APPLICATION NOTE

Deploy your own Hawkeye Management System in AWS EC2

Version: Hawkeye 6.0.x

Need to know

You must have an Amazon AWS account with a valid payment in place (invoice/CC) to proceed.

License Pre-Requisite

For the purposes of this document, the assumption is that you already possess an activation code or that you have received a demo activation code from your Ixia account manager.

Hawkeye management public AMI list

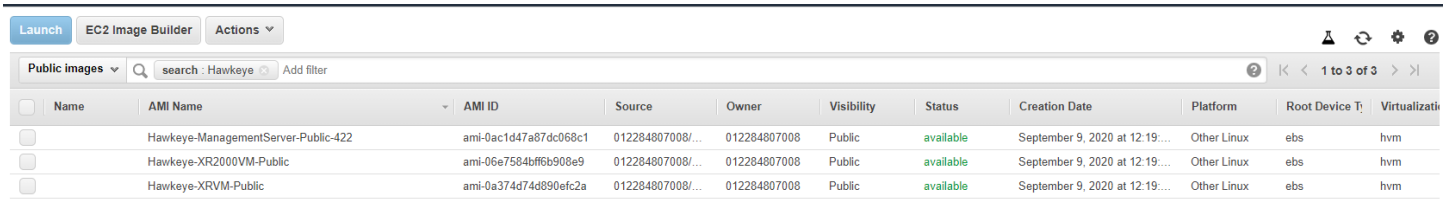
Following table lists the different public images available:

Region	Region name	AMI ID	AMI name
us-east-1	US East (N. Virginia)	ami-09d643e42df261dec	Hawkeye-ManagementServer-Public-6x
us-east-2	US East (Ohio)	ami-0c057112e5223ae96	Hawkeye-ManagementServer-Public-6x
us-west-1	US West (N. California)	ami-06f56a8f7b9bf1153	Hawkeye-ManagementServer-Public-6x
us-west-2	US West (Oregon)	ami-08525acbffe0c90f1	Hawkeye-ManagementServer-Public-6x
ca-central-1	Canada (Central)	ami-006cc8df1c3783c76	Hawkeye-ManagementServer-Public-6x
ap-southeast-2	Asia Pacific (Sydney)	ami-0c91bcb424c3df4e1	Hawkeye-ManagementServer-Public-6x
ap-northeast-2	Asia Pacific (Seoul)	ami-0eaa8d3e27080b354	Hawkeye-ManagementServer-Public-6x
ap-south-1	Asia Pacific (Mumbai)	ami-028aaa5f6dee094ad	Hawkeye-ManagementServer-Public-6x
eu-central-1	Europe (Frankfurt)	ami-0bf499eaf2d8167cf	Hawkeye-ManagementServer-Public-6x
eu-west-1	Europe (Ireland)	ami-07d2705582a312d63	Hawkeye-ManagementServer-Public-6x
eu-west-2	Europe (London)	ami-07c55ee923c0170b8	Hawkeye-ManagementServer-Public-6x
eu-west-3	Europe (Paris)	ami-043d39273e8dcfbb9	Hawkeye-ManagementServer-Public-6x
eu-north-1	Europe (Stockholm)	ami-0c4f47183c565a38b	Hawkeye-ManagementServer-Public-6x

Deploy AMI in your AWS

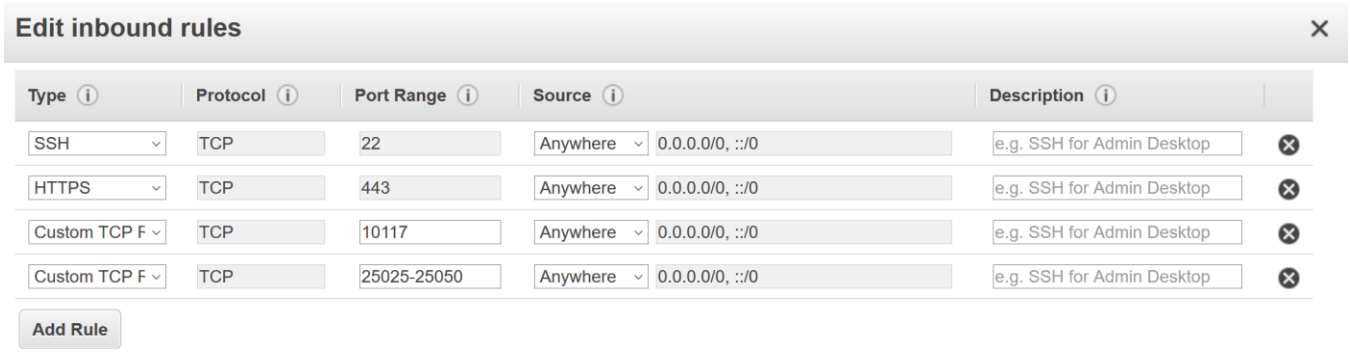
Select in AMI Region

1. Select your Region and pick **selected AMI** in public AMI.
   In EC2 AMI menu select public image and look for the corresponding Hawkeye



Launch Instance

2. Launch the **ami public** image and use the following as guidelines for sizing
   a) 1-10 user system → t2.large or t2.xlarge
   b) Network: Launch into VPC with public IP enabled
   c) Storage: Keep default at 256GiB (General Purpose SSD)
   d) Tag: (optional but highly recommended) purpose, date of launch, project code, etc.
   e) Security group: configure existing or new one with following requirements:



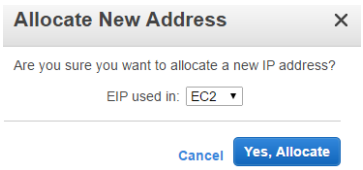
   i) Note: **DO NOT enable SSH inbound permanently**. The example above stats that ssh is opened from anywhere but it is highly recommended to restrict it from your originating IP address.

   f) "Review and Launch" will pose a Warning about SSH/Port-22 – you will need to select or create a key pair and continue.

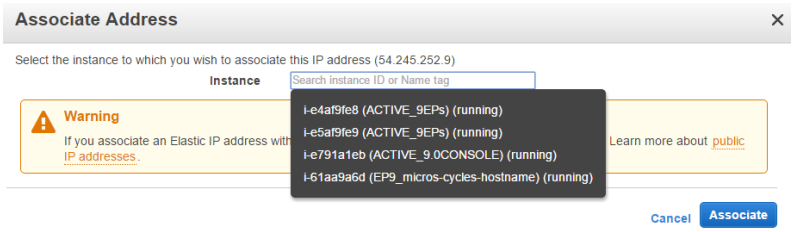
Add new Elastic IP to your instance (Optional but recommended)

First, why an elastic IP? Endpoints have a keep-alive to a registration service residing on the console, using a fixed IP means if the instance is shut down, you do not have to reconfigure any endpoints. Associate the same elastic IP to the new server's instance and endpoints will re-register automatically.

3. Make sure the Hawkeye Management server instance is **running**.
4. Go to Elastic IPs section. Allocate New IP address, pick the VPC

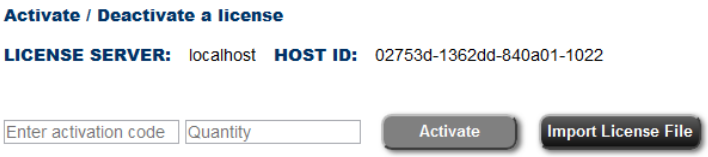


5. Select the new elastic IP and choose "Associate Address" option.
6. From the pop-up window, choose the recently launched instance



Next steps

7. Point your browser to the URL or the elastic IP of the instance. If you did not use elastic IP, find the instance's public IP and browse to it with https://(publicIP).
8. You will be presented with a page that states Licensing needs to be activated. Click this link. Enter the activation code that was provided by Ixia. This is a BYOL model.



9. Login as sysadmin/Password0 and immediately **change** the password.

10. For more detailed information on the Hawkeye server access, please refer the user guide and getting started guide in the product. Also, please refer the release notes for further information.

Note: **DO NOT enable SSH inbound permanently**. Note inbound SSH is disabled in the security group already. IF SSH access is required, limit to IP address you will access the server from and add to security for the duration of need and remove it after use.

Deploying XRVM AMI image

XRVM AMI image can be deployed in any supported regions and attached to the Hawkeye server. They can be used as public endpoints .

License Pre-Requisite

No license is needed for XRVM but you will need a Hawkeye server with public IP to attach to make use of it.

XRVM public AMI list

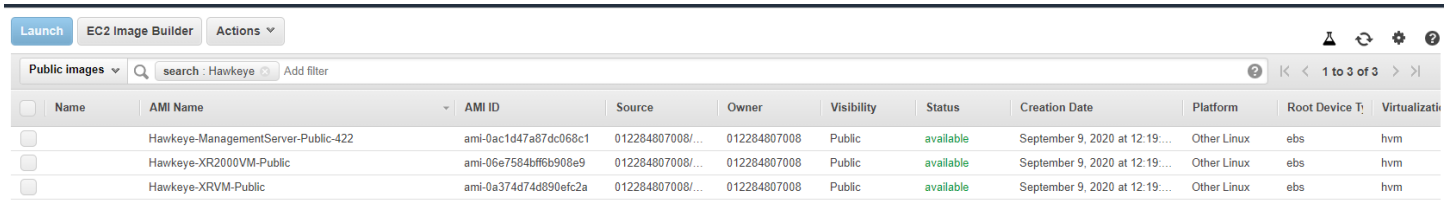
Following table lists the different public images available:

Region	Region name	AMI ID	AMI name

us-east-1	US East (N. Virginia)	ami-071f496b7b0ec5b80	Hawkeye-XRVM-Public-6x
us-east-2	US East (Ohio)	ami-0d51654b4ee019c3a	Hawkeye-XRVM-Public-6x
us-west-1	US West (N. California)	ami-0289cc5ebbbd62b78	Hawkeye-XRVM-Public-6x
us-west-2	US West (Oregon)	ami-0f788d2f0e860ed09	Hawkeye-XRVM-Public-6x
ca-central-1	Canada (Central)	ami-02fcbe02e1ae5e98d	Hawkeye-XRVM-Public-6x
ap-southeast-1	Asia Pacific (Singapore)	ami-0757237f4dae45430	Hawkeye-XRVM-Public-6x
ap-southeast-2	Asia Pacific (Sydney)	ami-00f351f33a6df1280	Hawkeye-XRVM-Public-6x
ap-northeast-2	Asia Pacific (Seoul)	ami-09a5a778e2884ffec	Hawkeye-XRVM-Public-6x
ap-south-1	Asia Pacific (Mumbai)	ami-0ff8a5850d55d913f	Hawkeye-XRVM-Public-6x
eu-central-1	Europe (Frankfurt)	ami-0905c93a846a1001f	Hawkeye-XRVM-Public-6x
eu-west-1	Europe (Ireland)	ami-04279bafd8d10798b	Hawkeye-XRVM-Public-6x
eu-west-2	Europe (London)	ami-08c876699992caa2e	Hawkeye-XRVM-Public-6x
eu-west-3	Europe (Paris)	ami-04c2ca459e4d96571	Hawkeye-XRVM-Public-6x
eu-north-1	Europe (Stockholm)	ami-097a8dc68bd01a4ab	Hawkeye-XRVM-Public-6x

Select in AMI Region

11. Select your Region and pick **selected AMI** in public AMI.
    In EC2 AMI menu select public image and look for the corresponding Hawkeye XRVM image



Launch Instance

1. Launch the **ami public** image and use the following as guidelines for sizing

   g) For low traffic t2.nano or t2.micro are sufficient. For bandwidth qualification tests t2.small or t2.medium are recommended

   h) Network: Launch into VPC with public IP enabled

   i) Storage: Keep default at 8GiB (General Purpose SSD)

   j) Tag: (optional but highly recommended) purpose, date of launch, project code, etc.

Security group: configure existing or new one with following requirements

For this the following security group needs to be configured:

Type	Protocol	Port range	Source
Custom TCP	TCP	10115 - 10116	0.0.0.0/0
SSH	TCP	22	80.149.122.40/29
SSH	TCP	22	54.89.32.11/32
Custom TCP	TCP	50000 - 60000	0.0.0.0/0
Custom UDP	UDP	10115 - 10116	0.0.0.0/0
Custom UDP	UDP	50000 - 60000	0.0.0.0/0

First set is for remote managements (ports 10115-10116) and second set is range of ports used for testing and need to be configured as well for a matching range into Hawkeye server under Traffic port management:

Review and Launch" will pose a Warning about SSH/Port-22 – you will need to select or create a key pair and continue.

To configure the XRVM, open ssh port in the security group temporarily, ssh with user ec2 and your key pair.

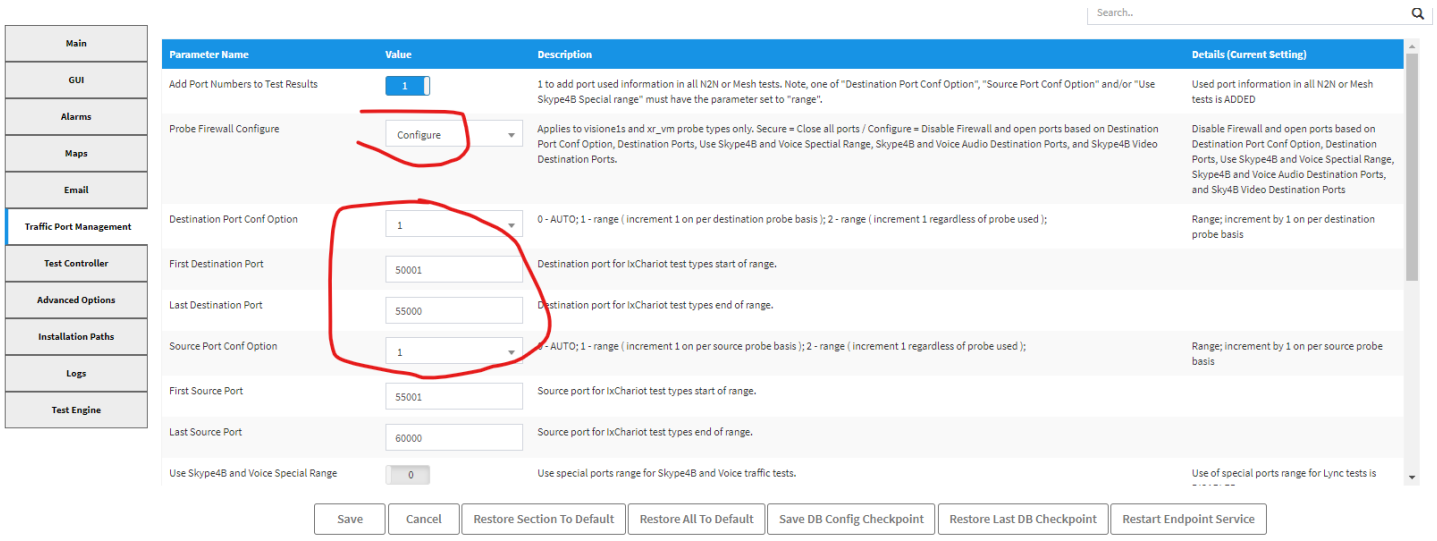
Before configuring XRVM for the first time make sure Hawkeye server is configured properly in preferences (see below)

After deployment, use your virtualization system's console solution to access the CLI.

The default login for XR-VM is username: ksuser and password: keysight , then run probeConfigure command that will prompt for probe name and Hawkeye server IP or URL.

Configuring Hawkeye server for running XRVM as public probes

The example below shows a matching configuration that will allow to use the settings as configured for the XRVM that you will find in Hawkeye sever :



Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

This information is subject to change without notice. © Keysight Technologies, 2019, Published in USA, Month XX, 2019, 5992-XXXEN