Kemp 360 Central for AWS

Installation Guide

UPDATED: 19 February 2019

Copyright Notices

Table of Contents

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.

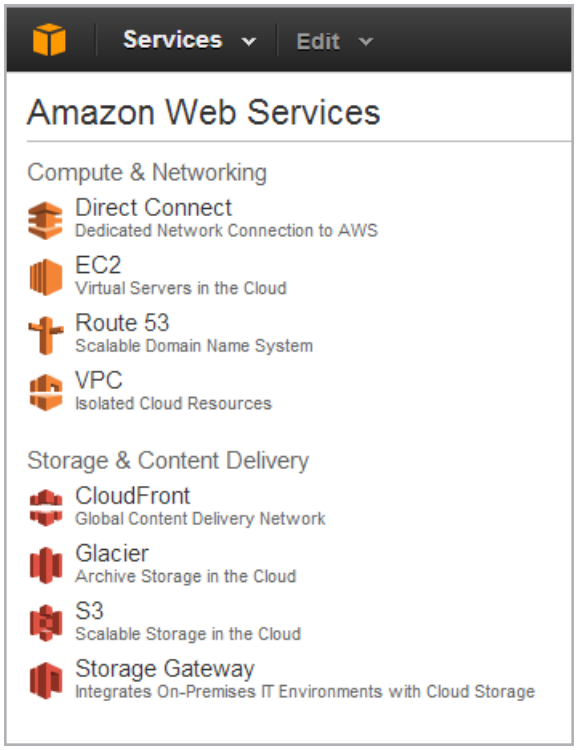
2 Deploy Kemp 360 Central in Amazon Web Services (AWS)

2.1 Create a New Key Pair

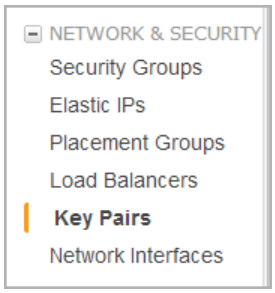
When starting a new instance, you will be prompted to select a key pair. A key pair is a certificate and key. It is used to SSH to the Kemp 360 Central instance. Keep the downloaded key in a safe place. Steps on how to add a key pair are below:

1. Log in to the AWS console.

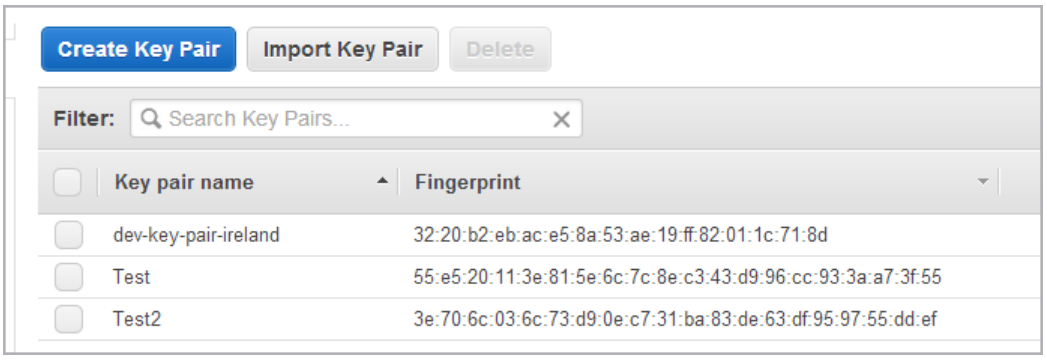
2. Click **EC2**.



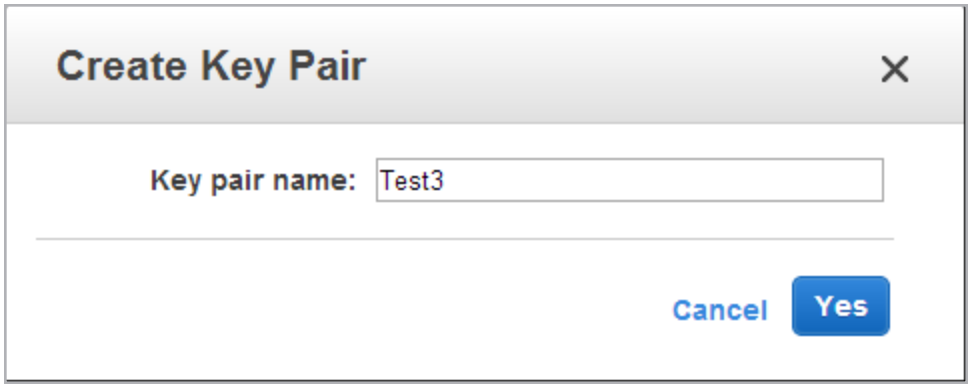
3. In the main menu, select **Key Pairs**.



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:

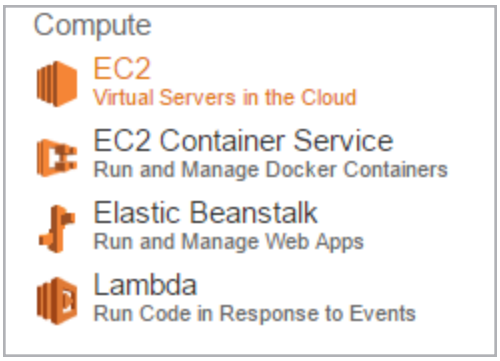
chmod 600 <FileName>

2.2 Start a New Instance

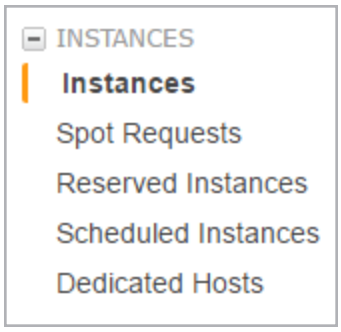
To start an instance, follow the steps below:

1. Access the **AWS** home page.

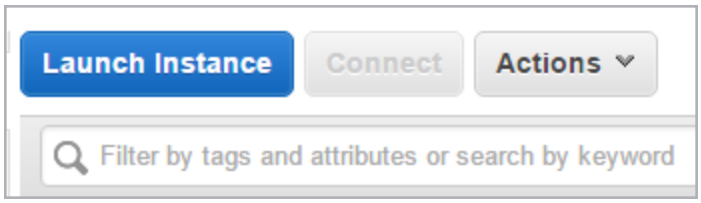
2. Click the **Sign In to the Console** button.
3. Log in using your account details.
4. Log in to the Amazon Web Services home page.



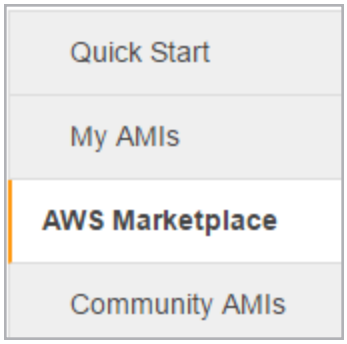
5. Click **EC2**.



6. Click **Instances**.

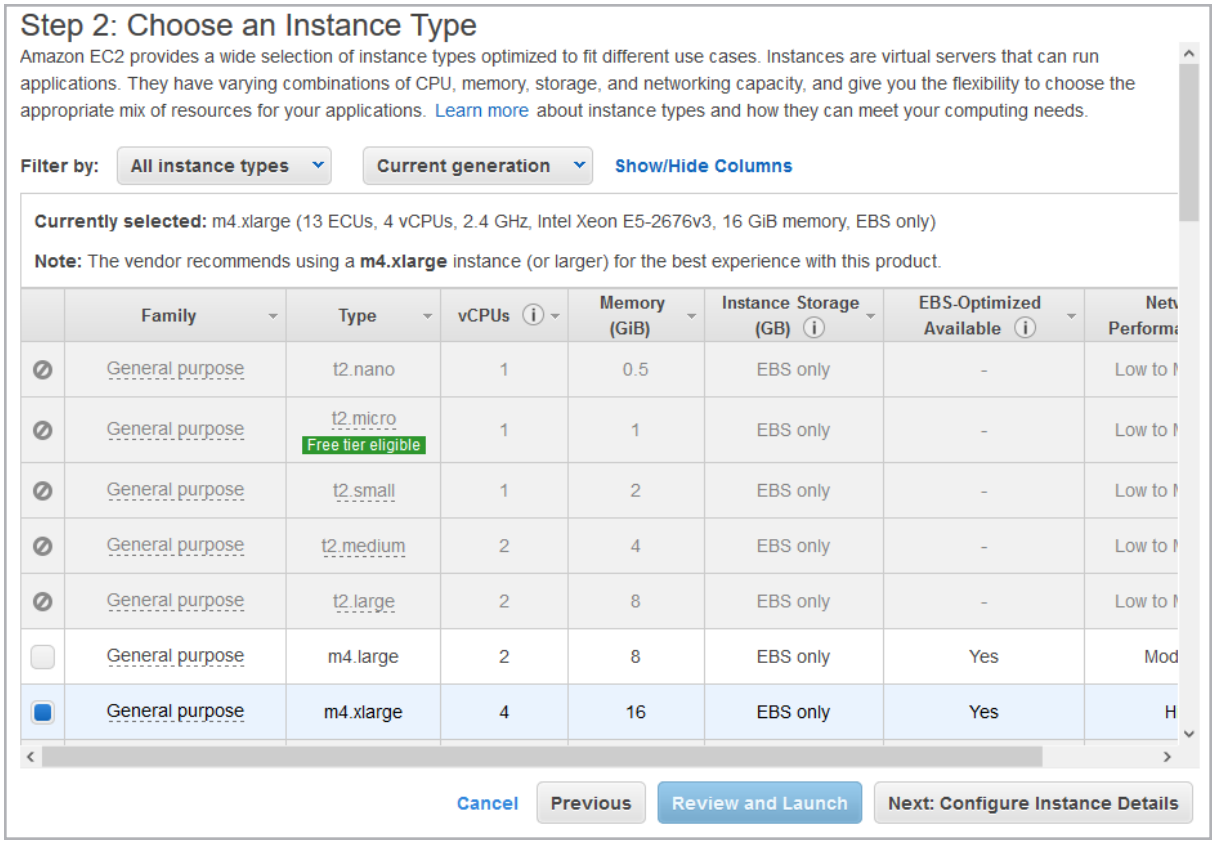


7. Click **Launch Instance**.

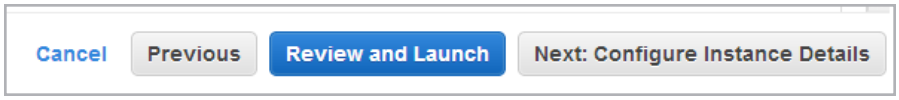


8. Select **AWS Marketplace**.

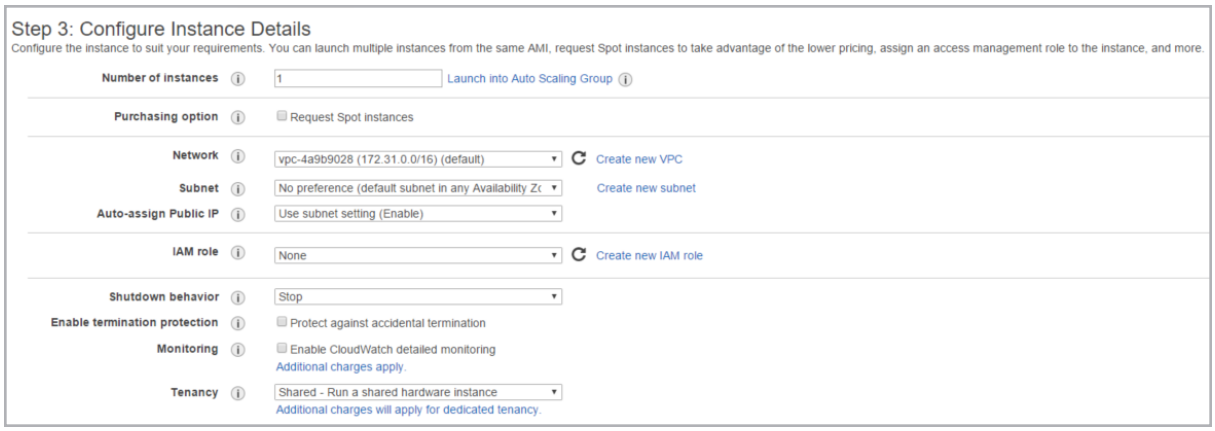
9. Click **Select** for the relevant version to be deployed.



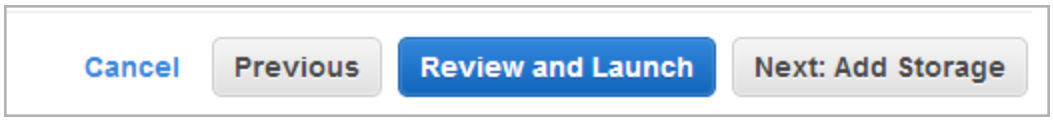
a) Select the appropriate instance type.



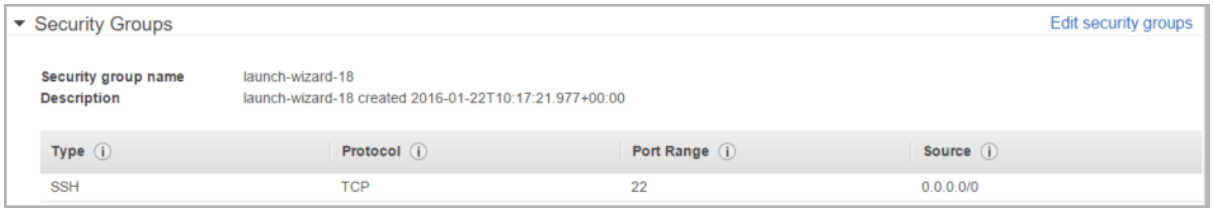
b) Click **Next: Configure Instance Details**.



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.

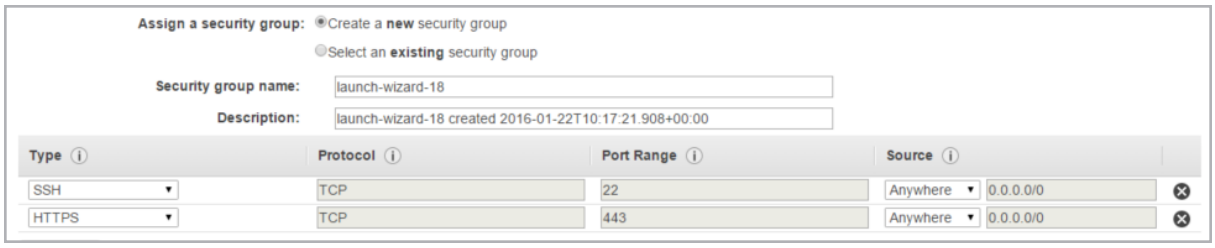


13. Click **Review and Launch**.



a) Before launching, click **Edit security groups**.

b) Select the **Security Group** of your choosing or create a new security group.



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:

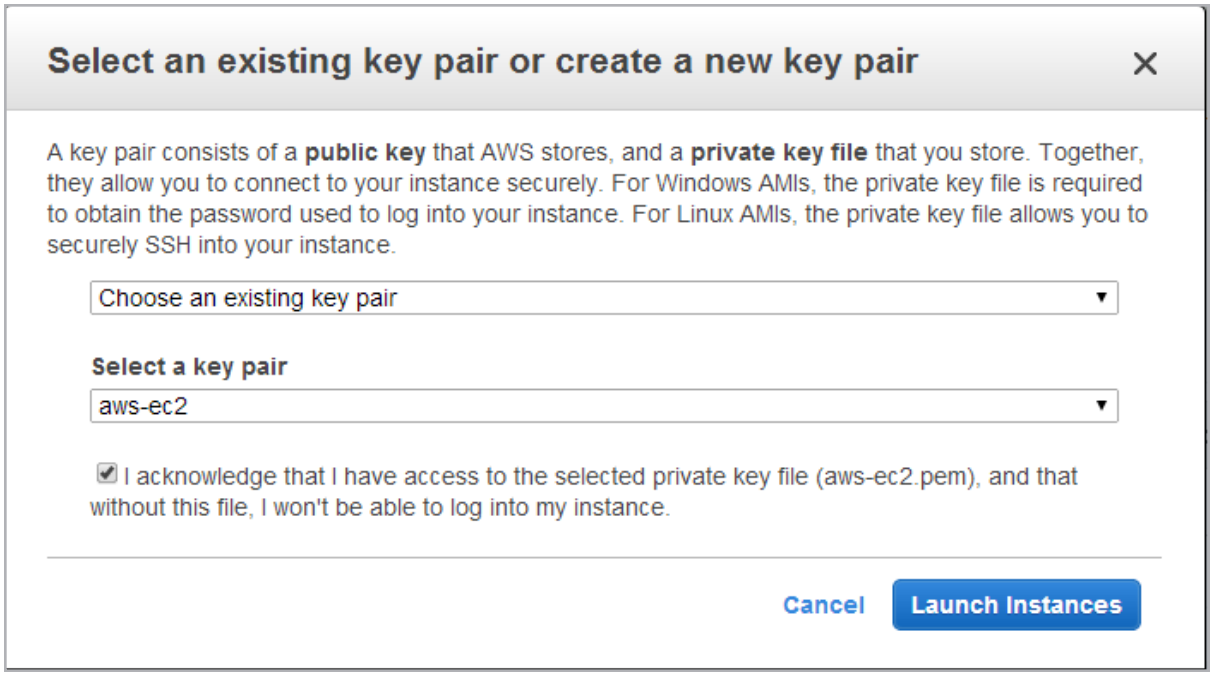
- TCP port 514
- UDP port 514

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**.

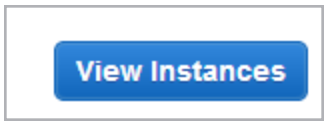
d) Click **Launch**.



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.

