Progress®
Kemp® LoadMaster®

Installation Guide LoadMaster for AWS GovCloud

Generated on: 18 December 2024

Copyright

Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend: Product Documentation Copyright Notice & Trademarks | Progress

Table of Contents

Chapter 1: Introduction 5

Document Purpose 6

Intended Audience 7

Supported AWS Instance types 8

Prerequisites 8

Chapter 2: LoadMaster for AWS GovCloud 9

Prerequisites 9

Differences from the Virtual LoadMaster (VLM) 10

Licensing Options 10

Security Best Practices 11

IAM Service 11

Access Keys 15

Storing Secrets 17

Create a New Key Pair 17

Start a New Instance 19

Initial Setup – Hourly Licensing 24

Restart Web Server Access - Hourly Licensing 31

Initial Configuration – Hourly Licensing 33

Initial Setup – BYOL 33

Activate your Support Subscription 37

Chapter 3: LoadMaster Firmware Downgrades 39

Chapter 4: LoadMaster Backup and Restore 40

Best Practices for Backups 40

Chapter 5: Monitoring LoadMaster Health in AWS 42

Monitoring with Kemp 360 Central 42

Monitoring with AWS 42

Chapter 6: References 45

1

Introduction

Amazon Web Services (AWS) GovCloud is a cloud service from Amazon aimed specifically at the United States government. It is designed to enable US government agencies and customers to move sensitive workloads into the cloud by addressing specific regulatory and compliance requirements - for example, the International Traffic in Arms Regulations (ITAR) which governs how defense-related data is managed and stored. Specifically, GovCloud segregates the data both logically and physically to ensure that it is only accessible by designated individuals within the United States.

The Progress Kemp Application Delivery Controller (ADC), Virtual LoadMaster, is available in AWS GovCloud Marketplace. Providing resilient pervasive secure delivery of applications within the AWS GovCloud, the Virtual LoadMaster guarantees high availability, ensures security of the application servers, and simplifies integration with on-premises infrastructure.

The AWS GovCloud platform enables existing on-premises applications to be easily provisioned in the cloud, providing customers the benefit of scalability, elasticity, and shift of capital expenses to operational ones.

Progress Kemp's Virtual LoadMaster (VLM) is a full-featured, advanced Layer 4-7 load balancer that supports a variety of workloads. Available in two versions, Bring Your Own License (BYOL) and the perpetual free license, the VLM provides the required throughput at the right price.

Along with advanced scheduling methods, intelligent traffic steering and support for multiple protocols, the VLM also provides Global Site Load Balancing (GSLB), RESTful, Python and PowerShell Application Program Interfaces (APIs).

In addition, the LoadMaster includes integration of the FIPS 140-2 certified encryption module, and supports security features such as access control lists, Web Application Firewall (WAF), Distributed Denial of Service (DDoS) protection, and multiple authentication methods, including: Kerberos Constrained Delegation (KCD), Department of Defense (DoD) Common Access Card (CAC) and Federal Personal Identity Verification (PIV) smart card, and Single Sign-On (SSO).

Some of the features and associated benefits of the VLM are listed in the table below.

Feature	Benefit
Application ubiquity	Regardless of where the applications are deployed (cloud, on premises, or in hybrid environments) the VLM can load balance them.
Hybrid enhancement	The VLM manages applications deployed in hybrid infrastructures on premises and in AWS GovCloud.
Scalable	Highly available ADCs, deployed on-demand to meet load requirements.
Resilient	VLM GEO load balancing supports application instances across multiple sites to accommodate growth and deliver additional resilience.

Related Links

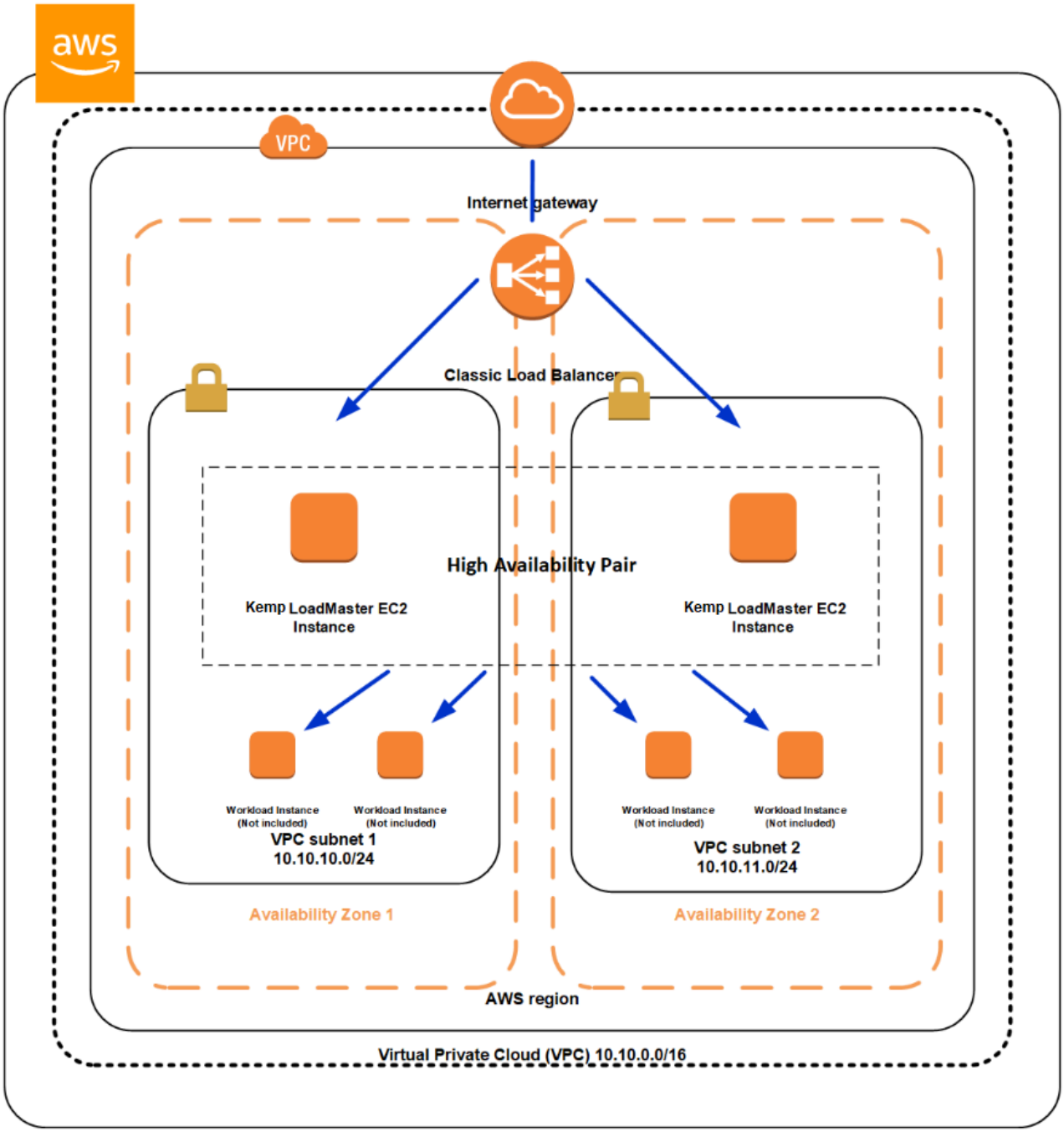
For details, see the following topics:

- Document Purpose
- Intended Audience
- Supported AWS Instance types
- Prerequisites

Document Purpose

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

It is also possible to configure the LoadMaster using Application Program Interface (API) commands. For further details, please refer to the Interface Description documents on the documentation page: https://docs.progress.com/.



Intended Audience

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

Supported AWS Instance types

In LoadMaster version 7.2.55 and above, the VLMs in the AWS Marketplace support Nitro based instance types. These Nitro based instances enable AWS to innovate faster with an ever-broadening selection of compute, storage, memory, and networking options. It also delivers added benefits such as:

- Enhanced security that continuously monitors, protects, and verifies the instance hardware and firmware.
- Reduce cost with better performance.

For further information, refer to the Amazon EC2 Instance Types.

Prerequisites

There are some perquisites to be aware of before following the steps in this document:

- Users should be familiar with the operation of AWS.
- If not already done, create a Progress ID at the registration page: https://sso.kemptechnologies.com/register
- Users should have access and be logged-in to the AWS GovCloud Management Console.

2

LoadMaster for AWS GovCloud

Refer to the following sections for details on deploying a LoadMaster in AWS GovCloud.

Related Links

For details, see the following topics:

- Prerequisites
- Differences from the Virtual LoadMaster (VLM)
- Licensing Options
- Security Best Practices
- Create a New Key Pair
- Start a New Instance
- Initial Setup – Hourly Licensing
- Initial Setup – BYOL
- Activate your Support Subscription

Prerequisites

Some requirements to be aware of when deploying a LoadMaster in AWS GovCloud 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.

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 GovCloud.

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

Note: 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.

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

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 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)

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

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.

IAM Service

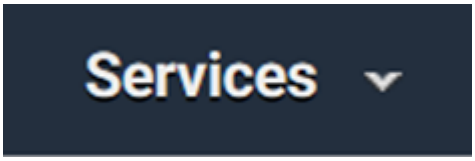
IAM is a centralized service that manages users, credentials, policies, and keys for the resources deployed in AWS. You should create individual accounts for each user that creates or accesses AWS resources. When possible, you should enable AWS Multi-Factor Authentication (MFA) for the IAM user account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

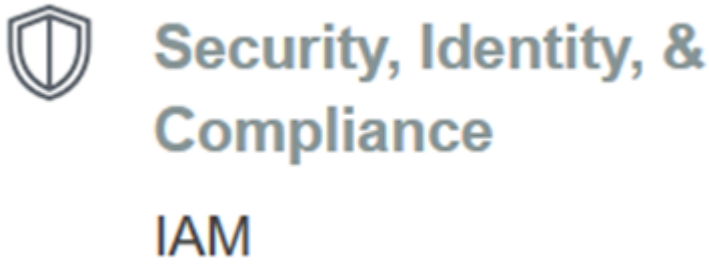
Create an IAM Policy

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

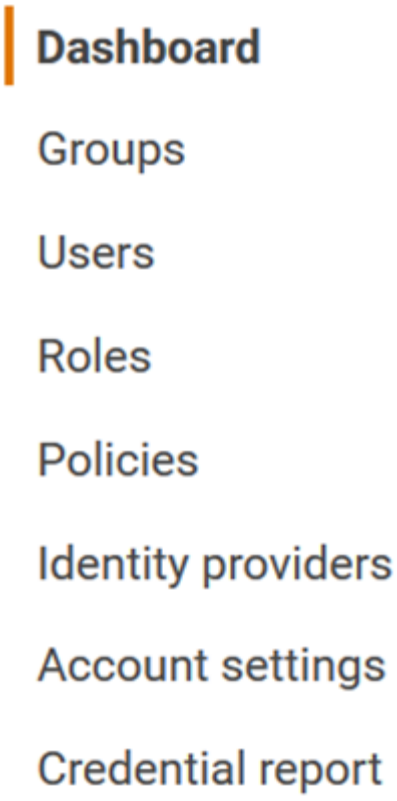
1. Log in to the AWS console.



2. Click **Services**.



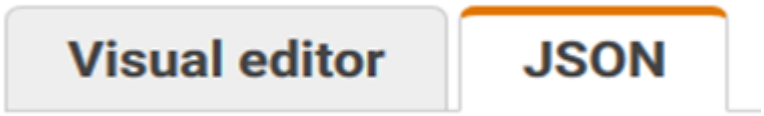
3. Under **Security, Identity, & Compliance**, select **IAM**.



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



5. Click **Create policy**.



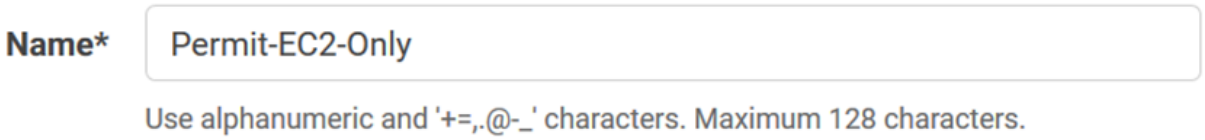
6. Select **JSON**.

```
{
    "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**.



9. Enter a unique **Name**.



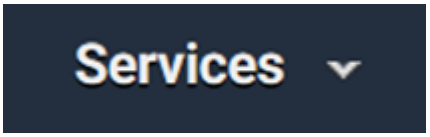
10. Click **Create policy**.

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

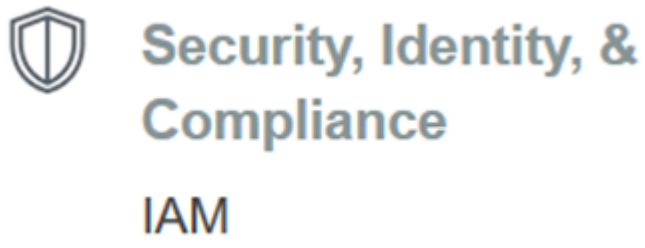
Assign an IAM Policy to an IAM User

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

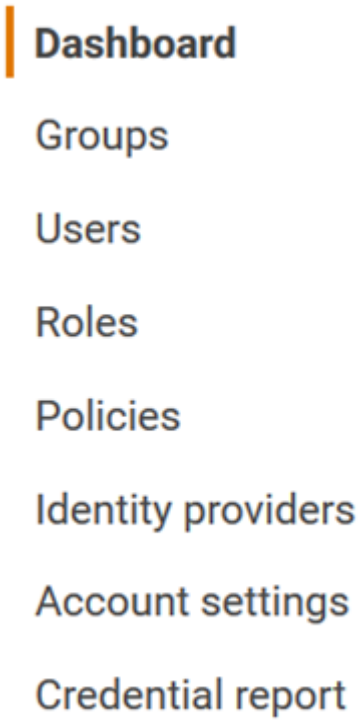
1. Log in to the AWS console.



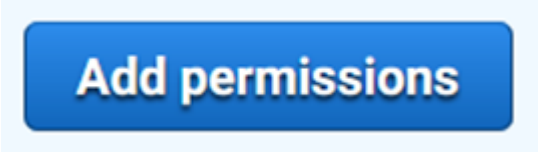
2. Click **Services**.



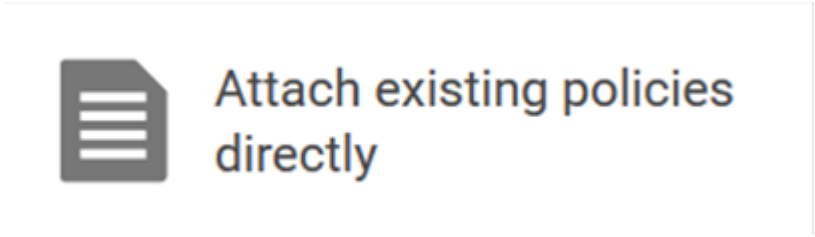
3. Under **Security, Identity, & Compliance**, select **IAM**.



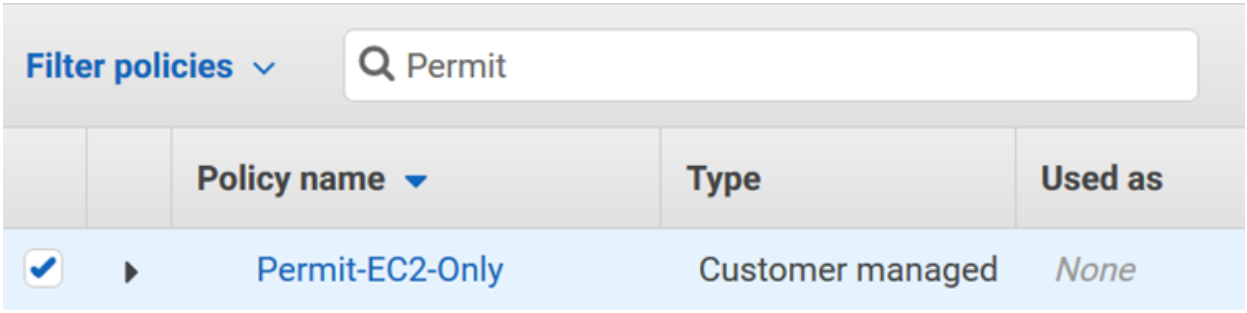
4. Select **Users**.
5. From the list of users, select the user to assign the policy to.



6. Click **Add permissions**.



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



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



9. Click **Next: Review**.



10. Click **Add permissions**.

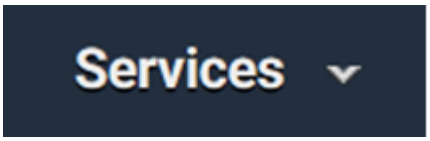
Access Keys

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.

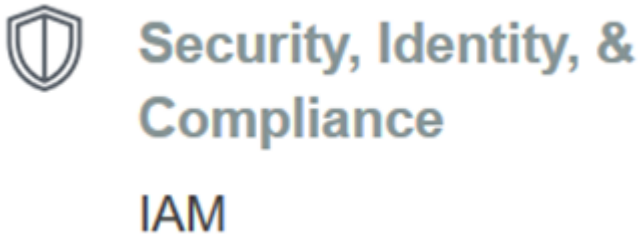
Rotate Access Key and Secret Key

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

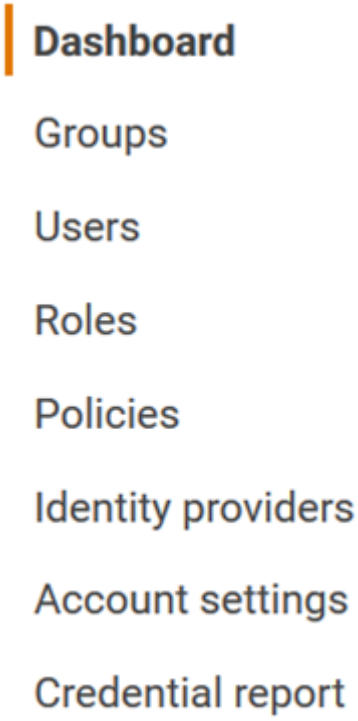
1. Log in to the AWS console.



2. Click **Services**.



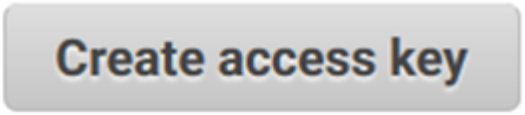
3. Under **Security, Identity, & Compliance**, select **IAM**.



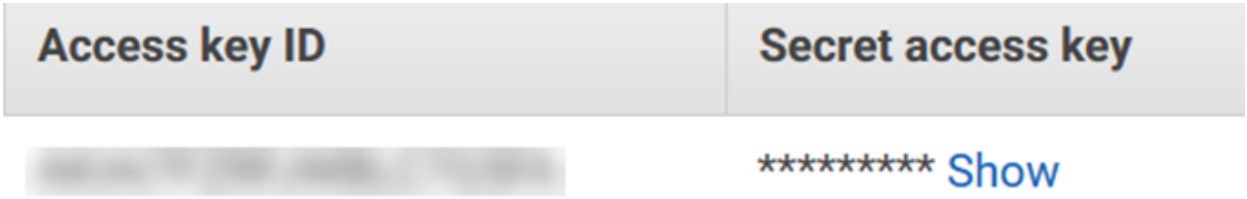
4. Select **Users**.
5. From the list of users, select the user to manage.



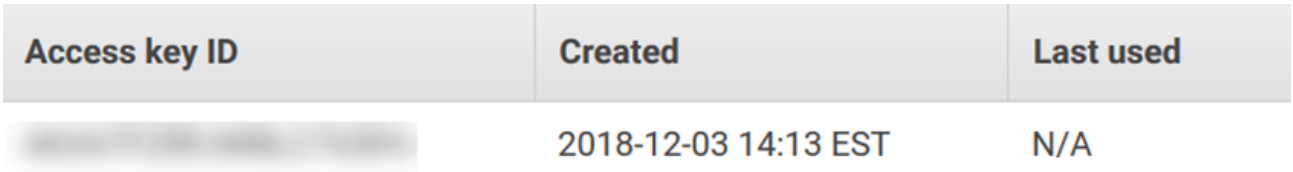
6. Click **Security credentials**.



7. Click **Create access key**.



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



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.

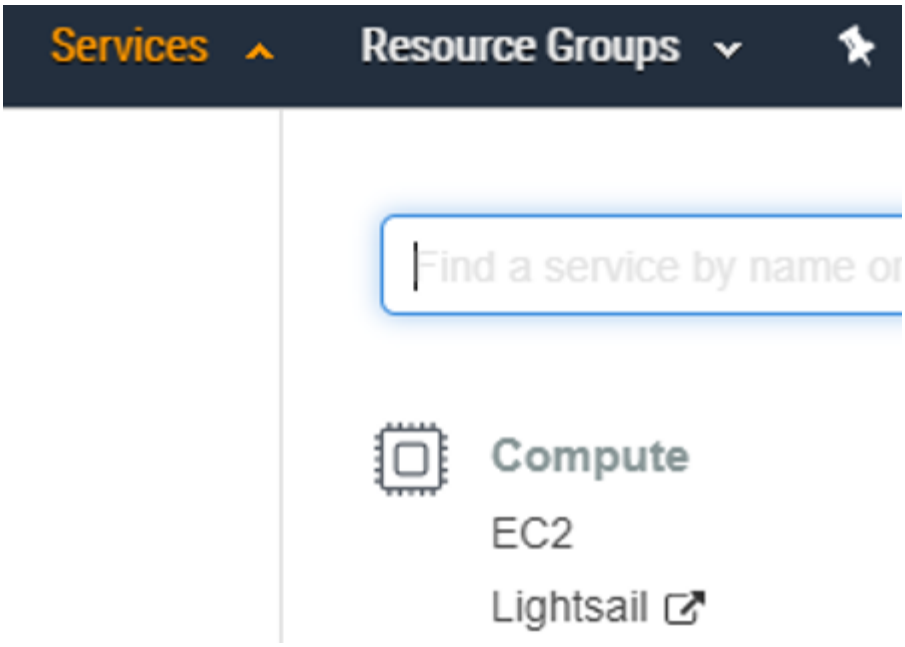
Storing Secrets

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

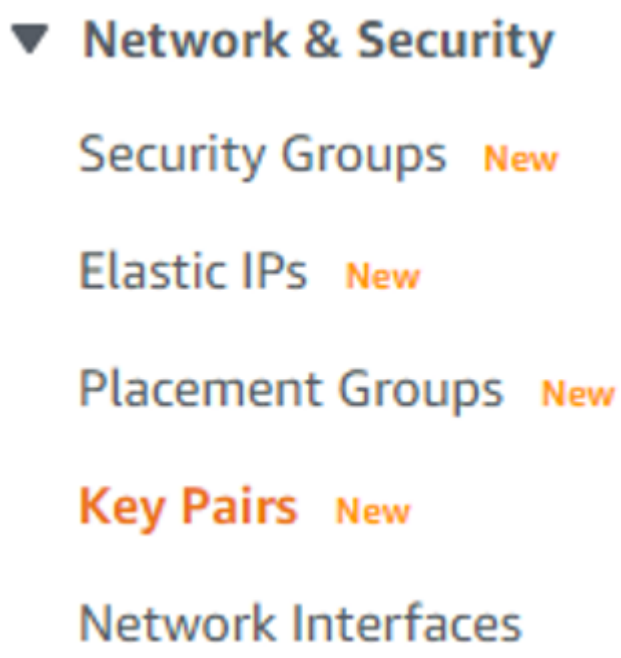
Create a New Key Pair

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:

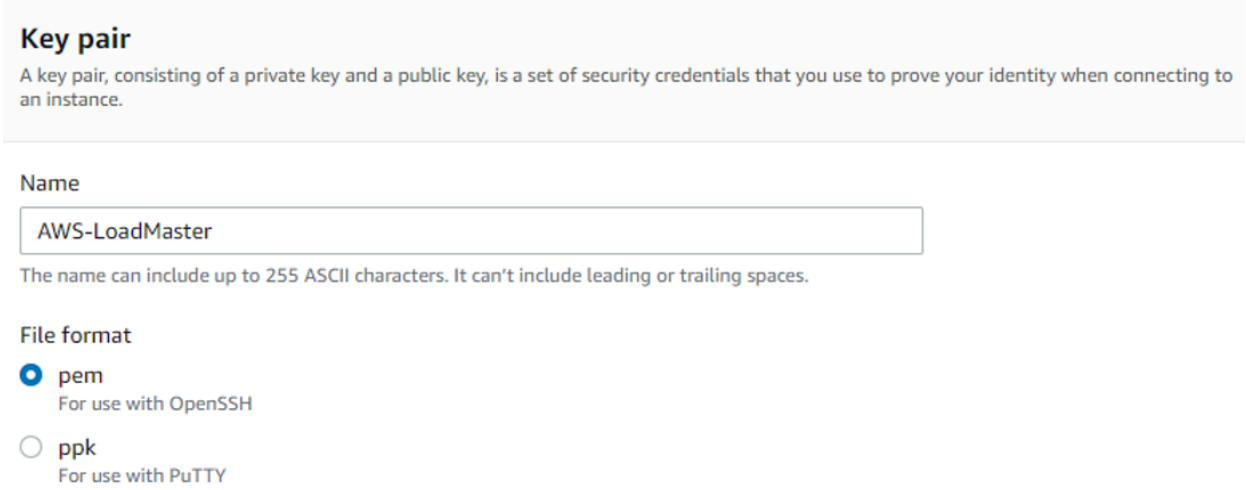
1. Log in to the AWS console.



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



3. In the main menu, select **Key Pairs**.
4. Click **Create Key Pair**.



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

Note: 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.

Note: 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>

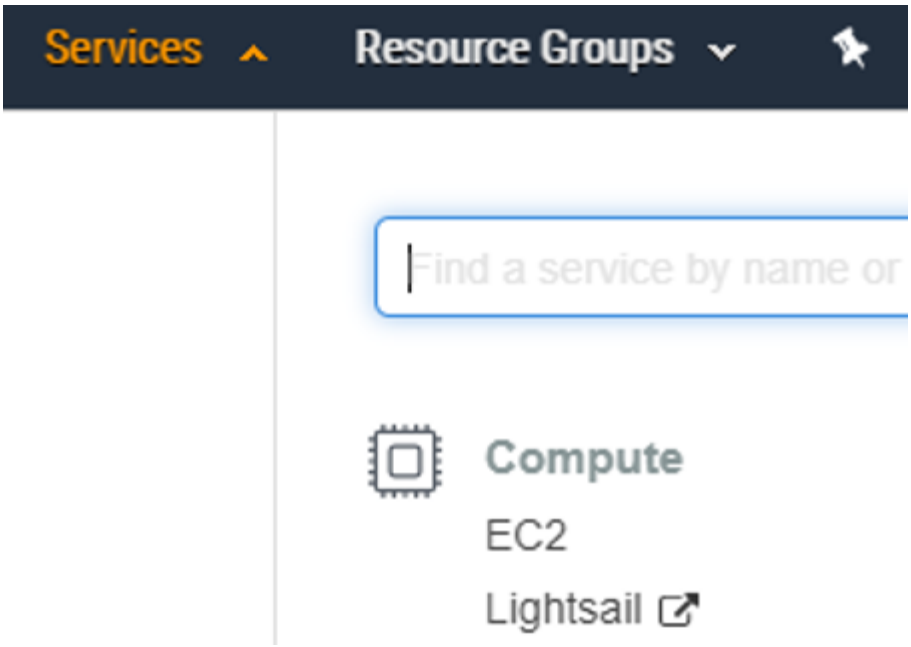
Start a New Instance

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

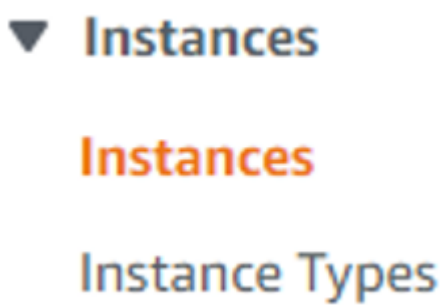
To start an instance, follow the steps below:

Note: 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.



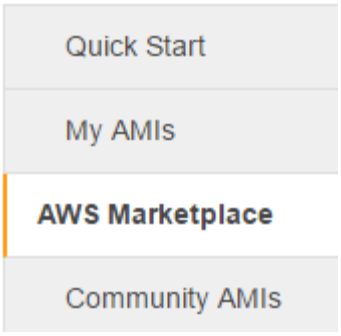
2. Click **Services** and **EC2**.



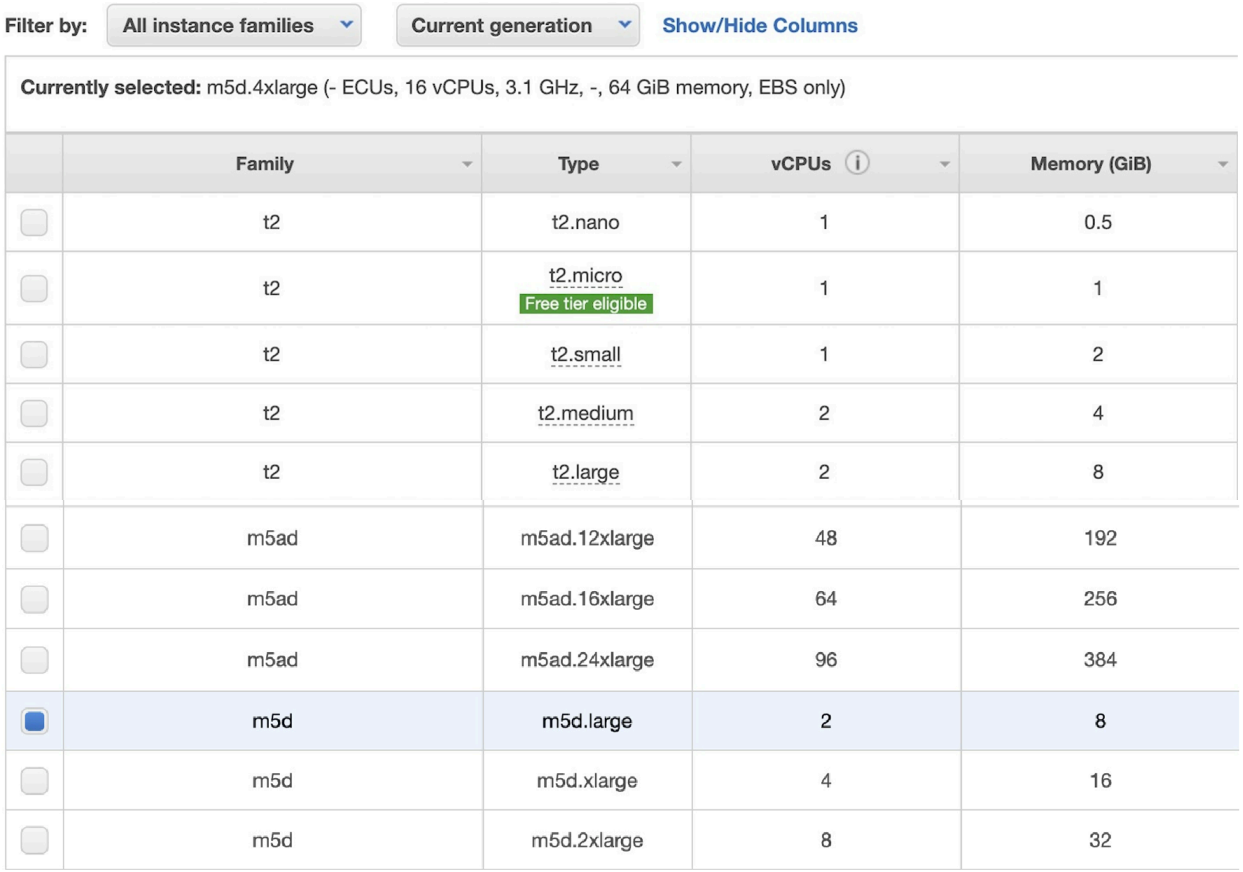
3. Click **Instances**.



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.



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

Note: All Nitro Instances are supported on the VLMs. For further information on Nitro instances, refer to the following Amazon link: Amazon EC2 Nitro.



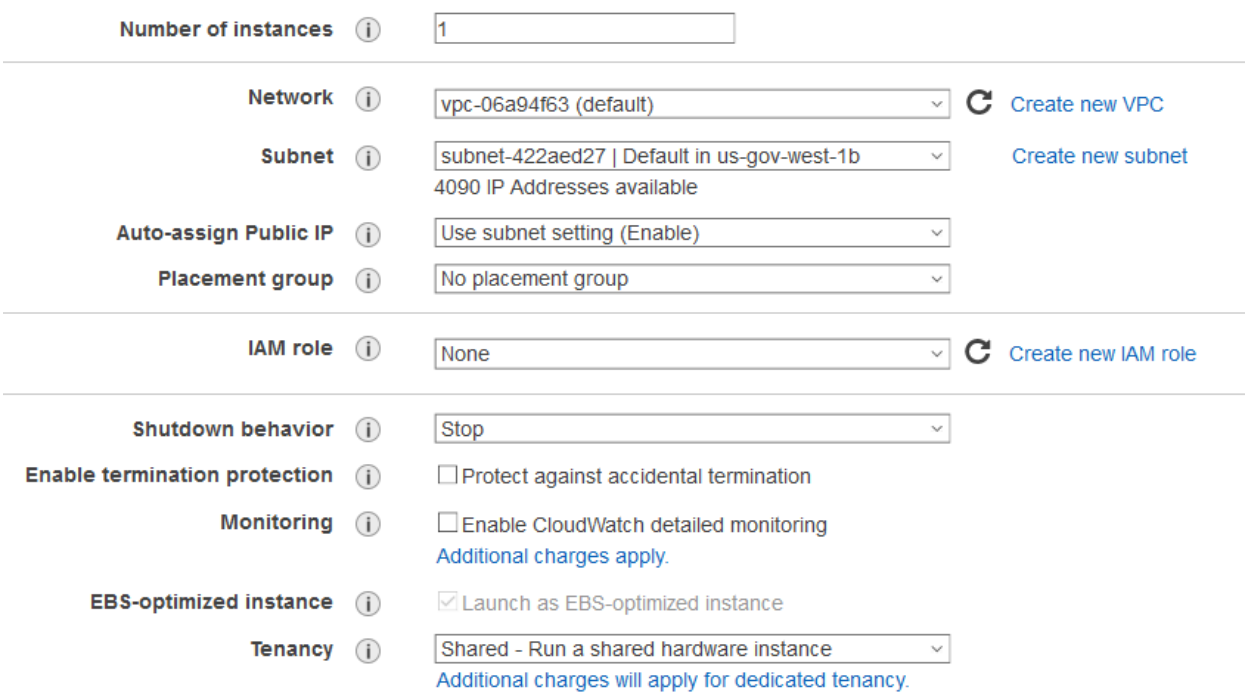
Note: For further information on instance types, refer to the following Amazon link: Amazon EC2 Instance Types.

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

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

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

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



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

Note: 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.

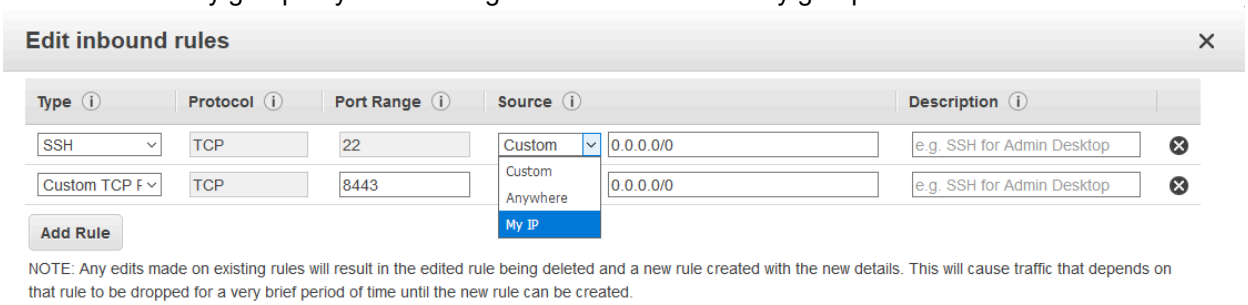
12. Ensure that the **Auto-assign Public IP** option is set to **Enable**.

13. Configure any other setting as needed.
14. Click **Next: Add Storage**.
15. Keep the defaults and click **Next: Add Tags**.

Note: 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.



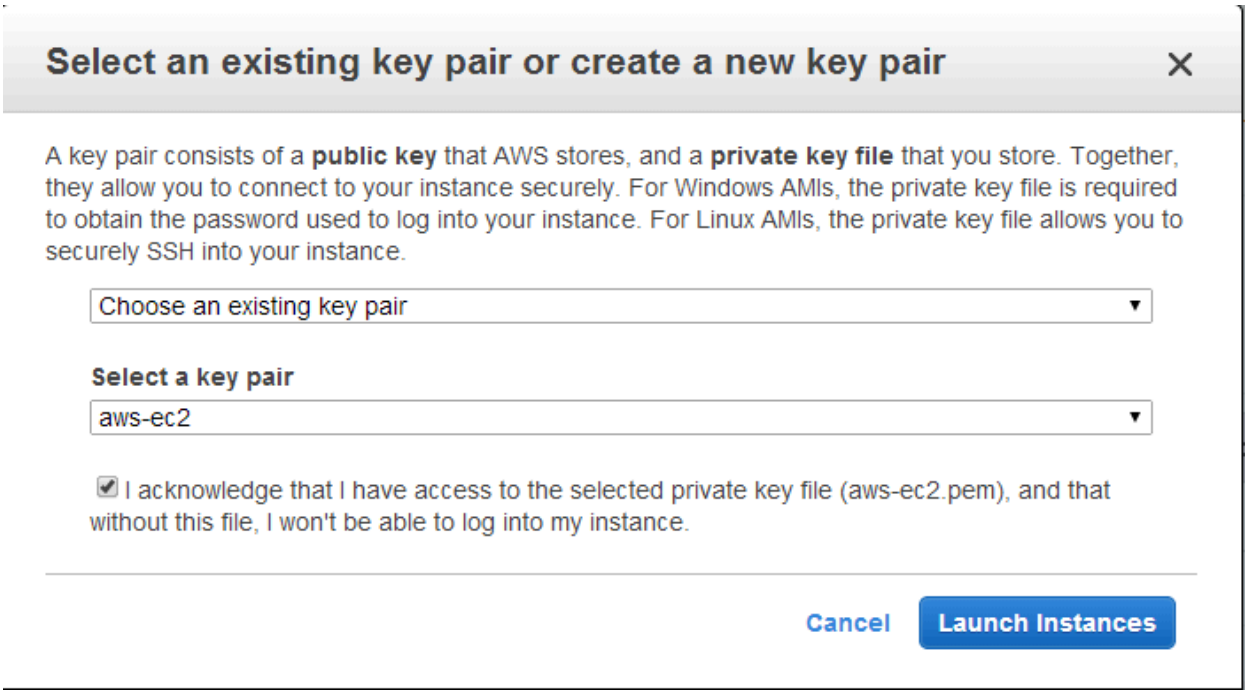
19. The following rules are needed in the security group:

    - 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

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

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

20. 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.
21. Click **Review and Launch**.
22. Click **Launch**.



23. 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.
24. Select the check box.
25. Click **Launch Instances**.

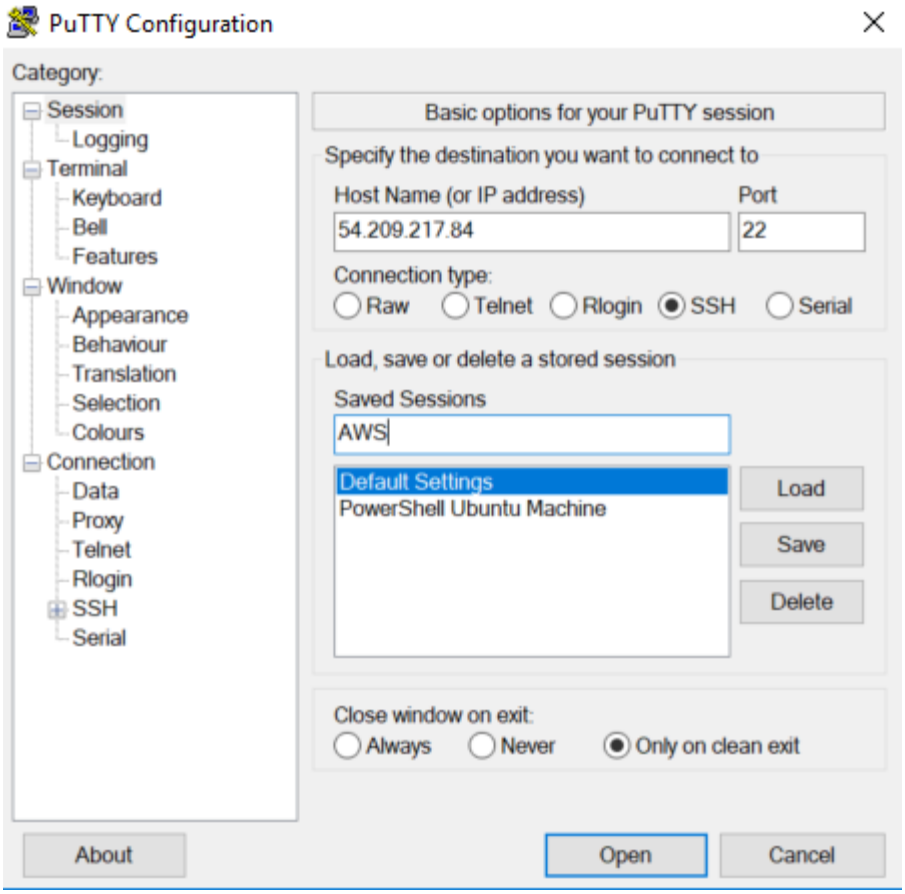


26. Click **View Instances**. The **Public IP** address or **Public DNS** address can be used to connect to the instance using HTTPS on port 8443.
27. After your instance state is **Running** , you can connect to your LoadMaster instance.

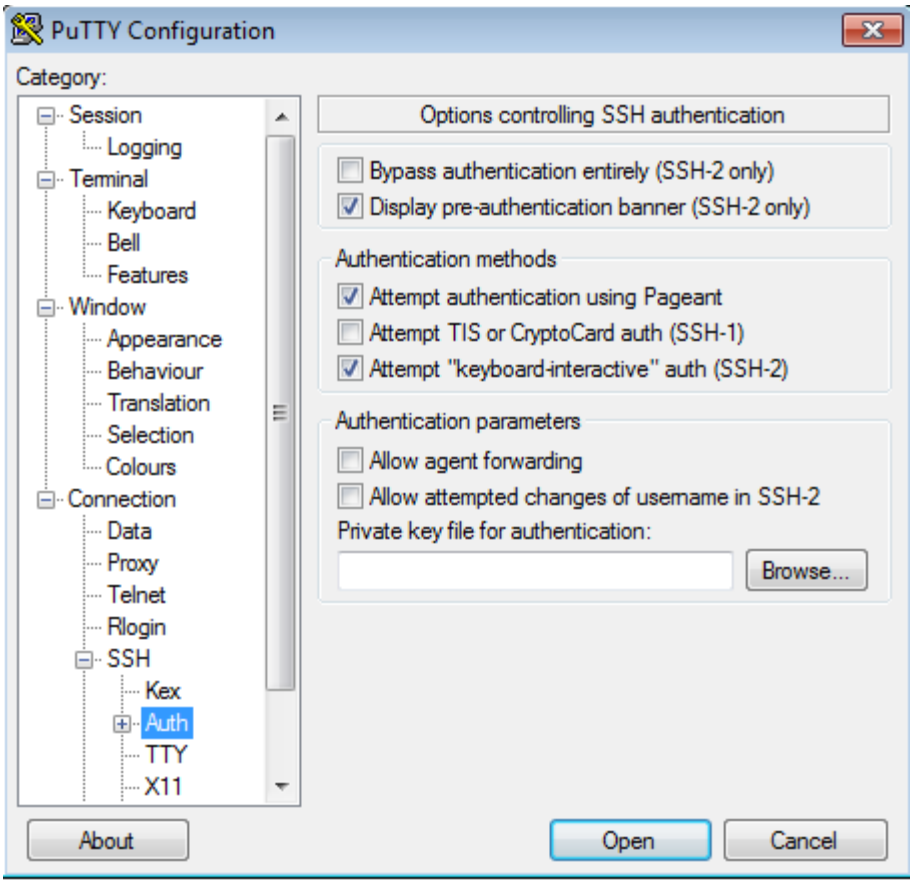
Initial Setup – Hourly Licensing

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.

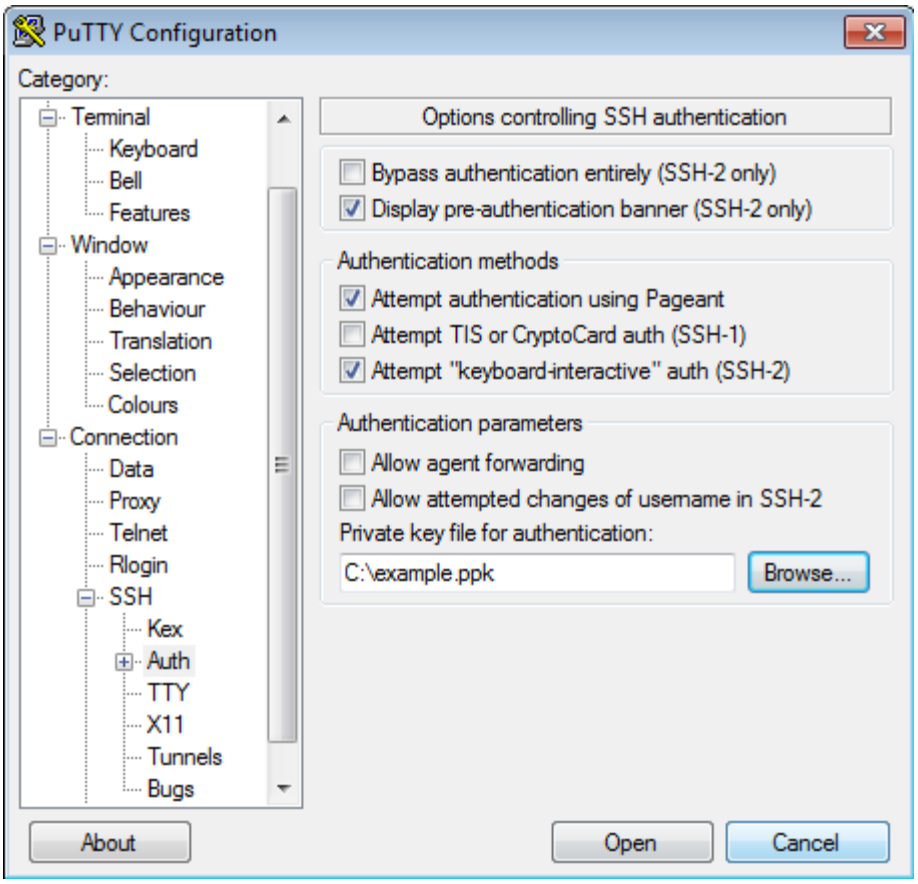
1. Open the PuTTY client.



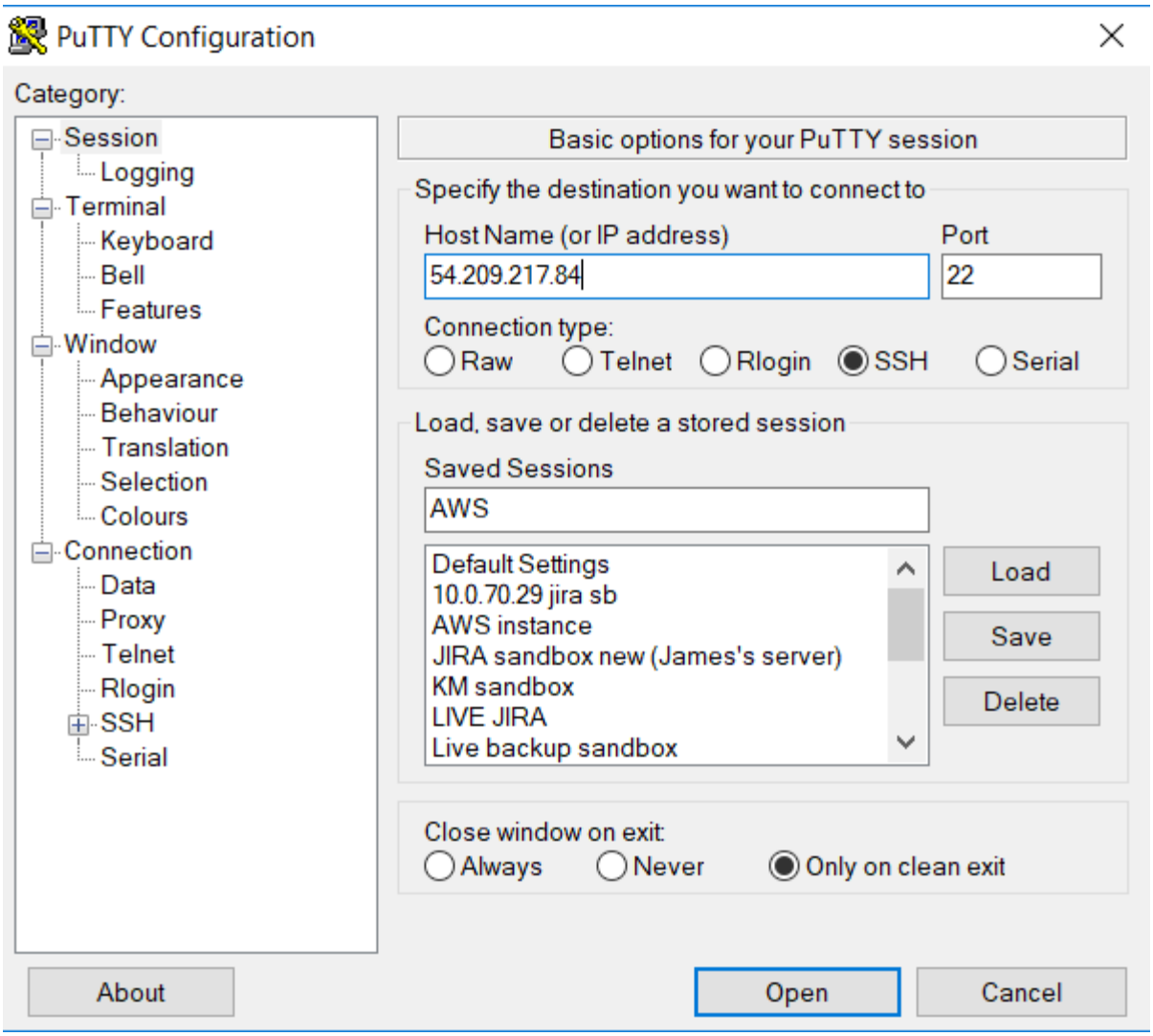
2. Enter the **IP address** of the LoadMaster instance. This is the IP address obtained in the Start a New Instance section.
3. In the main menu, navigate to **Connection > SSH > Auth**.



4. Click **Browse**.

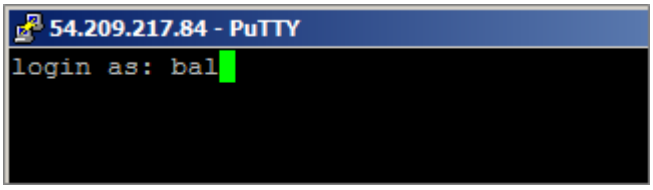


5. Navigate to and select the key pair file that was exported in the Licensing Options section.

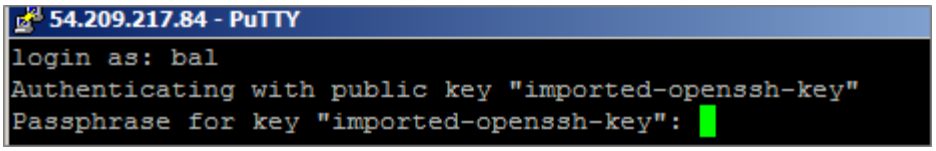


Note: If you are using a client that does not accept PEM you must convert the key pair file to another format, for example PPK for Putty. For instructions on how to do this, refer to the following TechRepublic article: Connect to Amazon EC2 with a private key using PuTTY and Pageant.

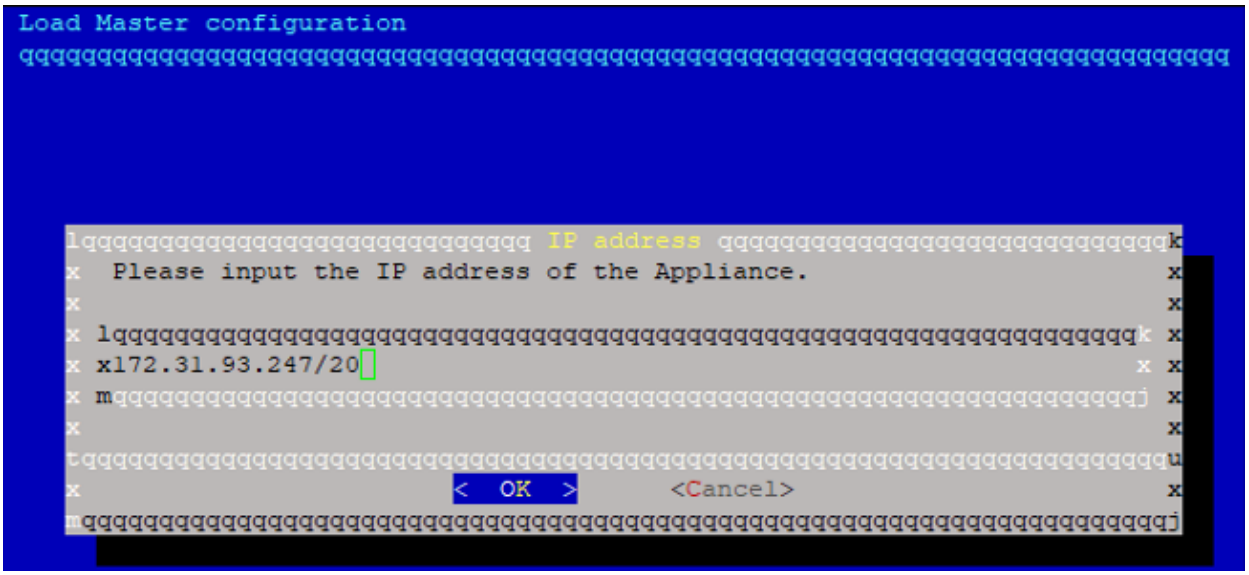
6. If desired, you can save the settings so that you do not have to perform these steps each time you open a Putty session for this IP address. To do this, enter a name in the **Saved Sessions** text box and click **Save**.
7. Click **Open**.



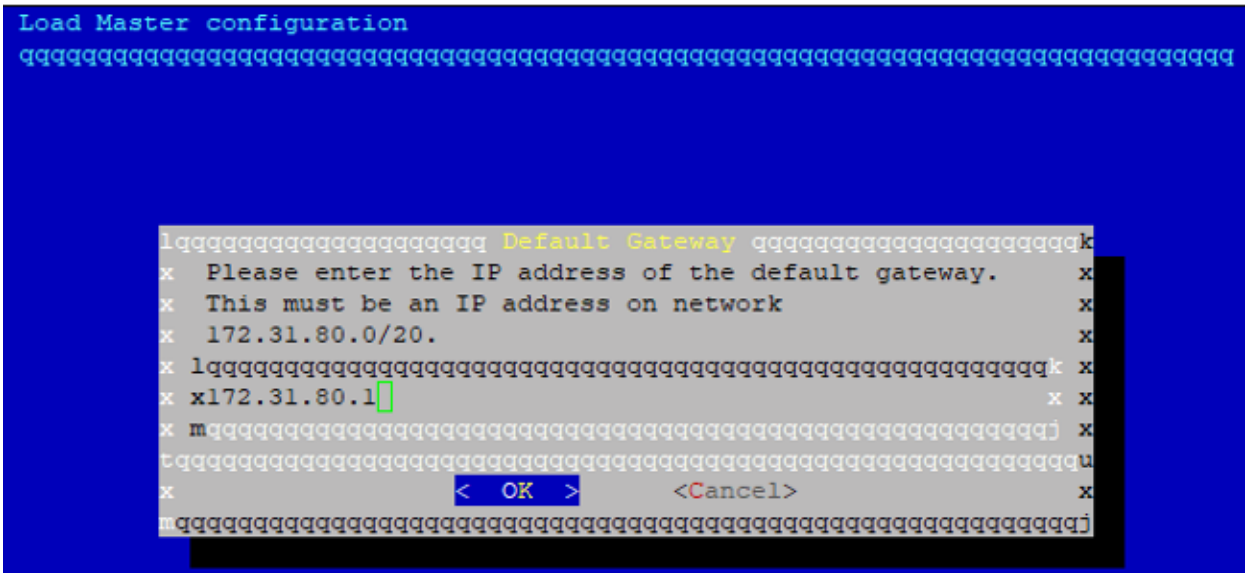
8. Log in with the username **bal**. This is the default LoadMaster username.



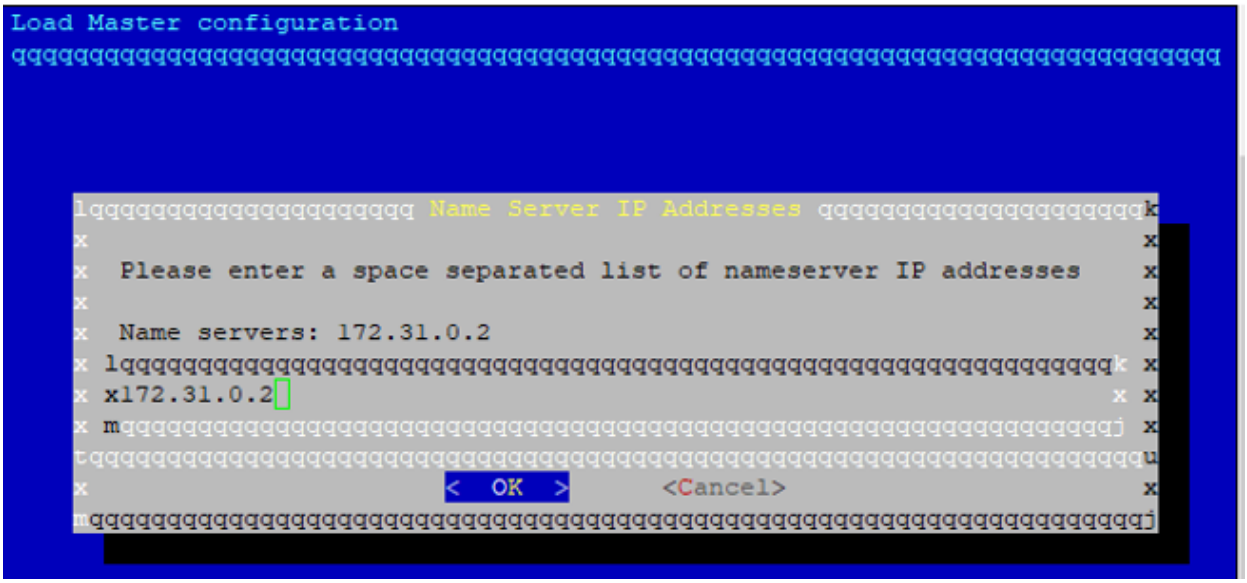
9. Enter the passphrase if you specified one to be used for the private key.
10. A number of screens appear relating to configuring various network options. These can be left as the default values but can be changed if needed. Press **OK** on each screen to proceed:



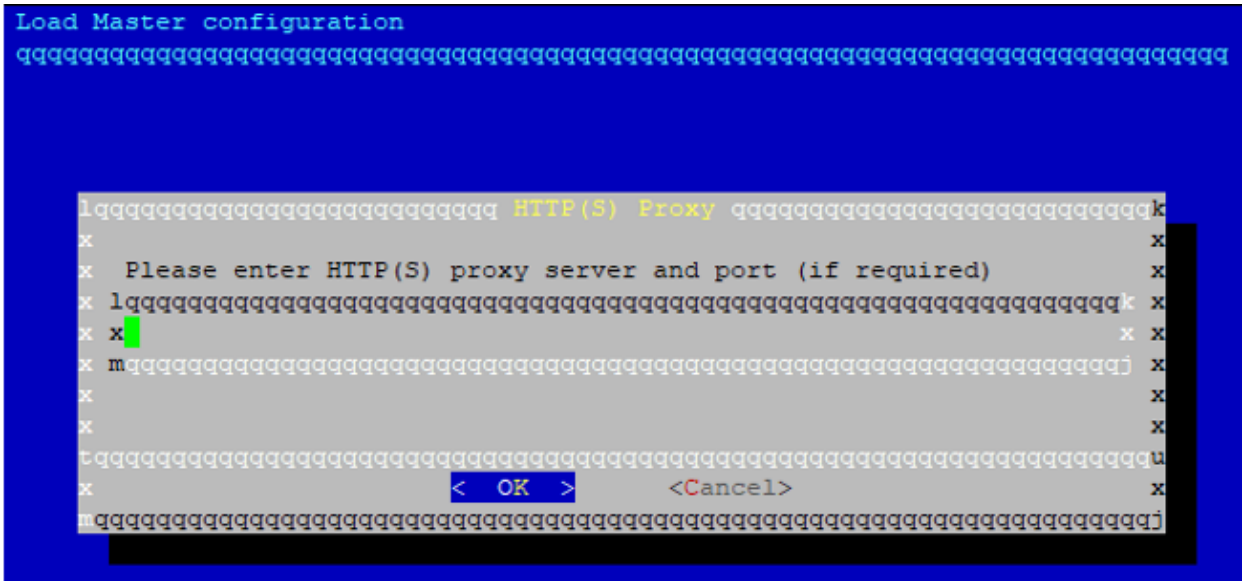
11. A screen appears relating to the IP address.



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



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



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



15. 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.

Note: The password must be reset to access the LoadMaster WUI. If you enter an incorrect password,

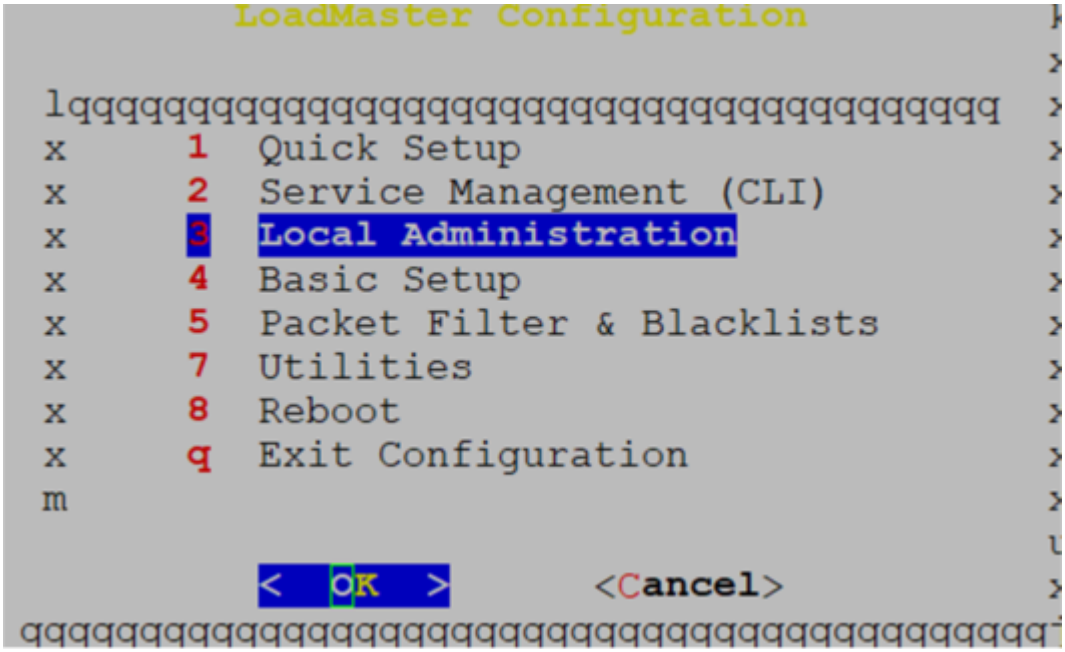
you must restart SSH and go through the setup again.

16. Log in with the new password.
17. 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.

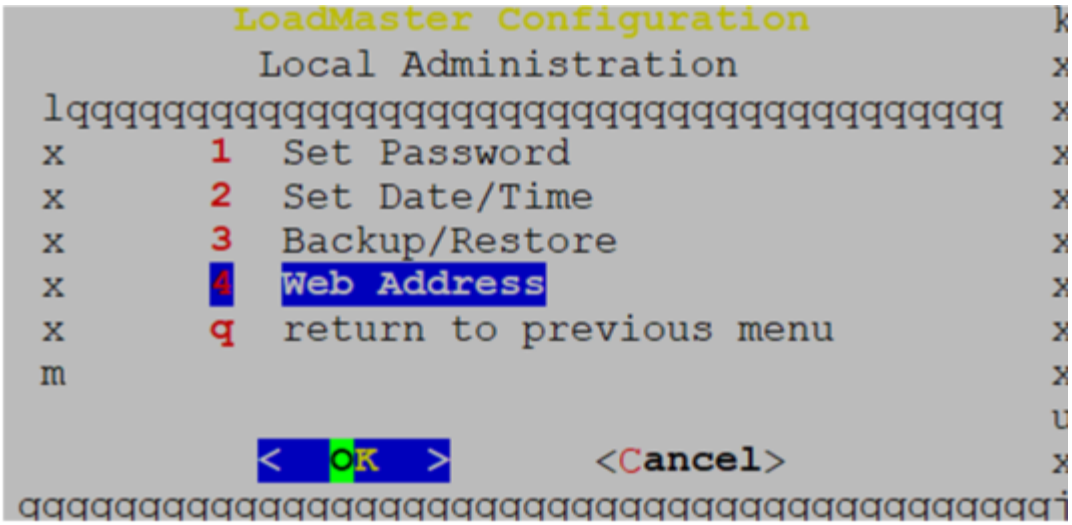
Note: If the first attempt to reset the password fails or if the WUI is not accessible, follow the steps in the Restart Web Server Access - Hourly Licensing section.

Restart Web Server Access - Hourly Licensing

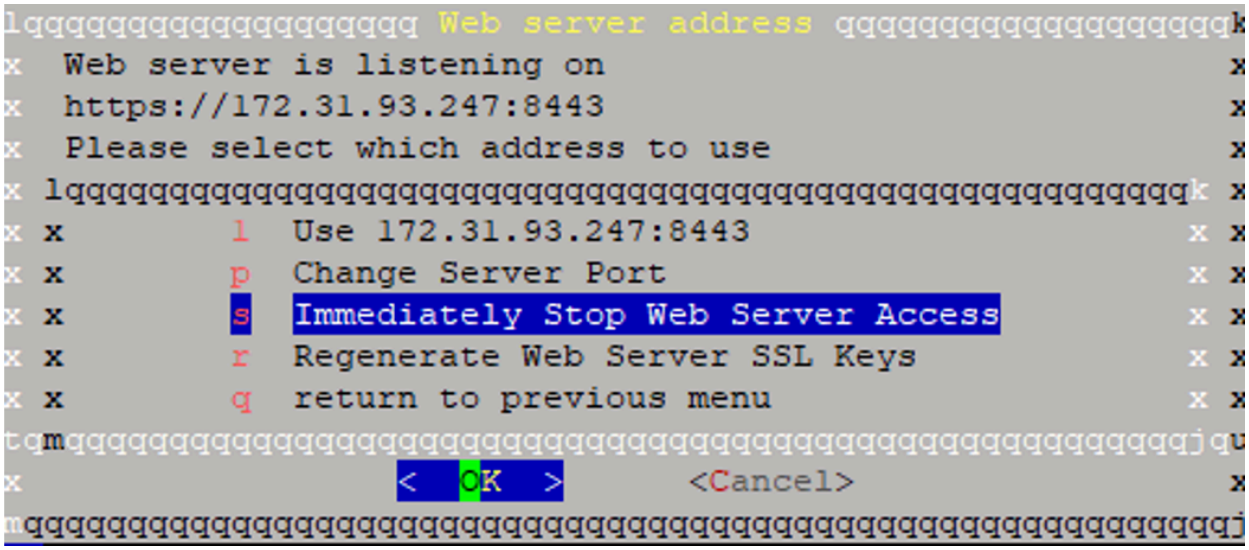
If the first attempt to reset the password fails or if the WUI is not accessible, follow the steps below. The existing SSH session can be used, or a new SSH session can be opened using **bal** and the new password created in the Initial Setup – Hourly Licensing section.



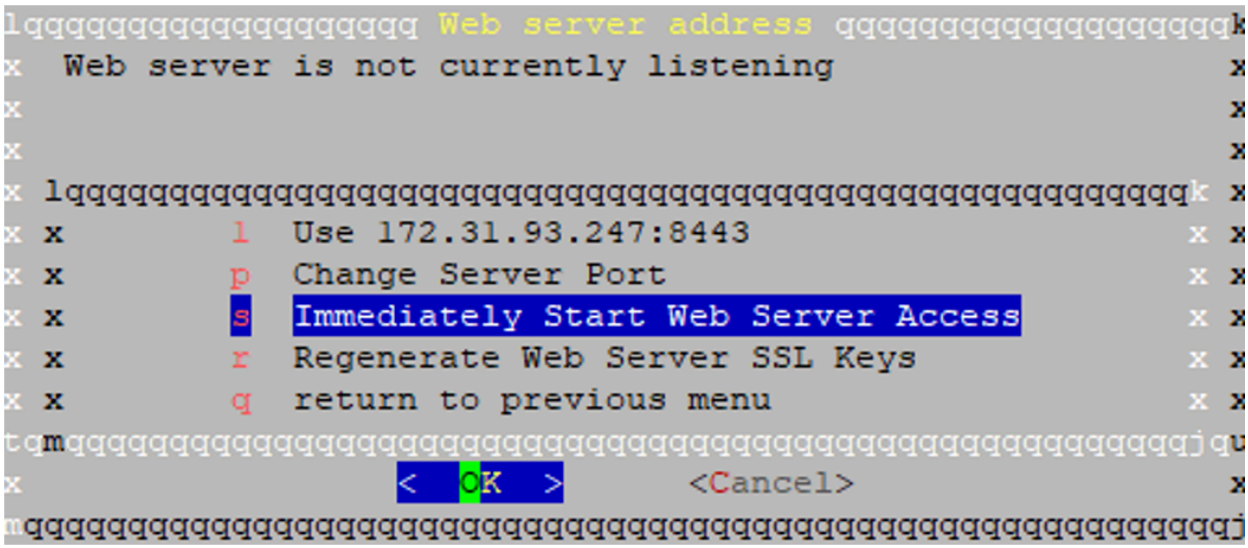
1. On the main menu, select **Local Administration**.



2. Select **Web Address**.



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



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.

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.

   Note: 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 Progress 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.

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).

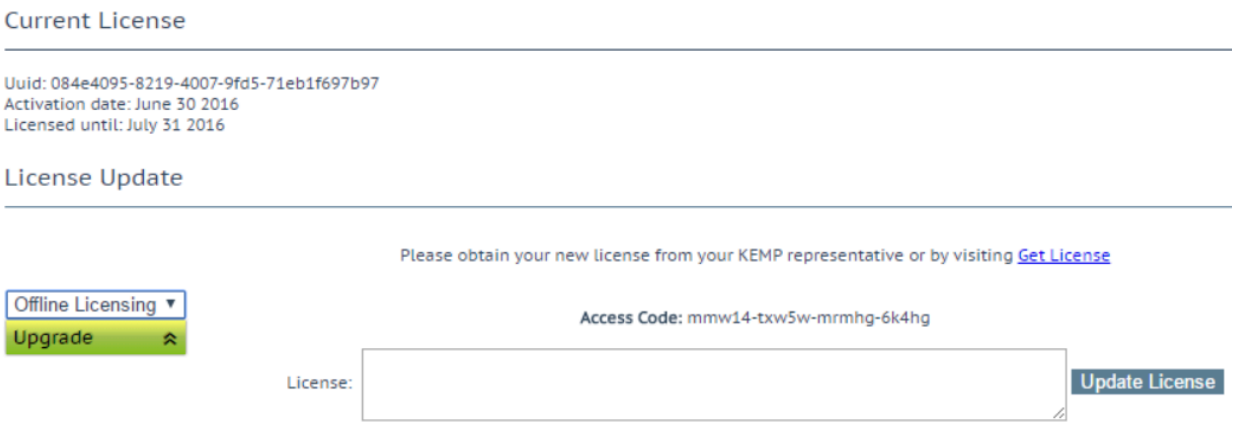
2. When the LoadMaster deploys successfully, connect to the LoadMaster WUI, for example, **https://52.45.31.111:8443**.
3. Acknowledge the self-signed certificate to proceed.
4. Accept the EULA.
5. Enter your Progress ID and password to obtain a trial license. If you have an Order ID#, enter it now to 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 Progress 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 Progress 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 Progress Kemp representative to get a license.
2. Log in to the LoadMaster WUI and navigate to **System Configuration > System Administration > License Management**.
3. Enter your Progress ID and Password to update the license.

   To get the license text using the **Get License** link:

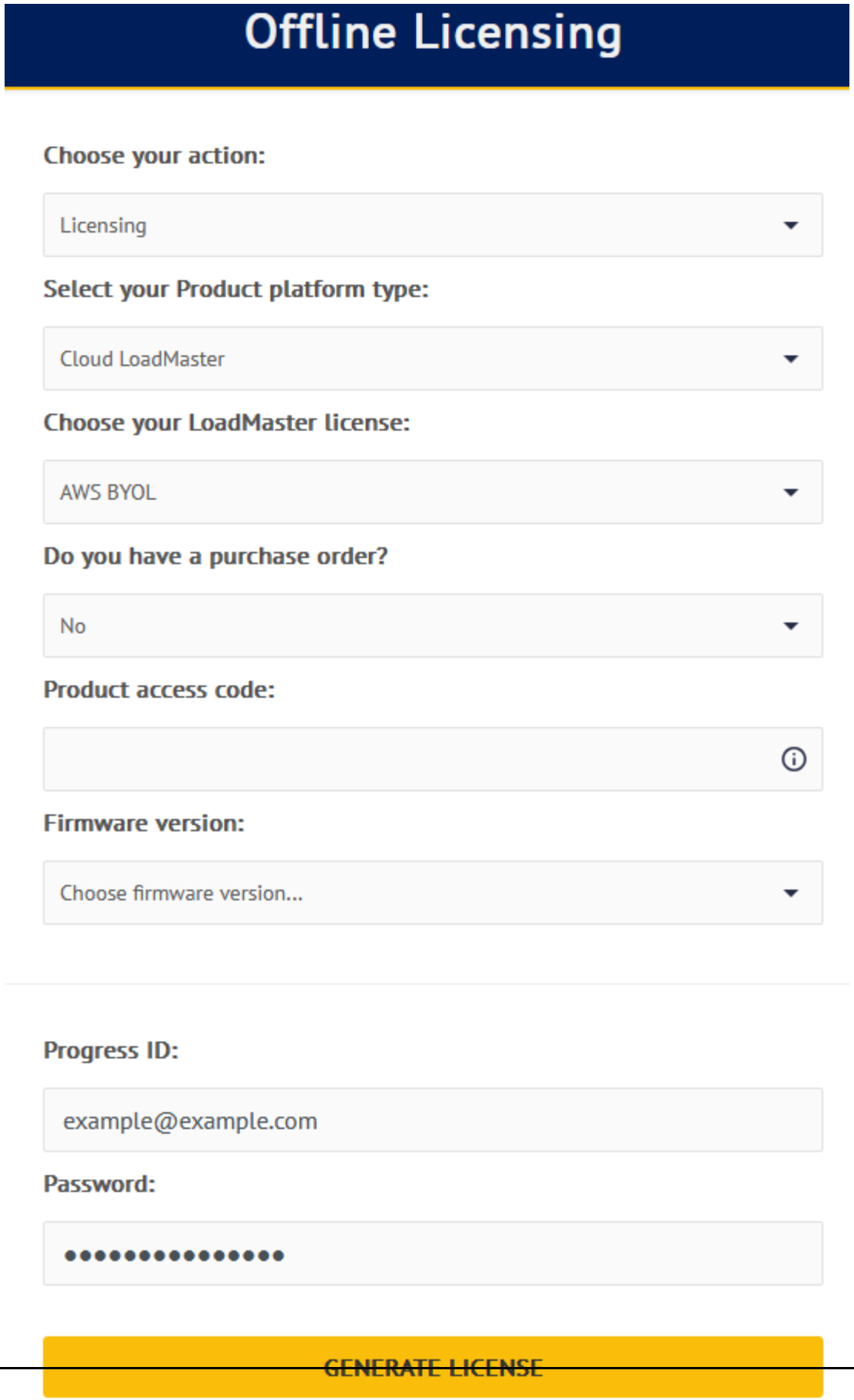
   To upgrade the license using the offline method, you must enter the license text in the LoadMaster. You can either get this from Progress Kemp or by using the **Get License** link.



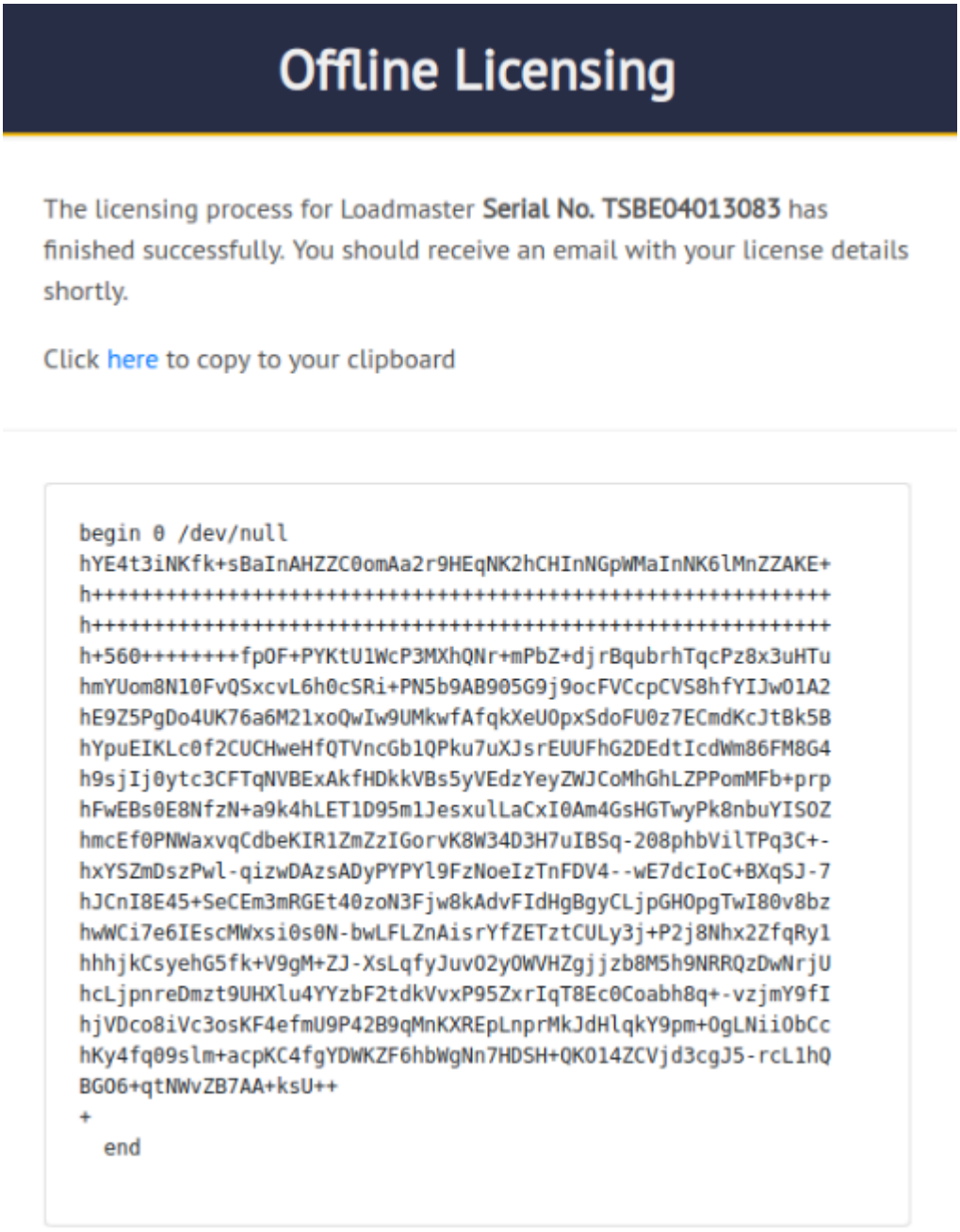
Note: For AWS GovCloud, use offline licensing.

Note: We recommend rebooting after updating the license.

4. Click the **Get License** link.


Offline Licensing
Choose your action:
Licensing
Select your Product platform type:
Cloud LoadMaster
Choose your LoadMaster license:
AWS BYOL
Do you have a purchase order?
No
Product access code:
Firmware version:
Choose firmware version...
Progress ID:
example@example.com
Password:
GENERATE LICENSE

5. Click **GENERATE LICENSE**.



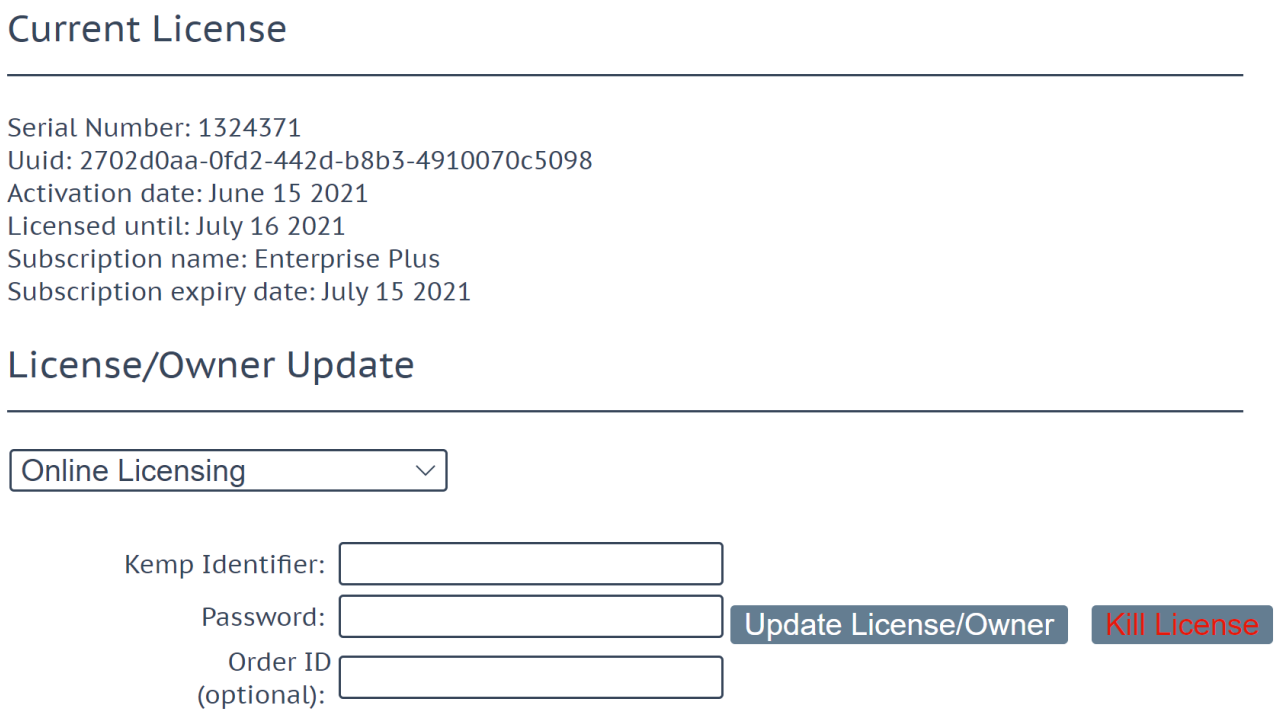
6. A page displays showing the license text. Click the **here** link to copy the license text.
7. Open the email and copy the text, from the start of the word **begin** to the end of the word **end**.
8. Open the LoadMaster.



9. Paste the license into the box provided.
10. Click **Update License**. We recommend rebooting after updating the license.

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 **Progress ID** and **Password** and click **Update License/Owner** to do this.



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

We recommend rebooting the LoadMaster after updating the license.

3

LoadMaster Firmware Downgrades

It is best practice to keep the 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

Note: 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

Progress 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.

Related Links

For details, see the following topics:

- Best Practices for Backups

Best Practices for Backups

Hypervisor snapshots cannot be used to restore a LoadMaster to a working state. The best way to back up your LoadMaster settings is by using the native backup and restore facility in the LoadMaster WUI or API.

To back up your LoadMaster configuration, follow these steps:

1. In the main menu, go to **System Configuration > System Administration > Backup/Restore**.
2. Click **Create Backup File**.

You can create a remote host for automated backups using SCP to save backups to a remote server.

For further details on backing up and restoring the LoadMaster configuration, including certificates and cipher sets, refer to the following links:

- Backup and Restore Technical Note
- How to Create and Restore a LoadMaster Configuration or Certificate Backup

5

Monitoring LoadMaster Health in AWS

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

Related Links

For details, see the following topics:

- Monitoring with Kemp 360 Central
- Monitoring with AWS

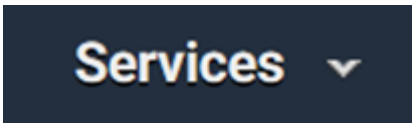
Monitoring with Kemp 360 Central

Progress Kemp provides network and application owners with the necessary tools to maintain and monitor the application delivery infrastructure. The product Kemp 360 Central is used for management and control of application delivery controllers. For further information, refer to: https://kemptechnologies.com/kemp360/central/.

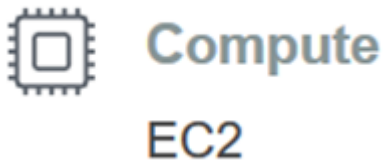
Monitoring with AWS

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:

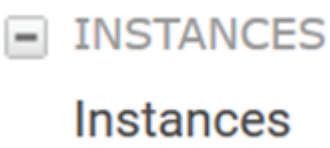
1. Log in to the AWS console.



2. Click **Services**.



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



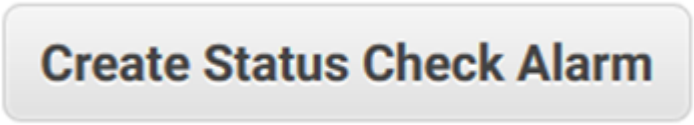
4. In the navigation on the left, click **Instances**.



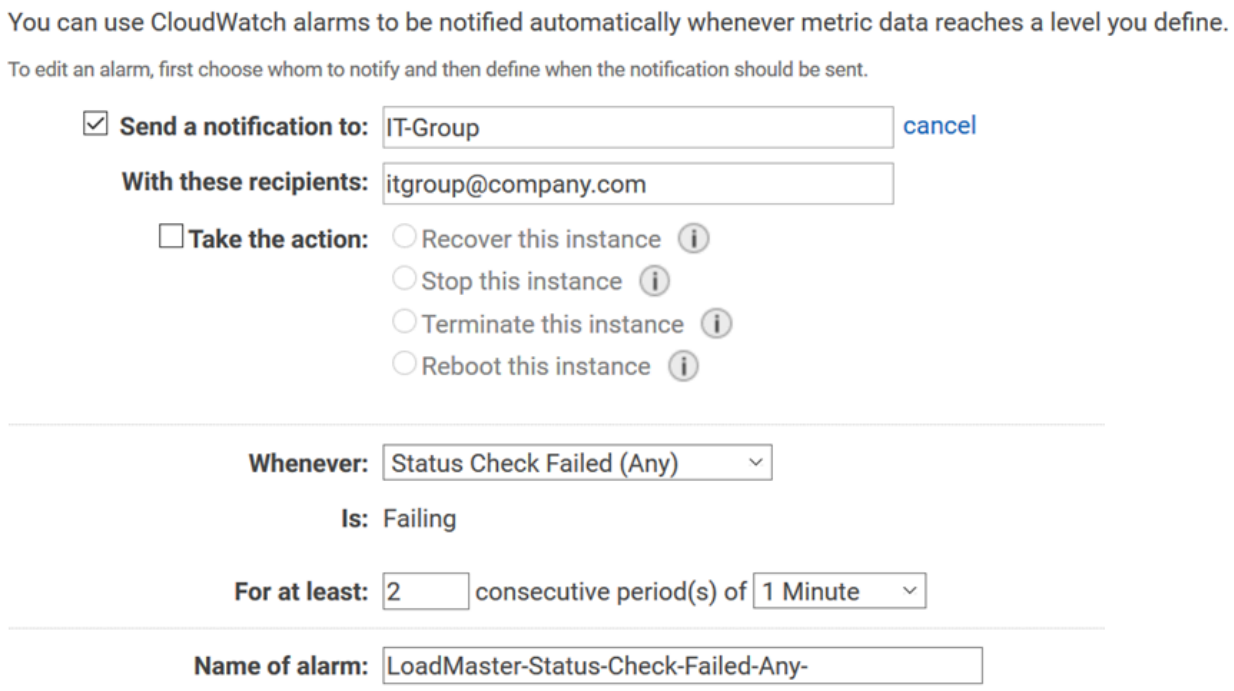
5. Click the relevant instance to create an alarm for.



6. Click **Status Checks**.



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



8. Complete the following fields:

1. Type a name for the notification group.
2. Type an email address for alarms to be sent to.
3. Select **Status Check Failed (Any)** in the **Whenever** drop-down list.
4. Keep the default interval of **2 consecutive period(s) of 1 Minute**.
5. Type a unique name for the alarm in the **Name of alarm** text box.



6. Click **Create Alarm**.

6

References

While the instructions above provide a basic overview of how to deploy and configure LoadMaster for AWS GovCloud, 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 Documentation Page.

LoadMaster Licensing, Feature Description

ESP, Feature Description

SSL Accelerated Services, Feature Description

Web Application Firewall, Feature Description

Web User Interface (WUI), Configuration Guide