HA for Azure Resource Manager

Feature Description

UPDATED: 31 January 2019

Copyright Notices

Copyright © 2002-2019 Kemp Technologies, Inc. All rights reserved. Kemp Technologies and the Kemp Technologies logo are registered trademarks of Kemp Technologies, Inc.

Kemp Technologies, Inc. reserves all ownership rights for the LoadMaster and Kemp 360 product line including software and documentation.

Used, under license, U.S. Patent Nos. 6,473,802, 6,374,300, 8,392,563, 8,103,770, 7,831,712, 7,606,912, 7,346,695, 7,287,084 and 6,970,933

Table of Contents

1 Introduction 5
2 Prerequisites 8
3 Manually Configure LoadMaster HA in Azure 10
3.1 Licensing Options 10
3.2 Recommended Pricing Tier 10
3.3 Create an SSH Key Pair 11
3.4 Create the First Virtual LoadMaster in Azure 14
3.5 Create the Second LoadMaster in Azure 24
4 Create the Internal Load Balancer (ILB) 25
5 Configure the Azure Load Balancer 29
5.1 Create a Backend Pool 29
5.2 Create Inbound NAT Rules 31
5.3 Create a Probe to Monitor LoadMaster Health 32
5.4 Create Load Balancing Rules to Allow Traffic 34
6 Network Security Groups 37
7 Configure the LoadMasters 38
8 LoadMaster Firmware Upgrades/Downgrades 41
8.1 Upgrade the LoadMaster Firmware 41
8.2 Downgrade the LoadMaster Firmware 41
9 Troubleshooting 43
9.1 Check which LoadMaster is Active 43
9.2 Master/Slave Unconnected 43
9.3 Connection to Default Gateway Failed 44
9.4 Virtual Machine Inaccessible 44

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

9.5 Run a TCP Dump 44
9.6 Sync Problems 45
9.7 Misconfigured ILB 46
9.8 Problems Reaching a Virtual Service 46
References **47**
Last Updated Date **48**

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

1 Introduction

Microsoft Azure has two different models for deploying services: **Resource Manager** and **Classic**. The main body of this guide covers setting up the LoadMaster with High Availability using the **Resource Manager** method. For steps using the **Classic** method, please refer to the **HA for Azure (Classic Interface), Feature Description**.

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 master are replicated to the slave and changes made to the slave are replicated to the master.
- The replication (synchronization) of settings (from master to slave) is not instant in all cases and may take a few moments to complete.
- When synchronizing the GEO settings from master to slave, any Fully Qualified Domain Name (FQDN) or cluster IP addresses that match the master's IP address are replaced with the slave's IP address. Likewise, when synchronizing from slave to master, the slave's IP address is replaced with the master's 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

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

- Admin default gateway

- Administrative certificate settings (.cert, .pem and .setadmin files)

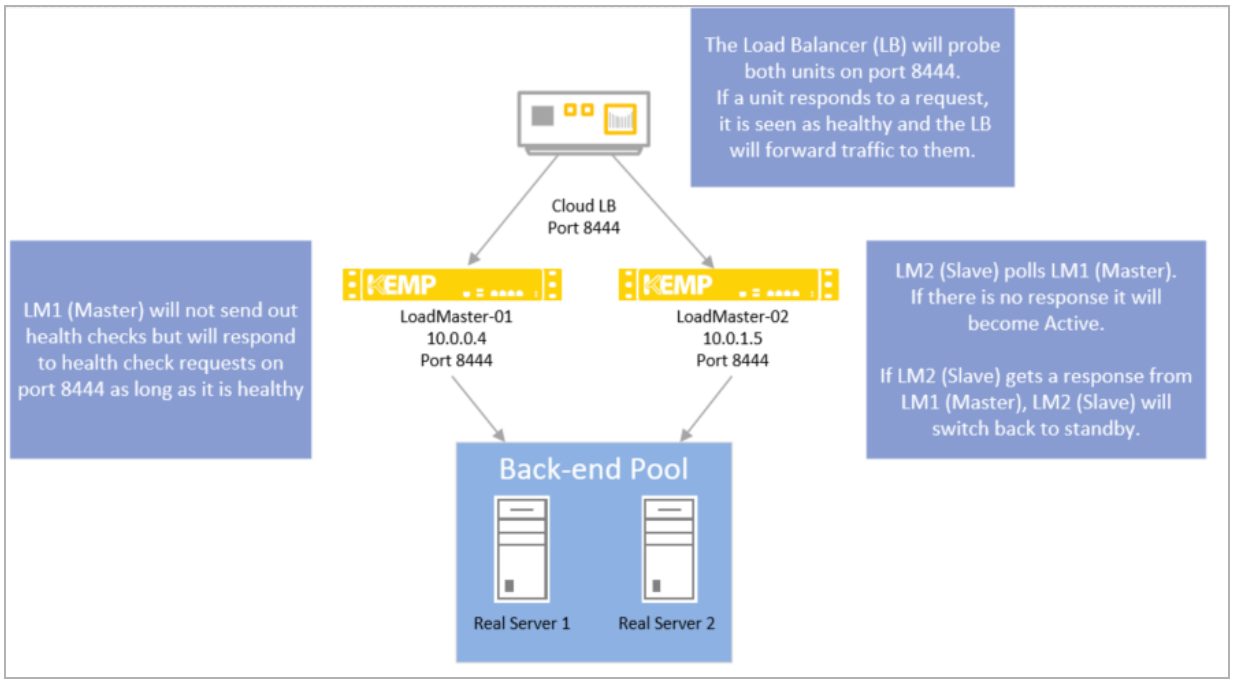
- Network interface settings: Link Status (Speed and Duplex), MTU and additional addresses

- 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 master unit is always set as active and the slave unit can be standby or active if the master fails. The master unit is the master and never becomes the slave, even if it fails. Similarly the slave unit never becomes the master. When the master unit comes back up it is set as active and connections are automatically directed to the master again. Either the master or slave unit can be active or standby.
- The **HA Check Port** must be set to the same port on both the master and slave 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.



 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

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

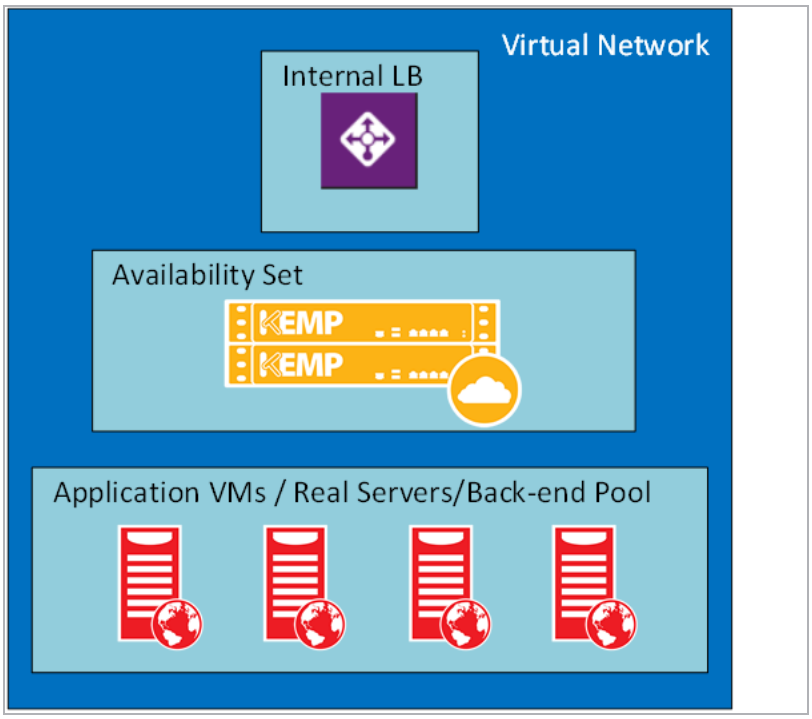
 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

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:

- Application VMs are installed and configured
- LoadMaster for Azure VMs are installed and configured

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

- **Important:** The **HA Check Port** must be set to the same port on both the master and slave 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.

 Copyright 2002-2019, Kemp Technologies, 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

The following licensing options when deploying a LoadMaster for Azure:

- Hourly consumption
- Bring Your Own License (BYOL)
- Metered Enterprise License Agreement (MELA)
- Service Provider License Agreement (SPLA)

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 > Update License**).
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 Recommended Pricing Tier

When creating a LoadMaster for Azure Virtual Machine, you must select a pricing tier. The recommended pricing tiers are listed in the table below.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

If the relevant pricing tier is not displayed in Azure, click **View all**.

Some availability groups only allow some Virtual LoadMaster (VLM) sizes.

VLM Model	Recommended Pricing Tier
VLM 200	A1, A2, A3
VLM 2000	A2, A3, A4
VLM 5000	A3, A4, A5
VLM 10G	A7, A8, A9

It is best practice to use Managed Disks.

If you are using Solid State Drive (SSD), Azure changes the Virtual Machine size for you: Standard DS3 (4 cores, 14 GB memory).

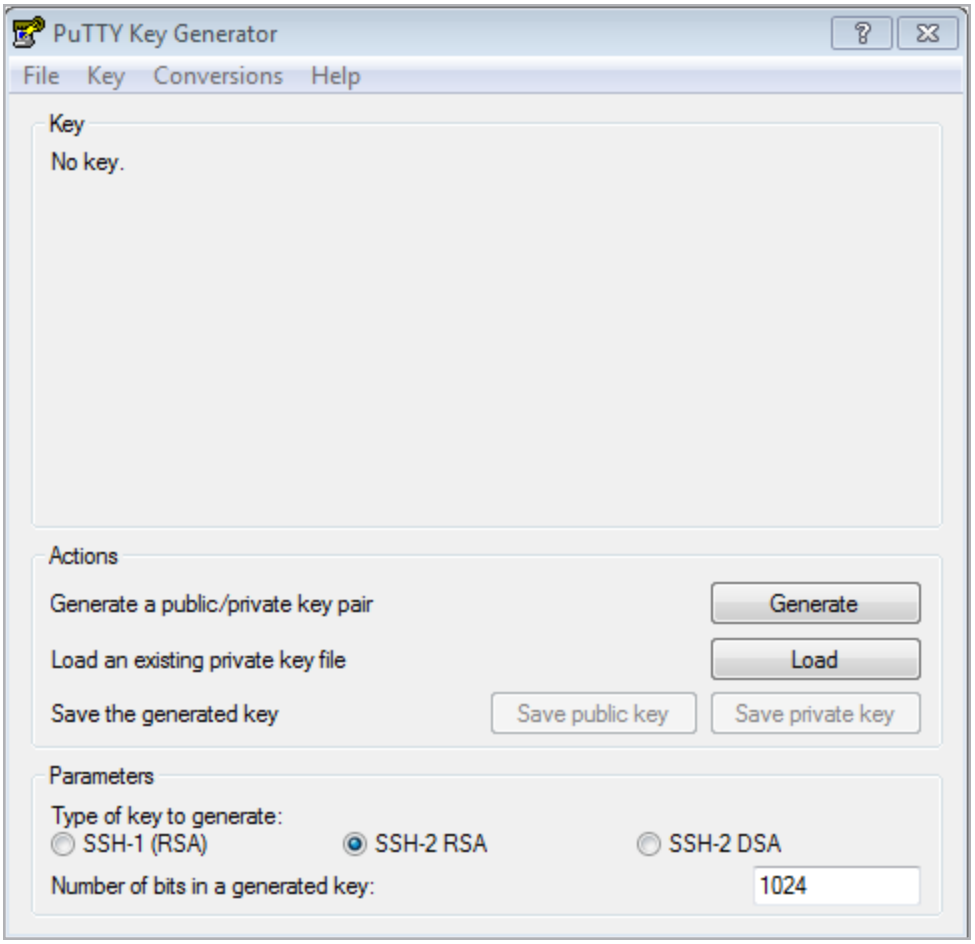
3.3 Create an SSH Key Pair

When creating a LoadMaster for Azure VM, there are two options for authentication - a password or an SSH public key. Kemp recommends using a password, but either way will work fine. If you choose to use a password, this section can be skipped and you can move on to the **Create the First Virtual LoadMaster in Azure** section to create the LoadMaster for Azure VM. If you choose to use an SSH public key, an SSH key pair will need to be created.

To create an SSH key pair, you will need to use a program such as the **PuTTYgen** or **OpenSSH**. As an example for this document, the steps in **PuTTYgen** are below:

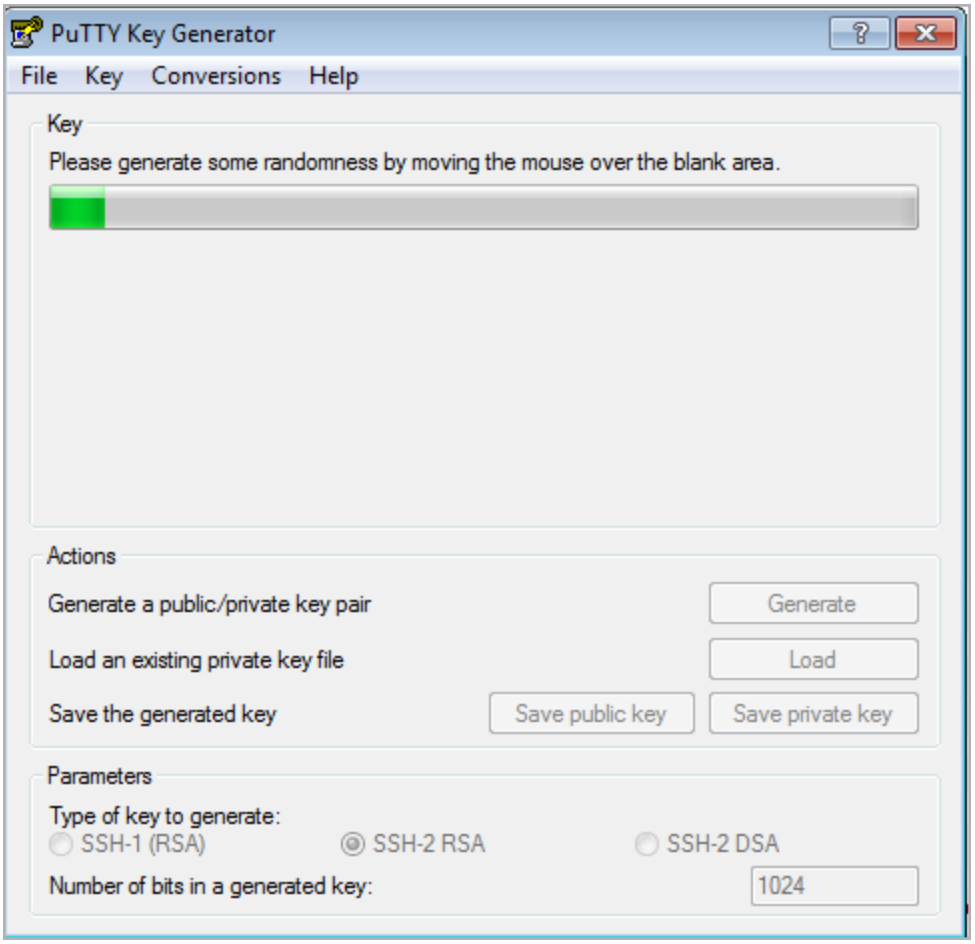
1. Open PuTTYgen.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved



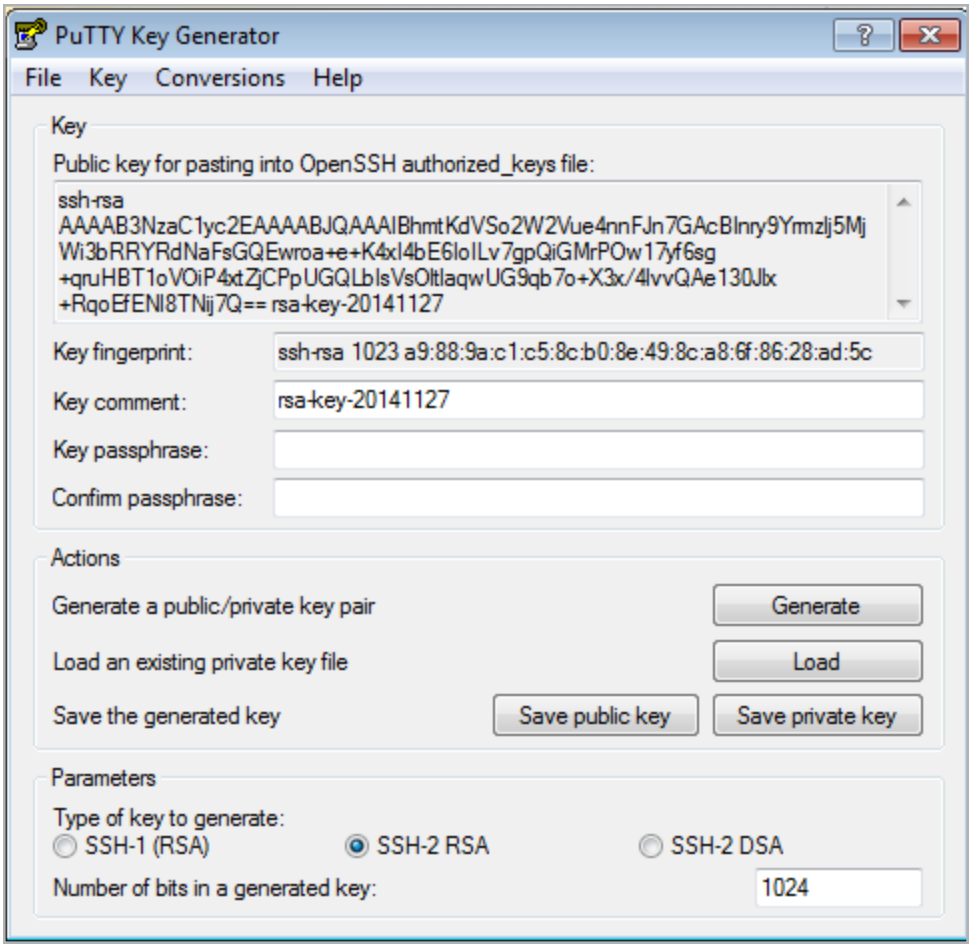
2. Click **Generate**.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved



3. Move the mouse over the blank area in the middle. This generates a random pattern that is used to generate the key pair.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved



4. Copy and save the public and private key as needed.

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

3.4 Create the First Virtual LoadMaster in Azure

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

The following procedure describes how to set up LoadMaster for Azure from the Microsoft Azure portal:

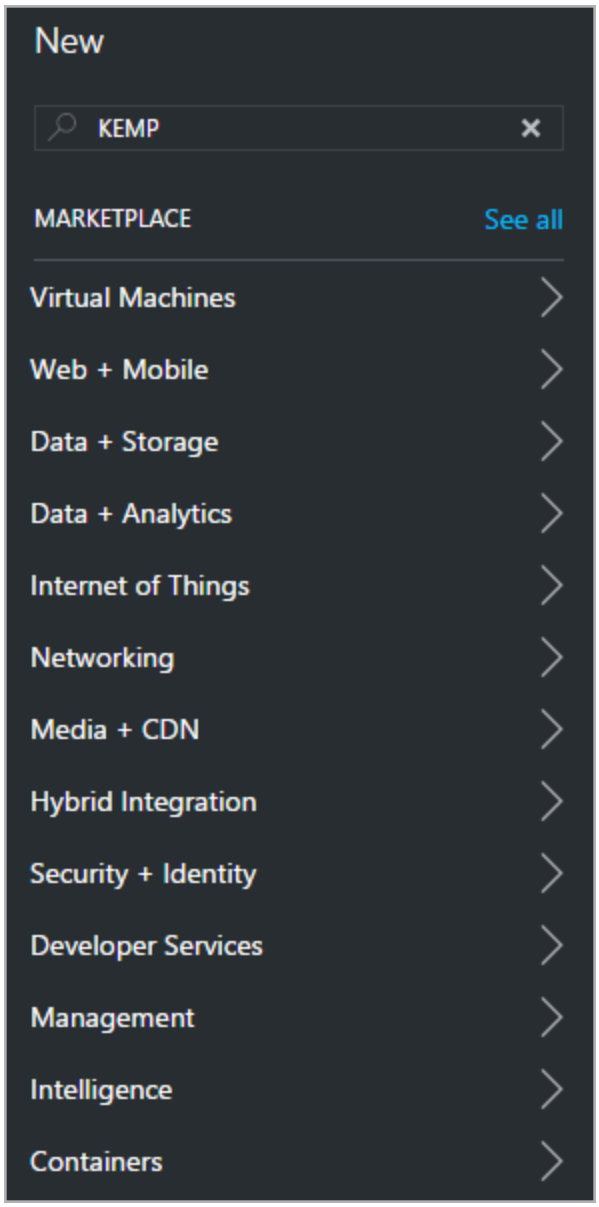
> The steps below are carried out from http://portal.azure.com and not from http://manage.windowsazure.com.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

1. From the Azure Management Portal dashboard, click **Marketplace**.

2. In the **Marketplace** section, click the **New** icon.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

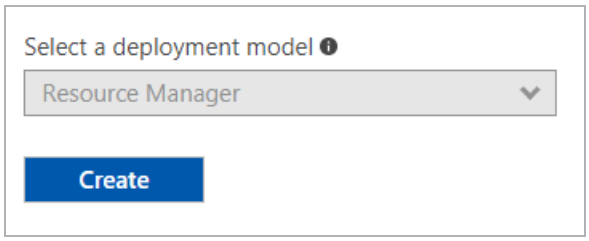


3. Type **Kemp** in the search field and press **Enter** on your keyboard.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

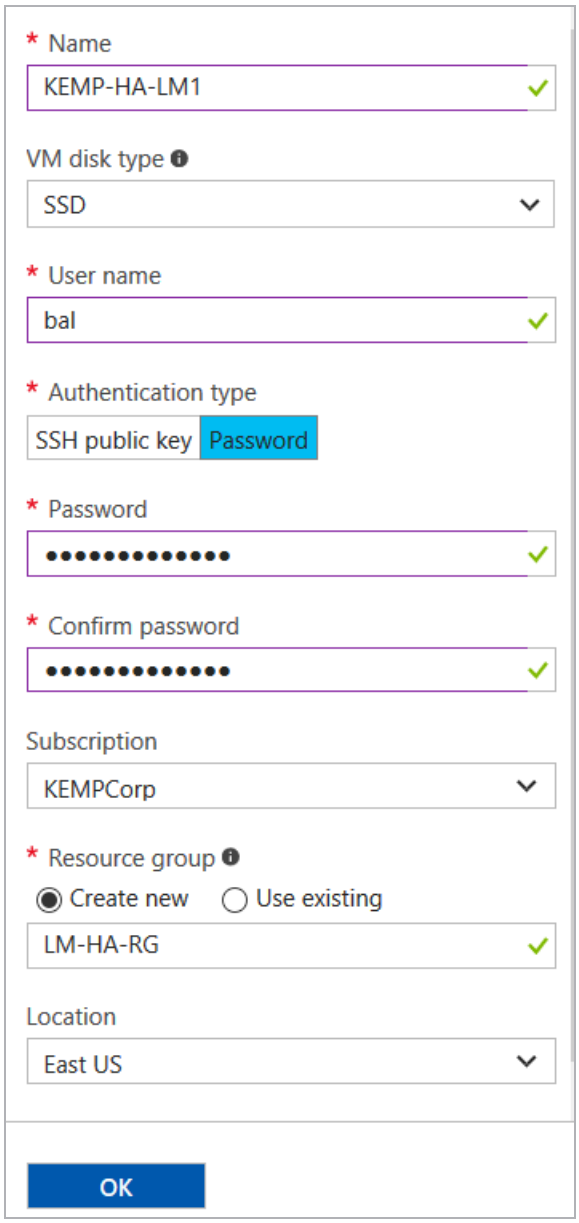
BYOL Load Balancer, ADC & WAF - Trial & Perpetual	KEMP Technologies Inc	Compute
Free 20Mbps Load Balancer, ADC & WAF	KEMP Technologies Inc	Compute
5 Gbps Load Balancer, ADC & WAF (Hourly)	KEMP Technologies Inc	Compute
2 Gbps Load Balancer, ADC & WAF (Hourly)	KEMP Technologies Inc	Compute
500 Mbps Load Balancer, Commercial WAF (Hourly)	KEMP Technologies Inc	Compute

4. Select the appropriate Kemp Virtual LoadMaster image to deploy.



5. Click **Create**.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved



6. Provide details in the **Create VM** section. The details required to create a new VM are:

    a) **Name**: Provide a unique name for VM identification. This is the host name.

    b) **User name**: This is not used by LoadMaster for Azure. Provide a name of your choice. The default username for accessing the LoadMaster is **bal**.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

c) Fill out the authentication details. There are two possible methods of authentication - using a password or an SSH key. Depending on what you select, complete the relevant step below:

- Password: Enter a password.

This password is used to access the LoadMaster WUI.

- SSH Public Key: Paste the SSH public key which was created in the **Create an SSH Key Pair** section. The private key is needed to connect to the LoadMaster using SSH.

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

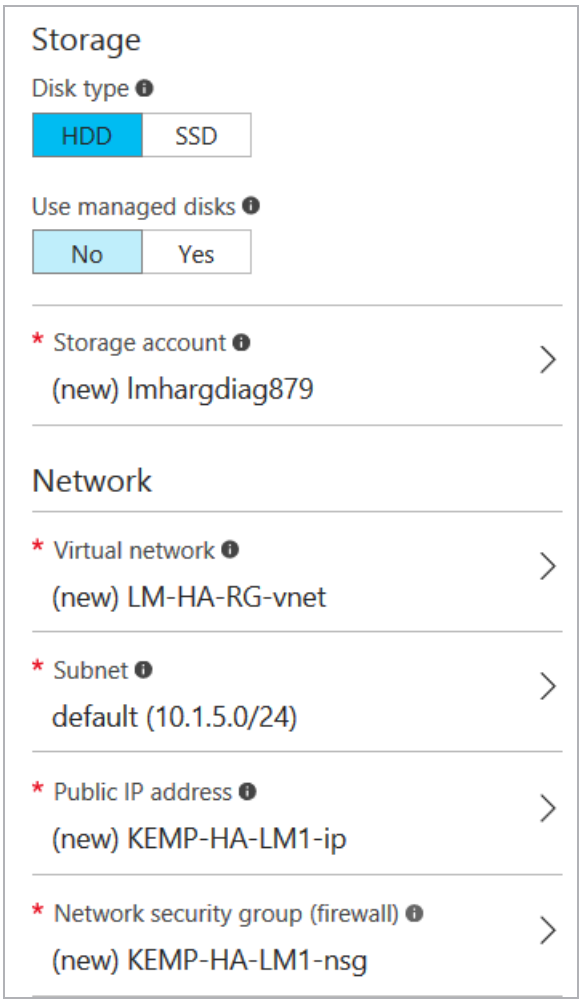
7. Use an existing or create a new **Resource group** for the LoadMasters to be a part of.

8. Select the **Location** in which to deploy the LoadMaster.

9. Click **OK**.

10. Select from the recommended pricing tiers. Click **View all** if the recommended pricing tiers do not meet the recommended requirements (see the **Licensing Options** section for further information regarding what tier to select).

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved



11. Select the relevant **Storage Account**, or create a new one if needed.
12. Select an existing **Virtual network**, or create a new one if needed.

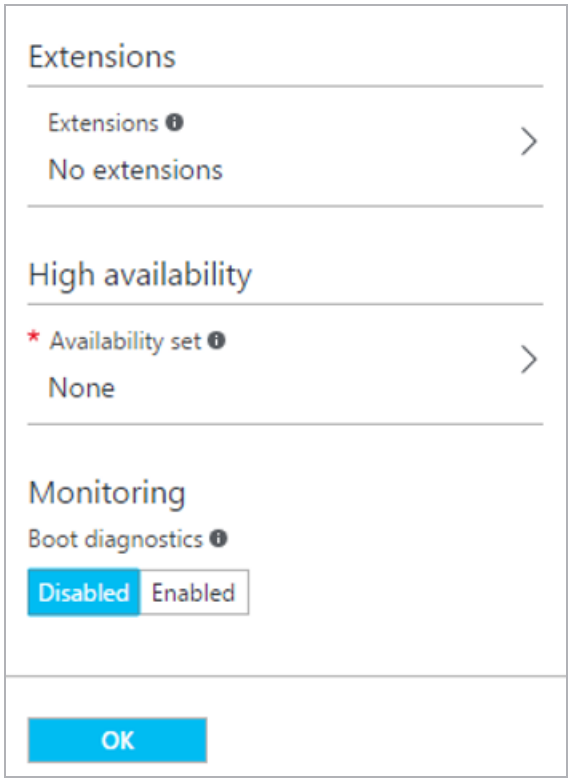
> A Public IP Address (PIP) is **not** required for each of the LoadMasters. A single PIP is created for the Azure Load Balancer and NAT Translation Rules are created to allow management access.

13. Select the relevant **Network security group**, or create a new one if needed.

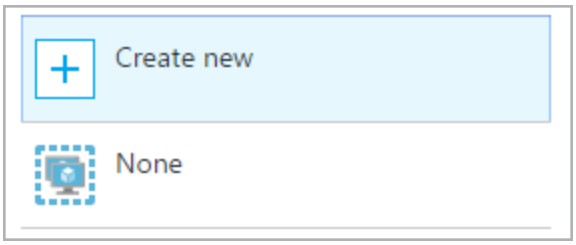
> The security group must contain a rule for 8443. This is the WUI port. If the LoadMaster is public-facing, other recommended (but not mandatory) ports that should be in the security group

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

for administrationare; 8441, 8442, 8443, 8444, 22, 221, 222, the Virtual Service ports (such as 80) and any other ports that are needed by the backend.



14. Select **Disabled** for **Diagnostics**.
15. Click **Availability set**.



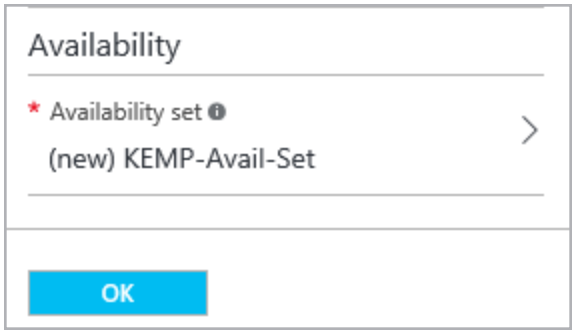
16. Click **Create new**.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

17. Provide a unique **Name** for the Availability Set.

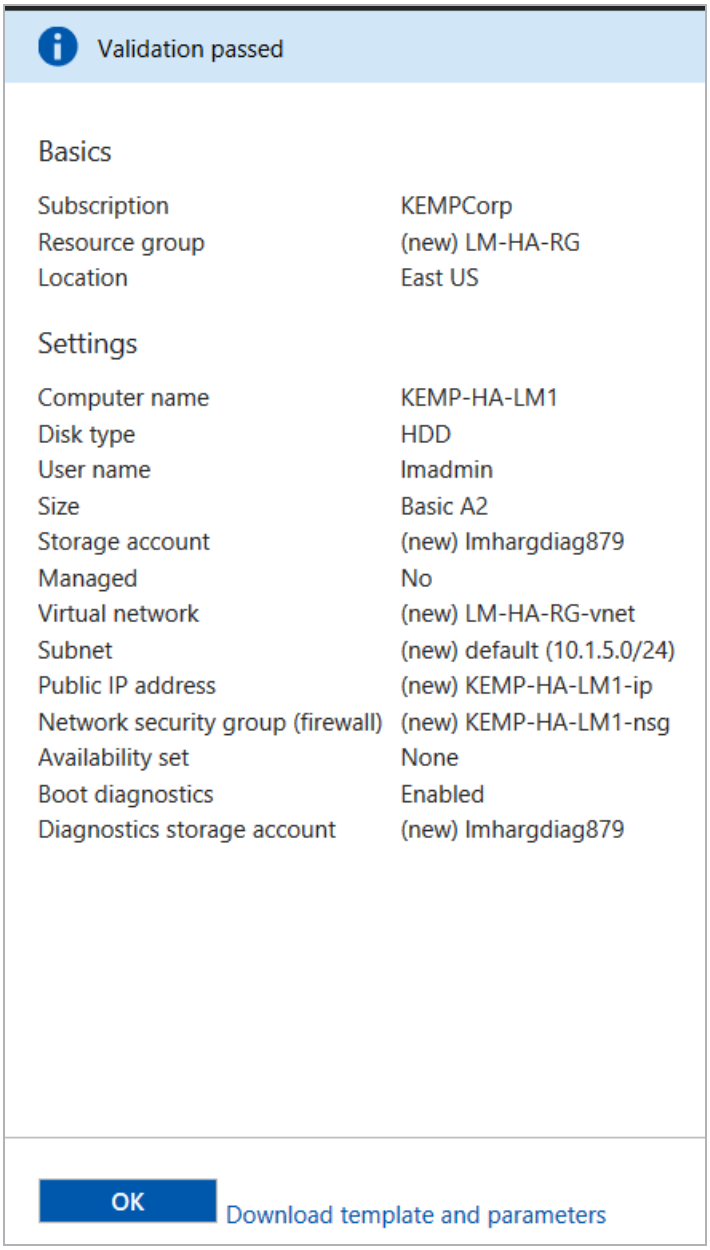
> Some availability groups only allow some Virtual LoadMaster (VLM) sizes.

18. Click **OK**.



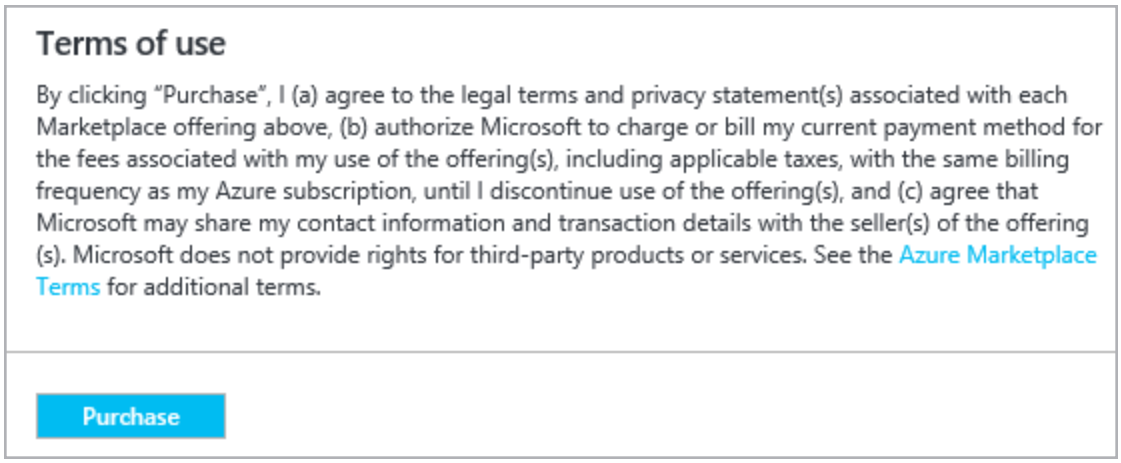
19. Click **OK.**

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved



20. Confirm that Validation Passed.
21. Click **OK**.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved



22. Click **Purchase**.

3.5 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 **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.

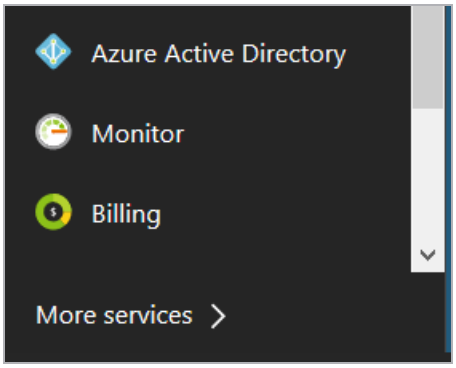
 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

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.

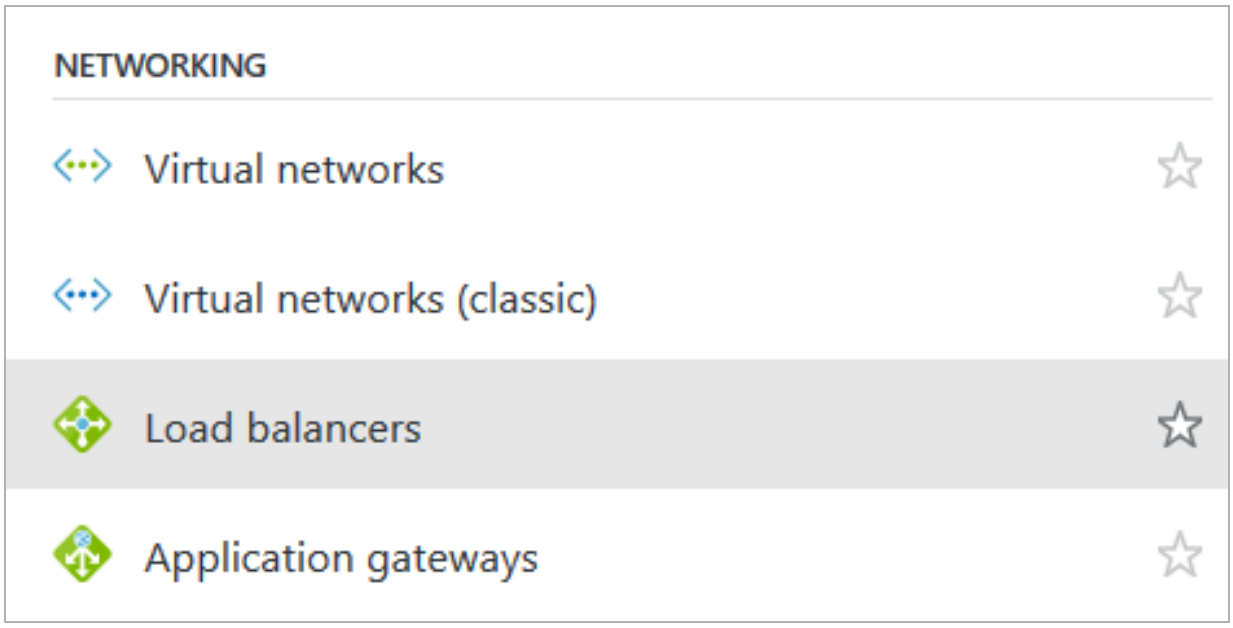
The following procedure describes how to set up an Azure Load Balancer from the Microsoft Azure portal:

> The steps below are carried out from http://portal.azure.com and not from http://manage.windowsazure.com.

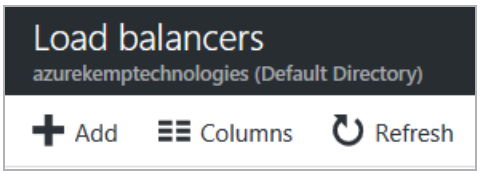


1. From the Azure Management Portal dashboard, click the **More services** icon.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

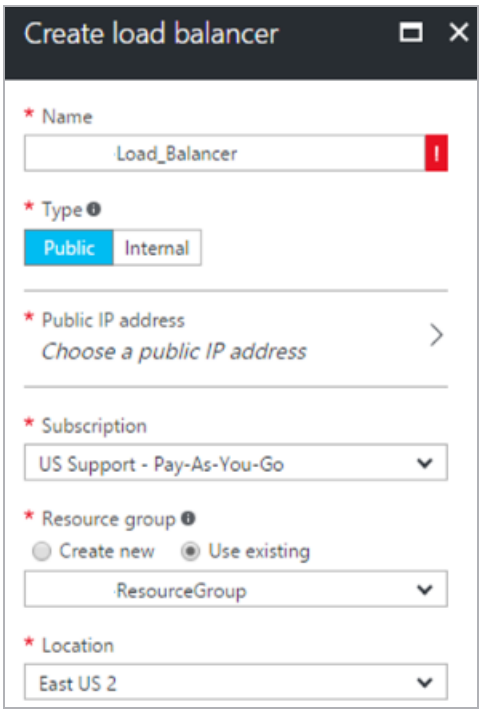


2. Select **Load balancers**.



3. Click **Add**.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved



4. Provide the necessary information for the Load Balancer:

    a) Assign the Load Balancer a **Name**.

    b) Select whether or not the Load Balancer is made available to the Internet (**Public** or **Internal**).

    c) If you chose **Public** as the **Type**:

        i. Click **Choose a public IP address**.

        ii. Click **Create new**.

        iii. Enter a **Name**.

        iv. Select the **Assignment** type.

        v. Click **OK**.

    d) Assign the same **Resource group** as the LoadMasters.

    e) Select the **Location**.

5. Click **Create**.

It may take some time for the ILB to propagate.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

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

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

5 Configure the Azure Load Balancer

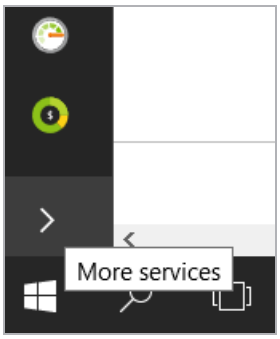
There are several settings that need to be configured to provide the high availability of the LoadMasters.

- Create a backend 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 Backend Pool

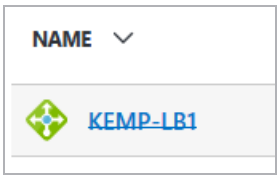
The Backend Pool is a collection of virtual machines (LoadMasters) which is load balanced to provide High Availability.



1. In the left hand navigation, click the **More services** icon.

2. Select **Load balancers**.

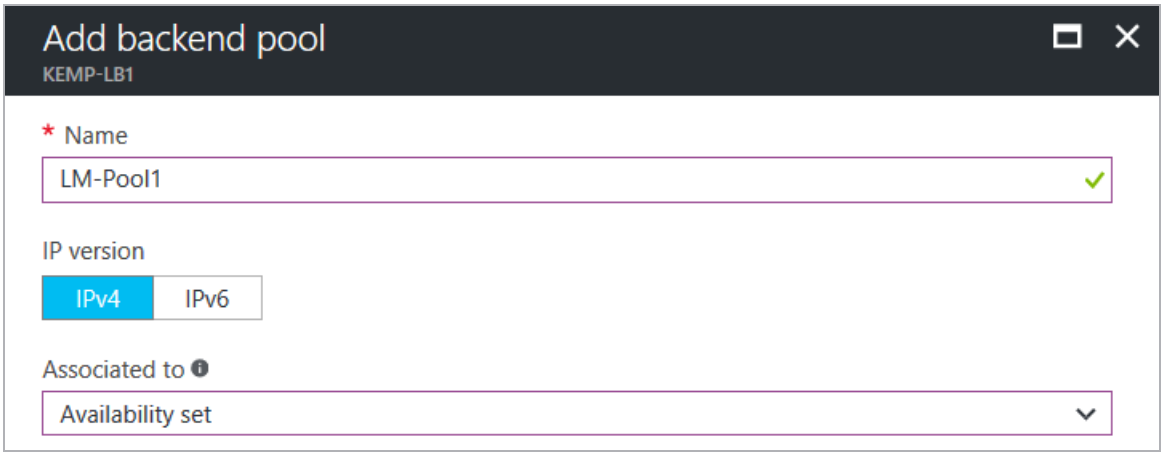
 Copyright 2002-2019, Kemp Technologies, All Rights Reserved



3. Click the name of the internal load balancer that was created in the **Create the Internal Load Balancer (ILB)** section.

4. Click **Backend pools**.

5. Click **Add**.



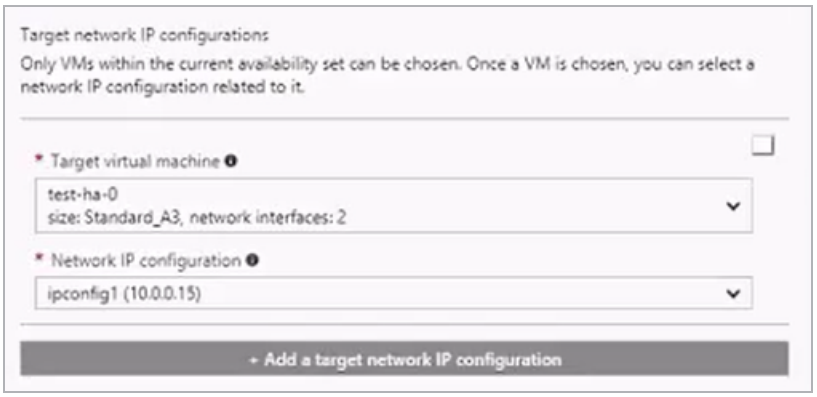
6. Provide a **Name** for the Backend Pool.

7. Click **Availability set** in the **Associated to** drop-down list.

8. Select the relevant **Availability set**.

9. Click **Add a target network IP configuration**.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved



10. Select the master LoadMaster in the **Target virtual machine** drop-down list.
11. As multiple Network Interface Cards (NICs) are supported, you must select the relevant NIC in the **Network IP configuration** drop-down list.
12. Click **OK**.
13. Click **Add a target network IP configuration** to add the other machine.
14. Select the slave LoadMaster in the **Target virtual machine** drop-down list.
15. Select the relevant NIC in the **Network IP configuration** drop-down list.
16. Click **OK**.

It takes some time to propagate the information.

VIRTUAL MACHINE	STATUS	NETWORK INTERFACE	PRIVATE IP ADDRESS
backend (2 virtual machines)			
test-ha-0	Running	test-ha-0-nic0	10.0.0.15
test-ha-1	Running	test-ha-1-nic0	10.0.0.20

When finished, you can see the two machines in the backend 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

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

> 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. 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.

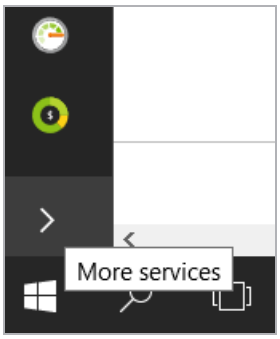
Inbound NAT rules provide a translation for management access into each of the LoadMasters in the Backend pool. Each LoadMaster does not require a Public IP Address (PIP). A unique port must be configured in an Inbound NAT rule for each LoadMaster. The example rules are the following:

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.

5.3 Create a Probe to Monitor LoadMaster Health

A probe must be created to monitor the health of the LoadMasters. This probe will determine which LoadMaster is active and send the necessary traffic. Should that LoadMaster go offline, the probe will take that LoadMaster out of service and direct all traffic to the secondary LoadMaster.



 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

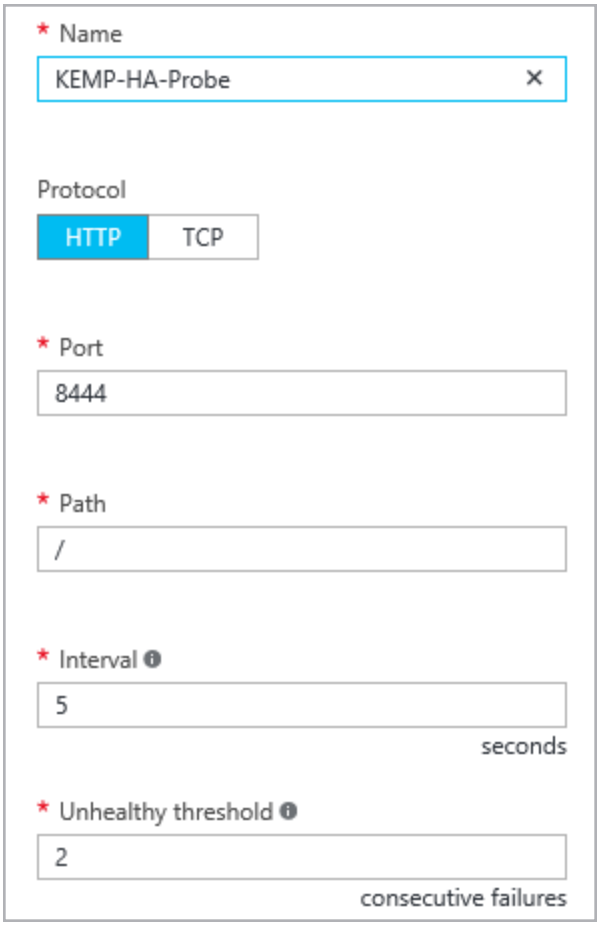
1. In the left hand navigation click the **More services** icon.

2. Click **Load balancers**.

3. Select the load balancer that was create in the **Create the Internal Load Balancer (ILB)** section.

4. Select **Health probes**.

5. Click **Add**.



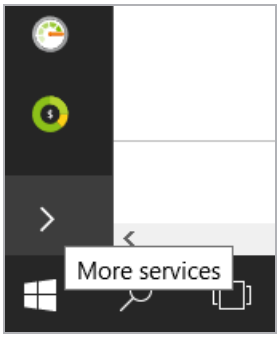
6. Provide the following information:

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

7. Provide a **Name**.
8. Select **HTTP** as the **Protocol**.
9. Enter **8444** as the **Port**.
10. Enter **/** as the **Path**.
11. Enter **5** as the **Interval**.
12. Enter **2** as the **Unhealthy threshold**.
13. Click **OK**.

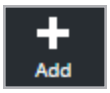
5.4 Create Load Balancing Rules to Allow Traffic

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.



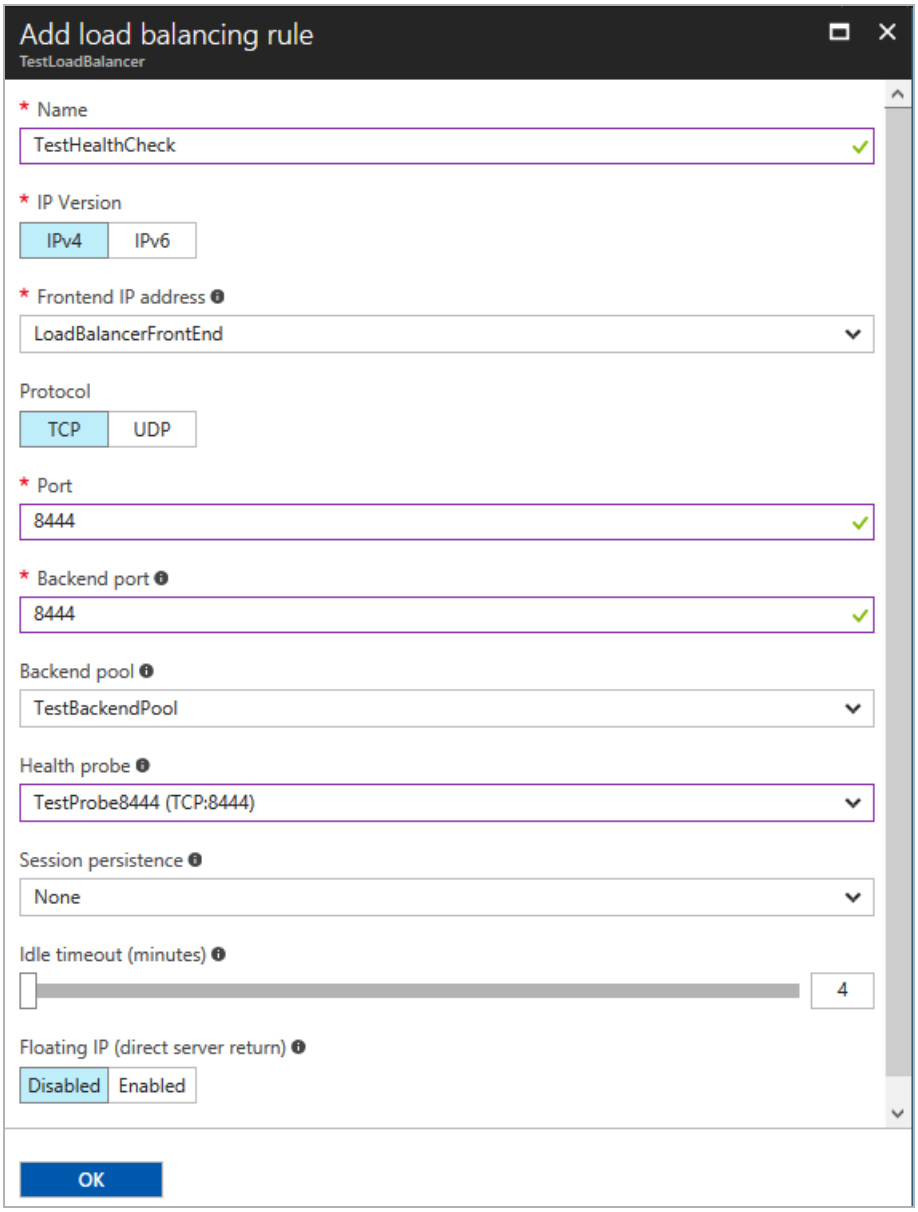
1. In the left hand navigation, click the **More services** icon.

2. Select **Load balancers**.
3. Select the load balancer that was created in the **Create the Internal Load Balancer (ILB)** section.
4. Click **Load balancing rules**.



5. Click **Add**.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved



6. Provide the following information:

    a) Provide a **Name**.

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

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

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

    e) Select your **Backend pool**.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

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

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

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

7. Click **OK**.

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

 Copyright 2002-2019, Kemp Technologies, 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.

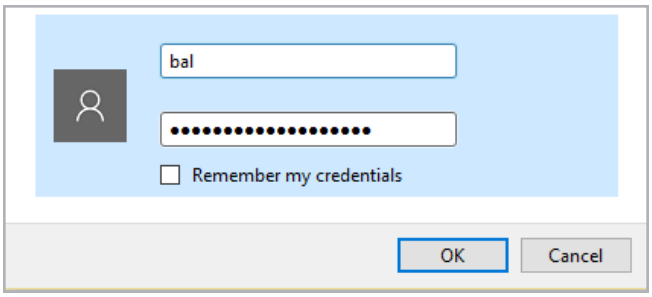
The security group must contain a rule for 8443. This is the WUI port. If the LoadMaster is public-facing, other best practice, recommended (but not mandatory) ports that should be in the security group, are; 8441, 8442, 8444, 22, 221, 222, the Virtual Service ports (such as 80) and any other ports that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

Do not block port 6973.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

7 Configure the LoadMasters

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



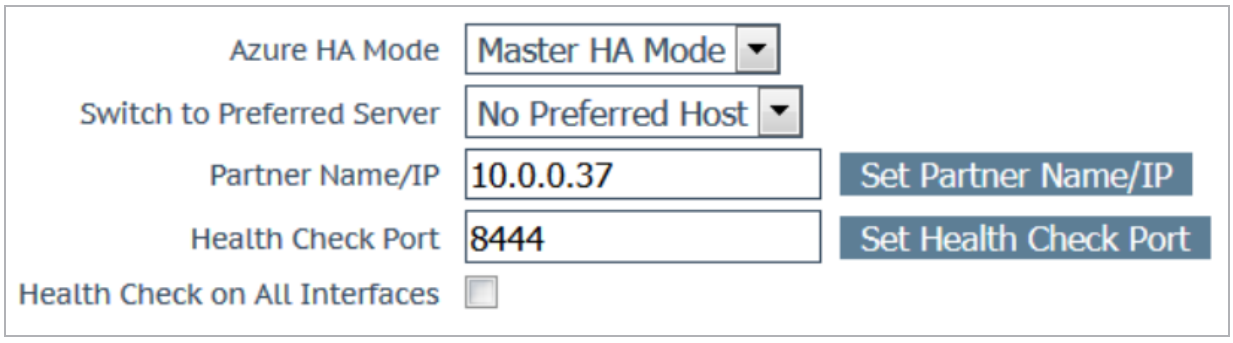
1. If the LoadMaster does not have a public address itself and you are going through the Internal Load Balancer (ILB), you can access the WUI of the LoadMaster which is the master unit:

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

    b) Access the WUI of the slave 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 **Master HA Mode** in the **Azure HA Mode** drop-down list.

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

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

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

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

5. Enter the internal address of the slave 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 master and slave 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.

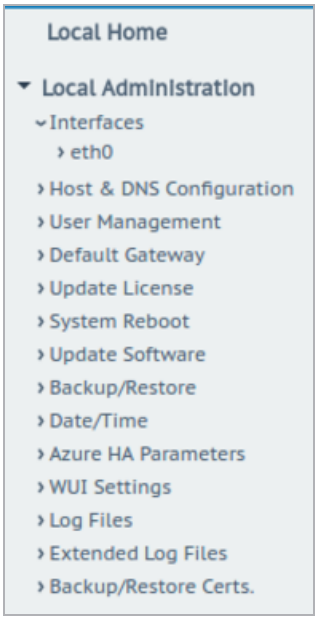
8. Then, access the WUI of the slave unit. Complete the following steps in the slave unit, but select Slave HA Mode as the Azure HA Mode instead: **In the main menu, go to System Configuration > Azure HA Parameters.** to **Enter the internal address of the slave LoadMaster unit in the Partner Name/IP 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 master unit is replicated to the slave.

 Copyright 2002-2019, Kemp Technologies, 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 the master, and which is the slave, 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 master LoadMaster and it is currently active.
	This is the slave LoadMaster and it is currently active.
	This is the slave unit and it is currently the standby unit.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

8 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.

8.1 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 Slave unit may failback over to the Master unit.

After these steps are completed the upgrade is finished.

8.2 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.

 Copyright 2002-2019, Kemp Technologies, 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 Slave unit may failback over to the Master unit.

After these steps are completed the downgrade is finished.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

9 Troubleshooting

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

9.1 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 "Master/Slave 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/

9.2 Master/Slave Unconnected

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

The slave unit should show **SLAVE**.

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

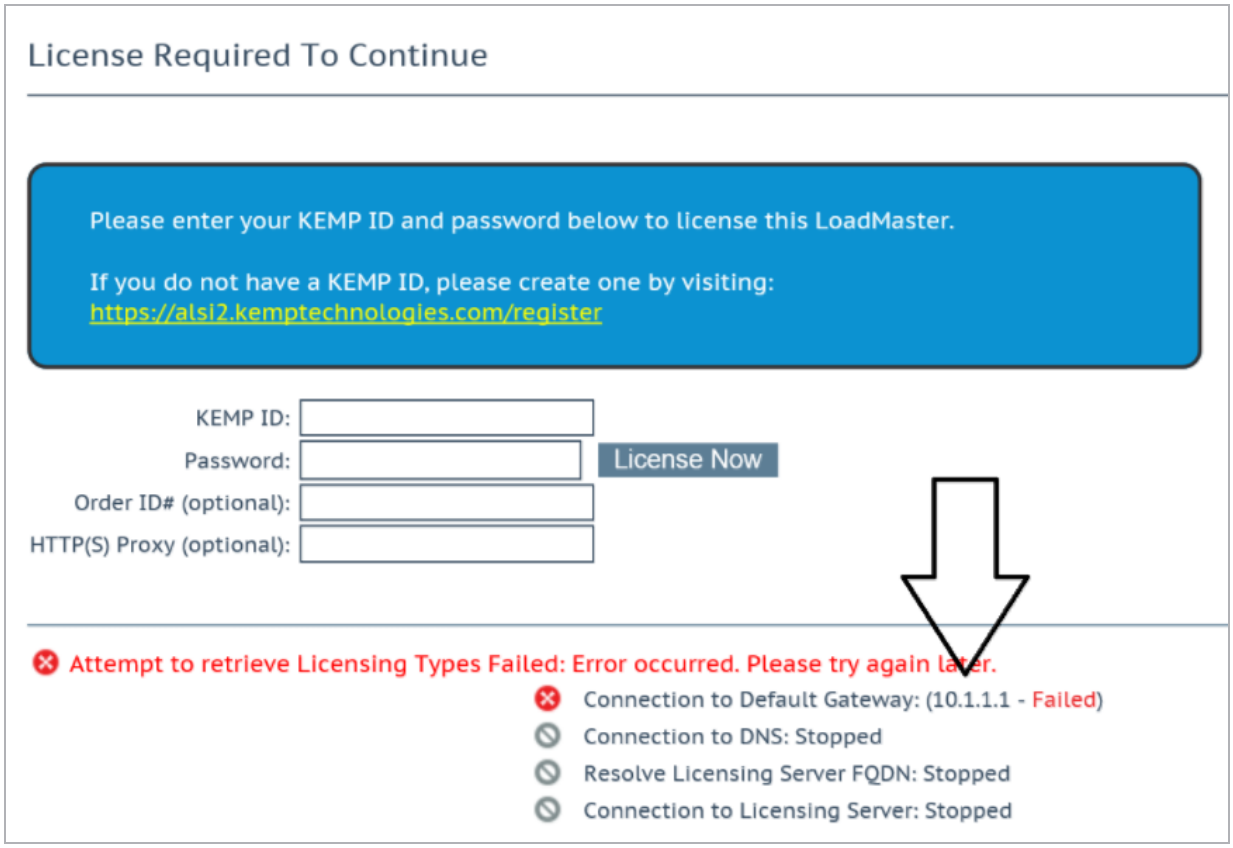
- Master to Master Unconnected
- Slave to Slave Unconnected

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:

- Master Unconnected to Master (Active)/Master (Standby)
- Slave (Unconnected) to Slave (Active)/Slave (Standby)

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

9.3 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.

9.4 Virtual Machine Inaccessible

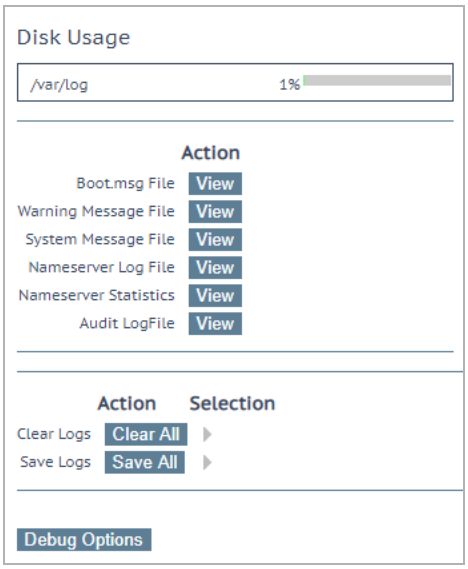
It takes approximately five minutes for the Virtual Machine to become accessible after booting.

9.5 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 > Logging Options > System Log Files**.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved



2. Click **Debug Options**.
3. In the **TCP dump** section, enter the relevant IP **Address** and the Azure HA **Port**.
4. Click **Start**.
5. Let the capture run for a few minutes.
6. Click **Stop**.
7. Click **Download**.
8. 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.

9.6 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.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

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.

9.7 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 "Master/Slave 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.

9.8 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.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

References

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

Licensing, Feature Description

LoadMaster for Azure, Feature Description

HA for Azure (Classic Interface), Feature Description

Azure Virtual Machines – tutorials and guides:

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

High Availability (HA), Feature Description

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved

Last Updated Date

This document was last updated on 31 January 2019.

 Copyright 2002-2019, Kemp Technologies, All Rights Reserved