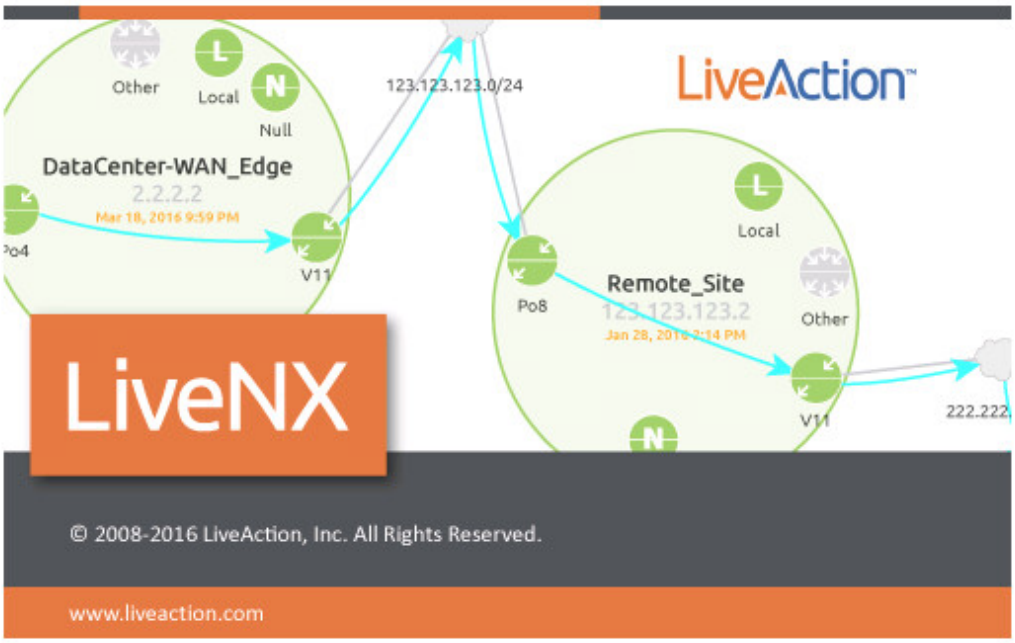
LiveNX AWS Cloud Monitoring

Summary

Product and Version	LiveNX 9.2.2
Affected Devices	LiveNX
Document Name	LiveNX AWS Cloud Monitoring Deployment Guide
Updated	LiveNX

This document serves the purpose of deploying LiveNX with Cloud-Monitoring in an AWS deployment.



If you have any questions about this guide, or need any assistance in general please contact LiveNX support: *support@liveaction.com*.

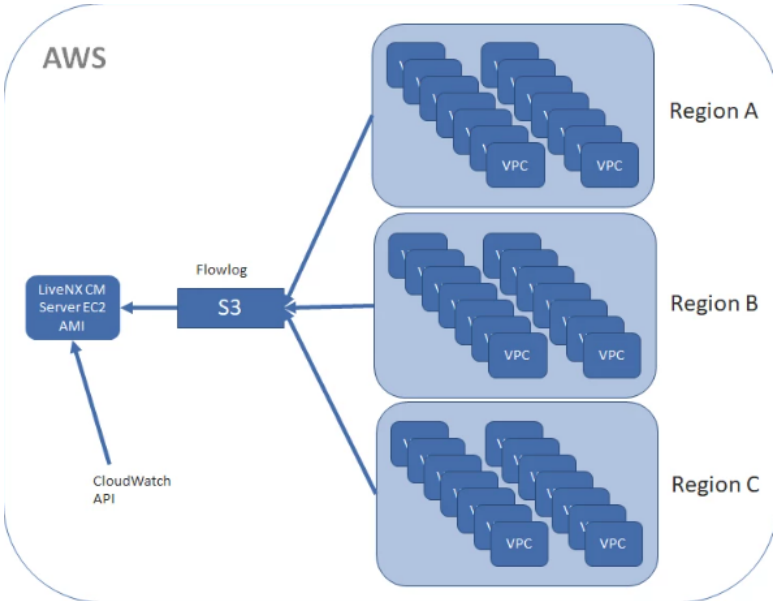
Overview

For deploying LiveNX cloud monitoring, these are the major conceptual components. This shows the LiveNX Server version, but it could also be a LiveNX node that can connect to a pre-existing LiveNX server as long as the version numbers are the same.

Major Components

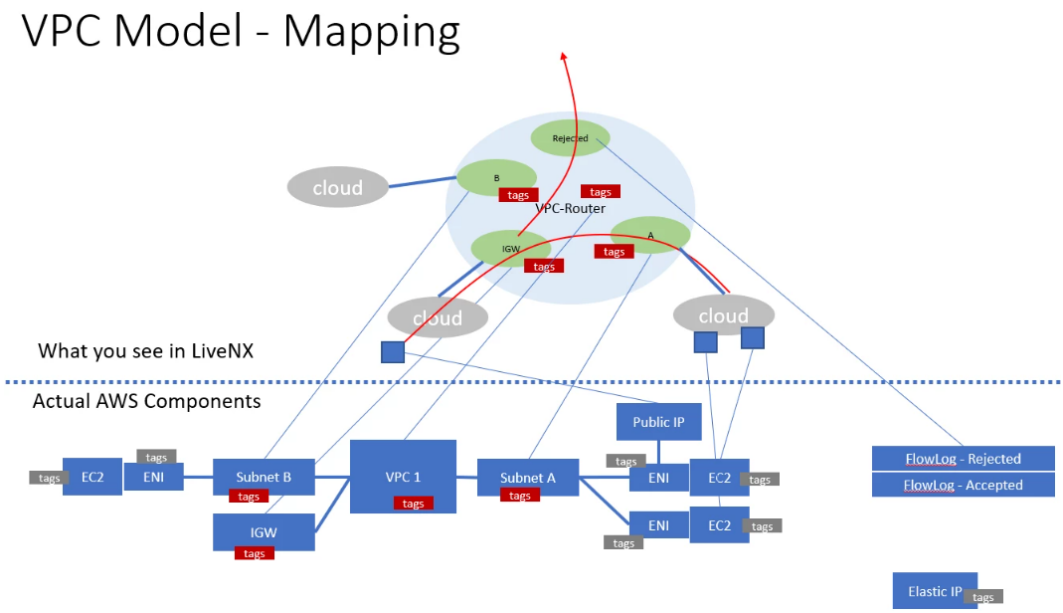
- Actual EC2 image based off the LiveNX CM AMI image.
- VPC and settings for it to export Flow Log into S3 storage bucket.

- Setup of the S3 storage bucket.
- LiveNX CM API calls to CloudWatch API to get the flowlogs from S3 and contextual info about the environment
- Security and permissions need to be setup so that LiveNX CM can call the API properly and have access to S3



AWS Modeling

In LiveNX the mapping of the customers AWS components is shown below. The VPC is modeled as a router with various interfaces connecting subnets to EC2 and AWS services. This model does have gaps in that AWS does not expose certain traffic through flowlog, for example Transit Gateways, Elastic Beanstalk etc.



Cost

The cost for deploying can be broken down into 3 components below. Other than the EC2 compute/store cost, the rest is very minimal if the LiveNX CM server lives in AWS and is

directly proportional to the amount of flowlogs collected. If the LiveNX CM node lives in AWS but talks to an on premises server, then there would be additional bandwidth costs for traffic exiting AWS but again, it would not be the raw flow as that would be stored local in the node.

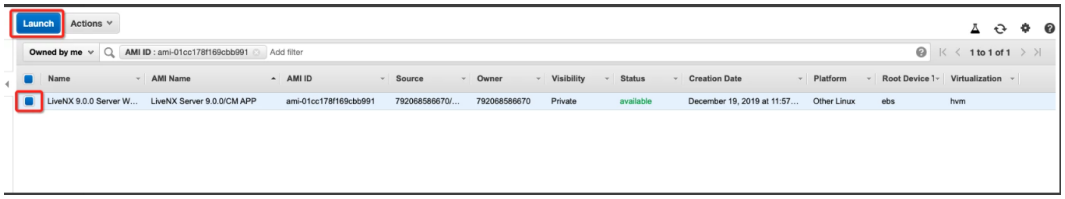
- EC2 costs to run LiveNX AMI
- S3 costs to temporarily store flowlog
- Note: this is very minimal since can be set to purge after 1 day
- CloudWatch API (Deliver Logs to S3 Cost)
- First 10TB $0.25 per GB
- Next 20TB $0.15 per GB
- Next 20TB $0.075 per GB
- Over 50TB $0.05 per GB
- Data Stored $0.03 per GB

Deploying AMI in AWS Cloud

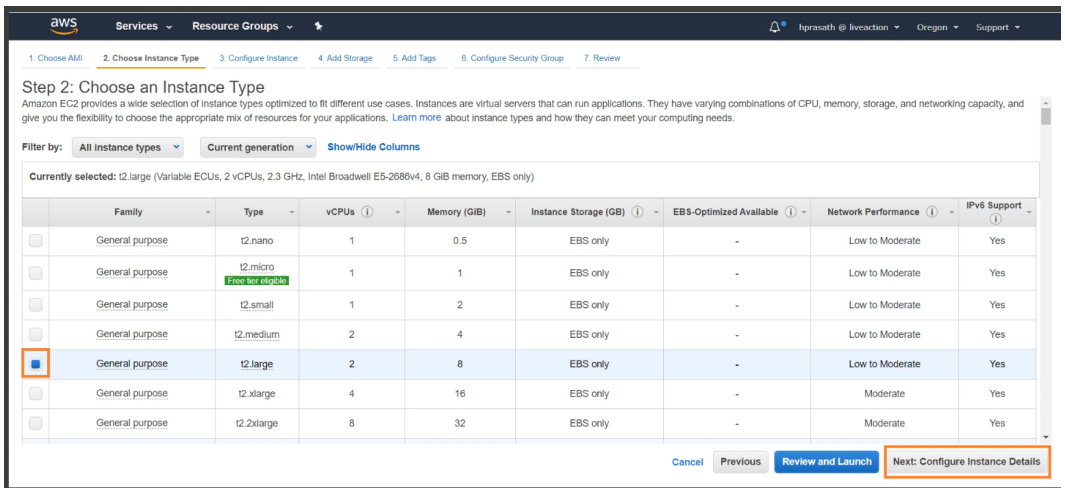
Contact the support/sales team to copy the latest AWS AMI with LiveNX-CM to your account-id. Once AMI is copied to the required region, we can deploy the same.

Deployment Steps

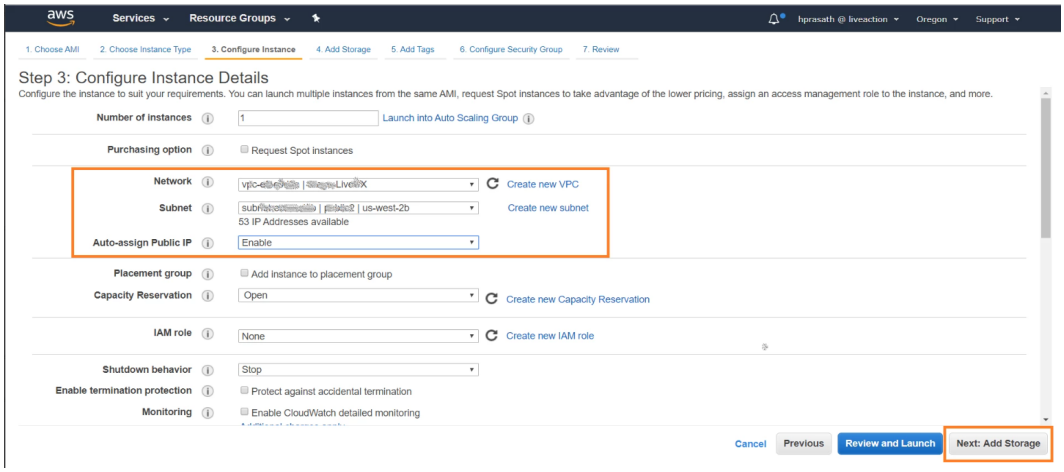
1. Login to AWS Console. Navigate to EC2 ? Images ? AMI and search with the provided `ami-id.



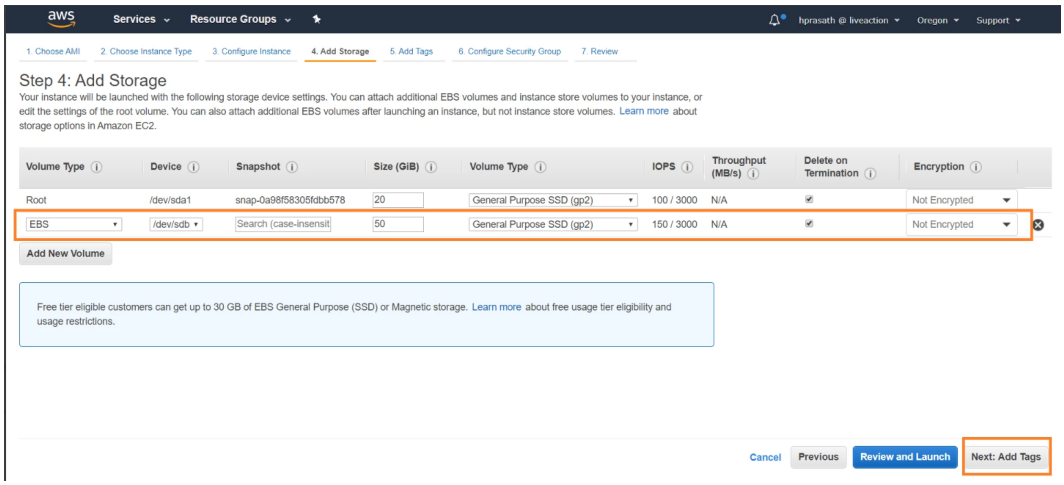
2. Select the instance type and click next.



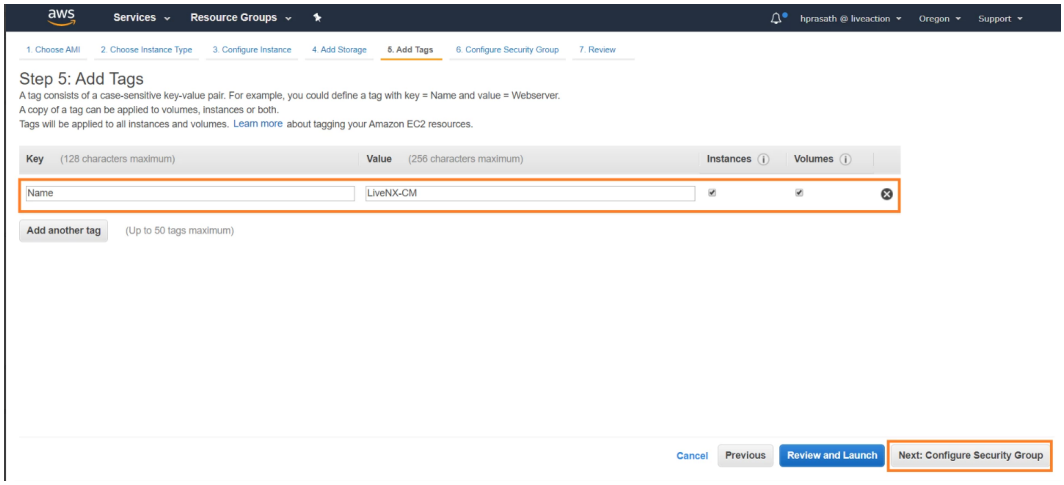
3. Select the VPC, Subnet, Public access and click next.



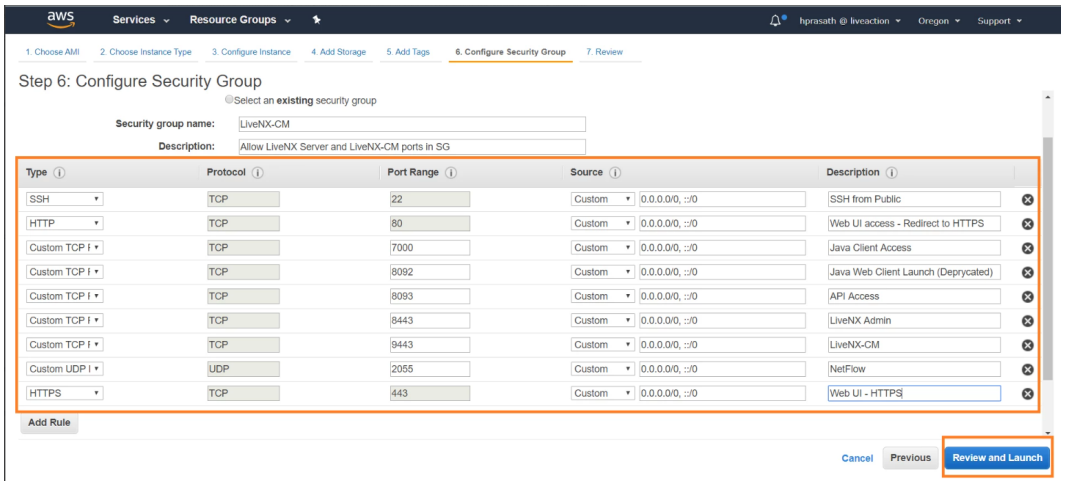
4. Modify the storage limit and Click next.

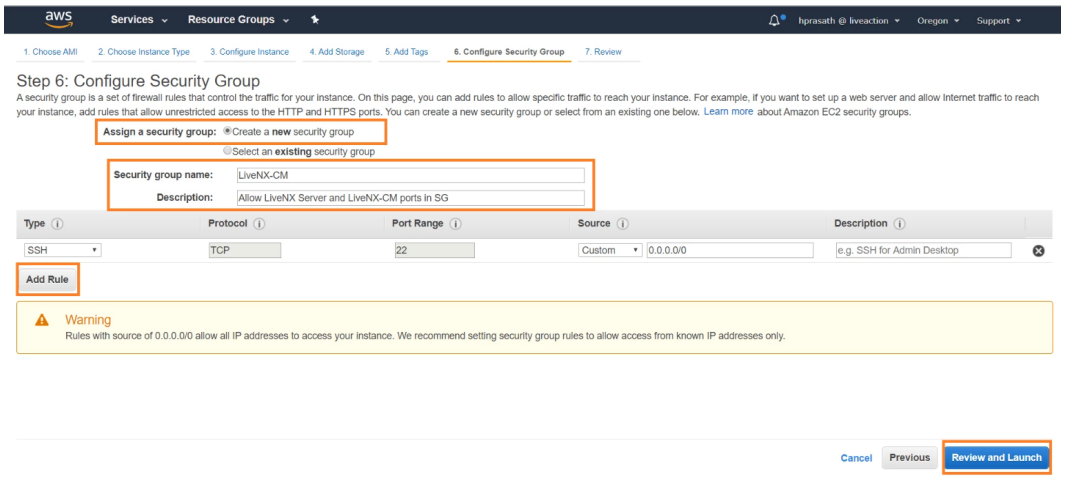


5. Add appropriate tags and Click next.



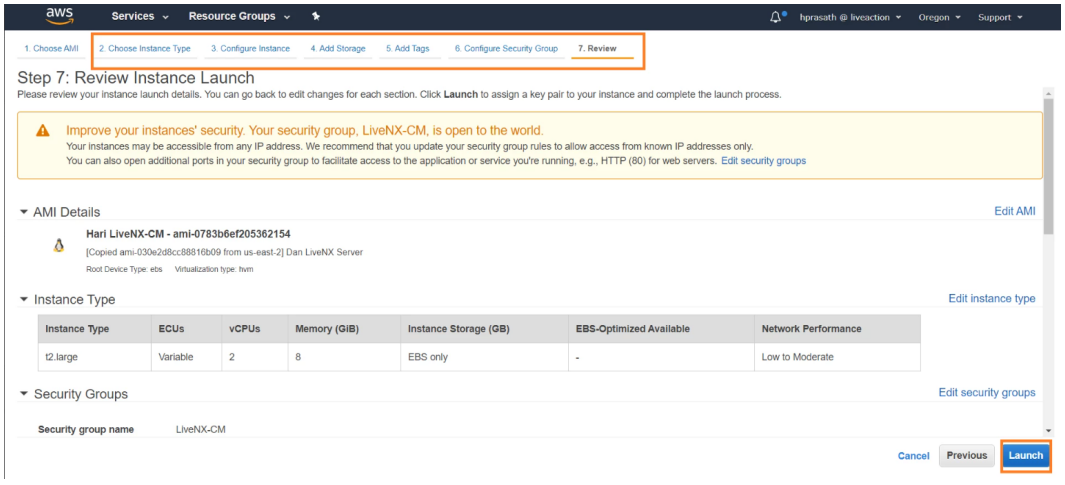
6. Add the required security group and then click review and launch.



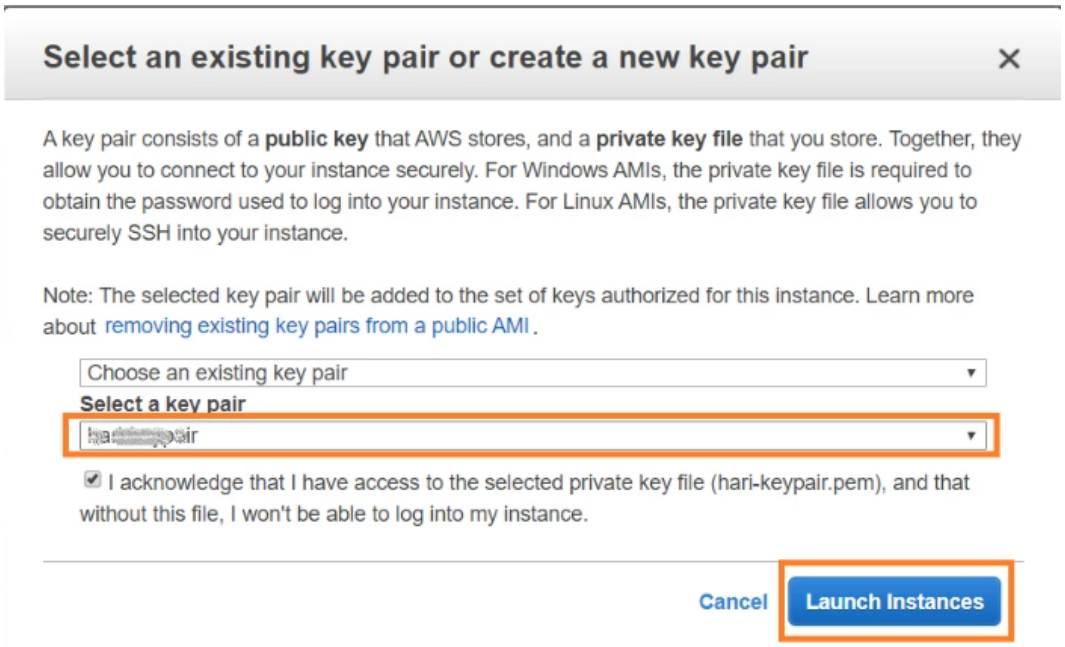


Note In documentation the ports are exposed to open world, harden the security group according to organization policy.

7. Navigate to previous tabs for modifying/Click on Launch.



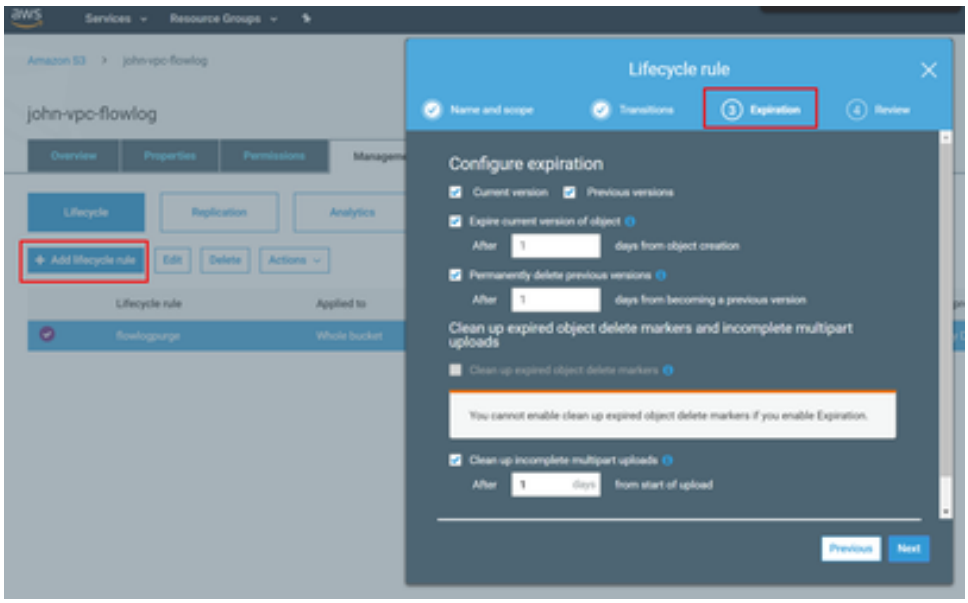
8. Select a key pair/add a new one to launch.



S3 Bucket Setup

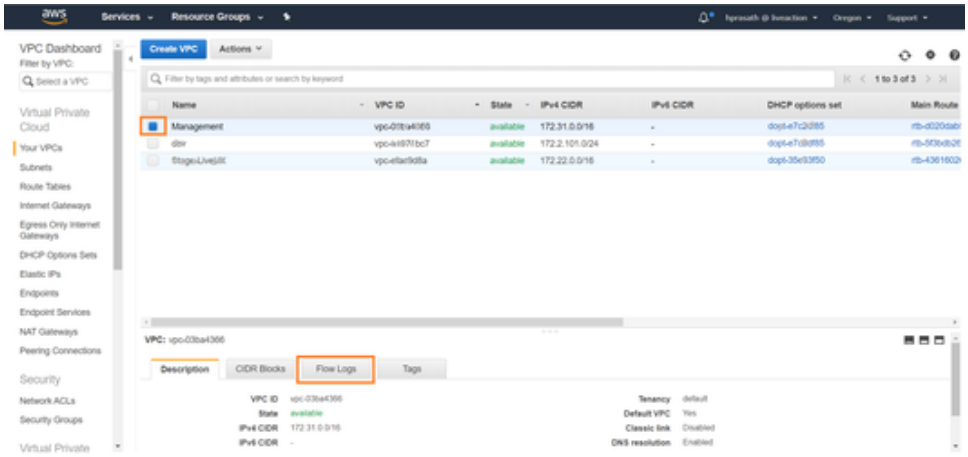
- We will be using flowlog stored in S3, if the customer already has it setup then simply reuse.
- Otherwise create an empty S3 bucket, AWS CloudWatch will automatically populate and create the folder hierarchy.
- Any S3 buckets with the proper permissions for LiveNX CM to have read access would work
- It is recommended to set the life cycle management on the S3 bucket so automatically purge as LiveNX CM polls, it is not necessary to keep the logs stored historically anymore.

Here is an example life cycle setting

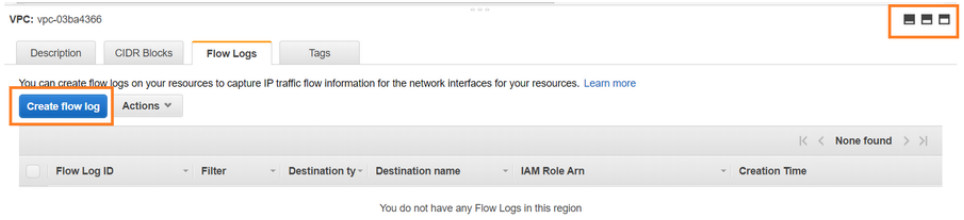


Enable AWS VPC Flow Log

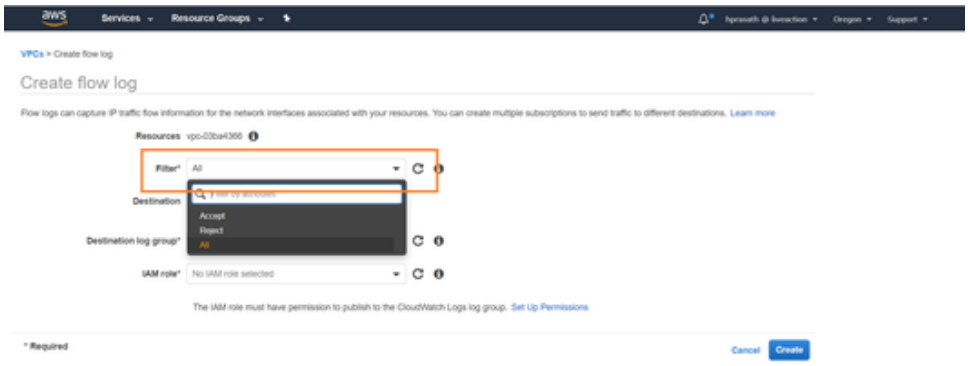
Go to AWS Console and navigate to VPC. Select the VPC and click on Flow Logs.



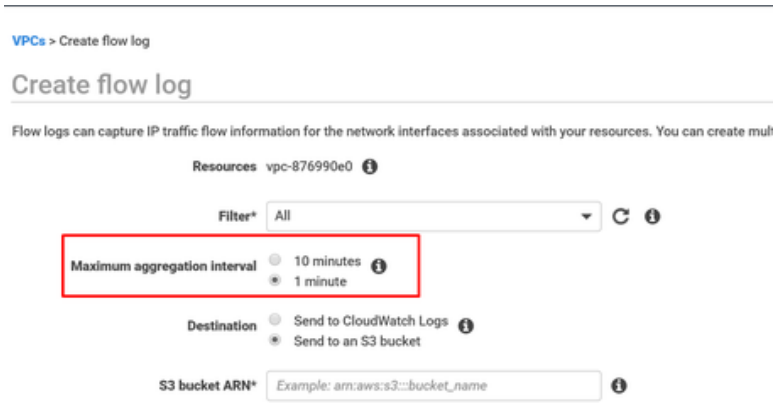
We can use the toggle buttons on the right to display different size screens. Click on 'Create flow log.'



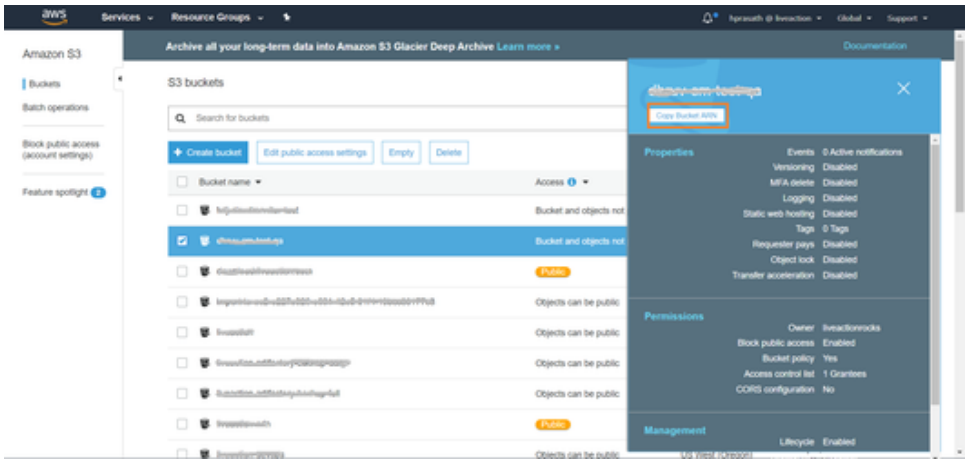
It will take us to Flow Log window. Select the filter 'All' in the dropdown.



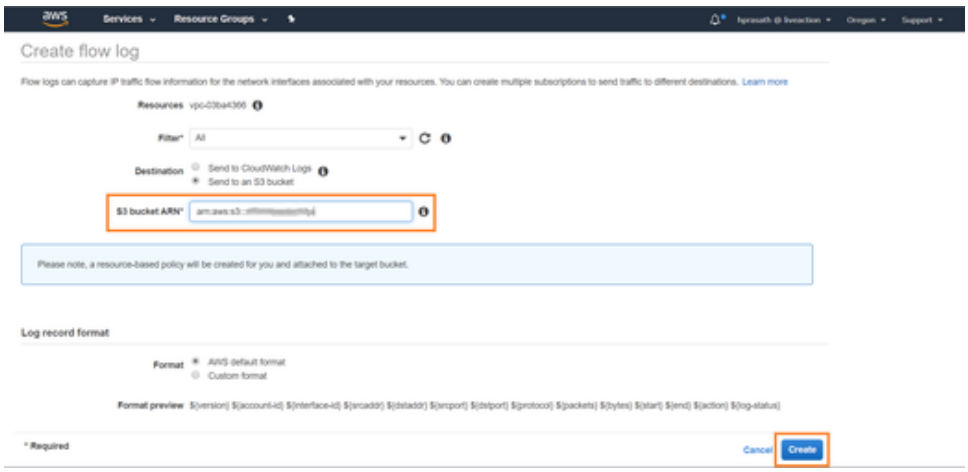
For Max Aggregation Interval:



Set it to 1 minute. So, each flow record would be aggregated for a 1-minute time interval, like time out setting in router NetFlow. But the records are written to S3 approximately every 5 minutes. And on interfaces attached to Nitro based EC2 instances, the maximum is always 1 minute even if a higher value is selected. For the Destination select 'Send to an S3 Bucket.' For bucket arn, open s3 in another tab and copy the ARN as below.



Paste the copied ARN value in the text box 'S3 bucket ARN*.'



On clicking 'Create,' AWS Flow logs will be sent to S3 bucket. We will now configure the LiveNX-CM to read from S3 bucket.

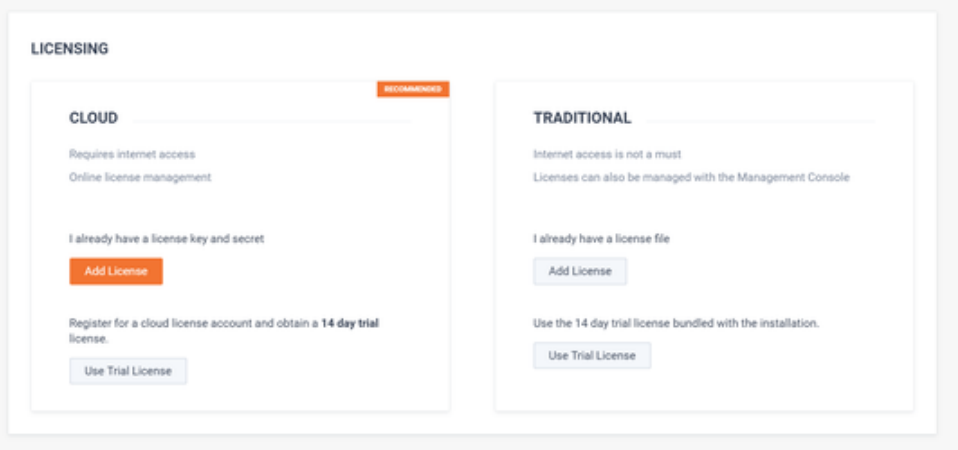
Setup LiveNX Server Instance

This step is required if the EC2 instance that was created is a LiveNX Server for Cloud Monitor. This is not required for a LiveNX Node for Cloud Monitoring instance that will connect to an existing LiveNX server.

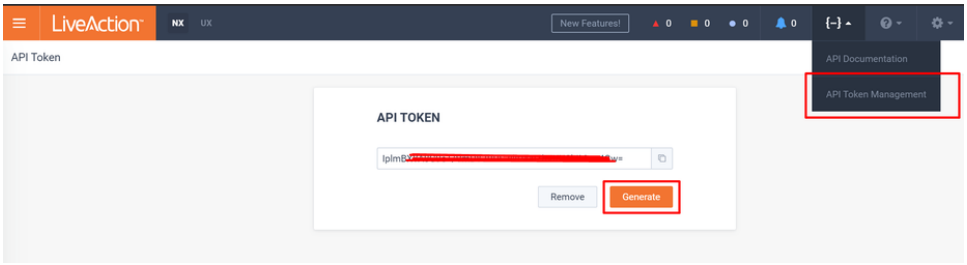
Navigate to https://<server-ip>

This will ask you to set a new password if you are setting up a LiveNX-CM Server. If setting up a LiveNX-CM Node, this is not necessary.

The default user and password is “admin”, “admin”, which will be prompted to be changed. Licensing may also need to be set up.



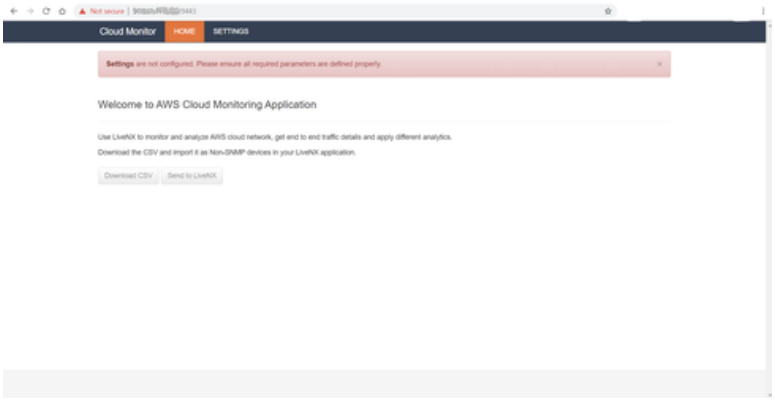
Create new API token, which will be needed in the CM setup screen.



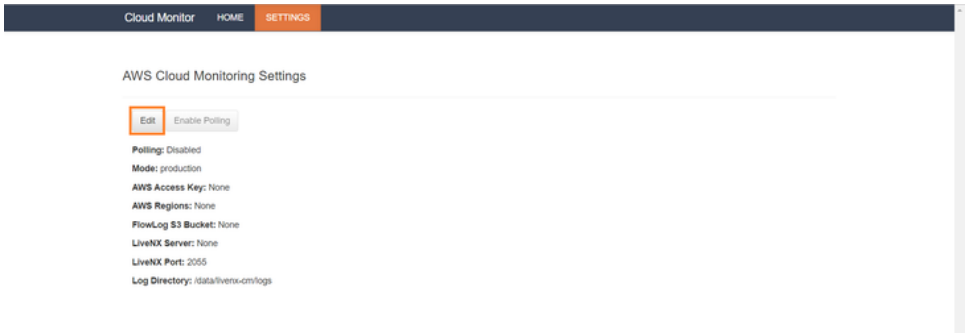
LiveNX-CM Cloud Monitoring Setup Page

Currently the settings for the CM portion is a separate page and not integrated with the main LiveNX UI.

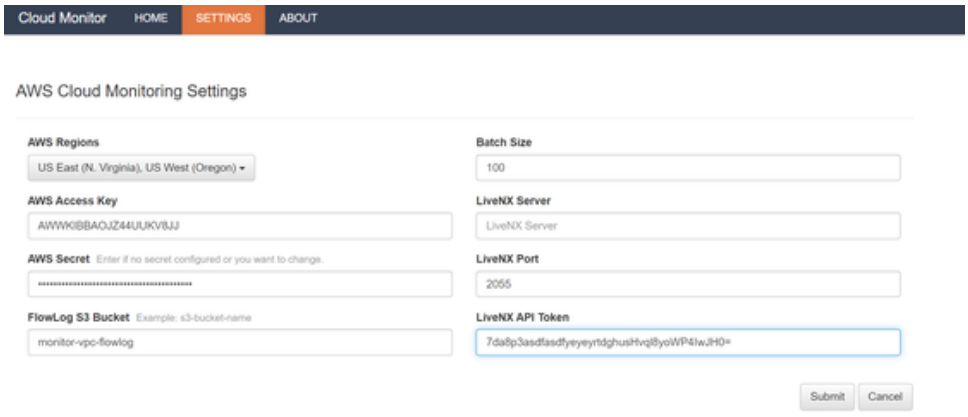
Navigate to https://<server-ip>:9443/.



Navigate to LiveNX-CM Settings and edit settings.



Provide the settings details described below for configuring the LiveNX-CM.



Note These are not real keys or tokens.

Settings Field Description

1. AWS Regions: Specify which regions should be monitored. CM will then query the VPC located in that region to poll. By default, none of the VPC information is obtained. Since there can be many VPC across various region, this can be used to select specific region.
2. AWS Access Key and Secret:
   - This is the AWS account access key and secret created by the AWS account owner
   - Access key will look like this “AWWKIBBAOJZ44UUKV8JJ”
   - Secret will look like this “B98j221XXrrrrrZli43ff23eZrrrrrrXG0Umiou4”
   - See for more details: https://docs.aws.amazon.com/general/latest/gr/aws-sec-cred-types.html#access-keys-and-secret-access-keys
3. FlowLog S3 Bucket:

   This should simply be the name "monitor-vpc-flowlog", not ARN. For example it should just be the portion in bold "arn:aws:s3:::**monitor-vpc-flowlog**"
4. Batch Size:

   This can be left as default, but this determines the size of each IPFIX record that is sent.
5. LiveNX Server:

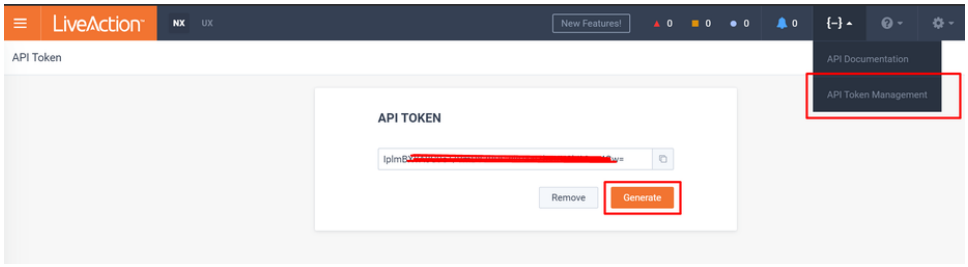
   Enter the IP address or DNS name of the server. Although the CM runs on the LiveNX server, it requires the IP address.

6. LiveNX Port:

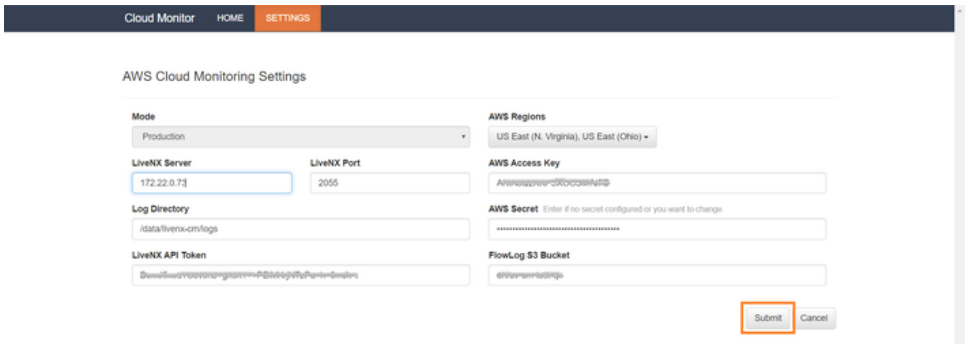
   This can be left as default 2055 if the NetFlow (IPFIX) port settings on LiveNX server was not modified. Otherwise this should be set to the NetFlow (IPFIX) port that LiveNX server was configured to listen for.

7. LiveNX API Token:

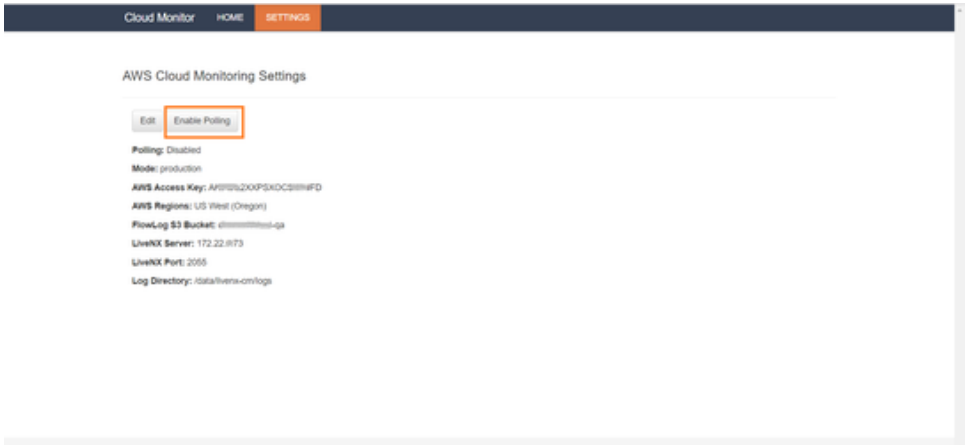
   This is gotten from the LiveNX server under "API Token Management", see below screen shot. If there is an existing token, that can be reused. If no token exists, then a new one can be generated by clicking the "Generate" button

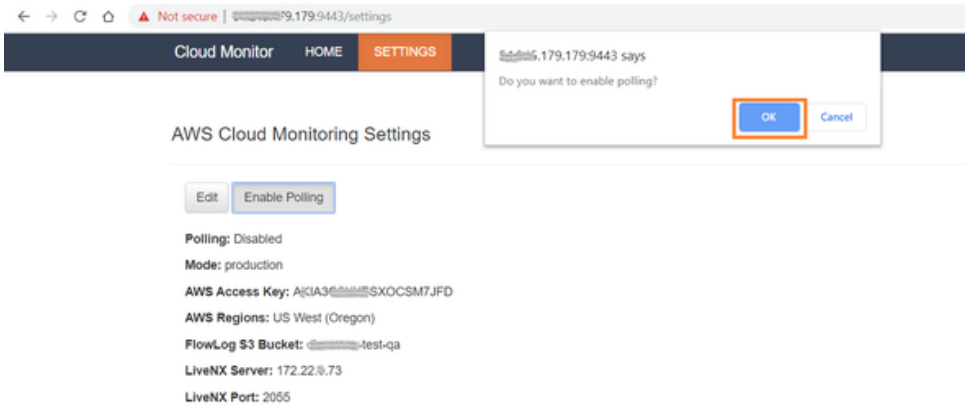


On submit, the configuration will be saved in LiveNX-CM.

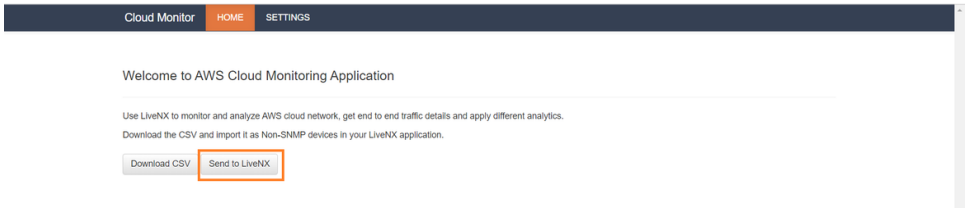


We must enable polling to start reading flow logs from S3. Once clicked it will ask to confirm.

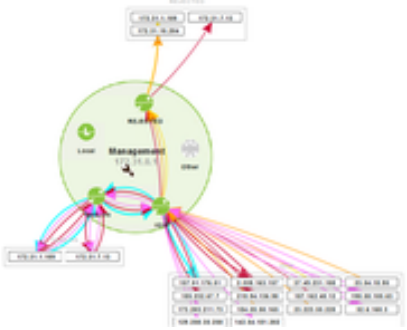




Once polling is enabled, navigate to Home page of LiveNX-CM. Wait for ~5 - 10 minutes, refresh manually and make sure 'Send to LiveNX' is enabled. If 'Send to LiveNX' is enabled, click the same. We have added the VPC as a virtual router in LiveNX.



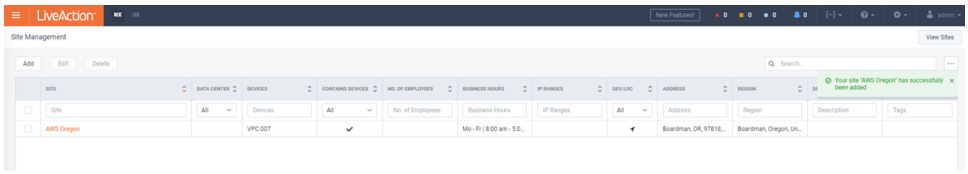
Login to LiveNX Client, we should be able to see the AWS flow log in the client. Mapped to the VPC.



Additional LiveNX Setup

Here are some optional setup steps in LiveNX to customize deployment:

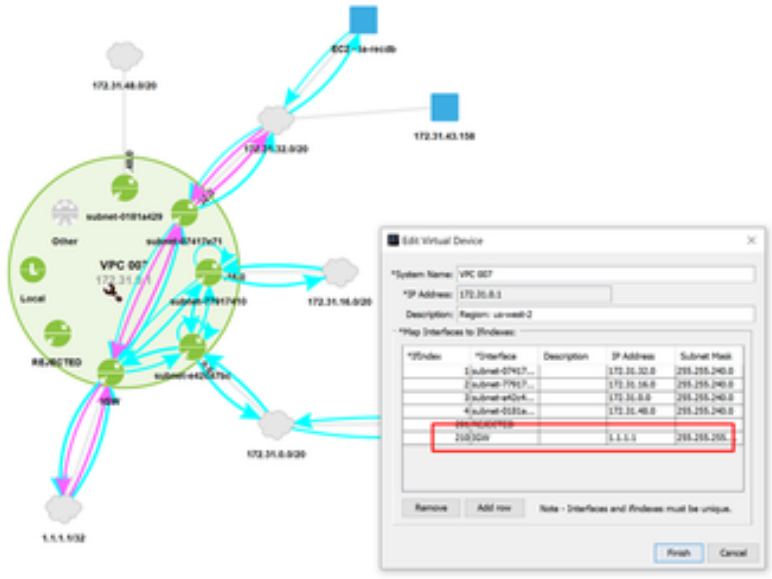
- Create sites that correspond to different regions that the VPC routers belong to.
    - Move the VPC routers into those sites, then site-based reporting and analysis will work.



- Make sure the WAN tag on the interfaces are setup properly on IGW.
- Make sure additional tags on the interfaces and VPC router are setup, they should have been automatically imported via csv or API.
- IP addresses and DNS:
  - The IP addresses shown are all internal IP addresses, so even if an EC2 may have an external IP, the flow log will show only the internal IP address.
  - Enable DNS in LiveNX and setting to show DNS names.
  - This will try to resolve IP addresses to DNS names. This is not incredibly useful since it does not resolve external IP addresses, and the internal DNS names are basically a little more descriptive IP addresses with AZ and some type information.

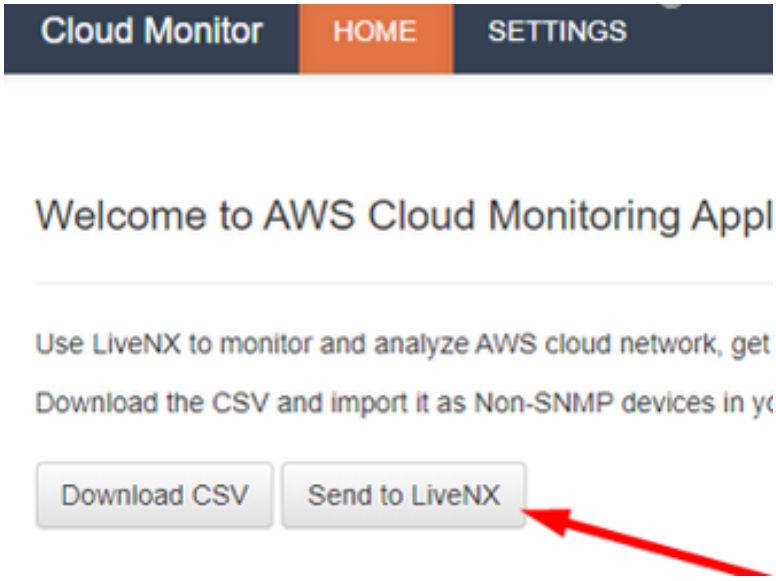
TCP	ip-172-31-2-234.us-west-2.compute.internal (172.31.2.234)	33710	52.218.160.10
TCP	ip-172-31-4-228.us-west-2.compute.internal (172.31.4.228)	443	208.70.172.62
TCP	ip-172-31-4-228.us-west-2.compute.internal (172.31.4.228)	443	208.70.172.62
TCP	174.47.77.142	55393	ip-172-31-21-27.us-west-2.compute.internal (172.31.21.27)
TCP	ip-172-31-2-234.us-west-2.compute.internal (172.31.2.234)	80	ip-172-31-4-228.us-west-2.compute.internal (172.31.4.228)
TCP	ip-172-31-2-234.us-west-2.compute.internal (172.31.2.234)	80	ip-172-31-4-228.us-west-2.compute.internal (172.31.4.228)
TCP	ip-172-31-2-234.us-west-2.compute.internal (172.31.2.234)	80	ip-172-31-4-228.us-west-2.compute.internal (172.31.4.228)

- Creating a subnet cloud for IGW:
  - As of LiveNX 9.0, we do not create a subnet cloud for the IGW interface, but a customer can manually add one by editing interfaces for the device.
  - Since the device is non-SNMP it is basically editing a table.
  - Since IGW is just a gateway, it really does not have a subnet, but for viewing purposes in topology view it makes it a bit easier at times to see the flows exiting.
  - Below is an example of assigning a place holder IP 1.1.1.1/32.

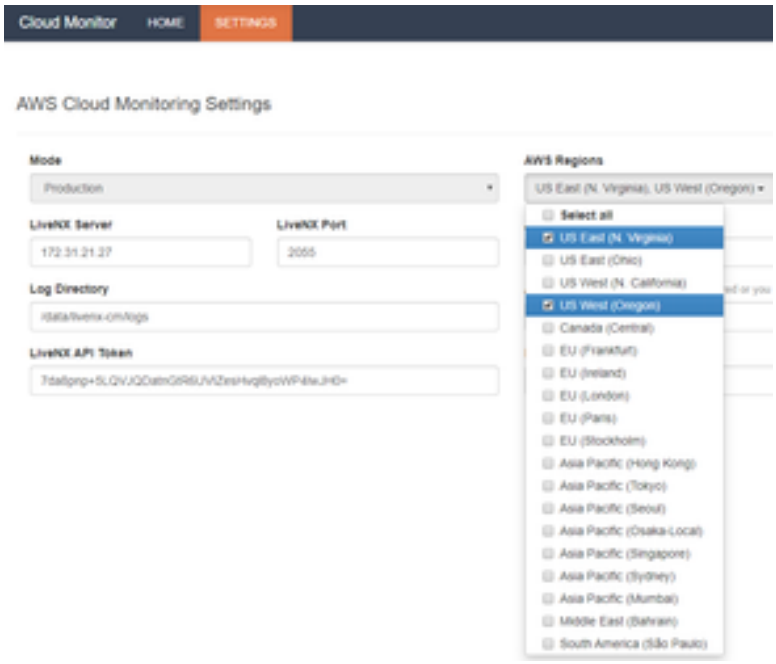


- Refreshing VPC information:
  - AWS networking environment is very dynamic and can change often.

- Currently, to refresh the information is going through the same initial import and or “Send to LiveNX” process.
- Be cautious since this process may overwrite any customer entered tags, interfaces, and new CIDR info.



- Adding new region:
  - If adding new region after setup, need to go back to settings to include the region to poll



Troubleshooting

AWS Permission

- EC2 Access
- VPC Access
- CloudWatch Logs

IAM Roles

1. AmazonVPCFullAccess
2. AmazonS3FullAccess
3. AmazonEC2FullAccess
4. CloudWatchFullAccess
5. In-line policy (AllowCloudWatchLogs)

```
{
    “Version”: “2012-10-17”,
    “Statement”: [
    {
        “Effect”: “Allow”,
        “Action”: [
        “logs:CreateLogDelivery”,
        “logs:DeleteLogDelivery”
    ],
    “Resource”: “*”
    }
  ]
}
```

Sample AWS Design – LiveNX Cloud Deployment (Draft)