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: <u>support@liveaction.com</u>.

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 preexisting 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

 Login to AWS Console. Navigate to EC2 ? Images ? AMI and search with the provided `amiid.

[Launch Actions >	6	¢ 6
	Owned by me v Q AMU to : emi-01cc1781180cb091 O Add ther	to 1 of 1	> >
4	🗧 Name 🔹 AMI Name 🔹 AMI ID 🔹 Source 🤟 Owner 🐃 Visibility 🤟 Status 🔹 Creation Date 🔹 Platform 👻 Root Device 1- Virtual	ization -	
1	UwNX 9.0.0 Server W LiveNX Server 9.0.0/CM APP ami-01cc178/16/bb991 792086586870/ 792086566870 Private available December 19, 2019 at 11:57 Other Linux ebs hvm		

2. Select the instance type and click next.

\sim	Services - F	lesource Groups 🐱	*			Д⁰ һр	rasath @ liveaction 👻 Oregon 👻	Support 👻
. Choose A	MI 2. Choose Instance Type	3. Configure Instance	4. Add Storage 5. A	dd Tags 6. Configure S	ecurity Group 7. Review			
nazon EC		instance types optimize			rvers that can run applications. The ypes and how they can meet your o	y have varying combinations of CF omputing needs.	U, memory, storage, and networkir	g capacity, and
ter by:	All instance types 👻	Current generation	 Show/Hide Colum 	ns				
Currently	selected: t2.large (Variable B	CUs, 2 vCPUs, 2.3 GH	z, Intel Broadwell E5-268	6v4, 8 GIB memory, EBS	only)			
	Family	- Туре -	vCPUs (i)	Memory (GiB) ~	Instance Storage (GB) 🕕 👻	EBS-Optimized Available () -	Network Performance () -	IPv6 Support
	General purpose	t2.nano	1	0.5	EBS only		Low to Moderate	Yes
	General purpose	t2.micro Free tier eligible	1	1	EBS only		Low to Moderate	Yes
	General purpose	t2.small	1	2	EBS only		Low to Moderate	Yes
	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
	General purpose	t2.large	2	8	EBS only		Low to Moderate	Yes
	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes

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

aws	Services - R	esource	Groups 🗸	*							Ĺ	}● hprasati	h @ liveaction 👻	Oregon 👻	Support 👻	
1. Choose All	II 2. Choose Instance Type	3. Con	figure Instance	4. Add Storage	5. Add Tags	6. Config	jure Se	ecurity Group 7. Revie	ew							
	Configure Instan															
Configure the	e instance to suit your require		u can launch mu	ultiple instances f					antage of the	e lower pricin	g, assign an i	access manag	gement role to the	instance, and	more.	Î
	Number of instances	()	1		Launch into Auto	o Scaling	Group	P 🕕								
	Purchasing option		Request Spo	t instances												
	Network	()	vpic-etter (SilegsyLivelitX		• 0	3 0	reate new VPC								
	Subnet		subriat automation 53 IP Addresses	iiii piisidic2 us-v s available	west-2b	٣	С	reate new subnet								l
	Auto-assign Public IP	(j)	Enable			*										ľ
	Placement group	(i)	Add instance	to placement gro	quo											
	Capacity Reservation	()	Open			· 0	C C	reate new Capacity Re	eservation							
	IAM role		None			· C	; ci	reate new IAM role			÷.					
	Shutdown behavior		Stop			*										
Enal	ble termination protection	()	Protect again	nst accidental terr	nination											
	Monitoring	()	Enable Cloud	Watch detailed r	nonitoring											÷
											Cancel	Previous	Review and L	aunch Ne	ext: Add Storag	0

4. Modify the storage limit and Click next.

	Service	s → Resourc	ce Groups 😽	*						4 •	hprasath @ liveaction 👻	Oregon 👻	Support 👻	
1. Choose AMI	2. Choose Ins	stance Type 3. Co	onfigure Instance	4. Add Storage	5. Add 1	ags 6	Configure Security Group	7. Review						
	be launched f the root volu	with the following s ume. You can also					volumes and instance store							
Volume Type	I)	Device (i)	Snapshot (j)		Size (GiB)	()	Volume Type (j)		IOPS (j)	Throughput (MB/s) (i)	Delete on Termination (i)	Encryption	i)	
Root		/dev/sda1	snap-0a98f5830	5fdbb578	20		General Purpose SSD	gp2) •	100 / 3000	N/A		Not Encrypted	-	
EBS	•	/dev/sdb *	Search (case-in	sensit	50		General Purpose SSD	gp2) •	150 / 3000	N/A	×	Not Encrypted	•	⊗
Add New Volum	ne			al Purnnee (SS				reade tier eligibi	24					
Free tier eligit usage restrict		s can get up to 30 (GB of EBS Gener.		D) or Magne	etic storage	. Learn more about tree	usage uer engivi	iity and					

5. Add appropriate tags and Click next.

aws Services - Resource Groups - 🔸		۵	hprasath @ liveaction	• Oregon •	e .
		4	nprasatn @ liveaction	♥ Oregon ♥	Support 👻
1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage	e 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 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 you					
Key (128 characters maximum)	Value (256 characters maximum)	Instances (j)	Volumes (i)		
Name	LiveNX-CM	2	× 8		
	Canc	el Previous	Review and Launch	Next: Configure S	ecurity Grou

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

tep 6: Co	Security group name:	Select an existing sec	urity group		
	Description:		and LiveNX-CM ports in SG		
Type 🕕		col (j)	Port Range (j)	Source ()	Description (j)
SSH •	TCP		22	Custom • 0.0.0.0/0, ::/0	SSH from Public
HTTP •	TCP		80	Custom • 0.0.0.0/0, ::/0	Web UI access - Redirect to HTTPS
Custom TCP F •	TCP		7000	Custom • 0.0.0.0/0, ::/0	Java Client Access
Custom TCP F •	TCP		8092	Custom • 0.0.0.0/0, ::/0	Java Web Client Launch (Deprycated)
Custom TCP F •	TCP		8093	Custom • 0.0.0.0/0, ::/0	API Access
Custom TCP F •	TCP		8443	Custom • 0.0.0.0/0, ::/0	LiveNX Admin
Custom TCP F •	TCP		9443	Custom • 0.0.0.0/0, ::/0	LiveNX-CM
Custom UDP I •	UDP		2055	Custom • 0.0.0.0/0, ::/0	NetFlow
Add Rule		e Groups 🗸 🖌	443 J Storage 5, Add Tags 6. Configure Se	Custom • 0.0.0.00, ::0	Web UI - HTTPS Cancel Previous Review and Lau A* hprasath @ liveaction * Oregon * Support *
Add Rule	Services v Resource Choose Instance Type 3. Co figure Security CgT set of freval rules that contri ules that allow unrestricted acc	OUD OUD I the traffic for your inst sess to the HTTP and H	i Storage 6. Add Tags 6. Configure Se tance. On this page, you can add rules to a ITTPS ports. You can create a new security	curity Group 7. Review	Cancel Previous Review and Lau byresath @ liveaction • Oregon • Support •
Add Rule	Services ~ Resource . Choose Instance Type 3. Ce figure Security Gr set of frewait rules that action unrestricted ac Assign a security group: *	OUD OUD If the traffic for your inst cess to the HTTP and H Create a new security of	J Storage 6. Add Tags 6. Configure 5a tance. On this page, you can add rules to a tance for this page. You can add rules to a group	curity Group 7. Review	Cancel Previous Review and Lau byresath @ liveaction • Oregon • Support •
Add Rule	Services ~ Resource . Choose Instance Type 3. Ce figure Security Gr set of frewait rules that action unrestricted ac Assign a security group: *	OUD OUD I the traffic for your inst sess to the HTTP and H	J Storage 6. Add Tags 6. Configure 5a tance. On this page, you can add rules to a tance for this page. You can add rules to a group	curity Group 7. Review	Cancel Previous Review and Lau byresath @ liveaction • Oregon • Support •
Add Rule	Services ~ Resource Choose Instance Type 3. Co figure Security Gr set of treveal rules that allow unrestricted ace Aasign a security group: *	A Add OUD of the traffic for your inst sess to the HTTP and H Create a new security (Select an existing sec LiveNX-CM	J Storage 6. Add Tags 6. Configure 5a tance. On this page, you can add rules to a tance for this page. You can add rules to a group	curity Group 7. Review	Cancel Previous Review and Lau byresath @ liveaction • Oregon • Support •
Add Rule	Services ~ Resource Choose Instance Type 3. Co figure Security Gri ales that allow unrestricted aca Assign a security group. « Security group name: Description:	A Add OUD of the traffic for your inst sess to the HTTP and H Create a new security (Select an existing sec LiveNX-CM	I Storage 5. Add Tags 6. Configure 54 tance. On this page, you can add rules to a TTPS ports. You can create a new security proup unity group	curity Group 7. Review	Cancel Previous Review and Lau byresath @ liveaction • Oregon • Support •
Add Rule	Services Resource Choose Instance Type Choose Instance Ch	A Add OUD of the traffic for your inst sess to the HTTP and H Create a new security : Select an existing secu LiveNX-CM [Allow LiveNX Server	J Storage 6. Add Tags 6. Configure 54 lance. On this page, you can add rules to a TTPS ports. You can create a new security proup unity group and LiveNX-CM ports in SG	curity droup 7. Review	Cancel Previous Review and Lau Mereiron Support + ble, if you want to set up a web server and allow Internet traffic to re about Amazon EC2 security groups.
Add Rule	Services Resource Choose Instance Type Choose Instance Ch	A Add OUD of the traffic for your inst sess to the HTTP and H Create a new security : Select an existing secu LiveNX-CM [Allow LiveNX Server	I Storage 6. Add Tags 6. Configure 5. tance. On this page, you can add rules to a TTPS ports. You can create a new security proup and LiveNX-CM ports in SG Port Range ()	curity droup 7. Review	Cancel Previous Review and Lau Mereiron Coregon Support + ble, if you want to set up a web server and allow Internet traffic to re- thore about Amazon EC2 security groups. Description ①
Add Rule	Services Resource Choose Instance Type Choose Instance Ch	A Add OUD of the traffic for your inst sess to the HTTP and H Create a new security : Select an existing secu LiveNX-CM [Allow LiveNX Server	I Storage 6. Add Tags 6. Configure 5. tance. On this page, you can add rules to a TTPS ports. You can create a new security proup and LiveNX-CM ports in SG Port Range ()	curity droup 7. Review	Cancel Previous Review and Lau Mereiron Coregon Support + ble, if you want to set up a web server and allow Internet traffic to re- thore about Amazon EC2 security groups. Description ①

- **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.

Č,	aws	Services	∽ Reso	urce Groups 😽	*					↓ hprasath @ liveaction	• Oregon	• Support •
1. Cho	ose AMI	2. Choose Inst	ance Type	3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review				
			tance La nch details. Yo		edit changes for each s	ection. Click L	aunch to assign a key pair	to your instance a	Ind complete the launch pr	ocess.		
A	Your in	stances may	be accessible	from any IP addre		it you update y	open to the world. rour security group rules to a tion or service you're runnir			urity groups		
▼ AN	II Details	3										Edit AMI
	<u>م</u> (۵	opied ami-030		3 b6ef205362154 09 from us-east-2] [in type: hvm								
▼ Ins	tance T	ype									E	dit instance type
h	nstance Ty	rpe	ECUs	vCPUs	Memory (GiB)	Instance	Storage (GB)	EBS-Optimize	d Available	Network Performance		
ť	2.large		Variable	2	8	EBS only		-		Low to Moderate		
▼ Se	curity G	roups									Edi	t security groups
Se	curity grou	up name	LiveNX-0	CM								
	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,										Cancel Pr	evious Launch

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

×

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Choose an existing key pair	•
Select a key pair	
his dimension con	•

I acknowledge that I have access to the selected private key file (hari-keypair.pem), and that without this file, I won't be able to log into my instance.



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

Bendoes - Resource Groups - %	
Amazon 53 > john-spo-flowlog	Lifecycle rule X
john-vpc-flowlog	Name and scope 2 transitions 3 Explosions 4 Review
Overview Properties Permissions Managem	Configure expiration
	Current version Previous versions
Lifecycle Replication Analytics	Expire current version of object ()
+ Add Mergele rule Edit Delete Actions -	After 1 days from object creation
	Permanently delete previous versions ()
Lifecycle rule Applied to	After 1 days from becoming a previous version
fouloguage Whole bucket	Clean up expired object delete markers and incomplete multipart uploads
	Clean-up expired object delete markers 0
	You cannot enable clean up expired object delete markers if you enable Expiration.
	Clean up incomplete multipart uploads ()
	After 1 days from start of upload
	· ·
	Previous Next

Enable AWS VPC Flow Log

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

aws servi	ces 🗸 Resource Groups 🗸 👂			Q* her	asath @ locaction + Oregon +	Support =
VPC Dashboard *	Create VPC Actions *					0 . 6
Q, Delett a VPC	Q. Filter by tags and attributes or search by keys	ord			14 K K	1 to 3 of 3 🔿 🖂
Virtual Private	Name	 VPC ID 	- State - IPv4 CIDR	IPv6 CIDR	DHCP options set	Main Route
Cloud	Management	vpc-01814066	available 172.31.0.0/16		dopt-e7c2d85	rt5-00200ab
Your VPCs	i der	vpc-ixi871bc7	available 172.2.101.0/24		dop5-e7c8d555	10-555682
Subnets	Stage-LiveSIX	vpc-elaritdita	available 172.22.0.016		dopt-35e/03f50	rtb-4361602
Route Tables						
Internet Gateways						
Egress Only Internet Gateways						
DHCP Options Sets						
East: Ps						
Endpoints						
Endpoint Services						
NAT Gateways	4					
Peering Connections	VPC: spc-03ba4366					880
Security	Description CIDR Blocks Fic	w Logs Tags				
Network ACLs	VPC ID spc-03bal	366		Tenancy default		
Security Groups	State evaluate			Default VPC Yes		
Virtual Private	IPv6 CIDR 172 31.01 IPv6 CIDR -	110		Classic link Disabled DNS resolution Enabled		

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

VPC: vpc-03ba4366							888
Description CIDR Bloc	ks Flow Logs	Tags					
You can create flow logs on you Create flow log Actions		traffic flow information	n for the network inter	aces for your resources. Lea	m more		
						I< <	None found > >
Flow Log ID	- Filter -	Destination ty -	Destination name	 IAM Role Arn 		- Creation Time	
			You do not have an	Flow Logs in this region			

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

atti Services - Re	source Groups + 🕨			٥.	hpravath @ liveraction +	Oregon +	Support +
VPCs > Create flow log							
Create flow log							
Flow logs can capture IP traffic flow inform	uation for the network interfaces associated with your res	louroe	. You can create multiple subscriptions to send traffic to different destin	ation	s. Learn more		
Filter* Destination Destination log group*	Co, y teat cy dat cuans Accept Report At	c					
* Required					Cancel Create		

For Max Aggregation Interval:

VPCs >	Create flow log			
Crea	te flow log			
Flow log		nation for the network interfaces assoc vpc-876990e0 🚯	iated with your re	sources. You can create mul!
	Filter*	All	•	C 0
	Maximum aggregation interval	 10 minutes () 1 minute 		
	Destination	 Send to CloudWatch Logs () Send to an S3 bucket 		
	S3 bucket ARN*	Example: am:aws:s3:::bucket_name		0

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.

aws services	v Resource Groups v 1e		A* hprawth 0 liveaction	 Global - Support -
mazon \$3	Archive all your long-term data into Amazon \$3 Glacier Deep Archive i	Learn more »		Documentation
Buckets 4	S3 buckets		diano am testino	
	Q. Search for buckets		Copy Bucket ANN	
ock public access ccount settings)	Create bucket Edt public access settings Empty Delete			0 Active notifications
sature spotlight	Bucket name	Access 0 -	Versioning MEA delete	Disabled
eacure spongrit	🛛 😮 helpelineliteretart	Bucket and objects not	Logging Static web hosting	Disabled Disabled
	🖬 🖉 dimensioning	Bucket and objects not	Tagn Requester pays	0 Tags Disabled
	🗌 😰 dezzliwałówawiterewa	0.00	Object lock Transfer acceleration	
	Cojec	Objects can be public		
	🗌 🖉 kroppilult	Objects can be public	Permissions Owner Block public access	Iveacliovocks
	🖉 Grandan.edforder/PORtesproop	Objects can be public	Bucket policy Access control list	
	Barretton attaction hadroning hadroning	Objects can be public	CORS configuration	
	🗌 📽 incontinuents	(Nac)		
	C . R. Annesisco (2010)	Objects can be public	Lifecycle	Enabled

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

aws s	ervices - Re	source Groups - %			. herasath @ lives	atton + Gregon +	Support +
Create flow	log						
Flow logs can capture	IP traffic flow inform	ation for the network interfaces associate	with your resources. You can create multiple	subscriptions to send traffic to different dest	Inations. Learn more		
	Resources	vpc-038a4305 0					
	Filter*	Al	- C 0				
	Destination	 Send to CoudWatch Logs 0 Send to an 53 bucket 					
	\$3 bucket ARN*	amawsis3-iffinitionis/life	0				
Please note, a res	ource-based policy	will be created for you and attached to the	larget bucket.				
						_	
Log record format							
		ANS default format Custom format					
	Format preview	S(version) S(account-id) S(interface-id) S	rcaddr) \$(dstaddr) \$(srcport) \$(dstport) \$(pro	oco] \$[packets] \$[bytes] \$[star]] \$[end] \$[a	action \$(log-status)		
* Required					Cancel	catte	

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.

RECOMMENDED	
CLOUD	TRADITIONAL
Requires internet access	Internet access is not a must
Online license management	Licenses can also be managed with the Management Console
already have a license key and secret	I aiready have a license file
Add License	Add License
Register for a cloud license account and obtain a 14 day trial license.	Use the 14 day trial license bundled with the installation.
Use Trial License	Use Trial License

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

≡ LiveAction [*]	NX UX		New Features!	A 0	0	• 0	🌲 0	{-} •	0-	¢ -
API Token								API Docu		
		APITOKEN						API Toke	n Manageme	ent
		IpIm82	and the second	0						
			Remove	erate	1					
				_						

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/.

Cloud Monitor Hour Stittmids Settings are not configured. Please ensure all required parameters are defined property × Welcome to AWS Cloud Monitorring Application	
Welcome to AWS Cloud Monitoring Application	
Use Likel/U to monitor and analyze AVIS doubt network, get end to and traffic details and apply different analytics. Desimate the CBV and import it as Non-DRMP devices in your Likel/V application.	
Countrast CDV Band to Lunktx	

Navigate to LiveNX-CM Settings and edit settings.

	Cloud Monitor	HOME	SETTINGS	î.
,	AWS Cloud Mo	onitoring	Settings	
	Edit Enable P	olling		
	Polling: Disabled			
	Mode: production			
	AWS Access Key:	None		
	AWS Regions: Nor	ne .		
	FlowLog \$3 Bucke	t: None		
	LiveNX Server: No	ne		
	LiveNX Port: 2055			
	Log Directory: /dat	a/liverox-cm/	logs	

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

loud Monitor	HOME	SETTINGS	ABOUT
WS Cloud Man	itoring	Cottings	
WS Cloud Mon	moning a	setungs	
AWS Regions			Batch Size
US East (N. Virginia), US West	(Oregon) +	100
AWS Access Key			LiveNX Server
AWWKIBBAOJZ44UUKV8JJ			UveNX Server
AWS Secret Enter if n	no secret conf	figured or you we	Int to charge. LiveNX Port
			2055
FlowLog S3 Bucket	Example: s3	-bucket-name	LiveNX API Token
monitor-vpc-flowlog			7da8p3asdfasdfyeyeyrtdghusHvq8yoWP4twJH0=



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 "B98j221XXrrrrrZli43ff23eZrrrrrXG0Umiou4"
 - 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

	New Features! 🔺 0 🔳 0 🖣	• 0 🔔 0	{-} •	0 -	¢ -
API Token			API Docu		
	API TOKEN		API Toke	n Manageme	nt
	Remove Generate				

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

Cloud Monitor HOME	SETTINGS	
AWS Cloud Monitorin	a Settinas	
	g centingo	AWS Regions
Mode Production		US East (N. Virginia), US East (Ohio)
LiveNX Server	LiveNX Port	AWS Access Key
172.22.0.73	2055	Anneugrour Citic constants
Log Directory		AWS Secret Enter if no secret configured or you want to change.
/data/liverx-cm/logs		
LiveNX API Token		FlowLog \$3 Bucket
Demiliare a recercicie grace en a Divisió y Reflector demins		entre-mentalities

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

Cloud Monitor HOME SETTINGS	
AWS Cloud Monitoring Settings	
Edit Enable Polling	
Polling: Disabled	
Mode: production	
AMS Access Key: AMUUN200P3xDC300F6	
AWS Regions: US West (Oregon)	
FlowLog \$3 Bucket: cimmini-jop	
LiveNX Server: 172.22.973	
LiveNX Port: 2005	
Log Directory: /data/livens-cm/logs	

← → C △ ▲ Not secure →→→→→ 9.179.9443/settings	
Cloud Monitor HOME SETTINGS	5mdm5.179.179.9443 says
	Do you want to enable polling?
AWS Cloud Monitoring Settings	OK Cancel
Edit Enable Polling	
Polling: Disabled	
Mode: production	
AWS Access Key: AKIA3@httl://SXOCSM7JFD	
AWS Regions: US West (Oregon)	
FlowLog S3 Bucket: dest-qa	
LiveNX Server: 172.22.0.73	
LiveNX Port: 2055	

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.

Cloud Monitor	HOME	SETTINGS
Welcome to AV	VS Clou	d Monitoring Application
Use LiveNX to monito	r and analyz	e AWS cloud network, get end to end traffic details and apply different analytics.
Download the CSV ar	id import it a	Non-SNMP devices in your LiveNX application.
Download CSV	Send to Live	NX

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

104	 Protocal 	SHIP AND	Sec.Part.	Dot IP AND	Det Parts	Application	Scius.	Packet Rate	SHI CAMERY	Scie	Del Cavelley	Det Site	First Create Time	How Brd Take	1.044	In Packets	101/1ap	94090
ev 26, 2018, 312-0 AM	UDP .	198.58.105.40	109	17531743	50944	100	1247304	0.02 years		Internet		Unknown	242.00					+ 90
ev 26, 2018, 3112-43 am	109	121112-012	50044	194.08.105.42	122	101	12.67366	0.02 year		Unknown		(internet)	240.00 49	24108 69	214			0.000
ev 28, 2018, 3102-44 AM	10*	07031230	22	181-232-67.7	10080	107	306-27 lips	0.18 ppm	,	Unknown.		Driverine	2-47.08 (84	2-40.08 (01	210	14		0.00
N 26, 2016, 2012, 44, 401	10	105-25247.7	50080	17531748	22	100	205-W0 bps	0.18 pps		Internet		Unknown	2-47-58-89	2-48-58-401	218	11		+ (H)
ov 26, 2018, 2022-44 Apr	702	10100-012	33890	17531742	12	Miner*	32.00 504	0.07ypm	- TO, Marco	Internet		Unknown	247.58 499	248.58 491	240.0			0.000
H 28, 2018, 3122-61 MH	104	10120-0030-000		17131-0.204	0	when	5.32 (64	0.02 year	 Utilized States 	Distant.		Unterdent	249.22.09	211213-091	126.0	2		0.000
ter 26, 2018, 3102-65 am	1049	20.84 (8.85		17131-0.204		unknown	5.0180	0.02 years	Colorial Dates	Internet		Unknown	3/60/20 484	2/52/28 484	136.8	2		4.000



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.

	.iveAction [•] 🔤 🖤															• •					
te Mana	igement																				View Sites
Add	Edit Delete															Q. Sea	ch				
	SITE	•	DATA CENTER 🗘	DEVICES	\$ CONTAINS DEVICES	NO. OF EMPLOYEES	BUSINESS HOURS	•	IP RANGES O	4	E0 L00 0	ADDRESS		0	EGION		0	er been a	te 'AWS Or Ided	egon' has su	ccessfully ×
	Site		All v	Devices	Al v	No. of Employees	Business Hours		IP Ranges		Al v	Address			Region			Description		Tags	
	AWS Oregon			VPC 007	~		Mo - Fr 8:00 am - 5:0				1	Boardman,	OR, 97818	I I	loardma	, Oregon, I	Jn.,				

- 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.

	0.0 I / Mai		
СР	ip-172-31-2-234.us-west-2.compute.internal (172.31.2.234)	33710	52.218.160.10
СР	ip-172-31-4-228.us-west-2.compute.internal (172.31.4.228)	443	208.70.172.62
ГСР	ip-172-31-4-228.us-west-2.compute.internal (172.31.4.228)	443	208.70.172.62
ГСР	174.47.77.142	55393	ip-172-31-21-27.us-west-2.compute.internal (172.31.21.27)
ГСР	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)
ГСР	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)
ГСР	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)
CD.	(TO 10 10 10 10 10 10 10 10 10 10 10 10 10	7000	174 77 77 10

- 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.

Cloud Monitor	HOME	SETTINGS	
			-
Welcome to A	WS Cloud	Monitoring Ap	pl
Use LiveNX to monito	or and analyze	AWS cloud network, g	jet
Download the CSV a	nd import it as I	Non-SNMP devices in	y ç
Download CSV	Send to LiveN	IX	
If adding new reg poll Cloud Monitor HOME SETTINGS AWVS Cloud Monitoring Settings	jion after setup	, need to go back to se	ttings to include the region to
Mode		AWS Regions	
Production		US East (N. Virginia), US West (Orego	e)) =
LivefOt Server Live	whick Priorit	Select all	
172.31.21.27	055	US East (N. Wegewa)	
Log Directory		US West (N. California) ed.	ar you
itata/wenx-on/logs		() Canada (Central)	
LiveNX API Token		E EU (Frankfurt) E EU (Insland)	
7dallprp+5LQVJQDatrGR6JV/ZesHvgByoWF	MaultiC+	EU (London)	
		EU (Paris) EU (Stockholm)	
		Asia Pacific (Hong Kong)	
		Asia Pacific (Tokyo) Asia Pacific (Secur)	
		 Asia Pacific (Oseka-Local) 	
		Asia Pacific (Singapore)	
		Asia Pacific (Bythey) Asia Pacific (Mumbal)	
		III Middle East (Balvain)	
		South America (58o Paulo)	

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)

