

Flowmon Virtual Appliances

- Flowmon for VMware
 - VMware Dedicated Port Monitoring
 - VMware vSwitch Monitoring
 - VMware Distributed vSwitch Monitoring
- Flowmon for KVM
 - KVM Open vSwitch Port Mirroring
- Flowmon for Hyper-V
 - Hyper-V Network Interface Mirroring
 - Hyper-V Virtual Switch Port Monitoring
- Flowmon for AWS
 - Amazon VPC Traffic Mirroring
 - Amazon VPC Flow Logs
- Flowmon for Azure
 - Azure Virtual Network TAP
 - Azure NSG Flow Logs v2
- Flowmon for Google Cloud
 - Google Cloud VPC Packet Mirroring
 - Google Cloud VPC Flow Logs
- Post-installation Steps
- 3rd-party Packet Brokers
 - Garland Prisms
 - Ixia CloudLens
 - Gigamon

A virtual appliance is a pre-configured virtual machine image, ready to run on a hypervisor or in the cloud. Virtual appliances are intended to eliminate the installation, configuration and maintenance costs associated with running complex stacks of software in heterogeneous environments.

Flowmon Networks provide a number of virtual appliances intended to simplify the deployment of Flowmon in onpremise virtualization platforms and public cloud environments. The following guide provides

- a description of types of appliances available to partners and customers,
- a list of supported platforms and environments,
- a set of step by step manuals for deploying Flowmon appliances in aforementioned platforms and environments.

For additional assistance, please contact Flowmon Support.

Virtual Appliance Types

Flowmon Probe

The Flowmon Probe appliance provides the functionality of a Flowmon Probe without the built-in Flowmon Collector. It is optimized for deployment in supported platforms listed below.

This specialized appliance enables cost-effective network traffic monitoring and flow data export in deployments with multiple Flowmon Probe instances and at least one Flowmon Collector instance. An additional Flowmon Collector instance, virtual or hardware-based, is <u>required</u> for flow data collection and analysis.

For the list of available models, refer to the Flowmon Probe Models List document.



Flowmon Collector

The Flowmon Collector appliance provides the functionality of a Flowmon Collector with a built-in Flowmon Probe. It is optimized for deployment in supported platforms listed below.

This combination enables flow data collection and network traffic monitoring <u>without the necessity for deploying</u> <u>additional appliances</u>.

For the list of available models, refer to the Flowmon Collector Models List document.



Overview

Flowmon for VMware gives network administrators and security engineers insight into what is happening in their infrastructure. Its powerful features can be used to gain control of bandwidth utilization, optimize network and application performance, reduce time to resolution during troubleshooting and keep the infrastructure protected against modern cyber-security threats.

Flowmon for VMware is

- a virtual appliance intended for the VMware environment,
- capable of collecting as well as generating flow data,
- fully under customer's control including updates, backups, and configuration.

Flowmon for VMware supports

- IPFIX, NetFlow v5/v9 or sFlow data collection from Flowmon Probes or other compatible devices (e.g., customer routers),
- ingestion of Amazon VPC Flow Logs from AWS,
- traffic monitoring on local vSwitches,
- traffic monitoring on local dedicated physical interfaces,
- 3rd-party packet brokers such as Garland Prisms, Ixia CloudLens, or Gigamon,
- ERSPAN/GRE traffic mirroring.

This guide describes the deployment procedure of Flowmon for VMware using an OVF template with a default storage capacity of 40 GB. The storage capacity can be later changed to match the purchased license.

Features

Flowmon for VMware supports three modes of operation

- Probe,
- Collector,
- Collector and Probe.

Flowmon Probe

In this mode, the virtual appliance acts as a Flowmon Probe. It accepts mirrored traffic on monitoring ports and exports flow data to at least one remote Flowmon Collector instance.

Supported traffic mirroring solutions:

- VMware vSwitch Monitoring
- VMware Distributed vSwitch Monitoring
- VMware Dedicated Port Monitoring

Supported 3rd-party packet brokers:

- Ixia CloudLens
- Gigamon
- Garland Prisms

- Features
- Licensing
- Prerequisites
- Deployment
- Virtual Disks
- Flowmon Configuration



Flowmon Collector

In this mode, the virtual appliance acts as a Flowmon Collector and accepts supported flow formats from external probes, network devices, or Amazon VPC Flow Logs on management ports. For details on supported flow sources and formats, refer to the official Flowmon User Guide.

Flowmon Collector and Flowmon Probe

In this mode, the virtual appliance acts both as a Flowmon Probe and Flowmon Collector. Probe sends data to the locally available Collector. For details on configuration, refer to the official Flowmon User Guide.

Licensing

Flowmon for VMware is a virtual appliance using the Bring-Your-Own-License (BYOL) licensing model.

With <u>BYOL</u>, you can apply for a Free Trial License at flowmon.com.

For support or inquiries, see our contact information.

Prerequisites

In order to follow this guide, you need the following:

- 1. VMware ESXi 5.5 or newer and VMware vSphere (demonstrated on vSphere v6.7).
- Flowmon for VMware downloaded from the Partner Portal, archives for download are located in Downloads / Products / Flowmon Virtual Appliances & Cloud / Flowmon for VMware. Unless directed otherwise, pick the latest stable version with the desired set of modules.
- 3. A valid Flowmon license or a trial license from flowmon.com.

Deployment

The deployment of Flowmon for VMware consists of the following steps:

- 1. Decompress the downloaded zip file containing all the files necessary for installation.
- 2. In your vSphere Client in the VMs and Templates tab, right click on your Datacenter and click on Deploy OVF Template.





3. Select all the files from the downloaded and decompressed zip archive, **.mk**, **.ovf** and **.vmdk**, and click on the **Next** button.

Deploy OVF Template

1 Select an OVF template	Select an OVF template
2 Select a name and folder	Select an OVF template from remote URL or local file system
3 Select a compute resource 4 Review details 5 Select storage	Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
- · · · · · · · · · · · · · · · · · · ·	URL http://remoteserver-address/filetodeploy.ovf .ova
	Local file Choose Files 4 files Flowmon Collector Virtual.mf Flowmon Collector Virtual.ovf Flowmon_Collector_Virtual-disk-0.vmdk
	Flowmon_Collector_Virtual-disk-1.vmdk CANCEL BACK NEXT

4. Enter a Virtual machine name and select a Location for your new virtual appliance and click on the Next button.



Deploy OVF Template

6 Ready to complete



- > 📋 Flowmon Development Cluster
- > 📋 QA Cluster

Compatibility





6. **Review details** and click on the **Next** button.

Deploy OVF Template

- ✓ 1 Select an OVF template Review details
- 2 Select a name and folder
- Verify the template details.
- ✓ 3 Select a compute resource

4 Review details

- 5 Select storage
- 6 Select networks
- 7 Ready to complete

Publisher	No certificate present
Product	Flowmon Collector Virtual.ovf
Version	10.00.02
Vendor	Flowmon Networks, a.s.
Description	Flowmon Collector Virtual.ovf v10.00.02
Download size	9.1 GB
Size on disk	Unknown (thin provisioned)
	48.0 GB (thick provisioned)

CANCEL



ВАСК

7. Select storage in which you want to store the configuration and disk files. After that, select Thin provisioning or Thick provisioning according to your preferences and click on the Next button.



Deploy OVF Template

I Select all OVP template	Select storage				
2 Select a name and folder	Select the datastore in which to	store the config	guration and disk f	iles	
3 Select a compute resource 4 Review details	Encrypt this virtual machine	(No encryption	policies available)		
5 Select storage 6 Select networks	Select virtual disk format:	Thin Prov	_ اس		
7 Ready to complete	VM Storage Policy:	~	\triangle	\bigcirc	
	Name	Capacity	Provisioned	Free	
	🗐 110 - Datastore 1 (no RAID)	458.25 GB	2.12 GB	456.13 GB	
	🗐 110 - Datastore 2 (no RAI	463.5 GB	977 MB	462.55 GB	
	🧐 117 - Datastore	923.5 GB	83.2 GB	849.7 GB	
	🗐 118 - Datastore	923.5 GB	487.2 GB	652.48 GB	
	datastore1	923.5 GB	976 MB	922.55 GE	
	datastore1 (1)	923.5 GB	976 MB	922.55 GE	
	🗐 Kamzık 1 - Shared ISCSI	4.32 TB	5.59 TB	953.08 GB	
	🗐 Kamzik 2 - Shared ISCSI	8.69 TB	12.49 TB	1.22 TB	
	4				
	Compatibility				
	✓ Compatibility checks succe	eded.			

8. Select networks to be used by the virtual appliance. Management ports are used for access to the web interface. Connect them to your LAN. Then click on the Next button.

CANCEL

BACK

NEXT



Deploy OVF Template

1 Select an OVF template2 Select a name and folder	Select networks Select a destination network for	each sou	urce network.		
3 Select a compute resource4 Review details	Source Network	Τ	Destination Network	Ŧ	
✓ 5 Select storage	Monitor port 2		Monitor port 2	\sim	*
6 Select networks 7 Ready to complete	Monitor port 1	Monitor port 1		~	
	Management Port 2		Management DPort Static VLAN 4	~	
	Management Port 1		Management DPort DHCP VLAN 5	0 ~	-
				4 item	ns
	IP Allocation Settings	St	tatic - Manual		
	IP protocol:	IP	₩4		
			CANCEL BACK	N	EXT,

9. Review all the information and click on the **Finish** button to start the deployment process. It may take several minutes.

Deploy OVF Template

ad size disk ce	9.1 GB Unknown Flowmon Networks Development Flowmon Development Cluster
disk ce	Unknown Flowmon Networks Development Flowmon Development Cluster
ce	Flowmon Networks Development Flowmon Development Cluster
ce	Flowmon Development Cluster
e mapping	1
lisks	Datastore: Kamzik 2 - Shared iSCSI Datastore; Format: Thin provision
k mapping	4
itor port 2	Monitor port 2
itor port 1	Monitor port 1
agement 2	Management DPort Static VLAN 4
	isks k mapping itor port 2 itor port 1 agement 2

10. Find the newly created Flowmon virtual appliance and click on **Power On** in the **Actions / Power** menu. Wait for the appliance to start.

Flowmor	Collector	10.0.2 Virt	ual	ACTIONS 🗸	_		
Monitor	Configure	Dermissions	Datasta	Actions - DJ - Flowmon Collector 10			
Monitor	Conligure	Permissions	Datasto	Power	·	' Power On ၂ၮ	
	Guest OS: Compatibility:	CentOS 4/5 or la ESX/ESXi 4.0 an	ter (64-bit) d later (VM	Guest OS	•	Power Off	
red Off	VMware Tools:	Not running, vers More info	sion:21474	Snapshots	•	Suspend	
	DNS Name:			🛃 Open Remote Console	6	Reset	
Console	IP Addresses: Host:	192.168.3.108		🖶 Migrate		Shut Down Guest OS	
ote Console 🧃	▶ 👃			Clone		Restart Guest OS	
					-		

Virtual Disks

Once the new instance is running, you may provision additional data storage. After attaching an additional disk following this guide, refer to Post-installation Steps / Data Storage to activate it.

To attach an additional/replacement disk for data, you have to:

1. Open the **vSphere Client**, select your Flowmon instance, click on **Actions** and choose **Edit settings**.

🖡 OK - Flowmon	10.01.06			ACTIONS -
Summary Monitor	Configure	Permissions	Datastores	Actions - OK - Flowmon 10.01.06 - n
Powered On aunch Web Console aunch Remote Console	Guest OS: Compatibility: VMware Tools: DNS Name: IP Addresses: Host:	CentOS 7 (64-bit ESX/ESXi 4.0 and Running, version: More info localhost 192.168.51.107 View all 3 IP add 192.168.3.119) d later (VM version 10336 (Guest Mana resses	Guest OS Snapshots Open Remote Console Migrate Clone Fault Tolerance
VM Hardware				VM Policies
Cluster				🔂 Edit Settings
Host		ua Piov	168.3.119	Move to folder
Networks		쓰 Man ⑨ Mon ⑨ Mon ▲ VM	agement DPort DH itor port 1 itor port 2 Monitor DPort	Edit Notes Tags & Custom Attributes
Storage				Remove from Inventory
				Delete from Disk



2. Click on the Add New Device button to add a new Hard Disk.

			ADD NEW DE
> CPU	4 v		CD/DVD Drive
> Memory	8	GB 🗸	Hard Disk
> Hard disk 1	27	GB 🗸	RDM Disk Existing Hard Disk
> Hard disk 2	40	GB 🗸	Network Adapter
> SCSI controller 0	LSI Logic P	arallel	USB Controller
> Network adapter 1	Managem	ent DPort DHCP VL. ~	SATA Controller NVMe Controller
> Network adapter 2	VM Monito	or DPort V	PCI Device
> Network adapter 3	Monitor p	ort1 v	Connected
> Network adapter 4	Monitor p	ort 2 🗸	Connected
> CD/DVD drive 1	Client Dev	vice v	
> Video card	Specify cu	ustom settings 🗸	
VMCI device	Device on t	the virtual machine PCI bus th	nat provides support for the

CANCEL O



3. Set disk size.

		ADD NEW DEVICE				
CPU	4 ~	0				
Memory	8 GB 🗸					
Hard disk 1	27 GB 🗸					
Hard disk 2	40 GB 🗸					
New Hard disk *	400 <u>GB</u> ~	_				
SCSI controller 0	LSI Logic Parallel					
Network adapter 1	Management DPort DHCP	VL ~ Connected				
Network adapter 2	VM Monitor DPort 🗸	Connected				
Network adapter 3	Monitor port 1 ∨	Connected				
Network adapter 4	Monitor port 2 🗸	Connected				
CD/DVD drive 1	Client Device ~					
Video card	Specify custom settings 🗸	Specify custom settings 🗸				
VMCI device	Device on the virtual machir	Device on the virtual machine PCI bus that provides support for the				

CANCEL OK

4. Check settings, click on the **OK** button.

Flowmon Configuration

Please refer to Post-installation Steps.



VMware Dedicated Port Monitoring

Overview

Flowmon for VMware has the ability to monitor traffic and generate NetFlow / IPFIX flow data. To enable this functionality for the monitoring of an external source connected to a physical port of the VMware host, please follow the steps outlined below.

- Prerequisites
 - A running instance of Flowmon for VMware Flowmon Collector (with a built-in Probe) or Flowmon Probe.
 - An external source of network traffic connected to a physical network interface of the VMware host.

Deployment

Setting up dedicated port monitoring is done by assigning a specific physical interface to a virtual switch and connecting Flowmon's monitoring interface to the same virtual switch.

1. In the vSphere client, click on the IP address of a VMware host. Then click on the **Configure** tab, select **Virtual switches** and click on **Add Networking**.

vm vSphere Client	Menu 🗸 🛛 🔍 Search		C @~
	192.168.3.120	Actions ¥	
× @	Summary Monitor	Configure Permissions VMs Datastores Networks Updates	
Flowmon Networks D Flowmon Develop	Storage Storage Adapters	Virtual switches	
192.168.3.102	Storage Devices	😥 Add Networking 😡 Refresh	
192.168.3.103	Host Cache Configur	Switch y Discovered Issues	
192.168.3.110	Protocol Endpoints	DSwitch - Monitoring	
192.168.3.117	I/O Filters	DSwitch - Management	
192.168.3.118	 Networking 	- T vSwitch0	
192.168.3.119	Virtual switches		
192.168.3.120	VMkernel adapters	TT vSwitch1 -	
🕞 ADS - Demo - 10	Physical adapters		
🔂 ADS - Demo - 11	TCP/IP configuration		
🐴 ADS - Demo - 9	 Virtual Machines 		
🗄 ADS-9.5	VM Startup/Shutdo	No items selected	
📅 Anet - lokalizace	Agent VM Settings		
APM DB ris	Default VM Compati		
APM DEVEL	Swap File Location		
APM devel - old	▼ System		

- Overview
- Prerequisites
- Deployment
- Flowmon Configuration



2. Select Virtual Machine Port Group for a Standard Switch and click on the Next button.

1 Select connection type 2 Select target device 3 Connection settings	Select connection type Select a connection type to create.
4 Ready to complete	◯ VMkernel Network Adapter
	The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN and host management.
	Virtual Machine Port Group for a Standard Switch
	A port group handles the virtual machine traffic on standard switch.
	O Physical Network Adapter
	A physical network adapter handles the network traffic to other hosts on the network.
	CANCEL BACK NEX
lect New standard switch	and click on the Next button.
192.168.3.120 - Add I	Networking
 1 Select connection type 2 Select target device 	Select target device Select a target device for the new connection.
4 Connection settings 5 Ready to complete	○ Select an existing standard switch
	BROWSE
	New standard switch

MTU (Bytes)

CANCEL васк .



4. Click on the **Plus** button.

 ✓ 1 Select connection type ✓ 2 Select target device 	Create a Standard Switch Assign free physical network adapters to the new switch.					
3 Create a Standard Switch 4 Connection settings 5 Ready to complete	Assigned adapters	Select a physical network adapte list to view its details.	r from the			
		CANCEL	KNEXT			
ect the Physical Adapter	you want to add to the switch	and click on the OK button.				
A dd Dhyraiad A da	ntara ta tha Cuvitah					

Network Adapters	All Properties CDP	LLDP
pi vmnic2 ▲	Adapter Name Location Driver	Intel Corporation Ethernet Server Adapter I350-T4 vmnic2 PCI 0000:af:00.0 igbn
	Status Status Actual speed, Duplex Configured speed, Duplex Networks	Disconnected Down Auto negotiate No networks
	Network I/O Control Status	Allowed
	Status Cisco Discovery Protocol	Disabled
Ŧ	 Cisco Discovery Protocol Link Layer Discovery Protocol Link Layer Discovery Prot 	is not available on this physical network adapter
		CANCEL

5.



6. Click on the **Next** button.

3 Create a Standard Switch4 Connection settings5 Ready to complete	Assigned adapters		
5 Ready to complete		All Properties CDP	LLDP
	+ X 🛧 🖡	Adapter	Intel Corporation E
	Active adapters	Name	vmnic2
	飅 (New) vmnic2	Location Driver	PCI 0000:af:00.0 igbn
	Standby adapters	Status	
	Unused adapters	Status	Disconnected
		Actual speed, Duplex Configured speed, Duplex	Down Auto negotiate
		Networks	No networks
		Network I/O Control	Allowed
		CD IOV	Allowed
		Status	Disabled
		Cisco Discovery Protocol	
a Network label , select 92.168.3.120 - Add N	the VLAN ID as All (4095) a Vetworking	nd click on the Next button	
a Network label , select 92.168.3.120 - Add N • 1 Select connection type • 2 Select target device	the VLAN ID as All (4095) a Networking Connection settings Use network labels to identify m	nd click on the Next button	mmon to two or more
a Network label, select 32.168.3.120 - Add N 1 Select connection type 2 Select target device 3 Create a Standard Switch 4 Connection settings	the VLAN ID as All (4095) an NetWorking Connection settings Use network labels to identify m hosts.	nd click on the Next button	
a Network label, select 22.168.3.120 - Add N 1 Select connection type 2 Select target device 3 Create a Standard Switch 4 Connection settings 5 Ready to complete	the VLAN ID as All (4095) and Networking Connection settings Use network labels to identify m hosts.	nd click on the Next button	mmon to two or more



8. Review settings and click on the **Finish** button.

 1 Select connection type 2 Select target device 	Ready to complete Review your settings selections before finishing the wizard.						
 3 Create a Standard Switch 4 Connection settings 5 Ready to complete 	New standard switch Virtual machine port group Assigned adapters Switch MTU VLAN ID	vSwitch2 VM Network 2 vmnic2 1500 All (4095)					
			CANCEL	ВАСК	FINISH		

9. Now continue with VMware vSwitch Monitoring and connect Flowmon's monitoring interface to the same virtual switch to complete the configuration.

Flowmon Configuration

No configuration specific for VMware dedicated port monitoring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.



 Overview • Prerequisites

Deployment

• Flowmon Configuration

VMware vSwitch Monitoring

Overview

Flowmon for VMware has the ability to monitor traffic and generate NetFlow / IPFIX flow data. To enable this functionality for the monitoring of a VMware vSwitch local to the VMware host where Flowmon is running, please follow the steps outlined below.

- Prerequisites
 - A running instance of Flowmon for VMware Flowmon Collector (with a built-in Probe) or Flowmon Probe.

Deployment

Setting up vSwitch monitoring is done by creating a new port group and configuring it to use the promiscuous mode.

1. In the vSphere client, click on the IP address of a VMware host. Then click on the **Configure** tab, select Virtual switches and click on Add Networking.





2. Select Virtual Machine Port Group for a Standard Switch and click on the Next button.

192.168.3.120 - Add Networking 1 Select connection type Select connection type 2 Select target device Select a connection type to create. **3** Connection settings 4 Ready to complete O VMkernel Network Adapter The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN and host management. Virtual Machine Port Group for a Standard Switch A port group handles the virtual machine traffic on standard switch. O Physical Network Adapter A physical network adapter handles the network traffic to other hosts on the network. CANCEL ВАСК

3. Click on the **Select an existing standard switch** option and browse the existing switches. Select the one for which you want to create a port group. Then click on the **Next** button.

1 Select connection type 2 Select target device 3 Connection settings	Select target device Select a target device	for the new connection.	
4 Ready to complete	 Select an existing 	standard switch	
	vSwitchO		BROWSE
	O New standard swi	tch	
	MTU (Bytes)	1500	



4. Enter a Network label, select the VLAN ID as All (4095) and click on the Next button.

 1 Select connection type 2 Select target device 3 Connection settings 	Connection settings Use network labels to identif hosts.	Connection settings Use network labels to identify migration-compatible connections common to two or more hosts.					
4 Ready to complete	Network label	MonitoringPortGroup					
	VLAN ID	All (4095)					
			CANCEL	ВАСК	NEX		
			CANCEL	ВАСК	NEX		
view settings and click on	the Finish button.		CANCEL	BACK	NEX		
view settings and click on 192.168.3.120 - Add	the Finish button. Networking		CANCEL	BACK	NEX		
view settings and click on 192.168.3.120 - Add 1 Select connection type 2 Select target device 	the Finish button. Networking Ready to complete Review your settings selection	ons before finishing the wize	CANCEL	BACK	NEX		
view settings and click on 192.168.3.120 - Add 1 Select connection type 2 Select target device 3 Connection settings 4 Ready to complete 	the Finish button. Networking Ready to complete Review your settings selected Virtual machine port group Standard switch	ons before finishing the wiza MonitoringPortGroup vSwitchO All (4005)	CANCEL	BACK	NEX		
view settings and click on 192.168.3.120 - Add 192.168.3.120 - Add 19	the Finish button. Networking Ready to complete Review your settings selection Virtual machine port group Standard switch VLAN ID	ons before finishing the wize MonitoringPortGroup vSwitch0 All (4095)	ard.	BACK	NEX		
view settings and click on 192.168.3.120 - Add 1 Select connection type 2 Select target device 3 Connection settings 4 Ready to complete 	the Finish button. Networking Ready to complete Review your settings selection Virtual machine port group Standard switch VLAN ID	ons before finishing the wiza MonitoringPortGroup vSwitch0 All (4095)	ard.	BACK	NEX		
view settings and click on 192.168.3.120 - Add 1 Select connection type 2 Select target device 3 Connection settings 4 Ready to complete	the Finish button. Networking Ready to complete Review your settings selection Virtual machine port group Standard switch VLAN ID	ons before finishing the wiza MonitoringPortGroup vSwitch0 All (4095)	ard.	BACK	NEX		
view settings and click on 192.168.3.120 - Add 1 Select connection type 2 Select target device 3 Connection settings 4 Ready to complete 	the Finish button. NetWorking Ready to complete Review your settings selection Virtual machine port group Standard switch VLAN ID	ons before finishing the wiza MonitoringPortGroup vSwitch0 All (4095)	ard.	BACK	NEX		
view settings and click on 192.168.3.120 - Add 1 Select connection type 2 Select target device 3 Connection settings 4 Ready to complete 	the Finish button. Networking Ready to complete Review your settings selection Virtual machine port group Standard switch VLAN ID	ons before finishing the wiza MonitoringPortGroup vSwitch0 All (4095)	ard.	BACK	NEX		
view settings and click on 192.168.3.120 - Add 1 Select connection type 2 Select target device 3 Connection settings 4 Ready to complete	the Finish button. Networking Ready to complete Review your settings selection Virtual machine port group Standard switch VLAN ID	ons before finishing the wiza MonitoringPortGroup vSwitch0 All (4095)	ard.	BACK	NEX		
view settings and click on 192.168.3.120 - Add 1 Select connection type 2 Select target device 3 Connection settings 4 Ready to complete	the Finish button. Networking Ready to complete Review your settings selection Virtual machine port group Standard switch VLAN ID	ons before finishing the wiza MonitoringPortGroup vSwitch0 All (4095)	ard.	BACK	NEX		
view settings and click on 192.168.3.120 - Add • 1 Select connection type • 2 Select target device • 3 Connection settings 4 Ready to complete	the Finish button. Networking Ready to complete Review your settings selection Virtual machine port group Standard switch VLAN ID	ons before finishing the wiza MonitoringPortGroup vSwitch0 All (4095)	ard.	BACK	NEX		
view settings and click on 192.168.3.120 - Add • 1 Select connection type • 2 Select target device • 3 Connection settings 4 Ready to complete	the Finish button. Networking Ready to complete Review your settings selection Virtual machine port group Standard switch VLAN ID	MonitoringPortGroup vSwitch0 All (4095)	ard.	BACK	NEX		
view settings and click on 192.168.3.120 - Add 1 Select connection type 2 Select target device 3 Connection settings 4 Ready to complete	the Finish button. Networking Ready to complete Review your settings selected Virtual machine port group Standard switch VLAN ID	ons before finishing the wiza MonitoringPortGroup vSwitch0 All (4095)	CANCEL	BACK	NEX		



6. Select the newly created port group and click on the **Edit** button.

vm vSphere Client Menu v Q Search		C
Image: Image	ACTIONS ~	
192.168.3.120 Summary Monitor	Configure Permissions VMs Datastores Networks Updates	
ADS - Demo - 10		
🛱 ADS - Demo - 11 🔹 Storage 🌰	Virtual switches	
ADS - Demo - 9 Storage Adapters	일 Add Networking 🔗 Refresh 🛛 🖀 Migrate VMkernel Adapter 👼 Manage Physical Adapters 🧷 Edit 🗙 Remove	
ADS-9.5 Storage Devices	Switch y Discovered issues	
📅 Anet - lokalizace Host Cache Configur	DSwitch - Monitoring	
APM DB ris Protocol Endpoints	DSwitch - Management	
APM DEVEL I/O Filters	日 日 vSwitch0	
APM devel - old Networking		
APM GUI DEVEL Virtual switches	T vSwitch1 -	
APM GUI devel VMkernel adapters	Standard switch: vSwitch0	
APM Test 1 Physical adapters		
APM Test 1 - old	Port Groups Properties Policies	
APM Test 2 cole Virtual Machines V/M Startup /Shutdo	Details / Edit. X Remove	
Appleters a probe VM Startup/Stutuo	Part Group	- Unlinks
APM test eshop Agent VM Settings		T Opiniks
APM test Oracle Swap Elle Location	MonitoringPortGroup All (4095)	0
APM test Via 10 System	9 VM Network	0
APM test Win 20		

7. Go to the **Security** tab and check the **Override** checkbox next to **Promiscuous mode** and set the value to **Accept**. Then click on the **OK** button.

Properties				
Security	Promiscuous mode	Override	Accept	~
Traffic shaping	MAC address changes	Override	Accept	~
Teaming and failover	Forged transmits	Override	Accept	~
				CANCEL

Flowmon Configuration

No configuration specific for VMware vSwitch monitoring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.



VMware Distributed vSwitch Monitoring

Overview

Flowmon for VMware has the ability to monitor traffic and generate NetFlow / IPFIX flow data. To enable this functionality for the monitoring of a VMware Distributed vSwitch (DSwitch), please follow the steps outlined below.

Network traffic from a virtual machine is monitored by a Flowmon instance running on the same host. This concept requires a Flowmon instance deployed on each physical host where monitored virtual machines could potentially run.

Prerequisites

• A running instance of Flowmon for VMware - Flowmon Collector (with a built-in Probe) or Flowmon Probe.

Deployment

In order to monitor a DSwitch, distributed port mirroring needs to be configured. Flowmon for VMware has to be deployed on each VMware host (ESXi server) and connected to the DSwitch you wish to monitor.

 Port IDs of all Flowmon monitoring ports need to be collected. Port IDs can be found in Edit settings – Network adapter settings. For an appliance with one monitoring port, check the port ID of Network adapter 2. For appliances with more monitoring ports, check port IDs of for Network adapters from 3 to x (x equals 4, 6, 8 depending on the number of monitoring ports – 2, 4, 6). Port IDs will be used as destinations

- Overview
- Prerequisites
- Deployment
- Flowmon Configuration



in the monitoring session.

🚯 VAVE - FlowmonProbe1	Actions *			
Getting Started Summary	Monitor Manage Related Objects			
	VAVE - FlowmonProbe1 Guest OS: CentOS 4/5/6/7 (64 Compatibility: ESX/ESX/ 4.0 and a Milware Tools: Buncion version 9 VAVE - FlowmonProbe1 - Edi	-bit) ster (VM version 7) M4 (Unorade available) t Settings		(()
Powered On	Virtual Hardware VM Options	SDRS Rules vApp Option	ons	
Launch Remote Console Download Remote Console	• G CPU	4	0	
A VMware Tools is outdate	d on F Memory	4096 👻	MB 💌	
VM Hardware	+ 🖾 Hard disk 1	8	GB 🛛	
+ CPU	G SCSI controller 0	LSI Logic Parallel		
Memory	Network adapter 1	Management DPort (DSwi	tch - Mana 🚽	Connected
+ Hard disk 1	👻 📜 Network adapter 2	Management DPort (DSwi	tch - Mana 🚽	Connected
Network adapter 1	Status	Connect At Power On		
 Network adapter 2 	Port ID	314		
CD/DVD drive 1	Adapter Type	E1000	Ŧ	
Floppy drive 1	MAC Address	00:50:56:9e:6c:55		Automatic -
 Video card 	GD/DVD drive 1	Host Device		Connected
> Other	🕨 📻 Floppy drive 1	Host Device		Connected
Compatibility	Video card	Specify custom settings		
	VMCI device			
- Tags	 Other Devices 			
Assigned Tag Cate	gory > Upgrade	Schedule VM Compatible	lity Upgrade	
Th	New device:	Select	• A	dd
Initiator	Compatibility: ESX/ESXI 4.0 and I	ater (VM version 7)		OK Cancel

2. Using the same procedure, collect **Port ID**s of virtual machines that should be monitored. These Port IDs will be used as sources in the monitoring session.



3. In DSwitch configuration, choose tab Manage and section Port mirroring.

DSwitch - Management	Action	IS ¥				
Getting Started Summary	Monite	or Manage	Related Objects			
Settings Alarm Definitions	Tags	Permissions	Network Protocol Profiles	Ports	Resource Allocation	
	P	ort mirroring				
Properties		🕂 New				
Topology	1	Session Name			Туре	
Private VLAN		vave-1			Distribu	uted Port I
NetFlow		vave2			Encaps	sulated R
Port mirroring						
Health check	1	M				

4. Create a new monitoring session by clicking on the New button. In the first step, choose the Distributed
 Port Mirroring option and click on the Next button.
 DSwitch - Management - Add Port Mirroring Session

1 Select session type	Select session type
2 Edit properties	Select the type of the port mirroring session.
3 Select sources	Distributed Port Mirroring
4 Select destinations	Mirror network traffic from a set of distributed ports to other distributed ports.
5 Ready to complete	 Remote Mirroring Source Mirror network traffic from a set of distributed ports to specific uplink ports.

Enter a name for the session and click on the Next button. DSwitch - Management - Add Port Mirroring Session

() H Edit properties 1 Select session type Specify a name and the properties of the port mirroring session. 2 Edit properties 3 Select sources Flowmon APM Mirror Name: 4 Select destinations Status: Enabled • 5 Ready to complete Session type: Distributed Port Mirroring Advanced properties Normal I/O on destination ports: Disallowed • Mirrored packet length (Bytes): Enable 60 * Sampling rate: 1 *



6. In the **Select sources** window, choose Port IDs of virtual machines that should be monitored and clink on the **Next** button.

1 Select session type 2 Edit properties	Select sou Select the s	rces source distribu	ted ports of the	port mirroring session. Traffic	rom these distributed ports will be m	irrored.
3 Select sources		Select Ports				*
5 Ready to complete	Port ID				Q, 421	•
		Port ID	Port Name	Connected Entity	Host	
		✓ 421		JP - Worker	192.168.3.103	
						- 1
						- 1

7. In the **Select destinations** window, choose Port IDs of Flowmon's monitoring interfaces and click on the **Next** button.

DSwitch - Management - Add Port	Mirroring Session			
 ✓ 1 Select session type ✓ 2 Edit properties 	Select destinations Select the destination	on distributed ports the traffic to which to be mirro	ored.	
✓ 3 Select sources	19 19 ×			
4 Select destinations	Port ID 1 *	Host	Connectee	
5 Ready to complete	890	192.168.3.110	VAVE - FlowmonProbe2	
	314	192.168.3.103	WAVE - FlowmonProbe1	

- 8. Check the settings before clicking on the **Finish** button.
- A When you add a new virtual machine that you would like to monitor, it is necessary to update the list of source ports.

Flowmon Configuration

A To ensure continuous traffic visibility, disable migration for all Flowmon instances.

No configuration specific for VMware Distributed vSwitch monitoring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.



Flowmon for KVM

Overview

Flowmon for KVM gives network administrators and security engineers insight into what is happening in their infrastructure. Its powerful features can be used to gain control of bandwidth utilization, optimize network and application performance, reduce time to resolution during troubleshooting and keep the infrastructure protected against modern cyber-security threats.

Flowmon for KVM is

- a virtual appliance intended for the KVM environment,
- capable of collecting as well as generating flow data,
- fully under customer's control including updates, backups, and configuration.

Flowmon for KVM supports

- IPFIX, NetFlow v5/v9 or sFlow data collection from Flowmon Probes or other compatible devices (e.g., customer routers),
- ingestion of Amazon VPC Flow Logs from AWS,
- traffic monitoring on local Open vSwitches,
- traffic monitoring on local dedicated physical interfaces,
- 3rd-party packet brokers such as Garland Prisms, Ixia CloudLens, or Gigamon,
- ERSPAN/GRE traffic mirroring.

This guide describes the deployment procedure of Flowmon for KVM using a set of qcow2 disk images. The storage capacity can be later changed to match the purchased license.

Features

Flowmon for KVM supports three modes of operation:

- Probe,
- Collector,
- Collector and Probe.

Flowmon Probe

In this mode, the virtual appliance acts as a Flowmon Probe. It accepts mirrored traffic on monitoring ports and exports flow data to at least one remote Flowmon Collector instance.

Supported traffic mirroring solutions:

• KVM Open vSwitch Port Mirroring

Supported 3rd-party packet brokers:

- Ixia CloudLens
- Gigamon
- Garland Prisms

- Features
- Licensing
- Prerequisites
- Deployment
- Flowmon Configuration



Flowmon Collector

In this mode, the virtual appliance acts as a Flowmon Collector and accepts supported flow formats from external probes, network devices, or Amazon VPC Flow Logs on management ports. For details on supported flow sources and formats, refer to the official Flowmon User Guide.

Flowmon Collector and Flowmon Probe

In this mode, the virtual appliance acts both as a Flowmon Probe and Flowmon Collector. Probe sends data to the locally available Collector. For details on configuration, refer to the official Flowmon User Guide.

Licensing

Flowmon for KVM is a virtual appliance using the Bring-Your-Own-License (BYOL) licensing model.

With <u>BYOL</u>, you can apply for a Free Trial License at flowmon.com.

For support or inquiries, see our contact information.

Prerequisites

In order to follow this guide, you need the following:

- 1. KVM-based host with a graphical user interface and **Virtual Machine Manager** installed.
- Flowmon for KVM downloaded from the Partner Portal, archives for download are located in Downloads / Products / Flowmon Virtual Appliances & Cloud / Flowmon for KVM. Unless directed otherwise, pick the latest stable version with the desired set of modules.
- 3. A valid Flowmon license or a trial license from flowmon.com.

Deployment

The deployment of Flowmon for KVM consists of the following steps:

- 1. Unzip the archive.
- 2. Start the Virtual Machine Manager application.
- 3. Select File New virtual machine.



4. Select Import existing disk image and click the Forward button.



5. Select path to the unzipped file from step 2, choose disk 0 and confirm the settings with the **Choose volume** button.



•	Choose Storage Volume		^	•	×
	Size: 4960.81 GiB Free / 561.95 GiB In U Location: /home/vm-images Volumes + 📀 m	se			
10% vm-images Filesystem Directory	Volumes	▼ Size	Format	U:	
	FMC-10.00-KVM-TEST-disk-0.qcow2	8.00 GiB	qcow2		I.
	FMC-10.00-KVM-TEST-disk-1.qcow2	100.00 GiB	qcow2	~ ~ ~	
+ > 3 m	Browse Loca	al 🖉 Cancel 🖣	🗸 Choose Vo	lume]



6. Choose **OS type** as **CentOS 7.0** and proceed with **Forward**.

···	New VM	+ ×
Create a new vi Step 2 of 4	irtual machine	
Provide the existing storage	je path:	
/home/vm-images/FMC-1	0.00-KVM-TEST-disk-0.qcow2	Browse
Choose the operating syste	em you are installing:	
🔅 CentOS 7.0		Ø
	⊘Cancel G Back	● Forward



7. Assign CPU cores and RAM to the appliance (Recommended minimum: 8 CPU, 16GB RAM).

-			New VM		+ ×
E C	r eate a n e ep 3 of 4	ew virt	ual machine		
Choose M	emory and	CPU set	tings:		
Memory:	8192	- +]		
	Up to 24530 I	MiB availa	ble on the host		
CPUs:	8	- +			
	Up to 24 avai	lable	_		
			⊘ Cancel	G Back	● Forward

8. Set a name for the appliance, check option **Customize configuration before install** and **Finish** the configuration.



New VM			
Create a new virtual machine Step 4 of 4	2		
Ready to begin the installation			
Name: MyFlowmonCollector			
OS: CentOS 7.0			
Install: Import existing OS image			
Memory: 8192 MiB			
CPUs: 8			
Storage:ges/FMC-10.00-KVM-TEST-disk-0.qcow	v2		
Customize configuration before install			
Network selection			
⊘ Cancel	G Back + Finish		

9. Select VirtIO Disk 1, set Disk bus to VirtIO and Apply the settings. Then click Add Hardware in order to add a data drive.



~		MyFlowmonCo	llector on QEMU/KVM: 19	92.16	8.6.99		^	٥	>
🗸 Be	gin Installation ⊘	Cancel Installation							
	Overview	Virtual Disk							
	OS information	Source path: /ho	ome/vm-images/FMC-10.	00-K\	/M-TEST-disk-0.d	cow2			
 		Device type: Vir	tIO Disk 1						
	PUS	Storage size: 8.0	00 GiB						
	viemory	Readonly:							
¢ ₿ B	3oot Options	Shareable:							
V	/irtIO Disk 1								
¶⊫ N	NIC :84:a8:e1	* Auvanceu opui	Vietto		1				
п, 🔲	ablet	DISK DUS:	VITTO						
	Display Spice	Serial number:							
💻 s	Sound ich6	Storage format:	acow2		Ĩ				
🗟 c	Console	b Daufaunan a							
à c	Channel qemu-ga	Performance d	puons						
	Channel spice								
💷 v	/ideo QXL								
— C	Controller USB 0								
 U 	JSB Redirector 1								
U	JSB Redirector 2								
d R	NG /dev/urandom								
	Add Hardware				Pemove	Cancel	Ar		

10. Select the **Storage** option and choose **Select or create custom storage**. The **Bus type** option has to be set to **VirtIO**. Then browse images by clicking on **Manage...**.



 Storage Controller Network Create a disk image for the virtual machine Create a disk image for the virtual machine 	•	Ac	ld New Virtual Hardware 🔷 🛧	×
Controller Create a disk image for the virtual machine	2	Storage	Storage	
 Input Graphics Sound Serial Parallel Console Channel USB Host Device Bus type: VirtIO - 		Controller Network Input Graphics Sound Serial Parallel Console Channel USB Host Device	 Create a disk image for the virtual machine 20.0 - + GiB 17.5 GiB available in the default location Select or create custom storage Manage /home/vm-images/FMC-10.00-k Device type: Disk device Bus type: VirtIO 	3
 Video Watchdog Filesystem Smartcard USB Redirection TPM RNG RNG Panic Notifier Virtio VSOCK 		Video Watchdog Filesystem Smartcard USB Redirection TPM RNG Panic Notifier Virtio VSOCK	► Advanced options	h



11. Select disk 1 and click on the **Choose Volume** button.

•	Choose Storage Volume			↑ □ X
))	Size: 4960.81 GiB Free / 561.95 GiB In Location: /home/vm-images) Use		
,	Volumes	✓ Size	Format	Used
0% VM-Images Filesystem Directory	FMC-10.00-KVM-TEST-disk-0.qcow2	8.00 GiB	qcow2	5
	FMC-10.00-KVM-TEST-disk-1.qcow2	100.00 GiB	qcow2	Ξ
			-	
+ > 3 🟛	Brows	e Local OCancel	🗸 Choos	e Volume



12. Confirm the setup by clicking on Finish

•		Add New Virtual Hardware 🔷 🗙
2	Storage	Storage
	Storage Controller Network Input Graphics Sound Sound Serial Parallel Console Channel Channel USB Host Device PCI Host Device Video Video Video Smartcard USB Redirection TPM RNG	 Storage Create a disk image for the virtual machine 200 - + GiB 17.5 GiB available in the default location Select or create custom storage Manage /home/vm-images/FMC-10.00-KV Device type: Disk device Bus type: VirtIO Advanced options
•8 10	Panic Notifier Virtio VSOCK	
		⊘Cancel ✓ Finish

13. Select the **Boot Options** category and select **VirtIO Disk 1** as a primary disk from which to boot the appliance.


		MyFlowmonCollector on QEMU/KVM: 192.168.6.99	≁		×
~	Begin Installation ⊘	Cancel Installation			
	Begin Installation Overview OS information CPUs Memory Boot Options VirtIO Disk 1 VirtIO Disk 2 NIC :fe:8a:d6 Tablet Display Spice Sound ich6 Console Channel qemu-ga Channel spice Video QXL Controller USB 0 USB Redirector 1	Cancel Installation Autostart Start virtual machine on host boot up Boot device order Enable boot menu			
8	USB Redirector 2 RNG /dev/urandom				
	🕂 Add Hardware	Cancel	A	ply	

14. Add as many interfaces as necessary to create all interfaces of a Flowmon appliance (three more for Flowmon Collector, 1+N for Flowmon Probe with N monitoring ports). Click on Add Hardware, select Network, choose Network source and Device model (virtio) and click on Finish.



•		Add New Virtual Har	dware ·	≁ ×
2	Storage Controller	Network		
14	Network	Network source:	Bridge br60: Host device eno2	-
	Network Input Graphics Sound Serial Parallel Console Channel USB Host Device PCI Host Device Video Video Watchdog Filesystem Smartcard USB Redirection TPM RNG	MAC address: Device model:	Bridge br60: Host device eno2	~
1.	Virtio VSOCK			
			🖉 Cancel 🖌 🖌 Fini	sh



15.	After adding the interfaces,	you can	begin the in	stallation by	clicking on I	Begin Installation

Overview	Basic Details	
OS information	Name:	MyFlowmonCollector
CPUs	UUID:	9f06d3da-137c-4d2f-8fe5-5329a4a9b5c1
Memory	Status:	Shutoff (Shut Down)
Boot Options VirtIO Disk 1	Title:	
VirtIO Disk 2	Description:	
NIC :de:2f:84		
NIC :cc:fc:6b		
NIC:65:45:10	Hypervisor De	tails
NIC :8f:28:6a	Hypervisor:	KVM
🔍 Tablet	Architecture	: x86_64
Display Spice	Emulator:	/usr/libexec/qemu-kvm
Sound ich6 Console	Chipset:	i440FX -
Channel qemu-ga	Firmware:	BIOS 🔹 🖪
Video OXI		

Flowmon Configuration

Please refer to Post-installation Steps.



KVM Open vSwitch Port Mirroring

Overview

Flowmon for KVM has the ability to monitor traffic and generate NetFlow / IPFIX flow data. To enable this functionality for the monitoring of an Open vSwitch local to the KVM host where Flowmon is running, please follow the steps outlined below.

Prerequisites

• A running instance of Flowmon for KVM - Flowmon Collector (with a built-in Probe) or Flowmon Probe.

Deployment

Since Virtual Machine Manager does not support Open vSwitch (OVS), you have to manually modify the configuration of your Flowmon instance.

1. Open Flowmon's XML descriptor for editing.

1

virsh edit <name-of-your-Flowmon-**in**-Virtual-Machine-Manager>

 Add each monitoring port of your Flowmon to an OVSbridge previously created in your OVS. Each monitoring port type has to be set to openvswitch. Substitute [name_of_your_OVSbridge] for the name of your OVS bridge.

1	<interface type="bridge"></interface>
2	<mac address="52:54:00:9f:46:cc"></mac>
3	<source bridge="[name_of_your_OVSbridge]"/>
4	<virtualport type="openvswitch"></virtualport>
5	<pre><parameter interfaceid="c9a700ed-9576-45aa-81f3-</pre></th></tr><tr><th></th><th>b7d94b73cc91"></parameter></pre>
6	
7	
8	

3. Create a mirror in your OVS bridge.

1	ovs-vsctl <mark>id</mark> =@m create mirror \
2	name= <custom-name-of-the-mirror> \</custom-name-of-the-mirror>
3	add bridge \
4	<name-of-the-ovs-bridge-where-to-add-the-mirror> \</name-of-the-ovs-bridge-where-to-add-the-mirror>
5	mirrors @m

 If you would like to mirror specific ports, configure per-port mirroring. Display UUIDs of all vnet interfaces associated with OVS.

- Overview
- Prerequisites
- Deployment
- Flowmon Configuration



1

ovs-vsctl show

This example shows UUIDs for vnet[0-5].

```
1 for p in vnet{0..5}; do
2 echo "$p: $(ovs-vsctl get port "$p" _uuid)"
3 done
```

For each interface created in OVS that you want to monitor set up its mirroring to the mirror created in step 3. The following command mirrors both ingress and egress traffic of the source port.

```
1 ovs-vsctl set mirror <name-of-the-mirror-from-step-3> \
2 select_src_port=<UUID-of-the-vnet-interface-you-want-to-
3 select_dst_port=<UUID-of-the-vnet-interface-you-want-to-
monitor>
```

5. If your traffic is isolated in VLANs, you can **select specific VLAN IDs to mirror**.

1 ovs-vsctl set mirror <name-of-the-mirror-from-step-3> selectvlan=<csv-list-of-vlan-ids-to-mirror>

6. Select and set VLAN ID for mirroring output. Flowmon's monitoring interface(s) must belong to this VLAN to receive mirrored traffic.

1 ovs-vsctl set mirror <name-of-the-mirror-from-step-3> outputvlan=<selected-vlan-id>

7. Tag Flowmon's monitoring interface(s) with VLAN ID.

1 ovs-vsctl set port <port-name> tag=<selected-vlan-id-from-step-7> 2 # or for multiple VLANs 3 ovs-vsctl set port <port-name> trunks=<csv-list-of-vlan-ids>

Flowmon Configuration

No configuration specific for KVM Open vSwitch monitoring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.



Flowmon for Hyper-V

Overview

Flowmon for Hyper-V gives network administrators and security engineers insight into what is happening in their infrastructure. Its powerful features can be used to gain control of bandwidth utilization, optimize network and application performance, reduce time to resolution during troubleshooting and keep the infrastructure protected against modern cyber-security threats.

Flowmon for Hyper-V is

- a virtual appliance intended for the Hyper-V environment,
- capable of collecting as well as generating flow data,
- fully under customer's control including updates, backups, and configuration,

Flowmon for Hyper-V supports

- IPFIX, NetFlow v5/v9 or sFlow data collection from Flowmon Probes or other compatible devices (e.g., customer routers),
- ingestion of Amazon VPC Flow Logs from AWS,
- traffic monitoring on local vSwitches,
- traffic monitoring on local dedicated physical interfaces,
- 3rd-party packet brokers such as Garland Prisms, Ixia CloudLens, or Gigamon,
- ERSPAN/GRE traffic mirroring.

This guide describes the deployment procedure of Flowmon for Hyper-V using a set of vhdx disk images. The storage capacity can be later changed to match the purchased license.

Features

Flowmon for Hyper-V supports three modes of operation:

- Probe,
- Collector,
- Collector and Probe.

Flowmon Probe

In this mode, the virtual appliance acts as a Flowmon Probe. It accepts mirrored traffic on monitoring ports and exports flow data to at least one remote Flowmon Collector instance.

Supported traffic mirroring solutions:

- Hyper-V Virtual Switch Port Monitoring
- Hyper-V Network Interface Mirroring

Supported 3rd-party packet brokers:

- Ixia CloudLens
- Gigamon
- Garland Prisms

- Overview
- Features
- Licensing
- Prerequisites
- DeploymentFlowmon Configuration



Flowmon Collector

In this mode, the virtual appliance acts as a Flowmon Collector and accepts supported flow formats from external probes, network devices, or Amazon VPC Flow Logs on management ports. For details on supported flow sources and formats, refer to the official Flowmon User Guide.

Flowmon Collector and Flowmon Probe

In this mode, the virtual appliance acts both as a Flowmon Probe and Flowmon Collector. Probe sends data to the locally available Collector. For details on configuration, refer to the official Flowmon User Guide.

Licensing

Flowmon for Hyper-V is a virtual appliance using the Bring-Your-Own-License (BYOL) licensing model.

With <u>BYOL</u>, you can apply for a Free Trial License at flowmon.com.

For support or inquiries, see our contact information.

Prerequisites

In order to follow this guide, you need the following:

- 1. A Hyper-V host with a graphical user interface and **Hyper-V Manager** installed.
- 2. Flowmon for Hyper-V downloaded from the Partner Portal, archives for download are located in **Downloads / Products / Flowmon Virtual Appliances & Cloud / Flowmon for Hyper-V**. Unless directed otherwise, pick the latest stable version with the desired set of modules.
- 3. A valid Flowmon license or a trial license from flowmon.com.

Deployment

For each Flowmon deployment, individual copies of the provided VHDX files are needed. You can reuse VHDX file to deploy multiple instances.

The deployment of Flowmon for Hyper-V consists of the following steps:

• Unzip the archive. In Hyper-V Manager, click in the main menu on Action, select New and Virtual Machine.



1 ·	Hyper-V Manager – 🗆 🗙
File Action View Help	
🗢 📢 New 🕨 Virtual Machine	
Hard Disk Hyper-V Settings Hard Disk Floppy Disk	Actions
Virtual SAN Manager Os 7 Off	CPU Usage Assigned Memory Uptime St New Import Virtual Mac
Topper Stop Se Action View Help	
Refrect Help	 Virtual Machine
The	selected virtual machine has no checkpoints.
	Sconnect
Flowmon Test	Start
Created: 3/9 Version: 5.0 Generation: 1 Notes: Nor	2015 12:21:02 PM Clustered: No is Checkpoint PMove e Export is Checkpoint PMove is Checkpoint is Checkpoint is Checkpoint is Checkpoi
Displays the New Virtual Machine Wizard.	lication

• Provide a **name** for the virtual machine.



à.	New Virtual Machine Wizard
Specify Na	ame and Location
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Choose a name and location for this virtual machine. The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload. Name: Flowmon Test You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server. C:\ProgramData\Microsoft\Windows\Hyper-V\ Browse If you plan to take checkpoints of this virtual machine, select a location that has enough the configured for that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location that has enough the configured for the select a location the select a location the default folder to the select a location the select a location the default folder to the select a location the
2	Name: Flowmon Test
	< Previous Next > Finish Cancel

- As the generation of the new virtual machine, select **Generation 2**.
- Assign **memory**.



i.	New Virtual Machine Wizard
Assign Memo	ry
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 9252 MB. To improve performance, specify more than the minimum amount recommended for the operating system. Startup memory: 4096 When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run. Startup memory: 4096 MB Use Dynamic Memory for this virtual Machine in the improvement of the operating system that it will run.

• In Configure Networking, select connection for Flowmon's Management Interface 1.



۵.	New Virtual Machine Wizard
Configure Ne	etworking
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. Connection: Management
5	Connection: Management
	< Previous Next > Finish Cancel

• In Connect Virtual Hard Disk, select Use an existing virtual hard disk. Pick the first VHDX file. Click on Finish.



۵.	New Virtual Machine Wizard
<u> </u>	nnect Virtual Hard Disk
🖲 Use an exis	sting virtual hard disk
Use this op	tion to attach an existing virtual hard disk, either VHD or VHDX format.
Location	: C:\Flowmon-Collector-disk1.vhdx Browse
6	Use an existing virtual hard disk Use this option to attach an existing virtual hard disk, either VHD or VHDX format. Location: C:\Flowmon-Collector-disk1.vhdx Browse Attach a virtual ha Use this option to Finish Nah ard disk later.
	< Previous Next > Finish Cancel

• Open **Settings** on the newly created virtual machine.



Flowmon Virtual Appliances Rev. 41, 30/07/2021



- Displays the virtual machine settings user interface.
- If the Firmware option is available, make sure Secure Boot is disabled.



• Add multiple network adapters. Click on **Add Hardware** and add a **Network Adapter**. For additional management interface add one adapter. For two monitoring ports add two networks adapters.





• For each new network adapter, select a virtual switch.



	Settings for Flowmon Test on HYPERV – 🗆 🗙
Flowmon Test	
★ Hardware Mardware BIOS Boot from CD Memory 4096 MB Image: Distance Processor 1 Virtual processor IDE Controller 0 Image: Hard Drive	Network Adapter
hv-hcl.vhd	Monitoring 🗸 🗸
None SCSI Controller I I Vetwork Adapter Management	Not connected Management
Network Adapter Not connected	Monitoring
Network Adapter Monitoring Network Adapter Network Adapter	Maximum bandwidth: 0 Mbps 0 To leave the minimum or maximum unrestricted, specify 0 as the value.
COM 1 None COM 2 None	Network Adapter
Diskette Drive None Management	Monitoring
Ivame Flowmon Test Flowmon Services Some services offered	OK Cancel Apply

• For each new network adapter intended for monitoring, click on **Advanced Features** and select **Mirroring mode** as **Destination**.





• Add the second VHDX file as a hard drive to your SCSI controller. Select **SCSI Controller**, select **Hard Drive** and click on the **Add** button.





• Click on the newly created Hard Drive and select path to the second VHDX file.





Flowmon Configuration

Please refer to Post-installation Steps.



Hyper-V Network Interface Mirroring

Overview

Flowmon for Hyper-V has the ability to monitor traffic and generate NetFlow / IPFIX flow data. To enable this functionality for the monitoring of network interfaces of virtual machines local to the Hyper-V host where Flowmon is running, please follow the steps outlined below.

Prerequisites

• A running instance of Flowmon for Hyper-V - Flowmon Collector (with a built-in Probe) or Flowmon Probe.

Deployment

• Right click on each virtual machine you would like to monitor and select **Settings**. For each selected network adapter click on **Advanced Features** and set **Mirroring mode** to **Source**. Keep in mind that your Flowmon's monitoring port must be attached to the same virtual switch as these network adapters.



• Make sure your Flowmon instance has **Mirroring mode** set to **Destination** and resides on the same virtual switch.

Optionally, if you intend to monitor VLAN traffic:

• **Connect** to the Hyper-V host hosting your Flowmon instance.

- Overview
- Prerequisites
- Deployment
- Flowmon Configuration



 Open powershell and rename all network adapters associated with your Flowmon instance. Adjust the number of interfaces, if necessary. Replace NameOfCreatedVirtualMachine with the name of your Flowmon instance in Hyper-V.

1	\$VMNetAdap = Get- VMNetworkAdapter -VMName "NameOfCreatedVirtualMachine"
2	rename-VMNetworkAdapter -VMNetworkAdapter <pre>\$VMNetAdap[0] -newname</pre>
	"Management 1"
3	rename-VMNetworkAdapter -VMNetworkAdapter \$VMNetAdap[1] -newname
	"Management 2"
4	<pre>rename-VMNetworkAdapter -VMNetworkAdapter \$VMNetAdap[2] -newname</pre>
	"Monitoring 1"
5	rename-VMNetworkAdapter -VMNetworkAdapter \$VMNetAdap[3] -newname
	"Monitoring 2"

• For each monitoring interface that is intended for VLAN traffic monitoring, configure a **trunk**. Replace **NameOfCreatedVirtualMachine** with the name of your Flowmon instance in Hyper-V.

1	Set-VMNetworkAdapterVlan -Trunk -AllowedVlanIdList "1-4094" -VMName "NameOfCreatedVirtualMachine" -VMNetworkAdapterName "Monitoring 1" -NativeVlanId 0
2	Set-VMNetworkAdapterVlan -Trunk -AllowedVlanIdList "1-4094" -VMName "NameOfCreatedVirtualMachine" -VMNetworkAdapterName "Monitoring 2" -NativeVlanId 0

Flowmon Configuration

No configuration specific for Hyper-V network interface mirroring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.



Hyper-V Virtual Switch Port Monitoring

Overview

Flowmon for Hyper-V has the ability to monitor traffic and generate NetFlow / IPFIX flow data. To enable this functionality for the monitoring of a Virtual Switch local to the Hyper-V host where Flowmon is running, please follow the steps outlined below.

- Prerequisites
 - A running instance of Flowmon for Hyper-V Flowmon Collector (with a built-in Probe) or Flowmon Probe.

Deployment

In order to create a new Hyper-V Virtual Switch, you have to:

• Open Hyper-V Manager and click on Virtual Switch Manager.... Hyper-V Manager Ĩ. File Action View Help 🗢 🔿 🖄 🖬 🚺 🔡 Hyper-V Manager Actions HYPERV Virtual Machines HYPERV CPU Usage Assigned Memory Name State New Flowmon Collector Running 0% 2048 MB 🚡 Import Virtual Machine.. Centos 7 **Bunning** 0% 2048 MB Hyper-V Settings... 👯 Virtual Switch Manager Virtual SAN Manage 🔏 Edit Disk... JUL E1 Inspect Disk... Stop Service Remove Serve Hyper-V Settings... Refresh Virtual Switch Manager... Virtual SAN Manager... + Disk...

Displays the Virtual Switch Manager user interface.

Click on **Create Virtual Switch** and select switch type. External switch is bound to a physical interface, Internal or Private is not.

- Overview
- Prerequisites
- Deployment
- Flowmon Configuration





• Choose a name for the virtual switch and, if it is an external switch, select the appropriate **External** network and click on **OK**.





In order to monitor an existing Hyper-V Virtual Switch, you have to:

- Connect to the Hyper-V host.
- Open powershell and set up traffic mirroring to the virtual switch of your choice. Replace NameOfCreatedSwitch with the name of your virtual switch. This configuration will mirror all external traffic to any virtual interface marked with Mirroring mode -Destination connected to the same virtual switch.







1 \$portFeature=Get-VMSystemSwitchExtensionPortFeature -FeatureName
 "Ethernet Switch Port Security Settings"
2 \$portFeature.SettingData.MonitorMode = 2
3
4
5 Add-VMSwitchExtensionPortFeature -ManagementOS
 -VMSwitchExtensionFeature \$portFeature

• Make sure your Flowmon instance is connected to this virtual switch and its monitoring interface is configured as a **Destination** for mirroring.

Optionally, if you intend to monitor VLAN traffic:

- **Connect** to the Hyper-V host.
- Open powershell and rename all network adapters associated with your Flowmon instance. Adjust the number of interfaces, if necessary. Replace NameOfCreatedVirtualMachine with the name of your Flowmon instance in Hyper-V.

1	\$VMNetAdap = Get- VMNetworkAdapter -VMName "NameOfCreatedVirtualMachine"
2	rename- VMNetworkAdapter -VMNetworkAdapter \$VMNetAdap[0] -newname "Management 1"
3	rename- VMNetworkAdapter -VMNetworkAdapter \$VMNetAdap[1] -newname "Management 2"
4	rename- VMNetworkAdapter -VMNetworkAdapter \$VMNetAdap[2] -newname "Monitoring 1"
5	rename- VMNetworkAdapter -VMNetworkAdapter \$VMNetAdap[3] -newname "Monitoring 2"

• For each monitoring interface that is intended for VLAN traffic monitoring, configure a **trunk**. Replace **NameOfCreatedVirtualMachine** with the name of your Flowmon instance in Hyper-V.

1	Set-VMNetworkAdapterVlan -Trunk -AllowedVlanIdList "1-4094" -VMName "NameOfCreatedVirtualMachine" -VMNetworkAdapterName "Monitoring 1" -NativeVlanId 0
2	Set-VMNetworkAdapterVlan -Trunk -AllowedVlanIdList "1-4094" -VMName "NameOfCreatedVirtualMachine" -VMNetworkAdapterName "Monitoring 2" -NativeVlanId 0

Flowmon Configuration

No configuration specific for Hyper-V Virtual Switch monitoring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.



Flowmon for AWS

Overview

Flowmon for AWS gives network administrators and security engineers insight into what is happening in their cloud infrastructure. Its powerful features can be used to gain control of bandwidth utilization, optimize network and application performance, reduce time to resolution during troubleshooting and keep the infrastructure protected against modern cyber-security threats.

Flowmon for AWS is

- published in the official AWS Marketplace,
- deployed in the form of an AWS Virtual Machine Instance,
- capable of collecting as well as generating flow data,
- suitable for cost optimization with dynamic instance resizing based on current/planned utilization.,
- fully under customer's control including updates, backups, and configuration.

Flowmon for AWS supports

- native traffic mirroring with Amazon VPC Traffic Mirroring,
- ingestion of Amazon VPC Flow Logs,
- 3rd party vTAP solutions such as Garland Prisms, Ixia CloudLens, or Gigamon,
- ERSPAN/GRE traffic mirroring.

Features

Flowmon for AWS supports three modes of operation:

- Probe,
- Collector,
- Collector and Probe.

Flowmon Probe

In this mode, the virtual appliance acts as a Flowmon Probe. It accepts mirrored traffic on monitoring ports and exports flow data to at least one remote Flowmon Collector instance.

Supported traffic mirroring solutions:

• Amazon VPC Traffic Mirroring

Supported 3rd-party packet brokers:

- Ixia CloudLens
- Gigamon
- Garland Prisms

Flowmon Collector

In this mode, the virtual appliance acts as a Flowmon Collector and accepts supported flow formats from external probes, network devices, or Amazon VPC Flow Logs on management ports. For details on supported flow sources and formats, refer to the official Flowmon User Guide.

- Overview
 - Features
 - Licensing
 - AWS Marketplace
 - Prerequisites
 - Deployment
 - Virtual Network Interfaces
 - Flowmon Configuration



Flow sources specific to AWS:

Amazon VPC Flow Logs

Flowmon Collector and Flowmon Probe

In this mode, the virtual appliance acts both as a Flowmon Probe and Flowmon Collector. Probe sends data to the locally running Collector. For details on configuration, refer to the official Flowmon User Guide.

Licensing

Flowmon for AWS is a virtual appliance with Bring-Your-Own-License (BYOL) and AWS Free Trial support.

With BYOL, you can apply for a Free Trial License at flowmon.com. We recommend this approach.

With <u>AWS Free Trial</u>, customers can try one instance of this appliance for 30 days. There will be no hourly software charges for that instance but AWS infrastructure charges will still apply. An AWS Free Trial will automatically convert to a paid hourly subscription upon expiration.

Select the licensing scheme appropriate for your use case and requirements. When in doubt, select the BYOL appliance and request a Free Trial License from flowmon.com.

For support or inquiries, see our contact information.

AWS Marketplace

Flowmon for AWS is available as a Virtual Appliance (VA) in AWS Marketplace.

In order to deploy virtual machines instances based on this appliance, you have to **Subscribe** to it. Activating a subscription involves the following steps:

- 1. Sign in or create a new account at AWS Marketplace.
- 2. Select the appropriate version of Flowmon for AWS based on your requirements and licensing limitations. When in doubt, select the most recent version available with the BYOL licensing scheme.
- 3. Subscribe to the appliance to make it available for deployment.

= Flowmon	Flowmon Co	Continue to Subscribe		
Driving Network Visibility	By: Flowmon Networ	ks Latest Versio	n: 9.02.05	Save to List
	Flowmon Collector is data (NetFlow, IPFIX, s > Show more	a AWS appliance fo Flow, and other te	r collection, long-term storage and analysis of flow chnologies compatible with NetFlow) from flow	Typical Total Price \$0.093/hr
	Linux/Unix 🖌	አትትት (0)	BYOL	Total pricing per instance for services hosted on t2.large in US East (N. Virginia). View Details

Prerequisites

In order to follow this guide, you need the following:

- 1. A web browser compatible with the AWS Console.
- 2. A trial license from flowmon.com.
- 3. An active AWS user account with a subscription (free or paid). <u>To properly evaluate all features of Flowmon</u> for AWS, a paid subscription is required!



Deployment

The deployment of Flowmon for AWS consists of the following steps:

- 1. Log in to the AWS Console. Select a region appropriate for your deployment.
- 2. Navigate to Launch a virtual machine.



3. Switch to AWS Marketplace tab on the left. Search for "Flowmon", with BYOL Software Pricing Plan. Select an appliance. Continue.

aws Services	 Resource Groups 	~ %				۵	N. Virginia 👻 Support 👻
1. Choose AMI 2. Choose Instant Step 1: Choose an A An AMI is a template that contain	Amazon Machine as the software configuration	e Image (AMI n (operating system, ap	5. Add Tags 6. Configure Secur) plication server, and applications)	rity Group 7. Review	select an AMI provided by AWS, our user communi	ity, or the AWS Marketplace; or you	Cancel and Exit can select one of your own AMIs.
Q, flowmon							×
Quick Start (0)							< < 1 to 1 of 1 Products > >
My AMIs (9) AWS Marketplace (1)	Flowmon Flow	rmon Collector । जन्म (0)। 10.01.08। By Flow	mon Networks				Select
Community AMIs (2)	Bring Linux Flow	Your Own License + AWS us 'Unix, CentOS 7 64-bit (x86) mon Collector is an AWS	ige fees Amazon Machine Image (AMI) Updated: 8 appliance for collection, long-term s	/29/19 torage, and analysis of flow data. It supports	NetFlow, IPFIX, sFlow, and other formats compatible wi	ith NetFlow	
 Categories All Categories 	More	e info					
Infrastructure Software (1) Clear Filter All Linux/Unix CentOS (1)	The following 12 result My AMIs an 2 results Community	results for "flowmor a in My AMIs a AMIs owned by you or : in Community AMIs AMIs are AMIs that are :	* were found in other catalogs shared with you shared by the general AWS community	9°.			
 Software Pricing Plans Hourly (1) Bring Your Own License (1) 							
 ▼ Region ☑ Current Region (1) □ All Regions (15) 							

🗨 Feedback 🔇 English (US)



4. Choose an instance type matching your sizing and budgetary requirements.

aws	S Services - Resource Grou	ps v 1e				۵	N. Virginia	• Support •
1. Choose Al	MI 2. Choose Instance Type 3. Configure	Instance 4. Add Storage	5. Add Tags 6. Configure 5	Security Group 7. Review				
Step 2: Amazon EC2 your applica	Choose an Instance Type 2 provides a wide selection of instance type tions. Learn more about instance types and	s optimized to fit different I how they can meet your	use cases. Instances are virtual computing needs.	servers that can run applications.	They have varying combinations of CPU, mer	nory, storage, and networking capacity, and	give you the flexibility to choose the appropria	te mix of resources for
Filter by:	All instance types 👻 Current gen	eration 👻 Show/Hide	e Columns					
Currently s	selected: t2.xlarge (Variable ECUs, 4 vCPUs,	2.3 GHz, Intel Broadwell E	5-2686v4, 16 GIB memory, EBS (only)				
	Family	Туре -	vCPUs (j) -	Memory (GiB) -	Instance Storage (GB) (i) -	EBS-Optimized Available (i) -	Network Performance (i) *	IPv6 Support (j) 👻
	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

5. Adjust instance configuration according to your needs, if necessary.

aws Services - Resour	rce Groups 🗸 🔥		N. Virginia	• Support •
1. Choose AMI 2. Choose Instance Type 3.	Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review			
Step 3: Configure Instance I Configure the instance to suit your requirement	Details fs. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance	ce, and more.		
Number of instances (j)	1 Launch Into Auto Scaling Group (j)			
Purchasing option (j)	Request Spot Instances			
Network (j)	vpc-129de26b (default) C Create new VPC			
Subnet (j)	No preference (default subnet in any Availability Zony * Create new subnet			
Auto-assign Public IP (j)	Use subnet setting (Enable)			
Placement group (j)	Add instance to placement group			
Capacity Reservation (i)	Open Create new Capacity Reservation			
IAM role (j)	None v Create new IAM role			
Shutdown behavior ()	Stop •			
Enable termination protection (j)	Protect against accidental termination			
Monitoring (j)	Enable CloudWatch detailed monitoring Additional charges apply.			
Tenancy (i)	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.			
Elastic Inference (j)	Add an Elastic Inference accelerator Additional charges apply.			
T2/T3 Unlimited (j)	Enable Additional charges may apply			
 Advanced Details 				
		Cancel	Previous Review and Launch	Next: Add Storage

Reddeck @ English (US) 6. Add storage configuration. <u>Make sure to uncheck disk deletion upon instance termination for a production-grade system!</u>

It is recommended to **add a separate data volume** matching the capacity allowed in your license. In any case, the volume **should not be smaller than 500 GB** for performance reasons.



	rvices 🗸 Resou	urce Groups 🐱 🔸									Virginia + Suj
1. Choose AMI 2. Choo	ose Instance Type 3	3. Configure Instance 4. Add Storag	je 5. Add Tags	6. Configure Security Group 7. Review							
Step 4: Add Sto our instance will be laun dit the settings of the roi torage options in Amazo	Drage iched with the followi ot volume. You can a in EC2.	ing storage device settings. You ca Ilso attach additional EBS volumes	an attach additional E s after launching an in	BS volumes and instance store volumes to y stance, but not instance store volumes. Lear	our instance, o n more about	r					
Volume Type (j)	Device (j)	Snapshot ()	Size (GiB) (j)	Volume Type (j)	IOPS (j)	Throughput (MB/s) (i)	Delete on Termination ()	Encryption (i)			
Root	/dev/xvda	snap-Odf46985105e80cb8	1000	General Purpose SSD (gp2)	3000	N/A		Not Encrypted	•		
Add New Volume											
Free tier eligible custo	omers can get up to 3	30 GB of EBS General Purpose (SS	D) or Magnetic storage	ge. Learn more about free usage tier eligibilit	y and usage						
restrictions.											
									Cancel F	rrevious Review an	d Launch Nex
									Cancel F	revious Review and	d Launch Nez
									Cancel F	revious Review an	d Launch Nez
● Easthack (A En	ualish (IIS)						0.000	1010 Amazon Web See	Cancel F	revious Review an	d Launch Nez
🗬 Feedback 🕑 En	kglish (US)						\$ 2008 -	1019, Amazon Web Serv	Cancel F	revious Review an	d Launch Nez Privacy Policy
🗣 Feedback 🍳 En	glish (US)						e 2008 -	1019, Amazon Web Serv	Cancel F rices, Inc. or its affi	rrevious Review an	d Launch Nez Privacy Policy
🗨 Feedback 🚱 En	ıglish (US)						¢ 2018 -	1019, Amazon Web Serv	Cancel F rices, Inc. or its affi	revious Review an	d Launch Nez Privacy Policy
e Feedback @ En	glish (US)	ssany Tags n	nav helr	Nou manage a	large	r numh	exer of instan	1019, Amazon Web Ser	Cancel F rices, Inc. or its affi	revious Review ar intes Allrights reserved στι uisch heri	d Launch Nez
₹ Feedback @ En Id tags,	glish (US) if neces	ssary. Tags n	nay help	o you manage a	large	r numb	exut-	1019, Amazon Web Serv CES OT C	Cancel F rece, Inc. or its affi disting	revious Review an lates. All rights reserved guish bet	d Launch Nez Privacy Policy
₹ Feedback @ En	glish (US) if neces	ssary. Tags n	nay help	o you manage a	large	r numb	e zore : Deer of instan	1019, Amazon Web Serv Ces or c	Cancel F rices, Inc. or its affi disting	revious Review an Inten Attopharmserved guish bet	d Launch Nez Privacy Policy
Feedback @ En Id tags,	glish (US) if neces	ssary. Tags n	nay help	o you manage a	large	r numb	exem- per of instan	1019 Amazon Web Son Ces or c	Cancel F Kees, Inc. or its affi disting	revious Review ar istes All rights resorved guish bet	d Launch Nez Privacy Policy WEEN
♥ Feedback ♥ Ef Id tags , milar ins	gliah (US) if neces tances.	ssary. Tags n	nay help	o you manage a	large	r numb	exour ber of instan	1019, Amazon Web Sen CES OT C	Cancel F Keet, Inc. of its aff disting	revious Review ar lates All optis reserved guish bet	d Launch Nez Privacy Policy



8. **Configure security group** rules. SSH and HTTP/HTTPS should be allowed from selected network segments. Here, consider adding ICMP rules to allow ping or TCP/UDP rules to allow connection to the Flowmon Collector listeners on specific ports.



AWS Services - Resource	ce Groups 🗸 🔸		۵), N. Virginia + S	iupport 👻
1. Choose AMI 2. Choose Instance Type 3. 0	Configure Instance 4. Add Storage 5. Add Tags	6. Configure Security Group 7. Review			
Step 6: Configure Security G A security group is a set of firewall rules that con HTTP and HTTPS ports. You can create a new s	roup ntrol the traffic for your instance. On this page, you ecurity group or select from an existing one below	ı can add rules to allow specific traffic to reach your instance. I t. Learn more about Amazon EC2 security groups.	For example, if you want to set up a web server and allow Internet tra	affic to reach your instance, add rules that allow unrestricted a	access to the
Assign a security group:	Create a new security group				
	Select an existing security group				
Security group name:	flowmon-collector-va-mgmnt-sg				
Description:	Flowmon Collector VA SG created 2019-09-03	T13:13:01.112+02:00			
Туре (і)	Protocol (j)	Port Range (j)	Source ()	Description (i)	
SSH T	TCP	22	Custom • 0.0.0/0	SSH for access to the flowmon user account	8
HTTPS •	TCP	443	Custom • 0.0.0.0/0, ::/0	HTTPS for access to the web GUI	8
Add Rule					
Warning Rules with source of 0.0.0.0/0 allow	all IP addresses to access your instance. We reco	mmend setting security group rules to allow access from know	vn IP addresses only.		

Cancel Previous Review and Launch

9. Review and Launch the instance.

🗨 Feedback 🔇 English (US)

Choose AMI 2. Choose								
	Instance Type 3. C	Configure Instance	4. Add Storage 5. Ad	dd Tags 6. Configure Security Group	7. Review			
en 7 [.] Review Ir	istance Lau	nch						
ise review your instance	launch details. You	can go back to e	edit changes for each sect	tion. Click Launch to assign a key pair t	o your instance and complete the launch p	rocess.		
	instances' con	urity. Your co	ourity group, flowing	on collector ve mampt ea is o	con to the world			
Your instances n	nay be accessible fro	om any IP addre	ss. We recommend that y	ou update your security group rules to a	allow access from known IP addresses only	у.		
You can also ope	en additional ports ir	n your security g	roup to facilitate access to	o the application or service you're runni	ing, e.g., HTTP (80) for web servers. Edit se	ecurity groups		
•								
A Your instance To launch an inst	e configuration i tance that's eligible f	is not eligible for the free usag	e for the free usage t tier, check your AMI sele	ller ection, instance type, configuration opti	ons, or storage devices. Learn more about	free usage tier eligibility and usage rest	trictions.	
								Don't show me this ag
AMI Details							Edit AM	
Flowmon C	ollector VA v10.01	BYOL 156742	3193 - ami-0e8c71ab36	5e2e2f1e				
Virtual applia	ince for Flowmon Coll	lector v10.01 BYC	DL. Version for a Bring-Your-	Own-License deployment. Built at 156742	3193.			
Root Device Ty	pe: ebs Virtualization to	ype: hvm						
nstance Type							Edit instance type	
Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance		
t2 vlarna	Variable	4	16	EBS only		Moderate		
t2.xlarge	Variable	4	16	EBS only		Moderate		
t2.xlarge Security Groups	Variable	4	16	EBS only		Moderate	Edit security groups	
t2.xlarge Security Groups	Variable	4	16	EBS only		Moderate	Edit security groups	
t2.xlarge Gecurity Groups Security group name Description	Variable flowmon-c: Flowmon C	4 ollector-va-mgm Collector VA SG (16 int-sg created 2019-09-03T13:13	EBS only :01.112+02:00		Moderate	Edit security groups	
t2.xlarge Security Groups Security group name Description	Variable flowmon-ce Flowmon C	4 ollector-va-mgm Collector VA SG (16 int-sg created 2019-09-03T13:13	EBS only 801.112+02:00	Source ()	Moderate	Edit security groups	
t2.xlarge Security Groups Security group name Description Type ①	Variable flowmon-cr Flowmon C	4 ollector-va-mgm collector VA SG o Protocol ()	16 Int-sg created 2019-09-03T13:13	EBS only k01.112+02:00 Port Range (j)	Source ①	Moderate Description ① SSH for access to	Edit security groups	
t2.xlarge Security Groups Security group name Description Type () SSH HTTPS	Variable flowmon-c: Flowmon C	4 collector-va-mgm collector VA SG o Protocol (j) TCP TCP	16 Int-sg created 2019-09-03T13:13	EBS only k01.112+02.00 Port Range ① 22 443	- Source () 0.0.0.00 0.0.0.00	Moderate Description () SSH for access to HTTPS for access t	Edit security groups	
t2.xlarge Security Groups Security group name Description Type () SSH HTTPS HTTPS HTTPS	Variable flowmon-c- Flowmon C	4 collector-va-mgm collector VA SG of Protocol () TCP TCP TCP	16 Int-sg created 2019-09-03T13:13	EBS only 101.112+02.00 Port Range ① 22 243 443	- Source () 0.0.0.0 0.0.0.0 ::0	Moderate Description ① SSH for access to HTTPS for access to HTTPS for access t	Edit security groups	
t2.xlarge Security Groups Security group name Description Type () SSH HTTPS HTTPS Instance Details	Variable flowmon-c- Flowmon C	4 collector-va-mgm collector VA SG of Protocol () TCP TCP TCP	16 wnt-sg created 2019-09-03T13:13	EBS only h01.112+02:00 Port Range ① 22 443 443	Source () 0.0.0.0 0.0.00 	Moderate Description ① SSH for access to HTTPS for access t HTTPS for access t	Edit security groups	
t2.xlarge Security Groups Security group name Description Type ① SSH HITTPS Instance Details	Variable flowmon-c- Flowmon C	4 ollector-va-mgm collector VA SG (Protocol () TCP TCP TCP	16 nnt-sg created 2019-09-03113-13	EBS only 8:01.112+02:00 Pert Range ① 22 443 443	Source ① 0.0.0.00 0.0.0.0 ⊐0	Moderate Description () SSH for access to HTTPS for access t HTTPS for access t	Edit security groups	
t2.xlarge Security Groups Security group name Description Type ① SSH HITPS Instance Details Storage	Variable flowmon-c- Flowmon C	4 ollector-va-mgm protocol ① TCP TCP	16 Int-sg created 2019-09-03T13-18	EBS only k01.112+02.00 Port Range ① 22 443 443	Source () 0.0.0.00 0.0.00 ⊐0	Moderate Description ① SSH for access to HTTPS for access t HTTPS for access t	Edit security groups Edit instance details Edit storage	
t2.xlarge Security Groups Security group name Description Туре () SSH HTTPS HTTPS HTTPS Instance Details Storage Гаgs	flowmon-cc Flowmon C	4 ollector-va-mgm collector VA SG of Protocol ① TCP TCP	16 Infrag (2019-09-03113:13 (1)	EBS only k01.112+02.00 Port Range ① 22 443 443	Source () 0.0.0.0/0 	Moderate Description ① SSH for access to HTTPS for access t HTTPS for access t	Edit security groups Edit instance details Edit storage Edit storage	
t2.xlarge Security Groups Security group name Description Type () SSH HTTPS Instance Details Storage Tags	Rowmon-c- Flowmon C	4 ollector-va-mgm collector VA SG of Protocol ① TCP TCP TCP	16 Integ created 2019-09-03T13-13	EB3 only 101.112+02:00 Port Range ① 22 24 443 443	Source () 0.0.0.0 0.0.0.0 ⇒0	Moderate Description () SSH for access to HTTPS for access to HTTPS for access t	Edit security groups Edit instance details Edit sorage Edit sorage Edit tags	Previous



10. Provide or generate an SSH key pair for initial instance access. Launch Instances.

Select	an existing key pair or create a new key pair
A key pair o allow you t obtain the securely SS	consists of a public key that AWS stores, and a private key file that you store. Together, the o connect to your instance securely. For Windows AMIs, the private key file is required to password used to log into your instance. For Linux AMIs, the private key file allows you to SH into your instance.
Note: The s about remo	selected key pair will be added to the set of keys authorized for this instance. Learn more oving existing key pairs from a public AMI .
Create	e a new key pair 🔹
Key pa	ir name
	Download Key Pair
	You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.
	Cancel Launch Instances
	Cancel Launch Instances

11. Wait for the launched instance to be Running.

Virtual Network Interfaces

By default, virtual machine instances in AWS EC2 are created with a single virtual network interface. In order to fully utilize the deployed appliance, to use it as a probe as well as a collector, you need to add at least one additional virtual network interface. In total, the appliance supports four virtual network interfaces, two for management and two for monitoring. The following steps outline the basic configuration, please, keep in mind that they may need to be adjusted for your deployment and use case.

Create a virtual network interface in the VPC and subnet used for traffic mirroring. This interface will be your **Mirror Target** when you configure Amazon VPC Traffic Mirroring. The security group should allow incoming **UDP** traffic on port **4789** from the mirrored subnet.



Services 🗸 Resource Groups 🗸 🛧

N. Virginia 👻 Support 👻

Network interfaces > Create Network Interface

aws

Description	flowmon-collector-va-mon-1			9		
Subnet*	subnet-f06a49b8	3	-	C 0		
IPv4 Private IP Auto-assign Custom						
Elastic Fabric Adapter	•					
Secur	rity groups* sg-0:	2434ac61275ddff6 🔅	0			
					•	
		Q Filter by attributes o	r search by keyword		$ \langle \langle 1 \text{ to 10 of 10} \rangle \rangle$	
		Group ID 👻	Group name 🔹	Description	~	
		sg-02434ac61	Traffic Mirrorin	Enabled everything.		
		sg-0297216d3	launch-wizard-5	launch-wizard-5 created 2019-09-03T12:08:16.711+02:00		
		sg-051d04e8a	launch-wizard-7	launch-wizard-7 created 2019-04-15T19:53:20.699+02:00		
		sg-0b96764dd	launch-wizard-3	launch-wizard-3 created 2019-09-02T13:41:51.910+02:00		
		sg-0bd92d446	flowmon-collec	Flowmon Collector VA SG created 2019-09-03T13:13:01.112+02:00		
		sg-0e3ba9f5ffc	launch-wizard-6	launch-wizard-6 created 2019-04-15T14:57:02.690+02:00		
		sg-0eb6bbb0f3	launch-wizard-4	launch-wizard-4 created 2019-09-03T09:29:03.433+02:00		
		sg-1d86256a	launch-wizard-2	launch-wizard-2 created 2018-02-01T10:16:52.199+01:00		
		sg-5d8b902c	default	default VPC security group		
		sg-9b1fb7ec	launch-wizard-1	launch-wizard-1 created 2018-02-02T11:49:07.500+01:00		

Flowmon Configuration

Please refer to Post-installation Steps.



Amazon VPC Traffic Mirroring

Overview

Flowmon takes advantage of Amazon Virtual Public Cloud (Amazon VPC) traffic mirroring in AWS to help customers get an instant insight, to resolve network performance issues, identify optimization opportunities and secure infrastructure across different environments to support business-critical services.



The aim is to mirror the network traffic passing through a desired network interface (**eni-a** in the figure below) and send it to an interface where the mirrored traffic can be processed, visualized and analyzed with Flowmon Collector (**eni-b** in the figure below).



Utilization of AWS traffic mirroring in achieving network visibility with Flowmon Collector.

Prerequisites

- 1. A running instance of Flowmon for AWS.
- 2. A number of running client instances where traffic mirroring can be configured.
- 3. A deployment compliant with Traffic Mirroring Limits and Considerations.

Deployment

In order to configure VPC traffic mirroring in AWS, you have to perform the following steps:

- Overview
- Prerequisites
- Deployment
 - Create Traffic
 Mirror Target
 - Create Traffic
 - Mirror Filter

 Create Traffic
 - Mirror Session
 - Allow VxLAN
 - Traffic To Collector
- Flowmon Configuration



- 1. Create a Traffic Mirror Target
- 2. Create a **Traffic Mirror Filter**
- 3. Create a Traffic Mirror Session
- 4. Allow VxLAN traffic to collector

Create Traffic Mirror Target

- 1. In AWS Web Console, choose the **VPC** service.
- 2. Choose Mirror Targets in the Traffic Mirroring section.
- 3. Click on the Create traffic mirror target button.
- 4. Choose any name and description you want, but it is important that the **Target type** is **Network Interface** and the **Target** is Flowmon's monitoring interface.
- 5. Create the mirror target.

Target settings

A description to help you identify the traffic mirror target

Name tag - optional

Flowmon Collector eth2

Description - optional

AWS vTAP test

Choose target

Target type cannot be modified after creation ...

Target type

Network Interface

Target

Q eni-0ef49a0c06452b895

Create Traffic Mirror Filter

- 1. Choose Mirror Filters in the Traffic Mirroring section.
- 2. Click on the **Create traffic mirror filter** button.
- 3. Choose any name and description you want.
- 4. Describe the type of inbound and outbound traffic you want to be mirrored (all traffic, in our example in the picture below).
- 5. Create the mirror filter.



Sort rules

Inbound rules - optional

Number	Rule action	Protocol	Source port range	Destination port range	Source CIDR block	Destination CIDR block	Description
100	accept 💌	All protocols	▼ N/A	N/A	0.0.0/0	0.0.0/0	٥
Add rule							
Outbound ru	ıles - optional						Sort rules

Number	Rule action	Protocol	Source port range	Destination port range	Source CIDR block	Destination CIDR block	Description	
100	accept 🔻 A	Il protocols	▼ N/A	N/A	0.0.0.0/0	0.0.0/0		0

Create Traffic Mirror Session

- 1. Choose Mirror Sessions in the Traffic Mirroring section.
- 2. Click on the **Create traffic mirror session** button.
- 3. Choose any name and description you want.
- 4. Set virtual instance's port as the Mirror source.
- 5. Provide Mirror target and Mirror filter created in Steps 1 and 2.
- 6. Create the mirror session.

Session settings

Set description, source, and target

Name tag - optional

Monitored Server

Description - optional

vTAP from Monitored Server to Flowmon Collector eth2

Mirror source

The resource that you want to monitor.

Q eni-07d28ec06ed52f6ad

Only network interfaces of type "interface" are allowed.

Mirror target

A network interface, or a network load balancer that is the destination for mirrored traffic.

Q tmt-063853a4c6e9e543e

Allow VxLAN Traffic To Collector

All mirrored traffic is encapsulated with VxLAN protocol which works over UDP on port 4789.

- 1. In AWS Web Console, choose the **EC2** service.
- 2. Find the Security Group applied to Flowmon's monitoring interface in the Security groups panel.
- 3. Add inbound rule to enable receiving VxLAN traffic from IP address of virtual instance's interface.



4. Save the inbound rule.

Description	Inbound	Outbound	Tags			
Edit						
Type (j)				Protocol (j)	Port Range (j)	Source (j)
Custom UDF	P Rule			UDP	4789	172.31.16.0/20

Flowmon Configuration

- 1. Go to Flowmon Configuration Center of your Flowmon Collector.
- 2. Choose the **Monitoring Ports** panel.
- 3. Under **Global settings -> Advanced settings** enable **VxLAN** decapsulation on port **4789**.
- 4. Click on the **Save** button.

Global settings							
Packet sampling rate 0							
Light mode							
OPTIONAL L2 VALUES FOR NETFLOW RECORD OPTIONAL	L3/L4 VALUES FOR IPFIX RECORD OPTION	AL L7 VALUES FOR IPFIX RECORD					
✓ MAC ✓ L3/L4 ext	ended 🕑 DHC	MSSQL	IEC 104				
MPLS NPM	DNS	PostgreSQL	COAP				
Auto Select decansulation mode of MPLS packets	NPM 🗹 HTT	MySQL					
	Emai	TLS main					
VLAN VLAN	✓ NBAI	₹2 ILS client					
	Saml	a ILS certificate	2				
	VolP	TLS JA3					
	5060	Select VoIP SIP ports					
DECAPSULATE TUNNEL PROTOCOLS							
GRE							
ESP							
✓ VxLAN							
4789 Select VxLAN port							
EDSDAN							
PPPoF							
Add L2 values enabled for NetFlow record to the key fields							
Use autonomous system list							
Default AS list O Custom AS list							
a save							


Amazon VPC Flow Logs

Overview

The AWS FlowLog Converter is a configurable module of Flowmon Monitoring Center (FMC). It enables the user to collect, process and visualize AWS VPC Flow Logs (further referred to as flow logs) which contain information about the traffic captured in Amazon Virtual Private Cloud.

The flow logs are periodically acquired from Amazon CloudWatch, processed, converted to IPFIX format and subsequently sent to Flowmon Collector to a defined UDP port. Flowmon Collector treats data from this port as regular flows recovered from any other port.

- Overview
- Prerequisites
- Deployment
- Flowmon Configuration
- Limitations

Prerequisites

To set up the flow logs in your cloud and forward them to AWS CloudWatch, please follow the instructions specified in the official AWS Flow Logs documentation. It is important that every flow log stream contains flow logs from one interface only.

Deployment

To start receiving flow logs in Flowmon Monitoring Center, follow these instructions.

First, configure the access information, regions and log groups from which the flow logs will be retrieved.

Configuration Center -> FMC Configuration -> AWS Flow Logs

The access key ID and the secret access key are mandatory credentials provided by Amazon.

Select any suitable listening port, the port must accept **UDP** with flows in **IPFIX**.

AWS Flow Logs			
Enable			
Access key ID	YourAWSKeyID		
Access key secret			
Listening port	AWS Flow Logs •		
Regions			
NAME		DESCRIPTION	ACTION
1 No data			
			+ ADD REGION

SAVE > VERIFY

Click the Add Region button to configure the endpoints where the flow logs should be retrieved.

Insert the name of the region (without availability zone) in which your flow logs are physically stored. List of all possible regions can be found here. Note that the region **Name** field is expected to contain values like *eucentral-1* rather than *EU (Frankfurt)*. It is also possible to define short description of the region.



Lastly, it is necessary to provide at least one log group (by clicking the **Add group** button and filling in the name). All flow log streams in the provided group will be processed and every stream will be shown as a unique interface of the log group in the **Monitoring Center**.

Flow Logs			
Add region	1	×	
Name	eu-central-1		
s ke Description	Some description		
t Groups			
	NAME	ACTION	
HelloFlowmo	n	/ II	ACTION
data	здGroup	Z 1	
		+ ADD GROUP	
		OK CLOSE	
> VERIFY			

The provided configuration can be optionally verified by clicking the **Verify** button. This will check whether the FMC is able to connect to the specified log groups using the provided AWS credentials.

Note that the provided configuration undergoes the verification process every time the **Save** button is clicked.

Visi Frow Logs	Alliage		×		
eu-central-1: eu-central-1: ter eu-nonexistent:	HelloFlowmon - ThirdGroup -	Failure. Log group does not en Failure. The entered region do problem with network connect	xist. The set of the s		
	NAME			DESCRIPTION	ACTIO
central-1			Some description		Z 1
nonexistent					/ 1

Newly created configuration must be saved (by clicking the **Save** button). This will start the process of retrieving the Flow logs. To stop the process of retrieving, disable it and click the **Save** button.

Flowmon Configuration

It can take up to 20 minutes (see Limitations) before first flow logs can be visualized.

Every log group has internally assigned a unique IP address (from subnet 127.128.0.0/16) and is treated as a unique flow source.

All sources can be found in **Flowmon Monitoring Center -> Sources.**



Click the **Profile** button to see traffic of the individual streams.

Select all available streams and click the **Save** button.



Switch to: Flowmon Monitoring Center -> Profiles -> Sources -> Your Log Group

It is possible to view and analyze flows from flow logs as if they were flows from regular data sources.



Limitations

There are some limitations which stem from the flow logs themselves that need to be taken into account.

- If your network interface has multiple IPv4 addresses and traffic is sent to a secondary private IPv4 address, the flow log displays the primary private IPv4 address in the destination IP address field.
- If traffic is sent to an ENI and the destination is not any of the ENI IP addresses, the flow log displays the primary private IPv4 address in the destination IP address field.
- If traffic is sent from an ENI and the source is not any of the ENI IP addresses, the flow log displays the primary private IPv4 address in the source IP address field.
- If traffic is sent to or sent by a network interface, the flow log always displays the primary private IPv4 address, regardless of the packet source or destination, in the interface IP address field.

Flow logs do not capture all IP traffic. The following types of traffic are not logged:

- Traffic generated by instances when they contact the Amazon DNS server. If you use your own DNS server, then all traffic heading to that DNS server is logged.
- Traffic generated by a Windows instance for activation of the Amazon Windows license.
- Traffic to and from 169.254.169.254 for the instance metadata.
- Traffic to and from 169.254.169.123 for the Amazon Time Sync service.
- DHCP traffic.



- Traffic to the reserved IP address for the default VPC router. For more information, see VPC and Subnet Sizing.
- Traffic between an endpoint network interface and a Network Load Balancer network interface. For more information, see VPC Endpoint Services (AWS PrivateLink).
- Some flow log records might get skipped during the capture window. This may be because of an internal capacity constraint, or an internal error.
- The delay between the time when the traffic actually occurred and the time it can be seen in Monitoring Center can reach up to 20 minutes in the worst case scenario, however; the delay will get smaller with a higher amount of traffic volume present in the monitored cloud. This is caused by the 10-15 minutes capture window in which the packets are aggregated to the flow logs before being published, and by the subsequent 5 minutes delay before Flowmon Collector closes the current profile and shows the traffic in the GUI.

Flowmon Collector stores incoming flows to a currently opened profile, and therefore it is advised to select multiple adjacent profiles when searching for flows in a particular time.



Flowmon for Azure

Overview

Flowmon for Azure gives network administrators and security engineers insight into what is happening in their cloud infrastructure. Its powerful features can be used to gain control of bandwidth utilization, optimize network and application performance, reduce time to resolution during troubleshooting and keep the infrastructure protected against modern cybersecurity threats.

Flowmon for Azure is

- published in the official Azure Marketplace,
- deployed in the form of an Azure Virtual Machine Instance,
- capable of collecting as well as generating flow data,
- suitable for cost optimization with dynamic instance resizing based on current/planned utilization,
- fully under customer's control including updates, backups, and configuration.

Flowmon for Azure supports

- native traffic mirroring with Azure Virtual Network TAP (in selected regions, as a preview),
- 3rd party vTAP solutions such as Garland Prisms, Ixia CloudLens, or Gigamon.

Features

Flowmon for Azure supports three modes of operation:

- Probe,
- Collector,
- Collector and Probe.

Flowmon Probe

In this mode, the virtual appliance acts as a Flowmon Probe. It accepts mirrored traffic on monitoring ports and exports flow data to at least one remote Flowmon Collector instance.

Supported traffic mirroring solutions:

• Azure Virtual Network TAP

Supported 3rd-party packet brokers:

- Ixia CloudLens
- Gigamon
- Garland Prisms

Flowmon Collector

In this mode, the virtual appliance acts as a Flowmon Collector and accepts supported flow formats from external probes, network devices on management ports. For details on supported flow sources and formats, refer to the official Flowmon User Guide.

- Overview
 - Features
 - Licensing
 - Azure Marketplace
 - Prerequisites
 - Deployment
 - Virtual Network Interfaces
 - Virtual Disks
 - Flowmon Configuration



Flowmon Collector and Flowmon Probe

In this mode, the virtual appliance acts both as a Flowmon Probe and Flowmon Collector. Probe sends data to the locally available Collector. For details on configuration, refer to the official Flowmon User Guide.

Licensing

Flowmon for Azure is a virtual appliance with a Bring-Your-Own-License (BYOL) support.

With **BYOL**, you can apply for a Free Trial License at flowmon.com.

For support or inquiries, see our contact information.

Azure Marketplace

Flowmon for Azure is available as a Virtual Appliance (VA) in Azure Marketplace.



Prerequisites

In order to follow this guide, you need the following:

- 1. A web browser compatible with the Azure Portal.
- 2. A trial license from flowmon.com.
- 3. An active Azure user account with a subscription (free or paid).

Deployment

The deployment of Flowmon for Azure consists of the following steps:

1. Log in to the Azure Portal.



- 2. Navigate to the Azure Marketplace page for Flowmon.
- 3. Get It Now!
- 4. **Continue** with the deployment in the Azure Portal.
- 5. **Create** a virtual machine instance.
- 6. Provide mandatory information such as **Virtual machine name**, **Resource group**, **SSH key** for the **flowmon** user account, etc.



You can use Flowmon Collector Model List to estimate the correct sizing of your instance.

🛕 Changing Basic options may rese	et selections you have made. Review all options prior to creating the virtual machine.	
Basics Disks Networking	Management Advanced Tags Review + create	
Create a virtual machine that runs Li image. Complete the Basics tab ther for full customization. Learn more c	inux or Windows. Select an image from Azure marketplace or use your own cust n Review + create to provision a virtual machine with default parameters or revie ?	omized ew each tab
Project details		
Select the subscription to manage d your resources.	leployed resources and costs. Use resource groups like folders to organize and r	nanage all
Subscription * (i)		~
Resource group * ()	(New) flowmon-deployment_group Create new	~
Instance details		
Virtual machine name * 🛈	flowmon-deployment	
Region * 🛈	(Europe) West Europe	~
Availability options ①	Availability zone	~
	High availability is recommended for production workloads.	
Availability zone * 🕕	1	~
Image * i	Flowmon for Azure - v11.0 Browse all public and private images	~
Azure Spot instance ①	Ves No	
Size * 🛈	Standard_D4s_v3 - 4 vcpus, 16 GiB memory (€147.75/month)	\sim
	D-series is recommended for general purpose workloads.	
Administrator account		
Authentication type ①	SSH public key Password	
	Azure now automatically generates an SSH key pair for you and allo store it for future use. It is a fast, simple, and secure way to connect virtual machine.	ws you to to your
Username * 🕕	flowmon	
SSH public key source	Generate new key pair	~



7. In **Disks**, add an additional block device to serve as data storage. Select disk types suitable for your performance vs. cost requirements.

Creat	e a vi	rtual mad	:hine						
Basics	Disks	Networking	Management	Advanced	Tags	Review -	+ create		
Azure VM The size o	Is have or of the VM	ne operating syste determines the t	em disk and a temp ype of storage you	oorary disk for s can use and th	short-term e number	storage. Y of data dis	ou can attach add sks allowed. Lear	ditional data n more	a disks.
Disk opt	tions								
OS disk t	ype * 🛈		Standard	SSD					\sim
			The selecte high IOPS 99.9% con	ed VM size sup workloads. Virt nectivity SLA.	ports prei tual mach	mium disks ines with P	s. We recommend remium SSD disk	d Premium cs qualify fo	SSD for or the
Encryptic	on type *		(Default)	Encryption at-r	est with a	platform-n	nanaged key		\sim
Enable U	ltra Disk (compatibility 🛈	🔵 Yes (No					
Data dis	ks								
You can a	add and o	onfigure addition	al data disks for yo	ur virtual mach	ine or atta	ch existing	disks This VM al	so comes w	/ith a
temporar	ry disk.					ich existing			
temporal	ry disk. N	lame	Size (GiB	3) Disk	type		Host caching		
temporal LUN 0	ry disk. N	lame owmon-deploym	Size (GiB ent 1024	l) Disk Prem	type nium SSD		Host caching Read-only	~	1
LUN 0 Create ar	ry disk. N fl	lame owmon-deploym a new disk At	Size (GiB ent 1024 tach an existing dis	8) Disk Prem	type nium SSD		Host caching Read-only	~	1
LUN 0 Create ar	ry disk. N fl nd attach a vanced	lame owmon-deploym a new disk At	Size (GiB ent 1024 tach an existing dis	8) Disk Prem Sk	type nium SSD		Host caching Read-only	~	Î 0
LUN 0 Create ar	ry disk. N fl nd attach a vanced Jse manaa	lame owmon-deploym a new disk At ged disks ①	Size (GiB ent 1024 tach an existing dis	8) Disk Prem Sk	type nium SSD		Host caching Read-only	~	1
LUN 0 Create ar	ry disk. N fl nd attach : vanced Jse manag	lame owmon-deploym a new disk At ged disks ①	Size (GiB ent 1024 tach an existing dis Ava	e) Disk Pren sk) No • Yes ailability zone (type nium SSD	nanaged di	Host caching Read-only	~	1
LUN 0 Create ar	ry disk. N fl nd attach a vanced Jse manag	lame owmon-deploym a new disk At ged disks ① neral OS disk ①	Size (GiB ent 1024 tach an existing dis Ava	e) Disk Prem sk) No O Yes ailability zone f	type nium SSD	nanaged di	Host caching Read-only	~) Î <i>O</i>
LUN 0 Create ar	ry disk. N fl nd attach a vanced Jse manag	lame owmon-deploym a new disk At ged disks ① neral OS disk ①	Size (GiB ent 1024 tach an existing dis Ava	e) Disk Prem sk) No • Yes ailability zone () No • Yes	type nium SSD	nanaged di	Host caching Read-only	~	〕
LUN 0 Create ar	ry disk. N fl nd attach i vanced Jse manag	lame owmon-deploym a new disk At ged disks ① neral OS disk ①	Size (GiB ent 1024 tach an existing dis Ava O	e) Disk Pren sk) No • Yes ailability zone () No • Yes	type iium SSD	nanaged di	Host caching Read-only	~	1
LUN O Create ar	ry disk. N fl nd attach : vanced Jse manag	lame owmon-deploym a new disk At ged disks () neral OS disk ()	Size (GiB ent 1024 tach an existing dis Ava 	e) Disk Prem sk	type iium SSD	nanaged di	Host caching Read-only	~	
LUN O Create ar	ry disk. N fl nd attach a vanced Jse manag	lame owmon-deploym a new disk At ged disks () neral OS disk ()	Size (GiB ent 1024 tach an existing dis Ava 	e) Disk Prem sk	type iium SSD	nanaged di	Host caching Read-only	~	
LUN O Create ar	ry disk. N fl nd attach a vanced Jse manag	lame owmon-deploym a new disk At ged disks () neral OS disk ()	Size (GiB ent 1024 tach an existing dis Ava 0	e) Disk Prem sk) No O Yes ailability zone n) No O Yes	type nium SSD	nanaged di	Host caching Read-only	~	



8. In **Networking**, review network interface settings and adjust them based on the specifics of your network topology.

opology.	
Create a virtual machi	ine
Basics Disks Networking M	lanagement Advanced Tags Review + create
Define network connectivity for your vir ports, inbound and outbound connectiv Learn more	tual machine by configuring network interface card (NIC) settings. You can control rity with security group rules, or place behind an existing load balancing solution.
Network interface	
When creating a virtual machine, a netw	vork interface will be created for you.
Virtual network * 🛈	(new) flowmon-deployment_group-vnet
	Create new
Subnet * (i)	(new) default (10.0.0/24)
Public IP	(new) flowmon-deployment-ip
	Create new
NIC network security group ①	O None O Basic Advanced
	(i) This VM image has preconfigured NSG rules
Configure network security group *	(new) flowmon-deployment-nsg
	Create new
Accelerated networking	On Off
	The selected image does not support accelerated networking.
Load balancing	
You can place this virtual machine in the	e backend pool of an existing Azure load balancing solution. Learn more
Review + create	revious Next · Management >
Review + create	evious intext. Management >



9.	In Management.	make sure Boot diagnostics are enabled.
----	----------------	--

Create	e a vi	rtual ma	chine				
Di	Dista	Naturalian			T	Deview to anothe	
Basics	DISKS	Networking	Manageme	Advanced	lags	Review + create	
Configure	monitori	ng and manag	ement options fo	or your VM.			
Azure Se	curity Ce	enter					
Azure Sec Learn mo	urity Cent pre	ter provides ur	ified security ma	nagement and adva	anced thre	at protection across hybri	d cloud workloads.
🥑 Your	subscript	ion is protecte	d by Azure Secur	ity Center basic pla	n.		
Monitori	ng						
Boot diag	nostics (ī)	o o	n 🔿 Off			
			₿ B	oot diagnostics is r	ecommen	ded for production work	loads.
Diagnosti	cs storag	e account * 🤇) (new) flowmondeployme	entgroupd	i	\checkmark
			Create	new			
Identity							
System as	signed m	nanaged identi	ty 🗊 🔿 o	n 💿 Off			
Azure Ac	tive Dire	ctory					
Login witl	h AAD cre	edentials (Prev	iew) 🛈 🔿 o	n 💿 Off			
🛕 Thi	s image d	oes not support	Login with AAD.				
Review	+ create		< Previous	Next : Advance	ed >		

10. **Review + create** the new instance.



11. Wait for the deployment to finish and retrieve the machine's **public IP address** from its details.

~	Your deployment is complete							
=	Deployment name: CreateVm-flowmon_flowmon_collector-preview Start time: 6/20/2020, 3:33:15 PM							
	Resource group: flowmon-deployment_group							
/	∖ De	eplov	vment details (Dowr	nload)				
	Resource Type Status Operation details							
		V	flowmon-deployment		Microsoft.Compute/virtualMachines	ОК	Operation	details
		V	flowmon-deployment		Microsoft.Network/networkInterfaces	Created	Operation	ı details
		v	flowmon-deployment	_DataDisk_0	Microsoft.Compute/disks	ОК	Operation	details
		V	flowmondeployment	jroupdi	Microsoft.Storage/storageAccounts	ок	Operation	details
		V	flowmon-deployment	_group-vnet	Microsoft.Network/virtualNetworks	ОК	Operation	details
		V	flowmon-deployment		Microsoft.Network/publicIpAddresses	ОК	Operation	details
		V	flowmon-deployment	-nsg	Microsoft.Network/networkSecurityGrou	u OK Operation det		details
		ovte	tons					
	· 11	exts	teps					
		Setu	p auto-shutdown Rec	commended				
		Mon	itor VM health, perform	mance and network d	ependencies Recommended			
		Kuna	a script inside the virtu	ai machine Recomm				
				Create another VM				
	flo	own	non-deploymen	nt x²				
	Virtu	ual mac	chine	Connect N start	C Bartant 🔲 Stars 🕅 Caratura 🏛 Dalata 🖒	Defeat		
	Overv	iew		Resource group (change) :	flowmon-deployment group	Reliesh	Operating system : Linux (centos 7.7.1908)
	Activit	ty log		Status :	Running		Size : Standar	rd D4s v3 (4 vcpus, 16 GiB memory)
જ્	Acces	s contr	ol (IAM)	Location :	West Europe (Zone 1)		Public IP address : 51.136.	
	Tags						Colocation status : N/A	
Þ	Diagn	iose an	d solve problems	Availability zone :			Virtual network/subnet : flowmo DNS name : Configu	n-deployment_group-vnet/default ure
Set	tings			Tags (change) :				
	Netwo	orking						
ø	Conne	ect		Proportion Monitorin	o Capabilitios Tutorials			
8	Disks Properties Monitoring Capabilities Tutorials							
	Size			Virtual machine			Networking	
۲	Securi	ity		Computer name	flowmon-deployment		Public IP address	
	Adviso	or reco	mmendations	Operating system	Linux (centos 7.7.1908)		Public IP address (IPv6)	-
E	Extens	sions		Publisher	flowmon		Private IP address (IPv6)	-
úß.	Contir	nuous o	delivery	VM generation	V1		Virtual network/subnet	
	Availa	bilib. 4	coling	Agont status	Porte		DNS name	

12. If you need to use this instance as Flowmon Probe, please refer to the Virtual Network Interfaces section below.

Virtual Network Interfaces

Once the new instance is running, you may provision additional monitoring interfaces (depending on your license). The most common configuration is **eth0** for management and **eth1/eth2** for monitoring.



Make sure to identify interfaces by MAC address inside the running instance, order and numbering may be different!

,⊃ Search (Ctrl+/) ≪	Search (Ctrl+/)								
 Overview Activity log 	Overview tp-vtap-fmc12 eth1 eth2 eth3 								
Access control (IAM)	Access control (IAM)								
🛷 Tags	Tags Virtual network/subnet: tp-vtap-test-vnet/default NIC Public IP: 13.77.204.187 NIC Private IP: 10.0.5.4 Accelerated networking: Disabled								
X Diagnose and solve problems	X Diagnose and solve problems								
Settings	Network secur	ity group to stap fmc-psg (attached to	network interface: to	-vtan-fmc12)					
🖄 Networking	Impacts 0 subn	ets, 4 network interfaces	network interface. (p	vap merzy			Add Inbound po	int rule	
😂 Disks	PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION		
👰 Size	1010	HTTPS	443	тср	Any	Any	Allow		
Security	1020	🔺 SSH	22	ТСР	Any	Any	Allow		
E Extensions	65000	Allow/notinPound	A	A	VirtualNetwork	VirtualNaturati	Allow		
G Continuous delivery (Preview)	65000	Allowvnetinbound	Any	Any	virtualNetwork	VIrtualNetwork	Allow		
Availability set	65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow		

Virtual Disks

Once the new instance is running, you may provision additional data storage if you haven't already done that during the initial deployment process. It is recommended to store flow data on a disk other than the OS disk automatically provided with the instance. Adjust disk capacity based on your license.

8	ifc-vm D	Disks ৵	
Q	Search (Ctrl+/)	« 🔚 Save 🗙 Discard 💍 Refresh 🔑 Encryption 🤁 Swap OS Disk	
9	Overview	A	
	Activity log	Managed disks created since June 10, 2017 are encrypted at rest with Storage Service Encryption (SSE). You may also want to	enable Azure Disk Encryption.
ጵ	Access control (IAM)		
	Tags	Disk caching cannot be changed for L-Series and B-series virtual machines.	
ß	Diagnose and solve problems		
Set	tings	1 Ultra Disk compatibility is not available for this location.	
۵	Networking	Disk settings	
Ø	Connect	Enable Ultra Disk compatibility ①	
8	Disks	OS disk	
Ţ	Size	Name	Size
٩	Security	ifc-osdisk	100 GiB
¢.	Extensions		
6	Continuous delivery		The value must not be empty.
9	Availability + scaling		r.
	Configuration	The value must not be em	
8	Identity		
łł†	Properties	+ Add data disk	
۵	Locks	No managed disks available.	
<u>±</u>	Export template		

Flowmon Configuration

Please refer to Post-installation Steps.



Azure Virtual Network TAP

• The Azure Virtual Network TAP service preview is currently suspended by Microsoft and therefore unavailable for customer deployments.



Azure NSG Flow Logs v2

• Azure NSG Flow Logs (v2) are currently not supported by Flowmon Collector.



Flowmon for Google Cloud

Flowmon for Google Cloud gives network administrators and security engineers insight into what is happening in their cloud infrastructure. Its powerful features can be used to gain control of bandwidth utilization, optimize network and application performance, reduce time to resolution during troubleshooting and keep the infrastructure protected against modern cyber-security threats.

Flowmon for Google Cloud is

- published in the official Google Cloud Marketplace,
- deployed in the form of a Google Cloud Compute Instance,
- capable of collecting as well as generating flow data,
- suitable for cost optimization with dynamic instance resizing based on current/planned utilization,
- fully under customer's control including updates, backups, and configuration.

Flowmon for Google Cloud supports

- native traffic mirroring with VPC Packet Mirroring,
- 3rd party vTAP solutions such as Garland Prisms, Ixia CloudLens, or Gigamon.

Features

Flowmon for Google Cloud supports three modes of operation:

- Probe,
- Collector,
- Collector and Probe.

Flowmon Probe

In this mode, the virtual appliance acts as a Flowmon Probe. It accepts mirrored traffic on monitoring ports and exports flow data to at least one remote Flowmon Collector instance.

Supported traffic mirroring solutions:

Google Cloud VPC Packet Mirroring

Support 3rd-party packet brokers:

- Ixia CloudLens
- Gigamon
- Garland Prisms

Flowmon Collector

In this mode, the virtual appliance acts as a Flowmon Collector and accepts supported flow formats from external probes, network devices on management ports. For details on supported flow sources and formats, refer to the official Flowmon User Guide.

- Flowmon Virtual Appliances Rev. 41, 30/07/2021
- Overview
- Features
- Licensing
- Google Cloud Marketplace
- Prerequisites
- Deployment
- Virtual Disks
- Flowmon Configuration



Flowmon Collector and Flowmon Probe

In this mode, the virtual appliance acts both as a Flowmon Probe and Flowmon Collector. Probe sends data to the locally available Collector. For details on configuration, refer to the official Flowmon User Guide.

Licensing

Flowmon for Google Cloud is a virtual appliance with a Bring-Your-Own-License (BYOL) support.

With <u>BYOL</u>, you can apply for a Free Trial License at flowmon.com.

For support or inquiries, see our contact information.

Google Cloud Marketplace

Flowmon for Google Cloud is available as a Virtual Appliance (VA) in Google Cloud Marketplace.

	n	٩	•	2 0 + :
÷				
;;	Flowmon Collector for Google Cloud Flowmon Networks Estimated costs: \$0.00/month + BYOL license fee Comprehensive platform for flow-based NetSecOps LAUNCH ON COMPUTE ENGINE			
Runs on Google Compute Engine Type Bingle VM BYOL Last updated 12/29/19, 739 PM Category Networking Security Version Version CentOS 7 Package contents FlowmonOS 10.3.3	Overview Flowmon is a comprehensive platform for flow-based (NetFlow/IPFIX) network month weinything you need to get an absolute control over the network through network viabl doogle Cloud is a software appliance for collection, long-term storage, and analysis of a Flow, and othy designed for deployment in the Google Cloud environment. Learn more 12 About flowmon Network applications for tomatics and deal with cyber threats. Learn more Mount get the provider 12 About flow provi	vring and security. It provides filty: Flowmon Collector for flow data (NetFlow, IPFIX, wrks. With our high mr absolute network traffic le using licenses purchased you the flexibility to		
	Pricing This is a BYOL solution which requires a valid license to use. You are responsible for purchasing and managing your own licenses from Flowmon	Item Flowmon Networks license fee (RVOL)	Estimated costs Variee	
		- In the second se	Variets	

Prerequisites

In order to follow this guide, you need the following:

- 1. A web browser compatible with the Google Cloud Marketplace page.
- 2. A trial license from flowmon.com.
- 3. An active Google Cloud project with a billing account associated with it. Google Cloud's Free Trial credit is supported.

Deployment

The deployment of Flowmon for Google Cloud consists of the following steps:



- 1. Log in to the Google Cloud Console.
- 2. Navigate to the Google Cloud Marketplace page for Flowmon.
- 3. Select Launch on Compute Engine.
- 4. You will be presented with a deployment configuration/overview page.



5. Adjust properties of the deployment. Pay special attention to **Boot Disk** size and **Networking**. Minimal **Boot Disk** size is 40 (in GB). You will be able to add a second disk suitable for your storage requirements later (see Virtual Disks below).

Minimal number of **Network Interfaces** is 1 (for a management port), maximal number is 4 (for an additional management interface or monitoring ports used for the built-in Flowmon Probe). Every interface must be assigned to a different VPC with a non-overlapping subnet addressing scheme. The first interface will have an **Ephemeral Public IP** address automatically assigned during deployment.

- 6. Select Deploy.
- 7. You will be presented with the deployment status overview and further instructions.





8. Google Cloud's Deployment Manager will notify you once the deployment has finished. Follow on-screen instructions and log in to your running instance. Pay attention to **Admin URL**, **Admin user** and **Admin password**.

Virtual Disks

Once the new instance is running, you may provision additional data storage. It is recommended to store flow data on a disk other than the OS disk automatically provided with the instance. Adjust disk capacity based on your license.

۲	Compute Engine	← VM instance details	/ EDIT	[™] RESET
A	VM instances	Additional disks 🕜 (Optional)		
6 14	Instance groups	New disk (disk-1, Blank, 500 GB)		• ^
	Instance templates	Name 🕝 Name is permanent		
8	Sole-tenant nodes	disk-1		
	Machine images	Description (Optional)		
0	Disks			//
0	Snapshots	Type 💿 Standard persistent disk		-
	Images	Snapshot schedule	Scheduled snapst	nots [⁷
8	TPUs	No schedule		•
۲	Migrate for Compute Engi	Create snapshot schedules to autom your data	natically back up	Dismiss
·%·	Committed use discounts	Learn more about creating snapshot sch	edules 🖸	
≣≣	Metadata	Source type 🕖 Blank disk Image Snapshot		
ß	Health checks	Mode		
:::	Zones	 Read/write Read only 		
*	Network endpoint groups	Deletion rule When deleting instance		
٢	Operations	 Keep disk Delete disk 		
٢	Security scans	Size (GB) 📀 500		
-				



Flowmon Configuration

Please refer to Post-installation Steps.



Google Cloud VPC Packet Mirroring

Overview

Google Cloud's VPC Packet Mirroring provides continuous mirroring of virtual machine network traffic to a packet collector without using agents.



This guide follows a simple deployment scenario in which a single Flowmon Collector resides within the same VPC as mirrored instances. For advanced deployment scenarios, please refer to the official VPC Packet Mirroring documentation.

Prerequisites

Before your start enabling VPC Packet Mirroring in your infrastructure, please make sure you

- · have considered budgetary implications of running packet mirroring,
- have a Flowmon Collector instance running with two or more network interfaces and an appropriate license (with at least one monitoring port),
- have instances you wish to monitor in the same VPC as one of the monitoring interfaces of your Flowmon instance.

Deployment

• Log in to the Google Cloud Console. In all following steps, always select the **Region** and/or **Zone** that hosts your instances.

- Overview
- Prerequisites
- Deployment
- Flowmon Configuration



• Create an unmanaged instance group for your Flowmon instance(s). Select the Network that contains the primary interface of your instances.

Create an instance group

To create an instance group, select one of the options:		Organize VM instances in a group to manage them together. Instance groups $\ensuremath{\mathbb{L}}^{\!\!\!2}$
		Name 💿 Name is permanent
New managed instance group A group of VMs created from a template. Supports autohealing, autoscaling, auto updating, regional deployments, and load balancing.		Instance-group-1 Description (Optional)
Rew unmanaged instance group A group of existing VMs that you manage. Supports load balancing.	>	Region @ Zone @ Region is permanent Zone is permanent europe-west3 (Frankfurt) europe-west3-c Specify port name mapping (Optional) Network @ default Subnetwork @ default (10.156.0.0/20) VM instances No available instances You will be billed for VM instances in this group. Compute Engine pricing L ²
		Equivalent REST or command line



• Create a regional health check rule. You should select the TCP protocol and port 22.

۲	Compute Engine	← Create a health check	
e A	VM instances Instance groups	Health checking mechanisms determine whether VM instances respond properly to traffic. You cannot create a legacy health check using this page. For more information, refer to the <u>Health Checks Concepts</u> documentation.	
	Instance templates Sole-tenant nodes	Name 🕐	
ŧ	Machine images	Description	
Create	Disks Snapshots Images TPUs Migrate for Compute Engi Committed use discounts Metadata Health checks Zones an internal TCP network	Scope Global Regional Region europe-west3 (Frankfurt) Protocol TCP Protocol Proxy protocol NONE Request Request Response Constance group.	
Æ	Network services	Create a load balancer	
A	Load balancing	LITTD(C) Load Palanaing	
÷	Cloud DNS Cloud CDN	HITP(S) Load Balancing ICP Load Balancing Layer 7 load balancing for HTTP and HTTPS Layer 4 load balancing or proxy for applications that rely on TCP/SSL protocol Learn more	3
4)+ ≁	Cloud NAT Traffic Director Service Directory	Configure Configure HTTP LB TCP LB HTTPS LB (includes HTTP/2 LB) SSL Proxy Options Options Internet-facing or internal Internet-facing or internal Single or multi-region Single or multi-region Start configuration Start configuration	

•





In the backend configuration, select the **Network** that contains the **monitoring interface** of your Flowmon instance. Select **Instance group** and **Health check** created in previous steps.

聶	Network services	 New Internal load balancer Backend configuration 	
А	Load balancing	Name @ Backend service	
	Cloud DNS	lowercase, no spaces	
<	Cloud CDN	Region @	
<u>*</u>)+	Cloud NAT	Backend configuration You have not configured your backend yet	•
ł	Traffic Director	Frontend configuration	•
Ŵ	Service Directory	You have not configured your frontend yet Protocol: TCP	
		O Review and finalize Backends	
		Optional New item	^
		Create Cancel	
		No instance groups in this region	*
		Open Concel	
		Concer Cancer	
		+ Add backend	
		7 Health check @	•
		Session affinity 📀	
		None	•

In the frontend configuration, select the **Subnetwork** that contains the **monitoring interface** of your Flowmon instance. **Enable the load balancer for packet mirroring.**



聶	Network services	← New	v Internal load balancer		Frontend configuration
A	Load balancing	Name 🔞 Name is permai	anent		
里	Cloud DNS	lowercase, n	io spaces		New Frontend IP and port
<ê>	Cloud CDN				Name (Optional) 🔞 Name is permanent
$\left(\frac{\partial}{\partial y}\right) +$	Cloud NAT	Backer You hav	nd configuration we not configured your backend yet	1	lowercase, no spaces
1ŀ	Traffic Director	Cronto	and configuration		Add a description Protocol
Ð	Service Directory	Your fro	ontend is configured	÷	TCP Subnetwork
		(i) Review	w and finalize	2	
		Optiona	al		Internal IP
		Questa Qu			Non-shared Shared
		Create	ancei		IP address
					Ephemeral (Automatic) -
					Ports 🕖
				3	Multiple All
					Global access 🔞
					Disable Enable
					Service label @ (Optional)
					Packet Mirroring @ (Ontional)
				4	Enable this load balancer for Packet Mirroring Hide advanced configurations
					Done Cancel
					+ Add frontend IP and port

• **Create a packet mirroring policy**. Select the **Network** containing your Flowmon and mirrored instances, provide a **Tag** marking the virtual machine instances you wish to mirror. **Collector destination** is the load balancer (its frontend) you created in the previous step.

H	VPC network	Create policy
8	VPC networks	
C ²	External IP addresses	Define policy overview — 2 Select VPC network — 3 Select mirrored source — 4 Select collector destination —
35	Firewall	5 Select mirrored traffic
×	Routes	Policy name 2
÷	VPC network peering	Region *
\bowtie	Shared VPC	·
\Leftrightarrow	Serverless VPC access	Policy priority 1000
ılııı	Packet mirroring	
		Enabled Disabled CONTINUE CANCEL



Н	VPC network	← Create policy
2	VPC networks	
c	External IP addresses	🤣 Define policy overview — 🥝 Select VPC network — 🚳 Select mirrored source — 🕘 Select collector destination —
	Firewall	5 Select mirrored traffic
×	Routes	Select the VPC network or networks where your mirrored and collector instances are
÷	VPC network peering	If the mirrored and collector instances are in the same network select Mirrored source
×	Shared VPC	and collector destination are in the same VPC network. If they are in different networks
\$	Serverless VPC access	VPC networks. Learn more
- Iĝi	Packet mirroring	Mirrored source and collector destination are in the same VPC network
.0.	ř	Network*
		O minored source and conector destination are in separate, peered ve c networks
		CONTINUE CANCEL
11	VPC network	← Create policy
	VPC networks	
- B	External IP addresses	🤣 Define policy overview — 🥑 Select VPC network — 🔞 Select mirrored source — 🕘 Select collector destination —
	Firewall	5 Select mirrored traffic
~	Pourtee	Specify the source that will be mirrored. Packet mirroring captures all the ingress and
~~ ~	VBC petwork peering	egress traffic of mirrored instances.
ф М	Cherred VRC	Mirrored source
		Instances in these subnetworks are mirrored
< 191	Barket minoring	Select with network tag Instances with matching tags are mirrored
ılili	Packet mirroring	
		Select individual instances Selected instances are mirrored
		CONTINUE CANCEL
11	VPC network	← Create policy
8	VPC networks	🖉 Define policy overview — 🤗 Select VPC network — 🤗 Select mirrored source — 🗿 Select collector destination —
Ľ	External IP addresses	Select mirrored traffic
55	Firewall	Select an L4 internal load balancer that balances traffic across your collector instances
N¢	Routes	(the backend instances), which delect all the mirrored traffic. The load balancer must
÷	VPC network peering	Collector destination *
×	Shared VPC	· · · ·
\otimes	Serverless VPC access	You can also create new L4 internal load balancer
light	Packet mirroring	CONTINUE CANCEL

For Google Cloud Console or API guides, please refer to the official VPC Packet Mirroring documentation.



Flowmon Configuration

A In order to accept and correctly respond to TCP health-checks, you must enable and configure an IP address on Flowmon's monitoring port. This also includes adjustments in local routing for the monitoring port in question, please refer to the official documentation for details.

No other configuration specific for VPC Packet Mirroring is necessary. See instructions on how to enable a monitoring port in the Flowmon User Guide.



Google Cloud VPC Flow Logs

• Google Cloud VPC Flow Logs are currently not supported by Flowmon Collector.



Post-installation Steps

Follows a basic set of important configuration steps that should be performed on each Flowmon instance after its deployment has been completed. It is by no means an exhaustive list, it is meant to serve as a jumping-off point for new users. Please refer to the Flowmon User Guide for detailed instructions and documentation of all available configuration options.

A full copy of the Flowmon User Guide is distributed with every Flowmon appliance and is accessible via the question mark (?) icon in the upper right corner of the web interface.

- Management Interface
- Web Interface
- DNS Servers
- Time and Date
- Upload License
- Data Storage
- Collector Listening Ports
- Collector Initialization
- Quotas
- Monitoring Traffic
- Collecting Data

Management Interface

(i) Note

This section applies only to Flowmon instances in virtualization platforms that require manual IP configuration of virtual network interfaces. Disregard this section if the platform of your choice:

- supports DHCP and you connected Flowmon's management interface to a network where DHCP is enabled,
- is a cloud platform, such as AWS EC2, Azure or Google Cloud.

To start using your Flowmon instance, it has to be accessible over the network. In order to do that, you have to configure an IP address on its first management interface.

- Access the (Virtual) Console of the running instance and click on the black area shown on the screen. You
 will be asked to log in. Type flowmon as login and inv3a-t3ch as password. After that, type sysconfig and
 press Enter.
- Select Management port 1 in the menu using the up/down arrow keys and press Enter. On the next screen, you can set a new IP address, Netmask and Gateway for the web interface. Use the TAB key to move to the Save button and press Enter.



Set the IP address,	mask and gateway for administration interface
IP address:	192.168.50.84
Netmask:	255.255.254.0
Gateway:	192.168.51.254
* Obtained from D	ICP, will be generated automaticaly every reboot.
L	
K Save	> <use &="" dhcp="" save=""> < Back ></use>

- 3. Log out and close the (Virtual) Console.
- Later on, this configuration is available in the web interface. Enter Configuration Center and navigate to the System tab and open Management Interface 1 settings to configure the IP address. Do not forget to Save the changes.

- 2	Flowmon > Cont	figuratio	on Center 👻							en 👻	0	0 a
0	≡	24	User Settings	Manager	nent Interface 1							
) Overview	0	GPG Settings	IPv4 config	ration	Ctatia B DUCD						
-	System	2	Maintenance	ir v4 comig		Static S DHCP						
C	Quotas Manager			IPv4 address		192.168.50.84						
6	Remote Access	INT	ERFACE SETTINGS	Notmack		255 255 254 0						
Ê	Logs	<>	Management Interface 1	Neullask		233.233.234.0						
Ľ	Versions	<>	Management Interface 2	Gateway		192.168.51.254						
٩	License	=	DNS Servers	IPv6 config	uration							
			Hostname	Change inte	rface settings							
		SYS	STEM SETTINGS									
		0	Time zone	Static routes								
		0	Data Storage		DESTINATION		NETMASK	GATEWAY		ACTION		
		0	External Data Storage	🚺 No d	ata							
			Email									
		•	Proxy						Available actions:	+ NEW S	TATIC RO	ле
			SNMP									
		B	SNMP Event Logging	B SAVE	\times clear dns cache							

Web Interface

Access to the web interface is secured with a password-based authentication. In order to configure the **GUI password**, access the newly created instance via SSH.



(i) Note

In the cloud, access to SSH is secured by a key pair and there is no default password. Please refer to the platform-specific official documentation for ways to provide SSH public keys to instances on boot.

In on-premise virtualization, access to SSH is secured by a default password **inv3a-t3ch**. This password should be changed immediately after the first successful SSH login, for security reasons.

- 1. Access the Flowmon instance via SSH. Using the user name **flowmon** and the IP address of its first management interface.
- 2. Enter the sysconfig command and set the GUI password.



- 3. Once the password is configured, access the Flowmon instance in the browser via HTTPS and proceed with Flowmon configuration as described below or in the official Flowmon User Guide.
- 4. Later on, this functionality is available in the web interface. Enter Configuration Center, the System tab, User Settings. To change the admin password, click on the Edit button (pencil icon) when logged in as admin, check the Change password checkbox and then type in and confirm the new password.

Flown Driving Network	Visibility					Flowmon Virtual Rev. 41,	Applia 30/07	ances /2021
Flowmon > 0	Configuration Center 👻						🔔 en 👻	00
Overview System Overview	User Settings GPG Settings Maintenance	User Se	ttings		×		ROLES	ACTION
 Remote Access Logs Versions License 	INTERFACE SETTINGS ↔ Management Interface 1 ↔ Management Interface 2 I DNS Servers III Hostname	admin	Login admin Name John Ø Change password New password	Email admin@company.com Surname Smith Confirm password		admin Available actions: + NEW USER	E LOGOUT	T ALL USERS
	SYSTEM SETTINGS C Time zone Data Storage	admin	Roles (1)		-	MODULES	actions:	
	 External Data Storage Email Proxy SNMP 		 Disabled Unable to change password User interface settings Default sort of flows by start Get default language from th 	t time he web browser	-1	Avandure	actions.	' NEW ROLE
	 SNMP Event Logging Syslog Server Syslog Event Logging 		Resolving Autonomous system resolv Domain name resolving IP geolocation	ing Port name resolving Router resolving Type of service (ToS) resolving				
	LDAP TACACS+			SAVE	CLOSE			

DNS Servers

In the web interface, enter Configuration Center, System tab and open DNS Servers settings. Configure IP addresses of the **Primary** and **Secondary DNS** servers.

	Flowmon > Configu	uration Center 👻		
Ø	≡ Overview	USER SETTINGS SYSTEM SETTING	IGS	
\rightarrow	Monitoring Ports	🔧 Maintenance	DNS Servers	
Ţ	System		Primary DNS	192.168.4.253
•	Distributed Architecture			
\$	FMC Configuration	Management Interrace 1	Secondary DNS	
	Configuration Templates	↔ Management Interface 2		
0	Resource Manager	DNS Servers	SAVE	
ᢒ	Remote Access	Hostname Hostname		
Ê	Logs	SYSTEM SETTINGS		
(L)	Versions	S Time zone		
٩	License	O Data Storage		

Time and Date

In the web interface, enter Configuration Center, System tab and open Time zone settings to set the current time and time zone. Precise time configuration is crucial for a correct flow data analysis. Do not forget to Save the changes.

Flowmon Virtual Appliances



~ ~

.. .

Elowmon

	Driving Network Visibility	uration Center +		
Ø	Overview	2 User Settings	Time zone	
		GPG Settings	Current time	2019-09-04 13:31
L.	System	A Maintenance		
0	Quotas Manager		Time zone (closest city)	Prague •
ᢒ	Remote Access	INTERFACE SETTINGS	Set time automatically	
Ê	Logs	 ↔ Management Interface 1 		_
(Ŧ)	Versions	↔ Management Interface 2	Use NTP servers supplied by DHCP	
٩	License	DNS Servers	Primary NTP server	pool.ntp.org
		Hostname	Secondary NTP server	
		SYSTEM SETTINGS	Allow inbound NTP connections	
		() Time zone		
		O Data Storage	SAVE	

Upload License

For a properly functioning appliance, it is necessary to apply a valid license. Enter **Configuration Center**, **License** tab, choose the license file and **Upload** it to your appliance.



Data Storage

It is recommended to use a separate disk for storing Flowmon's data. In the web interface, enter **Configuration Center**, **System** tab and open **Data Storage**.

Select the desired disk from the drop down menu (list of available disks can be updated by clicking the **Rescan** button). Confirm the selection by pressing the **Save** button. System will check the selected disk and verify the partition table and filesystem (only EXT3, EXT4 and XFS filesystems are supported). If there are any files or



directories present on the new disk, the system compares their names to those present on the old disk. The files and directories with same colliding names will be replaced! The migration operation is finished by rebooting the device. Thus the reboot can take (much) more time than usually, because all the data are being copied and checked.



If the new disk has no partition table (for example new data storage created in virtual environment), the system will alert this and ask the user to create new partition table by clicking on the button **Create partition**. This will destroy all data on this disk!



During the disk check, the following scenarios may occur:

- New disk has no partition table (described above) user will be asked whether to create a new partition table. If so, the system will be configured to perform new disk formatting to EXT3/4 or XFS and data migration.
- New disk has a valid partition table and is not formatted during the device reboot the disk is formatted to the EXT3/4 or XFS filesystem and data are copied.



- New disk is formatted to a filesystem different from EXT3/4 or XFS migration will not be performed and an error will be alerted.
- New disk is formatted to the EXT3/4 filesystem and is smaller than 16 TB and contains files or directories with the same names as on the old disk (i.e. their names collide) the user is warned that some files or directories on the new disk will be overwritten.
- New disk is formatted to the XFS filesystem and is bigger than 16 TB and contains files or directories with the same names as on the old disk (i.e. their names collide) the user is warned that some files or directories on the new disk will be overwritten.
- New disk is formatted to the XFS filesystem and is smaller than 16 TB during the device reboot the disk is formatted to the EXT3/4 filesystem and data are copied.
- New disk is formatted to the EXT3/4 or XFS filesystem and do not contain any files or directories with colliding names during the device reboot the data will be copied from original disk to the new one.

Collector Listening Ports

Enter **Configuration Center** and navigate to the **FMC Configuration** tab and open **Listening Ports** settings. Here you can add new sources or configure existing NetFlows/sFlow source parameters, like the source name, receiving port, protocol type and forwarding.

Ē	Flowmon > Configuration Center -									en 👻 🌘	3	9 adm
Ø	≡ Overview	BUILT-IN COLLECTOR		Listening Ports								
→	Monitoring Ports		Basic Settings		NAME	PORT	PROTOCOL	FORWARDING	SAMPLING RATE		A	CTION
	System		Autonomous systems	A	NetFlow-port2055	2055	NetFlow/IPFIX (udp)	No	Controlled by a flow source			r 🗉
	Distributed Architecture		S Flow Database Fields	0	NetFlow-port3000	3000	NetFlow/IPFIX (udp)	No	Controlled by a flow source			/ II
	Distributed Architecture		• •	A	NetFlow-port9996	9996	NetFlow/IPFIX (udp)	No	Controlled by a flow source			/ 1
•	FMC Configuration	Sources	•	sElow-port6343	6343	sFlow (udp)	No	Controlled by a flow source			/ =	
\$	Configuration Templates		Listening Ports									
•••	FTR settings		➡ Forwarding Targets							NEW LIS	ENING	PORT

Collector Initialization

Initialize the built-in collector database in **Configuration Center**, the **FMC Configuration** tab, **Basic Settings** by clicking on the **Clear Data Storage** button. This step will clear the database! All collected NetFlow data will be lost!





Quotas

To check the space allocated to the live profile and other plugins, open **Configuration Center** and the **Quotas Manager** tab. It is recommended that at least 10GB is allocated for the live profile and 2GB for each additional module. Do not forget to **Save** the changes.

- #	Flowmon > Co	onfiguration Cen	ter 👻				🔔 en 👻 🕜	😝 admin 👻
	≡	O Quotas	Manager					
Ø	Overview							
Ţ	System	=	Disk usage					
0			Total: 37.25 GiB	Monitoring Center (2.57 Gil	B) • FMC profiles chart data (1.15 G	SiB) • Modules (0) • Others (3.4	15 GiB) Free (30.08 GiB)	19%
0	Remote Access							
Ê	Logs	Flowmon M	onitoring Center					
[ł]	Versions		NAME		QUOTA		CURRENT SIZE	
٩		All Sources			• • • • • • • • • • • • • • • • • • •	10 GiB		88 KiB
		QoS_ToS			-•	1 GiB		560.0 MiB
		Total traffic				1 GiB		124.4 MiB
		icmp			•	1 GIB		311.1 MiB
		mail			•	1 GIB		373.3 MiB
		routers			-•	1 GiB		373.3 MiB
		service				1 GiB		435.6 MiB
		user				1 GiB		248.9 MiB
		Flowmon M	onitoring Center backend					
			NAME		QUOTA		CURRENT SIZE	
		Active devic	es			2 GIB		186.5 MiB
		Reports			-	2 GIB		17.9 MiB
		B SAVE						

Monitoring Traffic

The monitoring port is a process running over each monitoring interface. It analyzes every single received packet and computes flow statistics. The statistics are exported to a collector (e.g. external Flowmon Collector or the local collector). The administrator can check the status of monitoring ports, start/stop monitoring ports or set new configuration. Each monitoring port is configured by dedicated management panel or it can be switched to the global mode in which some tabs will be configured according to the Global settings.

Go to Monitoring Ports.


	Flowmon > Co	onfiguration Center 👻		🗾 en	• ?	e admin (Base tenant)
	≡	→ Monitoring Ports				
(Ø)	Overview	Number of licensed monitoring interfaces:	4 (eth2 eth3 eth4 eth5) Number of connected monitoring interfaces:	2 (eth2 eth3	0	
→	Monitoring Ports		- (curz, curo, curo, curo). Number of connected monitoring interfaces.	2 (0112, 0110	<i>.</i>	
Ţ	System	Global settings				
€	Distributed Architecture					
\$	FMC Configuration	TARGETS	ADVANCED SETTINGS			
	Configuration Templates	Active timeout	300			
0	Resources Manager	Inactive timeout	30			
\odot	Remote Access	mactive timeout				
Ê	Logs	Output Interface Index	Manual 0			
(L)	Versions		Same as input			
٩	License	B SAVE				

Active timeout ensures that the very long flows will be exported in specified time. Timeout is checked for each incoming packet. If corresponding flow is lasting longer than specified time interval, it is deleted from the flow cache and exported to collector.

Inactive timeout avoids keeping old, inactive flow records in the flow cache forever. When no packets belonging to the flow are observed for the specified time interval, flow record is exported to collector.

🕑 Monite	oring port 1 on eth2	is running		c	RESTART STOP
🛋 TARC	GETS ADVANC	ED SETTINGS 🛛 🔅 IN	TERFACE SETTINGS		
Used Inac Link Pack	d active timeout: ctive timeout: c: ket sampling:	300s 30s no link no packet sampling			
Use custor	m settings				
Enable flov	w export				
	TARGET		COLLECTOR PORT	PROTOCOL	ACTION
localhost		3000 (udp)		IPFIX	/ 1
FI SAVE	3			Available ac	tions: + NEW TARGET

To start the flow monitoring port press the **Start** button. If the monitoring port starts correctly, button **Start** will change to **Stop** and button **Set Defaults** will change to **Restart**. To use default monitoring port configuration, stop it and then press Set Defaults button.

In the **Targets** tab you can configure various number of targets (i.e. collectors) where the flow exports are to be exported. The targets can be added or removed by pressing the New target or Delete button. Every target is specified by items **Target address** and **Collector port**. The address item is an address to a collector. If the probe built-in collector is to be used, use the address localhost. The port item specifies the listener port of the collector. For the built-in collector use the port 3000. The **Flow sampling rate** value defines a deterministic sampling (e.g. sampling interval 1 in 3 flows) for monitoring port flows. If you enter a N value, every Nth flow will be exported. This is useful in situation when the collector is overloaded by incoming flows. The zero value disables this feature. The Network protocol option can be selected in corresponding drop-down menu. UDP (default) or TCP protocol can be selected. TCP protocol is supported for IPFIX export protocol only. If TCP is selected as network protocol, the



encryption TCP/TLS can be enabled. For TCP/TLS, the set of keys and certificates have to be generated for flow exporting device (monitoring port) and for collector. All certificates must be signed by the same certification authority (CA). Its certificate (CA certificate) must be provided together with the monitoring port key and certificate to each monitoring port target using TCP/TLS protocol. The provided key(s) must <u>not</u> be encrypted.

In the **Export protocol** tab you can select the Export protocol NetFlow v5, NetFlow v9 and IPFIX. By unchecking the **Use custom settings** toggle switch and clicking on button **OK** will be this tab configured according to the global configuration. Additionally, the frequency of sending the template can be configured.

Edit target	×
TARGETS + EXPORT PROTOCOL	
 This mode allows forwarding of flows via a UDP protocol using a spoofed IP address of the flow source. This mode is compatible with all Flowmon collectors and third-party collectors. Use custom settings Protocol NetFlow v5 NetFlow v9 IPFIX 	
Template's resending interval every 4096 packets or every 600 seconds.	
ок	CLOSE

Collecting Data

Send NetFlow v5, NetFlow v9 or IPFIX flow data to **Management Interface 1** of your Flowmon Collector. For available listening ports, corresponding supported flow data formats, and flow collection status, refer to **FMC Configuration / Listening Ports**.

To start analyzing your data, go to Monitoring Center.



3rd-party Packet Brokers

The following 3rd-party packet brokers are currently supported:

- Garland Prisms
- Ixia CloudLens
- Gigamon



Garland Prisms

Overview

This solution is leveraging Garland Prisms - to provide network traffic - and Flowmon with extension modules for NPMD, network behavior analysis, performance monitoring, DDoS detection and on-demand packet capture - to provide insight into network traffic. With Garland Prisms agents installed on all monitored virtual instances, a copy of the network traffic is routed to monitoring interfaces of a Flowmon instance for processing and analysis.

This document outlines steps necessary to start analyzing network traffic in your cloud deployment with Garland Prisms and Flowmon.

Prerequisites

- 1. A running instance of Flowmon (AWS, Azure or Google Cloud).
- 2. A number of running client instances where Garland Prisms agents can be installed.

Deployment

For an up-to-date deployment guide, please refer to the official documentation for Garland Prisms.

- Overview
- Prerequisites
- Deployment
- Flowmon Configuration



Flowmon Configuration

- 1. Go to Flowmon Configuration Center of your Flowmon instance.
- 2. Choose the **Monitoring Ports** panel.
- 3. Under Global settings -> Advanced settings enable VxLAN decapsulation on port 4789.
- 4. Click on the **Save** button.

Global settings	
ADVANCED SETTINGS ADVANCED SETTINGS	
Packet sampling rate 0	
Light mode	
OPTIONAL L2 VALUES FOR NETFLOW RECORD OPTIONAL L3/L4 VALUES FOR IPFIX RECORD	OPTIONAL L7 VALUES FOR IPFIX RECORD
MAC IJ/L4 extended	DHCP MSSQL IEC 104
MPLS NPM	DNS PostgreSQL COAP
Auto	MySQL
	🗆 Email 🖉 TLS main
✓ VLAN	✓ NBAR2 ✓ TLS client
	 Samba TLS certificate
	✓ VoIP ✓ TLS JA3
	5060 Select VoIP SIP ports
DECAPSULATE TUNNEL PROTOCOLS	
GRE	
ESP	
✓ VxLAN	
4789 Select VxLAN port	
ERSPAN	
U PPPOE	
Add L2 values enabled for NetFlow record to the key fields	
Use autonomous system list	
—	
Default AS list Custom AS list	
B SAVE	



Ixia CloudLens

Overview

Flowmon and Ixia have joined to provide true cloud visibility. The solution is leveraging Ixia CloudLens Agents - to provide network traffic - and Flowmon with extension modules for NPMD, network behavior analysis, performance monitoring, DDoS detection and on-demand packet capture - to provide insight into network traffic. With Ixia CloudLens Agents installed on all monitored virtual instances, a copy of the network traffic is routed to their counterpart running on the Flowmon Collector VA instance for processing and analysis.



This document outlines steps necessary to start analyzing network traffic in your cloud deployment with Ixia CloudLens and Flowmon.

Prequisites

- 1. A running instance of Flowmon (AWS, Azure or Google Cloud).
- 2. A number of running client instances where Ixia CloudLens Agents can be installed.

Deployment

For an up-to-date deployment guide, please refer to the official Ixia CloudLens documentation.

Flowmon Configuration

To install an Ixia CloudLens Agent on Flowmon, open an SSH connection to the Flowmon instance via its management IP address and run the following commands. Replace **PROJECT_KEY** with the value retrieved from the Ixia Portal during project creation.

1. Start **docker** and enable it as a service.

1 sudo systemctl start docker 2 sudo systemctl enable docker

2. Run container with Ixia CloudLens Agent.

- Overview
- Prequisites
- Deployment
- Flowmon Configuration



1	<pre>sudo docker runname ixia-cloudlens-agent-fmc \</pre>
2	-v /:/host \
3	<pre>-v /var/run/docker.sock:/var/run/docker.sock \</pre>
4	-drestart=alwaysnet=host \
5	privilegedrestart=on-failure \
6	ixiacom/cloudlens-agent \
7	server agent.ixia.cloud \
8	accept_eula yes \
9	apikey \$PROJECT_KEY

3. Verify that the container is running.

1 sudo docker ps | grep ixia-cloudlens-agent-fmc

See Post-installation Steps or follow instructions on how to enable a monitoring port in the Flowmon User Guide.



Gigamon

Overview

This solution is leveraging Gigamon Visibility Platform - to provide network traffic - and Flowmon with extension modules for NPMD, network behavior analysis, performance monitoring, DDoS detection and on-demand packet capture - to provide insight into network traffic. With Gigamon VTap agents installed on all monitored virtual instances, a copy of the network traffic is routed to monitoring interfaces of a Flowmon instance for processing and analysis.

This document outlines steps necessary to start analyzing network traffic in your cloud deployment with Gigamon and Flowmon.

Prerequisites

- 1. A running instance of Flowmon (AWS, Azure or Google Cloud).
- 2. A number of running client instances where Gigamon vTAP agents can be installed.

Deployment

In order to be able to use Gigamon, several components are needed. They can be either virtual or physical appliances. For a fully virtualized installation, you need to have instances of

- Gigamon Fabric Manager,
- VSeries Node,
- VSeries Controller,
- VTap Controller.

In order to send packets to Gigamon Visibility Fabric, you need to install Gigamon vTAP on every host you want to monitor.

For more information about the Gigamon Solution and up-to-date installation guides, see

- Gigamon Visibility Platform for AWS Configuration Guide
- GigaSECURE[®] Cloud for Azure Getting Started Guide

There is no need to install anything on your Flowmon.

Flowmon Configuration

- 1. Go to Flowmon Configuration Center of your Flowmon instance.
- 2. Choose the Monitoring Ports panel.
- 3. Under Global settings -> Advanced settings enable VxLAN decapsulation on port 4789.

- Overview
- Prerequisites
- Deployment
- Flowmon Configuration



4. Click on the **Save** button.

• Clobal settings • TARGETS • EXPORT PROTOCOL • ADVANCED SETTINGS Packet sampling rate 0 0 0
ARGETS ★ EXPORT PROTOCOL ADVANCED SETTINGS Packet sampling rate U Light mode Ught mode OPTIONAL L2 VALUES FOR NETFLOW RECORD OPTIONAL L3/L4 VALUES FOR IPFLX RECORD OPTIONAL L2 VALUES FOR IPFLX RECORD OPTIONAL Z2 V TLS client Samba TLS certificate
Packet sampling rate 0 Light mode OPTIONAL L2 VALUES FOR NETFLOW RECORD OPTIONAL L3/L4 VALUES FOR IPFLX RECORD MAC © L3/L4 extended © DHCP MSSQL IEC 104 MPLS NPM © DNS PostgreSQL COAP Auto Select decapsulation mode of MPLS packets © Extended NPM W HTTP MySQL VLAN VLAN © NBAR2 © TLS cellent
Packet sampling rate 0 Light mode OPTIONAL L2 VALUES FOR NETFLOW RECORD OPTIONAL L3/L4 VALUES FOR IPFLX RECORD MAC Ø L3/L4 extended Ø DHCP MSSQL I EC 104 MPLS NPM Ø DNS PostgreSQL COAP Auto Select decapsulation mode of MPLS packets Extended NPM HTTP MySQL VLAN VLAN NBAR2 TLS cellent
Light mode OPTIONAL L2 VALUES FOR NETFLOW RECORD OPTIONAL L3/L4 VALUES FOR IPFIX RECORD MAC L3/L4 extended L3/L4 extended DHCP DNS DHCP L3/L4 extended DHCP DNS PostgreSQL C0AP LC0AP L3/L4 L20A L3/L4 L3/
OPTIONAL L2 VALUES FOR NEFFLOW RECORD OPTIONAL L3/L4 VALUES FOR IPFIX RECORD OPTIONAL L7 VALUES FOR IPFIX RECORD MAC
✓ MAC ✓ L3/L extended ✓ DHCP MSOL EC104 ✓ MPLS ✓ NPM ✓ DNS PostgreSQL COAP Auto ✓ Select decapsulation mode of MPLS packets ✓ HTTP MySOL Email ✓ VLAN ✓ NBAR2 ✓ TLS cellent
MPLS NPM DNS PostgreSQL COAP Auto Select decapsulation mode of MPLS packets Extended NPM HTTP MySQL VLAN Extended NPM MS TS client Subscription Samba TLS certificate
Auto • Select decapsulation mode of MPLS packets © Extended NPM © HTTP MySQL © VLAN Email © TLS main © VLAN © Samba © TLS certificate
 ☑ VLAN ☑ VLAN ☑ NBAR2 ☑ TLS client ☑ Samba ☑ TLS criticate
 ✓ VLAN ✓ NBAR2 ✓ TLS client ✓ Samba ✓ TLS critificate
Samba 🗹 TLS certificate
5060 Select VolP SIP ports
DECAPSULATE TUNNEL PROTOCOLS
GRE
ESP
V VXLAN
4789 Select VxLAN port
ERSPAN
PPPoE
Add L2 values enabled for NetFlow record
to the key fields
Use autonomous system list
Default AS list Outrom AS list
B SAVE