LOADBALANCER

DEPLOYMENT GUIDE

Load Balancing Microsoft LDAP

Version 1.0.0

Table of Contents

1. About this Guide

This guide details the steps required to configure a load balanced Microsoft LDAP environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Microsoft LDAP configuration changes that are required to enable load balancing.

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 Microsoft LDAP. For full specifications of available models please refer to https://www.loadbalancer.org/products/enterprise.

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

- V8.13.2 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. Microsoft LDAP

- Windows Server 2022 with Active Directory Domain Services (LDAP version 3)

4. Microsoft LDAP

The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral application protocol used to query, manage, and authenticate users, systems, and network resources in a centralized directory. On Windows, LDAP is provided primarily through Active Directory Domain Services (AD DS), where the Domain Controllers act as the directory servers.

Enterprise applications, network services, and security tools rely on LDAP (port 389) and LDAPS (LDAP over SSL/TLS, port 636) to look up user credentials, network device connections, and security permissions held in Active Directory. In short, LDAP/LDAPS acts as the "librarian" that allows applications to quickly find directory information and authenticate users against Active Directory.

5. Load Balancing Microsoft LDAP

> **Note** It's highly recommended that you have a working Microsoft LDAP (Active Directory) environment first before implementing the load balancer.

5.1. Load Balancing & HA Requirements

Microsoft LDAP directory services can be deployed across multiple servers (Active Directory Domain Controllers) and load balanced to provide load sharing, high availability and resilience.

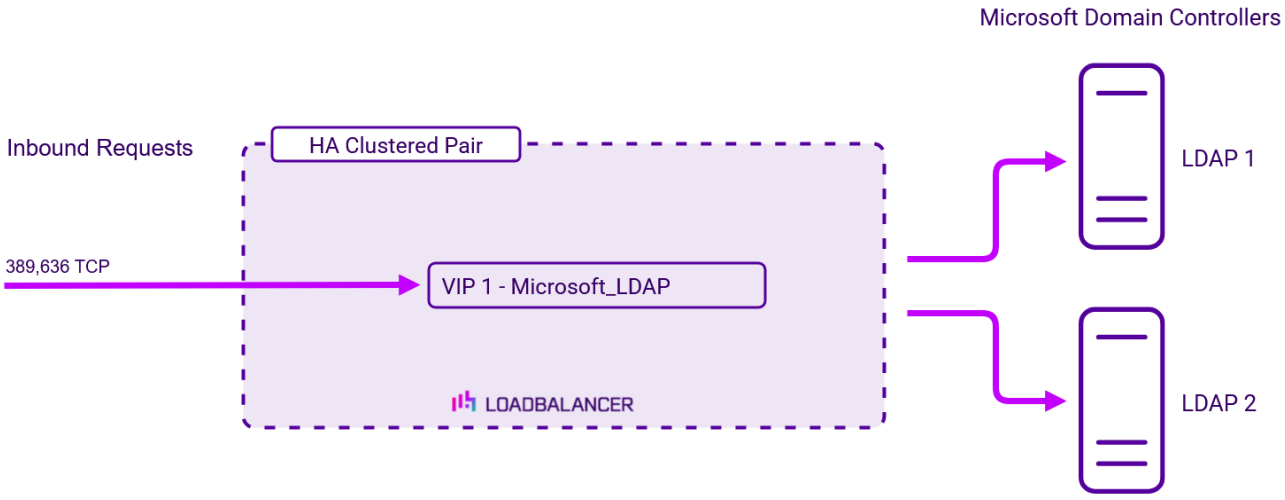
5.2. Virtual Service (VIP) Requirements

The load balancer supports three deployment modes for Microsoft LDAP. Only one mode is required - select the mode that best suits your network topology (for more details of each mode, see Load Balancer Deployment Methods). Each mode uses a single VIP that load balances both LDAP and LDAPS:

Ref.	VIP Name	Mode	Port(s)	Persistence Mode	Health Check	Topology
Mode 1	Microsoft_LDAP	L4 DR (TCP)	389,636	Source IP (300s)	Connect to Port	One-Arm
Mode 2	Microsoft_LDAP	L4 NAT (TCP)	389,636	Source IP (300s)	Connect to Port	Two-Arm
Mode 3	Microsoft_LDAP	L7 SNAT (TCP)	389,636	Source IP (300s)	Connect to Port	One-Arm or Two-Arm

6. Deployment Concept

Once the load balancer is deployed, clients connect to the Virtual Service (VIP) rather than connecting directly to one of the Microsoft LDAP servers. These connections are then load balanced across the Active Directory Domain Controllers to distribute the load according to the load balancing algorithm selected.



> **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

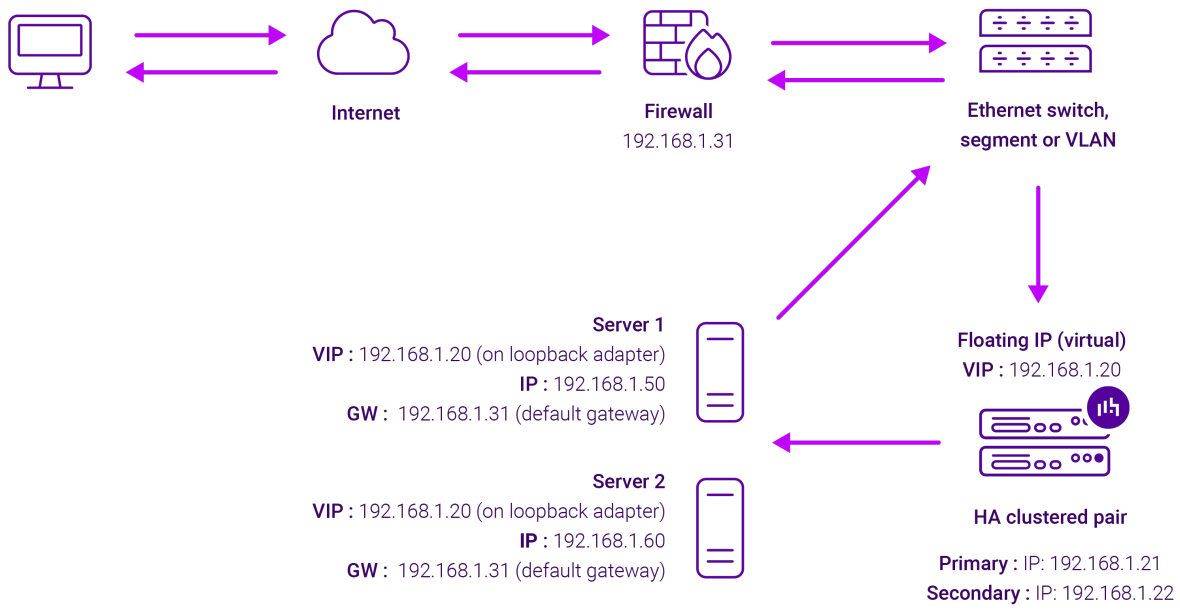
The load balancer can be deployed in 4 fundamental ways: ***Layer 4 DR mode***, ***Layer 4 NAT mode***, ***Layer 4 SNAT mode***, and ***Layer 7 SNAT mode***.

For Microsoft LDAP, layer 4 DR mode, layer 4 NAT mode and layer 7 SNAT mode are recommended. These modes are described below and are used for the three configurations 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***.

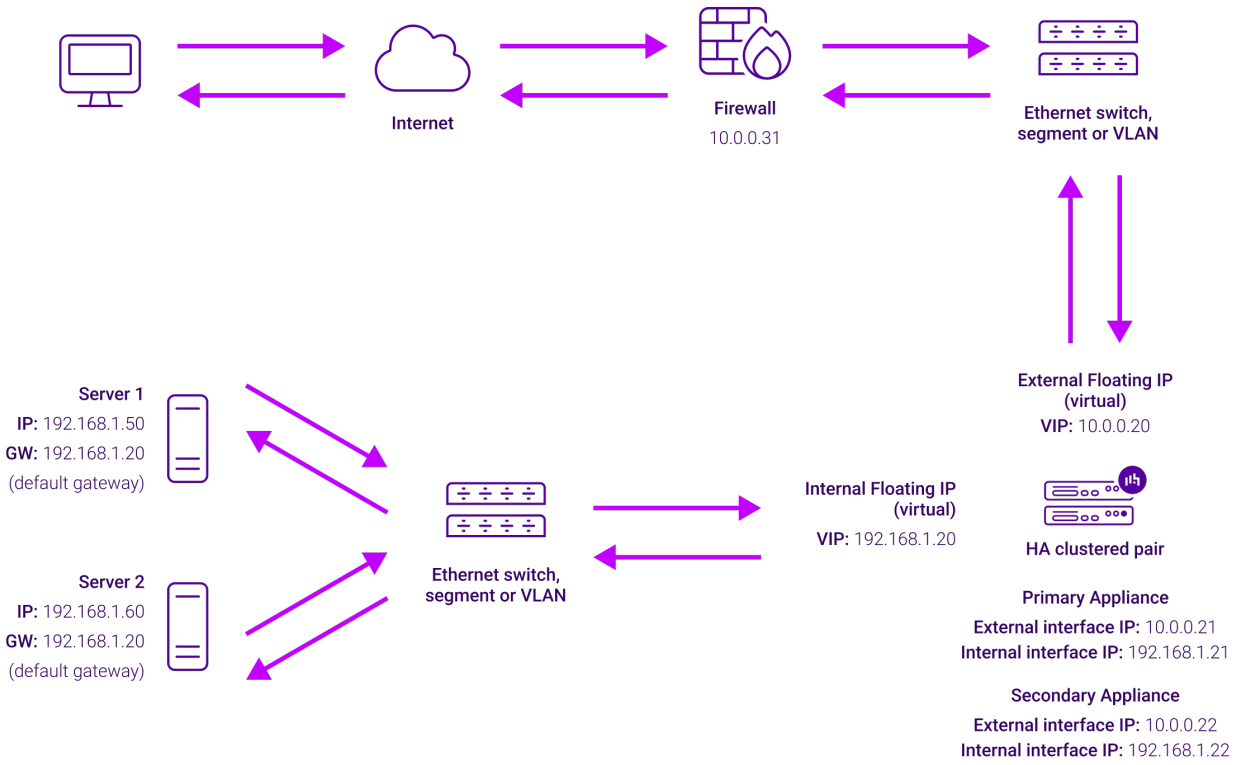


- DR mode works by changing the destination MAC address of the incoming packet to match the selected Real Server on the fly which is very fast.
- When the packet reaches the Real Server it expects the Real Server to own the Virtual Services IP address (VIP). This means that each Real Server (and the 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.

7.2. Layer 4 NAT Mode

Layer 4 NAT mode is a high performance solution, although not as fast as layer 4 DR mode. This is because real server responses must flow back to the client via the load balancer rather than directly as with DR mode. The image below shows an example network diagram for this mode.



- The load balancer translates all requests from the Virtual Service to the Real Servers.
- A **Two-arm** configuration is used where the load balancer has 2 network interfaces, one in each subnet. The VIP is brought up in one subnet and the load balanced Real Servers are located in the other.

> **Note** This can be achieved by using two network adapters, or by creating VLANs on a single adapter.

- Normally **eth0** is used for the internal network and **eth1** is used for the external network although this is optional. Any interface can be used for any purpose.
- If the Real Servers require Internet access, *Auto-NAT* should be enabled using the WebUI menu option: *Cluster Configuration > Layer 4 - Advanced Configuration*, the external interface should be selected.
- The default gateway on the Real Servers must be set to be an IP address on the load balancer.

> **Note** For an HA clustered pair, a floating IP should be added to the load balancer and used as

the Real Server's default gateway. This ensures that the IP address can "float" (move) between Primary and Secondary appliances.

- Clients can be located in the same subnet as the VIP or any remote subnet provided they can route to the VIP.
- If you want Real Servers to be accessible on their own IP address for non-load balanced services, e.g. RDP, you will need to setup individual SNAT and DNAT firewall script rules for each Real Server or add additional VIPs for this.
- Port translation is possible with Layer 4 NAT mode, e.g. VIP:80 → RIP:8080 is supported.
- NAT mode is transparent, i.e. the Real Server will see the source IP address of the client.

NAT Mode Packet re-Writing

In NAT mode, the inbound destination IP address is changed by the load balancer from the Virtual Service IP address (VIP) to the Real Server. For outbound replies the load balancer changes the source IP address of the Real Server to be the Virtual Services IP address.

The following table shows an example NAT mode setup:

Protocol	VIP	Port	RIP	Port
TCP	10.0.0.20	80	192.168.1.50	80

In this simple example all traffic destined for IP address 10.0.0.20 on port 80 is load-balanced to the real IP address 192.168.1.50 on port 80.

Packet rewriting works as follows:

1) The incoming packet for the web server has source and destination addresses as:

Source	x.x.x.x:34567	**Destination**	10.0.0.20:80

2) The packet is rewritten and forwarded to the backend server as:

Source	x.x.x.x:34567	**Destination**	192.168.1.50:80

3) Replies return to the load balancer as:

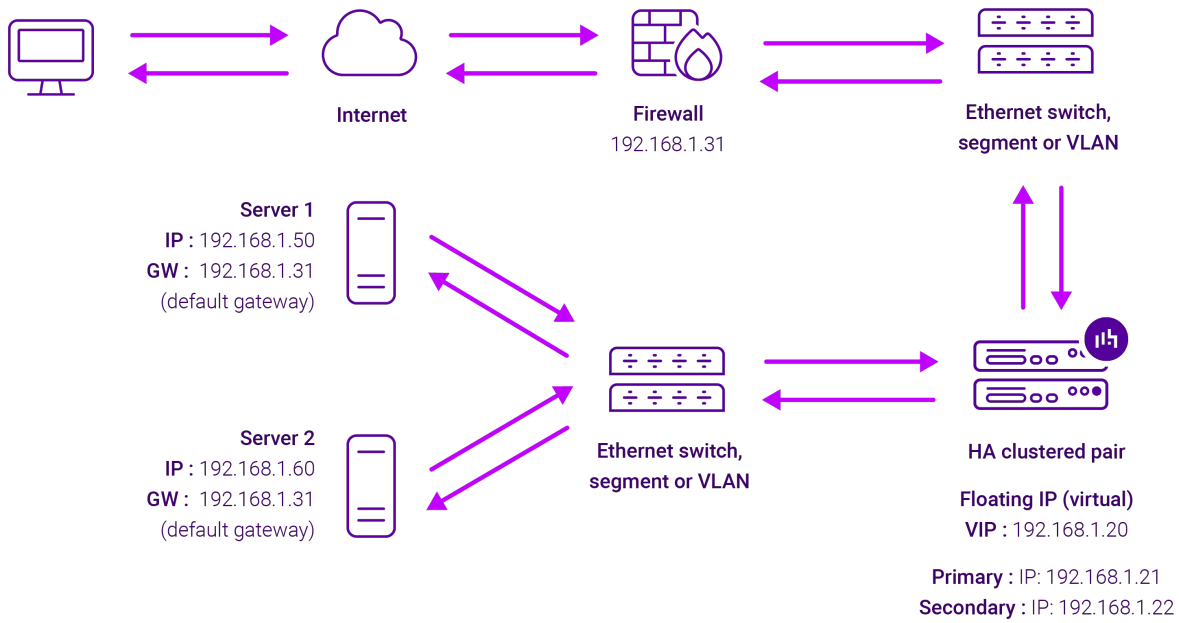
Source	192.168.1.50:80	**Destination**	x.x.x.x:34567

4) The packet is written back to the VIP address and returned to the client as:

Source	10.0.0.20:80	**Destination**	x.x.x.x:34567

7.3. Layer 7 SNAT Mode

Layer 7 SNAT mode uses a proxy (HAProxy) at the application layer. Inbound requests are terminated on the load balancer and HAProxy generates a new corresponding request to the chosen Real Server. As a result, Layer 7 is typically not as fast as the Layer 4 methods. Layer 7 is typically chosen when either enhanced options such as SSL termination, cookie based persistence, URL rewriting, header insertion/deletion etc. are required, or when the network topology prohibits the use of the layer 4 methods. The image below shows an example network diagram for this mode.



- Because layer 7 SNAT mode is a full proxy, Real Servers in the cluster can be on any accessible network including across the Internet or WAN.
- Layer 7 SNAT mode is not transparent by default, i.e. the Real Servers will not see the source IP address of the client, they will see the load balancer's own IP address by default, or any other local appliance IP address if preferred (e.g. the VIP address). This can be configured per layer 7 VIP. If required, the load balancer can be configured to provide the actual client IP address to the Real Servers in 2 ways. Either by inserting a header that contains the client's source IP address, or by modifying the Source Address field of the IP packets and replacing the IP address of the load balancer with the IP address of the client. For more information on these methods please refer to Transparency at Layer 7.
- Layer 7 SNAT mode can be deployed using either a one-arm or two-arm configuration. For two-arm deployments, **eth1** is typically used for client side connections and **eth0** is used for Real Server connections, although this is not mandatory since any interface can be used for any purpose.
- Requires no mode-specific configuration changes to the load balanced Real Servers.
- Port translation is possible with Layer 7 SNAT mode, e.g. VIP:80 → RIP:8080 is supported.
- You should not use the same RIP:PORT combination for layer 7 SNAT mode VIPs and layer 4 SNAT mode VIPs because the required firewall rules conflict.

8. Loadbalancer.org Appliance – the Basics

8.1. 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.

8.2. 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.

8.3. 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.

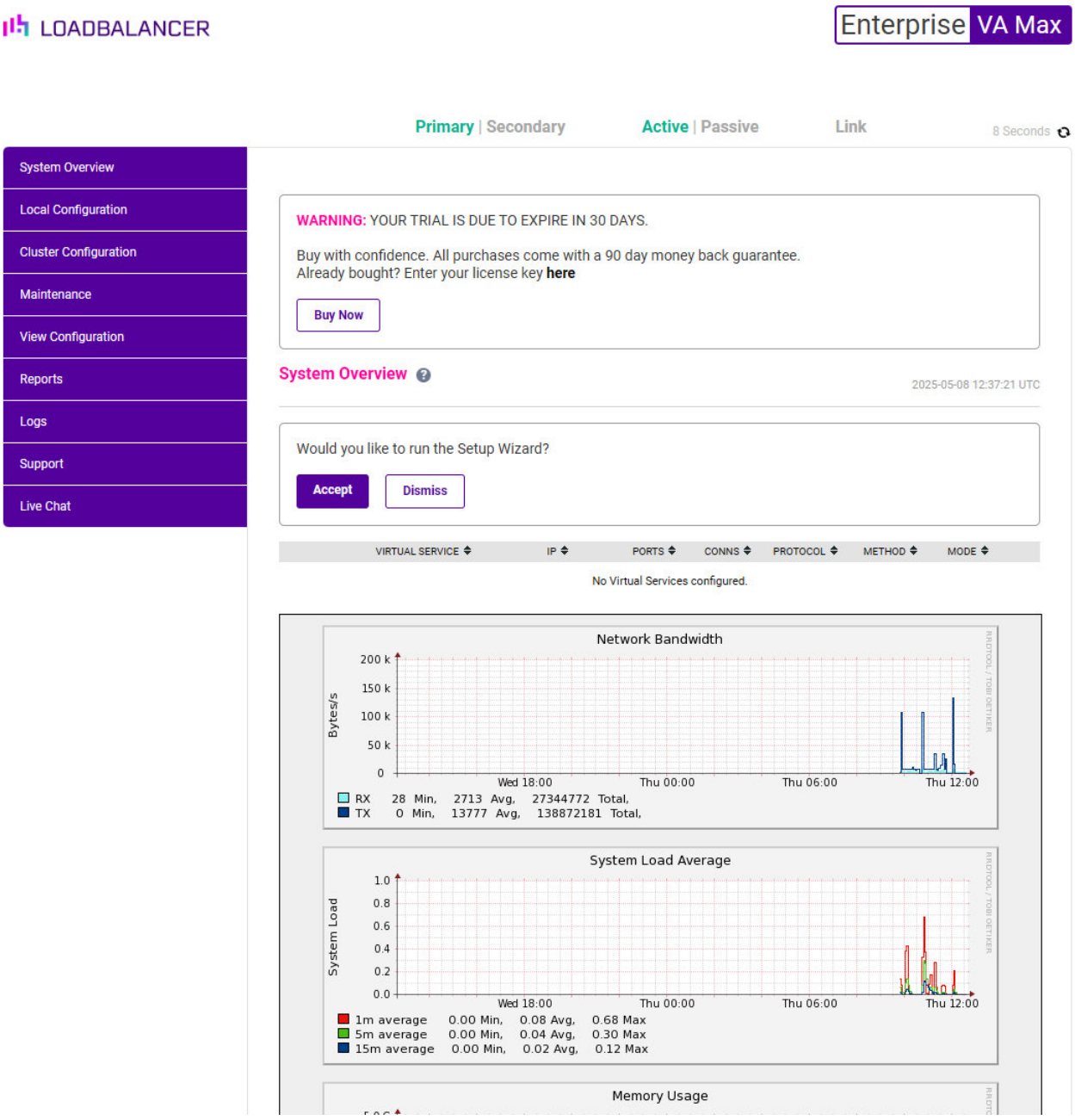
   > **Note** If you need to change the port, IP address or protocol that the WebUI listens on, please refer to Service Socket Addresses.

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:



3. You'll be asked if you want to run the Setup Wizard. Click **Dismiss** if you're following a guide or want to configure the appliance manually. Click **Accept** to start the Setup Wizard.

> **Note** The Setup Wizard can only be used to configure Layer 7 services.

8.3.1. 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

8.4. Appliance Software Update

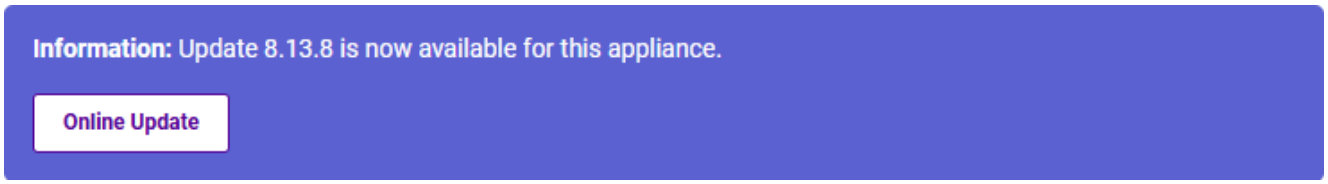
We recommend that the appliance is kept up to date to ensure that you benefit from the latest bug fixes, security updates and feature improvements. Both online and offline update are supported.

> **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.

8.4.1. Online Update

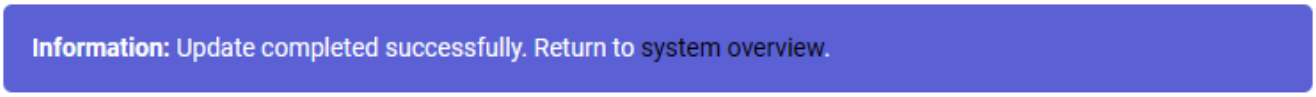
The appliance periodically contacts the Loadbalancer.org update server (**update.loadbalancer.org**) and checks for updates. This is the default behavior and can be disabled if preferred. If an update is found, a notification similar to the example below will be displayed at the top of the WebUI:



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:



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

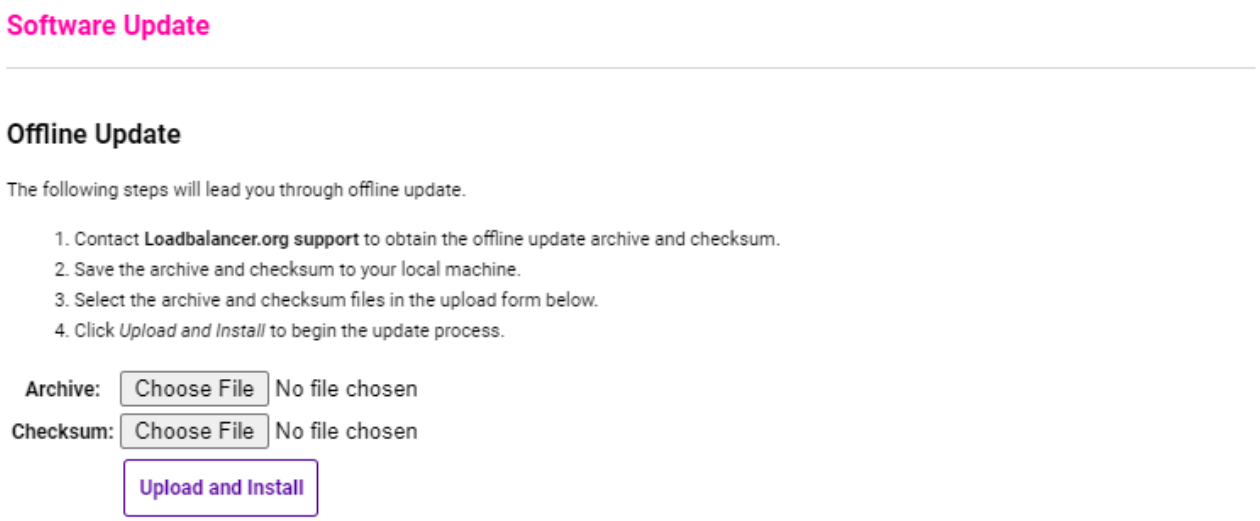
8.4.2. Offline Update

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:



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.

8.5. Ports Used by the Appliance

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

Protocol	Port	Purpose
TCP	22	SSH
TCP & UDP	53	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 for ADC Portal comms

Protocol	Port	Purpose
TCP	9080	WebUI - HTTP (disabled by default)
TCP	9081	Nginx fallback server
TCP	9443	WebUI - HTTPS
TCP	25565	Shuttle service for ADC Portal comms

> **Note** All ports listed above except port 123 (NTP) can be changed if required.

- To change the port used for heartbeat, refer to Configuring High Availability
- To change the port used for HAProxy replication, refer to Layer 7 - Advanced Configuration
- To change other ports, refer to Service Socket Addresses

8.6. 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.

9. Configuring Microsoft LDAP for Load Balancing

The Microsoft LDAP servers must be functioning Active Directory Domain Controllers before they are load balanced. The following summarizes the server-side prerequisites:

- **Static IP address:** Each Windows server should be configured with a static IPv4 address.
- **Active Directory Domain Services (AD DS):** Install the AD DS role (*Server Manager > Manage > Add Roles and Features*) and promote the server to a Domain Controller. Installing AD DS automatically enables LDAP on TCP port 389.
- **LDAPS (TCP 636):** To enable LDAPS, install Active Directory Certificate Services (AD CS) and issue a server certificate suitable for server authentication to the Domain Controller. Run `gpupdate /force` (or restart the server) to apply the new certificate. LDAPS will then be available on port 636.
- **Kerberos certificate (optional):** Where a downstream application using LDAPS additionally requires Kerberos authentication, create and issue a Kerberos certificate template (e.g. via the Certificate Templates console `certtmpl.msc` and `certsrv.msc`).
- **Windows Firewall:** Ensure inbound connections are permitted for LDAP (TCP 389) and LDAPS (TCP 636) on each Domain Controller.

> **Tip** LDAP diagnostic logging can be enabled for troubleshooting via the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics` (set **16 LDAP Interface Events** to **2**, and **15 Field Engineering** to **5**). LDAP events can then be viewed in Event Viewer under *Applications and Services Logs > Directory Service*.

9.1. When using Layer 7 SNAT Mode

Layer 7 SNAT mode VIPs do not require any mode specific configuration changes to the load balanced Real Servers (LDAP servers).

9.2. When using Layer 4 NAT Mode

Layer 4 NAT mode VIPs require the default gateway on the Real Servers to be an IP address on the load balancer. This ensures that return traffic passes back via the load balancer which is required for NAT mode to work.

For an HA clustered pair, a floating IP should be added to the load balancer and used as the Real Server's default gateway. This ensures that the IP address can "float" (move) between Primary and Secondary appliances.

9.3. When using Layer 4 DR Mode

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 each Real Server.

9.3.1. Windows Server 2012 & Later

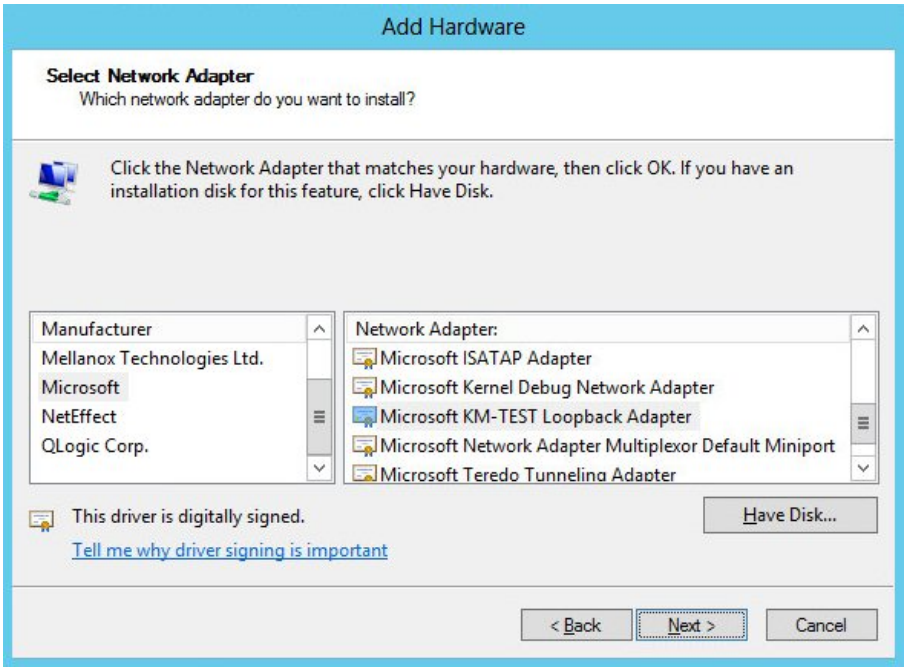
Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables 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**.



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

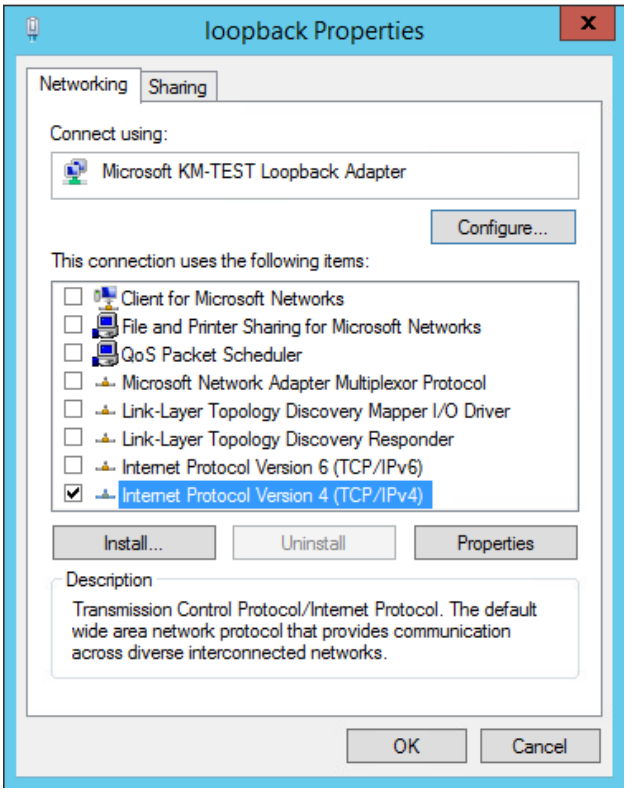
Step 2 of 3: Configure the Loopback Adapter

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**.

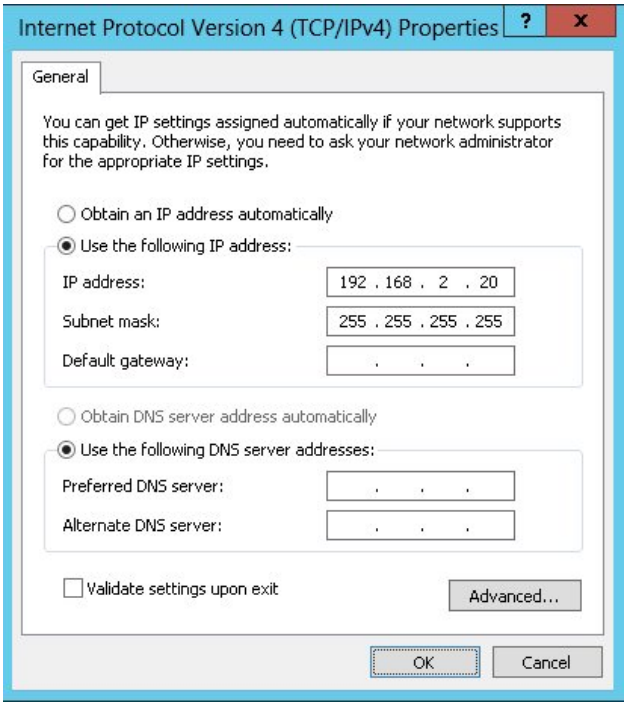
> **Note** You can configure IPv4 or IPv6 addresses or both depending on your requirements.

IPv4 Addresses

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



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:



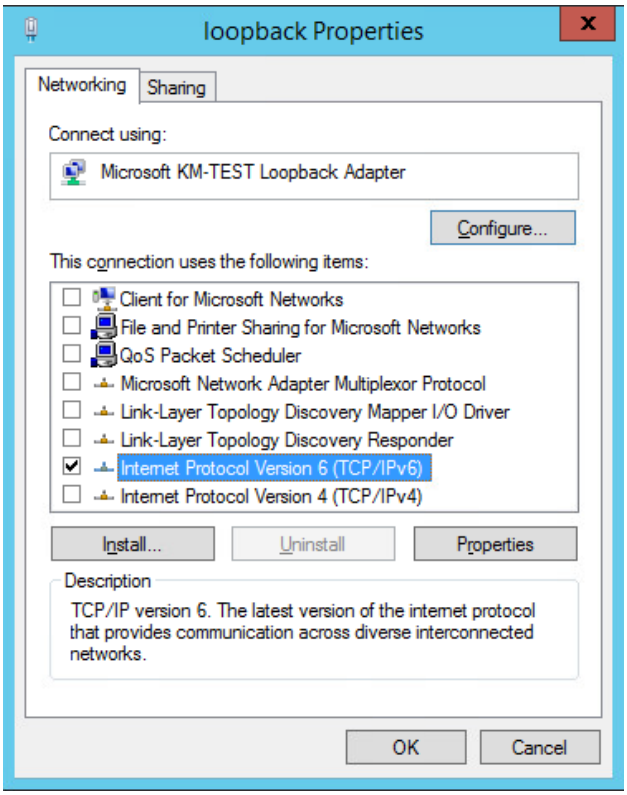
> **Note** **192.168.2.20** is an example, make sure you specify the correct VIP address.

> **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.

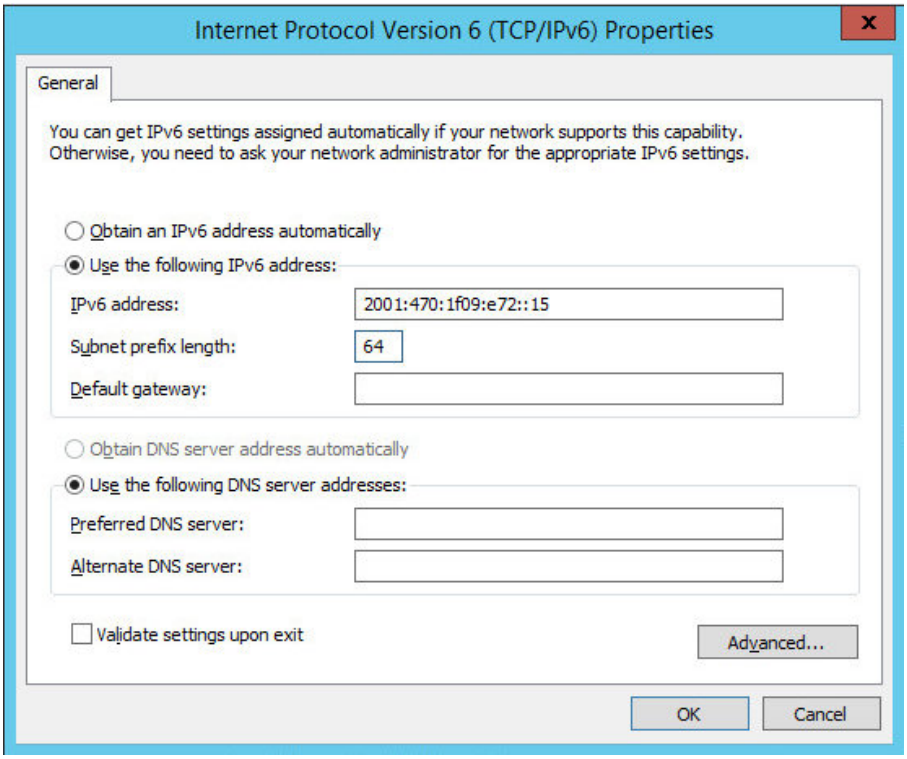
3. Click **OK** then click **Close** to save and apply the new settings.

IPv6 Addresses

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



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:



> **Note** **2001:470:1f09:e72::15/64** 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.

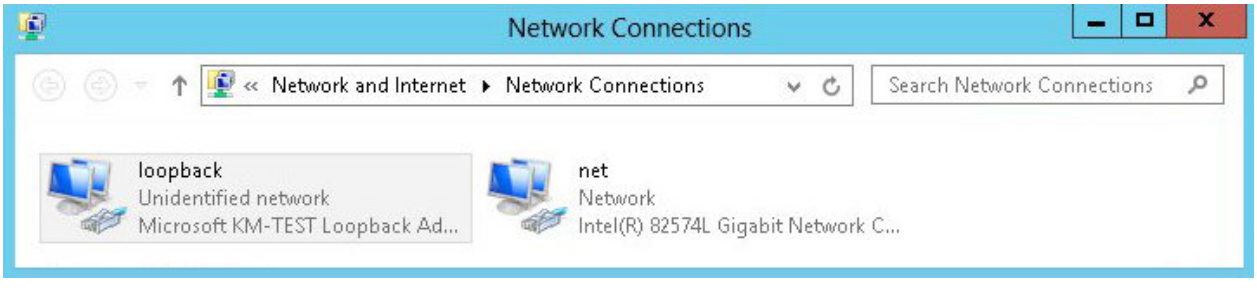
3. Click **OK** then click **Close** to save and apply the new settings.

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:



> **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
-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
```

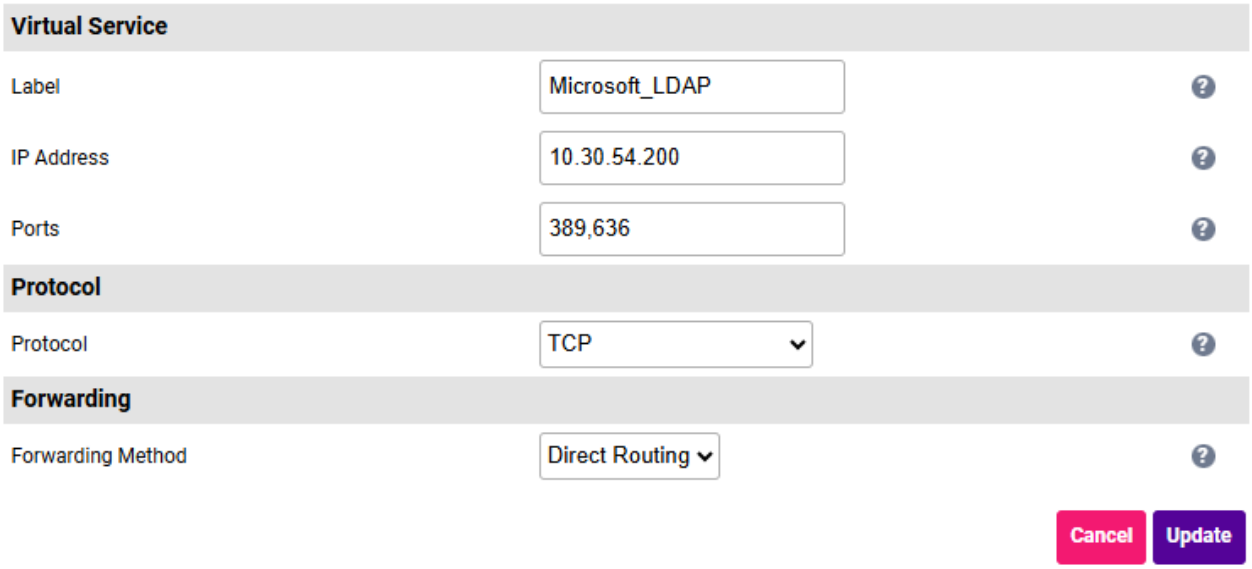
10. Mode 1 - Layer 4 DR Mode (One-Arm)

This mode load balances both LDAP and LDAPS using a single DR mode Virtual Service.

10.1. VIP 1 - Microsoft_LDAP

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**.

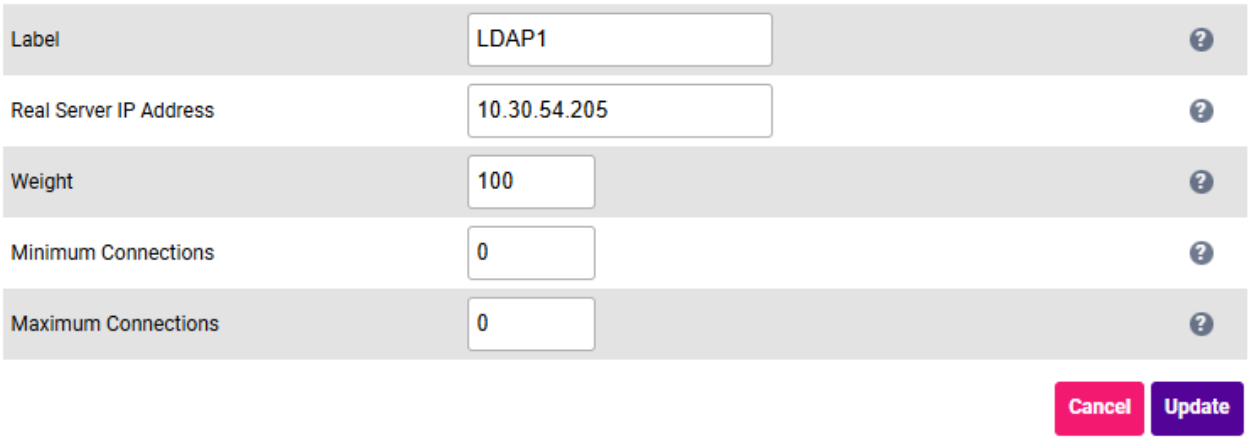


2. Enter a suitable *Label* (name) for the Virtual Service, e.g. **Microsoft_LDAP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.30.54.200**.
4. Set *Ports* to **389,636**.
5. Set the *Protocol* to **TCP**.
6. Leave the *Forwarding Method* set to **Direct Routing**.
7. Click **Update**.
8. Now click **Modify** next to the newly created VIP.
9. Scroll down to the *Persistence* section.
    - Ensure that the *Enable* checkbox is checked.
    - Ensure that the *Timeout* is set to **300** seconds.
10. Scroll down to the *Health Checks* section.
    - Ensure that *Check Type* is set to **Connect to port**.
11. Leave all other settings at their default value.
12. Click **Update**.

> **Note** A standard LDAP query is a one-time, stateless request and does not strictly require persistence. A persistence timeout of 300 seconds is used here to comfortably accommodate query latency and Real Server response times; a lower value (e.g. 120 seconds) is also sufficient.

10.1.2. Configure the Associated Real Servers (RIPs)

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.



2. Enter a suitable *Label* (name) for the Real Server, e.g. **LDAP1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.30.54.205**.
4. Leave all other settings at their default value.
5. Click **Update**.
6. Repeat these steps to add additional Real Server(s).

11. Mode 2 - Layer 4 NAT Mode (Two-Arm)

This mode load balances both LDAP and LDAPS using a single NAT mode Virtual Service.

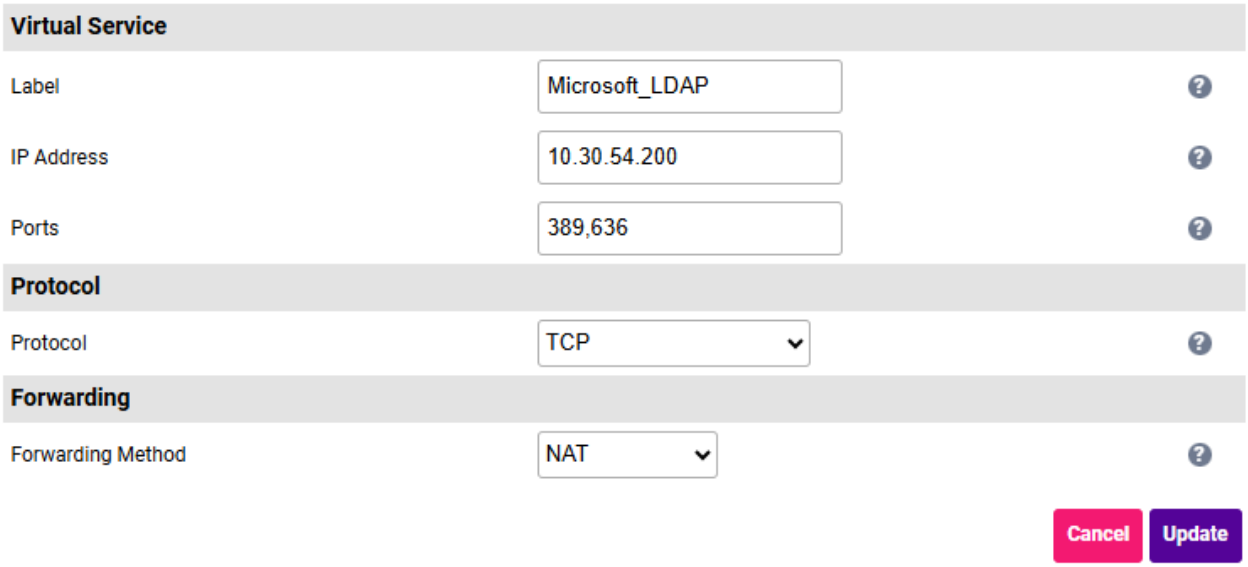
11.1. Network Configuration

Two subnets are used. The VIP is located in one subnet and the load balanced Real Servers are located in the other. The load balancer requires 2 interfaces, one in each subnet. This can be achieved by using two network adapters or by creating VLANs on a single adapter - for more details, please refer to Appliance Network Configuration.

11.2. VIP 1 - Microsoft_LDAP

11.2.1. Virtual Service (VIP) Configuration

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

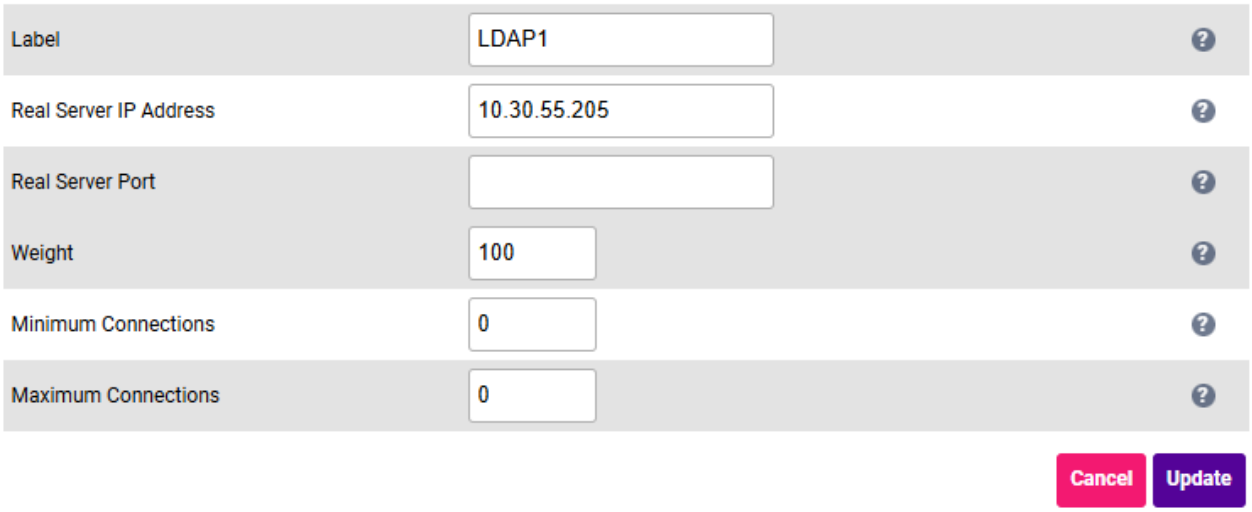


2. Enter a suitable *Label* (name) for the Virtual Service, e.g. **Microsoft_LDAP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.30.54.200**.
4. Set *Ports* to **389,636**.
5. Set the *Protocol* to **TCP**.
6. Set the *Forwarding Method* to **NAT**.
7. Click **Update**.
8. Now click **Modify** next to the newly created VIP.
9. Scroll down to the *Persistence* section.
   - Ensure that the *Enable* checkbox is checked.
   - Ensure that the *Timeout* is set to **300** seconds.
10. Scroll down to the *Health Checks* section.
    - Ensure that *Check Type* is set to **Connect to port**.
11. Leave all other settings at their default value.
12. Click **Update**.

> **Note** In NAT mode the default gateway of each Real Server must be set to an IP address on the load balancer. If the LDAP servers also require internet access, *Auto-NAT* can be enabled under *Cluster Configuration > Layer 4 – Advanced Configuration*.

11.2.2. Configure the Associated Real Servers (RIPs)

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.



2. Enter a suitable *Label* (name) for the Real Server, e.g. **LDAP1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.30.55.205**.
4. Leave the *Real Server Port* field blank — the same ports as the VIP (389 and 636) will be used.
5. Leave all other settings at their default value.
6. Click **Update**.
7. Repeat these steps to add additional Real Server(s).

12. Mode 3 - Layer 7 SNAT Mode (One-Arm or Two-Arm)

This mode load balances both LDAP and LDAPS using a single SNAT mode Virtual Service.

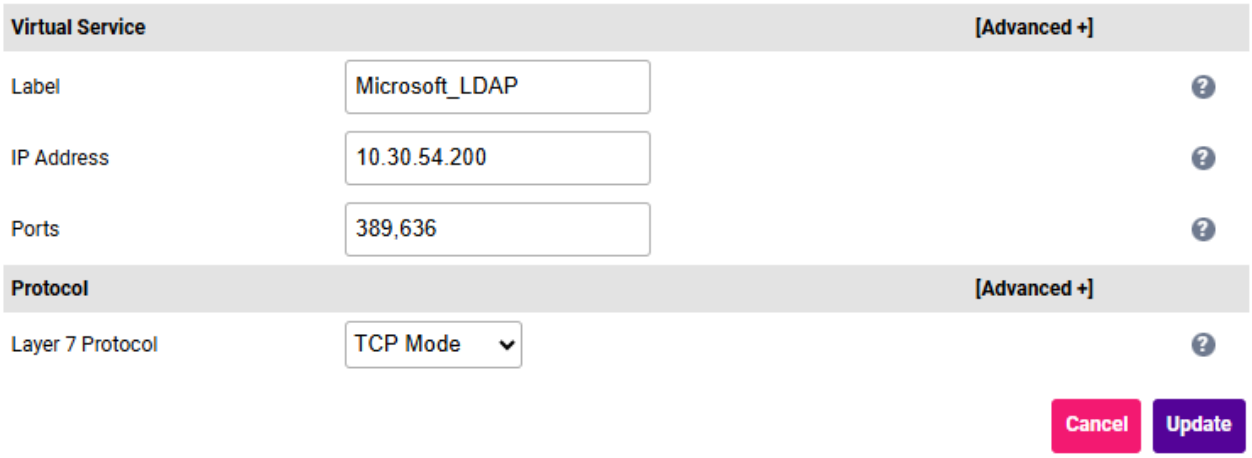
12.1. Network Configuration

For two arm configurations, the load balancer requires 2 interfaces, one in each subnet. This can be achieved by using two network adapters or by creating VLANs on a single adapter - for more details, please refer to Appliance Network Configuration.

12.2. VIP 1 - Microsoft_LDAP

12.2.1. Virtual Service (VIP) Configuration

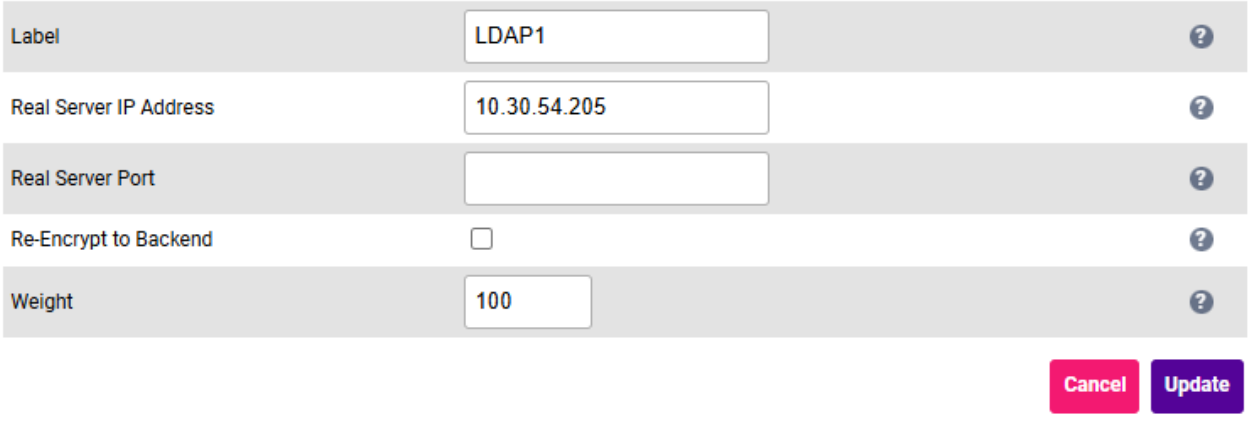
1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Virtual Services* and click **Add a new Virtual Service**.



2. Enter a suitable *Label* (name) for the Virtual Service, e.g. **Microsoft_LDAP**.
3. Set the *Virtual Service IP Address* field to the required IP address, e.g. **10.30.54.200**.
4. Set *Ports* to **389,636**.
5. Set the *Layer 7 Protocol* to **TCP Mode**.
6. Click **Update**.
7. Now click **Modify** next to the newly created VIP.
8. Scroll down to the *Persistence* section and click **[Advanced]**.
   - Ensure that *Persistence Mode* is set to **Source IP**.
   - Set the *Timeout* to **300s** (300 seconds).
9. Scroll down to the *Health Checks* section.
   - Ensure that *Health Checks* is set to **Connect to port**.
10. Leave all other settings at their default value.
11. Click **Update**.

12.2.2. Configure the Associated Real Servers (RIPs)

1. Using the WebUI, navigate to *Cluster Configuration > Layer 7 – Real Servers* and click on **Add a new Real Server** next to the newly created VIP.



2. Enter a suitable *Label* (name) for the Real Server, e.g. **LDAP1**.
3. Set the *Real Server IP Address* field to the required IP address, e.g. **10.30.54.205**.
4. Leave the *Real Server Port* field blank — the same ports as the VIP (389 and 636) will be used.
5. Leave all other settings at their default value.
6. Click **Update**.
7. Repeat these steps to add additional Real Server(s).

12.3. Finalizing the Configuration

If a Layer 7 (Mode 3) Virtual Service has been configured, HAProxy must be reloaded to apply the new settings. This can be done using the button in the "Commit changes" box at the top of the screen or by using the Restart Services menu option:

1. Using the WebUI, navigate to: *Maintenance > Restart Services*.
2. Click **Reload HAProxy**.

13. Testing & Verification

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

13.1. Accessing Microsoft LDAP via the Load Balancer

The load balanced service can be verified using the `ldapsearch` utility (available on the Loadbalancer.org appliance) or any LDAP client. It is recommended to first test directly against each Real Server to confirm the Domain Controllers are responding, then repeat the test against the Virtual Service.

The general format is:

```
ldapsearch -H ldap://<IP_or_FQDN>:<port> -D <user@domain> -W -b <Base DN>
```

Where:

- `-H` — the URI of the LDAP/LDAPS service (`ldap://…:389` or `ldaps://…:636`)
- `-D` — the bind DN or User Principal Name
- `-w` / `-W` — the bind password (supplied on the command line, or prompted for interactively)
- `-b` — the base DN from which to start the search

For example, an LDAP and an LDAPS query against the Virtual Service (filtered to show the directory users):

```
ldapsearch -H ldap://10.30.54.201:389 -D "lbadmin@testdomain.local" -W -b "DC=testdomain,DC=local"
```

```
| grep -i UserPrincipalName

ldapsearch -H ldaps://10.30.54.201:636 -D "lbadmin@testdomain.local" -W -b "DC=testdomain,DC=local"
| grep -i UserPrincipalName
```

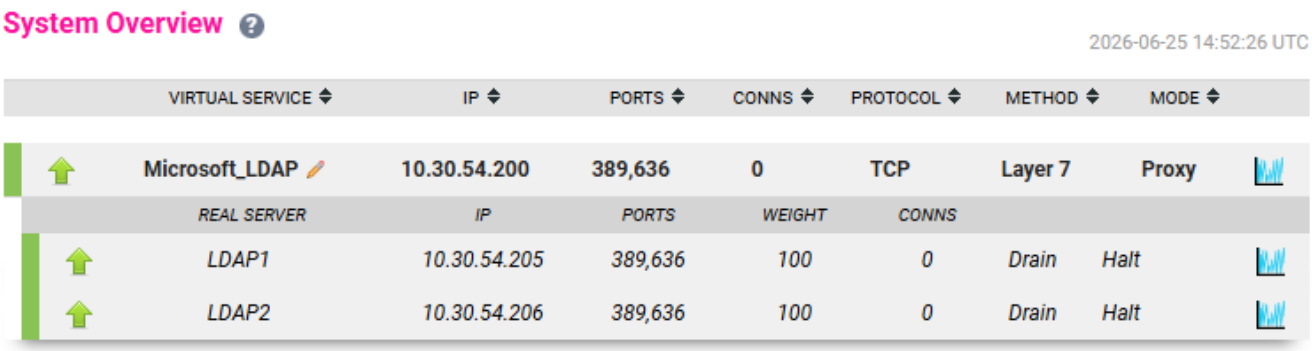
A successful query returns the requested directory information (e.g. the `userPrincipalName` of each user in Active Directory), confirming that both LDAP and LDAPS are being correctly load balanced across the Domain Controllers.

> **Note** Make sure that DNS is updated so that any FQDNs used point to the VIP rather than individual servers.

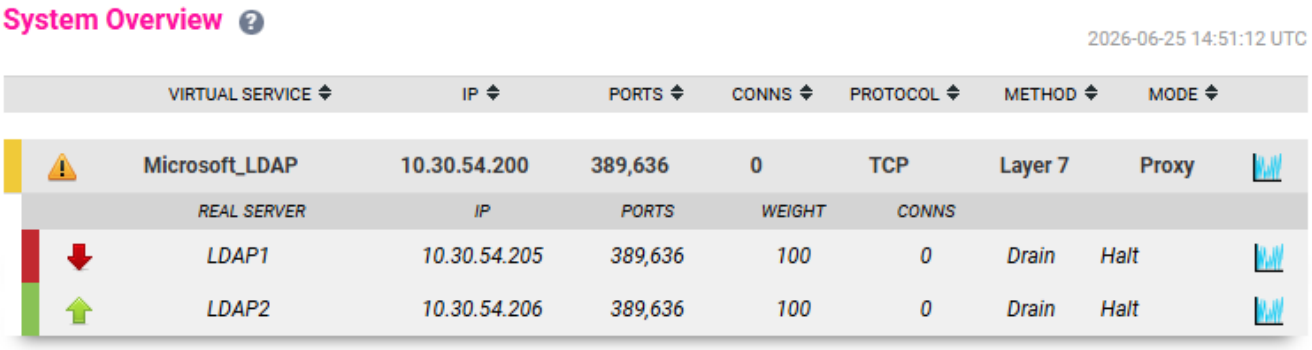
13.2. Using System Overview

The System Overview can be viewed in the WebUI. It shows a graphical view of all Virtual Services & the associated Real Servers (i.e. the Microsoft LDAP servers) and shows the state/health of each server as well as the overall state of each cluster.

The Mode 3 (Layer 7 SNAT) example below shows that all servers are healthy (green) and available to accept connections:



If one of the servers within a cluster fails its health check, that server will be colored red and the cluster will be colored yellow as shown below:



14. 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.

15. Further Documentation

For additional information, please refer to the Administration Manual.

16. Appendix

16.1. 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.

> **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.

16.1.1. 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	Firewall Script	Firewall (iptables) configuration
Maintenance	Firewall Lockdown Wizard	Appliance management lockdown settings

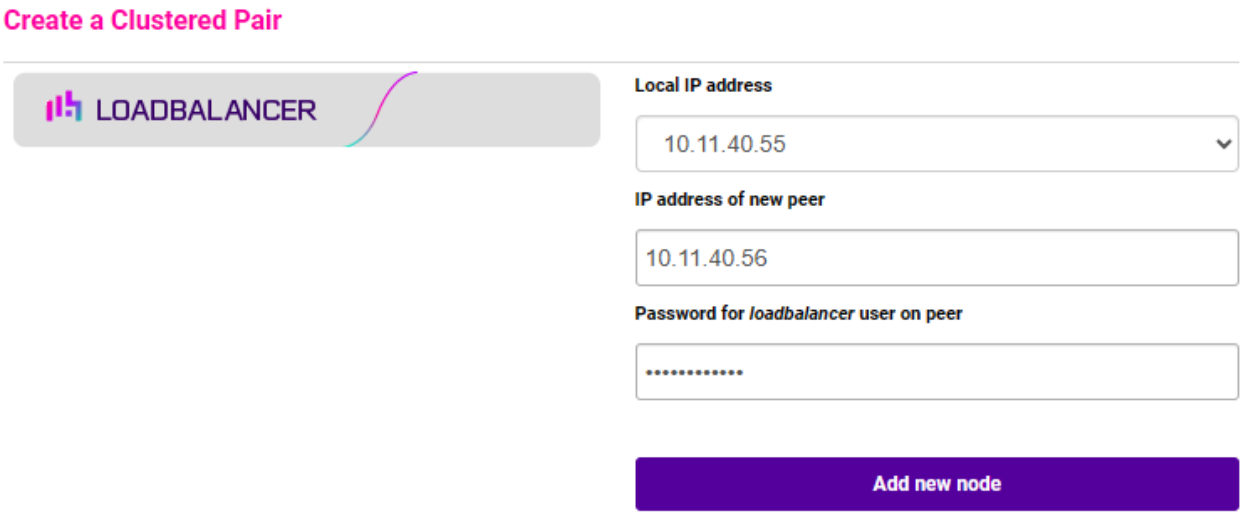
> **Important** Make sure that where any of the above have been configured on the Primary appliance, they're also configured on the Secondary.

16.1.2. Configuring the HA Clustered Pair

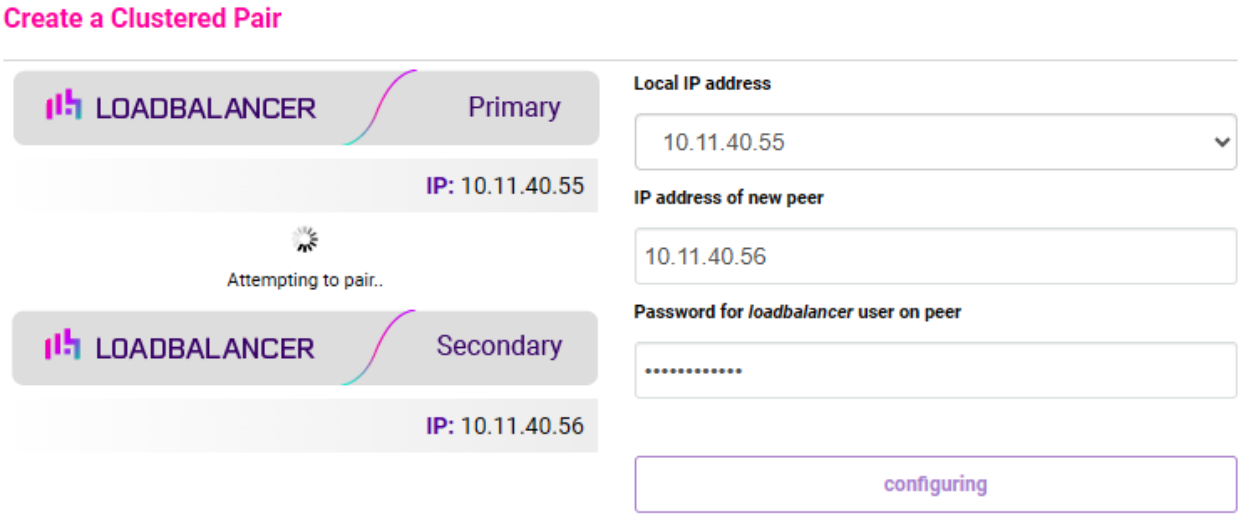
> **Important** During HA pairing, all WebUI users and passwords are synchronized from the Primary to the Secondary. After clustering completes (you will be logged out of the Secondary when this occurs), the Primary's credentials should be used to login to both nodes.

> **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.

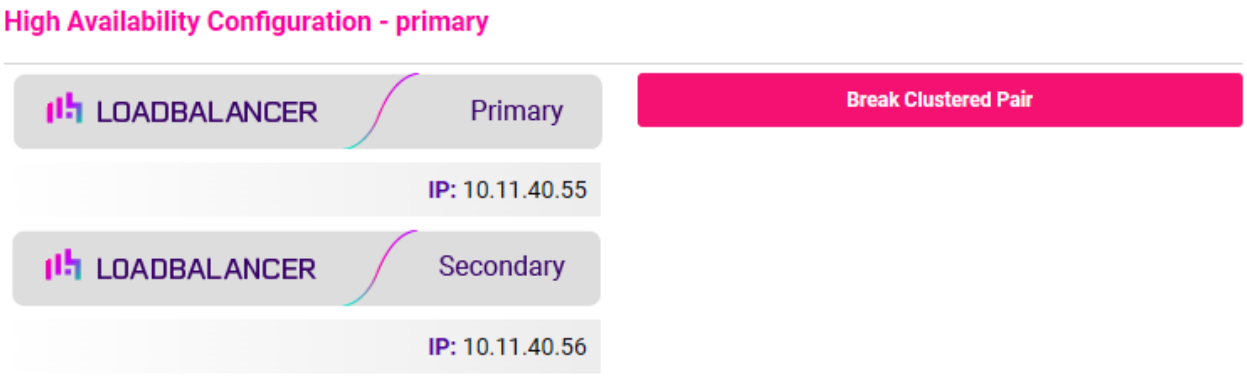
1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: ***Cluster Configuration > High-Availability Configuration***.



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:



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



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.

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

> **Note** For more details on configuring HA with 2 appliances, please refer to Configuring High Availability.

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

17. Document Revision History

Version	Date	Change	Reason for Change	Changed By
1.0.0	30 June 2026	Initial version		ER/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.