HA for Azure Classic Interface

Feature Description

UPDATED: 31 January 2019

Copyright Notices

Table of Contents

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 **Classic** method. For steps using the **Resource Manager** method, please refer to the **HA for Azure Resource Manager, Feature Description**.

When deploying an application using the Microsoft Azure Infrastructure as a Service (IaaS) offering, chances are you 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). When using Kemp's LoadMaster for Azure, you can not only address your needs of application delivery but also of 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.

2 Using LoadMaster HA for Azure

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

    - 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

    - Interface bonding

- Additional routes

- The cloud HA LoadMaster does not have a “force update” option.
- If the master unit fails, connections are directed to the slave unit. The master unit is the master and will never become the slave, even if it fails. Similarly, the slave unit will never become the master. When the master unit comes back up, connections will automatically be directed to the master again.
- The **HA Check Port** must be set to the same port on both the master and slave units for HA to work correctly.

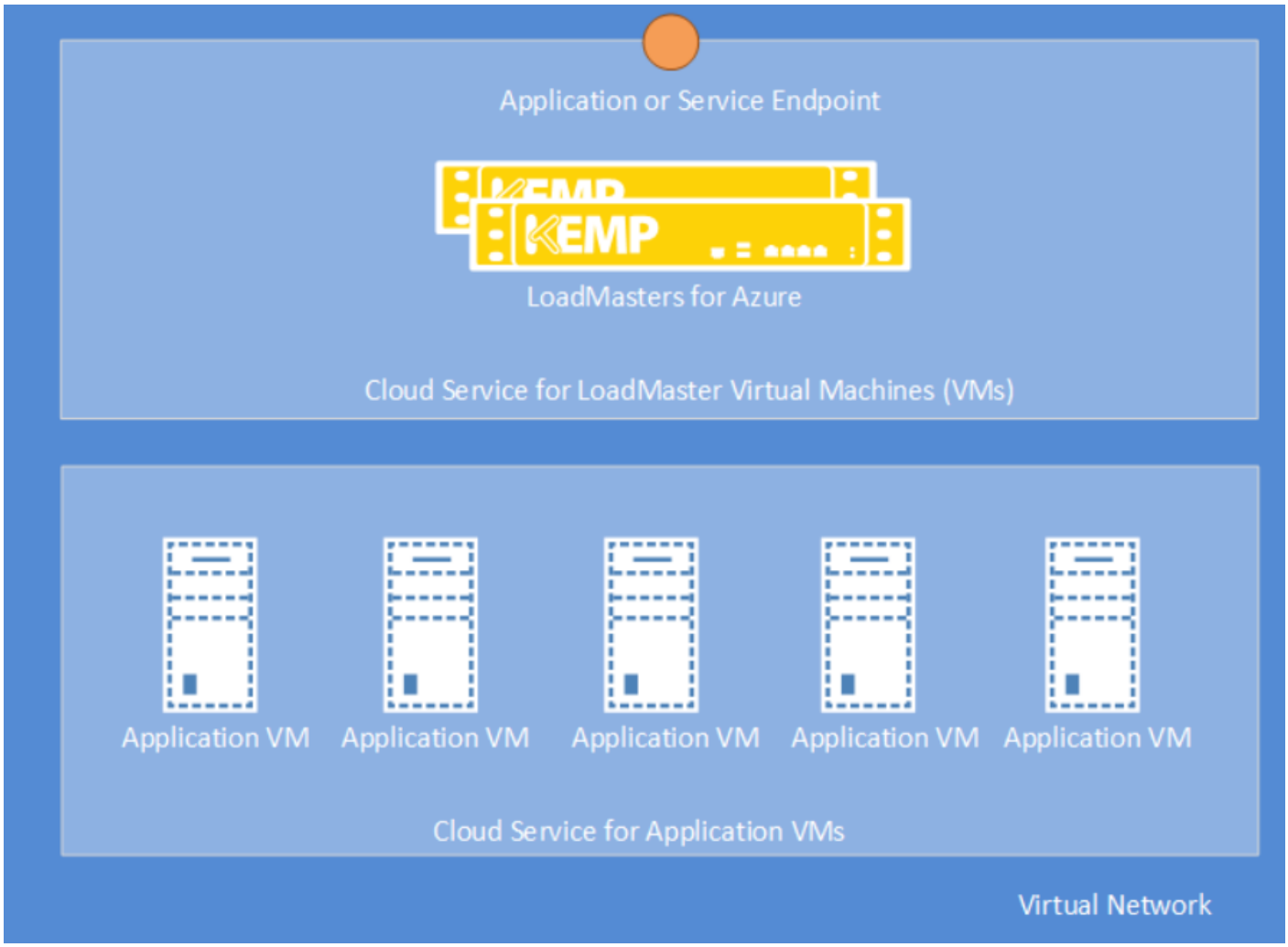
A complete description of non-cloud LoadMaster HA can be found in the **High Availability (HA), Feature Description** document.

3 Prerequisites

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

- A Virtual Network added to Azure to place the LoadMaster VMs
- Application VMs deployed in Azure in a Virtual Network
    - Application VMs may be configured to use single Cloud Service with no application endpoints created
    - Application endpoints are created on Cloud Services for LoadMaster VMs
    - Application VM management endpoints can be created if VPN is not used
- Two LoadMaster VMs deployed in Azure on same Virtual Network as Application VMs
    - Each published as part of the same cloud service
    - Both LoadMasters should be configured to be part of an availability set

The following diagram provides overview of 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
- Virtual Services for applications are created on both LoadMaster VMs
- Service Endpoints are created on Cloud Services for LoadMaster VMs
- The HA Check Port must be set to the same port on both the master and slave units for HA to work correctly
- Following Management Endpoints are created on Cloud Services for LoadMaster VMs

  - TCP Port 22 for SSH access

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

- UDP Port 53 for inbound DNS queries to GEO LoadMaster

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	
Domain Name/ Cloud Service	
Password for LoadMasters	
Availability Set Name	
Resource Group Name	
Virtual Network	
Load Balance Set(s)	

It is not possible to bond interfaces on Azure LoadMasters.

4 Configure LoadMaster High Availability 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 ensure that the prerequisites documented in the earlier section are met.

4.1 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.

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

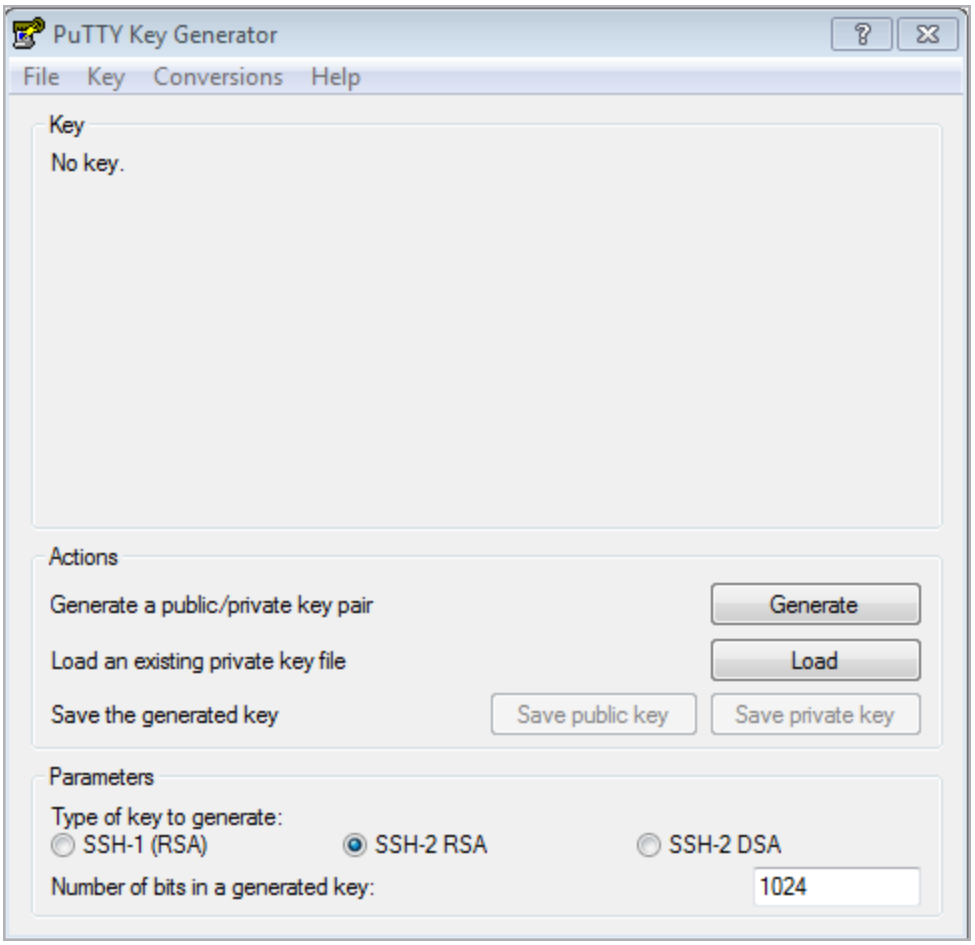
VLM Model	Recommended Pricing Tier
VLM-200	A1, A2, A3
VLM-2000	A2, A3, A4
VLM-5000	A3, A4, A5
VLM-10G	A7, A8, A9

4.2 Create an SSH Key Pair

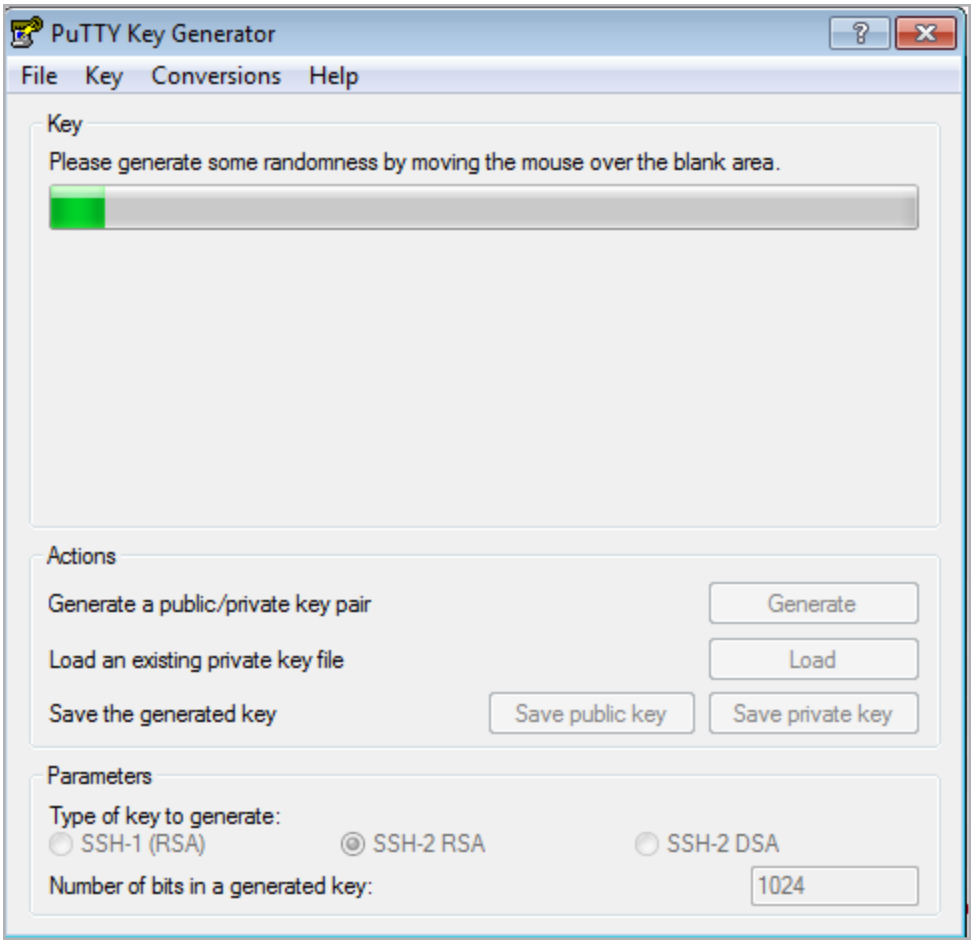
When creating a LoadMaster for Azure VM, there are two options for authentication - a password or an SSH public key. Kemp recommends using a password, but either way will work fine. If you choose to use a password, this section can be skipped and you can move on to the **Creating First Virtual LoadMaster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

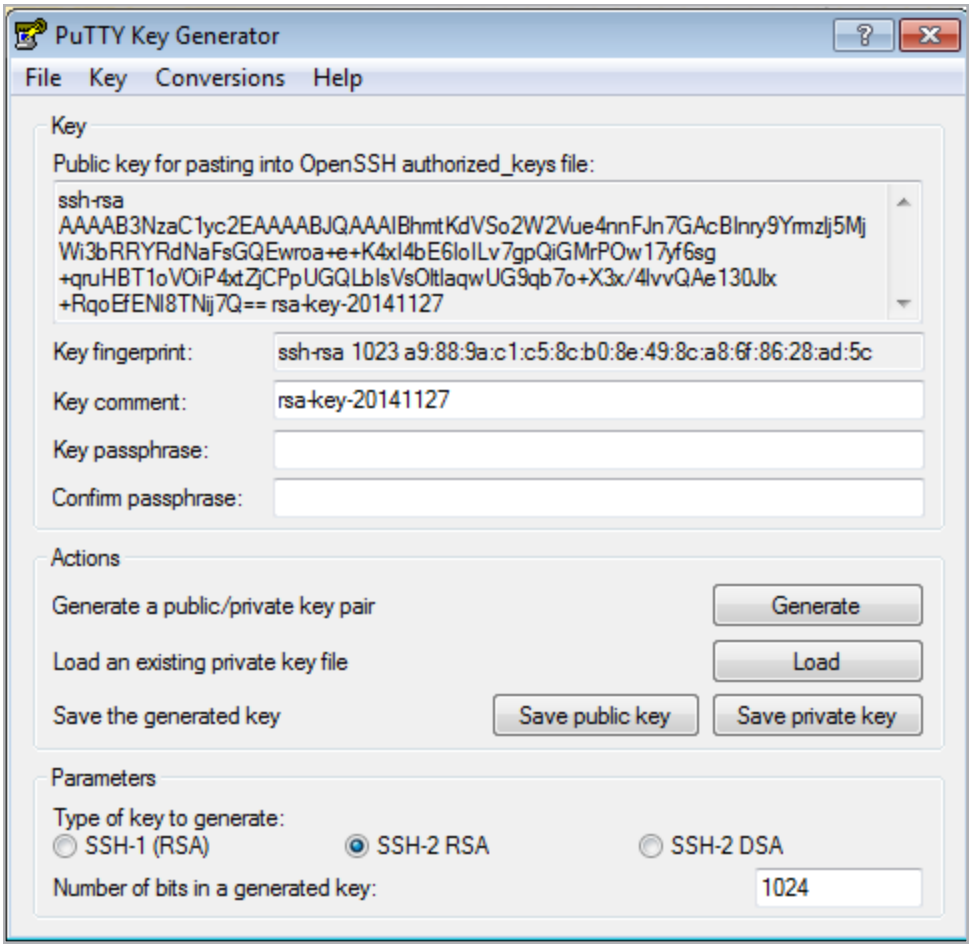
1. Open PuTTYgen.



2. Click **Generate**.



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



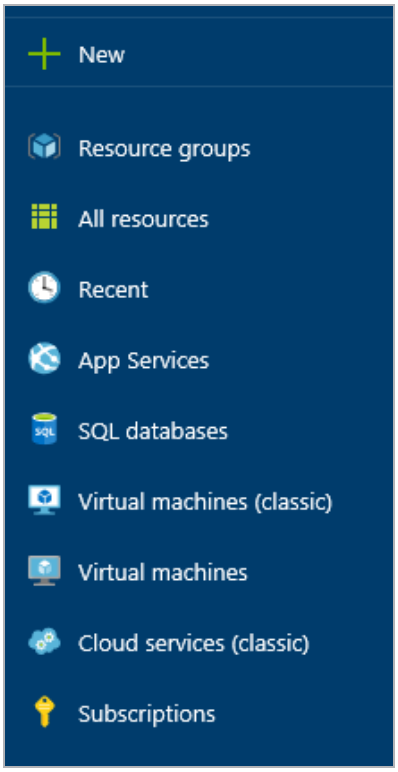
4. Copy and save the public and private key as needed.

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

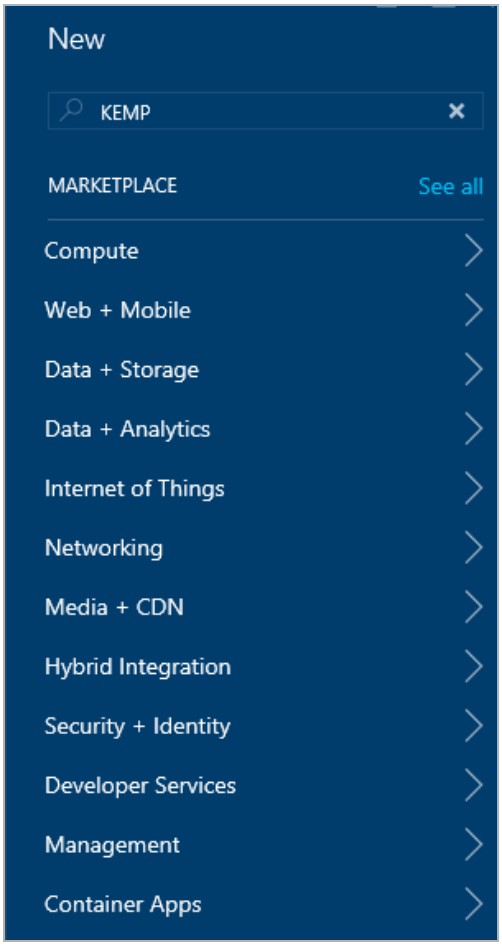
4.3 Creating First Virtual LoadMaster in Azure

The steps in this document are carried out in the Azure Portal (http://portal.azure.com).

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



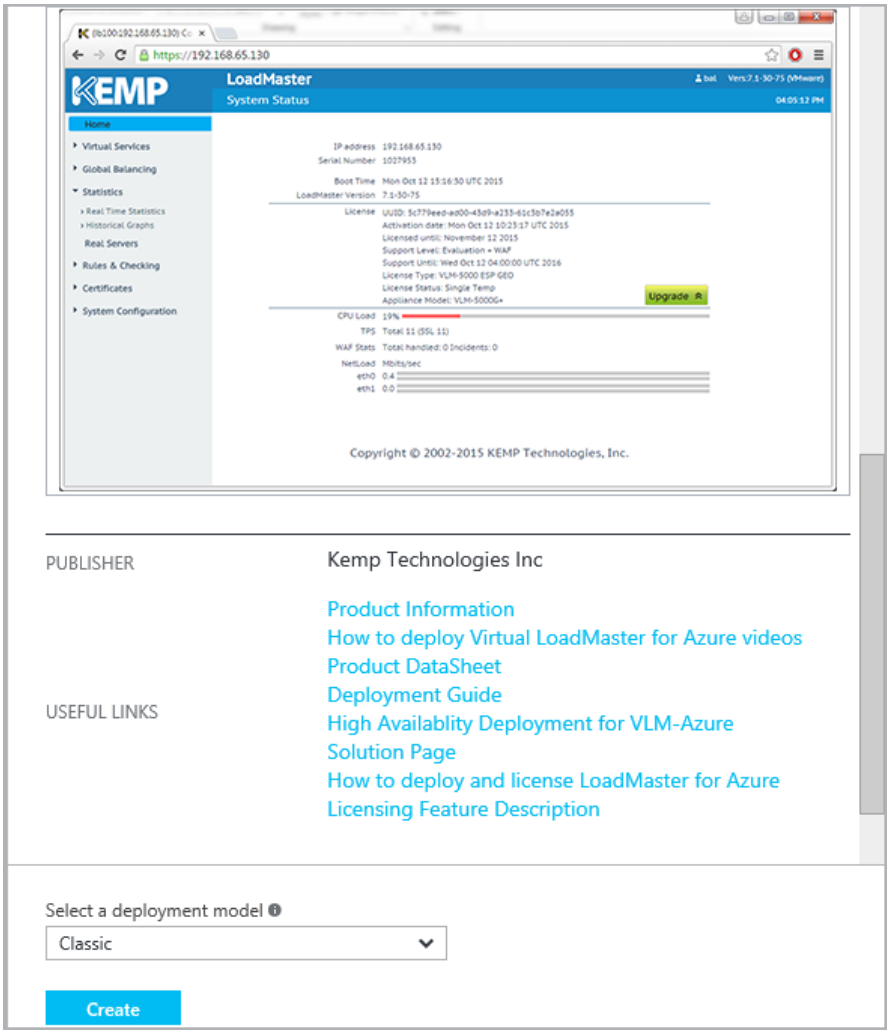
2. In the **Marketplace** section, click **New**.



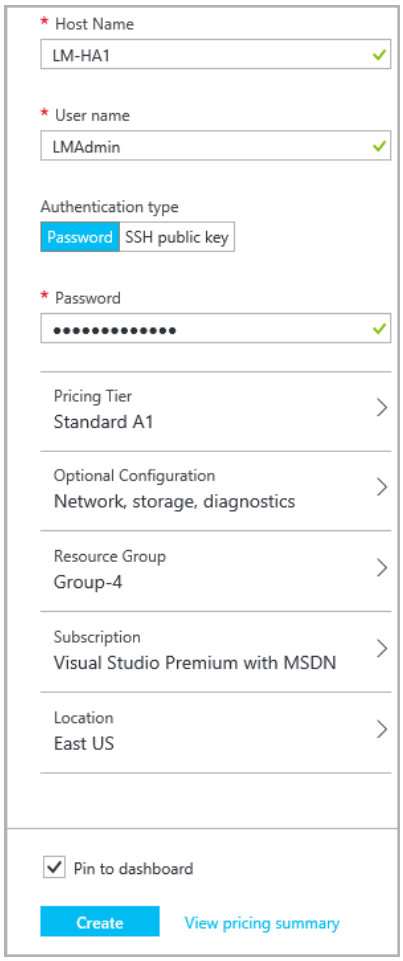
3. Type **Kemp** in the search field and **Enter**.

NAME	PUBLISHER	CATEGORY
10 Gbps KEMP VLM for Azure (Hourly Billing)	Kemp Technologies Inc	Compute
20 Mbps KEMP VLM for Azure (BYOL and Free)	Kemp Technologies Inc	Compute
200 Mbps KEMP VLM for Azure (Hourly Billing)	Kemp Technologies Inc	Compute
2 Gbps KEMP VLM for Azure (Hourly billing)	Kemp Technologies Inc	Compute
5 Gbps KEMP VLM for Azure (Hourly Billing)	Kemp Technologies Inc	Compute

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



5. Click **Create**.



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

    a) **Host Name**: Provide a unique name for VM identification

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

    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:

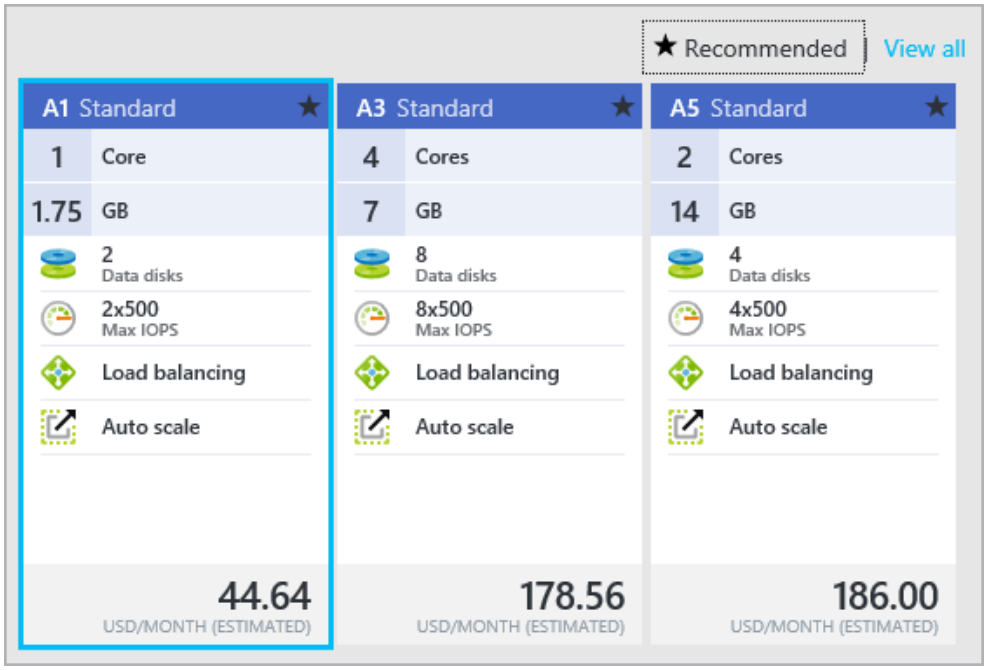
        - **Password:** Enter a password.

This password is used to access the LoadMaster WUI.

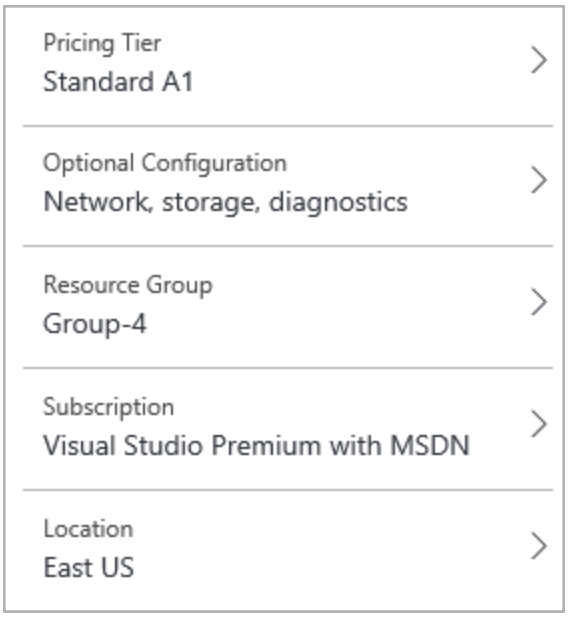
- **SSH Public Key:** Paste the SSH public key which was created in the **Create an SSH Key Pair** section. The private key is needed to connect to the LoadMaster using SSH.

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

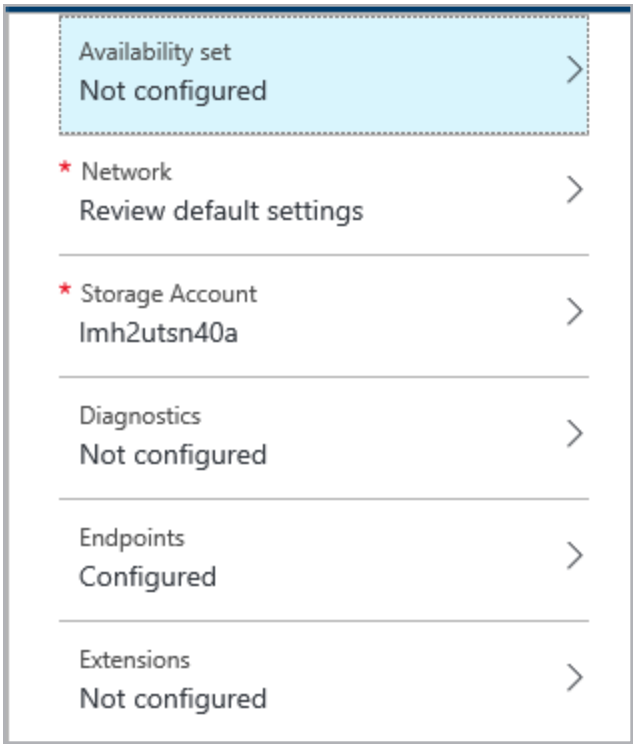
7. Click **Pricing Tier**.



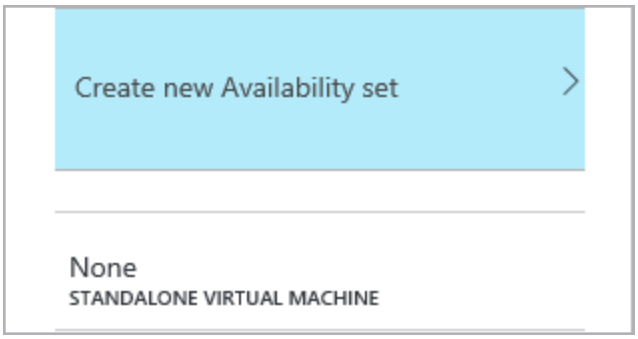
d) Select from the recommended pricing tiers. Select **View all** if the recommended pricing tier is not meeting the recommended requirements (see the **Recommended Pricing Tier** section for further information regarding what tier to select).



8. Select **Optional Configuration**.

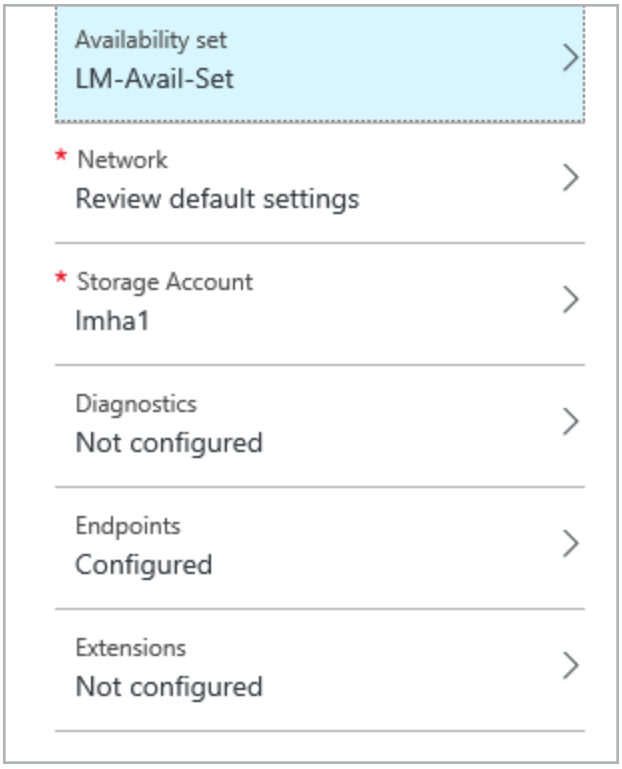


9. Select **Availability set**.

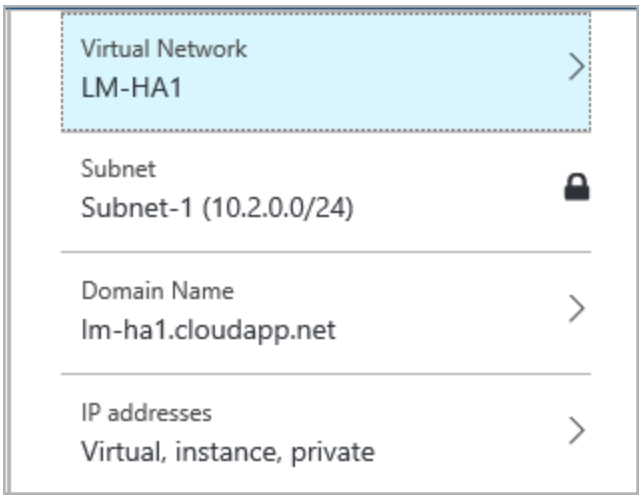


10. Select **Create new Availability set**.

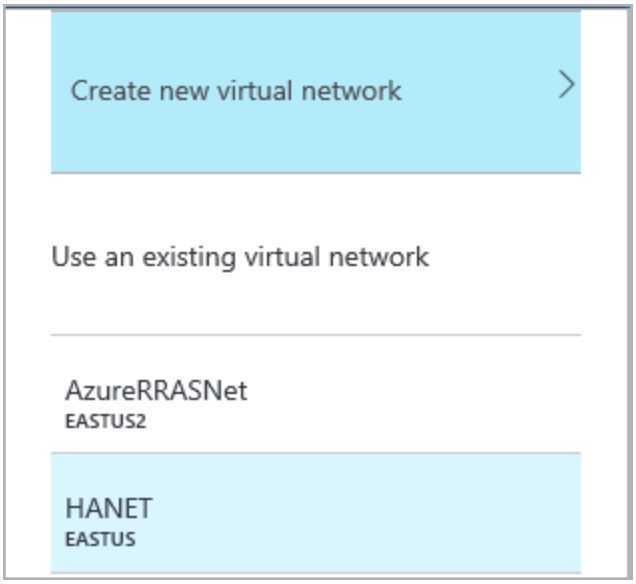
11. Provide a unique **Name** for the Availability Set.
12. Click **OK**.



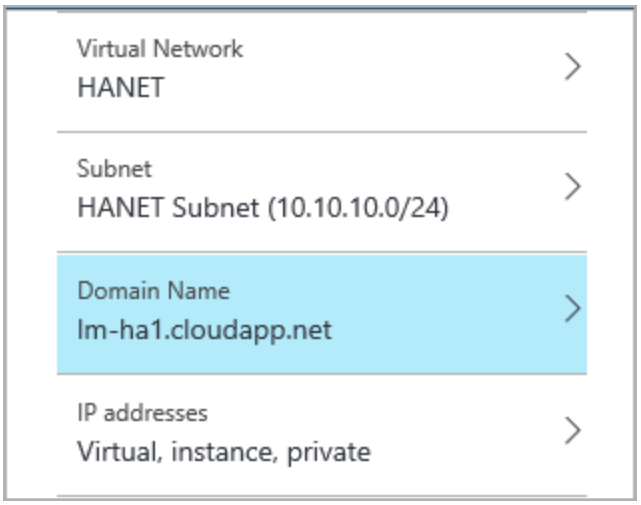
13. Select **Network**.



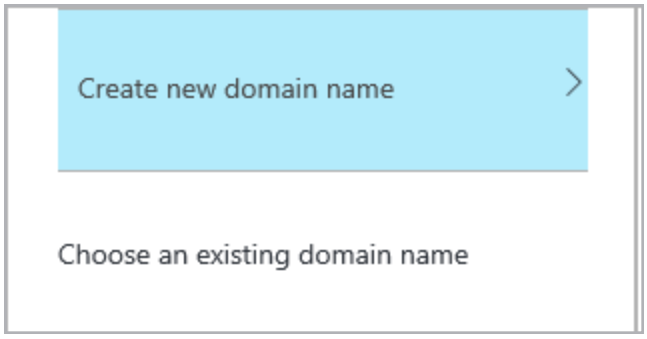
14. Select **Virtual Network**.



15. Select either **Create a new virtual network** or **Use an existing virtual network** based on the configuration of your Azure Environment.

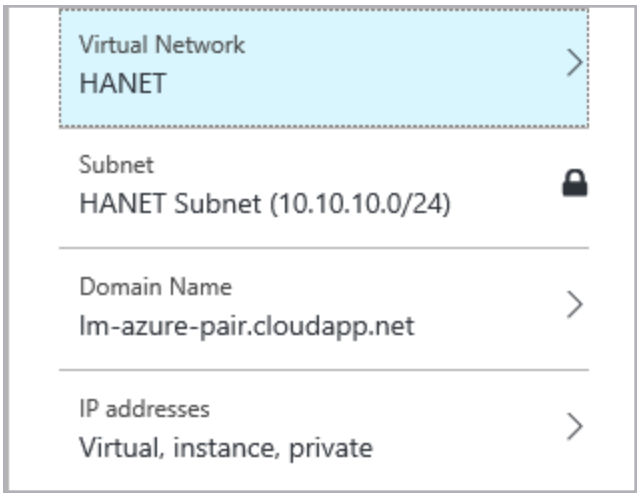


16. Select **Domain Name**.

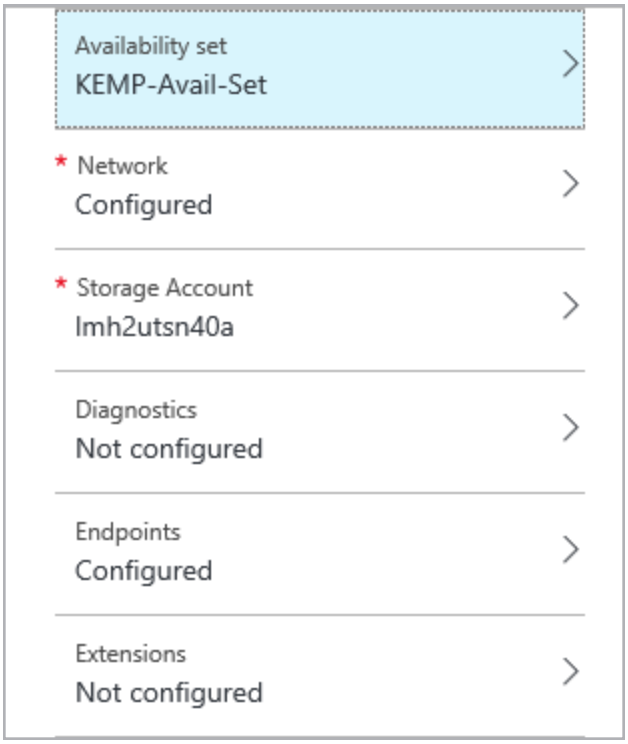


17. Select **Create new domain name**. This step will create a new Cloud Service.

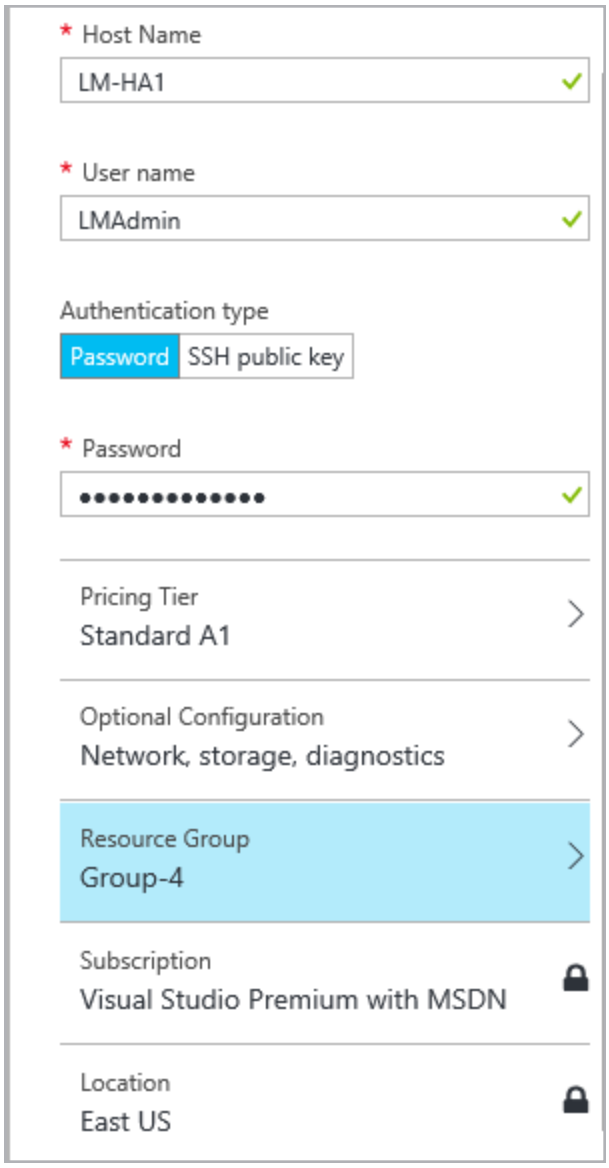
18. Provide a unique **Domain Name** for the new Cloud Service.
19. Click **OK**.



20. Confirm your settings and click **OK**.

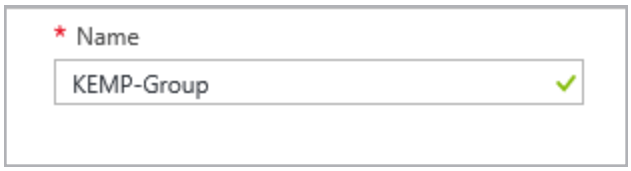


21. Click **OK** to close the **Optional Config**.

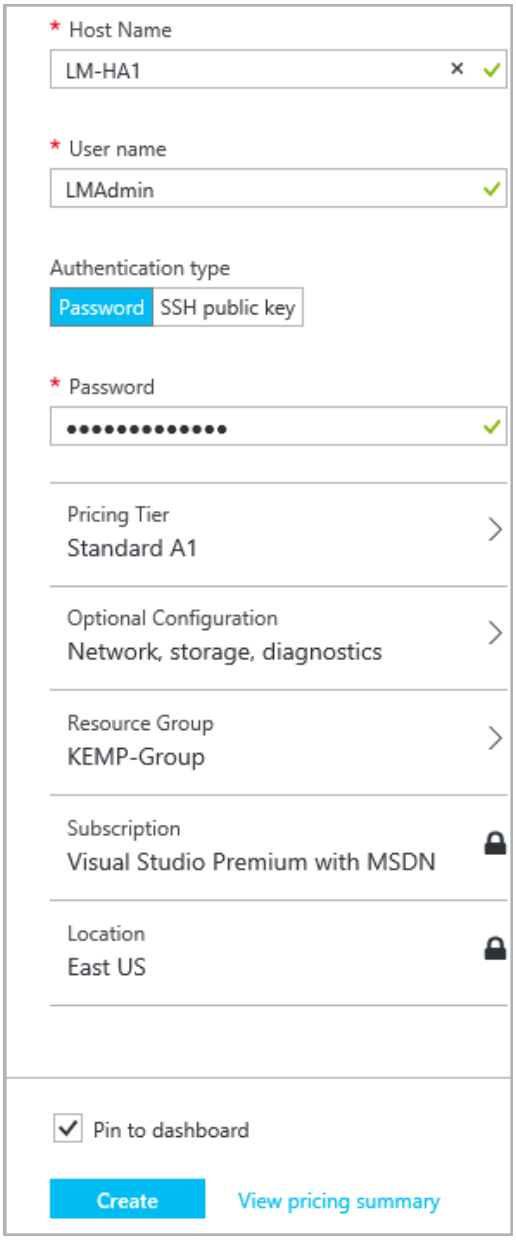


22. Select **Resource Group**.

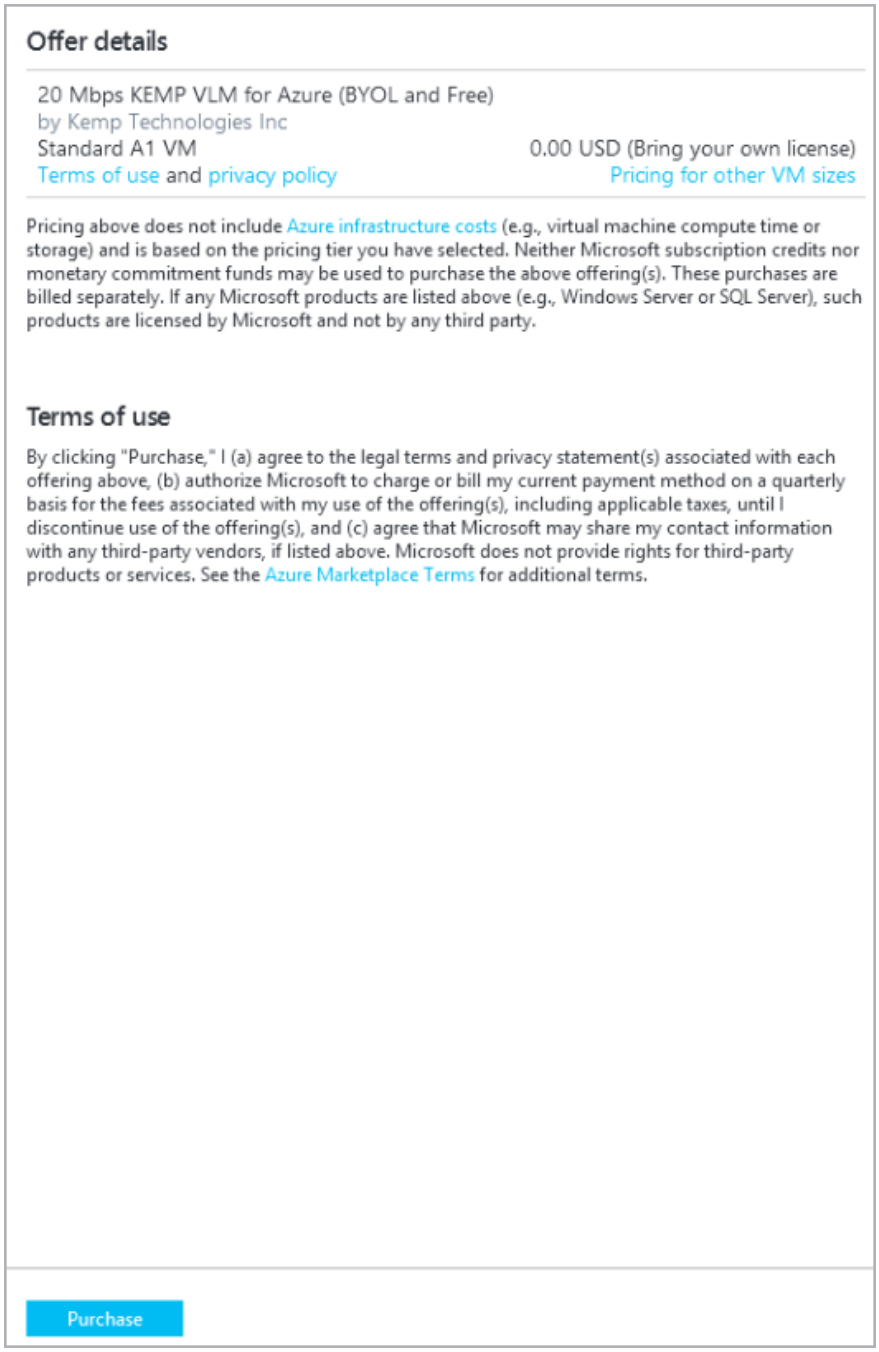
23. Select **Create a new resource group**.



24. Provide a unique **Name** for the Resource Group.
25. Click **OK**.



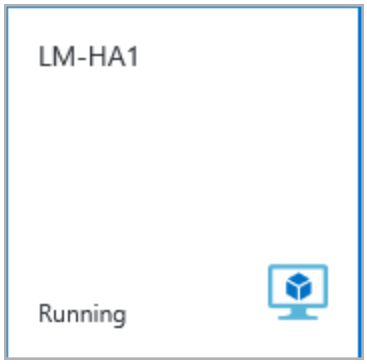
26. Click **Create**.



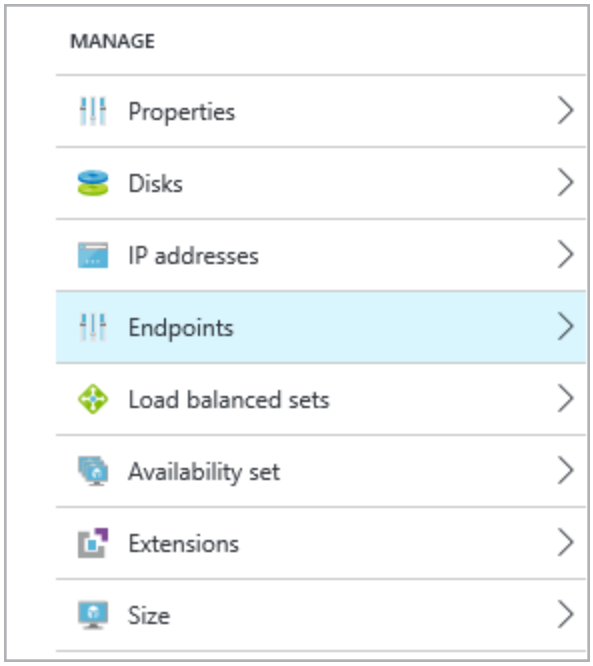
27. In the **Purchase** section, click **Purchase** to start creation of the LoadMaster for Azure Virtual Machine.

4.3.1 Configure the End Points on first LoadMaster

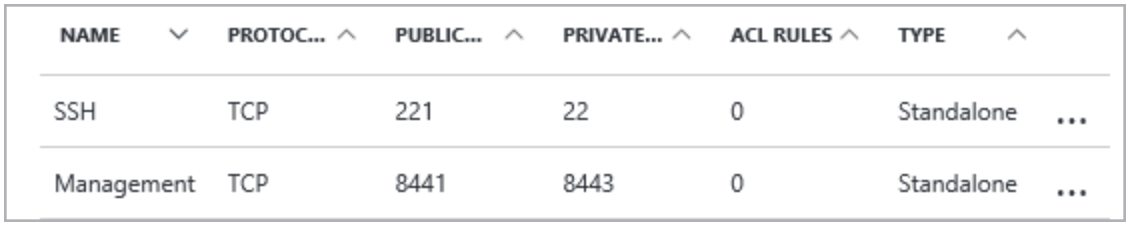
End points for port 22 and 8443 are automatically created. In a HA configuration, the ports need to be changed. To do this, follow the steps below after the LoadMaster VM has been created:



1. Click the VM on the Azure portal home page.



2. Click **Endpoints**.



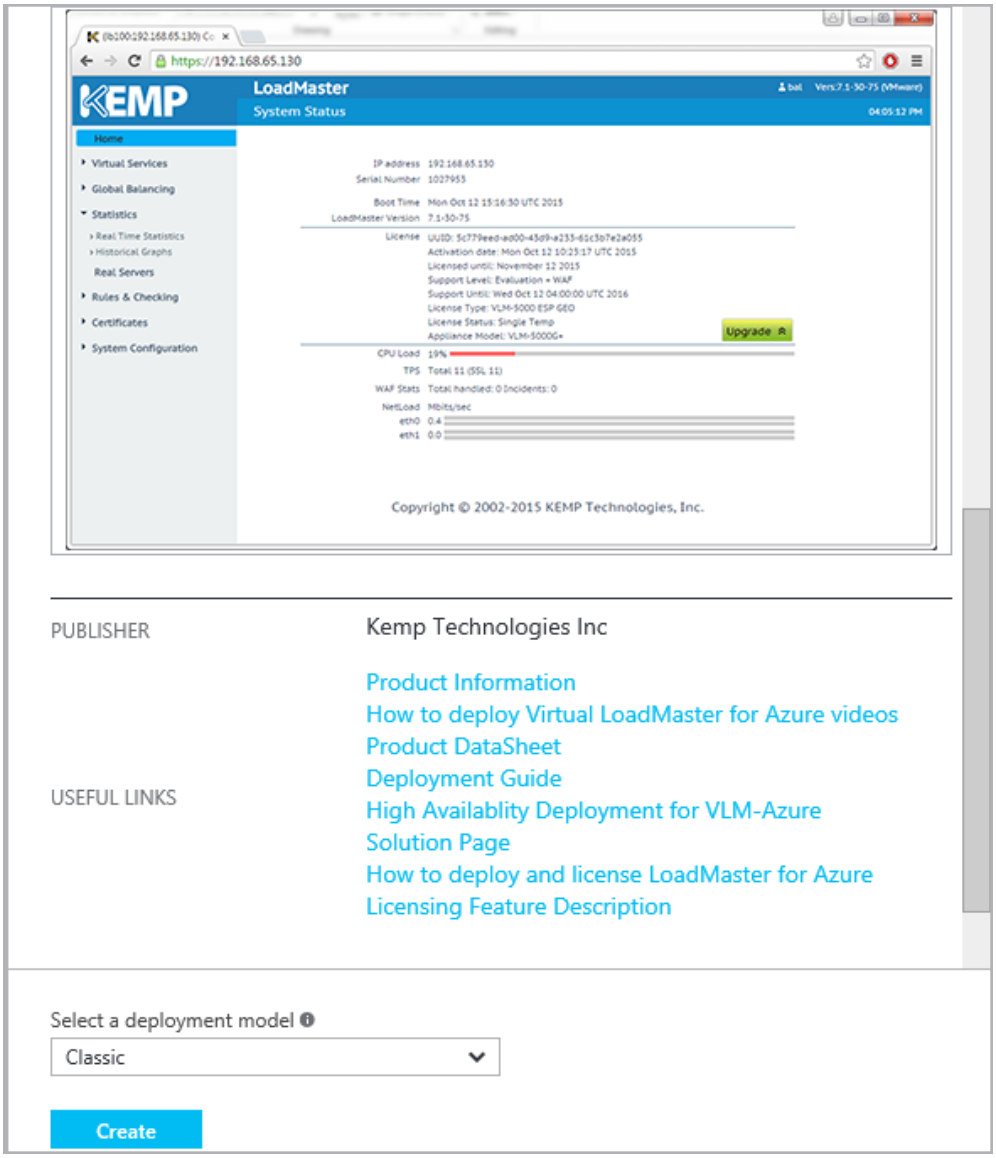
NAME	PROTOC...	PUBLIC...	PRIVATE...	ACL RULES	TYPE	
SSH	TCP	221	22	0	Standalone	...
Management	TCP	8441	8443	0	Standalone	...

3. Select the first end point.
4. Change the public port to **221**.
5. Change the private port to **22**.
6. Click **Save**.
7. Select the second end point.
8. Change the public port to **8441**.
9. Change the private port to **8443**.
10. Click **Save**.

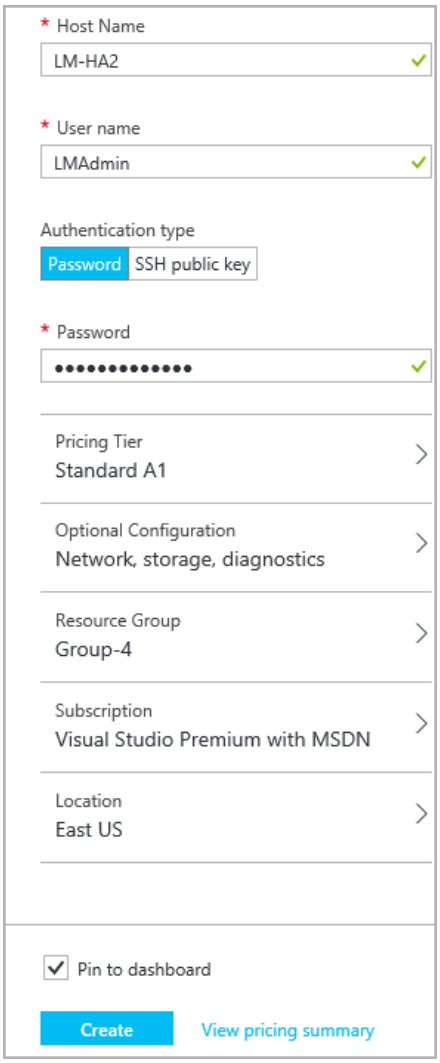
4.4 Create the Second LoadMaster in Azure

The process of setting up the second LoadMaster for Azure is similar to the first with a few exceptions.

1. Search for Kemp and Select the same LoadMaster that was used to create the LoadMaster in the **Creating First Virtual LoadMaster in Azure** section.



2. Click **Create**.



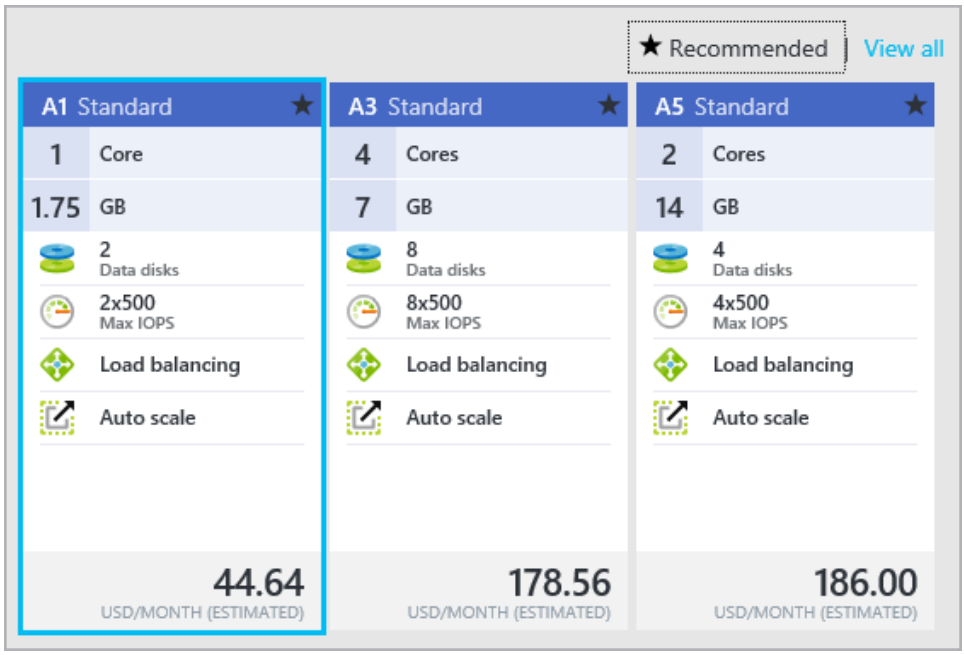
3. Provide details in the **Create VM** section. The details required to create new VM are:

   a) **Host Name**: Provide a unique name for VM identification

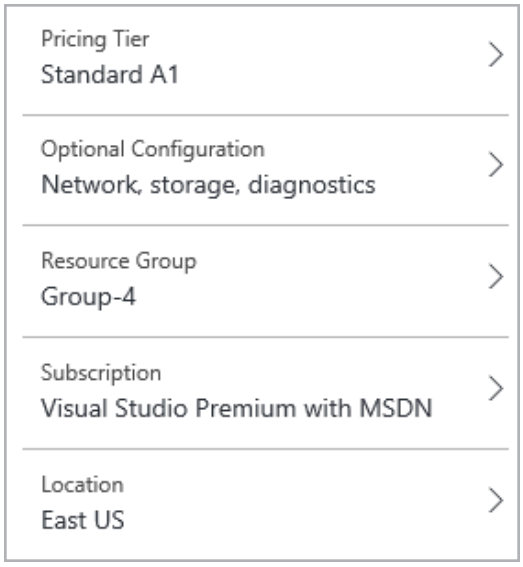
   b) **User Name**: This will not be used by LoadMaster for Azure. Provide a name of your choice.

   - Use the same authentication that was utilized when created the first Virtual LoadMaster in the **Creating First Virtual LoadMaster in Azure** section.

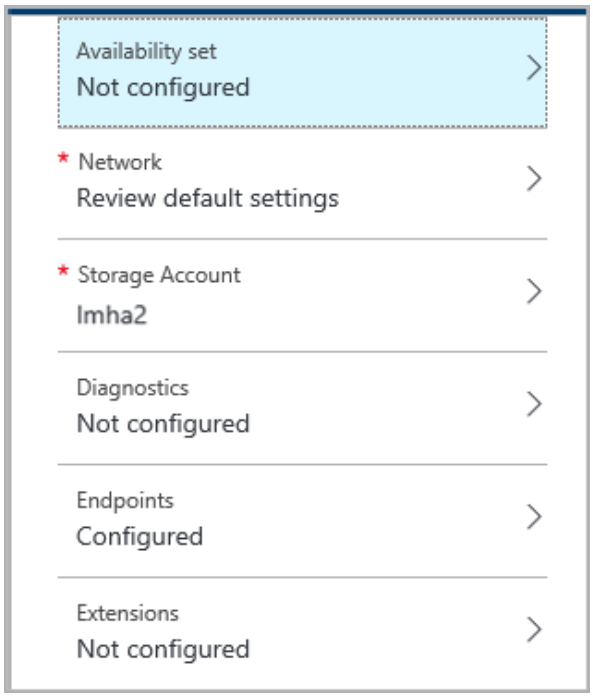
4. Click **Pricing Tier**.



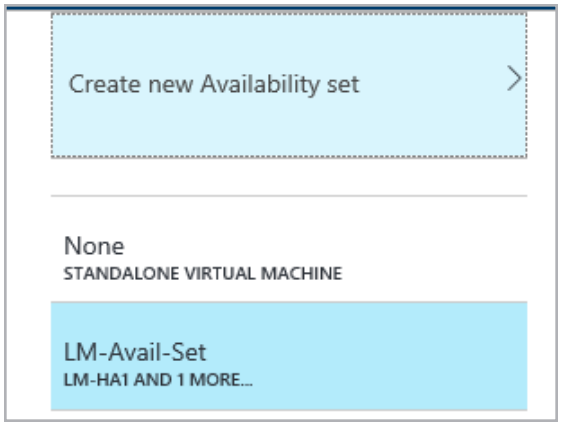
c) Select the same Pricing Tier that was used when creating the first Virtual LoadMaster in the **Creating First Virtual LoadMaster in Azure** section.



5. Select **Optional Configuration**.

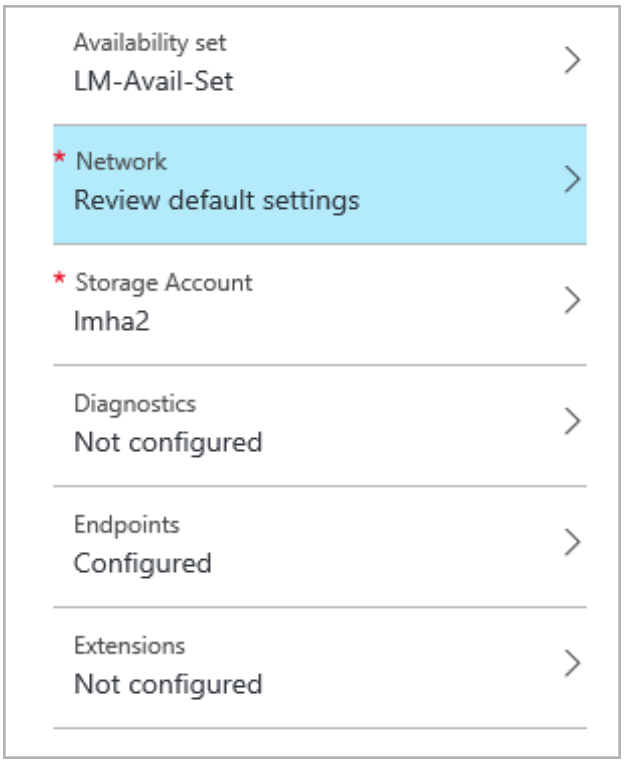


6. Select **Availability set**.

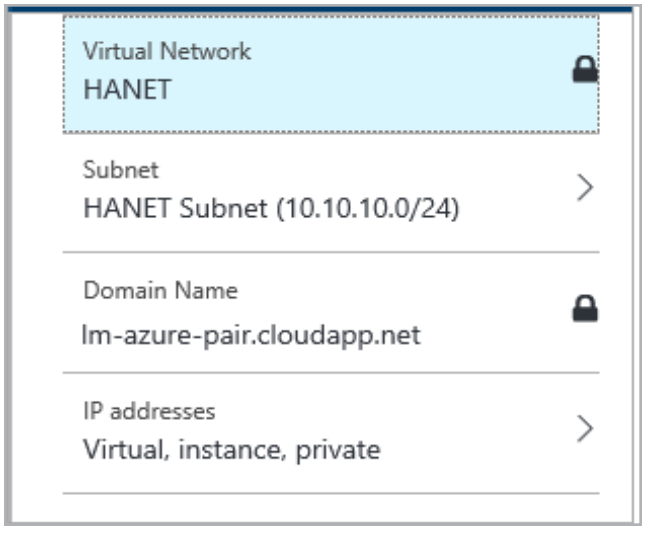


7. Select the Availability Set which was created during the creation of the first LoadMaster for Azure.

8. Click **OK**.

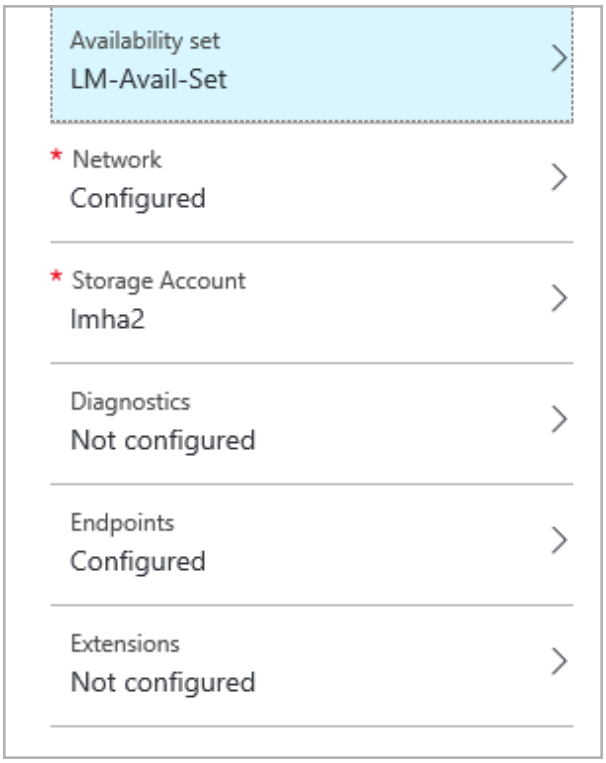


9. Select **Network**.

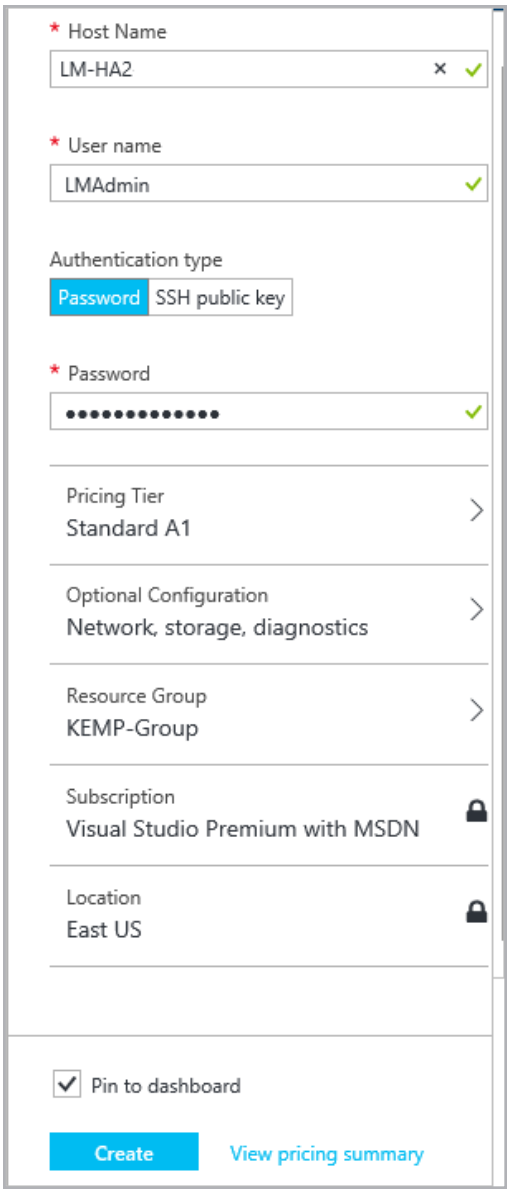


10. The Network Settings should be populated with the required settings based on the Availability Set.

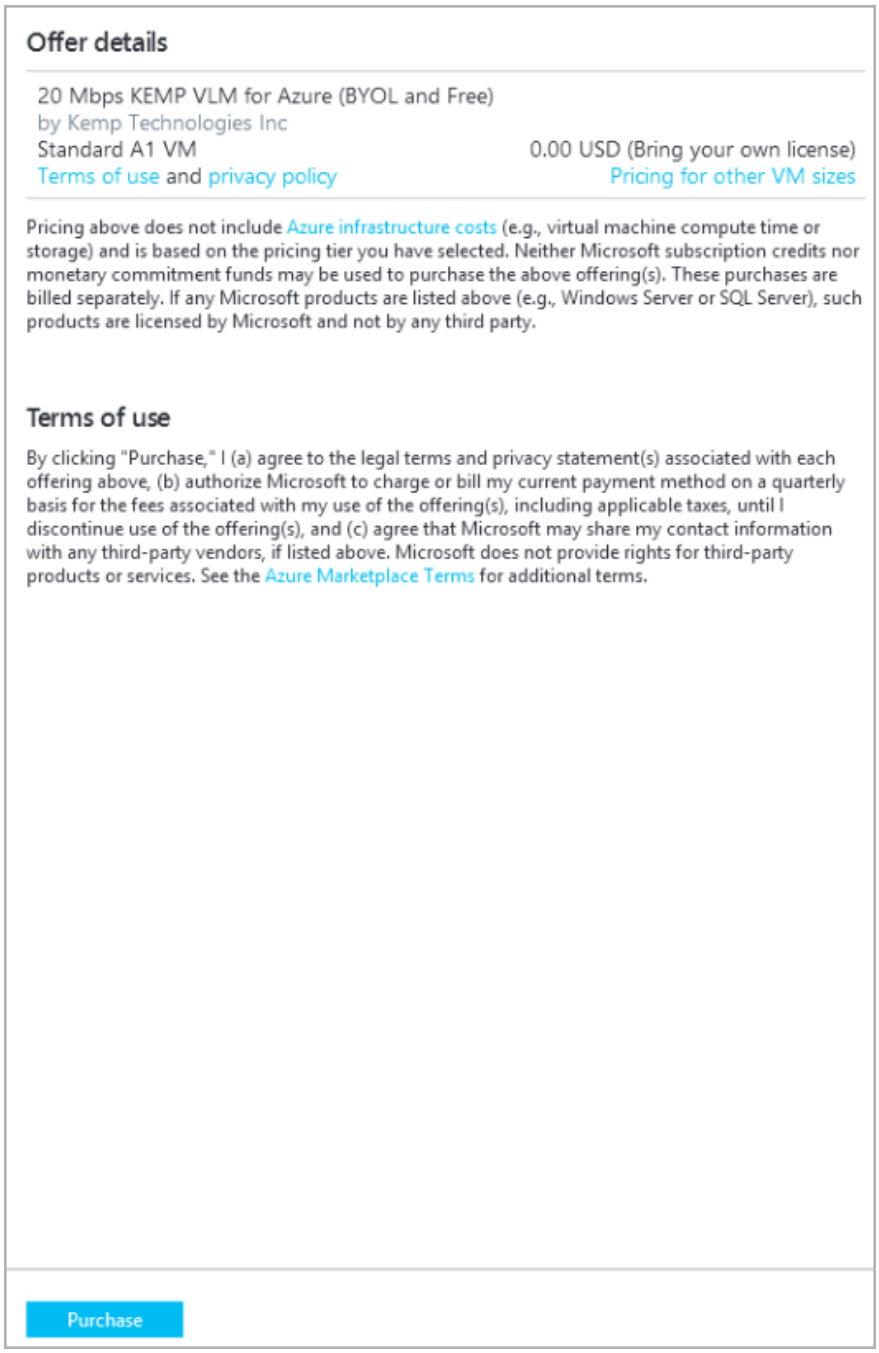
11. Confirm the settings and click **OK**.



12. Click **OK** to close the **Optional Config**.



13. Click **Create**.

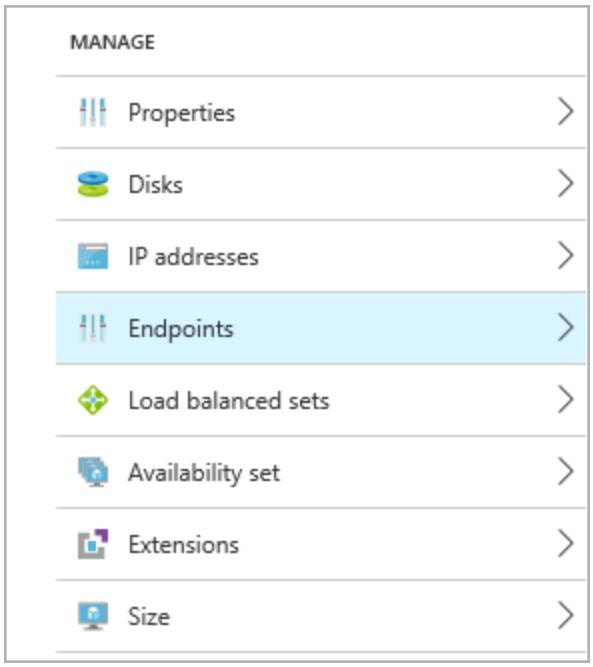


14. In the **Purchase** section, click **Purchase** to start creation of the LoadMaster for Azure Virtual Machine.

4.4.1 Configure the End Points for the second LoadMaster

End points for port 22 and 8443 are automatically created. In a HA configuration, the ports need to be changed. To do this, follow the steps below after the LoadMaster VM has been created:

1. Click the VM on the Azure portal home page.



2. Click **Endpoints**.

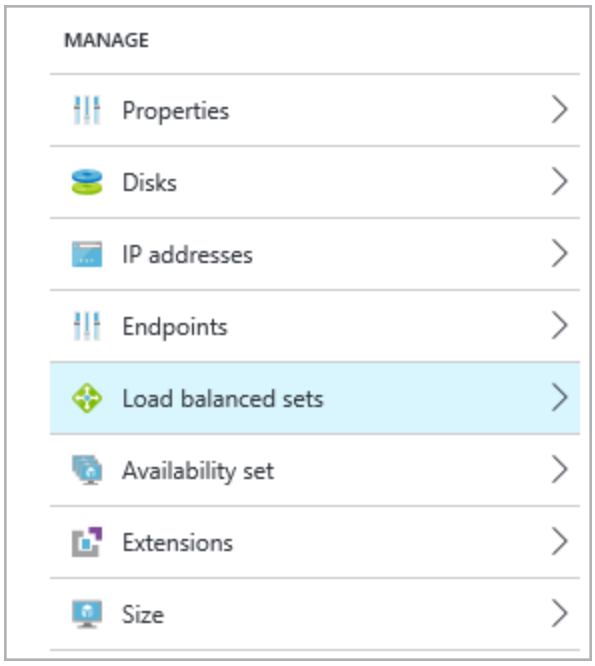
NAME	PROTOC...	PUBLIC...	PRIVATE...	ACL RULES	TYPE	
SSH	TCP	222	22	0	Standalone	...
Management	TCP	8442	8443	0	Standalone	...

3. Select the first end point.
4. Change the public port to **222**.
5. Change the private port to **22**.
6. Click **Save**.
7. Select the second end point.
8. Change the public port to **8442**.
9. Change the private port to **8443**.
10. Click **Save**.

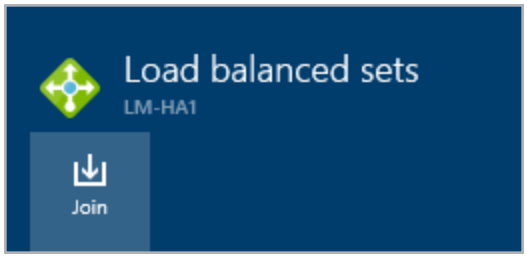
4.5 Create Load Balanced Set

Load Balanced Sets can now be added to the environment. The two LoadMasters for Azure need to be added to this Load Balanced Set. A Load Balanced Set needs to be created for each port that is published through the Kemp LoadMaster.

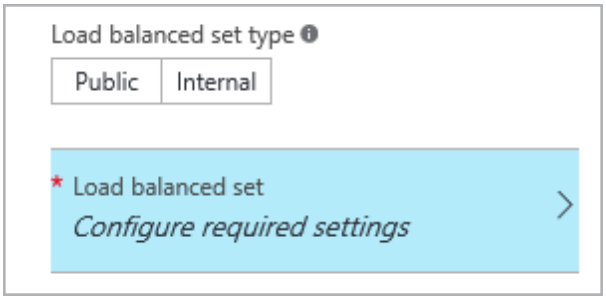
1. Select the first LoadMaster for Azure from the Azure Portal



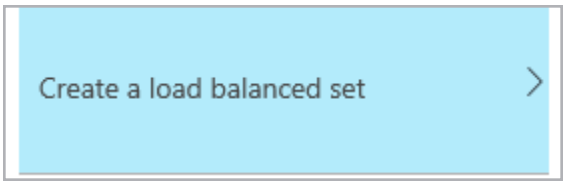
2. Select **Load Balanced Sets**.



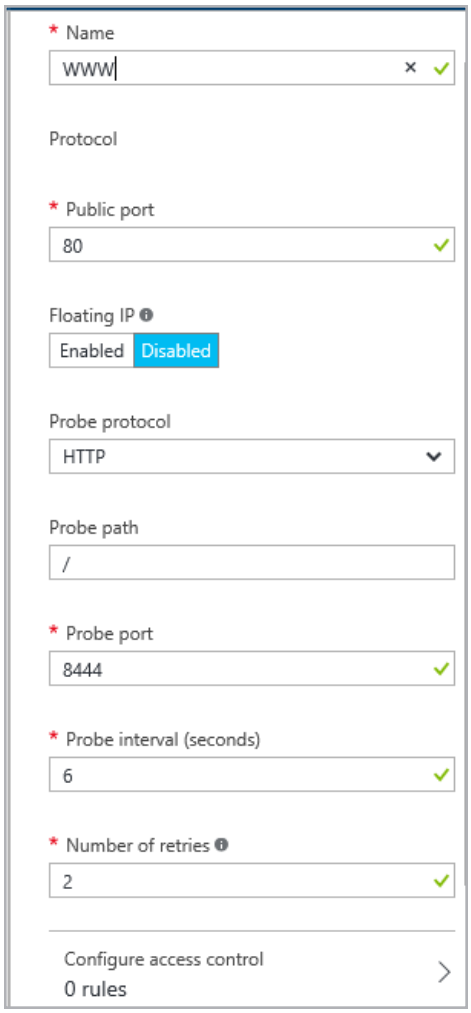
3. Select **Join**.



4. Select **Load Balanced Set**.



5. Select **Create a Load Balanced Set**.



6. Provide a unique name for the Load Balanced Set

    a) Enter port **80** for **Public Port (or required port based on application)**.

    b) Set **Probe Protocol** to **HTTP**.

    c) Enter **/** for **Probe Path**.

    d) Enter port **8444** for **Probe Port**.

e) Set **Probe Interval (Seconds)** to **6**.

f) Set **Number of Retries** to **2**.

7. Click **OK**.

8. Click **OK**.

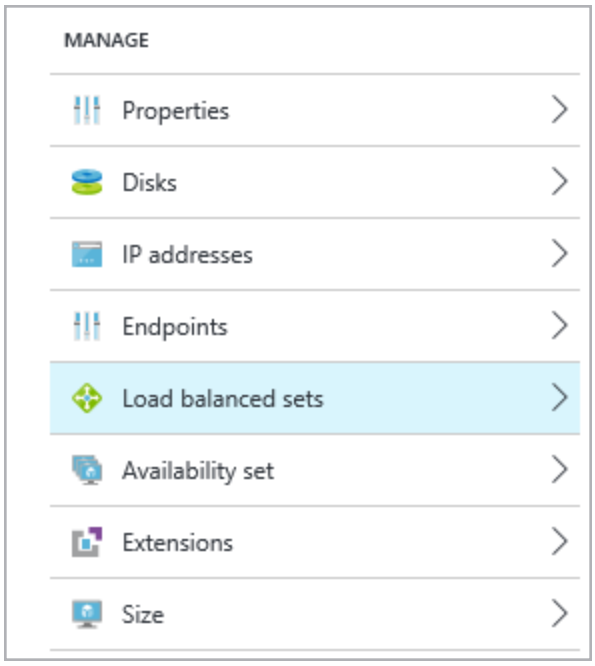
> If an error is thrown you should increase the Probe Interval to 15 and once it is created go back to reduce the Interval to 6.

9. The probe now needs to be changed to an actual HTTP request for it to work. This can be done by running a command in Azure PowerShell, for example:

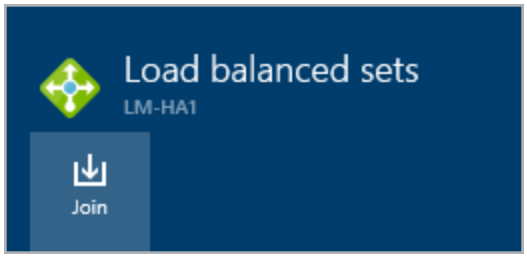
Set-AzureLoadBalancedEndPoint –ServiceName LM-HA1 –LBSetName WWW –ProbeProtocolHTTP –ProbePath / -ProbePort 8444 –ProbeIntervalInSeconds 5

4.5.1 Add Second LoadMaster to Load Balanced Set

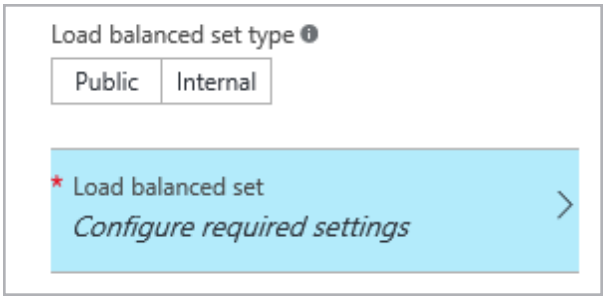
1. Select the second LoadMaster for Azure from the Azure Portal



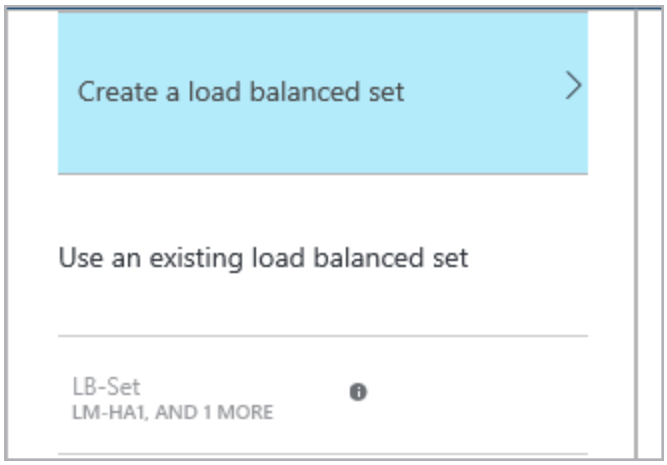
2. Select **Load Balanced Sets**.



3. Select **Join.**



4. Select **Load Balanced Set**.



5. Select the Load Balanced Set created in the **Create Load Balanced Set** section.

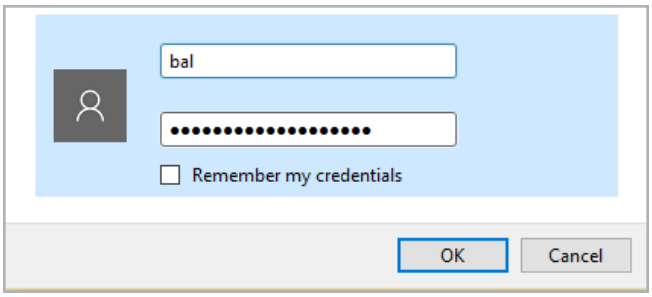
You can add additional Load Balanced Sets to your configuration based on the application requirements. A Load Balance Set for port 8444 can be created to check the state of the LoadMaster pair in Azure.

Once this is done license and set up the LoadMaster as usual. For more information and steps on how to license, refer to the **Licensing, Feature Description** document.

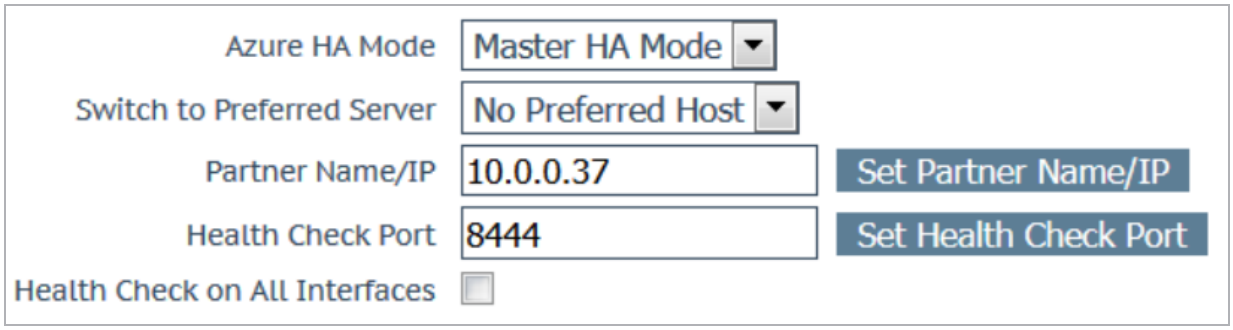
After licensing, follow the steps below to configure HA on the LoadMasters.

5 Configure the LoadMasters

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



1. Access the WUI of the LoadMaster which is the master unit.
2. Access the WUI of Master LoadMaster using https://<cloudserviceurl>:8441
3. Access the WUI of Slave LoadMaster using https://<cloudserviceurl>:8442
4. Default username is **bal** and the password entered during the creation of the LoadMaster.
5. In the main menu, select **System Configuration > Azure HA Parameters**.



6. Select **Master HA Mode** in the **Azure HA Mode** drop-down list.
7. 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 Master:** The HA1 (master) unit always takes over. This is the default option.

8. Enter the **Partner Name/IP** address of the slave LoadMaster unit and click **Set Partner Name/IP**.

9. 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.

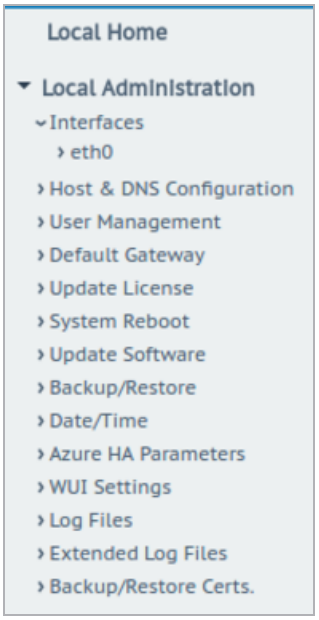
10. If using a multi-arm configuration, select the **Health Check on All Interfaces** check box.

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

11. Then, access the WUI of the slave unit. Complete steps 2 to 4 above in the slave unit, but select **Slave HA Mode** as the **Azure HA Mode** instead.

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

When HA is enabled on both devices, changes made to the Virtual Services in the master unit are replicated to the slave.



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:

6 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.

6.1 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.

6.2 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.

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.

7 Troubleshooting

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

7.1 Virtual Machine Inaccessible

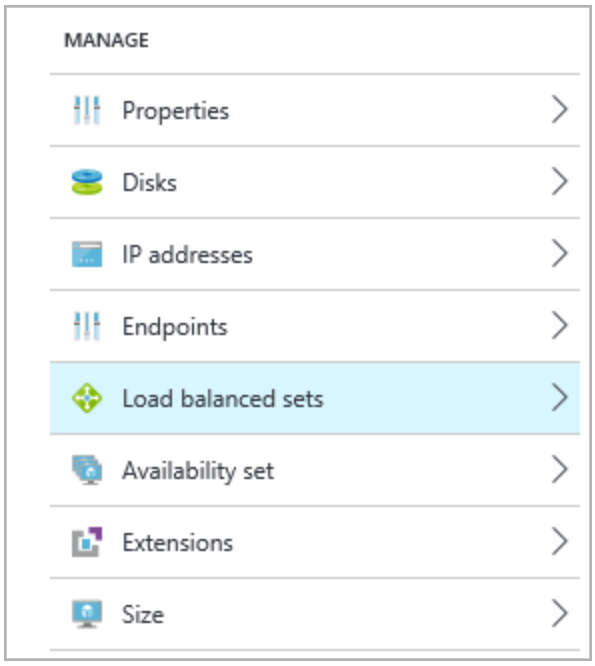
It takes approximately five minutes for the Virtual Machine to become accessible after booting.

7.2 Query the Health Check Port

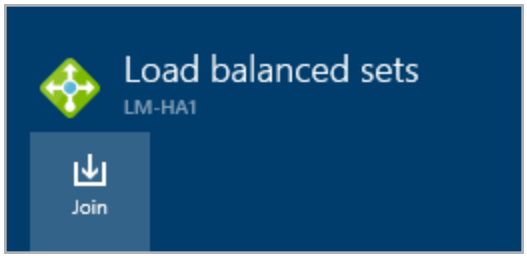
In order to determine which LoadMaster to use as the master, Azure performs a HTTP health check of the partners.

When experiencing issues with HA for Azure, it can be useful to query the HA health check port. This will provide information that can help to determine the status of the HA cluster.

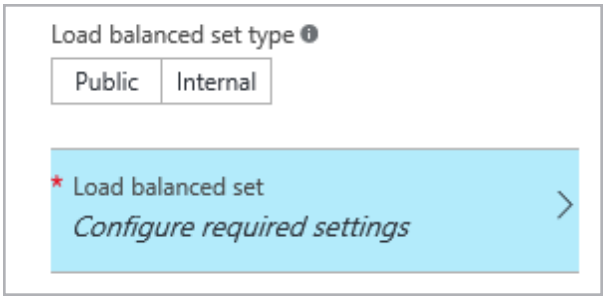
1. Select the first LoadMaster for Azure from the Azure Portal.



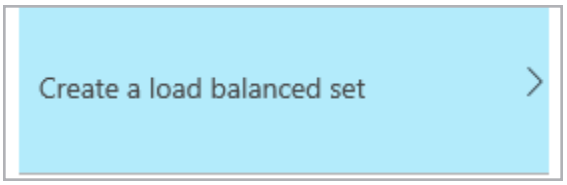
2. Select **Load balanced sets**.



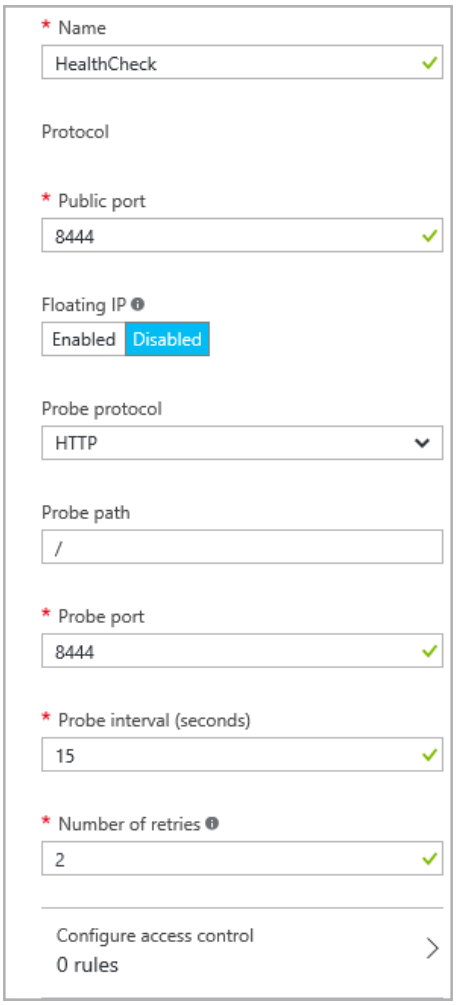
3. Select **Join**.



4. Select **Load Balanced Set**.



5. Select **Create a load balanced set**.



6. Provide a unique name for the Load Balanced Set.

    a) Enter port **8444** for **Public Port (or required port based on application)**.

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

    c) Enter **/** for the **Probe Path**.

    d) Enter port **8444** for the **Probe Port**.

e) Set the **Probe Interval (Seconds)** to **6**.

f) Set the **Number of Retries** to **2**.

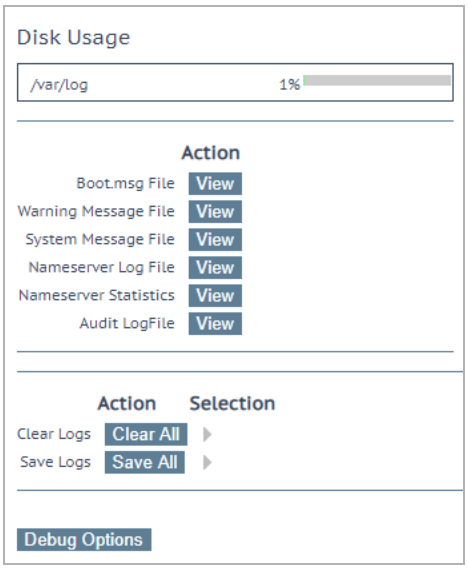
7. Click **OK**.
8. Click **OK**.

When querying or accessing this port on the LoadMasters - if the master is up, the master will report **200 OK, Master is UP** and the slave will report **503 Master is Up**. If the master is down the slave will report **200 OK, Slave is UP (Master is DOWN)**.

7.3 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**.



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.

7.4 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.

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 Resource Manager, Feature Description

Azure Virtual Machines – tutorials and guides:

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

High Availability (HA), Feature Description

Last Updated Date

This document was last updated on 31 January 2019.

