# ARISTA

# **Deployment Guide**

# Onboarding and Deploying CloudVision Sensor

### Version 1.1



Arista.com

Arista Networks

DOC-07825-01

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA		
+1-408-547-5500	+1-408-547-5502 +1-866-476-0000	+1-408-547-5501 +1-866-497-0000
www.arista.com/en/	support@arista.com	sales@arista.com

© Copyright 2025 Arista Networks, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos, and service marks ("Marks") displayed in this documentation are the property of Arista Networks in the United States and other countries. Use of the Marks is subject to the Arista Networks Terms of Use Policy, available at www.arista.com/en/terms-of-use. Use of marks belonging to other parties is for informational purposes only.

#### Contents

Chapter 1: Overview	1
Chanter 2: Deploying the CV Sensor	3
21 Concreting a Service Account Taken	······ <b>·······························</b>
2.2 Adding the Sensor to the III	
2.3 Getting the Latest Sensor OVA	
2.4 Deploving the Sensor OVA.	6
2.5 Booting up the Sensor	
2.6 Adding the Data Sources	11
2.6.1 Adding VMware vCenter as a Data Source	13
2.6.2 Adding SNMP Data Source	22
Chapter 3: Upgrading the Sensor	25
Chapter 4: Troubleshooting [New Installation]	
4.1 How to restart the sensor component?	
4.2 How to Monitor Sensor Resource Utilization?	
4.3 Where to check for logs?	
4.4 How to charge the access token is expired or not?	ວ∠ ເດ
4.6 How to change the log level and verbosity of the sensor on a VM?	
4.7 Are all components on the server running fine?	
Chapter 5: Troubleshooting Ungrade Issues	36
E 1 Where to shock upgrade logo?	
5.1 Where to check upgrade logs?	
Chapter 6: General Troubleshooting Issues	
6.1 Active sensor and data sources with no updates for applications in CVaaS	
6.2 How to check the sensor version on the sensor VM?	38
6.3 What does Error- dial TCP i/o timeout mean?	
6.4 How to collect debug logs?	
6.5 How to change the cluster name(CV_ADDR)?	40
6.6 What action to take when the Flow data source becomes inactive?	
6.7 The Cvpl status all command do not show component status	
o.o ralieu to verify certificate for a voenter data source	

#### **Overview**

CloudVision® Universal Network Observability<sup>TM</sup> (CV UNO) is a multi-domain network observability platform that integrates application visibility with CloudVision's network telemetry. This integration helps provide insights into the applications and workload performance across data centers, campuses, and wide area networks.

CV UNO is available along with the CloudVision-as-a-Service (CVaaS) platform. It offers cloudbased onboarding and feature delivery, using secure state-streaming to an Arista-managed cloudnative architecture.

The CV sensor is an integral component of CV UNO. The sensor is a VM deployed on-premises and facilitates viewing application data in CloudVision. The sensor collects, normalizes, and curates flow and SNMP data from various data sources. It also polls data from vCenter and subscribes to vCenter events, allowing you to view them in CloudVision. This data gets forwarded to the EOS Network Data Lake (NetDL), where the network data lake combines diverse datasets and performs a machine-learning-based analysis. With the help of this data, CV UNO quickly determines the source of an anomaly, whether a network or application-based anomaly. If it is a network anomaly, CV UNO determines where the issue occurs and why.

The following image provides a high-level overview of the functionality of the CV Sensor:



#### Figure 1-1: CV Sensor Architecture

Familiarize with the following terminology in this document:

- CV Sensor refers to the collector that streams the data from one or more data sources. The Sensor is responsible for starting different data sources, collecting third-party device data, and streaming it to CVP.
- Data Source refers to the target device in the onboarding work flow. For example: vCenter, Flow, DMF, SNMP (Cisco router/switch).
  - vCenter Data source includes:

- · State Provider Virtual Machines (VMs), Hosts, Distributed Virtual Switches (DVS), etc
- · Counters Provider system counters, network counters, etc
- Tags Provider vCenter tags
- Events Provider vCenter events
- DMF Data source includes: DMF Provider
- · SNMP Data sources include:
  - SNMP Provider: SNMP Walk for Fetching System, LLDP, and Interfaces Information.
- Flow Data source includes:
  - IPFIX Provider
  - NetFlow Provider
  - sFlow Provider
- Provider A worker or go-routine responsible for pulling or receiving a single type of data, and sending it to CVP. For example: State Provider, IPFIX Provider, DMF Provider, etc.

#### **Deploying the CV Sensor**

To view data from external data sources in CloudVision, you must deploy the CV Sensor and on board it as a data source so that it can listen to external data sources. The CV Sensor is deployed as an OVA appliance and is intended to run on top of an ESXi server.

When you deploy the sensor using the sensor OVA, it generates a VM with the following specifications:

- Number of CPU cores: 12
- Memory: 16 Gibibytes (GiB)
- Disk Space: 124 Gibibytes (GiB)

**Note**: Ensure that your system/host has sufficient resources available to accommodate the sensor OVA deployment.

**Note**: You must also on board any external *data sources* to CloudVision so that the sensor can stream or poll them for their data.

To deploy the CV Sensor, follow the steps described here:

- 1. Generate a Service Account Token
- 2. Add the Sensor in the UI
- 3. Get the latest Sensor OVA
- 4. Deploy Sensor OVA
- 5. Boot up the Sensor
- 6. Add Data Source

#### 2.1 Generating a Service Account Token

To generate a service account token:

- 1. Login to CVaaS cluster using the URL www.arista.io
- 2. Navigate to Settings -> Access Control -> Service Accounts -> New Service Account.
- 3. Create a new service account for UNO Sensor (see image):
  - a. Service Account Name (example, UNO-service-account )
  - b. Description
  - c. Status: Enabled
  - d. Roles: Select the pre-defined role sensor-enrollment.

4. Click the **Create** button. The newly added account (UNO-service-account) appears in the list of Service Accounts.

Figure 2-1: New Service Account

New Service Account		
* Service Account Name UNO-service-account		
* Description Service Account for UNO		
* Status		* Roles
Епаріео	~	Cancel Create

- 5. Click on the newly created Service Account (UNO-service-account).
- 6. To generate the Service Account Token:
  - a. Enter a Description and select a Valid Until field.
  - **b.** Select an **expiry date** that is at least after a year from the current date.
  - c. Click the Generate button.

#### Figure 2-2: Edit Service Account

#### Edit Service Account: UNO-service-account

Created by sandeep.pawar				
* Description		* Status	* Roles	
Service Account for UNO		Enabled $\checkmark$	$sensor-enrollment \times$	~
Generate Service Acc	count Token			
* Description			* Valid Until	
Service Account for UN	0		Dec 31, 20	26 00:00:00 曲 Generate
Service Account Toke	ens		C' Refresh	Delete All Expired Tokens
Token ID ↑	Description		Created By	Valid Until
Filter	Filter		Filter	Filter
		No data to display		
				Cancel Save

**Note**: When the token is generated, copy and securely save it in a location where it can be accessed during sensor deployment.

#### 2.2 Adding the Sensor to the UI

To add the sensor to the CVaaS UI:

- 1. Navigate to Devices -> Device Registration -> Data Sources
- 2. Click the + Add Sensor button
- **3.** Enter a desired sensor name (for example, **sensor1**). Make sure to use the same name while deploying the sensor.

Note: Do not use *default* as the sensor name.

4. Click the Add button.

No additional information is required except for the Sensor Name.



۲	Devices	Device Registration	to Claud Vision	Add Sensor	×
Q	Inventory	Onboard Devices Data Sources V	irtual Router Deployments Re	A sensor collects state from data sources and streams to CloudVision.	
	Endpoint Overview			Sensor Name	
8	Wired Authentication	Data Sources		sensor1	
Ø	Device Registration	Onboard third-party devices and manual control of the second s	nanagement systems.	> Step One	
Þ	Compliance Overview			> Step Two	
33i	Connectivity Monitor	Sensor Name 🗘	Hostname	> Step Three	
*	Traffic Flows			> Step Four	
$\odot$	Endpoint Search	+ () cv-sensor12	cv-sensor12.sjc.aristanetworks.r	> Step Elva	
	Comparison Multi-Cloud Dashboard	+ O dhaya	-	> Troubleshooting	
	Network Segmentation	(+) O mac	-		
	Virtual Topologies Pathfinder Devices	+ 🗸 non-default	uno-cvplay- sensor1.sjc.aristanetworks.com		
		+ O rajshree-test	-		
6		+ O read-only-access-test	-		
ø		+ O sensor1-1	-	Cancel	Add

#### 2.3 Getting the Latest Sensor OVA

Download the UNO Sensor if you already have the OVA file or contact your Arista support representative for download instructions.

#### 2.4 Deploying the Sensor OVA

To deploy the Sensor OVA:

- 1. Navigate to the vCenter where you intend to deploy the sensor OVA. Right-click on the ESXi server.
- 2. Proceed to Deploy OVF Template and enter the URL of the latest Sensor OVA (see images below).

	Actions - tst-esx-92.sjc.aristanetworks.com	(	New vCenter server updates are a	vailable VIEW UPDATES	
vSphere Client	الله New Virtual Machine				
	C Deploy OVF Template	< 🐣 t	st-esx-92.sjc.aristanetv	vorks.com	
<u>()</u> Þ =	🗷 New Resource Pool	Summa	ary Monitor Configure A	Permissions VMs Resource Pools	
<ul> <li>uno-dev-vcente</li> <li>DIRECT-FOLI</li> </ul>	Ed New vApp	ſ	Hypervisor: Model:	VMware ESXi, 6.7.0, 130066 ProLiant DL360 Gen9	
VINO-DEV-SE	ក្រី Import VMs		Processor Type	e: Intel(R) Xeon(R) CPU E5-262	
<ul> <li>TEST-FOI</li> <li>UNO-DEV</li> </ul>	Maintenance Mode		Logical Process     NICs:	ors: 32 6	
> [ tst-esx-91	Connection •		Virtual Machine State:	S: 10 Connected	
ت cvp-20	Power •		Uptime:	72 days	
DMF-U	Certificates •		Howlett	لم Backard	
D log-vn	Storage •		Enterpris	Se	
යා msster බා ruby1-	登 Add Networking		Xi Shell for the host has been enable	d	
ලී surence බී Ubunt	Host Profiles	(1) ss	H for the host has been enabled		
🔂 uno-cv	Export System Logs	Har	dware		
🗇 uno-se	Reconfigure for vSphere HA		Manufacturer HP		
	Assign License		Model Pr	oLiant DL360 Gen9	
Recent Tasks Al     Task Name     Task Name     Task Name	Settings	Dataile T	Initiator T	Queued Y Start Time	
Refresh dvPort state	Move To		VSPHERE.LOCAL\Administrator	For 09/30/2024, 11:27:28 0	
Refresh dvPort state	Tags & Custom Attributes		VSPHERE.LOCAL\Administrator	1 ms 09/30/2024, 11:27:28 0	
Refresh dvPort state	Remove from Inventory		VSPHERE.LOCAL\Administrator	2 ms 09/30/2024, 11:27:28 0	
Refresh dvPort state	Remove norminelitory		VSPHERE.LOCAL\Administrator	2 ms 09/30/2024, 11:27:27 0	
Refresh dvPort state	Add Permission		VSPHERE.LOCAL\Administrator	2 ms 09/30/2024, 11:27:27 0	

Figure 2-4: Deplying OVF Template

3. Specify the VM name, datastore, and other required details during the deployment (see image below).

Figure 2-5: Deploy OVF Template page



#### 2.5 Booting up the Sensor

To boot up the Sensor for the first time after the Sensor deployment is completed:

- 1. Power on the VM and choose to LAUNCH REMOTE or WEB CONSOLE.
- 2. Log in using the credential:

User name: cvpadmin

- 3. Set a password for the root user.
- 4. When the sensor installation menu is displayed, select the **install** option by typing "i" or "**install**" (case sensitive).

#### Figure 2-6: Installing Sensor from CLI



The initial configuration screen appears (see image).

- 5. Enter the following details:
  - a. IP Address of eth0: Obtain the static IP from the vCenter administrator.
  - b. DNS Domain Search List: Multiple entries can be added using a comma separator.
  - **c. CV\_ADDR**: This is a preconfigured field depending on the region, please refrain from making any changes in a production deployment. The expected URLS based on the regions are:
    - 1. United States 1a: www.arista.io
    - 2. United States 1c: www.cv-prod-us-central1-c.arista.io
    - 3. Japan: www.cv-prod-apnortheast-1.arista.io
    - 4. Germany: www.cv-prod-euwest-2.arista.io
    - 5. Australia: www.cv-prod-ausoutheast-1.arista.io
    - 6. Canada: www.cv-prod-na-northeast1-b.arista.io
    - 7. United Kingdom: www.cv-prod-uk-1.arista.io
  - d. Sensor Name: Provide the same name used while adding the sensor on UI (For example, sensor1).
- 6. Verify the configuration by typing "v" or "verify."

Figure 2-7: Sensor Configuration

Sensor Configuration:

```
*Device Interface Name: eth0
 *DHCP Enabled: no
 *DNS Server IPv4 Addresses (comma separated): 172.22.22.40, 172.22.50.40
 Domain Search List (comma separated): sjc.aristanetworks.com
 *Number of NTP Servers: 1
 NTP Server Address (IP address or FQDN) #1: ntp1.aristanetworks.com
 Is Auth enabled for NTP Server #1: no
 *Hostname (FQDN): nic3-uno-sensor.sjc.aristanetworks.com
 *IPv4 Address of eth0: 172.30.155.252
 *IPv4 Netmask of eth0: 255.255.255.128
 NAT IP Address of eth0:
 *Default Gateway: 172.30.155.129
 *CV_ADDR: www.cv-dev.corp.arista.io
*Sensor Name: sensor
 Proxy server address for sensor (optional):
Sensor Configuration Menu
[q]uit [p]rint [e]dit [v]erify [s]ave [a]pply [h]elp ve[r]bose
```

7. Once verification is successful, apply the configuration by typing "a" or "apply".

While the configuration is being applied, you are prompted to add the access\_token in the file /*etc/cvpi*/ *access\_token* as follows. The setup wizard waits for you to create this token file.

#### Figure 2-8: Sensor Configuration Menu



- 8. To add the token, SSH to the VM as the root user and use the token generated in Generating a Service Account Token section and enter it in the /etc/cvpi/access\_token file.
- 9. Copy the service account token and execute the following command on the sensor VM to set it:

```
echo "paste_token_here" > /etc/cvpi/access_token
```

The above command writes the copied token to the /etc/cvpi/access\_token file on the Sensor VM. Once you create and save this token file, the setup wizard automatically proceeds with the installation process.

- **10.** Type **s** or **save** to save the configuration.
- 11. Once the installation is successful, all the components, including the sensor, will be up and running.
- 12. Verify the status by SSHing to the VM and by using the command:

cvpi status all -v3

For Sensor Streaming to CVaaS, the sensor name configured in earlier steps (sensor1) shows up with a green tick indicating that deployment of Sensor OVA is successful and the Sensor is able to communicate with CVaaS.

#### Figure 2-9: Sensor Deployed Successfully

🔿 🔿 😫 geiger-prod-next	infra.corp.arista.io/cv/devices/device-or	nboarding?apiServer=cvStaging&deviceOnboarding1	ab=onboardDataSource	15			* Ð I
Devices	Device Registration Onboard physical and virtual device	es to CloudVision				Tloud Staging Clu	uster ∽ ຊິ <sup>v</sup> u
Inventory	Onboard Devices Data Sources	Virtual Router Deployments Re-ZTP Devices	Decommission Device	es			
Endpoint Overview ^							
Wired Authentication	Data Sources					+ Add Sensor + Onbo	bard via YAML F
Device Registration	Onboard third-party devices and third-party devices	id management systems.					
Compliance Overview							
Connectivity Monitor	Sensor Name	Hostname	IP	Version	Last Seen	0 Data Sources 0	
Traffic Flows	+ 🗸 sensor1	uvm311-sensor1.sjc.aristanetworks.com	10.239.6.231	v1.0.0-4736-g21c7aa3	Oct 7, 2024 11:28:13	77	0 0
Endpoint search							

#### 2.6 Adding the Data Sources

To add data sources:

- 1. Go to Network -> Device Registration -> Data Sources
- 2. Click the + Onboard Data Source button.
- 3. Choose the sensor from the drop-down list (for example, sensor1)
- 4. Select the required device type template, such as Cisco ISE, DMF, Flow, VMware vCenter, or YAML file.
- 5. Enter the necessary fields and click **Onboard** to add the data source.

#### Figure 2-10: Add Data Sources

	Applications Devices Events Provisioning Dashboards Topology	Onboard Data Source			
Devices > Device	Registration				
Inventory	Onboard Devices Data Sources Virtual Router Deployments Decommission Devices	Each data source is onboarded with an assigned sensor and a configu template for communication with CloudVision.			
Device Registration		Sensor ①			
Compliance Overview	Data Sources	sensor ~			
Endpoint Overview	Onboard third-party devices and management systems.	Onboard third-party devices and management systems.     Template ①			
Connectivity Monitor		Template Q			
Traffic Flows	Sensor Name Version Streaming Start	Cisco ISE			
Endpoint Search	+ O default v0.1.2-29091-g03be22a Mar 20, 2023 20:06:10	Flow			
Comparison		VMware			
Multi-Cloud Dashboard	+ O sensor v0.1.2-33875-gdd765de Jul 25, 2023 07:54:44	YAML File			
Network Segmentation					

After adding the data sources, check if the data is streaming successfully. A green tick in front of each data source (under sensor1) indicates successful streaming, and a red mark indicates an issue with the streaming (see image below).

#### Figure 2-11: Device Registration - Data Sources

Devices Inventory	Device Registration       Image: Constraint of the standard physical and virtual devices to CloudVision         Onboard physical and virtual devices to CloudVision       Image: Constraint of the standard physical and virtual devices to CloudVision         Onboard Devices       Data Sources       Virtual Router Deployments       Re-ZTP Devices       Decommission Devices
Endpoint Overview	
Device Registration	Data Sources     + Add Sensor     + Onboard Data Source     + Onboard via YAML File       Onboard third-party devices and management systems.
Compliance Overview	
Connectivity Monitor	Sensor Name
Traffic Flows	
Endpoint Search	□ ✓ sensor1 uvm311- sensor1.sjc.aristanetworks.com 10.239.6.231 v1.0.0-4736- g21c7aa3 Sep 30, 2024 11:55:39 77 Ø  ⓐ
Comparison	Name         Image: Type         Type         Type         Type
Multi-Cloud Dashboard	
Network Segmentation	✓ vCenter7-2-linked VMware vCenter 04ba20c2-b4eb-4815-a253-f5610bd0e404 Sep 30, 2024 11:55:37 Yes ····
Virtual Topologies Pathfinder Devices	✓ uvm143-vcsim1 VMware vCenter 25e8071c-c8e5-5b94-88d0-b0057632e9dd <u>Sep 30, 2024 11:55:38</u> Yes …
	✓ uvm244-vcsim4 VMware vCenter 294113eb-6858-529c-8f74-c17dff2ecba6 Sep 30, 2024 11:55:37 Yes ···
	O uvm244-vcsim3         VMware vCenter         2a09b277-44ff-537e-8973-85a47d297ef5         Sep 24, 2024 14:27:56         No         ···

6. Click the sensor to access the streamed data source details and for any status message indicating if the sensor has started or there is an error message under *Sensor Details*.

Devices Inventory Endpoint Overview	Device Registration           Onboard physical and virtual devices to CloudVision           Onboard Devices         Virtual Router Deployments         Re-ZTP Devices         Decommission Devices	P Sandeep.pawar
Wired Authentication	Data Sources > sensor1 ~ > Sensor Details	
Device Registration Compliance Overview Connectivity Monitor Traffic Flows	Status     Sensor ID     Hostname     IP Address     Version     Streaming Start       Streaming     sensor1     uvm311-sensor1.sjc.aristanetworks.com     10.239.6.231     v1.0.0-4736-g21c7aa3     Sep 27, 2024 20:01:49       Last Seen     Data Sources     77     77     77     77	
Endpoint Search	Sensor Logs	) Refresh
Comparison Multi-Cloud Dashboard	Time Message	
Network Segmentation	Sep 28, 2024 18:30:48 Sensor clock is in sync, starting Sensor	
Virtual Topologies	Sep 28, 2024 18:30:48 Sensor clock is not in sync, stopping Sensor	
Pathfinder Devices	Sep 27, 2024 20:01:50 Sensor started at 2024-09-27 14:31:49 UTC	

Similarly, click on each on-boarded data source to display the respective data source status messages (whether the data source has started or if there are any errors).

Figure 2-13: Data Source Details

Devices	Device Registration Choose to CloudVision
Inventory	Onboard Devices Data Sources Virtual Router Deployments Re-ZTP Devices Decommission Devices
Endpoint Overview	
Wired Authentication	Data Sources > sensor1 > vCenter7-2-linked ~ > Data Source Details         Edit Config         Edit Config as YAML
Device Registration	Status Name Device ID Type Sensor Log Level Streaming From
Compliance Overview	✓ Streaming vCenter7-2-linked 04ba20c2-b4eb-4815-a253-f5610bd0e404 VMware vCenter sensor1 Unspecified Logging Sep 28, 2024 18:30:58
Connectivity Monitor	Last Seen Sep 30, 2024 11:57:27
Traffic Flows	
Endpoint Search	Data Source Logs
Comparison	This data source has unspecified logging enabled.
Multi-Cloud Dashboard	Time Message
Network Segmentation	
Virtual Topologies	Sep 28, 2024 18/31:15 Inventory - vms: 13, hosts: 1, vdss: 1, vdsportgroups: 2, compute resources: 1, data centers: 1
Pathfinder Devices	Sep 28, 2024 18:31:14 The datasource configuration is correct
	Sep 28, 2024 18:31:13 vCenter url is reachable, URL: https://uno-vcenter7-2.sjc.aristanetworks.com

Now, you can view the on-boarded data sources and confirm that data streaming has started.

#### 2.6.1 Adding VMware vCenter as a Data Source

To add VMware vCenter as a Data source:

Select the **VMware vCenter** template to onboard vCenter as a Data Source in CloudVision. Use the *read-only credentials* to onboard your vCenters. CloudVision does not perform any write operations in vCenter.

**Note**: If you choose the option **Skip Certificate Verification** as *no* for vCenter data sources, provide the CA certificates if the vCenter servers are using certificates issued by a private or internal CA. These certificates are required for successful TLS verification between the Sensor and vCenter servers.

Or, if you do not have the CA certificate or wish to continue without CA certificate verification, choose the option **Skip Certificate Verification** as yes.

Figure 2-14:	Onboard a	Data Source
--------------	-----------	-------------

Onboard Data Source		×
Each data source is onboarded with an assigned sensor and a configuration t with CloudVision.	emplate for com	munication
* Sensor ①		
sensor1		$\sim$
* Template (i)		
VMware vCenter		~
Device ID (i)		
VWVC-BUFMK		
Display Name		
Enabled		
• Yes		
No		
Log Level 🛈		
General Information Logging		~
* vCenter URL or IP Address		
https://vCenterUrl.com		
* vCenter Username		
vCenter Username		
* vCenter Password		
vCenter Password		Ø
Skip Certificate Verification		
Yes		
O No		
	Cancel	Onboard

After adding VMware vCenter as a Data Source in CloudVision, it is recommended to configure the following in the vCenter to enable proper CV UNO functionalities:

• Enable LLDP transmission on Distributed Virtual Switches (DVS)

· Enable NetFlow on Distributed Virtual Switches

#### 2.6.1.1 Enabling LLDP in vCenter

To enable LLDP for ESXi hosts managed by a DVS:

- **1.** Log in to the vCenter.
- 2. Navigate to Hosts and Clusters -> Networking.
- 3. Right-click on the Distributed Virtual Switch used by the ESXi host in question by navigating to Settings → Edit settings → Advanced → Discovery Protocol
- 4. Choose the Discovery Protocol as Link Layer Discovery Protocol, and Both operations.
- 5. Click the OK button.

#### UNO-DEV-DS1 ACTIONS Summary Monitor Cor UNO-DEV-DS1 VMs Manut Distributed Port Group DPortGroup 12 Versi DPortGroup 13 Add and Manage Hosts. A DPortGroup 14 Edit Notes... DPortGroup 15 DPortGroup 16 Upgrade DPortGroup 6 Event-Grouping-D-DVUplinks-504 Settings Edit Settings. Switch Details > test-debug Move To. Edit Private VLAN. Netv > test-event-grouping-vds = test-new-dvs Hosts Rename Edit NetFlow. B DPortGroup Vite Tags & Custom Attributes Export Configuration. (a) testin ht-DV/Holiokt-162 Deve UNO-DEV-DS1 Add Pern Restore Cor figuration. DPortGroup 10 DPortGroup 7 Alarms Port m Notes 4 DPortGroup 8 🔀 Delete KIMP MLD M DPortGroup 9 DPortGroup-EventTest Tags DPortGroup-to-Id560-et33 DPortGroup-to-ph103-et3/33/1 Ass Custom Attributes UNO-DEV-DS1-DVUplinks-63 UNO-DPG-V101 Attribute UNO-DPG-V103 Recent Tasks Alarms τ.0 T Target T Statu T Deta T Ourord T Start.Time ÷ T Completion Time T Serve Port state 05.63 10/07/2024.10.48.09

#### Figure 2-15: Enable LLDP in vCenter

Figure 2-16:	Edit Setting	s on a	Distributed	Switch
inguic L io.	East Octing	5 011 u	Distributed	0111011

Distributed Switch - UNO-DEV-DS1 × Edit Settings						
General Advanced	Uplinks					
MTU (Bytes)	1500					
Multicast filtering mode	Basic ~					
Discovery protocol						
Туре	Link Layer Discovery Protocol 🗡					
Operation	Both ~					
Administrator contact						
Name						
Other details						

CANCEL	ок
--------	----

CV Sensor can receive Netflow records from the vCenter. The Sensor consumes the NetFlow records from the vCenter and sends processed flow information to the CVaaS instance.

Follow these configuration steps to enable Netflow:

- Sensor Configuration for Enabling Netflow
- vCenter Configuration for Enabling Netflow

#### 2.6.1.2 Sensor Configuration for Enabling Netflow

On the **Data Sources** screen, click the **Onboard Data Source**. Select the sensor name and then select **Flow** as the Template (see image).

#### Figure 2-17: Enabling NetFlow on Sensor

Onboard	Data	Source	
---------	------	--------	--

×

Each data source is onboarded with an assigned sensor and a configuration template for communication with CloudVision.

\* Sensor 🛈

sensor1

\* Template 🛈

Flow	~
Application Connector	
DMF	
Flow	
VMware vCenter	
Enabled	

0	Yes			
	No			
		_		

Log Level 🛈

General Information Logging

 $\sim$ 

Enter a name for the data source and click the **Onboard** button (see image).

#### Figure 2-18: Onboard Data Source

Onboard Data Source	×
Each data source is onboarded with an assigned sensor and a configuration template for communicatio with CloudVision.	'n
* Sensor (i)	
sensor1	$\sim$
* Template (i)	
Flow	$\sim$
Device ID (i)	
FLOW-HTOIC	
Display Name	
sensor1-flow	
Enabled	
O Yes	
○ No	
Log Level 🛈	
General Information Logging	$\sim$

#### 2.6.1.3 vCenter Configuration for Enabling Netflow

To enable Netflow on a vCenter, you must configure each Distributed Virtual Switch (DVS). On each of the Distributed Switch in your vCenter, follow the below steps:

Cancel

Onboard

1. Right-click the DVSwitch used by the ESXi host by navigating to Settings → Edit NetFlow

Figure 2-19: Enabling NetFlow on vCenter

$\equiv$ vSphere Client $Q$					Adminis	trator@VSPHERELOCAL ~	9
DPertGroup 11     DPertGroup 12     DPertGroup 13     DPertGroup 13     DPertGroup 14     DPertGroup 14     DPertGroup 15     DPertGroup 16     DPertGroup 6     DPertGroup 6     DeetGroup 6     test-event grouping-vds     test-event grouping-vds     test-event grouping-vds     DeprtGroup     DeprtGroup	Switch Details Networks Hosts Vortailmachines Ports	Actions - UNO-DEV-DS1 Distributed Port Group Add and Manage Hosts Edit Notes Upgrade Settings Move To Rename Tags & Custom Attributes Add Permission	VMs Netw (c) Edit Sett Edit Priva Edit NetF Export C Restore 4	ings ite VLAN Flow Configuration	Control Iscovery Protocol ation Control Protoco ation Timeout	Supported Supported Supported Eucoported Not supported	^
DPortGroup 7  DortGroup 8	Notes	Alarms •	~	Port mirrori IGMP/MLD	ng unooping	Supported Supported	
Divorticroup 9     Divorticroup-EventTest     Divorticroup-to-lod560-et33     Divorticroup-to-ph103-et3/33/1	Tags Assigned Tag	Category Description	^	Health cheo	k	Supported	
				Attribute		Value	
V Recent Tasks Alarms							

- 2. Add the necessary details in the form as shown in the image below.
  - a. Collector IP: Use the Sensor IP
  - b. Collector port: 4739
  - c. Sampling Rate: 10000

**Note:** A sampling rate of 10,000 means that one packet will be sampled for every 10,000 packets. To capture more samples and improve visibility on the topology page, reduce the sampling rate to 1000 or less. Remember that reducing the sampling rate may introduce a slight increase in network load.

**d.** Switch IP address: Unique IPv4 address across VDSs in a vCenter (not necessarily a pingable IPv4 address)

#### Figure 2-20: Edit NetFlow Setting for vCenter

Edit NetFlow Settings		UNO-DEV-DS1 ×
NetFlow		
Collector IP address	172.30.155.252	
Collector port	4739	
Observation Domain ID	0	
Switch IP address	1.2.3.4	(i)
Advanced settings		
Active flow export timeout (Seconds)	60	
ldle flow export timeout (Seconds)	15	
Sampling rate	10000	* *
Process internal flows only	Disabled 🗸	



**3.** Click **OK** to save the changes.

After enabling NetFlow on all the DV switches, ensure to enable NetFlow on all Distributed Port Groups of the DV switches by:

- 1. Right-click on the DVS → Distributed Port Group → Manage Distributed Port Groups
- 2. Select Monitoring
- 3. Select all of the Distributed port groups (Or select the applicable port groups in your environment)
- 4. Enable the **Netflow**
- 5. Click the Finish button.

After NetFlow is enabled on a port group, it sends NetFlow data to the collector specified in the DVS settings. However, the port group sends NetFlow data only for ingress packets (entering the port group) and not for egress packets (exiting the port group).

To collect data for all traffic, enable NetFlow for the Uplink port group as well. If you do not enable NetFlow for the uplink port group, the UNO sensor will not receive NetFlow for any traffic going out from the VMs to the physical network.

**Note**: In the bulk port group configuration, it is not possible to enable NetFlow for the Uplink port group. You must enable the uplink port group separately.

To enable the uplink port group:

- 1. Right-click on the Uplink Port group under the Distributed Virtual Switch section → Settings (The port group name should have the DVUPlinks on it).
- 2. Navigate to the Monitoring tab
- 3. Enable Netflow
- 4. Click the **OK** button to save the changes.

For details on Adding VMware vCenter as a Data Source, refer to: <u>https://faddom.com/network-visibility-in-virtual-environments-part-2/</u>

#### 2.6.2 Adding SNMP Data Source

Devices from third-party vendors that support SNMP can be integrated into Cloud Vision as SNMP data sources. Both SNMPv2c and SNMPv3 versions are supported.

To add SNMP data source:

1. Click the **Onboard Data Source** button, and choose either the **SNMPv2c** or **SNMPv3** template from the Template drop down menu.

← →	o 😫 https://www.ov-	staging.corp.arista.io/cv/devices/data-sources		🖈 🔚 🔁 🔞 Relaurch to update :
ڪ	Devices	Data Sources		Onboard Data Source X
Q	Inventory	Onboard third-party devices and management syst	tems.	Each data course is enhanded with an assigned sensor and a configuration tamplate for communication
	Endpoint Overview	Sensor Table		with CloudVision.
	Wined Authentication	5 items		• Sensor ①
Q	TITLES PARTICIPATION OF			sensor1 V
ΕΞ	Device Registration	Sensor Name 🕆 🖓	Status 0 🖓 Hostname 0 🖓	• Template ①
Þ	Data Sources	connector-local	() inactive	Select ~
35	Compliance Overview		Active committeeneert sic arist	SNMPv2c
*	Connectivity Monitor	tanana ASCause		SNMPv3
	Traffic Flows		United United and Unit	PitelarName
	Endpoint Search	uvm344-sensor2	✓ Active uvm344-sensor2.sjc.arit	Unsplay Name
	Comparison	uvm344-sensor3	✓ Active uvm344-sensor3.sjc.aris	· · · · · · · · · · · · · · · · · · ·
	Multi-Cloud Dashboard	Data Source Table		Enabled
	Network Segmentation	345 items		No No
	Virtual Topologies			
	Part Se des Des José	□ Data Source Name ↑ ▽ Statu	s ≎ ⊽ Type ≎ ⊽ D	General Information Logging
	Pathninder Devices	app_creator CSV connector	ctive Application Connector A	
		bigSwitch vcenter-8.0	tive VMware vCenter b	
		Cisco dut373 🗸 Ad	tive SNMPv3 J	
88		Cisco dut374	ctive SNMPv2c S	
6		Cisco n3k-257-38	tive SNMPv3 S	
0		Csv connector O Dis	abled Application Connector A	Cancel Onboard
		0.001015		Officer Officer

Figure 2-21: Onboarding SNMP Data Source

€→	$\epsilon  ightarrow \mathcal{O}$ (\$ https://www.cv-staging.corp.arista.lojcy/dev/ces/data-sources										
<b>&amp;</b>	Devices	Data Sources Onboard third-party devices and management systems	e.	Onboard Data Source	<						
80 3	Endpoint Overview	Sensor Table		SNMP/3 Device ID ①							
Ω E≣	Device Registration	Sensor Name 🛧 🗸	Status 0 ▽ Hostname 0 ▽	SNMP-RVXM7 Display Name							
29 22	Compliance Overview	connector-local sensor1	O inactive ✓ Active	Enabled							
*	Traffic Flows	uvm344-sensor1 uvm344-sensor2	Inactive uvm344-sensor2.sjc.aris     Active uvm344-sensor2.sjc.aris	Yes No							
	Comparison	uvm344-sensor3	Active uvm344-sensor3.sjc.aris	Log Level () General Information Logging ~	~						
	Network Segmentation	345 items		* Device Address IPv4 address or hostname							
	Pathfinder Devices	□ Data Source Name ↑ ▽         Status ○           □ app_creator CSV connector         ✓ Active	▼         Type © ▼         D           Application Connector         Al	Port 161							
		bigSwitch vcenter-8.0         ✓ Active           Cisco dut373         ✓ Active	VMware vCenter bo SNMPv3 JF	* Polling Interval 60 Seconds V							
88 6		Cisco dut374 ✓ Active	SNMPv2c Si SNMPv3 Sr	SNMP Auth Version							
۵		O csv connector O Disable	d Application Connector Al	Cancel Onboard	1						

🗧 🔆 🔿 🕫 https://www.ov-staging.corp.arista.lojcv/dev/ces/data-sources 🕫 🗴 👸 🖄 I 🙆 Relaunch to update										
<b>4</b>	Devices	Data Sources Onboard third-party devices and mar	agement systems.		Onboard Data Source					
2 10 10	Endpoint Overview	Sensor Table			161 * Polling Interval					
.⊟ ∕2	Device Registration	Sensor Name 🔶 🖓		0 ∇ Hostname 0 ∇	60 Seconds V SNMP Auth Version					
- 	Compliance Overview Connectivity Monitor	lew sensor1		tive	3 • Security ① Authentication and privacy	~				
	Traffic Rows Umm344-sensor1 Umm344 Endpoint Search Umm344-sensor2 Comparison Mut0-Cloud Dashboard Data Source Table Umm344 Data Source Table		✓ Act	tive uvm344-sensor2.sjc.ari	Authentication Authentication and privacy					
				* Authentication Protocol Select						
	Virtual Topologies	□ Data Source Name ↑ ♥	Status ≎ ⊽	Type ≎ ⊽ t	Authentication Key	ø				
		bigSwitch vcenter-8.0	✓ Active ✓ Active	Application Connector A VMware vCenter b	Privacy Protocol ①     Select	×				
88°		Cisco dut373	Active	SNMPV2C S	• Privacy Key ①	ø				
ø		C csv connector	<ul> <li>Disabled</li> </ul>	Application Connector		Cancel Onboard				

- 2. Enter the required information based on the selected template.
- 3. Common fields:
  - a. Device address
  - b. Port
  - c. SNMP version
- 4. For the SNMPv2c template, enter the Community string.
- 5. For the SNMPv3 template, specify the
  - a. Security Level
  - b. Security Name
  - c. Authentication Protocol
  - d. Authentication Key
  - e. Privacy Protocol
  - f. Privacy Key according to the chosen Security Level.

If the entered details are correct and the Sensor can successfully communicate with the device, then the device gets added to the sensor, and starts the data streaming from SNMP walk/get to CVaaS.

If there are any issues, the data source will be marked as red (inactive). Check the relevant log messages to identify the cause of the issue.

#### Upgrading the Sensor

To upgrade a sensor, perform the following steps:

1. To prepare for the upgrade, run following commands on the sensor VM:

```
rm -rf /tmp/upgrade
mkdir /data/upgrade
ln -s /data/upgrade /tmp/upgrade
```

**Note**: If the directory already exists, you may see an error message during the mkdir step. Ignore the error message.

- Get the latest sensor upgrade package (for example, cv-sensor-upgrade-1.1.0.tgz): Download the latest file from the <u>Software Download</u> page, scroll down to the CloudVision > CloudVision Sensor > cvsensor-1.1.0.
- 3. Run the upgrade command:
  - a. Access the VM by logging in as 'cvpadmin'.
  - b. Type 'u' or 'upgrade' (case sensitive) to select the upgrade option:

Figure 3-1: Upgrading the Sensor CLI Output



Confirm the base OS upgrade warning for the upgrade process to proceed.

4. Confirm reboot to complete the upgrade process.



After the system reboots, review the upgrade logs in the *cvpUpgrade.log* file available in the /data/ directory. Look for the latest directory with a name formatted as *upgrade.<timestamp>*. For example, /data/ upgrade.24\_12\_13\_05\_05\_56/cvpUpgrade.log.

Once the upgrade is successful, the log file displays a message confirming the upgrade: "*CV-SENSOR successfully upgraded from version x.x.x to y.y.y*"

[root@uno-sensor-test2 data]# tail -f upgrade.24_12_13_05_33_39/cvpUpgrade.log
(Fri Dec 13 05:34:40 UTC 2024) Waiting for cvpi service to start.
[Fri Dec 13 05:34:40 UTC 2024] cmd :  sudo systemctl is-activequiet cvpi
[Fri Dec 13 05:34:40 UTC 2024] stdout:
[Fri Dec 13 05:34:40 UTC 2024] stderr:
[Fri Dec 13 05:34:40 UTC 2024] rc : 0
[Fri Dec 13 05:34:40 UTC 2024] Cvpi service has started
[Fri Dec 13 05:34:40 UTC 2024] Starting all components.
[Fri Dec 13 05:34:40 UTC 2024] Checking status (it may take up to 0.0h 30.0m)
[Fri Dec 13 05:38:23 UTC 2024] All components are up and running
[Fri Dec 13 05:38:23 UTC 2024] CV-SENSOR successfully upgraded from version 1.1.0 to 1.1.0

If the upgrade step fails due to any components not running, conduct an initial investigation to determine the cause of the particular component's unavailability.

After you have identified the issue causing the component to be inactive and still wants to upgrade, proceed to the next step to initiate the sensor upgrade, even though the component is not running.

During a failure, an error message is displayed:

CV-SENSOR upgrade failed with the following error: ... CvpRuntimeError: Some components are not running, CV-SENSOR cannot be upgraded

Perform the following steps to proceed with the Sensor upgrade:

1. Navigate to the '/tmp/upgrade' directory by using the command:

cd /tmp/upgrade

2. Check the availability of cvpUpgrade.py file by using the command:

ls cvpUpgrade.py

If the above command returns no results, untar the upgrade.tgz file using the command:

tar -xvf cv-sensor-upgrade-\*.tgz

**3.** Execute the upgrade process by using the following command:

./cvpUpgrade.py --deployment-type cv-sensor --skip-status-check SKIP\_STATUS\_CHECK

The upgrade process is initiated.

#### Chapter 4

#### **Troubleshooting [New Installation]**

This section provides information on common issues that may arise during the CV Sensor deployment and suggests possible solutions to address them.

#### 4.1 How to restart the sensor component?

To restart the sensor:

- 1. SSH to the VM
- 2. Execute the following cvpi commands to restart the sensor:

```
cvpi stop sensor --is-local-action cvpi start sensor --is-local-action
```

Below is an example of the restart process:

```
[root@cvp230 ~]# cvpi stop sensor --is-local-action
- command: kubectl delete -f /cvpi/conf/kubernetes/sensor.yaml --ignore-not-found=true
 cmdfunc: StopActionCmd
 component: sensor
 action: stop
 node: primary
 result:
ip: ""
  stdout: ""
  stderr: ""
  err: null
  exitcode: 0
root@cvp230 ~]# cvpi start sensor --is-local-action
- command: bash -c "envsubst < /cvpi/conf/kubernetes/sensor.yaml | kubectl apply -f
    _ "
 cmdfunc: StartActionCmd
 component: sensor
 action: start
 node: primary
 result:
ip: ""
   stdout: ""
   stderr: ""
    err: null
    exitcode: 0
```

3. After the restart, verify if all components are running correctly:

cvpi status all -v3

Below is an example:

[root@cvp230 ~]# cvpi status all -v3
Executing command. This may take some time...

<pre>(E) =&gt; Enabled (D) =&gt; Disabled (?) =&gt; Zookeeper Down</pre>			
Action Output COMPONENT ERROR	ACTION	NODE	STATUS
containerd	status	primary	(E) RUNNING
coredns	status	primary	(E) RUNNING
descheduler	status	primary	(E) RUNNING
etcd	status	primary	(E) RUNNING
flannel	status	primary	(E) RUNNING
fluent-bit	status	primary	(E) RUNNING
kube-apiserver	status	primary	(E) RUNNING
kube-controller-manage	er status	primary	(E) RUNNING
kube-proxy	status	primary	(E) RUNNING
kube-scheduler	status	primary	(E) RUNNING
kubelet	status	primary	(E) RUNNING
mutating-webhook	status	primary	(E) RUNNING
mutating-webhook-serve	er status	primary	(E) RUNNING
sensor	status	primary	(E) RUNNING
sensor-monitor	status	primary	(E) RUNNING
zookeeper	status	primary	(E) RUNNING

#### 4.2 How to Monitor Sensor Resource Utilization?

The sensor metric is exported to the CVaaS to track sensor resource utilization, which is displayed on the dashboard. Enable the UNO features toggle to view the sensor dashboard. You can also access the Sensor Health Dashboard from the Dashboards:

To access the Sensor dashboards:

- **1.** Login to the CVaaS.
- 2. To access the Sensor Dashboard:
  - a. Navigate to Dashboards > Sensor Health Monitor
  - **b.** Select a sensor from the drop-down list.
- 3. For embedded sensor dashboard on the sensor details screen:
  - a. Navigate to Devices > Data sources
  - b. Click an available sensor
  - c. Scroll down for graphs

The dashboard includes the following metrics:

· Sensor VM CPU utilization

Sensor K8s Pod CPU utilization





- Sensor VM Memory utilization
- Sensor K8s Pod Memory utilization





- · Sensor VM Network utilization
- Sensor K8s Pod Network utilization



#### Figure 4-3: Sensor Network Usage

#### 4.3 Where to check for logs?

To check for the log files:

=

1. SSH to the VM. The logs are managed by journald and can be viewed using journalctl commands:

[root@cvp230 ~] # journalctl IO\_KUBERNETES\_CONTAINER\_NAME=sensor

Below is a sample log content for reference:

<pre>Jul 01 04:59:52 nic3-uno-sensor.sjc.aristanetworks.com sensor[3759]: time="2024-07-01T04:59:52Z" level=debug msg="v2Client: SetRequest {origin:\"openconfig\" elem:{name:\"interfaces\"} elem:{name:\"interface\" key: {key:\"name\" value:\"GigabitEthernet1/0/12\"} elem:{name:\"state\"} elem:{name:\"counters\"} target:\"FJB2 388B0GR\"}: 5 updates, 0 replaces, 0 deletes" file="v2/v2client.go:80"</pre>
<pre>Jul 01 04:59:52 nic3-uno-sensor.sjc.aristanetworks.com sensor[3759]: time="2024-07-01T04:59:52Z" level=debug msg="Send SetRequest: prefix:{elem:{name:\"interfaces\"} elem:{name:\"interface\" key:{key:\"name\" value: \"TenGigabitEthernet1/1/7\"} elem:{name:\"state\"} elem:{name:\"counters\"} update:{path:{elem:{name:\"in-</pre>
<pre>multicast-pkts\"} val:{uint_val:119653}} update:{path:{elem:{name:\"in-octets\"}} val:{uint_val:32160350}}" file="dedup/dedup proxy.go:203"</pre>
<pre>Jul 01 04:59:52 nic3-uno-sensor.sjc.aristanetworks.com sensor[3759]: time="2024-07-01T04:59:52Z" level=debug msg="v2Client: SetRequest {origin:\"openconfig\" elem:{name:\"interfaces\"} elem:{name:\"interface\" key: {key:\"name\" value:\"TenGigabitEthernet1/1/7\"} elem:{name:\"state\"} elem:{name:\"counters\"} target: \"FJB2338B0GR\"): 2 updates, 0 replaces, 0 deletes" file="v2/v2client.go:80"</pre>
Jul 01 04:59:52 nic3-uno-sensor.sjc.aristanetworks.com sensor[3759]: time="2024-07-01T04:59:52Z" level=debug msg="Send SetRequest: prefix:{elem:{name:\"interfaces\"} elem:{name:\"interface\" key:{key:\"name\" value:
<pre>\"TenGigabitEthernet1/1/4\"} elem:{name:\"state\" elem:{name:\"counters\"} update:{path:{elem:{name: \"in-multicast-pkts\"} val:{uint_val:5416661} update:{path:{elem:{name:\"in-octets\"} val:{uint_val :1009059178} update:{path:{elem:{name:\"out-multicast-pkts\"} val:{uint_val:1794289} update:{path:{elem: {name:\"out-octets\"} val:{uint_val:226080394}" file="dedup/dedup_proxy.go:203"</pre>
<pre>Jul 01 04:59:52 nic3-uno-sensor.sjc.aristanetworks.com sensor[3759]: time="2024-07-01T04:59:52Z" level=debug msg="v2Client: SetRequest {origin:\"openconfig\" elem:{name:\"interfaces\"} elem:{name:\"interface\" key: {key:\"name\" value:\"TenGigabitEthernet1/1/4\"} elem:{name:\"state\"} elem:{name:\"counters\"} target: \"FJB2338B0GR\"}: 4 updates, 0 replaces, 0 deletes" file="v2/v2client.go:80"</pre>

**Note:** Append -f to journalctl command to follow logs.

2. Check the logs between a specific time interval using the command:

```
journalctl IO_KUBERNETES_CONTAINER_NAME=sensor --since "2024-07-26 12:10:46" --until
"2024-07-26 12:11:46
```

Below are examples of journalctl commands to filter logs:

• To check all the error logs of system:journalctl -p err -b

You can change level from err to info, warning, alert, debug

- To check only stdout logs: journalctl \_TRANSPORT=stdout
- To check logs from specific time: journalctl --since "2024-01-24 17:15:00"
- To check logs for specific service: journalctl -u zookeeper.service --since today
- To check logs for specific process id: journalctl \_PID=3918
- To check last 100 lines of logs: journalctl -n 100
- To follow logs: journalctl -f
- Some helpful grep commands for data source specific logs: journalctl
   IO\_KUBERNETES\_CONTAINER\_NAME=sensor -n 1000 | grep
   Flow\_Datasource\_name ⇒ logs by datasource namejournalctl
   IO\_KUBERNETES\_CONTAINER\_NAME=sensor -n 1000 | grep provider=events ⇒
   logs for events providerjournalctl IO\_KUBERNETES\_CONTAINER\_NAME=sensor
   -n 1000 | grep datasource=uvm244-vcsim3 ⇒ logs for specific
   datasourcejournalctl IO\_KUBERNETES\_CONTAINER\_NAME=sensor
   -n 1000 | grep datasource=uvm244-vcsim3 ⇒ logs for specific
   datasourcejournalctl IO\_KUBERNETES\_CONTAINER\_NAME=sensor -n 1000
   | grep vcenterId=fda4fd5c-bd4e-4554-925d-f142a3232667 ⇒ logs for
   vcenter datasource matching given vcenter uuid

Below are some cvpi commands to check logs:

- To check current sensor pod logs: cvpi logs sensor
- To check all sensor logs: cvpi logs sensor --full
- To pack sensor logs to tar file: cvpi debug logs

#### 4.4 How to change the access\_token?

To change the access token:

- 1. SSH to the VM.
- 2. Obtain the new service account token.
- 3. Write down the new service account token into the file /etc/cvpi/access\_token. You can do this using a text editor or the commands:

echo "your\_new\_access\_token\_here" | sudo tee /etc/cvpi/access\_token

4. Run the following commands:

```
cvpi stop sensor --is-local-action
```

cvpi init sensor --is-local-action cvpi start sensor --is-local-action

```
The above commands stop the sensor, initiate the sensor, and then start the sensor with the
updated access_token. For example:
 root@cvp230 ~]# cvpi stop sensor --is-local-action
  - command: kubectl delete -f /cvpi/conf/kubernetes/sensor.yaml --ignore-not-found=true
    cmdfunc: StopActionCmd
    component: sensor
    action: stop
    node: primary
    result:
ip: ""
      stdout: ""
      stderr: ""
      err: null
      exitcode: 0
 [root@cvp230 ~] # cvpi init sensor --is-local-action
            '!=' 1
  + TOKEN DIR=/etc/cvpi
 + TOKEN_FILE=/etc/cvpi/access_token
+ '[' '!' -f /etc/cvpi/access_token ']'
+ '[' '!' -s /etc/cvpi/access_token ']'
   echo 'Creating kubernetes secret for cvp service access token'
kubectl delete secret secret-service-access-token --ignore-not-found=true
 + kubectl create secret generic secret-service-access-token --from-file=/etc/cvpi/access token
  + rm /etc/cvpi/access_token
 + touch /etc/cvpi/access_token
- command: /cvpi/apps/sensor/bin/init.sh
    cmdfunc: DefaultActionCmd
    component: sensor
    action: init
    node: primary
    result:
ip: ""
      stdout:
        Creating kubernetes secret for cvp service access token secret "secret-service-access-token" deleted
         secret/secret-service-access-token created
      stderr: |
+ '[' 0 '!=' 1 ']'
         + TOKEN_DIR=/etc/cvpi
+ TOKEN_FILE=/etc/cvpi/access_token
         + '[' '!' -f /etc/cvpi/access_token ']'
+ '[' '!' -s /etc/cvpi/access_token ']'
         + echo 'Creating kubernetes secret for cvp service access token'
         + kubectl delete secret secret-service-access-token --ignore-not-found=true
         + kubectl create secret generic secret-service-access-token --from-file=/etc/cvpi/access_token
         + rm /etc/cvpi/access_token
         + touch /etc/cvpi/access_token
      err: null
      exitcode: 0
 root@cvp230 ~]# cvpi start sensor --is-local-action
- command: bash -c "envsubst < /cvpi/conf/kubernetes/sensor.yaml | kubectl apply -f</pre>
    cmdfunc: StartActionCmd
    component: sensor
    action: start
    node: primary
    result:
ip: ""
      stdout: ""
      stderr: ""
      err: null
      exitcode: 0
```

#### 4.5 How to check if access\_token is expired or not?

To check whether the access\_token is expired or not, examine the sensor log file /cvpi/apps/sensor/logs/sensor-sensor1.log for the below error messages:

· Wrong service account token or expired token:

```
time="2022-11-18T14:14:41+05:30" level=error msg="Unable to reach gNMI service: rpc error: code
= Unauthenticated desc = unexpected HTTP status code received from server: 401 (Unauthorized). retrying
(attempt 5)..."
```

· No device enrollment read & write permissions:

```
time="2022-11-18T14:54:07+05:30" level=error msg="Datasource stopped unexpectedly: error starting providers
for device \"45733aec-c463-412c-a301-ea6f294d9692\" (vCenter_v2): gRPC connection to device 45733aec-c463
-412c-a301-ea6f294d9692 failed: AddEnrollmentToken failed: rpc error: code = PermissionDenied desc = not
authorized" datasource=vcenter1 sensor=sensor1
```

No gNMI read & write permissions:

```
time="2022-11-18T15:01:48+05:30" level=info msg="Config subscription returned: error: rpc error: code
= PermissionDenied desc = unexpected HTTP status code received from server: 403 (Forbidden)" sensor=sensor1
time="2022-11-18T15:01:48+05:30" level=info msg="Terminating 0 datasources..." sensor=sensor1
time="2022-11-18T15:01:48+05:30" level=info msg="All datasources closed" sensor=sensor1
time="2022-11-18T15:01:48+05:30" level=fatal msg="group returned with error: rpc error: code = PermissionDen
ied desc = unexpected HTTP status code received from server: 403 (Forbidden)"
```

#### Problem Resolution:

The above errors in the log files indicate either the service account token has expired or some issue with the token. To resolve this, re-generate the service account token by following the steps in Generating a Service Account Token section.

#### 4.6 How to change the log level and verbosity of the sensor on a VM?

To change the log level and verbosity of the sensor on a VM, perform the following steps:

- 1. SSH to the VM.
- 2. Edit the file /cvpi/conf/helm/standalone-sensor/template/values.yaml.
- 3. Change the following parameters with the appropriate values: logLevel: debugverbosityLevel: 1 where,
  - logLevel: Log level verbosity (available levels: trace, debug, info, warning, error, fatal, panic. The default value is "debug").
  - verbosityLevel: Log level for V logs.
- 4. Restart the sensor component with the updated configuration:

```
cvpi stop sensor --is-local-actioncvpi config sensorcvpi start sensor --is-local-action
```

These commands stop the sensor, apply the configuration changes, and then start the sensor with the new log level and verbosity settings.

#### 4.7 Are all components on the server running fine?

Check for any error messages in the log file (as in example):

```
E0613 16:28:15.590280 39508 publisher.go:723] ae4aa295-ed2e-48b3-95fb-b5dle031f1c6Unable to send 206 messages to dataset: type:"device" name:"ae4aa295-ed2e-48b3-95fb-b5dle031f1c6" for req #1: rpc error: code = Unimplemented desc = unimplemented
```

This error indicates that one or more components on the server are down, causing an issue. To resolve the problem, check and restart the components that are not running correctly.

#### Chapter 5

#### **Troubleshooting Upgrade Issues**

This section provides information on common issues that may arise during Sensor upgrade and suggests possible solutions to address them.

#### 5.1 Where to check upgrade logs?

To check upgrade logs:

- Locate the log file named cvpUpgrade.log in the /data/upgrade.<timestamp>location.
- When an upgrade file is missing or not copied properly, an error indicating the issue is displayed.

#### Figure 5-1: Upgrade Error

uno-sensor-test login: cvpadmin Last login: Tue Jun 13 11:58:48 on tty1								
Sensor Installation Menu								
[q]uit [p]rint [i]nstall [u]pgrade >u Could not find upgrade tgz at /tmp/upgrade, exiting upgrade								

- When an upgrade is not required, the following is displayed: The upgrade will not modify any existing RPMs. All RPMs are up to date. Exiting.
- After the upgrade, if some components are in a Not Running state:

#### Figure 5-2: Post Upgrade Errors

Action Output				
COMPONENT	ACTION	NODE	STATUS	ERROR
containerd	status	primary	(E) RUNNING	
coredns	status	primary	(E) RUNNING	
descheduler	status	primary	(E) RUNNING	
etcd	status	primary	(E) RUNNING	
flannel	status	primary	(E) RUNNING	
fluent-bit	status	primary	(E) NOT RUNNING	Only 0/1 pod(s) ready
kube-apiserver	status	primary	(E) RUNNING	
kube-controller-manage	er status	primary	(E) RUNNING	
kube-proxy	status	primary	(E) RUNNING	
kube-scheduler	status	primary	(E) RUNNING	
kubelet	status	primary	(E) RUNNING	
mutating-webhook	status	primary	(E) NOT RUNNING	
mutating-webhook-serve	er status	primary	(E) NOT RUNNING	
sensor	status	primary	(E) NOT RUNNING	
zookeeper	status	primary	(E) RUNNING	

#### Resolution:

Try the following possible solutions:

- Restart the container service by using the command: systemctl restart containerd.service.
- Check if all components are running by using the command: cvpi status all -v3.

If the issue persists, proceed to the next step:

- · Re-install the sensor.
- Go to the Sensor Installation Menu and select the "[i]nstall" option.
- Follow the steps and apply the configuration without making any modifications.
- · Check if all components are running now. If the issue still persists, further debugging is required.

For more advanced troubleshooting issues or to address issues beyond these steps, contact the Arista TAC team for assistance.

#### Chapter 6

#### **General Troubleshooting Issues**

This section provides information on common issues that you may encounter with CV Sensor and suggests possible solutions.

## 6.1 Active sensor and data sources with no updates for applications in CVaaS.

If data sources are active but there are no updates on the application view page or the VM/host counters on the CVaaS side, it indicates a problem with data transmission.

To troubleshoot the sensor pod status, SSH into the VM and execute the following command:

kubectl get pods

In the output, check the "Age" column of the sensor pod.

If the sensor pod's age is over 90 days and the data source was added around that time, expired certificates might be the cause.

To resolve this issue, restart the sensor pod by executing the following commands:

```
cvpi stop sensor
cvpi start sensor
```

#### 6.2 How to check the sensor version on the sensor VM?

To obtain the sensor version, choose one of the following two options:

Option 1:

Run the following command:

rpm -qa | grep sensor

This command displays the sensor RPM package installed. Below is a sample command output:

```
[root@uno-cvplay-sensor1 ~]# rpm -qa | grep sensor
sensor-v0.1.2_35826_g3876957_2023.3.0-base_1694543478.x86_64
```

In this output, **v0.1.2\_35826\_g3876957** is the sensor version. You can verify this against the sensor version on the UI.

#### Option 2:

Run the following command to display the logs with messages such as: "Running sensor <sensor name>, version <sensor version>".

Below is a sample command uutput:

```
[root@uno-cvplay-sensor1 ~]# journalctl | grep 'Running sensor .* version' | tail -n 1
Sep 11 13:11:39 uno-cvplay-sensor1.sjc.aristanetworks.com sensor[6429]: time="2023-09-11T13:11:39Z
" level=info msg="Running sensor \"non-default\", version v0.1.4-1997-g71e49ce" file="device/
sensor.go:972" sensor=non-default
```

#### 6.3 What does Error- dial TCP i/o timeout mean?

Certificate problems are the likely cause of sensor status errors like the one shown below:

```
sensor status primary (E) NOT RUNNING Get "https://10.42.128.1:443/apis/apps/v1/daemonsets?lab elSelector=app%3Dsensor": dial tcp 10.42.128.1:443: i/o timeout
```

To troubleshoot:

- **1.** Backup the /cvpi/tls/certs directory.
- 2. Empty the /cvpi/tls/certs directory.
- 3. Run /cvpi/bin/certs-gen.sh with user cvp
- 4. Now, access the sensor installation menu with the command su cvpadmin.
- 5. Choose the [i]nstall option followed by [a]pply config.
- 6. During this process, if you see the following error:

Unable to connect to the server: dial tcp 10.42.128.1:443: i/o timeout

. . .

. . .

- 7. Terminate the installation and stop kube-apiserver with the command: systemctl stop kube-apiserver
- 8. Restart the installation using the sensor installation menu.

#### 6.4 How to collect debug logs?

Run the following commands to gather all debug logs:

[root@uno-cvplay-sensor1 ~]# cvpi debug all --no-prom

#### Or

[root@uno-cvplay-sensor1 ~]# cvpi debug all -n

Execute the following command to gather debug logs specific to a sensor component:

[root@uno-cvplay-sensor1 ~] # cvpi debug sensor --no-prom

#### Or

[root@uno-cvplay-sensor1 ~]# cvpi debug sensor -n

#### 6.5 How to change the cluster name(CV\_ADDR)?

To change the cluster name:

- **1.** SSH to the VM.
- 2. Log in using su cvpadmin.
- 3. Select the install option from the menu.
- 4. Select the edit option.
- 5. Update the CV ADDR field.
- 6. Apply the configuration.

If you change the CV\_ADDR to point to a different cluster, update the service account token as well. For details, see the How to change the access token section.

#### 6.6 What action to take when the Flow data source becomes inactive?

The flow data source on-boarded on the Sensor collects the flow records. These records are sent to the CVaaS via the Sensor VM after the Netflow details are configured in the VDS settings with the correct collector IP and port. If the VDS settings are not configured with the correct collector IP, the Flow data source will become inactive.

✓ sensor nic	3-uno-sensor.sjc.aristanetworks.com	172.30.155.252 v0.1.2-42644-g246a343	Mar 18, 2024 16:57:52	8 🛆	🖉 Edit 📋 Delete
Data Source Name	Туре т	Device	Last Seen 0	Enabled 0	
CV Autotest	VMware vCenter	5c8b6266-aace-4c9d-97da-899c06bbd05f	Mar 18, 2024 16:57:51	Yes	🖉 Edit 📋 Delete
✓ DMFDevice	DMF	DMFController_172.30.155.225	Mar 18, 2024 16:57:51	Yes	🖉 Edit 🍵 Delete
✓ dut249	SNMPv2	dut249	Mar 18, 2024 16:57:50	Yes	🖉 Edit 🍵 Delete
(i) dut373	SNMPv3	dut373	Feb 22, 2024 02:38:13	No	🖉 Edit 🍵 Delete
✓ uno-dev-vcenter7	VMware vCenter	fda4ld5c-bd4e-4554-925d-l142a3232667	Mar 18, 2024 16:57:51	Yes	🖉 Edit 🍵 Delete
O UNOFlow	Flow	UN012345	Mar 18, 2024 16:31:24	Yes	🖉 Edit 📋 Delete

To check if vCenter VDS is configured with the correct collector IP:

Login to vCenter and navigate to VDS settings > NetFlow settings.

4 0	C O Herse	tours https://uno-dev-	-vcenter7.sjc.aristanetworks.c	2177/U(/a)	pg/dvs.mevrm/uncvmc	nt/invari	Ostributed (intue Switch de	ra-63:/d	e#d5c-bd4e	-4554-6 Quitino is	- Neigdeskipsriata.com 74 days. Cansider reboot	ing.
				œн	e vCenter server upda	ten ere evol	Idole VIEW UPDATES					×
= •	vSphere Client	Q							C	Anniniarecon(IVSPH	BRLOCAL V 🛛 😡	0~
	Descritorial     Descritorial	Control and the second	UNO-DEV-DS1      survivary Meetor      settings      Properties     Topology     L/CP      Preservise     Topology     Proteins     Proteins     Topology     Proteins     Topology     Proteins     Topology     Proteins     Topology     Proteins     Topology     Proteins     Proteins     Proteins     Topology     Proteins     Topology     Proteins     Proteins	I A Configuration of the Confi	TOPS Permissions Flow etcr Perdoness ector port and/on Donain on P autoness whow report out point site constructions flows tops	Ports 172.30.16 4729 0  60 secon 15 secon 0 Disabled	Hosis VM6 Netwo	995				COT
× .	Recent Tasks	Norms										
100.000	ч т	THOM	T MUNH	٣	betalls	٣	mitiator		Summed T For	Mattine 5 T	Completion Time	Server a
Refrech	ohiPort state	Sectorwork.	Completed				VSPHERELOCALVABrinkt	nakor	tm	03/18/2024, 9:50:10 P.,	0.3/10/2024, 9:50:10 P	. uno-de
0 A	a 🐳 Mare Ta	nies								1.25 # 3	Diam K K T	/B > H

#### Figure 6-1: NetFlow Settings

The Collector IP address should match the Sensor VM IP address, and the Collector Port should be 4739. Sometimes, despite the correct collector IP address and port, the flow records don't reach the Sensor VM; that could happen if port 4739 is blocked on the Sensor VM.

#### 6.7 The Cvpi status all command do not show component status

To check the status of all components, run the cvpi status all command. When there is any issue with the system, the cvpi commands fail and displays an error message.

#### For example,

[root@uno-sensor ~]# cvpi status all Please run sudo systemctl show -p SubState chronyd to ensure the Substate is running and run cvpi check all to ensure all scopes are OK. If these are both OK, please run systemctl enable zookeeper && systemctl restart zookeeper to restart zookeeper. If zookeeper continues to fail, please contact Arista support.

When you see this error message, run the following commands and check the status:

[root@uno-sensor~]# sudo systemctl show -p SubState chronyd SubState=start-pre

If the status shows start-pre, it indicates that the chronyd service is not running, preventing the zookeeper service from starting.

To resolve this issue, first verify if the chronyd service is running. If it is not running, the configured NTP servers may be down, or their configuration might have changed. If NTP server authorization is required, the authorization settings might have been updated.

[root@uno-sensor ~]# systemctl status chronyd

Check if the NTP server is UP:

[root@dcl-uno-sensor ~]# ping ntp-server.com PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data. From 1.2.3.4 icmp\_seq=1 Destination Host Unreachable From 1.2.3.4 icmp\_seq=2 Destination Host Unreachable

In this scenario, the NTP server is unreachable. Update the NTP server settings through the sensor configuration menu. Applying the new configuration initiates the installation process with the updated NTP server and starts all necessary services.

#### 6.8 Failed to verify certificate for a vCenter data source.

If the sensor application is unable to verify the server certificates of a vCenter data source, an error message resembling "tls: failed to verify certificate" is displayed on the data source details page (see image).



This issue occurs when the vCenter server uses a certificate issued by a private/internal CA, the data source configuration does not contain the necessary CA certificates, or the **Skip certificate** verification option is false.

To mitigate this issue, for a vCenter data source:

- 1. Edit Config in the Data Source Details page.
- 2. Do one of the following:
  - a. Upload the correct CA certificate file.

(i). The CA certificates file is a single file containing the necessary certificates in PEM format. It may contain multiple certificates, i.e., all the intermediate CA certificates and the root CA certificate.

(ii). Obtain the CA certificate file from the vCenter admin or browse the vCenter server base URL.



b. Or, select Yes for the Skip Certificate Verification option.

← →	C 🕾 geiger-trunk.in	fra.corp.arista.io/cv/devices/device-onboarding?dataSourceName=fda4fd5c-bd	4e-4554-925d-f142a3232667&deviceOnboardingTab=onboardDataS 🛧 🎯 🚺 🔅 🛛
<b>æ</b>	Devices	Device Registration Onboard physical and virtual devices to CloudVision	Edit Data Source ×
Q	Inventory	Onboard Devices Data Sources Virtual Router Deployments Re	
	Device Registration		ttps://uno-dev-vcenter7.sic.aristanetworks.com
8	Compliance Overview	Data Sources > sensor > fda4fd5c-bd4e-4554-92	
Ø	Endpoint Overview	Status Name Device ID	vcenter Username administrator@vsphere.local
p	Connectivity Monitor	✓ Streaming uno-dev-vcenter7 fda4fd5c-bd4e-4554-925d-f1-	
-111	Traffic Flows	Last Seen Aug 29, 2024 11:50:47	vCenter Password     vCenter Password     Change
~~~~	Endpoint Search		Chin Castilianta Varifantian
	Comparison	Data Source Logs	Yes
	Multi-Cloud Dashboard	This data source has unspecified logging enabled.	O No
	Network Segmentation Virtual Topologies	Time Message	CA Certificates File ① Select File
	Pathfinder Devices	Aug 29, 2024 11:27:58 Inventory - vms: 47, hosts: 3, vdss: 9, vd	
		Aug 29, 2024 11:26:58 Logging is too dense. Please check in the	Drop file here
		Aug 29, 2024 11:26:58 Failed to create provider metric, Error: Er	Supported file types: .cer, .cert, .crt, .pem, .pub
		Aug 29, 2024 11:26:58 Failed to create provider metric, Error: Er	
6		@ @ ^ Aug 29, 2024 10:50:54 - Now	Configure Advanced Settings
۵		12,00 15,00 18,00 21,00	Cancel Save

3. Save and choose to onboard the device.