Nubeva TLS Decrypt Using Open-Source Security Tools

Quick Start Reference Deployment

February 2020
(last update: March 2020)

Erik Freeland, Nubeva
Dylan Owen and Roy Rodan, Amazon Web Services

Visit our GitHub repository for source files and to post feedback, report bugs, or submit feature ideas for this Quick Start.

Contents

This Quick Start was created by Nubeva in collaboration with Amazon Web Services (AWS).

Quick Starts are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices.

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying an out-of-band, open-source monitoring stack for AWS. Launched tools come with the Nubeva Transport Layer Security (TLS) Decrypt platform pre-configured on the AWS Cloud. The stack includes the open-source tools Moloch, Ntopng, Suricata, Wireshark, and Zeek.

- **Moloch** is a large-scale, open-source, indexed packet-capture-and-search system.
- **Ntopng** is a free, open-source packet analyzer and flow collection tool.
- **Suricata** is a high-performance engine that comprises a network intrusion detection system (IDS), an intrusion prevention system (IPS), and network security monitoring (NSM).
- **Wireshark** is a free, open-source packet analyzer for network troubleshooting.
- **Zeek** is a powerful network analysis framework used for intrusion detection by looking at anomalous network activity to find suspicious data flows.

This Quick Start is for users who want to identify malicious activity, insider threats, and data leakage within their virtual private cloud (VPC) and Amazon Elastic Compute Cloud (Amazon EC2) instances with decrypted visibility.

Nubeva on AWS

Nubeva's TLS visibility solution is a software as a service (SaaS) that provides complete packet visibility of any public cloud with TLS decryption capabilities. All the open-source tools in this solution are complemented by Nubeva TLS Decrypt, which provides additional intelligence and insight into encrypted data.

Container-based Nubeva TLS Decrypt sensors are deployed on your monitored instances, which capture TLS session keys—as well as associated packet traffic for any instance where Amazon VPC traffic mirroring isn't available—as they flow through these instances. The packets are sent through a secure channel to be analyzed and visualized by the open-source tools you choose. This provides clear visibility of your network traffic so you can identify unexpected network behavior, perform network analysis, and detect intrusions.

Cost and licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will use. Prices are subject to change.

> **Tip**: After you deploy the Quick Start, we recommend that you enable the AWS Cost and Usage Report. This report delivers billing metrics to an Amazon Simple Storage Service (Amazon S3) bucket in your account. It provides cost estimates based on usage throughout each month and finalizes the data at the end of the month. For more information about the report, see the AWS documentation.

This Quick Start requires an account on the Nubeva SaaS console, as described in the Deployment Steps, later in this guide.

Architecture

Deploying this Quick Start for a new VPC with **default parameters** builds the following Nubeva network and security monitoring environment in the AWS Cloud.

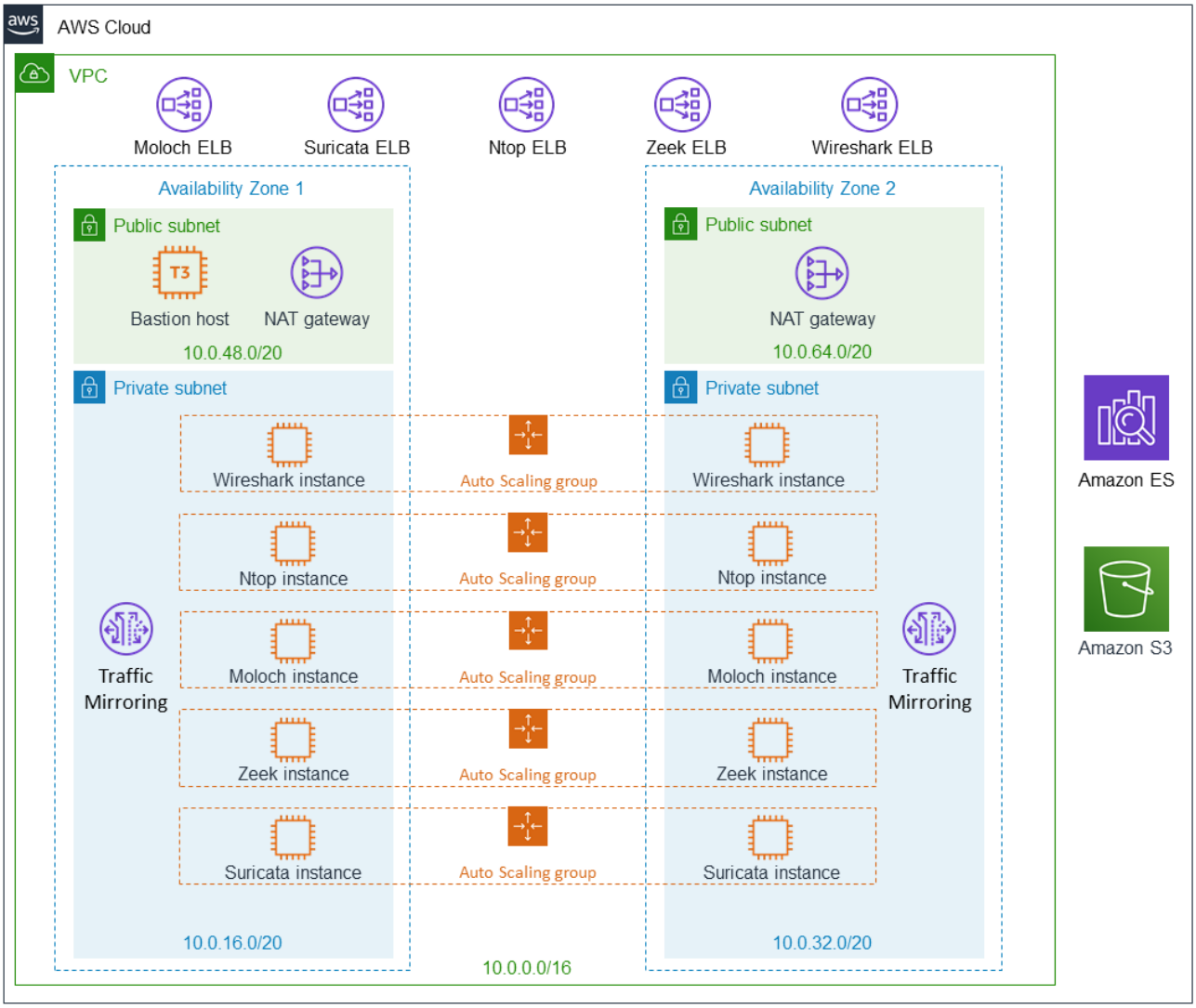


Figure 1: Quick Start architecture for Nubeva TLS Decrypt and open-source tools on AWS

The Quick Start sets up the following:

- A highly available architecture that spans two Availability Zones.*
- A VPC configured with public and private subnets, according to AWS best practices, to provide you with your own virtual network on AWS.*

- Elastic Load Balancing (ELB) for each open-source tool, to provide scaling for the tool operation itself and for inbound packet mirroring using Amazon VPC traffic mirrors or internal replication.
- Amazon Elasticsearch Service (Amazon ES) for the open-source tools that require Elasticsearch, Moloch, or for managing the logs from Zeek and Suricata.
- An Amazon S3 bucket for Moloch packet capture (PCAP) storage.
- Amazon VPC traffic mirroring targets connected to each open-source load balancer.
- In the public subnets:
  - Managed network address translation (NAT) gateways to allow outbound internet access for resources in the subnets.*
  - Bastion host for all inbound connectivity.*
- In the private subnets:
  - A source instance in an Auto Scaling group (of size 2). This is a sample instance you can use to monitor TLS traffic. After deployment, use the Nubeva SaaS console to add more instances to monitor.
  - The source instance has a container-based Nubeva TLS Decrypt agent deployed. This agent listens through all available interfaces, discovers TLS session keys, and, optionally, mirrors a copy of the packet stream to the open-source tools for analysis.
  - Moloch packet capture in an Auto Scaling group (of size 2).
  - Ntop network analysis in an Auto Scaling group (of size 2).
  - Suricata signature detection in an Auto Scaling group (of size 2).
  - Wireshark packet analysis in an Auto Scaling group (of size 2).
  - Zeek anomaly detection in an Auto Scaling group (of size 2).

* The template that deploys the Quick Start into an existing VPC skips this task and prompts you for your existing VPC configuration.

Planning the deployment

Technical Requirements

This Quick Start requires a free account from Nubeva.

Specialized Knowledge

Before you deploy this Quick Start, we recommend that you become familiar with the following AWS services. If you are new to AWS, see Getting Started with AWS.

- Amazon EC2
- Amazon VPC
- AWS CloudFormation

Deployment options

This Quick Start provides two deployment options:

- **Deploy Nubeva and open-source tools into a new VPC** (end-to-end deployment). This option builds a new AWS VPC, which contains subnets, NAT gateways, security groups, and other infrastructure components. It then deploys Nubeva and all the open-source tools into this new VPC.
- **Deploy Nubeva and open-source tools into an existing VPC**. This option provisions Nubeva and all the open-source tools in your existing AWS infrastructure.

The Quick Start provides separate templates for these options. It also lets you configure Classless Inter-Domain Routing (CIDR) blocks and settings for the source and tool instances, as discussed later in this guide.

Deployment steps

Step 1. Prepare your AWS account

1. If you don't already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions.
2. Use the Region selector in the navigation bar to choose the AWS Region where you want to deploy your security tools.
3. Create a key pair in your preferred Region.
4. If necessary, request service quota increases for the following resources. You might need to do this if an existing deployment uses these resources, and you might exceed the

default quotas with this deployment. The Service Quotas console displays your usage and quotas for some aspects of some services. For more information, see the AWS documentation.

5. Because this Quick Start uses Amazon ES, a service-linked role is required. If you do not already have one, see Creating a Service-Linked Role.

Step 2. Prepare your Nubeva account

1. Navigate to www.nubeva.com, and choose **Login** from the main menu.
2. First-time users are prompted to create an account. You can use one of the OAuth partners to log in.
3. Copy in the Nubeva token.

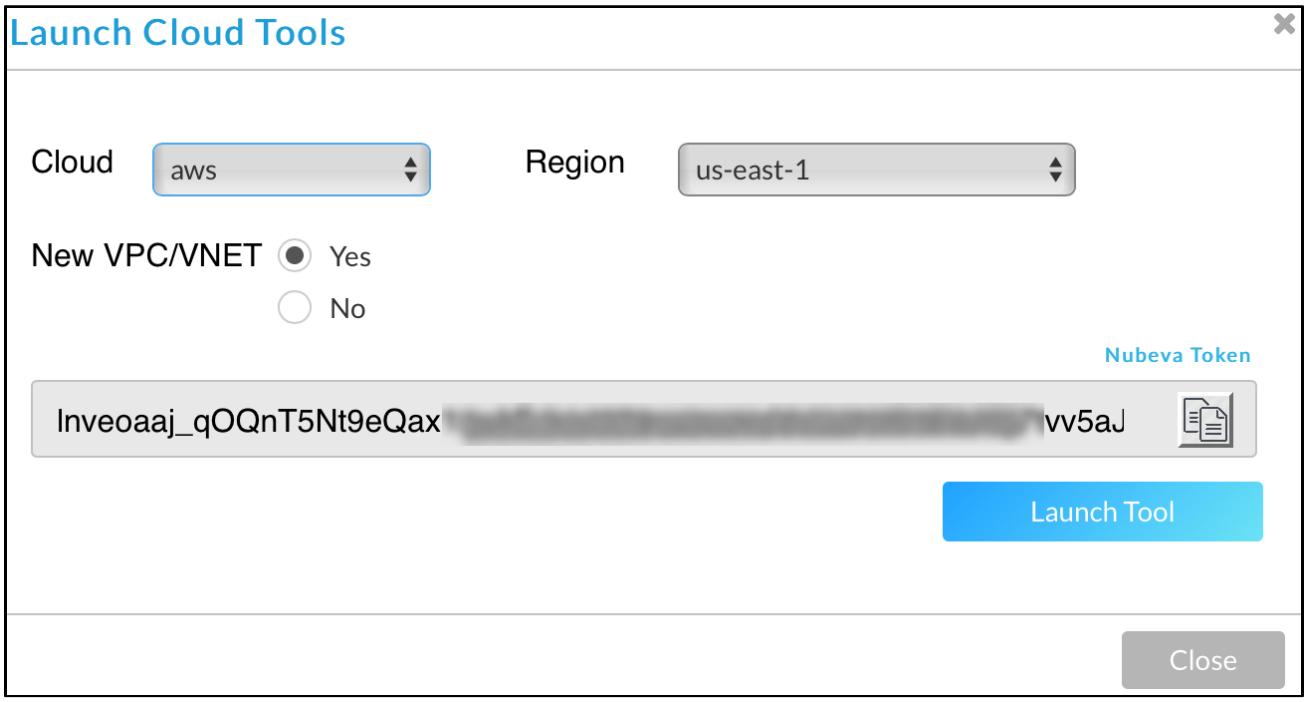
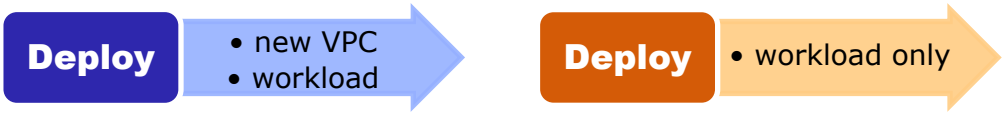


Figure 2: Copy the Nubeva token

Step 3. Launch the Quick Start

> **Note**: You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help with choosing an option, see Deployment options, earlier in this guide.



Deploy Nubeva into a new VPC on AWS

Deploy Nubeva into an existing VPC on AWS

> **Important**: If you're deploying Nubeva into an existing virtual private cloud (VPC), ensure that your VPC has two public subnets in different Availability Zones for the source and tool instances. These subnets require internet connectivity through an internet gateway or NAT gateway to allow the instances to download packages and software. You will be prompted for your VPC settings when you launch the Quick Start.

   Each deployment takes about 10 minutes to complete.

2. Check the Region that's displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the network infrastructure for Nubeva and the open-source tools will be built. The template is launched in the US East (Ohio) Region by default.
3. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.
4. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose **Next**.
5. In the following tables, parameters are listed by category and described separately for the two deployment options:
   - Parameters for deploying Nubeva TLS Decrypt into a new VPC
   - Parameters for deploying Nubeva TLS Decrypt into an existing VPC

OPTION 1: PARAMETERS FOR DEPLOYING NUBEVA INTO A NEW VPC

View template

VPC network configuration:

Parameter label (name)	Default	Description
Availability Zones (`AvailabilityZones`)	*Requires input*	List of Availability Zones to use for the subnets in the VPC. Two Availability Zones are used for this deployment.
VPC CIDR (`VPCCIDR`)	10.0.0.0/16	CIDR block for the VPC.
Private subnet 1 CIDR (`PrivateSubnet1CIDR`)	10.0.16.0/20	CIDR block for private subnet 1, located in Availability Zone 1.
Private subnet 2 CIDR (`PrivateSubnet2CIDR`)	10.0.32.0/20	CIDR block for private subnet 2, located in Availability Zone 2.
Public subnet 1 CIDR (`PublicSubnet1CIDR`)	10.0.48.0/20	CIDR block for the public (DMZ) subnet 1, located in Availability Zone 1.
Public subnet 2 CIDR (`PublicSubnet2CIDR`)	10.0.64.0/20	CIDR block for the public (DMZ) subnet 1, located in Availability Zone 2.
Allowed external access CIDR (`RemoteAccessCIDR`)	*Requires input*	CIDR IP range permitted to access the instances. We recommend setting this value to a trusted IP range.
Bastion AMI operating system (`BastionAMIOS`)	Amazon-Linux-HVM	Linux distribution for the Amazon Machine Image (AMI) to be used for the bastion instances.
Bastion instance type (`BastionInstanceType`)	t3.small	Amazon EC2 instance type for the bastion instances.

Nubeva configuration:

Parameter label (name)	Default	Description
Nubeva token (`APIKey`)	*Requires input*	Token for your Nubeva account.
Install Moloch ASG (`MolochInstall`)	true	Choose to install Moloch.
Install Ntop ASG (`NtopInstall`)	true	Choose to install Ntop.
Install Wireshark ASG (`WiresharkInstall`)	true	Choose to install Wireshark.
Install Suricata ASG (`SuricataInstall`)	true	Choose to install Suricata.

Parameter label (name)	Default	Description
Install Zeek ASG (ZeekInstall)	true	Choose to install Zeek.
Install TLS generation clients (ClientInstall)	true	Choose to install TLS generation clients.
Administrator name (ToolAdmin)	tooladmin	User name that is associated with the administrator account for the created tools.
Administrator password (ToolPassword)	*Requires input*	Choose a password that contains 8–32 alphanumeric characters.

Auto Scaling group configuration:

Parameter label (name)	Default	Description
SSH key name (KeyPairName)	*Requires input*	Name of an existing key pair that allows you to securely connect to your launched instance.
Tool instance type (NodeInstanceType)	m5.large	Type of EC2 instance for the node instances.
Desired nodes per tool (NumberOfNodes)	2	Number of EC2 instance nodes in each Auto Scaling group.
Maximum nodes per tool (MaximumNodes)	6	Maximum number of EC2 instance nodes in each Auto Scaling group.

AWS Quick Start configuration:

Parameter label (name)	Default	Description
Quick Start S3 bucket name (QSS3BucketName)	aws-quickstart	S3 bucket name for the Quick Start assets. This string can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Quick Start S3 bucket Region (QSS3BucketRegion)	us-east-1	AWS Region where the Quick Start S3 bucket (QSS3BucketName) is hosted. When using your own bucket, you must specify this value.
Quick Start S3 key prefix (QSS3KeyPrefix)	quickstart-nubeva-tlsdecrypt/	S3 key prefix for the Quick Start assets. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).

OPTION 2: PARAMETERS FOR DEPLOYING NUBEVA INTO AN EXISTING VPC

View template

VPC network configuration:

Parameter label (name)	Default	Description
VPC ID (VPCID)	*Requires input*	ID of your existing VPC (for example, vpc-0343606e).
VPC CIDR (VPCCIDR)	10.0.0.0/16	CIDR block for the VPC.
Private subnet 1 ID (PrivateSubnet1ID)	*Requires input*	ID of the private subnet in Availability Zone 1 in your existing VPC (for example, subnet-fe9a8b32).
Private subnet 2 ID (PrivateSubnet2ID)	*Requires input*	ID of the private subnet in Availability Zone 2 in your existing VPC (for example, subnet-be8b01ea).
Allowed external access CIDR (RemoteAccessCIDR)	*Requires input*	CIDR IP range that is permitted to access the instances. We recommend that you set this value to a trusted IP range.

Nubeva configuration:

Parameter label (name)	Default	Description
Nubeva token (APIKey)	*Requires input*	Token for your Nubeva account.
Install Moloch ASG (MolochInstall)	true	Choose to install Moloch.
Install Ntop ASG (NtopInstall)	true	Choose to install Ntop.
Install Wireshark ASG (WiresharkInstall)	true	Choose to install Wireshark.
Install Suricata ASG (SuricataInstall)	true	Choose to install Suricata.
Install Zeek ASG (ZeekInstall)	true	Choose to install Zeek.
Install TLS generation clients (ClientInstall)	true	Choose to install TLS generation clients.
Administrator name (ToolAdmin)	tooladmin	User name that is associated with the administrator account for the created tools.

Parameter label (name)	Default	Description
Administrator password (`ToolPassword`)	*Requires input*	Choose a password that contains 8–32 alphanumeric characters.

Auto Scaling group configuration:

Parameter label (name)	Default	Description
SSH key name (`KeyPairName`)	*Requires input*	Name of an existing key pair that allows you to connect securely to launch instances.
Node instance type (`NodeInstanceType`)	m5.large	Type of EC2 instance for the node instances.
Number of nodes (`NumberOfNodes`)	2	Number of EC2 instance nodes in each Auto Scaling group.
Maximum nodes per tool (`MaximumNodes`)	6	Maximum number of EC2 instance nodes in each Auto Scaling group.

AWS Quick Start configuration:

Parameter label (name)	Default	Description
Quick Start S3 bucket name (`QSS3BucketName`)	aws-quickstart	S3 bucket name for the Quick Start assets. This string can include numbers, lowercase letters, uppercase letters, and hyphens (-). It cannot start or end with a hyphen (-).
Quick Start S3 bucket Region (`QSS3BucketRegion`)	us-east-1	AWS Region where the Quick Start S3 bucket (QSS3BucketName) is hosted. When using your own bucket, you must specify this value.
Quick Start S3 key prefix (`QSS3KeyPrefix`)	quickstart-nubeva-tlsdecrypt/	S3 key prefix for the Quick Start assets. Quick Start key prefix can include numbers, lowercase letters, uppercase letters, hyphens (-), and forward slash (/).

6. On the **Options** page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you're done, choose **Next**.
7. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the two check boxes to acknowledge that the template will create IAM resources and that it might require the capability to auto-expand macros.
8. Choose **Create** to deploy the stack.

9. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the deployment is complete.

Step 4. Test the deployment

By default, this Quick Start includes TLS clients that generate standard web traffic as well as simulated attack instances. To validate the deployment and view the simulated threats, follow these steps:

1. Log in to the Nubeva SaaS console using the credentials you created in Step 2.
2. Ensure that you see two instances connected to the console.

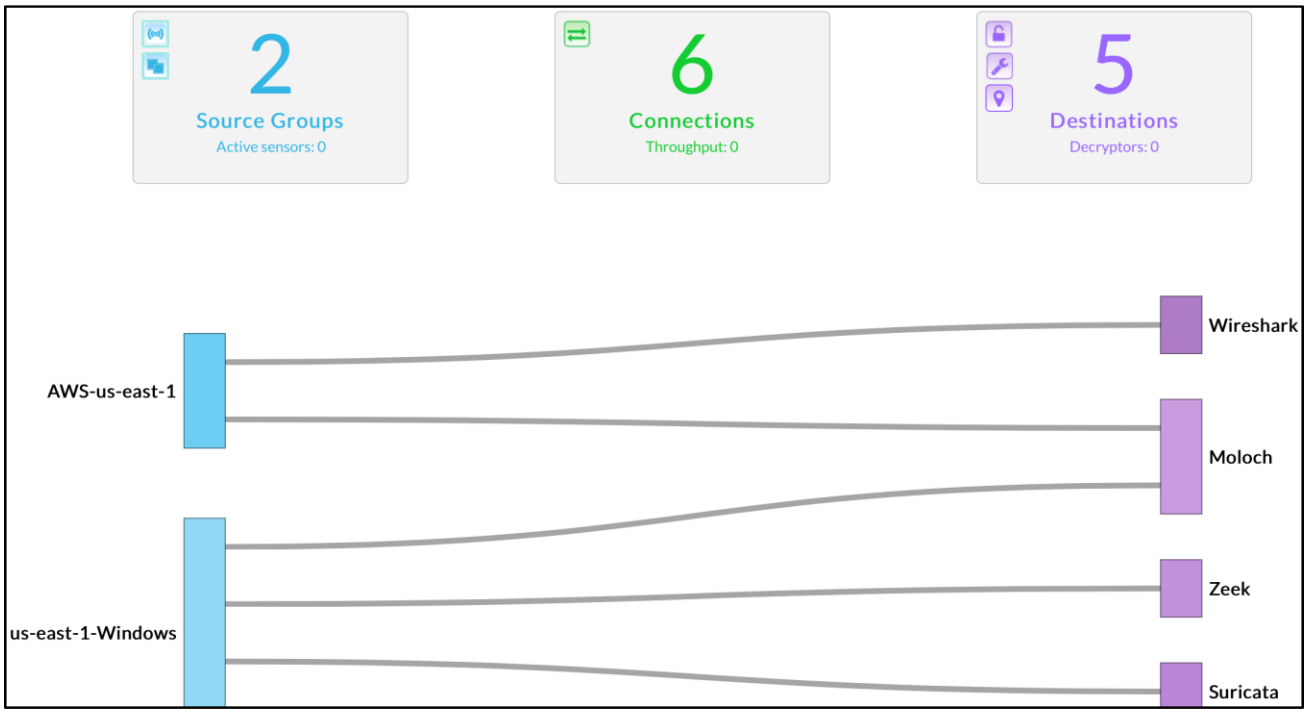


Figure 3: Checking instances in the Nubeva console

3. Mirror the traffic from the sources to the tools. Amazon VPC mirror targets have been preconfigured on the open-source tools. Create an Amazon VPC traffic mirroring session for your clients, and direct them to the pre-configured destinations.

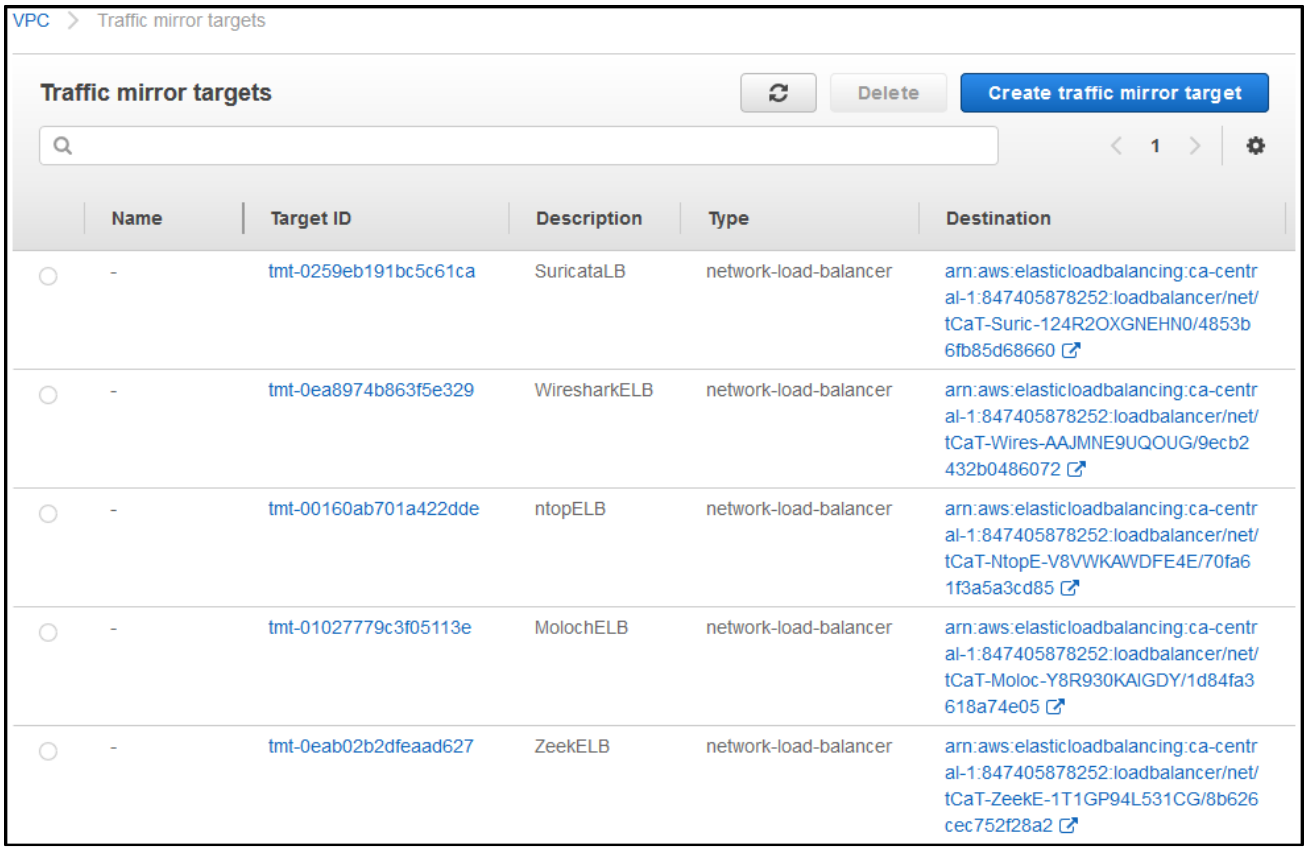


Figure 4: List of potential traffic mirror targets listed in the AWS Console

4. Optional: Monitor additional application instances by launching more Nubeva agents. Choose the **Launch a Sensor** icon for instructions on how to deploy a new agent. Ensure that you define a group for the newly launched agents.
5. Each tool should be accessed directly:
    a Moloch: Connect to the administration console using the link listed on the output of the CloudFormation stack, `http://elbaddress:8005`. The user name and password are the `tooladmin` credentials you submitted.
    b Ntopng: Connect to the administrator console using the link listed on the output of the CloudFormation stack, `http://elbaddress:3000`. The user name and password are the default Ntopng credentials.
    c Wireshark: Connect by using SSH to the instance with `ssh ubuntu@ipaddress`. Set the password for `tooladmin` using `sudo passwd tooladmin`. This enables remote desktop protocol (RDP) access for the defined user, which is used to connect to the Domain Name System of the Wireshark ELB instance. Then start Wireshark from the UI using `sudo wireshark`. Monitor the nurxo interface for decrypted cloud traffic.

d Suricata and Zeek: Connect to the Kibana interface using the link listed on the output of the CloudFormation stack.

FAQ

Q. I encountered a **CREATE_FAILED** error when I launched the Quick Start.

A. If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with **Rollback on failure** set to **Disabled**. (This setting is under **Advanced options** in the AWS CloudFormation console, under **Stack creation options**.) With this setting, the stack's state is retained and the instance is left running, so you can troubleshoot the issue. (For Windows, look at the log files in `%ProgramFiles%\Amazon\EC2ConfigService` and `C:\cfn\log`.)

> **Important**: When you set **Rollback on failure** to **Disabled**, you continue to incur AWS charges for this stack. Please ensure to delete the stack when you finish troubleshooting.

For additional information, see Troubleshooting AWS CloudFormation.

Q. I encountered a size limitation error when I deployed the AWS CloudFormation templates.

A. We recommend that you launch the Quick Start templates from the links in this guide or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-S3 location, you might encounter template size limitations. For more information about AWS CloudFormation quotas, see the AWS documentation.

Send us feedback

To post feedback, submit feature ideas, or report bugs, use the **Issues** section of the GitHub repository for this Quick Start. If you'd like to submit code, please review the Quick Start Contributor's Guide.

Additional resources

AWS resources

- Getting Started Resource Center
- AWS General Reference
- AWS Glossary

AWS services

- AWS CloudFormation
- Amazon EBS
- Amazon EC2
- IAM
- Amazon VPC

Nubeva documentation

- Nubeva Documentation
- Open-source tools documentation

Other Quick Start reference deployments

- AWS Quick Start home page

Document revisions

Date	Change	In sections
March 2020	Parameter `QSS3BucketRegion` added to both deployment options	Option 1, under **AWS Quick Start configuration**; Option 2, under **AWS Quick Start configuration**
February 2020	Initial publication	—

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.