

DEPLOYMENT GUIDE

Infoblox Trinzic V-x25 Series Appliances for AWS

NIOS version 8.2 | Oct. 2017

Contents

Overview	3
Introduction	3
Trinzic x25 Models	3
Availability	3
Creating a New Trinzic V-x25 Series Appliance	5
Launch Instance	5
Verifying Launch Status	12
AWS Console	12
EC2 Instance Screenshot	12
EC2 Instance System Logs	14
Managing Your Appliance	15
SSH (Secure Socket Shell)	15
Connecting to Your Appliance	15
Applying License Keys	17
Adding a new Infoblox appliance to an existing Grid	18
Join Appliance to a Grid	19
Using the Grid Manager GUI	20
Join Failures	22
Appendix	22
Using a Public IP Address	22
Creating an Elastic IP Address	22
Associating an Elastic IP	23
AWS User Data	25
Supported Directives	25
Obtaining the Certificate	26
Obtaining the Token	28

Overview

Introduction

The Trinzic (TE) x25 series appliances are the next generation of the Trinzic platform from Infoblox and provide enterprise-grade DNS and IPAM services across your AWS VPC's. The Trinzic x25 series appliances provide improved performance over older generation appliances, enabling you to keep up with today's increasingly complex demands for services, security, automation and visibility.

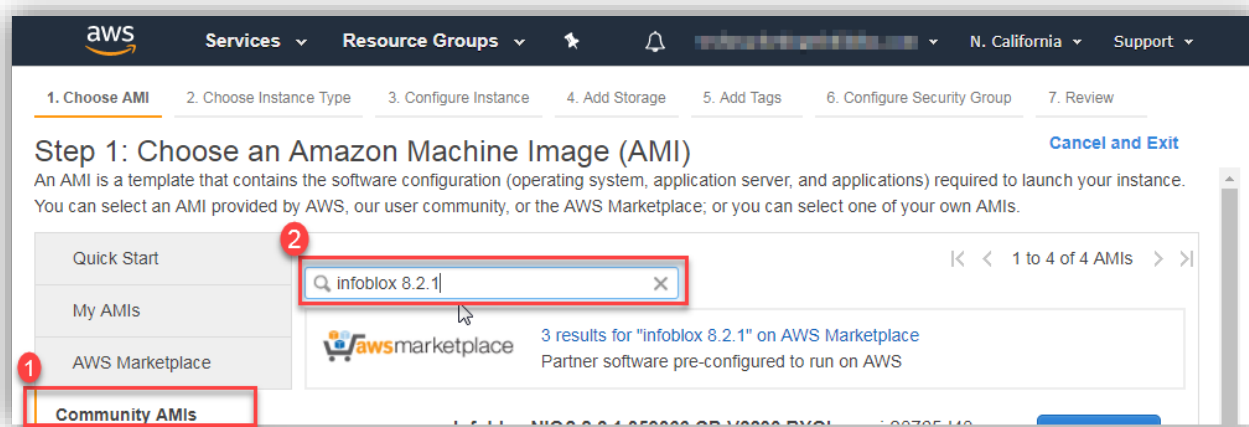
Trinzic x25 Models

The Trinzic x25 series appliances come in three model types that are designed to deliver the performance, capacity, and availability required in each unique environment, from the smallest branch office to the largest enterprise or service provider network.

NIOS VM Models	Description	Grid Master/Grid Master Candidate	vCPU	Amazon EC2 Shape
TE-V825	Designed to serve remote and branch locations.	Small Grids Only	2	r4.large
TE-V1425	Designed for larger remote and branch locations, as well as small-to-medium sized organizations.	Yes	4	r3.xlarge/r4.xlarge
TE-V2225	Designed for enterprises and large scale DNS/DHCP applications.	Yes	8	r4.2xlarge

Availability

The AMI's (Amazon Machine Images) for the Trinzic x25 series appliances can be found through the AWS Community AMI's page. In the **Search Community AMIs** text box, type Infoblox and press enter to search for all available Infoblox images. You can narrow down the results by also including a NIOS version in the search box. Example:



Note: The Trinzic x25 series appliances are available starting in NIOS version 8.2.

For each version of NIOS where the x25 model appliances are available, you will find a single EC2 image is used for each of the three different models. The 'shape' used for the appliance being created must match the recommendation provided in the table above, as well as in the description for the AMI.

The ID for each AMI will vary per region and are subject to change without notice. Contact Infoblox Support (<https://support.infoblox.com/>) for any further details regarding this or if any additional verification is required.

The following table provides the ID's for each x25 AMI known at the time of this publication:

Locale	NIOS Version	Region	AMI ID
Europe	8.2.1	eu-central-1 (Frankfurt)	ami-93e34dfc
	8.2.1	eu-west-1 (Ireland)	ami-26c83f5f
	8.2.1	eu-west-2 (London)	ami-26dacb42
Asia Pacific	8.2.1	ap-northeast-1 (Tokyo)	ami-e4886082
	8.2.1	ap-northeast-2 (Seoul)	ami-1003da7e
	8.2.1	ap-south-1 (Mumbai)	ami-3c84ff53
	8.2.1	ap-southeast-1 (Singapore)	ami-dc1688bf
	8.2.1	ap-southeast-2 (Sydney)	ami-60766f03
South America	8.2.1	sa-east-1 (São Paulo)	ami-ad5026c1
North America	8.2.1	ca-central-1 (Canada)	ami-76e35d12
	8.2.1	us-east-1 (N. Virginia)	ami-8988abf2
	8.2.1	us-east-2 (Ohio)	ami-4ffada2a
	8.2.1	us-west-1 (N. California)	ami-5a72593a
	8.2.1	us-west-2 (Oregon)	ami-ac20c6d4

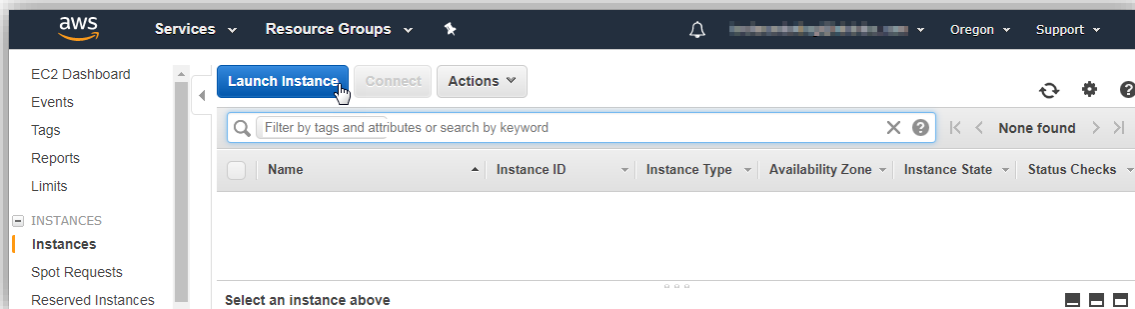
Note: The AMI ID's are subject to change at any time and without notice.

Creating a New Trinzic V-x25 Series Appliance

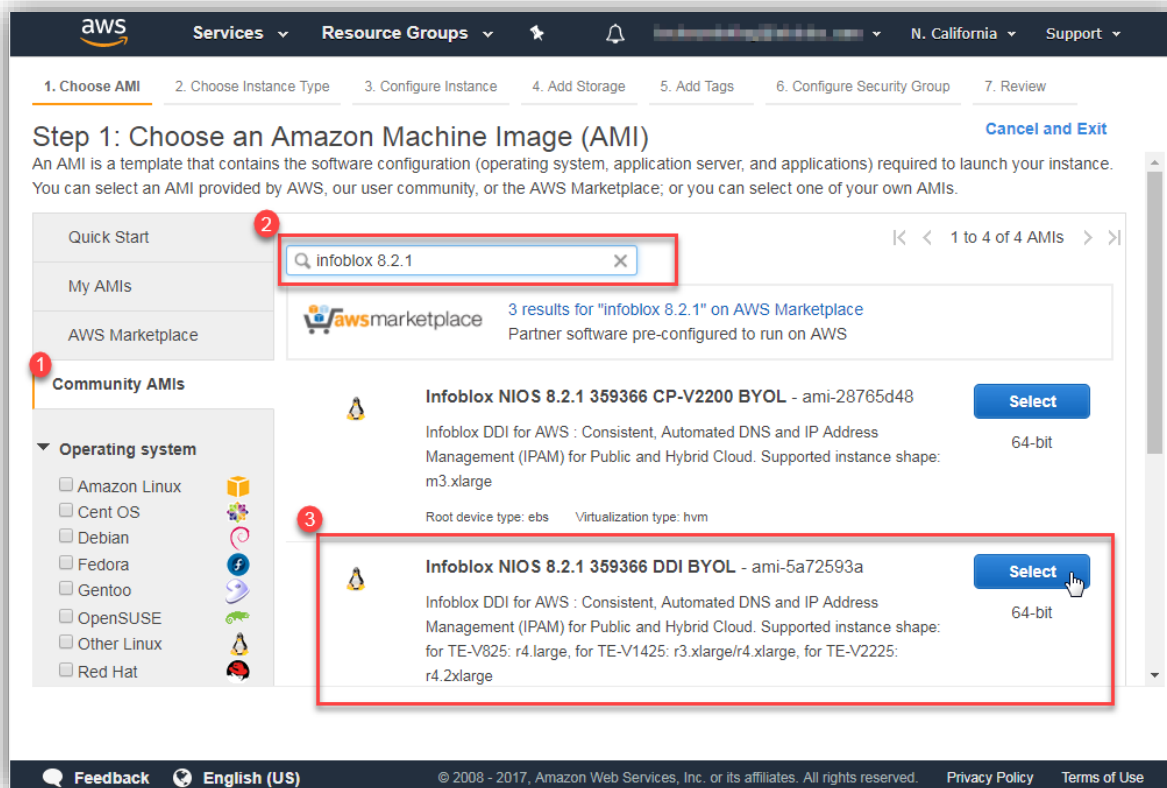
Launch Instance

Trinzic appliances can be launched using different methods, including the AWS console (GUI), AWS CLI, Auto-Scale Groups or numerous orchestration/automation platforms that are available. In this guide, we will complete all operations using the AWS console (<https://console.aws.amazon.com>).

1. In the AWS console, expand the **Services** menu and under **Compute**, select **EC2**.
2. Open the **Instances** tab and click **Launch Instance**.

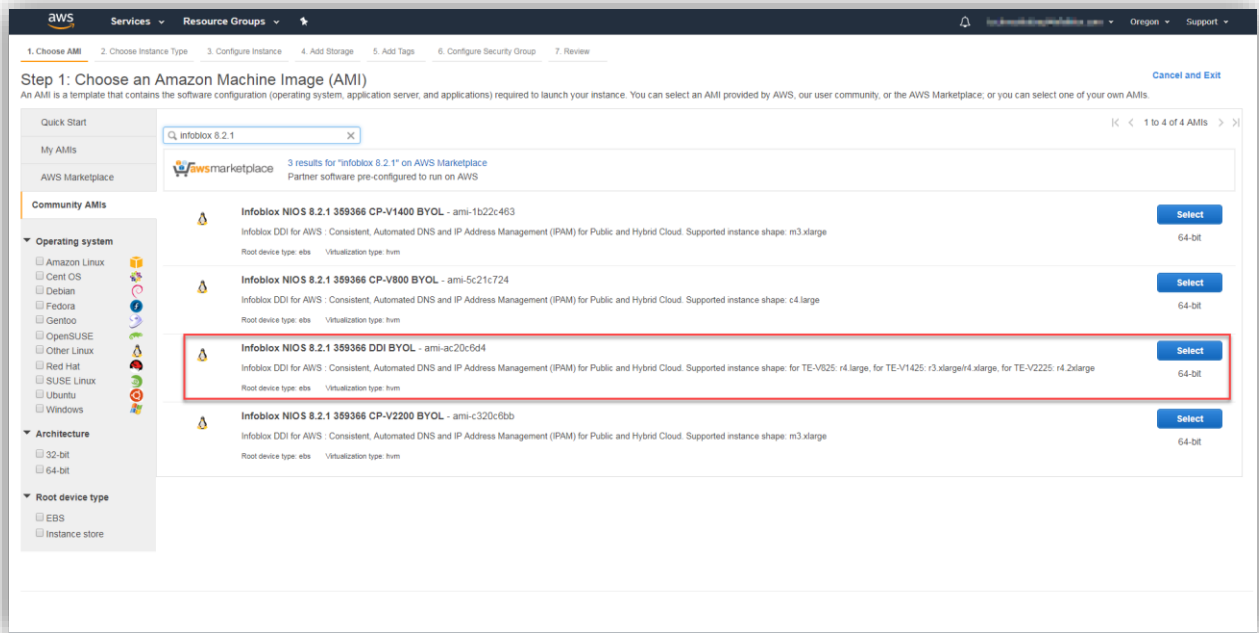


3. Switch to the **Community AMIs** tab.
4. In the Search Community AMIs text box, type "**Infoblox**", along with a NIOS version, and press **Enter**. Example:



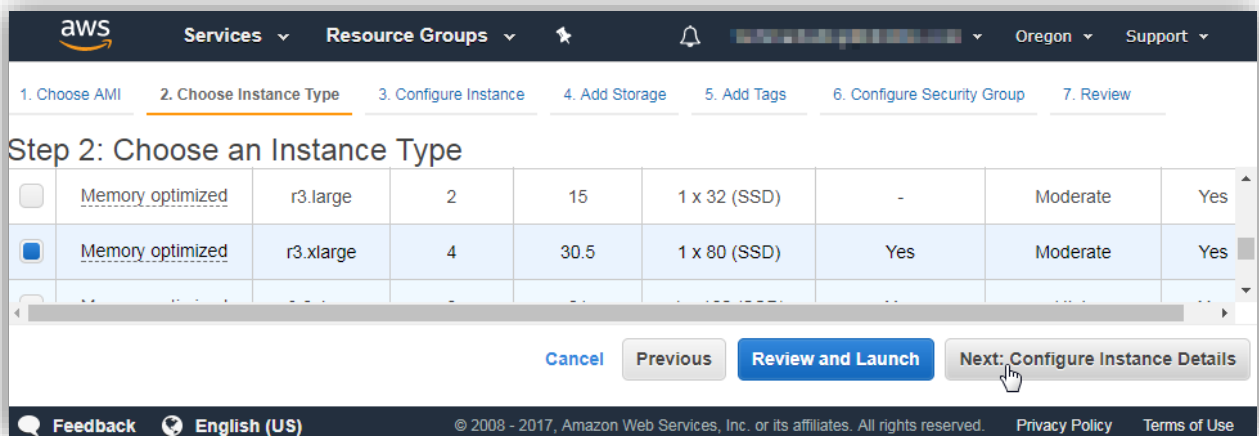
- Click on the **Select** button for the AMI which corresponds to the x25 AMI.

Note: Starting in NIOS version 8.2, you will see four AMI's per NIOS version (previous versions of NIOS used a total of six different images). Three of these will be for the Cloud Platform (CP) model appliances and include the model type in the AMI name. The x25 AMI image does not include a model type in the AMI name and will use a name such as “*Infoblox NIOS 8.2.1 359366 DDI BYOL*”. You will also find the supported x25 model types and shapes (machine sizes) in the description for the AMI.



- Select the instance type to be used for the model appliance being deployed and click **Next: Configure Instance Details**.

TE-V825= r4.large. TE-V1425= r3.xlarge or r4.xlarge. TE-V2225= r4.2xlarge



7. Configure the details for your x25 appliance, including the network and subnet that the appliance should operate on.

Note: A subnet must be assigned before completing the next step.

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: 1 [Launch into Auto Scaling Group](#)

Purchasing option: ☐ Request Spot instances

Network: vpc-67a20103 | VPC1 (default) [Create new VPC](#)

Subnet: No preference (default subnet in any Availability Zone) [Create new subnet](#)

Auto-assign Public IP: Use subnet setting (Disable)

Placement group: No placement group

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](#)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

8. Scroll down to the Network Interfaces section and click **Add Device**. Complete any required configurations to the interface. If a public IP address (PIP), this must be associated after the appliance has been launched. Refer to the section titled “**Assigning a Public IP Address**” later in this guide for more details. Eth0 is reserved for future use. Eth1 is used for the LAN1 interface.

Note: **This step is required.** Failing to add a second network interface will result in the appliance being unable to start. The error “Fatal Error During Infoblox Startup” will be visible in the appliances console.

Step 3: Configure Instance Details

EBS-optimized instance: ☐ Launch as EBS-optimized instance [Additional charges apply.](#)

Tenancy: Shared - Run a shared hardware instance [Additional charges will apply for dedicated tenancy.](#)

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-0021335f	Auto-assign	Add IP	

[Add Device](#)

Advanced Details

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

[Feedback](#) [English \(US\)](#) © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

- Under the **Advanced Details** section, set any **User data** directives that you want to apply. This is useful for automatically applying temporary license keys, setting the admin password and even to join an existing Grid. More details regarding this can be found in the **Appendix** in this guide, as well as the **Infoblox Installation Guide for vNIOS for AWS** (available on the Infoblox Support portal: <https://support.infoblox.com/>).

The following example demonstrates how to enable temporary license keys for a TE-V1425 appliance with the DNS, Grid and Cloud (Cloud Network Automation) licenses. These keys will be valid for 60 days. Note: License keys can also be applied by connecting to the appliance via SSH once it has successfully started. Refer to the section titled “**SSH (Secure Socket Shell)**” later in this guide for more details.

```
#infoblox-config
temp_license: nios,IB-V1425,enterprise,dns,cloud
default_admin_password: '$*&$#!'
```

- Click **Next: Add Storage**.

The screenshot shows the AWS Management Console interface for configuring an EC2 instance. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and a dropdown for 'Oregon'. Below the navigation bar, a progress bar shows seven steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance (active), 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. The main heading is 'Step 3: Configure Instance Details'. A note states: 'Instances with one network interface. To re-enable the auto-assign public IP address feature, please specify only the eth0 network interface.' Below this is an 'Add Device' button. The 'Advanced Details' section is expanded, showing 'User data' with a dropdown menu set to 'As text'. The user data field contains the configuration script: `#infoblox-config`, `temp_license: nios,IB-V1425,enterprise,dns,cloud`, and `default_admin_password: 'infoblox'`. At the bottom, there are four buttons: 'Cancel', 'Previous', 'Review and Launch', and 'Next: Add Storage'. A mouse cursor is pointing at the 'Next: Add Storage' button. The footer includes 'Feedback', 'English (US)', copyright information, and links to 'Privacy Policy' and 'Terms of Use'.

- Select the desired Volume Type. SSD type storage should be used for production environments as this can have a direct impact on performance. Magnetic storage can be used in lab/testing environments or for appliances which will not be expected to any experience heavy disk write activity.

aws Services Resource Groups Oregon Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-0979c35790a9659a1	245	Magnetic	N/A	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

General Purpose (SSD) volumes provide the ability to burst to 3000 IOPS per volume, independent of volume size, to meet the performance needs of most applications and also deliver a consistent baseline of 3 IOPS/GiB. [Set my root volume to General Purpose \(SSD\)](#).

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

Feedback English (US) © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

12. Click **Next: Add Tags**.

13. Configure any tags as required (such as **Name**, which assigns a name to the instance) and click **Next: Configure Security Group**.

aws Services Resource Groups Oregon Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)	Instances	Volumes
This resource currently has no tags			

Choose the Add tag button or [click to add a Name tag](#).
Make sure your [IAM policy](#) includes permissions to create tags.

[Add Tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

Feedback English (US) © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

14. Create a new Security Group, or select an existing one. Verify that the necessary ports required for connections to the appliance are allowed. Refer to the **Sources and Destinations for Services** section in the **NIOS Administrators Guide** for more details on ports commonly used, such as TCP 443 (for the GUI), UDP 2114 and 1194 for Grid communications (required to join a Grid), and both UDP and TCP 53 (for DNS).

aws Services Resource Groups Oregon Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

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

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desk

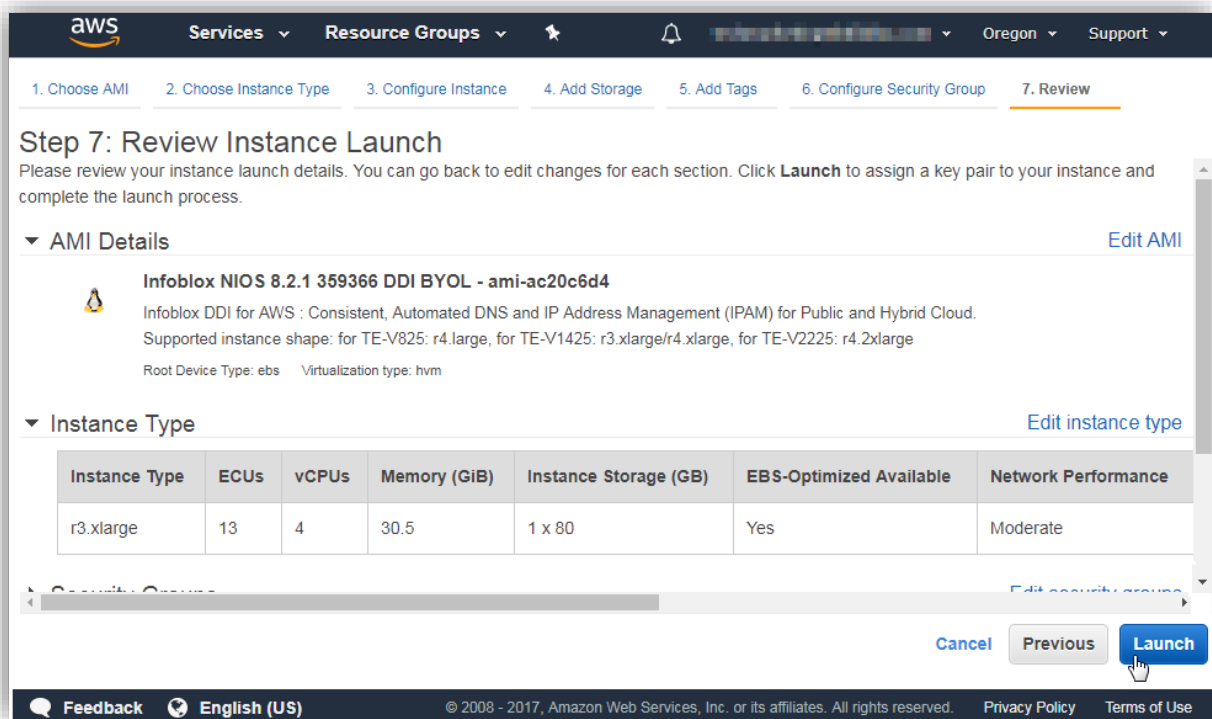
Cancel Previous **Review and Launch**

Feedback English (US) © 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

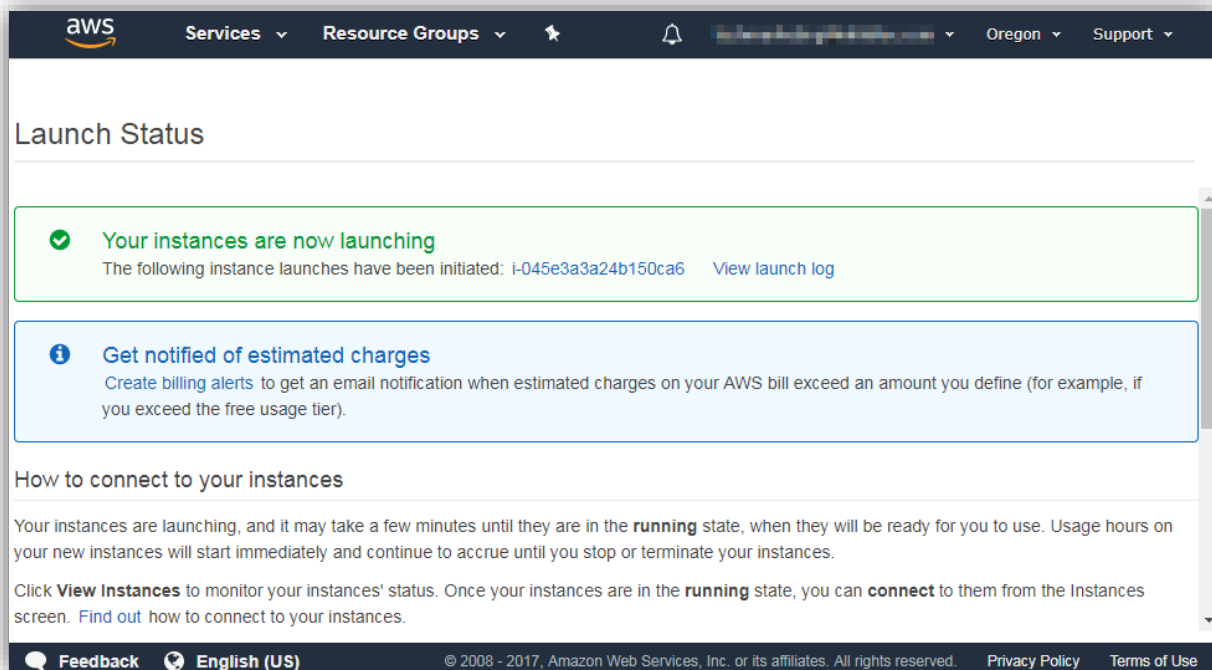
15. Click **Review and Launch**.

16. Verify the configuration and click **Launch**. Continue through any prompts that may be displayed, including for the Key Pair to be assigned to the instance, to complete the launch process.

Note: Access to the appliance via SSH will use the admin credentials, not a key pair.



17. The AWS console should show a confirmation that the instance is now launching.

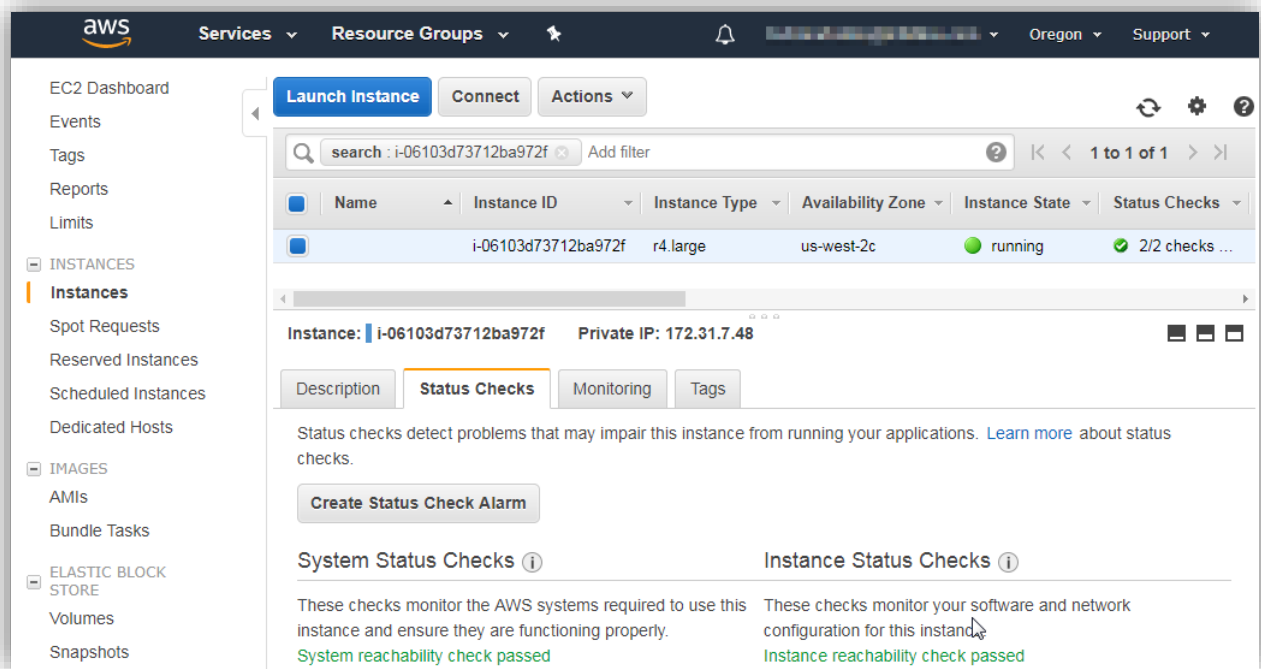


Verifying Launch Status

AWS Console

After the Trinzic V-x25 appliance has been launched, you can monitor its status in the AWS console under the **Services** -> **EC2** -> **Instances** page. AWS has two types of status checks built in to monitor the launch status:

1. System Status Checks: This will show a success once the instance has been created.
2. Instance Status Checks. This check will show a successful status once the instance becomes reachable.

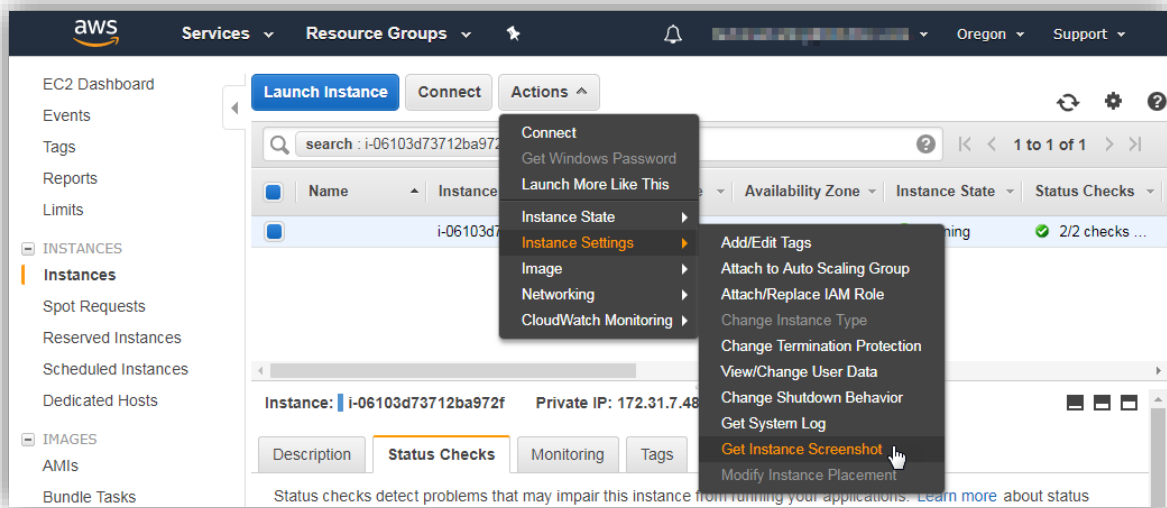


The AWS console also gives you the ability to get a screenshot of the console or view the most recent system logs for the instance.

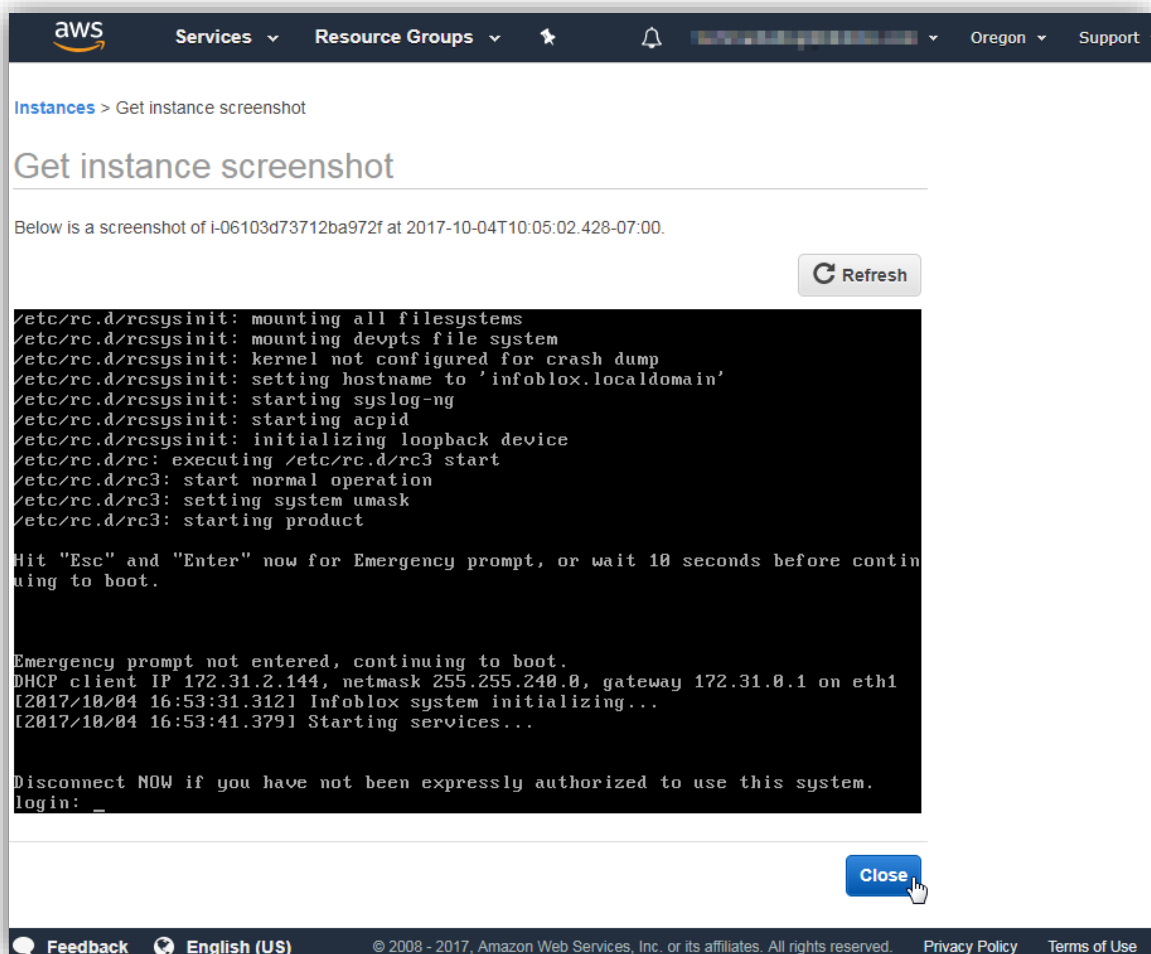
EC2 Instance Screenshot

Viewing the instance screenshot can be very useful to get the current status of your appliance and becomes available once NIOS has begun its startup process. To view the screenshot for your instance:

1. On the **Instances** page, select the row for your TE-x25 appliance
2. Expand the **Actions** -> **Instance Settings** menu and select **Get Instance Snapshot**.



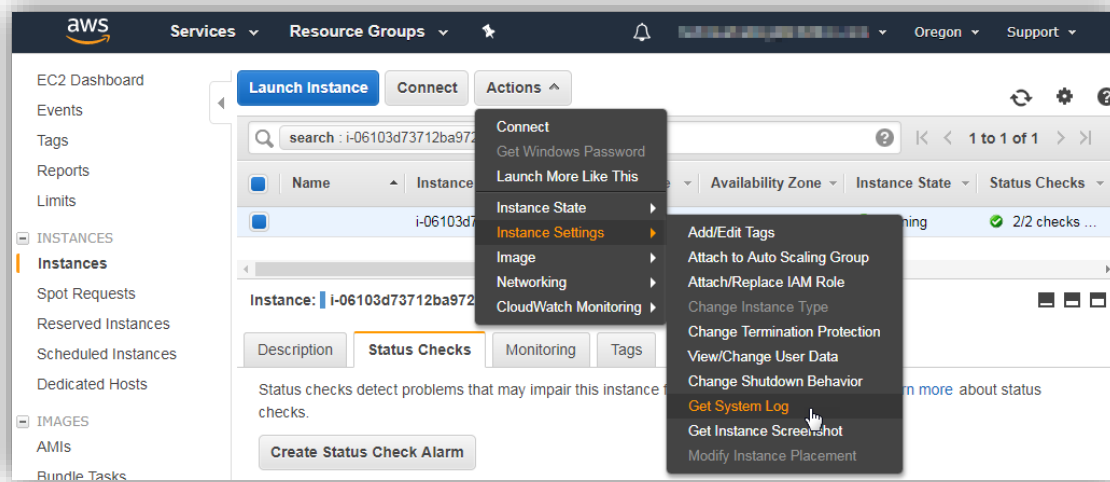
3. This will show a recent screenshot of the serial console output redirected from.



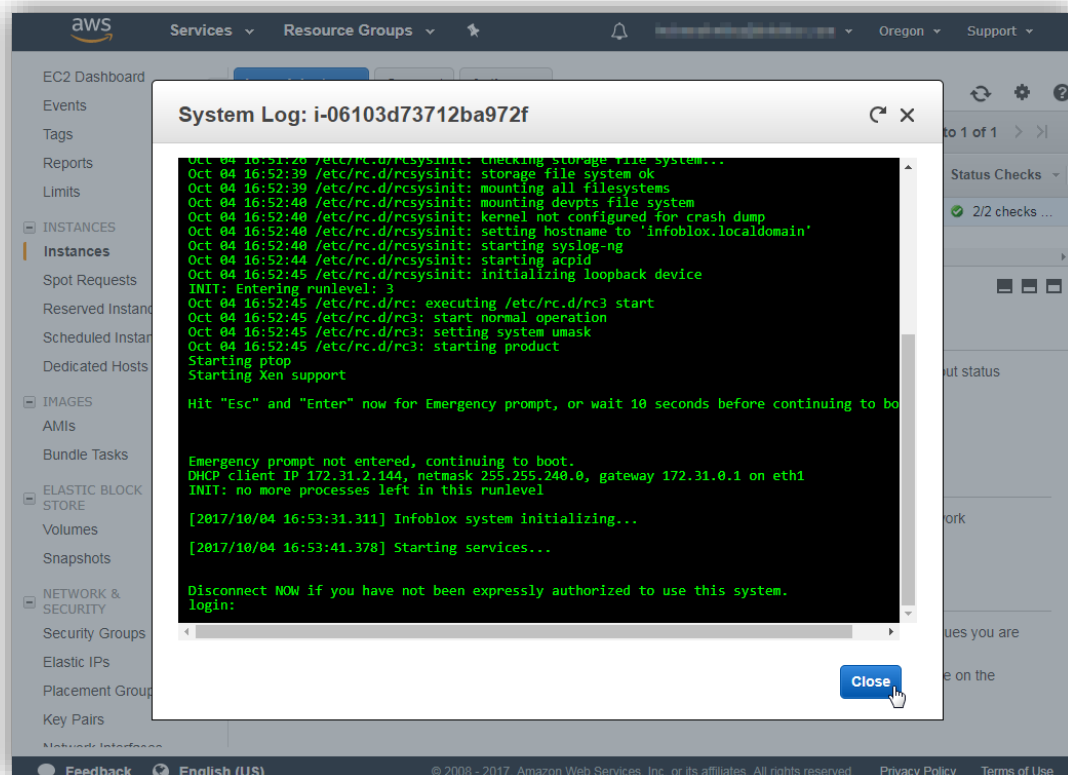
4. Click **Close** to return to the Instances page.

EC2 Instance System Logs

5. Select the row for your TE-x25 appliance
6. Expand the **Actions** -> **Instance Settings** menu and select **Get System Log**.



7. Review the log output which is displayed. Once the snapshot of the logs updates, an appliance which has successfully started will show the login prompt as the last entry.



Note: This is only a snapshot of the system logs and is updated very infrequently so this is not always indicative of the most recent status of the appliance, even after using the refresh button. Viewing the instance screenshot can frequently be a more useful way of viewing the current state of the appliance.

8. Click **Close** to return to the Instances page.

Managing Your Appliance

SSH (Secure Socket Shell)

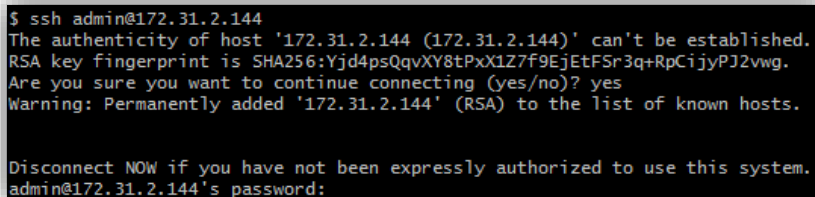
Remote Console Access is enabled automatically on Infoblox appliances being deployed in AWS as remote access would not be possible unless this was done through the **User data** field when launching the appliance. Once NIOS successfully starts, CLI (command line interface) access via SSH may be required to complete any remaining configurations. This can also be used to verify its current status and retry configurations for cases where configurations attempted through the **User data** field may not have applied successfully. The user name will be “admin” and the password will either be the default (infoblox), or the password applied in the User data field during the instance configuration.

Connecting to Your Appliance

Linux based (including Apple) computers can use the ssh command in a Terminal window:

```
ssh admin@<ip-address>
```

For example:

A terminal window showing the execution of the ssh command. The prompt is '\$ ssh admin@172.31.2.144'. The output shows a warning about the host's authenticity, the RSA key fingerprint, and a confirmation to continue connecting. The user responds 'yes'. A warning message states that the host has been added to the list of known hosts. The terminal then prompts for a password.

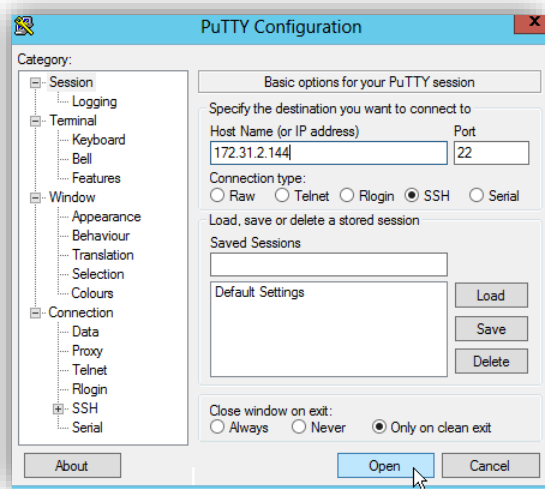
```
$ ssh admin@172.31.2.144
The authenticity of host '172.31.2.144 (172.31.2.144)' can't be established.
RSA key fingerprint is SHA256:Yjd4psQqvXY8tPxX1Z7f9EjEtFSr3q+RpCijyPJ2vwg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.31.2.144' (RSA) to the list of known hosts.

Disconnect NOW if you have not been expressly authorized to use this system.
admin@172.31.2.144's password:
```

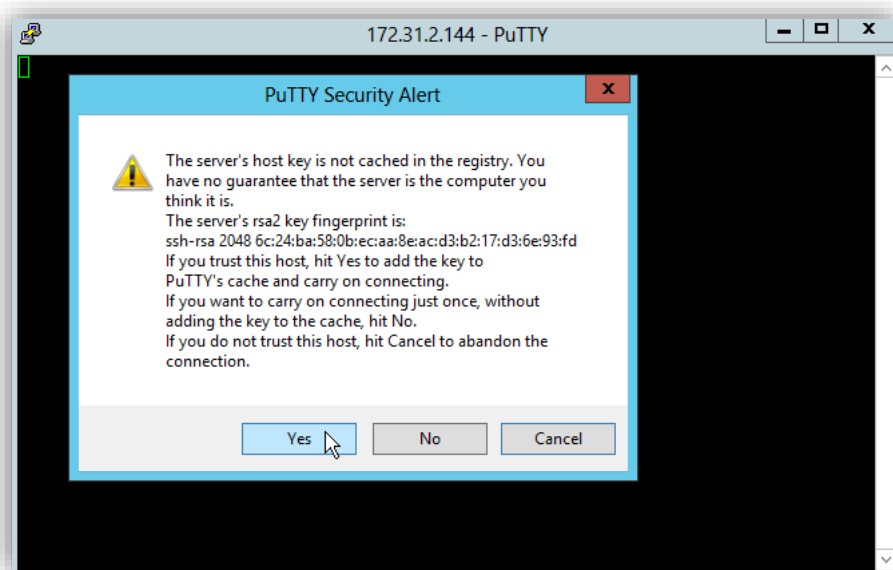
Administrators on Windows based computers will need to use a program when establishing SSH connections. These can include a program which can be executed through a command prompt, or a GUI based application (such as Putty or SecureCRT, among many others).

In this guide, we describe connecting using Putty.

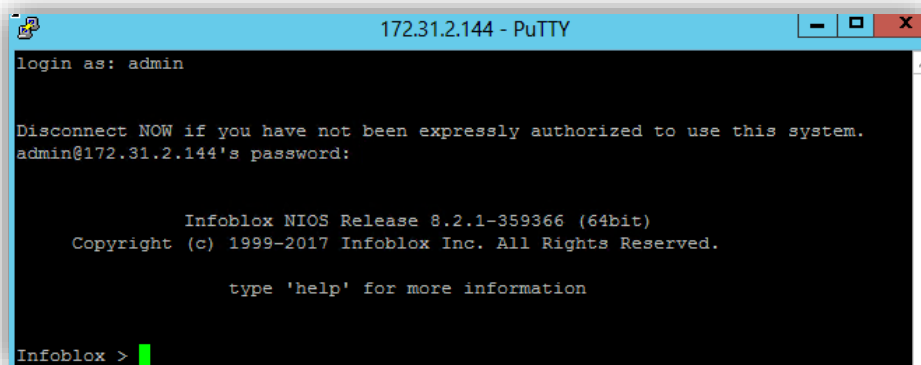
1. Install and launch putty.exe (an open source and freely available application- <http://www.putty.org/>).
2. Type the IP address (or resolvable DNS name) for your Infoblox appliance, set the **Port** number to 22, the **Connection type** to SSH and click **Open**.



3. Confirm or accept any prompts that appear asking to trust or update the host key and allow the connection to proceed to your Infoblox appliance.



4. Enter the credentials when prompted. This will bring you to the appliances CLI.



```
172.31.2.144 - PuTTY
login as: admin

Disconnect NOW if you have not been expressly authorized to use this system.
admin@172.31.2.144's password:

      Infoblox NIOS Release 8.2.1-359366 (64bit)
      Copyright (c) 1999-2017 Infoblox Inc. All Rights Reserved.

      type 'help' for more information

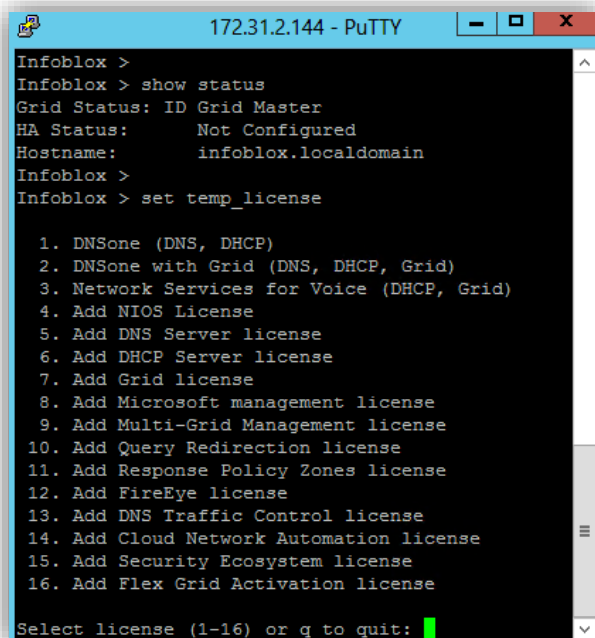
Infoblox > █
```

Applying License Keys

Once the appliance has been deployed, license keys can be manually applied if not done so during the launch process or when not using pool licensing. When enabling temporary license keys, this is done through the CLI. Permanent license keys can be applied through either the CLI, or for the Grid Manager GUI. In this guide, we will use the CLI to apply temporary license keys.

To enable temporary license keys:

1. Connect to the CLI for your Infoblox appliance.
2. Type the command "**set temp_license**" and press **Enter**.



```
172.31.2.144 - PuTTY
Infoblox >
Infoblox > show status
Grid Status: ID Grid Master
HA Status:      Not Configured
Hostname:       infoblox.localdomain
Infoblox >
Infoblox > set temp_license

  1. DNSone (DNS, DHCP)
  2. DNSone with Grid (DNS, DHCP, Grid)
  3. Network Services for Voice (DHCP, Grid)
  4. Add NIOS License
  5. Add DNS Server license
  6. Add DHCP Server license
  7. Add Grid license
  8. Add Microsoft management license
  9. Add Multi-Grid Management license
 10. Add Query Redirection license
 11. Add Response Policy Zones license
 12. Add FireEye license
 13. Add DNS Traffic Control license
 14. Add Cloud Network Automation license
 15. Add Security Ecosystem license
 16. Add Flex Grid Activation license

Select license (1-16) or q to quit: █
```

3. Type the number for the license being enabled and press **Enter**.
4. Enter '**y**' at any confirmation prompts to complete the license installation.

```

Infoblox > set temp_license

1. DNSone (DNS, DHCP)
2. DNSone with Grid (DNS, DHCP, Grid)
→ 3. Network Services for Voice (DHCP, Grid)
4. Add NIOS License
5. Add DNS Server license
6. Add DHCP Server license
7. Add Grid license
8. Add Microsoft management license
9. Add Multi-Grid Management license
10. Add Query Redirection license
11. Add Response Policy Zones license
12. Add FireEye license
13. Add DNS Traffic Control license
14. Add Cloud Network Automation license
15. Add Security Ecosystem license
16. Add Flex Grid Activation license

Select license (1-16) or q to quit: 7

This action will generate a temporary 60-day Add Grid license.
Are you sure you want to do this? (y or n): y
Grid temporary license installed.

Temporary license is installed.

The UI needs to be restarted in order to reflect license changes.
Restart UI now, this will log out all UI users? (y or n):y

Are you sure you want to do this? (y or n): y
UI restarted.
Infoblox > █

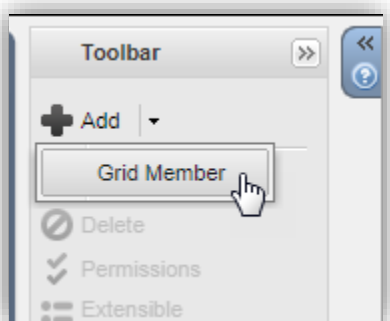
```

Note: The vNIOS or NIOS (referenced as just 'NIOS' going forward) license is required for the appliance to be able to start. After the NIOS license is installed, the appliance will restart and you need to reconnect to the appliance to complete any remaining steps. For this reason, it may be desirable to install the NIOS license last, but this is not a requirement and the licenses can be installed in any order.

Adding a new Infoblox appliance to an existing Grid

Before being able to join a new appliance to a Grid, it must be added (defined) in the Grid first. To add a new appliance to an existing Grid:

1. In your Grid Manager GUI, navigate to the **Grid -> Grid Manager -> Members** tab.
2. Click on the **Add** menu and select **Grid Member**.



3. Expand the **Member Type** dropdown menu and select **Virtual NIOS**.

Add Grid Member > Step 1 of 3

Member Type: Infoblox

Host Name*: Infoblox Must be a fully qualified domain name

Time Zone: Virtual NIOS Inherited from Grid Infoblox Override

Comment:

Master Candidate: ☐

Buttons: Cancel Previous Next Save & Close

4. In the **Host Name** field, type a name (using its intended fully qualified domain name, though this can always be changed later) and click **Next**.
5. Enter the **IP Address**, **Subnet Mask** and default **Gateway** for the appliance.

Note: You can verify the appliances network configuration by connecting to its CLI and entering the command “**show network**”.

Add Grid Member > Step 2 of 3

Type of Network Connectivity: IPv4

Type of Member:

- ☒ Standalone Member
- ☐ High Availability Pair

Required Ports and Addresses

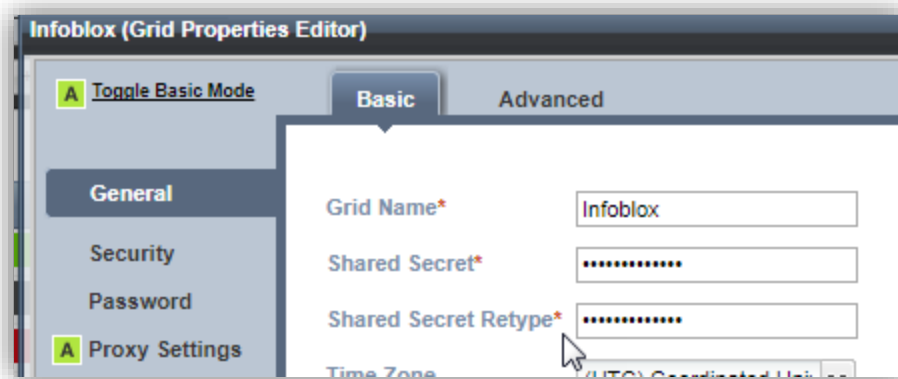
Interface	Address	Subnet Mask (IPv4) or Prefix Length (IPv4)	Gateway	VLAN Tag	Port Settings
LAN1 (IPv4)	<input type="text"/>				Automatic

Buttons: Cancel Previous Next Save & Close

6. Click **Save & Close**.

Join Appliance to a Grid

An Infoblox appliance can be joined to a Grid using the CLI, or the Grid Manager GUI. When joining a Grid, you will first want to take note of the Grid Masters IP address, the name of the Grid that you will be joining, and the Shared Secret which will be used to authenticate the connection. You can verify the Grid name and Shared Secret by navigating to Grid -> Grid Manager -> Members in the Grid Manager GUI for your Grid Master. There, click on the Grid Properties button and review these details under the General tab:



Note: The Shared Secret is encrypted once it is saved. There is no recovery mechanism should this be lost. The value can be changed without any impact to any appliances online in your Grid. Any offline Grid members would need to be reset before being joined back to the Grid after any change is made to the Shared Secret. The default Shared Secret is “test”.

Using the CLI:

1. Log in to your Infoblox appliance using an SSH client.
2. Type the command “**set membership**”.
3. Type the IP address of the Grid Master for the Grid being joined and press **Enter**.
4. Type the Grid Name if different from the default (*Infoblox*) and press **Enter**.
5. Type the Shared Secret (default is *test*) and press **Enter**.
6. Verify that the join details are correct and enter ‘y’ at the confirmation process to begin the join process.

```

Infoblox > set membership
Join status: No previous attempt to join a grid.
Enter New Grid Master VIP: 10.60.27.240
Enter Grid Name [Default Infoblox]:
Enter Grid Shared Secret: test
Join grid as member with attributes:
Grid Master VIP:      10.60.27.240
Grid Name:            Infoblox
Grid Shared Secret:   test

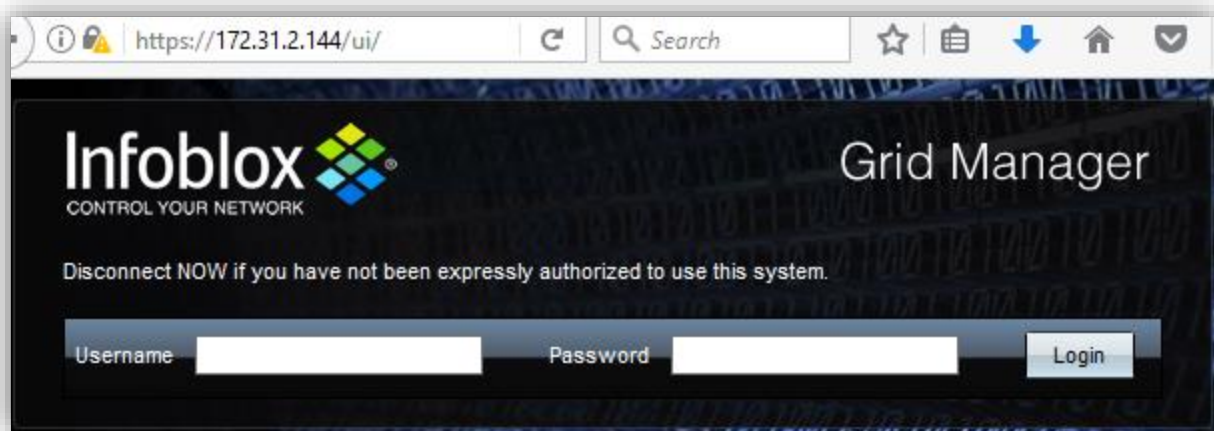
WARNING: Joining a grid will replace all the data on this node!
Is this correct? (y or n): y
Are you sure? (y or n): y

```

7. Your SSH session will then close. Further monitoring can be done using the Grid Manager GUI for the Grid the appliance is joining.

Using the Grid Manager GUI

Once your appliance is accessible on your network and is properly licensed (requires at least the NIOS license), you can connect to it using your web browser. NIOS uses the Grid Manager GUI for its graphical interface and can be accessed by typing <https://<IP Address>> in the address bar of your web browser.



Note: All NIOS appliances use a self-signed certificate with the name www.infoblox.com by default. Certificate validation warnings displayed by your browser are to be expected and you may need to trust this self-signed certificate or add exceptions before being able to connect to the Grid Manager GUI.

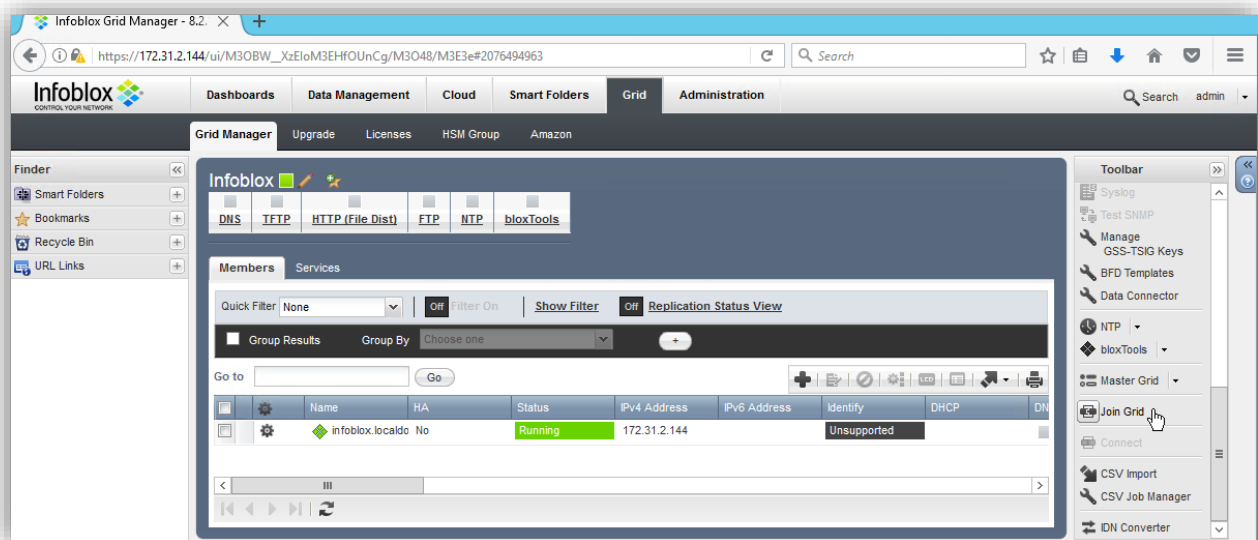
Join a Grid Using the Grid Manager GUI

To join your Infoblox appliance to an existing using its Grid Manager GUI:

1. Log in to the Grid Manager GUI for the appliance being joined to your Grid.

Note: First time connections will be prompted to accept the End-User License Agreement.

2. If the Grid Startup Wizard is displayed, click **Cancel**.
3. Navigate to the **Grid -> Grid Manager -> Members** tab.
4. In the vertical toolbar on the right-hand side of the page, click on the Join Grid button.



5. Type the IP address of the Grid Master for the Grid being joined, along with the Grid Name and Shared Secret.
6. Click **OK**.
7. Your GUI session will end at this point and the browser may stop responding. Use the Grid Manager GUI for the Grid the appliance is joining to monitor the join process. Multiple restarts can be expected on the appliance as it joins the Grid, including if the NIOS software must be synchronized and for it to apply the database it receives from the Grid Master.

Join Failures

Should the join attempt fail, you will want to do the following:

1. Verify that the new Grid member was added to the Grid being joined and that its network details are correct (use the “show network” command on the appliances CLI to view its network configuration).
2. Verify that the appliance has been properly licensed. It will require at least the NIOS and Grid (or sometimes referred to as *enterprise*) licenses.
3. Verify that the IP address of the Grid Master for the Grid being joined, along with the Grid name and Shared Secret provided during the join setup were entered in correctly.
4. Verify that there are no connectivity issues between the appliance and the Grid Master (requires at least UDP ports 2114 and 1194 by default).
5. Connect to the CLI for the appliance and enter the command “**show status**” to check for any errors that may be reported there.

```
Infoblox > show status
Grid Status: ID Grid Master
HA Status:      Not Configured
Hostname:       infoblox.localdomain
Previous grid join attempt FAILED.
Error: Failed to contact MASTER; wrong IP or node was not added at master
The join parameters were:
    Master VIP: 10.60.27.240
    Grid Name: Infoblox
    Grid Shared Secret: ****
```

Note: In the above example, the wrong IP address was configured in the Grid for this appliance.

6. Contact your Infoblox account (Sales) team, Infoblox Technical Support (<https://support.infoblox.com/>) or the Infoblox Community Forums (<https://community.infoblox.com/>) for assistance in troubleshooting join failures.

Appendix

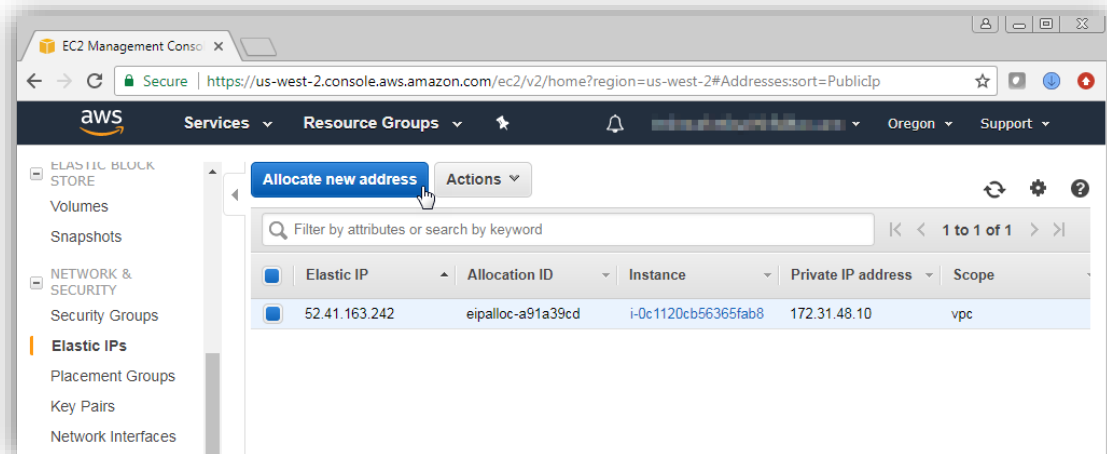
Using a Public IP Address

Connections to instances in AWS may require an IP address which is accessible across the Internet without using any special routing to connect back in to your AWS VPC. To accomplish this, you can use an Elastic IP Address and assign that to the Network Interface associated with the eth1 interface attached to your appliance.

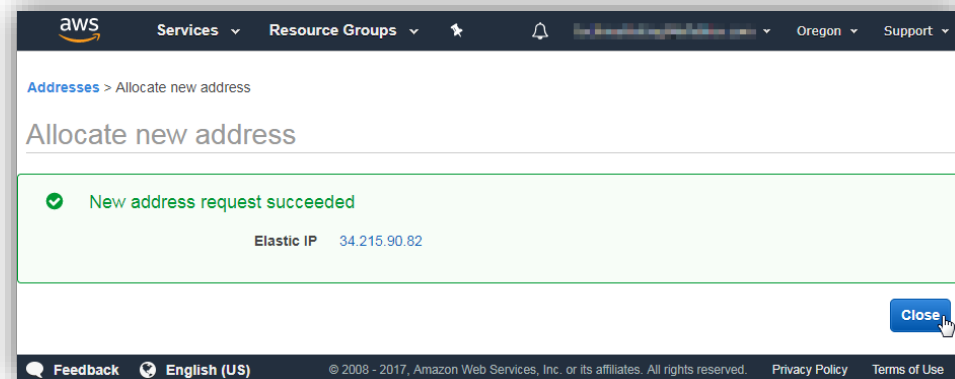
Creating an Elastic IP Address

Before being able to associate an elastic IP address to an EC2 instance, it must be created. To create the elastic IP:

1. In the AWS Console, navigate to **Services** -> **EC2** and open the **Elastic IPs** tab.
2. Click on the **Allocate new address** button.



3. Click on the **Allocate** button.

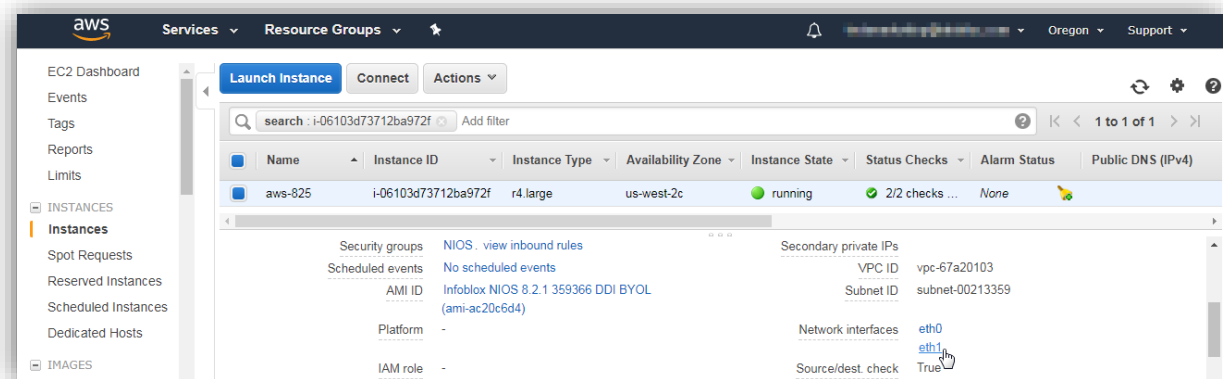


4. Click **Close**.

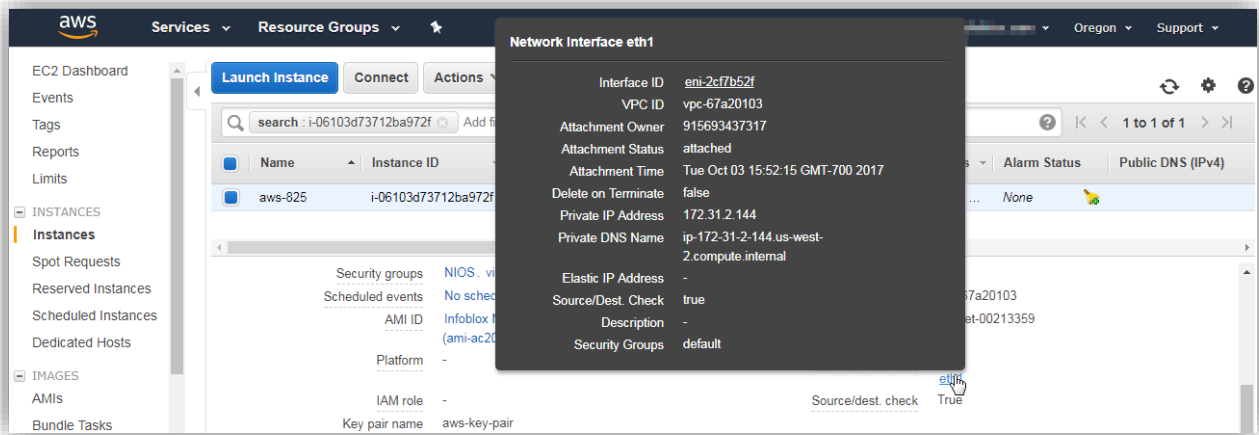
Associating an Elastic IP

To associate the elastic IP to your Infoblox appliance:

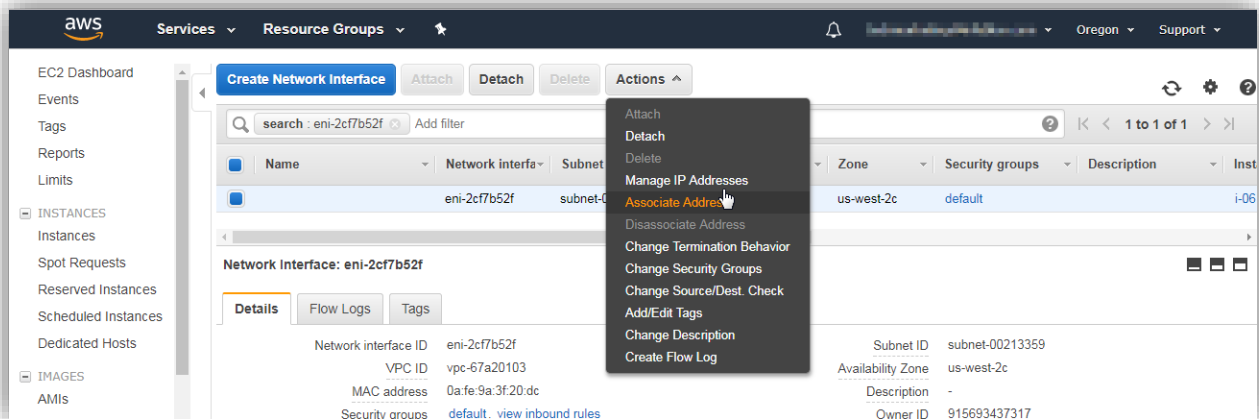
1. Navigate to **Services -> EC2 -> Instances**.
2. Select the row for your Infoblox appliance.
3. In the bottom panel, scroll to the **Network interfaces** section and click on the **eth1** link.



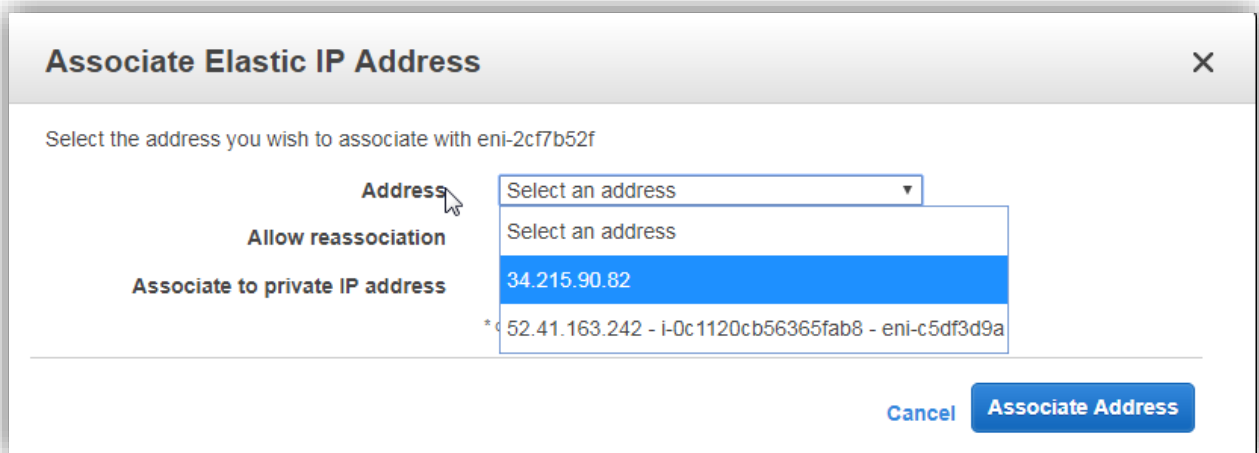
4. Click on the link for the Interface ID.



5. Expand the **Actions** menu and select **Associate Address**.



6. Select the **Elastic IP Address** to assign to your Infoblox appliance and click **Associate Address**.



7. Verify that connectivity now works. If the Elastic IP address does not respond, verify that all Security Groups and Route tables are setup correctly.

AWS User Data

When configuring the instance details while launching your Trinzic x25 appliance, you can include directives which will be used to configure your appliance once it successfully launches. The text entered user data field uses the YAML format and can be entered in directly as text, or uploaded in a YAML formatted text file. Optionally, you can also convert this content to base64 encoding prior to entering it in or uploading it. If not converted first, AWS will do so for you as the data is sent to the appliance using base64 encoding.

When structuring the user data, it is important to note that YAML uses indentations to identify each block in the data. When entering directives that include parameters spread across multiple lines, any lines after the first one **MUST** use matching indentations. If the indentations are not set correctly, a failure will occur when cloud-init (the internal service/process which sets up the environment for systems operating in AWS and other cloud environments) processes the data.

Any lines which include data that is line wrapped (spread across multiple lines) must begin with a pipe character to be processed correctly. Example:

```
Certificate: |
```

Supported Directives

Common Directives

The following is a list of commonly used directives. While not exhaustive, this list includes the directives applicable to an appliance being deployed in AWS. Any 'sub-parameters' are also shown with the required indentation.

Note: The "**#infoblox-config**" directive is required and be placed as the first line.

```
#infoblox-config
temp_license:
default_admin_password:
gridmaster:
    token:
    ip_addr:
    certificate:
```

Note: If pool licenses have been applied to the appliance, these will take precedence over any temporary license keys being applied here.

Example:

```
#infoblox-config
temp_license: cloud,vnios,IB-1425,dns,enterprise
gridmaster:
  token: uQB6bEHtwYGNqkd8gxdCWoLX1JKuy5yv
  ip_addr: 10.60.27.240
  certificate: |
    -----BEGIN CERTIFICATE-----
    MIIDdzCCA18CEGE5IRHoUY/vgTjrYH6ftn8wDQYJKoZIhvcNAQEFBQAwejELMAkG
    A1UEBhMCMVVMxEzARBgNVBAGTCkNhbg1mb3JuaWExEjAQBgNVBAcTCVN1bm55dmFs
    ZTERMA8GA1UEChMISW5mb2Jsb3gxZDASBgNVBAwTC0VuZ2luZWVyaW5nMRkwFwYD
    VQQDExB3d3cuaw5mb2Jsb3guY29tMB4XDTE2MTAyNTE4MTAyMVoXDTE3MTAyNTE4
    MTAyMVowejELMAkGA1UEBhMCMVVMxEzARBgNVBAGTCkNhbg1mb3JuaWExEjAQBgNV
    BAcTCVN1bm55dmFsZTERMA8GA1UEChMISW5mb2Jsb3gxZDASBgNVBAwTC0VuZ2lu
    ZWVyaW5nMRkwFwYDVQQDExB3d3cuaw5mb2Jsb3guY29tMIIBIjANBgkqhkiG9w0B
    AQEFAAOCAQ8AMIIBCgKCAQEAA1uUc8C10gRs5EtzWykkuu4rZ57u5E2cmWwVI8XBM
    64azvQw6W5mJ9FPcK61Pmzii3EXX6WfyDSRT1BVX05EiCQmx3vBoqtQAnGwo7Ldl
    xYRZ6ljovTDbBi++szTwRXcm001FADt4DCS2LqSki0Rh9XKyNTA9KHQNSAbI93BK
    c91r0Po13p6+PrnoLkLDZTdKYCthIqcJ4hUa73EVxzMkUP1z6UCta1y08jVqkZ2H
    YZS90y3bbHYXRu8V0yaaBSg6+nXLPrHrY7xDALFoF0UFeFtBHstS4w5t5Dy0w7wq
    n5To52UAdwMeJ2gKf7TrUxfXbavOBnaUwRgmADAom7bAlwIDAQABMA0GCSqGSIb3
    DQEBBQUAA4IBAQDFNYA6zbmsY1JSYDJv0dlldYJli7XtPexZnceyF6yy1HKvf6zb
    Ph6/BDfAwMPaFSCSDISLt3efwnWNjVPazoN3o9XL+wrnTKShS6bxbqC7GytBB/ge
    WeKJKhAwPlsAiBI/ePd9JxIuGyG1vWJx6TlUUN1I4x+Hg6HEILAqAAuaQgmWsbJH
    V5IAUNquodp7H7hVo1wwagA6DrayasJG15/6xtpjlhsuGswY6uBU7+ewbtK9wGL6
    YOaYosoGzBrE5j1M9BIMAY3p7krk33tKKjiymXOM2PMnQlEanyUDR63v4FrUJue7
    zApS0yNyIq9izrhn7UMCXyqurKvJKUQEV9ga
    -----END CERTIFICATE-----
```

Obtaining the Certificate

The certificate used here is the 'GUI' certificate for your Grid Master and is used to authenticate the connection when your appliance establishes its connection to it. To obtain the certificate, you can use a web browser or a command such as:

```
openssl s_client -showcerts -connect <GM IP>:443
```

When obtaining this certificate, you may find that multiple certificates are returned. The certificate chain details will list the name for the appliance the certificate is from and which can be used to help identify the correct certificate to use. The actual certificate string will be enclosed between the lines "**-----BEGIN CERTIFICATE-----**" and "**-----END CERTIFICATE-----**".

Important: These lines are part of the certificate.

Here is an example demonstrating this output, with the certificate portion highlighted in yellow:


```

certificate: |
-----BEGIN CERTIFICATE-----
MIIDdzCCA18CEGE5IRHoUY/vgTjrYH6ftn8wDQYJKoZIhvcNAQEFBQAwejELMAkG
A1UEBhMCVVMxEzARBgNVBAgTCkNhbmG1mb3JuaWExEjAQBgNVBAcTCVN1bm55dmFs
ZTERMA8GA1UEChMISW5mb2Jsb3gxZDASBgNVBA5TC0VuZ21uZWVyaW5nMRkwFwYD
VQQDEXB3d3cuaW5mb2Jsb3guY29tMB4XDTE2MTAyNTE4MTAyMVoXDTE3MTAyNTE4
MTAyMVowejELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbmG1mb3JuaWExEjAQBgNV
BACTCVN1bm55dmFsZTERMA8GA1UEChMISW5mb2Jsb3gxZDASBgNVBA5TC0VuZ21u
ZWVyaW5nMRkwFwYDVQQDEXB3d3cuaW5mb2Jsb3guY29tMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEA1uUc8C10gRs5EtzwYkkuu4rZ57u5E2cmWwVI8XBM
64azvQw6W5mJ9FPcK61Pmzii3EXX6WfyDSRT1BVX05EiCQmx3vBoqtQAnGwo7Ldl
xYRZ61jovTDbBi++szTwRXCm001FADt4DCS2LqSki0Rh9XKyNTA9KHQNSAbI93BK
c91roPo13p6+PrnoLkLDZTdKYCthIqcJ4hUa73EVxzMkUP1z6UCta1y08jVvkqZ2H
YZS90y3bbHYXRu8VOyaaBSg6+nXLPrHrY7xDAlFoF0UFeFtBHstS4w5t5DyOw7wq
n5To52UAdwMeJ2gKf7TrUxfXbavOBnaUwRgmADAom7bAlwIDAQABMA0GCSqGSIb3
DQEBBQUAA4IBAQDFNYA6zBmsY1J5YD3v0d1ldYJ1i7XtPexZnceyF6yy1HKvf6zb
Ph6/BDFAwMPaF5CSDISL3efwnWNjVPazoN3o9XL+wrnTKSh56bxbqC7GytBB/ge
WeKJkhAwPlsAiBI/ePd9JxIuGyG1vWJx6TlUUN1I4x+Hg6HEILaQAuaQgmWsbJH
V5IAUNquodp7H7hVo1wwagA6DruyasJG15/6xtpj1hsuGswY6uBU7+ewbtK9wGL6
Y0aYosoGzBrE5j1M9BIMAY3p7krk33tKKjiymXOM2PMnQ1EanyUDR63v4FrUJue7
zApS0yNyIq9izrhn7UMCXyqurKvJKUQEV9ga
-----END CERTIFICATE-----

```

Obtaining the Token

The token, or 'permission token', is a temporary token which is used only one time and will expire within a short time frame (has a maximum of 60 minutes' validity) if not used. When doing elastic scaling, you can use a Grid member configuration which has been saved previously, or automate this provisioning via the API upon instance creation. For security reasons, the token used during the join process must be generated during the time frame that the appliance will be attempting to join the Grid Master.

This token can be generating in the NIOS GUI but generally, this would be done with automation via the API. The following examples demonstrate cURL commands which can be used to generate and read the token, along with sample output.

Create Permission Token for a Pre-Provisioned Grid Member:

```

curl -k -u admin:infoblox -X POST
https://10.60.27.240/wapi/v2.7/member/b251LnZpcnR1YWxfbm9kZSsxOjA:autoscale.
example.local?_function=create_token

```

This demonstrates the example for this command:

```

{
  "pnode_tokens": [
    {
      "physical_oid": "18",
      "token": "5rdfSs1onZdUVLWopO2S4mlz1tmK0Sfp",
      "token_exp_date": 1505330636
    }
  ]
}

```

Get the Permission Token for a Pre-Provisioned Grid Member:

```
curl -k -u admin:infoblox -X POST
https://10.60.27.240/wapi/v2.7/member/b251LnZpcnR1YWxfbm9kZSQx0A:autos
cale.example.local?_function=read_token
```

As with the command which creates the token, the read_token command will provide similar output:

```
{
  "pnode_tokens": [
    {
      "physical_oid": "18",
      "token": "LhkFSVR2PLPYSikALdKFSIM8FWEF9sNR",
      "token_exp_date": 1505330314
    }
  ]
}
```

Note: Refer to the Infoblox WAPI Reference Guide for more details on these and other available commands.