



Kemp 360 Central for AWS

Installation Guide

UPDATED: 19 February 2019



Copyright Notices

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

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

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

Table of Contents

1 Introduction	4
1.1 Document Purpose	4
1.2 Intended Audience	4
1.3 Prerequisites	4
1.4 Check the Virtual Machine Settings	4
2 Deploy Kemp 360 Central in Amazon Web Services (AWS)	6
2.1 Create a New Key Pair	6
2.2 Start a New Instance	8
References	14
Last Updated Date	15

1 Introduction

Kemp 360 Central is a centralized management, orchestration, and monitoring application that enables the administration of deployed LoadMaster instances.

Kemp 360 Central can be used to perform administrative tasks on each LoadMaster instance. This provides ease of administration because multiple LoadMasters can be administered in one place, rather than accessing each LoadMaster individually.

1.1 Document Purpose

The purpose of this document is to provide step-by-step instructions on deploying Kemp 360 Central in Amazon Web Services (AWS).

1.2 Intended Audience

This document is for anyone who needs more information about deploying Kemp 360 Central within AWS.

1.3 Prerequisites

To support Kemp 360 Central for AWS, the following are required:

- An active subscription to Amazon Web Services (AWS) Virtual Machines
- A client computer running Windows 7 or higher
- Internet Explorer 11 or higher
- A Virtual Private Cloud (VPC) set up and configured in AWS
- Valid AWS credentials
- AWS Command Line Interface (CLI) must be installed

1.4 Check the Virtual Machine Settings

Note that since Version 1.25.2, the default minimum Virtual Machine provisioning requirements for new installs have been updated as follows:

Resource	V1.24 and earlier firmware	V1.25.2 and later firmware
----------	----------------------------	----------------------------

CPU	Two cores	Four cores
RAM	4 GB	8 GB
Disk Storage	40 GB	250 GB

Upgrades to Version 1.25.2 and later releases will not update existing Virtual Machine resources. To modify your current Virtual Machine configuration to conform to the above minimum values, contact Kemp Support.

2 Deploy Kemp 360 Central in Amazon Web Services (AWS)

2.1 Create a New Key Pair

When starting a new instance, you will be prompted to select a key pair. A key pair is a certificate and key. It is used to SSH to the Kemp 360 Central instance. 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.



Sign In or Create an AWS Account

You may sign in using your existing Amazon.com account or you can create a new account by selecting "I am a new user."

My e-mail address is:

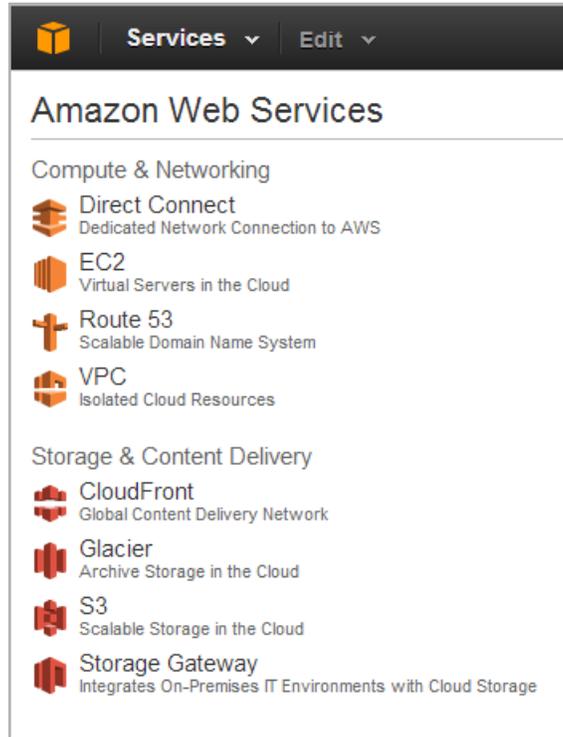
I am a new user.

I am a returning user and my password is:

[Forgot your password?](#)

[Has your e-mail address changed?](#)

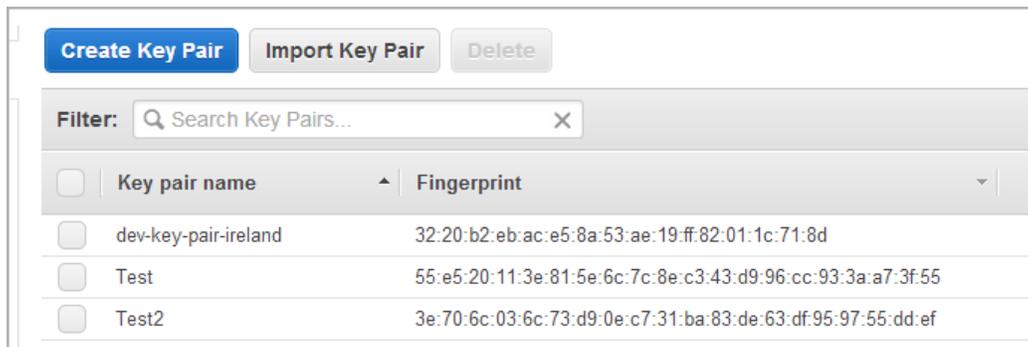
2. Click EC2.



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



4. Click **Create Key Pair**.



5. Enter a name for the key pair and click **Yes**. The .pem file downloads.



As this file is required to SSH into the Kemp 360 Central instance, make a note of where this file is stored. This file needs to reside on the client that is used to SSH to Kemp 360 Central.

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

6. If you are using Linux, change the permissions of the key pair file so it can work. To do this, go to the directory where the file is stored and run the following command:

```
chmod 600 <FileName>
```

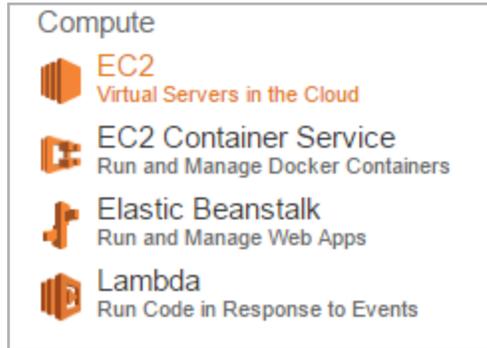
2.2 Start a New Instance

To start an instance, follow the steps below:

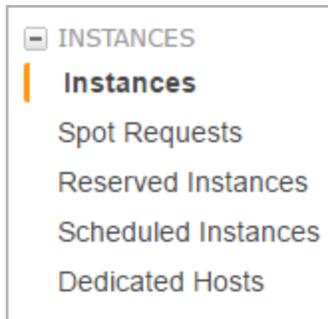
1. Access the [AWS](#) home page.



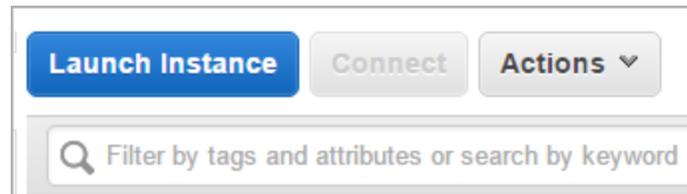
2. Click the **Sign In to the Console** button.
3. Log in using your account details.
4. Log in to the [Amazon](#) Web Services home page.



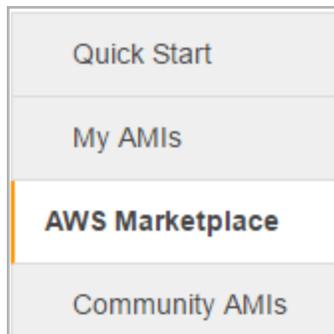
5. Click **EC2**.



6. Click **Instances**.



7. Click **Launch Instance**.



8. Select **AWS Marketplace**.

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

Step 2: Choose an Instance Type
 Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: **All instance types** **Current generation** [Show/Hide Columns](#)

Currently selected: m4.xlarge (13 ECUs, 4 vCPUs, 2.4 GHz, Intel Xeon E5-2676v3, 16 GiB memory, EBS only)

Note: The vendor recommends using a **m4.xlarge** instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Net Performance
<input checked="" type="radio"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to M
<input checked="" type="radio"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to M
<input checked="" type="radio"/>	General purpose	t2.small	1	2	EBS only	-	Low to M
<input checked="" type="radio"/>	General purpose	t2.medium	2	4	EBS only	-	Low to M
<input checked="" type="radio"/>	General purpose	t2.large	2	8	EBS only	-	Low to M
<input type="radio"/>	General purpose	m4.large	2	8	EBS only	Yes	Mod
<input checked="" type="radio"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	H

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

a) Select the appropriate instance type.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

b) Click **Next: Configure Instance Details**.



Step 3: Configure Instance Details
 Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances [Launch into Auto Scaling Group](#)

Purchasing option Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)

Auto-assign Public IP

IAM role [Create new IAM role](#)

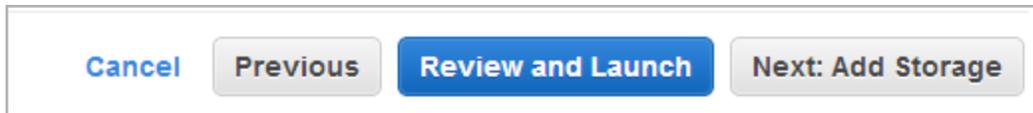
Shutdown behavior

Enable termination protection Protect against accidental termination

Monitoring Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy
Additional charges will apply for dedicated tenancy.

10. Ensure you select the correct item (Virtual Private Cloud) in the Network drop-down list.
11. Ensure that the **Auto-assign Public IP** option is set to **Enable**.
12. Configure any other setting as needed.



13. Click **Review and Launch**.

▼ Security Groups [Edit security groups](#)

Security group name launch-wizard-18
Description launch-wizard-18 created 2016-01-22T10:17:21.977+00:00

Type	Protocol	Port Range	Source
SSH	TCP	22	0.0.0.0/0

- a) Before launching, click **Edit security groups**.
- b) Select the **Security Group** of your choosing or create a new security group.

Assign a security group: Create a new security group
 Select an existing security group

Security group name:
Description:

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere 0.0.0.0/0
HTTPS	TCP	443	Anywhere 0.0.0.0/0

The default security group has entries that allow connections from any network over the following protocols and ports:

- TCP port 22 (SSH access for diagnostics)
- TCP port 443 (user interface and API)

You must add additional security group entries for the following:

- TCP port 514
- UDP port 514

The port 514 entries are required to allow managed devices to send Syslog packets to Kemp 360 Central. Use the controls in the screen shown above to add port 514 for both TCP and UDP protocols. The best practice is to create entries for specific networks, rather than allowing access across all networks (0.0.0.0/0).

You also need entries for all services on back-end servers to be able to communicate through the AWS firewall. These can be added to the security group now, or later after the services are defined. See the AWS documentation for more information on creating appropriate security group entries.

c) Click **Review and Launch**.

d) 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 ▼

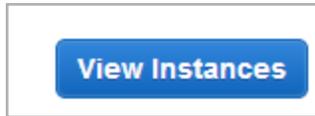
I acknowledge that I have access to the selected private key file (aws-ec2.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

e) Select the appropriate key pair for your environment. This is the key pair that was created in the **Create a New Key Pair** section. Use this key pair or another one that you might have. This key pair is needed to connect using SSH.

f) Select the check box.

g) Click **Launch Instances**.



h) Click **View Instances**. The **Public IP** address or Domain Name System (DNS) address can be used to connect to the instance using HTTPS on port 443.

After your instance state is **Running**, you can connect to your Kemp 360 Central instance. For more information on this, including instructions on how to license Kemp 360 Central, refer to the **Kemp 360 Central Feature Description** on the [Kemp Documentation Page](#).

References

Related documents are listed below:

Kemp 360 Central, Feature Description

Last Updated Date

This document was last updated on 19 February 2019.