

VOTIRO

Votiro VA On-prem v9.9

# Knowledge Base

July 2025

## 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](http://www.votiro.com)

# Contents

- 1 Assigning a Control Plane VIP and Default VIP in AWS VA ..... 8**
  - 1.1 Procedure ..... 8
- 2 Assigning a Control Plane VIP and External LB in Azure VA ..... 12**
  - 2.1 Procedure ..... 12
- 3 Changing the CA Certificate ..... 16**
  - 3.1 Converting a CA Certificate ..... 16
  - 3.2 Applying CA Certificate to Kubernetes Cluster ..... 16
- 4 Changing the Kibana Password ..... 17**
  - 4.1 Solution ..... 17
- 5 Email Arrival is Delayed ..... 18**
  - 5.1 Symptoms ..... 18
  - 5.2 Solution ..... 18
  - 5.3 Expected result ..... 18
    - 5.3.1 Before: ..... 18
    - 5.3.2 Action: ..... 18
    - 5.3.3 After: ..... 18
- 6 How to Check that the External Load Balancer is Working with the Votiro On-prem Cluster ..... 20**
  - 6.1 Prerequisites ..... 20
  - 6.2 Procedure ..... 20
    - 6.2.1 Verify the Load Balancer is Connected to the Cluster ..... 20
- 7 How to Configure SSL Passthrough Load Balancing using NGINX ..... 22**
  - 7.1 Prerequisites ..... 22
  - 7.2 Procedure ..... 22
  - 7.3 Next Steps ..... 25
  - 7.4 NGINX File Example ..... 25
- 8 How to Configure the Votiro Appliance for AWS ..... 27**
  - 8.1 Prerequisites ..... 27
  - 8.2 Procedure ..... 28
- 9 How to Configure the Votiro On-prem Cluster with External Storage ..... 32**

- 9.1 Prerequisites ..... 32
- 9.2 Procedure ..... 32
  - 9.2.1 Declare a Mount ..... 32
  - 9.2.2 Add External Storage Path ..... 33
  - 9.2.3 Restart Pods ..... 33
- 9.3 Troubleshooting ..... 33
  - 9.3.1 Issue 1: Windows Server NFS sharing permission ..... 33
  - 9.3.2 Issue 2: Missing metadata in blob-config ..... 37
- 10 How to Deploy the Votiro On-prem Cluster in Azure ..... 38**
  - 10.1 Prerequisites ..... 38
  - 10.2 Procedure ..... 38
- 11 How to Integrate Azure AD Single Sign-on with Votiro VA On-prem using the Entra SAML Toolkit ..... 45**
  - 11.1 Prerequisites ..... 45
  - 11.2 Configure the Azure Portal ..... 45
  - 11.3 Configure the Votiro Management Console ..... 48
- 12 How to Integrate SIEM with Azure Sentinel ..... 51**
  - 12.1 System prerequisites ..... 51
  - 12.2 Procedure ..... 51
    - 12.2.1 Manual/Offline Deployment ..... 51
- 13 How to Integrate Votiro On-prem Syslog Messages with Sumo Logic using HTTP Logs ..... 63**
  - 13.1 Procedure ..... 63
    - 13.1.1 Configure an HTTP Logs and Metrics Source in Sumo Logic ..... 63
    - 13.1.2 Create the Field Extraction Rules at Ingest Time ..... 65
    - 13.1.3 Install the Votiro App ..... 67
    - 13.1.4 Integrate the Votiro Management Console with the Sumo Logic HTTP Logs Collector ..... 69
    - 13.1.5 Verify the Integration ..... 70
- 14 How to Integrate Votiro with Google Workspace ..... 73**
  - 14.1 Procedure ..... 73
    - 14.1.1 Create a Host ..... 74

14.1.2 Configure content compliance rule for emails received from Votiro On-prem .....	75
14.1.3 Configure Content compliance rule for emails sent to Votiro On-prem ....	79
14.1.4 Votiro Cloud for Sanitization .....	80
14.1.5 Spam Rule .....	81
14.1.6 Prevent Email Authentication Protocol Failures .....	81
14.1.7 How To Resolve Google's SPAM Email Alert On SaaS .....	82
<b>15 How to Integrate Votiro On-prem with Sumo Logic .....</b>	<b>84</b>
15.1 System Requirements .....	84
15.2 Procedure .....	84
15.2.1 Configure the Sumo Logic Syslog Collection .....	84
15.2.2 Create the Field Extraction Rules at Ingest Time .....	88
15.2.3 Install the Votiro App .....	89
15.2.4 Integrate Votiro Management Console with Sumo Logic Syslog Collector ..	92
15.2.5 Search Ingested Data inside Sumo Logic .....	93
15.2.6 Event Simulator .....	94
<b>16 How to Obtain a Votiro On-prem License Key .....</b>	<b>96</b>
16.1 Obtaining a License key .....	96
16.1.1 Procedure .....	96
16.2 Verifying VotiroVotiro On-prem Activation .....	96
16.3 Renewing Your Votiro License Key .....	97
<b>17 How to Send Files to Votiro via Postman .....</b>	<b>98</b>
17.1 Prerequisites .....	98
17.2 Procedure .....	98
17.2.1 Generating a Service Token .....	98
17.2.2 Postman Setup .....	102
<b>18 How to Set a Profile for a Domain Group .....</b>	<b>109</b>
18.1 Instructions .....	109
<b>19 How to Sync with an NTP Server .....</b>	<b>110</b>
19.1 Solution .....	110
19.2 External NTP Server .....	110

- 19.3 Internal NTP Server ..... 110
- 19.4 Verify Time of Synchronization for each Node ..... 111
- 20 How to Troubleshoot NTP using Chrony in VA ..... 112**
  - 20.1 Solution ..... 112
  - 20.2 Troubleshooting Example: NTP not synchronized with external server ..... 116
- 21 How to Upgrade Votiro On-prem ..... 119**
  - 21.1 Upgrade Installation ..... 119
    - 21.1.1 Before You Begin ..... 119
    - 21.1.2 Procedure ..... 119
    - 21.1.3 Verification of Upgrade ..... 120
- 22 How to Use Kibana to Troubleshoot Votiro Incidents ..... 121**
  - 22.1 Example of Votiro Incident ..... 121
  - 22.2 Procedure ..... 121
    - 22.2.1 Create and Configure an Index Pattern ..... 121
  - 22.3 Analyze the Data ..... 123
    - 22.3.1 Discover ..... 124
    - 22.3.2 Votiro Explore Incident & File Info ..... 128
    - 22.3.3 File Sanitization Analysis ..... 128
- 23 Message Size Limits in Exchange ..... 131**
  - 23.1 Symptoms ..... 131
  - 23.2 Solution ..... 131
  - 23.3 Limitations ..... 131
- 24 How to Use QR Code Sanitization ..... 132**
  - 24.1 Disarm QR Codes behavior ..... 132
  - 24.2 Votiro Administrator view ..... 137
- 25 Unsanitized Due to Timeout ..... 138**
  - 25.1 Symptoms ..... 138
  - 25.2 Solution ..... 138
- 26 URL Protection ..... 139**
  - 26.1 Workflow - Sanitize URLs ..... 139
- 27 Votiro On-prem Monitoring Guidelines ..... 142**

- 27.1 Solution ..... 142
- 27.2 Votiro On-prem Services - Votiro Services .....143
  - 27.2.1 Additional Health Indicators: ..... 143
- 27.3 Votiro On-prem Management Dashboard - Votiro Services ..... 143
  - 27.3.1 Additional Health Indicators: ..... 144

# 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.

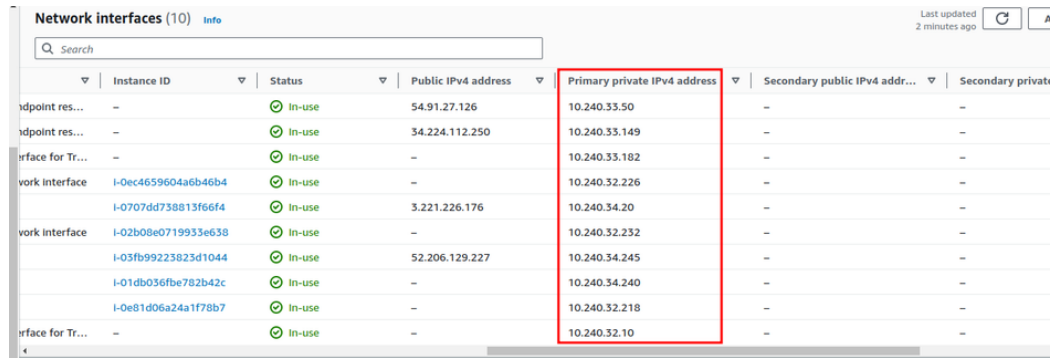
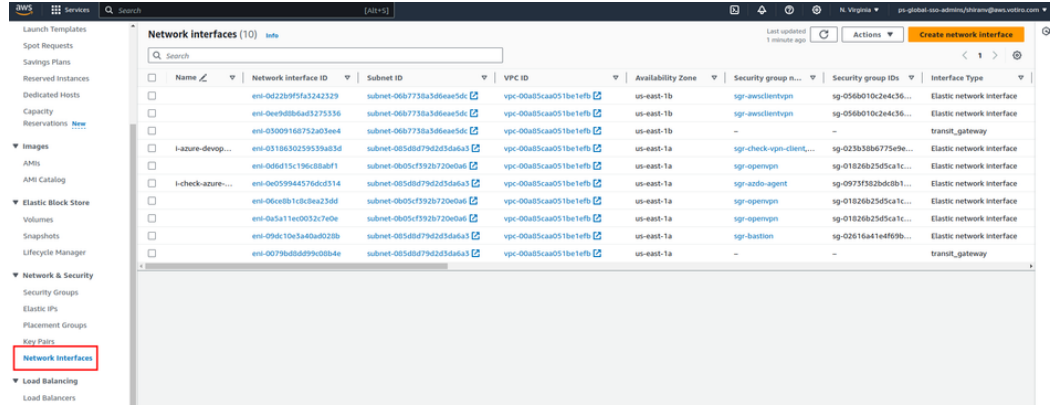
**Note:** If the customer is using an external load balancer, then only one IP should be added for Control plane vip and not paralus\_web\_vip.

## 1.1 Procedure

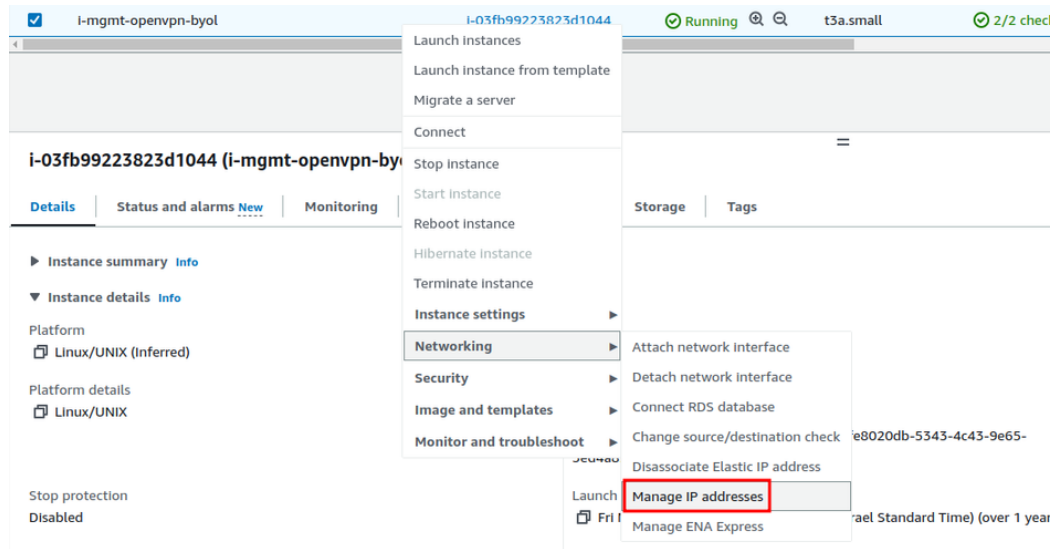
1. After creating three nodes in AWS VA, add two more IPs.
2. They are in the inventory.yaml in Ansible:

```
vars:
  approve_votiro_eula: no # read Votiro eula at: https://votiro.com/eula/ and set to yes to install.
  controlplane_vip_address: 4.4.4.4
  paralus_web_vip: 5.5.5.5 # false for external Load balancer. or set to a specific ip.
  votiro_cluster_fqdn: paralus-app.va.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\_zones
  ntp_servers: "pool.ntp.org time.google.com" # list of ntp servers separated 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.
  # Both volumes can have same nfs server and path.
  # example value(can use hostname): 10.10.11.11:/nfs_share_path
  blob_nfs: ""
  file_cache_nfs: ""
```

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**:



- 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**.



- The **IP addresses** window opens:

**IP addresses**

Instance ID  
 I-0e0efb314e253aea1 (shiran-test-va-1)

**ⓘ** To assign additional public IPv4 addresses to this instance, you must [allocate](#) Elastic IP addresses and associate them with the instance or its network interfaces.

▼ 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
<b>Assign new IP address</b>		

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.  
 Allow

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/cluster-infra/kube-vip/kube-vip.yaml** from **ens160** to the interface of your linux machine.

```
63     operator: Exists
64     - matchExpressions:
65       - key: node-role.kubernetes.io/control-plane
66         operator: Exists
67     containers:
68     - args:
69       - manager
70     env:
71     - name: vip_arp
72       value: "true"
73     - name: port
74       value: "6443"
75     - name: vip_interface
76       value: ens160
77     - name: vip_cidr
78       value: "32"
79     - name: cp_enable
80       value: "true"
81     - name: cp_namespace
82       value: kube-system
83     - name: vip_ddns
84       value: "false"
85     - name: svc_enable
86       value: "true"
87     - name: svc_leasename
88       value: plndr-svcs-lock
89     - name: vip_leaderelection
90       value: "true"
91     - name: vip_leasename
```

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):

```
55     app.kubernetes.io/version: v0.6.3
56     spec:
57       nodeSelector:
58         kubernetes.io/hostname: shiran-aws-va-1
59       affinity:
60       nodeAffinity:
```

```
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.

- 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
16 vars:
17   approve_votiro_eula: yes # read Votiro eula at: https://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 external Load balancer, 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
22   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 separated 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   # example value(can use hostname): 10.10.11.11:/nfs_share_path
29   blob_nfs: ""
30   file_cache_nfs: ""
    
```

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



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

## Add IP configuration ✕

shiran-va-2481\_z1

i A primary IP configuration already exists. Any additional IP configurations will be secondary. The virtual network this network interface is attached to only supports IPv4. [Learn more](#)

Name	<input style="border: 1px solid #ccc;" type="text" value="control-plane-vip"/>
IP version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Type	<input type="radio"/> Primary <input checked="" type="radio"/> Secondary
<b>Private IP address settings</b>	
Allocation	<input type="radio"/> Dynamic <input checked="" type="radio"/> Static
Private IP address	<input style="border: 1px solid #ccc;" type="text" value="10.0.0.25"/>
<b>Public IP address settings</b>	
Associate public IP address	<input type="checkbox"/>

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

```
15
16 vars:
17   approve_votiro_eula: yes # read Votiro eula at: https://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 external Load balancer, 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
22   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 separated 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   # example value(can use hostname): 10.10.11.11:/nfs_share_path
29   blob_nfs: ""
30   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
```

```
55 | app.kubernetes.io/version: v0.6.3
56 | spec:
57 |   nodeSelector:
58 |     kubernetes.io/hostname: shiran-aws-va-1
59 |   affinity:
60 |     nodeAffinity:
```

```
63 |     operator: Exists
64 |     - matchExpressions:
65 |       - key: node-role.kubernetes.io/control-plane
66 |         operator: Exists
67 |   containers:
68 |     - args:
69 |       - manager
70 |     env:
71 |       - name: vip_arp
72 |         value: "true"
73 |       - name: port
74 |         value: "6443"
75 |       - name: vip_interface
76 |         value: ens160
77 |       - name: vip_cidr
78 |         value: "32"
79 |       - name: cp_enable
80 |         value: "true"
81 |       - name: cp_namespace
82 |         value: kube-system
83 |       - name: vip_ddns
84 |         value: "false"
85 |       - name: svc_enable
86 |         value: "true"
87 |       - name: svc_leasename
88 |         value: plndr-svcs-lock
89 |       - name: vip_leaderelection
90 |         value: "true"
91 |       - name: vip_leasename
```

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 On-prem 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 On-prem appliance must be a `.pem` and `.key` pair. You can convert the format of your CA Certificate using SSL Certificate software, for example [OpenSSL](#).

### 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 [OpenSSL](#) 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 votiro`
- `kubectl create secret tls traefik-cert --key=/<path-to-certificate>/certificate.key --cert=/<path-to-certificate>/certificate.pem -n votiro`

## 4 Changing the Kibana Password

**Support requested this be included in VA documentation, then said to hold-off. Also awaiting context.**

### 4.1 Solution

To change the Kibana Password:

1. Go to <https://www.askapache.com/online-tools/htpasswd-generator/>.
2. Enter details:
  - a. Select **Encryption Algorithm** option **md5**.
  - b. Select **Authentication Scheme** option **Both**.
3. Click **Generate HTTPSWD**.

An output string is generated. For example,  
*admin:\$apr1\$tdea7nbo\$K0V/aYnScSwu27yH29IIM.*
4. Go to <https://www.base64encode.org/>.
5. Enter the string from Step 3, click **Encode**.

An output string is generated. For example,  
*YWRtaW46JGFwcjEkZTIpanlyZGckd3FvVEZCQldJZDRxMVhZY1ZSejhXLg==*
6. Login to Node1 and type: *kubectl edit secret kibana-auth*.
7. Modify the file. Click **Insert**.
8. Navigate to **Auth**. Replace the existing string with the one generated in Step 5.
9. Login to Kibana with the new credentials.

## 5 Email Arrival is Delayed

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

### 5.1 Symptoms

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

### 5.2 Solution

This situation might be related to Message throttling.

Get information of the Edge Connector:

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

### 5.3 Expected result

#### 5.3.1 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.

#### 5.3.2 Action:

Change the parameters using syntax:

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

#### 5.3.3 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

## 6 How to Check that the External Load Balancer is Working with the Votiro On-prem 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 On-prem cluster is working with an external load balancer.

### 6.1 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 On-prem, see [How to Configure SSL Passthrough Load Balancing using NGINX.htm](#).

### 6.2 Procedure

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

#### 6.2.1 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**:

```
[root@centos-nginx-king nginx]# curl https://10.130.1.30:30443 --insecure -vv
* About to connect() to 10.130.1.30 port 30443 (#0)
*   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_SHA256
* Server certificate:
*   subject: CN=TRAEFIK DEFAULT CERT
*   start date: Jul 07 12:55:05 2020 GMT
*   expire date: Jul 07 12:55:05 2021 GMT
*   common name: TRAEFIK DEFAULT CERT
*   issuer: CN=TRAEFIK DEFAULT CERT
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: 10.130.1.30:30443
> Accept: */*
>
< 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
< Content-Length: 19
<
404 page not found
* Connection #0 to host 10.130.1.30 left intact
[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:

```
[root@centos-nginx-king nginx]# curl https://king-va:443 --insecure -vv
* About to connect() to king-va port 443 (#0)
*   Trying 10.130.1.37...
* 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
*   expire date: Jul 05 12:54:59 2030 GMT
*   common name: king-va
*   issuer: CN=king-va
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: king-va
> Accept: */*
>
< HTTP/1.1 200 OK
< Accept-Ranges: bytes
< Cache-Control: private, no-cache, no-store, must-revalidate, pre-check=0, post-check=0, max-age=0, s-maxage=0
< Content-Length: 529
< Content-Security-Policy: default-src 'self';style-src 'self' 'unsafe-inline';img-src 'self' data;
< 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: Votiro
< Strict-Transport-Security: max-age=315360000; includeSubDomains; preload
< X-Content-Type-Options: nosniff
< X-Frame-Options: deny
< X-Xss-Protection: 1; mode=block
<
<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Votiro Management</title>
  <base href="/">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="icon" type="image/x-icon" href="assets/images/favicon.ico">
  <link rel="stylesheet" href="styles.css"></head>
<body>
  <app-root></app-root>
<script type="text/javascript" src="runtime.js"></script><script type="text/javascript" src="polyfills.js"></script><script type="text/javascript">
```

## 7 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.

### 7.1 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.

### 7.2 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
```
3. 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.

```
1  ## tcp LB and SSL passthrough for backend ##
2  stream {
3      upstream votirosfgva {
4          server 10.130.1.30:30443 max_fails=3 fail_timeout=10s;
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" "$upstream_bytes_received"
13         "$upstream_connect_time";
14
15         access_log /var/log/nginx/votirosfgva_access.log basic;
16         error_log /var/log/nginx/votirosfgva_error.log;
17
18         server {
19             listen 443;
20             proxy_pass votirosfgva;
21             proxy_next_upstream on;
22         }
23     }
```

```

## tcp LB and SSL passthrough for backend ##
stream {
  i upstream king-va {
    ii server 10.130.1.30:30443 max_fails=3 fail_timeout=10s;
    server 10.130.1.31:30443 max_fails=3 fail_timeout=10s;
    server 10.130.1.32:30443 max_fails=3 fail_timeout=10s;
  }

  log_format basic '$remote_addr [$time_local] '
    '$protocol $status $bytes_sent $bytes_received '
    '$session_time "$upstream_addr" '
    '"$upstream_bytes_sent" "$upstream_bytes_received" "$upstream_connect_time"';

  access_log /var/log/nginx/king-va_access.log basic;
  error_log /var/log/nginx/king-va_error.log;

  server {
    listen 443;
    iii proxy_pass king-va;
    proxy_next_upstream on;
  }
}

```

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
```

## 7.3 Next Steps

To connect the Paralus cluster to this external load balancer, see the following guide: [How to Check that the External Load Balancer is Working with the Votiro Cloud Cluster.](#)

## 7.4 NGINX File Example

The following code is an example of an NGINX File.

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

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

## 8 How to Configure the Votiro Appliance for AWS

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

To install Votiro On-prem 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.

### 8.1 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
  - ◆ 500 GB SSD

For these specs, an m6a.2xlarge EC2 instance for v9.9.344 clusters on AWS 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.

## 8.2 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**.



5. Under **Ownership** select **Shared with me**.



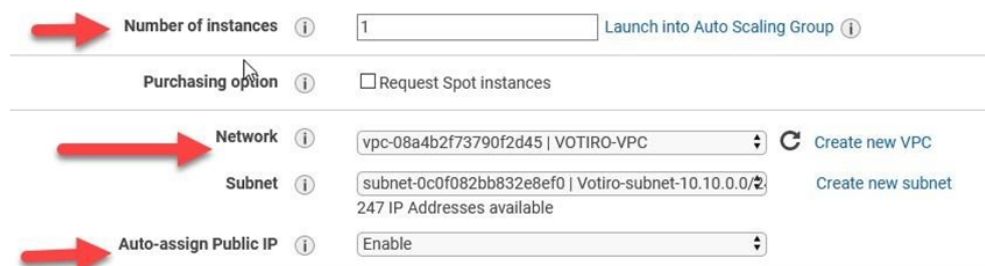
6. Select the Votiro Appliance.



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., "Votiro-subnet-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**.



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



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.

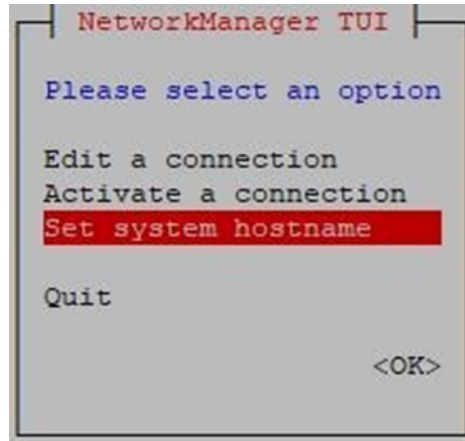
Key (128 characters maximum)	Value (256 characters maximum)	Instances (i)	Volumes (i)
Name	Votiro-N1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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:

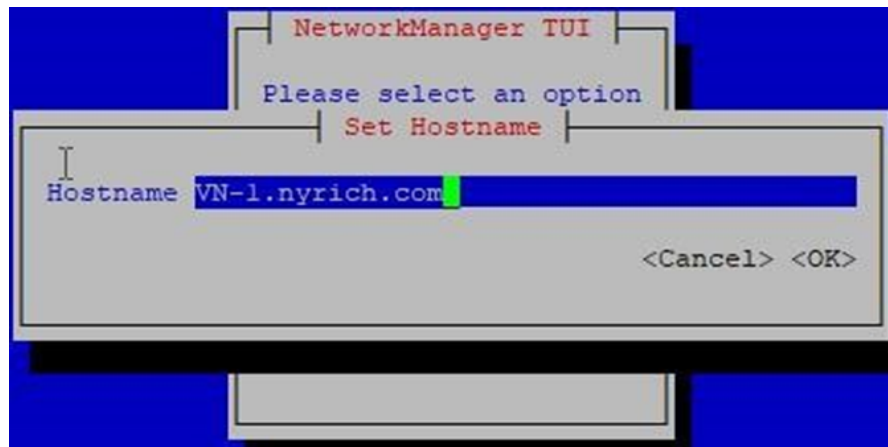
- ◆ Port 443 TCP to and from the VIP of the appliance on 30443. This port is used for web access to Votiro.
- ◆ Each Appliance should be able to communicate on the following ports that are required inside the VLAN between each appliance:
  - 6443/tcp
  - 2379-2380/tcp
  - 10250-10252/tcp
  - 22/tcp
  - 10255/tcp
  - 8472/udp
  - 24007 – 24008/tcp
  - 49152 – 49154/tcp

sg-0c96b62a7d4c4373		Votiro_Appliances	Firewall for votiro appliances
All TCP	TCP	0 - 65535	
Custom TCP Rule	TCP	6443	Use your own subnets here
Custom TCP Rule	TCP	2379 - 2380	
Custom TCP Rule	TCP	2379 - 2380	
Custom TCP Rule	TCP	2379 - 2380	
SSH	TCP	22	
SSH	TCP	22	
SSH	TCP	22	
Custom TCP Rule	TCP	30443	
Custom TCP Rule	TCP	10255	
Custom TCP Rule	TCP	10255	
Custom TCP Rule	TCP	10255	
Custom TCP Rule	TCP	30443	
Custom TCP Rule	TCP	8472	
Custom TCP Rule	TCP	8472	
Custom TCP Rule	TCP	8472	
All UDP	UDP	0 - 65535	
Custom TCP Rule	TCP	10250 - 10252	
Custom TCP Rule	TCP	10250 - 10252	
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**.



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.google.com (173.194.38.180) 56(84) bytes of data:
64 bytes from sin04s02-in-f20.1e100.net (173.194.38.180): icmp_seq=1 ttl=53 time
=117 ms
64 bytes from sin04s02-in-f20.1e100.net (173.194.38.180): icmp_seq=2 ttl=53 time
=118 ms
64 bytes from sin04s02-in-f20.1e100.net (173.194.38.180): icmp_seq=3 ttl=53 time
=111 ms
64 bytes from sin04s02-in-f20.1e100.net (173.194.38.180): icmp_seq=4 ttl=53 time
=121 ms
```

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

## 9 How to Configure the Votiro On-prem 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 On-prem cluster to work with external storage.

### 9.1 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.
- Is Linux-based (Windows-based external storage server is not supported).

### 9.2 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.

#### 9.2.1 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
```

## 9.2.2 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"**.

## 9.2.3 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.

## 9.3 Troubleshooting

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

### 9.3.1 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:

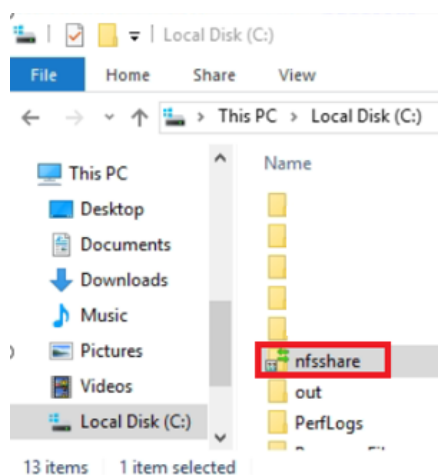
```
[root@sfg ~]# chown 1000:1000 -R /data/externalfs
chown: changing ownership of '/data/externalfs/nfsshare':
Permission denied
```

## Solution

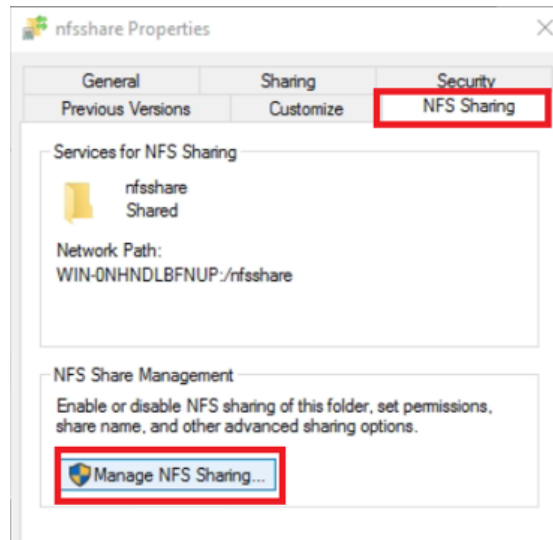
If you are using Windows Server as NFS, please follow this link to configure your Windows Server as a NFS server: [Deploy Network File System](#)

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

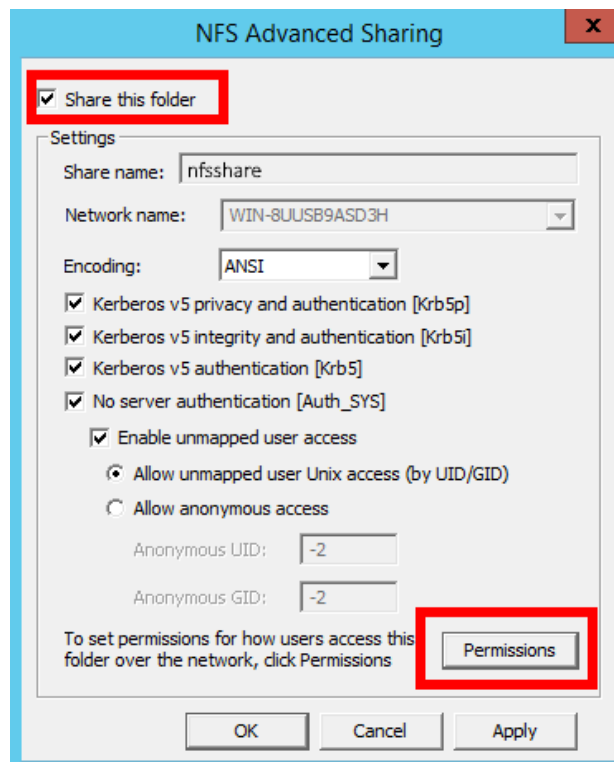
1. Right click on the **nfsshare** folder on your Windows Server and select **Properties**:



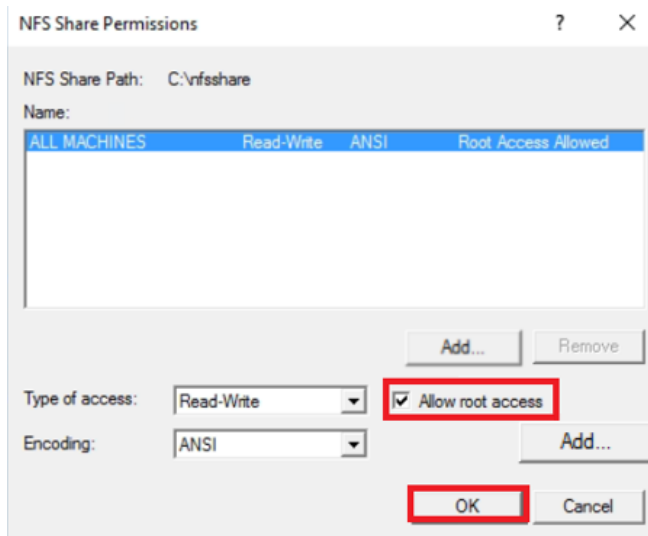
2. Select the **NFS Sharing** tab, and then select **Manage NFS Sharing...**:



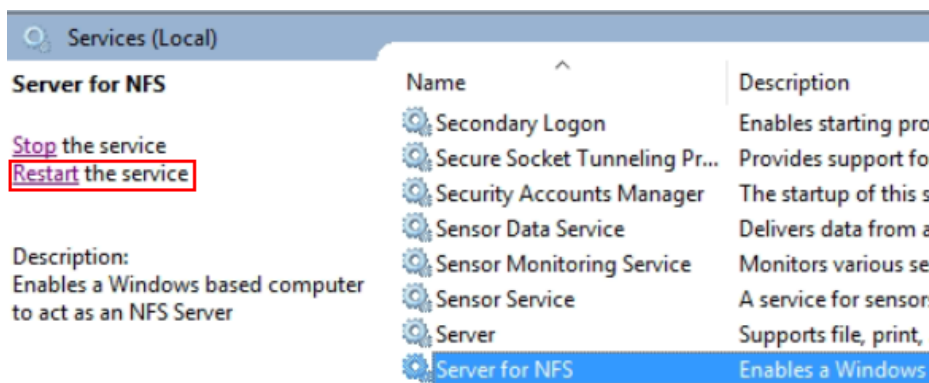
3. In the **NFS Advanced Sharing** window that opens, check the box **Share this folder** and leave the rest of the options as is. Then select **Permissions**.



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



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



- 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.

**9.3.2 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
```

```
kind: ConfigMap
metadata:
  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\": \"0\",\n    \"DisableDirectStreaming\": false,\n    \"SerializerFactory\": null,\n    \"encryptFiles\": true,\"externalStorageBackupInterval\":\"00:10:00\",\"externalStorageRootPath\":\"/externalblobs/nfsshare\",\"internalStorageRootPath\":\"/votiroblobs\",\"maxBlobStorageUsagePercentage\":\"95\",\"maxElasticStorageUsagePercentage\":\"70\",\"runCleanerAtHour\":\"02:00\",\"storageCheckInterval\":\"00:00:30\",\"storageHealthCheckTimeoutInMilliseconds\":\"10000\",\"warningBlobStorageUsagePercentage\":\"70\"},\"kind\":\"ConfigMap\",\"metadata\":{\"annotations\":{},\"labels\":{\"productVersion\":\"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",
```

## 10 How to Deploy the Votiro On-prem Cluster in Azure

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

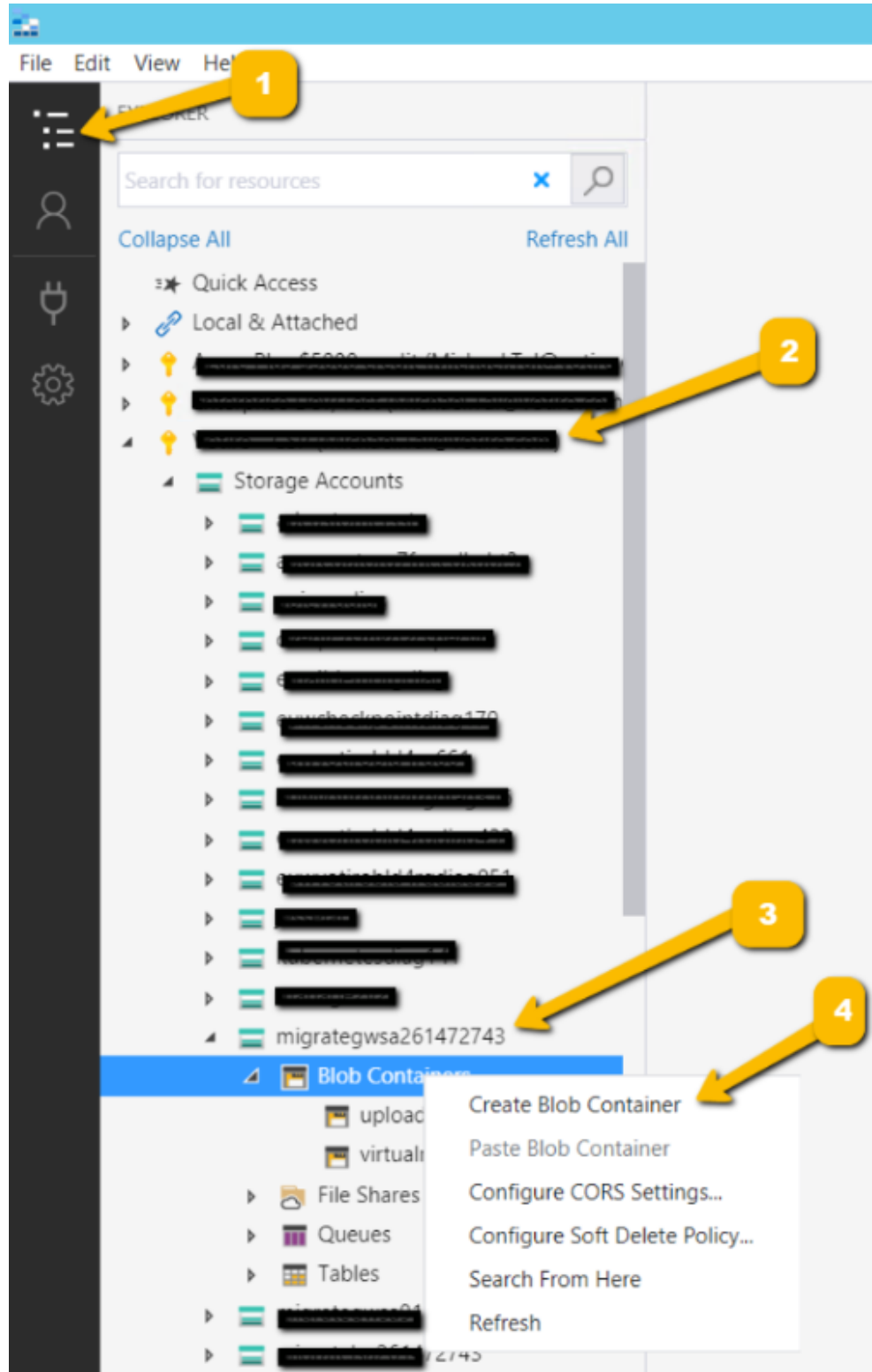
### 10.1 Prerequisites

Before you start, verify that the following are available:

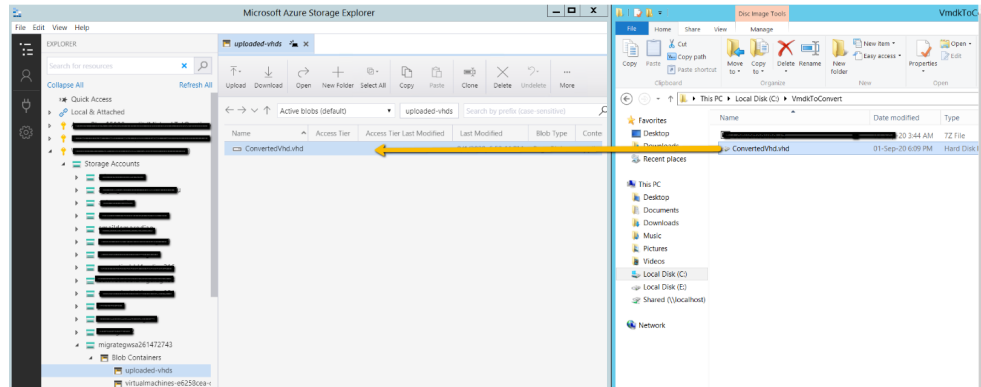
- An active Azure subscription
- The latest VHD (Virtual Hard Disk) provided by Votiro.
- The Azure Storage Explorer tool installed on a system that can access the Azure account and will be used to upload the VHD to your Storage account in Azure. This tool may be downloaded from [Azure Storage Explorer](#).
- The recommended disk size is 500 GB Premium SSD.
- For the Azure Dv4 series - Instance D8 v4:
  - ◆ 8v CPUs
  - ◆ 32 GiB RAM
  - ◆ Attached SSD

### 10.2 Procedure

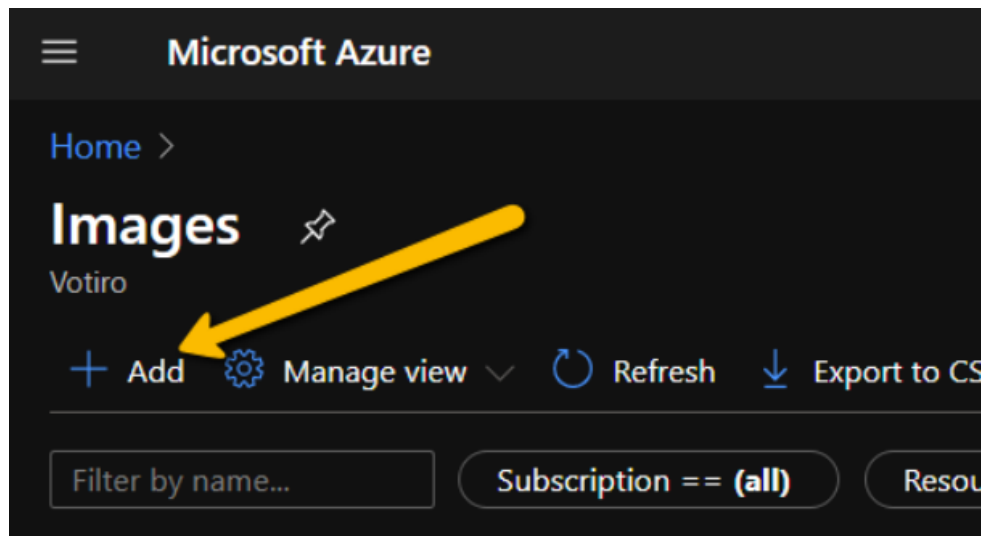
1. Run **Azure Storage Explorer** and authenticate with your Azure account.
2. On the left pane click on **Toggle Explorer**.
  - a. Expand the view of the desired subscription.
  - b. Expand **Storage Accounts**.
  - c. Select the desired Storage account and expand it.
  - d. Under Blob Containers,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



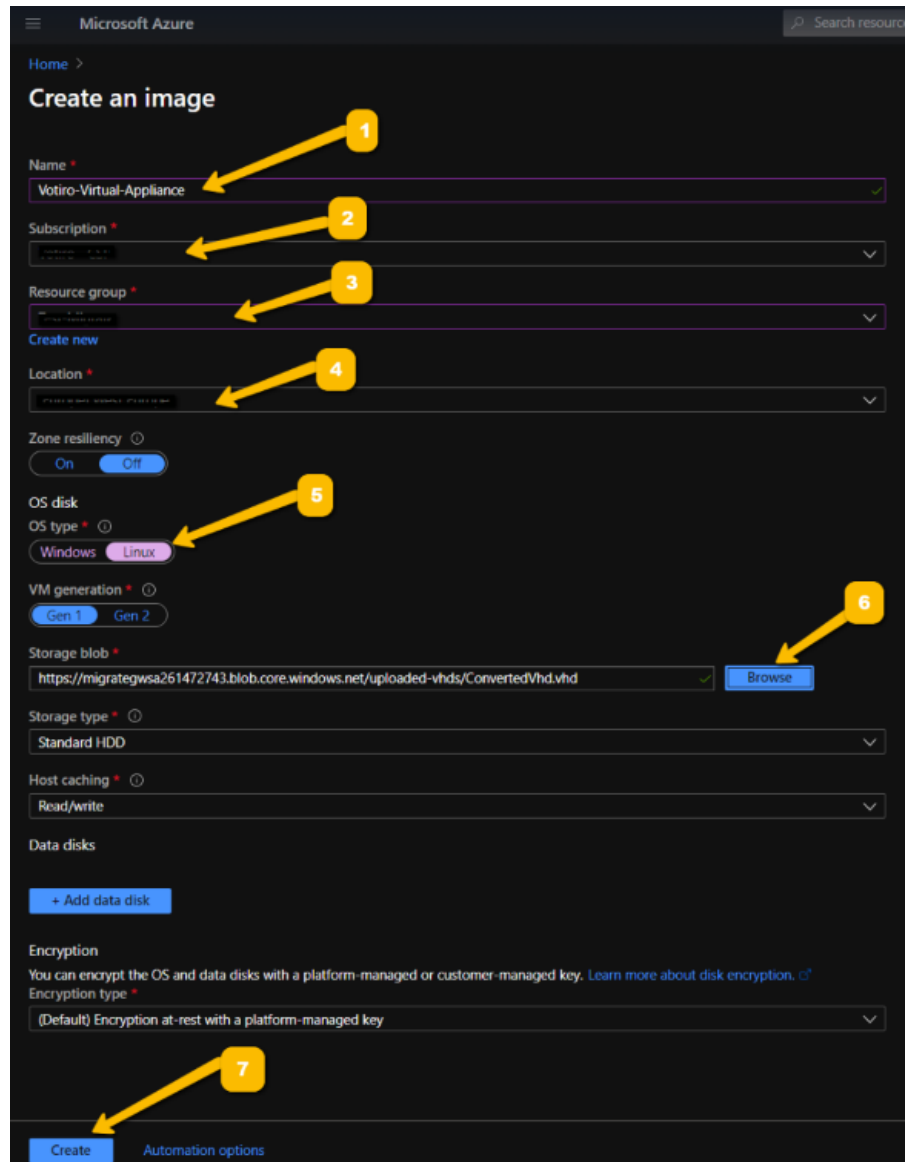
3. Drag and drop the extracted VHD file to the created Blob Container.



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.

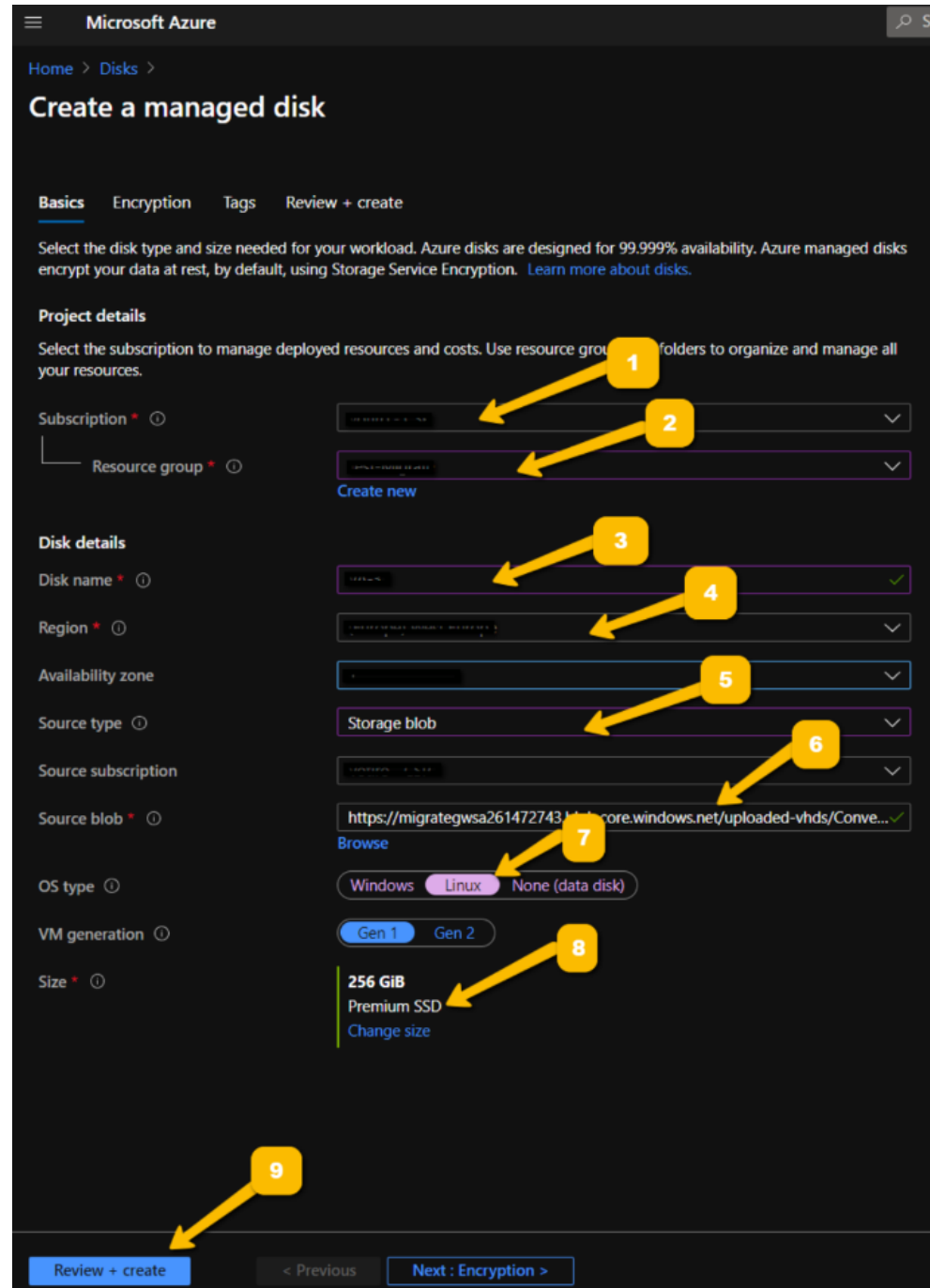


6. Fill in the information to build the image from the VHD:
  - a. Provide the image with a **Name**.
  - b. Select a **Subscription**.
  - c. Type in the **Resource group**.
  - d. Select the **Location**.
  - e. Select the **OS type** as **Linux**.
  - f. Click on **Browse** and select the uploaded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

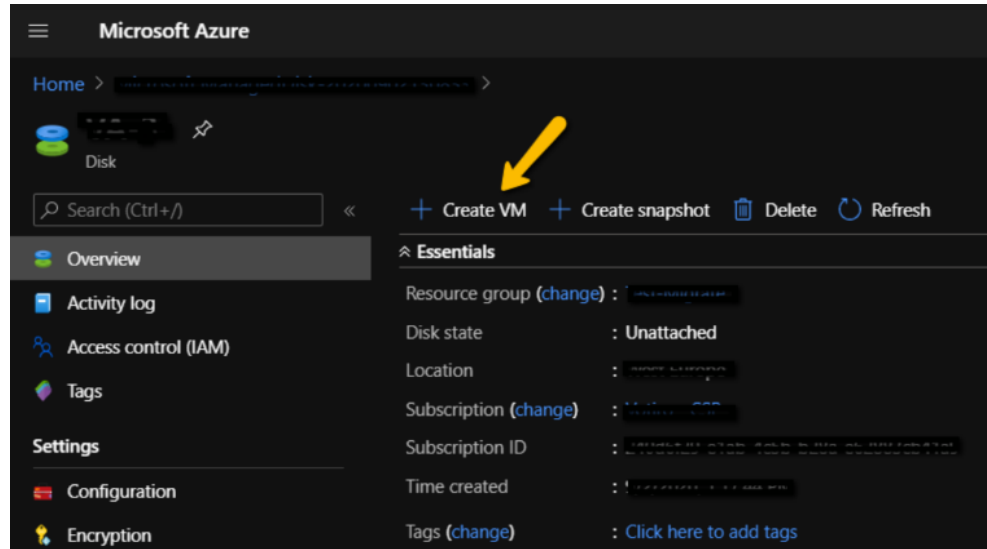


7. After the image is created, **Create a managed disk.**
8. Fill in the information as in the screenshot below:
  - a. Select a **Subscription.**
  - b. Select the **Resource group.**
  - c. Provide a **Name** for the disk, for example Node-1.
  - d. Select the **Region** which you would like the disk 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.**

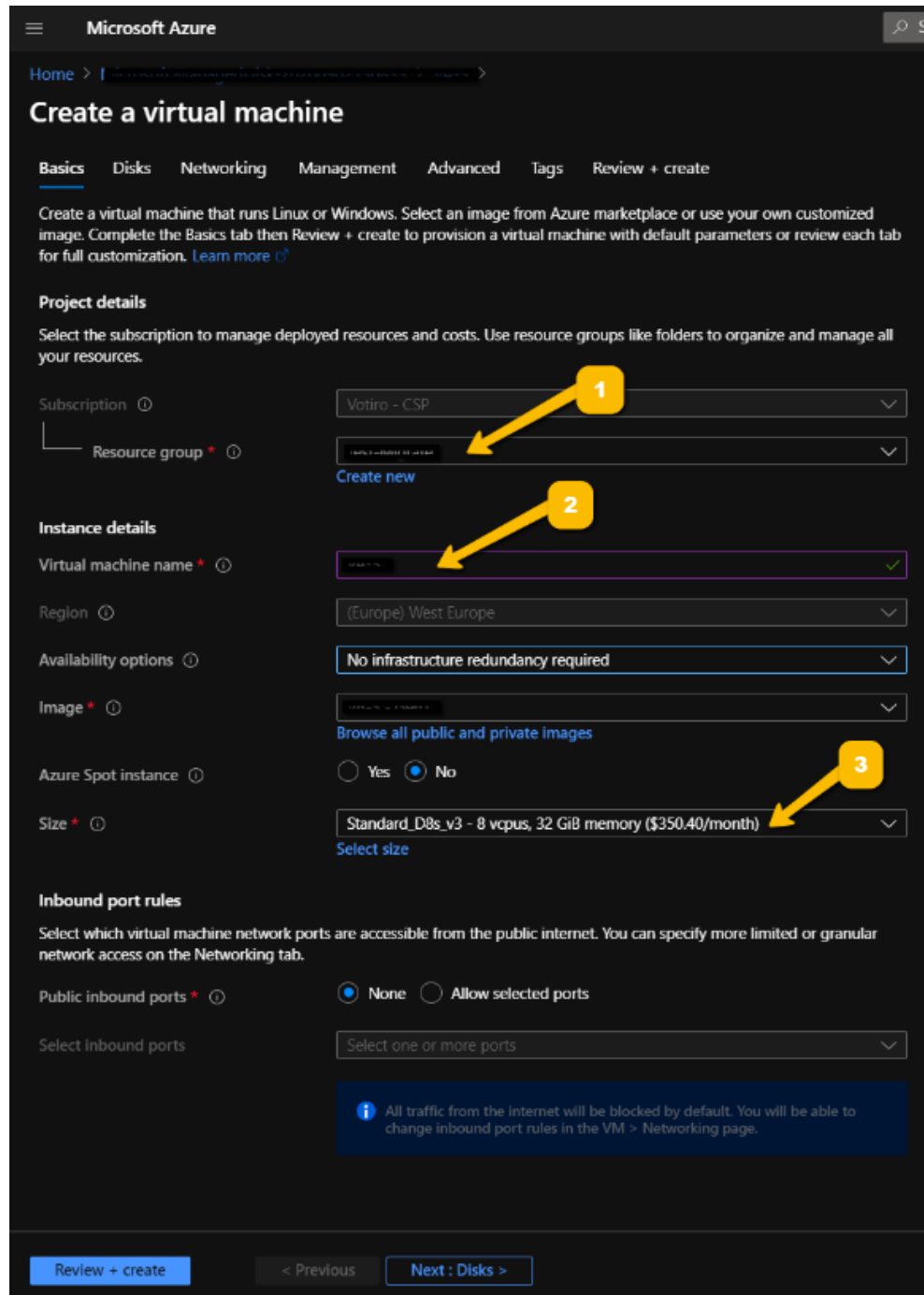
- i. Click on **Review + create**.



- 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:



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.

# 11 How to Integrate Azure AD Single Sign-on with Votiro VA On-prem using the Entra SAML Toolkit

This tutorial demonstrates how to integrate the Microsoft Entra SAML Toolkit App with Votiro, enabling users to access the Votiro Management console using their corporate credentials.

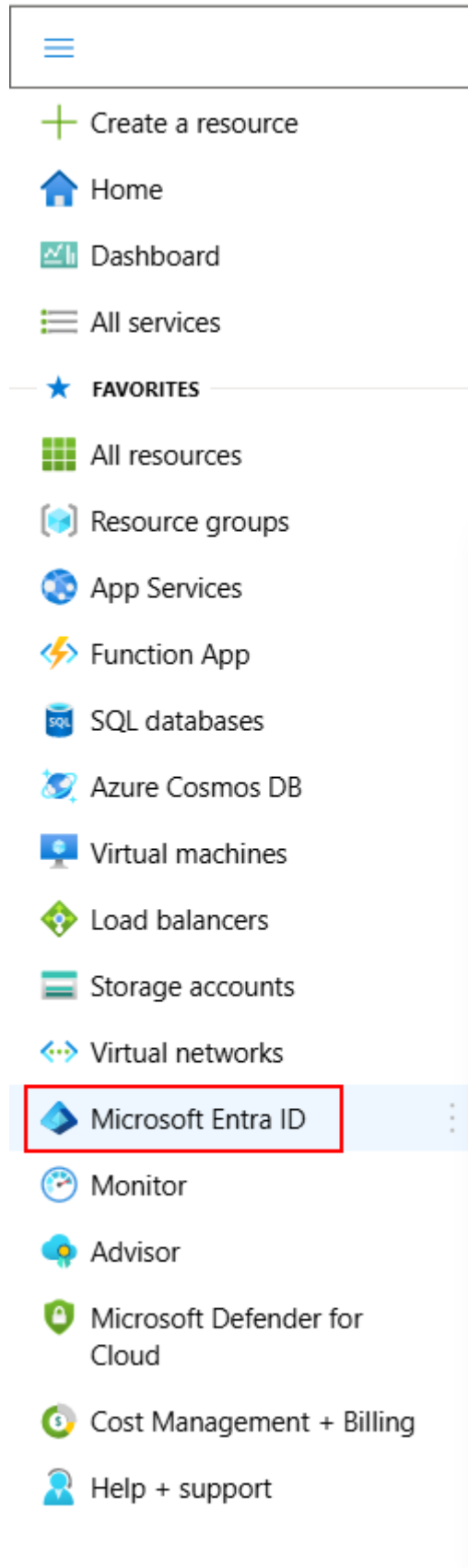
## 11.1 Prerequisites

Ensure you have the following items:

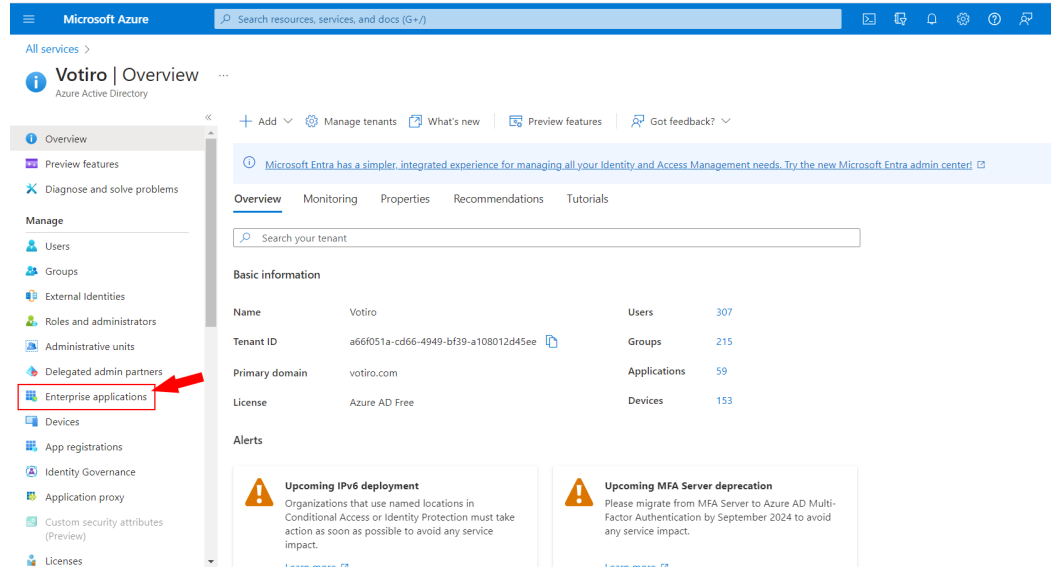
- Azure AD subscription
- Azure AD SAML Toolkit enabled on the above-mentioned subscription
- Admin permissions
- Votiro TenantID - to obtain, contact our Support Team at: [support@votiro.com](mailto:support@votiro.com)

## 11.2 Configure the Azure Portal

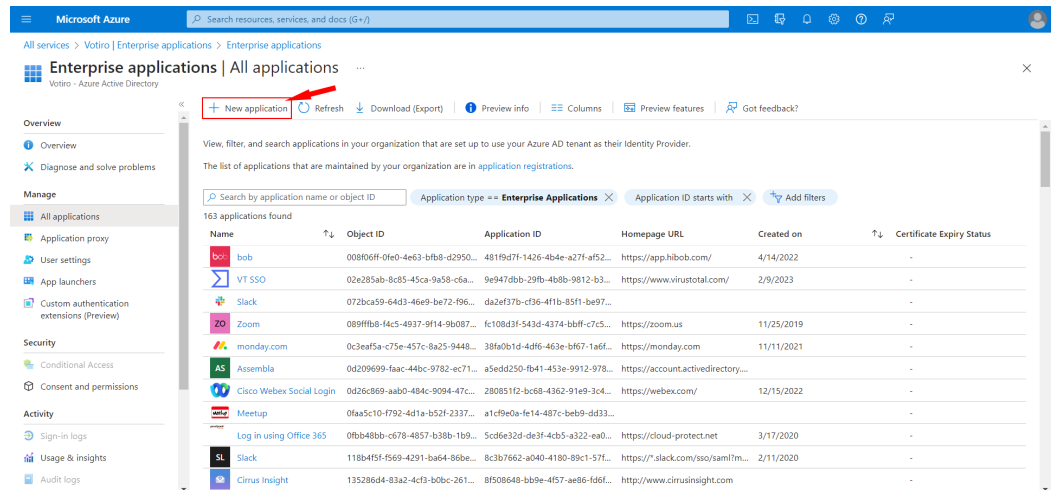
1. Sign in to the [Azure portal](#).
2. In the left pane, open the **portal menu** and select **Microsoft Entra ID**.



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



4. Select **New application**:

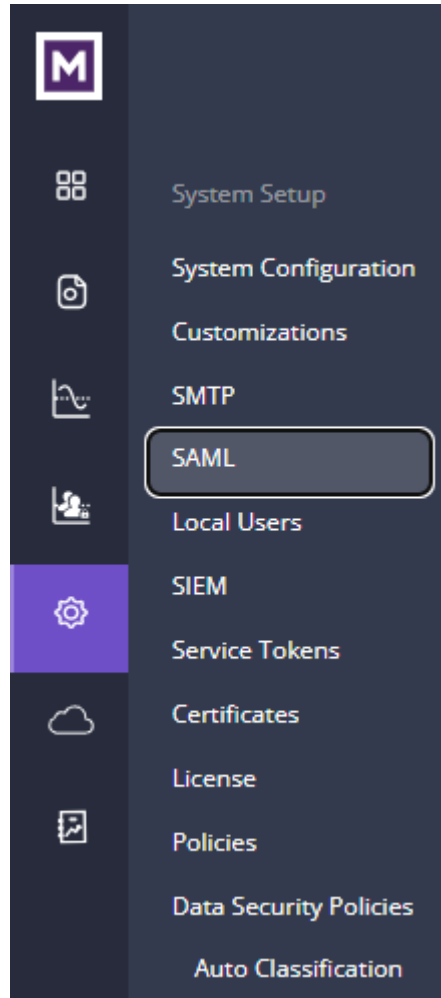


5. In the search field type **Azure AD SAML Toolkit**. In the **Search by application name or object ID** field, type "toolkit" to locate the **Microsoft Entra SAML Toolkit** and select it.
6. You will be prompted to select a new name for the application in a separate window, and once you have completed this step, click **Create**.
7. After a few moments, the app will be added to your tenant and is presented as an **Overview**.
8. Under **Getting Started**, select **Assign users and groups** to add the desired groups. Consider creating three groups with different permission levels to match Votiro's side (Admins, HelpDesk, Soc). Ensure they are created under the same domain name.
9. Select **Single sign-on** located under **Users and Groups**.

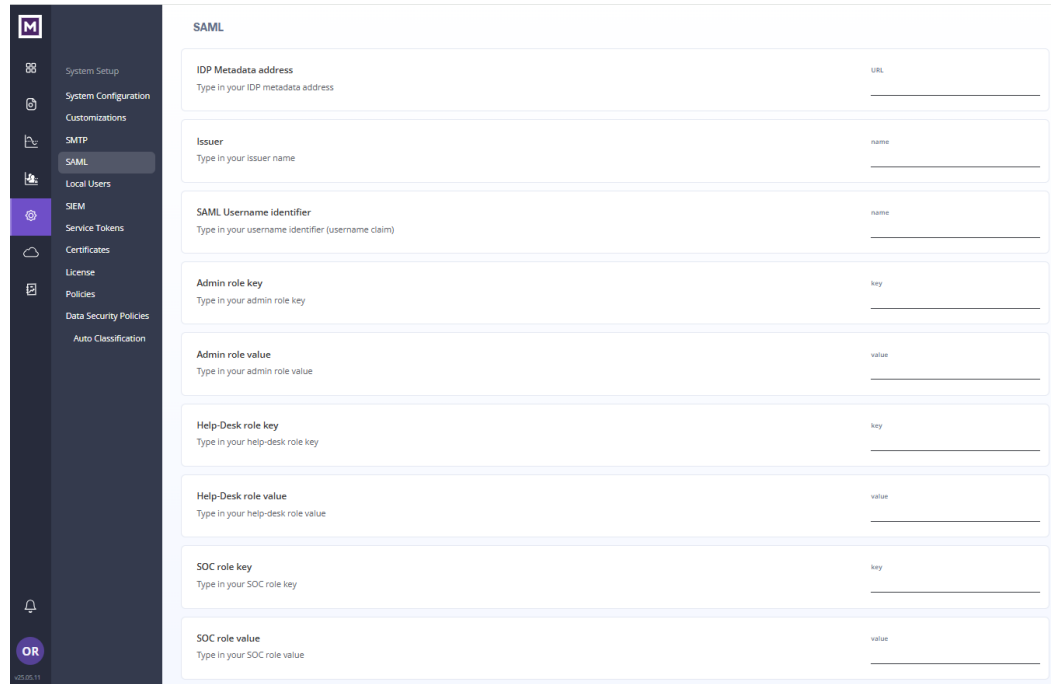
10. Select the Single Sign-On method: **SAML**, and click **Edit** under **Basic SAML Configuration**, and fill in as follows:
  - a. For **Identifier (Entity ID)**, leave as default - <https://samltoolkit.azurewebsites.net>.
  - b. Both **Reply URL (Assertion Consumer Service URL)** and **Sign on URL** should be in the following format: [https://<Votiro-FQDN>/assertionconsumerservice/<Votiro\\_TenantID>](https://<Votiro-FQDN>/assertionconsumerservice/<Votiro_TenantID>).
  - c. Click **Save**.
11. In the **Attributes & Claims** section, click **Edit**.
  - a. Click **+ Add a Group claim**.
  - b. Under **Which groups associated with the user should be returned in the claim?**, select **Groups assigned to the application** to direct a user's lookup to the groups assigned to the app, as configured in [step 8](#).
  - c. Under **Advanced Options**, check **Customize the name of the group claim**. Name the Group Claim as "VotiroGroups" under **Name**.
  - d. Click **Save**.

## 11.3 Configure the Votiro Management Console

1. Log in to Votiro's Management console using a local user account.
2. On the left pane, click on the cogwheel, and select **SAML**.



3. The SAML configuration page is displayed:



- a. For the **IDP Metadata address**, copy and paste the value from the **App Federation Metadata Url** field in Azure.
  - b. For the **Issuer**, copy and paste the value from the **Identifier (Entity ID)** the unique ID identifier field in Azure.
  - c. For the **SAML Username identifier**, leave by default: <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier>
  - d. The **Admin role key** should be the value you provided for the group above in **Group Claims**, in this example, "VotiroGroups".
  - e. The **Admin role value** should be the Object Id of the group "admins".
  - f. For **Help-Desk role key**, enter the name of the group claim - in this example, "VotiroGroups".
  - g. For **Help-Desk role value**, enter the ObjectID of group "HelpDesk".
  - h. For **SOC role key**, enter the name of the group claim - in this example, "VotiroGroups".
  - i. For **SOC role value**, enter the ObjectID of the group "Soc".
4. Save your changes.
  5. Log out as the local user from the Management console.
  6. Log in to the Votiro Management console with corporate credentials using SAML Single Sign On. For more information, see [Logging in to the Management Dashboard: VA on-premises](#).

# 12 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.

## 12.1 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](#)

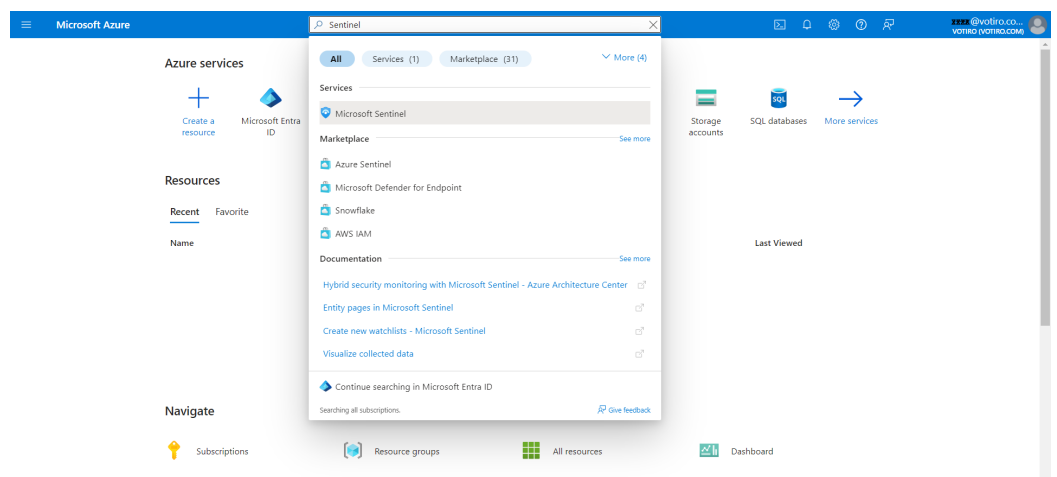
## 12.2 Procedure

### 12.2.1 Manual/Offline Deployment

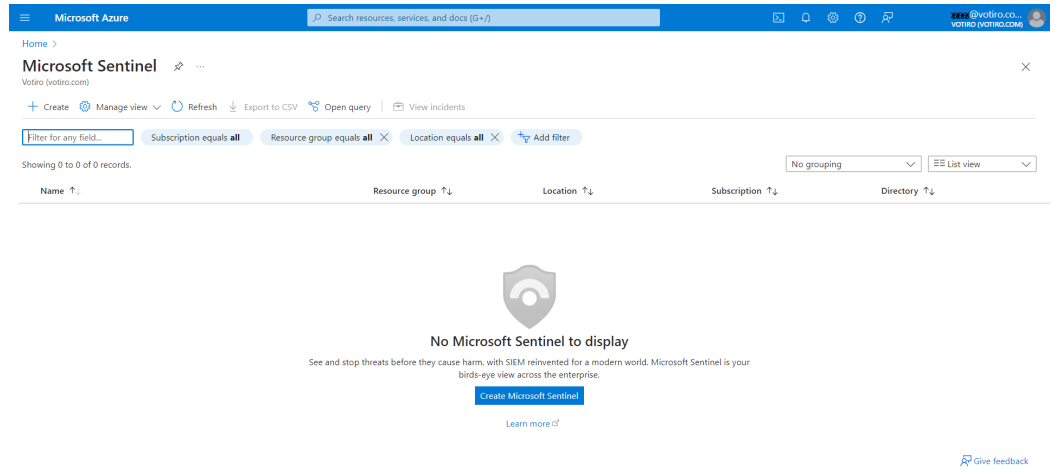
To test the solution before publishing, follow the below steps.

#### Deploy CEF Data Connector on Forwarder Machine

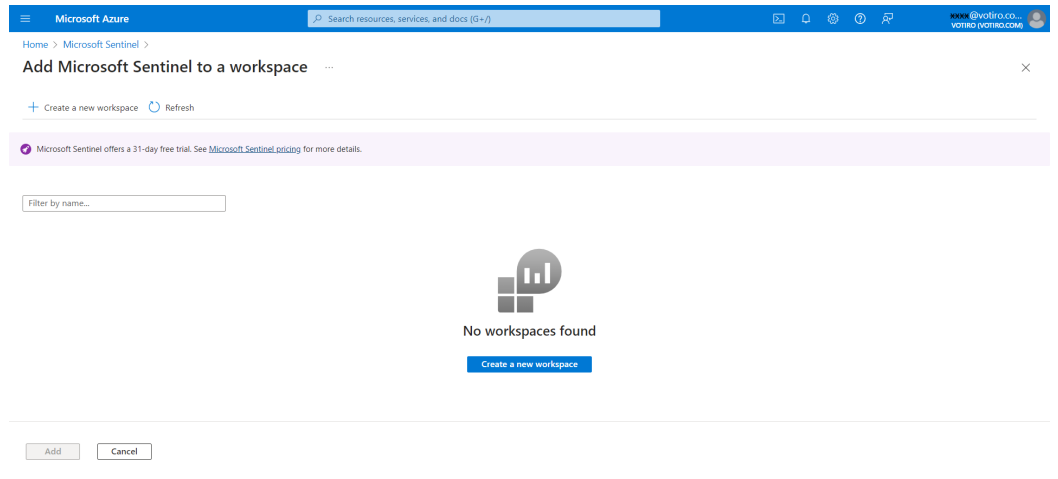
1. Sign in to the [Azure portal](#).
2. Search for **Microsoft Sentinel**.



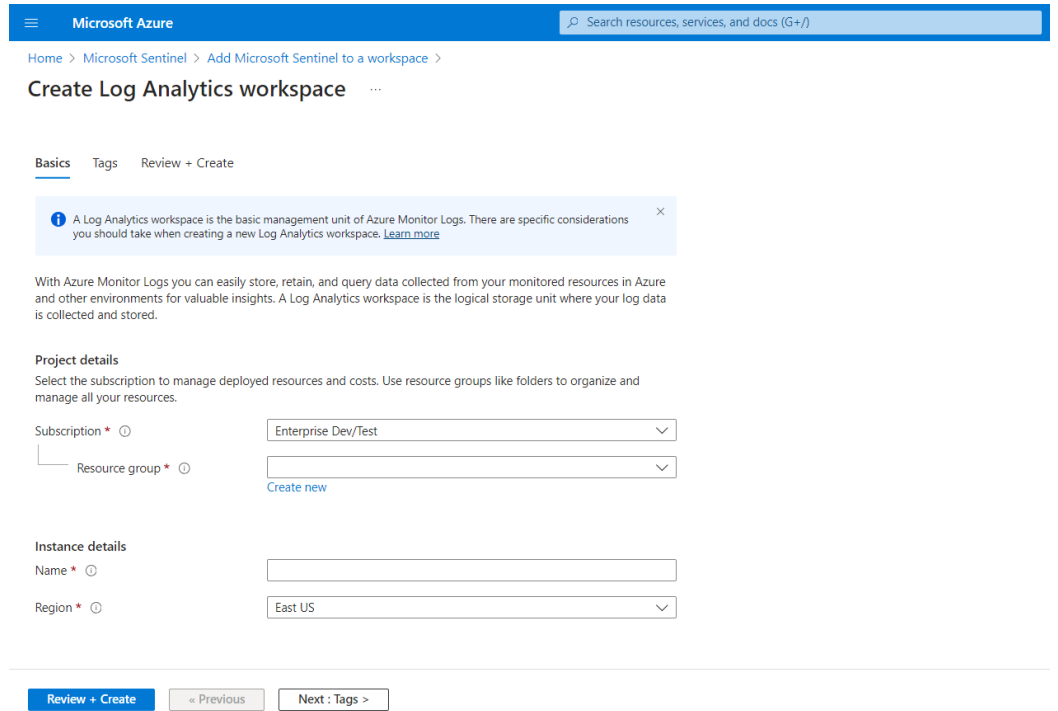
3. Select **Microsoft Sentinel** from **Services**.



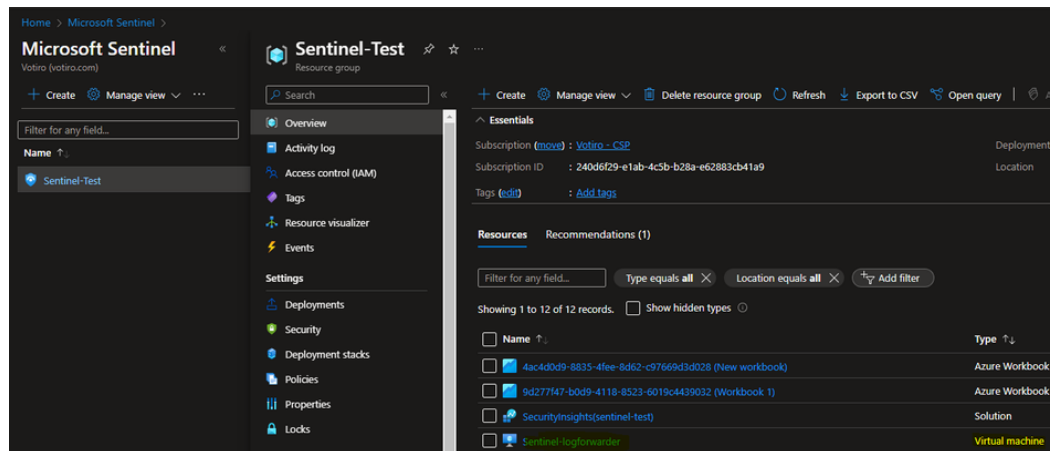
4. Press **+ Create** or **Create Microsoft Sentinel** to add **Microsoft Sentinel** to a **Workspace**:



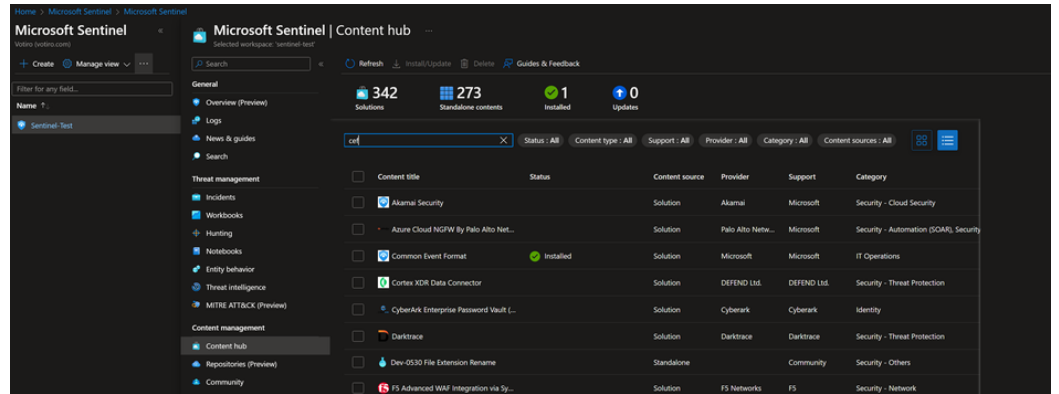
5. Press **+ Create a new workspace**:



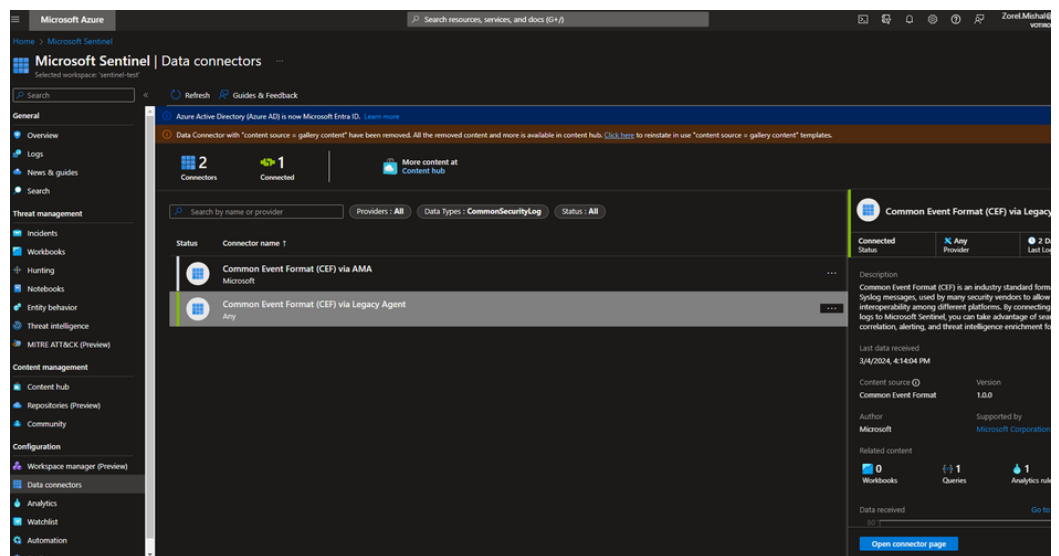
6. Create a new **Resource Group** if it does not exist yet. Then create a new machine with the system requirements mentioned above → via Resource Group > Create > select Virtual Machine (Ubuntu 22.06 server is recommended):



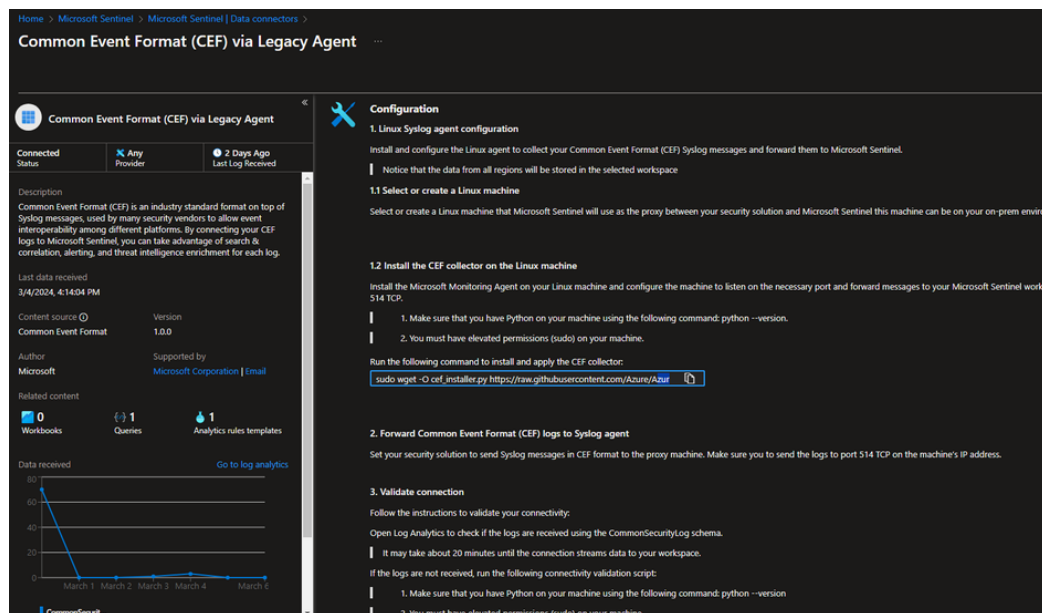
7. Select the created workspace, then go to Content Hub > Select Common Event Format (CEF) and install it:



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:

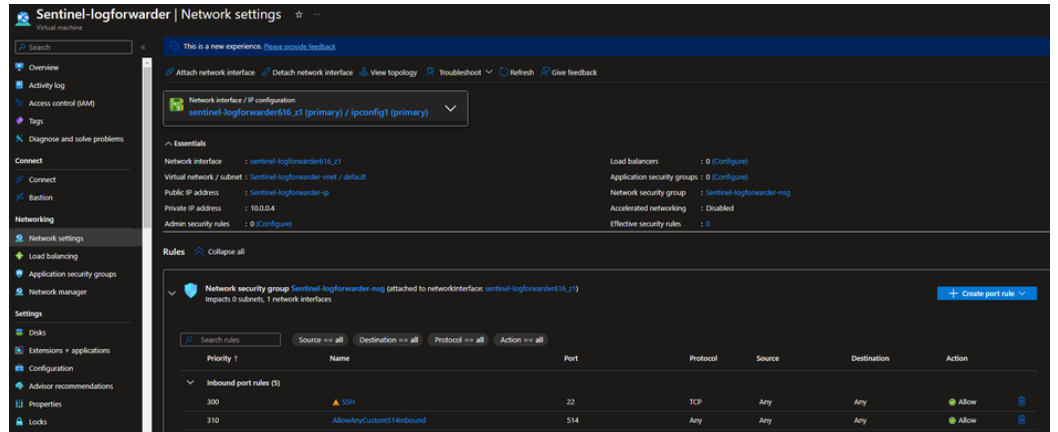
```
python --version or python3 --version
```

11. Copy the command below:

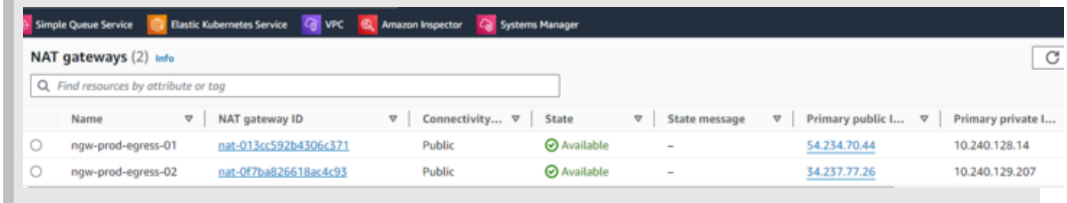
```
sudo wget -O cef_installer.py
https://raw.githubusercontent.com/Azure/Azure-
Sentinel/master/DataConnectors/CEF/cef_installer.py&&sudo
python cef_installer.py [WorkspaceID] [Workspace Primary
Key]
```

**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:



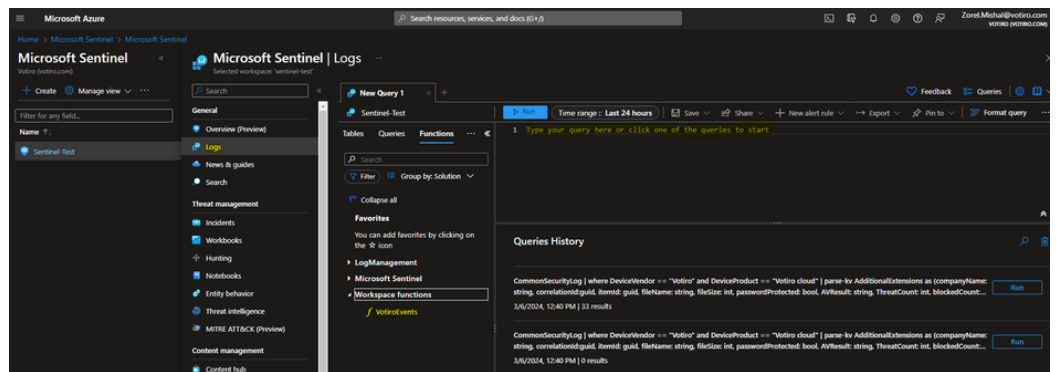
**Note:** In this case, we used TCP port 514 (default) and **Allow=any**, but the best practice is to use the TLS protocol with other ports used and restrict to specific IPs pointed to specific NAT gateways. For example, in [prod.us](#):



## 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 → Go to your created Workspace → Logs
3. Paste the content of **VotiroEvents.txt** in the area as shown below:



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

### Save as function ✕

Function name \*  
 ✓

Code  

```
dfgdfg
```

Legacy category \*  
 ✓

Save as computer group ⓘ

#### Parameters

Type	Name	Default value
<input type="text" value="Select type"/> ▾	<input type="text" value="Type name"/>	<input type="text" value="Type default value"/>

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

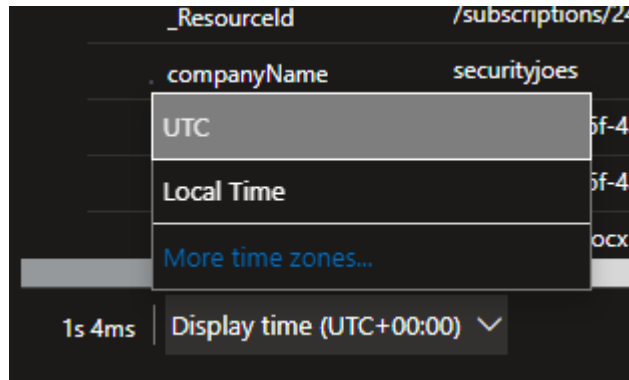
The screenshot shows the Azure Sentinel 'New Query' interface. The query is named 'VotiroEvents' and is set to run over the 'Last 7 days'. The results are displayed in a table with the following columns: TimeGenerated [UTC], DeviceVendor, DeviceProduct, DeviceVersion, DeviceEventClassID, Activity, LogSeverity, and FileHash. The table contains 16 rows of data, all representing 'Sanitization summary' events from the 'Votiro' vendor and 'Votiro cloud' product.

TimeGenerated [UTC]	DeviceVendor	DeviceProduct	DeviceVersion	DeviceEventClassID	Activity	LogSeverity	FileHash
3/3/2024, 2:04:30.713 PM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	fa2742
2/29/2024, 10:03:12.734 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	fa2742
2/29/2024, 10:10:40.876 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	980489
2/29/2024, 10:11:19.147 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	980489
2/29/2024, 10:11:47.788 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	980489
2/29/2024, 10:13:17.393 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	980489
2/29/2024, 10:15:45.742 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	3df79d
2/29/2024, 10:18:49.026 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	3df79d
2/29/2024, 10:19:03.034 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	3df79d
2/29/2024, 10:19:20.211 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	3df79d
2/29/2024, 10:23:10.279 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	3df79d
2/29/2024, 10:24:10.481 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	3df79d
2/29/2024, 10:25:07.792 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	38c979
2/29/2024, 10:26:14.751 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	38c979
2/29/2024, 10:28:03.185 AM	Votiro	Votiro cloud	1.0.0.0	500	Sanitization summary	1	38c979

The screenshot shows the expanded details for a specific log event. The event is selected with a checkmark and shows the following details:

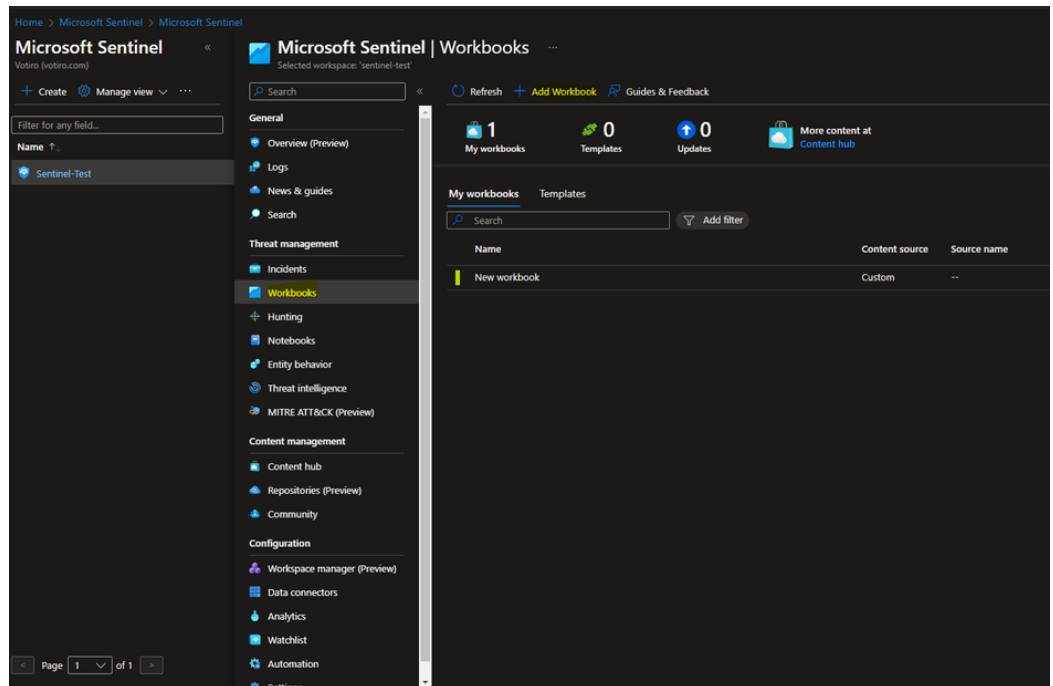
- TimeGenerated [UTC]:** 3/3/2024, 2:04:30.713 PM
- DeviceVendor:** Votiro
- DeviceProduct:** Votiro cloud
- DeviceVersion:** 1.0.0.0
- DeviceEventClassID:** 500
- Activity:** Sanitization summary
- LogSeverity:** 1
- FileHash:** fa2742aec57ae5a21e80a0c7767af566ba48e0b035fa5546f-34e2898a31ad6
- FileType:** Word (2007-2010)
- Computer:** ec2-54-234-70-44.compute-1.amazonaws.com
- SourceSystem:** OpsManager
- Type:** CommonSecurityLog
- \_ResourceId:** /subscriptions/240d6f29-e1ab-4c5b-b28a-e62883cb41a9/resourcegroups/sentinel-test/providers/microsoft.compute/virtualmachines/sentinel-logforwarder
- companyName:** securityjoes
- correlationId:** 6965c87-045f-4a6b-bda5-f0321c75a43f
- itemId:** 6965c87-045f-4a6b-bda5-f0321c75a43f
- SrcFileName:** sadsaDSA.docx

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

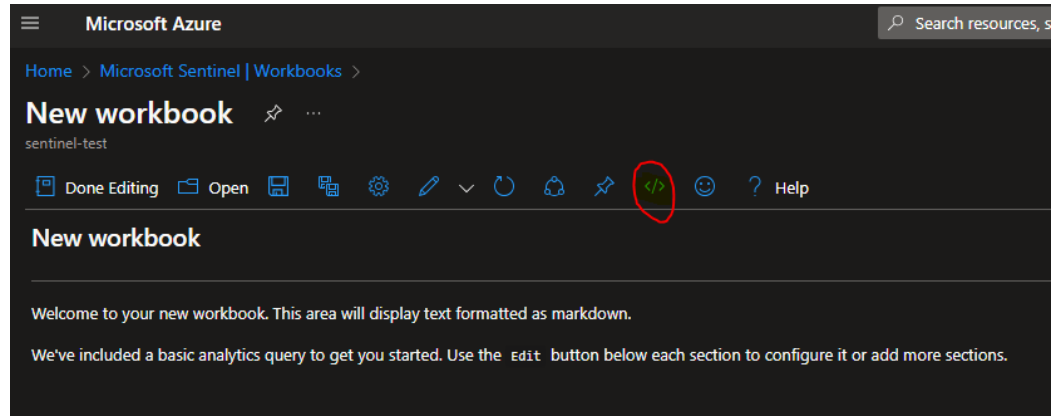


### Deploy the Workbook

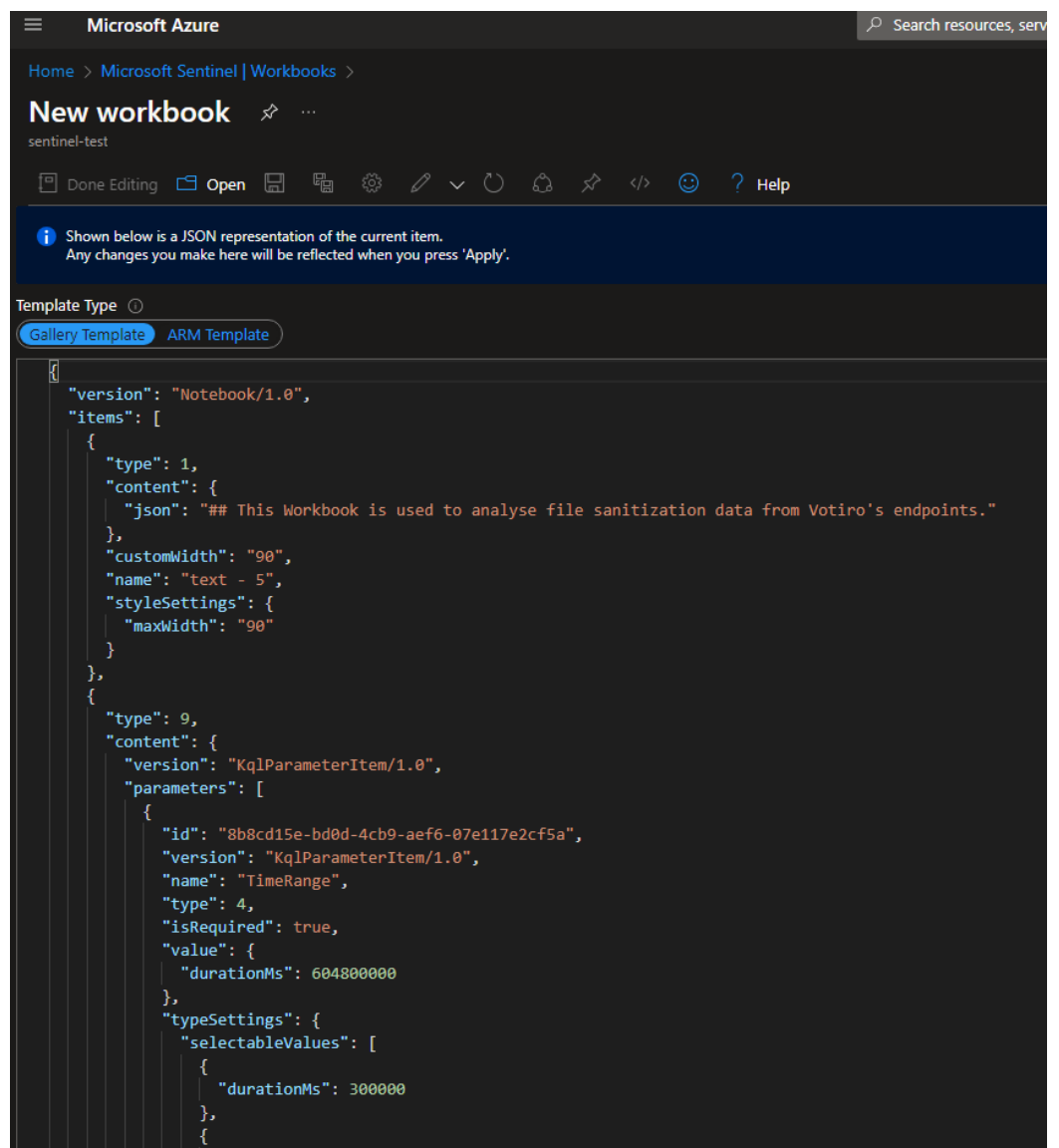
1. Copy the contents of the file:  
**/Votiro-Offline/Workbooks/Votiro Monitoring Dashboard.json**
2. On Microsoft Sentinel, go to your WorkSpace > Workbooks > **Add Workbook**:



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



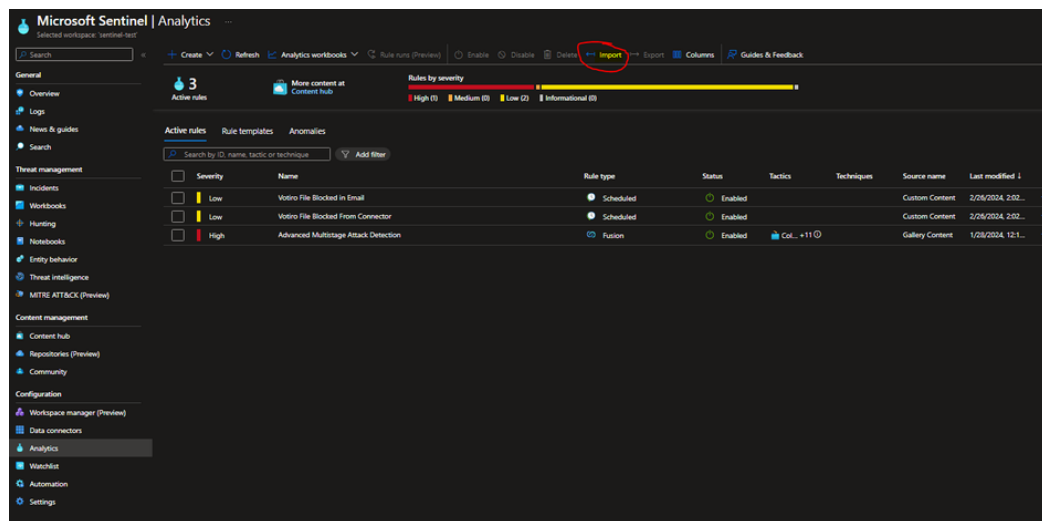
4. Replace the Gallery template contents with the copied contents, and click on **Apply**:



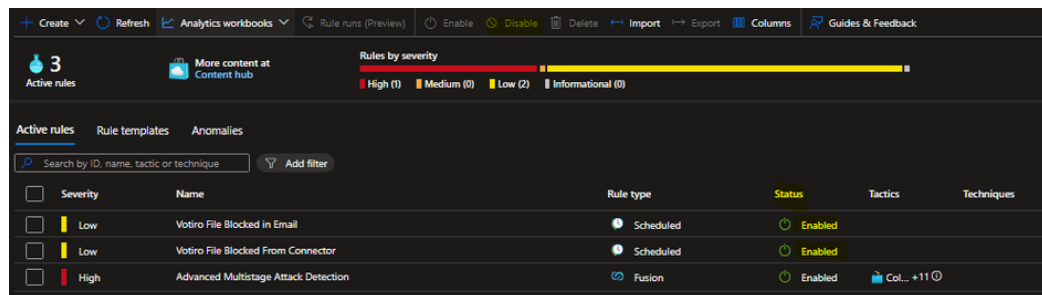
5. The Following Workbook must be visible:  
After a scroll

## Set Alert Queries for Incidents

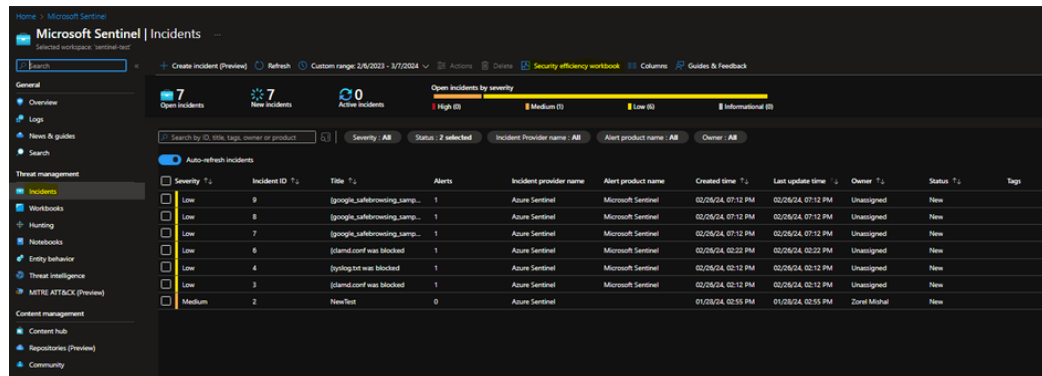
1. Go to **/Votiro-Offline/Analytic Rules**. Keep both **Votiro File Blocked FromConnector.json** and **Votiro File Blocked in Email.json** files ready.
2. On Microsoft Sentinel > Workspace, select **Analytics**.
3. Click **Import** (from the bar at the top of the screen) in the resulting dialog box,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



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



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



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]

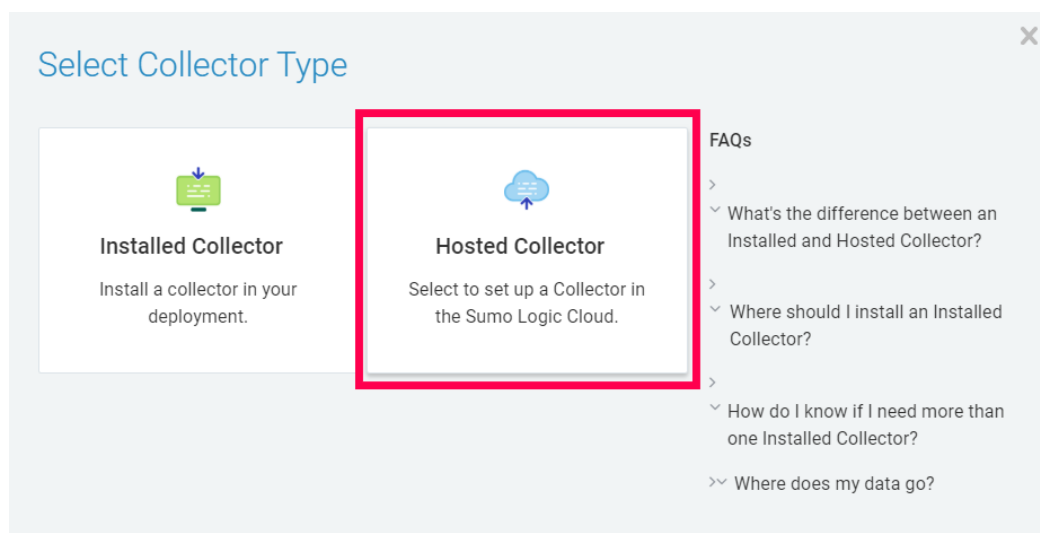
# 13 How to Integrate Votiro On-prem Syslog Messages with Sumo Logic using HTTP Logs

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

## 13.1 Procedure

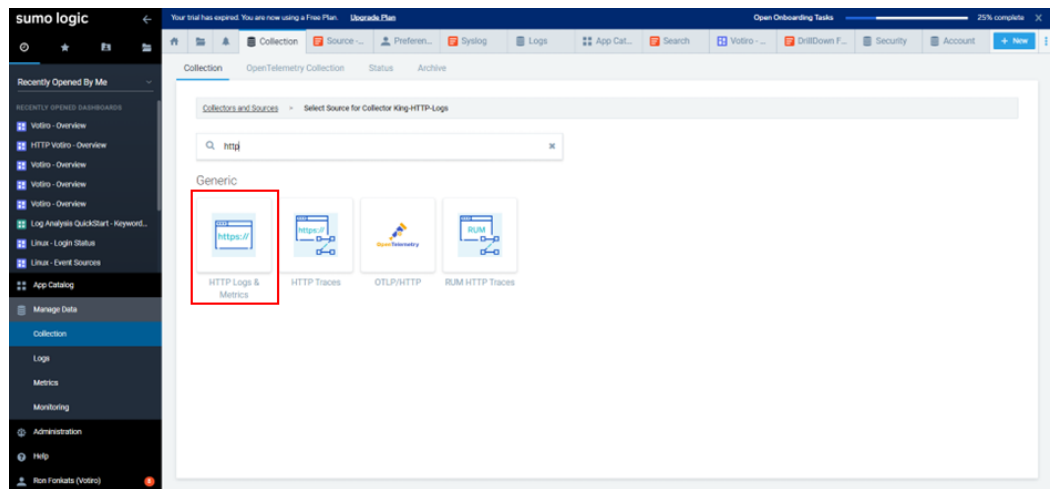
### 13.1.1 Configure an HTTP Logs and Metrics Source in Sumo Logic

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

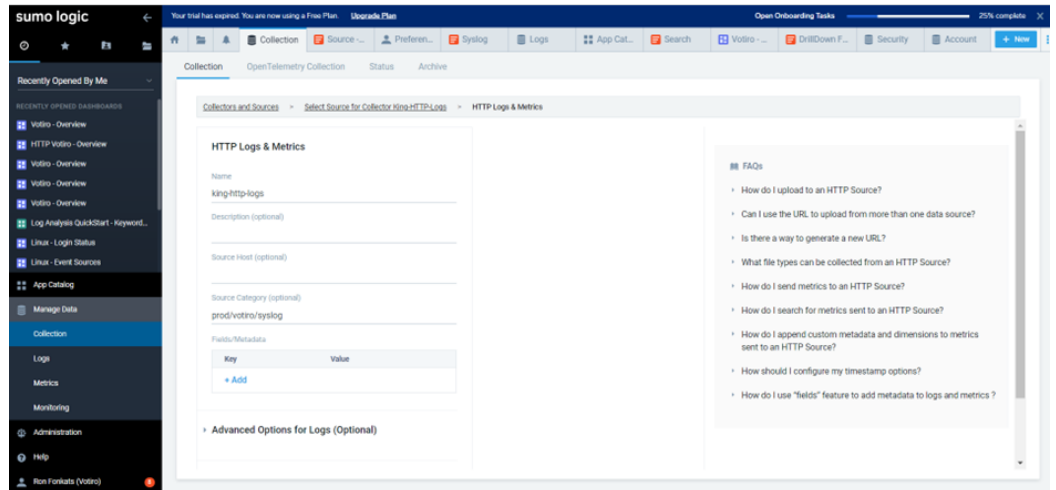


4. In the **Add Hosted Collector** window, type a **Name** and click on **Save**.

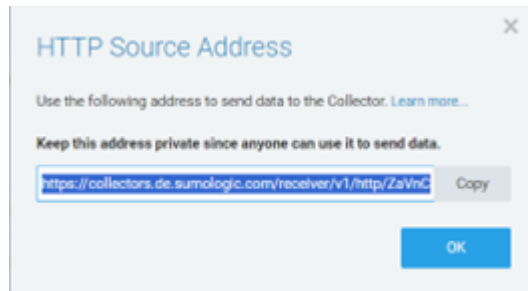
5. To add a source to the collector, click **HTTP Logs & Metrics**.



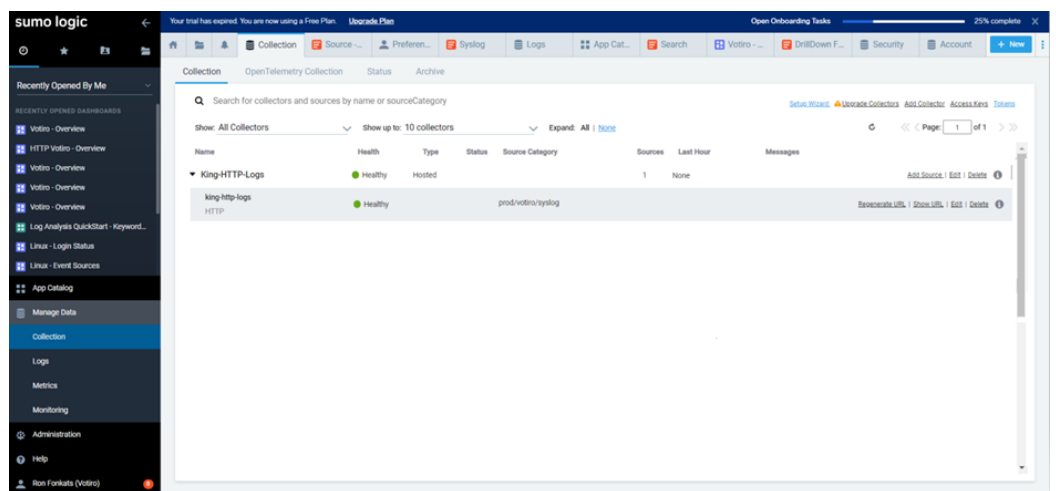
6. In the **HTTP Logs & Metrics** screen:
  - a. Type a **Name**.
  - b. Set the **Source Category** to **prod/votiro/syslog**.
  - c. Click **Save**.



- 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.



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



### 13.1.2 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:

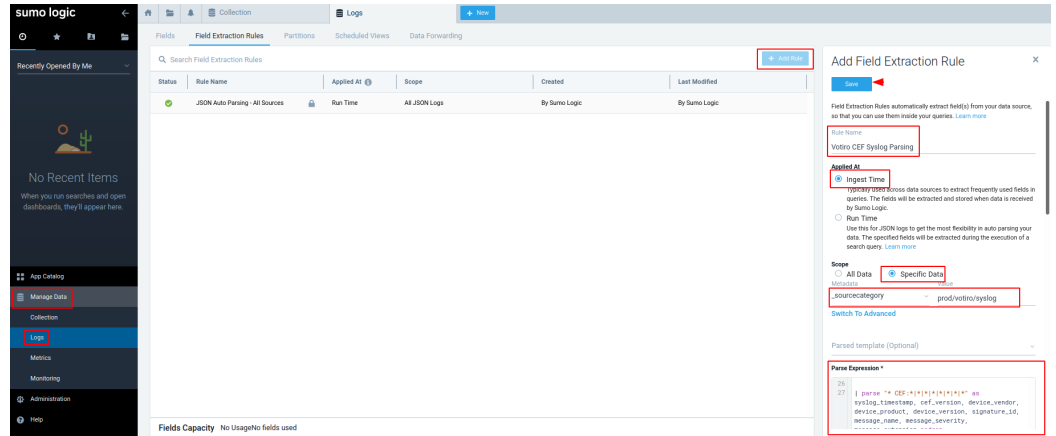
1. Login to the Sumo Logic tenant.
2. Navigate to **Manage Data > Logs > Field Extraction Rules**.
3. In the **Rule Name** field, enter the value **Votiro CEF Syslog Parsing**.
4. In **Applied At**, select **Ingest Time**.
5. In **Scope**, select **Specific Data**.
6. Under **Metadata**, select **\_sourcecategory**.
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

```

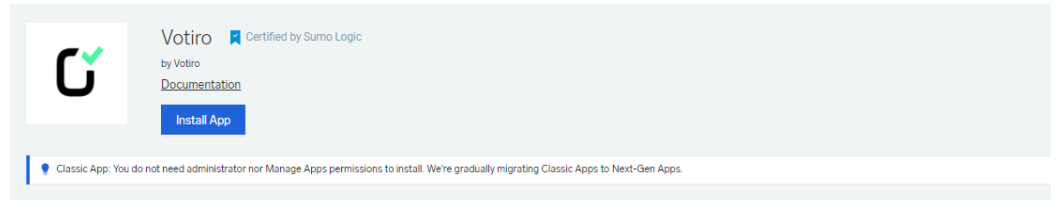
9. Paste the copied rules into the **Parse Expression \*** field.



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

### 13.1.3 Install the Votiro App

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



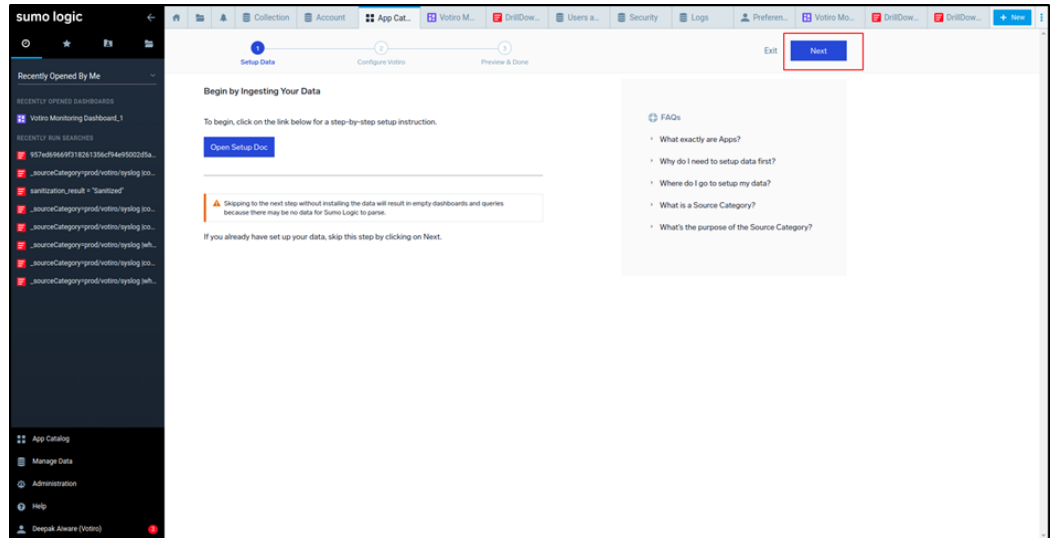
Threat related information sent from Votiro Sanitization engine to Sumo logic customers will allow them better mitigate cyber attacks, do effective threat hunting and enrich cyber security alerts

Preview dashboards included in this app:

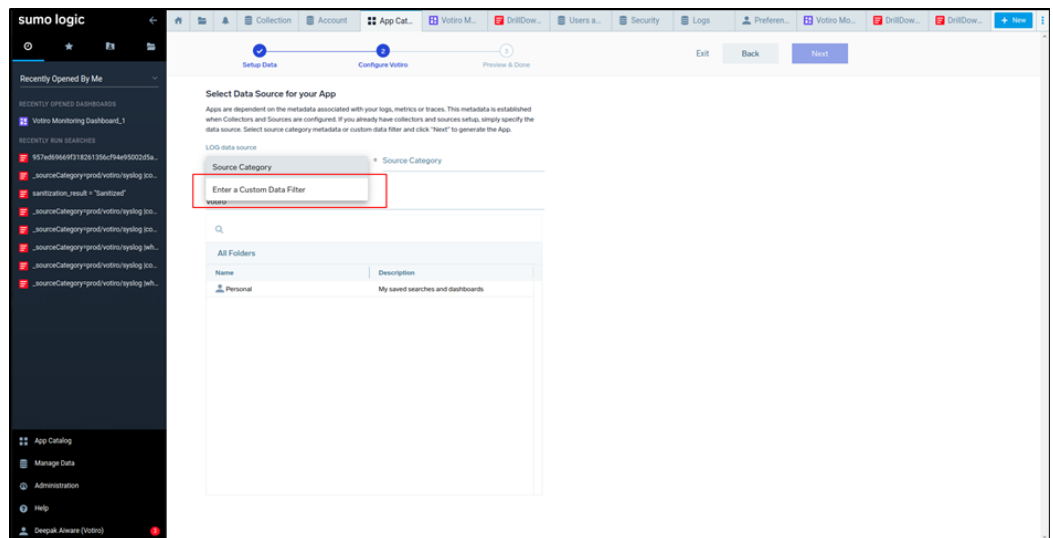


2. Click on **Install App**.

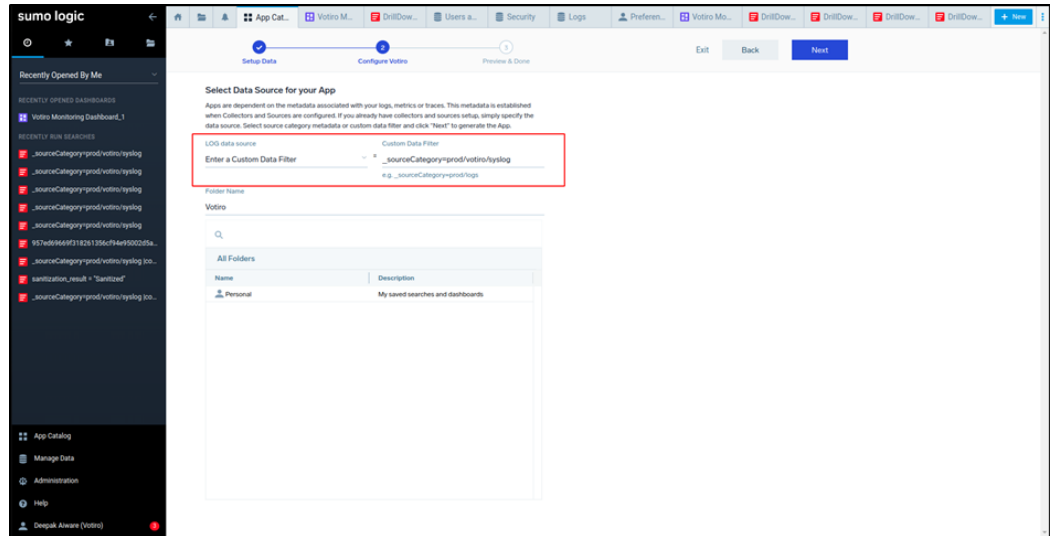
3. After configuring the **collector, syslog source** and **extraction rules**, click on **Next**.



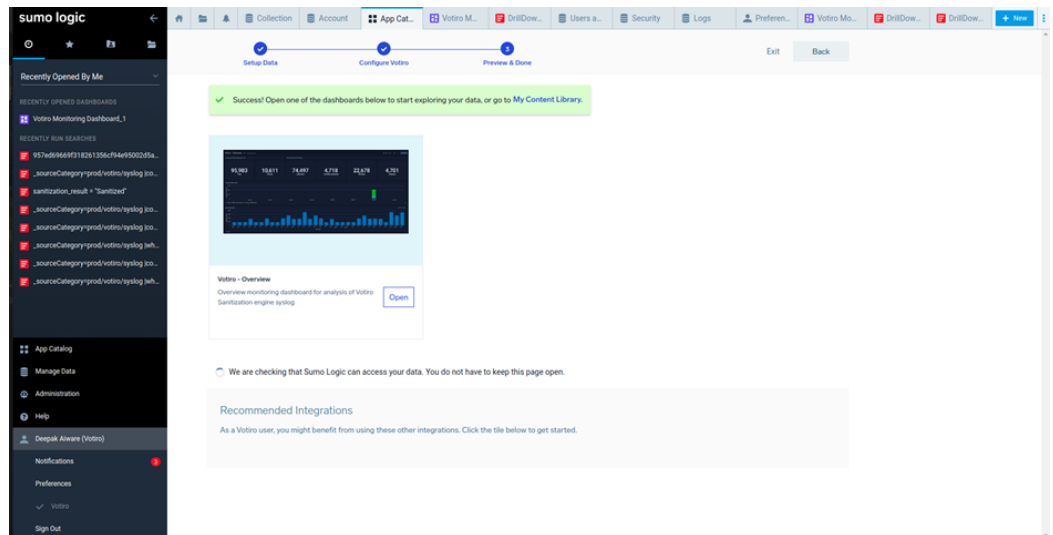
- Under **LOG data source**, in the **Source Category** field, select **Enter a Custom Data Filter** as you did in the above mentioned steps - use the one that you already created.



- 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`

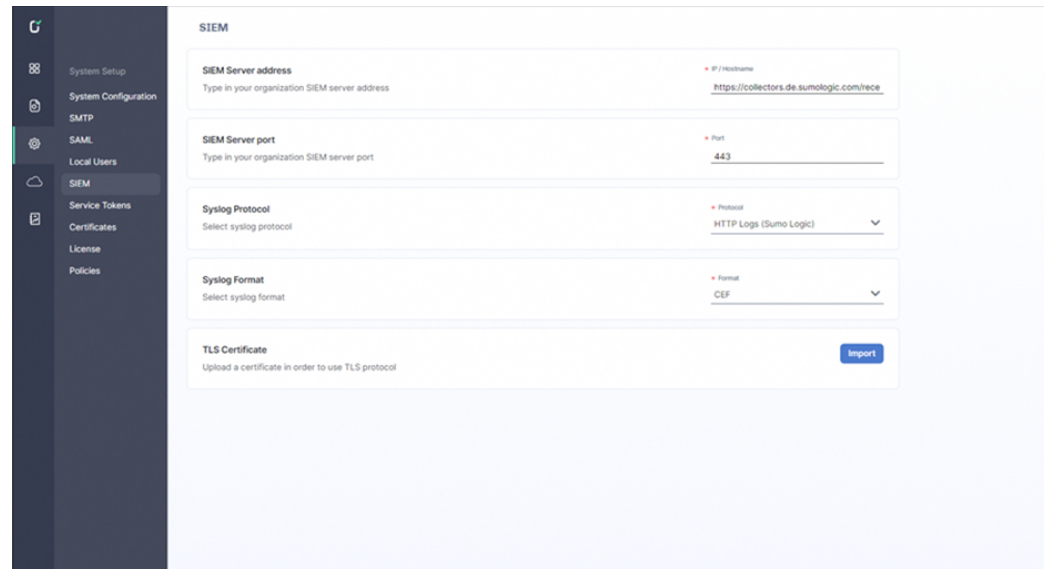


6. Click on **Next**. The Setup completes and a Success message appears and a dashboard is displayed.



### 13.1.4 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.



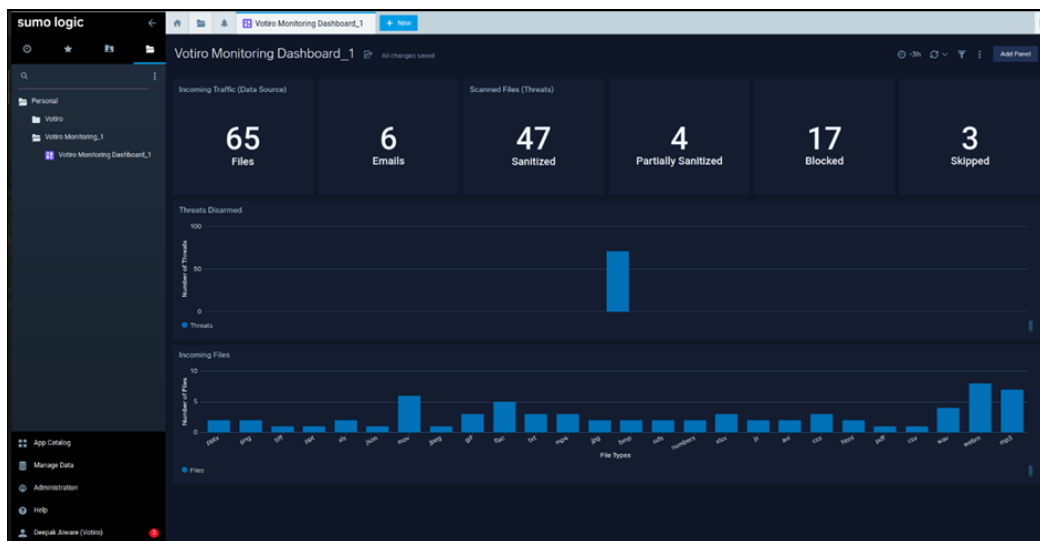
### 13.1.5 Verify the Integration

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

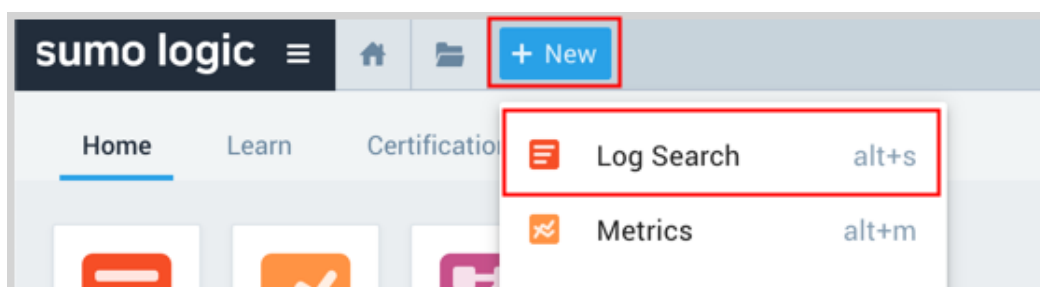
On the Sumo Logic website, open the newly imported folder **Votiro Monitoring Dashboard**. Data coming from the configured source should be shown on this dashboard.



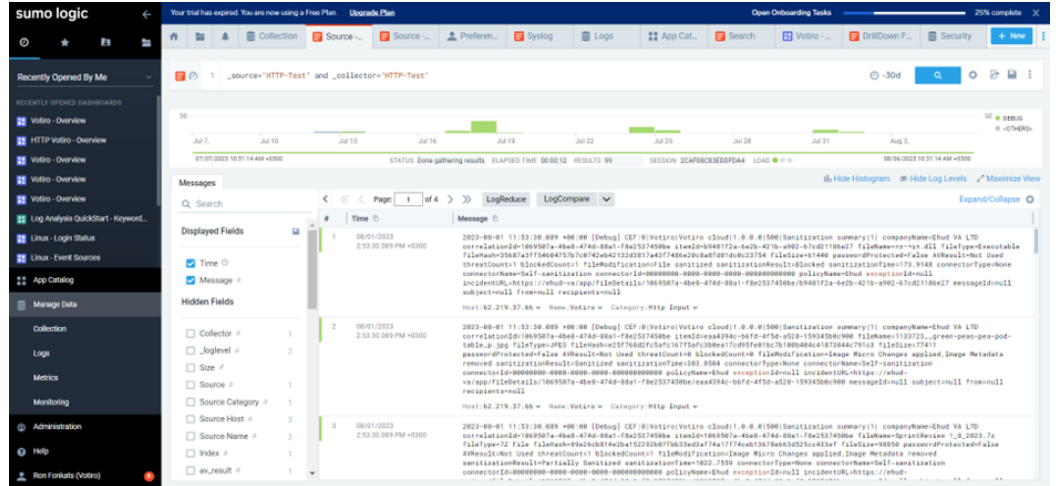
### 3.b Search Ingested Data inside Sumo Logic

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.



3. 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.

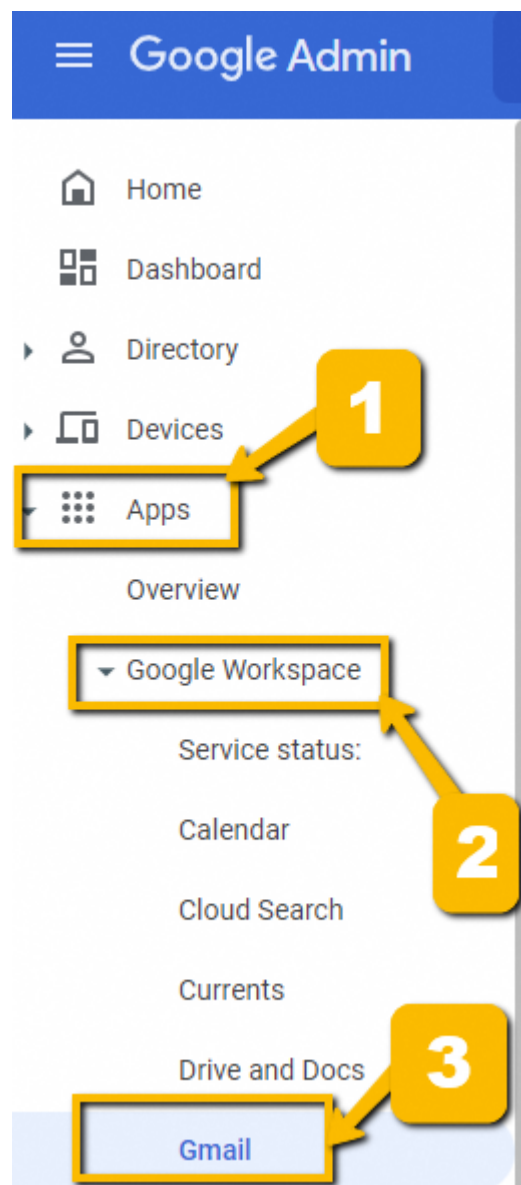


## 14 How to Integrate Votiro with Google Workspace

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

### 14.1 Procedure

1. Sign in to the [Google Admin console](#) with your Google Workspace account.
2. In the left pane, navigate to Apps > **Google Workspace** > **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](#)

Enable

1. Gateway IPs

IP addresses / ranges
[REDACTED]

[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

[i](#) Most changes take effect in a few minutes. [Learn more](#)  
You can view prior changes in the [Audit log](#)

CANCEL 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**.

### 14.1.1 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: "Forward to Votiro Cloud".
  - b. For the option **Specify email server**, select **Single host** and type the host name provided to you by Votiro support.
  - 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 on **Test TLS connection**:

Test TLS connection

TLS connection validated on January 16, 2025 4:45PM

g. Click on **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 (Recommended)
- Require CA signed certificate (Recommended)
- Validate certificate hostname (Recommended)

[Test TLS connection](#)

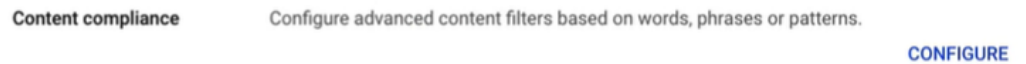
CANCEL [SAVE](#)

### 14.1.2 Configure content compliance rule for emails received from Votiro On-prem

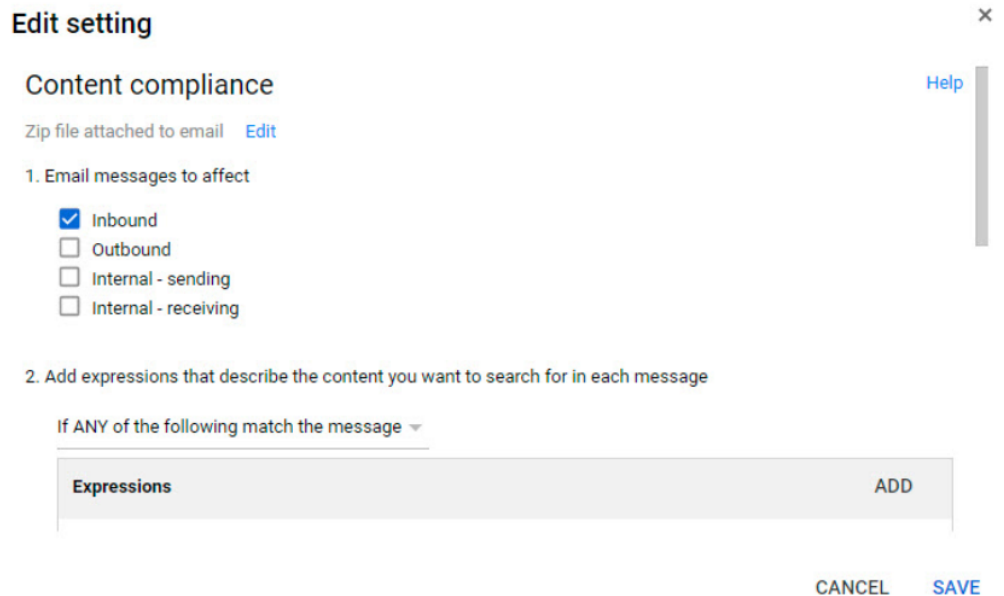
10. Return to **Settings for Gmail** and select **Compliance**:



11. Under **Content compliance**, select **CONFIGURE**.



- a. Specify a name for the new rule, for example “To 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**.



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



## Edit 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)**.
- l. 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
- Bypass this setting for specific addresses / domains
- Only apply this setting for specific addresses / domains

B. Account types to affect

- Users
- Groups
- Unrecognized / Catch-all

C. Envelope filter

- Only affect specific envelope senders
- Only affect specific envelope recipients

CANCEL SAVE

### 14.1.3 Configure Content compliance rule for emails sent to Votiro On-prem

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 On-prem.
  - 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 addresses provided by Votiro support.
    - 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 [REDACTED] [Edit](#)

[ADD](#)

- d. For 3 - If the above expressions match, do the following: Under **Route**, select **Change route** and make sure "Forward 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.

#### 14.1.4 Votiro Cloud for Sanitization

If incoming traffic is not from the IPs listed above, send it for sanitization.

14. Create a new rule "Sanitized Emails To Google Workspace".
15. Under **Email messages to affect**, check **Inbound**.
16. 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**.
17. For **Advanced content match**, select:

- a. **Location:** Full headers
  - b. **Match Type:** Contains text:
  - c. **Content:** X-MTConnectorResult
18. For **Metadata match**, select:
- a. **Attribute**
  - b. **Source IP**
  - c. **Match type**
  - d. For **Source IP is within the following range**, enter the IP addresses provided by Votiro support.
19. Under **Route**, select **Change route** and set to **Normal Routing**.
20. Under Encryption (onward delivery only), check **Require secure transport (TLS)**.
21. Click **Show options**.
- a. Under **Account types to affect**, check the following boxes:
    - **Users**
    - **Groups**
    - **Unrecognized / Catch-all**
22. Click **SAVE**.

The result of these actions is that for any email with the **X-MTConnectorResult** header and originating from the listed IPs, it is routed to the user's mailboxes as usual, since it has been sanitized.

### 14.1.5 Spam Rule

23. Select **Spam, phishing, and malware**.
24. Add a rule "Trusted Votiro Relay Servers".
25. Select **Options to bypass filters and warning banners**:
  - a. **Bypass spam filters for internal senders**
  - b. **Bypass spam filters for messages from senders or domains in selected lists**
26. Create a new list and name it "Votiro Relay Allow Addresses".
27. Enter the IP addresses provided by Votiro support.

### 14.1.6 Prevent Email Authentication Protocol Failures

To prevent email authentication protocol failures (DKIM, DMARC, and SPF), it is necessary to manually add Google's MX server prefix so that authentication checks are performed on the correct IP address of the originating sender.

This will prevent legitimate emails from being sent to your spam folder or flagged as suspicious.

To do so, follow the steps below:

1. In the Google Workspace Admin console, navigate to Menu > **Apps** > **Google Workspace** > **Gmail** > **Spam, Phishing, and Malware**.
2. Select your top-level organization on the left, scroll to the **Inbound gateway** setting, then click Edit.
3. Click **Add** and enter the IP range of the region. For example: 209.85.128.0/17

**Note:** Verify the IP range, as it may differ depending on the customer's location. Hint: Check the IP in the email header and look for similar [here](#).

4. At the bottom, ensure that the **Automatically detect external IP (recommended)** box is checked.
5. Save your changes and retest the configuration.

### 14.1.7 How To Resolve Google's SPAM Email Alert On SaaS

When utilizing Votiro's relay servers for SMTP traffic, our customers may encounter emails flagged as suspicious and in the "spam" folder. This occurs because the SPF (Sender Policy Framework) check fails, as Votiro's servers are not the original source IP that generated the email.

In this case, Gmail examines the "Received: from" message headers to identify the first public IP address not in the Gateway IP list and treats this IP address as the source IP for the message. This IP address is used for SPF authentication and spam assessment.

We must ensure that Google can continue to scan for the source IP received from the header in the flow to authenticate the source IP and not the first public IP address in the mail flow, as this is not the sender's source IP.

To address this issue, Google requires you to configure Votiro's servers as an inbound mail gateway. The instructions to do this are outlined in the article [Set up an inbound mail gateway](#). A summary of these instructions as applied to Votiro are as follows:

1. In the Google Admin console, navigate to Menu > **Apps** > **Google Workspace** > **Gmail** > **Spam, Phishing and Malware**.
2. Select your top-level organization on the left, scroll to the **Inbound gateway** setting, then click **Edit**. The Inbound gateway settings open on the page.
3. Click **Add** and enter the IP range: 209.85.128.0/17 in the **Add IP address/range** box. Verify this range, as it may differ depending on the customer's location (Hint: Check the IP in the email header).
4. At the bottom, ensure that the **Automatically detect external IP—(Optional)** box is checked.
5. At the bottom, click **Save**. Note that the changes may take time before going into effect.

6. Test the configuration again.

To summarize, by ensuring that the IP range is on the "Inbound" list, we allow Google to scan the first public IP address that is NOT on the list.

Here is an example of how it should look when an SPF check passes from "DocuSign".

Hops	Submitting host	Receiving host	Time	Delay	Type
1	docuSign.net ([127.0.0.1])	SE102F881.corp.docuSign.net	9/17/2024 12:26:23 PM		Microsoft SMTPSVC(10.0.17763.1697)
2	SE102F881.corp.docuSign.net [se-c101-f51-81.corp.docuSign.net [10.101.81.9]]	mailsea.docuSign.net (Postfix)	9/17/2024 12:26:23 PM	0 seconds	ESMTP
3	mailsea.docuSign.net [mailsea.docuSign.net [64.207.219.9]]	mx.google.com	9/17/2024 12:26:24 PM	1 second	ESMTPS
4	mail-qt1-f198.google.com	mail-qt1-f198.google.com	9/17/2024 12:26:26 PM	2 seconds	SMTP
5	mail-qt1-f198.google.com [209.85.160.198]	votiro-relay2.prod.votiro.com [10.241.50.238]	9/17/2024 12:26:26 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2; cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
6	votiro-relay2 [10.241.50.238]	SDSConnector2	9/17/2024 12:26:26 PM	0 seconds	SDSConnector2 Ver: 1.8.0.0
7	votiro-relay2.prod.votiro.com [ec2-44-206-222-91.compute-1.amazonaws.com [44.206.222.91]]	mx.google.com	9/17/2024 12:26:50 PM	24 seconds	ESMTPS
8		2002:a50:d7e:0:b0:5c:3:d892:1034	9/17/2024 12:26:50 PM	0 seconds	SMTP

# 15 How to Integrate Votiro On-prem with Sumo Logic

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

## 15.1 System Requirements

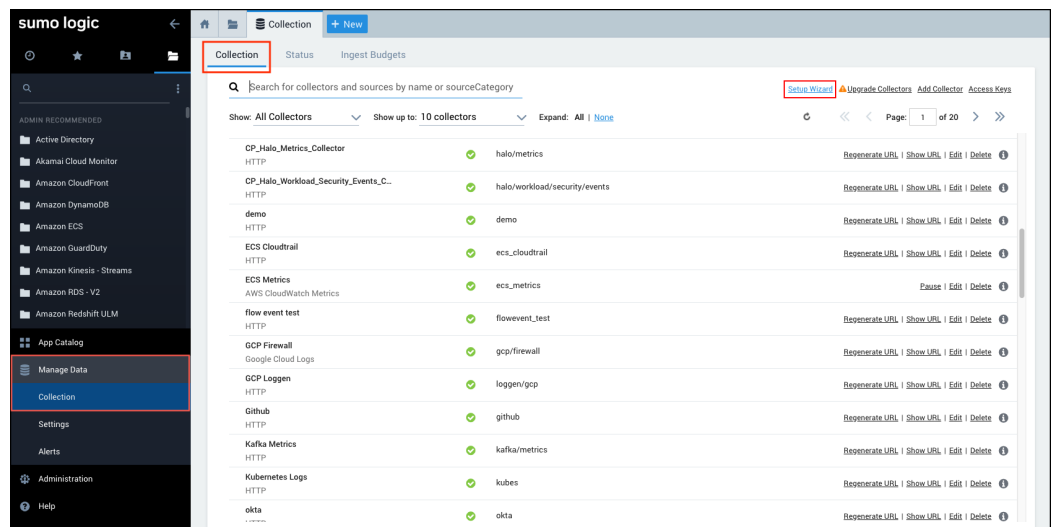
The specifications listed below are for installation of "installed collector" for sending data to the Sumo Logic server.

- 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

## 15.2 Procedure

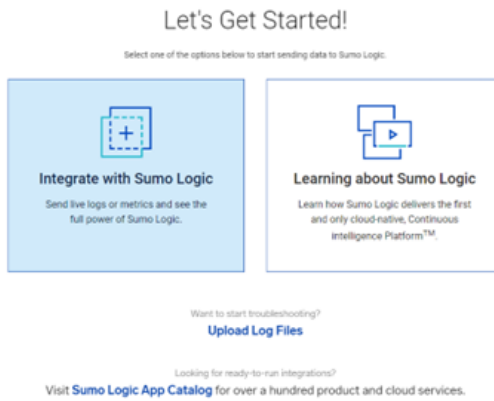
### 15.2.1 Configure the Sumo Logic Syslog Collection

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

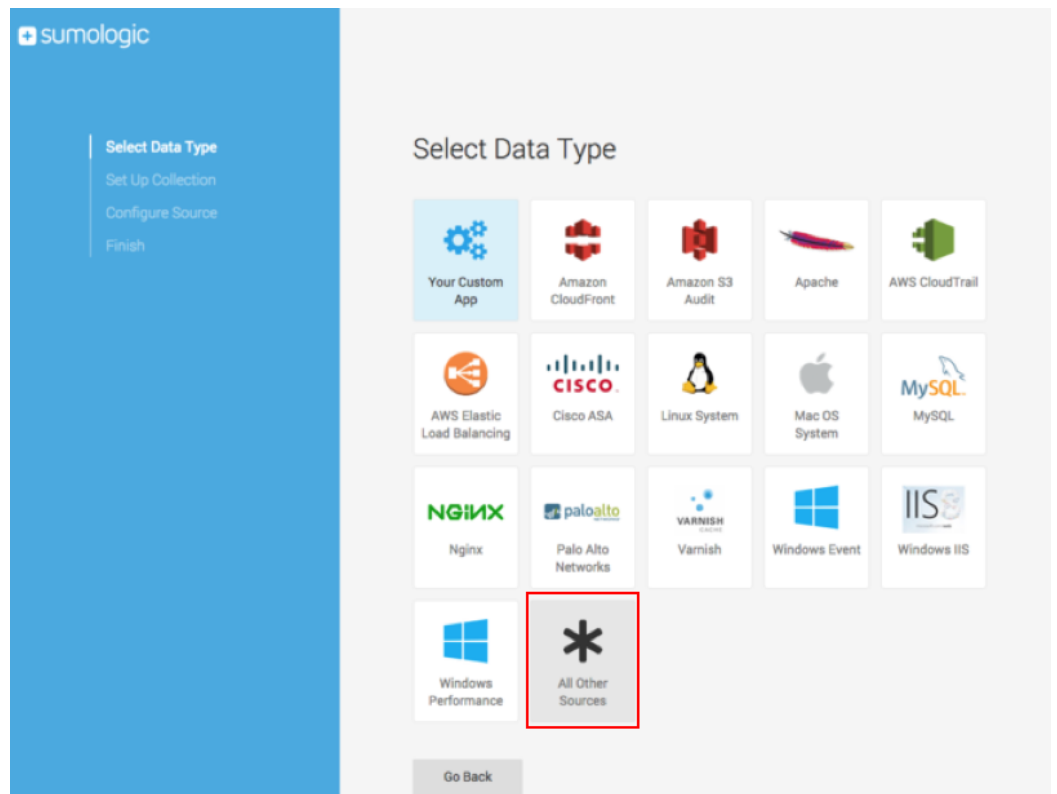


3. Click on **Integrate with Sumo Logic**.

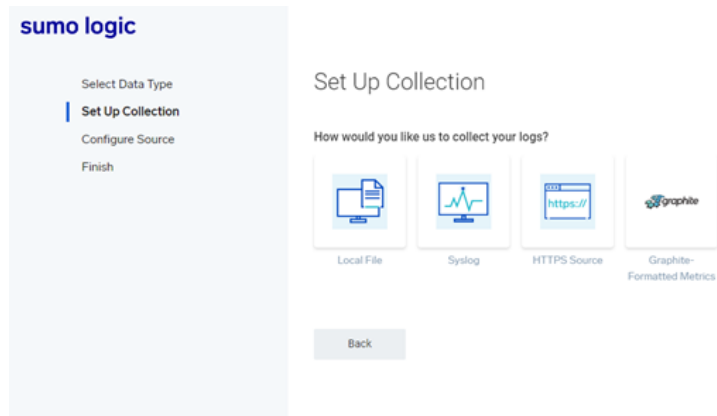
sumo logic



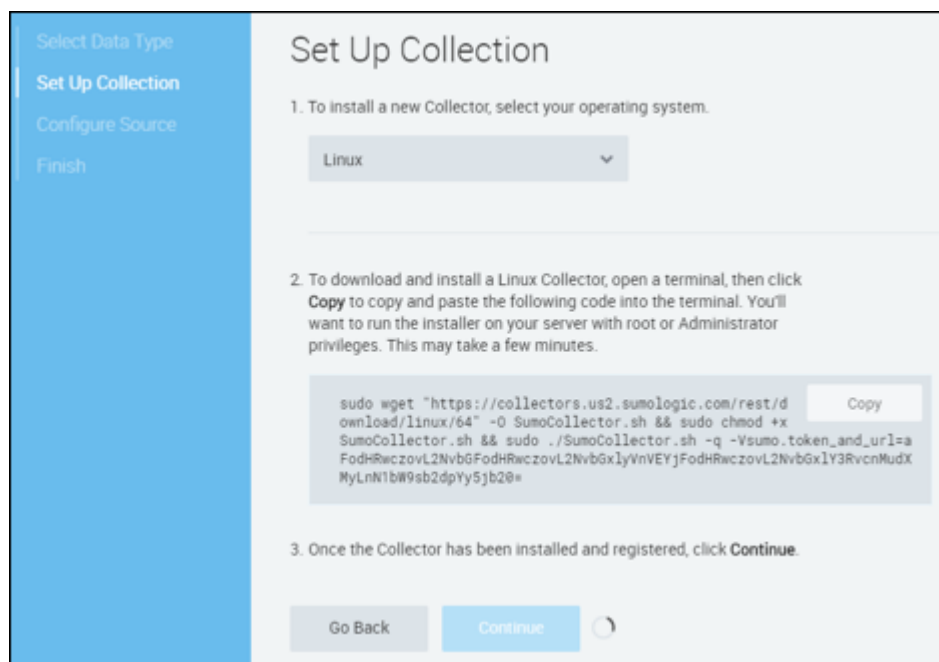
- Under **Select Data Type**, select **All other sources**.



- Under **Set Up Collection**, select **Syslog**.

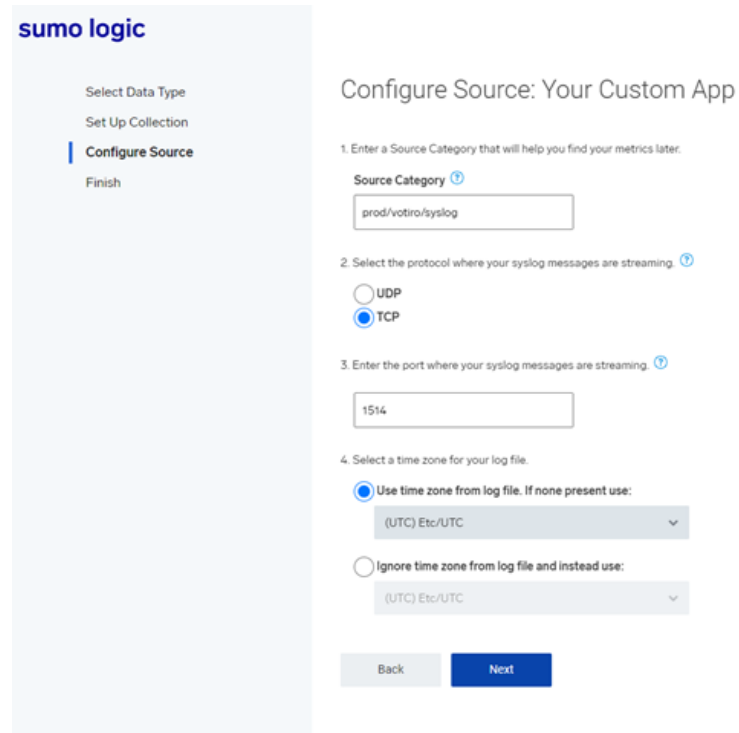


6. Under **Set Up Collection**:
  - a. In step **1. To install a new Collector...**, select **Linux**.
  - b. In step **2. To download and install a Linux Collector...** click **Copy** to copy the code, then paste it into the Linux terminal and run it in your Linux server as root or Administrator.
 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

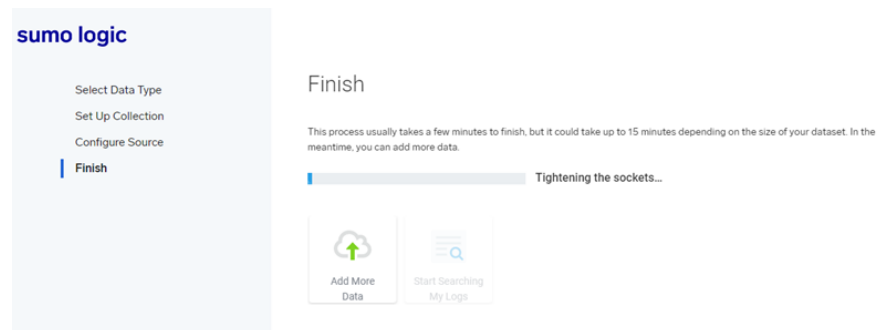


7. Under **Configure Source**:
  - a. In **1. Enter a Source Category...** field, type the value: **prod/votiro/syslog**.
  - b. In **2. Select the protocol...**, select **TCP**.
  - c. In **3. Enter the port...**, type the value **1514**.
  - d. In **4. Select a time zone...**, select **UTC**.

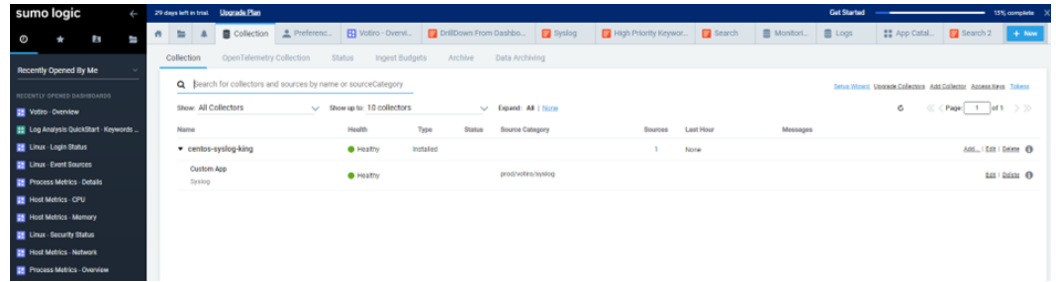
e. Click on **Next**.



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



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



### 15.2.2 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:

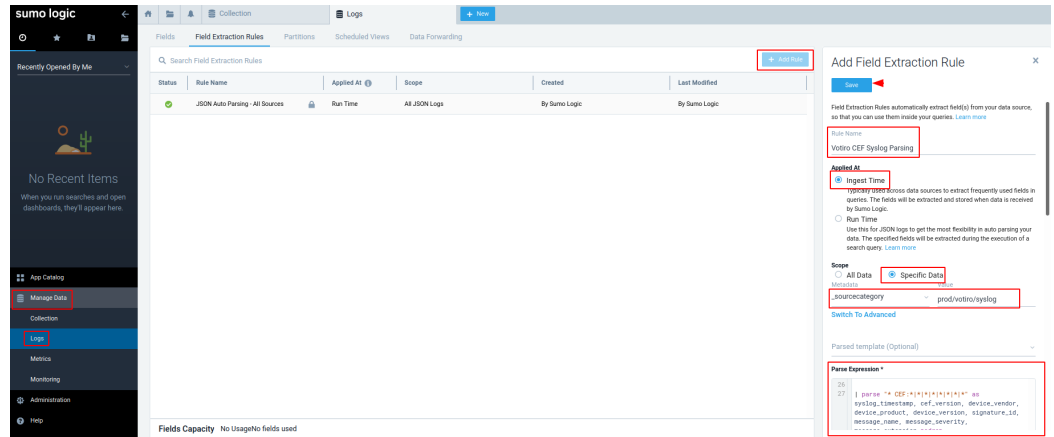
```

| 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
```

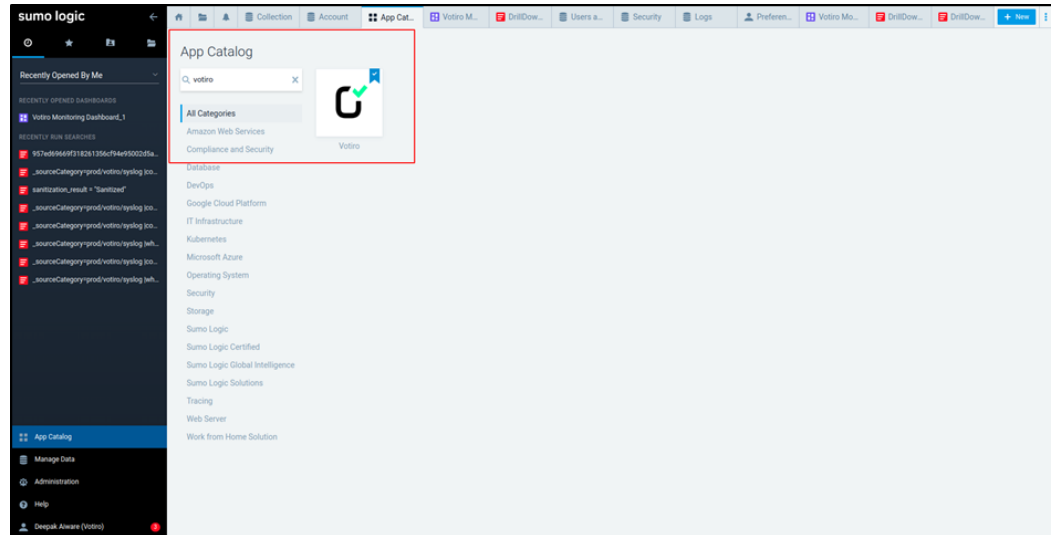
9. Paste the copied rules into the **Parse Expression \*** field.



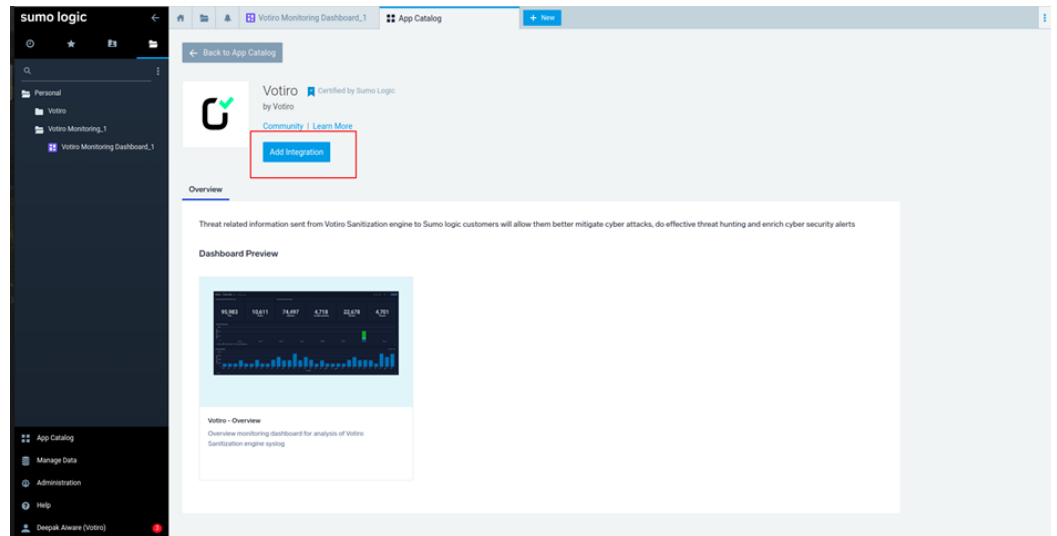
10. Click on the **Save** button.

### 15.2.3 Install the Votiro App

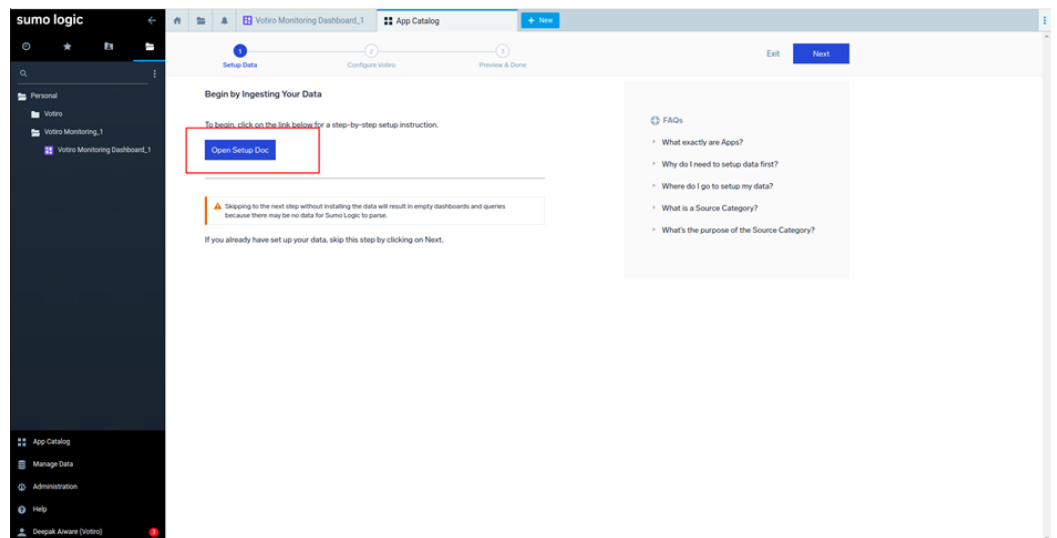
1. Navigate to the **App Catalog** on the Sumo Logic tenant and search for **Votiro**.



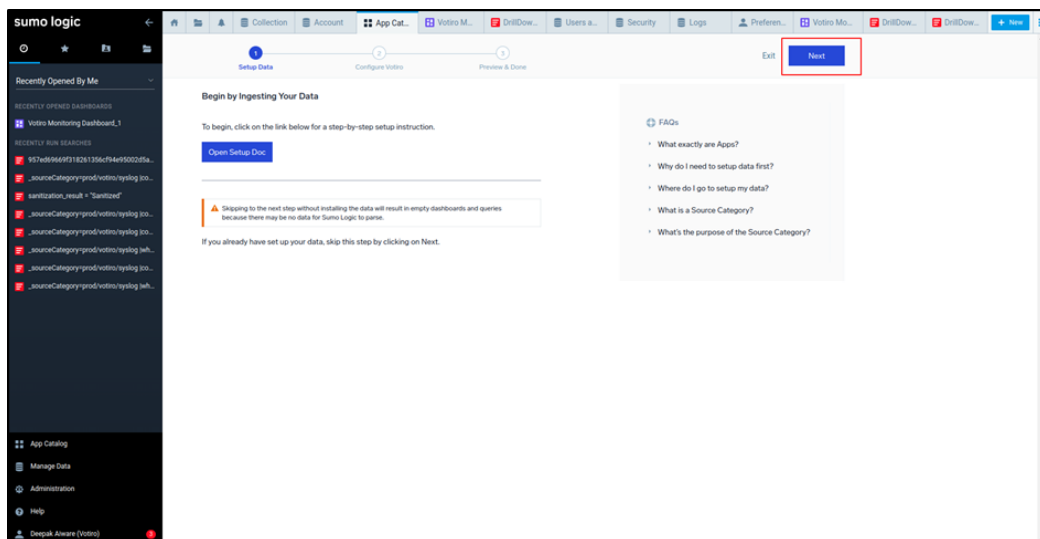
2. Click on **Add Integration**.



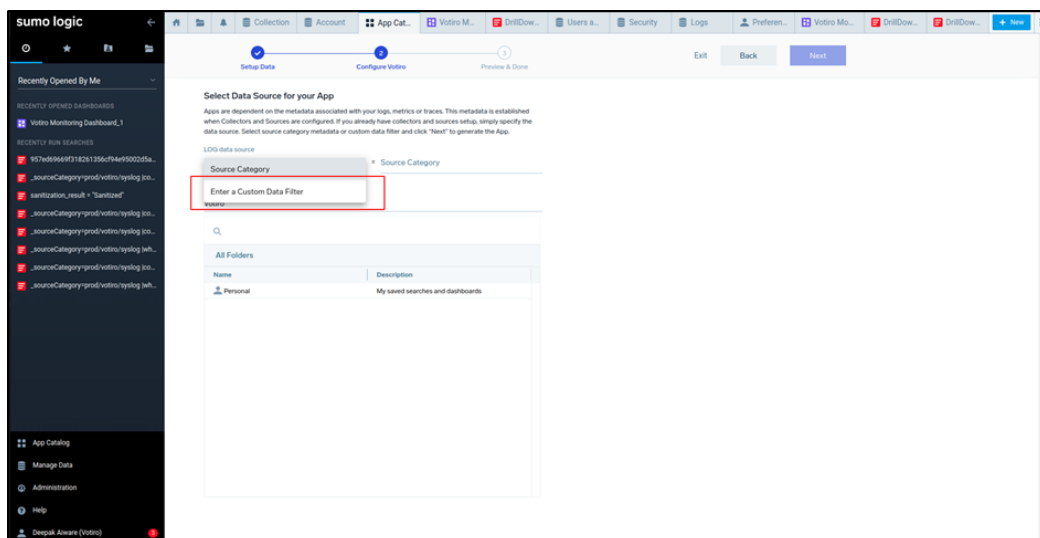
3. Click on **Open Setup Doc**. This will take you to the documentation on the Sumo Logic Github page.



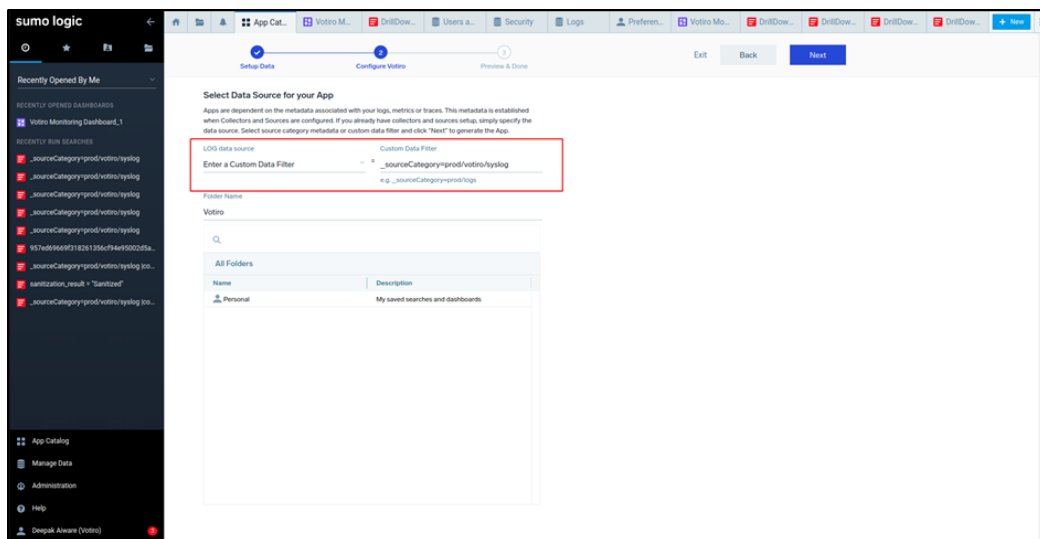
4. After configuring the **collector**, **syslog source** and **extraction rules** with the help of the Setup Doc, click on **Next**.



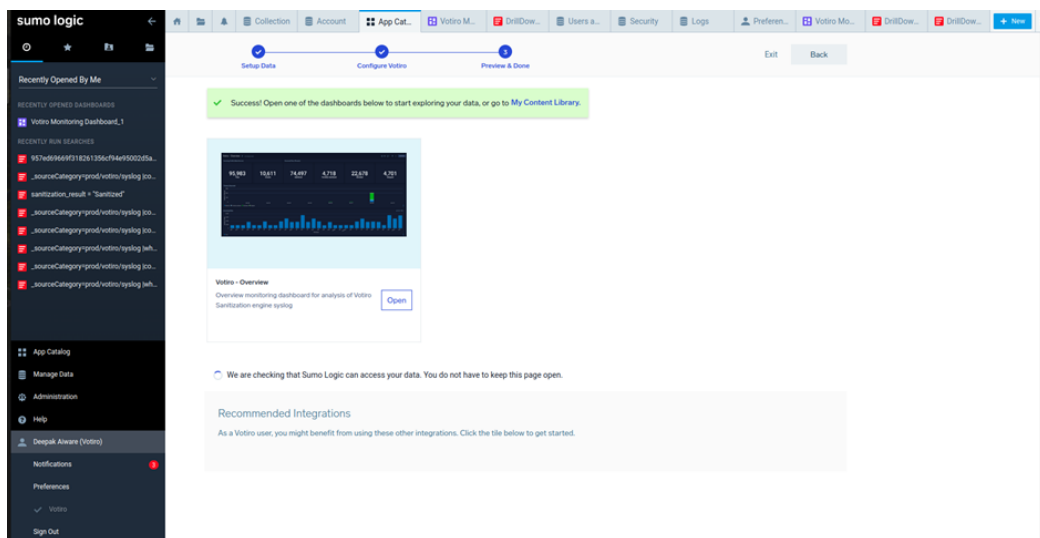
- Under **LOG data source**, in the **Source Category** field, select **Enter a Custom Data Filter** as you did in the above mentioned steps - use the one that you already created.



- 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`

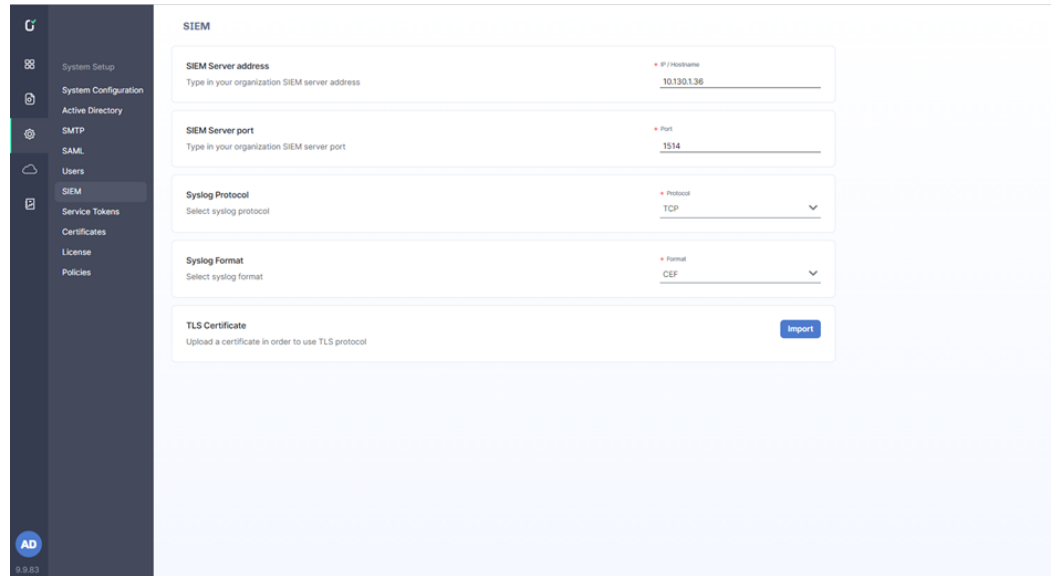


7. Click on **Next**. The Setup completes, a Success message appears and a dashboard is displayed.

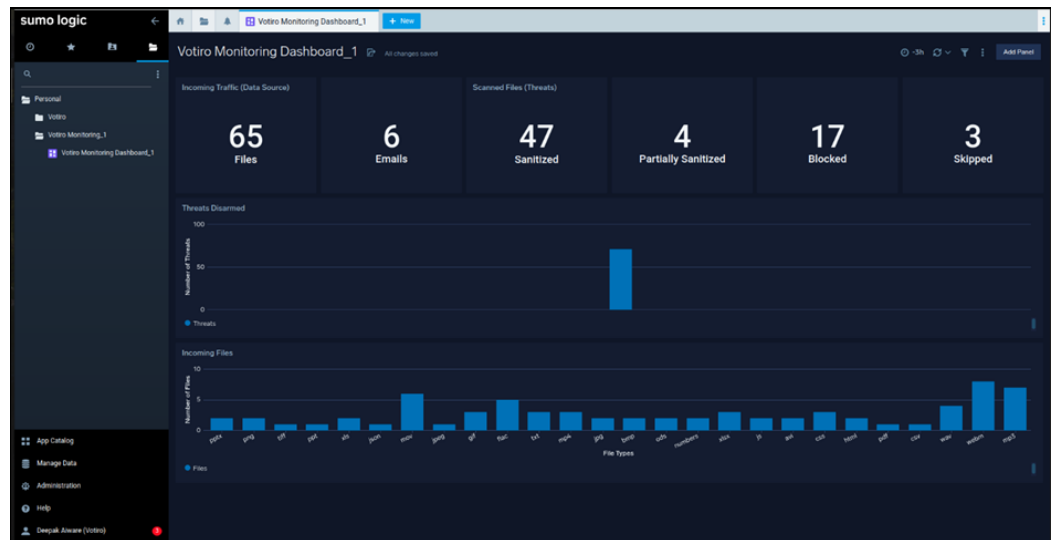


### 15.2.4 Integrate Votiro Management Console with Sumo Logic Syslog Collector

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.



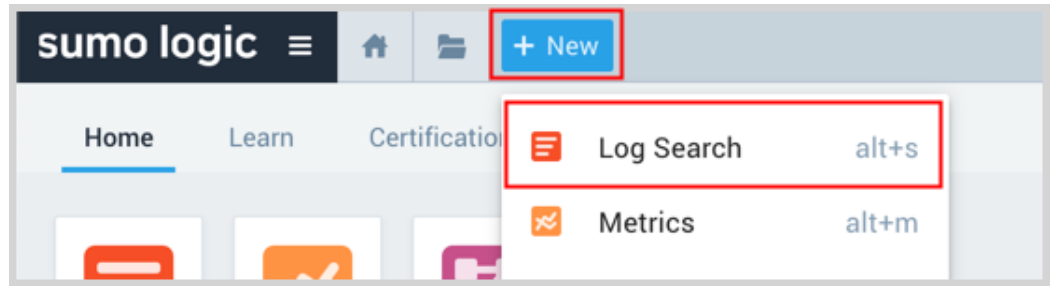
4. On the Sumo Logic website, open the newly imported folder **Votiro Monitoring Dashboard**. Data coming from the configured source should be shown on this dashboard.



### 15.2.5 Search Ingested Data inside Sumo Logic

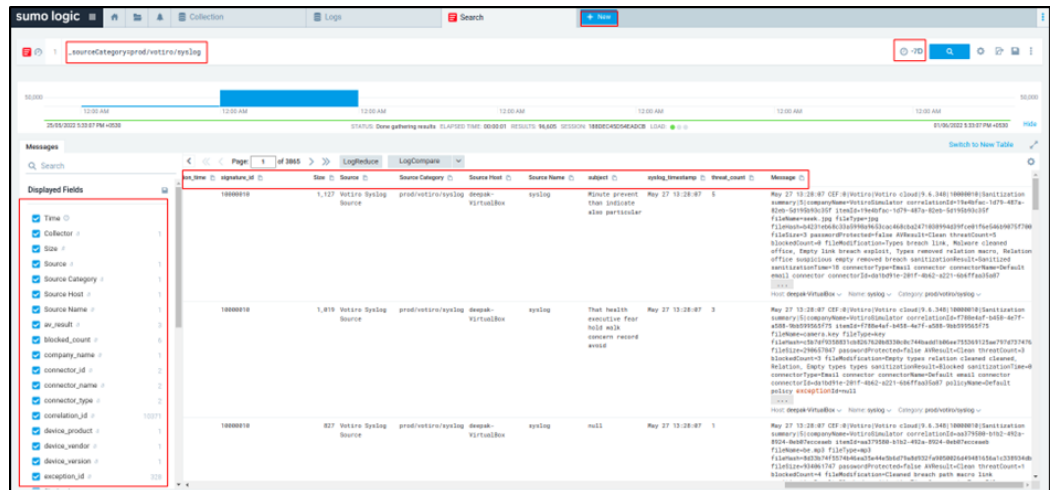
Data ingested inside Sumo Logic can be easily searched using the source category by which the data was indexed.

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



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.



## 15.2.6 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
```

```

metron@metron-VirtualBox: ~/Downloads/votiro-sumologic/event-simulator/src
metron@metron-VirtualBox:~/Downloads/votiro-sumologic/event-simulator/src$ pipenv install
Creating a virtualenv for this project...
Using Python (Python3.8.10) to create virtualenv...
Created virtual environment CPython3.8.10.final.0-64 in 1443ms
creator CPython3.8.10.final.0-64 /home/metron/.local/share/virtualenvs/event-simulator-GLNZAB0, clear=False, global=False)
header FromAppData(download=False, pip/latest, setuptools/latest, wheel/latest, pkg_resources/latest, via=copy, app_data_dir=/home/metron/.local/share/virtualenvs/seed-app-data/v1.0.1-debian.1)
activators BashActivator,CShellActivator,FishActivator,PowerShellActivator,PythonActivator,XonshActivator

Virtualenv location: /home/metron/.local/share/virtualenvs/event-simulator-GLNZAB0
Installing dependencies from Pipfile.lock (5819ee)...
#
# 4/4
#
To activate this project's virtualenv, run the following:
$ pipenv run

metron@metron-VirtualBox:~/Downloads/votiro-sumologic/event-simulator/src$
metron@metron-VirtualBox:~/Downloads/votiro-sumologic/event-simulator/src$
metron@metron-VirtualBox:~/Downloads/votiro-sumologic/event-simulator/src$
metron@metron-VirtualBox:~/Downloads/votiro-sumologic/event-simulator/src$
metron@metron-VirtualBox:~/Downloads/votiro-sumologic/event-simulator/src$
metron@metron-VirtualBox:~/Downloads/votiro-sumologic/event-simulator/src$

```

## 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
```

## 16 How to Obtain a Votiro On-prem License Key

To obtain a permanent Votiro On-prem license key you must perform the following steps:

1. Create a MachineStats.xml file.
2. Send the MachineStats.xml file to Votiro Support.
3. Receive a license file from Votiro Support.
4. Save to license file in the appropriate folder.

The MachineStats.xml file contains information on the machine that Votiro Votiro On-prem is installed on, such as OS version, memory size and number of cores.

Votiro Support generate a corresponding license key for Votiro Votiro On-prem, which is required for product activation.

### 16.1 Obtaining a License key

#### 16.1.1 Procedure

1. Using the link you received from Votiro Support, download the MachineStats.zip file to the Votiro On-prem server.
2. Extract the zip file.
3. Open CMD with Administrator privileges.
4. Navigate to the MachineStats folder.
5. Run the following command:

```
MachineKeyTool.exe -o c:\  
[FullFileOutputPath]\MachineStats.xml
```

A MachineStats.xml file is created in the chosen destination folder.

6. Send the MachineStats.xml file to Votiro Support via email or via Votiro's Customer Portal.  
  
Votiro Support will provide a license file (VotiroLicense.xml).
7. Place the license file in the SDS-WS installation root folder. The default location is:  
  
C:\Program Files\Votiro\SDS Web Service.

### 16.2 Verifying Votiro Votiro On-prem Activation

To verify that Votiro Votiro On-prem has been successfully activated, navigate to the API log file (the default location is:

C:\Program Files\Votiro\SDS Web Service\Logs\API).

The following is an example of output that should appear in the log:

```
4880-1 | 17/07/2018 16:16:00.208 | 2 Info | License was
validated successfully, license details.
```

**Note**

It can take up to 30 minutes for the information to appear in the API log.

## 16.3 Renewing Your Votiro License Key

To renew your license key contact Votiro Support for a replacement VotiroLicense.xml file. Provide a new MachineStats.xml file if the OS version, memory size or number of cores in your environment have changed since receiving the last VotiroLicense.xml file.

**WARNING!**

Replace your license key when renewal is required. Votiro Votiro On-prem will continue running for a grace period after the renewal date, providing time for you to receive and install the new license key.

At the expiration of the grace period Votiro Votiro On-prem services are stopped and files will not be sanitized.

# 17 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.

## 17.1 Prerequisites

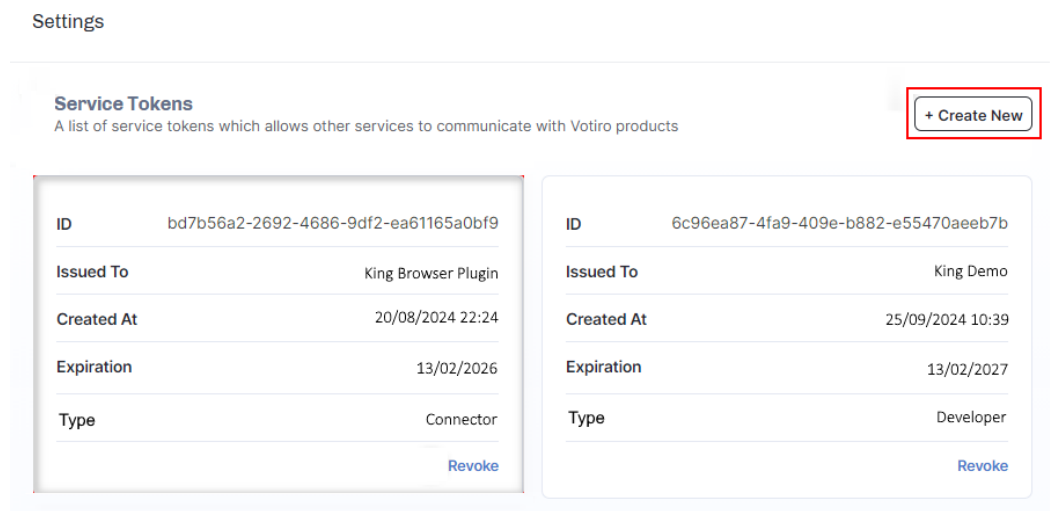
Install Postman by downloading one of the following:

- ◆ The Postman app from [Download Postman](#).
- ◆ The Postman portable app from [Postman™ portable](#).

## 17.2 Procedure

### 17.2.1 Generating a Service Token

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



2. Select the token **Type**:
  - a. **Connector** - Basic integration. Allows authentication for uploading files procedure.
  - b. **Developer** - Advanced integration. For all available APIs. Handle it with caution.
3. Enter a name for the new token under **Issued To**.
4. **Set Expiration Time**
5. Press **CREATE**:

Create New Service Token

---

Type

Connector ?

- Connector
- Developer

Issued To

King Demo

---

Set Expiration Time

<	Feb	2027	>			
Su	Mo	Tu	We	Th	Fr	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28						

CANCEL CREATE

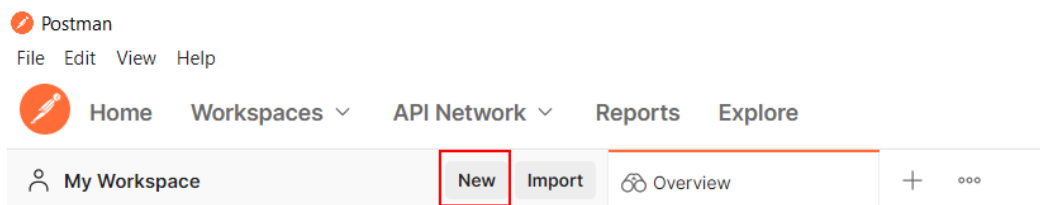
- 6. Copy and save the token string that appears on this page.

**WARNING!**

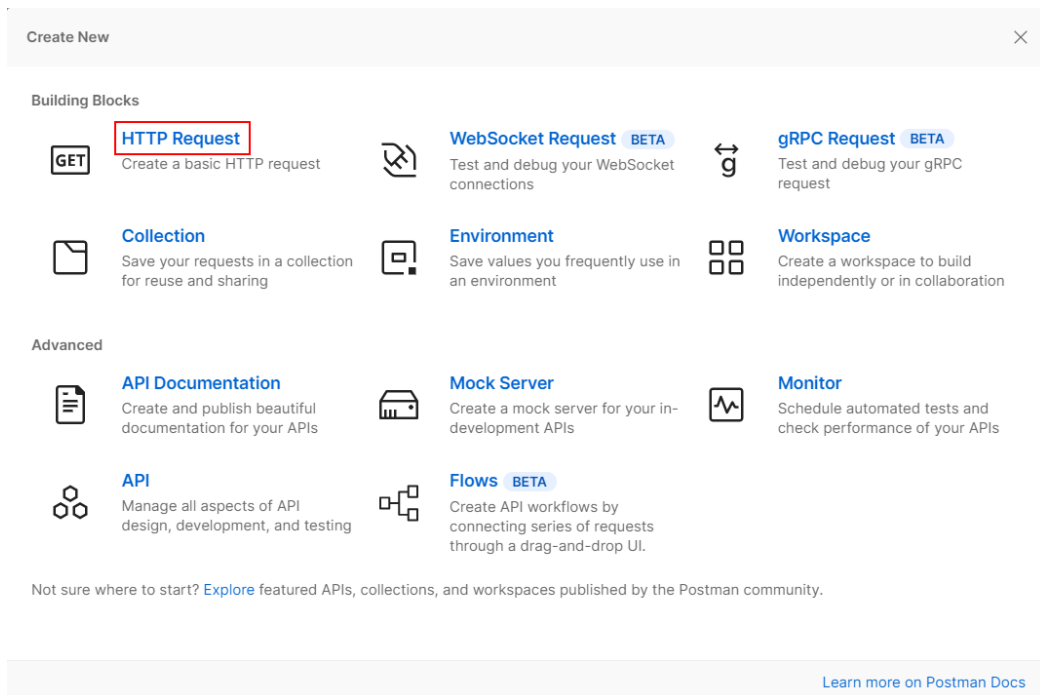


### 17.2.2 Postman Setup

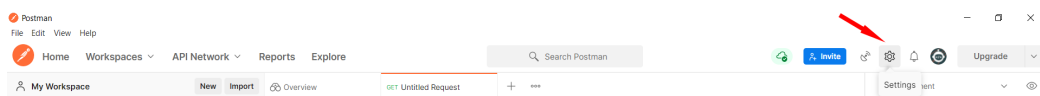
1. In the Postman app, go to **Workspaces > My Workspace** and press **New**:



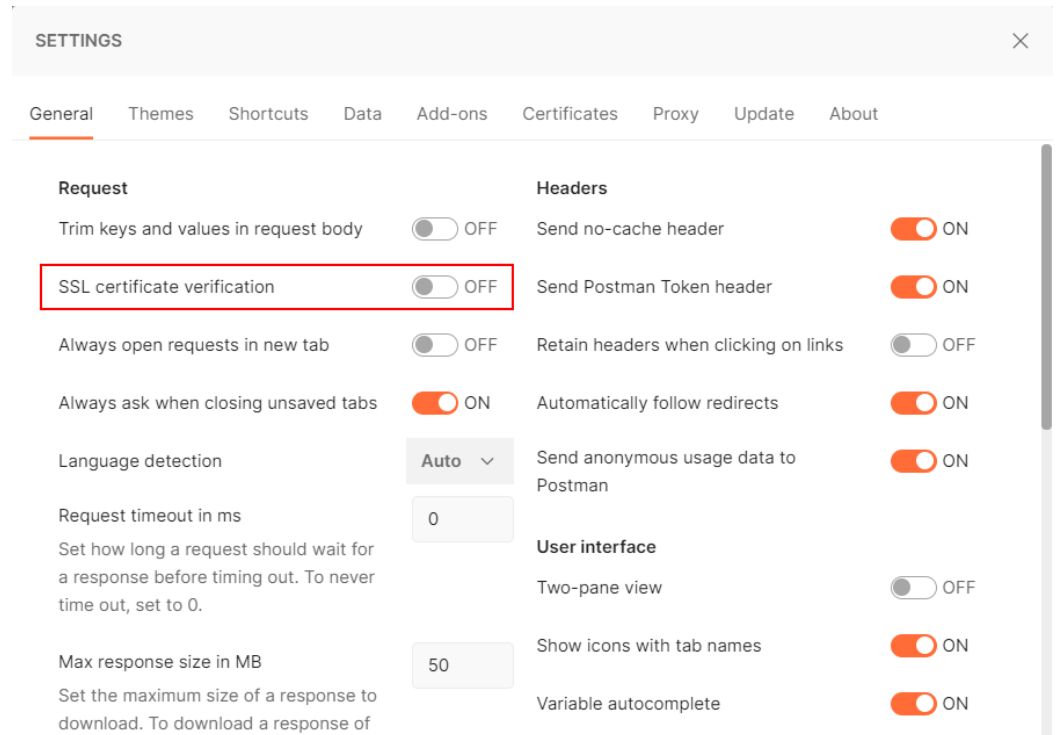
2. The **Create New** window opens. Select **HTTP Request**:



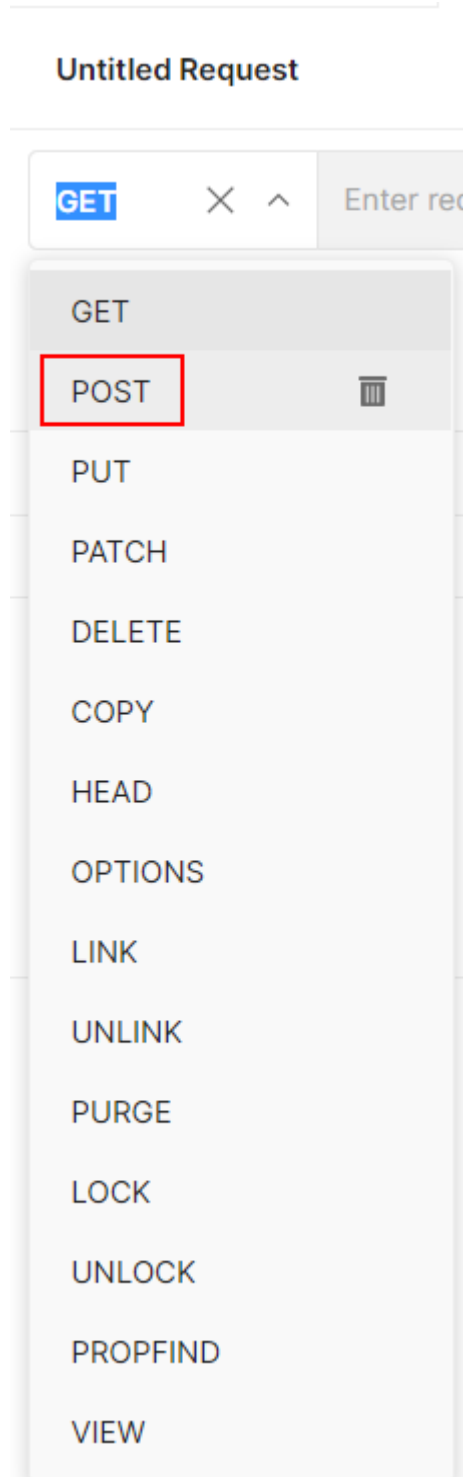
3. Press the **Settings** icon:



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**:

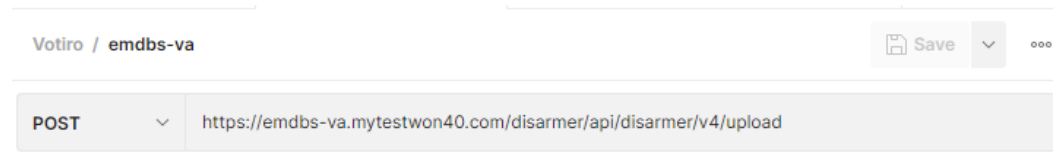


5. Close the **Settings** window.
6. Under the **Untitled Request** dropdown box, select **POST**:

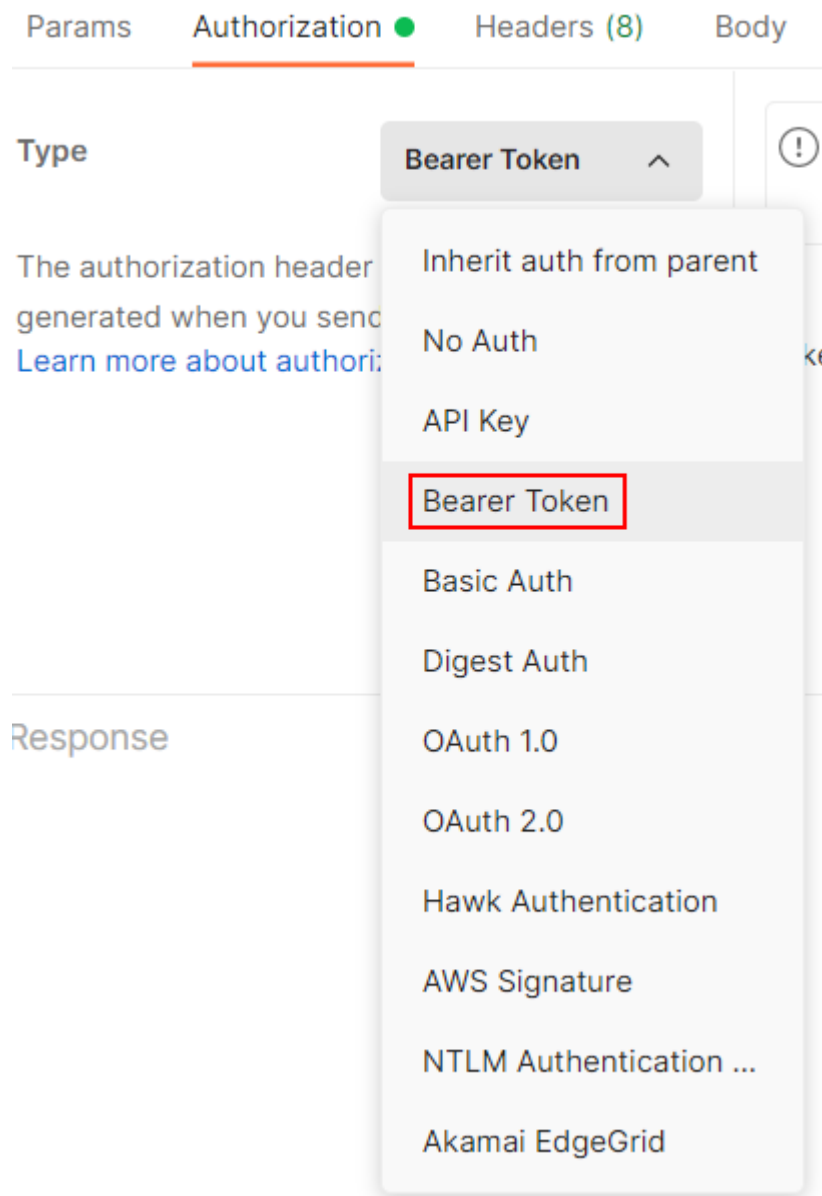


7. In the **Enter request URL** box, enter your VA FQDN in the following format:  
`https://<VA-FQDN>/disarmer/api/disarmer/v4/upload`

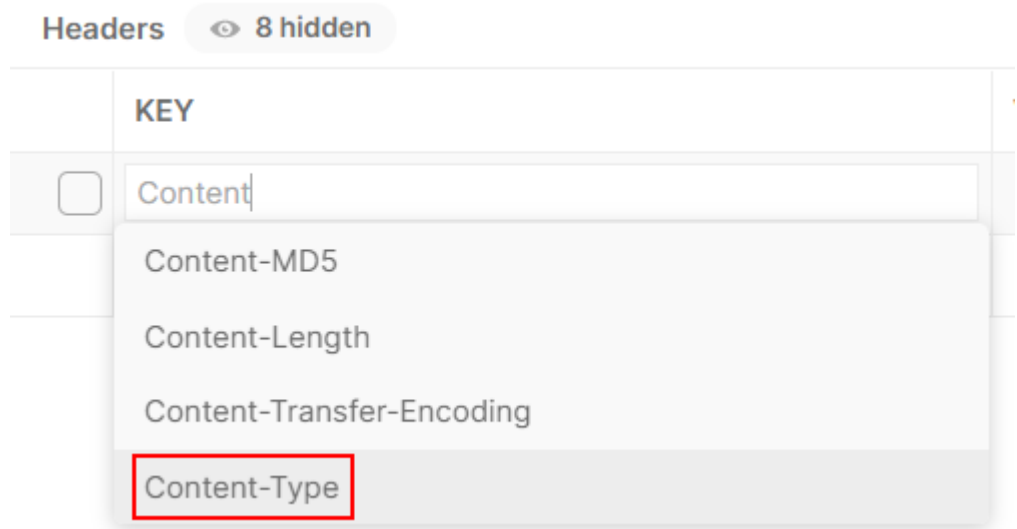
For example:



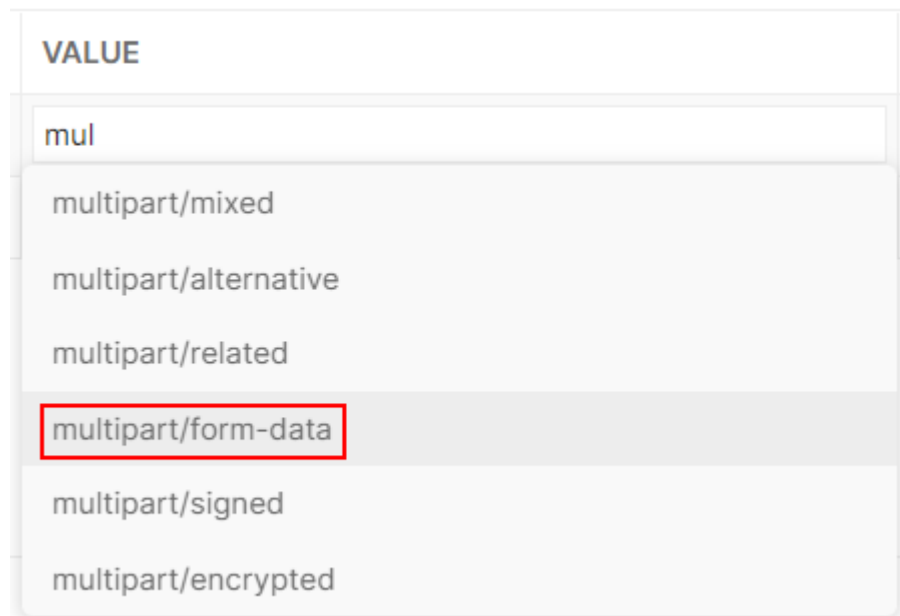
8. Select the **Authorization** tab and under the **Type** dropdown, select **Bearer Token**:



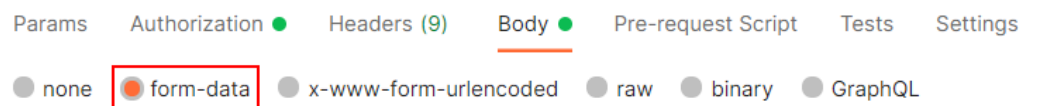
9. Select the **Headers** tab.
10. In the first row of the **Key** column, start to type **Content** until a dropdown list appears. Then select **Content-Type** from the dropdown list:



- 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:



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



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

	KEY	
<input checked="" type="checkbox"/>	File	File v
	Key	Text
		File

- In the first row of the **VALUE** column, press **Select Files** and select the desired file from the browser window that opens.
- In the second row of the **KEY** column, type **Properties**.
- 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" }
            
```
- After completing steps 13-16, the **KEY** and **VALUE** table should be identical to the below screenshot, with the exception of the file name:

Params Authorization Headers (10) **Body** Pre-request Script Tests Set

● none ● form-data ● x-www-form-urlencoded ● raw ● binary ● GraphQL

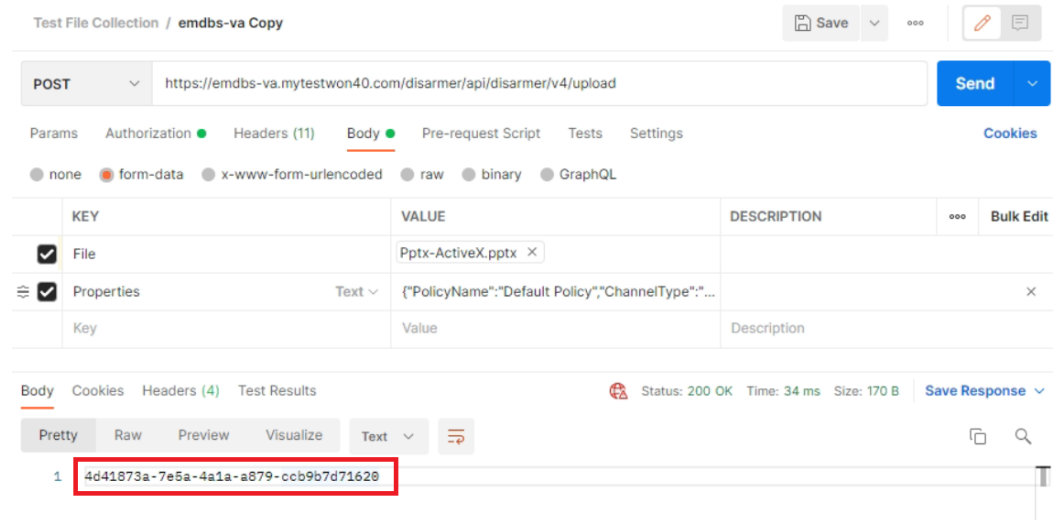
	KEY	VALUE
<input checked="" type="checkbox"/>	File	Pptx-ActiveX.pptx x
<input checked="" type="checkbox"/>	Properties	{"PolicyName": "Default Policy", "ChannelT...
	Key	Value

- Press the **Send** button:

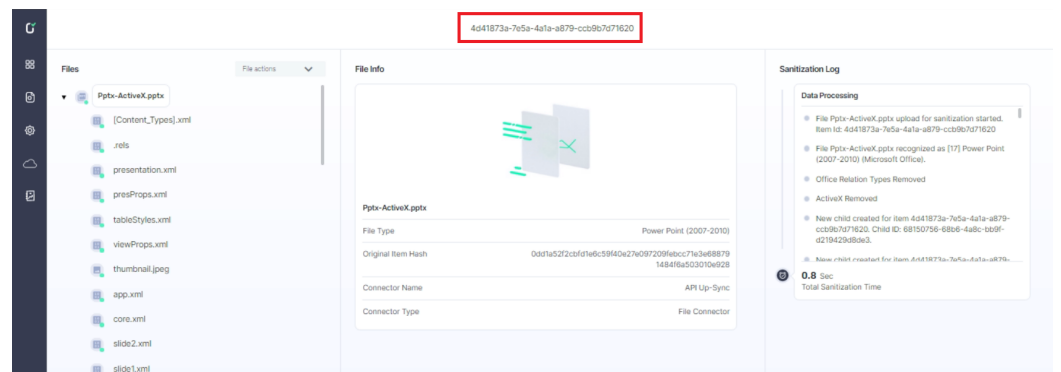
POST https://emdb-s-v-a.mytest140.com/disarmer/api/disarmer/v4/upload **Send**

- 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:



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



## 18 How to Set a Profile for a Domain Group

Having a specific domain group profile allows flexibility with Policy enforcement for users in diverse groups.

### 18.1 Instructions

To add a Profile for a specific Domain group, navigate to the Admin (Management Interface), and follow these steps:

1. Open the **Admin Interface**.
2. Select the **Profiles** tab.
3. Select **Add new profile**.
4. Select the checkbox close to **Verify against Active Directory**.
5. Navigate to **Profile name** and enter the name of the *domain group*.
6. Click **Add**.

## 19 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.

### 19.1 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.

### 19.2 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
```

### 19.3 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 pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#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
```

## 19.4 Verify Time of Synchronization for each Node

To verify the time of synchronization, 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
```

## 20 How to Troubleshoot NTP using Chrony in VA

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

### 20.1 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:

```
● ntpd.service                               not-found inactive dead    ntpd.service
● ntpdate.service                            not-found inactive dead    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-VA1 ~]# 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:

```
210 Number of sources = 3

.-- 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
||                                       \ | | zzzz = estimated error
||                                       | |
MS Name/IP address             Stratum Poll Reach LastRx Last sample
=====
^+ ntp92.kashra-server.com      2  10  377  543  +1370us[+1369us] +/- 3
^* time.cloudflare.com         3   9  377   73  -498us[ -499us] +/- 3
^+ time.cloudflare.com         3   9  377   92  -530us[ -531us] +/- 3
```

- 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:



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

## 20.2 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:

```
[root@dmzcdrem102 ~]# timedatectl
Local time: Tue 2022-07-12 12:36:31 IDT
Universal time: Tue 2022-07-12 09:36:31 UTC
RTC time: Tue 2022-07-12 09:36:30
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 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 ~]# timedatectl
Local time: Tue 2022-07-12 12:43:07 IDT
Universal 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 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.
||                                     .- xxxx [ yyyy ] +/- zzzz
|| Reachability register (octal) -.    | xxxx = adjusted offset,
|| Log2(Polling interval) --.        | | yyyy = measured offset,
||                                     \   | zzzz = estimated error.
||                                     \   |
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@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
Root dispersion  : 1.000000000 seconds
Update interval  : 0.0 seconds
Leap status      : Not synchronised
```

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.

## 21 How to Upgrade Votiro On-prem

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

The latest Votiro On-prem 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.

### 21.1 Upgrade Installation

#### 21.1.1 Before You Begin

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

#### 21.1.2 Procedure

To upgrade your installation of Votiro On-prem 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 -O 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 from version 9.6.3 or later:**

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.

### 21.1.3 Verification of Upgrade

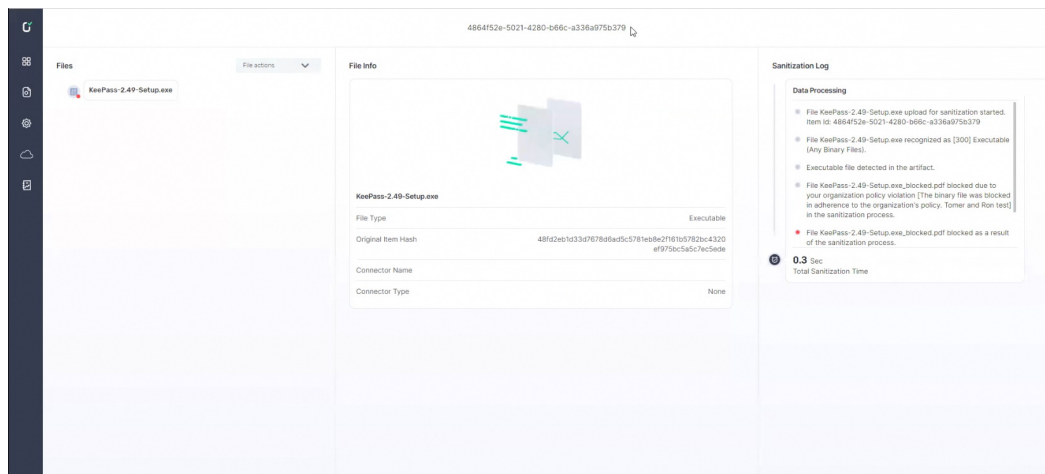
To verify that the upgrade has completed successfully, wait a few minutes, then login to the Management Dashboard. The version number you have upgraded to is displayed.

## 22 How to Use Kibana to Troubleshoot Votiro Incidents

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

### 22.1 Example of Votiro Incident

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



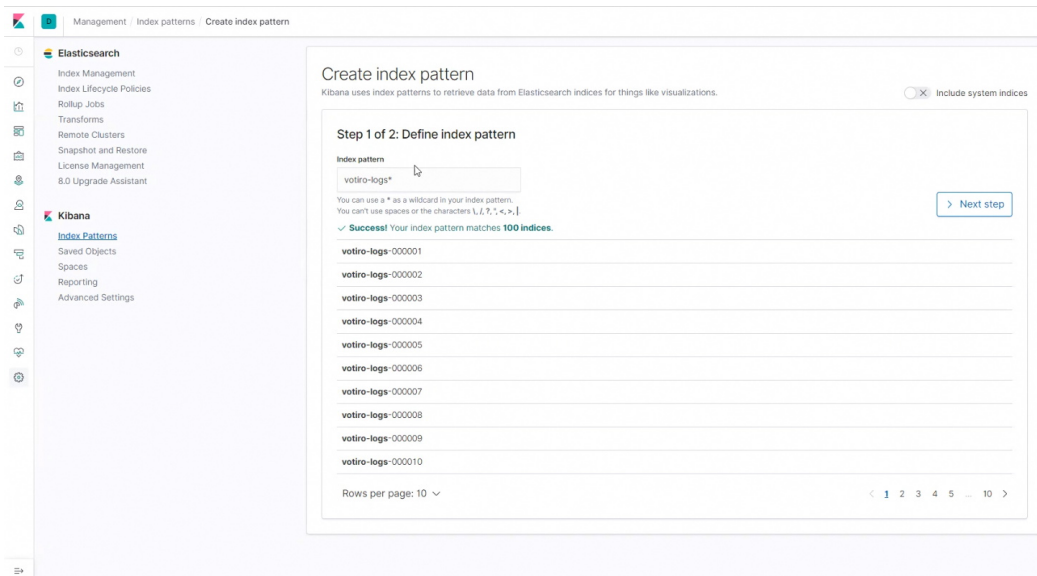
This screen shows the results of Votiro On-prem processing a file named KeePass-2.49-Setup.exe. The **File Info** pane displays some of the file properties and the **Sanitization Log** pane displays highlights of the file **Data Processing**.

## 22.2 Procedure

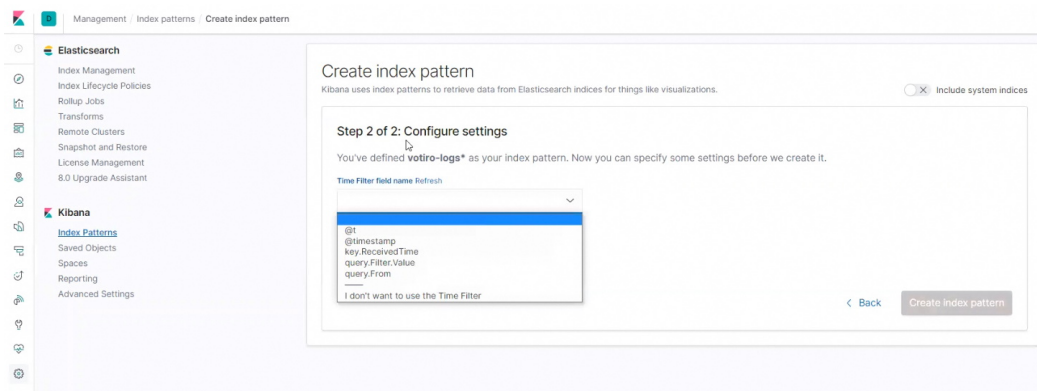
### 22.2.1 Create and Configure an Index Pattern

To begin, you must define a Kibana index pattern.

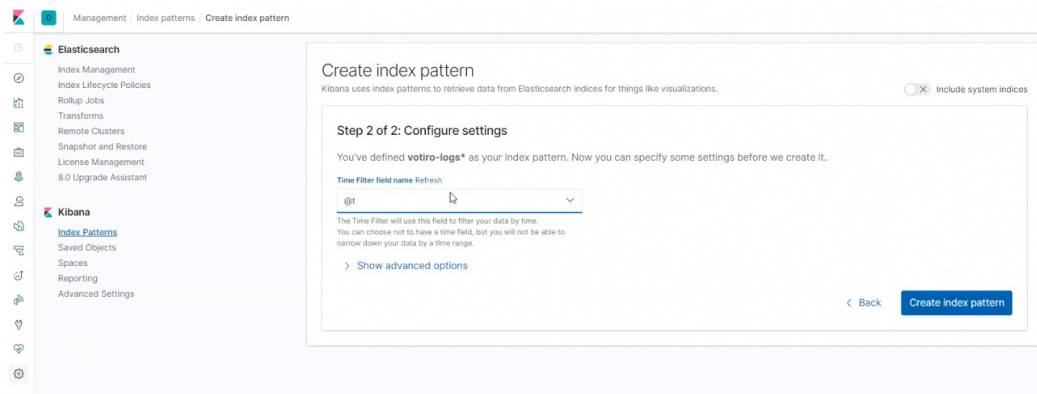
1. Login to the Kibana Discover interface with the credentials provided to you by Votiro Support.
2. Select **Create index pattern**. **Step 1 of 2 Define index pattern** appears.
3. Type **votiro-logs\*** (or similar) as the Index pattern. Kibana displays a list matching the index pattern:



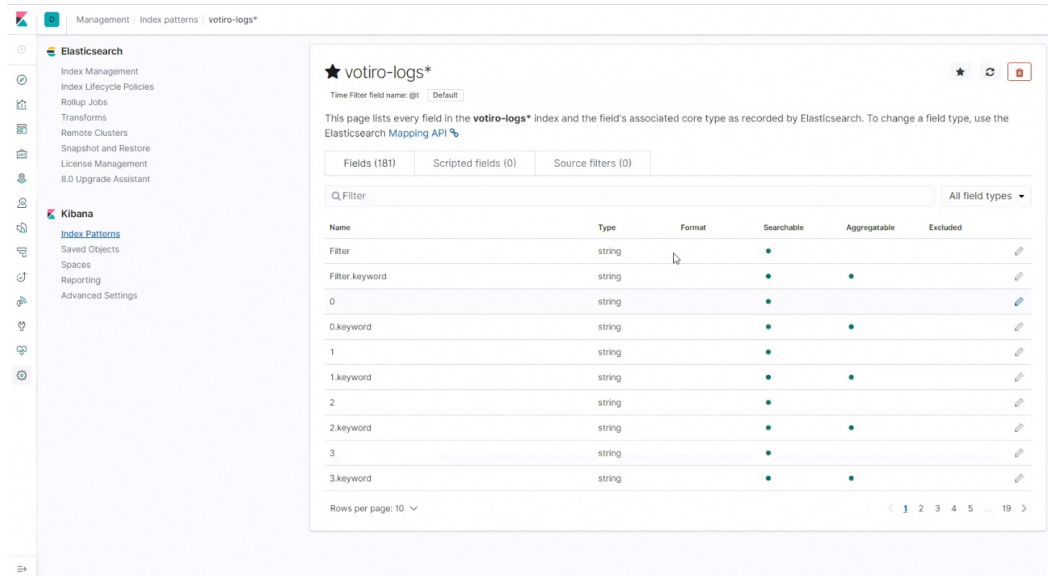
4. Click on **Next step**. Step 2 of 2 **Configure settings** appears.



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



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

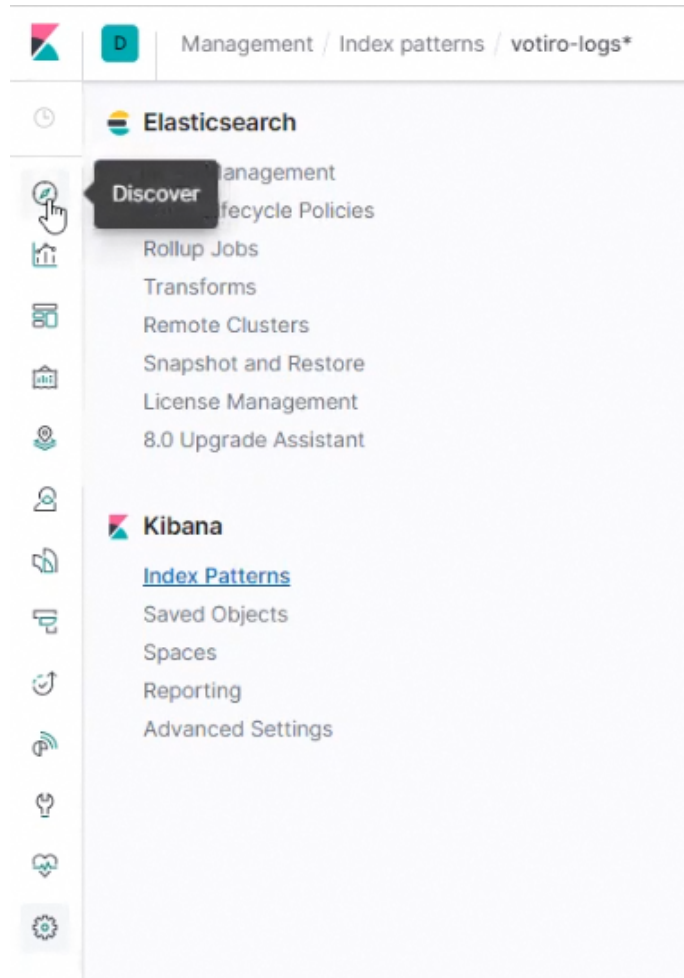


## 22.3 Analyze the Data

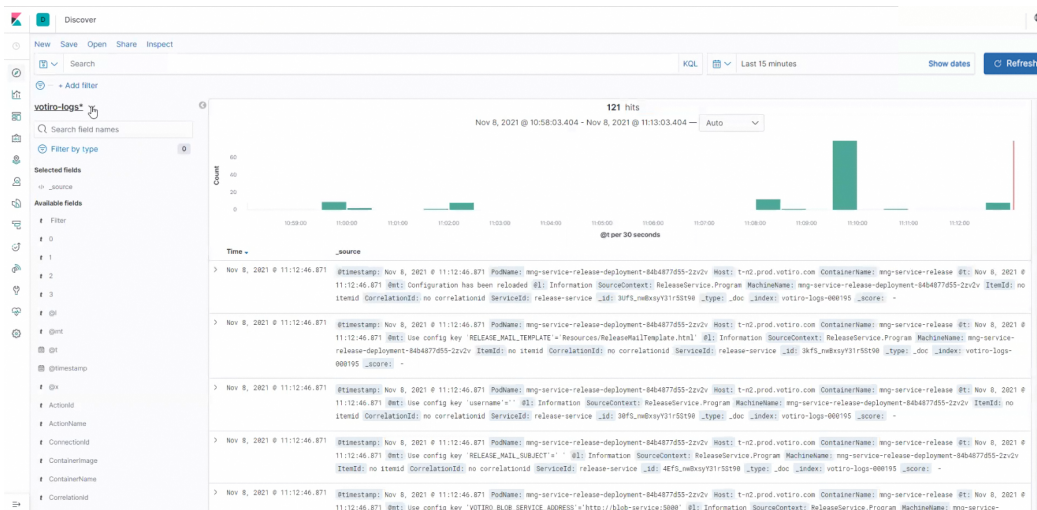
After the index pattern is created and configured, apply it to the data in Kibana's Discover mode to yield useful results by additional filtering of the data.

### 22.3.1 Discover

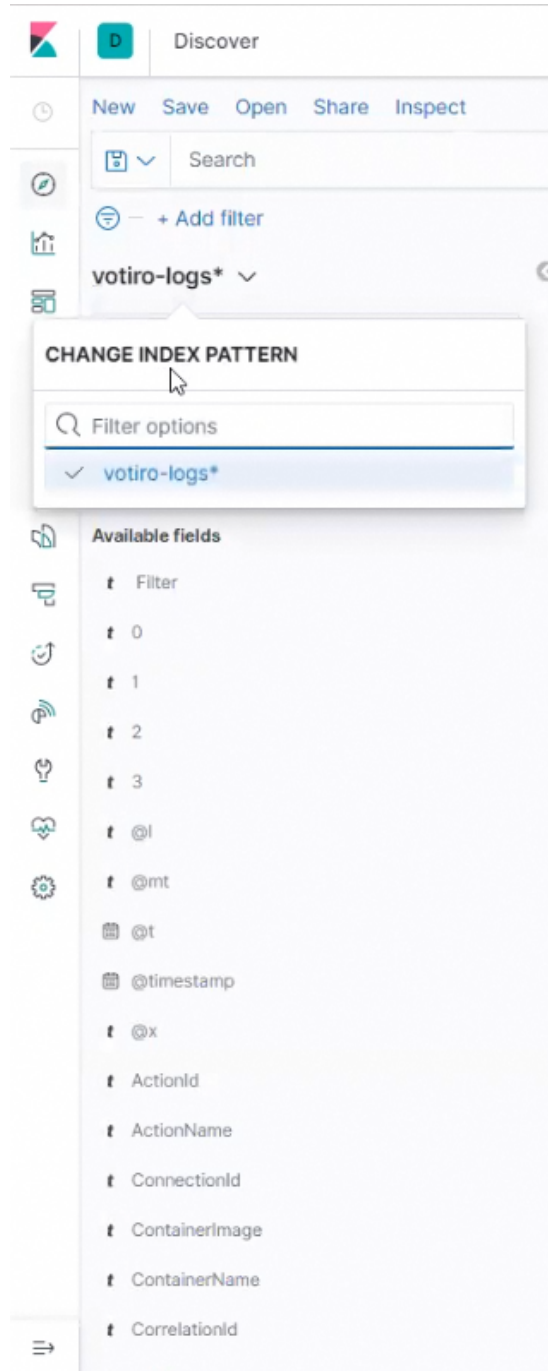
1. Click on the Discover icon on the left side of the screen:



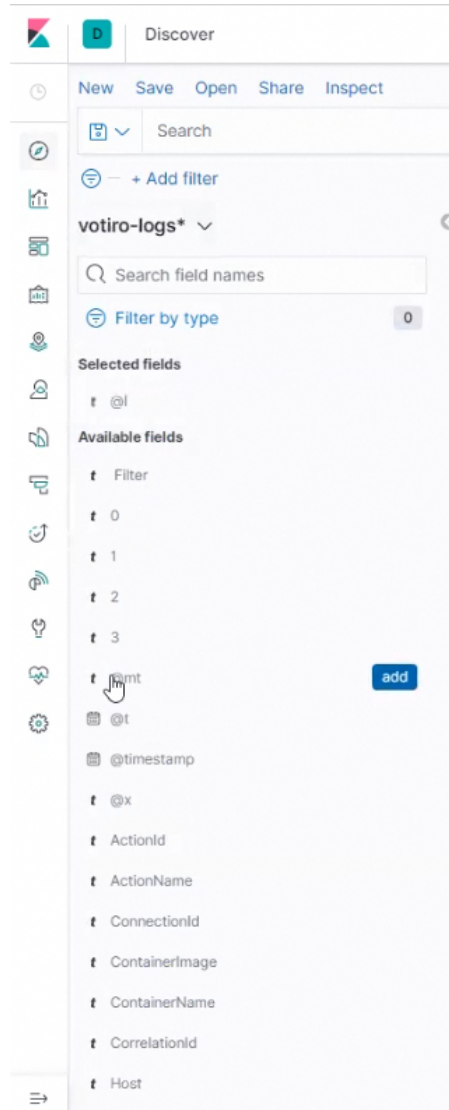
2. Kibana displays all hits that match the time filter criteria within the time range indicated (in this example, for the last 15 minutes):



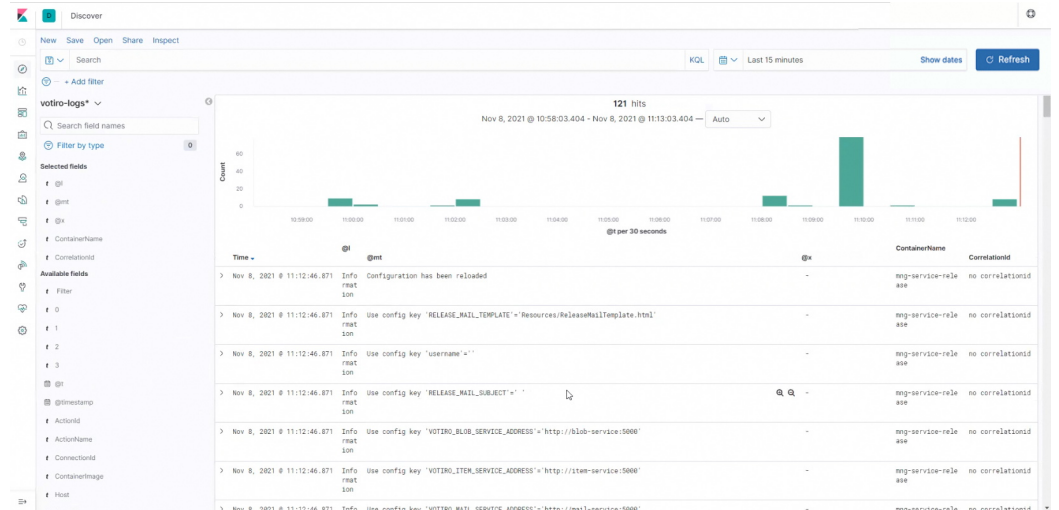
- To further filter the results, click on **v** next to the index pattern (votiro-logs\* by default) in the left side of the screen. The **CHANGE INDEX PATTERN** window opens:



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:



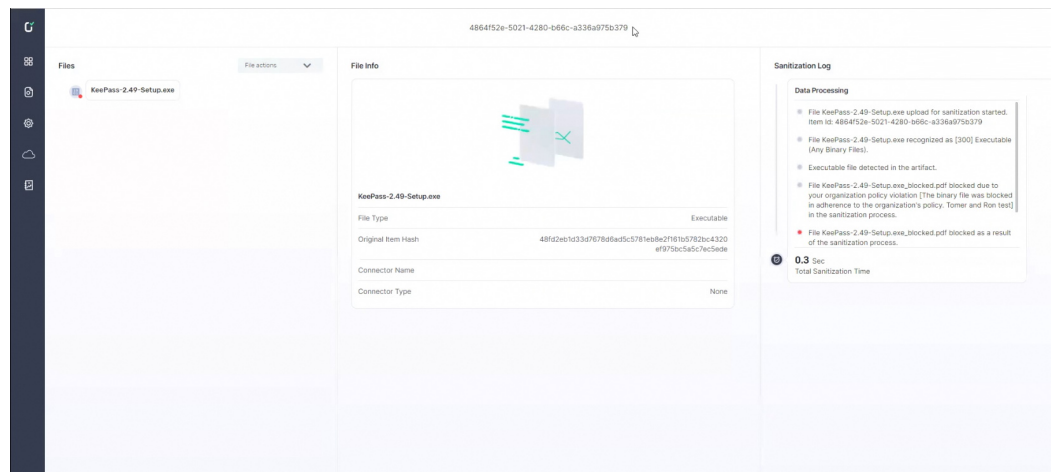
5. In the example below, the following fields are added:
  - ◆ @l - level
  - ◆ @mt - message template
  - ◆ @x - exception
  - ◆ ContainerName
  - ◆ CorrelationId
6. The display of hits is now updated to show only the selected fields:



### 22.3.2 Votiro Explore Incident & File Info

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

1. Open the Votiro Explore Incident:



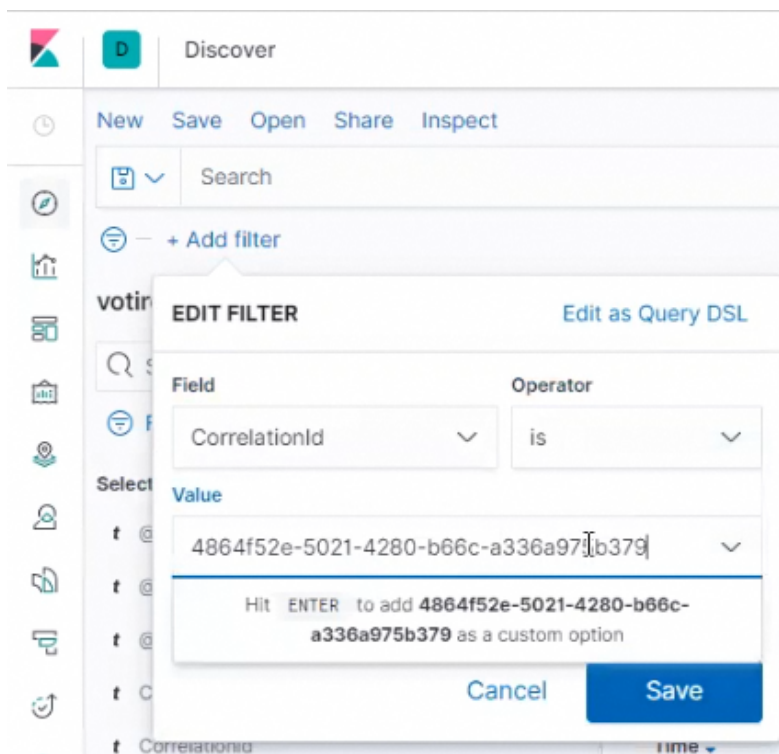
2. Copy to the clipboard the file ID at the top of the screen, in this example:

4864f52e-5021-4280-b66c-a336a975b379

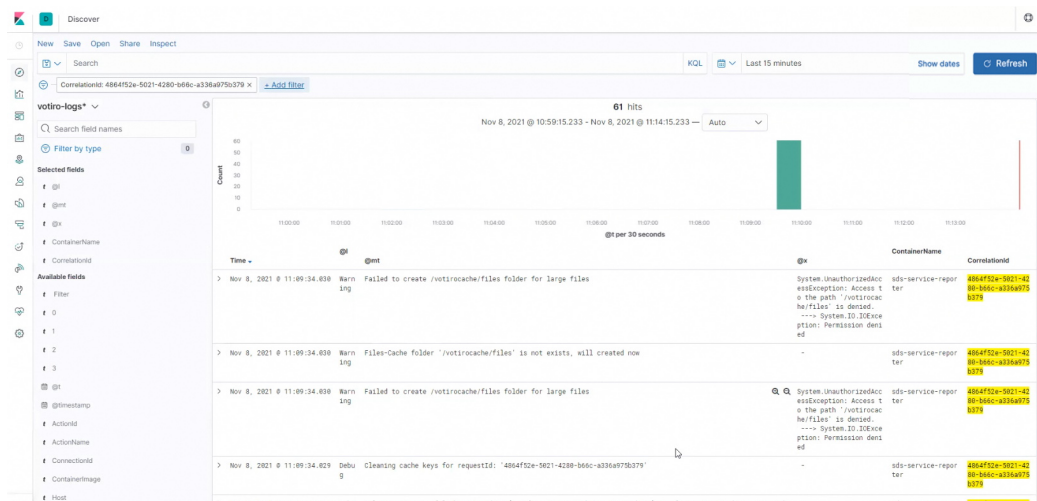
### 22.3.3 File Sanitization Analysis

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**.

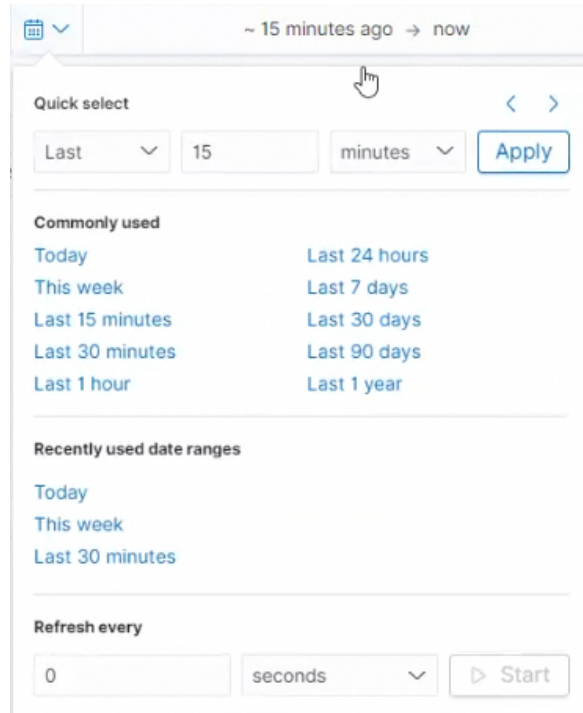
- In the **Value** field, paste the file ID from the clipboard .



- 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).



- To change the time frame of the display, click on the time icon . Then select the desired time interval:



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.

## 23 Message Size Limits in Exchange

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

### 23.1 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.

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

### 23.3 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 On-premcloud solution, contact Votiro Support.

## 24 How to Use QR Code Sanitization

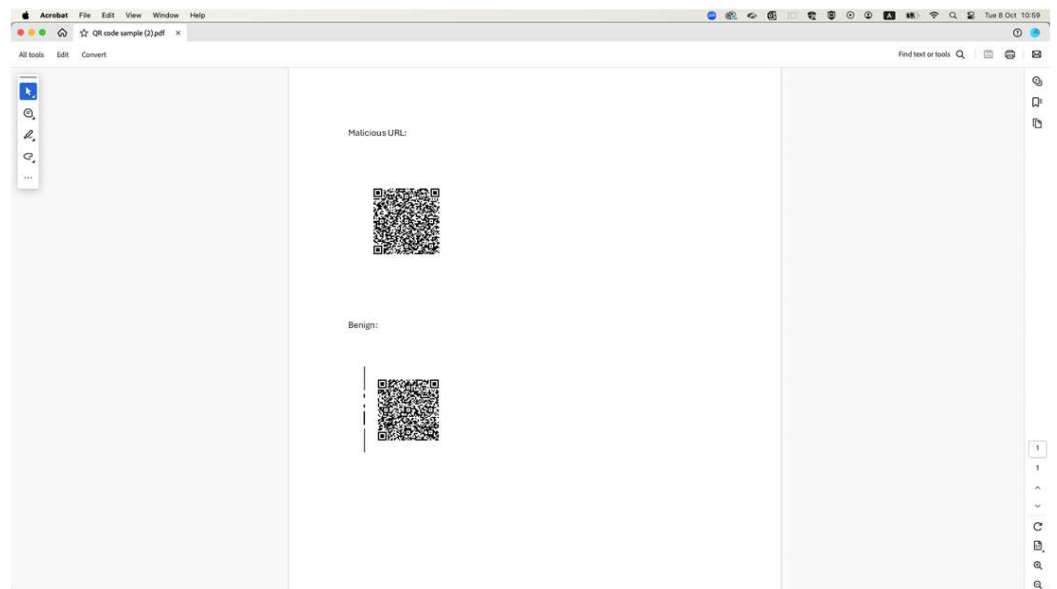
Votiro supports QR Code sanitization. This is relevant for PDFs and emails containing QR codes.

There are four options when dealing with QR codes:

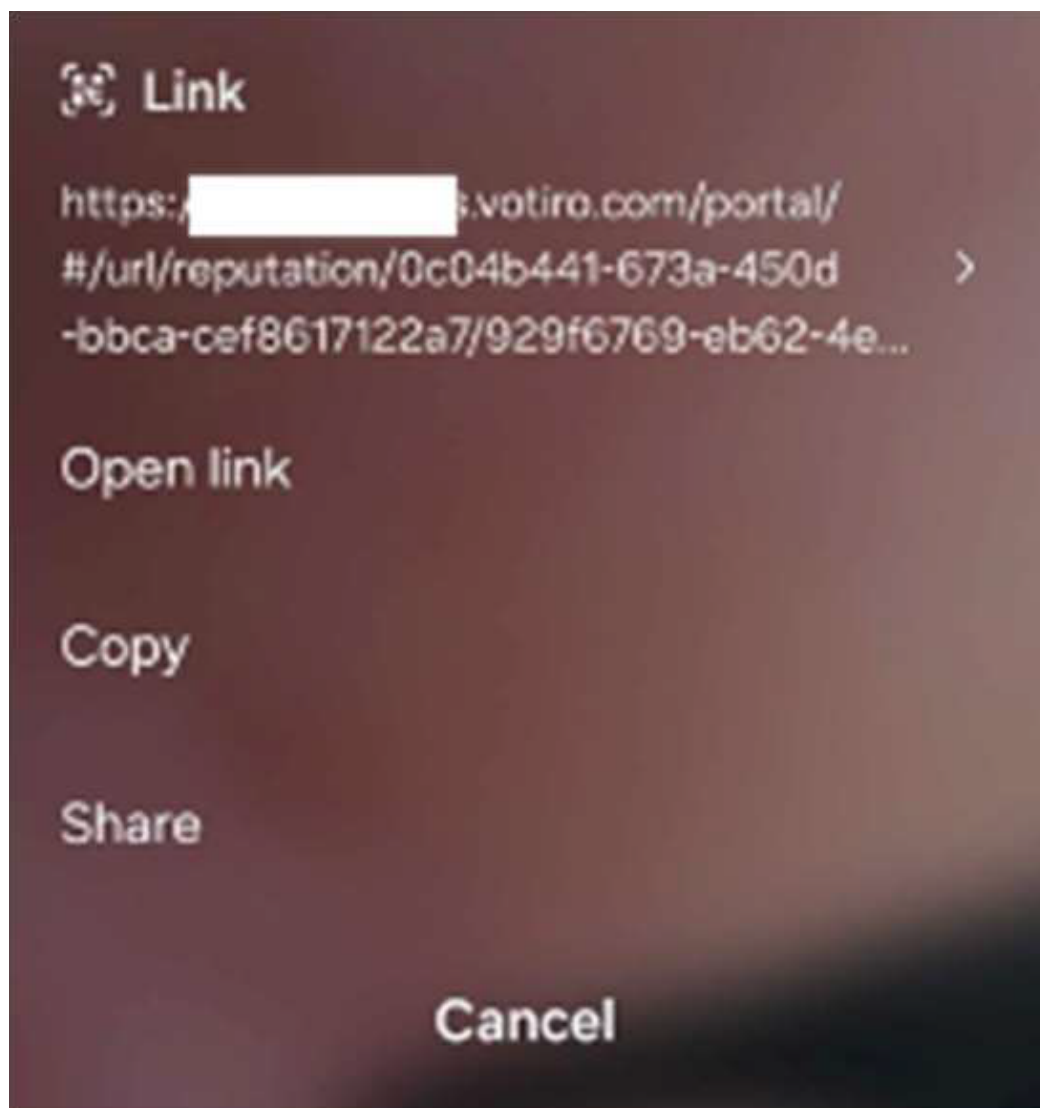
- Ignore - the QR Code is ignored. The file or email is passed on as-is.
- Detect QR Codes - detect if there is a QR Code in the file.
- Disarm QR Codes - the original QR code is rewritten with the Votiro QR Code.
- Block QR Codes - Votiro blocks the QR Code.

### 24.1 Disarm QR Codes behavior

1. The user scans the QR Code.



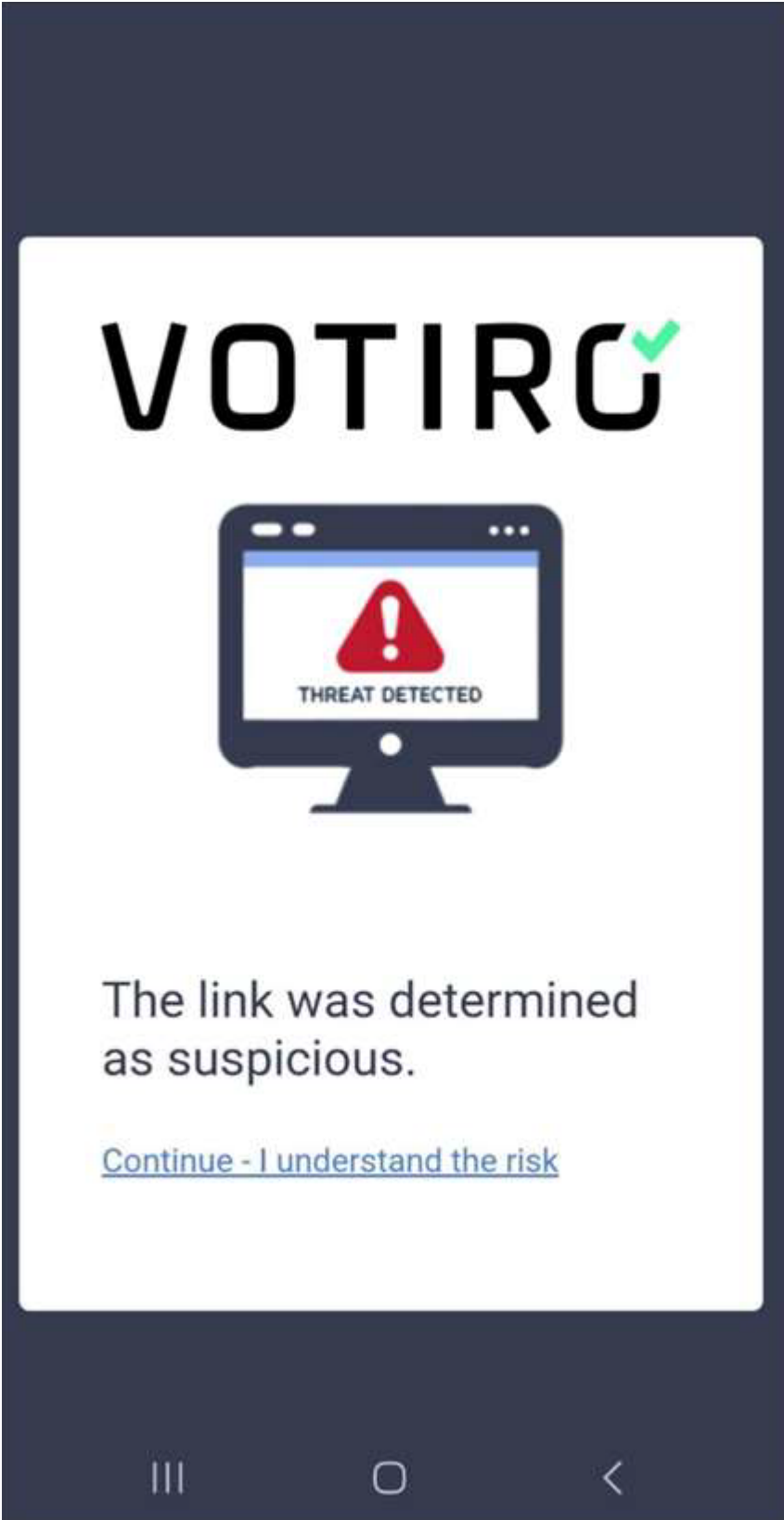
2. There will be an indication that the original QR Code was replaced with a Votiro QR Code pointing to the Votiro portal.



3. The user opens the link and is redirected to the Votiro portal. Votiro analyzes the URL for suspicious activity.



4. When the analysis completes:
  - ◆ If the URL was determined to be benign, the user will be redirected to the URL.
  - ◆ If the URL was determined as suspicious, the user will receive an indication that a threat was detected.





## 25 Unsanitized Due to Timeout

This article describes why files may not be sanitized due to a timeout limit being reached.

### 25.1 Symptoms

In some cases the process of sanitizing a complex email with file attachments may take longer than expected. In such cases the maximum processing time set in the Email-Connector configuration file is reached and the process will timeout.

In such cases, the email recipient receives the original email with the subject field changed by the addition of **\*\*\*Unsanitized\*\*\*** at the beginning of the original subject.

### 25.2 Solution

1. Open the last \ relevant Email-connector log installed on the Edge server - the logs are located by default under: C:\Program Files\Votiro\SDS-Connector\Logs.
2. Open the log with a text editor and search for "Unsanitized".
3. You should find the following:

"Unexpected error. Passing unsanitized email."

Just above this row you will see:

"result is Timeout."

4. Next, open and browse the following XML:

C:\Program Files\Votiro\SDS-Connector\WebApiHandlerConfig.xml.

In the XML you will find 2 timeout values:

- ◆ WebApiTimeoutInMS - The total length of time the SDS-Connector waits for a sanitization to be completed, in milliseconds.

Value Range: 5000 to 180000000 Default value is 90000. This is the value you should change.

- ◆ WebRequestTimeoutInMS - The length of time the SDS-Connector waits per API request from the SDS-WS, in milliseconds.

Value Range: 5000 to 180000000, Default value is 60000.

5. Increase the value of "WebApiTimeoutInMS". Save and Close the XML file.
6. Restart the MExchangeTransport service.

## 26 URL Protection

For file types PDF, Word and Excel the user can define how to handle suspicious URLs.

There are four possible actions:

- **Don't do anything** - the URL is passed as-is.
- **Mask suspicious links** - the URL is masked if it is determined to be suspicious.
- **Sanitize suspicious links** - the URL is redirected to the Votiro portal for analysis.
- **Block document containing suspicious links** - the entire document is blocked if the URL is determined to be suspicious. This is the default action.

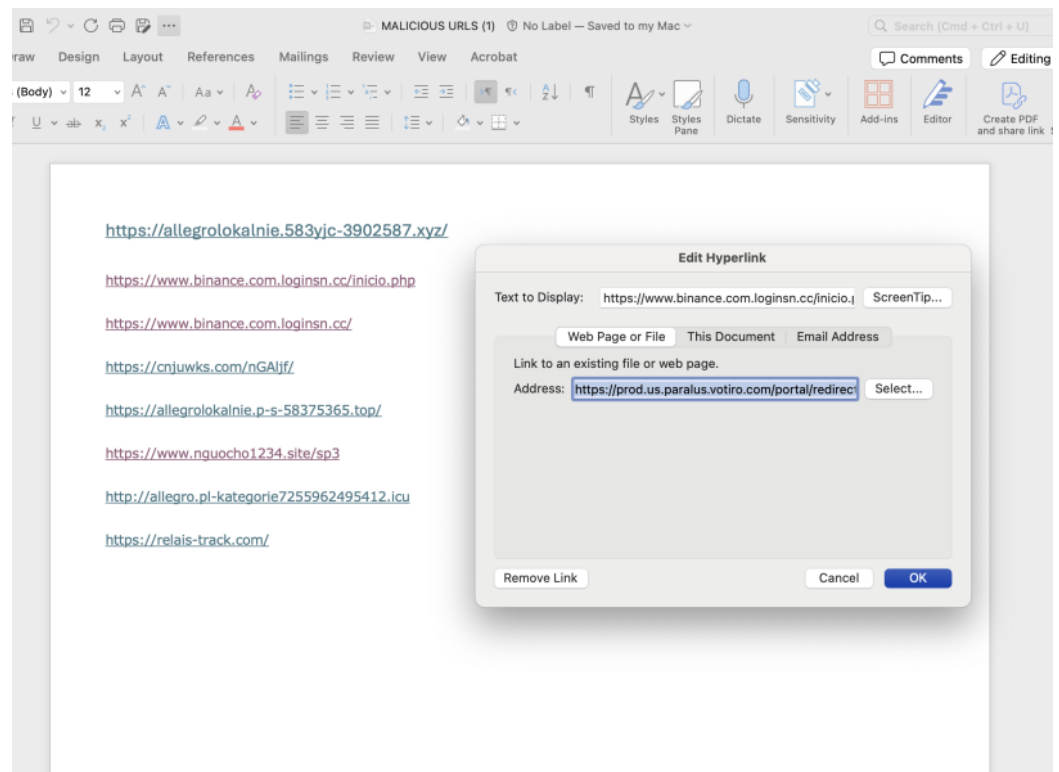
### 26.1 Workflow - Sanitize URLs

1. The user defines URL handling of PDF, Word and Excel files. See [Defining Policies by File Type](#):

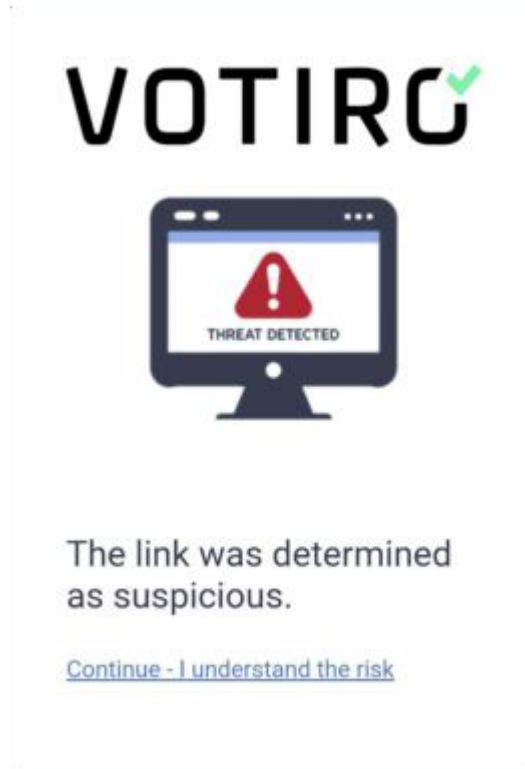
The screenshot displays the configuration interface for Microsoft Office. At the top, there is a header "Microsoft Office" and a button "+ Add Exception". Below this, a "Default Action" section contains three radio buttons: "Block" (red), "Sanitize" (green, selected), and "Allow" (blue). The "Macro handling" section includes a dropdown menu set to "Remove all macros". There are two checkboxes: "Remove metadata" (unchecked) and "Remove printer settings" (checked). The "URL handling" section has a dropdown menu set to "Sanitize suspicious links", which is open to show a list of options: "Don't do anything", "Mask suspicious links", "Sanitize suspicious links" (highlighted in blue), and "Block documents containing suspicious links". Below this, there are two checked checkboxes: "Remove Ex" and "Block Files". The "Block Reason" section is partially visible at the bottom.

2. A protected user receives a file from a URL.

3. When the user clicks on the URL, the user will be redirected to the Votiro portal.



4. If the URL was determined to be benign, the user will be redirected to the desired URL.
5. If the URL was determined to be suspicious, the user will receive a warning that a threat was detected.



6. Votiro administrator view - the file event will indicate that the URL was detected and was rewritten by Votiro.

**MALICIOUS URLs.docx**  
08/06/2025 | 10:27  
Using policy "King"

Processed Files: 12 Sanitized, 0 Blocked

Privacy Risks: 0 Detected

Suspicious Objects: 0 Detected

Sanitization Time: 0.4 sec

**Related Files Hierarchy**

- MALICIOUS URLs.docx
  - [Content\_Type].xml
  - .rels
  - document.xml
  - settings.xml
  - styles.xml
  - webSettings.xml
  - fontTable.xml
  - core.xml
  - app.xml
  - document.xml.rels
  - theme1.xml

**Private Information**  
No data found

**Suspicious Objects**  
No data found

**File Details**

- File Name: MALICIOUS URLs.docx
- ID: ecd7188e-55d1-4c9f-b280-251d18f1d82c
- File Type: Word (2007-2010)
- File Size: 12.2 KB
- Original Item Hash: 07f444248f43628e0f5e0f09fa314b0944b051...
- Connector name: Self-sanitization
- Users: -
- Groups: -
- Path: -

**Data Processing**

- URL\_Rewritten: https://alegrolkahne.p-548373365.togr.
- URL\_Rewritten: URLs have been rewritten in file MALICIOUS URLs.docx. URL: https://imgleaks.com/mGAGf/
- URL\_Rewritten: URLs have been rewritten in file MALICIOUS URLs.docx. URL: https://www.binance.com/login/ccr.
- URL\_Rewritten: URLs have been rewritten in file MALICIOUS URLs.docx. URL: https://relab-track.com/v.
- URL\_Rewritten: URLs have been rewritten in file MALICIOUS URLs.docx. URL: https://www.binance.com/login.cc/mcic.php.
- URL\_Rewritten: -

**Related Files by File Type**

Internal: [Bar chart showing 12 items]

Word (2010): [Bar chart showing 1 item]

**Email Information**  
No data found

## 27 Votiro On-prem Monitoring Guidelines

This article describes services installed as part of the Votiro On-prem product for you to monitor.

Also included are additional health indicators for your consideration.

### 27.1 Solution

To check that these services are all active and running:

1. Navigate to the Windows Services Screen: Windows > Administrative Tools > Services.
2. Locate the Votiro On-prem Windows Services for SFG Engine and the Votiro Management Platform Windows Services for Votiro On-prem Management.

Name	Description	Status	Startup Type	Log On As
Virtual Disk	Provides m...		Manual	Local System
VMware Alias Manager and ...	Alias Mana...	Running	Automatic	Local System
VMware Snapshot Provider	VMware Sn...	Running	Manual	Local System
VMware Tools	Provides su...	Running	Automatic	Local System
Volume Shadow Copy	Manages an...		Manual	Local System
<b>Votiro Scanner</b>	<b>Votiro File S...</b>	<b>Running</b>	<b>Automatic</b>	<b>Local System</b>
Votiro.Audit	Logger and ...	Running	Automatic	Local System
Votiro.Blobs	Manage Tot...	Running	Automatic	Local System
Votiro.Monitor	Monitoring ...	Running	Automatic	Local System
Votiro.NotificationCenter	Manage an...	Running	Automatic	Local System
Votiro.RetroScan	Retro-scan ...	Running	Automatic	Local System
Votiro.SelfService	Votiro self s...	Running	Automatic	Local System
W3C Logging Service	Provides W...		Manual	Local System
WalletService	Hosts objec...		Manual	Local System
Web Management Service	The Web M...		Manual	Local Service
Windows Audio	Manages au...		Manual	Local Service

3. For each of these services, ensure that the following details are displayed:
  - ◆ Status is Running
  - ◆ Startup Type is Automatic.

**Note**  
It can take up to 30 minutes for the information to appear in the API log.

## 27.2 Votiro On-prem Services - Votiro Services

Service	Description
Votiro Scanner	The Votiro Scanner service is located at: [installation_path]\Votiro\Votiro.Malware.Scanner.  The Votiro Scanner service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\Votiro.Malware.Scanner\Logs.
Votiro.Sanitization.API	The Votiro.Sanitization.API service is located at: [installation_path]\Votiro\SDS Web Service. The Votiro.Sanitization.API service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\SDS Web Service\Logs\API.
Votiro.SNMC	The Votiro.SNMC service is located at: [installation_path]\Votiro\SDS Web Service. The Votiro.SNMC service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\SDS Web Service\Logs\SNMC. The SNMC manages n sanitization nodes. Nodes have log files that are located at: [installation_path]\Votiro\Logs\SNMC\1 ... n
Votiro.Sandbox	The Votiro.Sandbox service is located at: [installation_path]\Votiro\Sandbox. The Votiro.Sandbox service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\Sandbox\Logs.

### 27.2.1 Additional Health Indicators:

- C:\ Drive space
- CPU load
- Memory Usage
- Uptime
- IIS Admin Service

## 27.3 Votiro On-prem Management Dashboard - Votiro Services

Service	Description
Votiro.Blobs	The Votiro.Blobs service is located at: [installation_path]\Votiro\BlobStorage. The Votiro.Blobs service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\BlobStorage\Logs.

Service	Description
Votiro.NotificationCenter	The Votiro.NotificationCenter service is located at: [installation_path]\Votiro\NotificationCenter. The Votiro.NotificationCenter service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\NotificationCenter\Logs.
Votiro.RetroScan	The Votiro.RetroScan service is located at: [installation_path]\Votiro\RetroScan. The Votiro.RetroScan service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\RetroScan\Logs.
Votiro Scanner	The Votiro Scanner service is located at: [installation_path]\Votiro\Votiro.Malware.Scanner. The Votiro Scanner service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\Votiro.Malware.Scanner\Logs.
Votiro.Audit	The Votiro.Audit service is located at: [installation_path]\Votiro\Audit. The Votiro.Audit service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\Audit\Logs.
Votiro.Monitor	The Votiro.Monitor service is located at: [installation_path]\Votiro\Monitor. The Votiro.Monitor service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\Monitor\Logs.
Votiro.SelfService	The Votiro.SelfService is located at: [installation_path]\Votiro\PpfSelfService. The Votiro.SelfService service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\PpfSelfService\Logs.
Votiro.Scheduler	The Votiro.Scheduler is located at: [installation_path]\Votiro\Scheduler. The Votiro.Scheduler service maintains a log file for all activity. The log file is located at: [installation_path]\Votiro\Votiro\Scheduler\Logs.
Elasticsearch	The Elasticsearch service is located at: C:\Program Files\Elastic\ElasticSearch. The Elasticsearch service maintains a log file for all activity. The log file is located at: C:\ProgramData\Elastic\Elasticsearch\logs.

### 27.3.1 Additional Health Indicators:

- C:\ Drive space
- CPU load
- Memory Usage
- Uptime
- IIS Admin Service