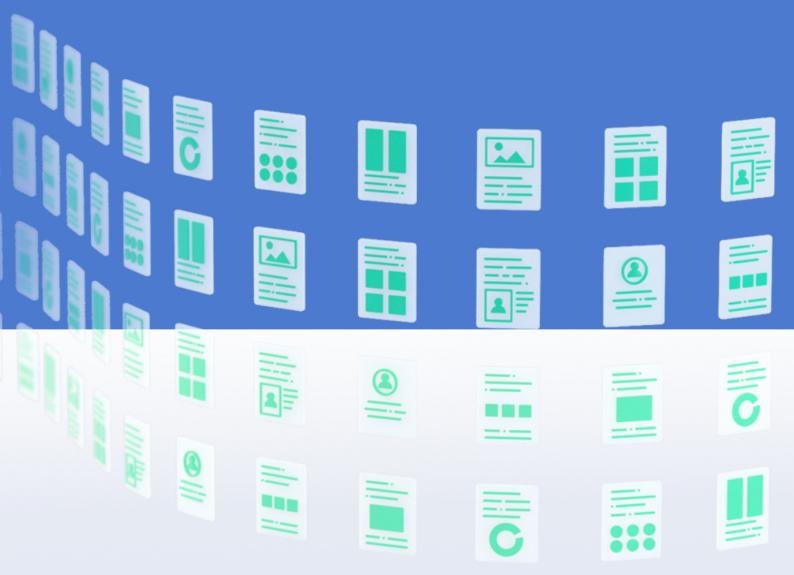
# Votiro Cloud Knowledge Base



July 2024



### **Copyright Notice**

The material herein is proprietary to Votiro CyberSec Ltd. This document is for informative purposes. Any unauthorized reproduction, use or disclosure of any part of this document is strictly prohibited.

Votiro CyberSec's name and logos are trademarks of Votiro CyberSec Ltd., its subsidiaries or affiliates. All other company or product names are the trademarks of their respective holders.

www.votiro.com

### Contents

1	Assigning a Control Plane VIP and Default VIP in AWS VA	7
	1.1 Procedure	. 7
2	Assigning a Control Plane VIP and External LB in Azure VA	. 11
	2.1 Procedure	. 11
3	Changing the CA Certificate	. 15
	3.1 Converting a CA Certificate	. 15
	3.2 Applying CA Certificate to Kubernetes Cluster	. 15
4	Email Arrival is Delayed	.16
	4.1 Symptoms	.16
	4.2 Solution	.16
	4.3 Expected result	.16
	4.3.1 Before:	. 16
	4.3.2 Action:	. 16
	4.3.3 After:	. 16
F		
	How to Check that the External Load Balancer is Working with the Votiro Cloud luster	
	-	.18
	luster	. <b>18</b> . 18
	luster5.1 Prerequisites	. <b>18</b> . 18 . 18
С	luster 5.1 Prerequisites 5.2 Procedure	. <b>18</b> . 18 . 18 . 18
С	Iuster         5.1 Prerequisites         5.2 Procedure         5.2.1 Verify the Load Balancer is Connected to the Cluster	. 18 . 18 . 18 . 18 . 20
С	Iuster         5.1 Prerequisites         5.2 Procedure         5.2.1 Verify the Load Balancer is Connected to the Cluster         How to Configure SSL Passthrough Load Balancing using NGINX	. 18 . 18 . 18 . 18 . 20 . 20
С	Iuster         5.1 Prerequisites         5.2 Procedure         5.2.1 Verify the Load Balancer is Connected to the Cluster         How to Configure SSL Passthrough Load Balancing using NGINX         6.1 Prerequisites	. 18 . 18 . 18 . 18 . 20 . 20
С	Iuster         5.1 Prerequisites         5.2 Procedure         5.2.1 Verify the Load Balancer is Connected to the Cluster         How to Configure SSL Passthrough Load Balancing using NGINX         6.1 Prerequisites         6.2 Procedure	. 18 . 18 . 18 . 18 . 20 . 20 . 20
С 6	Iuster         5.1 Prerequisites         5.2 Procedure         5.2.1 Verify the Load Balancer is Connected to the Cluster         How to Configure SSL Passthrough Load Balancing using NGINX         6.1 Prerequisites         6.2 Procedure         6.3 Next Steps	<b>18</b> 18 18 18 20 20 20 23 23
С 6	Iuster         5.1 Prerequisites         5.2 Procedure         5.2.1 Verify the Load Balancer is Connected to the Cluster         How to Configure SSL Passthrough Load Balancing using NGINX         6.1 Prerequisites         6.2 Procedure         6.3 Next Steps         6.4 NGINX File Example	<b>18</b> 18182020232325
С 6	Iuster         5.1 Prerequisites         5.2 Procedure         5.2.1 Verify the Load Balancer is Connected to the Cluster         How to Configure SSL Passthrough Load Balancing using NGINX         6.1 Prerequisites         6.2 Procedure         6.3 Next Steps         6.4 NGINX File Example         How to Configure the Votiro Appliance for AWS	<b>18</b> . 18 . 18 . 18 . 20 . 20 . 20 . 23 . 23 . 25 . 25
C 6 7	Iuster         5.1 Prerequisites         5.2 Procedure         5.2.1 Verify the Load Balancer is Connected to the Cluster         How to Configure SSL Passthrough Load Balancing using NGINX         6.1 Prerequisites         6.2 Procedure         6.3 Next Steps         6.4 NGINX File Example         How to Configure the Votiro Appliance for AWS         7.1 Prerequisites	<b>18</b> . 18 . 18 . 18 . 20 . 20 . 20 . 23 . 23 . 25 . 25 . 26
C 6 7	Iuster         5.1 Prerequisites         5.2 Procedure         5.2.1 Verify the Load Balancer is Connected to the Cluster         How to Configure SSL Passthrough Load Balancing using NGINX         6.1 Prerequisites         6.2 Procedure         6.3 Next Steps         6.4 NGINX File Example         How to Configure the Votiro Appliance for AWS         7.1 Prerequisites         7.2 Procedure	<b>18</b> . 18 . 18 . 18 . 20 . 20 . 20 . 23 . 23 . 25 . 25 . 26 <b>30</b>

8.2.1 Declare a Mount	30
8.2.2 Add External Storage Path	31
8.2.3 Restart Pods	31
8.3 Troubleshooting	31
8.3.1 Issue 1: Windows Server NFS sharing permission	31
8.3.2 Issue 2: Missing metadata in blob-config	35
9 How to Deploy the Votiro Cloud Cluster in Azure	36
9.1 Prerequisites	36
9.2 Procedure	36
10 How to Integrate Azure AD Single Sign-on with Votiro using SAML Toolkit	43
10.1 Prerequisites	43
10.2 Procedure	43
11 How to Integrate SIEM with Azure Sentinel	51
11.1 System prerequisites	51
11.2 Procedure	51
11.2.1 Manual/Offline Deployment	51
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP	
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs	63
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP	63
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs	<b>63</b> 63
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs 12.1 Procedure	<b>63</b> 63 63
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP         Logs         12.1 Procedure         12.1.1 Configure an HTTP Logs and Metrics Source in Sumo Logic	<b>63</b> 63 63
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs         12.1 Procedure         12.1.1 Configure an HTTP Logs and Metrics Source in Sumo Logic         12.1.2 Create the Field Extraction Rules at Ingest Time	<b>63</b> 63 63 65 67
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs         12.1 Procedure         12.1.1 Configure an HTTP Logs and Metrics Source in Sumo Logic         12.1.2 Create the Field Extraction Rules at Ingest Time         12.1.3 Install the Votiro App         12.1.4 Integrate the Votiro Management Console with the Sumo Logic HTTP	<ul> <li>63</li> <li>63</li> <li>63</li> <li>65</li> <li>67</li> <li>69</li> </ul>
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs         12.1 Procedure         12.1.1 Configure an HTTP Logs and Metrics Source in Sumo Logic         12.1.2 Create the Field Extraction Rules at Ingest Time         12.1.3 Install the Votiro App         12.1.4 Integrate the Votiro Management Console with the Sumo Logic HTTP Logs Collector	<ul> <li>63</li> <li>63</li> <li>65</li> <li>67</li> <li>69</li> <li>70</li> </ul>
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs         12.1 Procedure         12.1.1 Configure an HTTP Logs and Metrics Source in Sumo Logic         12.1.2 Create the Field Extraction Rules at Ingest Time         12.1.3 Install the Votiro App         12.1.4 Integrate the Votiro Management Console with the Sumo Logic HTTP Logs Collector         12.1.5 Verify the Integration	<ul> <li>63</li> <li>63</li> <li>65</li> <li>67</li> <li>69</li> <li>70</li> <li>73</li> </ul>
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs         12.1 Procedure         12.1.1 Configure an HTTP Logs and Metrics Source in Sumo Logic         12.1.2 Create the Field Extraction Rules at Ingest Time         12.1.3 Install the Votiro App         12.1.4 Integrate the Votiro Management Console with the Sumo Logic HTTP         Logs Collector         12.1.5 Verify the Integration         13 How to Integrate Votiro Cloud with Google Workspace	<ul> <li>63</li> <li>63</li> <li>65</li> <li>67</li> <li>69</li> <li>70</li> <li>73</li> </ul>
<ul> <li>12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs</li> <li>12.1 Procedure <ul> <li>12.1.1 Configure an HTTP Logs and Metrics Source in Sumo Logic</li> <li>12.1.2 Create the Field Extraction Rules at Ingest Time</li> <li>12.1.3 Install the Votiro App</li> <li>12.1.4 Integrate the Votiro Management Console with the Sumo Logic HTTP Logs Collector</li> <li>12.1.5 Verify the Integration</li> </ul> </li> <li>13 How to Integrate Votiro Cloud with Google Workspace</li> <li>13.1 Procedure</li> </ul>	<ul> <li>63</li> <li>63</li> <li>65</li> <li>67</li> <li>69</li> <li>70</li> <li>73</li> <li>74</li> </ul>
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs         12.1 Procedure         12.1.1 Configure an HTTP Logs and Metrics Source in Sumo Logic         12.1.2 Create the Field Extraction Rules at Ingest Time         12.1.3 Install the Votiro App         12.1.4 Integrate the Votiro Management Console with the Sumo Logic HTTP         Logs Collector         12.1.5 Verify the Integration         13 How to Integrate Votiro Cloud with Google Workspace         13.1 Procedure         13.1.1 Create a Host	<ul> <li>63</li> <li>63</li> <li>65</li> <li>67</li> <li>69</li> <li>70</li> <li>73</li> <li>74</li> <li>75</li> </ul>
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs         12.1 Procedure         12.1.1 Configure an HTTP Logs and Metrics Source in Sumo Logic         12.1.2 Create the Field Extraction Rules at Ingest Time         12.1.3 Install the Votiro App         12.1.4 Integrate the Votiro Management Console with the Sumo Logic HTTP         Logs Collector         12.1.5 Verify the Integration         13 How to Integrate Votiro Cloud with Google Workspace         13.1 Procedure         13.1.2 Configure content compliance rule for emails received from Votiro Cloud	<ul> <li>63</li> <li>63</li> <li>65</li> <li>67</li> <li>69</li> <li>70</li> <li>73</li> <li>74</li> <li>75</li> <li>79</li> </ul>

14.2 Procedure	. 81
14.2.1 Configure the Sumo Logic Syslog Collection	81
14.2.2 Create the Field Extraction Rules at Ingest Time	85
14.2.3 Install the Votiro App	86
14.2.4 Integrate Votiro Management Console with Sumo Logic Syslog Collector	.89
14.2.5 Search Ingested Data inside Sumo Logic	90
14.2.6 Event Simulator	91
15 Performing a Health Check	93
16 How to Send Files to Votiro via Postman	. 94
16.1 Prerequisites	. 94
16.2 Procedure	94
16.2.1 Generating a Service Token	94
16.2.2 Postman Setup	98
17 How to Sync with an NTP Server	105
17.1 Solution	105
17.2 External NTP Server	105
17.3 Internal NTP Server	105
17.4 Verify Time of Syncronization for each Node	106
18 How to Troubleshoot NTP using Chrony in VA	107
18.1 Solution	107
18.2 Troubleshooting Example: NTP not synchronized with external server	111
19 How to Upgrade Votiro Cloud	114
19.1 Upgrade Installation	114
19.1.1 Before You Begin	114
19.1.2 Procedure	.114
19.1.3 Verification of Upgrade	.115
20 How to Use Kibana to Troubleshoot Votiro Incidents	116
20.1 Example of Votiro Incident	116
20.2 Procedure	.116
20.2.1 Create and Configure an Index Pattern	.116
20.3 Analyze the Data	118

133

# 1

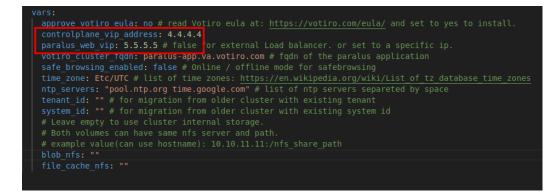
### Assigning a Control Plane VIP and Default VIP in AWS VA

This page describes the steps to configure a control plane Virtual IP (VIP) and default VIP for the Votiro Appliance (VA) when working with AWS (Amazon Web Services). This is necessary if the customer is not using an external load balancer.

**Note**: If the customer is using an external load balancer, then only one IP should be added for Control plane vip and not paralus\_web\_vip.

### 1.1 Procedure

- 1. After creating three nodes in AWS VA, add two more IPs.
- 2. They are in the inventory.yaml in Ansible:



3. Add two available IPs. You can verify the availability of the IPs by checking in the AWS EC2 console. Navigate to **Network & Security > Network Interfaces**:

Launch Templates	Network interfaces (	10) Infe				Last updated 1 minute app	C Actions V	Create network interface
Spot Requests	Q. Search					t minute ago t		< 1 > @
Savings Plans Reserved Instances	□ Name ∠ ▼	Network interface ID 🛛 🛡	Subnet ID V	VPCID	♥ Availability Zone	♥ Security group n 1	♥ Security group IDs ♥	Interface Type 🛛 🛡
Reserved Instances Dedicated Hosts		eni-0d22b9f5fa3242329	subnet-06b7738a3d6eae5dc 🖸	vpc-00a85caa051be1efb		sgr-awsclientvpn	sg-056b010c2e4c36	Elastic network interface
Capacity	0	eni-0ce9d8b6ad3275336	subnet-06b7738a3d6eae5dc	vpc-00a85caa051be1efb		sgr-awsclientvpn	sg-056b010c2e4c36	Elastic network interface
Reservations New		eni-03009168752a03ee4	subnet-06b7738a3d6eae5dc	vpc-00a85caa051be1efb		-	-	transit_gateway
Images	l-azure-devop	eni-0318630259539a83d	subnet-085d8d79d2d3da6a3	vpc-00a85caa051be1efb		sgr-check-vpn-client,	. sg-023b38b6775e9e	Elastic network interface
AMIS	0	eni-0d6d15c196c88abf1	subnet-0b05cf392b720e0a6	vpc-00a85caa051be1efb		sgr-openvpn	sg-01826b25d5ca1c	Elastic network interface
AMI Catalog	I-check-azure	eni-0e059944576dcd314	subnet-085d8d79d2d3da6a3 🔀	vpc-00a85caa051be1efb 🛃	us-east-1a	sgr-azdo-agent	sg-0973f382bdc8b1	Elastic network interface
Elastic Block Store	0	eni-06ce8b1c8c8ea23dd	subnet-0b05cf392b720e0a6 🔀	vpc-00a85caa051be1efb 🕑	us-east-1a	sgr-openvpn	sg-01826b25d5ca1c	Elastic network Interface
Volumes	0	eni-0a5a11ec0032c7e0e	subnet-0b05cf392b720e0a6 🔀	vpc-00a85caa051be1efb 🛃	us-east-1a	sgr-openvpn	sg-01826b25d5ca1c	Elastic network interface
Snapshots		eni-09dc10e3a40ad028b	subnet-085d8d79d2d3da6a3 🛃	vpc-00a85caa051be1efb 🛃	us-east-1a	sgr-bastion	sg-02616a41e4f69b	Elastic network interface
Lifecycle Manager		eni-0079bd8dd99c08b4e	subnet-085d8d79d2d3da6a3 🕑	vpc-00a85caa051be1efb 🛃	us-east-1a	-	-	transit_gateway
Network & Security	<u>×</u>							
Security Groups								
Elastic IPs								
Placement Groups								
Key Pairs								
Network Interfaces								
Load Balancing								
Load Balancing Load Balancers	nterfaces (10) Info							Last updated C
Load Balancing Load Balancers	nterfaces (10) Info							
Load Balancing Load Balancers Network in	nterfaces (10) Info	7   Status	⊽   Public IPv4 add	ress V Primar	y private IPv4 addr	zss ⊽   Secondar		2 minutes ago
Load Balancing Load Balancers Network in Q. Search V		7   Status Ø In-use	▼   Public IPv4 add 54.91.27.126	ress ♥ Primar 10.240		ess ⊽   Secondar -	2	2 minutes ago
Load Balancing Load Balancers Network in Q. Search		-			.33.50	zss ♥   Secondar - -	2	2 minutes ago
Load Balancing Load Balancers Network in Q. Search V dpoint res dpoint res	Instance ID 5	⊘ In-use	54.91.27.126	10.240	.33.50	-	2	≥ minutes ago U
Load Balancing Load Balancers Network ii Q. Search V   dpoint res	Instance ID T	⊘ In-use ⊘ In-use	54.91.27.126 34.224.112.250	10.240. 10.240.	.33.50	-	2	≥ minutes ago U U U Secondary pri – –
Lead Balancing Load Balancers Network in Q. Search ⊽ dpoint res rface for Tr	Instance ID T	<ul> <li>⊘ In-use</li> <li>⊘ In-use</li> <li>⊘ In-use</li> </ul>	54.91.27.126 34.224.112.250 -	10.240. 10.240.	.33.50 .33.149 .33.182 .32.226	-	2	≥ minutes ago U Secondary pr – –
Lead Balancing Load Balancers Network in Q. Search ⊽ dpoint res rface for Tr	Instance ID v - - - - I-Oec4659604a6b46b4	<ul> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> </ul>	54.91.27.126 34.224.112.250 - -	10.240 10.240 10.240 10.240 10.240	.33.50 .33.149 .33.182 .32.226	-	2	≥ minutes ago ⊂ Secondary pr – – – –
Load Balancing Load Balancers	Instance ID	<ul> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> </ul>	54.91.27.126 34.224.112.250 - - - 3.221.226.176	10.240 10.240 10.240 10.240 10.240 10.240	.33.50 .33.149 .33.182 .32.226 .34.20	- - - - -	2	R minutes ago ▼ Secondary pr
Load Balancing Load Balancers	Instance ID	<ul> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> </ul>	54.91.27.126 34.224.112.250 - - 3.221.226.176 -	10.240 10.240 10.240 10.240 10.240 10.240 10.240 10.240	.33.50 .33.149 .33.182 .32.226 .34.20 .32.232	- - - - -	2	R minutes ago ▼ Secondary pr  -  <
Load Balancing Load Balancers	Instance ID         N           -         -           -         -           -         -           I-Oec4659604a6b46b4         -           I-O707dd738813f66f4         -           I-O2b08e0719933e658         -           I-O3fb99223823d1044         -	<ul> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> <li>In-use</li> </ul>	54.91.27.126 34.224.112.250 - - 3.221.226.176 - 52.206.129.227	10.240 10.240 10.240 10.240 10.240 10.240 10.240 10.240 10.240	.33.50 .33.149 .33.182 .32.226 .34.20 .32.232 .34.245	- - - - - - - - - - - - - - - - - - -	2	▼ Secondary pr - - - - - - - - - - - - -
oed Balancing oad Balancers Network in Q search ⊽   Ipoint res face for Tr ork interface	Instance ID            -         -           -         -           -         -           I-Oec4659604a6b46b4         -           I-O707dd738813f66f4         -           I-O2b08e0719933e638         -           I-O3fb99223623d1044         -           I-O1db036fbe782b42c         -	<ul> <li>In-use</li> </ul>	54.91.27.126 34.224.112.250 - - 3.221.226.176 - 52.206.129.227	10.240 10.240 10.240 10.240 10.240 10.240 10.240 10.240 10.240	33.50 33.149 33.182 32.226 34.20 32.232 34.245 34.245 34.240 32.218	- - - - - - - - - - - - - - - - - - -	2	minutes ago

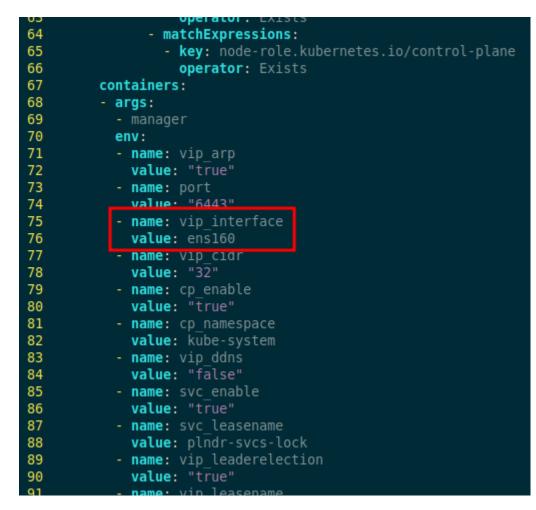
4. Assign the two IPs to the first node as follows: Go back to **Instances** and right click on one of the nodes. In the menu that opens, select **Networking**. In the submenu that opens, select **Manage IP addresses**.

✓ i-mgmt-openvpn-byol	i-03fb99223823d104 Launch instances	4	⊘ Running € ⊖ t3a.	small 📀 2/2 check
	Launch instance from templat	e		
	Migrate a server			
	Connect		=	:
i-03fb99223823d1044 (i-mgmt-openvpn-by	Stop instance			
Details Status and alarms New Monitoring	Start Instance Reboot Instance		Storage Tags	
► Instance summary Info	Hibernate Instance			
▼ Instance details Info	Terminate Instance Instance settings	•		
Platform D Linux/UNIX (Inferred)	Networking		Attach network interface	
Platform details	Security Image and templates	•	Detach network interface Connect RDS database	
	Monitor and troubleshoot	•	Change source/destination check	e8020db-5343-4c43-9e65-
Stop protection Disabled	Laun		Manage ENA Express	rael Standard Time) (over 1 year

5. The **IP addresses** window opens:

IP addresses					
Instance ID I-0e0efb314e253aea1 (shiran-test-va-1)					
To assign additional public IPv4 addresses to this instance associate them with the instance or its network interface.					
▼ eth0: eni-0f45a4bdb71d655be - 10.240.32.0/24					
IPv4 addresses					
Private IP address Public IP address					
10.240.32.64	Unassign				
10.240.32.155	Unassign				
10.240.32.156	Unassign				
Assign new IP address					
Auto-assign public IP Info					
Allow secondary private IPv4 addresses to be reassigned Allows you to reassign a private IPv4 address that is assigned to this instance to another instance or network interface.					

- 6. Add the IPs (as in the above screenshot) only on the first node.
- 7. Click the Assign new IP address button.
- 8. Change the value of **vip\_interface** in the file **/opt/votiro/package/clusterinfra/kube-vip/kube-vip.yaml** from **ens160** to the interface of your linux machine.



9. You can check the interface with this command:

ip link show

10. In the same file below the second spec line add **nodeSelector** ( with the name of your first node, as in the below example):



nodeSelector:

kubernetes.io/hostname: <my-first-node-name>

### 2 Assigning a Control Plane VIP and External LB in Azure VA

This page describes the steps to configure a control plane Virtual IP (VIP) and external LB (Load Balancer) for the Votiro Appliance (VA) when working with Azure.

#### 2.1 Procedure

#### Note

For Production environment, always use an external Load Balancer.

- 1. Assign the IP addresses to the **inventory.yaml** file:
  - Assign one IP address for **controlplane\_web\_vip**.
  - For the **Test** environment, assign a second IP address for **paralus\_web\_vip**.

15	
15 16	vars:
17	approve_votiro_eula: yes # <u>read Votir</u> o <u>eula at: htto</u> s://votiro.com/eula/ and set to yes to install.
18	controlplane_vip_address: 10.10.2.77 New IP Assign
19	paralus_web_vip: false # false for externat Load parancer. or set to a specific ip.
20	votiro_cluster_fqdn: aws-poc.prod.votiro.com # fqdn of the paralus application
21	safe_browsing_enabled: false # Online / offline mode for safebrowsing
17 18 19 20 21 22 23 24 25 26 27 28 29 30	time_zone: Etc/UTC # list of time zones: https://en.wikipedia.org/wiki/List_of_tz_database_time_zones
23	ntp_servers: "pool.ntp.org time.google.com" # list of ntp servers separeted by space
24	tenant_id: "" # for migration from older cluster with existing tenant
25	system_id: "" # for migration from older cluster with existing system id
26	# Leave empty to use cluster internal storage.
27	# Both volumes can have same nfs server and path.
28	<pre># example value(can use hostname): 10.10.11.11:/nfs_share_path</pre>
29	blob_nfs: ""
30	file_cache_nfs: ""

2. In the **IP configurations** for the VM, click + **Add**.

Risee > Wetadmachines > donas-se 2 > donas-se 2 all 11							
shiran-va-2481_z1   IP configurations * -							
₽ Search 0 ≪	O Retroli						
C Overview							
Activity log	IP Settings						
Access control (AM)	Enable IP forwarding ()						
🗢 Tags							
✓ Settings	Writual network	shiran-test					
🖬 IP configurations 🔹 🕸	Gateway load balancer ()	None			$\sim$		
CMS servers	Subnet ()	default (10.0.0.0/24) 238 free IP addresses			~ ]		
Network security group	STORE OF			238	free IP addresses		
1 Properties	River and a data in address on the second		we when some software software so		a the first statement of second	ary to a network interface, within the limits listed in the Azure limits article. Learn more (?	
🔒 Locks	misee and public in addresses can be as	signed to a virtual machine's network ellenace controls	er. You can alde as	many private and	public investorements an informa-	ey to a network interact, within the limits inter in the Aptre limits article, users more of	
> Monitoring	+ Add   Multi primary   Delete						
> Automation							
> Help	Name		IP Version	Туре	Private IP Address	Public IP Address	
	ipcomfg1		(Pvi	Primary	10.0.0.12 (Dynamic)	20.86.151.216 (shiran-va-2-ip)	

3. In the Add IP configuration window, leave the Associate public IP address box unchecked. and click on Add.

	ady exists. Any additional IP configurations will be second k interface is attached to only supports IPv4. <u>Learn mor</u>
Name	control-plane-vip
IP version	IPv4
	O IPv6
Туре	O Primary
	Secondary
Private IP address settings	
Allocation	O Dynamic
	Static
Private IP address	10.0.25
Public IP address settings	
Associate public IP address	

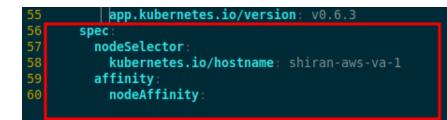


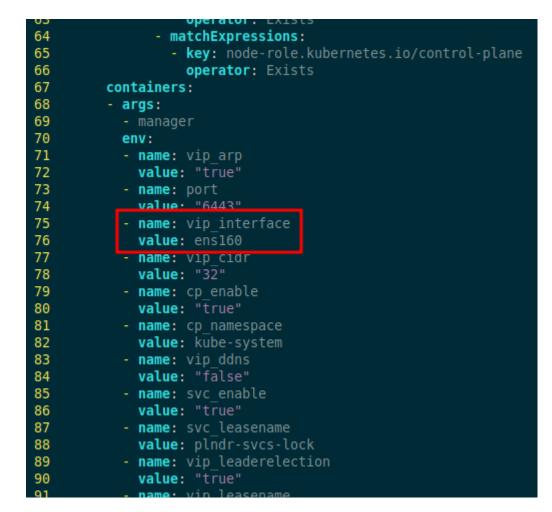
4. Assign your new IP to the first node in this section:

6 vars:	
.7 approve votiro eula: yes # read Votico eula at: https://votiro.com/eula/ and set to yes to install.	
.8 controlplane_vip_address: 10.10.2.77 New IP Assign	
.8 controlplane_vip_addréss: 10.10.2.77 New IP Assign .9 paralus_web_vip: false # false for external Load parancer. or set to a specific ip.	
<pre>votiro_cluster_fqdn: aws-poc.prod.votiro.com # fqdn of the paralus application</pre>	
1 safe_browsing_enabled: false # Online / offline mode for safebrowsing	
votiro_cluster_fqdn: aws-poc.prod.votiro.com # fqdn of the paralus application safe_browsing_enabled: false # Online / offline mode for safebrowsing time_zone: Etc/UTC # list of time zones: https://en.wikipedia.org/wiki/List_of_tz_database_time_zone ntp_servers: "pool.ntp.org time.google.com" # list of ntp servers separeted by space tenant_id: "" # for migration from older cluster with existing tenant system_id: "" # for migration from older cluster with existing system id # Leave empty to use cluster internal storage.	es
13 ntp_servers: "pool.ntp.org time.google.com" # list of ntp servers separeted by space	
4 tenant_id: "" # for migration from older cluster with existing tenant	
Is system_id: "" # for migration from older cluster with existing system id	
# Leave empty to use cluster internal storage.	
7 # Both volumes can have same nfs server and path.	
7 # Both volumes can have same nfs server and path. 8 # example value(can use hostname): 10.10.11.11:/nfs_share_path 9 blob_nfs: "" 6 file_cache_nfs: ""	
9 blob_nfs: ""	
0 file_cache_nfs: ""	
	_

- 5. In the file **/opt/votiro/package/cluster-infra/kube-vip/kube-vip.yaml**:
  - a. Edit the value for **vip\_interface** (line 77) and replace with your own NIC name (i.e, eth0).
  - b. Add specification for **nodeSelector** (below raw line 55).
  - c. Edit **kubernetes.io/hostname** and replace with your node name (i.e, node-1):

```
1 56 spec:
2 nodeSelector:
3 kubernetes.io/hostname: node-1
4 affinity:
5 nodeAffinity:
6 61
```





6. You can check the interface with this command:

ip link show

Do this for all nodes. You can copy this file to the other nodes using the **scp** command.

7. Save and run the book.

### **3** Changing the CA Certificate

CA Certificates are used as the HTTPS security layer to secure communications across computer networks when using applications.

The domain name of your Votiro Votiro Cloud appliance is used in the CA Certificate, binding the address to the certificate, enabling a secure connection. An example of an appliance address is *https://sfg-va.domain.com*.

The CA Certificate used with your Votiro Votiro Cloud appliance must be a *.pem* and *.key* pair. You can convert the format of your CA Certificate using SSL Certificate software, for example <u>OpenSSL</u>.

#### 3.1 Converting a CA Certificate

To convert a CA Certificate in *.pfx* format with password *Pa\$\$w0rd* to a *.pem* and *.key* pair, use the following <u>OpenSSL</u> commands:

- openssl pkcs12 -in /<path-to-certificate>/certificate.pfx out /<path-to-certificate>/certificate.pem -nodes -passin
  pass:<Pa\$\$w0rd>
- openssl pkey -in /<path-to-certificate>/certificate.pem -out
  /<path-to-certificate>/certificate.key

#### 3.2 Applying CA Certificate to Kubernetes Cluster

To apply the *.pem* and *.key* files to your Kubernetes cluster, use the following sets of commands to first *delete*, then *create*, a new certificate in the two namespaces *traefik* and *votiro*:

- kubectl delete secret traefik-cert -n traefik
- kubectl create secret tls traefik-cert --key=/<path-tocertificate>/certificate.key --cert=/<path-tocertificate>/certificate.pem -n traefik
- kubectl delete secret traefik-cert -n votiro
- kubectl create secret tls traefik-cert --key=/<path-tocertificate>/certificate.key --cert=/<path-tocertificate>/certificate.pem -n votiro

### 4 Email Arrival is Delayed

This page details why the arrival of emails may be delayed and remediation actions to solve this issue.

#### 4.1 Symptoms

- Mails arrive late in days delayed arrival
- No errors in Votiro logs
- No specific high resource consumption

#### 4.2 Solution

This situation might be related to Message throttling.

Get information of the Edge Connector:

Get-ReceiveConnector | Format-List
Name,Connection\*,MaxInbound\*,MessageRate\*,TarpitInterval

#### 4.3 Expected result

#### 4.3.1 Before:

Name : Default Connector Name

ConnectionTimeout : 00:05:00

ConnectionInactivityTimeout : 00:01:00

MaxInboundConnection : 5000

MaxInboundConnectionPerSource : 20

MaxInboundConnectionPercentagePerSource : 2

MessageRateLimit: 600

MessageRateSource : IPAddress

TarpitInterval: 00:00:05

>The configuration allows maximum of 20 simultaneous connections from a single IP.

#### 4.3.2 Action:

Change the parameters using syntax:

```
Set-ReceiveConnector -Identity <Put the Identity name> -
ConnectionTimeout 00:10:00)
```

#### 4.3.3 After:

Name: Default Connector Name

ConnectionTimeout: 00:10:00

ConnectionInactivityTimeout: 00:01:00

MaxInboundConnection: 5000

MaxInboundConnectionPerSource: 50

MaxInboundConnectionPercentagePerSource: 5

MessageRateLimit: 600

MessageRateSource: IPAddress

TarpitInterval: 00:00:05

### 5

### How to Check that the External Load Balancer is Working with the Votiro Cloud Cluster

Many organizations are using an external load balancer to load balance internet traffic to the virtual machines, rather than depend on built-in application load balancing. Using an external load balancer is considered more reliable than using an application's internal load balancer.

This page describes how to check that the Votiro Cloud cluster is working with an external load balancer.

### 5.1 Prerequisites

Before you start, ensure the NGINX load balance server is configured. For instructions how to configure a NGINX load balancer for use with Votiro Cloud, see <u>How to Configure SSL</u> Passthrough Load Balancing using NGINX.htm.

#### 5.2 Procedure

This procedure includes instructions and verification checks to ensure that the NGINX load balancer is providing the load balancing service to Votiro Cloud, instead of using the application's internal load balancing function.

#### 5.2.1 Verify the Load Balancer is Connected to the Cluster

- 1. Logon to the **NGINX** server.
- 2. On each node, use the following command:

curl https://10.130.1.30:30443 --insecure -vv



The result will contain the message **404 page not found**:

<pre>[root@centos-nginx-king nginx]# curl https://10.130.1.30</pre>	:30443insecure -vv
* About to connect() to 10.130.1.30 port 30443 (#0)	votiro
* Trying 10.130.1.30	
* Connected to 10.130.1.30 (10.130.1.30) port 30443 (#0)	
* Initializing NSS with certpath: sql:/etc/pki/nssdb	
* skipping SSL peer certificate verification	
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SH	A256
* Server certificate:	
<pre>* subject: CN=TRAEFIK DEFAULT CERT</pre>	1 Rup the command
<pre>* start date: Jul 07 12:55:05 2020 GMT</pre>	r. Run the community
* expire date: Jul 07 12:55:05 2021 GMT	
* common name: TRAEFIK DEFAULT CERT	1 curl https://
<pre>* issuer: CN=TRAEFIK DEFAULT CERT</pre>	
> GET / HTTP/1.1	
> User-Agent: curl/7.29.0	The result will be 404
> Host: 10.130.1.30:30443	
> Accept: */*	
>	6
< HTTP/1.1 404 Not Found	
< Content-Type: text/plain; charset=utf-8	
< X-Content-Type-Options: nosniff	
< Date: Wed, 08 Jul 2020 05:42:16 GMT	Related articles
< Content-Length: 19	Related al fieles
<	
404 page not found	The content by label fe
* Connection #0 to host 10.130.1.30 left intact	ontions for this feature
[root@centos-nginx-king nginx]#	

#### 3. Run the command with the cluster name:

curl https://king-va:443 --insecure -vv

The result will appear as follows:

<pre>[root@centos-nginx-king nginx]# curl https://king-va:443insecure -vv</pre>		
* About to connect() to king-va port 443 (#0)		
* Trying 10.130.1.37. Kubernetes. Q. Qverview - Kubernet. S. Traefik C		
* Connected to king-va (10.130.1.37) port 443 (#0)		
* Initializing NSS with certpath: sql:/etc/pki/nssdb		
* skipping SSL peer certificate verification		
* SSL connection using TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256		
* Server certificate:		
* subject: CN=king-va		
* start date: Jul 07 12:54:59 2020 GMT		
<pre>* expire date: Jul 05 12:54:59 2030 GMT</pre>		
* common_name: king-vausage data helps us manage and improve our products		
* issuer: CN=king-va		
> GET / HTTP/1.1		
> User-Agent: curl/7.29.0		
> Host: king-va		
> Accept: */*		
< HTTP/1.1 200_OKesearch		
< Accept-Ranges: bytes		
< Cache-Control: private, no-cache, no-store, must-revalidate, pre-check=0, pos	t-check=0, max-age=0, s-maxage=0	
< Content-Length: 529		
< Content-Security-Policy: default-src 'self';style-src 'self' 'unsafe-inline';		
< Content-Type: text/html		
< Date: Wed, 08 Jul 2020 05:43:26 GMT		
< Etag: "5ee8bb8b-211"		
< Last-Modified: Tue, 16 Jun 2020 12:31:07 GMT		
< Pragma: no-cache		
< Server: Votiroshot and Restore		
< Strict-Transport-Security: max-age=315360000; includeSubDomains; preload		
< X-Content-Type-Options: nosniff		
< X-Frame-Options: denyAssistant		
< X-Xss-Protection: 1; mode=block		
html		
<html lang="en"></html>		
<head></head>		
<meta charset="utf-8"/>		
<title>Votiro Management</title>		
<pre><base href="/"/></pre>		
(make name "vieweet" content "vidth device vidth initial1 d"		
<pre><meta content="width=device-width, initial-scale=1" name="viewport"/>   <link href="assets/images/favicon.ico" rel="icon" type="image/x-icon"/></pre>		
<pre><link href="assets/images/tavicon.ico" rel="icon" type="image/x-icon"/> <link href="styles.css" rel="stylesheet"/></pre>		
<body></body>		
<pre><app-root></app-root> </pre>		
<pre><script src="runtime.js" type="text/javascript"></script><script polyfills.js"="" type="text/java&lt;/pre&gt;&lt;/th&gt;&lt;th&gt;vascript src="></script><sc< th=""><th>ript type="text/javascript"</th></sc<></pre>	ript type="text/javascript"	
<pre><script src="runtime.js" type="text/javascript"></script></pre>		

### 6

### How to Configure SSL Passthrough Load Balancing using NGINX

Many organizations are using an external load balancer to load balance internet traffic to the virtual machines, rather than depend on built-in application load balancing. Using an external load balancer is considered more reliable than using an application's load balancer.

This page describes how to configure an SSL-passthrough load balancer using NGINX.

#### 6.1 **Prerequisites**

Before you start, ensure the following:

- CentOS 7 is installed on the Virtual Machine.
- A unique hostname and IP address are set for the Virtual Machine.

#### IMPORTANT!

The IP address set must be static.

#### 6.2 Procedure

To set and configure an external load balancer, follow these steps:

- 1. SSH to the VM.
- 2. Install **epel-release**, using the following command:

sudo yum install epel-release

- Install NGINX, using the following command: sudo yum install nginx
- 4. Enable **NGINX**, using the following command:

sudo systemctl enable nginx

5. Start **NGINX**, using the following command:

sudo systemctl start nginx

6. Verify **NGINX** is running, using the following command:

systemctl status nginx

7. Disable the built-in firewall, using the following commands:

systemctl stop firewalld

systemctl disable firewalld

8. In the **nginx.conf** file, add an **include** statement to the **passthrough.conf** file, using the following commands:

vi /etc/nginx/nginx.conf

Add the following code at the end of the file:

include /etc/nginx/passthrough.conf;

#### Note

The **passthrough.conf** file will be created in the following Step.

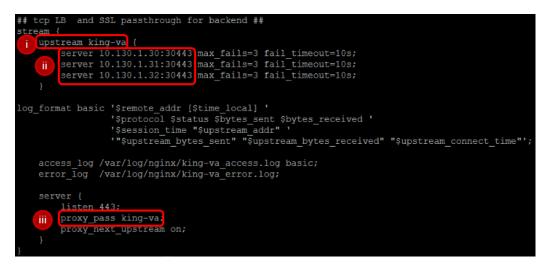
For an example of an NGINX.config, see NGINX\_File\_Example.

- 9. To create and edit the **passthrough.conf** file, and add node details to your cluster, follow these steps:
  - a. Navigate to **/etc/nginx**.
  - b. To create and edit the **passthrough.conf** file, use the following command:

vi /etc/nginx/passthrough.conf

- c. Paste the following code and edit details relevant to your environment:
  - i. Change the upstream name of your cluster. In this example **votirosfgva** is used.
  - ii. Change the IPs to the actual node IPs.
  - iii. Change the proxy\_pass to the cluster hostname (line 19). In this example **votirosfgva** is used.

```
## tcp LB and SSL passthrough for backend ##
1
2
    stream {
3
        upstream votirosfgva {
            server 10.130.1.30:30443 max_fails=3 fail_timeout=10s;
4
5
            server 10.130.1.31:30443 max_fails=3 fail_timeout=10s;
6
            server 10.130.1.32:30443 max fails=3 fail timeout=10s;
7
        }
8
9
    log_format basic '$remote_addr [$time_local] '
10
                      '$protocol $status $bytes_sent $bytes_received '
11
                      '$session_time "$upstream_addr"
12
                      '"$upstream_bytes_sent" "$upstream_bytes_received"
    "$upstream_connect_time"';
13
14
        access_log /var/log/nginx/votirosfgva_access.log basic;
        error_log /var/log/nginx/votirosfgva_error.log;
15
16
17
        server {
            listen 443;
18
19
            proxy_pass votirosfgva;
20
            proxy_next_upstream on;
21
        }
22
    }
```



10. Verify that your syntax has no errors, using the following command:

nginx -t

You should see the following output:

```
nginx: the configuration file /etc/nginx/nginx.conf syntax
is ok
```

nginx: configuration file /etc/nginx/nginx.conf test is successful

11. Reload NGINX configurations, using the following command:

systemctl reload nginx

12. Add the cluster FQDN to the host file (on a real environment it is not mandatory as they use an actual DNS server), using the following command:

vi /etc/hosts

Add the cluster FQDN and NGINX server IP:

10.130.1.34 <cluster name>

- 13. To pass the traffic to the nodes over 30443, follow these steps:
  - a. Download and install audit2allow:

sudo yum install setroubleshoot

b. Enable it:

```
cat /var/log/audit/audit.log | grep nginx | grep denied |
audit2allow -M mynginx
```

c. Execute the policy

semodule -i mynginx.pp

14. Verify that you are able to reach the nodes, using the following command:

curl https://10.130.1.30:30443 --insecure -vv

#### 6.3 Next Steps

To connect the Paralus cluster to this external load balancer, see the following guide: <u>How</u> to Check that the External Load Balancer is Working with the Votiro Cloud Cluster.

#### 6.4 NGINX File Example

The following code is an example of an NGINX File.

```
# For more information on configuration, see:
 1
 2
        * Official English Documentation: http://nginx.org/en/docs/
    #
         * Official Russian Documentation: http://nginx.org/ru/docs/
 3
    #
 4
 5
    user nginx;
 6
    worker_processes auto;
 7
    error_log /var/log/nginx/error.log;
 8
    pid /run/nginx.pid;
 9
    # Load dynamic modules. See /usr/share/doc/nginx/README.dynamic.
10
11
    include /usr/share/nginx/modules/*.conf;
12
13
    events {
14
         worker_connections 1024;
15
    }
16
17
    http {
        log_format main
                          '$remote_addr - $remote_user [$time_local]
18
     "$request" '
19
                           '$status $body_bytes_sent "$http_referer" '
                           '"$http_user_agent" "$http_x_forwarded_for"';
20
21
22
        access_log /var/log/nginx/access.log main;
23
24
         sendfile
                             on;
25
                             on;
         tcp_nopush
26
         tcp nodelay
                             on;
27
         keepalive_timeout
                             65;
28
         types_hash_max_size 2048;
29
30
         include
                             /etc/nginx/mime.types;
31
         default_type
                             application/octet-stream;
32
33
         # Load modular configuration files from the /etc/nginx/conf.d
     directory.
        # See http://nginx.org/en/docs/ngx_core_module.html#include
34
35
        # for more information.
36
        include /etc/nginx/conf.d/*.conf;
37
38
         server {
39
            listen
                          80 default server;
40
             #listen
                           [::]:80 default_server;
41
             server_name
                          _;
42
                          /usr/share/nginx/html;
             root
43
44
             # Load configuration files for the default server block.
45
             include /etc/nginx/default.d/*.conf;
```

```
46
47
            location / {
48
            }
49
50
            error_page 404 /404.html;
51
                location = /40x.html {
52
            }
53
54
            error_page 500 502 503 504 /50x.html;
55
                location = /50x.html {
56
            }
57
        }
58
59
60
61
    # Settings for a TLS enabled server.
62
    #
63
    #
         server {
64
    #
             listen
                           443 ssl http2 default_server;
65
    #
             listen
                           [::]:443 ssl http2 default_server;
66
    #
             server_name
                          ;
67
    #
             root
                           /usr/share/nginx/html;
68
    #
69
    #
             ssl_certificate "/etc/pki/nginx/server.crt";
             ssl_certificate_key "/etc/pki/nginx/private/server.key";
70
    #
71
    #
             ssl_session_cache shared:SSL:1m;
72
    #
             ssl_session_timeout 10m;
73
    #
             ssl ciphers HIGH:!aNULL:!MD5;
74
    #
             ssl_prefer_server_ciphers on;
75
    #
76
    #
             # Load configuration files for the default server block.
77
    #
             include /etc/nginx/default.d/*.conf;
78
    #
79
    #
             location / {
80
    #
             }
81
    #
82
    #
             error_page 404 /404.html;
83
    #
                 location = /40x.html {
84
    #
             }
85
    #
86
    #
             error_page 500 502 503 504 /50x.html;
87
    #
                 location = /50x.html {
88
    #
              }
89
    #
         }
90
91
92
    include /etc/nginx/passthrough.conf;
```

# 7

# How to Configure the Votiro Appliance for AWS

This page describes how to configure Votiro Cloud to work with AWS (Amazon Web Services).

To install Votiro Cloud quickly into your organization, we will create a cluster of three virtual machine instances. We will use three static IPs, one for each of the three VMs.

#### 7.1 Prerequisites

- 3 reserved IPs with DNS names. Name one DNS name of the VIP, and the rest for the VA (Votiro Appliance) nodes - a total of 5 IP addresses.
- **3** VMs, each of which has the following recommended hardware:
  - 8 CPUs
  - 32 GB RAM
  - 200 GB SSD

For these specs, an m5.2xlarge EC2 instance will be used.

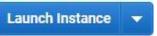
- (Optional) EFS (Amazon Elastic File System) share that will be used for file archiving. This is not required for the initial install.
- A shared AMI (Amazon Machine Image)
- AWS load balancer a load balancer is required. The following is an example of a possible load balancer configuration. For more information on configuring an AWS load balancer, see Create a Network Load Balancer:
  - a. Configure the target group with basic configuration:
    - Target type Instances
    - Protocol TLS
    - Port 30443
    - Protocol version HTTP/1.1
  - b. Configure health checks:
    - Protocol TCP
  - c. Register targets:
    - Ports for the selected instances 30443
  - d. Configure the load balancer: Create Network Load Balancer
    - Basic configuration
    - Scheme Internal
    - Listeners and routing:

- Protocol TLS
- Port 443

**Note**: You must contact Votiro support and provide your AWS account number and AWS region.

#### 7.2 Procedure

- 1. Open the Amazon EC2 (Elastic Compute Cloud) console at Amazon EC2 Console.
- 2. In the navigation bar at the top of the screen, select a Region for the instance that meets your needs. This choice is important because some Amazon EC2 resources can be shared between Regions, while others can't.
- 3. From the Amazon EC2 console dashboard, click on Launch instance.



4. On the Choose AMI (Amazon Machine Image) page, click on **My AMIs**.

My AMIs

5. Under Ownership select Shared with me.



6. Select the Votiro Appliance.



- 7. On the Choose an Instance Type page, select the M5 instance type **m5.2xlarge** or a larger instance.
- 8. On the Configure Instance Details page:
  - a. Deploy one instance at a time (Number of instances = 1).
  - b. Choose between an existing **Network** or **Create new VPC**.
- 9. If you selected **Create new VPC**:
  - a. Go to your newly created VPC and click in VPC ID
  - b. On the upper right side click Actions and choose Edit CIDRs.

- c. Add a new IPv4 CIDR, e.g. "172.16.1.0/24".
- d. Click save and "172.16.2.0/24".
- e. Click save and close.
- 10. For **Subnet**, select between an existing one or **Create new subnet**.
  - If you chose to create a new Subnet, provide it with a name, e.g., "Votirosubnet-172.16.1.0/24-1b". For the IPv4 CIDR block, provide the subnet, e.g., "172.16.1.0/24".
  - Note: for HA purposes you may proceed with creating additional subnets on different Availability Zones:
    - i. Create an internet gateway setting for the subnet.
    - ii. Provide with a name, e.g., "Votiro-IGW" and create an internet gateway.
    - iii. Select the newly created internet gateway, click Actions and Attach to VPC.
    - iv. Select your desired Route Tables, click edit routes.
    - v. Click Add route.
    - vi. Choose 0.0.0.0/0 and select Internet Gateway from the drop down.
    - vii. Save changes.

#### 11. Enable Auto-assign Public IP.

Number of instances	(j)	1 Launch into Auto Scali	ng Gr	roup (j)
Purchasing option	(j)	Request Spot instances		
Network	()	vpc-08a4b2f73790f2d45   VOTIRO-VPC	C	Create new VPC
Subnet	()	subnet-0c0f082bb832e8ef0   Votiro-subnet-10.10.0.0/2 247 IP Addresses available		Create new subnet
Auto-assign Public IP	(j)	Enable		

12. Define a static IP for each node according to the Network **Subnet** defined above.

<ul> <li>Network</li> </ul>	vork interfaces 🕕				
Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface $\checkmark$	subnet-0c0f082bl ~	10.10.0.40	Add IP	Add IP

- 13. On the Add Storage page, leave storage as is. Select **Delete on Termination**.
- 14. On the Add Tags page, add a Name value tag and name it according to your server naming convention.

Key	(128 characters maximum)	Value	(256 characters maximum)	Instances (j)	Volumes (j)	
Name	3	Votiro	NI			8

- 15. On the Configure Security Group page, define a specific Votiro Security group. Make sure you can ssh into any of the nodes. This will be required to complete the setup. The AWS Votiro Security Group should have the following access:
  - Port 443 TCP to and from the VIP of the appliance on 30443. This port is used for web access to Votiro.
  - Each Appliance should be able to communicate on the following ports that are required inside the VLAN between each appliance:
    - 6443/tcp
    - 2379-2380/tcp
    - 10250-10252/tcp
    - 22/tcp
    - 10255/tcp
    - 8472/udp
    - 24007 24008/tcp
    - 49152 49154/tcp

sg-0c96fb62a7d4c4373	Votiro_Applainces	Firewall for votiro applainces	
All TCP	TCP	0 - 65535	10.000
Custom TCP Rule	TCP	6443	Use your own subnets here
Custom TCP Rule	TCP	2379 - 2380	To make the second s
Custom TCP Rule	TCP	2379 - 2380	1.1.1.1.1
Custom TCP Rule	TCP	2379 - 2380	The rest of the re
SSH	TCP	22	10.00.000
SSH	TCP	22	to the same
SSH	TCP	22	10.0000
SSH	TCP	22	100.00 (0.000)
Custom TCP Rule	TCP	50443	termination of the second s
Custom TCP Rule	TCP	10255	10.0000
Custom TCP Rule	TCP	10255	10.00.000
Custom TCP Rule	TCP	10255	10.000
Custom TCP Rule	TCP	30443	100.00 (0.000)
Custom TCP Rule	TCP	8472	10.0000
Custom TCP Rule	TCP	8472	10.00.000
Custom TCP Rule	TCP	8472	10.000
All UDP	UDP	0-65535	10.0000
Custom TCP Rule	TCP	10250 - 10252	to the second se
Custom TCP Rule	TCP	10250 - 10252	10.00.000
custom TCP Rule	TCP	10250 - 10252	

- 16. Proceed without a keypair. The password and ssh keys are already defined on the appliance. The user name is root. To retrieve the password, contact the Votiro support team.
- 17. On the Review page, verify your configuration and then launch the three instances.
- 18. Use Putty or another client to ssh into each node.
- 19. Run the following command in the command line: **NMTUI**.



20. Select Set system hostname.

NetworkManager TUI Please select an option Set Hostname U Hostname VN-1.nyrich.com
<cancel> <ok></ok></cancel>

- 21. Use the FQDN tied to the internal IP in the earlier step. Each node should have its own DNS entry. For example, vn-1.yourdomain.com, vn-2.yourdomain.com, and vn-3.yourdomain.com. These DNS names should be registered in your internal DNS.
- 22. Verify that you have internet connectivity by running the following command:

#### ping google.com.

You should see a response similar to the screenshot below:

PING www.											
	from	sin04s02	-in-f20.	le100.	net	(173.	194.3	3.180):	icmp_seq=1	tt1=53	time
=117 ms											
64 bytes	from	sin04s02	-in-f20.	1e100.	net	(173.	194.3	3.180):	icmp_seq=2	ttl=53	time
=118 ms											
64 bytes	from	sin04s02	-in-f20.	1e100.	net	(173.	194.3	8.180):	icmp seg=3	tt1=53	time
=111 ms											
64 hutes	from	sinA4sA2	-in-f28	1e100.	net	(173.	194.3	8.180):	icmp_seq=4	tt1=53	time
=121 ms											

23. After successfully configuring the instances, contact Votiro presales before you cluster all three nodes.

8

### How to Configure the Votiro Cloud Cluster with External Storage

Many organizations are using external storage with the virtual appliance alone, to increase capabilities and support high request loads without increase virtual machine size. This is because files are backed-up to external storage instead of remaining within the virtual appliance.

This page describes how to configure Votiro Cloud cluster to work with external storage.

#### 8.1 Prerequisites

Before you start, ensure that any external storage server:

- Is reachable from your virtual appliance.
- Read / Write permissions are granted to user **1000** for the relevant path.

#### 8.2 Procedure

This procedure includes instructions and verification checks to ensure that your virtual appliance is configured to work with your external storage.

#### Note

When using external storage, the customer is responsible for file retention and deletion. Files won't be deleted according to files history retention and will be kept forever or until they are deleted manually.

#### 8.2.1 Declare a Mount

To declare a mount in all of the cluster's nodes, follow these steps:

1. Add folder /data/externalfs/nfsshare, using the following command:

mkdir -p /data/externalfs/nfsshare

2. Change the owner of folder /data/externalfs/nfsshare to user **1000**, using the following command:

chown 1000:1000 /data/externalfs/nfsshare

3. Set Read / Write permissions on folder /data/externalfs/nfsshare, using the following command:

chmod -R 755 /data/externalfs/nfsshare

- 4. In this step you will add a mount to the folder /data/externalfs/nfsshare.
  - a. Create mount, using the following command:

mount -t nfs SERVER\_IP:NFS\_EXPORT\_FOLDER
/data/externalfs/nfsshare

b. Add mount to **/etc/fstab**, using the following command:

SERVER\_IP:NFS\_EXPORT\_FOLDER /data/externalfs/nfsshare nfs
defaults 0 0

Replace the place holders above as follows:

- SERVER\_IP with the IP address, for example 10.130.1.97.
- **NFS\_EXPORT\_FOLDER** with the path to the external server.

For example:

mount -t nfs 10.130.1.97:/data/nfsshare
/data/externalfs/nfsshare

#### 8.2.2 Add External Storage Path

To add an external storage path to the configuration, follow these steps:

- 1. Edit blob-config.
- 2. Set the value of externalStorageRootPath to "/externalblobs/nfsshare".

#### 8.2.3 Restart Pods

1. Restart mng-service-blob, using the following command:

kubectl delete pod -l app=mng-service-blob -n votiro

2. Restart mng-blob-storage-manager, using the following command:

```
kubectl delete pod -l app=mng-blob-storage-manager -n votiro
```

#### Note

It may take up to 10 minutes for the file storage location to switch to the external configuration.

#### 8.3 Troubleshooting

This section contains troubleshooting steps to take when encountering problems configuring external NFS storage.

#### 8.3.1 Issue 1: Windows Server NFS sharing permission

#### Symptoms

After mounting the NFS share, when you list the **/data/externalfs** directory, the permissions are assigned to **nobody**.

```
[root@sfg ~]# mount -t nfs 10.10.10.50:/nfsshare
/data/externalfs/nfsshare
[root@sfg ~]# ls -l /data/externalfs
total 1
drwxr-xr-x. 2 nobody nobody 64 May 12 10:47 nfsshare
```

Even if you try to force change the owner and group using **chown 1000:1000**, you will get the following error:

```
[root@sfg ~] # chown 1000:1000 -R /data/externalfs
```

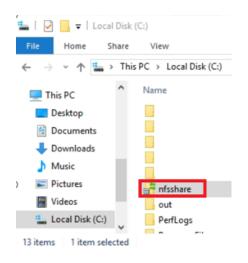
```
chown: changing ownership of `/data/externalfs/nfsshare':
Permission denied
```

#### Solution

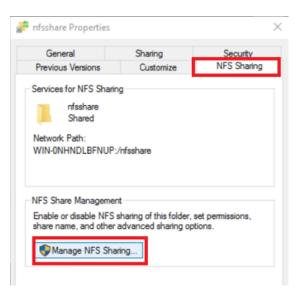
If you are using Windows Server as NFS, please follow this link to configure your Windows Server as a NFS server: <u>Deploy Network File System</u>

After configuring your Windows Server as a NFS server, follow these steps to allow root access on the shared folder:

1. Right click on the **nfsshare** folder on your Windows Server and select **Properties**:



2. Select the NFS Sharing tab, and then select Manage NFS Sharing...:



3. In the **NFS Advanced Sharing** window that opens, check the box **Share this folder** and leave the rest of the options as is. Then select **Permissions**.

NFS Advanced Sharing
✓ Share this folder
Settings
Share name: nfsshare
Network name: WIN-8UUSB9ASD3H 💌
Encoding: ANSI
Kerberos v5 privacy and authentication [Krb5p]
Kerberos v5 integrity and authentication [Krb5i]
Kerberos v5 authentication [Krb5]
✓ No server authentication [Auth_SYS]
Enable unmapped user access
<ul> <li>Allow unmapped user Unix access (by UID/GID)</li> </ul>
C Allow anonymous access
Anonymous UID; -2
Anonymous GID; -2
To set permissions for how users access this folder over the network, click Permissions
OK Cancel Apply

4. In the **NFS Share Permissions** window, check the box **Allow root access**. Then click on **OK** to save the configuration.

NFS Share Permiss	sions				?	$\times$
NFS Share Path: Name:	C:\nfsshare					
ALL MACHINES	Read-Write	AN:	SI	Root Acc	ess Allow	red
				Add	Ren	nove
Type of access:	Read-Write	•	~	Allow root acce	SS	
Encoding:	ANSI	•			Add	ł
				OK	Car	ncel

5. Restart the **Server for NFS** service for the changes to take effect.

Services (Local)		
Server for NFS	Name	Description
	Secondary Logon	Enables starting pro.
<u>Stop</u> the service <u>Restart</u> the service	Secure Socket Tunneling Pr	Provides support for
<u>Restart</u> the service	Security Accounts Manager	The startup of this s.
	🌼 Sensor Data Service	Delivers data from a
Description: Enables a Windows based computer to act as an NFS Server	🌼 Sensor Monitoring Service	Monitors various se
	🏟 Sensor Service	A service for sensors.
to act as an INI'S Server	🖏 Server	Supports file, print,
	Server for NFS	Enables a Windows

6. Run the **chown 1000:1000** command again on SFG to verify that the user permission can be changed successfully:

```
[root@sfg ~]# chown 1000:1000 -R /data/externalfs
[root@sfg ~]# ls -l /data/externalfs/
total 1
drwxr-xr-x. 3 sgvotiroadmin sgvotiroadmin 3 May 11 17:12
nfsshare
```

#### Note

In this example, **sgvotiroadmin** is the username that I use during the first login via putty to SFG.

Your username may vary according to what you have created during the initcluster phase.

#### 8.3.2 Issue 2: Missing metadata in blob-config

#### Symptoms

After changing the blob-config, the metadata portion might not be able to populate correctly.

#### Solution

To verify the blob-config, run the following command:

```
kubectl edit configmap blob-config -n votiro
```

xind: ConfigMap
netadata:
annotations:
kubectl.kubernetes.io/last-applied-configuration:
{"apiVersion":"v1","data":{"daysToKeepOriginal":"30","daysToKeepPpf":"180","daysToKeepSanitized":"30
deleteFilesBatchSize":"50","elastic.json":"{\n \"ElasticSearchConfig\": {\n \"ServerAddresses\":
http://elastic-service:9200\" ],\n \"DefaultIndexName\":\"votiro-blob-{tag}\",\n \"PoolType
),\n \"DisableDirectStreaming\": false,\n <u>\"SerializerFactory\": null,\n }\n}","encryp</u> tFil
"true","externalStorageBackupInterval":"00:10:00","externalStorageRootPath":"/externalblobs/nfsshare","ir
nalStorageRootPath":"/votiroblobs","maxBlobStorageUsagePercentage":"95","maxElasticStorageUsagePercentage"
)", "runCleanerAtHour":"02:00", "storageCheckInterval":"00:00:30", "storageHealthCheckTimeoutInMilliseconds":
000","warningBlobStorageUsagePercentage":"70"},"kind":"ConfigMap","metadata":{"annotations":{},"labels":{'
uctVersion":"9.6.174","vendor":"votiro"},"name":"blob-config","namespace":"votiro"}}
creationTimestamp: "2022-03-04T13:41:25Z"

Scroll down to the **metadata** section - the **externalStorageRootPath** may appear blank. Edit the file to ensure that this string is present. Be careful to preserve the commas (,) before and after the string:

,"externalStorageRootPath":"/externalblobs/nfsshare",

### 9 How to Deploy the Votiro Cloud Cluster in Azure

This page describes how to configure the Votiro Cloud cluster to work with Microsoft's Azure cloud computing platform.

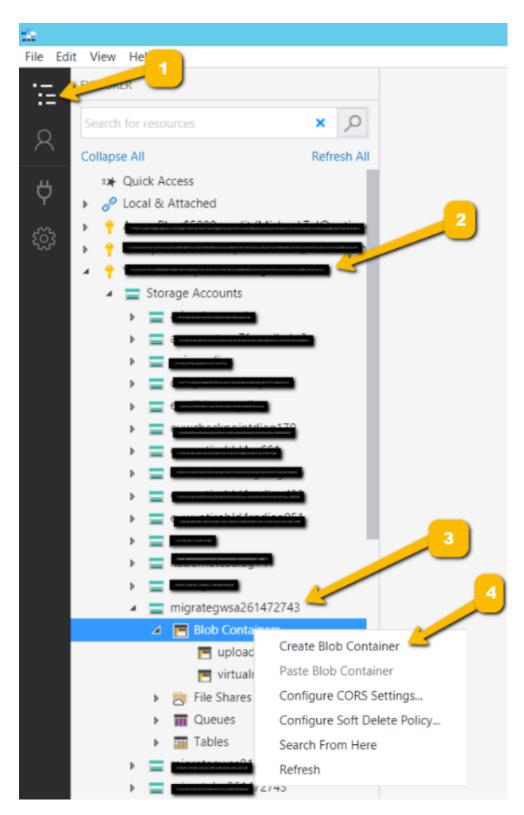
#### 9.1 Prerequisites

Before you start, verify that the following are available:

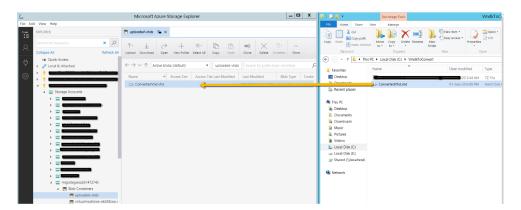
- An active Azure subscription
- The latest VHD (Virtual Hard Disk) provided by Votiro.
- The Azure Storage Explorer tool installed on a system that can access the Azure account and will be used to upload the VHD to your Storage account in Azure. This tool may be downloaded from <u>Azure Storage Explorer</u>.
- The recommended disk size is 500 GB Premium SSD.

#### 9.2 Procedure

- 1. Run Azure Storage Explorer and authenticate with your Azure account.
- 2. On the left pane click on **Toggle Explorer**.
  - a. Expand the view of the desired subscription.
  - b. Expand Storage Accounts.
  - c. Select the desired Storage account and expand it.
  - d. Under Blob Containers, right click it and select **Create Blob Container**.
  - e. Provide it with a name.



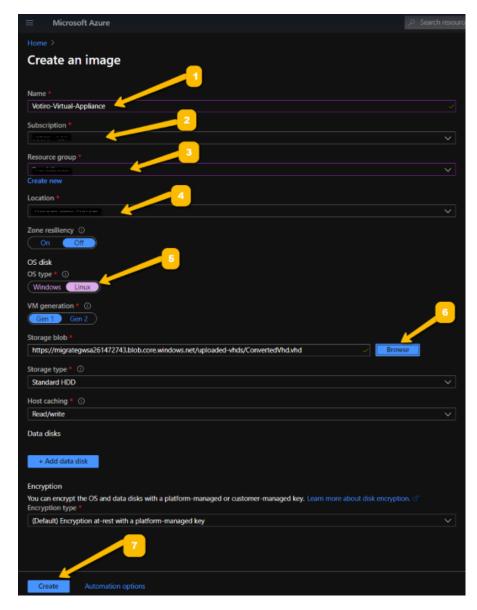
3. Drag and drop the extracted VHD file to the created Blob Container.



- 4. Once the upload process completes, open the Azure portal and navigate to the Images blade.
- 5. Click on Add. The Create an image screen is displayed.

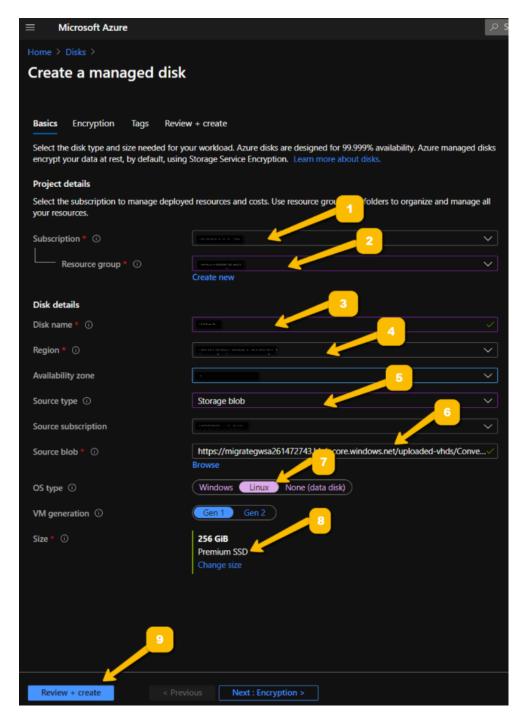
$\equiv$ Microsoft Azure
Home >
Images 🖈 <sub>Votiro</sub>
+ Add 🔯 Manage view $\checkmark$ 🖒 Refresh 🛓 Export to CS
Filter by name Subscription == (all) Resou

- 6. Fill in the information to build the image from the VHD:
  - a. Provide the image with a **Name**.
  - b. Select a Subscription.
  - c. Type in the **Resource group**.
  - d. Select the **Location**.
  - e. Select the **OS type** as **Linux**.
  - f. Click on **Browse** and select the uploaded VHD file.
  - g. Click on **Create**.

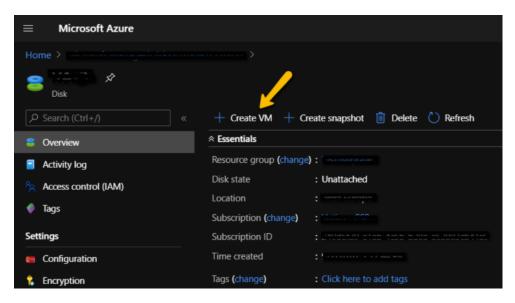


- 7. After the image is created, **Create a managed disk**.
- 8. Fill in the information as in the screenshot below:
  - a. Select a **Subscription**.
  - b. Select the **Resource group**.
  - c. Provide a **Name** for the disk, for example Node-1.
  - d. Select the **Region** which you would like the disk and VM to be in.
  - e. For Source type, select Storage Blob.
  - f. In **Source blob**, **Browse** to the uploaded VHD.
  - g. For **OS type**, select **Linux**.
  - h. The disk Size should be 500 GiB Premium SSD.

i. Click on **Review + create**.



9. After the deployment of the disk is complete, select it and create a VM from it.



10. Fill in the information in the **Create VM** wizard as in the screenshot below:

$\equiv$ Microsoft Azure	م
Home > 1 in cost in more apprinted as a cost	
Create a virtual machin	1e
Basics Disks Networking Ma	nagement Advanced Tags Review + create
	r Windows. Select an image from Azure marketplace or use your own customized ew + create to provision a virtual machine with default parameters or review each tab
Project details	
	red resources and costs. Use resource groups like folders to organize and manage all
your resources.	
Subscription ①	Votiro - CSP
Resource group * ①	
Resource group * U	Create new
	2
Instance details	
Virtual machine name * 🚯	ware 🖌 🗸
Region ①	
Availability options ①	No infrastructure redundancy required $\checkmark$
Image * 🛈	071-5 - 194911 V
	Browse all public and private images
Azure Spot instance ①	⊖ Yes
Size * 🛈	Standard_D8s_v3 - 8 vcpus, 32 GiB memory (\$350.40/month)
Inbound port rules	
Select which virtual machine network por network access on the Networking tab.	ts are accessible from the public internet. You can specify more limited or granular
Public inbound ports * 🕥	None Allow selected ports
Select inbound ports	
	All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.
Review + create < Pre	Next : Disks >

- 11. In the **Disks** blade, keep the defaults.
- 12. In the **Networking** blade, select the desired virtual network, NSG (network security group), etc.
- 13. To complete, click on **Review + create**.
- 14. Repeat steps 7-13 for the other Disks and VMs in the cluster.

### 10 How to Integrate Azure AD Single Sign-on with Votiro using SAML Toolkit

In this tutorial, you'll learn how to integrate Azure AD single sign-on with Votiro using SAML Toolkit to enable users to log in to the Votiro Management console using their corporate credentials.

### 10.1 Prerequisites

Ensure you have the following items:

- Azure AD subscription
- Azure AD SAML Toolkit enabled on the above-mentioned subscription

### 10.2 Procedure

- 1. Sign in to the <u>Azure portal</u>.
- 2. Select Azure Active Directory.

Microsoft Azure	$\mathcal{P}_{\rm c}$ Search resources, services, and docs	(G+/)				Þ	Q Q	-	ଡି ନ
Il services									
All	Filter services								
Favorites									
Recents		()		SQL	6	<b>{··&gt;</b>			
Categories		Resource App Services	Storage	SQL	Cost	Virtual			
Seneral	Directory machines	groups	accounts	databases	Management	networks			
Compute	General (18)								
Vetworking	All resources		Recent						
Storage	All resources		🕓 Recent						
Web	(\land) Management groups		📍 Subscriptic	ons					
Mobile	(i) Resource groups		🗿 Cost Mana	gement + Billing					
Containers	🖞 Marketplace		🧟 Help + sup	port					
Databases	Service Health		Templates			PREVIEW			
Analytics									
AI + machine learning	🇳 Tags		<ol> <li>What's new</li> </ol>						
nternet of Things Mixed reality	🚀 Quickstart Center		📶 Shared da:	shboards					
integration	Free services		🕓 Reservatio	ns					
	Resource Explorer		Preview fe	atures		PREVIEW			
Identity	·								

3. In the left pane, select **Enterprise applications**.

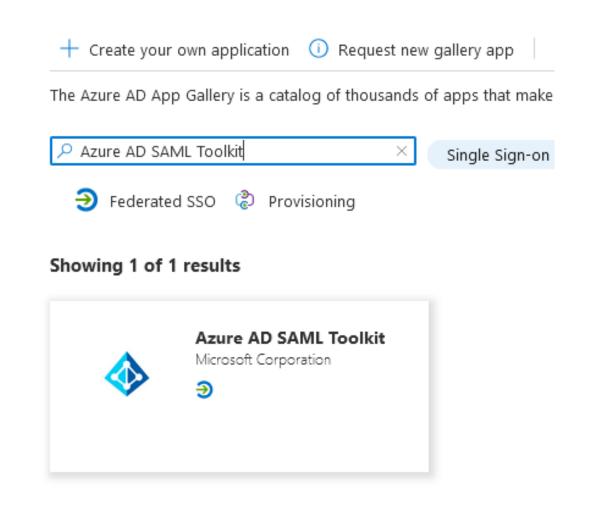
	, ₽ Search resources, sen	rices, and docs (G+/)					Ģ	Q	۲	?	ନ୍ଦି
All services >											
Votiro   Overview     Azure Active Directory											
Overview	+ Add 🗸 🛞 M	anage tenants 🛛 What's new 💽 Prev	view features	🔗 Got feedba	ck? $\checkmark$						
Preview features	<u>Microsoft Entra</u>	has a simpler, integrated experience for manag	<u>aing all your</u>	Identity and Access M	anagement needs. Try the new M	icrosoft Er	ntra ad	min ce	nter! 🛛		
X Diagnose and solve problems	Overview Monite	oring Properties Recommendations	Tutoria	ls							
Manage						_					
🚨 Users	Search your ten	ant									
A Groups	Basic information										
External Identities											
🚨 Roles and administrators	Name	Votiro		Users	307						
Administrative units	Tenant ID	a66f051a-cd66-4949-bf39-a108012d45ee	Ð	Groups	215						
🚸 Delegated admin partners	Primary domain	votiro.com		Applications	59						
Enterprise applications	License	Azure AD Free		Devices	153						
Devices											
App registrations	Alerts										
Identity Governance											
Application proxy		IPv6 deployment ons that use named locations in		Upcoming MFA Serv Please migrate from I	ver deprecation MFA Server to Azure AD Multi-						
<ul> <li>Custom security attributes (Preview)</li> </ul>		I Access or Identity Protection must take oon as possible to avoid any service		Factor Authentication any service impact.	by September 2024 to avoid						
🔓 Licenses 👻		. 12		Loom more 78							

#### 4. Select **New application**:

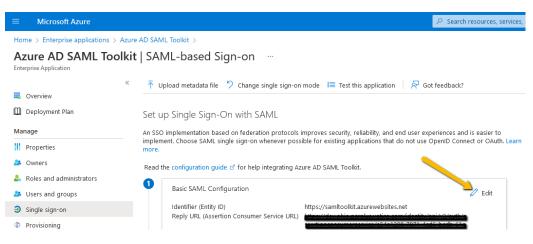
Microsoft Azure	$\mathcal{P}$ Search resources, services, and d	ocs (G+/)					
Il services > Votiro   Enterpris	applications > Enterprise applications						
Enterprise app	ications   All application	s					
	H New application      Refree	• rsh 🞍 Download (Export) 🕴 🚹 P	review info 🛛 🗮 Columns 🗍	💀 Preview features 🛛 🔗 G	ot feedback?		
verview							
Overview	View, filter, and search application	ns in your organization that are set up to	o use your Azure AD tenant as the	eir Identity Provider.			
Ciagnose and solve problems	The list of applications that are m	aintained by your organization are in ap	plication registrations.				
Manage	Search by application name of the second	r object ID Application type	== Enterprise Applications ×	Application ID starts with X	+ Add filter	-	
All applications	163 applications found	Application type	Enterprise Applications	Application to starts with 75	Y Add inter	3	
Application proxy		Object ID	Application ID	Homepage URL	Created on	↑↓ Certifi	cate Expiry Status
User settings	bob bob	008f06ff-0fe0-4e63-bfb8-d2950	481f9d7f-1426-4b4e-a27f-af52	https://app.hibob.com/	4/14/2022		
App launchers	VT SSO	02e285ab-8c85-45ca-9a58-c6a	9e947dbb-29fb-4b8b-9812-b3	https://www.virustotal.com/	2/9/2023		
Custom authentication	de Slack	072bca59-64d3-46e9-be72-f96	da2ef37b-cf36-4f1b-85f1-be97			-	
extensions (Preview)	ZO Zoom	089fffb8-f4c5-4937-9f14-9b087 1	c108d3f-543d-4374-bbff-c7c5	https://zoom.us	11/25/2019	-	
ecurity	# monday.com	0c3eaf5a-c75e-457c-8a25-9448	38fa0b1d-4df6-463e-bf67-1a6f	https://monday.com	11/11/2021		
Conditional Access	AS Assembla	0d209699-faac-44bc-9782-ec71 a	a5edd250-fb41-453e-9912-978	https://account.activedirectory			
ð Consent and permissions	Cisco Webex Social Logir	0d26c869-aab0-484c-9094-47c	280851f2-bc68-4362-91e9-3c4	https://webex.com/	12/15/2022		
ctivity	Meetup	0faa5c10-f792-4d1a-b52f-2337 ;	a1cf9e0a-fe14-487c-beb9-dd33			-	
	Log in using Office 365	0fbb48bb-c678-4857-b38b-1b9	5cd6e32d-de3f-4cb5-a322-ea0	https://cloud-protect.net	3/17/2020		
Sign-in logs	cog in doing onice ous						
Sign-in logs	SL Slack	118b4f5f-f569-4291-ba64-86be	3c3b7662-a040-4180-89c1-57f	https://*.slack.com/sso/saml?m	2/11/2020	-	

5. In the search field type **Azure AD SAML Toolkit**.

## Browse Azure AD Gallery



- 6. Lastly, select it from the results and add it. After a few moments, the app will be added to your tenant.
- 7. Navigate back to **Enterprise applications** | **All applications** and select the newly added app: **Azure AD SAML Toolkit**.
- 8. On the left pane, select **Single sign-on**.
- 9. On the **Basic SAML Configuration** page, click the pencil button to edit the configuration.



- 10. For Identifier (Entity ID), leave as default https://samltoolkit.azurewebsites.net.
- 11. Both Reply URL (Assertion Consumer Service URL) and Sign on URL should be in the following format: https://<VOTIRO-FQDN>/assertionconsumerservice.

#### Note:

If you're configuring SAML for SaaS cluster, please make sure to include the tenant id after the Reply URL and Sign on URL:

https://<VOTIRO-FQDN>/assertionconsumerservice/<TENANT\_ID>

12. Other fields are optional and will remain blank, lastly press the Save button.

 $\times$ 

Identifier (Entity ID) * 💿 The default identifier will be the audience of the SAML response for IDP-initiated SSO	Default
	Default
https://samltoolkit.azurewebsites.net	✓ 0
Add identifier <b>Patterns:</b> https://samltoolkit.azurewebsites.net	
Reply URL (Assertion Consumer Service URL) * ①	
The default reply URL will be the destination in the SAML response for IDP-initiated SSO	
	Default
https://dev.ohio.paralus.votiro.com/identity/api/v2/auth/assertionconsumerservice/e54e129	98-78 🗸 🛈
https://icomon.ug/assertionconsumerservice	
Add reply URL	
Patterns: https://samltoolkit.azurewebsites.net/SAML/Consume	
Sign on URL* 🛈	
https://	
Patterns: https://samltoolkit.azurewebsites.net/	
Balay State (Ostional)	
Relay State (Optional) 🕕	

- 13. On the **Attributes & Claims** section, click the pencil button to edit the configuration.
- 14. Select **Add a group claim** on the left-hand side, choose All groups, expand **Advanced options**, select **Customize the name of the group claim**, and provide it with a name, for instance, "AzureGroup1", then press the **Save** button.



<b>Group Claims</b> Manage the group claims used by Azure AD to populate SAML tokens issued to your app	×
This page includes previews available for your evaluation in the 'Advanced options' section.	
Which groups associated with the user should be returned in the claim? <ul> <li>None</li> <li>All groups</li> </ul>	
O Security groups	
O Directory roles	
Groups assigned to the application	
Source attribute *	
Group ID	$\sim$
<ul> <li>Advanced options</li> <li>Filter groups (Preview)</li> <li>Attribute to match</li> <li>Match with</li> </ul>	~
String	
Customize the name of the group claim	
Name (required)	
AzureGroup1	
Namespace (optional)	
Emit groups as role claims 🛈	

Apply regex replace to groups claim content (Preview)



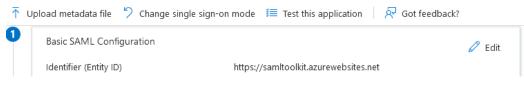
15. To avoid issues such as "User without any role", make sure the users that should have access to the environment via SAML are listed under **Azure AD SAML Toolkit |** Users and groups.

Microsoft Azure		$\mathcal P$ . Search resources, services, and docs (G+/)	E 6
Home > Enterprise	e applications > Azure AD SAML Toolkit		
Azure AD SAM	IL Toolkit   Users and groups		
_	* 🕂 Add user/group 🖉 Edit 🔋 Remove 🖉 Update Credentials   🎫 G	iumns 🛛 🞘 Got feedback?	
<ul> <li>Overview</li> <li>Deployment Plan</li> </ul>	The application will appear for assigned users within My Apps. Set 'visible to users?' to	to in properties to prevent this. $\rightarrow$	
Manage	P First 200 shown, to search all users & groups, enter a clipplay name.		
Properties	Display Name	Object Type	Role assigned
A Owners	🦯 🗆 😐 📖 📖 📖	User	Default Access
& Roles and administra	🗆 🞯 🚥	User	Default Access
Users and groups		User	Default Access
Single sign-on	- 💿 📥	User	Default Access
Provisioning	🗆 😡 📥	User	Default Access
😔 Self-service	🗆 🤒 📥	User	Default Access
<ul> <li>Custom security attributes (preview)</li> </ul>	🗆 🌝 🚥	User	Default Access

16. Log in to Votiro's Management console. On the left pane, click on the cogwheel, and select **SAML**. For the IDP Metadata address, copy and paste the value from the **App Federation Metadata Url** field in Azure.

Microsoft Azure		Search resources, services, and docs (G+/)	
Home > Enterprise applications   All ap	oplications > Azure AD SAML Toolkit - AWS TEST	>	
Azure AD SAML Toolkit	- AWS TEST   SAML-based Sig	n-on	
«	🔨 Upload metadata file 🏷 Change single sign-	on mode 📁 Test this application   🖗 Got feedback?	
Overview	Read the configuration guide 🖻 for help integrating a	Azure AD SAML Toolkit - AWS TEST.	
Deployment Plan	Basic SAML Configuration		
Manage	Identifier (Entity ID)	https://samltoolkit.azurewebsites.net.beta	
Properties		) https://prod.us.paralus.votiro.com/assertionconsumerse	
3 Owners	Sign on URL	rvice/ https://prod.us.paralus.votiro.com/assertionconsumerse	
👃 Roles and administrators		rvice/	
Users and groups	Relay State (Optional) Logout Url (Optional)	Optional Optional	
Single sign-on	-		
Provisioning	2 Attributes & Claims		
Self-service			
Custom security attributes (preview)	givenname surname emailaddress	user.givenname user.surname user.mail	
	name	user.userprincipalname	
Security	AzureGroup1 Unique User Identifier	user.groups user.userprincipalname	
Conditional Access		eschesciphicipentente	
Permissions	3		
Token encryption	SAML Certificates		
Activity	Token signing certificate		
Sign-in logs	Status Thumbprint	Active	
👔 Usage & insights	Expiration	5/2/2025, 8:25:10 AM	
Audit logs	Notification Email App Federation Metadata Url	https://login.microsoftonline.com/ca604247-726	
Provisioning logs	Certificate (Base64)	Download	
	Certificate (Raw)	Download	
Access reviews	Federation Metadata XML	Download	
Froubleshooting + Support	Verification certificates (optional) (Preview)		
Virtual assistant (Preview)	Required Active	No 0	

17. For the Issuer, copy and paste <u>https://samltoolkit.azurewebsites.net</u> from the **Basic SAML Configuration** you configured above.



- 18. For the SAML Username identifier, leave by default: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
- 19. The Admin role key should be the value you provided for the group above in **Group Claims**, in this case, AzureGroup1.
- 20. The Admin role value should be the Object Id of the group in which the admin's users are members.

Home > Concernent Groups >			
i admins ጵ … <sub>Group</sub>			
«	📋 Delete 🛛 📯 Got feedback?		
1 Overview	admins		
🗙 Diagnose and solve problems	AD		
Manage			
Properties			Copy to clipboard
🚨 Members	Membership type	Assigned	
🚨 Owners	Source	Cloud	
🔓 Roles and administrators	Туре	Security	D
Administrative units			
🔅 Group memberships	Object Id	1feef5b7-filmenningeren ministeren	
Applications	Creation date	7/6/2021, 5:07:22 AM	
🔓 Licenses			
📍 Azure role assignments	Direct members		
Activity	🕀 4 Total 🛛 🔒 4 User(s)	A Group(s) 🛛 🔤 O Device(s)	0 Other(s)
≆ Access reviews		Owners	Total members
Audit logs	Group memberships		
👶 Bulk operation results	A 0	<mark>گ</mark> 0	<b>@</b> 4
Troubleshooting + Support			
New support request			

21. Press the **Save changes** button, log out from the Management console and log in with the corporate credentials. You may continue and set up the Help Desk and SOC groups, similar to what was configured for the admins group.

### 11 How to Integrate SIEM with Azure Sentinel

In this tutorial, you'll learn how to integrate SIEM with Azure Sentinel using **Votiro Solution for Microsoft Sentinel**. **Votiro Solution for Microsoft Sentinel** is a collection of Data Connectors, Parser, Workbook and Analytic Rules that are used together to analyze data.

### **11.1** System prerequisites

Ensure you have the following:

- Linux machine with at least 4 CPU cores and 8 GB RAM
- Python 2.7 or 3 installed on the Linux machine
- Rsyslog: v8/Syslog-ng: 2.1 3.22.1
- Syslog RFC 3164/5424
- Download and unpack the file: Votiro-Offline.zip

#### **11.2 Procedure**

#### **11.2.1** Manual/Offline Deployment

To test the solution before publishing, follow the below steps.

#### **Deploy CEF Data Connector on Forwarder Machine**

- 1. Sign in to the <u>Azure portal</u>.
- 2. Search for Microsoft Sentinel.

≡ Microsoft Azure	∞ Sentinel	×	Þ Q	© R	XXXX @votiro.co
Azure services	All Services (1) Marketplace (31)	✓ More (4)			A
+ 🔺	Services		SOL	$\rightarrow$	
Create a Microsoft Entra	Microsoft Sentinel		Storage SQL databases	More services	
resource ID	Marketplace	See more	accounts		
	🛆 Azure Sentinel				
Resources	🗳 Microsoft Defender for Endpoint				
Recent Favorite	🛎 Snowflake				
Name	aws IAM		Last Viewed		
	Documentation	See more			
	Hybrid security monitoring with Microsoft Sentinel - Azu	e Architecture Center 🛛 🖻			
	Entity pages in Microsoft Sentinel	ೆ			
	Create new watchlists - Microsoft Sentinel	ď			
	Visualize collected data	c"			
	Continue searching in Microsoft Entra ID				
Navigate	Searching all subscriptions.	R Give feedback			
🔶 Subscriptions	Resource groups	All resources	Zh Dashboard		

3. Select Microsoft Sentinel from Services.

Microsoft Azure	$\mathcal P$ $$ Search resources, services, and docs (G+/) $$		Þ				NAME OF COMPARENT OF COMPARENT. COMPARENTE OF COMPARENTA OF	.со 🧧
Home >								
Microsoft Sentinel 🖈 …								×
🕂 Create 🛞 Manage view 🗸 🕐 Refresh 🚽	Export to CSV 🛛 😤 Open query 🕴 🖻 View incidents							
Filter for any field Subscription equals a	II Resource group equals all $ imes$ Location equals all $ imes$	+ <sub>♥</sub> Add filter						
howing 0 to 0 of 0 records.				No	prouping	$\sim$	≡≡ List view	$\sim$
Name 🕆 🌡	Resource group ↑↓	Location ↑↓	Subscription $\uparrow_{\downarrow}$			Directory	¢.↑↓	
	No Microsof	t Sentinel to display						
		t Sentinel to display	Keened Constant Lawrence					
	See and stop threats before they cause harm, with		Microsoft Sentinel is your					
	See and stop threats before they cause harm, with birds-eye vie	SIEM reinvented for a modern world.	Microsoft Sentinel is your					

4. Press + Create or Create Microsoft Sentinel to add Microsoft Sentinel to a Workspace::

■ Microsoft Azure		Ε	э с	0	0	R	KKKK @votiro.co Votiro (votiro.com
Home > Microsoft Sentinel >							
Add Microsoft Sentinel to a	workspace						
+ Create a new workspace 💍 Refresh							
Microsoft Sentinel offers a 31-day free trial. See Mic	osoft Sentinel pricing for more details.						
Filter by name							
Filter by name							
	No workspaces found						
	Create a new workspace						
Add Cancel							

5. Press + Create a new workspace:

Give feedback

Home > Microsoft Sentinel > Add	Microsoft Sentinel to a workspace >	
Create Log Analytics	workspace	
Basics Tags Review + Create		
	basic management unit of Azure Monitor Logs. There new Log Analytics workspace. <u>Learn more</u>	rre specific considerations $\times$
	ily store, retain, and query data collected from you insights. A Log Analytics workspace is the logical st	
Project details Select the subscription to manage de manage all your resources.	ployed resources and costs. Use resource groups li	xe folders to organize and
Subscription * ①	Enterprise Dev/Test	~
		~
Resource group * ①	Create new	
Kesource group * ()		
Resource group * ()		
Instance details	East US	

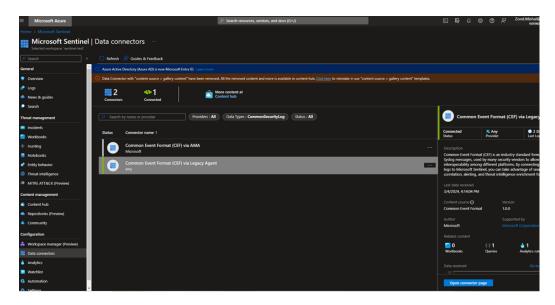
6. Create a new **Resource Group** if it does not exist yet. Then create a new machine with the system requirements mentioned above → via Resource Group > Create > select Virtual Machine (Ubuntu 22.06 server is recommended):

Home > Microsoft Sentinel >			
Microsoft Sentinel « Votiro (votiro.com)	Sentinel-Test 🖈 🛪	¢ ···	
+ Create  🛞 Manage view 🗸 …		🕂 Create 🛞 Manage view 🗸 📋 Delete resource group 🖒 Refresh 🞍 Export to CSV 😤 Op	en query 📔 🖉
Filter for any field	Overview		
Name 1	Activity log	Subscription (move) : Votiro - CSP	
Sentinel-Test	Access control (IAM)	Subscription ID : 240d6f29-e1ab-4c5b-b28a-e62883cb41a9	
Sentilier-rest	🔶 Tags	Tags (edit) : Add tags	
	🛧 Resource visualizer		
	🗲 Events	Resources Recommendations (1)	
	Settings	Filter for any field Type equals all $ imes$ Location equals all $ imes$ $^+\!\gamma$ Add filter	
	Deployments	Showing 1 to 12 of 12 records. Show hidden types 🔘	
	Security	Name ↑	Type ↑↓
	Deployment stacks		Azure Workboo
	Policies		
	Properties	9d277f47-b0d9-4118-8523-6019c4439032 (Workbook 1)	Azure Workboo
	Locks	SecurityInsights(sentinel-test)	Solution
		🔲 🕎 Sentinel-logforwarder	Virtual machine

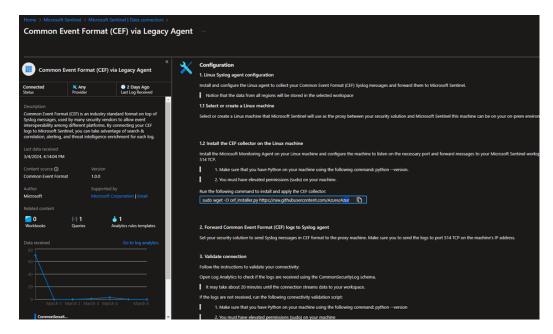
 Select the created workspace, then go to Content Hub > Select Common Event Format (CEF) and install it:

ome > Microsoft Sentinel > Microsoft Sen Microsoft Sentinel « otro (votiro.com)	Microsoft Sentinel   Selected workspace: 'Sentinel-test'	Content hub							
+ Create 🔘 Manage view 🗸 🚥		🕐 Refresh 过 Insta		Guides & Feedback					
	General	<b>a</b> 342	273	⊘1	<b>1</b> 0				
lame ↑.	Overview (Preview)	Solutions	Standalone contents	Installed	Updates				
Sentinel-Test	🧬 Logs								
	News & guides	cet		Status : All Conter	t type : All	Support : All P	rovider : All Cate	gory : All Cont	tent sources : All 🔐 🗮
	🔎 Search								
	Threat management	Content title		Status		Content source	Provider	Support	Category
	Incidents	📃 🔄 Akamai S	ecurity			Solution	Akamai	Microsoft	Security - Cloud Security
	Workbooks								
	4 Hunting	Azure Ck	ud NGPW By Palo Alto Net			Solution	Palo Alto Netw	Microsoft	Security - Automation (SOAR), Securit
	Notebooks	Common	Event Format	Installed		Solution	Microsoft	Microsoft	IT Operations
	Entity behavior								
	Threat intelligence	Cortex XI	R Data Connector			Solution	DEFEND Ltd.	DEFEND Ltd.	Security - Threat Protection
	MITRE ATT&CK (Preview)	🗌 🔍 CyberArk	Enterprise Password Vault (			Solution	Cyberark	Cyberark	identity
	Content management	Darktrace				Solution	Darktrace	Darktrace	Security - Threat Protection
	Content hub					2010/001	UNIXUBLE	Carkbace	second - meat Protection
	<ul> <li>Repositories (Preview)</li> </ul>	📃 🍐 Dev-0530	File Extension Rename			Standalone		Community	Security - Others
	Community	C C States	ced WAF Integration via Sy			Solution	F5 Networks		Security - Network

8. Once installed, go to your workspace > Data Connectors > Open Connector Page:



9. Follow the instructions in 1.2 below, Install the CEF collector on the Linux machine:



10. Verify that you have Python 2.7 or Python 3 installed on the Linux machine by running:

python --version or python3 --version

11. Copy the command below:

```
sudo wget -O cef_installer.py
https://raw.githubusercontent.com/Azure/Azure-
Sentinel/master/DataConnectors/CEF/cef_installer.py&&sudo
python cef_installer.py [WorkspaceID] [Workspace Primary
Key]
```

Note: You must have the GNU Wget package installed on the Linux machine.

- 12. Paste the command into the command line on your log forwarder, and replace [WorkspaceID] and [Workspace Primary Key] with their values.
- 13. Run the command. This installs the CEF connector and Log Analytics Agent on the forwarder machine. Once done, the connector is now listening to events on TCP port 514.
- 14. Verify that the port used is indeed opened via the Virtual Machine's Network settings:

Sentinel-logforwar	der   Network settings 🛸 …		
🔎 Search	This is a new experience. <u>Please provide feedback</u>		
Overview	🖉 Attach network interface 🔗 Detach network interface 🎄 View topology 🤶 Troubleshoot 🗸 🕐 Refresh 🔗 Give Feedback		
Activity log			
Access control (IAM)	Retwork interface / IP configuration sentinel-logforwarder616.z1 (primary) / ipconfig1 (primary)		
🔷 Tags	sentinet-togrorwarderoto_zt (primary) / ipcontigt (primary)		
X Diagnose and solve problems	∧ Essentials		
Connect	Network interface : sentinel-logforwarder616,z1	Load balancers : 0 (Configure)	
🖉 Connect	Virtual network / subnet : Sentinel-logforwarder-vnet / default	Application security groups : 0 (Configure)	
メ Bastion	Public IP address : Sentinel-logforwarder-ip	Network security group : Sentinel-logforwarder-nsg	
Networking	Private IP address : 10.0.0.4	Accelerated networking : Disabled Effective security rules : 0	
Retwork settings	Admin security rules : 0 (Configure)	Effective security rules : 0	
Load balancing	Rules \land Collapse all		
Application security groups			
2 Network manager	Network security group Sentinel-logforwarder-nsg (attached to networkinterface: sentinel-logforwarder616_z1)      Impacts 0 subnets. 1 network interfaces		$+$ Create port rule $\vee$
Settings			
Disks	Search rules     Search rules     Search rules     Search rules     Search rules		
Extensions + applications	Priority 1 Name Port	Protocol Source Destination	Action
Configuration	Privily i Name Port	Protocol Source Destination	ALUUN
Advisor recommendations	<ul> <li>Inbound port rules (5)</li> </ul>		
11 Properties	300 <u>▲</u> SSH 22	TCP Any Any	😪 Allow 🔋
🔒 Locks		Any Any Any	😔 Allow 🔋

**Note**: In this case, we used TCP port 514 (default) and **Allow=any**, but the best practice is to use the TLS protocol with other ports used and restrict to specific IPs pointed to specific NAT gateways. For example, in prod.us:

NAT	gateways (2) Info											
Q	Find resources by attribute	e or t	ag									
	Name	7	NAT gateway ID	▼	Connectivity ▼	State	▼	State message	▼	Primary public I	⊽	Primary private I
0	ngw-prod-egress-01		nat-013cc592b4306c371		Public	⊘ Available		-		54.234.70.44		10.240.128.14
0	ngw-prod-egress-02		nat-0f7ba826618ac4c93		Public	Available		-		34.237.77.26		10.240.129.207

#### **Deploy Parser Function**

Follow the instructions to parse ingested data:

- 1. Copy the function code from the downloaded package file: /Votiro-Offline/Parser/VotiroEvents.txt
- 2. On Microsoft Sentinel  $\rightarrow$  Go to your created Workspace -> Logs
- 3. Paste the content of **VotiroEvents.txt** in the area as shown below:

Microsoft Azure		🔎 Search resources, services,	and docs (G+/)	S 5		Zorel.Mishal@votiro.com voniio.voniio.com
Microsoft Sentinel «	Microsoft Sentine	l   Logs				
+ Create 🔘 Manage view 🗸 \cdots		🗧 🖉 New Query 1 🛛 🔀 🕂			💛 Feedbad	k 📰 Queries 🛛 🛞 🛄
Filter for any field	General	Sentinel-Test	D Run Time range : Last 24 hours Save V	년 Share - + New alert rule -		🗸 🛛 📨 Format query 🔹
Name 1.	Overview (Preview)	Tables Queries Functions ··· ≪				
Section-Text	🔮 Logs					
	News & guides	P Search				
	🔎 Search	▼ Fiter I Group by: Solution ∨				
	Threat management	T* Collapse all				
	Incidents	Favorites				
	Workbooks	You can add favorites by clicking on the 🖈 icon	Queries History			
	Hunting	LogManagement				
	Notebooks	Microsoft Sentinel	CommonSecurityLog   where DeviceVendor == "Votiro" and De	viceDeviart = = "Untire cloud"   name-ity	Additionallytensions as (com	mandame
	💣 Entity behavior	Workspace functions	string, correlationid:guid, itemid: guid, fileName: string, fileSize			
	Threat intelligence	f VotiroEvents	3/6/2024, 12:40 PM   33 results			
	MITRE ATT&CK (Preview)		CommonSecurityLog   where DeviceVendor == "Votico" and De	- feature "Minter claud" I mare hu	additional telescience on fear	
	Content management		string, correlationid:guid, itemid: guid, fileName: string, fileSize			
	Content hub		3/6/2024, 12:40 PM   0 results			

4. Then click on Save > Save as function. Enter the Function name as VotiroEvents and click on Save:

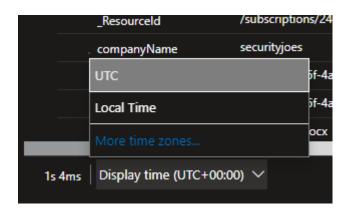
Function name *			
VotiroEvents			
Code			
dfgdfg			
Legacy category *			
VotiroEvents			
Save as compu	ter group 🕕		
Parameters			
Туре	Name	Default value	
Select type	✓ Type name	Type default value	]
	✓ Type name		]
	✓ Type name		]
	✓ Type name		]
	✓ Type name		]
	✓ Type name		
	✓ Type name		]
	✓ Type name		]
	✓ Type name		
Select type	Type name		

5. Try running the query to see the following type of results (adjust the time range according to data ingested):

🧬 Sentinel-Test	▶ Run Time rang	e: Last 7 days	🔚 Save 🗸 🖻	Share $\vee$ + N	ew alert rule 🗸 🛏 Ex	port 🗸 📌 Pin to 🗸	📄 📰 Format qu	iery
fables Queries ··· «	1 VotiroEvents							
P Search								
🝸 Filter 📔 Group by: Solut								
T Collapse all								
Favorites								
You can add favorites by	Results Chart Results							
clicking on the 🖈 icon		DeviceVendor	DeviceProduct	DeviceVersion	DeviceEventClassID	Activity	LogSeverity	Filet
LogManagement				1.0.0.0				
Microsoft Sentinel		Votiro	Votiro cloud		500	Sanitization summary		fa27
<ul> <li>Workspace functions</li> </ul>	> 2/29/2024, 10:03:12.734 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		fa27
f VotiroEvents	> 2/29/2024, 10:10:40.876 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		980
	> 2/29/2024, 10:11:19.147 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		980
		Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		980
	> 2/29/2024, 10:13:17.393 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		980
	> 2/29/2024, 10:15:45.742 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		3dfi
	> 2/29/2024, 10:18:49.026 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		3df7
	> 2/29/2024, 10:19:03.034 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		3df7
	> 2/29/2024, 10:19:20.211 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		3df7
	> 2/29/2024, 10:23:10.279 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		3df7
	> 2/29/2024, 10:24:10.481 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		3df7
	> 2/29/2024, 10:25:07.792 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary		38c9
			Votiro cloud	1.0.0.0	500	Sanitization summary		38c9
	> 2/29/2024, 10:26:14.751 AM	Votiro	Votiro cloud	1101010		Sanitization summary		5005

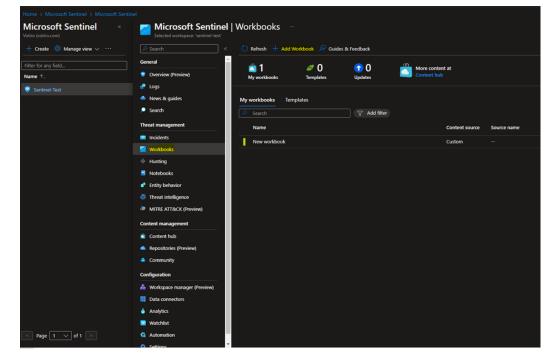
	~	3/3/2024, 2:04:30.713 PM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	fa2742
		Tenantld	6c0fa6d8-ec71-4593-8e5f	-45b4f7770685					
		TimeGenerated [UTC]	2024-03-03T14:04:30.7132	Z					
		DeviceVendor	Votiro						
		DeviceProduct	Votiro cloud						
		DeviceVersion	1.0.0.0						
		DeviceEventClassID	500						
		Activity	Sanitization summary						
		LogSeverity							
		FileHash	fa2742aec57ae5a21e80a0	cf7767af566ba48e0b0	35fa5546fc34e2898a31	ad6			
		FileType	Word (2007-2010)						
_		Computer	ec2-54-234-70-44.comput	te-1.amazonaws.com					
_		SourceSystem	OpsManager						
_		Туре	CommonSecurityLog						
		_ResourceId	/subscriptions/240d6f29-e	e1ab-4c5b-b28a-e6288	33cb41a9/resourcegro	ups/sentinel-test/providers/	microsoft.compute/virtualm	nachines/sentinel-log	gforwarde
		companyName	securityjoes						
		correlationId	6965cf87-045f-4a6b-bda5	5-f0321c75a43f					
		itemId	6965cf87-045f-4a6b-bda5	5-f0321c75a43f					
		SrcFileName	saddsaDSA.docx						

6. Results can be viewed in **Local Time** zone by changing the option in the bottom bar:

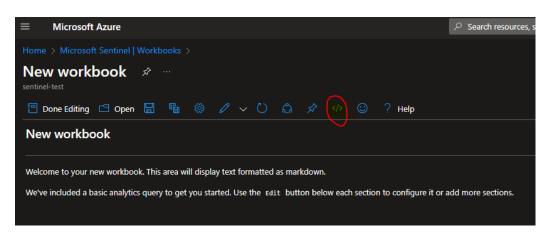


#### **Deploy the Workbook**

- Copy the contents of the file: /Votiro-Offline/Workbooks/Votiro Monitoring Dashboard.json
- 2. On Microsoft Sentinel, go to your WorkSpace > Workbooks > Add Workbook":



3. On the New Workbook page, click on Edit > Advanced Editor icon:



4. Replace the Gallery template contents with the copied contents, and click on **Apply**:

$\equiv$ Microsoft Azure	$ \mathcal{P} $ Search resources, ser
Home > Microsoft Sentinel   Workbooks >	
New workbook 🖈 … sentinel-test	
$\square$ Done Editing $\square$ Open $\square$	
Shown below is a JSON representation of the current item. Any changes you make here will be reflected when you press 'Apply'.	
Template Type 💿	
Gallery Template ARM Template	
E Contraction of the second seco	
"version": "Notebook/1.0",	
"items": [	
{   "type": 1,	
content": {	
"json": "## This Workbook is used to analyse file sanitization data from	Votiro's endpoints."
"customWidth": "90",	
"name": "text - 5",	
"styleSettings": {	
"maxWidth": "90" }	
"type": 9,	
"content": {	
"version": "KqlParameterItem/1.0",	
"parameters": [	
<pre>"id": "8b8cd15e-bd0d-4cb9-aef6-07e117e2cf5a",</pre>	
"name": "TimeRange",	
"type": 4,	
"isRequired": true,	
"value": {	
"durationMs": 604800000	
"typeSettings": {	
"selectableValues": [	
{ "durationMs": 300000	
}, {	

5. The Following Workbook must be visible: After a scroll

#### **Set Alert Queries for Incidents**

- 1. Go to /Votiro-Offline/Analytic Rules. Keep both Votiro File Blocked FromConnector.json and Votiro File Blocked in Email.json files ready.
- 2. On Microsoft Sentinel > Workspace, select Analytics.
- 3. Click **Import** (from the bar at the top of the screen) in the resulting dialog box, navigate to and select the JSON files one by one, and select **Open**:

	+ Create 🗸 🕐 Refre	sh 🛃 Analytics workbooks 🗡 📿 Rule		Delete Harport Hoport	🔟 Columns 🛛 🕅 Guide	is & Feedback			
	<b>4</b> 3	More content at	Rules by severity						
niew	Active rules	Content hub	High (1) Medium (0) Low (2)	Informational (0)					
ws & guides	Active rules Rule terr	nplates Anomalies							
arch	Search by ID, name, t	tactic or technique							
management	Severity	Name		Rule type	Status	Tactics	Techniques	Source name	Last modifi
dents		Votiro File Blocked in Email		Scheduled	C Inabled			Custom Content	2/26/2024
rkbooks		Votiro File Blocked From Connector		Scheduled	© Enabled			Custom Content	
nting		Advanced Multistage Attack Detection		© Fution	© trabled	Col_ +110		Gallery Content	1/28/2024
tebooks		novaliced monitolage hubble believed		Cor Publich	U Enabled	Call +110		casely content	(And an and
tity behavior									
treat intelligence									
ITRE ATT&CK (Preview)									
nt management									
ontent hub									
positories (Preview)									
ommunity									
uration									
orkspace manager (Preview)									
ta connectors									
ilytics									
tchást									
tomation									

4. Make sure that the status of each active rule is enabled:

+ Create 🗸 🖒 Refre	sh 🗠 Analytics workbooks 🗠 🖓 R	ule runs (Preview) 🖒 Enab	ble 🚫 Disable 🗊 Delete 억 Impor	t ↦ Export 🛄 Columns	🔗 Guides & Feedback	
<b>4</b> 3	More content at	Rules by severity				
Active rules	Content hub	High (1) 📕 Medium	(0) Low (2) Informational (0)			
Active rules Rule tem						
Active rules Rule tem	iplates Anomalies					
Search by ID, name, t	actic or technique Y Add filter					
Severity	Name		Rule type	Statu	a Tactics	Techniques
Low	Votiro File Blocked in Email		Scher	duled 🕐	Enabled	
Low	Votiro File Blocked From Connect	or	Scher	duled 🕐	Enabled	
High	Advanced Multistage Attack Dete	ction	5 Fusio	n O	Enabled 📄 Col +11 🛈	

5. Check for recent alerts or incidents on the **Overview** page. Incidents are also available on the **Microsoft Sentinel** > **Incidents** page.

Search	< + Create incident (Pre	niew) Ů Refresh 🕚 C	ustom range: 2/6/2023 - 3/7/2024		Delete K Security efficiency w	rorkbook 💷 Columns 💂	Guides & Feedback				
Overview	- 27	<b>#7</b>	€0	Open incidents I							
Logs	Open incidents	New incidents	Active incidents	High (0)	Medium (1)	Low (6)	Informational	m			
News & guides	C Sauch by ID Bills 1	ags, owner or product	S Severity : All S	Ratus : 2 selected	Incident Provider name : All	Alert product name : All	Owner: All				
Search	Auto-refresh in										
nat management	Severity †↓	Incident ID 1	Tide 15	Alerts	Incident provider name	Alert product name	Created time 1	Last update time 10	Owner 1	Status 15	Tag
Incidents			(google_safebrowsing_samp.		Azure Sentinel	Microsoft Sentinel	02/26/24, 07:12 PM	02/26/24, 07:12 PM	Unassigned	New	
Workbooks			locogle safebrowsing same		Azure Sentinel	Microsoft Sentinel	02/26/24, 07:12 PM	02/26/24, 07:12 PM	Unassigned	New	
funting			(google_safebrowsing_samp.		Azure Sentinel	Microsoft Sentinel	02/26/24, 07:12 PM	02/26/24, 07:12 PM	Unassigned	New	
Votebooks			Iclamd.conf was blocked		Azure Sentinel	Microsoft Sentirel	02/26/24, 02:22 PM	02/26/24 02:22 PM	Unamigned	New	
ntity behavior			(syslog.bt was blocked		Azure Sentinel	Microsoft Sentinel	02/26/24, 02:12 PM	02/25/24, 02:12 PM	Unassigned	New	
hreat intelligence	-		(systog bit was blocked		Azure Sentinel	Microsoft Sentinel	02/26/24, 02:12 PM	02/26/24, 02:12 PM	Unassigned	New	
MITRE ATTRICK (Preview)	-				Azure Sentinel	Microsoft sensine					
ent management	Medium		NewTest		Azure Sentinel		01/28/24, 02:55 PM	01/28/24, 02:55 PM	Zorel Mishal	New	

Select the security efficiency workbook for a better view.

- 6. Alerts Logic:
- Votiro File Blocked From Connector: If the syslog message includes "blocked" under -Sanitization result- field and "false" under -password protected- field and "null" under -from- field create an alert with the following message: [file name] with hash [file hash] that was sent from connector [connector name] was blocked by Votiro due to Policy [policy name], see more detail in the following link [incident url]
- Votiro File Blocked in Email: If the syslog message includes "blocked" under -Sanitization result- field and "false" under -password protected- field and not "null" under -from- field create an alert with the following message: Attachment [file name] with the hash [file hash] was blocked in an email that was sent from user [from] to the following recipients [Recipients] by Votiro due to Policy [policy name], see more detail in the following link [incident URL]

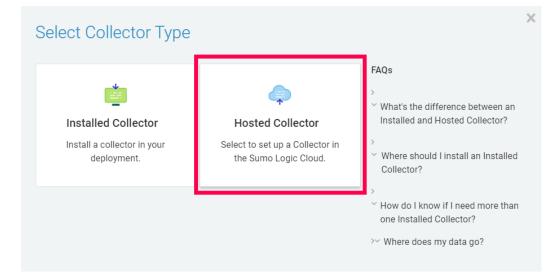
### 12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs

In this tutorial, you'll learn how to integrate Votiro Cloud Syslog messages with Sumo Logic using the HTTP logs method.

#### 12.1 Procedure

#### **12.1.1** Configure an HTTP Logs and Metrics Source in Sumo Logic

- 1. In Sumo Logic, select Manage Data > Collection > Collection.
- 2. Click Add Collector.
- 3. In the Select Collector Type window, select Hosted Collector.



4. In the Add Hosted Collector window, type a Name and click on Save.



Add Ho	sted Collector	ĺ
Name *	King-HTTP-Logs	
Description		
Category	Unless overwritten by Source metadata, the Collector will set the Source category of all messages to this value.	
Fields	+Add Field	
Assign to a	Not Assigned	
Budget	Collector will participate in the selected budget's criteria.	
Time Zone	(UTC) Etc/UTC	
	Unless overwritten by Source time zone, the Collector will set the Source time zone of all messages to this value.	
	Cancel Save	

5. To add a source to the collector, click **HTTP Logs & Metrics**.

sumo logic 🗧 🗧 🗧	Your trial ha	as expired. You ar	e now using a	Free Plan. Upon	ada Plan					Open	Onboarding Tasks -	_	- 25	& compliete 🛛 🗙
0 * B b	*		Collection	Source	2 Preferen	📴 Syslog	E Logs	## App Cat	📴 Search	Votiro	DrillDown F	Security	Account	+ Now
Recently Opened By Me	Collect	tion Ope	nTelemetry	Collection	Status Arch	ive								
RECENTLY OPENED DASHBOARDS	2	ollectors and So	irces >	Select Source for C	offector King-HTTP-L	ogs								
Votiro - Overview														
HTTP Votiro - Overview	(	Q http					ж							
11 Votiro - Overview														
11 Votiro - Overview	Ge	eneric	_											
11 Votiro - Overview														
1 Log Analysis QuickStart - Keyword			5	ttos://	1	RUM								
🔢 Linux - Login Status		https://	ι.	ttps:// −0−0 0−0	OpenToismetry									
🔛 Linux - Event Sources				0-0										
App Catalog		HTTP Logs & Metrics	HT	TP Traces	OTLP/HTTP	RUM HTTP Trace	15							
📋 Manage Data														
Collection														
Logs														
Metrics														
Monitoring														
Administration														
O Help														
💄 Ron Fonkats (Votiro) 🚺														

- 6. In the **HTTP Logs & Metrics** screen:
  - a. Type a **Name**.
  - b. Set the Source Category to prod/votiro/syslog.
  - c. Click Save.

sumo logic 🛛 🗧 🤟	Your trial has expired	d. You are now using a	Free Plan. Upgri	ada Plan					Open	Onboarding Tasks -		25	Ni complete 🛛 🗙
0 * 19 1	n 😑 A	Collection	Source	2 Preferen	📴 Syslog	E Logs	# App Cat	Search	Votiro	DrillDown F	Security	Account	+ New
Recently Opened By Me	Collection	OpenTelemetry	Collection	Status Archiv	e								
RECENTLY OPENED DASHBOARDS	Collectors	and Sources > (	elect Source for Co	elector King-HTTP-Log	s > HTTPLO	gs & Metrics							
🚼 Votiro - Overview													
HTTP Votiro - Overview	нттр	Logs & Metrics											- 11
12 Votiro - Overview									M FAQs				
Votiro - Overview	Name	ttp-logs							How do	upload to an HTTP	Source?		
1 Votiro - Overview		tion (optional)							<ul> <li>Can Luss</li> </ul>	e the URL to upload f	rom more than or	e data source?	
Log Analysis QuickStart - Keyword	Descrip	tion (optional)											
🔢 Linux - Login Status		Host (optional)								a way to generate a r			
🚼 Linux - Event Sources	0.000	Prose (operanae)							<ul> <li>What file</li> </ul>	types can be collect	ted from an HTTP	Source?	
App Catalog		Category (optional)							<ul> <li>How do</li> </ul>	I send metrics to an	HTTP Source?		
Manage Data		otiro/syslog							<ul> <li>How do</li> </ul>	I search for metrics	ent to an HTTP S	ource?	
Collection	Fields/	Metadata								I append custom me in HTTP Source?	tadata and dimen	sions to metrics	
Logs	Key	r	Value							uld I configure my ti	and the section of		
Metrics	+ A	ldd											
Monitoring									<ul> <li>How do</li> </ul>	l use "fields" feature	to add metadata t	io logs and metrics	?
Administration	Advar	nced Options for	Logs (Optiona	ul)									
HHp													
👤 Ron Fonkats (Votiro) 📀													

- 7. After saving the source, the **HTTP Source Address** window is displayed. Copy the address\* value and click on **OK**.
  - \* This address will be used to configure the Votiro Management console.



8. If the installation was successful, the installed HTTP Logs Collector shows up in the **Collection** console as **Healthy** and **Hosted**.

umo	o logic			You	r trial ha	s expired	. You are now using a	Free Plan. Upor	ade Plan					Open	Onboarding Tasks -	_	25	% complete
0		Þ	IJ	ń	=	.#	Collection	Source	Preferen	n 📴 Syslog	E Logs	## App Cat	🗃 Search	Votiro	📴 DrillDown F	Security	Account	+ New
	y Opened B	be Ma			Collect	ion	OpenTelemetry	Collection	Status A	rchive								
					Q	Search	h for collectors an	nd sources by nar	ne or sourceCa	itegory					Setuo Wizard.	orade Collectors Adv	Collector Access Key	a Tokena
	OPENED DA				sho		ollectors		show up to: 10 c	ollectors	Erne	nd: All   None				c «	Page: 1 of	
	o - Overview P Votiro - Ove						onectors					NU. AN   MARK				0	(Page ] VI	
	o - Overview				Nan			н	saith	Type Statue	Source Category		Sources Last	Hour N	lessages			1
	o - Overview				• к	ng-HTT	'P-Logs	•	iealthy Ho	isted			1 None			E.	td Source   Edit   Delet	• 0
	o - Overview					ing-http- ITTP	logs		Healthy		prod/votiro/syslog					Regenerate URL 1	Show URL   Edit   Dele	. 0
	Analysis Quic		word		'	TTP												_
Linux	- Login Stat	us																
Linux	- Event Sour	rces																
Арр	Catalog																	- 1
Man	age Data																	
Colle	ection																	
Logs																		
Metr	rics																	
Mon	itoring																	
Adm	inistration																	
Help																		
Boa	Fonkats (Vo	tiro)																

#### **12.1.2** Create the Field Extraction Rules at Ingest Time

When configuring the Votiro App, the Sumo Logic Admin should perform the following procedure to create field extraction rules at ingest time:

- 1. Login to the Sumo Logic tenant.
- 2. Navigate to Manage Data > Logs > Field Extraction Rules.
- 3. In the Rule Name field, enter the value Votiro CEF Syslog Parsing.
- 4. In Applied At, select Ingest Time.
- 5. In Scope, select Specific Data.
- 6. Under Metadata, select \_sourcecategory.
- 7. Under Value, select prod/votiro/syslog.
- 8. Copy the following Sumo Logic Votiro Field Extraction rules:

```
parse regex "companyName=(?<company_name>.*?)\s\w*[=]|$" nodrop
 parse regex "correlationId=(?<correlation_id>.*?)\s\w*[=]|$" nodrop
 parse regex "itemId=(?<item_id>.*?)\s\w*[=]|$" nodrop
parse regex "fileName=(?<file name>.*?)\s\w*[=]|$" nodrop
parse regex "fileType=(?<file_type>.*?)\s\w*[=]|$" nodrop
 parse regex "fileHash=(?<file_hash>.*?)\s\w*[=]|$" nodrop
 parse regex "fileSize=(?<file_size>.*?)\s\w*[=]|$" nodrop
parse regex "passwordProtected=(?<password protected>.*?)\s\w*[=]|$"
nodrop
parse regex "AVResult=(?<av result>.*?)\s\w*[=]|$" nodrop
 parse regex "threatCount=(?<threat count>.*?)\s\w*[=]|$" nodrop
parse regex "blockedCount=(?<blocked_count>.*?)\s\w*[=]|$" nodrop
parse regex "fileModification=(?<file_modification>.*?)\s\w*[=]|$"
nodrop
parse regex "sanitizationResult=(?<sanitization_result>.*?)\s\w*[=]|$"
nodrop
parse regex "sanitizationTime=(?<sanitization_time>.*?)\s\w*[=]|$"
nodrop
| parse regex "connectorType=(?<connector_type>.*?)\s\w*[=]|$" nodrop
| parse regex "connectorName=(?<connector_name>.*?)\s\w*[=]|$" nodrop
 parse regex "connectorId=(?<connector_id>.*?)\s\w*[=]|$" nodrop
 parse regex "policyName=(?<policy_name>.*?)\s\w*[=]|$" nodrop
 parse regex "exceptionId=(?<exception id>.*?)\s\w*[=]|$" nodrop
parse regex "incidentURL=(?<incident_url>.*?)\s\w*[=]|$" nodrop
parse regex "messageId=(?<message_id>.*?)\s\w*[=]|$" nodrop
 parse regex "subject=(?<subject>.*?)\s\w*[=]|$" nodrop
 parse regex "from=(?<from>.*?)\s\w*[=]|$" nodrop
 parse regex "recipients=(?<recipients>.*?)\s\w*[=]|$" nodrop
parse "* CEF:*|*|*|*|*|*|* as syslog_timestamp, cef_version, device_
vendor, device product, device version, signature id, message name,
message_severity, message_extension nodrop
| fields - message_extension, cef_version
```

#### 9. Paste the copied rules into the **Parse Expression** \* field.

sumo logic 🛛 🗧	🕂 🔚 🌲 🛢 Collection	E Logs	+ New		
o * 🖻 🖕	Fields Field Extraction Rules Partitions	Scheduled Views Data Forward	ing		
Recently Opened By Me	Q. Search Field Extraction Rules			+ Add Rule	Add Field Extraction Rule ×
	Status Rule Name	Applied At 🚯 Scope	Created	Last Modified	Save
	🥥 JSON Auto Parsing - All Sources 🔒	Run Time All JSON Logs	By Sumo Logic	By Sumo Logic	Field Extraction Rules automatically extract field(s) from your data source,
<b>2</b> 4					so that you can use them inside your guartes. Learn more Rule Nome Votiro CEF Syslog Parsing
No Recent Items					Applied At  Ingest Time
When you run searches and open dashboards, they'll appear here.					Typeary defect losses data sources to entract frequently used fields in queries. The fields will be entracted and stored when data is necessed by Jamo Logic. Run Timon Use this for JGON box to get the most finality in auto parsing your data. The specifier fields will be entracted during the execution of a search query. Learn more
App Catalog					Scope All Data Metadata Value
Manage Data					_sourcecategory prod/votiro/syslog
Collection					Switch To Advanced
Logs					Parsed template (Optional)
Metrics					Parse Expression *
Monitoring  Administration					<pre>26 27 1 parse "* CEF:*!*!*!*!*!*!* as     pyslog.timestamp.cef.version, device_vendor,     device_product, device_version, signature_id,</pre>
G Help	Fields Capacity No UsageNo fields used				message_name, message_severity,

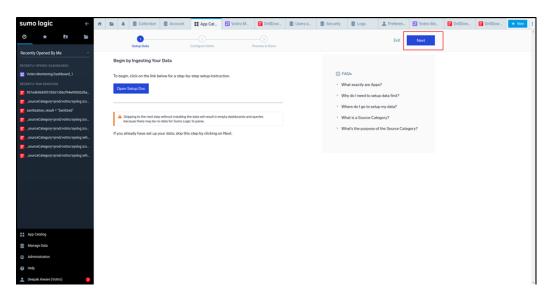
10. Click on the **Save** button.

#### 12.1.3 Install the Votiro App

1. Navigate to the **App Catalog** on the Sumo Logic tenant and search for **Votiro**.

C	Votiro Certified by Sumo Logic by Votiro Documentation
📍 Classic App: You do n	not need administrator nor Manage Apps permissions to install. We're gradually migrating Classic Apps to Next-Gen Apps.
Preview dashboards ind	on sent from Votiro Sanitization engine to Sumo logic customers will allow them better mitigate cyber attacks, do effective threat hunting and enrich cyber security alerts cluded in this app:
	na sa Filipina (kana sa Filipina) Kana sa Kana sa
Votiro - Overview Overview monitoring das analysis of Votiro Sanitiz syslog	

- 2. Click on Install App.
- 3. After configuring the **collector**, **syslog source** and **extraction rules**, click on **Next**.



 Under LOG data source, in the Source Category field, select Enter a Custom Data Filter as you did in the above mentioned steps - use the one that you already created.

5. In the **Custom Data Filter** field, enter the custom source category (starting with the underscore character "\_") you entered when creating the Field Extraction rules. For example: **\_sourceCategory=prod/votiro/syslog** 

sumo logic	*	<b>1</b>	App Cat	Votiro M	DrillDow	Users a	Security	E Logs	🛢 Logs 🔔 Preferen	🛢 Logs 🔹 Preferen 🖪 Votiro Mo	🛢 Logs 🔹 Preferen 🖪 Votiro Mo 📑 DrillDow	E Logs Logs E Preferen. E Votiro Mo DrillDow DrillDow	E Logs Logs Votiro Mo	E Logs & Preferen. E Votiro Mo E DrilDow DrilDow DrilDow E DrilDow
0 * E t			0		0					Exit	Exit Back	Exit Back Next	Exit Back Next	Exit Back Next
Recently Opened By Me			Setup Data		Configure Votiro		Preview & Done				-			
RECENTLY OPENED DASHBOARDS	r	Apps are o when Colli data source	ectors and Sources a ce. Select source cate	tadata associated wi re configured. If you	th your logs, metrics or already have collectors stom data filter and cli	and sources setup ck "Next" to genera	, simply specify the					_	_	_
_sourceCategory*prod/votiro/syslog		LOG data	source Sustom Data Filter		Custom Data		iro/syslog							
sourceCategory=prod/votiro/syslog		Critici a c				ategory=prod/logs								
sourceCategory=prod/votiro/syslog	۲ I	Folder Na	me					_	_					
sourceCategory=prod/votiro/syslog		Votiro												
_sourceCategory*prod/votiro/syslog 957ed69669f318261356cf94e95002d5a		۹												
sourceCategory=prod/votiro/syslog joo		All Fo	olders											
sanitization_result = 'Sanitized'		Name			Description									
_sourceCategory+prod/votiro/syslog.jco		2 Per	sonal		My saved searc	hes and dashboard	25							
App Catalog														
Manage Data														
Administration														
0 HHp														
Leepak Alware (Votiro)														

6. Click on **Next**. The Setup completes and a Success message appears and a dashboard is displayed.

sun	no logic		÷	<b>a</b> 4	Collection	Account	# App Cat	E Votiro M	DrillDow	Users a	Security	E Logs	2 Preferen	E Votiro Mo	DrillDow	DrillDow	+ New E
Ø	*	b	n.		Setup Data		Configure Votiro		3 Preview & Done				Exit	Back			
Rece	ntly Opened B	ly Me															
RECEN				~	Success! Open one	of the dashboar	ds below to start e	ploring your data,	or go to My Conte	nt Library.							
11 V	tiro Monitoring	Dashboard_1															
RECEN																	
<b>2</b> 95	7ed69669f318;	261356cf94e950	002d5a		r Marine I I I I I I I I I I I I I I I I I I I	-											
<b>-</b>	ourceCategory=	prod/votiro/sys	ilog (co		95,963 10,611 24	497 4718	22,678 4,221										
<b>2</b> 54	nitization_resul	t = "Sanitized"					1										
_		prod/votiro/sys				dan s	and bill										
		prod/votiro/sys															
		prod/votiro/sys															
		prod/votiro/sys		10.0	ro - Overview												
	ourcecanegory*	rprod/votiro/sys	iog jan	Ove	rview monitoring dasht tization engine syslog	oard for analysis of	Votiro Open										
11 A	pp Catalog																
8 1	lanage Data			0	We are checking the	it Sumo Logic ca	an access your data	. You do not have	to keep this page o	ipen.							
φ 4	dministration																
0 H	elp				ecommended												
<u> </u>	eepak Alware (\	viotino)		As	a Votiro user, you m	ight benefit from	using these other i	ntegrations. Click t	he tile below to get	started.							
N	otifications																
	references																
s	ign Out																

#### 12.1.4 Integrate the Votiro Management Console with the Sumo Logic HTTP Logs Collector

- 1. Log in to the Votiro Management Dashboard.
- 2. Go to the **Settings > SIEM** page.
- 3. Set up the Sumo Logic collector information:
  - a. For **SIEM Server address**, enter the collector HTTP source URL.
  - b. For **SIEM server port**, enter the default HTTPS port number **443**.
  - c. For Syslog protocol, select HTTP Logs (Sumo Logic).
  - d. For **Syslog format**, select **CEF** (for this method, this field is not relevant).
  - e. Save the SIEM settings.



C		SIEM	
88 ©	System Setup System Configuration	SIEM Server address Type in your organization SIEM server address	P/Hothame     https://collectors.de.sumologic.com/rece
	SMTP SAML Local Users	SIEM Server port Type in your organization SIEM server port	+ Post 
0	SIEM Service Tokens Certificates License	Sysiog Protocol Select sysiog protocol	+ Protect HTTP Logs (Sumo Logic)
	Policies	Syslog Format Select syslog format	• format CEF V
		TLS Certificate Upload a certificate in order to use TLS protocol	Import

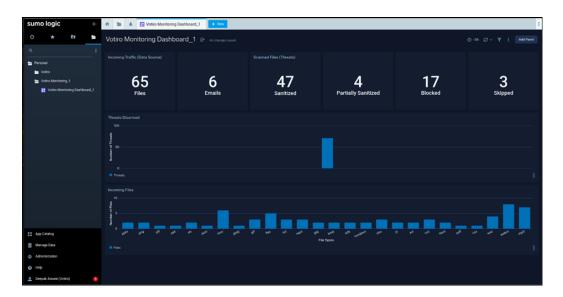
#### **12.1.5** Verify the Integration

To check if the integration was successful:

- 1. Send files to sanitization.
- 2. Open a Sumo Logic instance.
- 3. There are two ways to check syslog events:
  - a. Votiro Dashboard
  - b. Logs search

#### **3.a Votiro Dashboard**

On the Sumo Logic website, open the newly imported folder **Votiro Monitoring Dashboard**. Data coming from the configured source should be shown on this dashboard.



### **3.b Search Ingested Data inside Sumo Logic**

Data ingested inside Sumo Logic can be easily searched using the source category by which the data was indexed.

- 1. Login to the tenant.
- 2. Click + New -> Log Search.

sumo lo	ogic ≡	* =	+ New	
Home	Learn	Certificati	ol 🗐 Log Search	alt+s
			Metrics	alt+m

- In the search field, enter: \_source={source name} and \_collector={collector name} For example: \_source="HTTP-Test" and \_collector="HTTP-Test"
- 4. Set the time and date fields.

sumo logic 🛛 🗧 🤶	Your triat has expired. You are now using a Free Plan. Libograde Plan. 2004										2	25% complete 🛛 💥	
0 * 19 1	ff 🖿 🔺 🗏 🕬	ection 📴 Source	Source	2 Preferen	冒 Syslog	E Logs	# App Cat	📴 Search	Votiro	DrillDown F	Security	+ Nov	
Recently Opened By Me	📴 🕐 1 _source="H	TP-Test' and _collect	r="HTTP-Test"							⊙ -30d	۵ ۵	0.0	
🔛 Votiro - Overview	50			_								- 50 e DEBUG e «OTHERS	
HTTP Votiro - Overview	Jul 7, Jul 1	0 Jul 13	Jul 1	6 Jul 1	0	Jui 22	Jul 25	Jul 28	Jul 31	Aug 3,		a company	
Votiro - Overview	07/07/2023 10:31:14 AM +0	100	STATUS Done	gathering results ELAPS	ED TIME 00:00:10	RESULTS 49	SESSION 2CAFO	BCB3EDDFDA4 LOAD		06/04/2023	10.31:14 AM +0300		
Votiro - Overview	Messages								di b	ide Histogram 🚿 H	ide Log Levels 💡	Maximize V	
Votiro - Overview	Q. Search	< « <	Page: 1 of	4 > >> LogRe	luce LogCo	mpare 🗸					Expan	d/Collapse 4	
Log Analysis QuickStart - Keyword	G, OPAICH	# Time	6	Message D									
Linux - Login Status	Displayed Fields		/01/2023		2021-08-01 11:51:08-00 +00:00 (Orboy) (GF:0)Totiro(Voiro cloud)1.0.0.01500(Sastization summary11) companyNamerLoid VA 17D correlated=01005551-08-0-07-04-08-07-05257650e ited=04048172a-62b-071-0402-0520110827 (Labomercu-tra-Li file)pue=Cencetable Elaboma-05372155480(5)75702042152051754247420817454204248504051744620354 (Labomercu-tra-Li file)pue=Cencetable Use								
Linux - Event Sources		2.57	30,089 PM +0300	fileHesh-350									
App Catalog	Time  Message #			connectorNam	threatCount=1 blockedCount=1 fileModification=File samitized samitizationResult=Blocked samitizationTime=173.9148 connectorType=None connectorName=Self=samitization connectorId=00000000-0000-0000-00000000000 policyMame=Ehud msceptionId=null								
				incidentUBL=https://ehud-ws/app/fileDetails/1065507a-4be8-474d-88a1-f8e2537458be/b9481f2a-6e2b-421b-a902-67cd21186e27 messageId=null wsbject=null from=null recipients=null									
Manage Data	Hidden Fields			Host:62.219	Host:62.219.37.66 w Name:Votiro w Category:Hitp Input w								
Collection	Collector		01/2023 1:30.089 PM +0300		2023-08-01 11:52:58.009 +00:00 [Debug] CEF:0 Votiro Votiro cloud 1.0.0.0 500 Sanitization summary 1  companyName-Ehud VA LTD correlation[d:000907a-dbed-4746-88a1-f8e253745000 iten/duesa4194c-b6/d-4756-8528-15994500:000 f12eMase1133722,_creen-peas-pea-pod-								
Loga	_loglevel #	2		<pre>table_p.pg fileType.JPEG fileMashie257760276367616775676308e37769576106270108400404378044679103 fileMashie277411 passmerdProtected=false ANNex1LMst Used threatCourt=0 fileMashie1 fileMashie267606176367647781</pre>									
	Size #			removed samitizationResult=Samitized samitizationTime=383.8584 connectorType=None connectorName=Self-samitizatio connectorId=08000000-0000-0000-0000-00000000000 policyName=Dod exceptionId=null incidentUR.=https://ebod-									
Metrics	Source a	1.1	va/app/fileDetails/1009507a-4be0-474d-80a1-f6e2537450b/eaa4394d-b6fd-475d-a528-1593450dc900 messageId=null subject=null rectingt=renull								ubject=null from	e=null	
Monitoring	Source Category	1.1				:Votire - Categ	ory:Http Input -						
Administration	Source Host #	3 3 68/6	1/2023	2023-08-01	SD-Feeder (11) [3:488-4684 [bbs] [20] STATISTICS (204)]. 8.4.8 [MM] Institution search]: competition search [3:50] Statistics (204)]. 8.4.8 [MM] Institution search]: competition (204) [20] Statistics (204)]. Statistics (204)]								
	Source Name a	2 253	30.089 PM +0300										
O Help	Index a	1											
Ron Fonkats (Votiro)	av_resuit #	1 w		connectorId	00000000-0000	-0000-0008-0000	BBBBBBBB policyNam		Idenull incident	URL=https://ehud-			

### 13 How to Integrate Votiro Cloud with Google Workspace

In this tutorial, you'll learn how to integrate Votiro Cloudusing with Google Workspace (formerly G Suite).

### 13.1 Procedure

- 1. Sign in to the <u>Google Admin console</u> with your Google Workspace account.
- 2. In the left pane, navigate to Apps > Google Workspace > Gmail

	=	Google Admin
		Home
		Dashboard
•	°	Directory
•	61	Devices
E		Apps
		Overview
	Ŀ	Google Workspace
		Service status:
		Calendar 2
		Cloud Search
		Currents
	_	Drive and Docs 3
		Gmail

3. On the Settings for Gmail page, scroll down and select Spam, phishing, and malware



4. Move the cursor over **Inbound gateway** and click the pencil button to edit the settings:

Inbound gateway	If you use email gateways to route incoming email, please enter them here to improve spam handling Learn more	
	C Enable	
	1. Gateway IPs	
	IP addresses / ranges	
		ADD
	✓ Automatically detect external IP (recommended)	
	Reject all mail not from gateway IPs	
	Require TLS for connections from the email gateways listed above	
	2. Message Tagging	
	Message is considered spam if the following header regexp matches	
	Most changes take effect in a few minutes. Learn more You can view prior changes in the Audit log	
	CANCEL	L SAVE

- 5. Enter the IP address provided by Votiro.
- 6. Verify that the following boxes are checked:
  - Automatically detect external IP (recommended)
  - Require TLS for connections from the email gateways listed above
- 7. Click **SAVE**.

#### **13.1.1** Create a Host

8. Navigate back to **Settings for Gmail** and select **Hosts**.

Hosts	~
Add mail hosts for use in advanced routing, for example to direct messages to Microsoft Exchange.	

#### 9. Click Add route.

- a. Type a name, for example: "Workspace to Votiro Cloud".
- b. Select **Single host** and type the host name provided by Votiro.
- c. Check Require mail to be transmitted via secure (TLS) connection (Recommended).
- d. Check Require CA signed Certificate (Recommended).
- e. Check Validate certificate hostname (Recommended).
- f. Click **SAVE**.

Edit mail route	
Name	Learn more
Workspace to Votiro Cloud	
This field is required.	
1. Specify email server	
Only ports numbered 25, 587, and 1024 through 65535 are allowed.	
Single host 🔍	
: 25	
2. Options	
Perform MX lookup on host	
Require mail to be transmitted via a secure (TLS) connection (Recommer	ided)
Require CA signed certificate (Recommended)	
Validate certificate hostname (Recommended)	
Test TLS connection	

CANCEL SAVE

### 13.1.2 Configure content compliance rule for emails received from Votiro Cloud

10. Return to Settings for Gmail and select Compliance:

Compliance	~
Configure compliance features	

11. Under Content compliance, select CONFIGURE.

Content compliance	Configure advanced content filters based on words, phrases or patterns.	CONFIGURE

- a. Specify a name, for example "Votiro Cloud to Workspace"
- b. For Email messages to affect, check Inbound.
- c. For Add expressions that describe the content you want to search for in each message, select If ANY of the following match the message and click ADD.

Edit setting		
Content compliance		He
Zip file attached to email Edit		
1. Email messages to affect		
✓ Inbound		
Outbound		
Internal - sending		
Internal - receiving		
2. Add expressions that describe the content you want to search for in each message		
If ANY of the following match the message $\neg$		
Expressions	ADD	
	CANCEL	S

- d. Select Metadata match, Attribute, Source IP and Match type.
- e. Select **Source IP is within the following range** and enter the IP address provided by Votiro.
- f. Click SAVE.

Edit setting	
Metadata match 👻	
Attribute	
Source IP	
Match type	
Source IP is within the following range	

CANCEL SAVE

- g. Add another expression, select Advanced content match, Location, Full headers, Match type, Contains text.
- h. In **Content**, enter "X-MTConnectorResult".
- i. Click SAVE.

- 124	
Fait	setting
	Setting

Advanced content match 💌	
Location Full headers	
Match type Contains text	
Content	
X-MTConnectorResult	

CANCEL SAVE

- j. For 3 If the above expressions match, do the following: Under **Route** select **Change route** and make sure **Normal routing** is selected.
- k. Under Encryption, check Require secure transport (TLS).
- I. Click **Show options**.
  - i. Under Account types to affect, check the following boxes:
    - Users
    - Groups
    - Unrecognized / Catch-all
  - ii. Click SAVE.

Hide options A. Address lists
Use address lists to bypass or control application of this setting
O Bypass this setting for specific addresses / domains
Only apply this setting for specific addresses / domains
B. Account types to affect
Vsers
Groups
✓ Unrecognized / Catch-all
C. Envelope filter
Only affect specific envelope senders
Only affect specific envelope recipients

CANCEL SAVE

### 13.1.3 Configure Content compliance rule for emails sent to Votiro Cloud

- 12. By now, you should have one rule enabled for Content compliance. Click on **ADD ANOTHER RULE** for traffic sent from Google Workspace to Votiro.
  - a. Specify a name, for example "Workspace to Votiro Cloud".
  - b. Under Email messages to affect, check Inbound.
  - c. For Add expressions that describe the content you want to search for in each message, select If ALL of the following match the message and click ADD,
    - i. Select Metadata match, Attribute, Source IP and Match type.
    - ii. Select **Source IP is not within the following range** and enter the IP address provided by Votiro.
    - iii. Click SAVE.

2. Add expressions that describe the content you want to search for in each message

If ALL of the following match the message 💌

Expressions	
Metadata match: Source IP is not within the range Teacher and	Edit
	ADD

- d. For 3 If the above expressions match, do the following: Under **Route**, select **Change route** and make sure "Workspace to Votiro Cloud" is selected.
- e. Under Encryption, check Require secure transport (TLS).
- f. Click Show options.
  - i. Under Account types to affect, check the following boxes:
    - Users
    - Groups
    - Unrecognized / Catch-all
  - ii. Click SAVE

**Note**: It can take a while for the changes to be applied.

- 13. After the rules are successfully configured:
  - a. Send a test email.
  - b. Under Reporting > Email Log Search, see if the message was routed through Votiro's Cloud instance.
  - c. Verify you're able to see the sanitized email in Votiro's dashboard.

### 14 How to Integrate Votiro Cloud with Sumo Logic

In this tutorial, you'll learn how to integrate Votiro Cloud with Sumo Logic.

### 14.1 System Requirements

The specifications listed below are for installation of "installed collector" for sending data to the Sumo Logic server.

- Linux, major distributions 64-bit, or any generic Unix capable of running Java 1.8
- Single core, 512MB RAM
- 8GB disk space
- Package installers require TLS 1.2 or higher

### 14.2 Procedure

### **14.2.1** Configure the Sumo Logic Syslog Collection

- 1. In Sumo Logic select Manage Data > Collection > Collection.
- 2. Click on **Setup Wizard**.

sumo logic $\leftarrow$	E Collection	
0 ★ 🖻 🖿	Collection Status Ingest Budgets	
۹ :	Q Search for collectors and sources by name or sourceCategory	Seture Wizard Augerade Collectors Add Collector Access Keys
ADMIN RECOMMENDED	Show: All Collectors V Show up to: 10 collectors V Ex	pand: All   <u>None</u> C < Page: 1 of 20 > >>
<ul> <li>Active Directory</li> <li>Akamai Cloud Monitor</li> </ul>	CP_Halo_Metrics_Collector  HTTP halo/metrics	Regenerate URL   Show URL   Edit   Delete 🚯
Amazon CloudFront	CP_Halo_Workload_Security_Events_C	//security/events Regenerate UBL   Show UBL   Edit   Delete 🚯
Amazon DynamoDB	demo Semo	Begenerate UBL i Show UBL i Edit i Delete 🕚
Amazon GuardDuty	ECS Cloudtrail	Regenerate URL   Show URL   Edit   Relete 🌒
Amazon Kinesis - Streams	ECS Metrics AWS CloudWatch Metrics	Pause   Edit   Delste 🚯
Amazon Redshift ULM	flow event test Silverent_test	Regenerate URL   Show URL   Edit   Delete 🌒
App Catalog	GCP Firewall Coople Cloud Logs Cp/firewall	Regenerate URL   Show URL   Edit   Delete 🌒
🛢 Manage Data	GCP Loggen Cogen/gcp HTTP S loggen/gcp	Regenerate URL   Show URL   Edit   Delete 🚯
Collection	Github S github	Regenerate URL   Show URL   Edit   Delete 🚯
Settings	Kafka Metrics 🔗 kafka/metrics	Regenerate URL   Show URL   Edit   Delete 🚯
Administration	HTTP Kubernetes Logs Ø kubes	Regenerate URL   Show URL   Edit   Delete 🚯
😮 Help	HTTP okta Ø okta	Regenerate URL   Show URL   Edit   Delete 🌒

3. Click on Integrate with Sumo Logic.

sumo logic



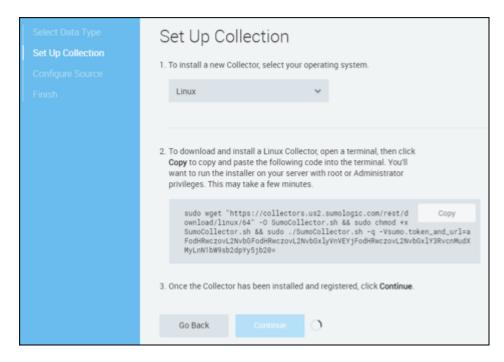
4. Under Select Data Type, select All other sources.

sumologic	
Select Data Type Set Up Collection	Select Data Type
Configure Source Finish	Your Custom App
	AWS Elastic Load Balancing     Cisco ASA     Linux System     Mac OS System     MySQL
	NG:IXX Nginx Palo Alto Networks Varnish Varnish Windows Event Windows IIS
	Windows Performance Sources
	Go Back

5. Under Set Up Collection, select Syslog.

sumo logic				
Select Data Type Set Up Collection Configure Source	Set Up Co		ır logs?	
Finish		<u>_</u>	https://	gggaphite
	Local File	Syslog	HTTPS Source	Graphite- Formatted Metrics
	Back			

- 6. Under Set Up Collection:
  - a. In step 1. To install a new Collector..., select Linux.
  - b. In step **2. To download and install a Linux Collector,...** click **Copy** to copy the code, then paste it into the Linux terminal and run it in your Linux server as root or Administrator.
  - c. In step **3. Once the Collector has been installed and registered**, click **Continue**.



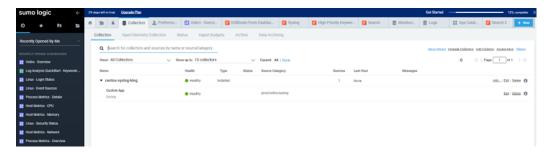
- 7. Under **Configure Source**:
  - a. In **1. Enter a Source Category...** field, type the value: **prod/votiro/syslog**.
  - b. In 2. Select the protocol..., select TCP.
  - c. In **3. Enter the port...**, type the value **1514**.
  - d. In **4. Select a time zone...**, select **UTC**.

e.	Click on <b>Next</b> .	
sumo	logic	
	Select Data Type Set Up Collection	Configure Source: Your Custom App
1	Configure Source	1. Enter a Source Category that will help you find your metrics later.
	Finish	Source Category 🕐 prod/votiro/syslog
		2. Select the protocol where your syslog messages are streaming. UDP TCP
		3. Enter the port where your syslog messages are streaming. (3)
		4. Select a time zone for your log file.
		Use time zone from log file. If none present use:
		(UTC) Etc/UTC 🗸
		Ignore time zone from log file and instead use: (UTC) Etc/UTC ~
		Back Next

8. Under **Finish**, the Setup Wizard displays the progress bar while performing the installation. Wait until the installation finishes. This may take some time.

sumo logic	
Select Data Type Set Up Collection Configure Source Finish	Finish This process usually takes a few minutes to finish, but it could take up to 15 minutes depending on the size of your dataset. In the meantime, you can add more data.
	Tightening the sockets

9. If the installation was successful, the Installed Collector shows up in the **Collection** console as **Healthy** and **Installed**.



### 14.2.2 Create the Field Extraction Rules at Ingest Time

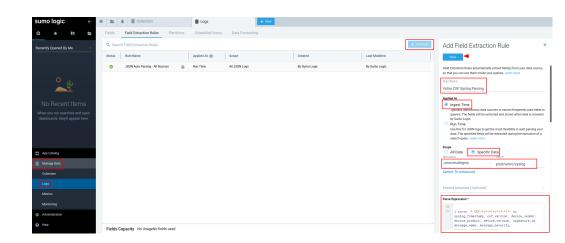
When configuring the Votiro App, the Sumo Logic Admin should perform the following procedure to create field extraction rules at ingest time:

- 1. Login to the Sumo Logic tenant.
- 2. Navigate to Manage Data > Logs > Field Extraction Rules.
- 3. In the Rule Name field, enter the value Votiro CEF Syslog Parsing.
- 4. In Applied At, select Ingest Time.
- 5. In Scope, select Specific Data.
- 6. Under **Metadata**, select **\_sourcecategory**.
- 7. Under Value, select prod/votiro/syslog.
- 8. Copy the following Sumo Logic Votiro Field Extraction rules:

```
parse regex "companyName=(?<company_name>.*?)\s\w*[=]|$" nodrop
 parse regex "correlationId=(?<correlation_id>.*?)\s\w*[=]|$" nodrop
 parse regex "itemId=(?<item_id>.*?)\s\w*[=]|$" nodrop
 parse regex "fileName=(?<file_name>.*?)\s\w*[=]|$" nodrop
 parse regex "fileType=(?<file_type>.*?)\s\w*[=]|$" nodrop
 parse regex "fileHash=(?<file_hash>.*?)\s\w*[=]|$" nodrop
 parse regex "fileSize=(?<file_size>.*?)\s\w*[=]|$" nodrop
parse regex "passwordProtected=(?<password_protected>.*?)\s\w*[=]|$"
nodrop
parse regex "AVResult=(?<av_result>.*?)\s\w*[=]|$" nodrop
 parse regex "threatCount=(?<threat count>.*?)\s\w*[=]|$" nodrop
 parse regex "blockedCount=(?<blocked_count>.*?)\s\w*[=]|$" nodrop
parse regex "fileModification=(?<file_modification>.*?)\s\w*[=]|$"
nodrop
| parse regex "sanitizationResult=(?<sanitization_result>.*?)\s\w*[=]|$"
nodrop
parse regex "sanitizationTime=(?<sanitization_time>.*?)\s\w*[=]|$"
nodrop
parse regex "connectorType=(?<connector_type>.*?)\s\w*[=]|$" nodrop
 parse regex "connectorName=(?<connector_name>.*?)\s\w*[=]|$" nodrop
parse regex "connectorId=(?<connector_id>.*?)\s\w*[=]|$" nodrop
 parse regex "policyName=(?<policy_name>.*?)\s\w*[=]|$" nodrop
 parse regex "exceptionId=(?<exception_id>.*?)\s\w*[=]|$" nodrop
 parse regex "incidentURL=(?<incident_url>.*?)\s\w*[=]|$" nodrop
 parse regex "messageId=(?<message_id>.*?)\s\w*[=]|$" nodrop
 parse regex "subject=(?<subject>.*?)\s\w*[=]|$" nodrop
 parse regex "from=(?<from>.*?)\s\w*[=]|$" nodrop
```

```
| parse regex "recipients=(?<recipients>.*?)\s\w*[=]|$" nodrop
| parse "* CEF:*|*|*|*|*|*|*" as syslog_timestamp, cef_version, device_
vendor, device_product, device_version, signature_id, message_name,
message_severity, message_extension nodrop
| fields - message_extension, cef_version
```

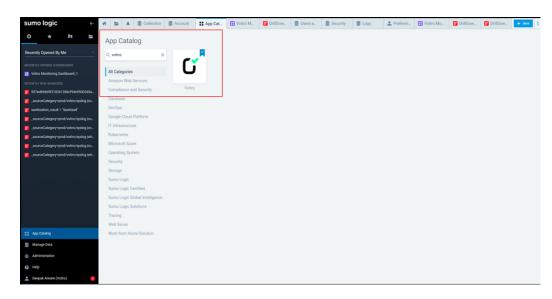
9. Paste the copied rules into the **Parse Expression** \* field.



10. Click on the **Save** button.

### 14.2.3 Install the Votiro App

1. Navigate to the **App Catalog** on the Sumo Logic tenant and search for **Votiro**.



2. Click on Add Integration.

Sumo logic - A 🖆 🛦 🗄 Uvitro Monitoring Deshboard, 1 👬 App Catalog	1
O * E · Back to App Catalog	
Q 1	
Percoal     Vote     Vote	
22 varie Montoring Castroame, 3 Add Intergration	
Coverview Coverview	
Threat related information sent from Votiro Sambization engine to Sumo logic customers will allow them better miligate cyber attacks, do effective threat hunting and enrich cyber security alerts	
Dashboard Preview	
Dashboard Preview	
Volte - Ownitee	
App Catalog Overview monthing database for analysis of Vitro Sandhare regime spring	
Manga bata	
Admentation	
0 Heb	
▲ DeepA Awar (Vdr2)	

3. Click on **Open Setup Doc**. This will take you to the documentation on the Sumo Logic Github page.

sumo logic	A 🖆 🛦 🗄 Votiro Monitoring Dashboard_1 👬 App Catalog 🔸 New	
0 * E <b>=</b>	O     Senigraduat     Configure Voltro     Preview A Dare	Exit Next
Image: Control of Contro of Contro of Contro of Control of Control of Control of Control	Begin by Ingesting Your Data The basis cities on the look begins for a step-by-rise setup instruction.	<ul> <li>FACM</li> <li>Nutrated and Appendix</li> <li>Wind on lowed to active data first?</li> <li>Wind on a Source Category?</li> <li>Wind is the purpose of the Source Category?</li> </ul>

4. After configuring the **collector**, **syslog source** and **extraction rules** with the help of the Setup Doc, click on **Next**.

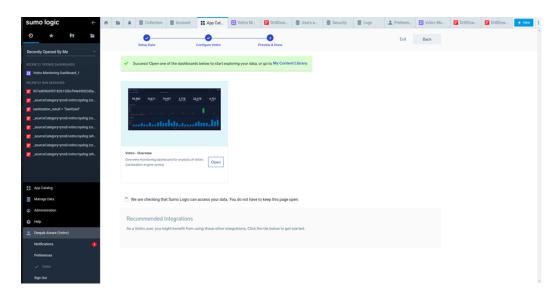
	a la sia																
sun	io logic		¢	 5 A	Collection	Account	App Cat	Votiro M	DrillDow	Users a	Security	E Logs	2 Preferen	Votiro Mo	DrillDow	DrillDow	+ New I
0	*	a	1		1 Setup Data		2 Configure Votiro		3 Preview & Done				Exit	Next			
Recen	tly Opened By	Me	<u> </u>	Decis													
				Begin	by Ingesting You	r Data											
🔢 Və	tiro Monitoring D	ashboard_1		To begi	n, click on the link b	elow for a step-b	y-step setup instru	ction.			🗘 FA	iQs					
				Open	Setup Doc						<ul> <li>Wh</li> </ul>	hat exactly are Ap	ps?				
	7ed69669f31826										> WE	ty do I need to set	tup data first?				
	ourceCategory=p		og ico								> we	here do I go to set	up my data?				
	vitization_result			A S	ipping to the next step	p without installing t	he data will result in e	mpty dashboards and	queries		· we	hat is a Source Ca	teoory?				
	kurceCategory*p kurceCategory*p			be	cause there may be n	o data for Sumo Log	ic to parse.						of the Source Cate				
	xirceCategory=p		-	If you al	ready have set up y	your data, skip thi	s step by clicking o	n Next.				ats the purpose	or the aburde call	igory:			
	urceCategory=p		-														
	urceCategory*p																
:: A	o Catalog																
	anage Data																
	ministration																
0 H	\$																
<b>2</b> 0	epak Alware (Vo	itiro)	8														

 Under LOG data source, in the Source Category field, select Enter a Custom Data Filter as you did in the above mentioned steps - use the one that you already created.

6. In the **Custom Data Filter** field, enter the custom source category (starting with the underscore character "\_") you entered when creating the Field Extraction rules. For example: **\_sourceCategory=prod/votiro/syslog** 

sun	no logic		÷	*	5 A	# App Cat	Votiro M	DrillDow	Users a	Security	E Logs	ELogs Logs	🛢 Logs 😩 Preferen 🚯 Votiro Mo	E Logs Logs Preferen E Votiro Mo	E Logs Logs E Preferen. E Votiro Mo DrillDow DrillDow	E Logs Preferen E Votiro Mo E DrillDow DrillDow	🛢 Logs 😩 Preferen 🚯 Votiro Mo 🔂 DrillDow 🔂 DrillDow 🔂 DrillDow
Ø		b				0		0					Exit	Exit Back	Exit Back Next	Fuit Back Next	Exit Back Next
Deces	ntly Opened By	Ma	J.			Setup Data		Configure Votiro		Preview & Done							
RECEIN We RECEIN RECEIN	TLY OPENED DASH the Monitoring D TLY RUN SEARCHE ourceCategory*pr ourceCategory*pr ourceCategory*pr	BOARDS ashboard_1 5 rod/votiro/syslo rod/votiro/syslo rod/votiro/syslo rod/votiro/syslo	9 9 9		Apps are when Col data sour LOG data	lectors and Sources roe. Select source cat a source Custom Data Filte	etadata associated wi are configured. If you i legory metadata or cu		and sources setup, A "Next" to genera	simply specify the te the App.							
	ourceCategory*p		-		۹												
	7ed69669f31826 ourceCategory=pr				All F	olders											
	nitization_result =				Name			Description									
	ourceCategory*pr	od/votiro/syslo	g (co		2. Pe	rsonal		My saved searc	hes and dashboard	6							
:: ^	pp Catalog																
•	lanage Data																
φ 4	dministration																
0 н	elp																
<u>*</u> 0	eepak Alware (Vo	tiro)	3														

7. Click on **Next**. The Setup completes, a Success message appears and a dashboard is displayed.

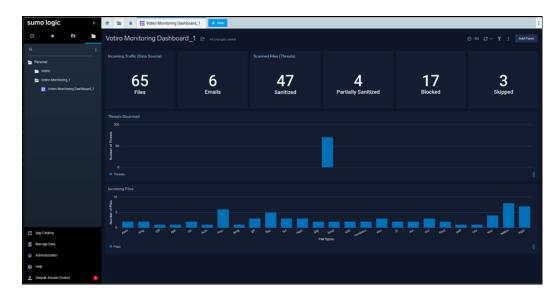


### 14.2.4 Integrate Votiro Management Console with Sumo Logic Syslog Collector

- 1. Log in to the Votiro Management Dashboard.
- 2. Go to the **Settings > SIEM** page.
- 3. Set up the Linux server Sumo Logic collector information.

C		SIEM	
88 ©	System Setup System Configuration	SIEM Server address Type in your organization SIEM server address	* 17/Hodhame 10/30/136
<u>ه</u>	Active Directory SMTP SAML	SIEM Server port Type in your organization SIEM server port	+ Pot 1514
2	Users SIEM Service Tokens Certificates	Syslog Protocol Select syslog protocol	• Protocol TCP V
	License Policies	Syslog Format Select syslog format	• funat CEF V
		TLS Certificate Upload a certificate in order to use TLS protocol	Import
<b>AD</b> 9.9.83			

4. On the Sumo Logic website, open the newly imported folder **Votiro Monitoring Dashboard**. Data coming from the configured source should be shown on this dashboard.



### 14.2.5 Search Ingested Data inside Sumo Logic

Data ingested inside Sumo Logic can be easily searched using the source category by which the data was indexed.

- 1. Login to the tenant.
- 2. Click + New -> Log Search.

sumo lo	ogic ≡	* 3	= + Ne	ew		
Home	Learn	Certific	catio 冒	Log Search	alt+s	
				Metrics	alt+m	

- 3. In the search field, enter: \_sourceCategory=prod/votiro/syslog
- 4. Set the time and date fields.

**Note**: If the table is not available by default, then select all the fields on the left side and click on **Save** before **Displayed Fields**, for persistence.

0 1 _tourceCategoryz					_					
19 1 sourcecategory.p	prod/#01110/1	NaTob							UND C UP	-
000										
12:00 AM		12:00 AM	12:00 AM	12:00.7			DD AM	12:00 AM	12:00 AM	
25/05/2022 5:33:07 PM +0530			STATUS Done	pethering results ELAPSED TIME 00:00:01 RE	SULTS 94,405 SESSION 10	BEDECASOSAEADCB	L04D: • • •		01/06/2022 5 33/07 PM +0530	
essages									Switch to New Table	•
Search		K 🔍 C Page: 1 of 305	S > >> LogReduce	LogCompare ~						
		ion_time D_ signature_id D	Size 👌 Source 🖒	Source Category 🗅 Source Host 🖒	Source Name 🖒 🛛 🛪	ubject 🖒	syslog_timestamp 🗅 threat_count 🗅	Message 🗅		
Time  Time  Collector a Source a Source Category a Source Host a	1	1900919	1,127 Votire Syslog Source	prod/votiru/sysing deepak- VirtualBex	0 8	han indicate lao particular	May 27 13:28:47 6	<pre>summary[5]compare #2eb-G01950%003 fileNumerasek.pp fileNumerasek.pp fileNumerasek.pp fileSizer3 passe blockedCount-0 f office supploin mentificationTime enail connector </pre>	<pre>6c03209904550cc046cbg2770099540397cc01956540900 entrystester/air/air/air/air/air/air/air/air/air/ai</pre>	487) (255 1 fmu2
Source Name # ar_issuit # blocked_count # company_name # connector_id # connector_iname # connector_iname # connector_iname #	1 3 6 1 2 2 2 10071	10200210	3,019 Vettre Syslog Source	prod/votiru/sysing deepak- VirtualBex	e h	hat health xecutive feor old wolk sentern record wold	Rey 27 13:21:47 3	summary Sicompar atom-Resp755557 fileNome-compre- fileNime-compre- fileNime-compre- blockedCourt-3 4 Relation_Empty connectorId=da1 policy_exceptio 	CT dipersiparties (and 14.3.40)(NMMMP)[builted) Manuscriptical (and 14.3.40)(NMMMP)[builted) Manuscriptical (and 14.3.40)(NMMMP)[builted) Manuscriptical (And 14.3.40)(NMMMP)[builted] Manuscriptical (And 14.3.40)(NMMP)[builted] Manuscriptical (And 14.3.40)(NMMP)[builted]	4e71 4737 481. 481. 481. 471.4
device_product = device_vendor = device_vension = exception_id =	1 1 1 328	10000010	827 Votiro Symlog Source	prod/votiro/syslog deepak- Virtual@ox	syslog n	ull	May 27 13:28:07 1	summary 5 compar 8924-Deb07eccess fileNome-be.mp3 fileNome-be.mp3 fileNome-be.mp3 fileNome-be.mp3	CEF.8 Votire Votire cloud 9.6.348 1NB0ND18 Santtiza Water+VotireSublator correlation(5-aa)79508-b102-4 1 tendf=wa179508-b102-428-0292-40487-corea fileType=wa3 (5574404ca31x444054d73abs1922/w28082644441616a1c33 47 passacdFrotected-false AVMesult-Clean threatOou 148605ffcation-Cleaned Breach path macro lak	4924 5852

### 14.2.6 Event Simulator

For testing purposes Votiro has an Event Simulator for Votiro Syslog (CEF).

#### **Prerequisites**

- Event Simulator contact Votiro support to obtain the Event Simulator code.
- Python 3.8 or higher
- pipenv (https://pypi.org/project/pipenv/) installed on the system where you want to run the simulator. To install pipenv, run the command:

pipenv install



### Using the simulator

- 1. Navigate to the **src/** folder.
- 2. Generate events using the following command:

```
pipenv run python3 simulate.py --ip=<target_ip> --
port=<target port>
```

The <target\_port> and <target\_ip> should be of the target machine for which the Configuration was done. For example:

pipenv run python3 simulate.py --ip=localhost --port=1514

### **15 Performing a Health Check**

To run a health check on your installation, navigate to the **/root** folder and use the following command:

#./healthcheck

The expected results are:

- All pods are running with no issues.
- The Redis cluster is running with no issues.
- Elastic pods are running with no issues.
- Disk speeds are at the required rates.

If you experience unexpected results, please see the Troubleshooting Playbook.

### 16 How to Send Files to Votiro via Postman

Postman is an API platform for developers to design, build, test and iterate their APIs. It is an HTTP client that tests HTTP requests, utilizing a graphical user interface, through which different types of responses are returned that need to be subsequently validated. This article describes how to use Postman with Votiro.

### **16.1 Prerequisites**

Install Postman by downloading one of the following:

- The Postman app from <u>Download Postman</u>.
- The Postman portable app from Postman<sup>™</sup> portable.

### **16.2 Procedure**

#### 16.2.1 Generating a Service Token

1. Generate a Service Token. Go to Settings > Service Tokens > Create New :

ũ		Service Tokens A list of service toke	ens which allows other services to communicate with Votiro	products	+ Create N
88	System Setup System Configuration	ID	b8cbfb6e-01cb-46aa-a5d0-54931893fe08	ID	2ccc5120-eee7-4852-bfee-4c671af024a
Ø	Active Directory	Issued To	WinCurl	Issued To	swagger-i
Ø	SMTP	Created At	04/03/2022 22:21	Created At	07/03/2022 16:4
$\bigcirc$	Users	Expiration	17/03/2023	Expiration	31/03/202
Ø	SIEM		Revoke		Revok
Ľ	Service Tokens				
	License Policies	ID	4b200f23-8a40-42da-900a-a1da93136fd1		
		Issued To	swagger token		
		Created At	18/03/2022 13:22		
		Expiration	16/03/2023		
			Revoke		

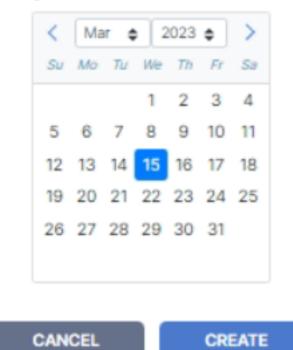
2. Create a name for the new token, set an expiration date and press **CREATE**:

### Create New Service Token

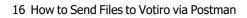
Issued To

Test-Token

Set Expiration Time



3. Copy and save the token string that appears on this page.



WARNING!



#### Save the token string. This page will only appear once.

#### Please Save Your Token, You Won't Be Able To See It Again

ID	ff5e09af-0867-4514-bfed-4186e86ef2fe
Issued To	Test-Token
Expiration	15/03/2023

#### Token

eyJhbGciOiJSUzI1NiIsImtpZCI6IjI0OTMxRUM5QzA4NTIGOEV GNkMONUY0MDExQTU0MTAzNzhGMTY5REEiLCJ0eXAiOiJK V1QifQ.eyJ1bmlxdWVfbmFtZSI6IIRIc3QtVG9rZW4iLCJncm91c HNpZCI6IIZvdGlyb0ludGVybmFsU2VydmljZXMiLCJyb2xIljoiQ WRtaW5pc3RyYXRvciIsImp0aSI6ImZmNWUwOWFmLTA4Njct NDUxNC1iZmVkLTQx0DZI0DZIZjJmZSIsIm5iZiI6MTY0NzgzN DQxMCwiZXhwIjoxNjc40DA5NjAwLCJpYXQi0jE2NDc4MzQ0 MTB9.EYm24-

YcS6RnXSCh7LiYDFAMA5d\_U7Z6nBW670FOgiA6AH3tG14am RWc6wjo2LpKxNAVLbrnMUbrVUTCRToAWABPvT47gJslBdafP 9R0sPOh0voAdbh\_hjt-

J9jspYuF8hu7NfukUxUVhDd3oKRnGDmWizBANbqCbXXw2fE GLgWpn0VuR88y\_o7vxoBp5mqlqRWvQ1p3mGTEAem6sI1U8 HhYgvOvKMYY9TH9cxnuRbnpA-

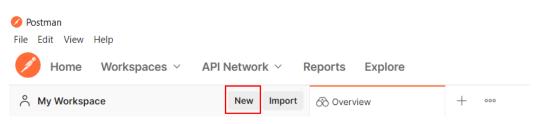
xVwGCQ8OFQuA6ITJw9ehwl34vUA22qri65-xNvWoakgXVAtiHSpWxdgWrmeLK88wKum7dUyFfDu4rrEadvvmLFZK3eEZ1K pZ0v1DcDg

ОК

4. Press **OK** to close the Token window.

### 16.2.2 Postman Setup

1. In the Postman app, go to **Workspaces** > **My Workspace** and press **New**:



2. The Create New window opens. Select HTTP Request:

Create New	1				×
Building Blo	ocks				
GET	HTTP Request Create a basic HTTP request	<u>মি</u>	WebSocket Request BETA Test and debug your WebSocket connections	ţ	<b>gRPC Request BETA</b> Test and debug your gRPC request
	Collection Save your requests in a collection for reuse and sharing	▣	Environment Save values you frequently use in an environment		Workspace Create a workspace to build independently or in collaboration
Advanced					
	API Documentation Create and publish beautiful documentation for your APIs		Mock Server Create a mock server for your in- development APIs	<b>^</b>	Monitor Schedule automated tests and check performance of your APIs
00	API Manage all aspects of API design, development, and testing	어 않	Flows BETA Create API workflows by connecting series of requests through a drag-and-drop UI.		
Not sure wi	here to start? Explore featured APIs, o	collections	, and workspaces published by the Po	ostman co	mmunity.
					Learn more on Postman Docs
ress the	Settings icon:				
Portman					

🤣 Postman File Edit View Help						- a ×
🥖 Home 🛛 Workspaces 🗸 🛛 API Ne	etwork ~ I	Reports Explore		Q Search Postman	4 🔒 🕺 Invite 🗞 🕸 🗘 🌀	Upgrade v
A My Workspace	New Import	🐼 Overview	GET Untitled Request	+ ***	Settings yent	~ ©

4. The **Settings** window opens. To ensure that http requests will go through even if your VA is using a self-signed certificate, toggle **SSL certificate verification** to **OFF**:

3.

SETTINGS			×
eneral Themes Shortcuts Data	Add-ons	Certificates Proxy Update About	
Request		Headers	
Trim keys and values in request body	OFF OFF	Send no-cache header	ON ON
SSL certificate verification	OFF	Send Postman Token header	ON
Always open requests in new tab	OFF	Retain headers when clicking on links	OFF
Always ask when closing unsaved tabs	ON ON	Automatically follow redirects	ON
Language detection	Auto 🗸	Send anonymous usage data to Postman	ON
Request timeout in ms	0	- ostnun	
Set how long a request should wait for		User interface	
a response before timing out. To never time out, set to 0.		Two-pane view	OFF
Max response size in MB	50	Show icons with tab names	ON ON
Set the maximum size of a response to download. To download a response of		Variable autocomplete	ON ON

#### 5. Close the **Settings** window.

#### 6. Under the **Untitled Request** dropdown box, select **POST**:

### **Untitled Request**

GET	× ^	Enter rec
GET		I
POST	]	Ī
PUT		
PATCH		
DELETE	E	
COPY		
HEAD		
OPTION	۹S	
LINK		
UNLINK	< C	
PURGE		
LOCK		
UNLOC	к	
PROPFI	ND	
VIEW		

7. In the Enter request URL box, enter your VA FQDN in the following format: https://<VA-FQDN>/disarmer/api/disarmer/v4/upload

#### For example:

Votiro / er	mdbs-v	a	🖺 Save	~	000
POST	~	https://emdbs-va.mytestwon40.com/disarmer/api/disarmer/v4/upload			

8. Select the Authorization tab and under the Type dropdown, select Bearer Token:

Params	Authorization	Headers (8) Body	У
Туре		Bearer Token ^	!
The authorization header generated when you send Learn more about authori		Inherit auth from parent No Auth API Key	ke
		Bearer Token Basic Auth	
		Digest Auth	
Response		OAuth 1.0	
		OAuth 2.0	
		Hawk Authentication	
		AWS Signature	
		NTLM Authentication Akamai EdgeGrid	

#### 9. Select the **Headers** tab.

10. In the first row of the **Key** column, start to type **Content** until a dropdown list appears. Then select **Content-Type** from the dropdown list:

Head	ders 💿 8 hidden	
	KEY	
	Content	
	Content-MD5	
	Content-Length	
	Content-Transfer-Encoding	
	Content-Type	

11. In first row of the **Value** column, start to type **multipart** until a dropdown list appears. Then select **multipart/form-data** from the dropdown list:

mul
multipart/mixed
multipart/alternative
multipart/related
multipart/form-data
multipart/signed
multipart/encrypted

12. Select the **Body** tab and then select **form-type**:

Params	Authorization	1 <b>•</b>	Headers (9)	Body 🔵	Pre-r	equest Scrip	t Tests	Settings
none	🖲 form-data	• ×	-www-form-urle	ncoded	raw	binary	GraphQL	

13. In the first row of the **KEY** column, type **File**, and select **File** from the hidden dropdown list:

KEY	
File	File $\sim$
Кеу	Text
	File

- 14. In the first row of the **VALUE** column, press **Select Files** and select the desired file from the browser window that opens.
- 15. In the second row of the **KEY** column, type **Properties**.
- 16. In the second row of the VALUE column, enter the following:

```
{"PolicyName":"Default
Policy","ChannelType":"FileConnector",
"ChannelId":"827b50a3-d585-4ba5-a5ca-
100b09068123","ChannelName":"API Up-Sync"}
```

17. After completing steps 13-16, the **KEY** and **VALUE** table should be identical to the below screenshot, with the exception of the file name:

Parar	ms Authorization • Headers (10)	Body  Pre-request Script Tests Set						
no	one 🦲 form-data 🕘 x-www-form-urlend	oded 🌑 raw 🌑 binary 🌑 GraphQL						
	KEY	VALUE						
	File	Pptx-ActiveX.pptx ×						
	Properties	{"PolicyName":"Default Policy","ChannelT						
	Кеу	Value						

18. Press the Send button:

POST	~	https://emdbs-va.mytest140.com/disarmer/api/disarmer/v4/upload	Send ~	

19. You should get a HTTP/200 response and a GUID string in the body. This will be the Correlation ID of the file that you have submitted.

#### For example:

Test	File Collection / emdbs-va Copy		🖺 Save 🗸 👓	4	<b>/</b>
POST	<ul> <li>https://emdbs-va.mytestwon40.com</li> </ul>	m/disarmer/api/disarmer/v4/upload		Sei	nd ~
Param		Pre-request Script Tests Settings     raw      binary      GraphQL			Cookies
	KEY	VALUE	DESCRIPTION	000	Bulk Edit
~	File	Pptx-ActiveX.pptx ×			
	Properties Text ~	{"PolicyName":"Default Policy","ChannelType":"			×
	Кеу	Value	Description		
Body Preti	Cookies Headers (4) Test Results ty Raw Preview Visualize Text 4d41873a-7e5a-4a1a-a879-ccb9b7d71628		DK Time: 34 ms Size: 170 B S	ave Re ເ	sponse ∽

20. On the Incidents page, you will be able to see the exact string:

Files	File actions V File Info		Sani	itization Log
Pptx-ActiveX.pptx				Data Processing
[Content_Types].xml     .rels		= ×		<ul> <li>File Pptx-ActiveX.pptx upload for sanitization started. Item Id: 4d41873a-7e5a-4a1a-a879-ccb9b7d71620</li> <li>File Pptx-ActiveX.pptx recognized as [17] Power Point</li> </ul>
presentation.xml	1	-		(2007-2010) (Microsoft Office).  Office Relation Types Removed
presProps.xml     tableStyles.xml	Pptx-ActiveX.pptx	Power Point (2007-2010)		<ul> <li>ActiveX Removed</li> <li>New child created for item 4d41873a-7e5a-4a1a-a879- ccb9b7d71620. Child ID: 68150756-68b6-4a8c-bb9f-</li> </ul>
viewProps.xml	Original Item Hash	0dd1a52f2cbfd1e8c59f40e27e097209febcc71e3e68879 1484f6a503010e928	0	d219429d8de3. 
app.xml	Connector Name	API Up-Sync		Total Sanitization Time
core.xml	Connector Type	File Connector		

### **17** How to Sync with an NTP Server

This page describes how to sync Votiro's Virtual Appliance with an NTP Server.

The Virtual Appliance standard installation contains the pre-configured CentOS NTP server.

### 17.1 Solution

Obtain a list of servers, using the following command:

# cat /etc/ntp.conf | grep server

server 0.centos.pool.ntp.org iburst
server 1.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
server 3.centos.pool.ntp.org iburst

To configure the NTP server there are two methods for you to choose from:

- External NTP server.
- Internal NTP server.

### 17.2 External NTP Server

To work with the pre-configured CentOS public NTP servers, follow these steps:

- 1. On your organization's firewall open port **123 UDP**.
- 2. Add the NTP servers, using the following command:

\*.centos.pool.ntp.org

### 17.3 Internal NTP Server

To work with an internal NTP server, follow these steps:

- 1. Ensure port **123 UDP** is opened between the VA network and the NTP server.
- 2. Ensure you can access your NTP server from each node, using the following command:

# ntpdate -u -s <ntp-server-fqdn>

3. Add the FQDN to the NTP configuration file, using the following command:

# vi /etc/ntp.conf

- 4. To edit the file, click the **Insert** key on your keyboard.
- 5. Enter the server address in the following format:

# Use public servers from the	
# Please consider joining the	<pre>pool (http://www.pool.ntp.org/join.html).</pre>
#server 0.centos.pool.ntp.org	iburst
#server 1.centos.pool.ntp.org	iburst
#server 2.centos.pool.ntp.org	iburst
#server 3.centos.pool.ntp.org	iburst
server ad-qa-2016.qa.local	iburst

server <ntp-server-fqdn> iburst

6. To Save and Exit, key the following commands:

:wq!

# sudo systemctl restart ntpd

### **17.4** Verify Time of Syncronization for each Node

To verify the time of syncronization, log in to each node, using the following command:

```
# timedatectl
```

Local time:	Wed 2020-10-14 06:11:44 EDT
Universal time:	Wed 2020-10-14 10:11:44 UTC
RTC time:	Wed 2020-10-14 10:11:44
Time zone:	America/New_York (EDT, -0400)
NTP enabled:	yes
NTP synchronized:	yes
RTC in local TZ:	no
DST active:	yes
Last DST change:	DST began at
	Sun 2020-03-08 01:59:59 EST
	Sun 2020-03-08 03:00:00 EDT
Next DST change:	DST ends (the clock jumps one hour backwards) at
	Sun 2020-11-01 01:59:59 EDT
	Sun 2020-11-01 01:00:00 EST

# 18 How to Troubleshoot NTP using Chrony in VA

Because ntpd was replaced by chrony in Votiro Cloud v9.6.174, you may need to configure NTP using the steps below.

### 18.1 Solution

1. Verify the currently used service/daemon (ntpd or chronyd) for NTP by running the commands below:

```
systemctl list-units --type=service -all | grep ntpd
systemctl list-units --type=service -all | grep chrony
```

 If ntpd is disabled and chronyd is used, the command outputs should like this:

<ul> <li>ntpd.service</li> <li>ntpdate.service</li> </ul>	not-found not-found			ntpd.service ntpdate.service
chronyd.service	loaded	active	running	NTP client/server

If ntpd is active, run the following commands to disable ntpd:

```
systemctl stop ntpd.service
```

systemctl disable ntpd.service

2. To check if the clock is synchronized, run the following command:

timedatectl | grep synchronized

If synchronized, the command output should display synchronized: yes, as shown:

[root@zorel-VAl ~]# timedatectl | grep synchronized NTP synchronized: yes

- If it's not synchronized, troubleshoot using the following steps:
  - Check the chrony service status by running one of the following commands (the output is the same):

```
systemctl status chronyd
```

systemctl status chrony.service

Start/restart the chrony service/daemon using one of the following commands:

systemctl restart chronyd systemctl restart chrony.service

• If the service is running, run the following command to verify the synchronization of the local system with the reference server:

chronyc tracking

• Run the following command to display information about the current time sources that chronyd is accessing:

chronyc sources -v

For example:

ala Number of commence of a								
210 Number of sources = 3								
Source mode '^' = s	erver, '=	' = F	peer,	'#' = 1	ocal cl	ock.		
/ Source state '*' = c	urrent sy	nced,	, '+' =	= combi	.ned , '	-' = not	combi	ne
<pre>/ '?' = unreachable, '</pre>	x' = time	may	be in	error,	1~1 =	time too	varia	bl
11					- xxxx	[ עעעע ]	+/- z	zz
Reachability regist	ter (octa	1)			XXXX	= adjuste	d off	se
<pre>   Log2(Polling inter</pre>	val)				YYYY	= measure	d off	se
11					ZZZZ	= estimat	ed er	ro
11								
MS Name/IP address	Stratum	Poll	Reach	LastRx	Last s	ample		
								==
^+ ntp92.kashra-server.com	2	10	377	543	+1370us	[+1369us]	+/-	
^* time.cloudflare.com	3	9	377	73	-498us	[ -499us]	+/-	
<pre>^+ time.cloudflare.com</pre>	3	9	377	92	-530us	[ -531us]	+/-	
r . 0								

 To display the information about the drift rate and offset estimation process for each of the sources listed by chronyd, run the following command:

chronyc sourcestats

• To edit the chrony configuration, run the command:

vi /etc/chrony.conf



For example, with public servers:

```
Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org iburst
server l.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
server 3.centos.pool.ntp.org iburst
# Record the rate at which the system clock gains/losses time.
driftfile /var/lib/chrony/drift
# Allow the system clock to be stepped in the first three updates
# if its offset is larger than 1 second.
makestep 1.0 3
# Enable kernel synchronization of the real-time clock (RTC).
rtcsync
# Enable hardware timestamping on all interfaces that support it.
#hwtimestamp *
# Increase the minimum number of selectable sources required to adjust
# the system clock.
#minsources 2
# Allow NTP client access from local network.
#allow 192.168.0.0/16
# Serve time even if not synchronized to a time source.
#local stratum 10
# Specify file containing keys for NTP authentication.
#keyfile /etc/chrony.keys
# Specify directory for log files.
logdir /var/log/chrony
# Select which information is logged.
#log measurements statistics tracking
"/etc/chrony.conf" 38L, 1108C
```

**Note**After each action or saved change on the chrony.conf file, a service restart is required.

# 18.2 Troubleshooting Example: NTP not synchronized with external server

Although all servers were configured properly, when running the sources command, "last sample" showed a gap of 10.8s between the servers as shown:

Local time: Tue 2022-07-12 12:36:31 INT Universal time: Tue 2022-07-12 (9:36:30 NTP enabled; yes NTP enabled; yes NTP synchronized: no BST active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 01:59:59 IST Sun 2022-10-30 01:59:59 INT Sun 2022-10-30 01:59:59 INT Universal time: Tue 2022-07-12 12:48:07 INT Universal time: Tue 2022-07-12 09:43:06 Time zone: Ana/Jerusalem (IDT, +0300) NTP enabled; yes NTP synchronized: no BST active: yes Last DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 INT Genetic Tue 2022-07-12 09:43:06 Time zone: Ana/Jerusalem (IDT, +0300) NTP enabled; yes NTP synchronized: no BST active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 INT Fri 2022-03-25 01:59:59 INT Sun 2022-10-30 01:90:59 INT Next DST change: DST began at Fri 2022-03-25 01:59:59 INT Sun 2022-10-30 01:59:59 INT Sun 200:20 Sun 200:20 INT Sun 200:20 Sun 20	[root@dmzcdrem102 ~]# timedatect1
<pre>FTC time: Tue 2022-07-12 09:36:30 Time zone: Axia/Jerusalem (IDT, +0300) NTP enabled: yes NTP synchronized: no ETC in local T2: no DST active: yes Lest D5T change: D5T began at fr1 2022-03-25 01:59:59 IST fr1 2022-03-25 03:00:00 IDT Next D5T change: D5T ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Local T2: no DC2-10-30 01:00:00 IST [root@dmzcdrenl02 -]# timedatect1 Local time: Tue 2022-07-12 12:43:07 IDT Universal time: Tue 2022-07-12 09:43:06 Time zone: Axia/Jerusalem (IDT, +0300) NTP enabled: yes HTP synchronized: no NTC in local T2: no DST active: yes Last D5T change: D5T began at Sun 2022-10-30 01:59:59 IST fr1 2022-03-25 03:59:59 IST fr1 2022-03-25 03:00:00 IDT Next D5T change: D5T began at Sun 2022-10-30 01:59:59 IST fr1 2022-03-25 03:00:00 IDT Next D5T change: D5T began at Sun 2022-10-30 01:59:59 IST fr1 2022-03-25 03:00:00 IDT Next D5T change: D5T began at Sun 2022-10-30 01:59:59 IST fr1 2022-03-25 03:00:00 IDT Next D5T change: D5T ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 IDT Sun 2022-10-30 IDT Sun 2022-10-30 IDT Sun 2022-10-30 IDT Sun 2022-10-3</pre>	Local time: Tue 2022-07-12 12:36:31 IDT
<pre>Time zone: Asia/Jerusalem (IDT, +0300) NTP enabled: yes NTP synchronized: no BT active: yes Last DST change: DST began at Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Cool@dmzcdrenl0 - j4 timedatect1 Local time: Tue 2022-07-12 12:43:07 IDT Universal time: Tue 2022-07-12 09:43:06 Time zone: Asia/Jerusalem (IDT, +0300) NTP enabled: yes HTP synchronized: no BT active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT DT enabled: yes HTP synchronized: no DST active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT Next DST change: DST began at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:</pre>	Universal time: Tue 2022-07-12 09:36:31 UTC
<pre>NTP enabled: yes NTP synchronized: no RTC in local TZ: no DST active: yes Last DST change: DST began at Fri 2022-03-28 03100:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT Local time: Tue 2022-07-12 12:43:07 UTC RTC time: Tue 2022-07-12 09:43:07 UTC RTC time: Tue 2022-07-12 09:43:06 Time zone: Asia/Jerusalem (IDT, +0300) NTP enabled; yes NTP synchronized: no RTC in local TZ: no DST active: yes Last DST change: DST began at Fri 2022-03-25 03:00:00 IDT Next DST change: DST began at Fri 2022-03-25 03:00:00 IDT Next DST change: DST began at Sun 2022-10-30 01:59:59 IST Fri 2022-03-25 03:00:00 IDT Next DST change: DST began at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:00:00 IST [root@dmzcdrenl02 -] # chronyc sources -v 210 Number of sources = 2  Source mode 'A' = screer, '=' = peer, '#' = local clock. / Source state '* = current synced, '+' = combined , '-' = not combined, / ' '? = unreachable, 'X' = time may be in error, '*' = time too variable. I Log2(Polling interval) I xxxx = adjusted offset, I Log2(Polling interval) I yyyy measured offset, I Log2(Polling interval) I yyyy measure</pre>	RTC time: Tue 2022-07-12 09:36:30
<pre>NTP synchronized: no RTC in local TZ: no DST actuve: yes Last DST change: DST began at Fri 2022-03-25 03:00:00 IDT Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT Local time: Twe 2022-07-12 09:43:07 IDT Universal time: Twe 2022-07-12 09:43:06 Time zone: Asia/Jerusalem (IDT, +0300) NTP enabled: yes HTP synchronized: no RTC time: Twe 2022-07-20 09:43:06 Time zone: Asia/Jerusalem (IDT, +0300) NTP enabled: yes HTP synchronized: no RTC time: DST began at Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:05:95 IDT Sun 2022-10-30 01:05:95 IDT Sun 2022-10-30 01:05:00 IBT (root@dmzodrenl02 -] t chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '*' = peer, '\$' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined, / '?' = unreachable, 'x' = time may be in error, '-' = time too variable. / '?' = unreachable, 'x' = time may be in error, '-' = time too variable. // '?' = unreachable, 'x' = time may be in error, '-' = time too variable. // 'Dyyy 14/- zzz II Reachability register (octal) I xxxx = adjusted offset, II Log2(Polling interval) I xxxx = adjusted offset, II Log2(Polling interval) I yyyy = maauzed offset, II Log2(Polling interval) I yyyy = maauzed offset, II Log2(christiceal 2 6 377 32 +1814ms[+1816ms] +/- 10.8s ?? dmzdo02.dmz.local 1 7 377 59 +1816ms[+1816ms] +/- 10.8s ?? dmzdo02.dmz.local 1 7 377 59 +1816ms[+1816ms] +/- 10.8s ?? dmzdo02.dmz.local 1 7 077 59 +1816ms[+1816ms] +/- 10.8s Prequence ID : 00000000 seconds RMS offset : 0.00000000 seconds SKW  0.0000 pm Skew : 0.0000000 seconds</pre>	Time zone: Asia/Jerusalem (IDT, +0300)
<pre>RTC in local T2: no DST active: yes Last DST change: DST began at Fri 2022-03-28 03100:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:09:00 IST [root@dmzcdrenl02 -]# timedatect1 Local tame: Twe 2022-07-12 12:43:07 IDT Diversal time: Twe 2022-07-12 12:43:07 UTC RTC time: Twe 2022-07-12 09:43:07 UTC NTP enabled: yes NTP enabled: yes NTP enabled: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 01:59:59 IST Sun 2022-10-30 01:59:59 IST Sun 2022-10-30 01:59:59 IST Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:50:00 IST [root@dmzcdreml02 -]# chronyc sources -v 210 Number of sources - 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '*' = combined, '-' = not combined, / / '?' = unreachable, 'x' = time may be in error, '-' = intme too Variable. 11 Sunder/IP address Stratum Poll Reach LastKx Last sample </pre>	NTP enabled: yes
DST active: yes Last DST change: DST began at Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT Double and the clock jumps one hour backwards) at Sun 2022-07-30 01:00:00 IST [root@dmzcdrenl02 ~]# timedatect1 Local time: Tue 2022-07-12 09:43:07 IDT NET clime: Tue 2022-07-12 09:43:07 UTC RTC time: Tue 2022-07-12 09:43:07 UTC RTC time: Tue 2022-07-12 09:43:06 Time zone: Asin/Serusalem (IDT, +0300) NTP enabled: yes HTP synchronized: no RTC in local T2: no DST active: yes Last DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IST Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:00:00 IST [root@dmzcdrenl02 ~]* chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '*' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined, [/ '?' = unreachable, 'x' = time may be in error, 'v' = time too variable. II Reachability register (octal) I xxxx = adjusted offset, II Reachability register (octal) I xxxx = adjusted offset, II Name/IP address Stratum Poll Reach LastRx Last sample 	NTP synchronized: no
Lest DST change: DST began at Yri 2022-03-25 03:00:00 HDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 HDT Jun 2022-10-30 01:59:59 HDT (root@dmzcdreml02 ~) # timedatectl Local time: Tue 2022-07-12 12:43:07 HDT Universal time: Tue 2022-07-12 09:43:07 HDT Universal time: Tue 2022-07-12 09:43:06 Time sone: Asia/Jerusalem (HDT, +0300) NTP enabled: yes HTP synchronized: no RTC in local T2: no DST enabled: yes Last DST change: DST began at Fri 2022-03-25 03:00:00 HDT Next DST change: DST began at Sun 2022-10-30 01:59:59 HST Fri 2022-03-25 03:00:00 HDT Next DST change: DST began at Sun 2022-10-30 01:59:59 HST Sun 2022-10-30 01:00:00 HST [root@dmzcdreml02 -) # chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock. / Source mode '^' = server, '=' = peer, '#' = local clock. / Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '' = current synced, '+' = combined , '-' = not combined, // '?' = unreachable, 'x' = time may be in error, 'w' = time too variable. 11 Log2(Polling interval)   yyyy = measured offset, 11 Log2(Polling interval)   yyyy = measured offset, 12   I Reachability register (octal)   xxxx = adjusted offset, 13   J   '   J   '   J   '   J   '   J   '   J   '   '	RTC in local TZ: no
<pre>Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:00:00 IST [root@dmzcdrem102 ~]# timedatect1 Local time: Tue 2022-07-12 09:43:07 IDT Universal time: Tue 2022-07-12 09:43:06 Time tone 2022-07-12 09:43:07 UTC RTC time: Tue 2022-07-12 09:43:06 Time tone 2022-07-12 09:43:07 NTP enabled: yes HTP synchronized: no DST active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 03:00:00 IDT Sun 2022-10-30 01:00:00 IST [root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined, / ' '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  xxxx [ yyyy ] +/- zzzz II Reachability register (octal) I xxxx = adjusted offset, II Log2(Polling interval) I xxxx = adjusted offset, II Log2(Polling interval) I xxx [ yyyy ] +/- zzzz Troot@dmzcdrem102 ~]# chronyc tracking Reference ID : 00000000 () Stratum : 0 Ref time (UTC) : Thu Jan 01 00:00:00 1970 System time : 0.00000000 seconds RMS offset : 0.00000000 seconds</pre>	DST active: yes
<pre>Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:05:05 IDT Sun 2022-10-30 01:00:00 IST [root@dmzcdrem102 ~]4 timedatect1 Local time: Tue 2022-07-12 12:43:07 IDT Universal time: Tue 2022-07-12 09:43:07 UTC RTC times ince Asia/Jerusalem (IDT, +0300) NTP enabled: yes NTP synchronized: no RTC in local T2: no DST active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 03:00:00 IDT Next DST change: DST began at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT [root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined, / '?' = unreachable, 'x' = time may be in error, '~' = time too variable. // '?' = unreachable, 'x' = time may be in error, '~' = time too variable. // '?' = unreachable, 'x' = time may be in error, '~' = time too variable. // '?' = unreachable, 'x' = time may be in error, '~' = time too variable. // '?' = unreachable, 'x' = time may be in error, '~' = time too variable. // '?' = unreachable, 'x' = time may be in error, '~' = time too variable. // '?' = unreachable, 'x' = time may be in error, '~' = time too variable. // '?' = unreachable, 'x' = time may be in error, '~' = time too variable. // '?' = unreachable, 'x' = time may be in error, '~' = time too variable. // '?' = unreachable, 'x' = time may be in error, 'A' = time dor variable. // '?' = unreachable, 'x' = time may be in error, 'A' = time too variable. // '?' = unreachable, 'x' = time too variable. // '?' = unreachable, 'x' = time too variable. // '?' = unreachable, 'x' = time may be in error, 'A' = time too variable. // '?' = unreachable, 'x' = time may be in error, 'A' = time too variable. // '?' = unreachable, 'X' = time too variable. // '?' = unreachable, 'X' = time too variable. // '?' = time too variable. // '?' = tinde too variable. // '?' = time too variable. //</pre>	Last DST change: DST began at
<pre>Next DST change: DST ends (the clock jumps one hour backwards) at</pre>	Fri 2022-03-25 01:59:59 IST
<pre>Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:00:00 IST [root@dmzcdren102 -]# timedatect1 Local time: Tue 2022-07-12 12:43:07 IDT Universal time: Tue 2022-07-12 09:43:06 Time zone: Asia/Acrusalem (IDT, +0300) NTP enabled; yes NTP synchronized: no RTC tin local TZ: no DST active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IST Sun 2022-10-30 01:09:595 IST Sun 2022-10-30 01:09:59 IST Sun 2022-10-30 01:09:59 IST Sun 2022-10-30 01:09:59 IST Sun 2022-10-30 01:09:59 IST Sun 2022-10-30 01:00:00 IST [root@dmzcdren102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined, [/ ''' = unreachable, 'x' = time may be in error, 'w' = time too variable. II Reachability register (octal) I xxxx f yyyy I+' zzzz II Reachability register (octal) I xxxx f wyyy I+' zzzz II Log2(Polling interval) I xxxx f adjusted offset, II Log2(Polling interval) I yyyy measured offset, II Log2(Polling interval) I xzxz = estimated error. II L J Y I unreachable / 'A' = trate Last sample </pre>	Fri 2022-03-25 03:00:00 IDT
Sun 2022-10-30 01:00:00 IST [root@dmzcdrenl02 ~]# timedatec11 Local time: Tue 2022-07-12 03:43:07 UTC RTC time: Tue 2022-07-12 03:43:07 UTC RTC time: Tue 2022-07-12 03:43:06 Time zone: Asia/Jerusalem (IDT, +0300) NTP enabled; yes NTP synchronized: no RTC in local T2: no DST active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT [root@dmzcdrenl02 ~]# chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined, '.' = not combined,   / '?' = unreachable, 'x' = time may be in error, '.' = time too variable. 11 Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy measured offset,   Log2(Polling interval)   yyyy measured offset,   Log2(Polling interval)   yyyy measured offset,   S Name/IP address Stratum Poll Reach LastRx Last sample 	Next DST change: DST ends (the clock jumps one hour backwards) at
<pre>[root@dmzcdren102 ~]# timedatect1 Local time: Twe 2022-07-12 03:43:07 IDT Diversal time: Twe 2022-07-12 03:43:07 IDT RTC time: Twe 2022-07-12 03:43:06 Time zone: Asia/Jerusalem (IDT, +0300) NTF enabled: yes NTF synchronized: no RTC in local T2: no DST active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 03:00:00 IDT Next DST change: DST means at Sun 2022-10-30 01:59:59 IST Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:00:00 IST Foot@dmzcdrenD12 -)# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / . '?' = unreachable, 'x' = time may be in error, 'w' = time too variable.  xxxx [ yyyy ] +/- zzzz  Source mode '^' = server (cotal)</pre>	Sun 2022-10-30 01:59:59 IDT
Local time: Twe 2022-07-12 12:43:07 IDT Universal time: Twe 2022-07-12 09:43:07 UTC RTC time: Twe 2022-07-12 09:43:06 Time zone: Asia/Jerusalem (IDT, +0300) NTP enabled: yes NTP synchronized: no RTC in local T2: no DST active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT In 2022-10-30 01:00:00 IST [root@dmzcdreml02 ~]# chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '*' = time too variable. I Reachability register (octal)   xxxx [ yvyy ] +/- zzzz   Reachability register (octal)   yyyy measured offset,   Log2(Polling interval)   yyyy measured offset,   Log2(Polling interval)   yyyy measured offset,   S Name/IP address Stratum Poll Reach LastRx Last sample 	Sun 2022-10-30 01:00:00 IST
Universal time: Tue 2022-07-12 09:43:07 UTC RTC time zone: Asia/Jerusalem (IDT, +0300) NTP enabled: yes NTP synchronized: no RTC in local 72: no DST active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:00:00 IST [root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock. / Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined, / '?' = unreachable, 'x' = time may be in error, '*' = time too variable. 11 Xxxx [ yyyy ] +/- zzz 11 Reachability register (octal)   xxxx = adjusted offset, 12 Log2(Polling interval)     yyyy = measured offset, 13 Log2(Polling interval)     yyyy = measured offset, 14 Log2(Polling interval)     yyyy = measured offset, 15 Log2(mz.local 2 6 377 32 +1814ms[+1814ms] +/- 10.8s 7? dmzdc01.dmz.local 1 7 377 59 +1816ms[+1816ms] +/- 10.8s [root@dmzcdrem102 ~]# chronyc tracking Reference ID : 00000000 () Stratum : 0 Ref time (UTC) : Thu Jan 01 00:00:00 1970 System time : 0.00000000 seconds RMS offset : 0.00000000 seconds	[root@dmzcdrem102 ~]# timedatect1
<pre>RTC time: Tue 2022-07-12 09:43:06 Time zone: Asia/Jerusalem (IDT, +0300) NTP enabled: yes NTF synchronized: no RTC in local T2: no DST active: yes Last DST change: DST began at Fri 2022-03-25 03:00:00 HDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 HDT Sun 2022-10-30 01:00:00 HST [root@dmzcdreml02 ~]* chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '*' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  xxxx [ yyyy ] */- zzzz II Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,   Log2(Polling interval)   yyyy = measured offset,   Log2(Polling interval)   yyyy = measured offset,   Log2(Polling interval)   NS Name/IP address Stratum Poll Reach LastRx Last sample </pre>	Local time: Tue 2022-07-12 12:43:07 IDT
<pre>Time zone: Asia/Jerusalem (IDT, +0300) NTP enabled: yes NTP synchronized: no RTC in local T2: no DST active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:00:00 IST [root@dmzcdrem102 ~]\$ chronyc sources -v 210 Number of sources - 2  Source mode '^' = server, '=' = peer, '\$' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable. ! I Reachability register (octal) I xxxx = adjusted offset, !I Log2(Polling interval) I yyyy measured offset, !I I log3 Stratum Poll Reach LastRx Last sample </pre>	Universal time: Tue 2022-07-12 09:43:07 UTC
<pre>NTP enabled: yes NTP synchronized: no RTC in local T2: no DST active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:00:00 IST [root@dmzcdrem102 ~]\$ chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '\$' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '*' = time too variable.   / '?' = unreachable, 'x' = time may be in error, '*' = time too variable.   / '?' = unreachable, 'x' = time may be in error, '*' = time too variable.   / '?' = unreachable, 'x' = time may be in error, '*' = time too variable.   / '?' = unreachable, 'x' = time may be in error, '*' = time too variable.   / '?' = unreachable, 'x' = time may be in error, '*' = time too variable.   / '?' = unreachable, 'x' = time may be in error, '*' = time too variable.   / '?' marked offset,   Locg2(Polling interval)   xxxx [ yyyy ] */- zzzz   Locg2(Polling interval)   xxxx adjusted offset,   Locg2(Polling interval)   xxxx adjusted offset,   Locg2(Polling interval)   xzzz = estimated error.   H</pre>	RTC time: Tue 2022-07-12 09:43:06
<pre>NTP synchronized: no RTC in local T2: no DST active: yes Last DST change: DST began at Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT (root@dmzodrem102 ~]# chronye sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock. / Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined, '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '*' = time too variable. 11 Sun 2022-10-30 (class) 14 Reachability register (octal) 15 Surce state '*' = current synced, '+' = combined, '-' = not combined, 16 Surce state '*' = current synced, '+' = combined, '-' = not combined, 17 Surce state '*' = current synced, '+' = combined, '-' = not combined, 17 Ns Name/IP address Stratum Poll Reach LastRx Last sample</pre>	Time zone: Asia/Jerusalem (IDT, +0300)
<pre>RTC in local T2: no DST active: yes Last DST change: DST began at Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:00:00 IST [root@dmzcdreml02 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable. !! Reachability register (octal)   xxxx = adjusted offset, !! Log2(Polling interval)   yyyy measured offset, !! Log2(Polling interval)   yyyy measured offset, !!   Nemar/IP address Stratum Poll Reach Last x Last sample </pre>	NTP enabled: yes
<pre>DST active: yes Last DST change: DST began at</pre>	NTP synchronized: no
Last DST change: DST began at Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:00:00 IST [root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   I xxxx [ yyyy] +/- ZZZZ   Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,   Log2(Polling interval)   yyyy = measured offset,   (   ( ! (   (   ( ! ( ! ( ! ( ( ! ( ( ( ! ( ( ! ( ( ! ( ( ( ! (	RTC in local TZ: no
<pre>Fri 2022-03-25 01:59:59 IST Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:00:00 IST [root@dmzcdreal02 -]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  xxxx [ yyyy ] +/- zzzz [I Reachability register (octal) I xxxx = adjusted offset, II Log2(Polling interval) I xxxx = adjusted offset, II Log2(Polling interval) I xxxx = adjusted error. II xzzz = estimated error. II x = unreachability register (octal) I xxxx = adjusted offset, II Log2(Polling interval) I szzz = estimated error. II x = unreachability register (octal) I xxxx = adjusted offset, II Log2(Polling interval) I szzz = estimated error. II x = unreachability register (octal) I zzzz = estimated error. II z zzz = estimated error. II z zzz = estimated error. II z zzz = estimated error. II = u v MS Name/IP address Stratum Poll Reach LastRx Last sample Eroot@dmzcdreml02 -]# chronyc tracking Reference ID : 000000000 () Stratum : 0 Ref time (UTC) : Thu Jan 01 00:00:00 1970 System time : 0.000000000 seconds Frequency : 86.941 ppm slow Residual freq : +0.0000 ppm Reot delay : 1.000000000 seconds</pre>	DST active: yes
<pre>Fri 2022-03-25 03:00:00 IDT Next DST change: DST ends (the clock jumps one hour backwards) at     Sun 2022-10-30 01:59:59 IDT     Sun 2022-10-30 01:00:00 IST [root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable. 11 xxxx [ yyyy ] +/- zzzz 11 Reachability register (octal)   xxxx = adjusted offset, 11 Log2(Polling interval)   yyyy = measured offset, 11 Log2(Polling interval)   yyyy = measured offset, 11 '' = unreachable (octal)   yyyy = measured offset, 12 '' = unreachability register (octal)   yyyy = measured offset, 13 '' = '' = '' = '' = '' = '' = '' =</pre>	Last DST change: DST began at
<pre>Next DST change: DST ends (the clock jumps one hour backwards) at</pre>	Fri 2022-03-25 01:59:59 IST
Sun 2022-10-30 01:59:59 IDT Sun 2022-10-30 01:00:00 IST [root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined, '-' = not combined, / '?' = unreachable, 'x' = time may be in error, '= time too variable. I XXXX [ yyyy] +/- zzzz II Reachability register (octal) I XXXX = adjusted offset, II Log2(Polling interval) I I yyyy = measured offset, II Log2(Polling interval) I yyyy = measured offset, II J J J J J J J J J J J J J J J J J J	Fri 2022-03-25 03:00:00 IDT
Sun 2022-10-30 01:00:00 IST [root@dmzcdreml02 ~]# chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable. 	Next DST change: DST ends (the clock jumps one hour backwards) at
<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   xxxx [ yyyy ] +/- zzzz   Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,   Log2(Polling interval)   yyyy = measured offset,   Log2(Polling interval)   yyyy = measured offset,   MS Name/IP address Stratum Poll Reach LastRx Last sample </pre>	Sun 2022-10-30 01:59:59 IDT
<pre>210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   xxxx [ yyyy ] +/- zzzz   Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,   Log2(Polling interval)   yyyy = measured offset,     zzzz = estimated error.       yyyy = measured offset,  </pre>	Sup 2022-10-30 01:00:00 TST
<pre> Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined, '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  xxxx [ yyyy ] +/- zzz    Reachability register (octal)   xxxx = adjusted offset,    Log2(Polling interval)   yyyy = measured offset,    Log2(Polling interval)   yyyy = measured offset,      zzzz = estimated error.      xxxx = adjusted offset,        yyyy = measured offset,          yyyy = measured offset,              yyyy = measured offset,   </pre>	Duit 2022-20-00 02100100 201
<pre>/ Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   xxxx [ yyyy ] +/- zzzz   Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,  </pre>	
<pre>/ Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   xxxx [ yyyy ] +/- zzzz   Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,     Log2(Polling interval)   yyyy = measured offset,     .</pre>	[root@dmzcdrem102 ~]# chronyc sources -v
<pre>/ '?' = unreachable, 'x' = time may be in error, '~' = time too variable. // xxxx [ yyyy ] +/- zzzz // Reachability register (octal)   xxxx = adjusted offset, // Log2(Polling interval)   xxxx = adjusted offset, // Log2(Polling interval)   yyyy = measured offset, //   zzzz = estimated error. //   zzzz = estimated error. // MS Name/IP address Stratum Poll Reach LastRx Last sample // / / / / Stratum Poll Reach LastRx Last sample // / / / / / / / / / / / / / / / / / /</pre>	[root8dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2
<pre>// xxxx [ yyyy ] +/- zzzz // Reachability register (octal)   xxxx = adjusted offset, // Log2(Polling interval)   yyyy = measured offset, // Log2(Polling interval)   yyyy = measured offset, //   zzzz = estimated error. // / zzzz = estimated error. // / / zzzz = estimated error. // / / / zzzz = estimated error. // / / zzzz = estimated error. // / / / / / zzzz = estimated error. // / / / / / zzzz = estimated error. // / / / / / / zzzz = estimated error. // / / / / / / / / zzzz = estimated error. // / / / / / / / / / / / / / / / / / /</pre>	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock.</pre>
<pre>11 Reachability register (octal)   xxxx = adjusted offset, 11 Log2(Polling interval)   yyyy = measured offset, 11   zzzz = estimated error. 14   zzzz = estimated error. 15   zzzz = estimated error. 16   zzzz = estimated error. 17 dmzdc01.dmz.local 2 6 377 32 +1814ms[+1814ms] +/- 10.8s 2 6 377 59 +1816ms[+1816ms] +/- 10.8s 2 7 dmzdc02.dmz.local 1 7 377 59 +1816ms[+1816ms] +/- 10.8s 17 oot§dmzcdrem102 ~]# chronyc tracking Reference ID : 00000000 () Stratum : 0 Ref time (UTC) : Thu Jan 01 00:00:00 1970 System time : 0.000000000 seconds errors Frequency : 86.941 ppm slow Residual freq : +0.000 ppm Skew : 0.000 ppm Root delay : 1.00000000 seconds </pre>	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,</pre>
<pre>// Log2(Polling interval) / / yyyy = measured offset, // / zzzz = estimated error. // / zzzz = estimated error. // / zzzz = estimated error. // // / zzzz = estimated error. // // // // // // // // // // // // //</pre>	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,</pre>
<pre>11 // / zzzz = estimated error. 11 // / zzzz = estimated error. 14 // / zzzz = estimated error. 15 // // // // // // // // // // // // //</pre>	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2 Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.</pre>
<pre>11 1 1 1 MS Name/IP address Stratum Poll Reach LastRx Last sample ^?? dmzdc01.dmz.local 2 6 377 32 +1814ms[+1814ms] +/- 10.8s ^? dmzdc02.dmz.local 1 7 377 59 +1816ms[+1816ms] +/- 10.8s [root@dmzcdreml02 ~]# chronyc tracking Reference ID : 00000000 () Stratum : 0 Ref time (UTC) : Thu Jan 01 00:00:00 1970 System time : 0.0000000015 seconds slow of NTP time Last offset : +0.00000000 seconds Frequency : 86.941 ppm slow Residual freq : +0.000 ppm Skew : 0.000 ppm Root delay : 1.00000000 seconds</pre>	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.    xxxx [ yyyy ] +/- zzzz</pre>
MS Name/IP address         Stratum Poll Reach LastRx Last sample           ^? dmzdc01.dmz.local         2         6         377         32         +1814ms[+1814ms] +/-         10.8s           ^? dmzdc02.dmz.local         1         7         377         59         +1816ms[+1816ms] +/-         10.8s           [root@dmzcdreml02 ~]# chronyc tracking         Image: Contend of the stratum         1         0         Stratum         10.8s           System time         :         0         0         00000000 ()         Stratum         :         0           Ref time (UTC)         :         Thu Jan 01 00:00:00 1970         System time         :         0.00000000 seconds           RMS offset         :         0.00000000 seconds         Stratum         :         0           Frequency         :         86.941 ppm slow         Residual freq         :         0.0000 ppm           Skew         :         0.0000 ppm         .         .         0.000 ppm           Skew         :         0.0000 ppm         .         .         .	<pre>[root@dmzcdreml02 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.    xxxx [ yyyy ] +/- zzzz    Reachability register (octal)   xxxx = adjusted offset,</pre>
<pre>^? dmzdc01.dmz.local 2 6 377 32 +1814ms[+1814ms] +/- 10.8s ^? dmzdc02.dmz.local 1 7 377 59 +1816ms[+1816ms] +/- 10.8s [root@dmzcdreml02 ~]# chronyc tracking Reference ID : 00000000 () Stratum : 0 Ref time (UTC) : Thu Jan 01 00:00:00 1970 System time : 0.000000015 seconds slow of NTP time Last offset : 0.00000000 seconds RMS offset : 0.00000000 seconds Frequency : 86.941 ppm slow Residual freq : +0.000 ppm Skew : 0.0000 ppm Root delay : 1.00000000 seconds</pre>	<pre>[root@dmzcdreml02 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   xxxx [ yyyy ] +/- zzzz   Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,</pre>
<pre>^? dmzdc02.dmz.local 1 7 377 59 +1816ms[+1816ms] +/- 10.8s [root@dmzcdrem102 ~]# chronyc tracking Reference ID : 00000000 () Stratum : 0 Ref time (UTC) : Thu Jan 01 00:00:00 1970 System time : 0.000000015 seconds slow of NTP time Last offset : +0.000000000 seconds RMS offset : 0.000000000 seconds Frequency : 86.941 ppm slow Residual freq : +0.000 ppm Skew : 0.000 ppm Root delay : 1.000000000 seconds</pre>	<pre>[root@dmzcdreml02 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   xxxx [ yyyy ] +/- zzzz   Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,     zzzz = estimated error.</pre>
<pre>^? dmzdc02.dmz.local 1 7 377 59 +1816ms[+1816ms] +/- 10.8s [root@dmzcdrem102 ~]# chronyc tracking Reference ID : 00000000 () Stratum : 0 Ref time (UTC) : Thu Jan 01 00:00:00 1970 System time : 0.000000015 seconds slow of NTP time Last offset : +0.000000000 seconds RMS offset : 0.000000000 seconds Frequency : 86.941 ppm slow Residual freq : +0.000 ppm Skew : 0.000 ppm Root delay : 1.000000000 seconds</pre>	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  </pre>
<pre>[root@dmzcdrem102 ~]# chronyc tracking Reference ID : 00000000 () Stratum : 0 Ref time (UTC) : Thu Jan 01 00:00:00 1970 System time : 0.000000015 seconds slow of NTP time Last offset : +0.000000000 seconds RMS offset : 0.000000000 seconds Frequency : 86.941 ppm slow Residual freq : +0.000 ppm Skew : 0.000 ppm Root delay : 1.000000000 seconds</pre>	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  </pre>
Reference ID       : 000000000 ()         Stratum       : 0         Ref time (UTC)       : Thu Jan 01 00:00:00 1970         System time       : 0.000000015 seconds slow of NTP time         Last offset       : +0.000000000 seconds         RMS offset       : 0.000000000 seconds         Frequency       : 86.941 ppm slow         Residual freq       : +0.000 ppm         Skew       : 0.000 ppm         Root delay       : 1.00000000 seconds	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  </pre>
Stratum       : 0         Ref time (UTC)       : Thu Jan 01 00:00:00 1970         System time       : 0.000000015 seconds slow of NTP time         Last offset       : +0.00000000 seconds         RMS offset       : 0.00000000 seconds         Frequency       : 86.941 ppm slow         Residual freq       : +0.000 ppm         Skew       : 0.000 ppm         Root delay       : 1.00000000 seconds	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   xxxx [ yyyy ] +/- zzzz   Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,   xxx = adjusted offset,   xxx = adjusted offset,   xxx = adjusted offset,       yyyy = measured offset,            </pre>
Ref time (UTC) : Thu Jan 01 00:00:00 1970         System time : 0.000000015 seconds slow of NTP time         Last offset : +0.000000000 seconds         RMS offset : 0.000000000 seconds         Frequency : 86.941 ppm slow         Residual freq : +0.000 ppm         Skew : 0.000 ppm         Root delay : 1.00000000 seconds	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   xxxx [ yyyy ] +/- zzzz   Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,   Log2(Polling interval)   yyyy = measured offset,   xxxx = adjusted offset,       yyyy = measured offset,         yyyy = measured offset,   .</pre>
System time         : 0.000000015 seconds slow of NTP time           Last offset         : +0.000000000 seconds           RMS offset         : 0.000000000 seconds           Frequency         : 86.941 ppm slow           Residual freq         : +0.000 ppm           Skew         : 0.000 ppm           Root delay         : 1.00000000 seconds	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   xxxx [ yyyy ] +/- zzzz   Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,   Log2(Polling interval)   yyyy = measured offset,   xxxx = adjusted offset,     xxxx = adjusted offset,       yyyy = measured offset,       yyyy = measured offset,           yyyy = measured offset,  </pre>
Last offset : +0.00000000 seconds RMS offset : 0.00000000 seconds Frequency : 86.941 ppm slow Residual freq : +0.000 ppm Skew : 0.000 ppm Root delay : 1.00000000 seconds	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   xxxx [ yyyy ] +/- zzzz   Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,     zzzz = estimated error.       MS Name/IP address Stratum Poll Reach LastRx Last sample </pre>
RMS offset       : 0.00000000 seconds         Frequency       : 86.941 ppm slow         Residual freq       : +0.000 ppm         Skew       : 0.000 ppm         Root delay       : 1.00000000 seconds	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   xxxx [ yyyy ] +/- zzzz   Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,     zzzz = estimated error.       MS Name/IP address Stratum Poll Reach LastRx Last sample </pre>
Frequency         : 86.941 ppm slow           Residual freq         : +0.000 ppm           Skew         : 0.000 ppm           Root delay         : 1.00000000 seconds	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  xxxx [ yyyy ] +/- zzzz !! Reachability register (octal) ! xxxx = adjusted offset, !! Log2(Polling interval) ! yyyy = measured offset, !! Log2(Polling interval) ! yyyy = measured offset, !!</pre>
Residual freq : +0.000 ppm Skew : 0.000 ppm Root delay : 1.000000000 seconds	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  xxxx [ yyyy ] +/- zzzz !! Reachability register (octal) ! xxxx = adjusted offset, !! Log2(Polling interval) ! yyyy = measured offset, !! Log2(Polling interval) ! yyyy = measured offset, !!</pre>
Skew : 0.000 ppm Root delay : 1.000000000 seconds	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined, '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   xxxx [ yyyy ] +/- zzzz   Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,   Log2(Polling interval)   yyyy = measured offset,   Log2(Polling interval)   yyyy = measured offset,   MS Name/IP address Stratum Poll Reach LastRx Last sample </pre>
Root delay : 1.00000000 seconds	<pre>[root@dmzcdrenl02 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  </pre>
이 같이 가지 않는 것 것 이 밖에 가지 않는 것 같아. 이 것 이 것 이 것 이 것 이 것 이 것 이 것 이 것 이 것 이	<pre>[root@dmzcdrenl02 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  </pre>
Root dispersion + 1 00000000 seconds	<pre>[root@dmzcdreml02 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  xxxx [ yyyy ] +/- zzzz !! Reachability register (octal) ! xxxx = adjusted offset, !! Log2(Polling interval) ! yyyy = measured offset, !! Log2(Polling interval) ! yyyy = measured offset, !! Log2(Polling interval) ! yyyy = measured offset, !!</pre>
ware araberated , rightanana accounts	<pre>[root@dmzcdreml02 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  xxxx [ yyyy ] +/- zzzz !! Reachability register (octal) ! xxxx = adjusted offset, !! Log2(Polling interval) ! yyyy = measured offset, !! Log2(Polling interval) ! yyyy = measured offset, !! Log2(Polling interval) ! yyyy = measured offset, !!</pre>
Update interval : 0.0 seconds	<pre>[root@dmzcdreml02 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  xxxx [ yyyy ] +/- zzzz !! Reachability register (octal) ! xxxx = adjusted offset, !! Log2(Polling interval) ! yyyy = measured offset, !! Log2(Polling interval) ! yyyy = measured offset, !! Log2(Polling interval) ! yyyy = measured offset, !!</pre>
	<pre>[root@dmzcdreml02 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.  xxxx [ yyyy ] +/- zzzz [] Reachability register (octal)   xxxx = adjusted offset, [] Log2(Polling interval)   yyyy = measured offset, [] Log2(Polling interval)   yyyy = measured offset, []   log2(Polling interval)   yyyy = measured offset, []                                      </pre>
Lean status / Not sunchronised	<pre>[root@dmzcdrem102 ~]# chronyc sources -v 210 Number of sources = 2  Source mode '^' = server, '=' = peer, '#' = local clock. / Source state '*' = current synced, '+' = combined , '-' = not combined,   / '?' = unreachable, 'x' = time may be in error, '~' = time too variable.   xxxx [ yyyy ] +/- zzzz    Reachability register (octal)   xxxx = adjusted offset,   Log2(Polling interval)   yyyy = measured offset,   Log2(Polling interval)   yyyy = measured offset,   MS Name/IP address Stratum Poll Reach LastRx Last sample </pre>

To resolve this behavior, we added a parameter called "maxdistance" with a value of 15 to mitigate this gap.

Root cause: in the "chrony sources" output, "+/- 10.8 s" is larger than the default "maxdistance" of 3 seconds (if not part of the chrony.conf). The maxdistance parameter was added in chrony-2.2, so that's why it worked with chrony-2.1. Older versions only have



a hardcoded limit for the root dispersion to be smaller than 16 seconds. The NTP server has a root dispersion of about 3.6 seconds.

### **19 How to Upgrade Votiro Cloud**

To obtain the benefits provided by the latest version of Votiro Cloud it is recommended to run on the most recent release of the product.

The latest Votiro Cloud version has new and enhanced features, improved security, and bug fixes. A new product release is announced to customers via an email from Votiro.

We recommend upgrading your installation to the latest version as soon as possible. Votiro's Support team will be available to provide any required assistance.

#### **19.1 Upgrade Installation**

#### **19.1.1** Before You Begin

Take VM snapshots of the three nodes before starting the upgrade.

#### **19.1.2 Procedure**

To upgrade your installation of Votiro Cloud to the latest version, you must perform the following steps:

- 1. Request the Dropbox link to the upgrade package from Votiro Support.
- 2. Create the **upgrade** folder under **root** if it does not exist and then copy the upgrade package to the **upgrade** folder in Node 1. Note that the **upgrade** folder name must be lowercase.

For example:

yum install wget -y && mkdir -p /root/upgrade && cd upgrade wget -0 upgrade.zip https://www.dropbox.com/.../upgrade-9.6.xxx.zip dl=1

where ... and xxx are components in the Dropbox link specific to the release version

3. Extract the zip file in the **upgrade** folder, using the following command:

#unzip upgrade.zip

4. Run the upgrade script to install the upgrade:

#./upgrade.sh

- 5. At the end of the installation, the message Upgrade complete! appears.
  - If you are upgrading to version 9.6.3:

Below this message will appear a list of three encryption keys: **KEY**, **IV** and **SALT** for Blob storage operations. You must save these keys in a safe place because they cannot be retrieved.

If you are upgrading <u>from version 9.6.3 or later</u>:



The encryption keys are not displayed.

6. The installation log is saved in the file **votiro-upgrade.log**. If any problems are encountered during the installation, you must provide this file to Votiro Support.

#### Note

The upgrade installation is automatic and unattended, with no user prompts. All nodes in the cluster will be automatically upgraded. The entire installation process may take some time, typically between ten minutes to a half hour.

#### **19.1.3** Verification of Upgrade

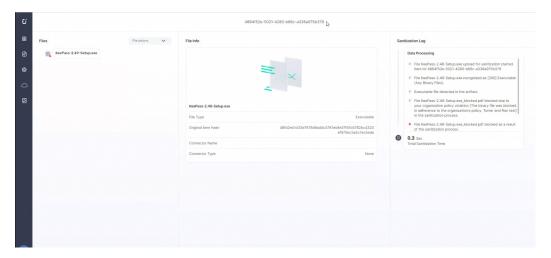
To verify that the upgrade has completed successfully, wait a few minutes, then login to the Management Dashboard. The version number you have upgraded to is displayed.

### 20 How to Use Kibana to Troubleshoot Votiro Incidents

This page describes how to use Kibana to view and troubleshoot Votiro Incidents.

#### 20.1 Example of Votiro Incident

The following screenshot displays the Votiro Item/Incident sanitization information for a file that has undergone sanitization:



This screen shows the results of Votiro Cloud processing a file named KeePass-2.49-Setup.exe. The **File Info** pane displays some of the file properties and the **Sanitization Log** pane displays highlights of the file **Data Processing**.

#### 20.2 Procedure

#### 20.2.1 Create and Configure an Index Pattern

To begin, you must define a Kibana index pattern.

- 1. Login to the Kibana Discover interface with the credentials provided to you by Votiro Support.
- 2. Select Create index pattern. Step 1 of 2 Define index pattern appears.
- 3. Type **votiro-logs\*** (or similar) as the Index pattern. Kibana displays a list matching the index pattern:

Elasticsearch		
Elasticidad      Index Management     Index Management     Index Management     Index Management     Index Management     Sangabita and Restore     License Management     Soluparade Assistant     Most Ratients     Spaces     Reporting     Advanced Settings	Create index patterns to retrieve data from Eastlosserch indices for things like visualizations.	Include system indication (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)

#### 4. Click on Next step. Step 2 of 2 Configure settings appears.

K	Management / Index patterns / Create index pattern			
• •	Elasticsearch Index Management Index Lifecycle Policies Rollip, Jose Transforms Remote Clusters	Create index pattern Ribana uses index patterns to retrieve data from Elasticsearch indices for things like visualizations. Step 2 of 2: Configure settings		X Include system indices
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Snapshot and Restore License Management 8.0 Upgrade Assistant	You've defined <b>votiro-logs</b> * as your index pattern. Now you can specify some settings before we create it. Time Filter field name Refresh		
9 III (5	Kibana Index Paterns Saved Objects Spaces Reporting	©t Gtimostamp Nay Received Timo con Received allow quiery/From		
8 9	Advanced Settings	I don't want to use the Time Filter C	Back	Create index pattern
6				

5. Select a **Time Filter field name** from the list. For example, **@t**:

Elasticsearch Index Management Index Lifecycle Policies Rollup Jobs	Create index pattern Klana usei index patterns to retrieve data from Elasticsearch indices for things like visualizations.	X Include system indi
Transforms Remote Custers Snapshot and Restore License Management 8.0 Upgrade Assistant <b>K kiban</b> Index Patters Saved Objects Spaces Reporting	Step 2 of 2: Configure settings         You've defined votiro-logs* as your index pattern. Now you can specify some settings before we create it.         The Time Filter will use the fact to the your data by time.         You can choose not how a stime filter buy you will not be able to narrow dawn your data by a time tange.         > Show advanced options	
Advanced Settings	< Ba	Create index pattern
	< Ha	ck Create index pat

6. Click on **Create index pattern**. Kibana displays every field and field type in the selected index (in this example, votiro-logs\*):

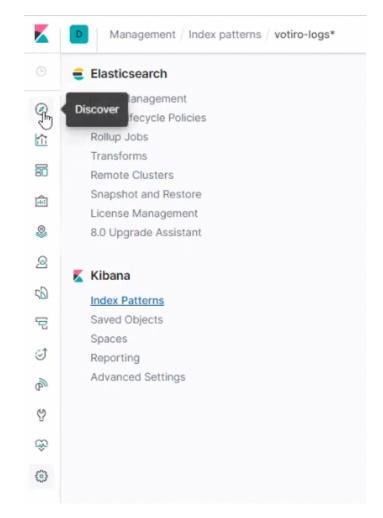
Elasticsearch Index Management Index Lifecycle Policies Rollup Jobs Transforms Remote Clusters Snapshot and Restore	★ VOTIFO-LOG Time Filter field name: This page lists eve Elasticsearch Map		index and the field's asso	ciated core type a	s recorded by Elast	icsearch. To chang	* C I
License Management	Fields (181)	Scripted fields (0)	Source filters (0)				
8.0 Upgrade Assistant	Q Filter						All field types
Kibana	Name		Туре	Format	Searchable	Aggregatable	Excluded
Saved Objects Spaces	Filter		string		•		
Reporting	Filter.keyword		string		•	•	
Advanced Settings	0		string				
	0.keyword		string		•	•	
	1		string		•		
	1.keyword		string		•	•	
	2		string				
	2.keyword		string		•	•	
	3		string				
	3.keyword		string		•	•	
	Rows per page: 10	~				< 1	2 3 4 5 19

#### 20.3 Analyze the Data

After the index pattern is created and configured, apply it to the data in Kibana's Discover mode to yield useful results by additional filtering of the data.

#### 20.3.1 Discover

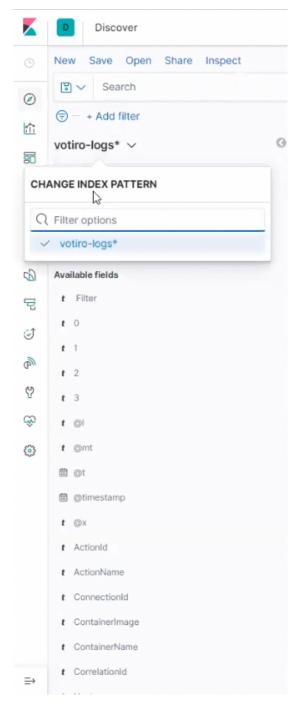
1. Click on the Discover icon on the left side of the screen:



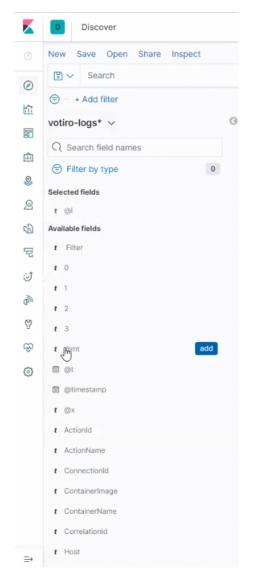
2. Kibana displays all hits that match the time filter criteria within the time range indicated (in this example, for the last 15 minutes):

New Save Open Share Inspect		
😰 🗸 Search		KQL 🛗 🗸 Last 15 minutes Show dates Cl Refresh
😨 – + Add filter		
votiro-logs* (r)	9	121 hits
Q Search field names		Nov 8, 2021 @ 10:58:03.404 - Nov 8, 2021 @ 11:13:03.404 - Auto 🗸
<ul> <li>Filter by type</li> <li>0</li> </ul>		
Selected fields	00 00	
()_source	90 00 20	
Available fields		
t Filter	10:59:00	11:00:00 11:01:00 11:02:00 11:00:00 11:06:00 11:00 11:00 11:00 11:00 11:00 11:00 11:00 11:00 11:00 11:00 11:00 11:00 11:
10		@t per 30 seconds
e 1	Time 🗸	Tente
1 2	> Nov 8, 2021 @ 11:12:46.871	#timestamp: Nov 8, 2021 0 11:12:46.871 PodName: mg-service-release-deployment-84b4877655-22v2v Host: t-n2.prod.votiro.com ContainerName: mg-service-release dt: Nov 8, 2021 0 11:12:46.871 Bmt: Configuration has been reloaded #1: Information SourceContext: ReleaseService.Program MachineName: mg-service-release-deployment-84b4877655-22v2v ItemId: no
t 3		In Live of the comparison of the second
r 0i	> Nov 8, 2021 0 11:12:46.071	
t Ont	/ NOV 6, 2021 0 11:12:40:6/1	<pre>@timestamp: Nov 8, 2021 0 11:12:46.871 PodName: mg-service-release-deployment-84b4877d55-2x/2v Host: t=n2.prod.vetire.com ContainerName: mg-service-release dt: Nov 8, 2021 0 11:12:46.871 Bet: Use config key 'RELEXSE_MAIL_TEMPLATE'='Resources/ReleaseMailTemplate.html' 01: Information SourceContext: ReleaseService.Program MachineName: mg-service-</pre>
10 OT		release-deployment-8404877d55-2zv2v ItemId: no itemid CorrelationId: no correlationId ServiceId; release-service _id; SkfS_nm8xsyV31r5St00 _type: _doc _index: votiro-logs-
Ctimestamp		600195 _score: -
t ©×	> Nov 8, 2021 0 11:12:46.871	@timestamp: Nov 8, 2021 0 11:12:46.871 Publiane: mg-service-release-deployment-84b4877d55-2zv2v Host: t-n2.prod.votiro.com ContainerName: mg-service-release @t: Nov 0, 2021 0
t ActionId		11:12:46.871 Bmt: Use config key 'username's'' 01: Information SourceContext: ReleaseService.Program Hachinetame: mg-service-release-deployment-8454877655-22:2V ItemId: no itemid CorrelationId: no correlationid ServiceId: release-service _id: 30f5_meXxsY31r55108 _type: _doc _index: votiro-loos-000105 _score: -
t ActionName		Itemio row.erartouro: wo co.erartouro seiviteiro: Latesee.seivite 18: seiz unexsize izoite 7006: 7000 Tuodesee isoitio, 7600.6.
t ConnectionId	> Nov 8, 2021 0 11:12:46.871	
t Containerimage		11:12:46.871 Omt: Use config key 'RELEASE_MAIL_SUBJECT's' ' 01: Information SourceContext: ReleaseService.Program MachineMame: mg-service-release-deployment-8404877d55-2zv2v ItemId: no itemid CorrelationId: no correlationid ServiceId: release-service_id: 4EF5_nmeXxyY31r5S198_type:_doc_index: votiro-log-000105_score: -
t ContainerName		
	> Nov 8, 2821 @ 11:12:46.871	Stimestamp: Nov 8, 2021 0 11:12:46.871 PodName: mng-service-release-deployment-84b4877d55-22v2v Host: t-n2.prod.votiro.com ContainerName: mng-service-release 0t: Nov 8, 2021 0

3. To further filter the results, click on  $\vee$  next to the index pattern (votiro-logs\* by default) in the left side of the screen. The **CHANGE INDEX PATTERN** window opens:



4. Move the cursor down the list of **Available fields** to select fields to filter. Then click on the **add** button to add the field to the filter:



- 5. In the example below, the following fields are added:
  - @I level
  - @mt message template
  - @x exception
  - ContainerName
  - CorrelationId
- 6. The display of hits is now updated to show only the selected fields:

New Save Open Share Inspect				
🛐 🗸 Search		KQL 🗒	<ul> <li>Last 15 minutes</li> </ul>	Show dates C Refre
- + Add filter				
votiro-logs* ~	0	121 hits		
Q Search field names		Nov 8, 2021 @ 10:58:03.404 - Nov 8, 2021 @ 11:13:03.404 - Auto	~	
<ul> <li>Filter by type</li> </ul>				
	60			
f Gl	05 Count			
t Gmt	20			
t Gx	0 10.59:00	1100.00 1101.00 1103.00 1104.00 1105.00 11.0800 11.0700	11.08.00 11.09.00 11.10.00	11.11.00 11.12.00
t ContainerName		@t per 30 seconds		ContainerName
t CorrelationId	Time 🗸	@mt	@×	Correlationid
Available fields	> Nov 8, 2021 0 11:12:46.871	Info Configuration has been reloaded rmat	-	mng-service-rele no correletio ase
t Filter		100		#36
10	> Nov 8, 2021 0 11:12:46.871	Info Use config key 'RELEASE_MAIL_TEMPLATE'='Resources/ReleaseMailTemplate.html'		
	> Nov 8, 2021 0 11:12:46.871	Info Use config key 'RELEASE_MAIL_TEMPLATE'='Resources/ReleaseMailTemplate.html' rmat son		mng-service-rele no correlatio ase
t 0 t 1 t 2		rmat ion Info Use config key 'username'=''		ase mng-service-rele no correlatio
1.1		reat ion		ase
t 1 t 2	> Nov 8, 2021 @ 11:12:46.871	rmat 2nn Defn Ube config key 'username'=' 2nn Son	- - 0.0	asè mng-service-rele no correlatio ase
t 1 t 2 t 3 00 01	> Nov 8, 2021 @ 11:12:46.871	rmat 200 Dofo Use config key "coername"=" 300		asé mng-service-rele no correlatic ase
f 1     f 2     f 3     Ø 01     Ørtestamp     f Actorid	<ul> <li>Nov 8, 2021 0 11:12:46.871</li> <li>Nov 8, 2021 0 11:12:46.871</li> </ul>	rmat Toto Use config key 'username's'' Toto Use config key 'RELEAR_MAIL_DEALET's' ' Proto Use config key 'RELEAR_MAIL_DEALET's' '		ase mg-service-rele no correlatio ase mg-service-rele no correlatio ase
f 1 f 2 f 3 m 0t @ otimestamp	<ul> <li>Nov 8, 2021 0 11:12:46.871</li> <li>Nov 8, 2021 0 11:12:46.871</li> </ul>	rmat Defo Use config key 'HELEASE_DEDUCT_FORMER's'' Lon Defo Use config key 'HELEASE_DEDUCT's'' rmat Lon Defo Use config key 'HELEASE_DEDUCT_ACOMESS''http://blm-service.com		ase mg-sarvice-rele no correlatio ase mg-sarvice-rele no correlatio ase
f 1     f 2     f 3     Ø 01     Ørtestamp     f Actorid	<ul> <li>Nov 8, 2021 0 11:12:46.871</li> <li>Nov 8, 2021 0 11:12:46.871</li> <li>Nov 8, 2021 0 11:12:46.871</li> </ul>	rmat Inf Use config key 'usernam' *'' Inf Use config key 'NELKAEL_NAIL_DAUCT'*' Inf Inf Use config key 'NELKAEL_NAIL_DAUCT'*' Inf		mg-service-rele no correlatio ase mg-service-rele no correlatio ase mg-service-rele no correlatio

#### 20.3.2 Votiro Explore Incident & File Info

To examine a specific file that was processed by Votiro Cloud, the threat ID is obtained from the Votiro Item/Incident sanitization information.

1. Open the Votiro Explore Incident:

ũ		4864f52e-5021-4280-b66c-a336a975b379 🎝	
88	Files File actions V	File Info	Sanitization Log
0	KeePass-2.49-Setup.exe		Data Processing File KeePass-2.49-Setup.eve upload for sanitization started.
ه ۵			Item Id: 4864/52e-5021-4280-b66c-a336a075b379 File KeePass-2.49-Setup.exe recognized as [300] Executable (Any Binary Files).
2		KeePass-2.49-Setup.exe	<ul> <li>Executable file detected in the artifact.</li> <li>File KeePass-2.49-Setup.exe, blocked pdf blocked due to your organization policy violation [The binary file was blocked</li> </ul>
		File Type	in adherence to the organization's policy. Tomer and Ron test] Executable in the santization process. • File KeePass-2,49-Setup.exe, blocked, pdf blocked as a result
		Original Item Hash 48fd2eb1d33d7678d8ad5c5781eb8e2f1 ef975	61b5782bc4320 of the sanitization process. bc535c7ec5ede 0 0.3 Sec
		Connector Name	Total Santization Time
		Connector Type	None

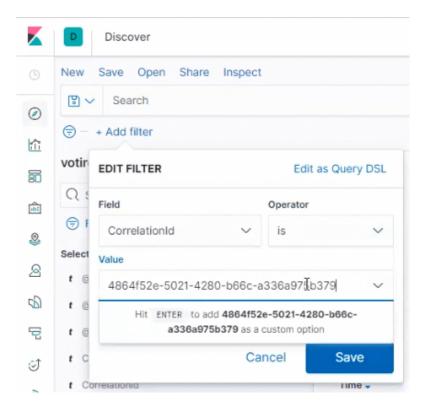
2. Copy to the clipboard the file ID at the top of the screen, in this example:

4864f52e-5021-4280-b66c-a336a975b379

#### 20.3.3 File Sanitization Analysis

- 1. Return to the Kibana Discover screen.
- 2. In the left side of the Kibana Discover screen, click on **Add filter**. The **EDIT FILTER** window opens.
- 3. From the **Field** list, select **CorrelationId**.
- 4. From the **Operator** list, select **is**.

5. In the **Value** field, paste the file ID from the clipboard .



6. Click on **Save**. The list of hits displayed is updated to show only those hits for the relevant file, according to the CorrelationId (= Votiro item).

Net	w Save Open Share Inspect									
2	ĵ ∽ Search					KQL 🗇 V Last 15	minute	15	Show dates	C Refre
6	CorrelationId: 4864152e-5021-4280-b66c-a3	336a975	5b379 × + Add filter							
vot	tiro-logs* v	0			61 hits					
Q	Search field names				Nov 8, 2021 @ 10:59:15.233 - Nov 8, 2021 @ 11:14:15.233	Auto V				
	) Filter by type 0		60 50							
Sele	ected fields	ŧ	40							
	01	Cou	30 20							
ŧ	8mt		10							
t	Øx		11.00.00	11.01.00	11:02:00 11:03:00 11:04:00 11:05:00 11:07:00 (01 per 30 seconds	11.08.00 11.09:00	1	110:00 11:11:00	11:12:00 11:13:00	
t	ContainerName			0	Billing to seconds				ContainerName	
t	Correlationid		Time 🗸	•	@mt			@×		CorrelationId
	allable fields	>	Nov 8, 2821 0 11:09	:34.030 Warn	n Failed to create /votirocache/files folder for large files			System.UnauthorizedAcc essException: Access t		4864f52e-582 88-b66c-a336
	Filter							o the path '/votirocac he/files' is denied.		b379
	0							> System.IO.IOExce ption: Permission deni		
t								ed		
t	2	>	Nov 8, 2021 0 11:09	:34.030 Warn	n Files-Cache folder '/votirocache/files' is not exists, will created now				sds-service-repor ter	4864f52e-582 88-b66c-a336
t	3			1.19						b379
	(Gt	>	Nov 8, 2021 0 11:09		n Failed to create /votirocache/files folder for large files			System.UnauthorizedAcc		4864f52e-582
8	©timestamp			ing				essException: Access t o the path '/votirocac he/files' is denied.	Cer	88-b66c-a336 b379
	ActionId							> System.IO.IOExce ption: Permission deni		
t	ActionName				P			ed		
t	ConnectionId	>	Nov 8, 2021 0 11:09		u Cleaning cache keys for requestId: '4864f52e-5021-4280-b66c-a336a975b379'					4864f52e-582
	ContainerImage			9					ter	88-b66c-a336

7. To change the time frame of the display, click on the time icon  $\stackrel{\text{def}}{=}$   $\checkmark$ . Then select the desired time interval:

		շիդ		
Quick select		0		< >
Last 🗸	15	minu	ites ~	Apply
Commonly used				
Today		Last 24	hours	
This week		Last 7 da	ays	
Last 15 minutes		Last 30	days	
Last 30 minutes		Last 90	days	
Last 1 hour		Last 1 ye	ear	
Recently used date	ranges			
Today				
This week				
Last 30 minutes				
Refresh every				

8. To view the file processing history in Votiro, scroll down the list of hits. The selected fields displayed in the columns provide more information as to what occurred during the processing. Using the *@l* (message level), *@mt* (message template) and *@x* (exceptions) columns provides you with detailed information that can help you to troubleshoot the incident.

### 21 Message Size Limits in Exchange

This article describes why emails may not reach their destination or appear in sanitization log files.

#### 21.1 Symptoms

The email (eml) size may increase as a result of the sanitization process. The size of the email message may then exceed the size limit set in Exchange Server.

#### 21.2 Solution

To avoid blocked emails in Exchange servers due to message size limitations, follow this TechNet guide:

https://technet.microsoft.com/en-us/library/bb124345(v=exchg.160).aspx

#### 21.3 Limitations

Organizational limits apply to Exchange 2016 servers, Exchange 2013 Mailbox servers, and Exchange 2010 Hub Transport servers that exist in your organization. Organizational limits that you configure on Edge Transport servers are applied to the local server.

By default the "Maximum size of a message received" is set to 10MB.

If Exchange is your responsibility change this parameter according to your organization policy. If Exchange is part of the Votiro Votiro Cloudcloud solution, contact Votiro Support.

### 22 MSSP User Guide

A Managed Security Service Provider (MSSP) provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services.

Examples of MSSP use cases supported by Votiro include:

- Creating new customers and assigning licenses by the MSSP admin
- Viewing/filtering all the MSSP customer's data on the MSSP dashboard
- Using the MSSP incidents to see/filter all the MSSP customer's incidents data
- Creating reports on each MSSP customer's data

#### 22.1 MSSP Tenant Management

1. Login

To login to MSSP Tenant Management, use the following URL address:

"https://{clusterName}/portal/#/votiro/login"

A login page will be displayed. Contact Votiro support to get the admin user credentials.

Email	
LOG IN	

After successful login, the Votiro MSSP Tenant Management screen is displayed:

ADD TENANT							
Name	ID	Domains	License Type	License Quota	License Expiration	License Features	
test-tomer	2a167928#d0##d0##67d18f8	tomer.com	Consumption	0Bytes / 4TB	05-06-2024 (352 days remaining)	<ul><li>menlo</li><li>awsS3</li><li>chrome</li></ul>	ACTIONS
votiroapj-mssp	3aa2940a <b>4da15 4103 et al</b> ec5490da997	votiroapj-mssp.com	Consumption	224.8KB / 10TB	15-06-2024 (361 days remaining)	<ul><li>menlo</li><li>awsS3</li><li>chrome</li></ul>	ACTIONS
demo-mssp	7aa33a3b-61-01-01-01-04810423410c	demo-mssp.com	Consumption	25.8MB / 46TB	05-06-2024 (352 days remaining)	<ul><li>menlo</li><li>awsS3</li><li>chrome</li></ul>	ACTIONS
king	93d29e214000 100000000000000000000000000000000	king.com					ACTIONS
demotenant1	96d257cb-6b-20219c2b25	demotenant1.com	Consumption	3.1MB / 10TB	05-06-2024 (352 days remaining)	<ul><li>menlo</li><li>awsS3</li><li>chrome</li></ul>	ACTIONS
votiro-dev	be9d9b4b4f	votiro-dev.com	Requests	0 / 10,000,000,000	15-06-2024 (362 days remaining)		ACTIONS

The MSSP admin can use the Tenant Management screen to:

Add a customer tenant

- View the list of customer tenants
- View customer traffic information
- Manage each customer tenant's license
- View total actual usage compared to total license quota
- Delete customer tenants

#### 2. Add a customer tenant

To add a new customer tenant, press the **ADD TENANT** button.

Comma separated domain list
Comma separated domain list
Comma Separated domain list

#### Enter:

- Tenant name for example, King Demo
- Comma separated domain list for example, kingdemo.com. If there are multiple domains, separate the domains by a comma. For example, kingdemo.com, rontest.com

After adding a new customer tenant, a default admin user will be created. Contact Votiro support to get the admin user credentials.

#### 3. View the customer's tenant list

The following information is displayed on the Tenant Management screen for each tenant:

- Name Tenant name as configured in creation
- ID Tenant ID generated in UUID format
- Domains As configured in creation
- License Type The possible options are:
  - **Consumption** count by volume usage
  - Requests count by files

- License Quota Actual usage / License quota, as configured in the license import. The system will display up to date tenant usage.
- License expiration Expiration date and days remaining
- License features Currently, the possible options are:
  - menlo
  - aws s3
    - chrome
- 4. Import a license

To import a license for a customer tenant, press the corresponding **ACTIONS** button and select **IMPORT LICENSE**.

License type		
REQUESTS	CONSUMPTION	OBSOLETE
License Usa	ge: 110TB/50TB	
0		
GB TB		
Start date		
12/06/2023		
End date		
19/06/2024		
Feature flags		
Menlo		
AWS S3		
Chrome		
URL Reput	ation Coming soon	
	ADD LICENSE	
ter or select:		
License type		

- License Usage
- Start date
- End date
- Feature flags (if needed)

After creating a license, the system will display the imported license in:

- Votiro MSSP Tenant Management screen
- Customer tenant Management console license page
- 5. **Download Analytics Report**

To download an analytics report for any of the customer's tenants, press the corresponding **ACTIONS** button and select **DOWNLOAD REPORT**.

01/05/2023	
nd date	
19/06/2023	

Enter the **Start date** and **End date** to select the report's time interval, and press **GENERATE REPORT**. The report will be downloaded in CSV format.

		Formulas Data Review View Automate He	elp	Acro	opat					
	Cut Calibri	- 11 - A^ A = Ξ Ξ 🗞 - >¶ - ab Wrap			p Text		General ~			B
	Paste Copy ~ B I U	· 🖽 • 🖄 • 🔺 • 🛛 = = = = = =		🕀 Mer	ge & Cente	r v	<b>1</b>	% ,	€0.00	Cor
	<ul> <li>✓ Sormat Painter</li> </ul>		1		ge et cente		-0	/0 /	.00 -00	Form
	Clipboard 😼	Font 🛛 Alignmer	nt			۲ <sub>2</sub>		Number	F3	i
B	24 $\checkmark$ : $\times \checkmark f_x$									
	A	В		с	D		E	F	G	H
1	Customer name	Ron company								
2	Report dates	01/05/2023 - 20/06/2023								
3	Total Files processed	16								
4	Total Files sanitized	15								
5	Total Files blocked	1								
6	Total PPF files detected	0								
7	Number of emails	1								
8	Number of threats detected	2								
9	Average file size	1672870 bytes								
10	Average processing time	6.3325 seconds								
11										
12	License mode files	Consumption								
13	License permitted files	5.05775E+13								
14	Number of Files used so far	16								
15	License permitted consumption quota	5.05775E+13								
16	License consumption used so far	27024047								
17	License usage	0.00%								
18	Expiration date	05/06/2024 15:13								
19										

#### 6. **Delete a customer tenant**

To delete a customer tenant, press the corresponding **ACTIONS** button and select **DELETE TENANT**.

### 22.2 Monitoring Tenant Activity

#### 1. MSSP Dashboard

The MSSP user can view and filter Dashboard data by customers tenant selection.

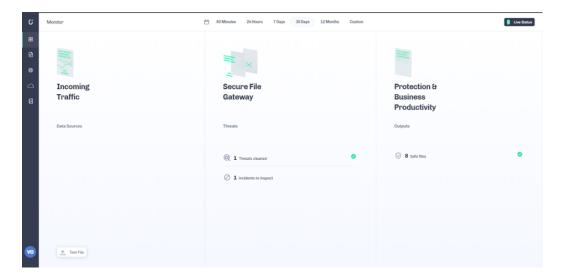
ď	Moniton Tenants ·	😂 60 Minutes 24 Hours 7 Days 30 Days 12 Months Custom	Uve Status
88	Q Bearch Checkal Undexial		
0	V test-turner V demo-masp V King-test	× ×	
٢	Gerrotenanet Gy votre-dev	-	
	Incoming Traffic	Secure File Gateway	Protection & Business
0			Productivity
	Data Sources	Threats	Outputs
		① Threats cleaned     ③	279 Safe files
		1 incidents to inspect	
HS	1 Test File		
-	C. marine		

#### 2. MSSP Incidents

The MSSP user can view and filter incidents data by customer tenant selection in the **Tenants** column.

G	Incidents									٩
88	Date time 👻 Status 👻	Release status 👻	Connectors - Tenants - K							c
0	Date & Time 💌	Tenant name	File name Check all	From	То	Cc	Connector type	Connector name	Blocked files	
0	11/06/2023 12:51	demo-mssp	Votiro_Auditi				None	Self-sanitization		
	11/06/2023 12:51	demo-mssp	☑ Votiro-MSTe ☑ demotenant1 ☑ votiro-dev				None	Self-sanitization		
	11/06/2023 12:48	demo-mssp	Votiro_AuditReport_03,				None	Self-sanitization		
	07/06/2023 12:26	demotenant1	Votiro_AuditReport_16_1				None	Self-sanitization		
	07/06/2023 12:25	demo-mssp	B Ripp				None	Self-sanitization		
	07/06/2023 12:25	demo-mssp	11248-close-up-portrai				None	Self-sanitization		
	07/06/2023 12:24	demo-mssp	Ripg				None	Self-sanitization		
	07/06/2023 10:48	demo-mssp	11248-close-up-portrai				None	Self-sanitization		
	06/06/2023 12:06	demotionant1	Votiro_AuditReport_16_I				None	Self-sanitization		
MS	06/06/2023 12:05	demotenant1	Votiro_AuditReport_16_I				None	Self-sanitization		
					1 2 > >>					1/2

#### 3. MSSP Customer's Dashboard



An MSSP customer's user can view data only from their own tenant.

#### 4. MSSP Customer's Incidents

An MSSP customer's user can view data only from their own tenant.

							(
Status 👻 Release status							
Time · File name	Subject	From	То	Ce	Connector type	Connector name	Blocked files
1023 13:44 🔳 Chromes	etup.exe				None	Self-sanitization	⊘1
1023 13:43 💿 SMTP C	nnector User Ouic				None	Self-sanitization	
			1				
	Time • File name	Time • File name Subject	223 13:44 🥫 CivoneSetup axe	ine • Fiterane Babjet From fo 2023 13.44 Chandistepsee 2023 13.43 Chandistepsee 2023 13.43	ine • Fiterane Babjet From to Co 2023 13.44 Connector Bae Out 2023 13.43 Strift Connector Bae Out	Pile name     Stabled     Pilem     To     Oc     Connector type       2023 13.43     © Dromsdordugase     Nome     Nome	Pile name     Stadpet     Pem     To     Cc     Connector type     Connector rame       2023 13.43     © Chronoctor tiber Guit     Nome     Self-sentization