Load Balancing Microsoft SQL Server
Version 1.0.0
Table of Contents

1. About this Brief .................................................. 3
2. Loadbalancer.org Appliances Supported ...................... 3
3. Software Versions Supported .................................. 3
    3.1. Loadbalancer.org Appliance .............................. 3
    3.2. Microsoft SQL Server .................................... 3
4. Microsoft SQL Server ........................................... 3
5. Load Balancing Microsoft SQL Server .......................... 3
    5.1. Read / Write Database Access ........................... 3
    5.2. Virtual Service (VIP) Requirements .................... 4
6. Deployment Concept ............................................. 4
7. Load Balancer Deployment Methods ............................ 5
    7.1. Layer 7 SNAT Mode ....................................... 5
8. Loadbalancer.org Appliance – the Basics ....................... 6
    8.1. Virtual Appliance .......................................... 6
    8.2. Initial Network Configuration ............................ 6
    8.3. Accessing the Appliance WebUI .......................... 6
        Main Menu Options ........................................ 8
    8.4. Appliance Software Update ................................ 9
        Determining the Current Software Version .............. 9
        Checking for Updates using Online Update ........... 9
        Using Offline Update .................................... 9
    8.5. Ports Used by the Appliance .............................. 10
    8.6. HA Clustered Pair Configuration ........................ 11
9. Appliance Configuration for Microsoft SQL Server ............. 11
    9.1. VIP1 - MS-SQL-SERVER ................................ 11
        Configuring the Virtual Service (VIP) ................. 11
        Defining the Real Servers (RIPs) ...................... 12
    9.2. Finalizing the Configuration ............................. 12
10. Testing & Verification .......................................... 12
    10.1. Using System Overview ................................ 13
    10.2. Access the Database/Application ....................... 13
11. Technical Support .............................................. 13
12. Further Documentation ......................................... 13
13. Appendix ................................................................ 14
    13.1. Configuring HA - Adding a Secondary Appliance ...... 14
        Non-Replicated Settings ................................... 14
        Configuring the HA Clustered Pair .................... 15
    13.2. SQL Server Health Check ................................ 16
14. Document Revision History .................................... 17
1. About this Brief

This brief outlines the steps required to configure a load balanced Microsoft SQL Server environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Microsoft SQL Server 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 SQL Server. 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

- V8.9.1 and later

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 SQL Server

- 2012 and later

4. Microsoft SQL Server

Microsoft SQL Server is a relational database management system (RDBMS) that supports a wide variety of transaction processing, business intelligence (BI) and data analytics applications in corporate IT environments.

5. Load Balancing Microsoft SQL Server

It’s highly recommended that you have a working Microsoft SQL Server environment first before implementing the load balancer.

5.1. Read / Write Database Access

If all SQL servers have identical copies of the database and only provide read access, load balancing is straightforward and read requests can be directed at any server.
When data is also written to the database, an appropriate synchronisation technology must be used to ensure that all SQL servers are kept in sync following each write operation. Also, depending on the particular synchronisation method, it may be required that write operations are handled by one particular server whilst read operations can be handled by any server.

Various database synchronisation methods are supported, the most appropriate depends on the version of SQL server, the read & write transaction workload, IT infrastructure and the available budget:

- **Replication** - for more information refer to [SQL Server Replication](#)
- **Log shipping** - for more information refer to [About log shipping (SQL Server)](#)
- **Mirroring** - for more information refer to [Database Mirroring (SQL Server)](#)
- **Always On Failover Clustering** - for more information refer to [Always On Failover Cluster Instances (SQL Server)](#)
- **Always On Availability Groups** - for more information refer to [What is an Always On availability group](#)

The configuration presented in this guide assumes that only read operations are supported, or the synchronisation method in use allows read & write operations from/to any SQL server.

### 5.2. Virtual Service (VIP) Requirements

To provide load balancing and HA for Microsoft SQL Server, the following VIP is required:

<table>
<thead>
<tr>
<th>Reference</th>
<th>VIP Name</th>
<th>Mode</th>
<th>Port(s)</th>
<th>Persistence Mode</th>
<th>Health Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP1</td>
<td>MS-SQL-SERVER</td>
<td>L7 SNAT</td>
<td>1433</td>
<td>Source IP</td>
<td>Connect to Port *</td>
</tr>
</tbody>
</table>

**Note**

A more robust SQL Server health check can be used if preferred that reads and verifies data from the database. For more details, please refer to [SQL Server Health Check](#).

### 6. Deployment Concept
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 SQL Server, layer 7 SNAT mode is recommended. This mode is described below and is used for the configurations presented in this guide.

### 7.1. 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.

- Because layer 7 SNAT mode is a full proxy, any server in the cluster can be on any accessible subnet 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, **eth0** is normally used for the internal network and **eth1** is used for the external network although this is not mandatory.

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


   **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 which can be used to configure layer 7 services. Click **Dismiss** if you’re following a guide or want to configure the appliance manually or click **Accept** to start the wizard.

**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 taking 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

To ensure that the appliance(s) are running the latest software version, we recommend a software update check is performed.

Determining the Current Software Version

The software version is displayed at the bottom of the WebUI as shown in the example below:

Checking for Updates using Online Update

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

2. Select Online Update.

3. If the latest version is already installed, a message similar to the following will be displayed:

   Information: Version v8.11.1 is the current release. No updates are available

4. If an update is available, you'll be presented with a list of new features, improvements, bug fixes and security related updates.

5. Click Online Update to start the update process.

   Note: Do not navigate away whilst the update is ongoing, this may cause the update to fail.

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

   Information: Update completed successfully.

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

Using Offline Update

If the load balancer does not have access to the Internet, offline update can be used.
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 support@loadbalancer.org 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: [Choose File] No file chosen
   Checksum: [Choose File] No file chosen
   
   [Upload and Install]

   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:

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

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.

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. Appliance Configuration for Microsoft SQL Server

9.1. VIP1 - MS-SQL-SERVER

Configuring the Virtual Service (VIP)

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

2. Enter the following details:

3. Specify the Label for the virtual service, e.g. MS-SQL-Server.

4. Set the Virtual Service IP Address field to the required IP address, e.g. 192.168.110.100.

5. Set the Ports field to 1433.

6. Set the Layer 7 Protocol to TCP Mode.

7. Click Update to create the Virtual Service.

8. Now click Modify next to the newly created VIP.
9. Scroll to the Persistence section.
   - Ensure that the Persistence Mode is set to Source IP.

10. Scroll to the Health Checks section.
    - For a simple check, leave Health Check set to Connect to Port.
    - For a more robust check, refer to the steps in SQL Server Health Check.

11. Click Update.

**Defining the 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 the following details:

   ![Real Server Configuration](image)

   - Define the Label for the real server as required, e.g. SQL-Server1.
   - Set the Real Server IP Address field to the required IP address, e.g. 192.168.110.160.
   - Set the Real Server Port field to 1433.
   - Click Update.
   - Repeat these steps to add additional Real Servers as required.

**9.2. Finalizing the Configuration**

To apply the new settings, HAProxy must be reloaded. 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.

**10. Testing & Verification**

- **Note**: For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.
10.1. Using System Overview
The System Overview can be viewed in the WebUI. It shows a graphical view of all VIPs & R IPs (i.e. the Microsoft SQL Server servers) and shows the state/health of each server as well as the state of the cluster as a whole. The example below shows that the Virtual Service and all three application servers are healthy and available to accept connections:

10.2. Access the Database/Application
First ensure that any DNS records that are used to access the database are updated so that the FQDN resolves to the MS-SQL-Server VIP. Then verify that you're able to successfully access the database/application.

11. 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.

12. Further Documentation
For additional information, please refer to the Administration Manual.
13. Appendix

13.1. 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.

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:

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

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: \textit{Cluster Configuration > High-Availability Configuration}.

3. Specify the IP address and the \textit{loadbalancer} user's password for the Secondary (peer) appliance as shown in the example above.
4. Click \textit{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 **Appliance Clustering for HA**.

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

13.2. **SQL Server Health Check**

Follow the steps below to configure a more robust health check. This reads and verifies data from a table in the database to verify SQL server health.

1. First, follow these steps to install the SQL Server health check on the load balancer.

2. Next, using the WebUI, navigate to **Cluster Configuration > Health Check Scripts**.

3. Click **Add New Health Check**.

4. Specify a **Name** for the health check, e.g. **SQL-Server**.

5. Ensure **Type** is set to **Virtual Service**.

6. Using the **Template** dropdown, select **ms-sql-check**.

7. Click **Update**.

8. Now click **Modify** next to the **MS-SQL-Server** VIP created earlier.

9. Scroll to the **Health Checks** section and change the **Health Check** to **External Script**.

10. Using the **Check Script** dropdown, select the health check script just created.

11. Click **Update**.

12. To apply the new settings, reload HAProxy using the button in the “Commit changes” box at the top of the screen.
## 14. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>10 April 2024</td>
<td>Initial version</td>
<td></td>
<td>AG, RJC</td>
</tr>
</tbody>
</table>
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.

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