

# LoadMaster HA for Azure

## Installation Guide

UPDATED: 27 July 2023

**© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.**

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# Table of Contents

**1 Introduction** ..... **5**

1.1 Known Issues/Limitations ..... 7

**2 Prerequisites** ..... **9**

**3 Manually Configure LoadMaster HA in Azure** ..... **11**

3.1 Licensing Options ..... 11

3.2 Create the First Virtual LoadMaster in Azure ..... 11

3.3 Create the Second LoadMaster in Azure ..... 17

3.4 Enable a 10 Gb Interface (Optional) ..... 17

3.4.0.1 Add a Single Interface to the LoadMaster ..... 17

3.4.0.2 Add Multiple Interfaces to the LoadMaster ..... 19

**4 Create the Internal Load Balancer (ILB)** ..... **21**

**5 Configure the Azure Load Balancer** ..... **24**

5.1 Create a Back-end Pool ..... 24

5.2 Create Inbound NAT Rules ..... 26

5.3 Create a Probe to Monitor LoadMaster Health ..... 28

5.4 Create Load Balancing Rules to Allow Traffic ..... 30

**6 Network Security Groups** ..... **33**

**7 Configure the LoadMasters** ..... **34**

**8 Configure GEO Clusters with HA** ..... **37**

8.1 Configure the Master IP Address for one HA Pair ..... 37

8.2 Configure Clusters of HA IP Addresses Between Two HA Pairs ..... 37



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

8.3 Configuring Clusters of HA IP Addresses Between a HA Pair and a Standalone System ..... 39

8.4 Configure Clusters of HA IP Addresses Between Two HA Pairs and Two Standalone LoadMasters ..... 40

**9 LoadMaster Firmware Upgrades/Downgrades ..... 43**

9.1 Upgrade the LoadMaster Firmware ..... 43

9.2 Downgrade the LoadMaster Firmware ..... 43

**10 Troubleshooting ..... 45**

10.1 Check which LoadMaster is Active ..... 45

10.2 First/Second Unconnected ..... 45

10.3 Connection to Default Gateway Failed ..... 46

10.4 Virtual Machine Inaccessible ..... 46

10.5 Run a TCP Dump ..... 46

10.6 Sync Problems ..... 47

10.7 Misconfigured ILB ..... 47

10.8 Problems Reaching a Virtual Service ..... 48

**References ..... 49**

**Last Updated Date ..... 50**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 1 Introduction

When deploying an application using the Microsoft Azure Infrastructure as a Service (IaaS) offering, you usually need to provide load balancing and other application delivery functions such as content switching, SSL Termination and IPS. Some of this functionality may also be necessary when deploying applications in Microsoft Azure Platform as a Service (PaaS). Kemp's LoadMaster for Azure enables you to address your needs of application delivery and High Availability (HA).

Deploying a single LoadMaster for Azure does not provide you with the high availability you need for your applications. When deploying a pair of LoadMasters in Azure, you can achieve high availability for your application. This document provides the details for a HA Kemp LoadMaster solution.

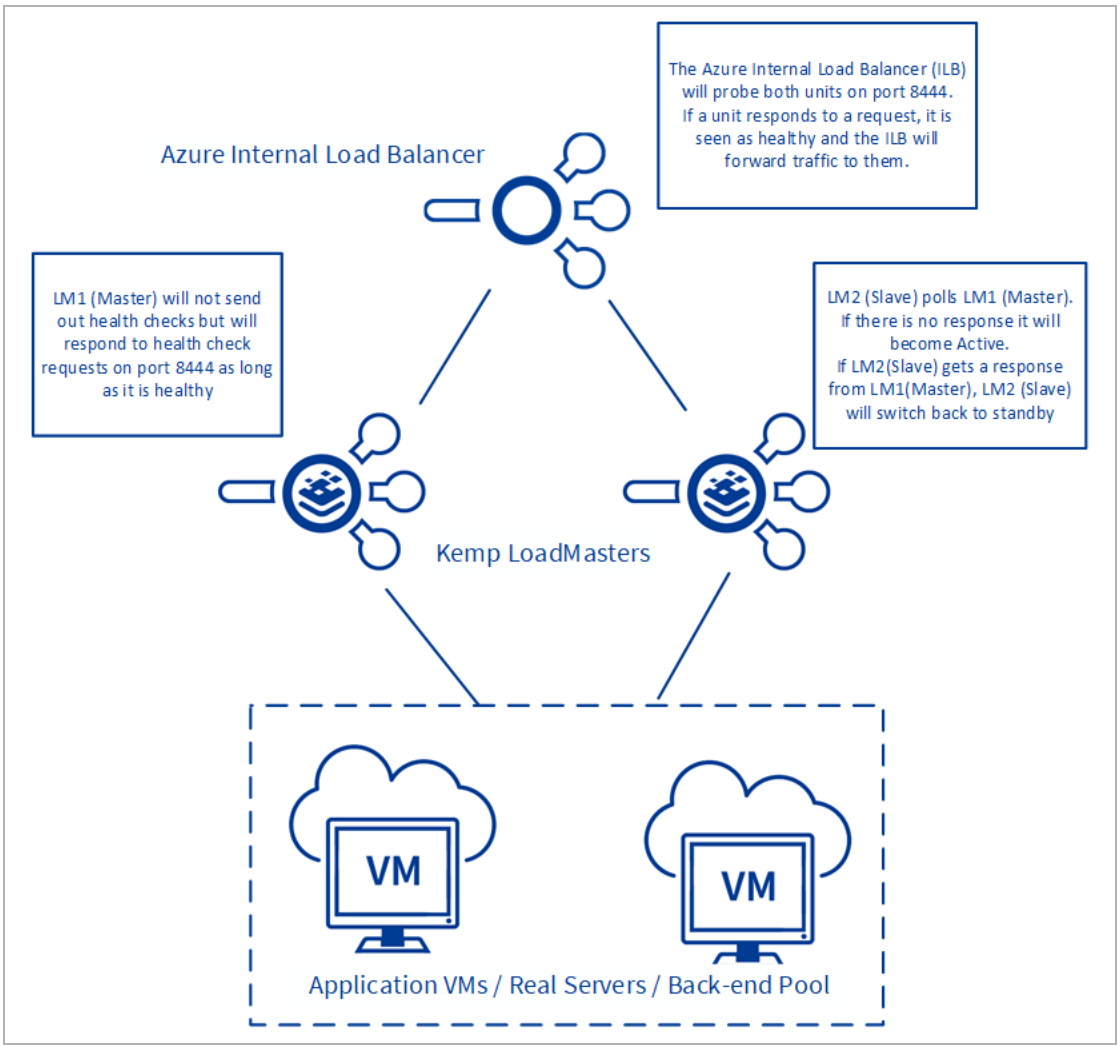
When using LoadMaster in High Availability on Azure, HA operates in much the same way as it does on non-cloud platforms, but with some key differences, which are listed below:

- LoadMaster HA for Azure involves two LoadMasters that synchronize settings bi-directionally. Changes made to the active unit are replicated to the standby unit and changes made to the standby unit are replicated to the active unit.
- The replication (synchronization) of settings (from active to standby) is not instant in all cases and may take a few moments to complete.
- When synchronizing the GEO settings from active to standby, any Fully Qualified Domain Name (FQDN) or cluster IP addresses that match the active unit IP address are replaced with the standby unit IP address. Likewise, when synchronizing from standby to active, the standby unit IP address is replaced with the active unit IP address.
- All user-defined settings are synchronized, with the exception of the following:
    - Default gateway (both IPv4 and IPv6)
    - IP addresses and netmasks
    - Hostname
    - Name server
    - Domain
    - Admin default gateway
    - Administrative certificate settings (.cert, .pem and .setadmin files)


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

    - Network interface settings: Link Status (Speed and Duplex), MTU and additional addresses
    - Virtual LAN (VLAN) configuration
    - Virtual Extensible LAN (VXLAN) configuration
    - Additional routes
- The cloud HA LoadMaster does not have a "force update" option.
- By default, the active unit is always set as active and the standby unit can be standby or active if the active unit fails. The active unit is active and never becomes the standby, even if it fails. Similarly the standby unit never becomes the active unit. When the active unit comes back up it is set as active and connections are automatically directed to the active again. Either the active or standby unit can be active or standby.
- The **HA Check Port** must be set to the same port on both the active and standby units for HA to work correctly.
- Depending on the design of the Network Security Groups, you must ensure the necessary ports are open inbound to allow for the traffic.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.




A complete description of non-cloud LoadMaster HA can be found in the High Availability (HA), Feature Description document.

For details on all of the supported configurations regarding multiple Public IP addresses along with multiple interfaces, refer to the following Knowledge Base article: Supported Network Configurations for LoadMaster in Azure.

## 1.1 Known Issues/Limitations

There are some known issues/limitations to be aware of:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- Transparency is not possible in HA setups in Azure environments. For more information and requirements, refer to the **Transparency Feature Description** document on the Kemp Documentation page.
- Do not downgrade from firmware version 7.2.36 or higher to a version below 7.2.36. If you do this, the LoadMaster becomes inaccessible and you cannot recover it.
- The Virtual Service IP address must be the same IP address as the network interface.
- Alternate default gateway support is not permitted in a cloud environment.
- When setting up the LoadMaster in Azure, ensure that the **Enable OS guest diagnostics** check box is disabled because there is no support available for collection of diagnostics from the LoadMaster in Azure. If this option is enabled, the LoadMaster will not boot correctly.

The table below summarizes some of the limitations in Azure:

| | Single unit, one-armed | Single unit, two-armed | HA pair one-armed | HA pair two-armed |
|---|---|---|---|---|
| **Access Control List (ACL)** | Requires that Server NAT is disabled | Requires that Server NAT is disabled | Requires that Server NAT is disabled | Requires that Server NAT is disabled |
| **Transparency** | Does not work | Works | Does not work | Does not work |
| **10Gb NICs** | 7.2.48 and above | 7.2.48 and above | 7.2.48 and above | 7.2.48 and above |
| **Additional addresses** | Works | Works | Does not work | Does not work |
| **Virtual Service not on eth0** | Not applicable | Works | Not applicable | Does not work |

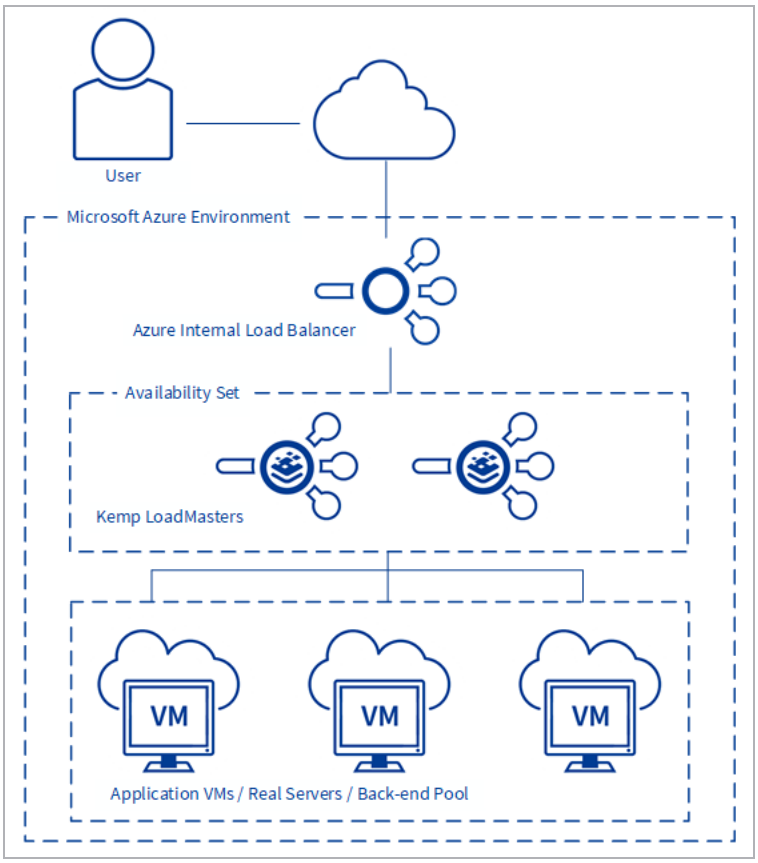

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 2 Prerequisites

The following prerequisites must be met before proceeding to a high availability configuration:

- An Azure Resource Manager (ARM) (V2) Virtual Network added to Azure to place the LoadMaster VMs
- Application VMs deployed in Azure in the Virtual Network
- An Azure Internal Load Balancer deployed to create the high availability pair
- Two LoadMaster VMs deployed in ARM on the same Virtual Network as the Application VMs
    - Both LoadMasters should be configured to be part of an availability set

The following diagram provides overview of the configuration described above:




To configure high availability using the LoadMaster, the following configuration must be in place:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

- Application VMs are installed and configured
- LoadMaster for Azure VMs are installed and configured
- **Important:** The **HA Check Port** must be set to the same port on both the active and standby units for HA to work correctly. The same port must be configured as the probe port on the Internal Load Balancer.
- The following management Load Balanced NAT Rules may be needed to access the LoadMasters:

  - TCP Port 22 for SSH access

  - TCP Port 8443 for Management Web User Interface (WUI) access

  - Additional Load Balanced Rules for any traffic that is being transmitted through the LoadMaster

> If using Kemp 360 Central, you must configure special NAT rules.

Use this table to record the necessary information required to create the LoadMaster Pair in Azure:

| Fields Required for creation of LoadMaster Pair | |
|---|---|
| Primary LoadMaster Name | |
| Secondary LoadMaster Name | |
| Pricing Tier | |
| Password for LoadMasters | |
| Availability Service Name | |
| Resource Group Name | |
| Virtual Network | |
| Internal Load Balancer Name | |
| Internal Load Balancer Public IP Address (PIP), if required | |

> It is not possible to bond interfaces on Azure LoadMasters.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 3 Manually Configure LoadMaster HA in Azure

> The steps in this section were correct at the time of writing. However, the Azure interface changes regularly so please refer to Azure documentation for up-to-date steps if needed.

Please complete the prerequisites documented in the earlier section.

## 3.1 Licensing Options

There are four main licensing options when deploying a LoadMaster for Azure:

- Hourly consumption
- Bring Your Own License (BYOL)
- Free version
- License Agreement - Service Provided License Agreement (SPLA)/Metered

To use the BYOL option, follow the steps below:

1. Download the **BYOL – Trial and perpetual license** version of the Virtual LoadMaster (follow the steps in the section below to do this).
2. Contact a Kemp representative to get a license.
3. Update the license on your LoadMaster to apply the license change (**System Configuration > System Administration > License management**).
4. Kemp recommends rebooting the LoadMaster after updating the license.

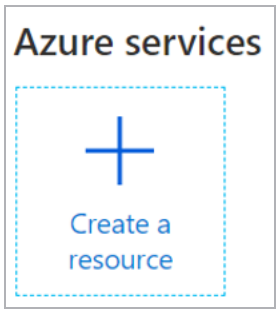
For more information on MELA and SPLA, refer to the relevant Feature Description on the Kemp documentation page.

## 3.2 Create the First Virtual LoadMaster in Azure

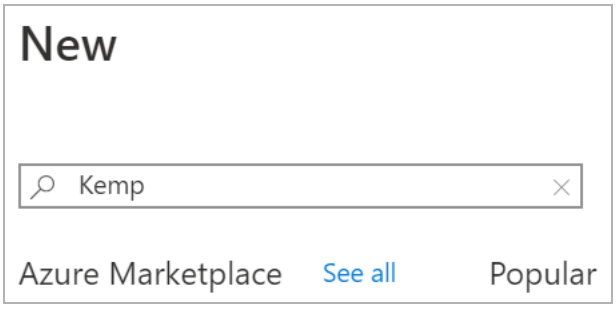
The steps in this document reflect the steps in the Azure Marketplace (http://portal.azure.com).

To deploy a new LoadMaster using ARM, follow the steps below::

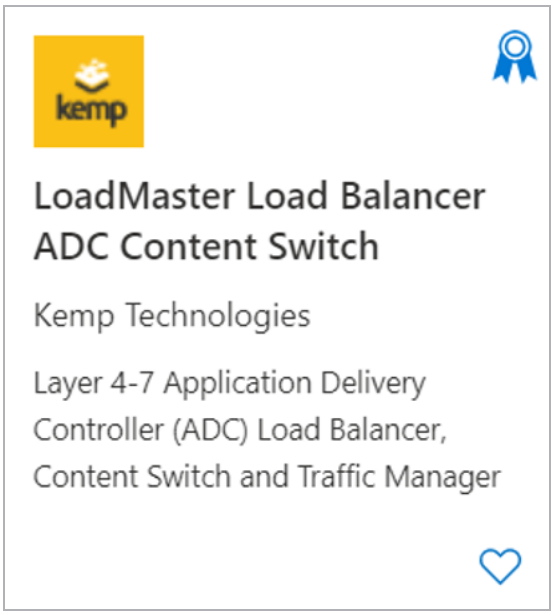

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.




1. From the Azure Management Portal dashboard, click **Create a resource**.



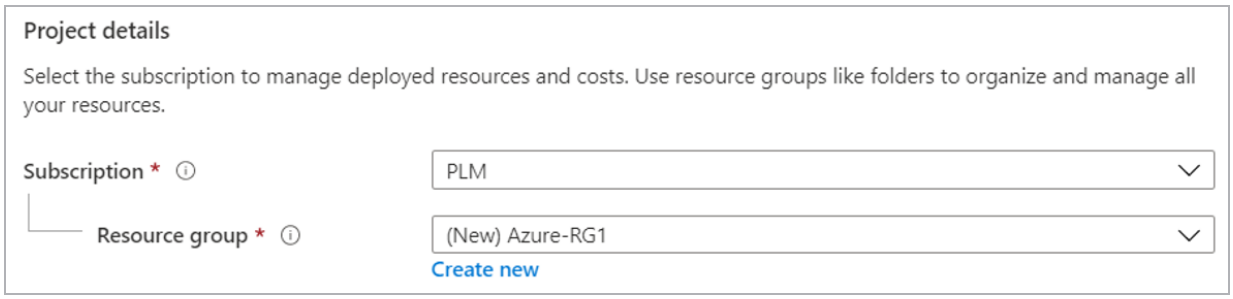

2. Enter **Kemp** in the search bar and press Enter on your keyboard.




3. Select **LoadMaster Load Balancer ADC Content Switch**.

4. From the drop-down menu, select the desired LoadMaster type and click **Create**.

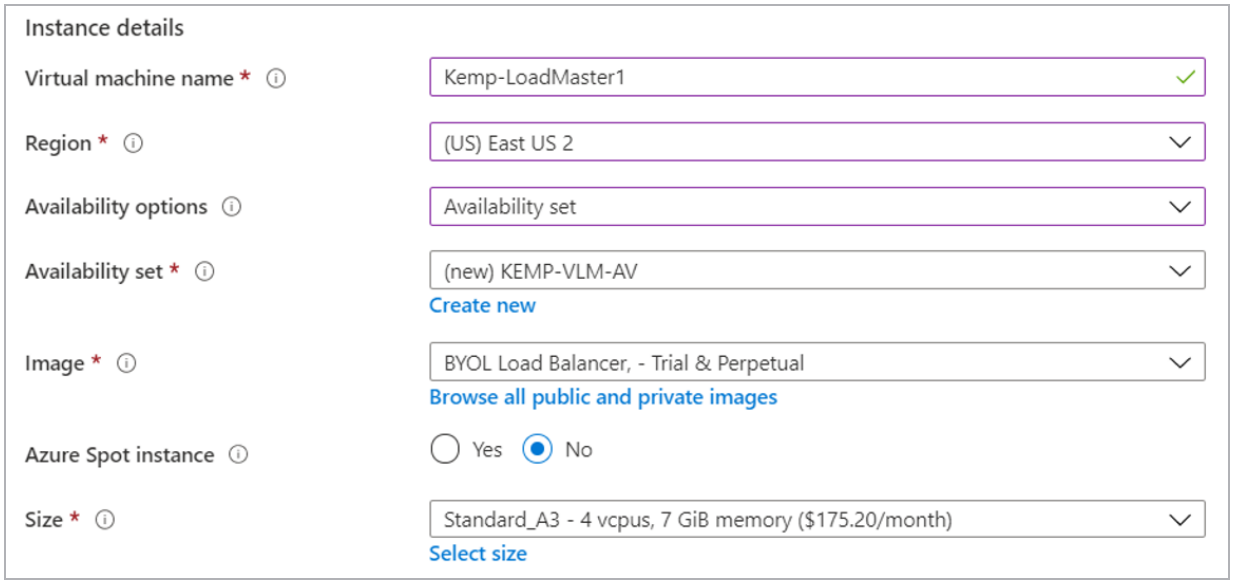

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.




5. Under **Project details**, complete the following fields:

   a) Select the Azure **Subscription**.

   b) Select an existing or create a new **Resource group** to deploy the LoadMaster into.




6. Under **Instance details**, complete the following fields:

   a) Enter a **Virtual machine name** for the LoadMaster.

   b) Select an Azure **Region**.

   c) Select **Availability set** under **Availability options**.

   d) Select an existing or new **Availability set** for the HA pair.

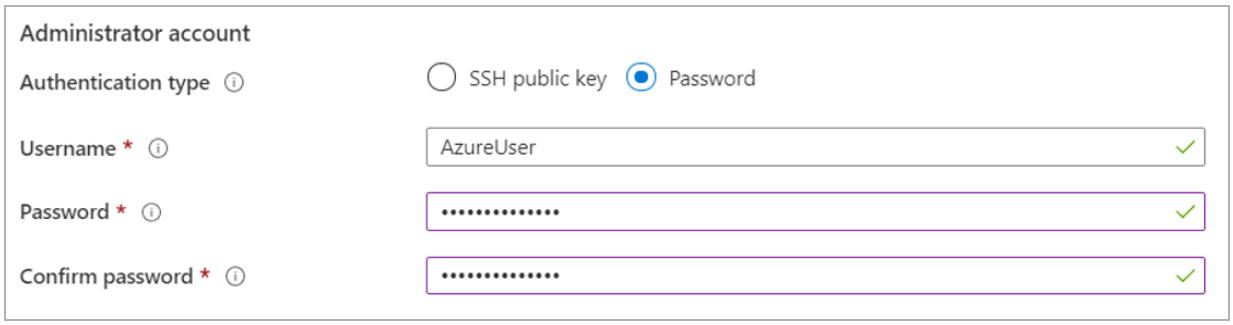
   e) Confirm the desired LoadMaster type is selected in the **Image** drop-down list.

   f) Enable or disable **Azure Spot instance**.

   g) Select the desired **Size** for the virtual machine.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> If you want to enable 10 Gb throughput for a LoadMaster virtual machine (VM) in Azure, you must select an Azure VM instance type that supports the 10 Gb Mellanox driver. For more information, refer to the **Enable a 10 Gb Interface (Optional)** section.




7. Under **Administrator account**, complete the following fields:

   a) Select the **Authentication type** (**SSH public key** or **Password**).

   > Kemp recommends using a password, but either way will work fine.

   b) Enter a **Username**.

   > This username is not used by the LoadMaster for Azure. The default username to access the LoadMaster is **bal**.

   c) Enter a **Password** for the **bal** account and confirm it.

   > The password is used to access the LoadMaster WUI.

   d) **SSH public key source:** You can either create a new key pair, use an existing key stored in Azure, or use an existing public key.

   > It is recommended to store SSH keys in a secure location.



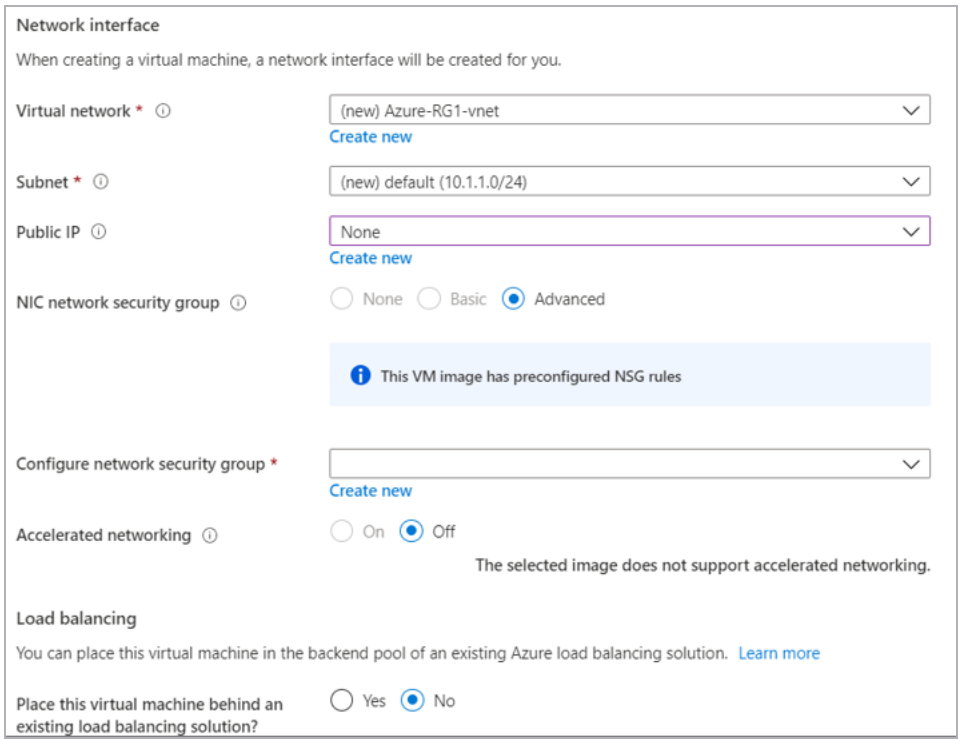

8. Click **Next: Disks**.

9. Leave the default options for **Disk options** and **Data disks**.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.




10. Click **Next: Networking**.




11. Under **Network interface**, complete the following fields:

    a) Select an existing or create a new **Virtual network**.

    b) Select an existing or create a new **Subnet**.

    c) (Optional) A **Public IP** is not required to do the access provided using the Azure Load Balancer outlined later in this guide.

    d) Keep the default setting for **NIC network security** group.

    > The security group should contain rules for port 8443 (management), 22 (SSH), and any other ports that are needed by the back-end. Do not block port 6973.

    e) If the VM size selected supports **Accelerated networking**, select **On**.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

f) (Optional) Select an existing load balancer or follow the steps outlined later in this document to create one.




12. Click **Next: Management**.

13. You can optionally make any necessary updates to the **Monitoring**, **Identity**, and **Auto-Shutdown** sections or leave them as the default settings.

> Ensure that the **Enable OS guest diagnostics** check box is disabled because there is no support available for collection of diagnostics from the LoadMaster in Azure. If this option is enabled, the LoadMaster will not boot correctly.




14. Click **Next: Advanced**.

15. You can optionally make any necessary updates to the **Extensions** and **Custom data** sections or leave them as their defaults.




16. Click **Next: Tags**.

17. You can optionally make any necessary changes to the **Tags** section or leave the defaults.




18. Click **Next: Review + create**.

19. You can optionally click **Download a template for automation** to download an ARM template.




20. Click **Create**.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> If you chose to create a new SSH key pair, you are now prompted to store the private key for the public key you created. Azure does not store the private key. After the SSH key is created, you will not be able to download the private key.

## 3.3 Create the Second LoadMaster in Azure

The process of setting up the second LoadMaster for Azure is similar to the first with a few exceptions, which are listed below:

- You must select the same **Resource Group** that was used during the first LoadMaster deployment.
- You must select the same **Virtual Network** that was used during the first LoadMaster deployment.
- You must select the same **Availability Set** that was created during the first LoadMaster deployment.

# 3.4 Enable a 10 Gb Interface (Optional)

Follow one of the two procedures below depending on whether you are adding a single network interface or multiple network interfaces to the LoadMaster.

To enable 10 Gb throughput for a LoadMaster virtual machine (VM) in Azure, you must select an Azure VM instance type that supports the 10 Gb Mellanox driver. Accelerated Networking is supported on most general purpose and compute-optimized instance sizes with two or more vCPUs. These supported series are: D/DSv2 and F/Fs. On instances that support hyperthreading, Accelerated Networking is supported on VM instances with four or more vCPUs. Supported series are: D/Dsv3, E/Esv3, Fsv2, Lsv2, Ms/Mms and Ms/Mmsv2. Refer to the Sizes for Linux virtual machines in Azure page for further details.

#### 3.4.0.1 Add a Single Interface to the LoadMaster

To enable 10 Gb interfaces on the LoadMaster, perform the following steps:

1. Deploy the LoadMaster.

> For the purposes of this document, the Standard DSv2 machine size is used.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

> When you instantiate a 10 Gb interface, it appears as two interfaces in the LoadMaster Web User Interface (WUI). The two interfaces are related and have the same MAC address. Only the first interface has an IP address. If you want to modify the interface, you must do this on the interface that has the IP address listed.

2. License the LoadMaster.

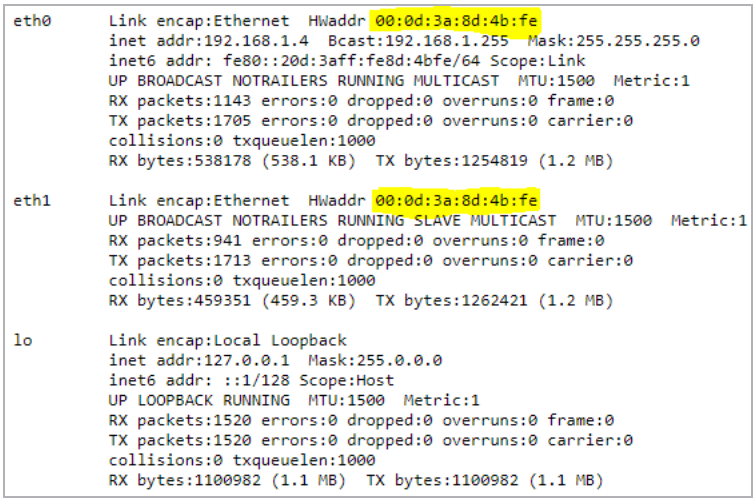
3. Verify that the Mellanox driver has instantiated correctly by performing the following steps:

a) If the LoadMaster was deployed with a single interface, two interfaces are displayed under **System Configuration > Interfaces** on the LoadMaster WUI. If only one interface is displayed this means that the Mellanox driver has not instantiated.

b) To instantiate the Mellanox driver, you must shut down the LoadMaster. Navigate to: **System Configuration > System Administration > System Reboot** and click **Shutdown**. You must also stop the LoadMaster from the Azure WUI by clicking **Stop**.

c) To start the LoadMaster on the Azure WUI, click **Start**.

d) When the LoadMaster boots up, navigate to: **System Configuration > Interfaces** on the LoadMaster WUI and verify that two interfaces (**eth0** and **eth1**) are displayed under **System Configuration > Interfaces**.




e) You can also verify that two interfaces are active by checking performing an Ifconfig. To perform an Ifconfig, navigate to **System Configuration > Troubleshooting**. On the


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

**Troubleshooting** screen, click **Ifconfig**. This displays two interfaces with the same hardware address.

#### 3.4.0.2 Add Multiple Interfaces to the LoadMaster

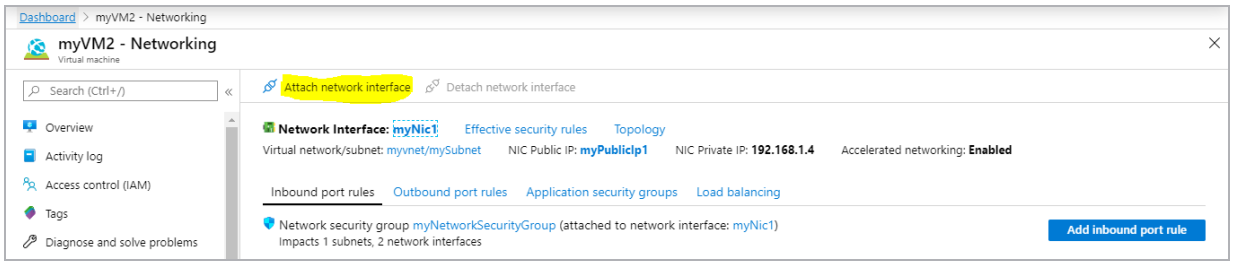
The Azure WUI does not allow interfaces with accelerated networking to be added. You must add the interface by using the Azure command line interface (CLI) or by using PowerShell.

> You must run the command with the LoadMaster in a powered off state.

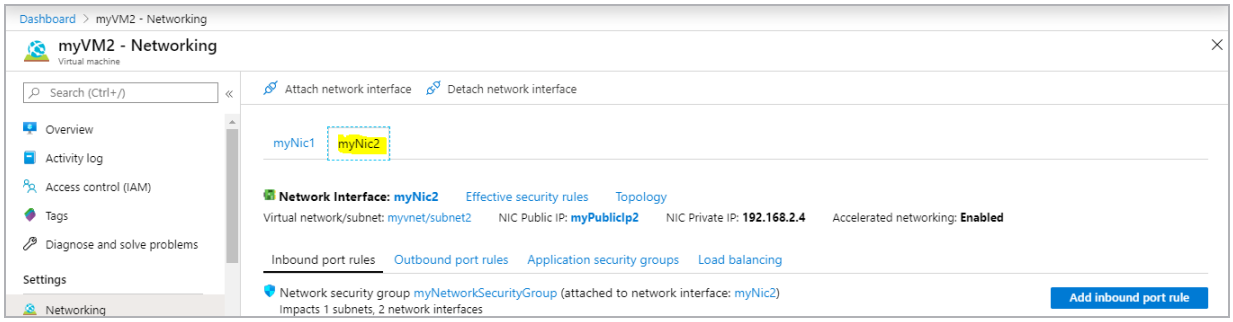
1. Create the interface using the Azure CLI similarly to the example below:

```
PS C:\Users\test> az network nic create --resource-group testdoc --name myNic2 --vnet-name myVnet --subnet subnet2 --accelerated-networking true --public-ip-address myPublicIp2 --network-security-group myNetworkSecurityGroup --location eastus
```

2. When the interface is created, you can add this interface to the LoadMaster when it is in a powered off state. Navigate to the **Networking** tab of the LoadMaster on the Azure WUI.




3. Click **Attach network interface**.



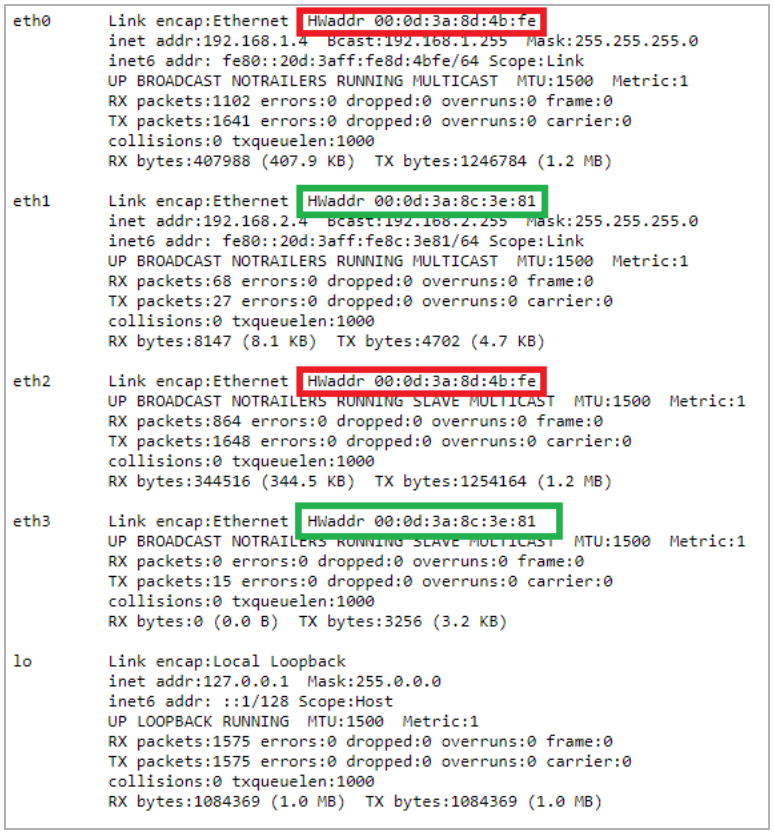

4. When the attachment is complete, both interfaces appear on the Azure WUI.

5. Restart the LoadMaster.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

6. Verify that the interfaces are displayed under **System Configuration > Interfaces** on the LoadMaster WUI. The LoadMaster WUI should now display four interfaces.

You can also verify that four interfaces are active by checking performing an Ifconfig. To perform an Ifconfig, navigate to **System Configuration > Troubleshooting**. On the **Troubleshooting** screen, click **Ifconfig**.




Unlike the single interface case where **eth0** and **eth1** are related, for multiple interfaces, **eth0** and **eth2** and **eth1** and **eth3** are related (with the same MAC address). **eth0** and **eth1** have the IP addresses, the other interfaces without the IP addresses are related by the **HWaddr** (the MAC address).


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

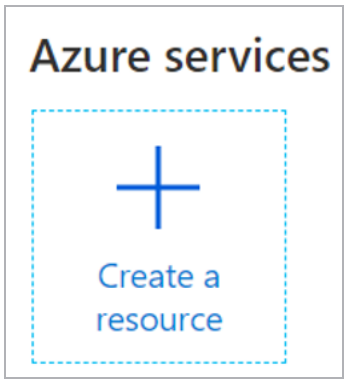
# 4 Create the Internal Load Balancer (ILB)

An Azure Internal Load Balancer must be deployed to monitor the health of the LoadMasters and direct traffic accordingly.

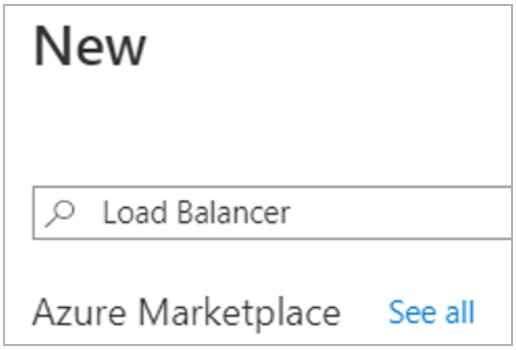
The following procedure describes how to set up an Azure Load Balancer from the Microsoft Azure portal:

> The steps in this document reflect the steps in the Azure Marketplace (http://portal.azure.com).

To deploy a new load balancer using ARM, follow the steps below:

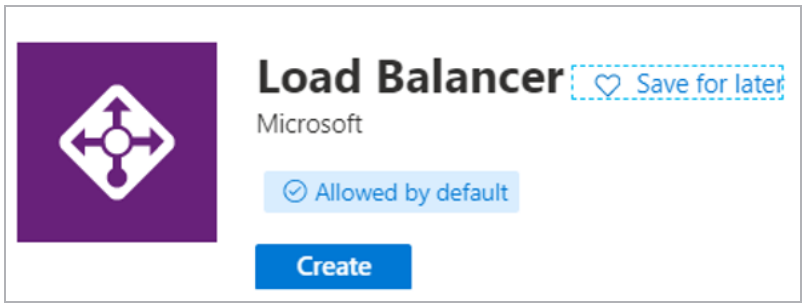



1. From the Azure Management Portal dashboard, click **Create a resource**.

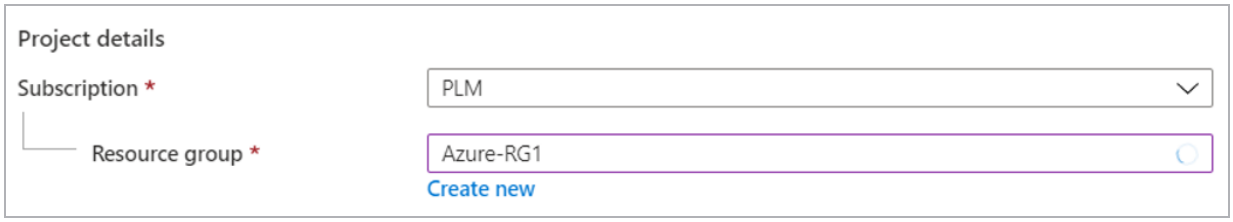



2. Enter **Load Balancer** in the search bar and press Enter on your keyboard.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



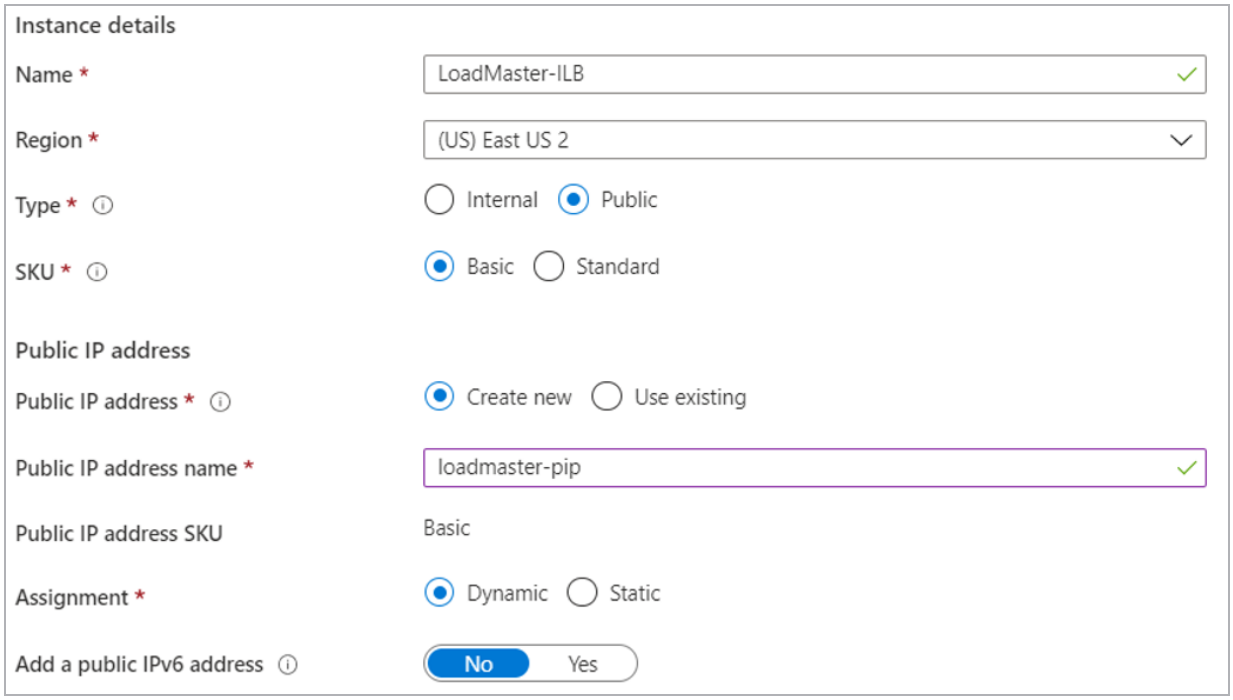

3. Click **Create**.




4. Under **Project details**, complete the following fields:

   a) Select the Azure **Subscription**.

   b) Select the existing **Resource Group** used to deploy the LoadMasters.




5. Under **Instance details**, complete the following fields:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

a) Enter a **Name** for the load balancer.

b) Select the Azure **Region** used to deploy the LoadMasters.

c) Select the **Type** of load balancer determined by **Public** access or **Internal** only.

d) Select the load balancer **SKU**.

e) If creating a public load balancer, provide a new or use an existing **Public IP address**.

f) Enter a **Public IP address name**.

g) Select either **Dynamic** or provide a **Static** IP **Assignment**.

h) Select whether or not to **Add a public IPv6 address**.




6. Click **Next: Tags**.

7. You can optionally make any necessary changes to the **Tags** section or leave the defaults.




8. You can optionally click **Download a template for automation** to download an ARM template.




9. Click **Create**.

It may take some time for the ILB to propagate.

If you chose to use a Public IP (PIP) address the front end IP configuration is created automatically.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 5 Configure the Azure Load Balancer

There are several settings that need to be configured to provide the high availability of the LoadMasters:

- Create a back-end address pool and add the LoadMasters to the pool.
- Create Inbound NAT rules to direct traffic to the appropriate LoadMaster.
- Create a Probe to monitor the health of the LoadMasters.
- Create Load Balancing Rules to allow the necessary traffic.

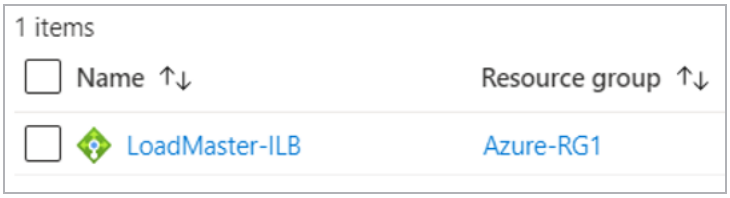
Refer to the sections below for further information on each of these.

## 5.1 Create a Back-end Pool

The Backend Pool is a collection of virtual machines (LoadMasters) which is load balanced to provide High Availability.



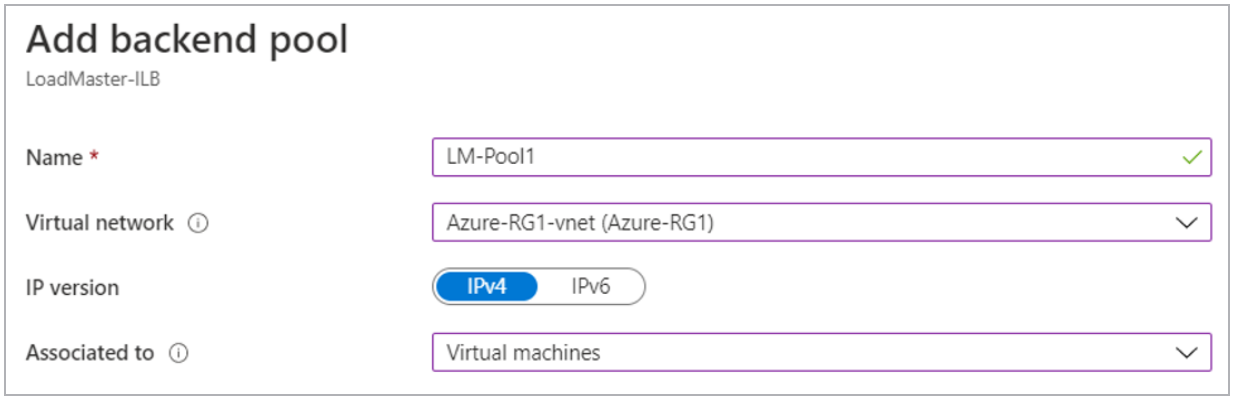

1. In the search bar, search for **Load Balancer** and press Enter on your keyboard.




2. Select the load balancer that was created in a previous section.
3. Click **Backend pools**.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

4. Click **Add**.



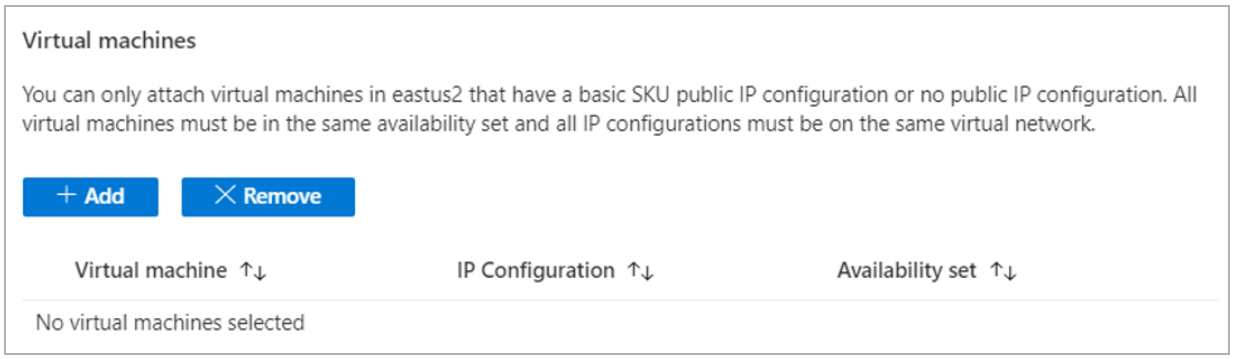

5. Provide the following:

   a) Enter a **Name** for the back-end pool.

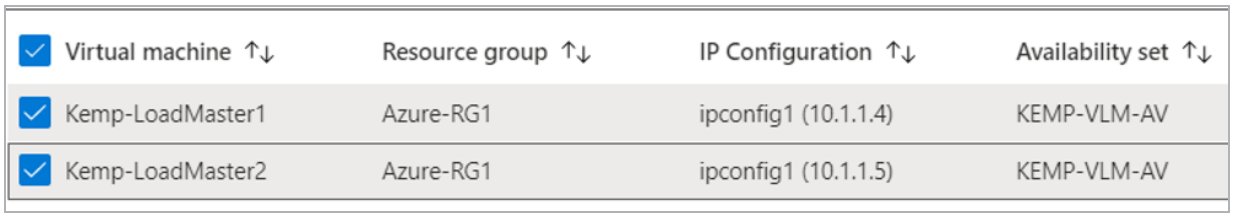
   b) Select the **Virtual network** used for the LoadMasters.

   c) Select either **IPv4** or **IPv6** as the **IP version**.

   d) Select **Virtual machines** in the **Associated to** drop-down list.



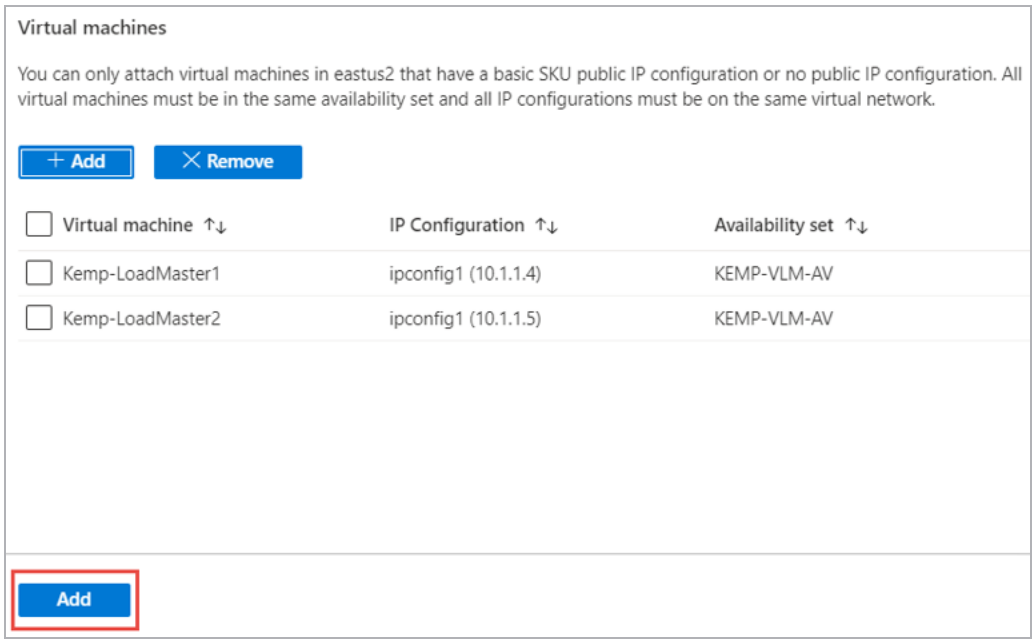

6. Under **Virtual machines**, click **Add**.



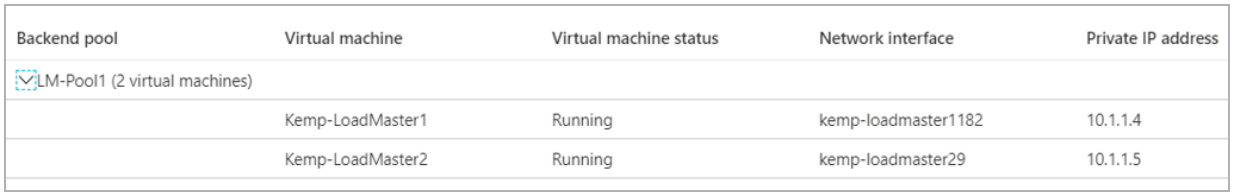

7. Select the LoadMasters for the HA pair.

8. Click **Add**.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.




9. Click **Add** to create the back-end pool.



| Backend pool | Virtual machine | Virtual machine status | Network interface | Private IP address |
|---|---|---|---|---|
| LM-Pool1 (2 virtual machines) | | | | |
| | Kemp-LoadMaster1 | Running | kemp-loadmaster1182 | 10.1.1.4 |
| | Kemp-LoadMaster2 | Running | kemp-loadmaster29 | 10.1.1.5 |

When finished, you can see the two machines in the back-end pool.

## 5.2 Create Inbound NAT Rules

On Azure cloud, the ILB is used to create the Shared IP address (SIP) and to probe and route traffic to the LoadMaster instances. To allow 'public' access to the WUI of each LoadMaster, Kemp recommends creating ILB NAT rules:

- <*SIP*>:8441 maps to Node-1 port 8443
- <*SIP*>:8442 maps to Node-2 port 8443

> If using the HA pair awareness functionality in Kemp 360 Central, you must be able to probe the shared IP address on the WUI port (for example, <*SIP*>:8443). This requires an ILB inbound rule for 8443 to allow access to the back-end pool.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

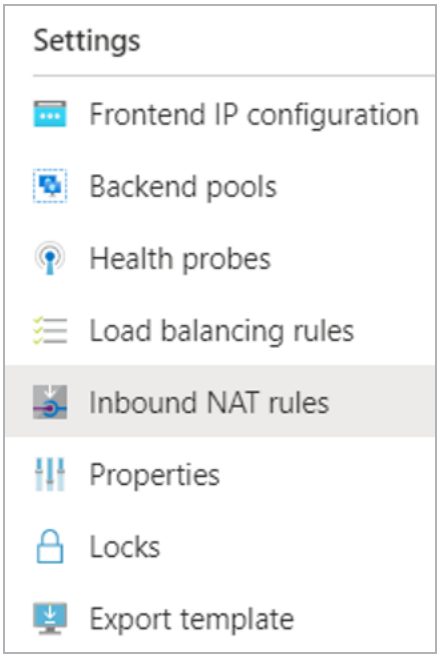
> However, the ILB does not allow a port used in a NAT rule to also be used in an inbound rule. Therefore, if you want to use the HA pair awareness in Kemp 360 Central, you must create a different set of NAT rules.

Inbound NAT rules provide a translation for management access into each of the LoadMasters in the back-end pool. Each LoadMaster does not require a Public IP Address (PIP). A unique port must be configured in an Inbound NAT rule for each LoadMaster. The example rules are the following:

| Target | Port | Target Port |
|---|---|---|
| LoadMaster1 - WUI | 8441 | 8443 |
| LoadMaster1 – SSH | 221 | 22 |
| LoadMaster2 – WUI | 8442 | 8443 |
| LoadMaster2 – SSH | 222 | 22 |

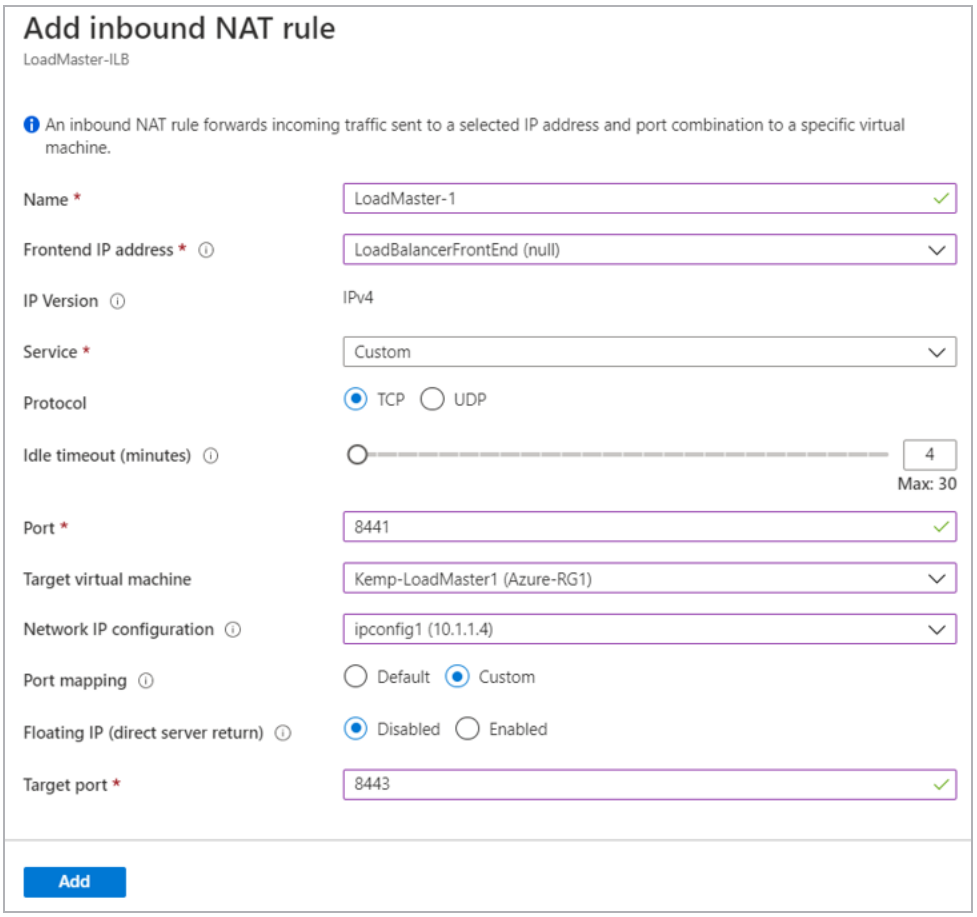
The LoadMaster uses port 22 and 8443 by default. The remaining port numbers listed above are recommended, but you can use other port numbers if needed.

To create the inbound NAT rules, follow the steps below:




1. Select **Inbound NAT rules** in the load balancer navigation.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.




2. Create four inbound NAT rules based on the table provided earlier in this section.

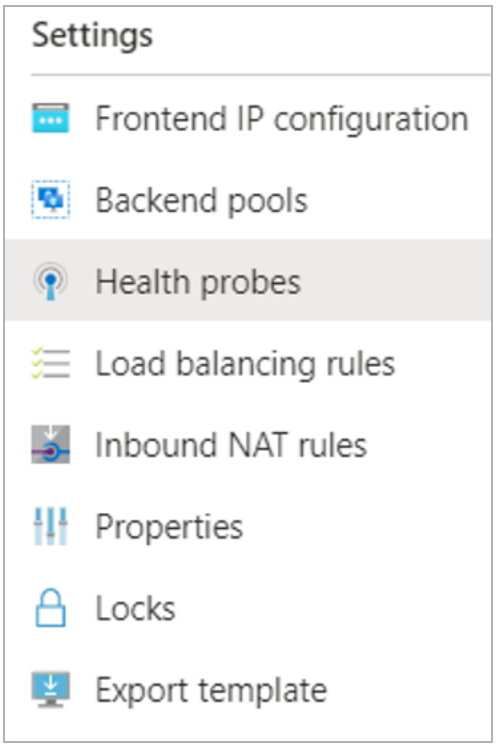
| | | | | |
|---|---|---|---|---|
| LoadMaster-1 | IPv4 | - | Kemp-LoadMaster1 | Custom (TCP/8441) |
| LoadMaster-2 | IPv4 | - | Kemp-LoadMaster2 | Custom (TCP/8442) |
| LoadMaster-1-SSH | IPv4 | - | Kemp-LoadMaster1 | Custom (TCP/221) |
| LoadMaster-2-SSH | IPv4 | - | Kemp-LoadMaster2 | Custom (TCP/222) |

When finished, you can see the four inbound NAT rules.

## 5.3 Create a Probe to Monitor LoadMaster Health

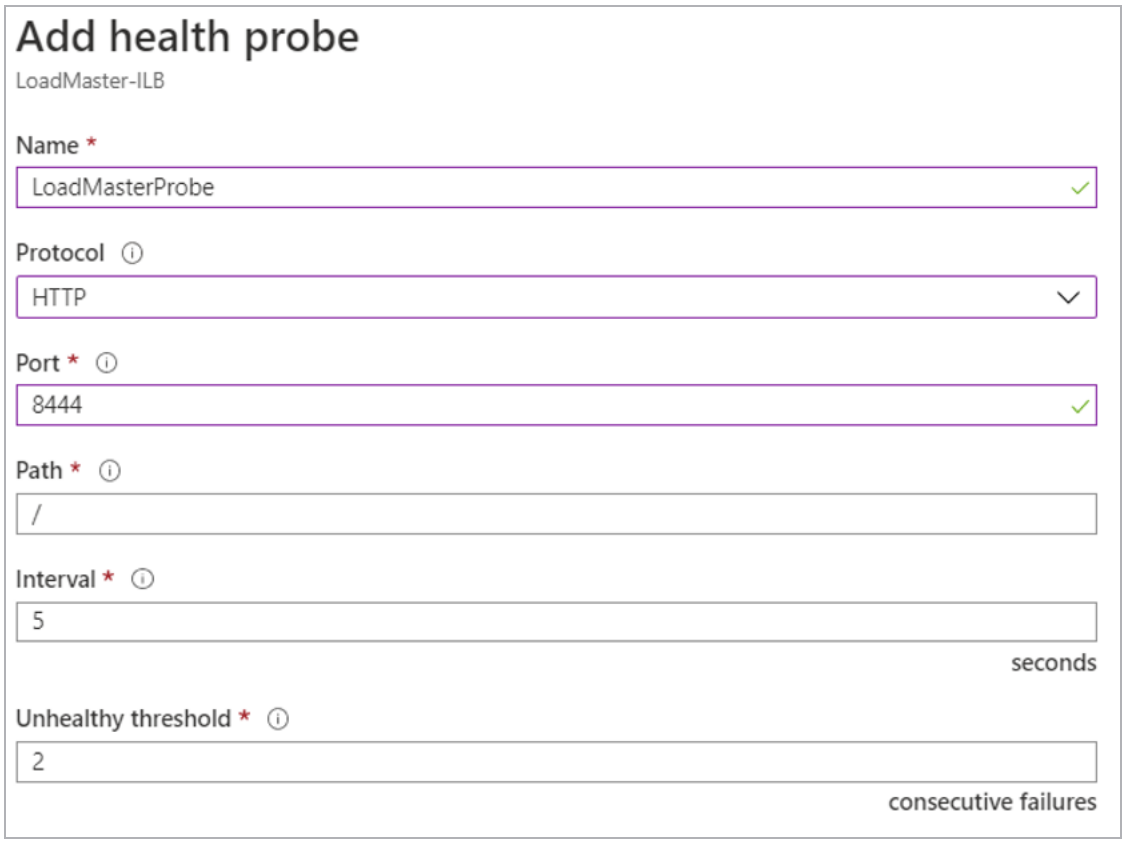
A probe must be created to monitor the health of the LoadMasters. This probe determines which LoadMaster is active and sends the necessary traffic. Should that LoadMaster go offline, the probe takes that LoadMaster out of service and directs all traffic to the secondary LoadMaster.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.




1. Select **Health probes** in the load balancer navigation.
2. Click **Add**.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.




3. Provide the following information:

   a) Provide a **Name**.

   b) Select **HTTP** as the **Protocol**.

   c) Enter **8444** as the **Port**.

   d) Enter **/** as the **Path**.

   e) Enter **5** as the **Interval**.

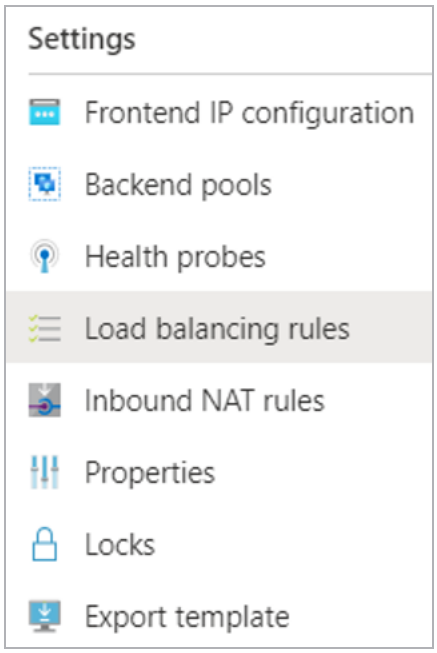
   f) Enter **2** as the **Unhealthy threshold**.

4. Click **OK**.

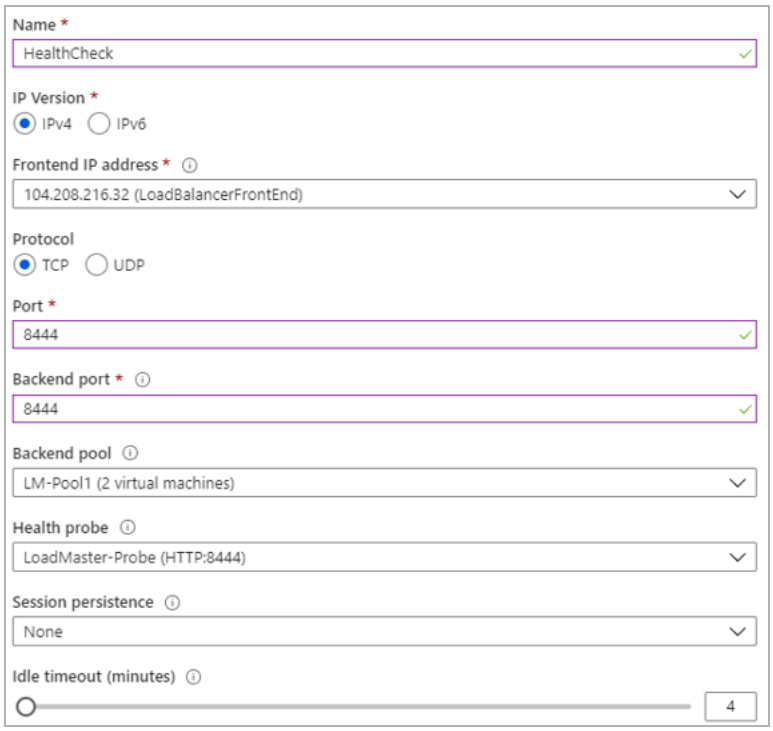
## 5.4 Create Load Balancing Rules to Allow Traffic

Load Balancing Rules must be configured for any traffic that is published through the LoadMaster. A Rule is set up for Port 8444 which can be used to check the state of the LoadMasters within the Backend Pool.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.




1. Select **Load balancing rules** in the load balancer navigation.
2. Click **Add**.




3. Provide the following information:


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

a) Provide a **Name**.

b) Select the **IP Version**.

c) Select **TCP** as the **Protocol**.

d) Enter **8444** as the **Port**.

e) Enter **8444** as the **Backend port**.

f) Select your **Backend pool**.

g) Select the **Health probe** for port **8444**.

h) Select **None** as the **Session persistence**.

i) Select **4** as the **Idle timeout (minutes)**.

j) Select **Disabled** for **Floating IP (direct server return)**.

4. Click **OK**.

Create additional Load Balancing Rules for any other traffic that is published through the LoadMaster.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 6 Network Security Groups

Network Security Groups are used in Azure to control what traffic is allowed or denied access to Virtual Machines. Depending on your configuration, you are required to update one or more Network Security Groups to allow published traffic to access the LoadMasters and backend Real Servers.

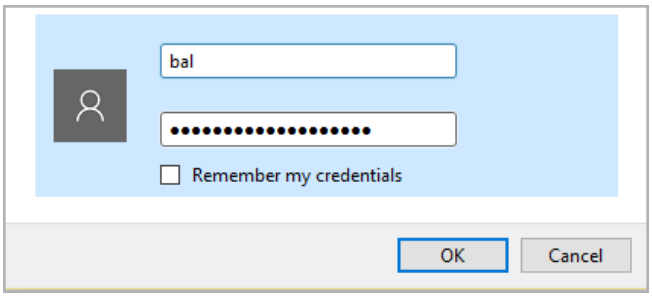
The security group must contain a rule for 8443. This is the WUI port. If the LoadMaster is public-facing, other best practice, recommended (but not mandatory) ports that should be in the security group, are; 8441, 8442, 8444, 22, 221, 222, the Virtual Service ports (such as 80) and any other ports that are needed by the backend.

Do not block port 6973.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 7 Configure the LoadMasters

To configure LoadMaster for HA, follow the steps outlined in the sections below:



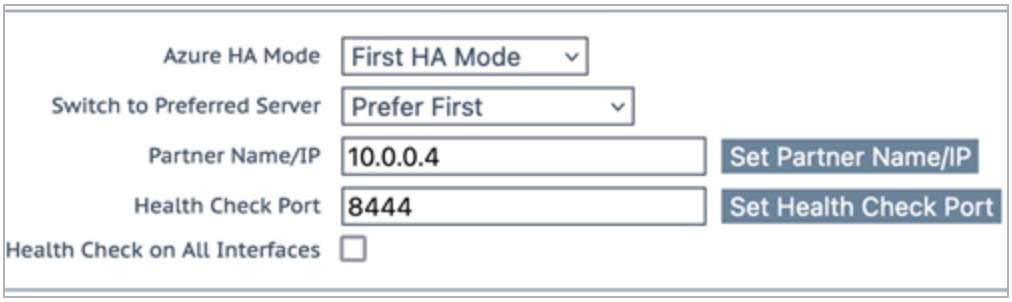

1. If the LoadMaster does not have a public address itself and you are going through the Internal Load Balancer (ILB), you can access the WUI of the LoadMaster which is the active unit:

   a) Access the WUI of active LoadMaster by going to **https://<DNSNameURL>:8441**.

   b) Access the WUI of the standby LoadMaster by going to **https://<DNSNameURL>:8442**.

   c) The default username is **bal** and the password is the password entered during the creation of the LoadMaster.

2. In the main menu, go to **System Configuration > Azure HA Parameters**.




3. Select **First HA Mode** in the **Azure HA Mode** drop-down list.

4. Select the desired option in the **Switch to Preferred Server** drop-down list:

   - **No Preferred Host:** Each unit takes over when the other unit fails. No switchover is performed when the partner is restarted.

   - **Prefer First:** The HA1 (active) unit always takes over. This is the default option.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

5. Enter the internal address of the standby LoadMaster unit in the **Partner Name/IP** text box and click **Set Partner Name/IP**.

6. Enter **8444** as the **Health Check Port** and click **Set Check Port**.

> The **Health Check Port** must be set to **8444** on both the active and standby units for HA to function correctly.

7. If using a multi-arm configuration, select the **Health Check on All Interfaces** check box.

> If this option is disabled, the health check listens on the primary eth0 address.

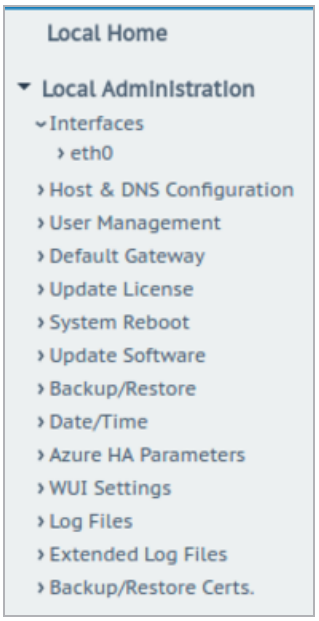
8. Then, access the WUI of the standby unit. Complete the following steps in the standby unit, but select Second HA Mode as the Azure HA Mode instead: **In the main menu, go to System Configuration > Azure HA Parameters.** to **Enter the internal address of the standby LoadMaster unit in the Partner Name/IP text box and click Set Partner Name/IP.**

> HA will not work if both units have the same value selected for the **Azure HA Mode**.

9. After configuring both LoadMasters, reboot both units (System Configuration > System Administration > System Reboot > Reboot).

When HA is enabled on both devices, changes made to the Virtual Services in the active unit is replicated to the standby.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.




If a unit is in standby mode, WUI access is restricted to **Local Administration** only. Full WUI access is available if the unit is in an active or unchecked state.




You can tell, at a glance, which unit is active, and which is the standby, by checking the mode in the top bar of the LoadMaster.

The current status of each LoadMaster, when HA is enabled, is shown as follows:

| Status | Description |
|---|---|
|  | This is the first LoadMaster and it is currently active. |
|  | This is the second LoadMaster and it is currently active. |
|  | This is the second unit and it is currently the standby unit. |


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 8 Configure GEO Clusters with HA

There is no shared IP addresses for cloud HA LoadMasters, so individual LoadMaster IP addresses must be used when configuring GEO clusters. When creating a GEO cluster, use the IP address of the master LoadMaster. If there is a failover and the standby machine takes the active role, the cluster IP address changes automatically.

To configure a working configuration of a HA pair with GEO clusters, follow the steps below, depending on your type of configuration.

## 8.1 Configure the Master IP Address for one HA Pair

To configure the master IP address as a cluster on a HA pair, follow these steps in the LoadMaster WUI:

1. In the main menu, go to **Certificates & Security > Remote Access**.
2. Enter the IP address of the master LoadMaster in the **Remote GEO LoadMaster Access** text box and click **Set GEO LoadMaster access**.
3. In the main menu, go to **Global Balancing > Manage Clusters**.
4. In the **IP address** text box, enter the master LoadMaster IP address.
5. Enter a **Name** for the cluster and click **Add Cluster**.
6. Select **Remote LM** in the **Type** drop-down list.

## 8.2 Configure Clusters of HA IP Addresses Between Two HA Pairs

To configure clusters of HA IP addresses between two HA pairs, follow the steps below.

On HA pair 1, complete these steps:

1. In the main menu, go to **Certificates & Security > Remote Access**.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2. Enter the IP address of the master LoadMaster and the IP addresses of both partners in the second HA pair in the **Remote GEO LoadMaster Access** text box and click **Set GEO LoadMaster access**.

3. Enter the IP addresses of both partners in the second HA pair In the **GEO LoadMaster Partners** text box and click **Set GEO LoadMaster Partners**.

On HA pair 2, complete these steps:

1. In the main menu, go to **Certificates & Security > Remote Access**.

2. Enter the IP address of the master LoadMaster and the IP addresses of both partners in the first HA pair in the **Remote GEO LoadMaster Access** text box and click **Set GEO LoadMaster access**.

3. Enter the IP addresses of both partners in the first HA pair In the **GEO LoadMaster Partners** text box and click **Set GEO LoadMaster Partners**.

Then, complete these steps:

1. Reboot the master LoadMaster of the first HA pair.

2. Submit the **GEO LoadMaster Partners** configuration again on the new active LoadMaster.

3. Reboot the master LoadMaster of the second HA pair.

4. Submit the **GEO LoadMaster Partners** configuration again on the new active LoadMaster.

Then, create the GEO clusters with the **TypeRemote LM** using the master IP address of both HA pairs:

1. In the main menu, go to **Global Balancing > Manage Clusters**.

2. In the **IP address** text box, enter the master LoadMaster IP address.

3. Enter a **Name** for the cluster and click **Add Cluster**.

4. Select **Remote LM** in the **Type** drop-down list.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

## 8.3 Configuring Clusters of HA IP Addresses Between a HA Pair and a Standalone System

To configure clusters of HA IP addresses between a HA pair and a standalone system, follow the steps below.

On the HA pair LoadMaster, complete these steps:

1. In the main menu, go to **Certificates & Security > Remote Access**.

2. Enter the IP address of the master LoadMaster and the IP address of the standalone LoadMaster in the **Remote GEO LoadMaster Access** text box and click **Set GEO LoadMaster access**.

3. Enter the IP address of the standalone system in the **GEO LoadMaster Partners** text box and click **Set GEO LoadMaster Partners**.

On the standalone system, complete these steps:

1. In the main menu, go to **Certificates & Security > Remote Access**.

2. Enter the IP address of the standalone LoadMaster and the IP addresses of both partners in the HA pair in the **Remote GEO LoadMaster Access** text box and click **Set GEO LoadMaster access**.

Then, complete these steps:

1. Reboot the master LoadMaster of the HA pair.

2. Submit the **GEO LoadMaster Partners** configuration again on the new active LoadMaster.

3. On the standalone LoadMaster, submit the **GEO LoadMaster Partners** configuration again.

Then, create the GEO clusters with the **TypeRemote LM** using the master IP address of the HA pair and the IP address of the standalone LoadMaster:

1. In the main menu, go to **Global Balancing > Manage Clusters**.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2. In the **IP address** text box, enter the LoadMaster IP address.

3. Enter a **Name** for the cluster and click **Add Cluster**.

4. Select **Remote LM** in the **Type** drop-down list.

## 8.4 Configure Clusters of HA IP Addresses Between Two HA Pairs and Two Standalone LoadMasters

To configure clusters of HA IP addresses between two HA pairs and two standalone systems, follow the steps below.

On HA pair 1, complete these steps:

1. In the main menu, go to **Certificates & Security > Remote Access**.

2. Enter the IP address of the master LoadMaster, the IP addresses of both partners of the second HA pair, and the IP addresses of both standalone LoadMasters in the **Remote GEO LoadMaster Access** text box and click **Set GEO LoadMaster access**.

3. Enter the IP addresses of both partners of the second HA pair and the IP addresses of both standalone LoadMasters in the **GEO LoadMaster Partners** text box and click **Set GEO LoadMaster Partners**.

On HA pair 2, complete these steps:

1. In the main menu, go to **Certificates & Security > Remote Access**.

2. Enter the IP address of the master LoadMaster, the IP addresses of both partners of the first HA pair, and the IP addresses of both standalone LoadMasters in the **Remote GEO LoadMaster Access** text box and click **Set GEO LoadMaster access**.

3. Enter the IP addresses of both partners of the first HA pair and the IP addresses of both standalone LoadMasters in the **GEO LoadMaster Partners** text box and click **Set GEO LoadMaster Partners**.

On standalone LoadMaster 1, complete these steps:

1. In the main menu, go to **Certificates & Security > Remote Access**.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2. Enter the IP address of standalone LoadMaster 1, the IP addresses of both partners of both HA pairs, and the IP addresses of the second standalone LoadMaster in the **Remote GEO LoadMaster Access** text box and click **Set GEO LoadMaster access**.

3. Enter the IP addresses of both partners of HA pairs and the IP address of the second standalone LoadMasters in the **GEO LoadMaster Partners** text box and click **Set GEO LoadMaster Partners**.

On standalone LoadMaster 2, complete these steps:

1. In the main menu, go to **Certificates & Security > Remote Access**.

2. Enter the IP address of standalone LoadMaster 2, the IP addresses of both partners of both HA pairs, and the IP addresses of the first standalone LoadMaster in the **Remote GEO LoadMaster Access** text box and click **Set GEO LoadMaster access**.

3. Enter the IP addresses of both partners of HA pairs and the IP address of the first standalone LoadMasters in the **GEO LoadMaster Partners** text box and click **Set GEO LoadMaster Partners**.

Then, complete these steps:

1. Reboot the master LoadMaster of the first HA pair.

2. Submit the **GEO LoadMaster Partners** configuration again on the new active LoadMaster.

3. Reboot the master LoadMaster of the second HA pair.

4. Submit the **GEO LoadMaster Partners** configuration again on the new active LoadMaster.

5. On both standalone LoadMasters, submit the **GEO LoadMaster Partners** configuration again.

Then, create the GEO clusters with the **TypeRemote LM** using the master IP address of both HA pairs and the IP addresses of both standalone LoadMasters:

1. In the main menu, go to **Global Balancing > Manage Clusters**.

2. In the **IP address** text box, enter the LoadMaster IP address.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3. Enter a **Name** for the cluster and click **Add Cluster**.
4. Select **Remote LM** in the **Type** drop-down list.

Here is an example configuration for the scenario outlined above (involving two HA pairs and two standalone systems).

**HA Pair 1**

172.24.1.5

172.24.1.6

**Remote GEO LoadMaster Access:** 172.24.1.7 172.24.1.8 172.24.1.5 172.24.1.9 172.24.1.10

**GEO LoadMaster Partners:** 172.24.1.7 172.24.1.8 172.24.1.9 172.24.1.10

**HA Pair 2**

172.24.1.7

172.24.1.8

**Remote GEO LoadMaster Access:** 172.24.1.8 172.24.1.5 172.24.1.6 172.24.1.9 172.24.1.10

**GEO LoadMaster Partners:** 172.24.1.5 172.24.1.6 172.24.1.9 172.24.1.10

**Standalone LoadMaster 1**

172.24.1.9

**Remote GEO LoadMaster Access:** 172.24.1.7 172.24.1.8 172.24.1.5 172.24.1.6 172.24.1.9 172.24.1.10

**GEO LoadMaster Partners:** 172.24.1.7 172.24.1.8 172.24.1.5 172.24.1.6 172.24.1.10

**Standalone LoadMaster 2**

172.24.1.10

**Remote GEO LoadMaster Access:** 172.24.1.7 172.24.1.8 172.24.1.5 172.24.1.6 172.24.1.9 172.24.1.10

**GEO LoadMaster Partners:** 172.24.1.7 172.24.1.8 172.24.1.5 172.24.1.6 172.24.1.9


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 9 LoadMaster Firmware Upgrades/Downgrades

Do not downgrade from firmware version 7.2.36 or higher to a version below 7.2.36. If you do this, the LoadMaster becomes inaccessible and you cannot recover it.

You should never leave two LoadMasters with different firmware versions paired as HA in a production environment. To avoid complications, follow the steps below in sequence and do not perform any other actions in between the steps. Please upgrade/downgrade during a maintenance window and expect service disruption because there are reboots.

The steps below are high-level, for detailed step-by-step instructions on how to upgrade the LoadMaster firmware, refer to the Updating the LoadMaster Software Feature Description on the Kemp documentation page: https://kemptechnologies.com/loadmaster-documentation.

## 9.1 Upgrade the LoadMaster Firmware

To upgrade the LoadMaster firmware with the least disruption, follow the steps below in sequence:

1. Identify the STAND-BY unit.

2. Upgrade the LoadMaster firmware on the STAND-BY unit. Once the STAND-BY unit has rebooted, it remains in the STAND-BY state and the WUI is limited to the Local Administration options.

3. Upgrade the LoadMaster firmware on the ACTIVE unit. When the ACTIVE unit is rebooting, the STAND-BY unit becomes ACTIVE.

4. Depending on Preferred Host settings in the HA configuration, the Standby unit may failback over to the Active unit.

After these steps are completed the upgrade is finished.

## 9.2 Downgrade the LoadMaster Firmware

To downgrade the LoadMaster firmware with the least disruption, follow the steps below in sequence:

1. Identify the STAND-BY unit.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2. Downgrade the LoadMaster firmware on the STAND-BY unit. Once the STANDY-BY unit has rebooted, it remains in the STAND-BY state and the WUI is limited to the Local Administration options.

3. Downgrade the LoadMaster firmware on the ACTIVE unit. When the ACTIVE unit is rebooting, the STAND-BY unit becomes ACTIVE.

4. Depending on Preferred Host settings in the HA configuration, the Standby unit may failback over to the Active unit.

After these steps are completed the downgrade is finished.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# 10 Troubleshooting

The sections below provide some basic troubleshooting tips. If further assistance is required, please contact Kemp Support: https://support.kemptechnologies.com.

## 10.1 Check which LoadMaster is Active

In addition to checking the status in the top-right of the LoadMaster WUI, it is also possible to check which LoadMaster is active by accessing port 8444 through the Public IP address since the Load Balanced Rule was created for this port, that is,

**http://<PublicIPofAzureLoadBalancer>:8444**

Ensure to use HTTP, not HTTPS. On the active unit, you should see "Active/Standby is active". On the standby, you should see a 503 service unavailable error. If you see these messages, it means the LoadMasters are working correctly/

## 10.2 First/Second Unconnected

When initially setting up cloud HA, the active unit should have **First** in the top-right corner of the LoadMaster WUI.

The standby unit should show **Second**.

After setting up the load balancer (Internal Load Balancer (ILB) for Azure or Network Load Balancer for AWS) the units should switch from:

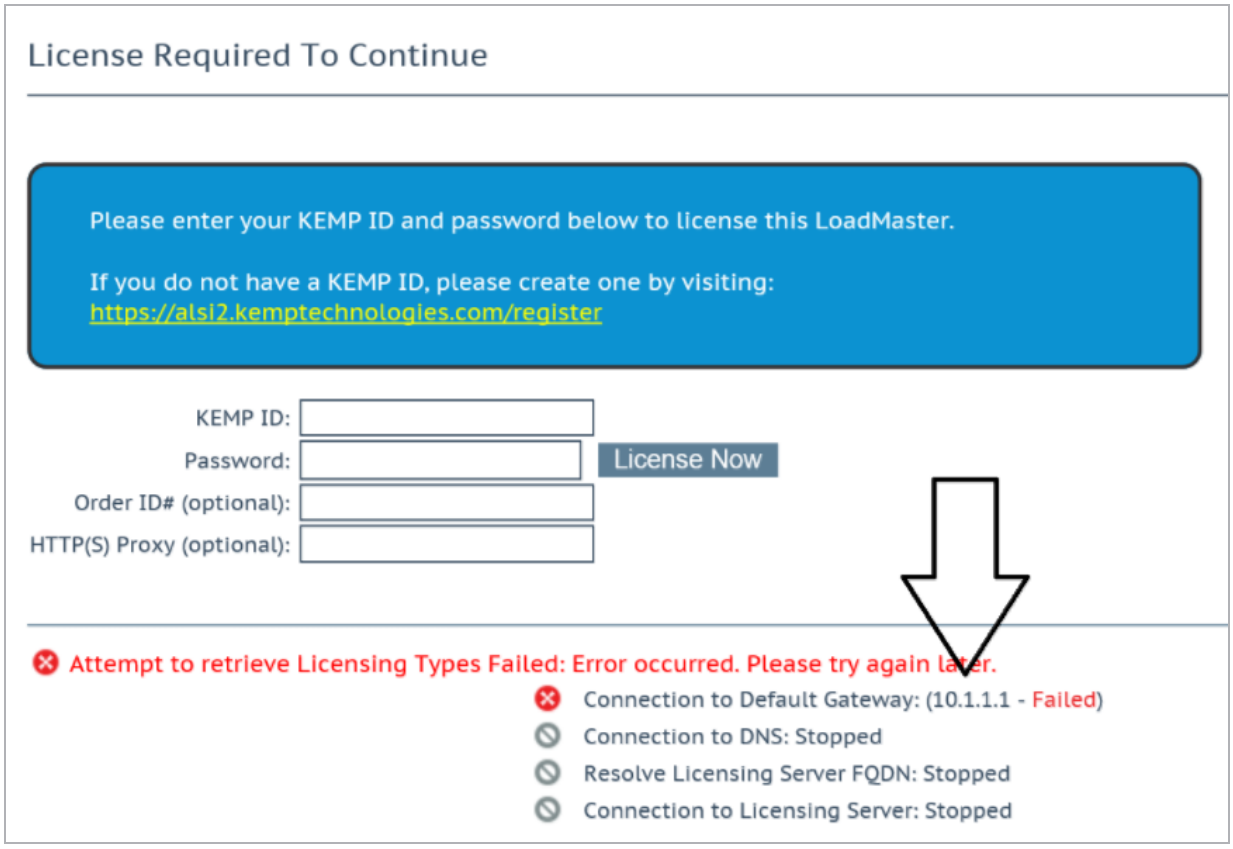
- First to First Unconnected
- Second to Second Unconnected

This means the LoadMasters have not been polled by the load balancer. Once the load balancer has the health check correctly set, the units should switch from:

- First Unconnected to First (Active)/First (Standby)
- Second (Unconnected) to Second (Active)/Second (Standby)


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

## 10.3 Connection to Default Gateway Failed




Azure blocks pings in some cases. Therefore, on older LoadMaster firmware you may see an error message like the one above when licensing. This is a red herring and can be ignored - there is likely another problem such as an incorrect Kemp ID/password. If you are running the latest version of LoadMaster firmware, this check should be skipped.

## 10.4 Virtual Machine Inaccessible

It takes approximately five minutes for the Virtual Machine to become accessible after booting.

## 10.5 Run a TCP Dump

Running a TCP dump and checking the results can also assist with troubleshooting. To do this, follow the steps below in the LoadMaster WUI:

1. In the main menu, go to **System Configuration > Troubleshooting**.
2. In the **TCP dump** section, enter the relevant IP **Address** and the Azure HA **Port**.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3. Click **Start**.
4. Let the capture run for a few minutes.
5. Click **Stop**.
6. Click **Download**.
7. Analyse the results in a packet trace analyser tool such as Wireshark.

Checks from the partner LoadMaster should appear in the results. If nothing is shown there is a problem, for example Azure may be blocking the connection.

## 10.6 Sync Problems

In most scenarios, the configuration settings are automatically synchronized between partners every two minutes. If a new Virtual Service is created, the settings are immediately synchronized. Because of this, creating a new Virtual Service is a good way of checking if the synchronization is working. To trace this, follow the steps below:

1. Start a TCP dump, as detailed in the **Run a TCP Dump** section, but use port 6973.
2. Create a Virtual Service.
3. Stop the TCP dump.
4. Download the TCP dump file.
5. Analyse the results.

After creating a Virtual Service, a lot of traffic should have been immediately triggered.

Generally, if a lot of packets are being transferred it means that the synchronization is working. If only a few packets are transferred, it may mean that the connection was unsuccessful. In this case, there may be a problem such as unmatched SSH keys.

# 10.7 Misconfigured ILB

It is possible that the two LoadMasters are able to communicate but the ILB might be misconfigured. Connect to both units on http://*LoadMasterAddress*:8444. On the active unit, you should see "Active/Standby is active". On the standby, you should see a 503 service unavailable error. If you see these messages, it means the LoadMasters are working correctly and the problem is elsewhere. Confirm that the health check probe on the ILB is configured correctly.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

## 10.8 Problems Reaching a Virtual Service

If you experience problems reaching a Virtual Service, confirm the network security group and the ILB inbound rules are configured correctly.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# References

Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation.

**Licensing, Feature Description**

**LoadMaster for Azure, Installation Guide**

**Azure Virtual Machines – tutorials and guides:**

http://www.windowsazure.com/en-us/documentation/services/virtual-machines/

**High Availability (HA), Feature Description**


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

# Last Updated Date

This document was last updated on 27 July 2023.


© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.