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 Y																		4 €	÷ (0
Owned b	by me 👻 🔍 🗛	II ID : ami-01cc178f169cbb99	Ad 🖸 Ad	d filter													ØR	< 1	I to 1 of		н
Nan	me	- AMI Name	-	AMI ID	*	Source -	Owner	÷	Visibility	×	Status	¥	Creation Date	+	Platform	*	Root Device 1-	Virtua	lization	•	
Live	eNX 9.0.0 Server W	LiveNX Server 9.0.0/CM	APP	ami-01cc178f169cbb99	1	792068586670/	792068	86670	Private		available		December 19, 2019 at 11:57		Other Linux		ebs	hvm			

2. Select the instance type and click next.

aw	S Services ~	Resource Groups 🗸	*			Д ^е hр	rasath @ liveaction 👻 Oregon 🤊	▼ Support ▼
1. Choose	AMI 2. Choose Instance Ty	3. Configure Instance	4. Add Storage 5. /	Add Tags 6. Configure S	ecurity Group 7. Review			
Step 2 Amazon E0 give you th	: Choose an Inst 22 provides a wide selection e flexibility to choose the ap	tance Type of instance types optimize propriate mix of resources	to fit different use case for your applications. Let	es. Instances are virtual se arn more about instance ty	rvers that can run applications. The ypes and how they can meet your c	ey have varying combinations of CF computing needs.	PU, memory, storage, and networki	ng capacity, and
Filter by:	All instance types 👻	Current generation	 Show/Hide Colur 	nns				
Currently	/ selected: t2.large (Variable	e ECUs, 2 vCPUs, 2.3 GHz	z, Intel Broadwell E5-268	6v4, 8 GiB memory, EBS	only)			
	Family	~ Туре ~	vCPUs (i) -	Memory (GIB) ~	Instance Storage (GB) () -	EBS-Optimized Available (i) +	Network Performance (i) -	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
						Cancel Previous Revie	w and Launch Next: Configu	re Instance Details

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							
Step 3:	Configure Instan	ce De	tails													
Configure the	e instance to suit your require	ments. Yo	u can launch mu	ultiple instances f	rom the same AN	II, request	t Spol	t instances to take adv	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	р 🕕								
	Purchasing option		Request Spo	t instances												
	Network	()	vpic-etter (1998)	SilegsyLive®X		• 0	3 0	reate new VPC								
	Subnet		subriat automation 53 IP Addresses	iiii piisidie2 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.

<u> </u>	Service	es ∽ Resourc	e Groups 😽	*						4 •	hprasath @ liveaction 👻	Oregon 👻	Support 👻	
1. Choose AMI	2. Choose In	stance Type 3. Co	onfigure Instance	4. Add Storage	5. Add T	ags 6.	Configure Security Group	7. Review						
Step 4: Ad Your instance will edit the settings o storage options in	d Stora be launched of the root vol a Amazon EC	ge with the following s ume. You can also 2.	storage device settir attach additional EE	ngs. You can a 3S volumes af	attach additi ter launchin	onal EBS \ g an instar	volumes and instance sto ice, but not instance store	re volumes to yo e volumes. Lean	ur instance, or n more about					
Volume Type	j)	Device (j)	Snapshot (i)		Size (GiB)	1	Volume Type (j)		IOPS (j)	Throughput (MB/s) (i)	Delete on Termination (i)	Encryption	D	
Root		/dev/sda1	snap-0a98f58305f	fdbb578	20]	General Purpose SSD	(gp2) •	100 / 3000	N/A	2	Not Encrypted	•	_
EBS	٣	/dev/sdb *	Search (case-inse	ensit	50		General Purpose SSD	(gp2) •	150 / 3000	N/A	×	Not Encrypted	•	⊗
Add New Volum	ble customer	s can get up to 30 C	3B of EBS General	Purpose (SS	D) or Magne	tic storage	. Learn more about free	usage tier eligibi	lity and					

5. Add appropriate tags and Click next.

aws services Becourse Crowns 1		0			
		4	nprasatn @ liveaction	 Oregon < Suppo 	n v
1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage	e 8. 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	a tag with key = Name and value = Webserver. Ir Amazon EC2 resources.				
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 Securi	ty Group

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

	Security group name:	Select an existing sec	urity group		
	Description:	Allow LiveNX Server	and LiveNX-CM ports in SG		
/pe (i)	Proto	col (j	Port Range (i)	Source (i)	Description (i)
SH •	TCP		22	Custom • 0.0.0.0/0, ::/0	SSH from Public
TTP •	TCP		80	Custom • 0.0.0.0/0, ::/0	Web UI access - Redirect to HTTPS
ustom TCP F •	TCP		7000	Custom • 0.0.0.0/0, ::/0	Java Client Access
ustom TCP F •	TCP		8092	Custom • 0.0.0.0/0, ::/0	Java Web Client Launch (Deprycated)
ustom TCP F •	TCP		8093	Custom • 0.0.0.0/0, ::/0	API Access
ustom TCP F •	TCP		8443	Custom • 0.0.0.0/0, ::/0	LiveNX Admin
ustom TCP F •	TCP		9443	Custom • 0.0.0.0/0, ::/0	LiveNX-CM
ustom UDP I •	UDP		2055	Custom • 0.0.0.0/0, ::/0	NetFlow
ATTPS • Add Rule AWS Choose AMI	TCP Services ~ Resource	e Groups 🗸 🔭	443 J Storage 6. Add Tags 6. Configure S4	Custom • 0.0.0.00, ::10	Web UI - HTTPS Cancel Previous Review and L
Add Rule aws Choose AMI ecurty group is a instance, add	Services ~ Resource choose instance Type 3. Co figure Security Gr set of frewalt rules that contri uses that allow unrestricted are	e Groups v s Ingure Instance 4.Add OUD Uthe traffic for your inst ess to the HTTP and H	443 I Storage 5: Add Tags 6: Configure 54 Iance. On this page, you can add rules to a ITTPS ports. You can create a new security	Custom 0.0.0.00, :::0 curity droup 7. Review low specific traffic to reach your instance. For examproup or select from an existing one below. Learn in	Web UI - HTTPS Cancel Previous Review and L Image: A structure of the structure o
ATTPS • • • • • • • • • • • • • • • • • • •	Services ~ Resource Choose Instance Type 3.00 figure Security ta contri- ules that allow unrestricted acc Assign a security group: %	e Croups	443 I Storage 5: Add Tags 6: Configure 54 Iance. On this page, you can add rules to a TITPS pots. You can create a new security group	Custom	Web UI - HTTPS Cancel Previous Review and L Image: A structure of the structure o
Attres • • • • • • • • • • • • • • • • • • •	Services Resource Croose instance Type 3.00 figure Security Gr iset of firewait rules that contrive that allow instance that contrive astign a security group:	s Groups > tigure Instance 4. Ad- due traffic for your Inst ess to the HTTP and H4 Create a new security / Select an existing secu- Select an existing secu-	443 I Storage 6. Add Tags 6. Cenfigure 54 tance. On this page, you can add rules to a TTPPS ports. You can create a new security group urity group	Custom	Web UI - HTTPS Cancel Previous Review and L Q* hpraseth @ levesction * Oregon * Support cle, if you want to set up a web server and allow internet traffic to note about Amazon EC2 security groups. internet traffic to note about Amazon EC2 security groups.
ddd Rule	Services Resource Croose Instance Type 3. Co figure Security Gr set of frewait rules that alcour meta-ficted ac Assign a security group: Security group name Description:	Croups	443 I Storage 5. Add Tags 6. Configure 54 Iance. On this page, you can add rules to a TTPS ports. You can create a new security group unity group and LiveNX-CM ports in SG	Custom	Web UL - HTTPS Cancel Previous Review and L Image: Previous Review and L
ATTPS • • • • • • • • • • • • • • • • • • •	Services Resource Services Resource Services Security Gri Gigure Security Gri Security group Security S	Croups	443 J 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 group and LiveNX-CM ports in SG Port Range ()	Custom	Web UI - HTTPS Cancel Previous Review and L Image: Previous Previous Previous Previous Image: Previous Previous<
dd Rule dd Rule aws choose AM ap 6: Cor curvity group is instance, add a sha	Services Resource Choose Instance Type Security Gri Security group name Bescurity group name Description: TOP	Croups	443 3 Storage 5 Add Tags 6. Configure 54 tance. On this page, you can add rules to a ITTPS ports. You can create a new security group and LiveNX-CM ports in SG Port Range () 22	Custom	Web UI - HTTPS Cancel Previous Review and L A [®] hyrasath @ lovaction * Oregon * Support ple, if you want to set up a web server and allow internet traffic to nore about Amazon EC2 security groups. Description () leg. SSH for Admin Desktop
atter and a second at a second	Services Resource Croose Instance Type 3. Co figure Security Gr set of frewait rules that allow unrestricted ace Assign a security group: Gecurity group name: Description: Prote TCP	a Croups • • tigure Instance • A. Ads OUD all the traffic for your instance ass to the HTTP and HTTP and the security Select an existing second LivenX-CM Allow LivenX Server a col ①	443 i Storage 6. Add Tags 6. Configure Se tance. On this page, you can add rules to a tTTPS ports. You can create a new security urity group urity group and LiveNX-CM ports in SG Port Range () 22	Custom	Web UI - HTTPS Cancel Previous Review and L A* hpraseth @ lovaction * Oregon * Support ble, if you want to set up a web server and allow internet traffic to tore about Amazon EG2 security groups. Description () e.g. SSH for Admin Desktop
dd Rule dd Rul	Services Resource Choose Instance Type 3.00 figure Security Gri set of firewail rules that contrives that advort unrestricted ac Assign a security group: Becurity group name: Description: TCP	Croups	443 I Storage 5. Add Tags 6. Configure 54 I ance. On this page, you can add rules to a TTPS ports. You can create a new security group urity group and LiveNX-CM ports in SG Port Range () 22	Custom	Web UI - HTTPS Cancel Previous Review and L Image: Cancel Previous Image: Cancel Image: Cance

- **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.

ġ	aws	Services	∽ Reso	urce Groups 😽	*					↓ hprasath @ liveaction	• Oregon •	• Support •
1. Cho	ose AMI	2. Choose Inst	ance Type 3	8. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review				
Step Please	7: Re	view Ins r instance lau	tance La nch details. Yo	aunch ou can go back to	edit changes for each s	ection. Click L	aunch to assign a key pair	to your instance a	Ind complete the launch pr	ocess.		
•	Your in You ca	ove your ins istances may l in also open a	stances' ser be accessible : dditional ports	curity. Your se from any IP addre in your security g	curity group, Livel ss. We recommend that roup to facilitate access	NX-CM, is on the sto the application of the store of the	open to the world. rour security group rules to a tion or service you're runnir	allow access from ng, e.g., HTTP (80	known IP addresses only.)) for web servers. Edit sec	urity groups		
▼ AN	II Detail	S										Edit AMI
	∆ [C R	ari LiveNX-C opied ami-030 ot Device Type: e	M - ami-0783 a2d8cc88816b0 bs Virtualizatio	3 b6ef205362154 19 from us-east-2] [n type: hvm	an LiveNX Server							
Ins	stance T	уре									E	dit instance type
1	nstance T	ype	ECUs	vCPUs	Memory (GiB)	Instance	Storage (GB)	EBS-Optimize	d Available	Network Performance		
t	2.large		Variable	2	8	EBS only		-		Low to Moderate		
▼ Se	curity G	roups									Edit	security groups
Se	curity aro	up name	LiveNX-0	M								
	, ,										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	
hadiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	*

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-vpo-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 ()
A AND RESIDENT	After 1 days from object creation
	Permanently delete previous versions ()
Lifecycle rule Applied to	After 1 days from becoming a previous version
Soulogarge Whole backet	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

Enable AWS VPC Flow Log

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

aws Service	s - Resource Groups - 5			💭 * hprasath @ horaction + Oregon +	Support =
VPC Dashboard Finer by VPC: Q, Select a VPC	Create VNC Actions * Q, Filter by tags and attributes or search by keyword			K < 1	• • •
Virtual Private	Name -	VPC ID * State ·	IPv4 CIDR IPv6 CIDR	DHCP options set	Main Route
Cloud	Management	vpc-0104060 available	172.31.0.016 .	dopt-e7c2d85	rtb-d0200abr
Your VPCs	Etspel/velit	vpo-elacilidita avalable	172.22.0.016	dopt-35e83f50	10-4361602
Noute Tables Internet Gateways Egness Only Internet Gateways DHCPP Options Sens Elantic IPs Elantic IPs Encipoints Encipoint Services					
NAT Gateways Peering Connections	VPC: spc.00ba1366 Description CIDR Blocks Flow Logs	Taga			
Network ACLa	VPC ID spc-0364506		Tenancy defa	ut.	
Security Groups	Pv4 CDR 172 31.0 016		Classic link Disc	Died Died	

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

VPC: vpc-03ba4366								E	
Description	CIDR Blocks	Flow Logs	Tags						
You can create flow Create flow log	ogs on your reso Actions ¥	urces to capture IF	P traffic flow information	on for the network inter	faces for your resources. Les	arn more			
							к <	None found >	>
Flow Log ID	۰ °	Filter	 Destination ty - 	Destination name	 IAM Role Arm 		Creation Time		
				You do not have any	y Flow Logs in this region				

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

aws services - Re	source Groups 🚽 🖌			۵.	hprassith (i) location: τ	Oregon +	Support +
VPCs > Create flow log							
Create flow log							
Flow logs can capture IP traffic flow inform	ation for the network interfaces associated with your r	HOUTOR	s. You can create multiple subscriptions to send traffic to different de	estinatio	s. Learn more		
Resources Filter* Destination Destination log proop* IAM role*	All All All All Accept Depend And Accept Depend And No IAMI role selected The IAMI role must have permission to publish to the	• c	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0				
* Required					Cascal Create		

For Max Aggregation Interval:

VPCs >	Create flow log			
Crea	te flow log			
Flow log	s can capture IP traffic flow inform Resources	nation for the network interfaces associated with your vpc-876990e0	resourc	es. You can create mult
	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 service	s 🗸 Resource Groups 🖌 🖌		A* hprasath @ liveaction	* Global * Support *
Amazon S3	Archive all your long-term data into Amazon \$3 Glacier Deep Archive			Documentation
Buckets 4	S3 buckets		deser-om-textings	×
	Q. Search for buckets		Copy Buchet AVIN	
Block public access (account settings)	Create bucket Edit public access settings Empty Delete		Properties Event	Active notifications
Easture scotlight	Bucket name	Access 0 •	Mi A delete	Disabled
	🗌 🕱 heljolisederedariaet	Bucket and objects not	Logging Static web honling	p Disabled p Disabled
	5 8 amaana 8	Bucket and objects not	Tag Requester pays	s Disabled
	🗋 📱 dezzionikiwanismen	0.00	Object look Transfer acceleration	k Disabled
	B Importante and additional and an additional and a second and a se	Objects can be public		
	. Strasslut	Objects can be public	Owner Block public access	r Iveactionrocks
	🗌 📱 investigatetteringitationprocept	Objects can be public	Bucket policy	Yes
	🗋 🖉 Sumetina antisaturphanturphat	Objects can be public	CORS configuration	1 No
	B Promiseda	0.00		
	C S Invertion Section	Objects can be public	Lilecycle Lilecycle	Enabled

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

aws serv	vices - Re	source Groups 🚽 🔹				۵.	Ingreseth () Investion +	Oregon +	Support +
Create flow lo	og								
Flow logs can capture IP t	traffic flow inform	ation for the network interfaces associate	I with your resources. Yo	u can create multiple sub	scriptions to send traffic to different (destination	s. Learn more		
	Resources	vpc-038a4366 0							
	Filter*	Al	- C 0						
_	Destination	 Send to CoudWatch Logs 0 Send to an 53 bucket 							
s	3 bucket ARN*	amavss3-iffimiuuiumpi	0						
Please note, a resour	rce-based policy r	will be created for you and attached to the	target bucket.						
Log record format									
	Format	ANS default format Custom format							
,	format preview	S(version) S(account-id) S(interface-id) S(arcaddr) \$(dstaddr) \$(arc	port) \$(dstport) \$(protoco	\$ packets \$(byles) \$(start) \$(end)	\$(action)	\$[og-status]		
* Required							Cancel		

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

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

≡ Liv	e∧ction⁻	NX UX		New Features!	A 0	0	• 0	🌲 0	{-} •	0 -	۰.4
API Token									API Docu		
			API TOKEN	Remove	Tate				API Toke	n Managem	ent

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	
Settings are not configured. Please ensure all required parameters are defined property. × Welcome to AWS Cloud Monitoring 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 CDV and import it as Non-DRMP devices in your Likel/V application.	
Countrast CDV Band to Lunkty	

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.

In the monitor	HOME	SETTINGS	ABOUT
WS Cloud Man	itaring C	ottings	
WS Cloud Mon	illioning a	settings	
AWS Regions			Batch Size
US East (N. Virginia)), US West ((Oregon) +	100
AWS Access Key			LiveNX Server
AWWKIBBAOJZ44U	JUKVBJJ		LiveNX Server
AWS Secret Enter if re	no secret confi	lgured or you wa	nt to change. LiveNX Port
			2055
FlowLog S3 Bucket	Example: s3-	bucket-name	LiveNX API Token
monitor-vpc-flowlog			7da8p3asdfasdfyeyeyrtdghusHvql8yoWP41wJH0=



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! A 0 B 0 4	• 0 🔔 0	{-} •	0 -	¢ -
API Token			API Docu		
	API TOKEN		API Toke	n Manageme	nt
	Remove				

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

Cloud Monitor HOME	SETTINGS	
AWS Cloud Monitoring	n Settings	
Arro oloud montoning	, ootango	
Mode		AWS Regions
Production		 US East (N. Virginia), US East (Ohio) -
LiveNX Server	LiveNX Port	AWS Access Key
172.22.0.73	2055	Annouse and Account ACD
Log Directory		AWS Secret Enter if no secret configured or you want to change.
/data/livenx-cm/logs		
LiveNX API Token		FlowLog \$3 Bucket
		and an and a state of the state

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 →→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→	
Cloud Monitor HOME SETTINGS	51199-119-1443 says
	Do you want to enable polling?
AWS Cloud Monitoring Settings	OK Cancel
Edit Enable Polling	
Polling: Disabled	
Mode: production	
AWS Access Key: AKIA3@httlsSXOCSM7JFD	
AWS Regions: US West (Oregon)	
FlowLog \$3 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.

Search Description (alter all	tenshaha (si	k - Orașe) k	on Alfred	an - seber ner	ang														
Time .	Protocal	SHIP AND	ScPet	Dri IP AND	Det Parts	Application	Scilute .	Packet Rate	Src Gewithy	5159	Del Ceurtry	Det She	File Ceate Time	flow the Take	1-3ym	In Packets	101/1ap	910909	i.
ev 26, 2018, 2122-03484	upe	198.58 (05.40)	109	175312-00	50944	rep ⁴	1247304	4-62 years		Internet		Unknown	241.0144	2415844	35.8			+ (H)	j.
ev 26, 2018, 3102-43 MP	100	179.31.7.13	10044	198-38-105-62	123	197	1247304	0.02 year		Unknown		(historie)	240.00 69	2413849	25.0			0.000	1
No. 28, 2018, 3112-H MH	10*	02317-03	22	185-232477	10080	107	306.27 bps	0.18 ppm		Unknown.		Internet	247.08 89	2-40-58 404	248	14		0.040	
No. 26, 2018, 2112-14 Apr	70*	10523247.7	50080	17531748	22	100 F	205-80 bps	0.00 ppm		internet.		Unknown	2-47:58 401	2-48-58-494	218	11		+ (H)	i.
No. 26, 2018, 2012-44 Apr	707	107062-010	23890	17531742	12	Minut*	3209 504	0.07/www.	- TO, Monto	(manual)		(primperty)	247.58 491	248.58 491	2408			0.000	i.
NY 28, 2018, 31(2-6) MM	10#	10120-0030-000		17131-00204	0	wanter	8.30 804	0.02 year	K visioniel States	(internet)		(planet)	249.31 69	211213-091	126.0	2		0.000	i.
Inter 26, 2018, 3152-45 AM	1049	20.84 (8.85)		17131-0.004		unknown	5.24304	0.02 years	COUNTRAL States	Drivenet		Unknown	3/80/20 484	2/52/28 484	126.8	2		4.943	i.



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.

≡	Li	veAction [.] 📧 💷							[New Features! A 0	• •	• 0 🐥	o {-} -	· 0-	۰۰	🛔 admin -
Site M	anage	ement														View Sites
Add	1	Edit Delete										Q Search.				
		NTE Ŷ	DATA CENTER 🗘	DEVICES 0	CONTAINS DEVICES	NO. OF EMPLOYEES	BUSINESS HOURS	IP RANGES	GEO LOC 🗘	ADDRESS C	REGION	0	er Dr	ur site 'AWS C en added	regon' has suc	cessfully ×
		Site	Al v	Devices	Al v	No. of Employees	Business Hours	IP Ranges	Al v	Address	Region		Descript	ion	Tags	
	1	AWS Gregon		VPC 007	~		Mo - Fr 8:00 am - 5:0		1	Boardman, OR, 97818,	Boardma	n, Oregon, Un				

- 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 x , mai	0.0.0.0	
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)
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)
TCD.	(C. 17) 14 15 17 16 16 16 16 16 16 16 16 16 16 16 16 16	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	I Monitoring App	I
Use LiveNX to monit	or and analyze	AWS cloud network, ge	t
Download the CSV a	ind import it as	Non-SNMP devices in y	ic .
Download CSV	Send to Live	vх	
Adding new region.			
If adding new region. If adding new region. Coul Montor HOME SETTINGS	gion after setur	o, need to go back to sett	ings to include the region to
Adding new region. If adding new re poll Coud Montor How Settings Mass	gion after setur	o, need to go back to sett	ings to include the region to
Adding new region. If adding new region. If adding new region. Coud Montor Rose Retings Mode Protector	gion after setur	o, need to go back to sett	ings to include the region to
Adding new region. If adding new region. If adding new region. Coud Montor HOM Settings Mode Production Linetal Lenver Li	gion after setur	o, need to go back to sett Arti Regions	ings to include the region to
Adding new region. If adding new region. Coud Montor HOME BETTINGS Mode Protection Linetic terver IT2.31.21.27	gion after setur	o, need to go back to sett	ings to include the region to
Adding new region. If adding new region. If adding new region. Coud Montor 1000 actives AWS Cloud Monitoring Settings Mode Protector Linetic terver Li	gion after setur	o, need to go back to sett Avis Regions Avis Calculated Visions Control of Calculated Visi	ings to include the region to
Adding new region. If adding new region. If adding new region. Coud Montor HOM DETTINGS Mode Production United terver If 23: 21: 27 Lag Directory Italitems contage	gion after setur	AWS Regions AWS Regions US East (N. Vrgma), US West (Oregon) US East (N. Vrgma), US West (Oregon) US East (Oregon) C US Vest (N. Castoma) C US Vest (Castoma) C US Vest (C	ings to include the region to
Adding new region. If adding new region. Coul Montor HOME Settings Mode Protection Linetic Terver Linetic Te	gion after setur	ANSE Regions AN	ings to include the region to
Adding new region. If adding new region. Coul Montor HOME BETTHOS Mode Protection Livetic terver Light ter	gion after setup	o, need to go back to sett AVS Regions	ings to include the region to
Adding new region. If adding new region. Could Monitor HOME SETTINGS AWS Cloud Monitoring Settings Mode Protector United terver United ter	gion after setur	Avia Regions Avia Regions US East (N. Virginal, US Viest (Oregon) US East (N. Virginal, US Viest (Oregon) US Viest (Compos) US Viest (Co	ings to include the region to
Adding new region. If adding new region. If adding new region. Coul Montor HOM DETTINGS Mode Protection LivetX terver Lig Directory LivetX terver LivetX	gion after setur	AWS Regions AWS Regions US East (N Vrgma), US West (Dregor) Seriest all G US East (N Vrgma), US West (Dregor) G US East (Dreg) G US Vest (Cocool G U (Frankfur) G U (F	ings to include the region to
Adding new region. If adding new region. If adding new region. Coul Montor HOME BETTHOS AWS Cloud Monitoring Settings Mode Protection LiterAt terver L	gion after setur	AVS Regions AVS Regions AVS Regions AVS Regions CUS East (N. Vrgmas, US West (Dregor) Galaxy CUS East (N. Vrgmas, US West (Dregor) Galaxy CUS East (N. Vrgmas, US West (Dregor) CUS East (N. Caltonia) CU (Plantar) CU (P	ings to include the region to
Adding new region. If adding new region. If adding new region. Cloud Monitor HOME BETTINGS Mode Protection Linetic terver Linetic terver Linetic terver Linetic API Taken Tatiopo-5. CV/JCCamOR6./Advertingted	gion after setur	AVS Regions * US East (N. Vrgmal, US West (Oregon) * Select all * US East (N. Vrgmal, US West (Oregon) * Select all * US East (N. Vrgmal, US West (Oregon) * * US East (Ches) US West (N. California) * US (US Cast (Ches) * US (Cast (Ches) * US (Ca	ings to include the region to
Adding new region. If adding new region. If adding new region. Courd Monitor 14040 BETTAKE AWS Cloud Monitoring Settings AWS Cloud Monitoring Settings Mode Protocon United Terme United Terme United Terme United Terme Testings LiveAX API Terme Testings-S. CV.200mCRBU/M2minupyer	gion after setur	AWS Regions AWS Regions US East (N. Vryma), US West (Dregor) US East (N. Vryma), US West (Dregor) US East (Dreg US East (Dreg) US Vest (N. Cathona) US Vest (N. Cathona) US Vest (N. Cathona) US Vest (Dregor) Aua Pactic (Dregor) Aua	ings to include the region to
Adding new region. If adding new region. If adding new region. Courd Montor HOM DETTINGS Mode Production LivetX terver LivetX tervex LivetX tervex LivetX terver LivetX tervex Livet	gion after setur	AWS Regions AWS Regions US East (N. Vrgma), US West (Dregor) Select all G US East (N. Vrgma), US West (Dregor) G US East (Dreg) G US Vest (Catomic) G U (FixekTur) G U	ings to include the region to

Troubleshooting

AWS Permission

- EC2 Access
- VPC Access
- CloudWatch Logs

IAM Roles

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

Sample AWS Design – LiveNX Cloud Deployment (Draft)

