Load Balancing Planmeca Romexis

Version 1.0.0

Table of Contents

1. About this Guide

This guide details the steps required to configure a highly available Planmeca Romexis environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Planmeca Romexis configuration changes that are required.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used with Planmeca Romexis. For full specifications of available models please refer to https://www.loadbalancer.org/products.

Some features may not be available or fully supported in all cloud platforms due to platform specific limitations. For more details, please refer to the "Main Differences to our Standard (Non-Cloud) Product" section in the appropriate cloud platform Quick Start Guide or check with Loadbalancer.org support.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance

- V8.13.0 and later

Note	The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If you're using an older version, or the very latest, the screenshots presented here may not match your WebUI exactly.

3.2. Planmeca Romexis

- v6.4.8.904R and later

4. Planmeca Romexis

Planmeca Romexis® is a comprehensive and user-friendly all-in-one dental software platform developed by Planmeca, a leading manufacturer of dental equipment. It's designed to integrate various dental imaging modalities, CAD/CAM workflows, and other digital dentistry tools into a single, efficient system.

5. Load Balancing Planmeca Romexis

Note	It's highly recommended that you have a working Planmeca Romexis environment first before implementing the load balancer.

5.1. Load Balancing & HA Requirements

Due to software constraints there cannot be multiple active Romexis servers running simultaneously. Therefore, the Virtual Service (VIP) on the load balancer is configured with one Romexis server as a Real Server (RIP) and the other as a fallback server. In this way, the second server is ready to take over should anything happen to the primary server, thus providing a highly available solution.

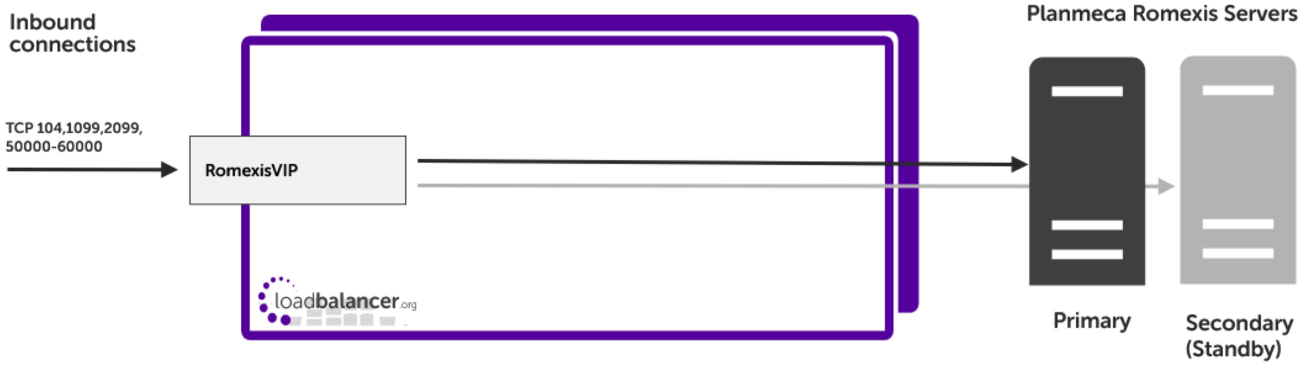
5.2. Virtual Service (VIP) Requirements

To provide load balancing and HA for Planmeca Romexis, the following VIP is required:

Ref.	VIP Name	Mode	Port(s)	Persistence Mode	Health Check
VIP 1	RomexisVIP	L4 DR	104,1099,2099, 50000-60000	Source IP	Connect to Port (1099)

6. Deployment Concept

Once the load balancer is deployed, clients connect to the Virtual Service (VIP) rather than connecting directly to a Planmeca Romexis server. These connections are then sent to the primary server if it's up and passing health checks, and to the secondary server if not.



VIP = **V**irtual **IP** Address

Note: The load balancer can be deployed as a single unit, although Loadbalancer.org recommends a clustered pair for resilience & high availability. Please refer to the section Configuring HA - Adding a Secondary Appliance in the appendix for more details on configuring a clustered pair.

7. Load Balancer Deployment Methods

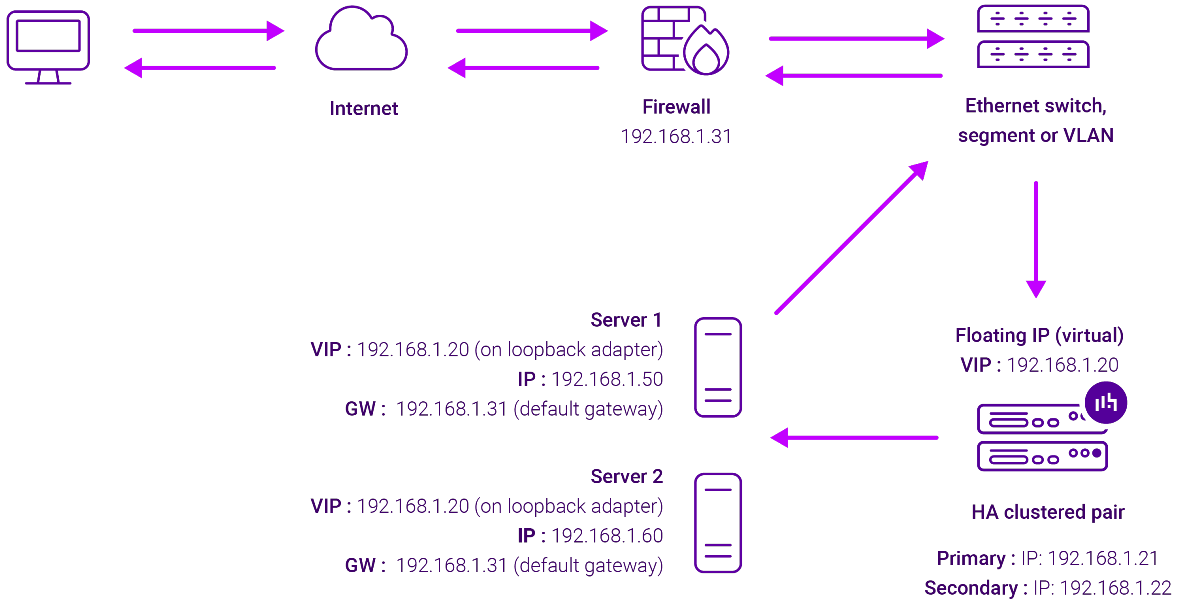
The load balancer can be deployed in 4 fundamental ways: ***Layer 4 DR mode***, ***Layer 4 NAT mode***, ***Layer 4 SNAT mode***, and ***Layer 7 SNAT mode***.

For Planmeca Romexis, layer 4 DR mode is recommended. This mode is described below and is used for the configuration presented in this guide.

7.1. Layer 4 DR Mode

Layer 4 DR (Direct Routing) mode is a very high performance solution that requires little change to your existing infrastructure. The image below shows an example network diagram for this mode.

> **Note** Kemp, Brocade, Barracuda & A10 Networks call this ***Direct Server Return*** and F5 call it ***nPath***.

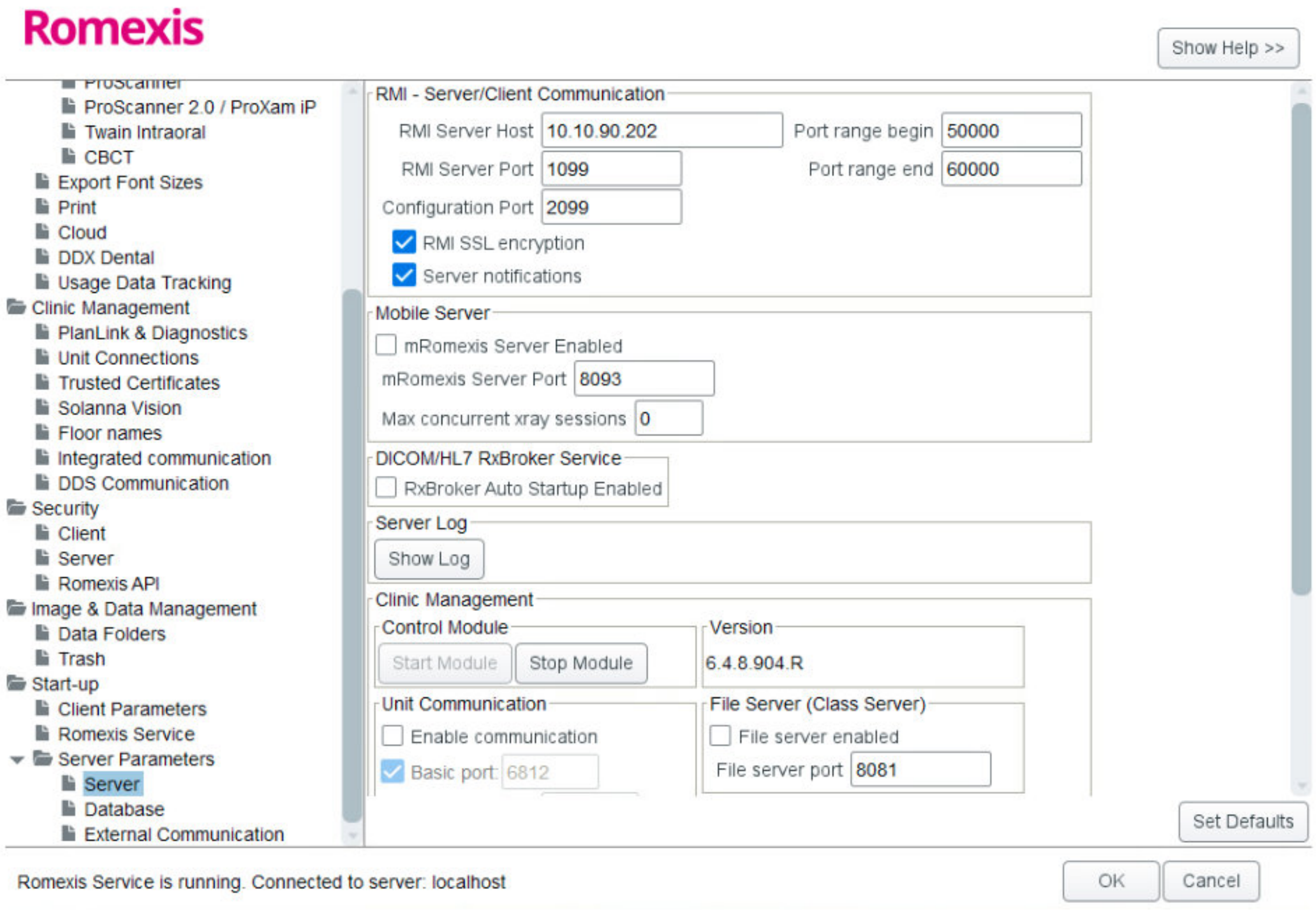

Internet
Firewall
192.168.1.31
Ethernet switch,
segment or VLAN
Server 1
VIP : 192.168.1.20 (on loopback adapter)
IP : 192.168.1.50
GW : 192.168.1.31 (default gateway)
Floating IP (virtual)
VIP : 192.168.1.20
Server 2
VIP : 192.168.1.20 (on loopback adapter)
IP : 192.168.1.60
GW : 192.168.1.31 (default gateway)
HA clustered pair
Primary : IP: 192.168.1.21
Secondary : IP: 192.168.1.22

- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that each Real Server (and the load balanced application) must respond to both the Real Server's own IP address and the VIP.
- The Real Server should not respond to ARP requests for the VIP. Only the load balancer should do this. Configuring the Real Server in this way is referred to as "Solving the ARP Problem". For more information please refer to DR Mode Considerations.
- On average, DR mode is 8 times quicker than NAT mode for HTTP and much faster for other applications such as Remote Desktop Services, streaming media and FTP.
- The load balancer must have an interface in the same subnet as the Real Servers to ensure layer 2 connectivity which is required for DR mode to operate.
- The VIP can be brought up on the same subnet as the Real Servers or on a different subnet provided that the load balancer has an interface in that subnet.
- Port translation is not possible with DR mode, e.g. VIP:80 → RIP:8080 is not supported.
- DR mode is transparent, i.e. the Real Server will see the source IP address of the client.

8. Configuring Planmeca Romexis for Load Balancing

8.1. Application Configuration

Configure each Romexis server as per the screenshot below:



RMI - Server/Client Communication

RMI Server Host: 10.10.90.202
Port range begin: 50000
RMI Server Port: 1099
Port range end: 60000
Configuration Port: 2099
☑ RMI SSL encryption
☑ Server notifications

Mobile Server

☐ mRomexis Server Enabled
mRomexis Server Port: 8093
Max concurrent xray sessions: 0

DICOM/HL7 RxBroker Service

☐ RxBroker Auto Startup Enabled

Server Log

Clinic Management

Control Module

Version: 6.4.8.904.R

Unit Communication

☐ Enable communication
☑ Basic port: 6812

File Server (Class Server)

☐ File server enabled
File server port: 8081

Romexis Service is running. Connected to server: localhost

> **Note**
>
> The ephemeral port range shown above is 50000-60000. The rule of thumb is that for each connected client 2 ports will be used by the server. Therefore this range should support up to 5000 concurrent client machines. Please adjust accordingly to fit your environment.

8.2. Server Configuration

Layer 4 DR mode VIPs require the "ARP problem" to be solved on each load balanced Real Server. This enables DR mode to work correctly.

Detailed steps on solving the "ARP problem" for Windows 2012 & later are presented below. These steps must be followed on both Real (Planmeca Romexis) Servers.

8.2.1. Windows Server 2012 & Later

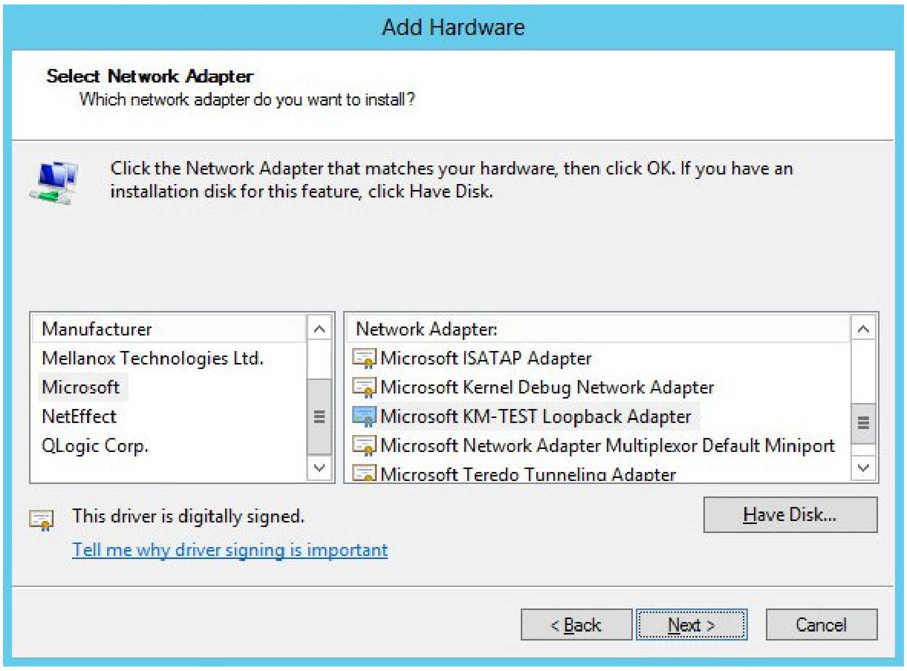
Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables the server to receive packets that have their destination set as the VIP address. If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

In addition, the strong/weak host behavior must be configured on each Real Server. The weak host model allows packets with any IP to be sent or received via an interface. The strong host model only allows packets with an IP belonging to the interface to be sent or received.

Important The following 3 steps must be completed on ***all*** Real Servers associated with the VIP.

Step 1 of 3: Install the Microsoft Loopback Adapter

1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard.
2. Once the Wizard has started, click **Next**.
3. Select **Install the hardware that I manually select from a list (Advanced)**, click **Next**.
4. Select **Network adapters**, click **Next**.



Add Hardware

Select Network Adapter
Which network adapter do you want to install?

Click the Network Adapter that matches your hardware, then click OK. If you have an installation disk for this feature, click Have Disk.

Manufacturer
Mellanox Technologies Ltd.
Microsoft
NetEffect
QLogic Corp.

Network Adapter:
Microsoft ISATAP Adapter
Microsoft Kernel Debug Network Adapter
Microsoft KM-TEST Loopback Adapter
Microsoft Network Adapter Multiplexor Default Miniport
Microsoft Teredo Tunneling Adapter

This driver is digitally signed.
Tell me why driver signing is important

5. Select **Microsoft** & **Microsoft KM-Test Loopback Adapter**, click **Next**.
6. Click **Next** to start the installation, when complete click **Finish**.

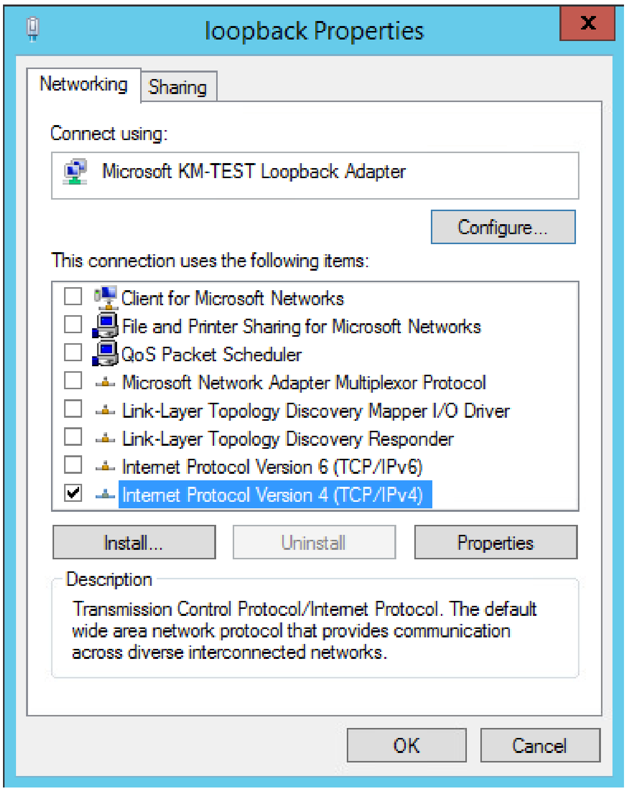
Step 2 of 3: Configure the Loopback Adapter

1. Open Control Panel and click **Network and Sharing Center**.
2. Click **Change adapter settings**.
3. Right-click the new Loopback Adapter and select **Properties**.

Note You can configure IPv4 or IPv6 addresses or both depending on your requirements.

IPv4 Addresses

1. Uncheck all items except **Internet Protocol Version 4 (TCP/IPv4)** as shown below:



loopback Properties

Networking | Sharing

Connect using:

Microsoft KM-TEST Loopback Adapter

Configure...

This connection uses the following items:

- ☐ Client for Microsoft Networks
- ☐ File and Printer Sharing for Microsoft Networks
- ☐ QoS Packet Scheduler
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☐ Link-Layer Topology Discovery Mapper I/O Driver
- ☐ Link-Layer Topology Discovery Responder
- ☐ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

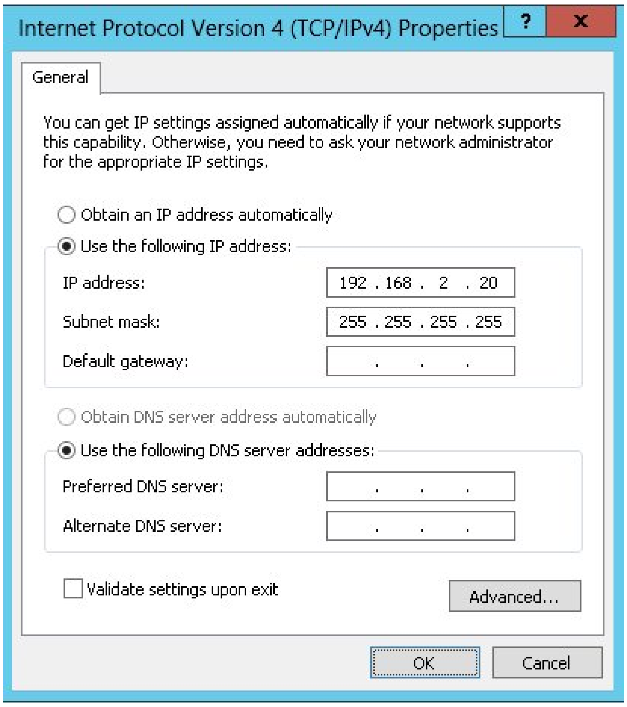
Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

2. Ensure that **Internet Protocol Version (TCP/IPv4)** is selected, click **Properties** and configure the IP address to be the same as the Virtual Service address (VIP) with a subnet mask of **255.255.255.255**, e.g. **192.168.2.20/255.255.255.255** as shown below:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 20

Subnet mask: 255 . 255 . 255 . 255

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK | Cancel

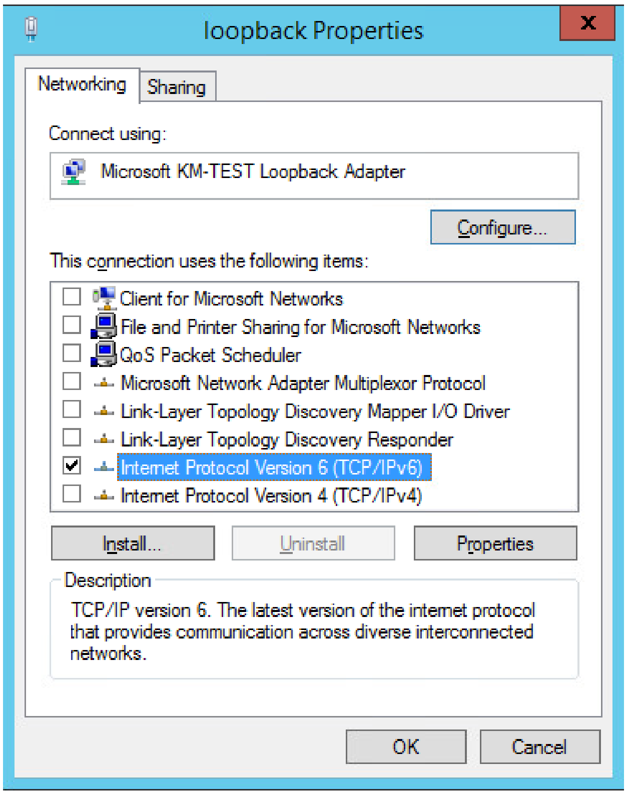
Note: **192.168.2.20** is an example, make sure you specify the correct VIP address.

Note: If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

3. Click **OK** then click **Close** to save and apply the new settings.

IPv6 Addresses

1. Uncheck all items except **Internet Protocol Version 6 (TCP/IPv6)** as shown below:



loopback Properties

Networking | Sharing

Connect using:

Microsoft KM-TEST Loopback Adapter

Configure...

This connection uses the following items:

- ☐ Client for Microsoft Networks
- ☐ File and Printer Sharing for Microsoft Networks
- ☐ QoS Packet Scheduler
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☐ Link-Layer Topology Discovery Mapper I/O Driver
- ☐ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☐ Internet Protocol Version 4 (TCP/IPv4)

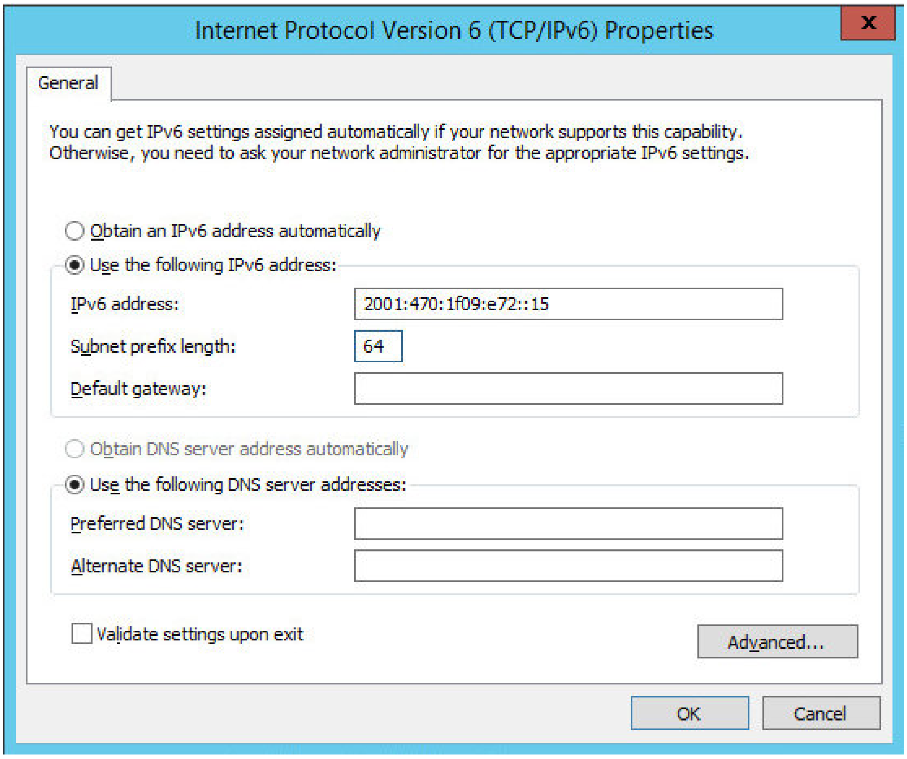
Install... | Uninstall | Properties

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

OK | Cancel

2. Ensure that **Internet Protocol Version (TCP/IPv6)** is selected, click **Properties** and configure the IP address to be the same as the Virtual Service (VIP) and set the ***Subnet Prefix Length*** to be the same as your network setting, e.g. **2001:470:1f09:e72::15/64** as shown below:



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

○ Obtain an IPv6 address automatically

● Use the following IPv6 address:

IPv6 address: 2001:470:1f09:e72::15

Subnet prefix length: 64

Default gateway:

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

ℹ Note **2001:470:1f09:e72::15/64** is an example, make sure you specify the correct VIP address.

ℹ Note If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

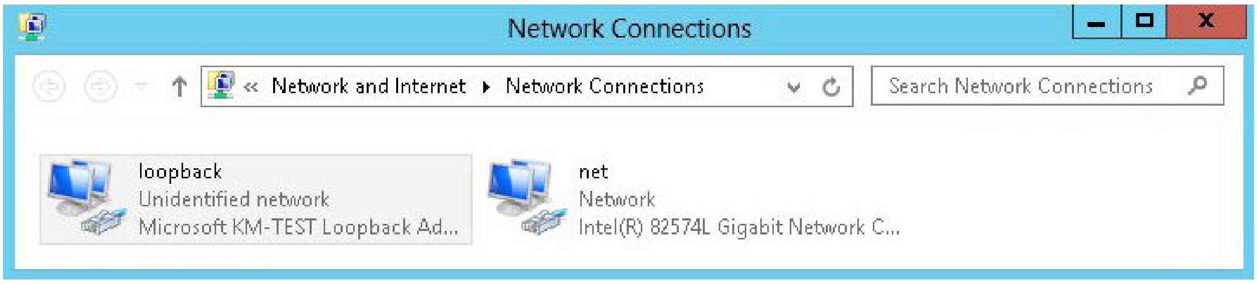
3. Click **OK** then click **Close** to save and apply the new settings.

Step 3 of 3: Configure the strong/weak host behavior

The strong/weak host behavior can be configured using either of the following 2 methods:

- Option 1 - Using network shell (netsh) commands
- Option 2 - Using PowerShell cmdlets

The commands in this section assume that the LAN Adapter is named "**net**" and the Loopback Adapter is named "**loopback**" as shown in the example below:



Network Connections

« Network and Internet ▸ Network Connections

Search Network Connections

loopback
Unidentified network
Microsoft KM-TEST Loopback Ad...

net
Network
Intel(R) 82574L Gigabit Network C...

ⓘ Important Either adjust the commands to use the names allocated to your LAN and loopback adapters, or rename the adapters before running the commands. Names are case sensitive so make sure that the interface names used in the commands match the adapter names exactly.

Option 1 - Using Network Shell (netsh) Commands

To configure the correct strong/weak host behavior run the following commands:

For IPv4 addresses:

```
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

For IPv6 addresses:

```
netsh interface ipv6 set interface "net" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostsend=enabled
netsh interface ipv6 set interface "loopback" dadtransmits=0
```

Option 2 - Using PowerShell Cmdlets

For IPv4 addresses:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled
-DadTransmits 0 -AddressFamily IPv4
```

```
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv4
```

For IPv6 Addresses:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled
-DadTransmits 0 -AddressFamily IPv6
```

```
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv6
```

9. Loadbalancer.org Appliance – the Basics

9.1. Virtual Appliance

A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM, XEN and Nutanix AHV and has been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB virtual disk. The Virtual Appliance can be downloaded here.

Note

The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance's WebUI.

Note

Please refer to Virtual Appliance Installation and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.

Note

The VA has 4 network adapters. For VMware only the first adapter (**eth0**) is connected by default. For HyperV, KVM, XEN and Nutanix AHV all adapters are disconnected by default. Use the network configuration screen within the Hypervisor to connect the required adapters.

9.2. Initial Network Configuration

After boot up, follow the instructions on the appliance console to configure the management IP address, subnet mask, default gateway, DNS servers and other network and administrative settings.

Important

Be sure to set a secure password for the load balancer, when prompted during the setup routine.

9.3. Accessing the Appliance WebUI

The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to External Authentication.

Note

There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant Quick Start / Configuration Guide.

1. Using a browser, navigate to the following URL:

   https://<IP-address-configured-during-the-network-setup-wizard>:9443/lbadmin/

   Note

   You'll receive a warning about the WebUI's SSL certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more information, please refer to Appliance Security Features.

   Note

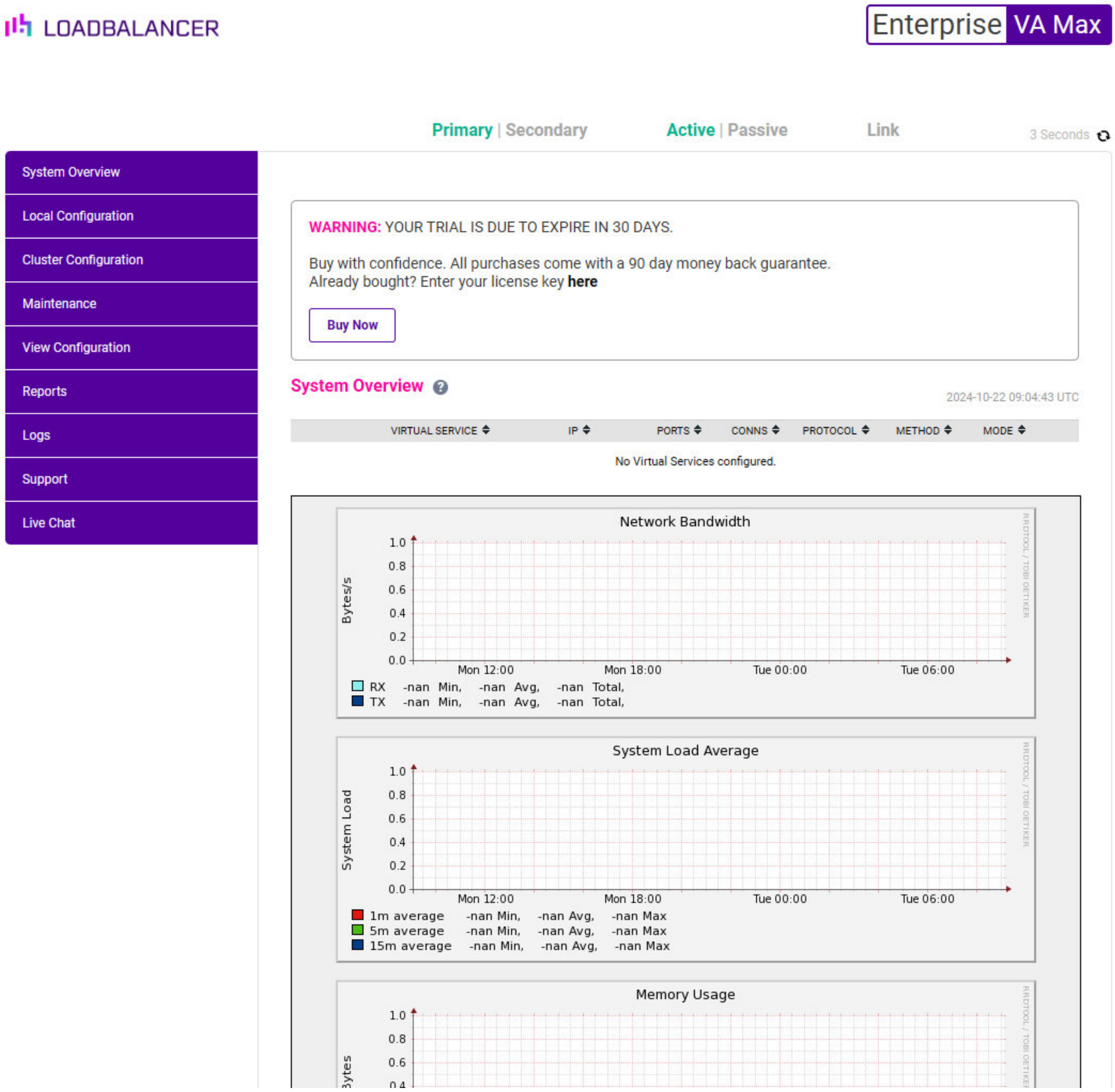
   If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

2. Log in to the WebUI using the following credentials:

   Username: loadbalancer
   Password: <configured-during-network-setup-wizard>

Note To change the password, use the WebUI menu option: *Maintenance > Passwords.*

Once logged in, the WebUI will be displayed as shown below:



WARNING: YOUR TRIAL IS DUE TO EXPIRE IN 30 DAYS.

Buy with confidence. All purchases come with a 90 day money back guarantee.
Already bought? Enter your license key **here**

Buy Now

System Overview

2024-10-22 09:04:43 UTC

VIRTUAL SERVICE	IP	PORTS	CONNS	PROTOCOL	METHOD	MODE

No Virtual Services configured.

Network Bandwidth
Bytes/s
1.0
0.8
0.6
0.4
0.2
0.0
Mon 12:00
Mon 18:00
Tue 00:00
Tue 06:00
RX -nan Min, -nan Avg, -nan Total,
TX -nan Min, -nan Avg, -nan Total,
System Load Average
System Load
1m average -nan Min, -nan Avg, -nan Max
5m average -nan Min, -nan Avg, -nan Max
15m average -nan Min, -nan Avg, -nan Max
Memory Usage
Bytes
RRDTOOL / TOBI OETIKER

9.3.1. Main Menu Options

System Overview - Displays a graphical summary of all VIPs, RIPs and key appliance statistics
Local Configuration - Configure local host settings such as IP address, DNS, system time etc.
Cluster Configuration - Configure load balanced services such as VIPs & RIPs
Maintenance - Perform maintenance tasks such as service restarts and creating backups
View Configuration - Display the saved appliance configuration settings
Reports - View various appliance reports & graphs
Logs - View various appliance logs
Support - Create a support download, contact the support team & access useful links
Live Chat - Start a live chat session with one of our Support Engineers

9.4. Appliance Software Update

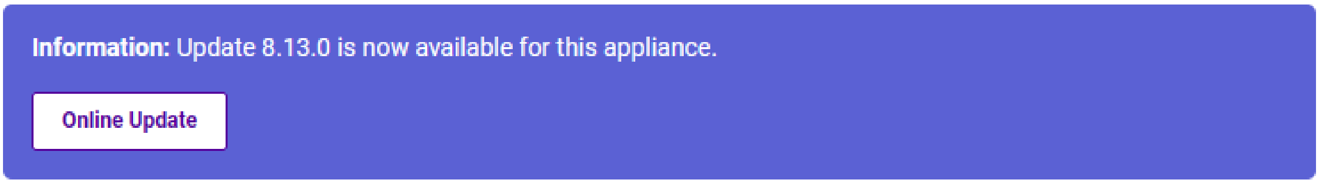
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

> **Note** For full details, please refer to Appliance Software Update in the Administration Manual.

> **Note** Services may need to be restarted/reloaded after the update process completes or in some cases a full appliance restart may be required. We therefore recommend performing the update during a maintenance window.

9.4.1. Online Update

The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:

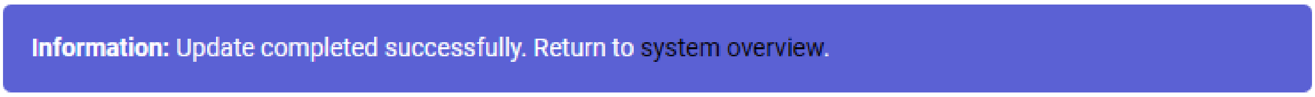


Information: Update 8.13.0 is now available for this appliance.

Click **Online Update**. A summary of all new features, improvements, bug fixes and security updates included in the update will be displayed. Click **Update** at the bottom of the page to start the update process.

> **Important** Do not navigate away whilst the update is ongoing, this may cause the update to fail.

The update can take several minutes depending on download speed and upgrade version. Once complete, the following message will be displayed:



Information: Update completed successfully. Return to system overview.

If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

9.4.2. Offline Update

If the appliance does not have access to the Internet, offline update can be used.

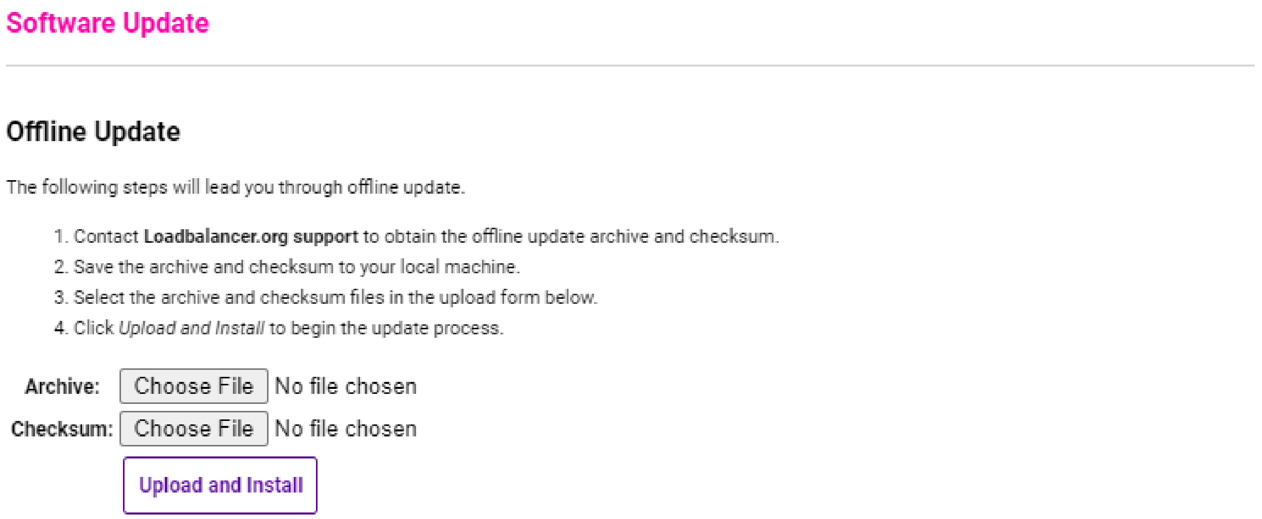
To check for the latest version, please refer to our product roadmap page available here. To obtain the latest offline update files contact support@loadbalancer.org.

To perform an offline update:

1. Using the WebUI, navigate to: *Maintenance > Software Update*.

2. Select **Offline Update**.

3. The following screen will be displayed:



Software Update

Offline Update

The following steps will lead you through offline update.

1. Contact **Loadbalancer.org support** to obtain the offline update archive and checksum.
2. Save the archive and checksum to your local machine.
3. Select the archive and checksum files in the upload form below.
4. Click *Upload and Install* to begin the update process.

Archive: No file chosen

Checksum: No file chosen

4. Select the ***Archive*** and ***Checksum*** files.

5. Click **Upload and Install**.

6. If services need to be reloaded/restarted or the appliance needs a full restart, you'll be prompted accordingly.

9.5. Ports Used by the Appliance

By default, the appliance uses the following TCP & UDP ports:

Protocol	Port	Purpose
TCP	22 *	SSH
TCP & UDP	53 *	DNS / GSLB
TCP & UDP	123	NTP
TCP & UDP	161 *	SNMP
UDP	6694	Heartbeat between Primary & Secondary appliances in HA mode
TCP	7778	HAProxy persistence table replication
TCP	9000 *	Gateway service (Centralized/Portal Management)
TCP	9080 *	WebUI - HTTP (disabled by default)
TCP	9081 *	Nginx fallback page
TCP	9443 *	WebUI - HTTPS
TCP	25565 *	Shuttle service (Centralized/Portal Management)

Note

The ports used for SSH, GSLB, SNMP, the WebUI, the fallback page, the gateway service and the shuttle service can be changed if required. For more information, please refer to Service Socket Addresses.

9.6. HA Clustered Pair Configuration

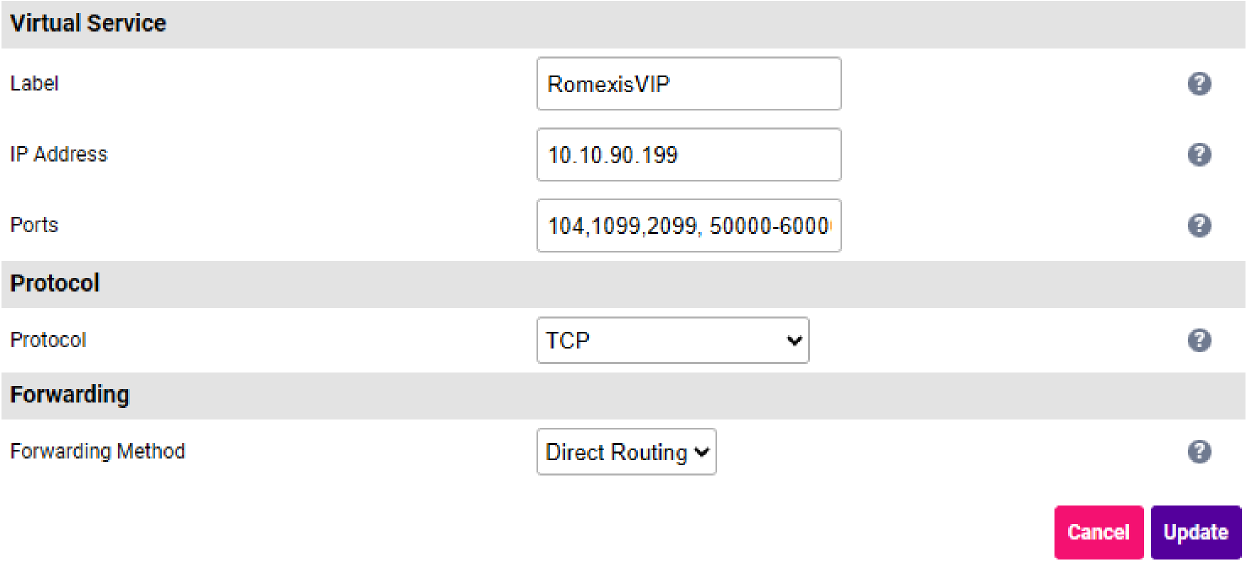
Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary unit is covered in the section Configuring HA - Adding a Secondary Appliance of the appendix.

10. Appliance Configuration for Planmeca Romexis

10.1. VIP 1 - RomexisVIP

10.1.1. Virtual Service (VIP) Configuration

1. Using the WebUI, navigate to *Cluster Configuration > Layer 4 – Virtual Services* and click **Add a new Virtual Service**.



Virtual Service

Label	RomexisVIP
IP Address	10.10.90.199
Ports	104,1099,2099, 50000-6000

Protocol

Protocol	TCP

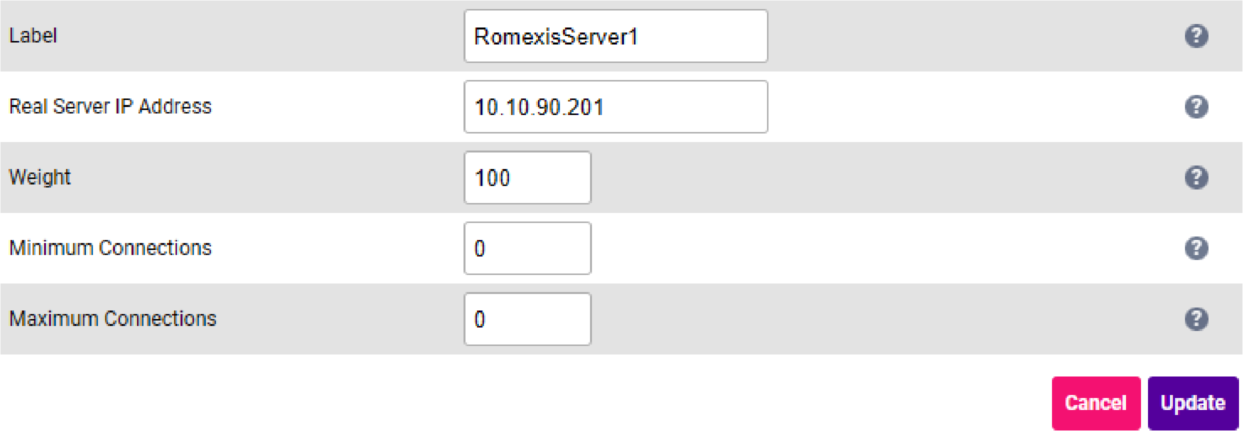
Forwarding

Forwarding Method	Direct Routing

2. Enter a suitable *Label* (name) for the Virtual Service, e.g. **RomexisVIP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.10.90.199**.
4. Set *Ports* to **104,1099,2099, 50000-60000**.
5. Set the *Protocol* to **TCP**.
6. Leave *Forwarding Method* set to **Direct Routing**.
7. Click **Update**.
8. Now click **Modify** next to the newly created VIP.
9. Scroll down to the *Fallback Server* section.
   - Set the *IP address* to the address of the secondary Romexis Server, e.g. **10.10.90.202**.
   - Leave the *Port* field blank and *MASQ Fallback* unchecked.
10. Click **Update**.

10.1.2. Configure the Associated Real Server (RIP)

1. Using the WebUI, navigate to *Cluster Configuration > Layer 4 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.



Label	RomexisServer1
Real Server IP Address	10.10.90.201
Weight	100
Minimum Connections	0
Maximum Connections	0

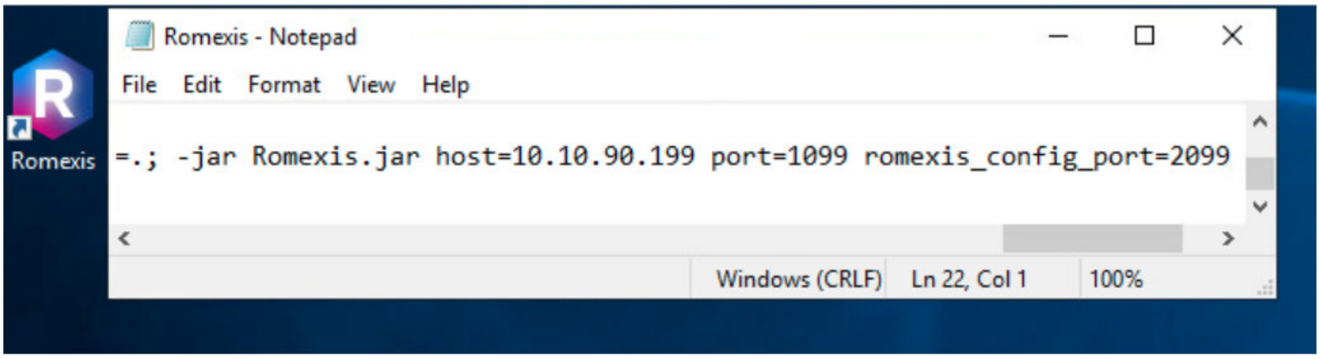
2. Enter a suitable ***Label*** (name) for the Real Server, e.g. **RomexisServer1**.
3. Set the ***Real Server IP Address*** to the address of the primary Romexis Server, e.g. **10.10.90.201**.
4. Click **Update**.

11. Testing & Verification

> Note
>
> For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.

11.1. Accessing Planmeca Romexis via the Load Balancer

Right click on the Romexis Icon on the client machine and change the startup command so the host is set to the VIP address or an FQDN that resolves to the VIP address as shown in the following example:

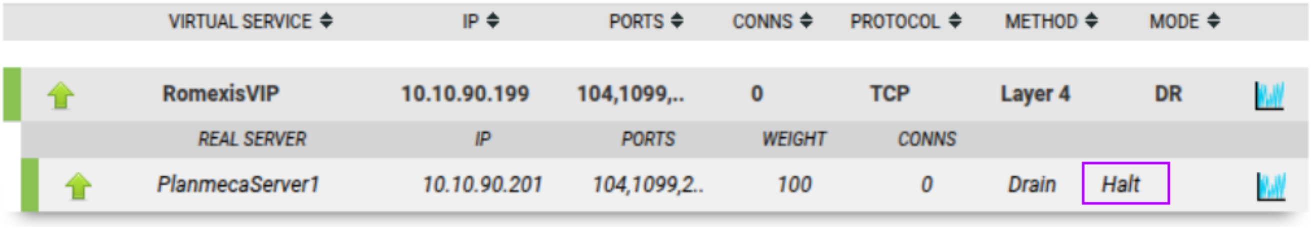


```
=.; -jar Romexis.jar host=10.10.90.199 port=1099 romexis_config_port=2099
```

Once updated, verify that the application can be accessed successfully.

11.2. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of the Virtual Service & the associated Real Server (i.e. the primary Planmeca Romexis server). The example below shows that the primary Planmeca Romexis server is healthy (green) and available to accept connections:



VIRTUAL SERVICE ⬍	IP ⬍	PORTS ⬍	CONNS ⬍	PROTOCOL ⬍	METHOD ⬍	MODE ⬍
RomexisVIP	10.10.90.199	104,1099,..	0	TCP	Layer 4	DR
REAL SERVER	IP	PORTS	WEIGHT	CONNS		
PlanmecaServer1	10.10.90.201	104,1099,2..	100	0	Drain	Halt

To verify that the secondary server takes over, halt the primary server using the halt button in the System Overview (highlighted above) and ensure that everything still functions correctly.

12. Technical Support

For more details about configuring the appliance and assistance with designing your deployment please don't hesitate to contact the support team using the following email address: support@loadbalancer.org.

13. Further Documentation

For additional information, please refer to the Administration Manual.

14. Appendix

14.1. Configuring HA - Adding a Secondary Appliance

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution. We recommend that the Primary appliance is fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

ℹ Note

For Enterprise Azure, the HA pair should be configured first. For more information, please refer to the Azure Quick Start/Configuration Guide available in the documentation library

The clustered HA pair uses Heartbeat to determine the state of the other appliance. Should the active device (normally the Primary) suffer a failure, the passive device (normally the Secondary) will take over.

14.1.1. Non-Replicated Settings

A number of settings are not replicated as part of the Primary/Secondary pairing process and therefore must be manually configured on the Secondary appliance. These are listed by WebUI menu option in the table below:

WebUI Main Menu Option	Sub Menu Option	Description
Local Configuration	Hostname & DNS	Hostname and DNS settings
Local Configuration	Network Interface Configuration	Interface IP addresses, bonding configuration and VLANs
Local Configuration	Routing	Default gateways and static routes
Local Configuration	System Date & time	Time and date related settings
Local Configuration	Physical – Advanced Configuration	Various appliance settings
Local Configuration	Portal Management	Portal management settings
Local Configuration	Security	Security settings
Local Configuration	SNMP Configuration	SNMP settings
Local Configuration	Graphing	Graphing settings
Local Configuration	License Key	Appliance licensing
Maintenance	Backup & Restore	Local XML backups
Maintenance	Software Updates	Appliance software updates
Maintenance	Fallback Page	Fallback page configuration
Maintenance	Firewall Script	Firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

Important

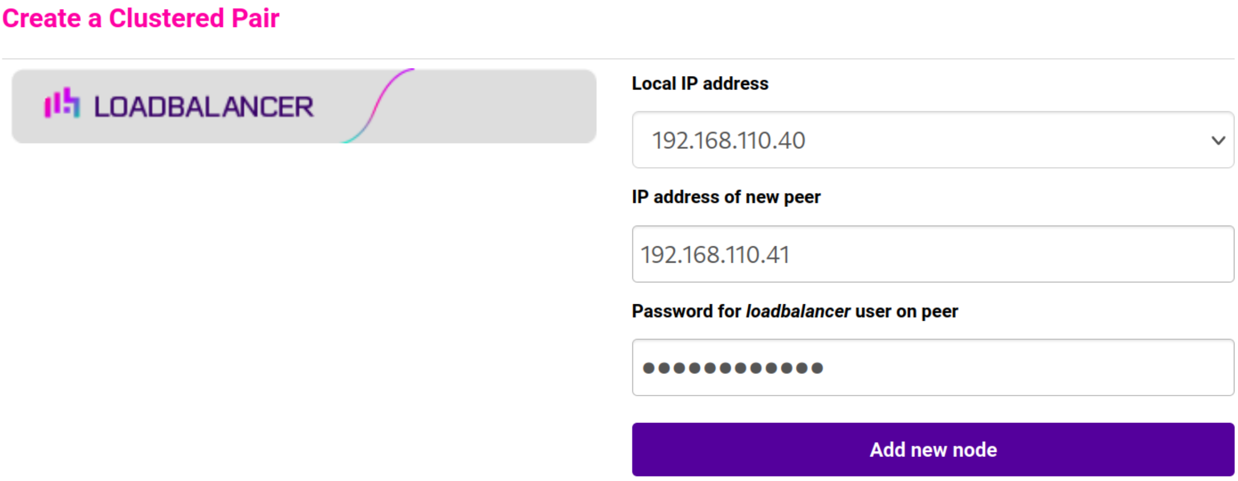
Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

14.1.2. Configuring the HA Clustered Pair

Note

If you have already run the firewall lockdown wizard on either appliance, you'll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: *Cluster Configuration > High-Availability Configuration*.



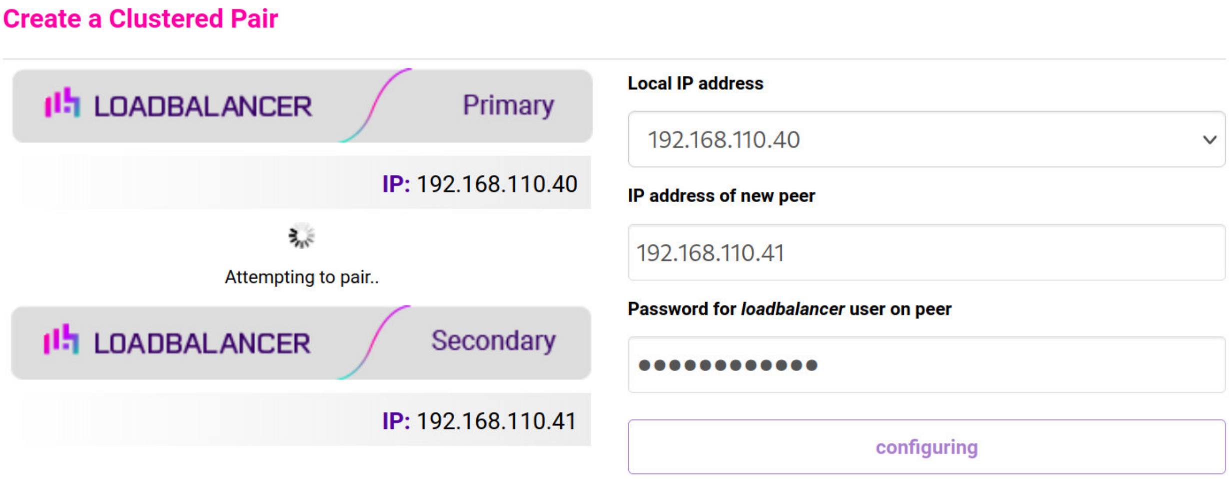
Create a Clustered Pair

Local IP address: 192.168.110.40

IP address of new peer: 192.168.110.41

Password for *loadbalancer* user on peer: ●●●●●●●●●●●●

3. Specify the IP address and the *loadbalancer* user's password for the Secondary (peer) appliance as shown in the example above.
4. Click **Add new node**.
5. The pairing process now commences as shown below:



Create a Clustered Pair

Primary IP: 192.168.110.40

Attempting to pair..

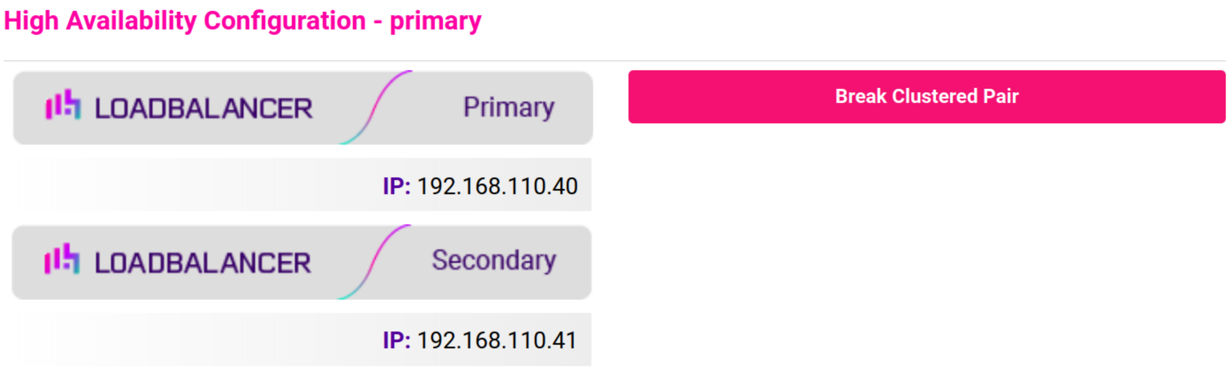
Secondary IP: 192.168.110.41

Local IP address: 192.168.110.40

IP address of new peer: 192.168.110.41

Password for *loadbalancer* user on peer: ●●●●●●●●●●●●

6. Once complete, the following will be displayed on the Primary appliance:



High Availability Configuration - primary

LOADBALANCER Primary

IP: 192.168.110.40

LOADBALANCER Secondary

IP: 192.168.110.41

7. To finalize the configuration, restart heartbeat and any other services as prompted in the "Commit changes" message box at the top of the screen.

ℹ Note	Clicking the **Restart Heartbeat** button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

ℹ Note	For more details on configuring HA with 2 appliances, please refer to Appliance Clustering for HA.

ℹ Note	For details on testing and verifying HA, please refer to Clustered Pair Diagnostics.

15. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	02 May 2025	Initial version		RJC

LOADBALANCER

Visit us: www.loadbalancer.org

Phone us: +44 (0)330 380 1064

Phone us: +1 833 274 2566

Email us: info@loadbalancer.org

Follow us: @loadbalancer.org

About Loadbalancer.org

Loadbalancer.org's mission is to ensure that its clients' businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.