LoadMaster for AWS

Feature Description

UPDATED: 07 December 2020

Copyright Notices

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

1.1 Document Purpose 5

1.2 Intended Audience 6

1.3 Related Firmware Version 7

2 LoadMaster for AWS 8

2.1 Prerequisites 8

2.2 Differences from the Virtual LoadMaster (VLM) 8

2.3 Licensing Options 9

2.4 Security Best Practices 9

2.4.1 IAM Service 10

2.4.1.1 Create an IAM Policy 10

2.4.1.2 Assign an IAM Policy to an IAM User 12

2.4.2 Access Keys 14

2.4.2.1 Rotate Access Key and Secret Key 14

2.4.3 Storing Secrets 16

2.5 Create a New Key Pair 16

2.6 Start a New Instance 18

2.7 Enable a 10 Gb Interface 24

2.8 Initial Setup – Hourly Licensing 25

2.8.1 Restart Web Server Access - Hourly Licensing 31

2.8.2 Initial Configuration – Hourly Licensing 32

2.9 Initial Setup – BYOL 33

2.10 Activate your Support Subscription 34

3 LoadMaster Firmware Downgrades 36

4 LoadMaster Backup and Restore 37

5 Monitoring LoadMaster Health in AWS 38

5.1 Monitoring with Kemp 360 38

5.2 Monitoring with AWS 38

References 41

Last Updated Date 42

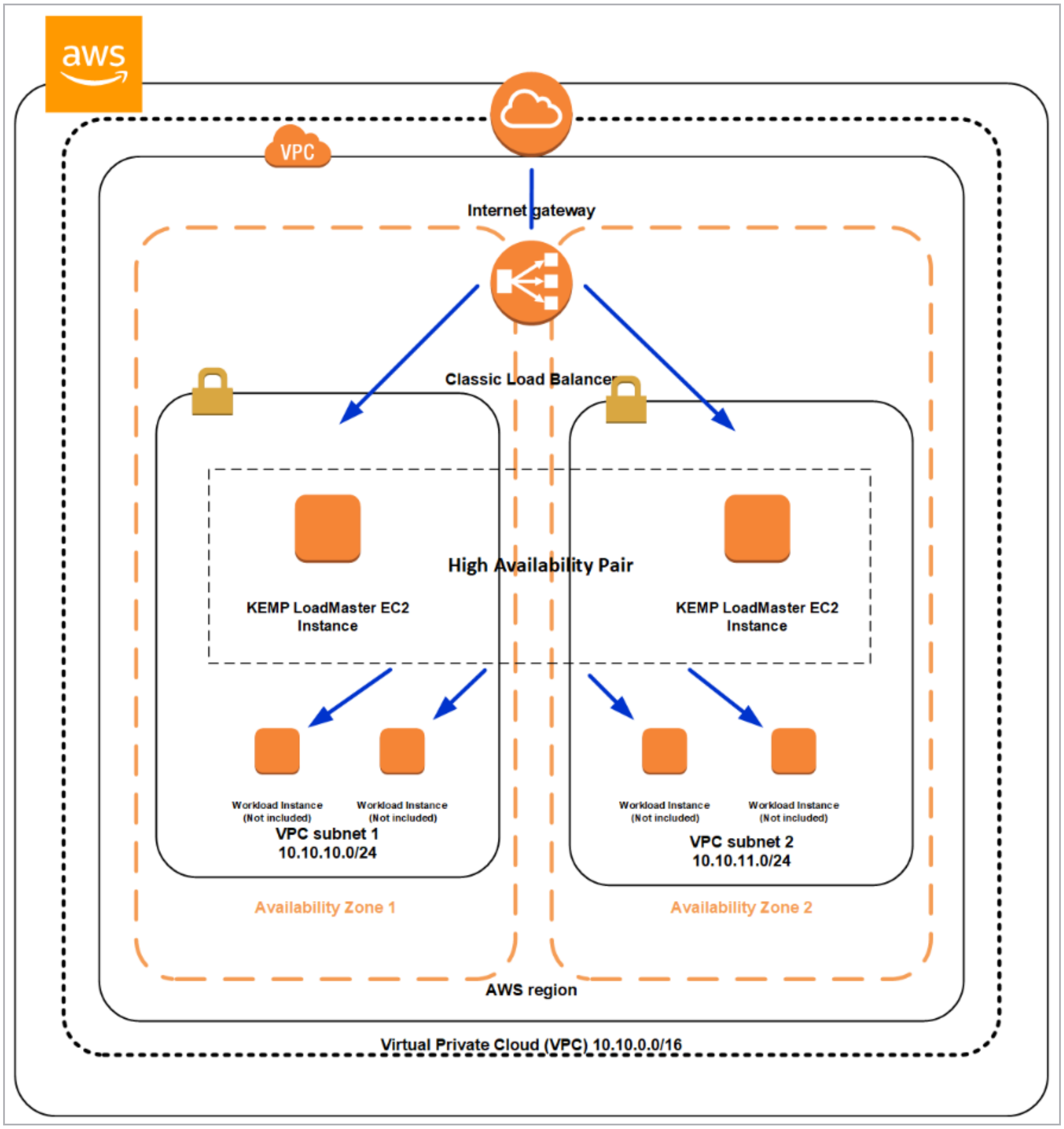
1 Introduction

Amazon Web Services (AWS) is a collection of remote computing services (also called web services) that together make up Amazon's cloud computing platform.

1.1 Document Purpose

This document is intended to brief you on the LoadMaster for AWS product and assist the reader to set up a basic LoadMaster for AWS instance and create a service.

It is strongly encouraged to use High Availability (HA) when using the LoadMaster for AWS for production workloads. For further information on this, refer to the **HA for AWS, Feature Description** on the KEMP Documentation Page.


aws
VPC
Internet gateway
Classic Load Balancer
High Availability Pair
KEMP LoadMaster EC2 Instance
KEMP LoadMaster EC2 Instance
Workload Instance (Not included)
Workload Instance (Not included)
Workload Instance (Not included)
Workload Instance (Not included)
VPC subnet 1 10.10.10.0/24
VPC subnet 2 10.10.11.0/24
Availability Zone 1
Availability Zone 2
AWS region
Virtual Private Cloud (VPC) 10.10.0.0/16

1.2 Intended Audience

This document is intended for anyone who is interested in finding out about the LoadMaster for AWS product.

1.3 Related Firmware Version

Published with LMOS version 7.2.48.3 LTS. This document has not required changes since 7.2.48.3 LTS. However, the content is in sync with the latest LoadMaster LTS firmware.

2 LoadMaster for AWS

2.1 Prerequisites

Some requirements to be aware of when deploying a LoadMaster in AWS are below:

- Internet access in the Virtual Private Cloud (VPC) is required to license free and hourly-usage LoadMasters.
- Using Bring Your Own License (BYOL) licensing in an AWS VPC does work without internet access when using the private IP address but only if Offline Licensing is used during the deployment.
- Alternate default gateway support is not permitted in a cloud environment.
- If you want to enable 10 Gb throughput for a LoadMaster in AWS, you must select an AWS virtual machine (VM) instance type that supports the 10 Gb ENA driver. You can do this on initial install, or by moving to a new instance type after installation. The following AWS VM instance types support the 10 Gb ENA driver: A1, C5, C5d, C5n, F1, G3, H1, I3, I3en, m4.16xlarge, M5, M5a, M5ad, M5d, P2, P3, R4, R5, R5a, R5ad, R5d, T3, T3a, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, X1, X1e, and z1d. Refer to the Supported Instance Types AWS page for further details.

2.2 Differences from the Virtual LoadMaster (VLM)

First, the initial IP address that is obtained is assigned by AWS using Dynamic Host Configuration Protocol (DHCP). The LoadMaster obtains this address at instantiation and uses it as its interface address. This address is permanent for this instance and this private address is associated with a public IP address as well. Additional private addressing can be assigned according to your needs if you have additional private networks in AWS.

In addition, a public address that maps to the private address is issued by AWS. Unlike the private address, the public IP address can be changed by purchasing an Elastic IP.

> For more information on Elastic IPs, refer to the Amazon EC2 Elastic IP Addresses Feature Guide. Elastic IPs can be requested by opening a Support case with AWS. Elastic IPs can be

allocated in the AWS EC2 Console in **NETWORK & SECURITY > Elastic IPs**.

Interface IP addresses can be changed administratively as usual from the LoadMaster, but this requires an additional AWS configuration to prevent disconnection.

To preserve public ports, the Web User Interface (WUI) is available on port 8443 rather than 443. This allows port 443 to be used for a Virtual Service.

Due to AWS limitations, it is not possible to bond interfaces on AWS LoadMasters.

2.3 Licensing Options

There are three main licensing options when deploying a LoadMaster for AWS:

Hourly consumption (PAYG)

The hourly consumption option includes Enterprise Plus Support. You can find details on Kemp subscriptions at the following link: LoadMaster Support Subscriptions.

BYOL

You must purchase a Standard, Enterprise, or Enterprise Plus subscription as part of the BYOL option.

Metered Enterprise Licensing Agreement (MELA)

Kemp MELA is a monthly subscription that allows for unlimited LoadMaster deployments and is billed based on aggregate consumption.

2.4 Security Best Practices

AWS has many security features to protect customers' cloud assets. This section outlines some security best practices pertaining to AWS. See the AWS Security Best Practices Whitepaper for further details.

If you already have an Identity and Access Management (IAM) role for administration of the Elastic Compute Cloud (EC2) and SSH key pair, you can skip to the **Start a New Instance** section.

2.4.1 IAM Service

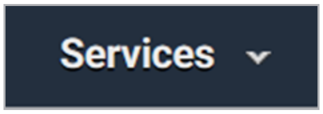
IAM is a centralized service that manages users, credentials, policies, and keys for the resources deployed in AWS. You should create individual accounts for each user that creates or accesses AWS resources. When possible, you should enable AWS Multi-Factor Authentication (MFA) for the IAM user account to further secure unauthorized access to assets running in the public cloud.

You should always leverage IAM Policies to assign permissions to IAM user accounts. You should scope these permissions with the least privilege security model by only permitting access based on users' job requirements.

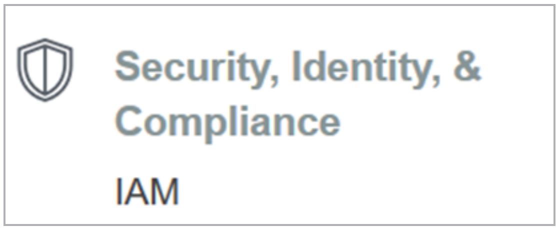
2.4.1.1 Create an IAM Policy

This section provides step-by-step instructions on creating an IAM Policy allowing an IAM user to create and manage EC2 Services:

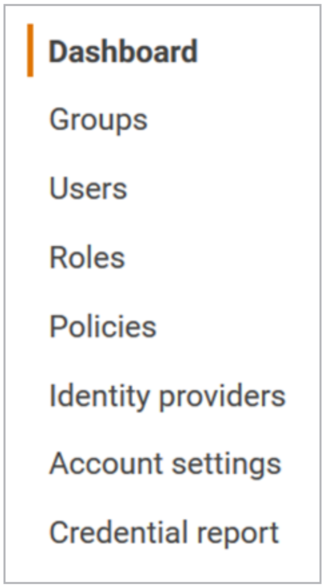
1. Log in to the AWS console.



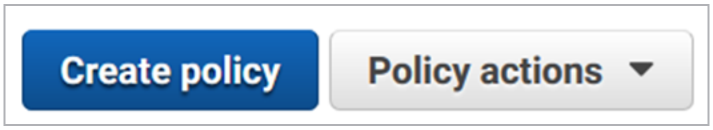
2. Click **Services**.



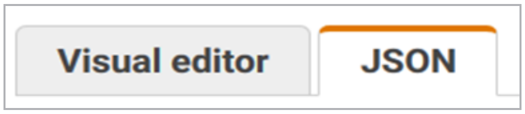
3. Under **Security, Identity, & Compliance**, select **IAM**.



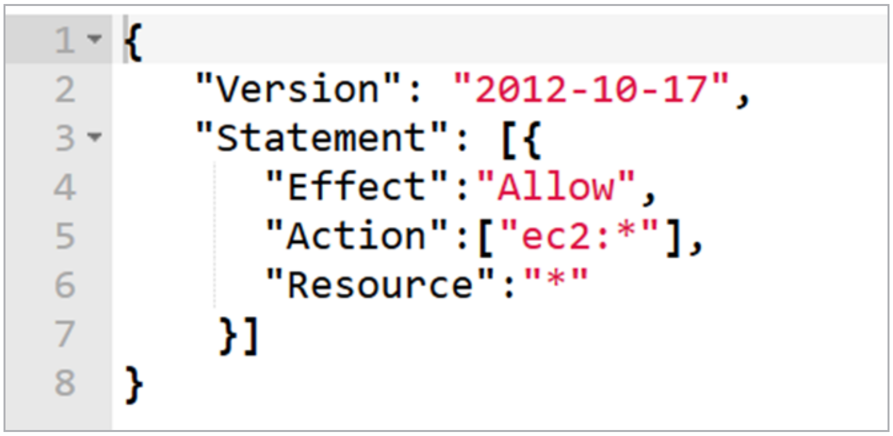
4. In the navigation on the left, click **Policies**.



5. Click **Create policy**.

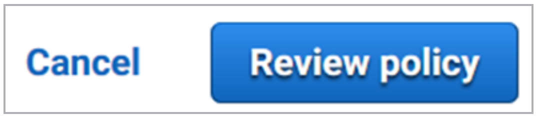


6. Select **JSON**.

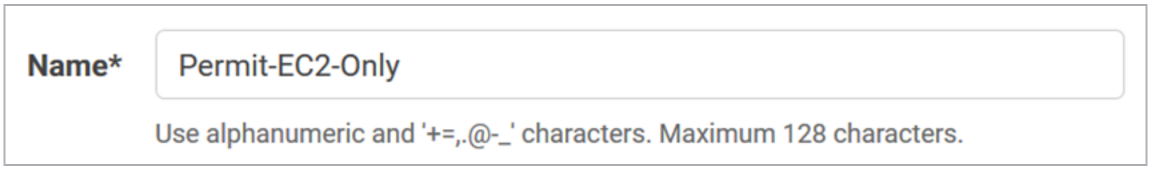


```
{
    "Version": "2012-10-17",
    "Statement": [{
      "Effect":"Allow",
      "Action":["ec2:*"],
      "Resource":"*"
     }]
}
```

7. Enter the IAM Policy in the provided area. The text shown above is only an example. Policies created in AWS should be reviewed with your organization's security team.



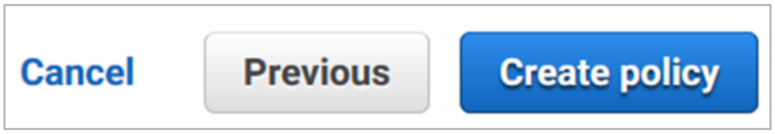
8. Click **Review policy**.



Name* Permit-EC2-Only

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

9. Enter a unique **Name**.



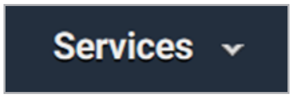
10. Click **Create policy**.

You can find further information on IAM Policies at the following link: Policies and Permissions.

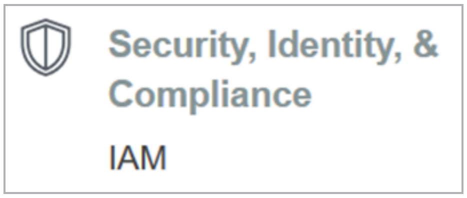
2.4.1.2 Assign an IAM Policy to an IAM User

This section provides step-by-step instructions on assigning an IAM Policy to an IAM user:

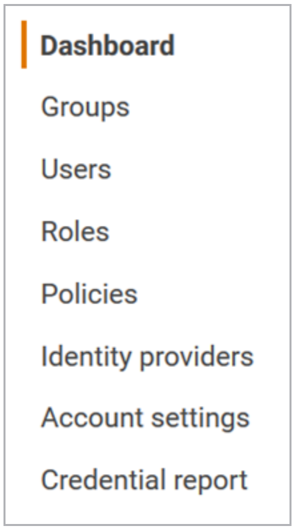
1. Log in to the AWS console.



2. Click **Services**.

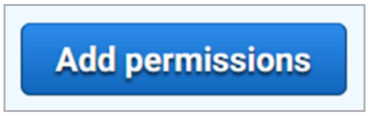


3. Under **Security, Identity, & Compliance**, select **IAM**.

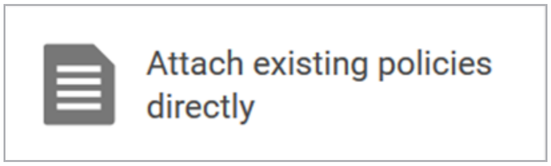


4. Select **Users**.

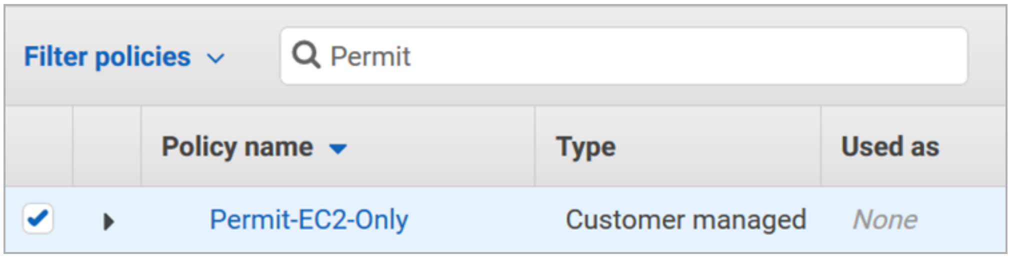
5. From the list of users, select the user to assign the policy to.



6. Click **Add permissions**.

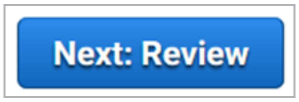


7. Click **Attach existing policies directly**.

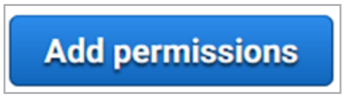


		Policy name	Type	Used as
☑	▸	Permit-EC2-Only	Customer managed	*None*

8. Search for and select the IAM Policy to apply.



9. Click **Next: Review**.



10. Click **Add permissions**.

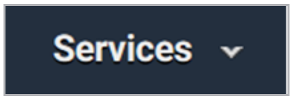
2.4.2 Access Keys

Access Keys are credentials for an IAM user that allow programmatic requests to the AWS Command Line Interface (CLI) or AWS Application Programming Interface (API). These keys consist of two parts; an access key ID and a secret access key. You should leverage multiple keys and use them across the different applications requiring access to AWS resources. In addition, you should rotate these keys regularly.

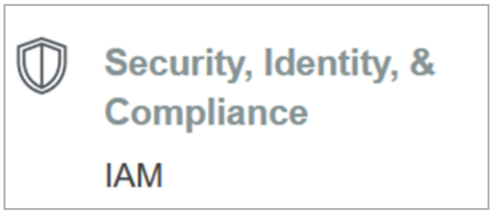
2.4.2.1 Rotate Access Key and Secret Key

This section provides step-by-step instructions for creating and rotating Access Keys and Secret Keys:

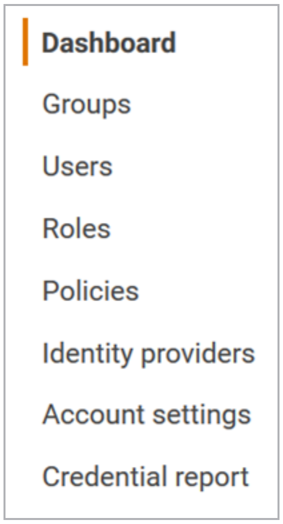
1. Log in to the AWS console.



2. Click **Services**.

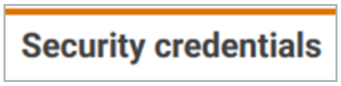


3. Under **Security, Identity, & Compliance**, select **IAM**.

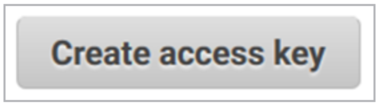


4. Select **Users**.

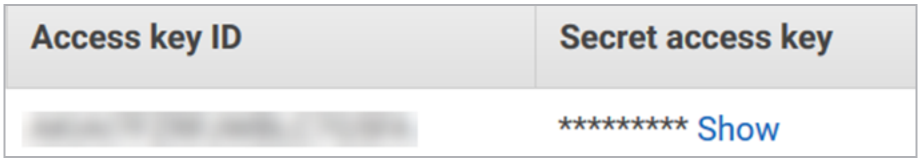
5. From the list of users, select the user to manage.



6. Click **Security credentials**.

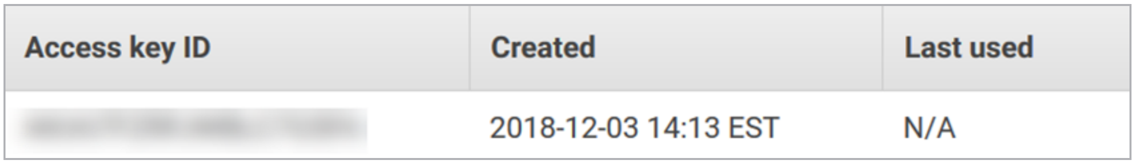


7. Click **Create access key**.



Access key ID	Secret access key
[redacted]	********* Show

8. Copy the **Access key ID** and **Secret access key**.



Access key ID	Created	Last used
[redacted]	2018-12-03 14:13 EST	N/A

You can now use these keys in the application or direct access to the CLI or API. When viewing the Access Key, there is a **Last used** column. You can leverage this to ensure the Access Key is no longer in use and can be deleted as part of the key rotation schedule.

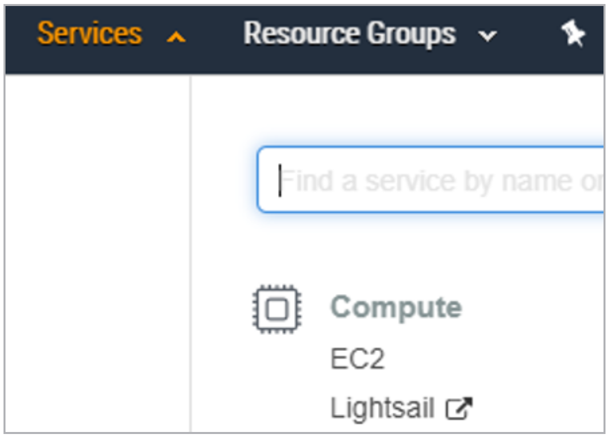
2.4.3 Storing Secrets

The handling and storing of secrets is a critical component of the overall security of the assets. AWS provides AWS Secrets Manager, which makes it easy to store and retrieve secrets. You should use the AWS Secrets Manager whenever possible to improve the overall security in AWS. For more information on AWS Secrets Manager, visit the following website: AWS Secrets Manager: Store, Distribute, and Rotate Credentials Securely

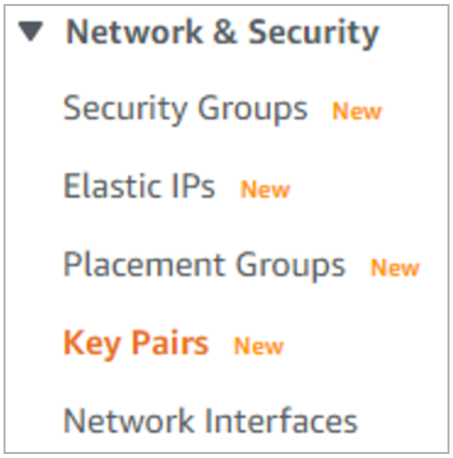
2.5 Create a New Key Pair

When starting a new instance in EC2, you are prompted to select a key pair. A key pair is a certificate and key. It is used to SSH to the LoadMaster. You must keep the downloaded key in a safe place. Steps on how to add a key pair are below:

1. Log in to the AWS console.

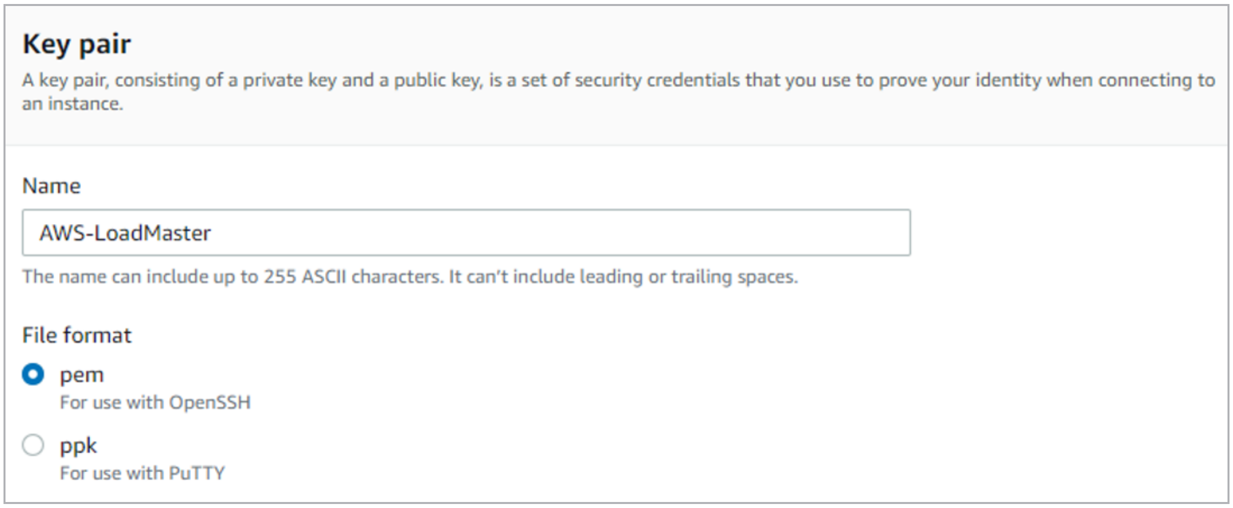


2. Click **Services** and **EC2**.



3. In the main menu, select **Key Pairs**.

4. Click **Create Key Pair**.



Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

AWS-LoadMaster

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

File format

● pem
For use with OpenSSH

○ ppk
For use with PuTTY

5. Enter a name for the key pair, select **pem**, and click **Create key pair**.

6. The .pem file downloads.

> This file is required to SSH into the LoadMaster so make a note of where this file is stored. This file needs to reside on the client that is used to SSH to the LoadMaster.

If you are using a client that does not accept PEM format, you must convert the file to another format, for example PPK for Putty.

7. The permissions of the key pair file must be changed for it to work. To do this in Linux, go to the directory where the file is stored and run the following command:

```
chmod 600 <FileName>
```

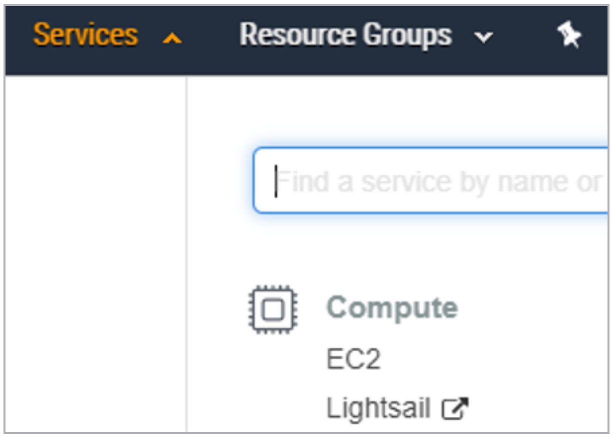
2.6 Start a New Instance

You can deploy new LoadMaster instances through the AWS Marketplace. For greater availability, Kemp recommends deploying a pair of Kemp LoadMasters in HA mode. For more information on deploying an HA pair, refer to the following feature guide: HA for AWS Feature Description.

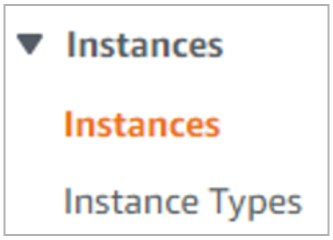
To start an instance, follow the steps below:

Note that it is also possible to deploy a LoadMaster using a different flow using the AWS Marketplace. Configure the same settings as outlined below, in particular – ensure to select a VPC as the network.

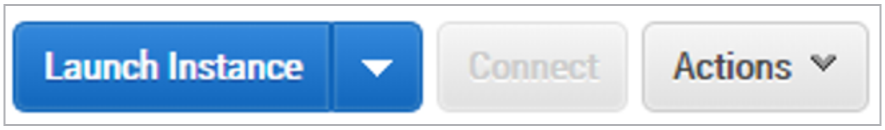
1. Log in to the AWS console.



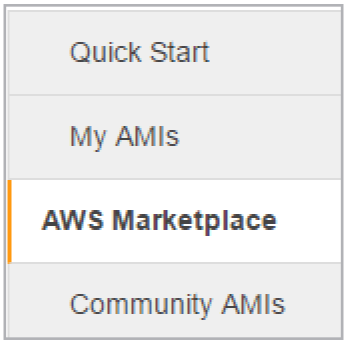
2. Click **Services** and **EC2**.



3. Click **Instances**.



4. Click **Launch Instance**.

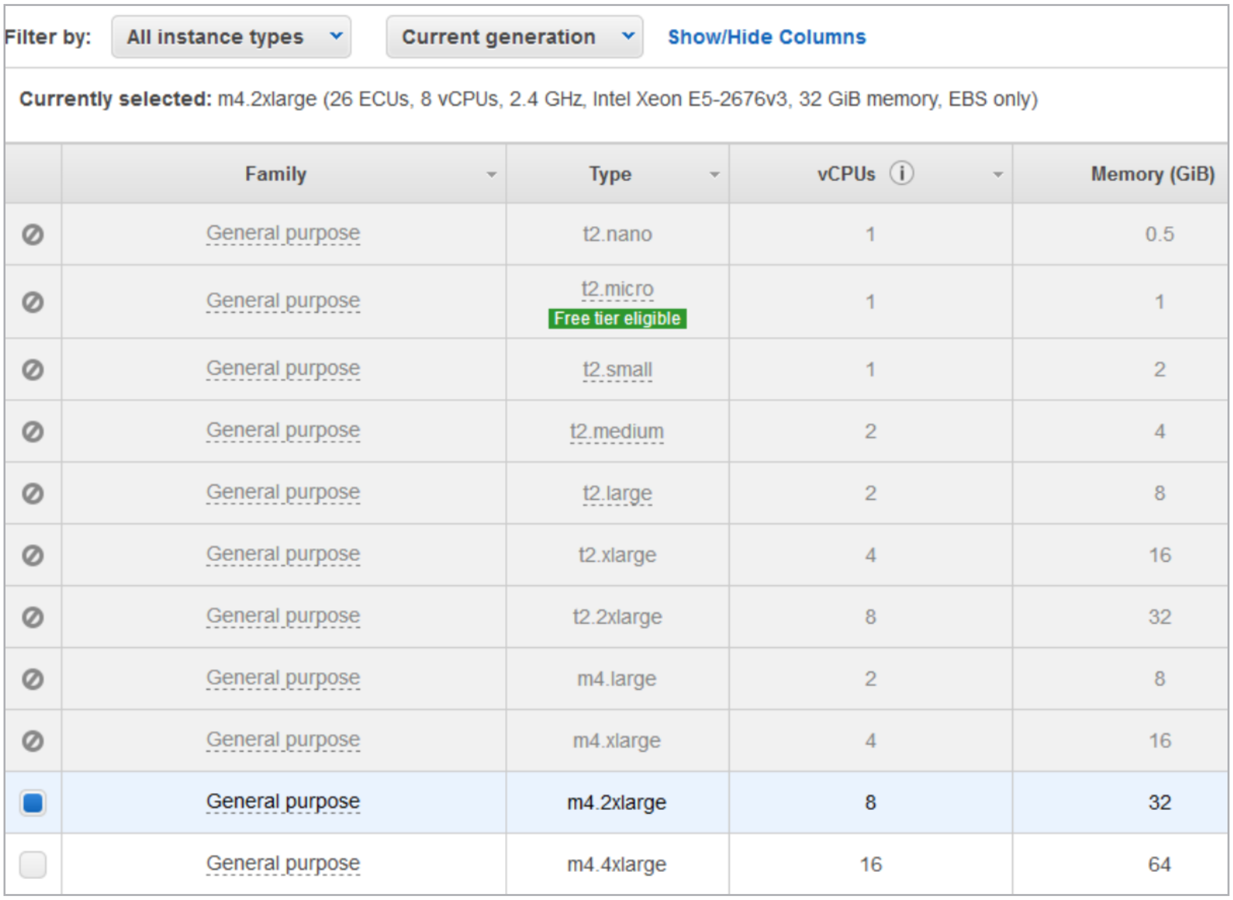


5. Select **AWS Marketplace**.

6. Search for **Kemp**.

7. Click **Select** for the relevant version to be deployed.

8. If you select an hourly licensing model, click **Continue** to proceed.



Filter by: All instance types ⌄ Current generation ⌄ Show/Hide Columns

Currently selected: m4.2xlarge (26 ECUs, 8 vCPUs, 2.4 GHz, Intel Xeon E5-2676v3, 32 GiB memory, EBS only)

	Family	Type	vCPUs ⓘ	Memory (GiB)
⊘	General purpose	t2.nano	1	0.5
⊘	General purpose	t2.micro Free tier eligible	1	1
⊘	General purpose	t2.small	1	2
⊘	General purpose	t2.medium	2	4
⊘	General purpose	t2.large	2	8
⊘	General purpose	t2.xlarge	4	16
⊘	General purpose	t2.2xlarge	8	32
⊘	General purpose	m4.large	2	8
⊘	General purpose	m4.xlarge	4	16
■	General purpose	m4.2xlarge	8	32
□	General purpose	m4.4xlarge	16	64

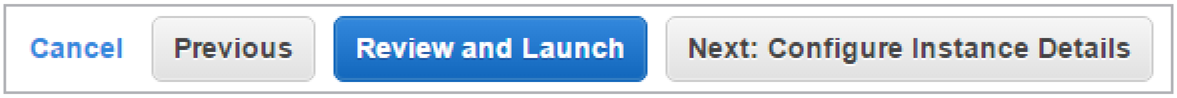
9. Select the desired **Instance Type**.

Use the following LoadMaster sizing table as a reference only because some workloads may require more vCPU or memory than others:

LoadMaster	Recommended vCPU	Recommended RAM
VLM-500	2 vCPU	4 GiB
VLM-3000	4 vCPU	8 GiB
VLM-MAX	User defined *	User defined *

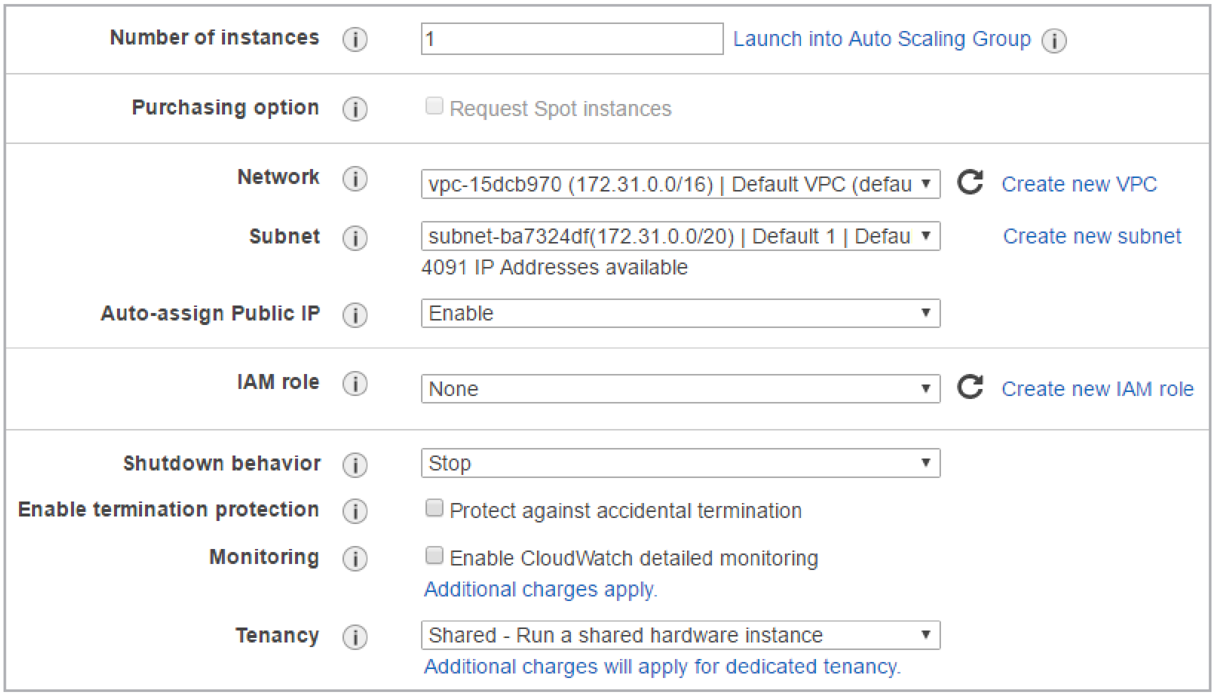
* VLM-MAX vCPU and RAM allocation can be assigned based on your requirements due to the uncapped performance available.

For further information on instance types, refer to the following Amazon link: Amazon EC2 Instance Types.



If you want to enable 10 Gb throughput for a LoadMaster in AWS, you must select an AWS VM instance type that supports the 10 Gb ENA driver. You can do this on initial install, or by moving to a new instance type after installation. The following AWS VM instance types support the 10 Gb ENA driver: A1, C5, C5d, C5n, F1, G3, H1, I3, I3en, m4.16xlarge, M5, M5a, M5ad, M5d, P2, P3, R4, R5, R5a, R5ad, R5d, T3, T3a, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, X1, X1e, and z1d. For more information, refer to the **Enable a 10 Gb Interface** section.

10. Click **Next: Configure Instance Details**.



Number of instances	1 — Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-15dcb970 (172.31.0.0/16) | Default VPC (defau — Create new VPC
Subnet	subnet-ba7324df(172.31.0.0/20) | Default 1 | Defau — Create new subnet 4091 IP Addresses available
Auto-assign Public IP	Enable
IAM role	None — Create new IAM role
Shutdown behavior	Stop
Enable termination protection	□ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.
Tenancy	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.

11. Ensure to select the correct item (a VPC) in the **Network** drop-down list.

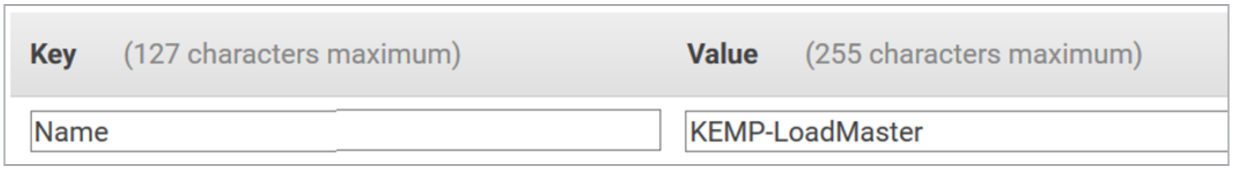
> If multiple LoadMasters on multiple networks are needed, choose the different networks as required. If more networks need to be created, contact your AWS administrator to add them. The **Create new VPC** link can be used to add more networks if needed.

12. Ensure that the **Auto-assign Public IP** option is set to **Enable**.

13. Configure any other setting as needed.

14. Click **Next: Add Storage**.

15. Keep the defaults and click **Next: Add Tags**.



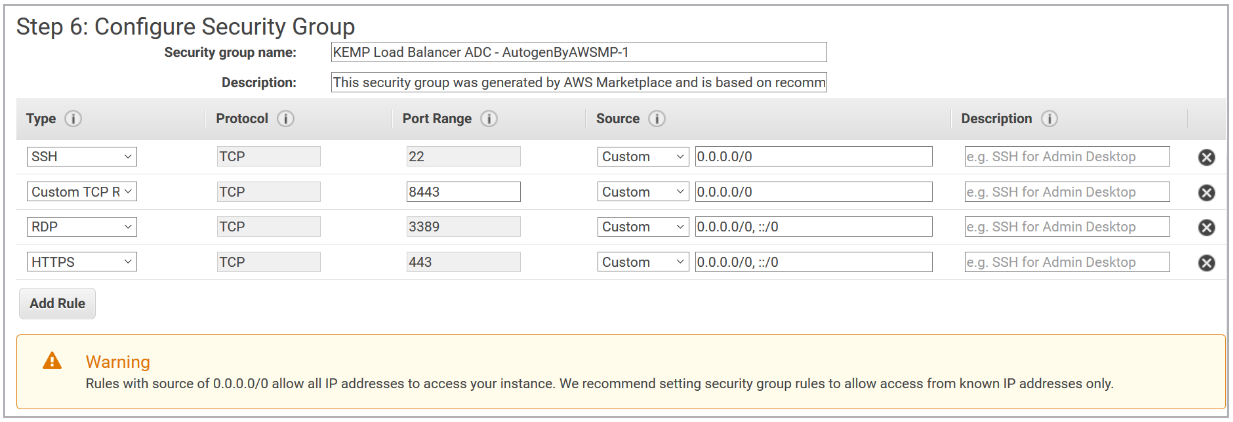
Key (127 characters maximum)	**Value** (255 characters maximum)
Name	KEMP-LoadMaster

AWS tags allow you to categorize resources in different ways. You can categorize by application, owner, purpose, or any custom tag.

16. Enter tags.

17. Click **Next: Configure Security Groups**.

18. Select the security group of your choosing or create a new security group.



Step 6: Configure Security Group

Security group name: KEMP Load Balancer ADC - AutogenByAWSMP-1

Description: This security group was generated by AWS Marketplace and is based on recomm

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
Custom TCP R	TCP	8443	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
RDP	TCP	3389	Custom	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom	0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

Add Rule

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

a) The following rules are needed in the security group:

- Custom TCP Rule with the Port Range 8443 for the WUI
- **SSH** for the SSH management interface
- Any additional rules that are needed for other ports for services to be load balanced, for example Remote Desktop Protocol (**RDP**) if load balancing Windows RDP servers, or **HTTPS** for a secure website

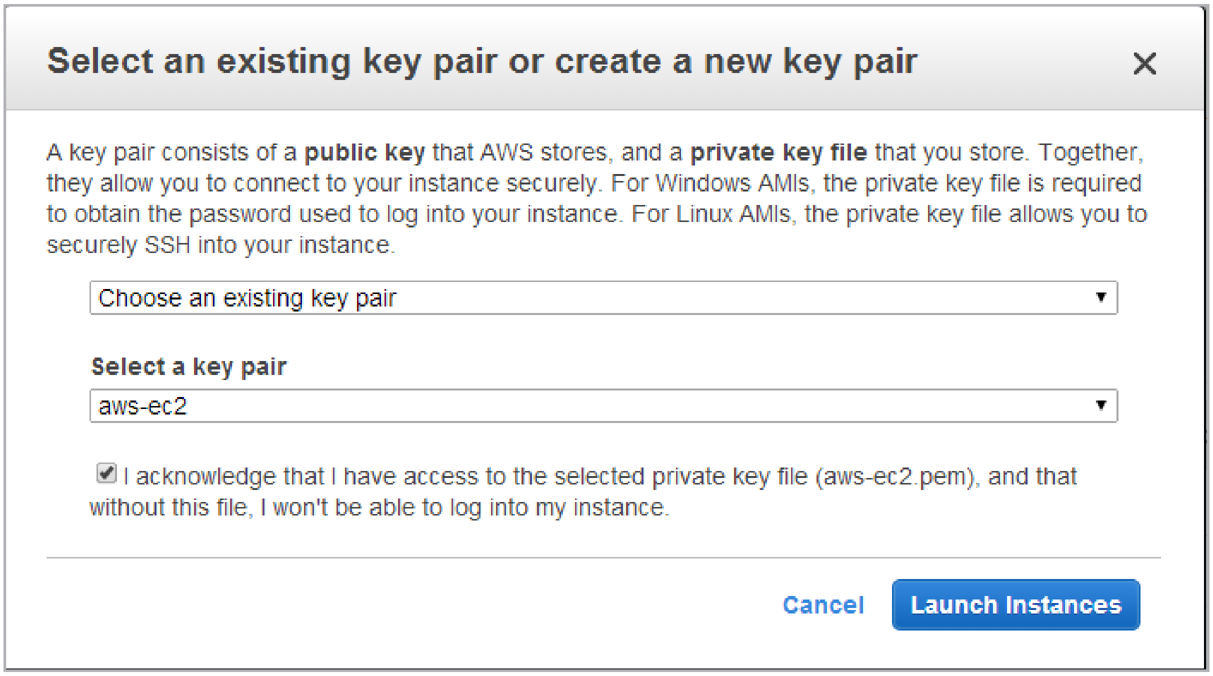
Do not block port 6973. This port is used for synchronization when using the LoadMaster in a HA configuration.

Select the relevant source option from the drop-down list and enter the custom IP addresses as needed.

19. It is recommended that management services only be allowed using trusted IP addresses. You should also add rules for any services you intend on creating. You can always revisit this security group later if additional services become necessary.

20. Click **Review and Launch**.

21. Click **Launch**.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Choose an existing key pair

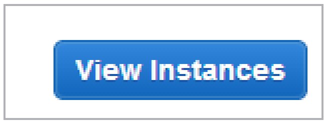
Select a key pair: aws-ec2

☑ I acknowledge that I have access to the selected private key file (aws-ec2.pem), and that without this file, I won't be able to log into my instance.

22. Select the appropriate key pair for your environment. This is the key pair that was created in the **Create a New Key Pair** section. This key pair is needed to connect using SSH.

23. Select the check box.

24. Click **Launch Instances**.



25. Click **View Instances**. The **Public IP** address or **Public DNS** address can be used to connect to the instance using HTTPS on port 8443.

26. After your instance state is **Running**, you can connect to your LoadMaster instance.

2.7 Enable a 10 Gb Interface

Virtual LoadMasters deployed within the AWS Cloud now support 10 Gb interfaces. This support comes with the following limitations:

- Interface graphs for 10 Gb interfaces on the **Statistics** page may be displayed incorrectly. This will be addressed in a future release.

If you upgrade from a release prior to 7.2.48 to 7.2.48 or a later release and your AWS VM is running a VM instance type that does not support 10 Gb interfaces (for example, m4.10xlarge), you must convert the VM to a machine type that supports 10 Gb interfaces (for example, m4.16xlarge).

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

1. Shut down the LoadMaster using the LMOS WUI or API.

2. Enable ENA driver support on the AWS VM using the following command:

```
aws ec2 modify-instance-attribute --instance-id instanceID --ena-support
```

> The **Instance ID** can be found in the AWS **EC2 Dashboard** by selecting **Instances** within the **INSTANCES** section of the main menu.

3. Change the AWS VM instance type to one that supports the ENA 10 Gb driver (for example, m4.16xlarge) using the AWS UI.

4. Start the LoadMaster VM.

For further details on this, refer to the AWS document on Enabling Enhanced Networking with the Elastic Network Adapter (ENA) on Linux Instances.

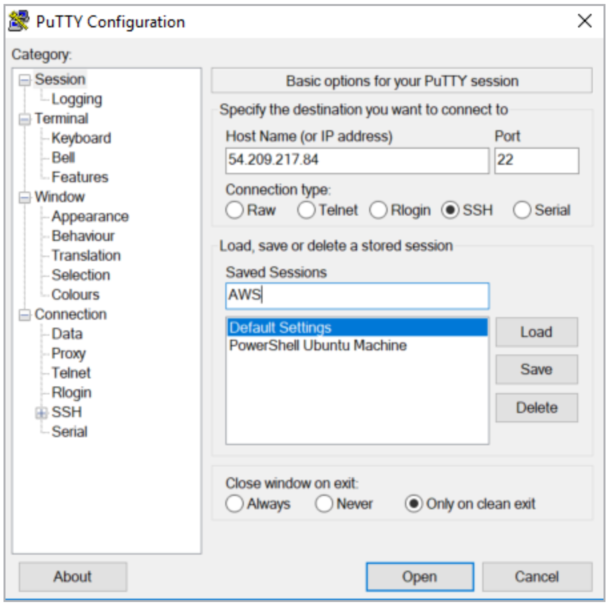
For details on how to get started with AWS command line, refer to the following AWS documentation:

- What is the AWS Command Line Interface?
- Installing the AWS CLI

2.8 Initial Setup – Hourly Licensing

If you chose an hourly licensing method - after the instance is launched, you must first access the LoadMaster using SSH with the required key pair to enable WUI access. The example steps below use PuTTY as the SSH client.

1. Open the PuTTY client.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 54.209.217.84

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

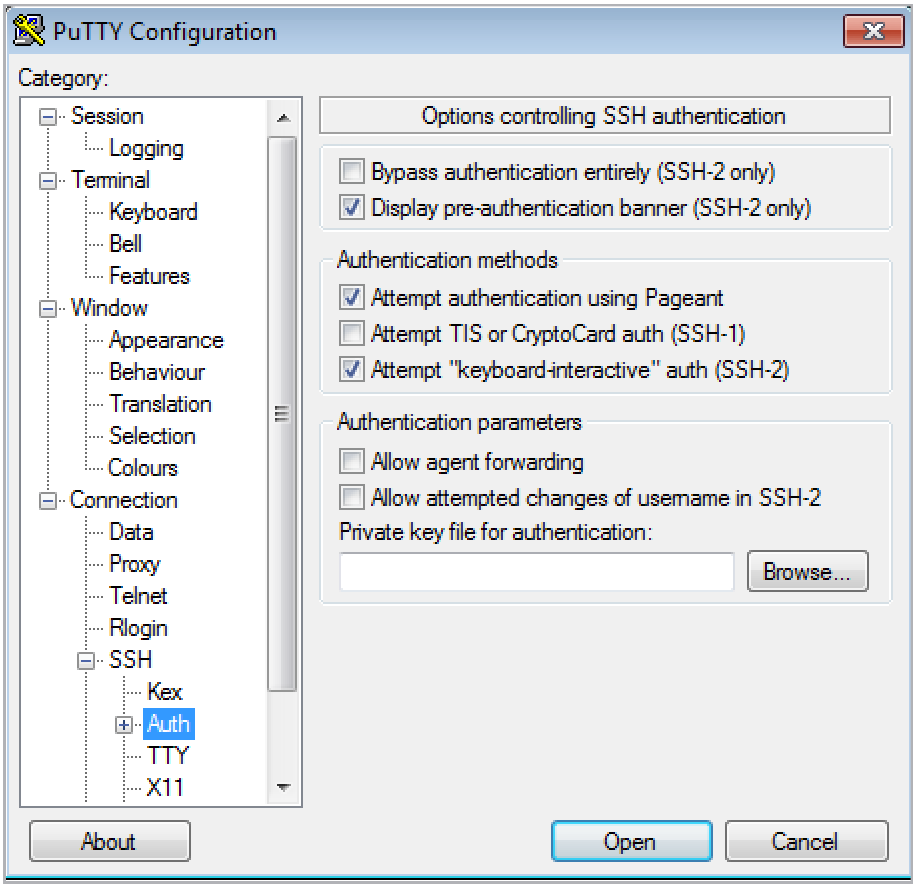
Load, save or delete a stored session

Saved Sessions: AWS

Close window on exit: ○ Always ○ Never ● Only on clean exit

2. Enter the **IP address** of the LoadMaster instance. This is the IP address obtained in the **Start a New Instance** section.

3. In the main menu, navigate to **Connection > SSH > Auth**.



PuTTY Configuration

Category:

Options controlling SSH authentication

☐ Bypass authentication entirely (SSH-2 only)
☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

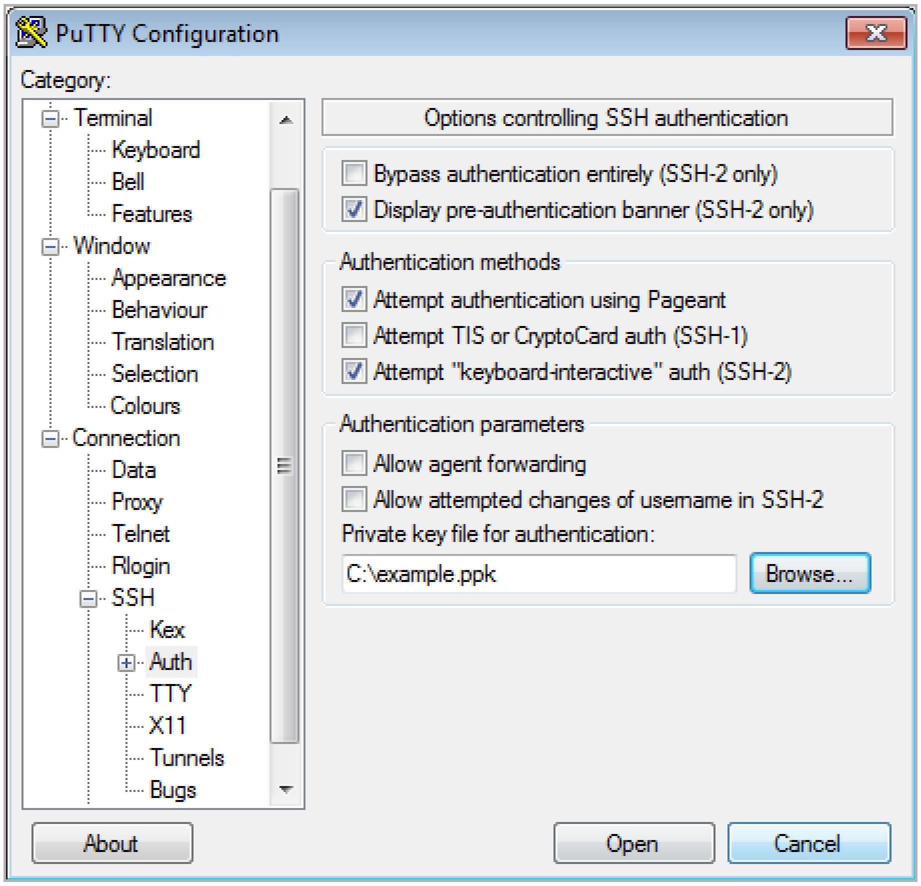
☑ Attempt authentication using Pageant
☐ Attempt TIS or CryptoCard auth (SSH-1)
☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

☐ Allow agent forwarding
☐ Allow attempted changes of username in SSH-2

Private key file for authentication:

4. Click **Browse**.



Options controlling SSH authentication

- □ Bypass authentication entirely (SSH-2 only)
- ☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

- ☑ Attempt authentication using Pageant
- □ Attempt TIS or CryptoCard auth (SSH-1)
- ☑ Attempt "keyboard-interactive" auth (SSH-2)

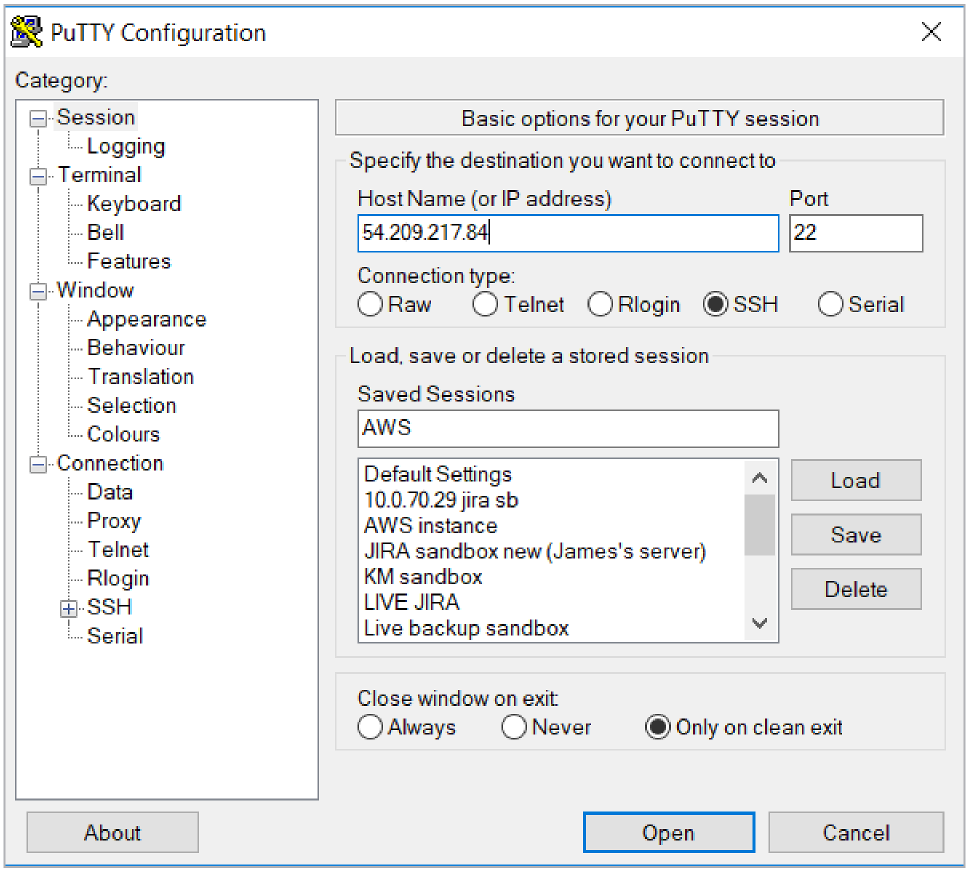
Authentication parameters

- □ Allow agent forwarding
- □ Allow attempted changes of username in SSH-2

Private key file for authentication: C:\example.ppk

5. Navigate to and select the key pair file that was exported in the **Licensing Options** section.

> If you are using a client that does not accept PEM you must convert the key pair file to another format, for example PPK for Putty. For instructions on how to do this, refer to the following TechRepublic article: Connect to Amazon EC2 with a private key using PuTTY and Pageant.



Specify the destination you want to connect to

Host Name (or IP address): 54.209.217.84

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

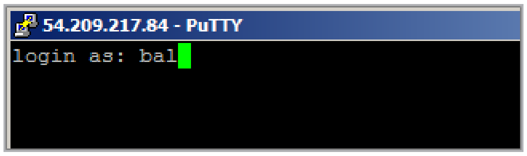
Saved Sessions: AWS

Default Settings
10.0.70.29 jira sb
AWS instance
JIRA sandbox new (James's server)
KM sandbox
LIVE JIRA
Live backup sandbox

Close window on exit: ○ Always ○ Never ● Only on clean exit

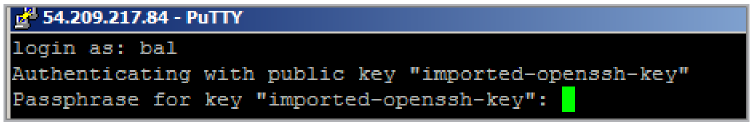
6. If desired, you can save the settings so that you do not have to perform these steps each time you open a Putty session for this IP address. To do this, enter a name in the **Saved Sessions** text box and click **Save**.

7. Click **Open**.



```
login as: bal
```

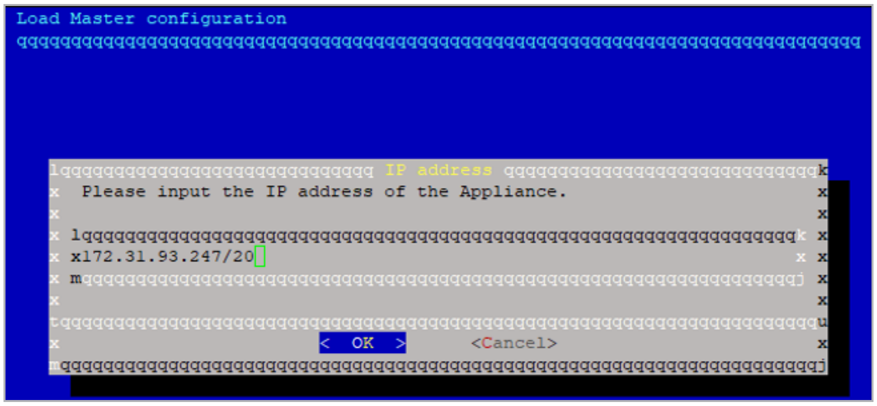
8. Log in with the username **bal**. This is the default LoadMaster username.



```
login as: bal
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":
```

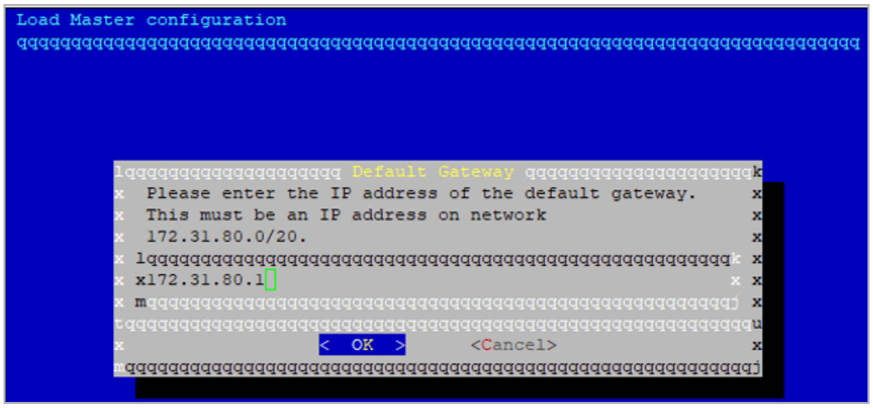
9. Enter the passphrase if you specified one to be used for the private key.

10. A number of screens appear relating to configuring various network options. These can be left as the default values but can be changed if needed. Press **OK** on each screen to proceed:



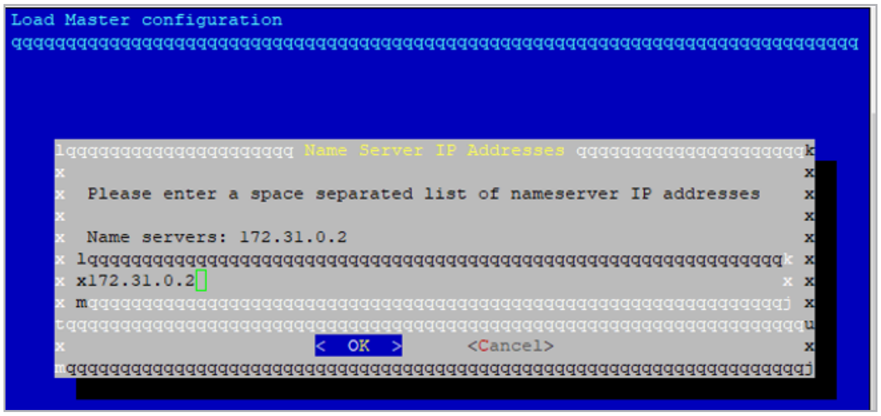
```
Load Master configuration

                         IP address
  Please input the IP address of the Appliance.

 172.31.93.247/20

                    <  OK  >       <Cancel>
```

a) A screen appears relating to the IP address.



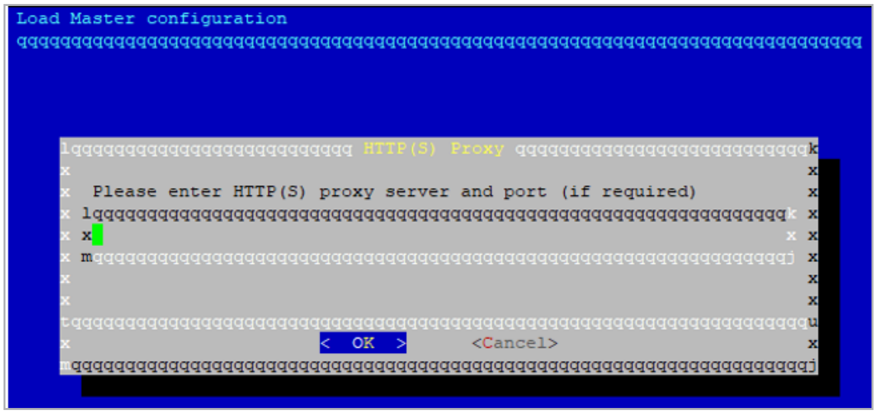
```
Load Master configuration

                   Default Gateway
  Please enter the IP address of the default gateway.
  This must be an IP address on network
  172.31.80.0/20.

 172.31.80.1

              <  OK  >       <Cancel>
```

b) The IP address for the default gateway should only be changed if you have an alternative gateway configured.



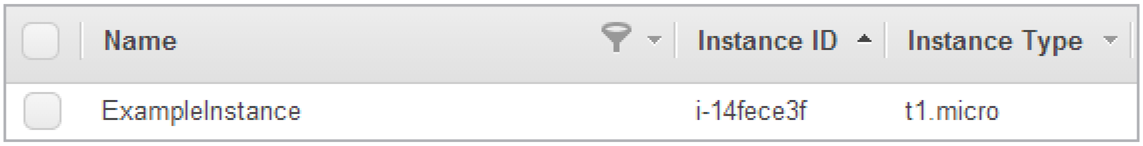
```
Load Master configuration

                  Name Server IP Addresses

  Please enter a space separated list of nameserver IP addresses

  Name servers: 172.31.0.2

 172.31.0.2

                    <  OK  >       <Cancel>
```

c) The default name server appears. You can optionally change this to an alternative name server if required.



```
Load Master configuration
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq

     lqqqqqqqqqqqqqqqqqqqqqqqqqqqq HTTP(S) Proxy qqqqqqqqqqqqqqqqqqqqqqqqqqqqk
     x                                                                       x
     x  Please enter HTTP(S) proxy server and port (if required)             x
     x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
     x x                                                                 x x
     x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
     x                                                                       x
     x                                                                       x
     tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
     x                    <  OK  >        <Cancel>                           x
     mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

d) Leave this option blank unless your environment requires a proxy server to access the internet.



□	Name	Instance ID ▲	Instance Type
□	ExampleInstance	i-14fece3f	t1.micro

11. If you selected an hourly licensing model, you are asked to enter the current LoadMaster password. By default, the password is set to the **Instance ID** which can be found in the AWS **EC2 Dashboard** by selecting **Instances** within the **INSTANCES** section of the main menu. Enter and confirm the new password.

The password must be reset to access the LoadMaster WUI. If you enter an incorrect password, you must restart SSH and go through the setup again.

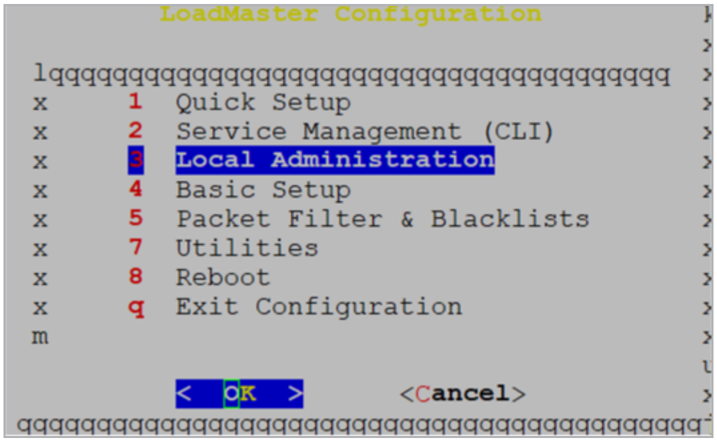
12. Log in with the new password.

13. Connect to the LoadMaster using a browser by entering **https://*InstanceAddress*:8443** in the address bar to continue configuration. The instance address can be the public IP address or the public DNS, both of which can be found in the EC2 Console in the **Description** tab.

If the first attempt to reset the password fails or if the WUI is not accessible, follow the steps in the **Restart Web Server Access - Hourly Licensing** section.

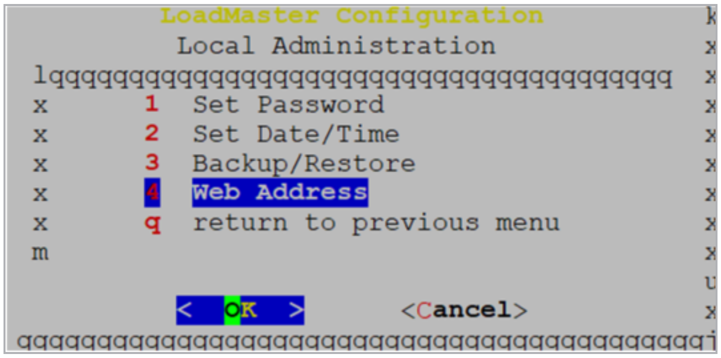
2.8.1 Restart Web Server Access - Hourly Licensing

If the first attempt to reset the password fails or if the WUI is not accessible, follow the steps below. The existing SSH session can be used, or a new SSH session can be opened using **bal** and the new password created in the **Initial Setup – Hourly Licensing** section.



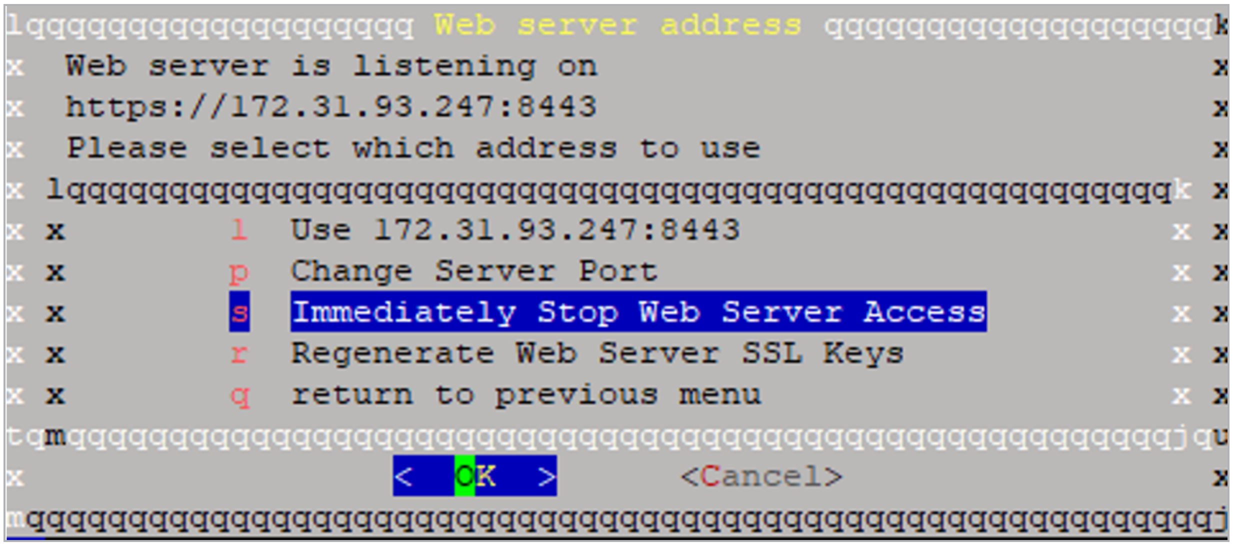
```
                 LoadMaster Configuration                     k
                                                              x
  lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq                    x
  x      1  Quick Setup                                       x
  x      2  Service Management (CLI)                          x
  x      3  Local Administration                              x
  x      4  Basic Setup                                       x
  x      5  Packet Filter & Blacklists                        x
  x      7  Utilities                                         x
  x      8  Reboot                                            x
  x      q  Exit Configuration                                x
  m                                                           x
                                                              u
            <  OK  >          <Cancel>                        x
 qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
```

1. On the main menu, select **Local Administration**.



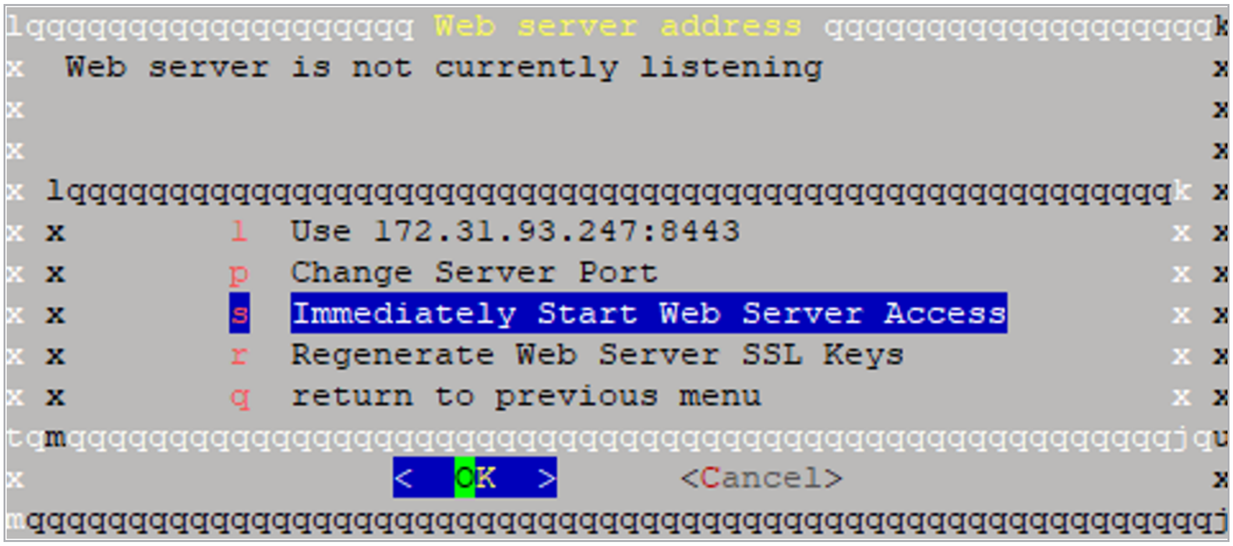
```
                 LoadMaster Configuration                     k
                   Local Administration                       x
  lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq                    x
  x       1  Set Password                                     x
  x       2  Set Date/Time                                    x
  x       3  Backup/Restore                                   x
  x       4  Web Address                                      x
  x       q  return to previous menu                          x
  m                                                           x
                                                              u
            <  OK  >          <Cancel>                        x
 qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

2. Select **Web Address**.



```
lqqqqqqqqqqqqqqqqqqqq Web server address qqqqqqqqqqqqqqqqqqqk
x  Web server is listening on                                 x
x  https://172.31.93.247:8443                                 x
x  Please select which address to use                         x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x        l  Use 172.31.93.247:8443                       x x
x x        p  Change Server Port                           x x
x x        s  Immediately Stop Web Server Access           x x
x x        r  Regenerate Web Server SSL Keys               x x
x x        q  return to previous menu                      x x
tqmqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqjqu
x              <  OK  >         <Cancel>                      x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

3. Select **Immediately Stop Web Server Access**.



```
lqqqqqqqqqqqqqqqqqqqq Web server address qqqqqqqqqqqqqqqqqqqk
x  Web server is not currently listening                      x
x                                                             x
x                                                             x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x        l  Use 172.31.93.247:8443                       x x
x x        p  Change Server Port                           x x
x x        s  Immediately Start Web Server Access          x x
x x        r  Regenerate Web Server SSL Keys               x x
x x        q  return to previous menu                      x x
tqmqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqjqu
x              <  OK  >         <Cancel>                      x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

4. Select **Immediately Start Web Server Access**.

5. Connect to the LoadMaster using a browser by entering **https://*InstanceAddress*:8443** in the address bar to continue configuration. The instance address can be the public IP address or the public DNS, both of which can be found in the EC2 console in the **Description** tab.

2.8.2 Initial Configuration – Hourly Licensing

If you chose an hourly licensing model, follow the steps below to initially set up the LoadMaster:

1. Open the VLM in a web browser by entering **https://*InstanceAddress*:8443** in the address bar. The instance address can be the public IP address or the public DNS, both of which can be found in the EC2 Console in the **Description** tab.

2. Acknowledge the self-signed certificate to proceed.

> The certificate used by the WUI takes the public name used by AWS.

3. Accept the End User License Agreement (EULA).

4. A screen appears asking if you are OK with the LoadMaster regularly contacting Kemp to check for updates and other information. Click the relevant button to proceed.

A prompt appears asking for the username and password. Enter **bal** as the username and the password that was set previously. The LoadMaster is now licensed and is ready for administration and configuration.

2.9 Initial Setup – BYOL

When using the BYOL method, the normal LoadMaster licensing and activation process is used. Access the LoadMaster using the WUI by entering the Public Address, preceded with **https://** and followed by **:8443**. Then, proceed through the steps and license the LoadMaster.

To use the BYOL option, follow the steps below:

1. Deploy the **BYOL – Trial and perpetual license** version of the VLM (follow the steps in the **Start a New Instance** section).

2. When the LoadMaster deploys successfully, connect to the LoadMaster WUI, for example, **https://52.45.31.111:8443**.

3. Acknowledge the self-signed certificate to proceed.

4. Accept the EULA.

5. Enter your Kemp ID and password to obtain a trial license. If you have an Order ID#, enter it now to apply the purchased license. If you do not have an Order ID#, you can proceed with these steps and then enter an Order ID# later after contacting a Kemp representative to purchase a license (see steps below).

6. Select your license and click **Continue**.

7. A screen appears asking if you are OK with the LoadMaster regularly contacting Kemp to check for updates and other information. Click the relevant button to proceed.

8. Enter a new password for the default **bal** account and click **Set password**.

If you did not enter the Order ID# during the initial configuration, follow the steps below to license the LoadMaster:

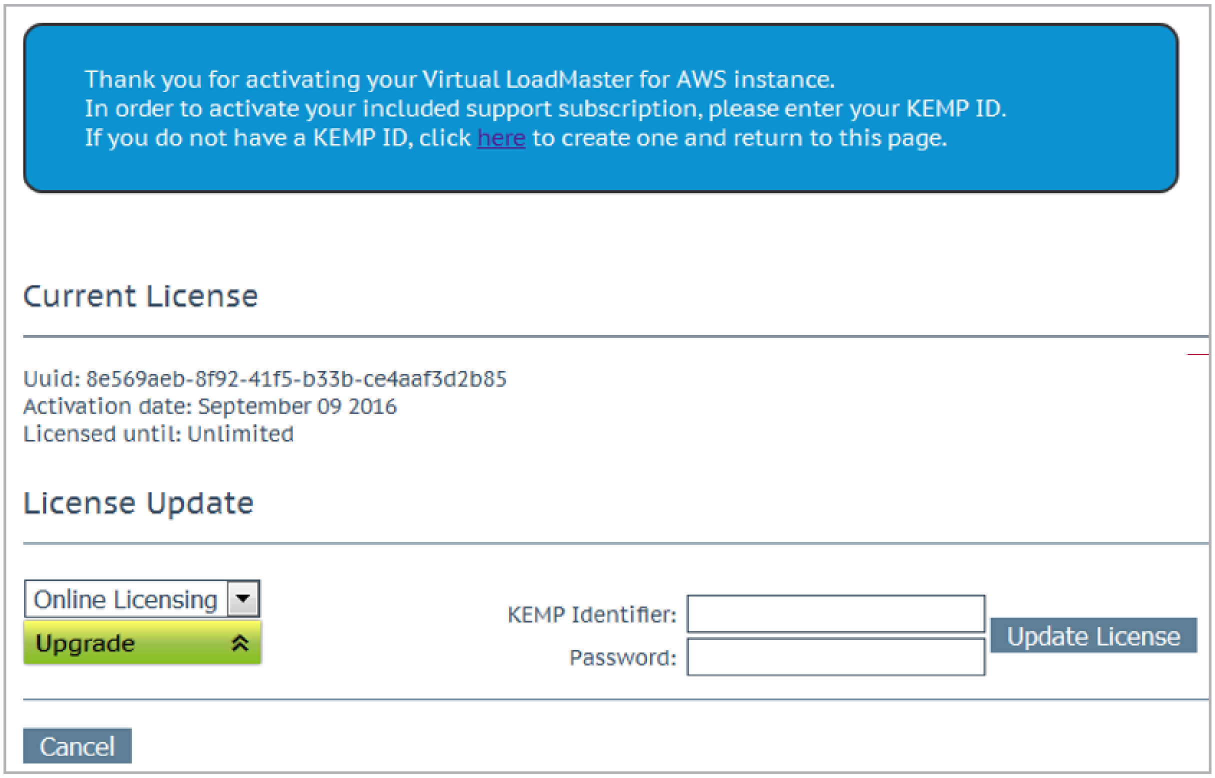
1. Contact a Kemp representative to get a license.

2. Log in to the LoadMaster WUI and navigate to **System Configuration > System Administration > Update License**.

3. Enter your Kemp ID and Password to update the license.

2.10 Activate your Support Subscription

If you are using a Pay Per Use (Hourly Usage) LoadMaster, three days after initially setting up the LoadMaster, a prompt appears asking you to activate your support subscription. Enter your **Kemp ID** and **Password** and click **Update License** to do this.



Thank you for activating your Virtual LoadMaster for AWS instance.
In order to activate your included support subscription, please enter your KEMP ID.
If you do not have a KEMP ID, click here to create one and return to this page.

Current License

Uuid: 8e569aeb-8f92-41f5-b33b-ce4aaf3d2b85
Activation date: September 09 2016
Licensed until: Unlimited

License Update

You can activate your support subscription before three days by expanding **System Configuration > System Administration**, clicking the **Update License** option and filling in your Kemp ID and password.

Kemp recommends rebooting the LoadMaster after updating the license.

3 LoadMaster Firmware Downgrades

It is best practice to keep the Kemp LoadMaster firmware at the latest version. In the event an issue occurs after an upgrade to the latest firmware version, the system can be rolled back to the previous version.

You can find steps for upgrading/downgrading the LoadMaster firmware at the following link:

Updating the LoadMaster Software

> 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.

4 LoadMaster Backup and Restore

Kemp provides several methods to backup and restore configuration and certificates on the LoadMaster. Depending on the Recovery Point Objective (RPO) and Recovery Time Objective (RTO), you can take these backups manually or automatically on a daily or weekly schedule. For information on the backup and restore features, refer to this Technical Note: Backup and Restore Technical Note

5 Monitoring LoadMaster Health in AWS

Refer to the sections below for details on monitoring LoadMaster health.

5.1 Monitoring with Kemp 360

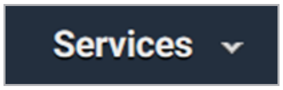
Kemp provides network and application owners with the necessary tools to maintain and monitor the application delivery infrastructure:

Product	Description	Link
Kemp 360 Central	Management and control of application delivery controllers	https://kemptechnologies.com/kemp360/central/
Kemp 360 Vision	Proactive monitoring of application delivery controllers and application health	https://kemptechnologies.com/kemp360/vision/

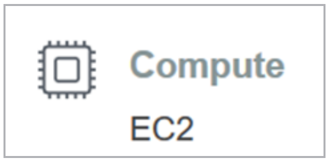
5.2 Monitoring with AWS

AWS provides monitoring on the system and instances. These status checks can be leveraged to alert on certain outages such as in an availability zone or region. You can configure status check alerts to email an administrator in such an event. This section outlines the configuration of status check alerts:

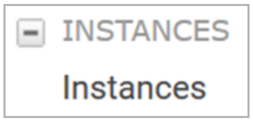
1. Log in to the AWS console.



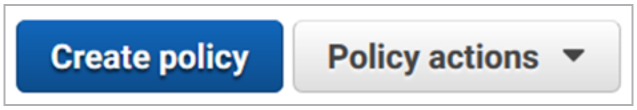
2. Click **Services**.



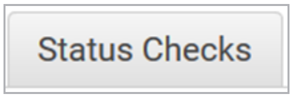
3. Under **Compute**, select **EC2**.



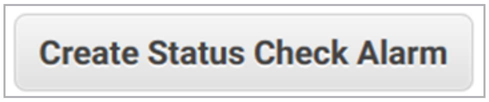
4. In the navigation on the left, click **Instances**.



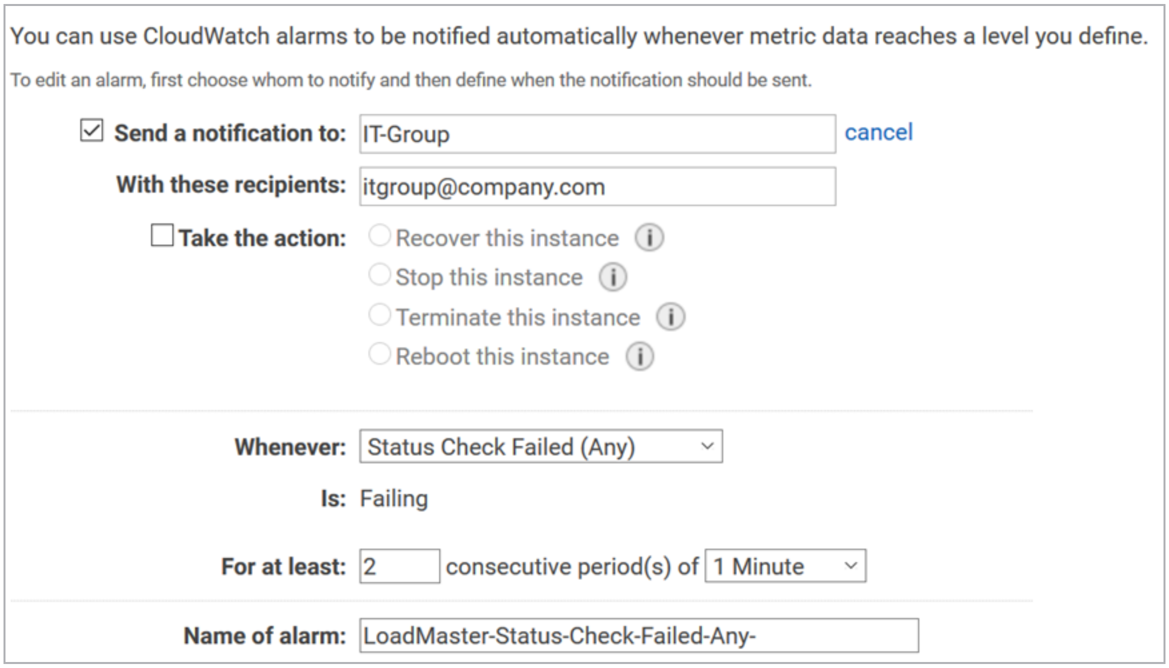
5. Click the relevant instance to create an alarm for.



6. Click **Status Checks**.



7. Click **Create Status Check Alarm**.



You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

☑ **Send a notification to:** IT-Group cancel

With these recipients: itgroup@company.com

□ **Take the action:**
○ Recover this instance
○ Stop this instance
○ Terminate this instance
○ Reboot this instance

Whenever: Status Check Failed (Any)

Is: Failing

For at least: 2 consecutive period(s) of 1 Minute

Name of alarm: LoadMaster-Status-Check-Failed-Any-

8. Complete the following fields:

a) Type a name for the notification group.

b) Type an email address for alarms to be sent to.

c) Select **Status Check Failed (Any)** in the **Whenever** drop-down list.

d) Keep the default interval of **2 consecutive period(s) of 1 Minute**.

e) Type a unique name for the alarm in the **Name of alarm** text box.

9. Click **Create Alarm**.

References

While the instructions above provide a basic overview of how to deploy and configure LoadMaster for AWS, it is not designed to be a comprehensive guide to configure every possible workload. This section identifies some of many guides published on our resources section of our website. Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation.

LoadMaster Licensing, Feature Description

ESP, Feature Description

SSL Accelerated Services, Feature Description

Kemp Web Application Firewall, Feature Description

Web User Interface (WUI), Configuration Guide

HA for AWS, Feature Description

Last Updated Date

This document was last updated on 07 December 2020.