
 - source-ip
 - destination-ip
 - ip-protocol
 - source-port
 - destination-port

Buttons: Cancel, Save

3. Under **Encapsulation Priority Order** select one of the following:

- MPLS over UDP
- MPLS over GRE
- VXLAN

Click the **+** icon to the right of the first priority to add a second priority or third priority.

Note: VXLAN is only supported for EVPN unicast. It is not supported for IP traffic or multicast traffic. VXLAN priority and presence configured in the Web UI is ignored for traffic not supported by VXLAN. The configuration is applied globally for all virtual networks.

Configuring DNS Servers

DNS Overview

Domain Name System (DNS) is the standard protocol for resolving domain names into IP addresses so that traffic can be routed to its destination. DNS provides the translation between human-readable domain names and their IP addresses.

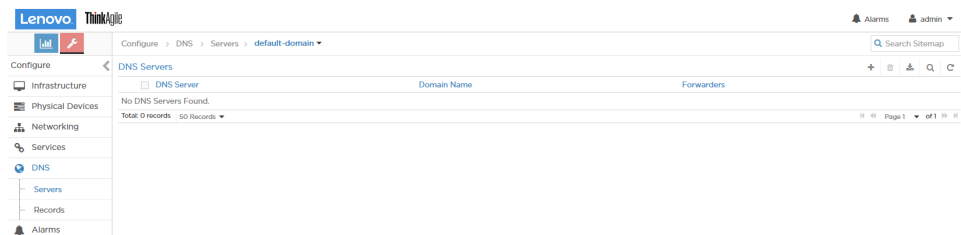
Configuring DNS Using the Interface

To configure DNS through the TNC interface, follow the procedure below:

1. Navigate to **Configure > DNS > Servers** to create or delete virtual DNS servers and records. The DNS Servers page is displayed (see [Figure 12 on page 25](#)).

Note: DNS Records page can be accessed only after a virtual DNS server is created.

Figure 12. DNS Servers Page



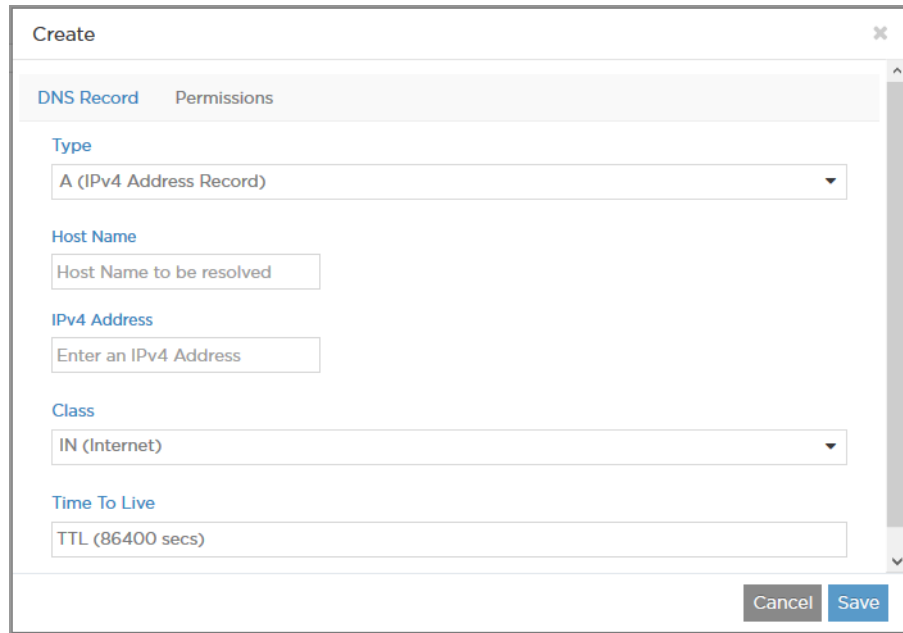
2. To add a new DNS server, click the **+** icon. The *Create DNS Server* window is displayed (see [Figure 13 on page 25](#)).

Figure 13. Create DNS Server Window

The screenshot shows the 'Create' window for a new DNS Server. The window has a title bar with a close button. Inside, there are two tabs: 'DNS Server' (selected) and 'Permissions'. The form contains several fields and options: 'Name' (text input), 'Domain Name' (text input), 'DNS Forwarder' (dropdown menu with the placeholder 'Enter Forwarder IP or Select a DNS Serv'), 'Record Resolution Order' (dropdown menu with 'Random' selected), 'Floating IP Record' (dropdown menu with 'Dashed IP Tenant' selected), 'Time To Live' (text input with 'TTL (86400 sec)' placeholder), 'External Visibility' (checkbox, unchecked), 'Reverse Resolution' (checkbox, unchecked), and 'Associate IPAMs' (text input). At the bottom right, there are 'Cancel' and 'Save' buttons.

3. To add a new DNS record, from the **DNS Records** page, click the **+** icon. The *Create DNS Record* window is displayed (see [Figure 14 on page 26](#)).

Figure 14. Create DNS Record Window



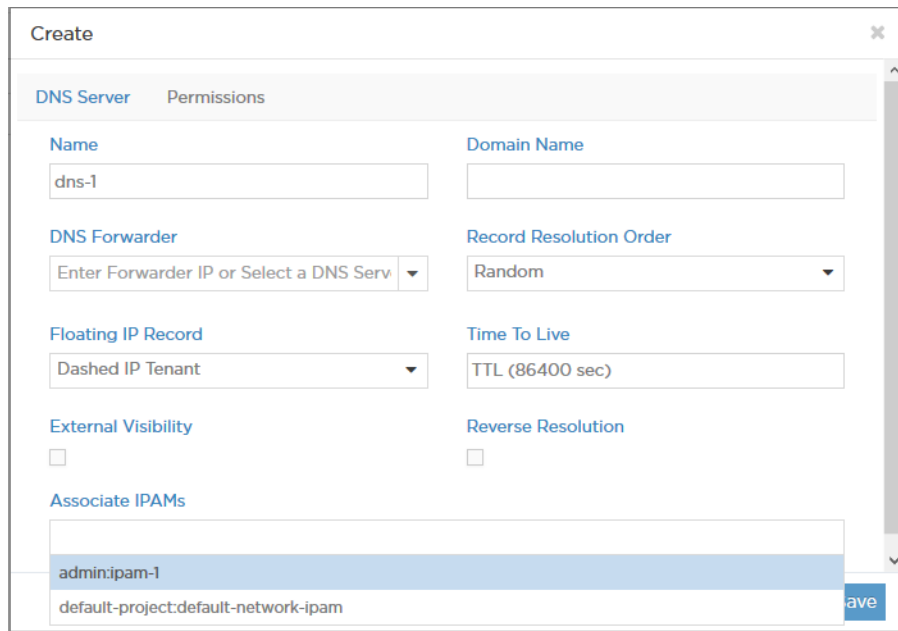
The 'Create' window for a DNS Record is shown. It has two tabs: 'DNS Record' (selected) and 'Permissions'. The 'DNS Record' tab contains the following fields:

- Type:** A dropdown menu with 'A (IPv4 Address Record)' selected.
- Host Name:** A text input field with the placeholder 'Host Name to be resolved'.
- IPv4 Address:** A text input field with the placeholder 'Enter an IPv4 Address'.
- Class:** A dropdown menu with 'IN (Internet)' selected.
- Time To Live:** A text input field with the placeholder 'TTL (86400 secs)'.

At the bottom right, there are 'Cancel' and 'Save' buttons.

4. To associate an IPAM to a virtual DNS server, from the **Create** page, select the **Associate IPAMs** tab (see [Figure 15 on page 26](#)).

Figure 15. Associate IPAMs Tab



The 'Create' window for a DNS Server is shown, with the 'Associate IPAMs' tab selected. The 'DNS Server' tab contains the following fields:

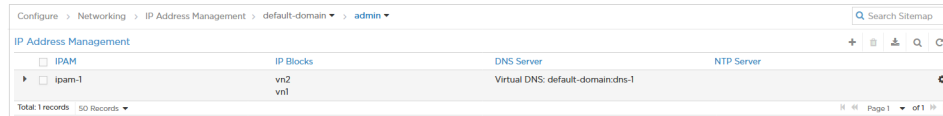
- Name:** A text input field with 'dns-1' entered.
- Domain Name:** A text input field.
- DNS Forwarder:** A dropdown menu with 'Enter Forwarder IP or Select a DNS Serv' selected.
- Record Resolution Order:** A dropdown menu with 'Random' selected.
- Floating IP Record:** A dropdown menu with 'Dashed IP Tenant' selected.
- Time To Live:** A text input field with 'TTL (86400 sec)' entered.
- External Visibility:** A checkbox that is unchecked.
- Reverse Resolution:** A checkbox that is unchecked.

Below these fields is the **Associate IPAMs** section, which contains a list of IPAMs:

- admin.ipam-1
- default-project:default-network-ipam

A 'Save' button is located at the bottom right of the window.

5. Navigate to **Configure > Networking > IP Address Management** to configure the DNS mode for any DNS server and to associate an IPAM to DNS servers of any mode or to tenants' IP addresses.

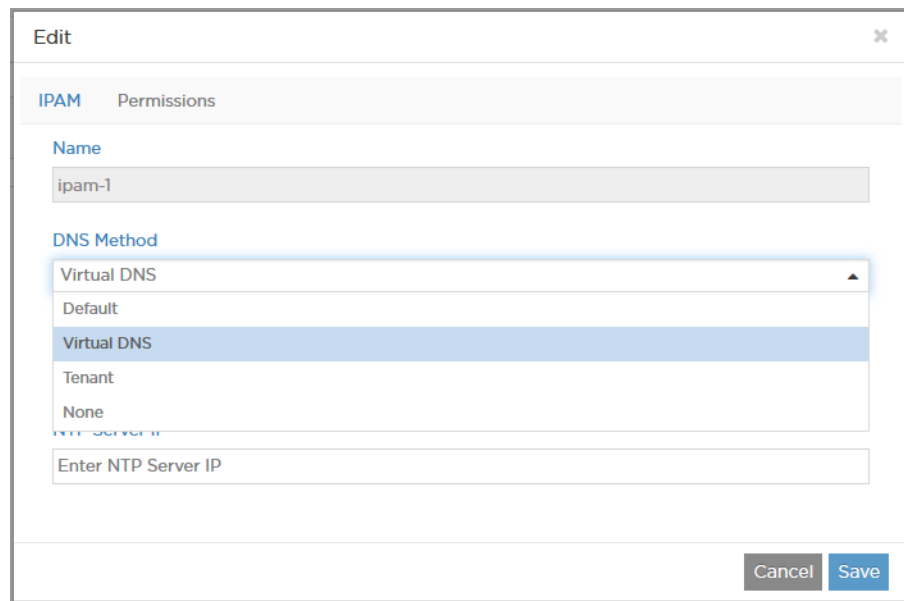


The screenshot shows a web interface for IP Address Management. At the top, there is a breadcrumb trail: 'Configure > Networking > IP Address Management > default-domain > admin'. Below this is a search bar labeled 'Search Sitemap'. The main content area is titled 'IP Address Management' and contains a table with four columns: 'IPAM', 'IP Blocks', 'DNS Server', and 'NTP Server'. There is a '+' icon and a 'C' icon in the top right of the table area. The table has one row with the following data: 'ipam-1' in the IPAM column, 'vn2' in the IP Blocks column, 'Virtual DNS: default-domain:dnss-1' in the DNS Server column, and an empty cell in the NTP Server column. Below the table, it says 'Total: 1 records' and '50 Records' with a dropdown arrow. On the right side of the table, there is a 'Page 1 of 1' indicator.

IPAM	IP Blocks	DNS Server	NTP Server
ipam-1	vn2	Virtual DNS: default-domain:dnss-1	

6. To associate an IPAM to a virtual DNS server or to tenant's IP addresses, at the **IP Address Management** page, select the network associated with this IPAM, then click the **Action** button and click **Edit** (see [Figure 16 on page 27](#)).

Figure 16. Edit IPAM Window



The screenshot shows the 'Edit' window for an IPAM. The window has a title bar 'Edit' with a close button. Inside, there are two tabs: 'IPAM' (selected) and 'Permissions'. Under the 'IPAM' tab, there is a 'Name' field with the value 'ipam-1'. Below that is a 'DNS Method' dropdown menu with the following options: 'Virtual DNS' (selected), 'Default', 'Virtual DNS', 'Tenant', and 'None'. Below the dropdown is a text input field labeled 'Enter NTP Server IP'. At the bottom right of the window, there are two buttons: 'Cancel' and 'Save'.

Configuring Static Routes with Services

This section addresses the following topics:

- [“Configuring Static Routes for Service Instances” on page 28](#)
- [“Configuring Static Routes as Host Routes” on page 33](#)

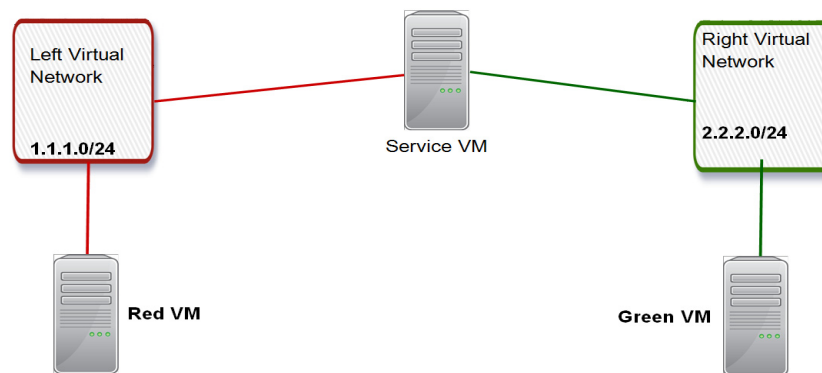
Configuring Static Routes for Service Instances

Static routes can be configured in a virtual network to direct traffic to a service virtual machine.

To configure static routes on a Service Instance version 2, follow the procedure below:

1. By using the OpenStack application, create the service VM and add it to the two networks in the below example (see [Figure 17 on page 28](#)).

Figure 17. Static Routes Example

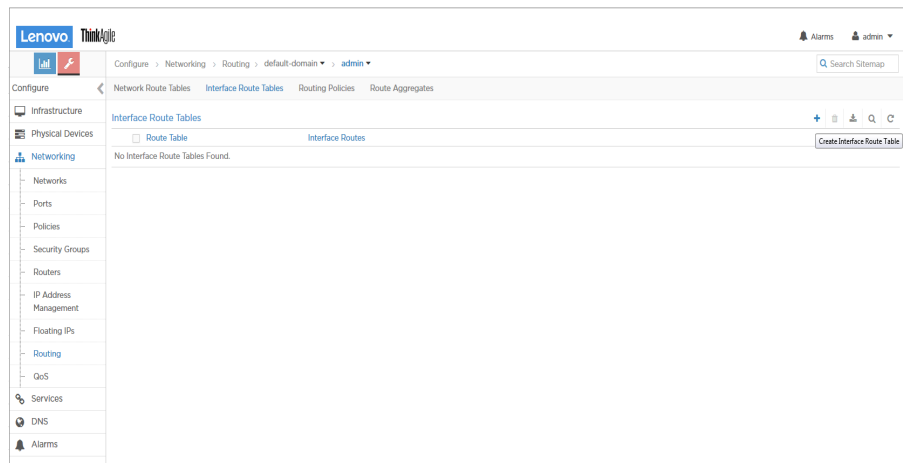


- To create a service template, navigate to **Configure > Services > Service Templates** and click **Create**. The *Create Service Template* window is displayed (see [Figure 18 on page 29](#)).

Figure 18. Create Service Template Window

- Select version **v2** and complete the fields for **Name**, **Service Mode**, **Image Name**, **Interfaces** types.
- To create interface route tables for the static routes, navigate to **Configure > Networking > Routing** page. Select the **Interface Route Tables** tab.

Figure 19. Interface Route Tables Tab



5. Click the **+** icon to add the route table for the left interface of the service. This should contain the route for the green network (see [Figure 17 on page 28](#)):

Figure 20. Create Route Table Window

The screenshot shows a 'Create' window with a close button (X) in the top right corner. Below the title bar, there are two tabs: 'Route Table' (selected) and 'Permissions'. Under the 'Route Table' tab, there is a 'Name' field containing 'left_table'. Below that, there are two fields: 'Prefix' containing '2.2.2.0/24' and 'Communities' containing 'Select or Enter Communities'. To the right of the 'Communities' field is a '+' icon. At the bottom right of the window, there are 'Cancel' and 'Save' buttons.

6. Click the **+** icon to add the route table for the right interface of the service. This should contain the route for the red network (see [Figure 17 on page 28](#)):

Figure 21. Create Route Table Window

The screenshot shows a 'Create' window with a close button (X) in the top right corner. Below the title bar, there are two tabs: 'Route Table' (selected) and 'Permissions'. Under the 'Route Table' tab, there is a 'Name' field containing 'right_table'. Below that, there are two fields: 'Prefix' containing '1.1.1.0/24' and 'Communities' containing 'Select or Enter Communities'. To the right of the 'Communities' field is a '+' icon. At the bottom right of the window, there are 'Cancel' and 'Save' buttons.

7. To create the service instance for static routes, go to **Configure > Services > Service Instances** and click the **+** icon. The *Create Service Instance* window is displayed (see [Figure 22 on page 31](#)). Set the name, choose the service template and set the left interface to the red network and the right interface to the green network.

Figure 22. Create Service Instance Window

Create

Service Instance Permissions

Name: static_route_instance

Service Template: static_route_template - [in-network (left...

Interface Type: left, right

Virtual Network: red, green

Port Tuples

Service Health Check

Routing Policy

Route Aggregate

Cancel Save

8. On the **Port Tuples** tab, add a port tuple to attach the already spawned VM to the service. Choose the left interface to be the VM port in the red network and the right interface to be the VM port in the green network (see [Figure 17 on page 28](#)).

Figure 23. Port Tuples Tab

Create

Port Tuples Service Health Check

left: red

right: green

Port Tuples

Tuple: port-tuple0 : 1.1.1.3, 2.2.2.3

Interface Type: left, right

Virtual Machine Interface: (1.1.1.3) - 69ad1325-8d76-407b..., (2.2.2.3) - 3847974c-2f5d-48e...

Service Health Check

Cancel Save

9. On the **Static Routes** tab, add two static routes (see [Figure 24 on page 32](#)):
- associate the left interface with the interface route table that contains the route for the green network
 - associate the right interface with the interface route table that contains the route for the red network.

Figure 24. Interface Type Tab

The screenshot shows a 'Create' dialog box with a close button (X) in the top right corner. At the top, there is a text input field containing 'right' and a dropdown menu showing '(2.2.2.3) - 3847974c-2f5d-48e...'. Below this is a list of configuration options on the left, each preceded by a right-pointing triangle (▶) except for the last one which has a downward-pointing triangle (▼):

- Service Health Check
- Routing Policy
- Route Aggregate
- Allowed Address Pair
- Static Route

The 'Static Route' option is expanded, showing a table with two columns: 'Interface Type' and 'Interface Route Table'. There is a blue '+' button to the right of the column headers.

Interface Type	Interface Route Table
left ▼	left_table ✕ + -
right ▼	right_table ✕ + -

At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

Configuring Static Routes as Host Routes

Static routes can also be used for host routes for a virtual machine, by using the classless static routes option in the DHCP server response that is sent to the virtual machine.

The routes to be sent in the DHCP response to the virtual machine can be configured for each virtual network as it is created.

To configure static routes as host routes, follow the procedure below:

1. Navigate to **Configure > Network > Networks** and click **Create**. The *Create* window is displayed.
2. On the **Host Routes** tab, add the host routes to be sent to the virtual machines (see [Figure 25 on page 33](#)).

Figure 25. Host Route(s) Tab

The screenshot shows the 'Create' window with the 'Host Route(s)' tab selected. The 'Subnets' section is collapsed. The 'Host Route(s)' section contains a table with the following data:

Route Prefix	Next Hop
2.2.2.0/24	1.1.1.254

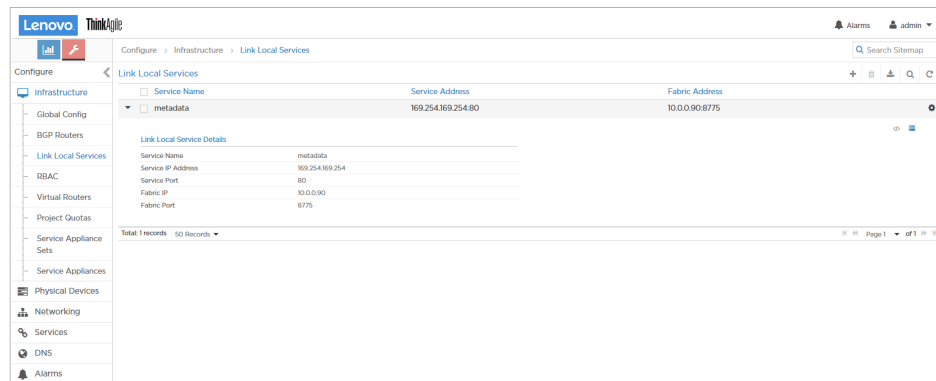
Below the table, there are three expandable sections: 'Advanced Options', 'DNS Server(s)', and 'Floating IP Pool(s)'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Configuring Metadata Service

The OpenStack application enables virtual machines to access metadata by sending an HTTP request to the link-local address 169.254.169.254. The metadata request from the virtual machine is proxied to Nova with additional HTTP header fields that Nova uses to identify the source instance, and then responds with appropriate metadata.

To set the linklocal-services properties, navigate to **TNC UI > Configure > Infrastructure > Link Local Service** (see [Figure 26 on page 34](#)).

Figure 26. Link Local Services Page



Configuring Service Chaining

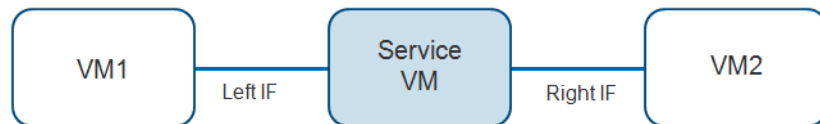
Service Chaining Overview

TNC supports chaining of various Layer 2 through Layer 7 services such as firewall, NAT, IDP, and others.

Services are offered by instantiating service virtual machines to dynamically apply single or multiple services to virtual machine (VM) traffic. It is also possible to chain physical appliance-based services.

Figure 27 shows the basic service chain schema, with a single service. The service VM spawns the service, using the convention of left interface (left IF) and right interface (right IF). Multiple services can also be chained together.

Figure 27. Service Chain Example



Service chaining requires the following configuration elements:

- Service template
- Service instance
- Service policy

Load Balance Service Chain Example

To run load balance service chain, you must create corresponding virtual network and service VMs. The following example uses the two previous integrated VM images.

To implement load balance service chain, follow the procedure below:

1. Create virtual network interfaces left-vn, right-vn. For this example, left-vn is 192.168.1.0/24 and right-vn is 192.168.2.0/24.
2. Upload load balance service image in the OpenStack application; choose **haproxy** as application load balance service.
3. Use the following command to upload the image:

```
openstack image create "ha" --file SFC-loadbalance-service-ubuntu.qcow2 \
--disk-format qcow2 --container-format bare --public
```

4. Create the service template in TNC. To do this, navigate to **Configure > Services > Service Templates** and click the **+** icon. The *Create Service Template* window is displayed (see [Figure 28 on page 36](#)).

Figure 28. Create Service Template Window

The screenshot shows the 'Create Service Template' window. It has a title bar with a close button. Below the title bar are two tabs: 'Service Template' and 'Permissions'. The 'Service Template' tab is active. It contains the following fields:

- Name:** v2-loadbalance-template
- Version:** v2 (dropdown)
- Virtualization Type:** Virtual Machine (dropdown)
- Service Mode:** In-Network (dropdown)
- Service Type:** Firewall (dropdown)
- Interface (s):** A section with two entries: 'left' and 'right', each with a dropdown arrow and '+' and '-' buttons.

At the bottom right are 'Cancel' and 'Save' buttons.

5. Set v2 as the version number.
6. Spawn the service VM from the OpenStack application and attach it to the two networks: left-vn and right-vn.
7. Create the service instance in TNC. To do this, navigate to **Configure > Services > Service Instances** and click the **+** icon. The *Create Service Instance* window is displayed (see [Figure 29 on page 36](#)).

Figure 29. Create Service Instance Window

The screenshot shows the 'Create Service Instance' window. It has a title bar with a close button. Below the title bar are two tabs: 'Service Instance' and 'Permissions'. The 'Service Instance' tab is active. It contains the following fields:

- Name:** v2-loadbalance-instance
- Service Template:** v2-loadbalance-template - [in-network (...)] (dropdown)
- Interface Type:** A section with two entries: 'left' and 'right', each with a dropdown arrow.

At the bottom right are 'Cancel' and 'Save' buttons.

8. Apply the created service template and attach the left interface to the left-vn and right interface to the right-vn.
9. Add a port tuple to attach the spawned service VM. Set the left interface to be the VM port in left-vn and the right interface to be the VM port in right-vn (see [Figure 30 on page 37](#))

Figure 30. Port Tuples Tab

10. Configure the network policy. To do so, navigate to **Configure > Networking > Policies**. The *Create Policy* window is displayed (see [Figure 31 on page 37](#)).

Figure 31. Create Policy Window

11. Name the policy and associate it to the networks created earlier (left_vn and right_vn).
12. Set the source network as left_vn and the destination network as right_vn.
13. Check **Apply Service** and select the service **v2-loadbalance-instance**.

Check the **Services** box to make the packet pass through the service from left-vn to right-vn.

14. Inject policy into left-vn and right-vn. Associate the policy to both the left_vn and the right_vn. To do so, navigate to **Configure > Networking > Network**. On the right side of left_vn, click the gear icon to enable **Edit Network** (see [Figure 32 on page 38](#)).

Figure 32. Edit Network Window

The screenshot shows the 'Edit Network' window. The 'Network' tab is active. The 'Name' field is set to 'right-vn'. The 'Network Policy(s)' field is set to 'default-domain:admin:load_balancing *'. The 'Subnets' section is expanded, showing a list of subnets. The 'Host Route(s)' section is expanded, showing a list of host routes. The 'Advanced Options' section is expanded, showing a list of advanced options. The 'DNS Server(s)' section is expanded, showing a list of DNS servers. The 'Floating IP Pool(s)' section is expanded, showing a list of floating IP pools. The 'Route Target(s)' section is expanded, showing a list of route targets. The 'Cancel' and 'Save' buttons are at the bottom right.

15. In the *Edit Network* window of the left_vn network, select **load_balancing** policy in the **Network Policy(s)** tab.

Repeat the same process for the right_vn.

Note: Additional OpenStack configuration is needed for implementing load balance service chain.

Configuring Source Network Address Translation (SNAT)

SNAT Overview

Source Network Address Translation (source-nat or SNAT) is typically used by internal users to access the Internet; the source address is translated and thereby kept private. Virtual machines launched on a private network can get to the internet by going through a gateway capable of performing SNAT. The gateway has one arm on the public network and as part of SNAT, it replaces the source IP of the originating packet with its own public side IP. As part of SNAT, the source port is also updated so that multiple VMs can reach the public network through a single gateway public IP.

As stated before, a virtual network from TNC does not have access to the public network. For this, a gateway is needed to provide connectivity to the public network from a virtual network. This gateway can be a physical device or a software gateway - Software Simple Gateway (SSG). We will detail how a Software Simple Gateway can be configured in TNC.

Software Simple Gateway can be used in conjunction with Floating IP, to provide Internet access from a VM inside a TNC private network. Furthermore, it also permits access from the public network to a VM inside a TNC private network.

Note: Proxy ARP needs to be enabled on the compute node interface which has a public IP address.

To enable Proxy ARP, run the following command:

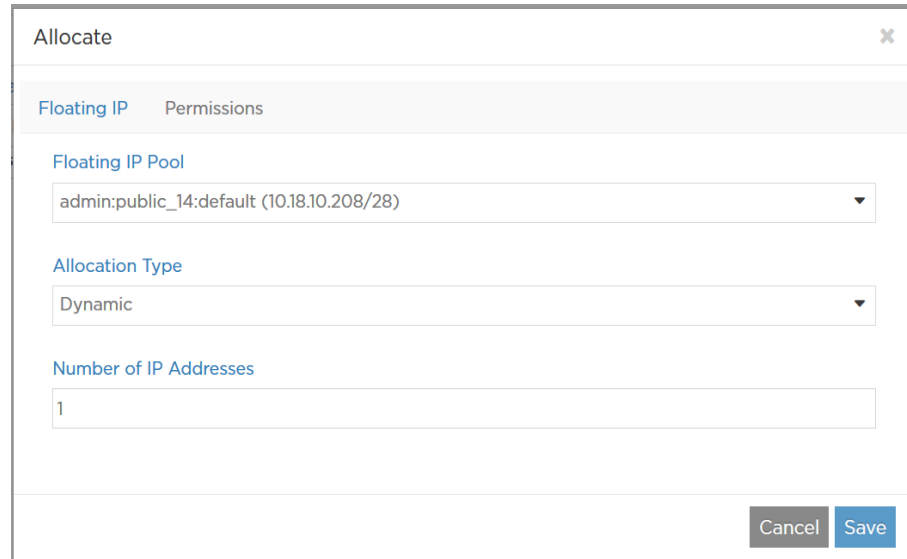
```
echo 1 > /proc/sys/net/ipv4/conf/<interface_name>/proxy_arp
```

Associating a Floating IP to a VM

To associate a floating IP to a VM, follow the procedure below:

1. Add a Floating IP pool with a public network IP address. To do so, see [“Creating a Floating IP Address Pool” on page 16](#).
2. Assign a Floating IP address to the VM. To do so, navigate to **Configure > Networking > Floating IPs** and click on the **+** icon. The Allocate Floating IP window is displayed (see [Figure 33 on page 40](#)).

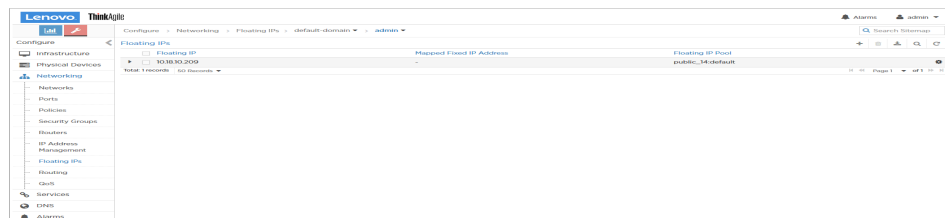
Figure 33. Allocate Floating IP Window



The 'Allocate' window is a modal dialog with a close button (X) in the top right corner. It contains two tabs: 'Floating IP' (selected) and 'Permissions'. Under the 'Floating IP' tab, there are three sections: 'Floating IP Pool' with a dropdown menu showing 'admin:public_14:default (10.18.10.208/28)', 'Allocation Type' with a dropdown menu showing 'Dynamic', and 'Number of IP Addresses' with a text input field containing '1'. At the bottom right, there are 'Cancel' and 'Save' buttons.

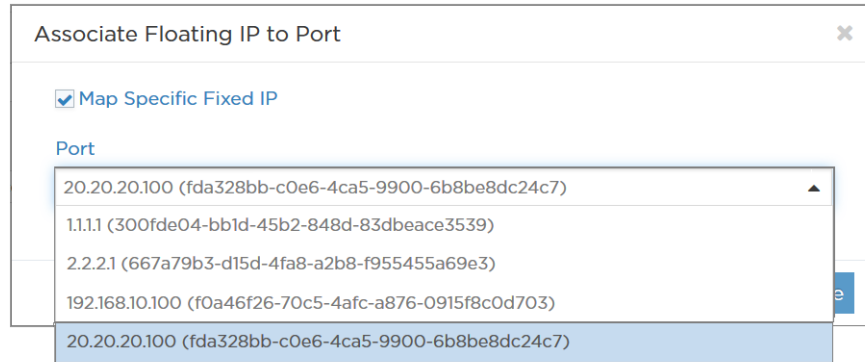
3. As floating IP pool, select the previously created floating IP pool.
4. Associate the previously created VM to the floating IP entry. Click on the gear icon and select **Associated Port** (see [Figure 34 on page 40](#)).

Figure 34. Floating IP Associated Port Page



The **Associate Floating IP to Port** window is displayed (see [Figure 35 on page 41](#)).

Figure 35. Associate Floating IP to Port Window



5. From the drop-down list, select the IP address of the VM you want to associate a floating IP address.
6. To add SSG, **provision_vgw_interface.py** script needs to be run:

```
sudo /opt/contrail/utils/provision_vgw_interface.py --oper create --interface vgw1 \
--subnets <public_network_IP_address>/<public_network_netmask> --routes \
0.0.0.0/0 --vrf \
default-domain:admin:<public_network_name>:<public_network_name>
```

This script adds vgw1 interface on the compute node it was run.

Note: For redundancy purposes, vgw1 interface can be added on more than one compute node.

Note: A route is added in the route table of the compute node: packets with the destination <public_network> should be forwarded via vgw1 interface. This is used when the connection to the VM is initiated from the public network, using VM's floating IP address.

Multicast Support

This section describes how the TNC supports broadcast and multicast.

All-Broadcast/Limited-Broadcast and Link-Local Multicast

The address group 255.255.255.255 is used with all-broadcast (limited-broadcast) and multicast traffic. The route is installed in the multicast routing instance. The source address is recorded as ANY, so the route is ANY/255.255.255.255 (*,G). It is unique per routing instance, and it is associated with its corresponding virtual network. When a virtual network is spawned, it usually contains multiple subnets, in which virtual machines are added. All of the virtual machines, regardless of their subnets, are part of the recipient list for ANY/255.255.255.255. The replication is sent to every recipient except the originator.

Link-local multicast also uses the all-broadcast method for replication. The route is deleted when all virtual machines in this virtual network are turned off or the virtual network itself is deleted.

All-Broadcast/Limited-Broadcast Example

The following configuration is made:

- Virtual networks: vn1, vn2
- Subnets allocated: 20.20.20.0/24 (for vn1) and 30.30.30.0/24 (for vn2)
- Virtual machines spawned: vm1 (20.20.20.10); vm2 (20.20.20.20); vm3 (20.20.20.100); vm4 (30.30.30.60)

Traffic originates for 20.20.20.255 from vm1 (20.20.20.10) and then the traffic is forwarded to vm2 (20.20.20.20) and vm3 (20.20.20.100) and not to vm4 (30.30.30.60). The originator vm1 (20.20.20.10) will not receive the traffic even though it is listed as a recipient in the next hop.

Link-Local Multicast Example

Link-local multicast also uses the all-broadcast method for replication. The route is deleted when all virtual machines in this virtual network are turned off or the virtual network itself is deleted.

The same configuration is used as in the previous example. Iperf tool is used for sending/ receiving multicast traffic.

Suppose that traffic originates for multicast address 239.255.1.3 from vm1. Only vm2 listens on multicast address 239.255.1.3, vm2 and vm3 do not listen on this multicast address.

Traffic will be forwarded to vm2 only (20.20.20.20) and not to vm3 (20.20.20.100) and vm4.

Note: Inter-network multicast (multicast between virtual machines in different networks) is currently not supported.

Host Broadcast

The host broadcast route is present in the host routing instance so that the host operating system can send a subnet broadcast/all-broadcast (limited-broadcast). This type of broadcast is sent to the fabric by means of a vhost interface. Additionally, any subnet broadcast/all-broadcast received from the fabric will be handed over to the host operating system.

TNC Analytics Application Programming Interfaces (APIs) and User-Visible Entities (UVEs)

The TNC analytics-api server provides a REST API interface to extract the operational state of the TNC system.

APIs are used by the TNC Web user interface to present the operational state to users. Other applications might also use the server's REST APIs for analytics or other uses.

To see all of the available APIs, navigate the URL tree at the REST interface, starting at the root **http://<analytics_ip_address>:8081**

Chapter 3. Monitoring the System

The **Monitor** icon on the TNC Controller provides numerous options so you can view and analyze usage and other activity associated with all nodes of the system, through the use of reports, charts, and detailed lists of configurations and system activities.

Monitor pages support monitoring of infrastructure components: control nodes, virtual routers, analytics nodes, and config nodes. Additionally, users can monitor networking and debug components.

Use the menu options available from the **Monitor** icon to configure and view the statistics you need for better understanding of the activities in your system:

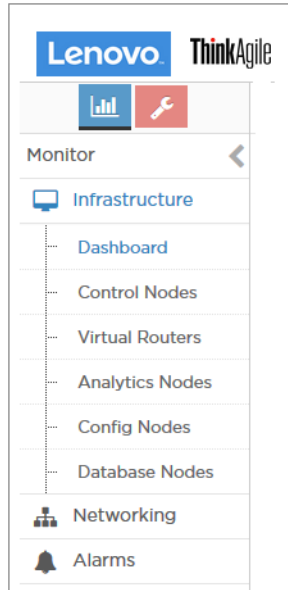
- Infrastructure, see [“Infrastructure menu” on page 46](#)
- Networking, see [“Networking menu” on page 48](#)
- Alarms - View the list of Alarms reported for all TNC nodes

In addition, you can access node information on a physical server by using a set of specific commands, see [“TNC Commands” on page 51](#).

Infrastructure menu

The following figure displays the **Monitor > Infrastructure** menu (see [Figure 36 on page 46](#)).

Figure 36. Infrastructure Menu



See Table 6 on page 46 for a description of the items available under the **Infrastructure** menu.

Table 6. Infrastructure Menu fields

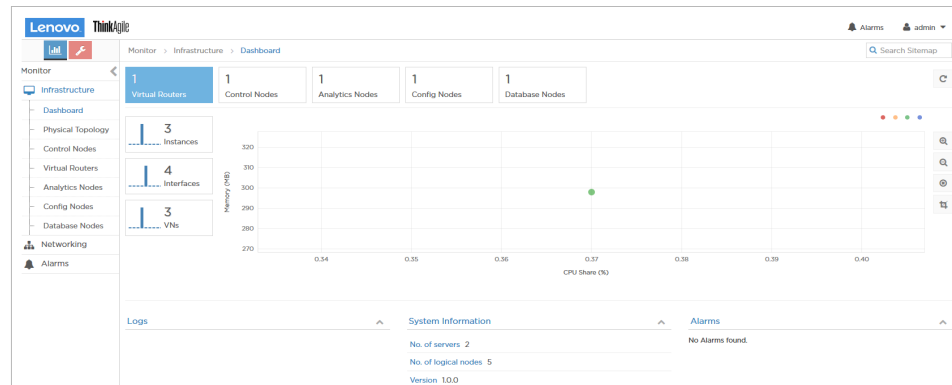
Field	Description
<i>Dashboard</i>	Displays an overview of the infrastructure components, including the numbers of virtual routers, control nodes, analytics nodes, config nodes and database nodes currently operational, and a bubble chart of virtual routers showing the CPU and memory utilization, log messages, system information, and alerts. For further details, see “Infrastructure>Dashboard” on page 47 .
<i>Physical Topology</i>	Displays an overview of the physical routers that TNC is connected to.
<i>Control Nodes</i>	Displays a summary of all the control nodes in the system, and for each control node displays the following details: <ul style="list-style-type: none">● Graphical reports of memory usage and average CPU load.● Console information for a specified time period.● A list of all peers with details about type, ASN, and the like.● A list of all routes, including next hop, source, local preference, and the like.

Field	Description
<i>Virtual Routers</i>	Displays a summary of all vRouters in the system, and for each vRouter displays the following details: <ul style="list-style-type: none"> ● Graphical reports of memory usage and average CPU load. ● Console information for a specified time period. ● A list of all interfaces with details such as label, status, associated network, IP address etc. ● A list of all associated networks with their ACLs and VRFs. ● A list of all active flows with source and destination details, size, and time.
<i>Analytics Nodes</i>	Displays activity for the analytics nodes, including memory and CPU usage, analytics host names, IP address, status, and more.
<i>Config Nodes</i>	Displays activity for the config nodes, including memory and CPU usage, config host names, IP address, status, and more.
<i>Database Nodes</i>	Displays activity for the database nodes, including memory and CPU usage, config host names, IP address, status, and more.

Infrastructure>Dashboard

Use **Monitor > Infrastructure > Dashboard** to get an overview of the system infrastructure components, including the numbers of virtual routers, control nodes, analytics nodes, config nodes and database nodes currently operational, a bubble chart of virtual routers showing the CPU and memory utilization, log messages, system information, and alerts (see [Figure 37 on page 47](#)).

Figure 37. Infrastructure Dashboard Page

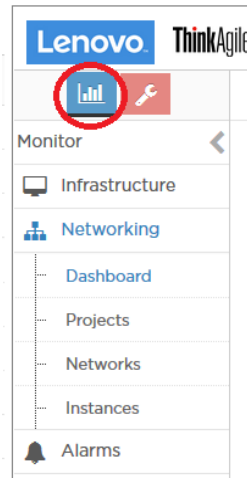


Across the top of the Dashboard screen are summary boxes representing the components of the system that are shown in the statistics. Any of the control nodes, virtual routers, analytics nodes, config nodes and database nodes can be monitored individually and in detail from the Dashboard by clicking an associated box, and drilling down for more detail.

Networking menu

The following figure displays the **Monitor > Networking** menu (see [Figure 38 on page 48](#)).

Figure 38. Networking Menu



See Table 7 on page 48 for a description of the items available under the **Networking** menu.

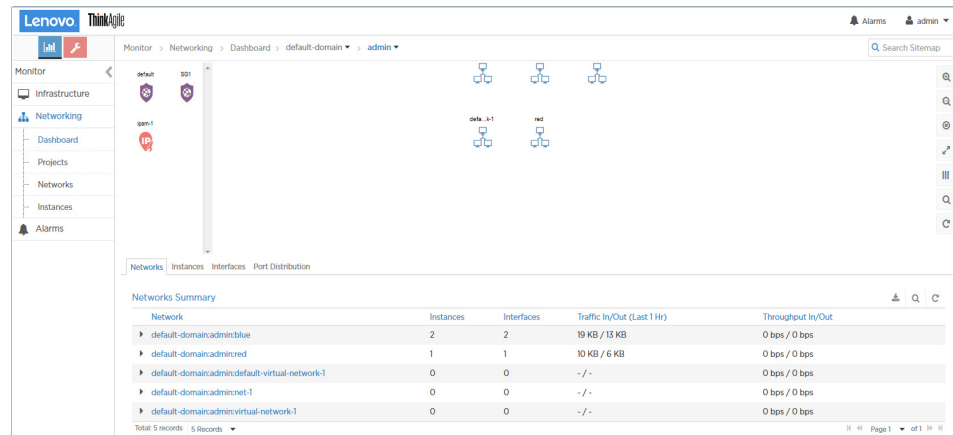
Table 7. Networking Menu Fields

Field	Description
<i>Dashboard</i>	For all virtual networks for all projects in the system, displays graphical traffic statistics, including: <ul style="list-style-type: none">● Total traffic in and out.● Inter VN traffic in and out. You can view the statistics in varying levels of granularity, for example, for a whole project, or for a single network.
<i>Projects</i>	Displays essential information about projects in the system including name, associated networks, and traffic in and out.
<i>Networks</i>	Displays essential information about networks in the system including name and traffic in and out.
<i>Instances</i>	Displays essential information about instances in the system including name, associated networks, interfaces, vRouters, and traffic in and out.

Networking>Dashboard

Use **Monitor > Networking > Dashboard** to gain insight into usage statistics for domains, virtual networks, projects, and virtual machines (see [Figure 39 on page 49](#)).

Figure 39. Networking Dashboard Page



The **Networks** tab is displayed at the bottom part of the screen. For each network, the following fields are shown:

Table 8. *Networks fields*

Field	Description
<i>Network</i>	The fully qualified name (FQ name) of the network.
<i>Instances</i>	The number of virtual machines attached to the network.
<i>Interfaces</i>	The number of interfaces attached to the network.
<i>Traffic In/Out (Last 1hr)</i>	The size of input and output traffic over the last hour
<i>Throughput In/Out</i>	The input and output traffic throughput

Select the **Instances** tab to view information about the running instances:

Figure 40. Instances Tab

UUID	Instance Name	Networks	Interfaces	Floating IPs	Virtual Router	IP Address	Aggr. Traffic In/Out (Last 1 Hr)
Od620c1b-fe28-49...	vm3	blue (admin)	1	0	RHELCompute	IPv4: 2.2.2.5	24 KB / 22 KB
3ed4f5a7-a953-466...	vm2	red (admin)	1	0	RHELCompute	IPv4: 111.3	25 KB / 23 KB
9258a975-56f3-473...	vm1	blue (admin)	1	0	RHELCompute	IPv4: 2.2.2.3	26 KB / 24 KB

Total: 3 records | 5 Records

TNC Commands

This section describes how to view node information on a physical server.

Viewing Node Status

Displays a list of all components of a TNC server node (such as control, configuration, database, Web-UI, analytics, or vrouter) and reports their current status of active or inactive.

Syntax

```
[root@host ~]# contrail-status
```

Privilege level

admin

Sample Output

The following example usage displays on a server that is configured for the roles of vrouter, controller, analytics, configuration, web-ui, and database:

On a TNC Controller Node:

```
[root@RHELContrail ~]# contrail-status
== Contrail Control ==
supervisor-control:    active
contrail-control       active
contrail-control-nodemgr active
contrail-dns           active
contrail-named         active

== Contrail Analytics ==
supervisor-analytics:  active
contrail-alarm-gen     active
contrail-analytics-api active
contrail-analytics-nodemgr active
contrail-collector     active
contrail-query-engine  active
contrail-snmp-collector active
contrail-topology      active

== Contrail Config ==
supervisor-config:    active
contrail-api:0        active
contrail-config-nodemgr active
contrail-device-manager active
contrail-discovery:0  active
contrail-schema       active
contrail-svc-monitor  active
ifmap                 active

== Contrail Web UI ==
supervisor-webui:     active
contrail-webui        active
contrail-webui-middleware active

== Contrail Database ==
contrail-database:    active

== Contrail Supervisor Database ==
supervisor-database:  active
contrail-database-nodemgr active
kafka                 active
```

On a TNC Compute Node:

```
[root@RHELCompute ~]# contrail-status
== Contrail vRouter ==
supervisor-vrouter:    active
contrail-vrouter-agent  active
contrail-vrouter-nodemgr active
```

Viewing Version Information

Displays a list of all installed components with their version and build numbers.

Syntax

```
[root@host]# contrail-version
```

Privilege level

admin

Sample Output

The following example shows version and build information for all installed components.

```
[root@RHELContrail ~]# contrail-version
```

Package	Version	Build-ID Repo RPM Name
contrail-analytics	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-config	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-config-openstack	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-control	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-database	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-database-common	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-dns	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-docs	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-fabric-utils	3.2.5.0-lenovo0012	lenovo0012
contrail-install-packages	3.2.5.0-lenovo0012-newton.el7.centos	installed
contrail-lib	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-nodemgr	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-openstack-analytics	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-openstack-config	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-openstack-control	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-openstack-database	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-openstack-webui	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-setup	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-utils	3.2.5.0-lenovo0012.el7.centos	lenovo0012
contrail-web-controller	3.2.5.0-lenovo0012	lenovo0012
contrail-web-core	3.2.5.0-lenovo0012	lenovo0012
neutron-plugin-contrail	3.2.5.0-lenovo0012.el7.centos	lenovo0012
python-contrail	3.2.5.0-lenovo0012.el7.centos	lenovo0012

Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

Use this information to obtain additional information about Lenovo and Lenovo products, and determine what to do if you experience a problem with your Lenovo system or optional device.

Note: This section includes references to IBM web sites and information about obtaining service. IBM is Lenovo's preferred service provider for the System X, Flex System, and NeXtScale System products.

Before you call, make sure that you have taken these steps to try to solve the problem yourself.

If you believe that you require warranty service for your Lenovo product and you have purchased the plug-in through the “Lenovo Networking Bundle for vRealize”, the service technicians will be able to assist you more efficiently if you prepare before you call.

- Go to the [Lenovo Support portal](#) to check for information to help you solve the problem.
- Gather the following information to provide to the service technician. This data will help the service technician quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
 - Pertinent information such as error messages and logs
- Start the process of determining a solution to your problem by making the pertinent information available to the service technicians. The IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.

Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties.

Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

Lenovo, the Lenovo logo, Flex System, System x, NeXtScale System, ThinkSystem and X-Architecture are trademarks of Lenovo in the United States, other countries, or both.

VMware®, vRealize®, and Orchestrator™ are trademarks of VMware.

Other company, product, or service names may be trademarks or service marks of others.