CLOUDMON NTM

Version 2.3

Getting started guide – AWS

Part Number: T /GS – Veryx Cloudmon NTM 2.3 - 1221/1.0

Table of Contents

INTRODUCTION

As businesses grow, network infrastructure growth across physical, virtual and public cloud, more often than not are bound to result in complexity and in-efficiency. The very mission critical infrastructure that should help businesses realize the benefits of digital transformation and innovation, often plays spoil-sport because of unknown problems lurking in the network and the resulting performance and availability challenges.

Veryx Cloudmon NTM helps businesses by providing:

- *100% network visibility and analytics of all traffic across their business-critical infrastructure, whether on-premises, private cloud, or AWS cloud*
- *Performance monitoring of applications in hybrid environments.*
- *Visibility of end user digital experience for consistency and high-quality*
- *Better control and realization of the power of digital innovation at a fraction of the cost of competing solutions.*

Figure 1 illustrates a sample hybrid deployment of Cloudmon NTM. Cloudmon NTM Controller operates as a centralized orchestrator. It manages

- *Virtual NTM probes in public cloud*
- *Physical NTM probes on-premises*

Deploying Cloudmon NTM probes in strategic locations could help in minimizing cloud traffic passing through inter-regions / VPCs, which in turn reduces additional cloud network data consumption expenses.

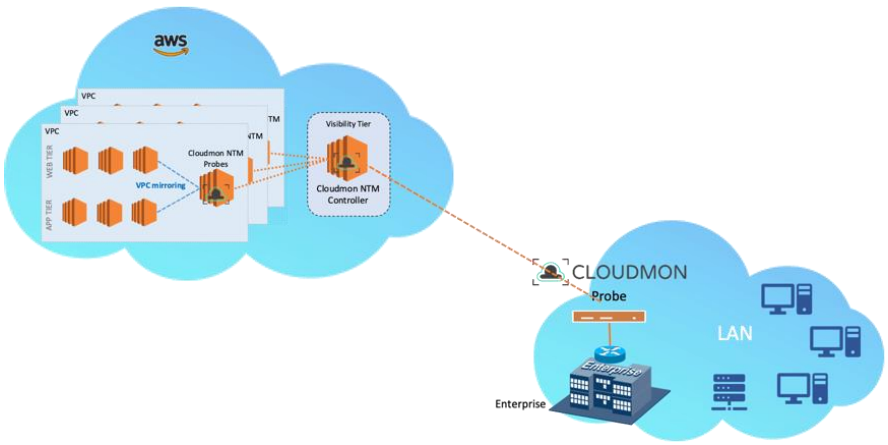

Figure 1 - Sample hybrid deployment

COMPONENTS

NTM Controller

- *Orchestrates meta-data from NTM probes and provides intuitive dashboards and reports*
- *Provides analytics of the orchestrated data*
- *Generates notifications and alarms, and performs automated remediation*
- *Provides seamless management of NTM probes, on-premises, and in cloud environments.*

NTM Probe

- *Could be deployed:*
    - *As a virtual appliance in AWS EC2 using ready-made AMI,*
    - *As a virtual appliance in private cloud using ready-made VMs, or*
    - *as a physical appliance in on-premises using software package*
- *Supports scalable provisioning depending on Instance Type selected during deployment.*
- *Receives traffic forwarded from multiple virtual taps (vTAPs) or from VPC mirroring for full packet capture & analysis*

DEPLOYMENT ARCHITECTURE – ALL-IN-ONE CONTROLLER

Figure 2 illustrates a sample of a multi-VPC deployment, including an application with multi-AZ databases.

Note the following:

- *In case of Cloudmon NTM All-in-One Controller, both the Controller and the Probe reside in same instance and are placed in VPC separate from the monitored Application deployment. Although this example shows both VPCs in the same AWS Region, they can also be in separate regions.*
- *Cloudmon NTM's CloudFormation templates in the AWS Marketplace are used to perform the deployment of All-in-One virtual appliance instance, necessary security groups, addition memory for datastore, and additional Ethernet adapter for capturing monitored traffic.*

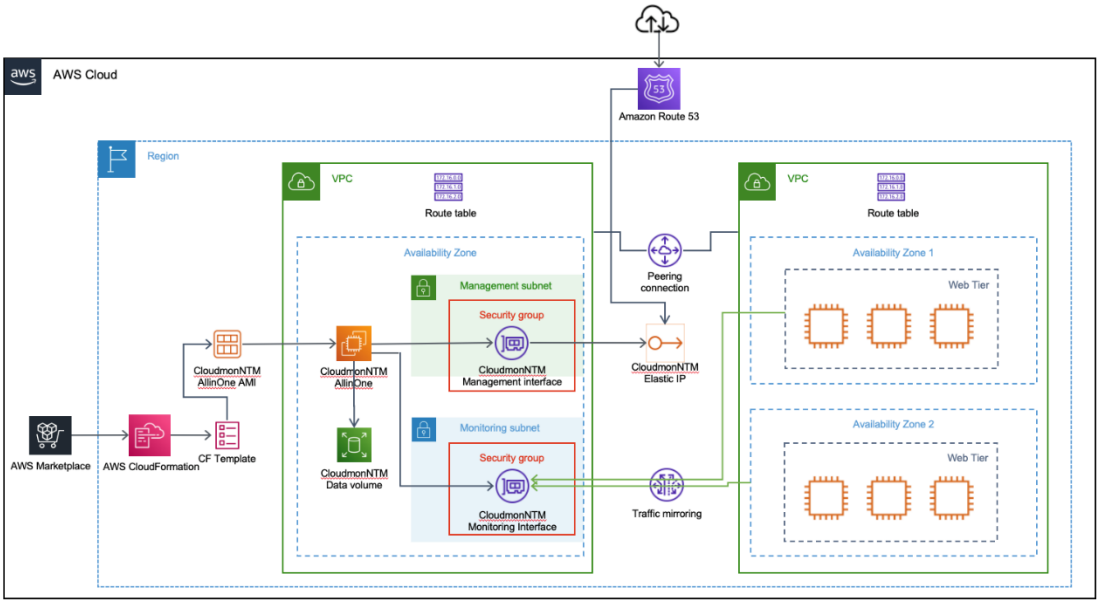

Figure 2 – Detailed deployment diagram

SYSTEM REQUIREMENTS – AWS

This document assumes that you are familiar with the networking and configuration of the AWS VPC. In order to provide context for the terms used in this section, here is a brief refresher on the AWS terms (some definitions are taken directly from the AWS glossary) that are referred to in this document:

AWS TERMINOLOGY

Term	Description
EC2	Elastic Compute Cloud A web service that enables you to launch and manage Linux/UNIX and Windows server instances in Amazon's data centers.
Amazon Machine Image (AMI)	An AMI provides the information required to launch an instance, which is a virtual server in the cloud.
Elastic Network Interface (ENI)	An additional network interface that can be attached to an EC2 instance. ENIs can include a primary private IP address, one or more secondary private IP addresses, a public IP address, an elastic IP address (optional), a MAC address, membership in specified security groups, a description, and a source/ destination check flag.
IP address types for EC2 instances	An EC2 instance can have different types of IP addresses. - *Public IP address: An IP address that can be routed across the internet.* - *Private IP address: An IP address in the private IP address range as defined in the RFC 1918. You can choose to manually assign an IP address or to auto assign an IP address within the range in the CIDR block for the subnet in which you launch the EC2 instance.* If you are manually assigning an IP address, Amazon reserves the first four (4) IP addresses and the last one (1) IP address in every subnet for IP networking purposes. - *Elastic IP address (EIP): A static IP address that you have allocated in Amazon EC2 or Amazon VPC and then attached to an instance. Elastic IP addresses are associated with your account, not with a*

Term	Description
	specific instance. They are elastic because you can easily allocate, attach, detach, and free them as your needs change. An instance in a public subnet can have a Private IP address, a Public IP address, and an Elastic IP address (EIP); an instance in a private subnet will have a private IP address and optionally have an EIP.
Instance type	Amazon-defined specifications that stipulate the memory, CPU, storage capacity, and hourly cost for an instance. Some instance types are designed for standard applications, whereas others are designed for CPU-intensive, memory-intensive applications, and so on.
Virtual Private Cloud (VPC)	An elastic network populated by infrastructure, platform, and application services that share common security and interconnection.
Identity and Access Management (IAM) Role	The IAM role defines the API actions and resources the application can use after assuming the role. An IAM role is also required for VM Monitoring.
Subnets	A segment of the IP address range of a VPC to which EC2 instances can be attached. EC2 instances are grouped into subnets based on your security and operational needs. There are two types of subnets: - *Private subnet: The EC2 instances in this subnet cannot be reached from the internet.* - *Public subnet: The internet gateway is attached to the public subnet, and the EC2 instances in this subnet can be reached from the internet.*
Security groups	A security group is attached to an ENI, and it specifies the list of protocols, ports, and IP address ranges that are allowed to establish inbound/outbound connections on the interface.
Key pair	A set of security credentials you use to prove your identity electronically. The key pair consists of a private key and a public key.

Table 1 – AWS terminology

AWS COMPONENTS & PERMISSIONS

Table 2 summarizes the necessary requirements to deploy Cloudmon NTM in AWS environment.

Component	Description
Amazon Web Services Account	You must have an active Amazon Web Services account with access to the EC2 Management Console to deploy in an AWS environment.
Amazon Web Services Permissions	The Amazon Web Services account used to deploy Cloudmon NTM must have appropriate permissions granted. The simplest way to do this is to grant the **AdministratorAccess** policy. However, if granting administrator access is not acceptable in your environment, assign the following policies to the account used to deploy Cloudmon NTM components: • *Assign the built-in **AmazonEC2FullAccess** policy.*
Existing AWS VPC	An existing AWS VPC with subnets for both Management and Monitoring.
Route Tables/Security Groups	Appropriate Route Tables and Security Groups for communication between Cloudmon NTM Controller and NTM Probes
Access to Marketplace Images	You must have access to the Veryx Cloudmon NTM AMI images in the AWS Marketplace in the AWS region you are using.
SSH Key Pair	You must have a key pair for SSH access to deployed AMIs. You can create or import the key pair in AWS using these instructions. SSH key pairs created in AWS are: - *Public keys are stored in AWS, are not confidential and are protected at the account level.* - *Private keys are stored by the user and are their responsibility to protect.*

Table 2 – AWS deployment requirements

ABOUT PRICING AND COST

The Veryx site on the AWS Marketplace provides helpful tools that let you estimate the costs of using Veryx Cloudmon NTM solutions with different configuration choices. After navigating to the Veryx site on the AWS Marketplace, click on the Pricing tab and fill out the fields to estimate your costs. Keep in mind that your usage and costs may vary from the estimate depending on actual usage.

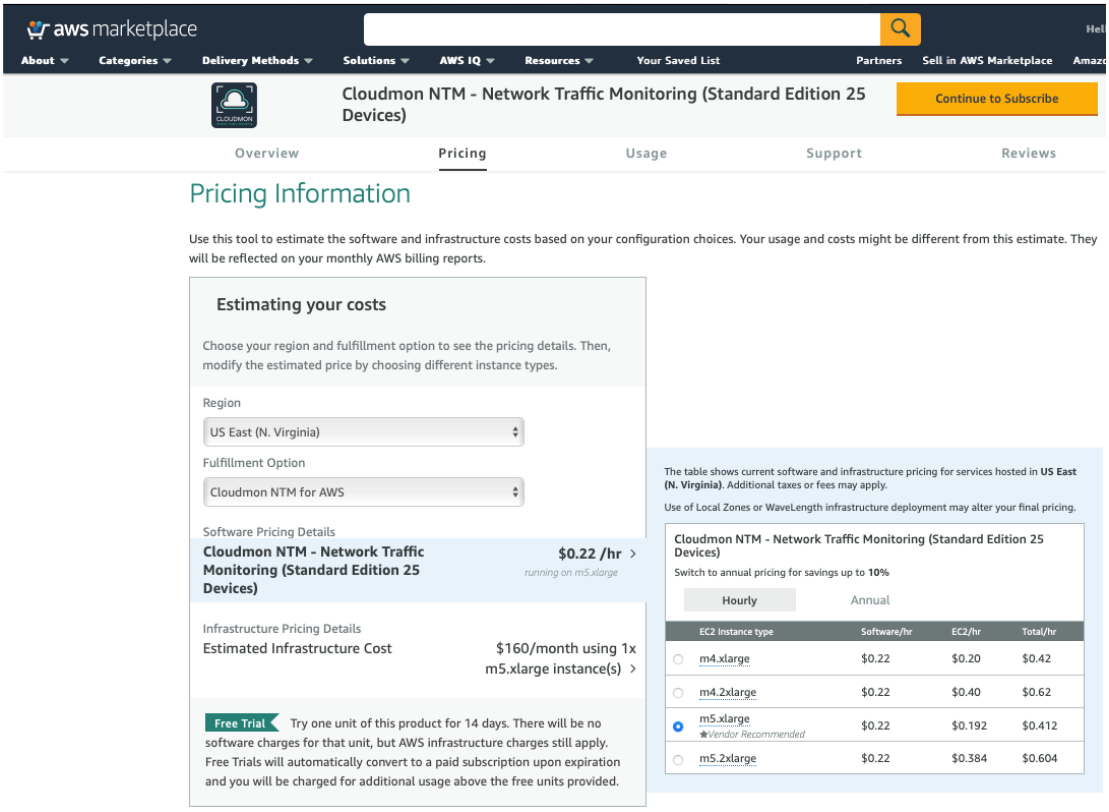

Figure 3 – Detailed deployment diagram

DEPLOYMENT

LAUNCHING CLOUDMON NTM ALL-IN-ONE TEMPLATE

This section describes how to deploy the Cloudmon NTM All-in-One Controller (both controller and probe are co-located) using the CloudFormation template and AMI available in the Veryx site on the AWS Marketplace.

STEP 1

Search the Amazon Marketplace for Veryx Cloudmon NTM.

The Amazon Marketplace shows available flavors for the Cloudmon NTM for AWS.

STEP 2

Select the Cloudmon NTM All-in-One Controller. Click the 

button.

STEP 3

Accept the Terms and Conditions.

STEP 4

*Click **Continue to Configuration** button.*

Use the Software Version dropdown to select the version of the selected CFT to deploy

STEP 5

Click Continue to Launch to continue.

*Review the configuration details in the Launch page and click **Launch** when ready to continue.*

*The **Create stack** wizard appears with the **Select Template** screen pre-populated with the selected CloudFormation template. For example,* Figure 6 *shows the **Create stack** wizard pre-populated with the **Cloudmon NTM All-in-One** CloudFormation template.*

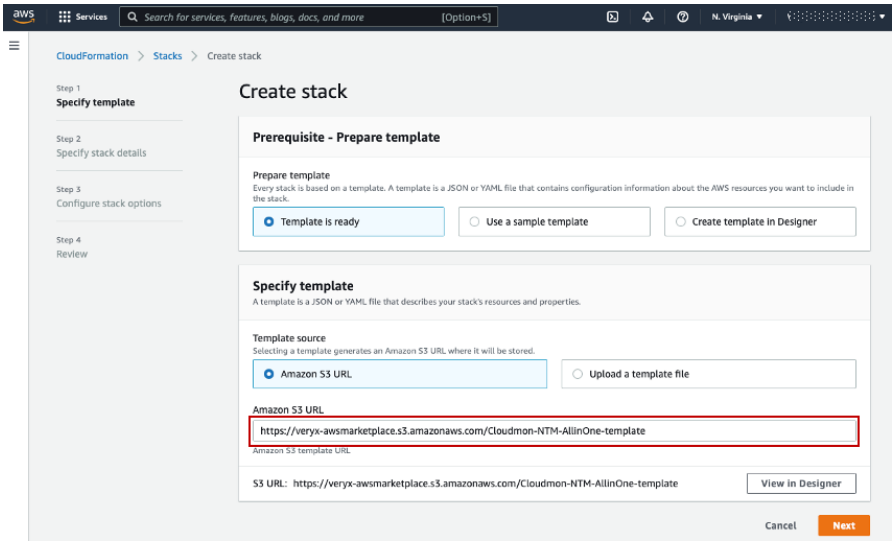

Figure 4 – Create Stack Wizard with CFT for Cloudmon NTM All-in-One

STEP 6

*Click **Next** to continue.*

STEP 7

*The **Specify stack details** page appears. Provide a Stack name and fill out the Parameters for the CloudFormation template using the information in* Table 3.

Figure 5 shows an example configuration.

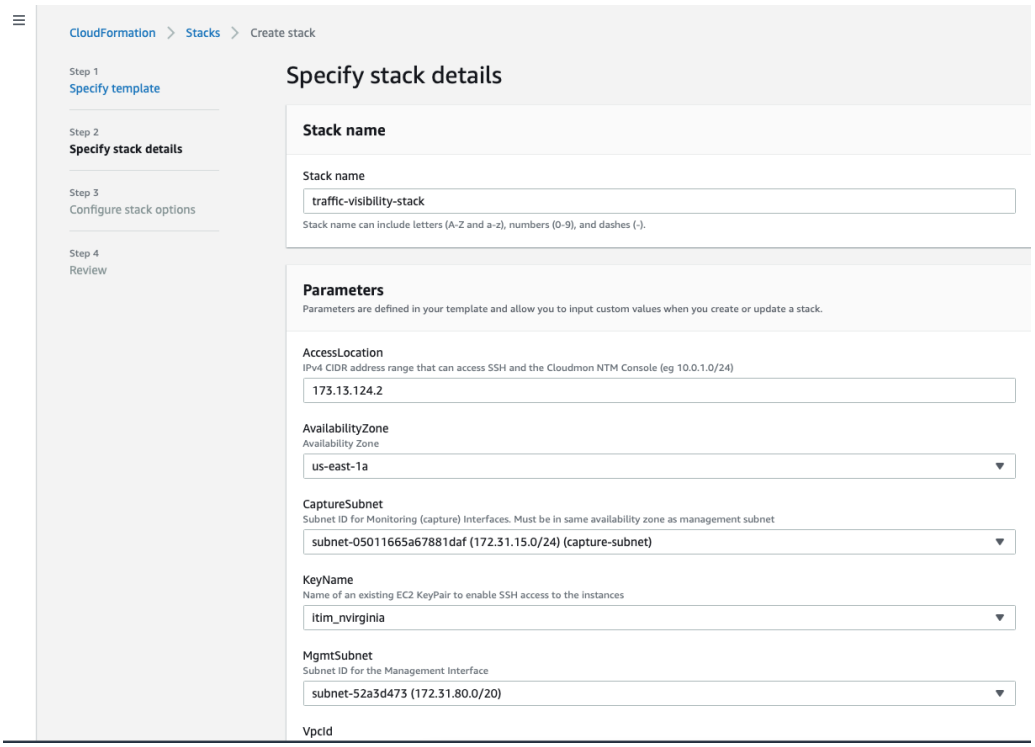

Figure 5 – Supplying values for the CFT

STEP 8

*When you have finished configuring the CloudFormation parameters, click **Next** to continue.*

STEP 9

*The **Configure stack options** page appears, allowing you to configure the standard CloudFormation Stack settings. These are all optional; none are required. Use the links below to learn more about these AWS options.*

- *Tags*
- *Permissions*
- *Stack failure options*
- *Advanced options*

When you have finished setting Options, click Next to continue.

STEP 10

*The Create Stack Wizard displays a summary of the settings for the new stack. Review the settings and use the **Previous** button to correct if necessary. When you are satisfied with your settings, click **Create stack** to launch the new instance.*

*The Stack Wizard begins to create the requested resources (*Figure 6*) and eventually launches the instance.*

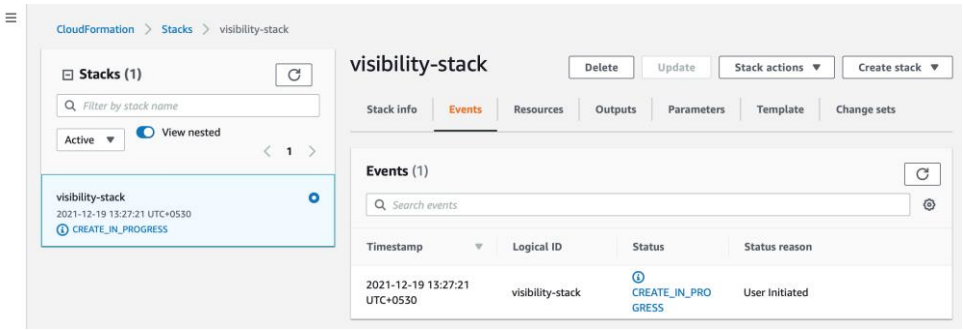

Figure 6 – Stack creation is in progress

STEP 11

After a few minutes, you can see the instance(s) in the EC2 Management Console's Instances list. (Figure 7).

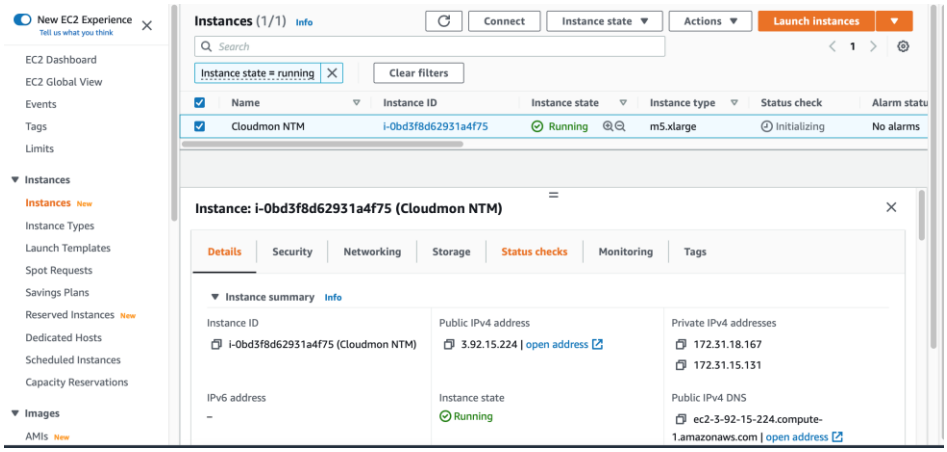

Figure 7 – Newly created instance

TEMPLATE PARAMETERS

Table 3 lists and describes the parameters you must supply as part of the deployment of the Veryx Cloudmon NTM CloudFormation template.

Parameter	Description
Stack name	Provide a unique name for this stack.
AccessLocation	Use this field to limit the range of IP addresses from which the deployed instance will accept HTTP / HTTPS / SSH connections. This field is mandatory. However, if you want to allow SSH connections from any location, you can enter a value of 0.0.0.0/0. You can edit the Security Group settings later to change the IP addresses for which access is allowed. Refer to Working with Security Groups in the AWS documentation for details.
AvailabilityZone	Select an AWS Availability Zone to be used for the deployment from the dropdown lists. The list includes the Availability Zones accessible from your account.
CaptureSubnet	Use the dropdown lists to select an existing subnet for the monitoring interface. The dropdown lists the subnets already provisioned for your account. You can either select the same subnet you are using for Management traffic or choose a different one. Note that the Capture and Management subnets must both be in the same AWS Availability Zone. In general, it's a good practice to keep management traffic separate from the capture subnet. This way, you aren't adding additional traffic to the monitored subnet, and you also have a means of contacting a managed Cloudmon NTM even if its capture subnet goes down.

	If you have many subnets associated with your account, you can type an entry in the field to narrow the results to matching IDs or name tag values.
KeyName	Select an existing keypair from the dropdown to be used for access to the instance. You can review your existing keypairs in Network & Security > Key Pairs from the EC2 Dashboard.
MgmtSubnet	Use the dropdown list to select an existing subnet for managing your Cloudmon NTM instance. The dropdown lists the subnets already provisioned for your account. Note that the Capture and Management subnets must both be in the same AWS Availability Zone. If you have many subnets associated with your account, you can type an entry in the field to narrow the results to matching IDs or name tag values.
VpcId	Use the dropdown to select an existing VPC for the deployment. If you have many VPCs associated with your account, you can type an entry in the field to narrow the results to matching IDs or name tag values.
ntmInstanceType	Choose an Instance Type for the Cloudmon NTM All-in-One deployment from the dropdown list. Each Instance Type provides a different combination of computing resources (CPU, memory, storage, and networking). You can select from the following Instance Types: • m5.xlarge (default - Flows per minute up to 0.5 million)) • m5.2xlarge (Flows per minute up to 1.5 million) • m5.4xlarge (Flows per minute up to 3.5 million)) NOTE: Instance Types are priced differently in the AWS Public Cloud based on the amount of resources provisioned. Refer to https://aws.amazon.com/ec2/instance-types for details.
ntmMgmtSecGrpId	Use this field to assign the management interface (eth0) to a Security Group. If you leave these options set to CREATE (the default), the template automatically assigns the corresponding interface to a Security Group with the necessary permissions and open ports to allow communication
ntmMonitorSecGrpId	Use this field to assign the monitor interface (eth1) to a Security Group. If you leave these options set to CREATE (the default), the template automatically assigns the corresponding interface to a Security Group with the necessary permissions and open ports to allow communication
ntmVolumeSize	Specify the size of the Cloudmon NTM database in GB. The default value is 80GB.

Table 3 – Configuration parameters for CloudFormation template

SECURITY GROUP DETAILS

As described in Table 3, the Cloudmon NTM CFT template provide the options of creating AWS Security Groups for the solution. This section describes the ports opened by each of these Security Groups.

The default settings for Cloudmon NTM Security Groups ensure that the necessary communications between Cloudmon NTM components in these different groups can take place successfully.

If you did not create Security Groups as part of the CFT templates, you can also use the information in these sections to open the necessary ports for Cloudmon NTM communications in your own Security Groups:

Management Security Group

Description	Protocol	Port Range
HTTP access	TCP	80
HTTPS access	TCP	443
SSH access	SSH	22
All ICMP IPv4 (PING)	All	N/A

Table 4 – Traffic allowed for Management Security Group

Monitor Security Group

Description	Protocol	Port Range
UDP from AWS traffic mirroring	UDP	4789
GRE from Virtual TAPs	GRE (47)	All
All ICMP IPv4 (PING)	All	N/A

Table 5 – Traffic allowed for Monitoring Security Group

Note:

We recommend allow all traffic for the monitoring interface, so that Cloudmon NTM Probe and capture and monitor all packets received.

INSTANCE TYPE RECOMMENDATIONS

The CloudFormation templates for the Cloudmon NTM solution let you select an Instance Type for both the Controller and Probe virtual appliance. Each Instance Type provides a different combination of computing resources (CPU, memory, storage, and networking; refer to Table 6) and is priced differently based on the amount of resources provisioned.

Instance Type	vCPUs	Memory	Flows Per Minute	Concurrent Users
m5.xlarge	8	16 GB	0.5 million	1
m5.2xlarge	8	32 GB	1.5 million	3
m5.4xlarge	16	64 GB	3.5 million	3

Table 6 – Instance Type recommendation and System load

AWS TRAFFIC MIRRORING

In addition to forwarding packets from vTAP Agents to Cloudmon NTM All-in-Once controller or NTM probe, AWS provides additional tools that help Cloudmon NTM provide visibility on cloud-based traffic:

- *Amazon VPC traffic mirroring allows you to acquire packet data from multiple application workloads in an Amazon VPC and mirror it to a Cloudmon NTM All-in-One controller or NTM probe instance's monitor port.*

CONFIGURING AWS VPC TRAFFIC MIRRORING

AWS VPC Traffic Mirroring lets you send packets from a mirror source to a destination – a Cloudmon NTM All-in-One controller or NTM probe instance's monitoring interface for our purposes. Traffic Mirroring sessions consist of the following main components:

- *Mirror source. This is where the traffic will be mirrored from.*
- *Mirror destination. This is where mirrored traffic will be sent – a Cloudmon NTM All-in-One controller or NTM probe instance's monitoring port in our case.*
- *Optional filter - This lets you limit which traffic is mirrored to just the packets of interest.*

Refer Amazon AWS documentation for more information.

Traffic Mirroring Prerequisites and Rules

In general:

- *Traffic mirror sources and destinations must either be in the same VPC or in VPCs that are reachable from one another.*
- *The traffic mirror target must have **UDP Port 4789** open to receive traffic.*
- *The traffic mirror source must have a route table entry for the target.*
- If mirrored traffic is not reaching the destination, check to see if there are any security group or access control list (ACL) rules that are preventing the traffic from arriving.

Creating a Traffic Mirror Target

1. *Log in to the AWS Management Console and select the **Services > Networking & Content Delivery > VPC** option to launch the VPC Console.*
2. *Locate and select the **Traffic Mirroring > Mirror Targets** option in the navigation panel at the left of the console.*

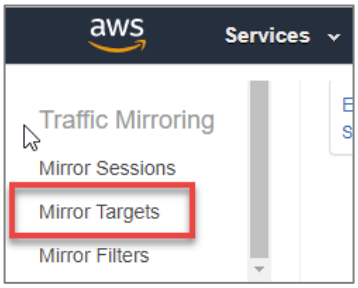

Figure 8 – Creating a Mirror Target

The Traffic mirror targets page appears, listing the existing targets for traffic mirroring.

3. *Click the **Create traffic mirror target** button to create a new target.*
4. *Use the options in the **Create traffic mirror target** page to define the new target*
   - *Target – Cloudmon NTM All-in-One controller or NTP probe's monitoring interface*
   - *Tags – optional*
5. *Click the **Create** button to create the new traffic mirror target and add it to the list of available traffic mirror targets*

Creating a Traffic Mirroring Filter

1. *Log in to the AWS Management Console and select the **Services > Networking & Content Delivery > VPC** option to launch the VPC Console.*
2. *Locate and select the **Traffic Mirroring > Mirror Filters** option in the navigation panel at the left of the console.*

Figure 9 – Creating a Mirror Filter

The **Traffic mirror filters** page appears, listing the existing filters for traffic mirroring.

3. *Click the **Create traffic mirror filter** button to create a new filter.*
4. *Use the options in the **Create traffic mirror filter** page to define the Inbound and Outbound rules for the new filter:*

- ***Inbound*** *rules - apply to traffic arriving at whatever mirror source port you apply this filter to. Click the Add rule button and then use the available criteria to define the filter. You can accept or reject traffic based on L4 protocol, source/destination port ranges (optional), and source/destination CIDR blocks (mandatory). Filters are applied based on their priority, as specified by the Number field at the left of each rule's entry in the list.*
- ***Outbound*** *rules - apply to traffic sent out of whatever mirror source port you apply this filter to. The same filtering criteria available for Inbound rules are available for Outbound rules.*

5. *Click the Create button to create new traffic mirror filter.*

Creating a Traffic Mirroring Session

Once you've created both a target and a filter, you're ready to establish a traffic mirroring session. Use the following procedure:

1. *Log in to the AWS Management Console and select the* ***Services > Networking & Content Delivery > VPC*** *option to launch the VPC Console.*
2. *Locate and select the* ***Traffic Mirroring > Mirror Sessions*** *option in the navigation panel at the left of the console.*

Figure 10 – Creating a Mirror Session

The Traffic mirror sessions page appears, listing the existing traffic mirroring sessions.

3. *Click the* ***Create traffic mirror session*** *button to create a new session.*
4. *Use the options in the* ***Create traffic mirror session*** *page to set up the mirroring session*
   - *Mirror source – select the interface whose traffic you want to mirror and monitor*
   - *Mirror target – select the interface where you want to send the monitored traffic. This will be monitored interface of Cloudmon NTM All-in-One or NTM probe monitored interface in our case.*
   - *VNI – optional VXLAN network identifier*
   - *Packet length – By default, the entire packet will be mirrored. You can optionally slice the packet before sending it to mirror target*
   - *Filters – optional, select any of the filters created.*
5. *Click the* ***Create*** *button to create the new traffic mirror session and add it to the list of active sessions.*

Note

Keep in mind that the mirroring session remains active until you cancel it from the Traffic mirror sessions page.

CONTACTING SUPPORT

For any queries or support needed for installing Veryx Cloudmon NTM, please contact Veryx Technical Support at support@veryxtech.com