syslog-ng Store Box 6.9.0

Deploying on Amazon Web Services

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

SSB Deploying on Amazon Web Services
Updated - 15 November 2021, 12:28
Version - 6.9.0

Contents

1

Introduction

The aim of this guide is to provide detailed, step-by-step instructions on how to set up and install syslog-ng Store Box in an Amazon Web Services (AWS) virtual environment.

NOTE: When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. Please consult One Identity's Product Support Policies for more information on environment virtualization.

The document comprises the following sections:

- Prerequisites on page 5 collects the requirements that you must comply with before deploying SSB on AWS.
- Limitations on page 6 lists the limitations that apply when installing SSB in an AWS virtual environment.
- Installing SSB on Amazon Web Services on page 10 describes how to install SSB in an AWS virtual environment.

2

Prerequisites

The following prerequisites must be met before deploying SSB on Amazon Web Services:

- You have a valid One Identity syslog-ng Store Box license.

  syslog-ng Store Box uses the "Bring your own license" model. Note that to deploy two active SSB nodes as an availability set, you must purchase two standalone SSB licenses. To purchase a license, contact our Sales Team.
- You have an Amazon Web Services account and privileges to access the Amazon Elastic Compute Cloud (EC2) service.
- You have secure access to your Amazon Virtual Private Cloud (VPC) resources, for example, through the use of a Virtual Private Network (VPN).
- You have working knowledge of the SSB installation process.
- You have familiarity with AWS EC2.

3

Limitations

The following limitations apply when deploying SSB on Amazon Web Services:

- If High Availability (HA) operation mode is required in a virtual environment, use the HA function provided by the virtual environment.
- Hardware-related alerts and status indicators of SSB may display inaccurate information, for example, display degraded RAID status.
- When running SSB in a virtual environment, it is sufficient to use a single network interface.
- During AWS installation, connecting directly to the Internet using a public IP address is not supported. Instead, you must access the Internet via a Virtual Private Network or a jump host.

Finding or copying SSB AMIs on Amazon Web Services

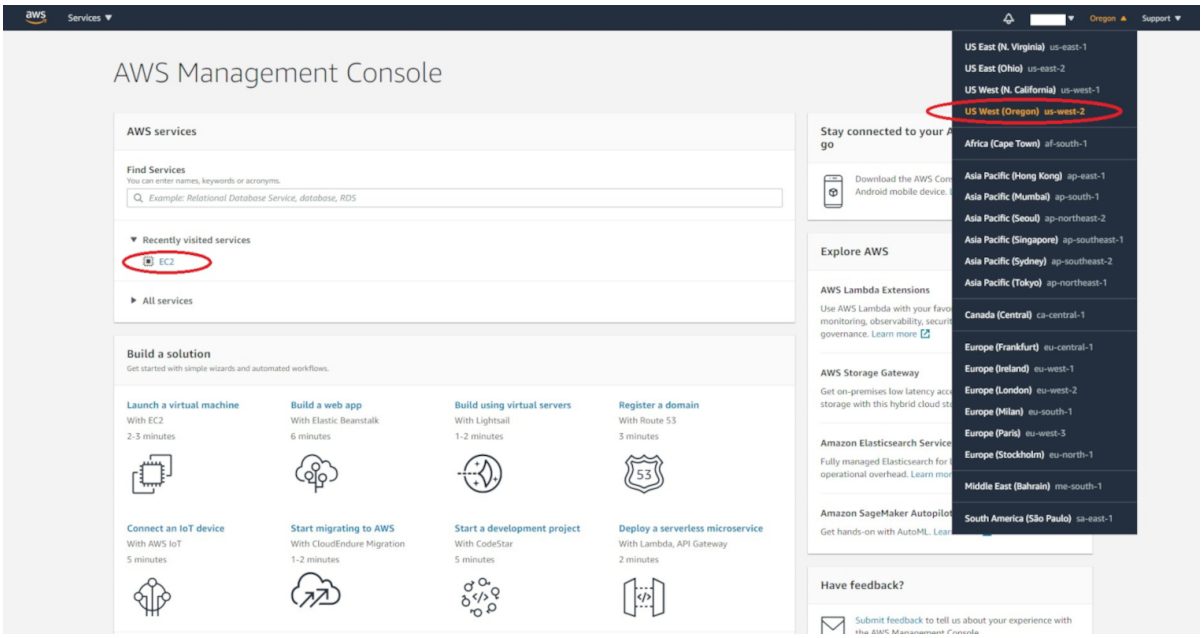
This section describes how you can find or copy syslog-ng Store Box (SSB) Amazon Machine Images (AMIs) on Amazon Web Services (AWS).

For more information about AWS and installing SSB on AWS, see Installing SSB on Amazon Web Services.

Finding or copying SSB AMIs on AWS

By default, the publicly available SSB AMIs can be found under **Services > AWS Management Console > AWS services > EC2**, in the **US West (Oregon)** region.

Figure 1: Services > AWS Management Console > AWS services > EC2 - Publicly available AMIs under the US West (Oregon) region



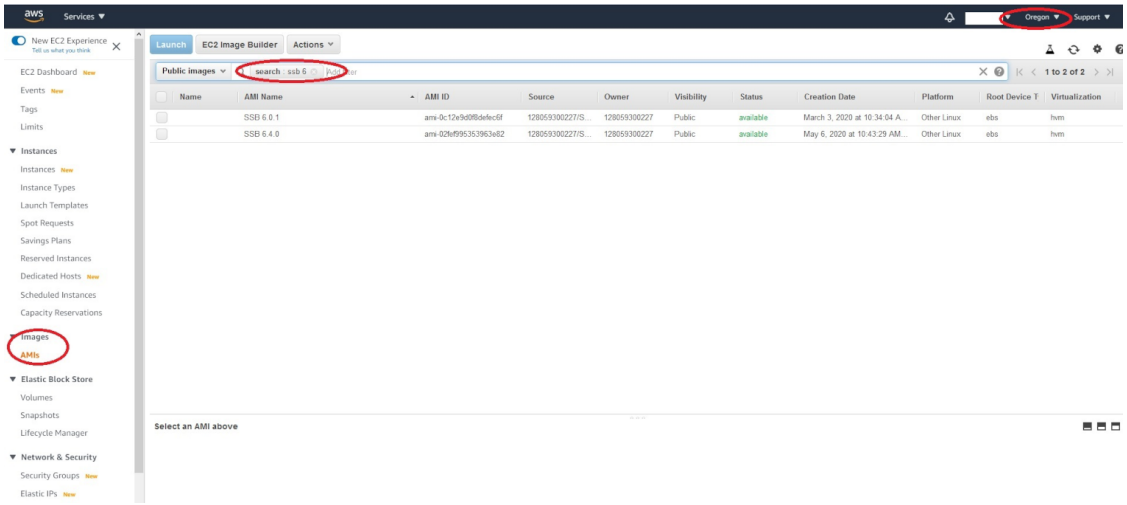
If you need a region other than the standard US West (Oregon), you have to copy the AMIs to the destination region of your choice.

To copy your SSB AMIs on AWS to the destination region of your choice

1. Enter your AWS Services account, and navigate to **Services > AWS Management Console > AWS services > EC2**.
2. Navigate to **Images > AMIs**, then filter the available AMIs for SSB 6 versions.

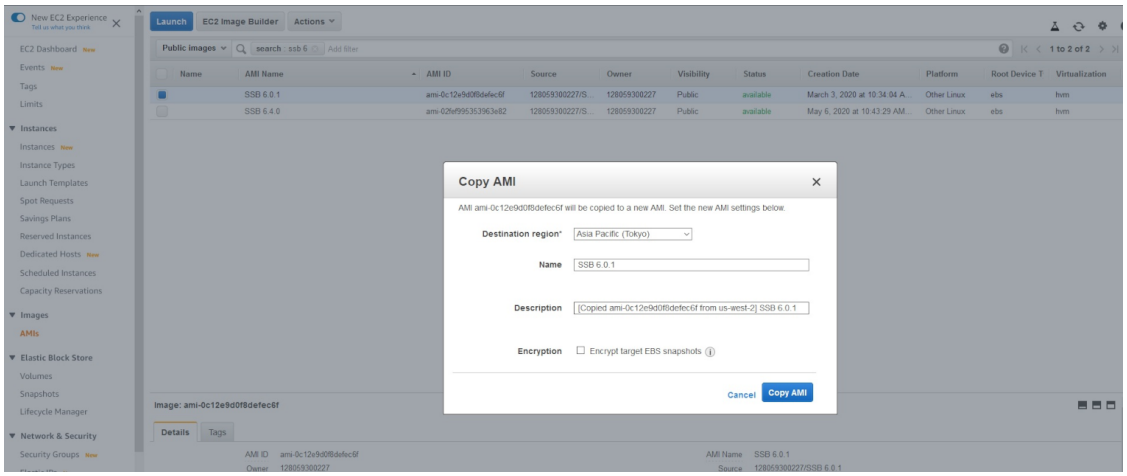
TIP: The `ssb 6` search expression will filter for the AMIs of all available release versions of SSB within the 6 release set. For more information about release version numbering in SSB, see the description of LTS and Feature releases under the syslog-ng Store Box Product Life Cycle table.

Figure 2: Images > AMIs - Available AMIs after filtering for SSB 6 versions



3. Select the SSB AMI of your choice (for example, **SSB 6.0.1**), then select **Actions > Copy**, and select the **Destination region** of your choice (for example, **Asia Pacific (Tokyo)**, in this example).

Figure 3: Images > AMIs > Actions > Copy AMI pop-up window opened from <the AMI of your choice> - Customizing your AMI copying preferences



4. (Optional) Enter a **Description** for the AMI you want to copy, and enable **Encryption** if you prefer to use it.

TIP: If you are not sure what enabling **Encryption** results in, click ⓘ (info) next to **Encrypt target EBS snapshots**.

5. Click **Copy AMI** to finish copying the AMI of your choice with the settings you customize.

Installing SSB on Amazon Web Services

This section describes how to deploy syslog-ng Store Box (SSB) on Amazon Web Services.

NOTE: This section uses a number of screenshots for illustration purposes. Note that these are added here for reference only as the look and feel (but not the contents) of the Amazon user interface may change without this guide containing the most recent changes.

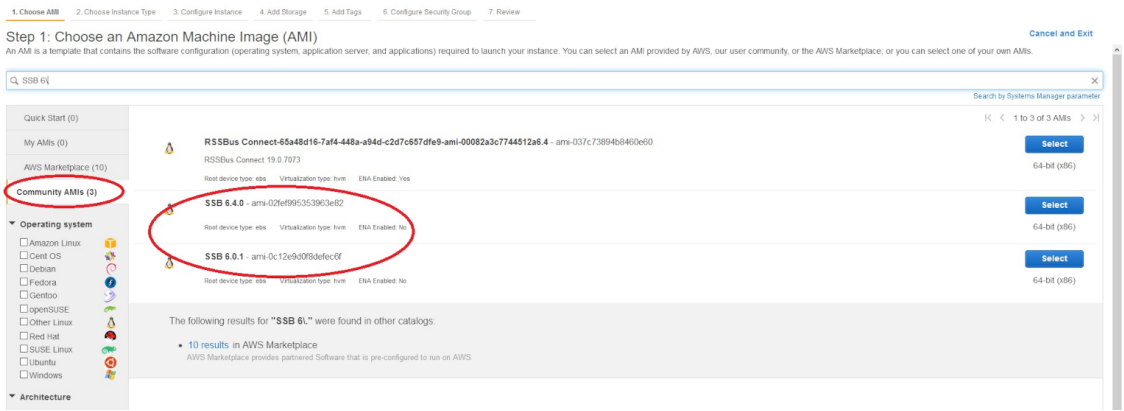
To deploy syslog-ng Store Box on AWS

1. Log in to Amazon Web Services.
2. Once logged in, go to **INSTANCES > Instances** in the left-hand navigation pane, and then click **Launch Instance**.

   NOTE: If you can not find the SSB AMIs you are looking for listed under **Community AMIs**, you have to copy them first from the publicly available AMIs (located under **Services > AWS Management Console > AWS services > EC2**, in the **US West (Oregon)** region by default). For more information about copying SSB AMIs to the region of your choice, see Finding or copying SSB AMIs on Amazon Web Services.

   The **Step 1: Choose an Amazon Machine Image (AMI)** page comes up.

Figure 4: Step 1: Choose an Amazon Machine Image (AMI)



3. Choose an Amazon Machine Image (AMI) that corresponds to the type of Virtual Machine (VM) that you want to launch an instance from.

   To choose the AMI that corresponds to the type of Virtual Machine (VM) that you want to launch an instance from

   a. Navigate to **Community AMIs**.

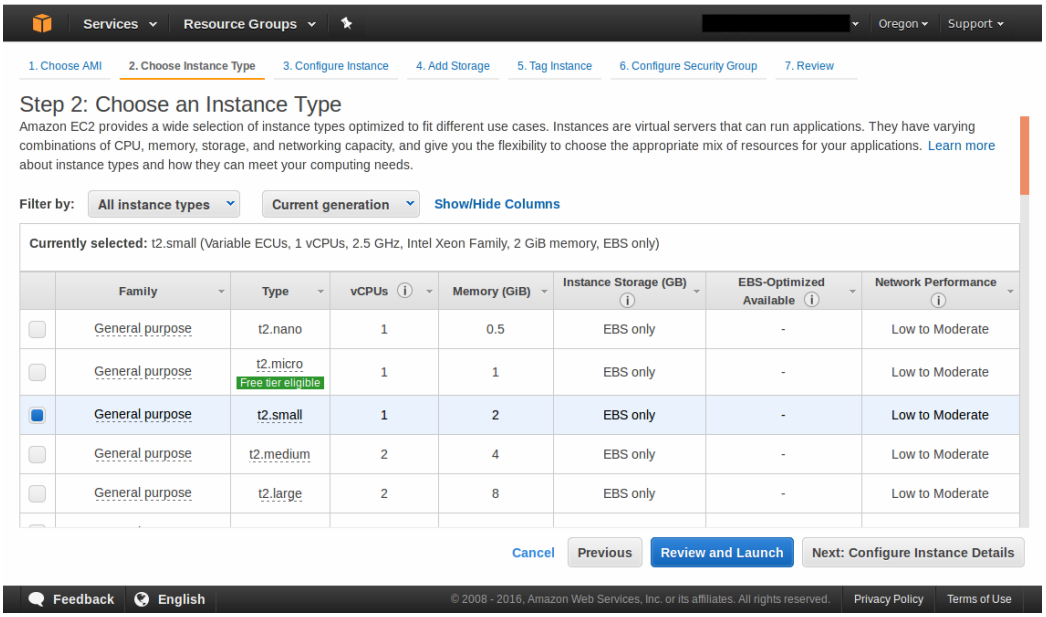
   b. Filter the available AMIs for SSB 6.

      TIP: The `SSB 6\.` search expression will filter for the AMIs of all available release versions of SSB within the 6 release set. For more information about release version numbering in SSB, see the description of LTS and Feature releases under the syslog-ng Store Box Product Life Cycle table.

   c. Click on the SSB AMI of your choice (for example, SSB 6.0.1), and click the corresponding **Select** button.

      The **Step 2: Choose an Instance Type** page comes up.

Figure 5: Step 2: Choose an Instance Type



4. Choose an instance type:

   a. Select an instance type by clicking the checkbox next to it.

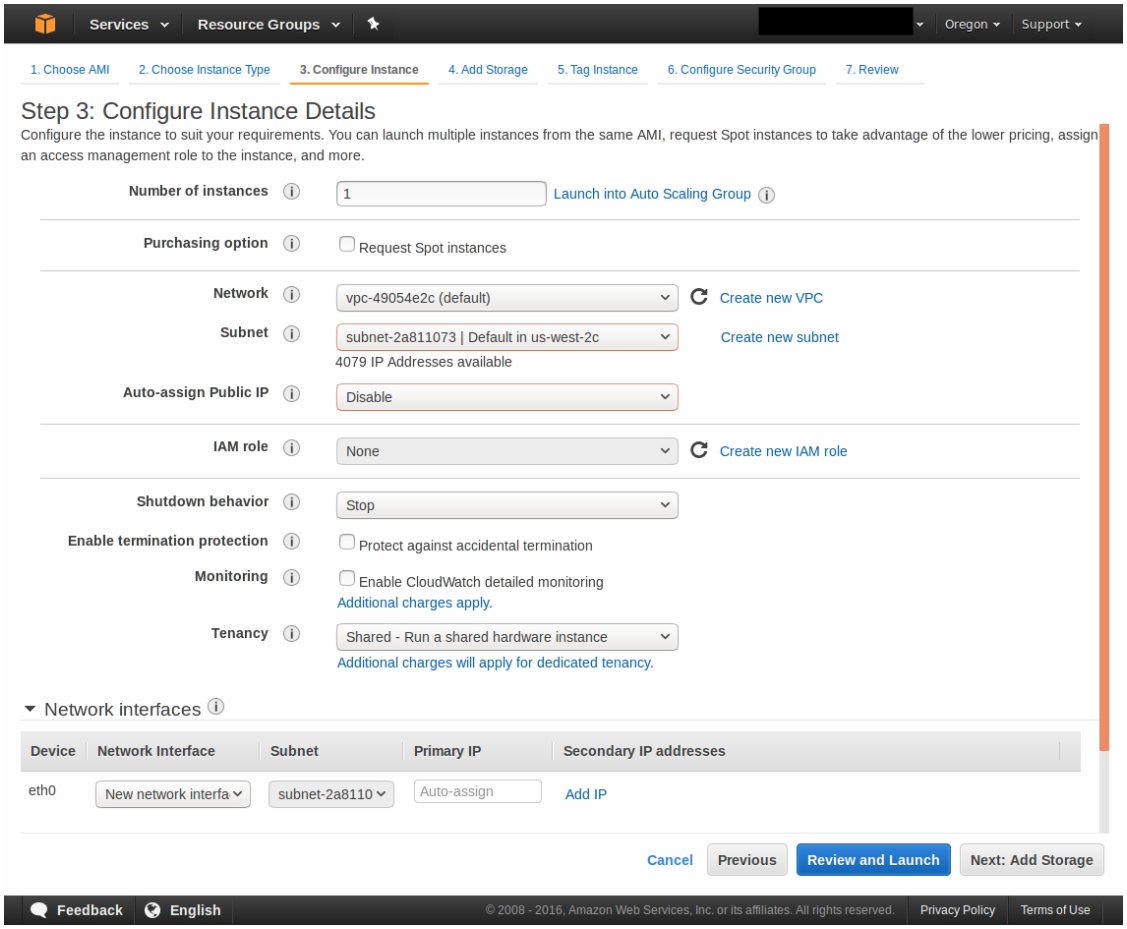
      The minimum memory requirement is 2 GiB, that is, type *t2.small*. This instance type is able to handle 10,000 Events per Second (EPS).

      The recommended memory requirement is 7.5 GB, that is, type *c4.xlarge*. The capacity of this instance type is the closest to the physical hardware.

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

The **Step 3: Configure Instance Details** page comes up.

Figure 6: Step 3: Configure Instance Details



5. Configure instance details:
    a. Select the required Virtual Private Cloud (VPC) from the **Network** list.
    b. Choose a subnet to launch the instance into.

        NOTE: Exposing SSB to the public Internet during installation is not supported at all, therefore you must use a VPN or jump host to reach your instance and configure it.

        As for exposing the logging interface to the Internet after installation, contact our Support Team to discuss your needs and how those could be met.

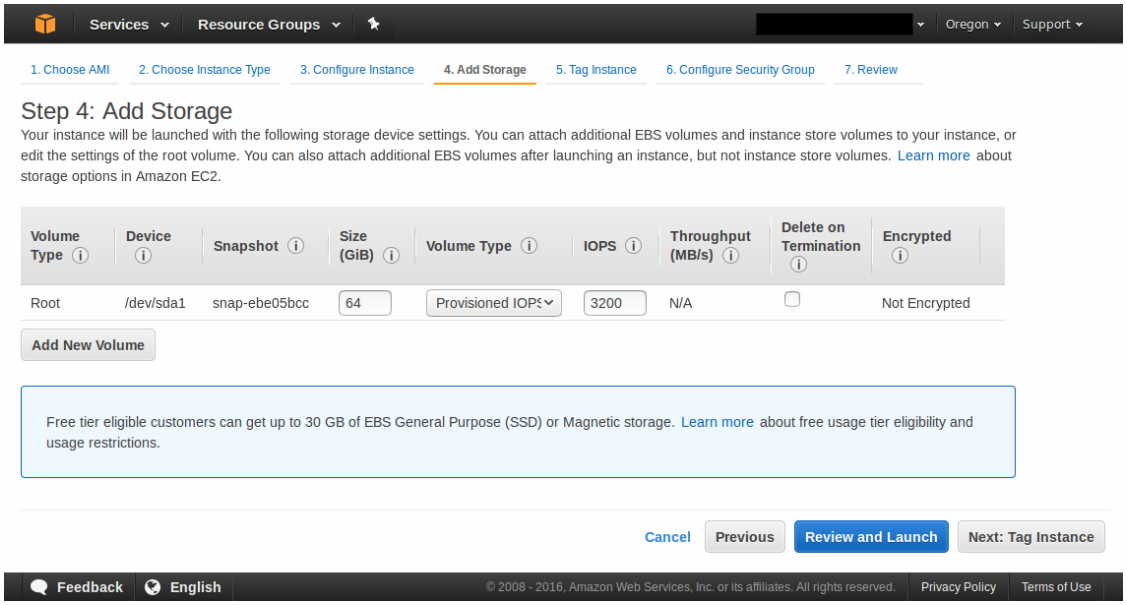
    c. Ensure that the **Auto-assign Public IP** field is set to **Disable** or **Use subnet setting (Disable)**. This is required so that you do not get assigned a public IP address.
    d. Use the default values for all other fields or change them as required.
    e. You can leave the **Network interfaces** part untouched as using just one network interface will suffice.

Note, however, that if you launch SSB with a single interface configured, then that interface will act as the management interface.

f. Click **Next: Add Storage**.

The **Step 4: Add Storage** page comes up.

Figure 7: Step 4: Add Storage



6. Add storage to your instance:

   a. Set the size of your instance's store volume.

      NOTE: It is important that you choose this value wisely as once you have launched the instance, you will not be able to go back and modify it. The minimum storage size is 8 GiB, while the maximum allowed value is 16 TB (16384 GB).

   b. Set the volume type of your instance's store volume.

      SSD provides better performance than a Magnetic hard drive, however, it is also more expensive.

      The following recommendations apply:

      - If you choose a volume that is larger than 500 GB in size or your SSB is expected to handle volumes of traffic lower than 15,000 EPS, then select volume type **General Purpose SSD (GP2)**. This volume type comes with an I/O credit balance, which will be used when your volume requires more I/O operations per second (IOPS) than the baseline performance I/O level. If you emtpy your credit balance, the maximum IOPS performance of the volume will remain at the baseline IOPS performance level, which may result in slower-than-required performance.

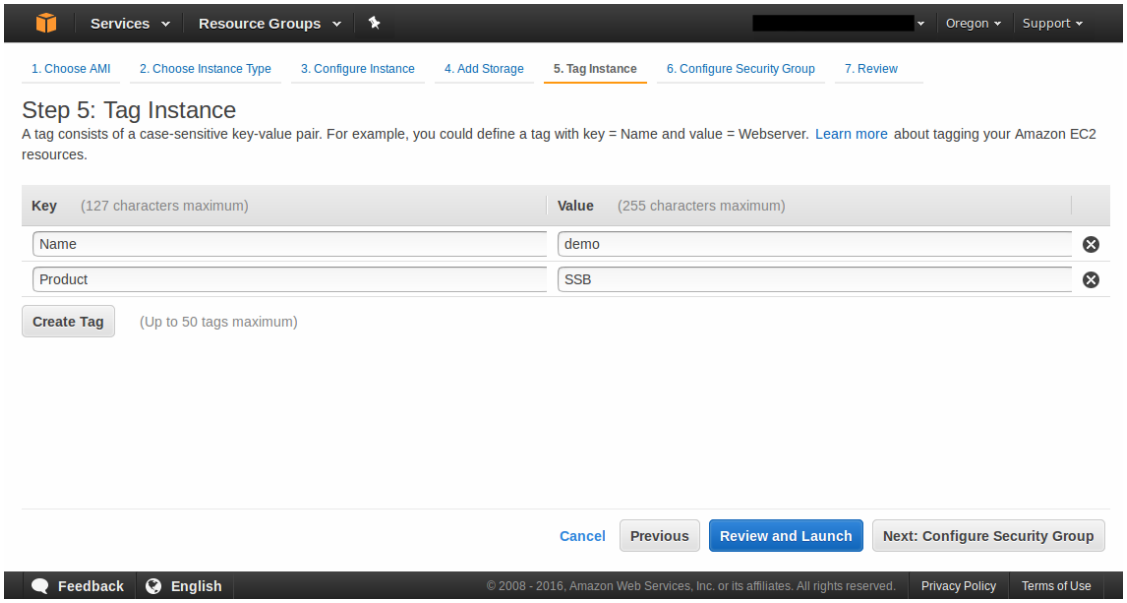
- If your SSB is required to handle traffic exceeding 15,000 EPS or you choose a volume that is smaller than 500 GB in size, then select volume type **Provisioned IOPS SSD (IO1)**. This volume type does not use a credit model, it allows you instead to specify a consistent IOPS rate.

> TIP: Selecting the **Delete on Termination** checkbox will automatically delete your store volume on terminating the instance. This is useful as this will free up storage place, and you will not have to pay for a store volume you are not using anymore. However, note that deleting the store volume will also delete your logs.

c. Click **Next: Tag Instance**.

The **Step 5: Tag Instance** page comes up.

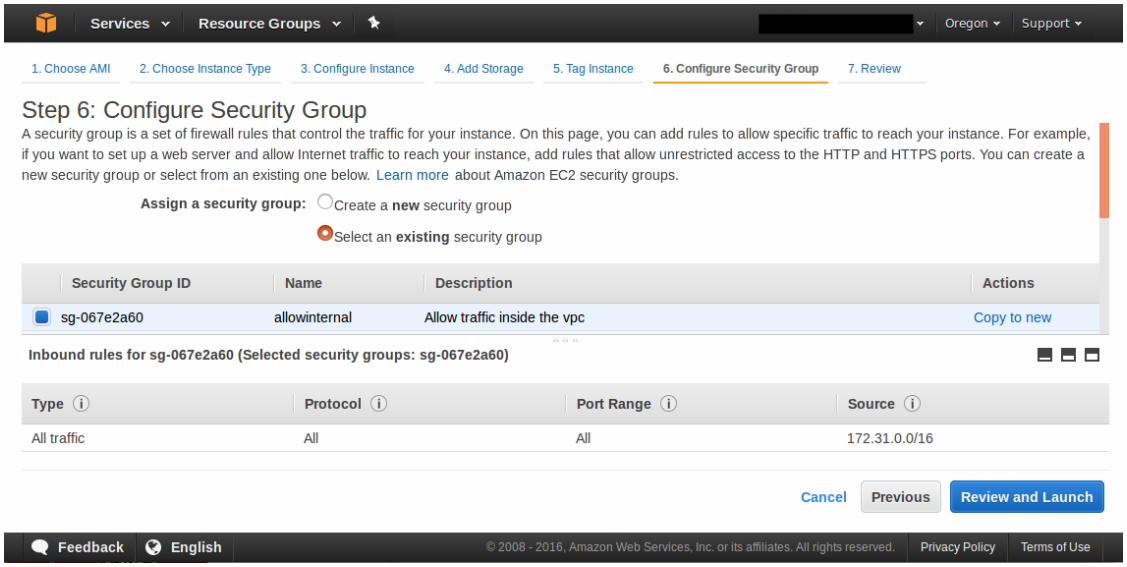
Figure 8: Step 5: Tag Instance



7. Create a tag for your instance:
   a. Add a meaningful key-value pair that will help you later on to easily identify your instance.
   b. Click**Next: Configure Security Group**.

The **Step 6: Configure Security Group** page comes up.

Figure 9: Step 6: Configure Security Group



8. Configure security group:
   a. Set a new or an existing security group to control how SSB is accessed.

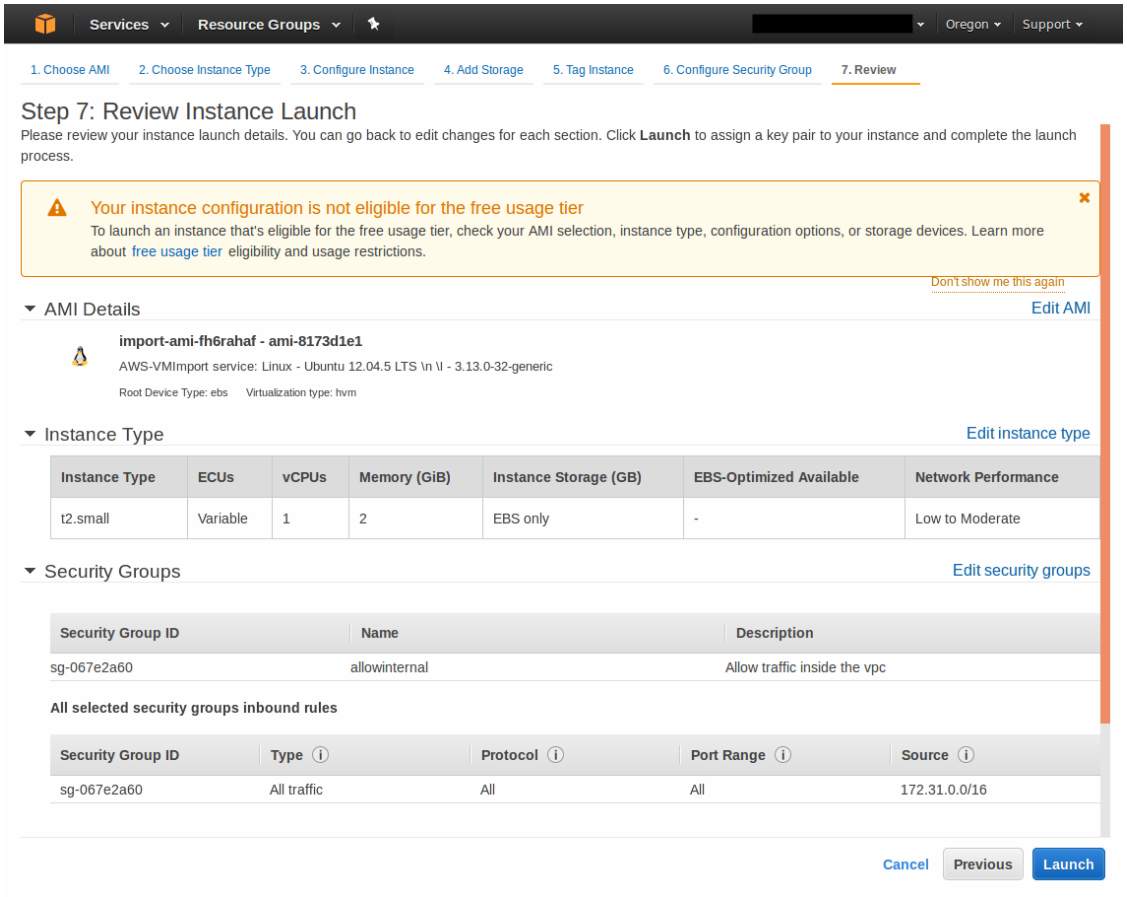
      Exposing SSB to the public Internet during installation is not supported at all, therefore you must use a VPN or jump host to reach your instance and configure it. As for exposing the logging interface to the Internet after installation, contact Support to discuss your needs and how those could be met.

      To achieve the above: restrict your security group to those users and log clients that access SSB from a secure network, and not over the public Internet. For example, if you are using a jump host, then you need a security group that will allow only your dedicated VPC to connect to your SSB. If there is a VPN to your home network or some other secure network, that can be allowed as well.

   b. Click **Review and Launch**.

The **Step 7: Review Instance Launch** page comes up.

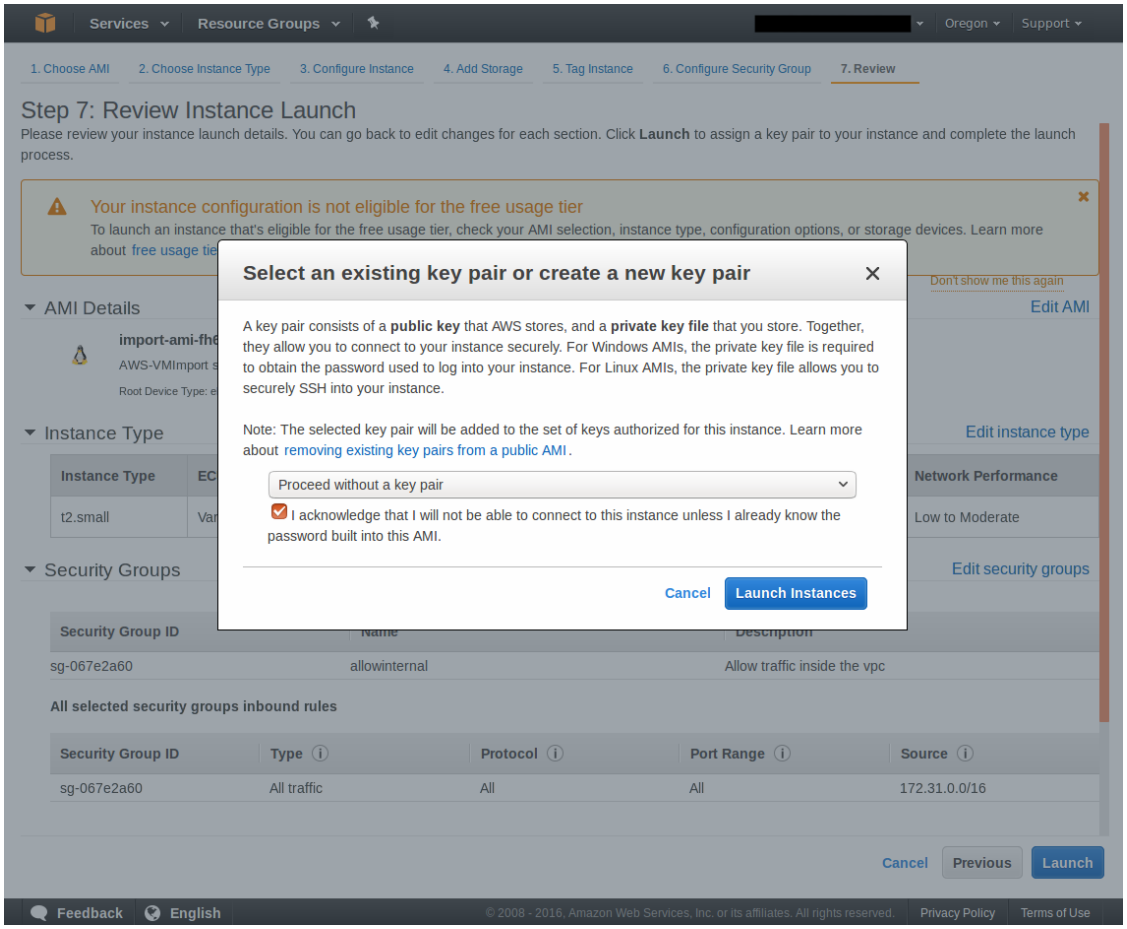
Figure 10: Step 7: Review Instance Launch



9. Before launching your instance, double-check whether all details have been set as intended:
    a. Ensure that:
        - Under **Instance Type**, you have at least 2 GiB of memory assigned.
        - Under **Instance Details**, the **Assign Public IP** option is set to **Disable** or **Use subnet setting (Disable)**.
    b. Make any changes if required.
    c. Once you are happy with all settings, click **Launch**.

The **Select an existing key pair or create a new key pair** pop-up window comes up.

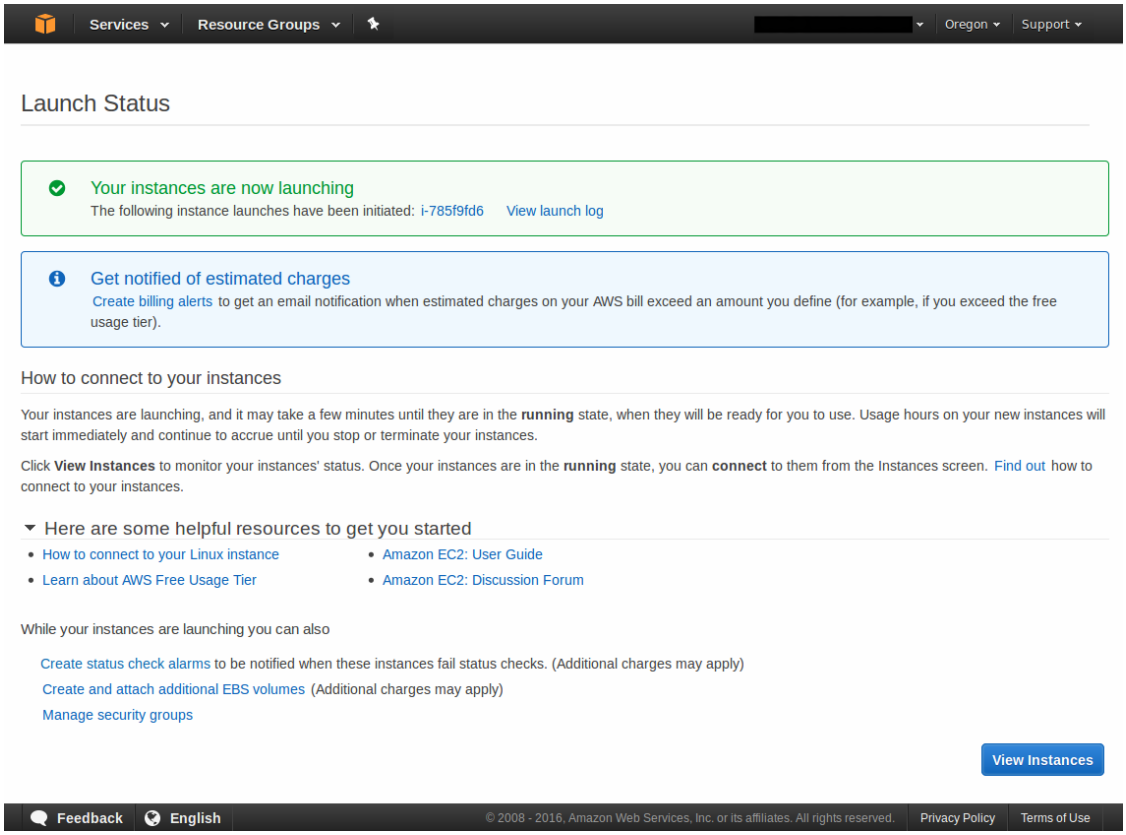
Figure 11: Step 7: Review Instance Launch — Key pair pop-up window



10. On the **Select an existing key pair or create a new key pair** pop-up window:
    a. Select the **Proceed without a key pair** option.
    b. Tick the checkbox that says "I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI".
    c. Click **Launch Instances**.

The **Launch Status** page comes up informing you that your instance is launching.

Figure 12: Launch Status page



11. To view your instance's status, click **View Instances**.

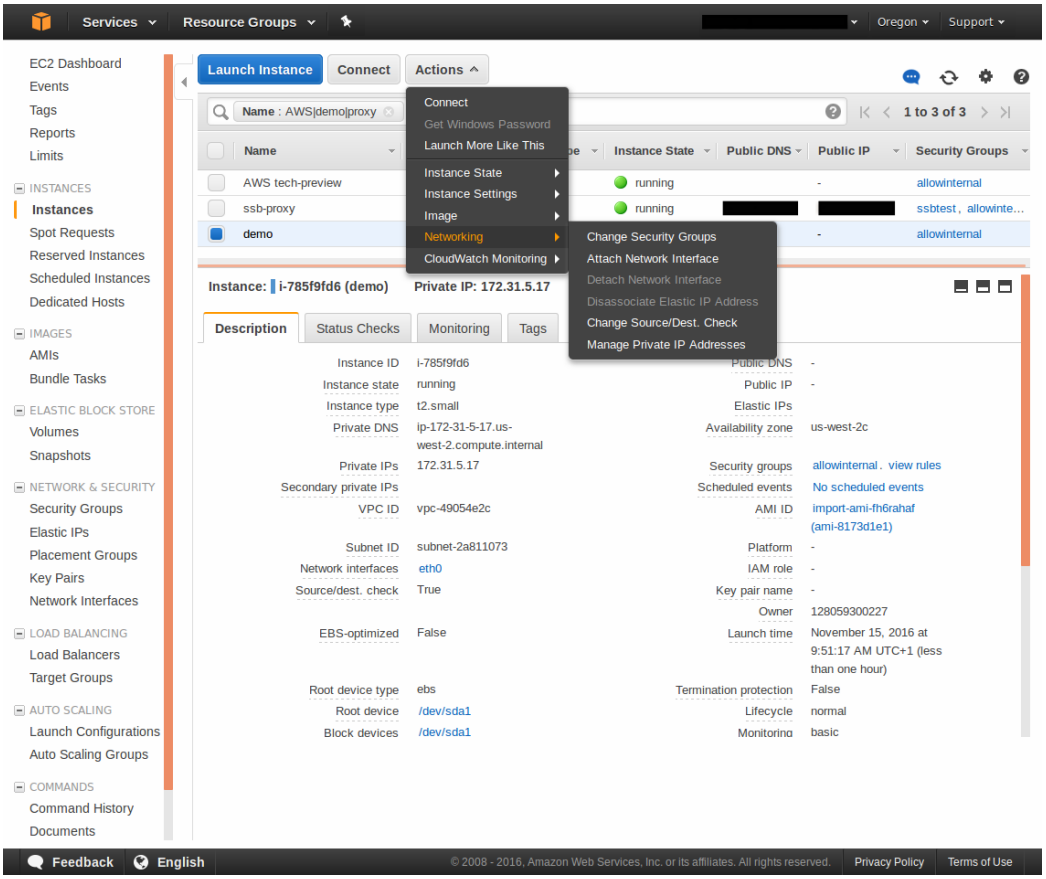
    The **Instances** page comes up, which should now display the instance you have just launched. Depending on the size of the instance, installation may take up to 1-5 minutes.

    To access your SSB instance and start configuring it using the welcome wizard, you will need your instance's IP address and the netmask of your chosen subnet, both of which you can obtain from the AWS user interface.

12. SSB expects that the IP address provided will not change, therefore, before retrieving the IP address, perform the following check:

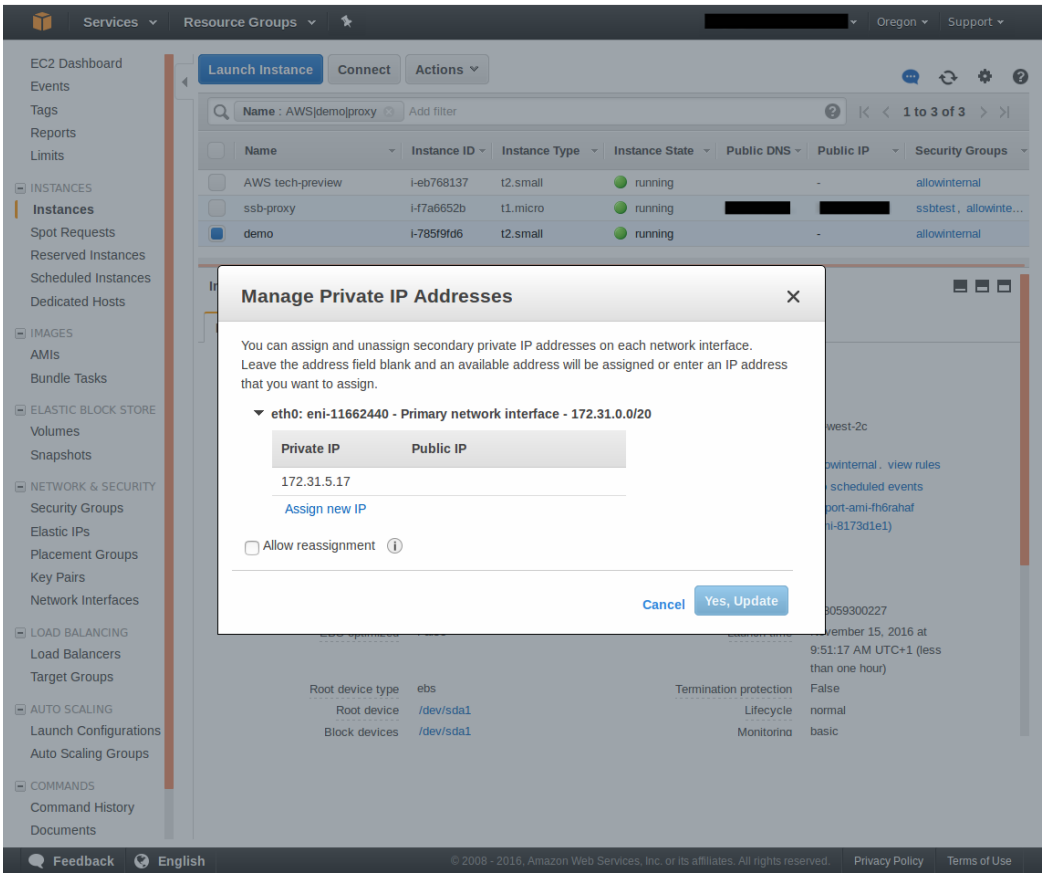
    a. Click the instance you have just added, and select **Actions > Networking > Manage Private IP Addresses** from the menu at the top.

Figure 13: Instances page — Actions menu



The **Manage Private IP Addresses** pop-up window comes up.

Figure 14: Instances page — Manage Private IP Addresses pop-up window



b. To ensure that the IP address stays the same, make sure that the **Allow reassignment** option is unchecked.

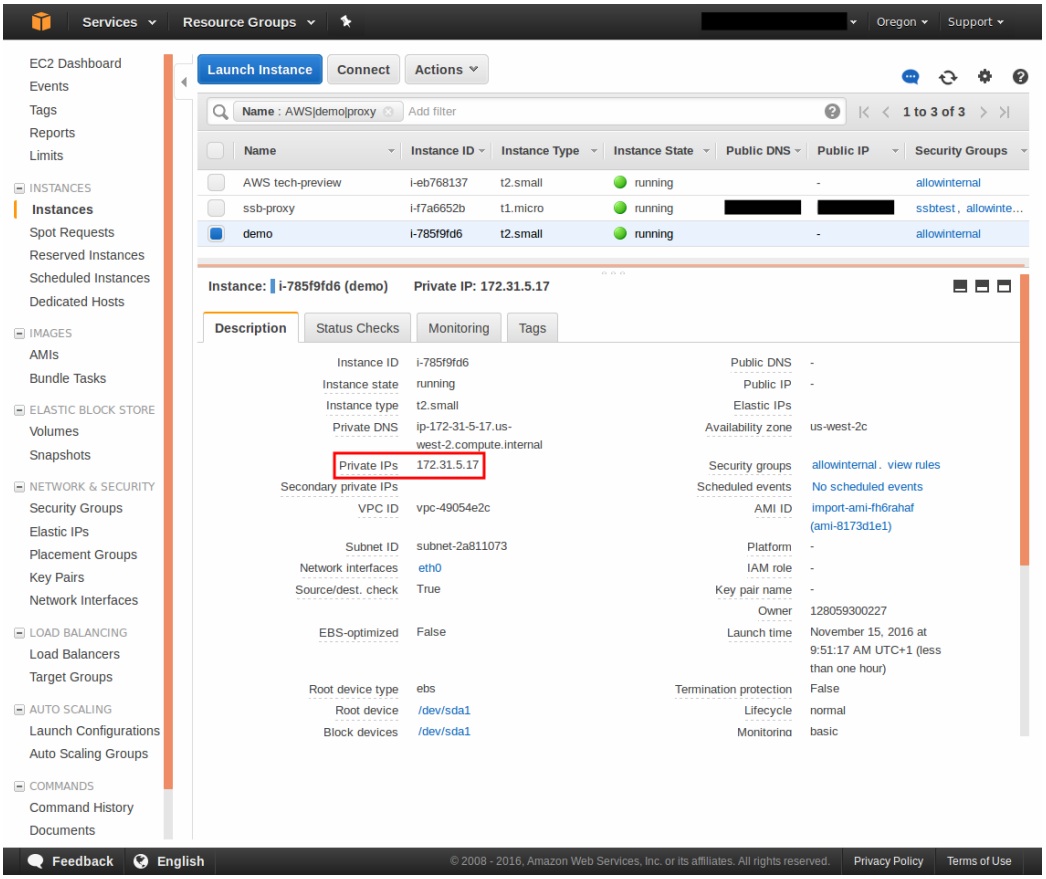
   Note down the netmask of the subnet you selected (**/20** in the example provided) because you will need this piece of information later on, when configuring SSB via the welcome wizard.

13. To obtain and use the IP address of the instance:

    a. Click the instance on the **Instances** page.

       This will display the description of the instance, including its private IP address.

Figure 15: Instances page — instance description



b. Select the value in the **Private IPs** field and copy it.

c. Paste this value in the **Networking > External interface > IP address** field of the SSB welcome wizard.

   For detailed information on the SSB welcome wizard, see "The Welcome Wizard and the first login" in the Administration Guide.

14. To obtain and use the subnet's netmask:

    a. Retrieve the netmask information you noted down earlier in Step 12b.

    b. AWS provides the netmask value in CIDR format (for example, /24), while SSB expects this value in the octet format (for example, 255.255.255.0).

       Convert the value from the CIDR to the octet format.

    c. Enter the result in the **Networking > External interface > Netmask** field of the SSB welcome wizard.

       For detailed information on the SSB welcome wizard, see "The Welcome Wizard and the first login" in the Administration Guide.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product