VOTIRO

Votiro Cloud

Knowledge Base

July 2024

Copyright Notice

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

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

www.votiro.com

Contents

1 Assigning a Control Plane VIP and Default VIP in AWS VA 7

1.1 Procedure 7

2 Assigning a Control Plane VIP and External LB in Azure VA 11

2.1 Procedure 11

3 Changing the CA Certificate 15

3.1 Converting a CA Certificate 15

3.2 Applying CA Certificate to Kubernetes Cluster 15

4 Email Arrival is Delayed 16

4.1 Symptoms 16

4.2 Solution 16

4.3 Expected result 16

4.3.1 Before: 16

4.3.2 Action: 16

4.3.3 After: 16

5 How to Check that the External Load Balancer is Working with the Votiro Cloud Cluster 18

5.1 Prerequisites 18

5.2 Procedure 18

5.2.1 Verify the Load Balancer is Connected to the Cluster 18

6 How to Configure SSL Passthrough Load Balancing using NGINX 20

6.1 Prerequisites 20

6.2 Procedure 20

6.3 Next Steps 23

6.4 NGINX File Example 23

7 How to Configure the Votiro Appliance for AWS 25

7.1 Prerequisites 25

7.2 Procedure 26

8 How to Configure the Votiro Cloud Cluster with External Storage 30

8.1 Prerequisites 30

8.2 Procedure 30

8.2.1 Declare a Mount 30
8.2.2 Add External Storage Path 31
8.2.3 Restart Pods 31
8.3 Troubleshooting 31
8.3.1 Issue 1: Windows Server NFS sharing permission 31
8.3.2 Issue 2: Missing metadata in blob-config 35
9 How to Deploy the Votiro Cloud Cluster in Azure 36
9.1 Prerequisites 36
9.2 Procedure 36
10 How to Integrate Azure AD Single Sign-on with Votiro using SAML Toolkit 43
10.1 Prerequisites 43
10.2 Procedure 43
11 How to Integrate SIEM with Azure Sentinel 51
11.1 System prerequisites 51
11.2 Procedure 51
11.2.1 Manual/Offline Deployment 51
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs 63
12.1 Procedure 63
12.1.1 Configure an HTTP Logs and Metrics Source in Sumo Logic 63
12.1.2 Create the Field Extraction Rules at Ingest Time 65
12.1.3 Install the Votiro App 67
12.1.4 Integrate the Votiro Management Console with the Sumo Logic HTTP Logs Collector 69
12.1.5 Verify the Integration 70
13 How to Integrate Votiro Cloud with Google Workspace 73
13.1 Procedure 73
13.1.1 Create a Host 74
13.1.2 Configure content compliance rule for emails received from Votiro Cloud 75
13.1.3 Configure Content compliance rule for emails sent to Votiro Cloud 79
14 How to Integrate Votiro Cloud with Sumo Logic 81
14.1 System Requirements 81

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

20.3.1 Discover 119
20.3.2 Votiro Explore Incident & File Info 123
20.3.3 File Sanitization Analysis 123
21 Message Size Limits in Exchange 126
21.1 Symptoms 126
21.2 Solution 126
21.3 Limitations 126
22 MSSP User Guide 127
22.1 MSSP Tenant Management 127
22.2 Monitoring Tenant Activity 133

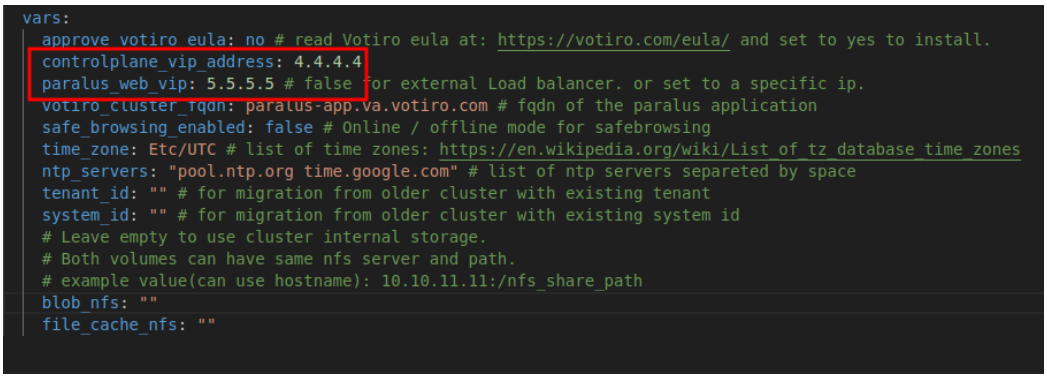
1 Assigning a Control Plane VIP and Default VIP in AWS VA

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

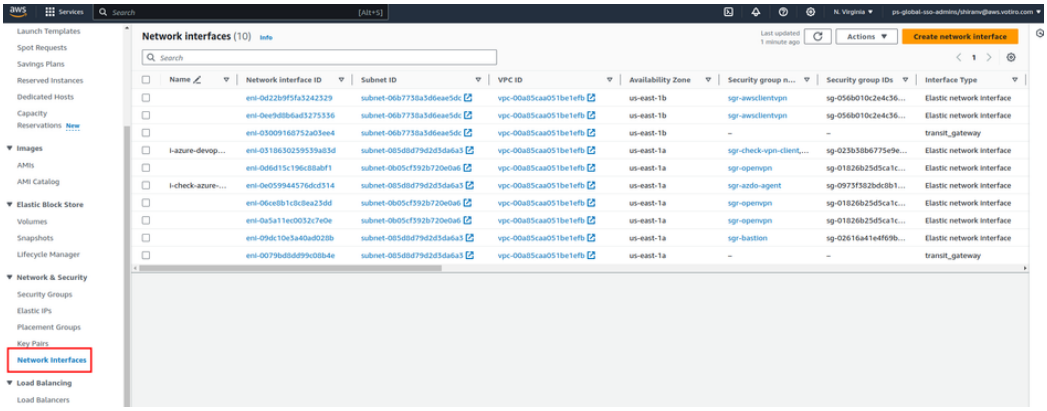
> **Note**: If the customer is using an external load balancer, then only one IP should be added for Control plane vip and not paralus_web_vip.

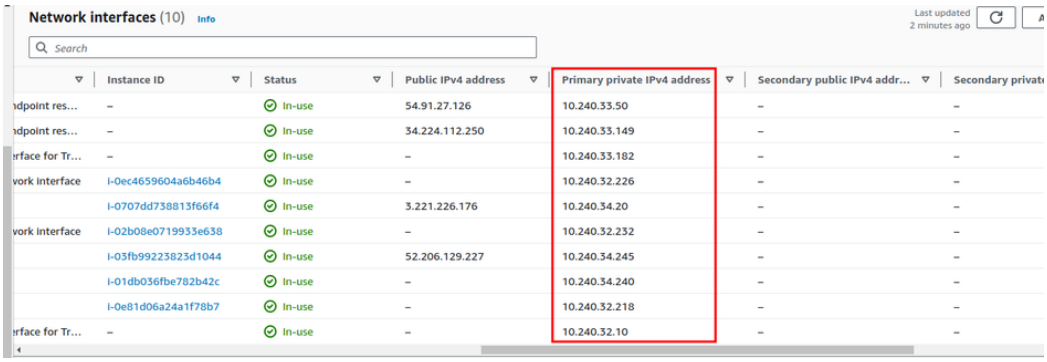
1.1 Procedure

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

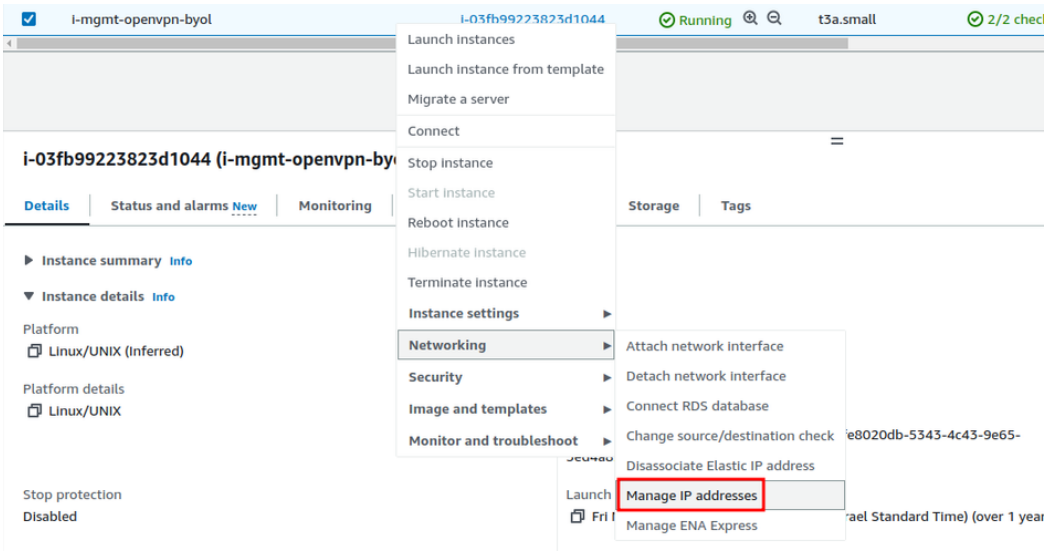


3. Add two available IPs. You can verify the availability of the IPs by checking in the AWS EC2 console. Navigate to **Network & Security** > **Network Interfaces**:

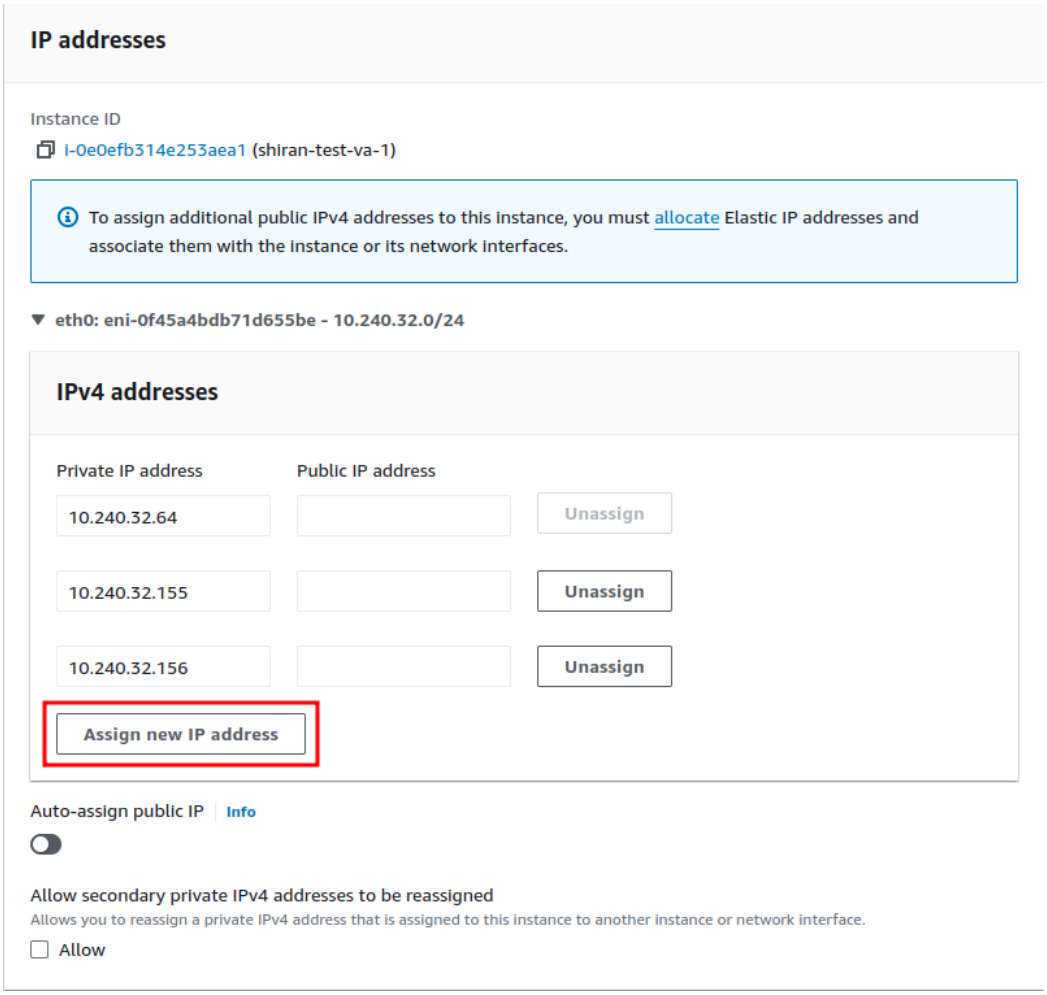




4. Assign the two IPs to the first node as follows: Go back to **Instances** and right click on one of the nodes. In the menu that opens, select **Networking**. In the submenu that opens, select **Manage IP addresses**.



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



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.

```
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

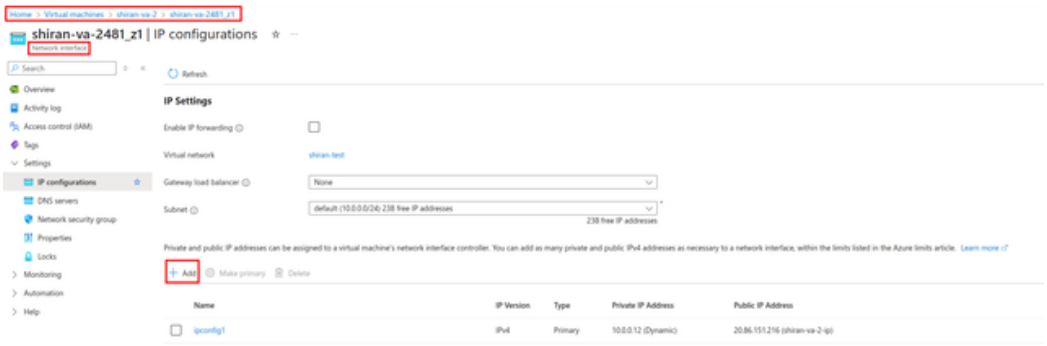
> **Note**
> For Production environment, always use an external Load Balancer.

1. Assign the IP addresses to the **inventory.yaml** file:
   - Assign one IP address for **controlplane_web_vip**.
   - For the **Test** environment, assign a second IP address for **paralus_web_vip**.

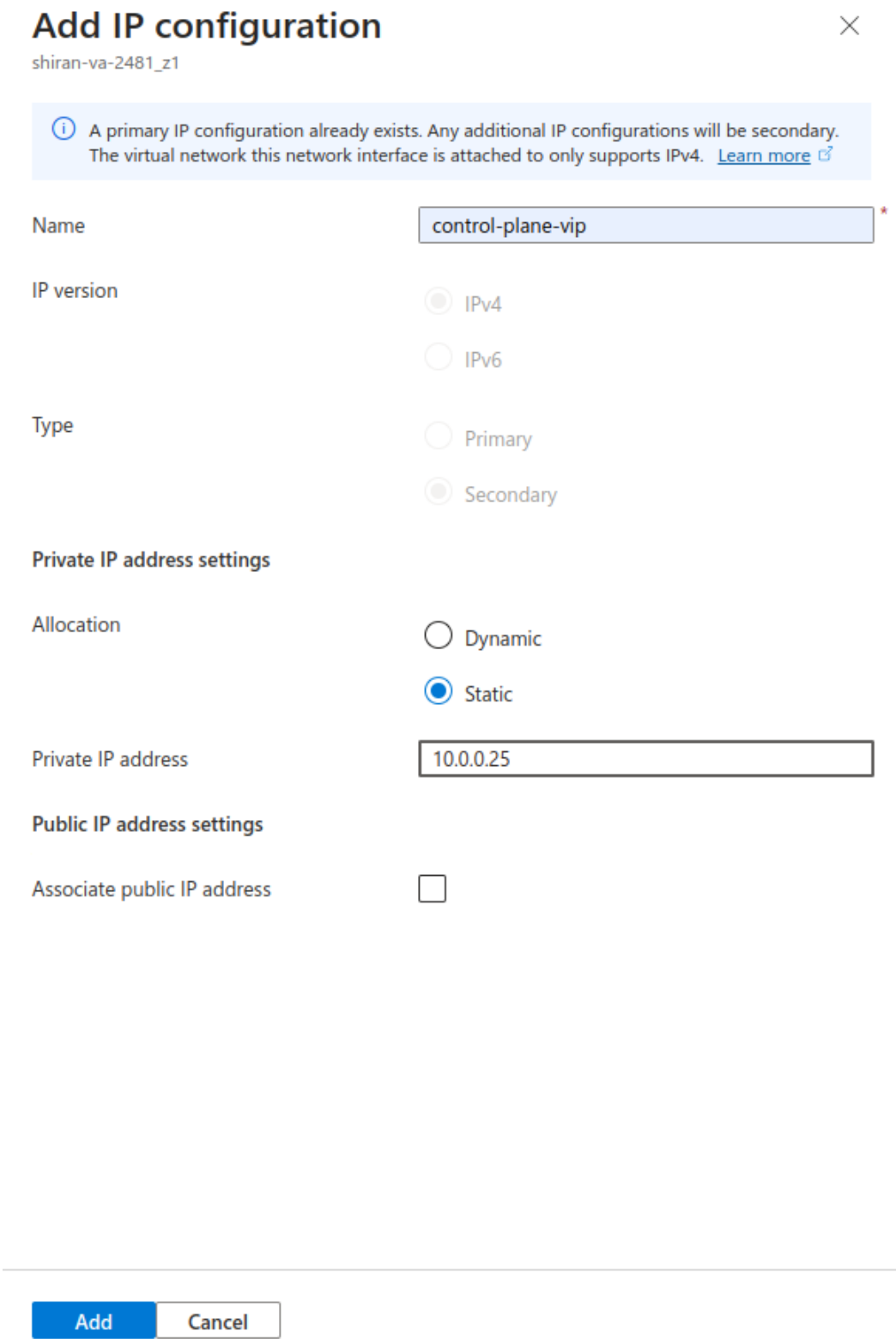
```
15
16  vars:
17    approve_votiro_eula: yes # read Votiro eula at: https://votiro.com/eula/ and set to yes to install.
18    controlplane_vip_address: 10.10.2.77
19    paralus_web_vip: false # false for external Load Balancer. or set to a specific ip.
20    votiro_cluster_fqdn: aws-poc.prod.votiro.com # 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 separeted by space
24    tenant_id: "" # for migration from older cluster with existing tenant
25    system_id: "" # for migration from older cluster with existing system id
26    # Leave empty to use cluster internal storage.
27    # Both volumes can have same nfs server and path.
28    # example value(can use hostname): 10.10.11.11:/nfs_share_path
29    blob_nfs: ""
30    file_cache_nfs: ""
```

New IP Assign

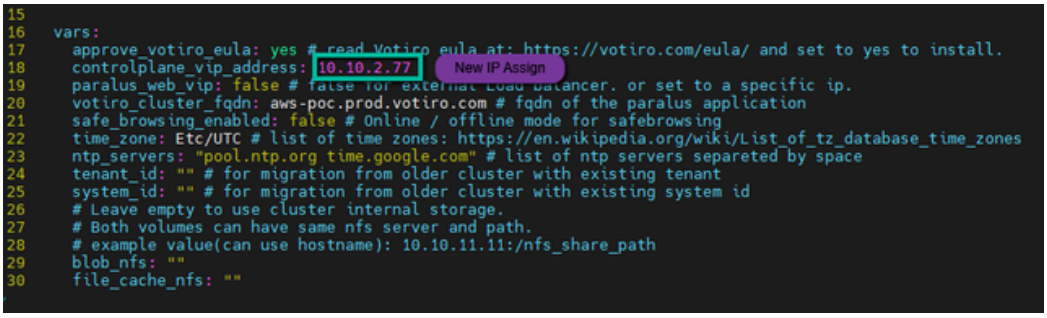
2. In the **IP configurations** for the VM, click + **Add**.



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



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



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:
```

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

The CA Certificate used with your Votiro Votiro Cloud appliance must be a *.pem* and *.key* pair. You can convert the format of your CA Certificate using SSL Certificate software, for example 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 traefik`
- `kubectl create secret tls traefik-cert --key=/<path-to-certificate>/certificate.key --cert=/<path-to-certificate>/certificate.pem -n traefik`
- `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 Email Arrival is Delayed

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

4.1 Symptoms

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

4.2 Solution

This situation might be related to Message throttling.

Get information of the Edge Connector:

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

4.3 Expected result

4.3.1 Before:

Name : Default Connector Name

ConnectionTimeout : 00:05:00

ConnectionInactivityTimeout : 00:01:00

MaxInboundConnection : 5000

MaxInboundConnectionPerSource : 20

MaxInboundConnectionPercentagePerSource : 2

MessageRateLimit : 600

MessageRateSource : IPAddress

TarpitInterval : 00:00:05

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

4.3.2 Action:

Change the parameters using syntax:

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

4.3.3 After:

Name: Default Connector Name

ConnectionTimeout: 00:10:00

ConnectionInactivityTimeout: 00:01:00

MaxInboundConnection: 5000

MaxInboundConnectionPerSource: 50

MaxInboundConnectionPercentagePerSource: 5

MessageRateLimit: 600

MessageRateSource: IPAddress

TarpitInterval: 00:00:05

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

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

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

5.1 Prerequisites

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

5.2 Procedure

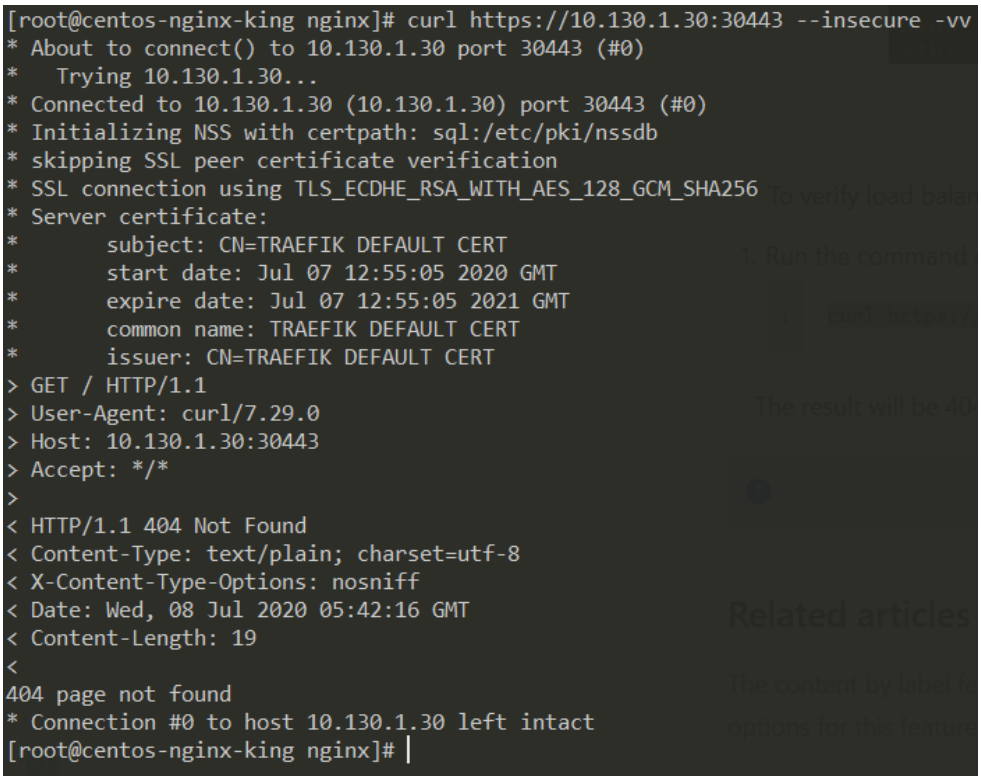
This procedure includes instructions and verification checks to ensure that the NGINX load balancer is providing the load balancing service to Votiro Cloud, instead of using the application's internal load balancing function.

5.2.1 Verify the Load Balancer is Connected to the Cluster

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

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

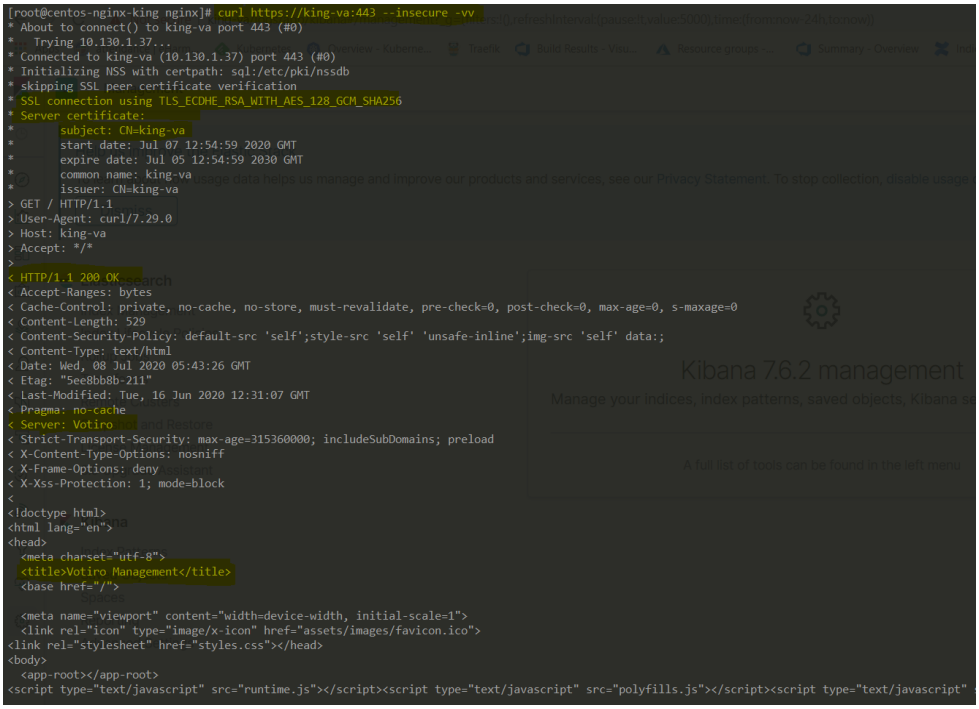
The result will contain the message **404 page not found**:



3. Run the command with the cluster name:

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

The result will appear as follows:



6 How to Configure SSL Passthrough Load Balancing using NGINX

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

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

6.1 Prerequisites

Before you start, ensure the following:

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

> **IMPORTANT!**
> The IP address set must be static.

6.2 Procedure

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

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

   ```
   sudo yum install epel-release
   ```

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
   ```

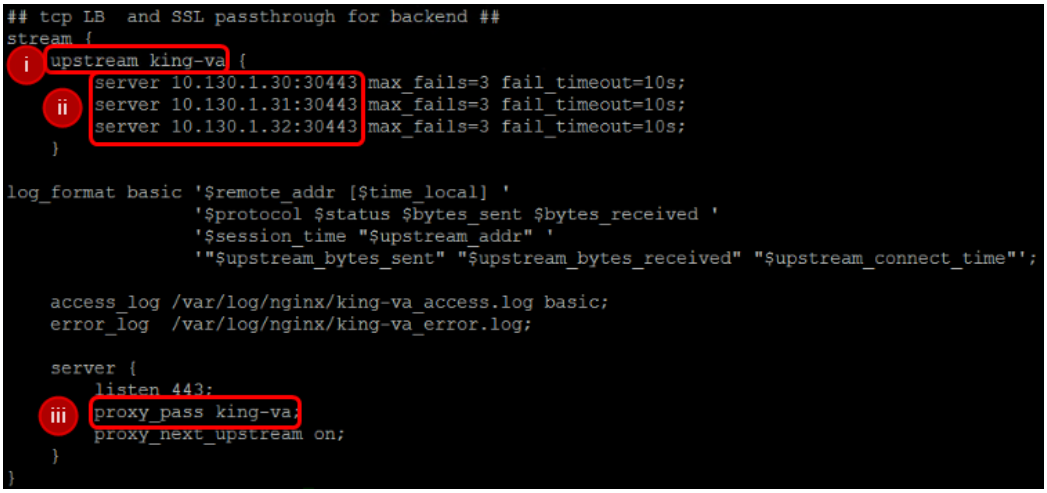
   c. Paste the following code and edit details relevant to your environment:

      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" "$upstream_bytes_received"
   "$upstream_connect_time"';
13
14     access_log /var/log/nginx/votirosfgva_access.log basic;
15     error_log  /var/log/nginx/votirosfgva_error.log;
16
17     server {
18         listen 443;
19         proxy_pass votirosfgva;
20         proxy_next_upstream on;
21     }
22 }
```



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

    ```
    nginx -t
    ```

    You should see the following output:

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

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

11. Reload NGINX configurations, using the following command:

    ```
    systemctl reload nginx
    ```

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

    ```
    vi /etc/hosts
    ```

    Add the cluster FQDN and NGINX server IP:

    ```
    10.130.1.34 <cluster name>
    ```

13. To pass the traffic to the nodes over 30443, follow these steps:

    a. Download and install audit2allow:

    ```
    sudo yum install setroubleshoot
    ```

    b. Enable it:

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

    c. Execute the policy

    ```
    semodule -i mynginx.pp
    ```

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

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

6.3 Next Steps

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

6.4 NGINX File Example

The following code is an example of an NGINX File.

```
# For more information on configuration, see:
#   * Official English Documentation: http://nginx.org/en/docs/
#   * Official Russian Documentation: http://nginx.org/ru/docs/

user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;

# Load dynamic modules. See /usr/share/doc/nginx/README.dynamic.
include /usr/share/nginx/modules/*.conf;

events {
    worker_connections 1024;
}

http {
    log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile            on;
    tcp_nopush          on;
    tcp_nodelay         on;
    keepalive_timeout   65;
    types_hash_max_size 2048;

    include             /etc/nginx/mime.types;
    default_type        application/octet-stream;

    # Load modular configuration files from the /etc/nginx/conf.d directory.
    # See http://nginx.org/en/docs/ngx_core_module.html#include
    # for more information.
    include /etc/nginx/conf.d/*.conf;

    server {
        listen       80 default_server;
        #listen       [::]:80 default_server;
        server_name  _;
        root         /usr/share/nginx/html;

        # Load configuration files for the default server block.
        include /etc/nginx/default.d/*.conf;
```

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

7 How to Configure the Votiro Appliance for AWS

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

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

7.1 Prerequisites

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

  For these specs, an m5.2xlarge EC2 instance will be used.
- (Optional) EFS (Amazon Elastic File System) share that will be used for file archiving. This is not required for the initial install.
- A shared AMI (Amazon Machine Image)
- AWS load balancer - a load balancer is required. The following is an example of a possible load balancer configuration. For more information on configuring an AWS load balancer, see Create a Network Load Balancer:

  a. Configure the target group with basic configuration:
     - Target type - Instances
     - Protocol - TLS
     - Port - 30443
     - Protocol version - HTTP/1.1

  b. Configure health checks:
     - Protocol - TCP

  c. Register targets:
     - Ports for the selected instances - 30443

  d. Configure the load balancer: Create Network Load Balancer
     - Basic configuration
     - Scheme - Internal
     - Listeners and routing:

- Protocol - TLS
- Port - 443

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

7.2 Procedure

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

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

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.

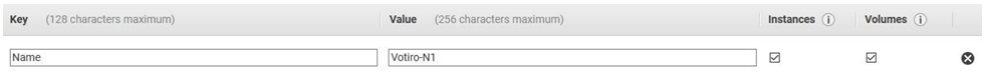
  vii. Save changes.

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

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

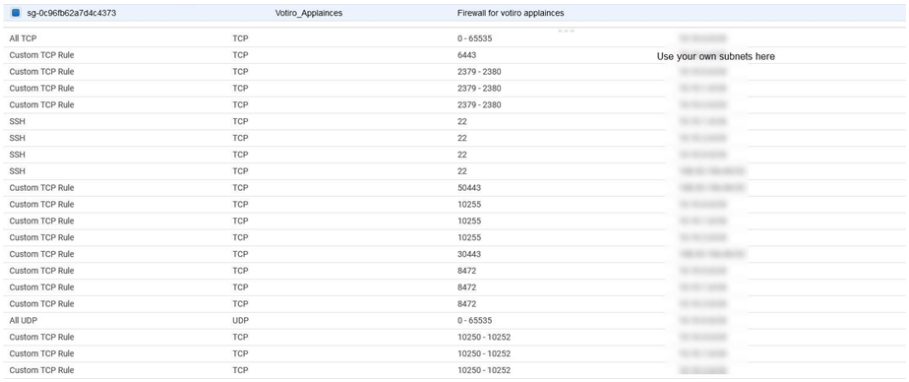
13. On the Add Storage page, leave storage as is. Select **Delete on Termination**.

14. On the Add Tags page, add a Name value tag and name it according to your server naming convention.

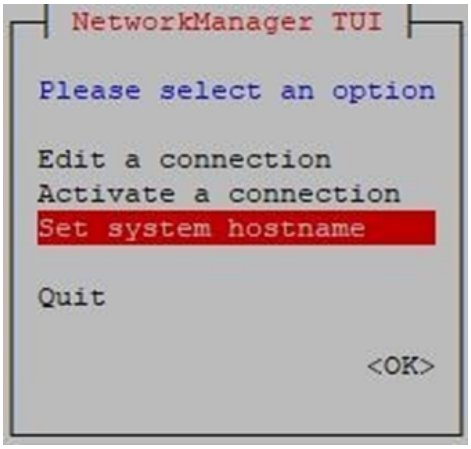


15. On the Configure Security Group page, define a specific Votiro Security group. Make sure you can ssh into any of the nodes. This will be required to complete the setup. The AWS Votiro Security Group should have the following access:

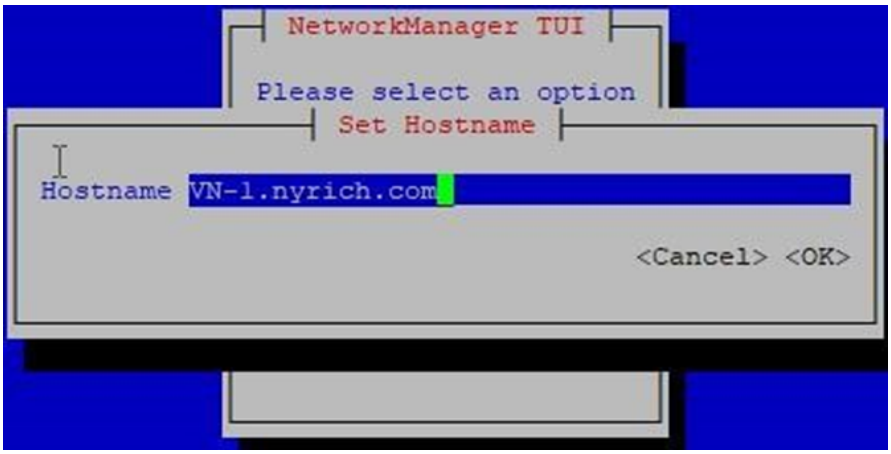
    - Port 443 TCP to and from the VIP of the appliance on 30443. This port is used for web access to Votiro.
    - Each Appliance should be able to communicate on the following ports that are required inside the VLAN between each appliance:
        - 6443/tcp
        - 2379-2380/tcp
        - 10250-10252/tcp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



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**.

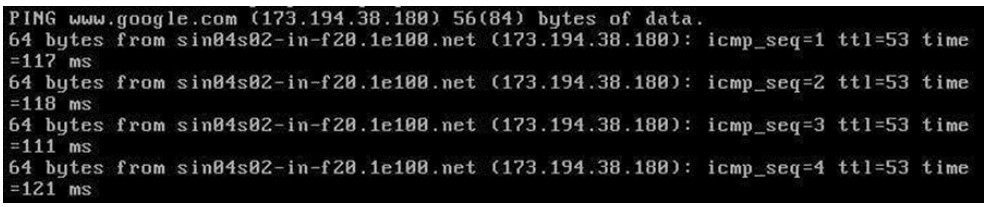


21. Use the FQDN tied to the internal IP in the earlier step. Each node should have its own DNS entry. For example, vn-1.yourdomain.com, vn-2.yourdomain.com, and vn-3.yourdomain.com. These DNS names should be registered in your internal DNS.

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:



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

8 How to Configure the Votiro Cloud Cluster with External Storage

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

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

8.1 Prerequisites

Before you start, ensure that any external storage server:

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

8.2 Procedure

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

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

8.2.1 Declare a Mount

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

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

   ```
   mkdir -p /data/externalfs/nfsshare
   ```

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

   ```
   chown 1000:1000 /data/externalfs/nfsshare
   ```

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

   ```
   chmod -R 755 /data/externalfs/nfsshare
   ```

4. In this step you will add a mount to the folder **/data/externalfs/nfsshare**.

   a. Create mount, using the following command:

   ```
   mount -t nfs SERVER_IP:NFS_EXPORT_FOLDER
   /data/externalfs/nfsshare
   ```

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

```
SERVER_IP:NFS_EXPORT_FOLDER /data/externalfs/nfsshare nfs
defaults 0 0
```

Replace the place holders above as follows:

- **SERVER_IP** with the IP address, for example 10.130.1.97.
- **NFS_EXPORT_FOLDER** with the path to the external server.

For example:

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

8.2.2 Add External Storage Path

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

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

8.2.3 Restart Pods

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

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

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

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

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

8.3 Troubleshooting

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

8.3.1 Issue 1: Windows Server NFS sharing permission

Symptoms

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

```
[root@sfg ~]# mount -t nfs 10.10.10.50:/nfsshare
/data/externalfs/nfsshare

[root@sfg ~]# ls -l /data/externalfs

total 1

drwxr-xr-x. 2 nobody nobody 64 May 12 10:47 nfsshare
```

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

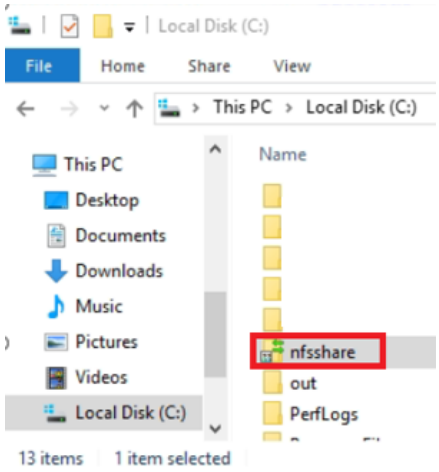
```
[root@sfg ~]# chown 1000:1000 -R /data/externalfs

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

Solution

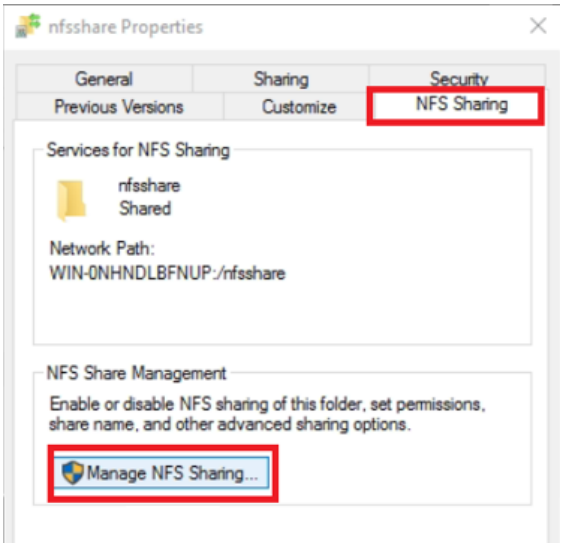
If you are using Windows Server as NFS, please follow this link to configure your Windows Server as a NFS server: Deploy Network File System

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

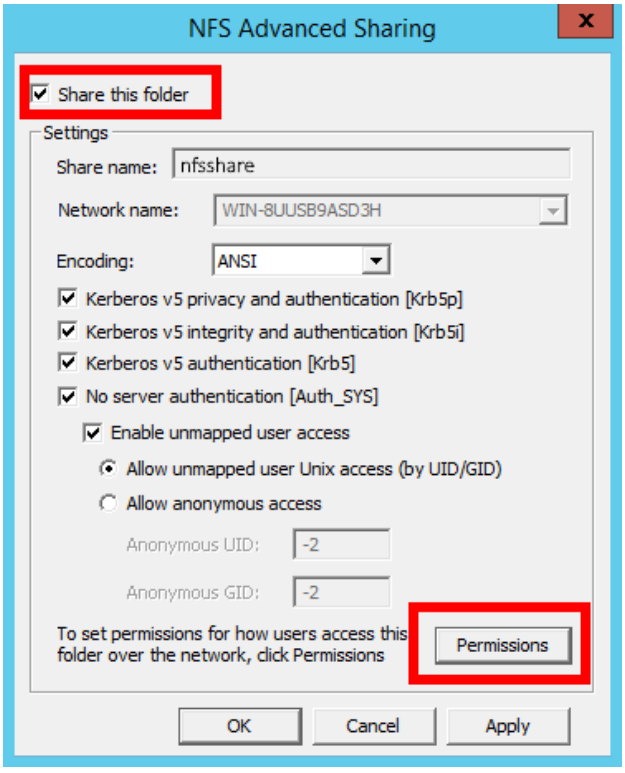
1. Right click on the **nfsshare** folder on your Windows Server and select **Properties**:



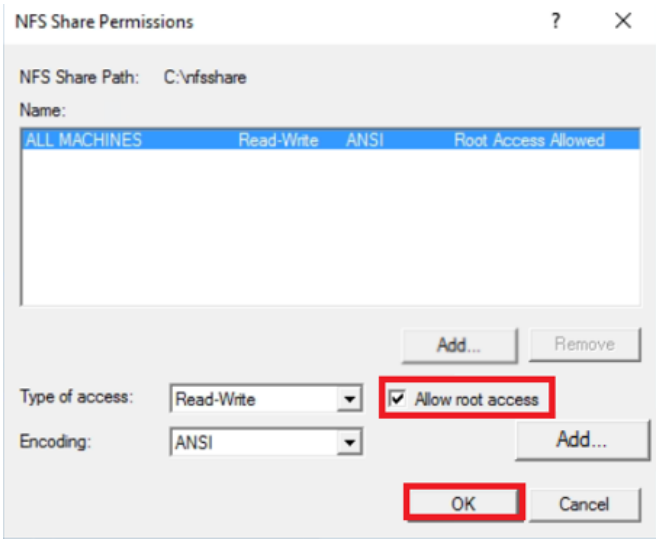
2. Select the **NFS Sharing** tab, and then select **Manage NFS Sharing...**:



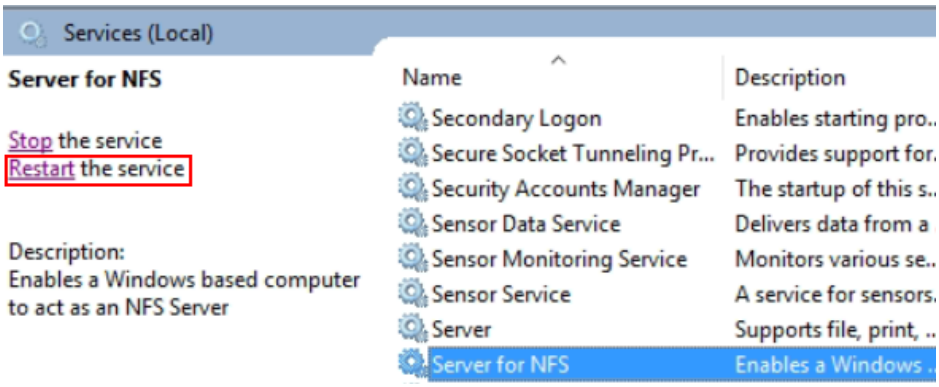
3. In the **NFS Advanced Sharing** window that opens, check the box **Share this folder** and leave the rest of the options as is. Then select **Permissions**.



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



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



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

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

[root@sfg ~]# ls -l /data/externalfs/

total 1

drwxr-xr-x. 3 sgvotiroadmin sgvotiroadmin 3 May 11 17:12
nfsshare
```

> **Note**
> In this example, **sgvotiroadmin** is the username that I use during the first login via putty to SFG.
> Your username may vary according to what you have created during the initcluster phase.

8.3.2 Issue 2: Missing metadata in blob-config

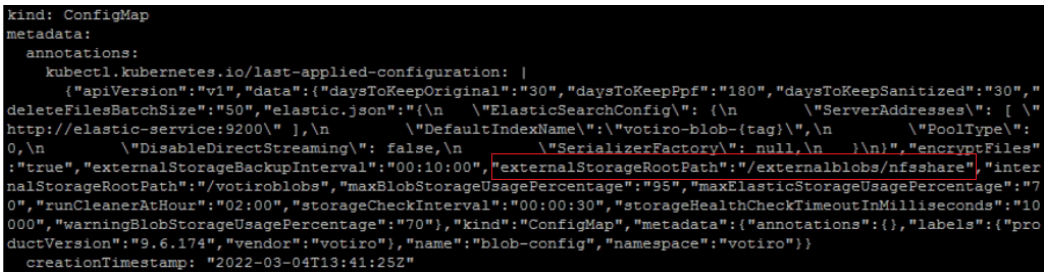
Symptoms

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

Solution

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

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



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

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

9 How to Deploy the Votiro Cloud Cluster in Azure

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

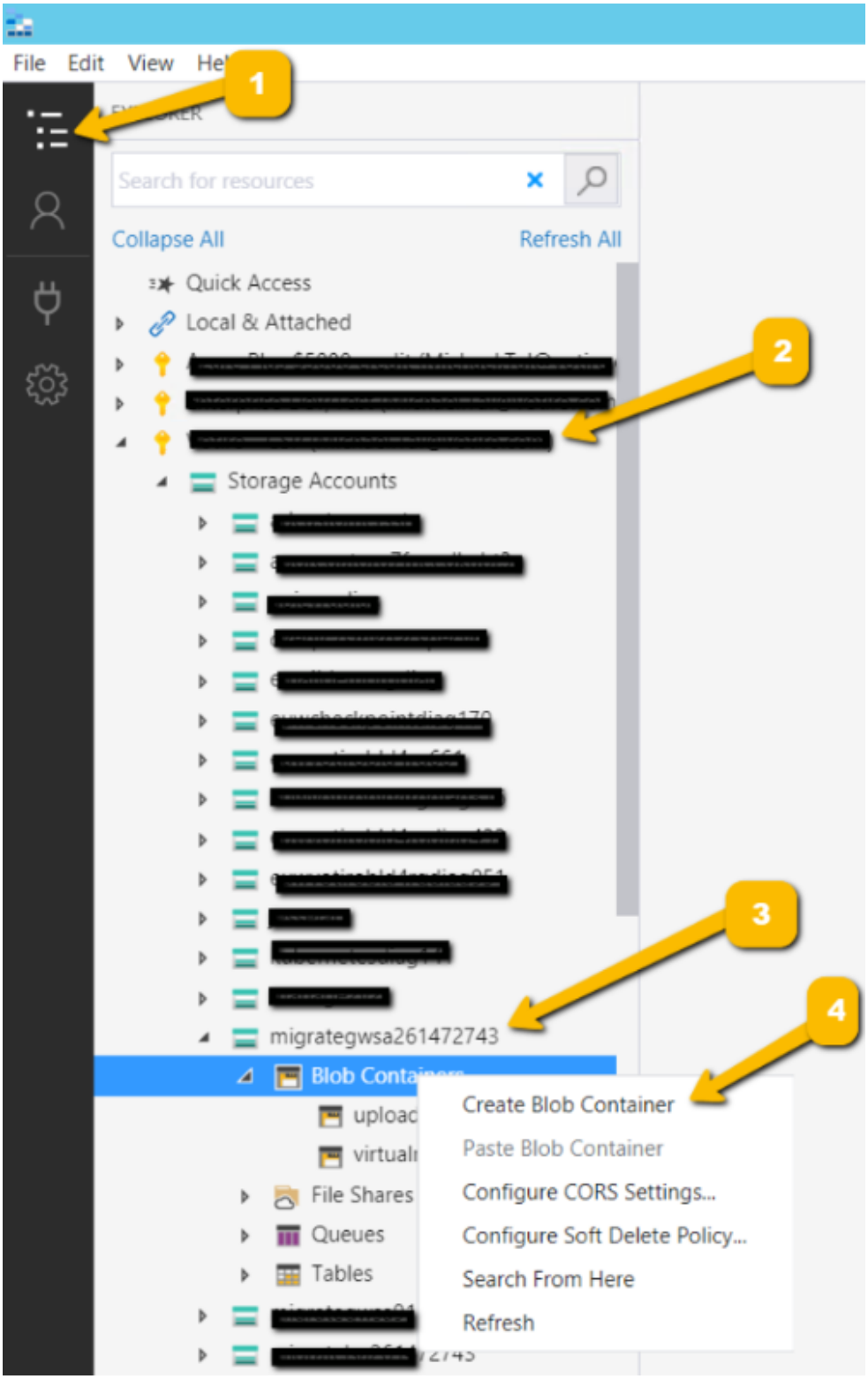
9.1 Prerequisites

Before you start, verify that the following are available:

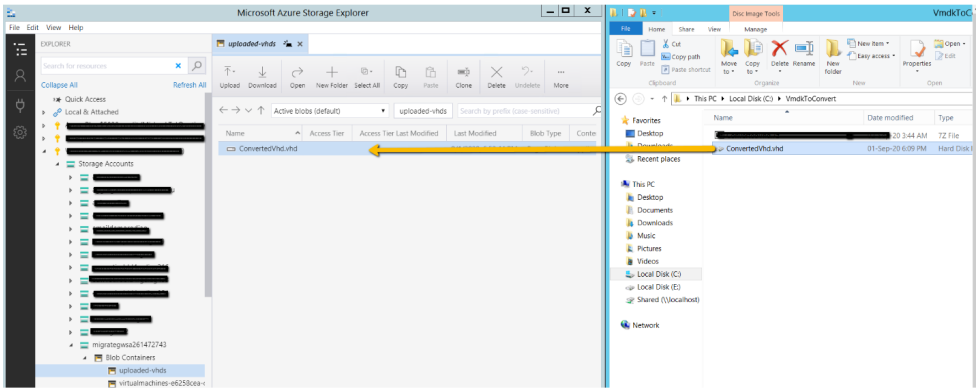
- An active Azure subscription
- The latest VHD (Virtual Hard Disk) provided by Votiro.
- The Azure Storage Explorer tool installed on a system that can access the Azure account and will be used to upload the VHD to your Storage account in Azure. This tool may be downloaded from Azure Storage Explorer.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

9.2 Procedure

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

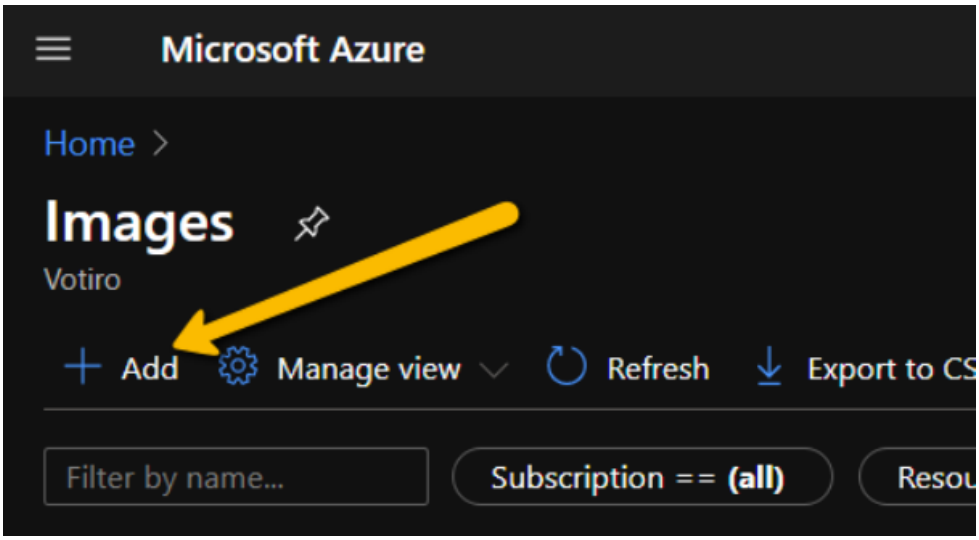


3. Drag and drop the extracted VHD file to the created Blob Container.



4. Once the upload process completes, open the Azure portal and navigate to the Images blade.

5. Click on **Add**. The **Create an image** screen is displayed.



6. Fill in the information to build the image from the VHD:

   a. Provide the image with a **Name**.

   b. Select a **Subscription**.

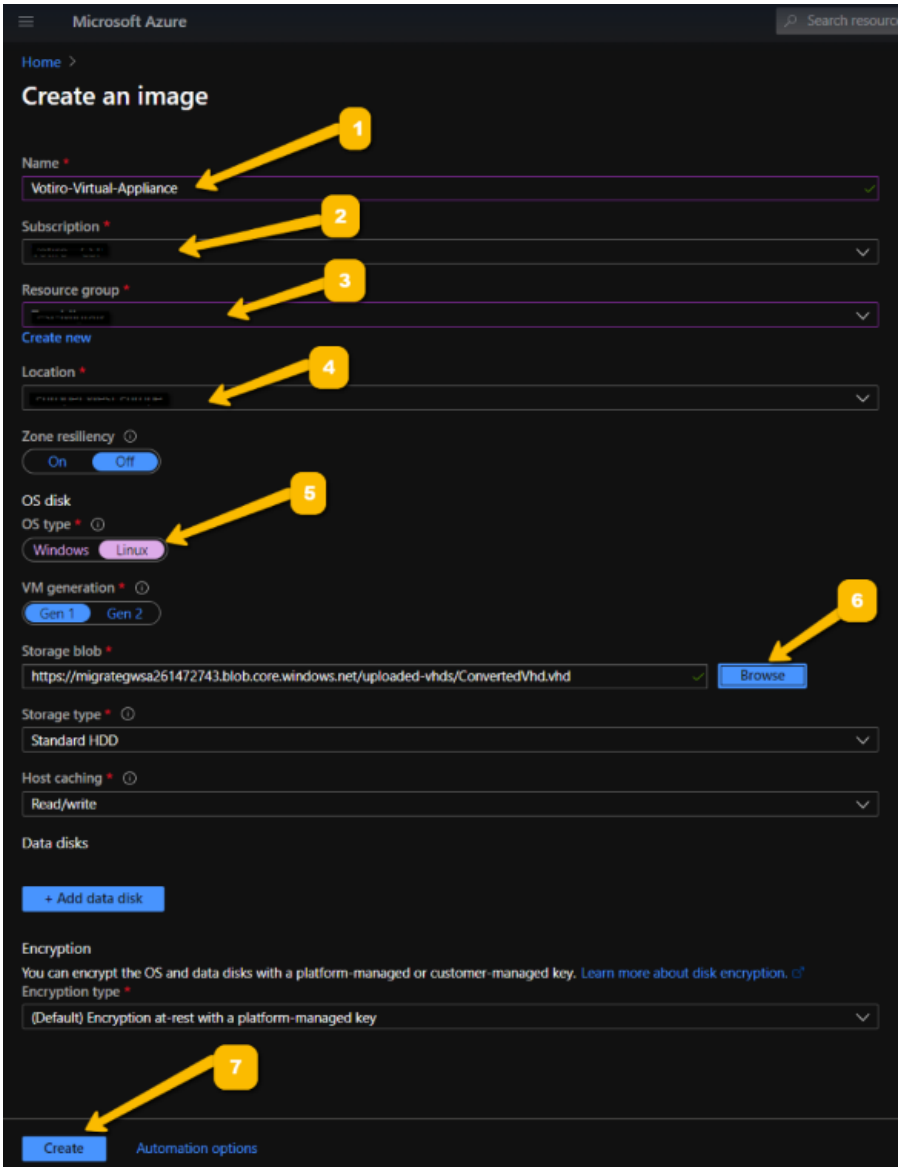
   c. Type in the **Resource group**.

   d. Select the **Location**.

   e. Select the **OS type** as **Linux**.

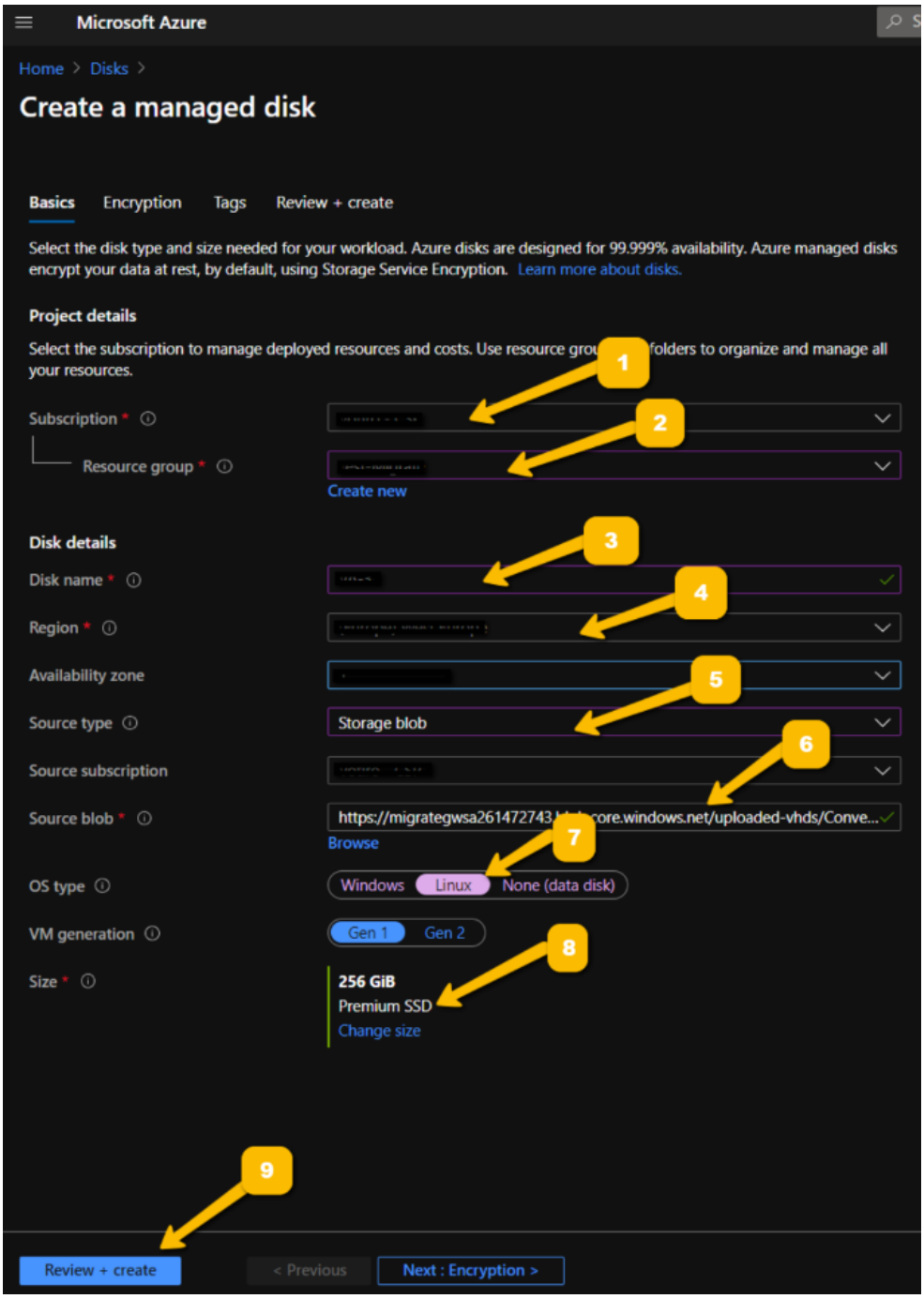
   f. Click on **Browse** and select the uploaded VHD file.

   g. Click on **Create**.

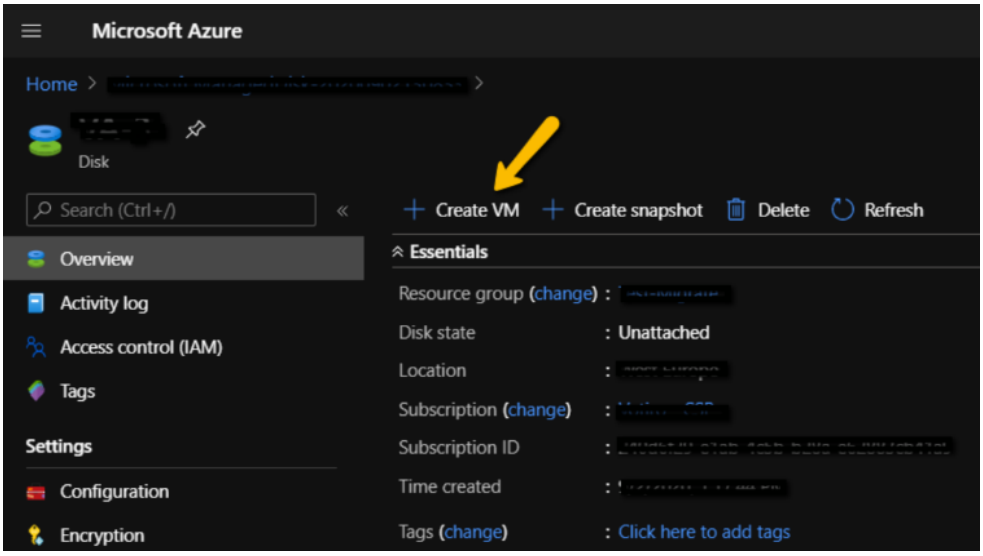


7. After the image is created, **Create a managed disk**.
8. Fill in the information as in the screenshot below:
    a. Select a **Subscription**.
    b. Select the **Resource group**.
    c. Provide a **Name** for the disk, for example Node-1.
    d. Select the **Region** which you would like the disk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

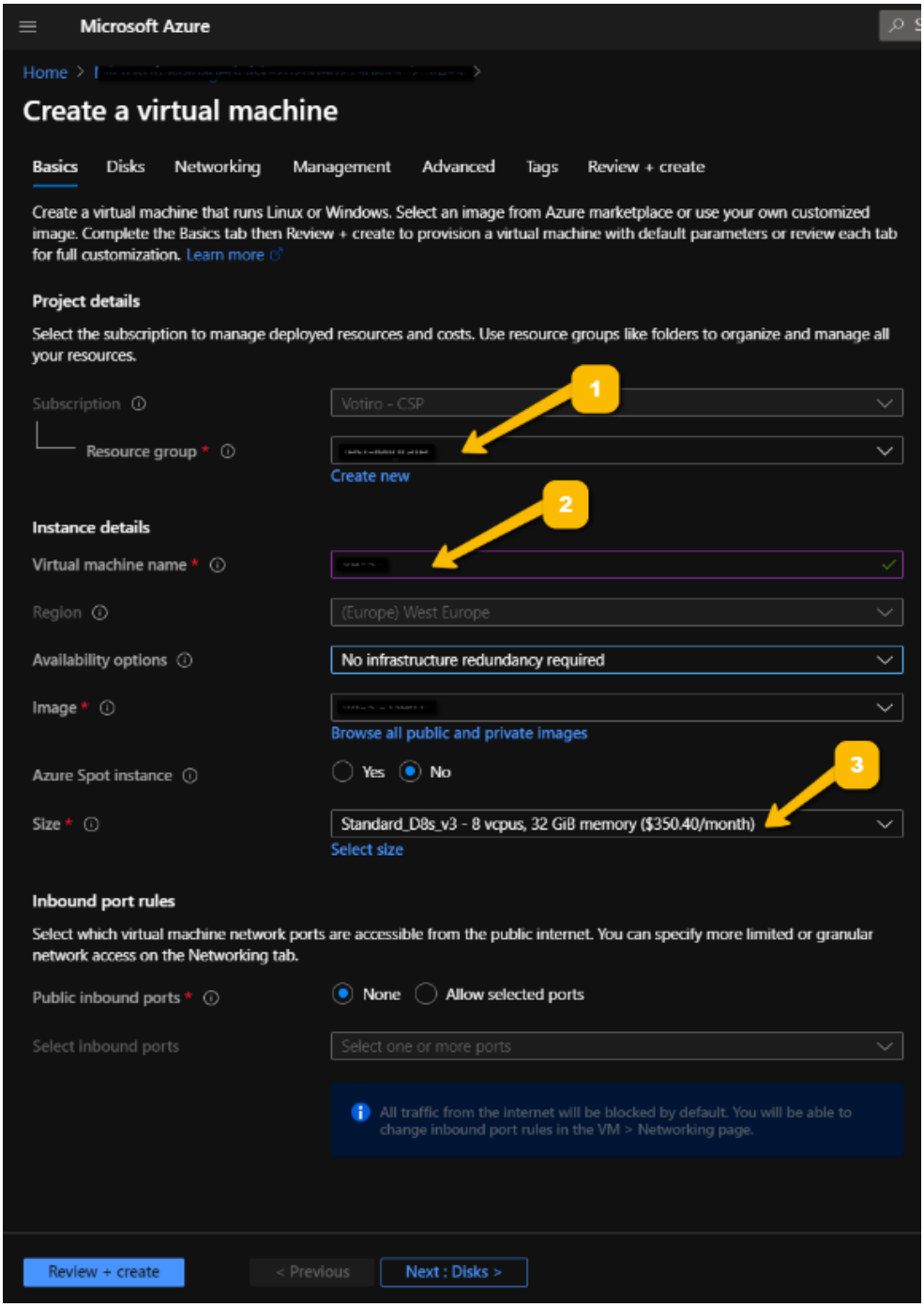
i. Click on **Review + create**.



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.

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

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

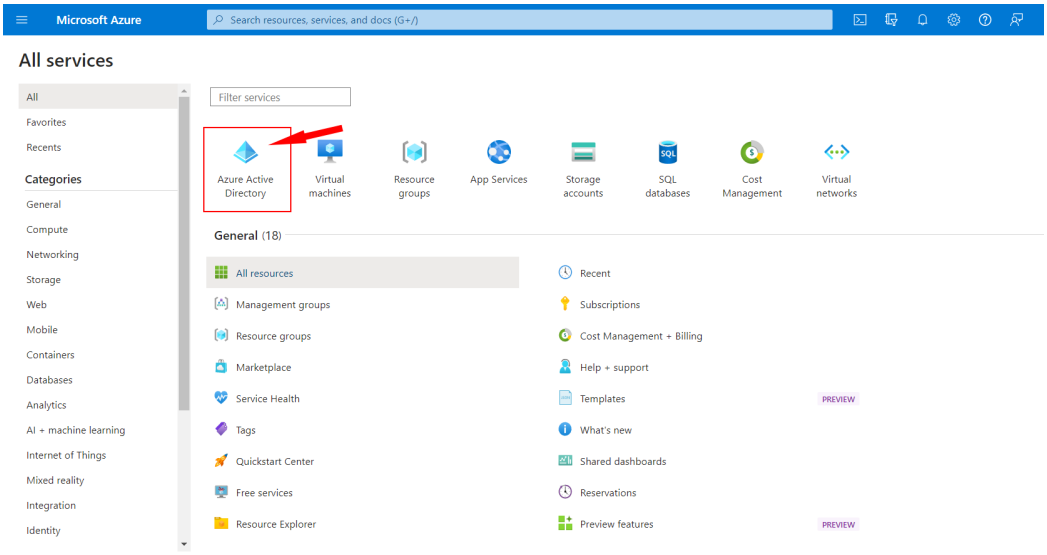
10.1 Prerequisites

Ensure you have the following items:

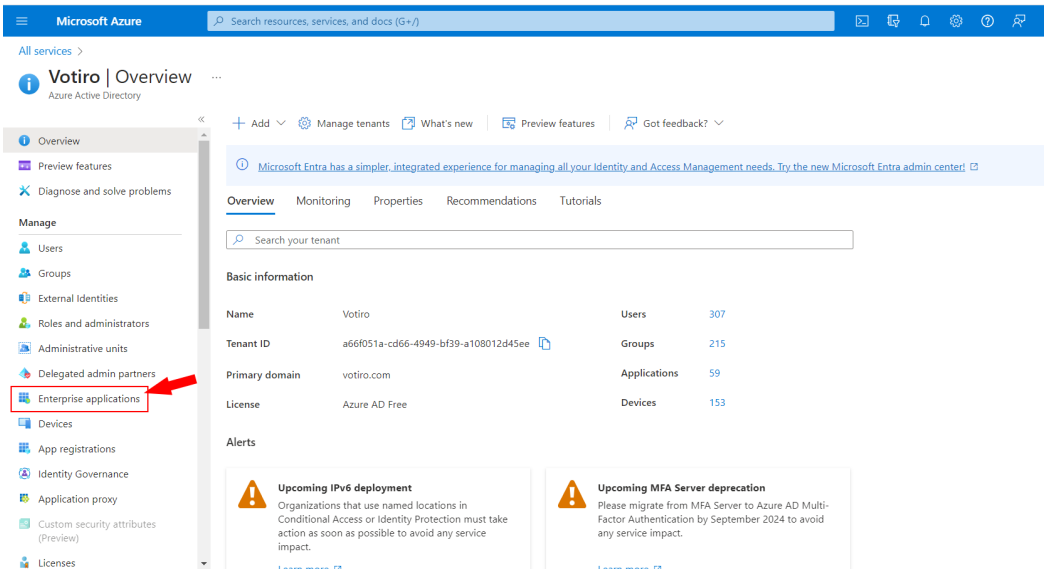
- Azure AD subscription
- Azure AD SAML Toolkit enabled on the above-mentioned subscription

10.2 Procedure

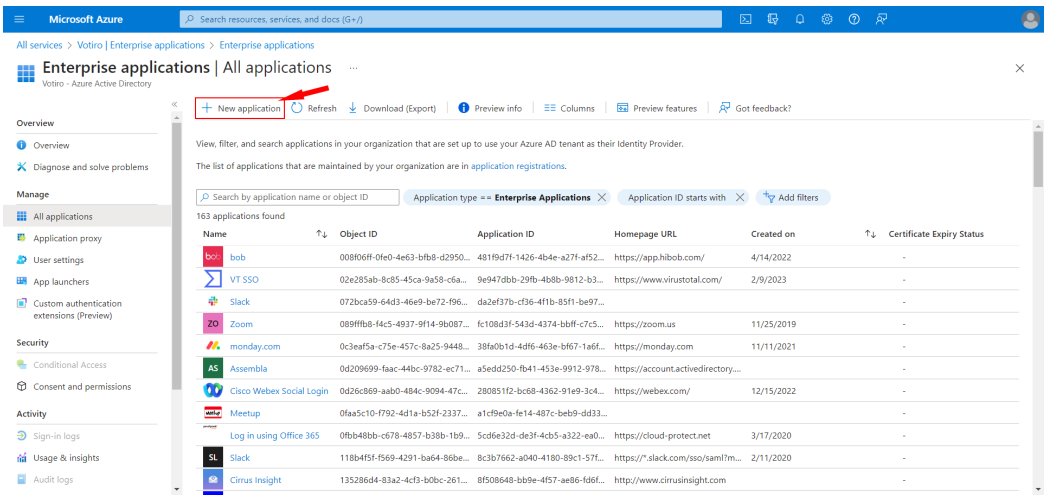
1. Sign in to the Azure portal.
2. Select **Azure Active Directory**.



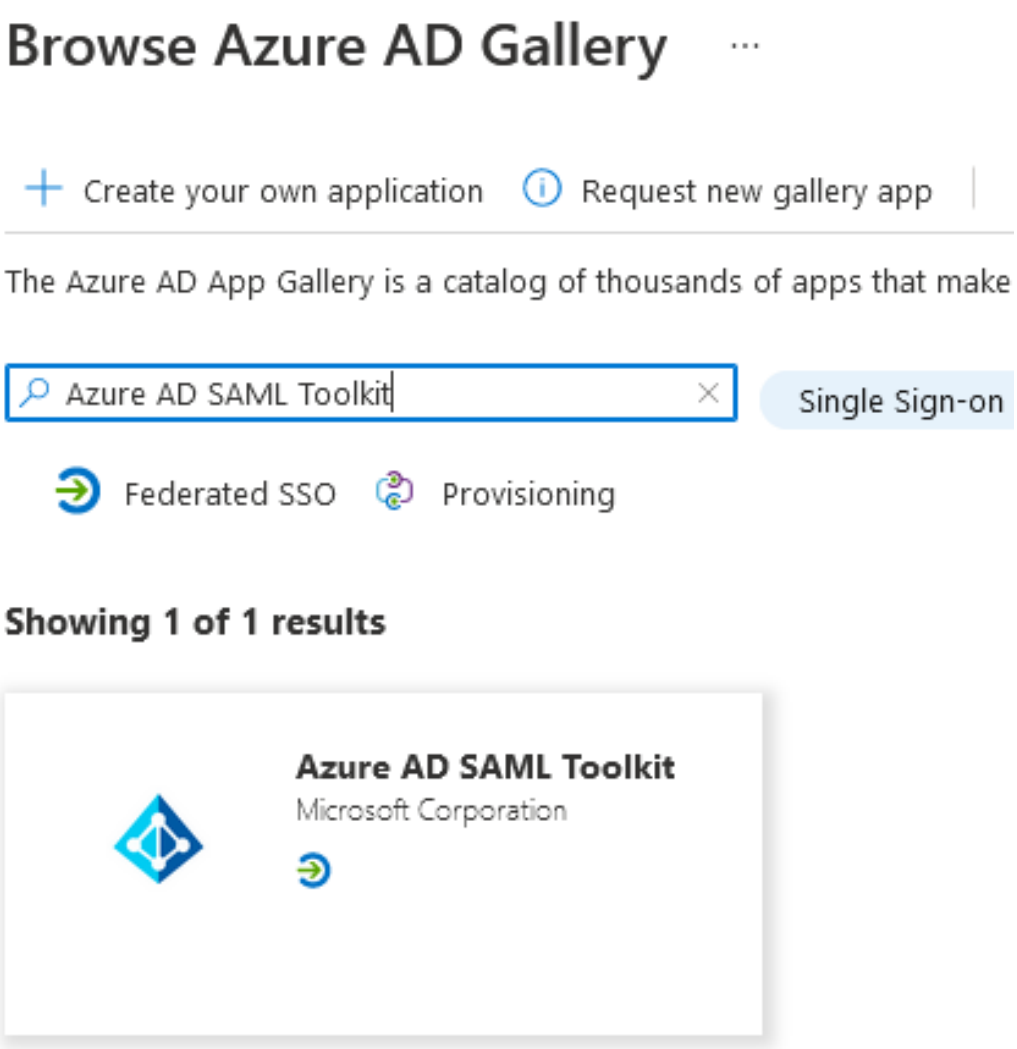
3. In the left pane, select **Enterprise applications**.



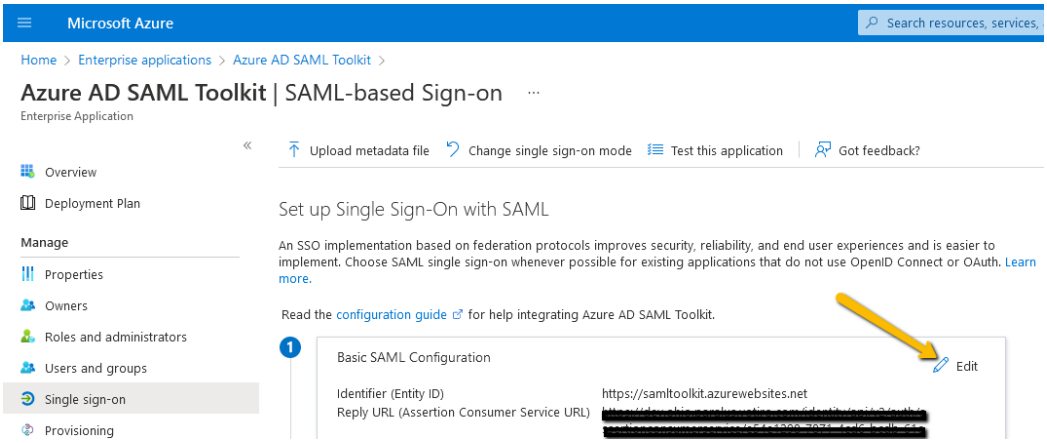
4. Select **New application**:



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



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

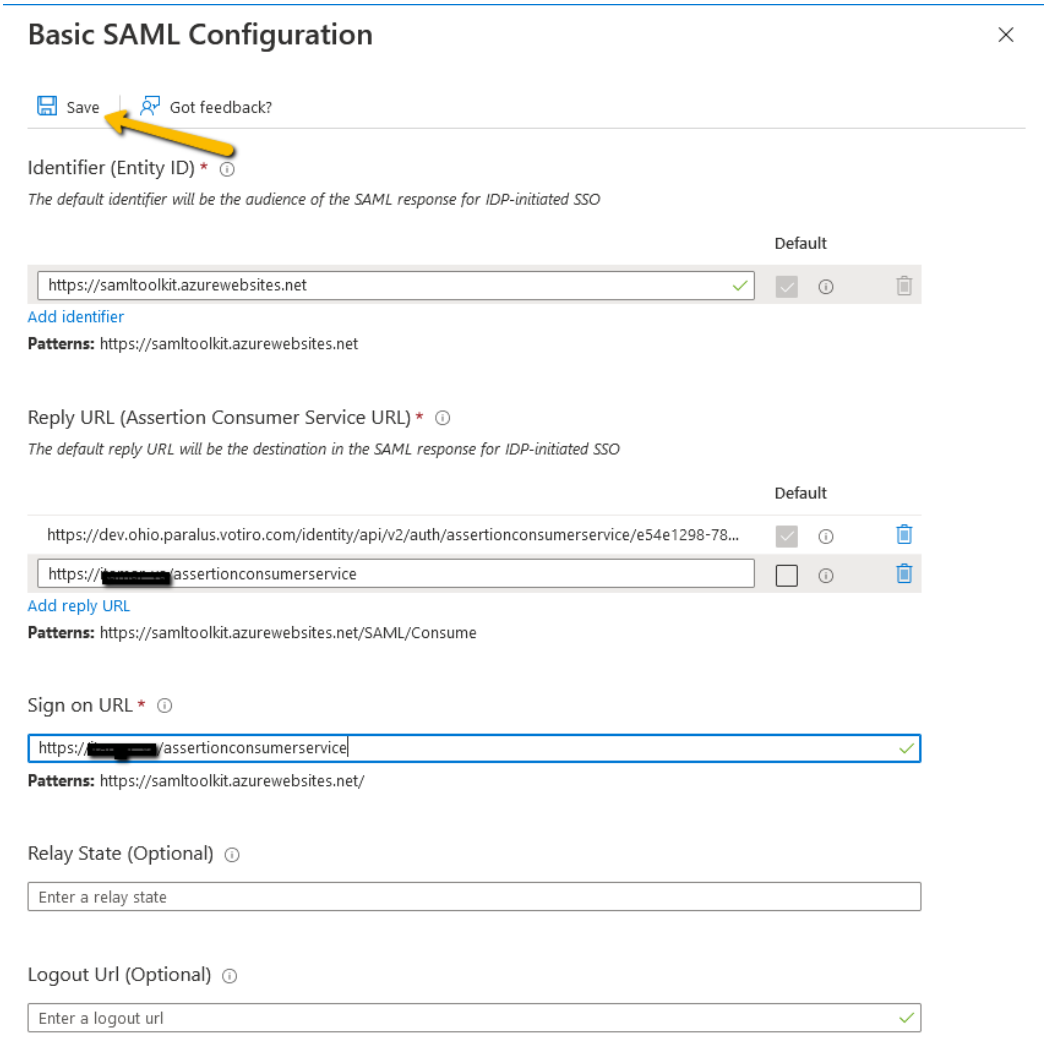


10. For **Identifier (Entity ID)**, leave as default - https://samltoolkit.azurewebsites.net.

11. Both Reply URL (Assertion Consumer Service URL) and Sign on URL should be in the following format: https://<VOTIRO-FQDN>/assertionconsumerservice.

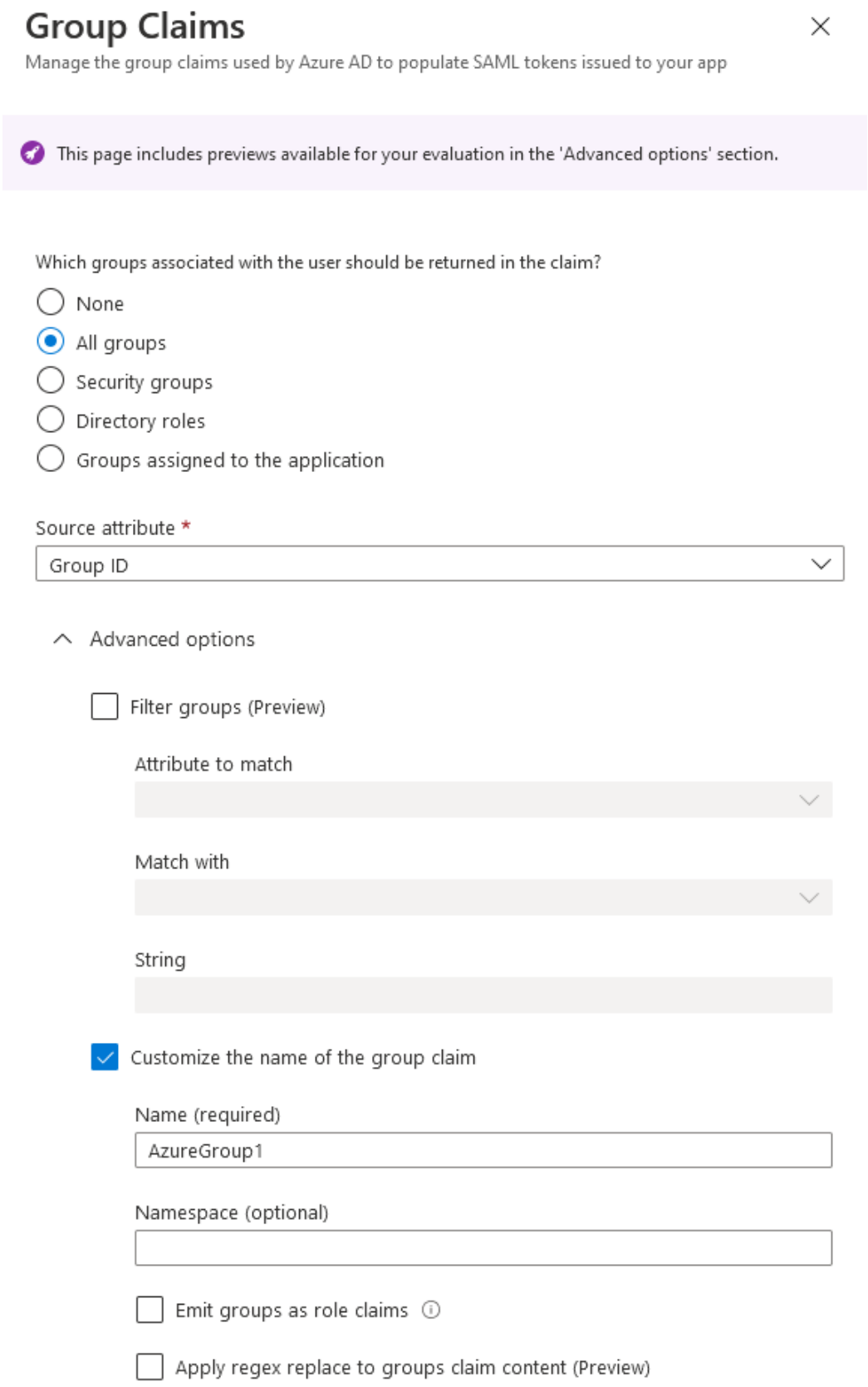
> **Note**:
>
> **If you're configuring SAML for SaaS cluster, please make sure to include the tenant id after the Reply URL and Sign on URL:**
>
> https://<VOTIRO-FQDN>/assertionconsumerservice/<TENANT_ID>

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

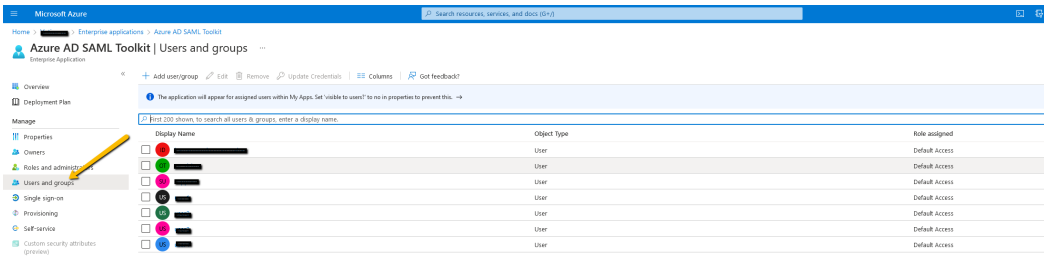


13. On the **Attributes & Claims** section, click the pencil button to edit the configuration.

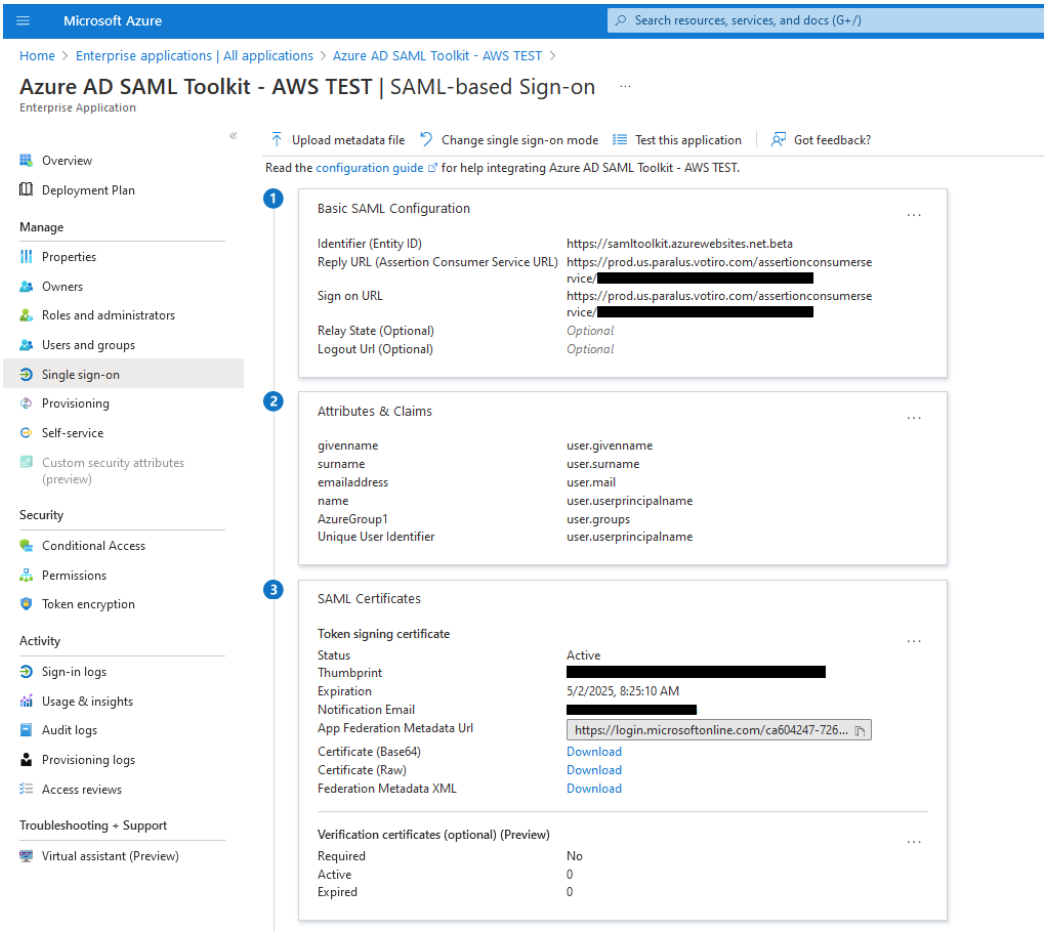
14. Select **Add a group claim** on the left-hand side, choose All groups, expand **Advanced options**, select **Customize the name of the group claim**, and provide it with a name, for instance, “AzureGroup1”, then press the **Save** button.


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

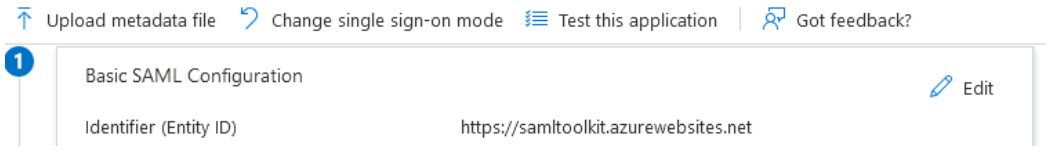
15. To avoid issues such as “User without any role”, make sure the users that should have access to the environment via SAML are listed under **Azure AD SAML Toolkit | Users and groups**.



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



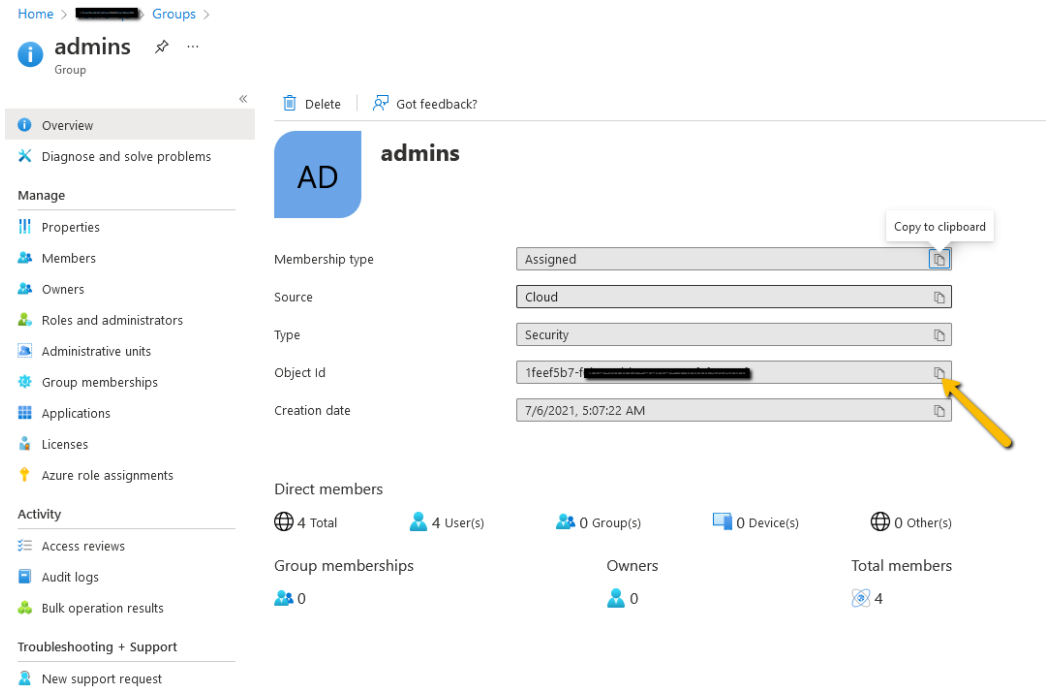
17. For the Issuer, copy and paste https://samltoolkit.azurewebsites.net from the **Basic SAML Configuration** you configured above.



18. For the SAML Username identifier, leave by default: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier

19. The Admin role key should be the value you provided for the group above in **Group Claims**, in this case, AzureGroup1.

20. The Admin role value should be the Object Id of the group in which the admin's users are members.



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

11 How to Integrate SIEM with Azure Sentinel

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

11.1 System prerequisites

Ensure you have the following:

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

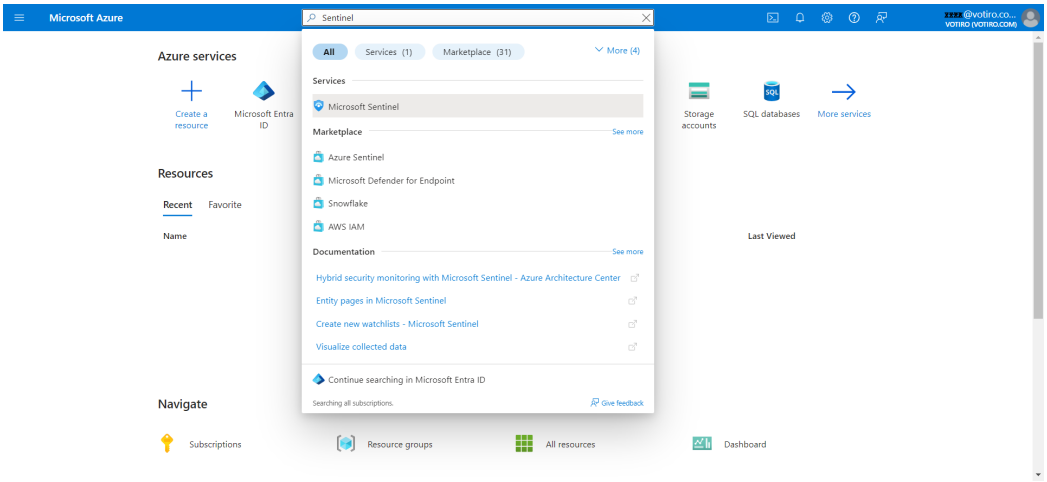
11.2 Procedure

11.2.1 Manual/Offline Deployment

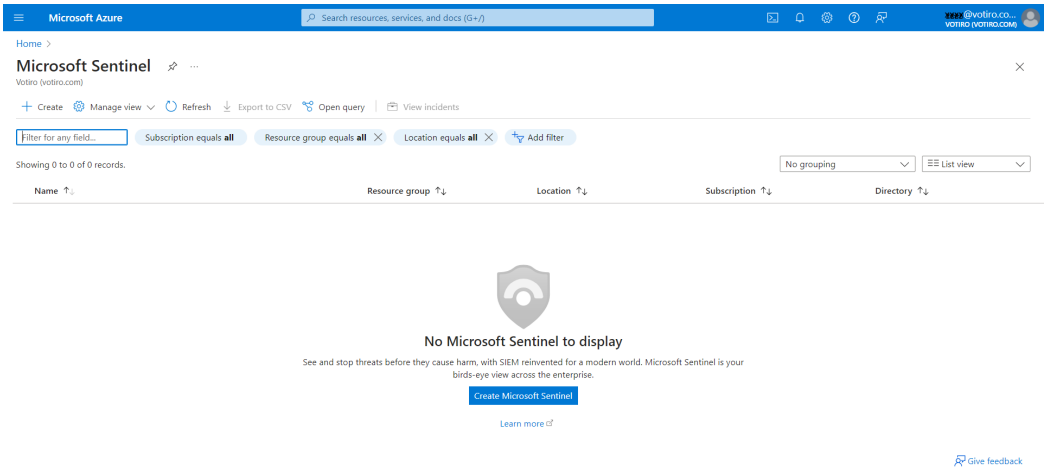
To test the solution before publishing, follow the below steps.

Deploy CEF Data Connector on Forwarder Machine

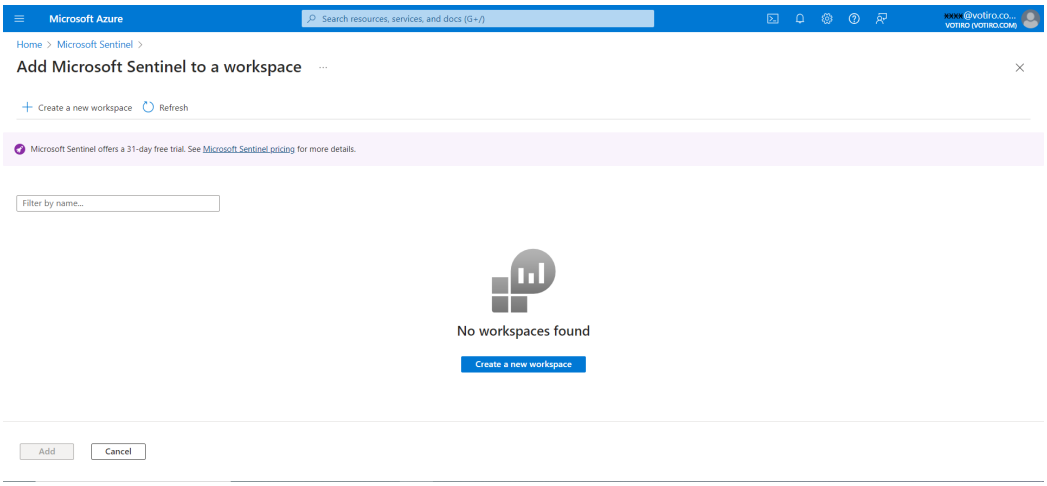
1. Sign in to the Azure portal.
2. Search for **Microsoft Sentinel**.



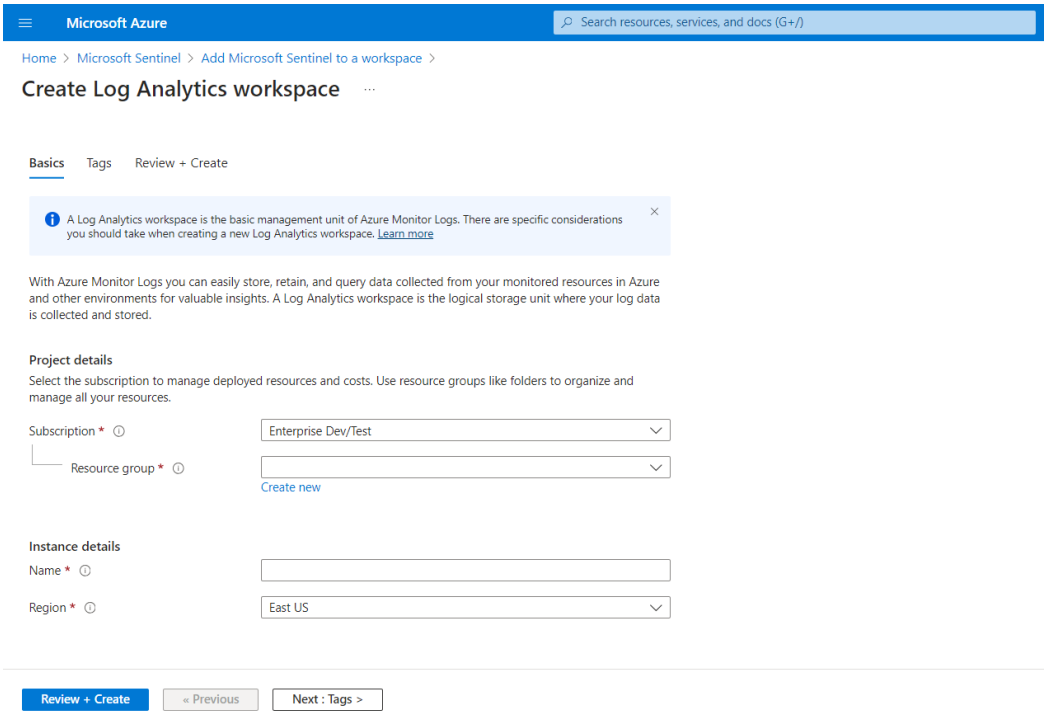
3. Select **Microsoft Sentinel** from **Services**.



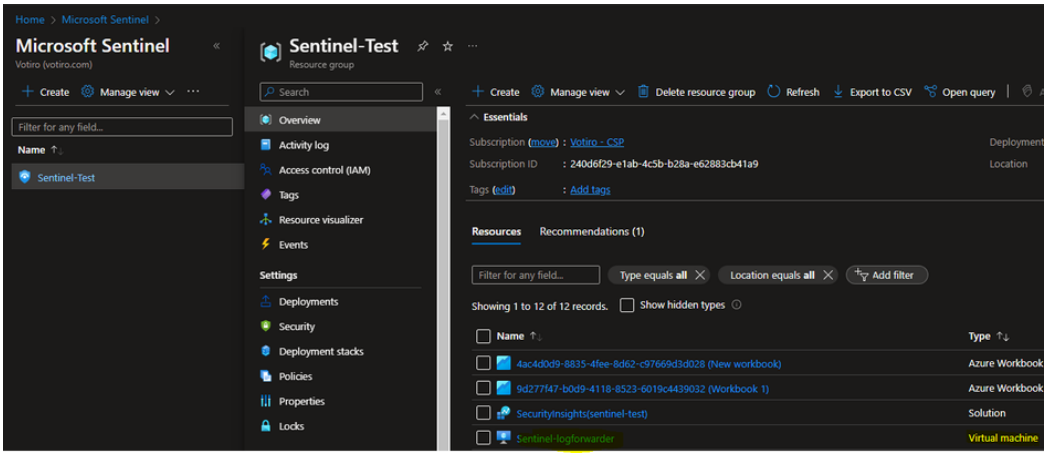
4. Press **+ Create** or **Create Microsoft Sentinel** to add **Microsoft Sentinel** to a Workspace::



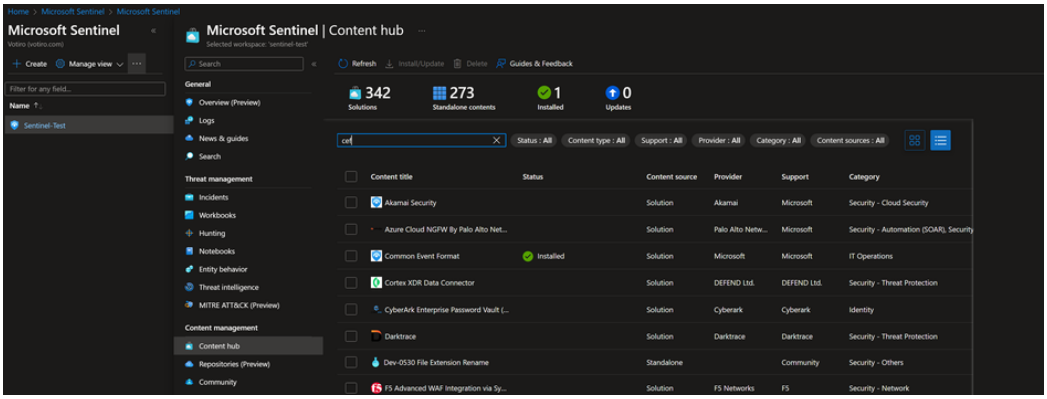
5. Press **+ Create a new workspace**:



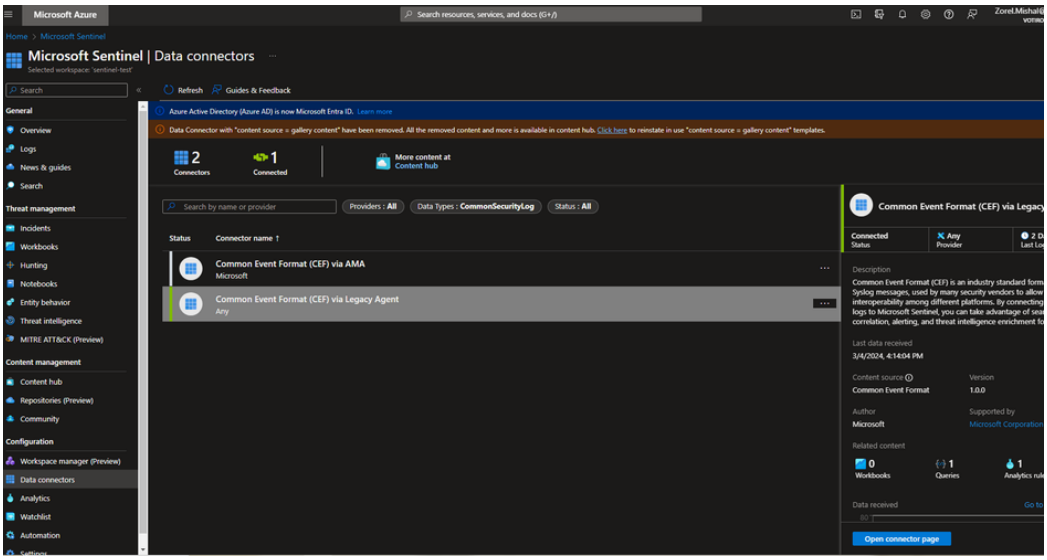
6. Create a new **Resource Group** if it does not exist yet. Then create a new machine with the system requirements mentioned above → via Resource Group > Create > select Virtual Machine (Ubuntu 22.06 server is recommended):



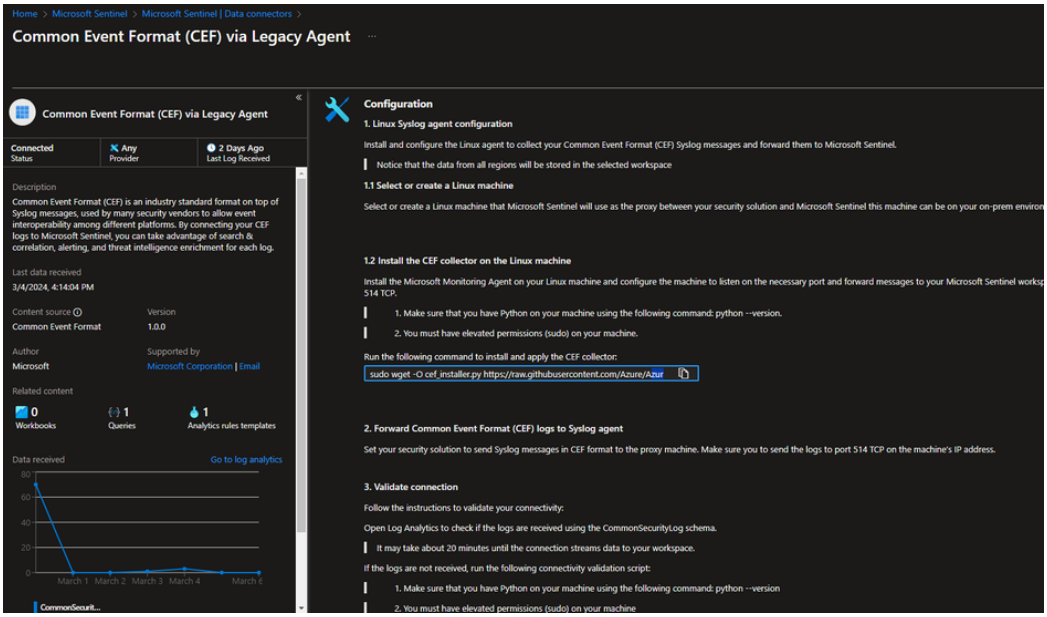
7. Select the created workspace, then go to Content Hub > Select Common Event Format (CEF) and install it:



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:

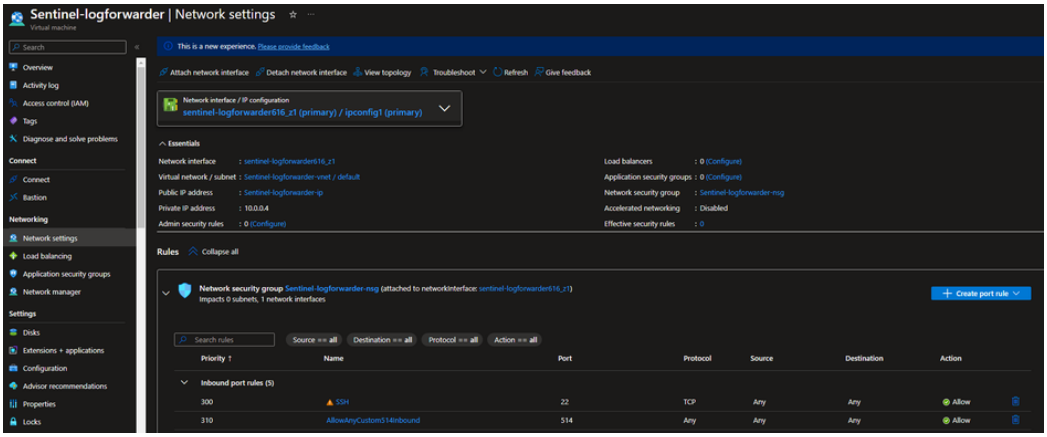
    ```
    sudo wget -O cef_installer.py
    https://raw.githubusercontent.com/Azure/Azure-
    Sentinel/master/DataConnectors/CEF/cef_installer.py&&sudo
    python cef_installer.py [WorkspaceID] [Workspace Primary
    Key]
    ```

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

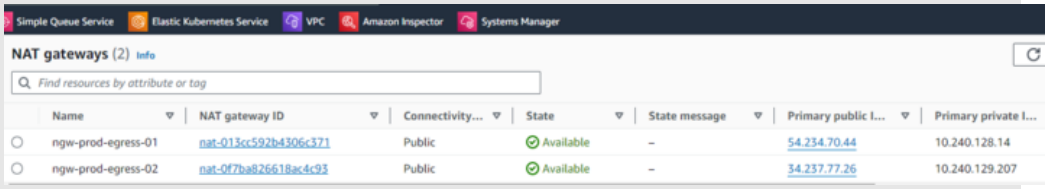
12. Paste the command into the command line on your log forwarder, and replace **[WorkspaceID]** and **[Workspace Primary Key]** with their values.

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:



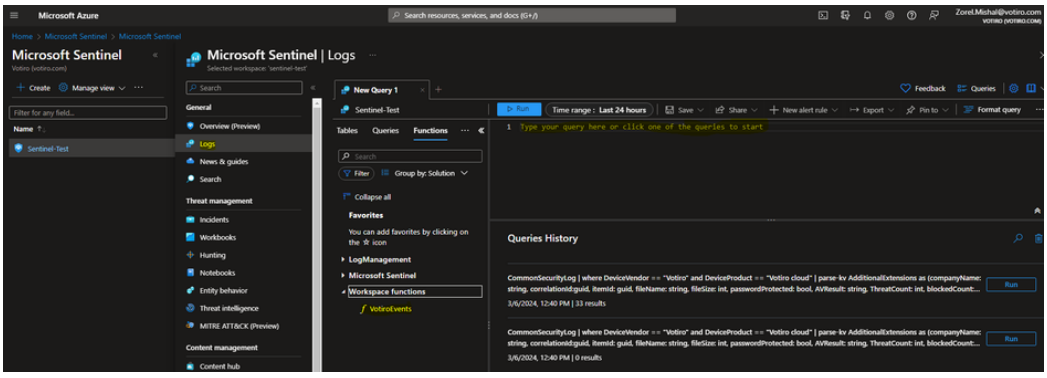
Note: In this case, we used TCP port 514 (default) and **Allow=any**, but the best practice is to use the TLS protocol with other ports used and restrict to specific IPs pointed to specific NAT gateways. For example, in [prod.us]:



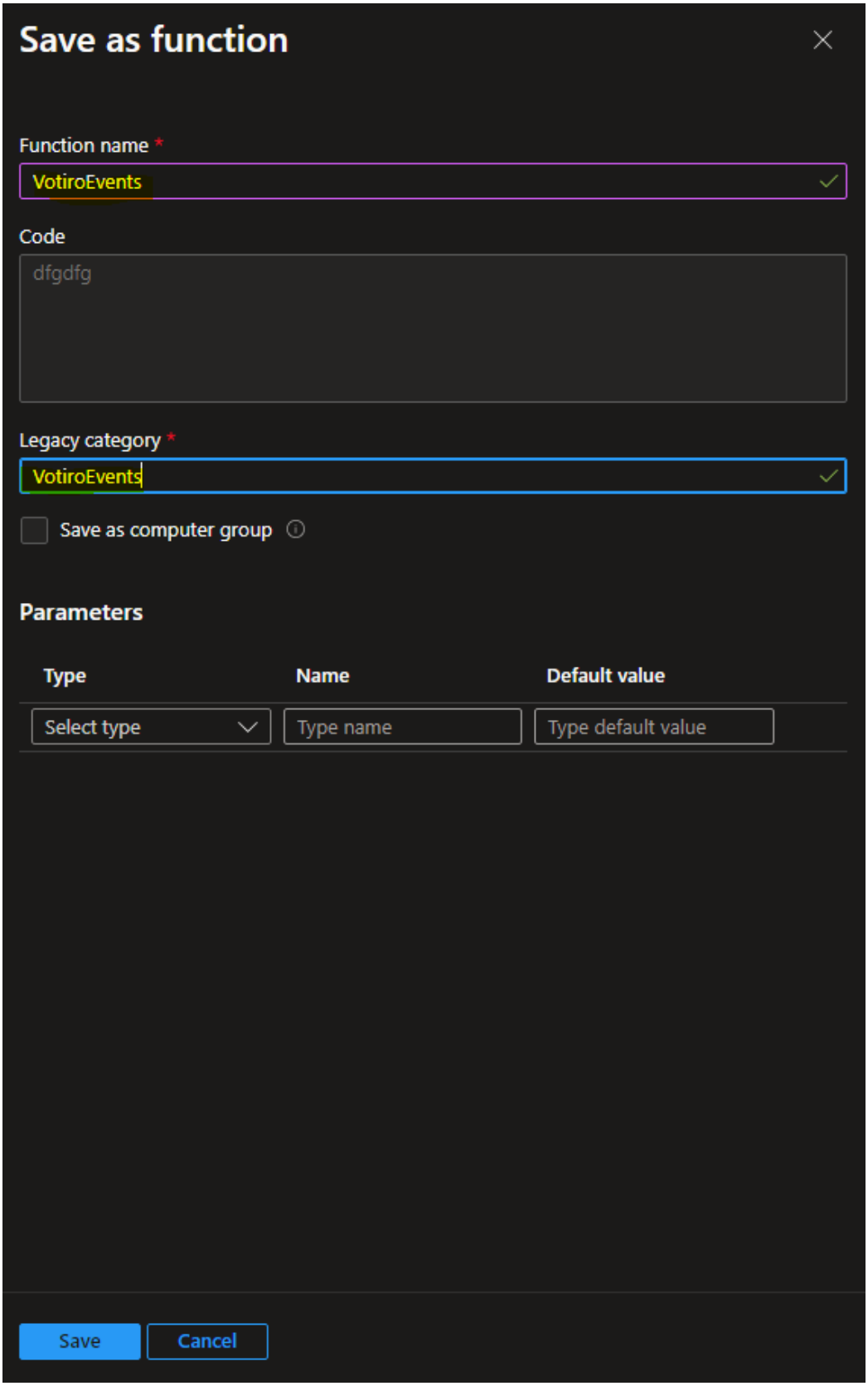
Deploy Parser Function

Follow the instructions to parse ingested data:

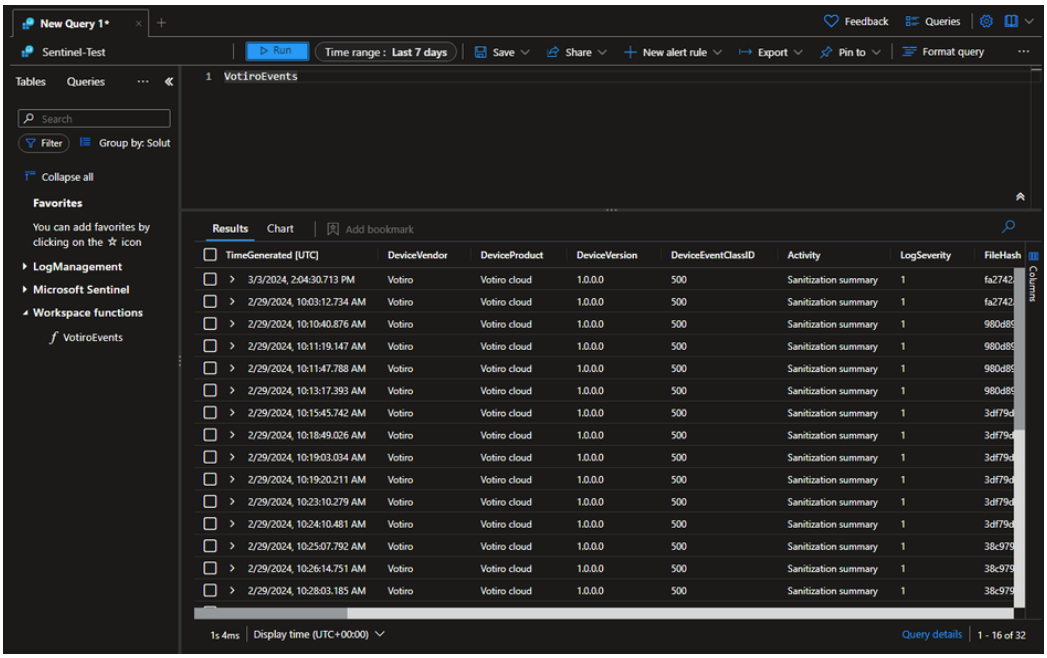
1. Copy the function code from the downloaded package file: **/Votiro-Offline/Parser/VotiroEvents.txt**
2. On Microsoft Sentinel → Go to your created Workspace -> Logs
3. Paste the content of **VotiroEvents.txt** in the area as shown below:

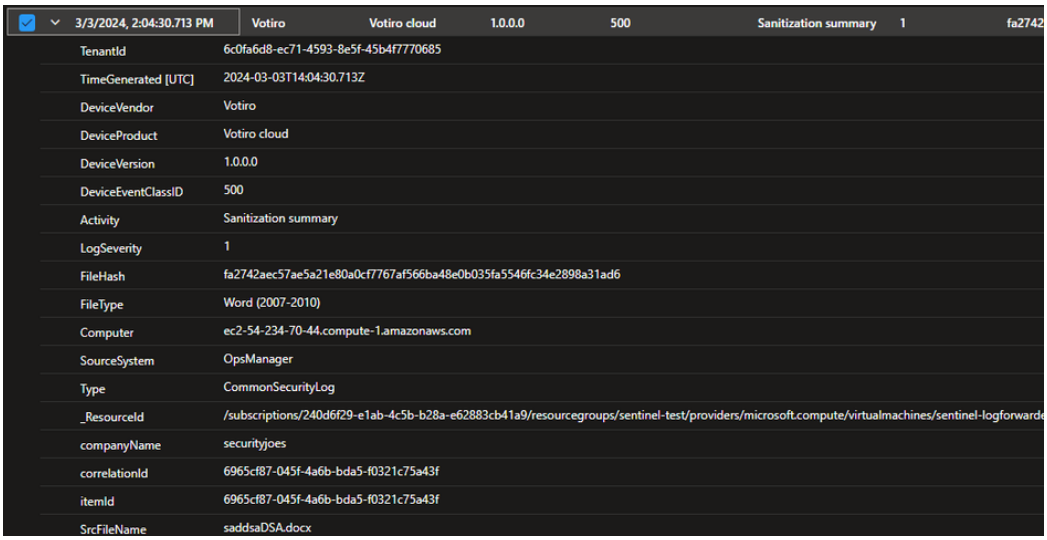


4. Then click on **Save** > **Save as function**. Enter the **Function name** as **VotiroEvents** and click on **Save**:

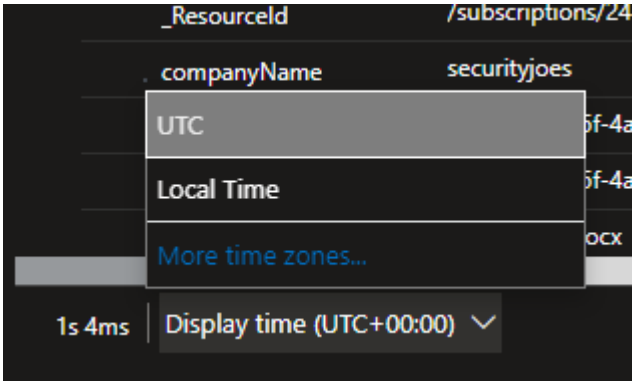

Save as function
Function name *
VotiroEvents
Code
dfgdfg
Legacy category *
VotiroEvents
Save as computer group
Parameters
Type
Name
Default value
Select type
Type name
Type default value
Save
Cancel

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





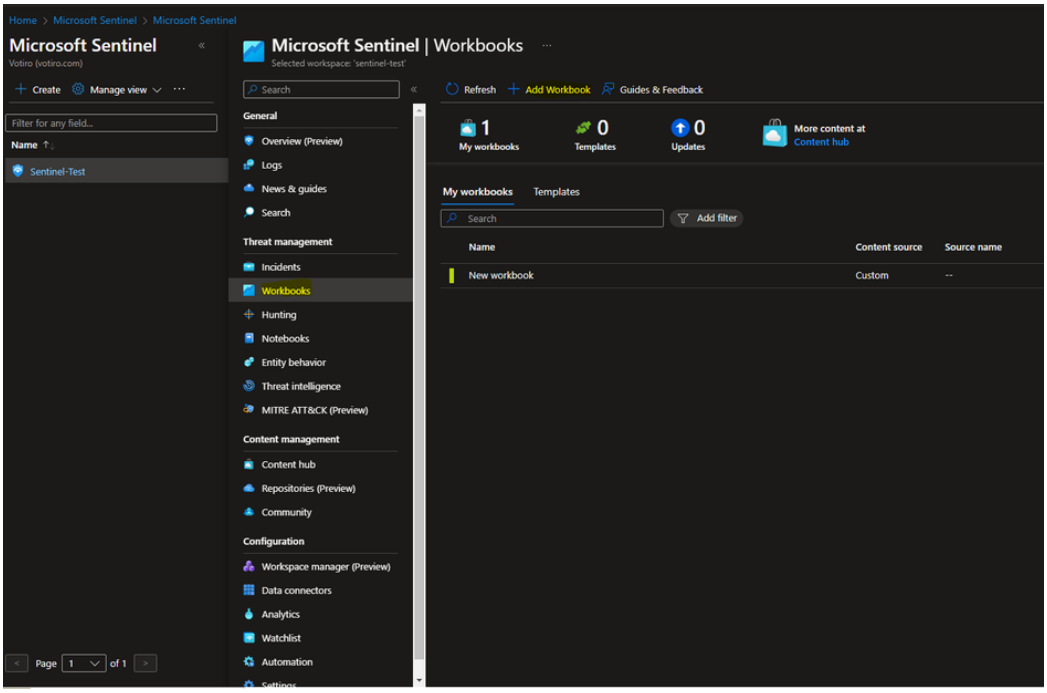
6. Results can be viewed in **Local Time** zone by changing the option in the bottom bar:



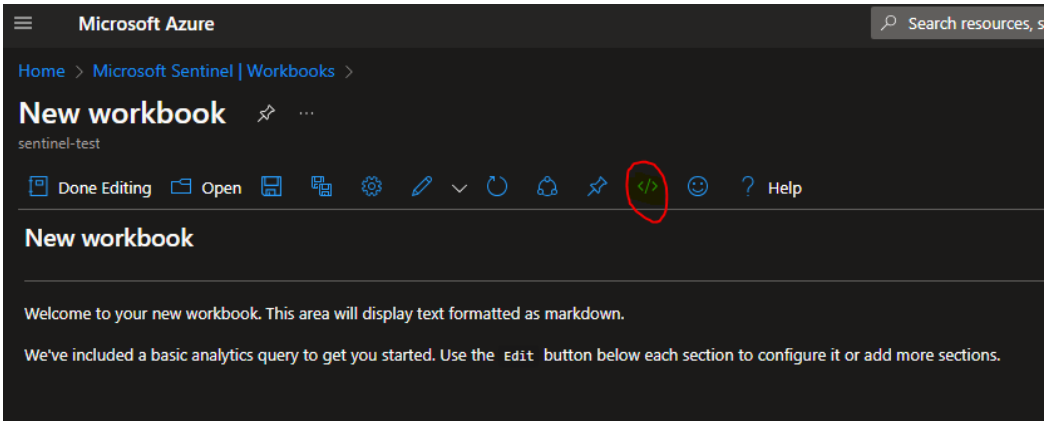
Deploy the Workbook

1. Copy the contents of the file:
   /Votiro-Offline/Workbooks/Votiro Monitoring Dashboard.json

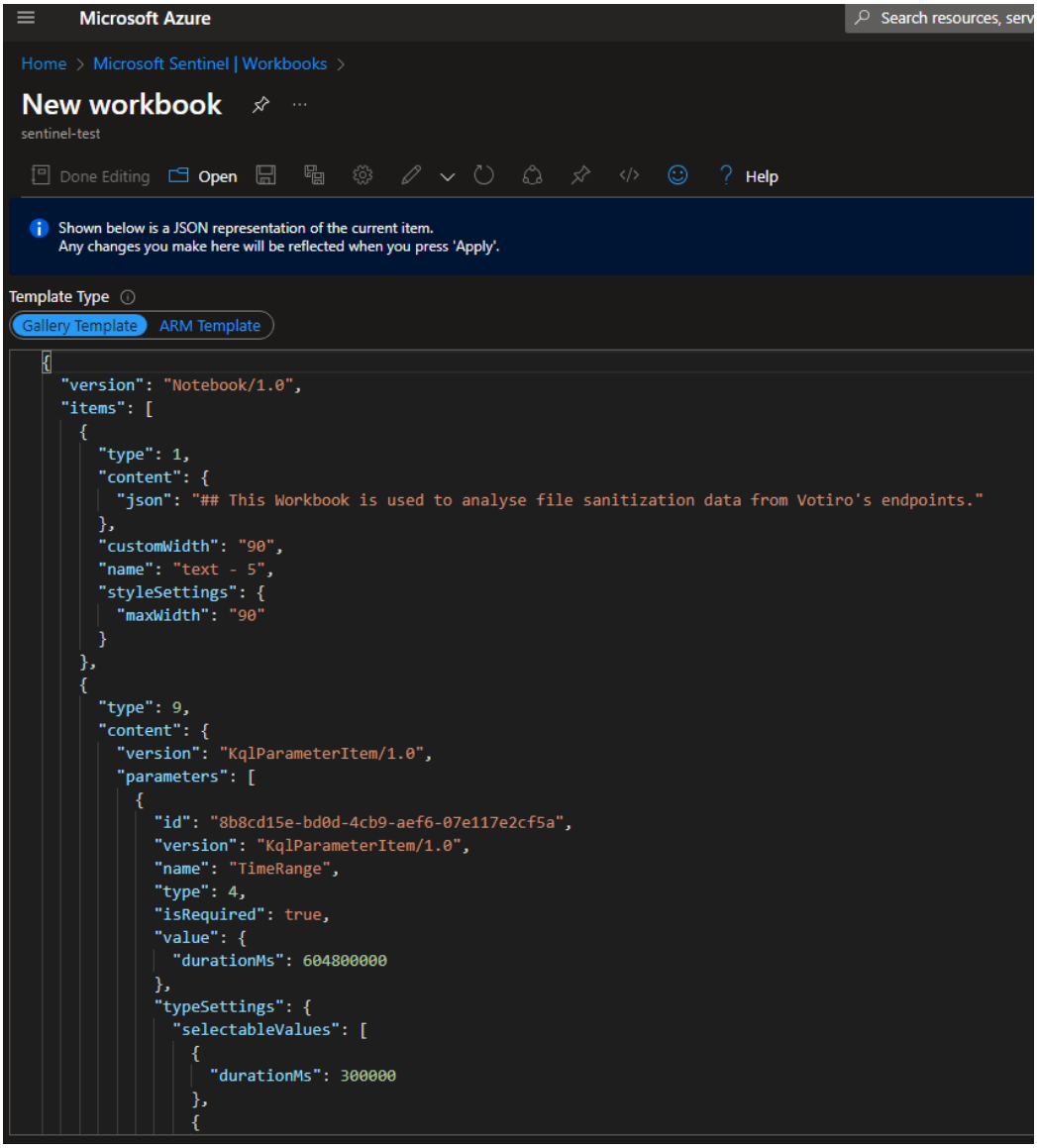
2. On Microsoft Sentinel, go to your WorkSpace > Workbooks > **Add Workbook**":



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**:



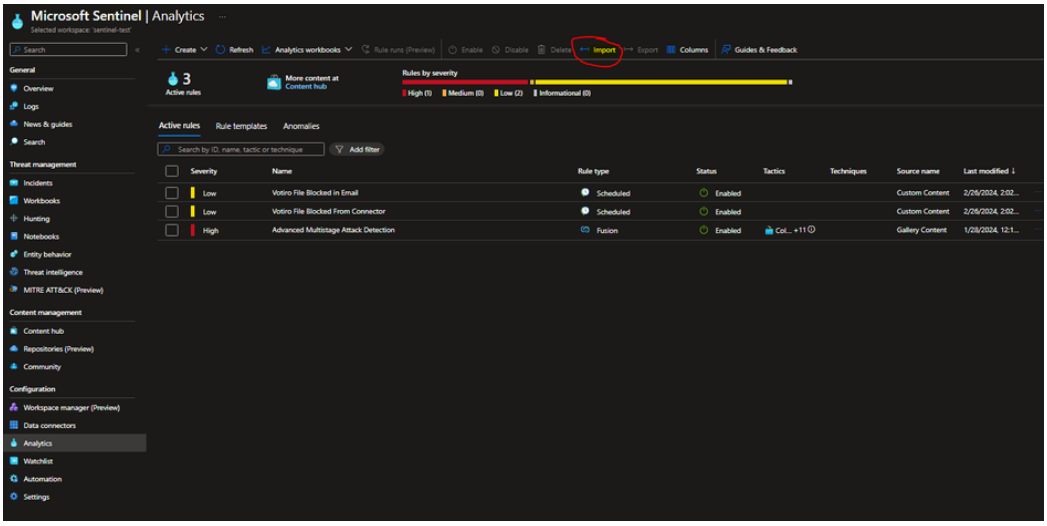
5. The Following Workbook must be visible:
After a scroll

Set Alert Queries for Incidents

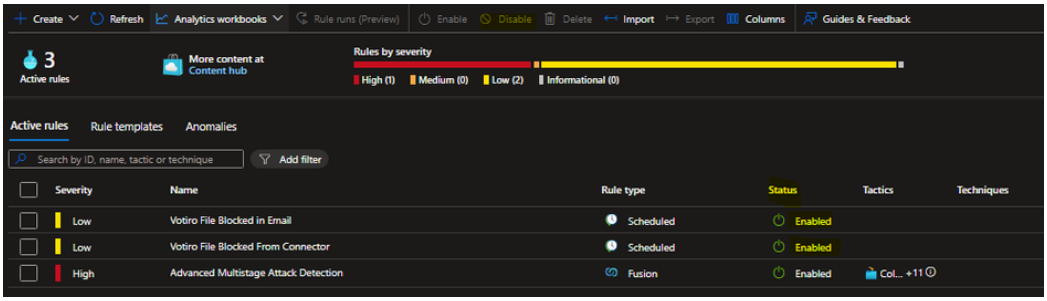
1. Go to **/Votiro-Offline/Analytic Rules**. Keep both **Votiro File Blocked FromConnector.json** and **Votiro File Blocked in Email.json** files ready.

2. On Microsoft Sentinel > Workspace, select **Analytics**.

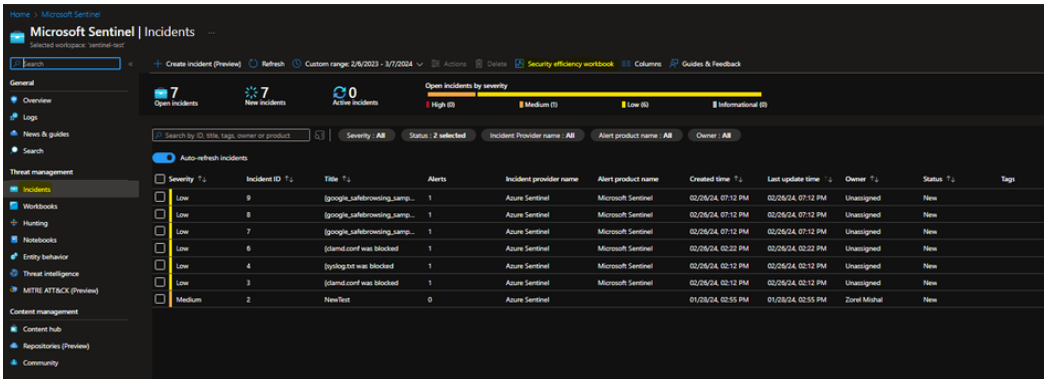
3. Click **Import** (from the bar at the top of the screen) in the resulting dialog box, navigate to and select the JSON files one by one, and select **Open**:



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]

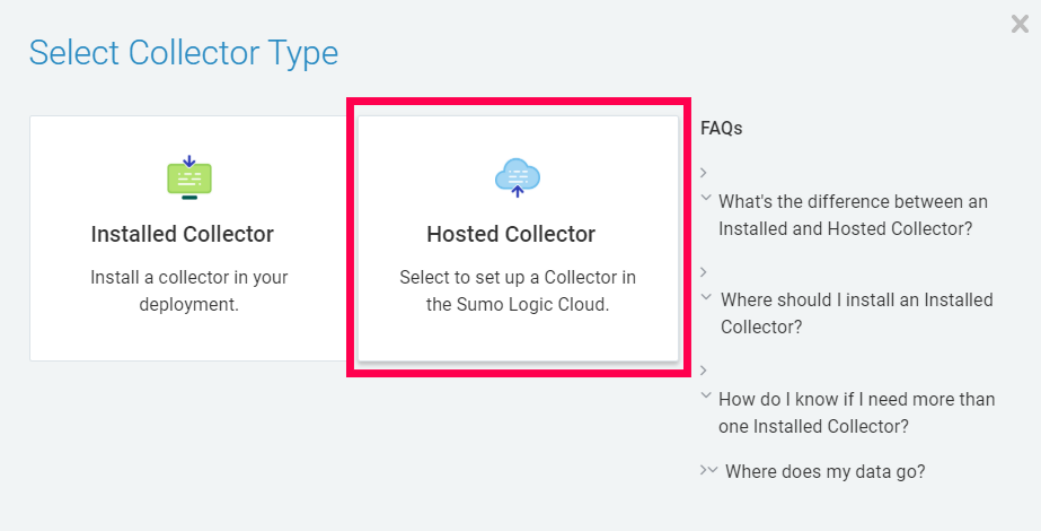
12 How to Integrate Votiro Cloud Syslog Messages with Sumo Logic using HTTP Logs

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

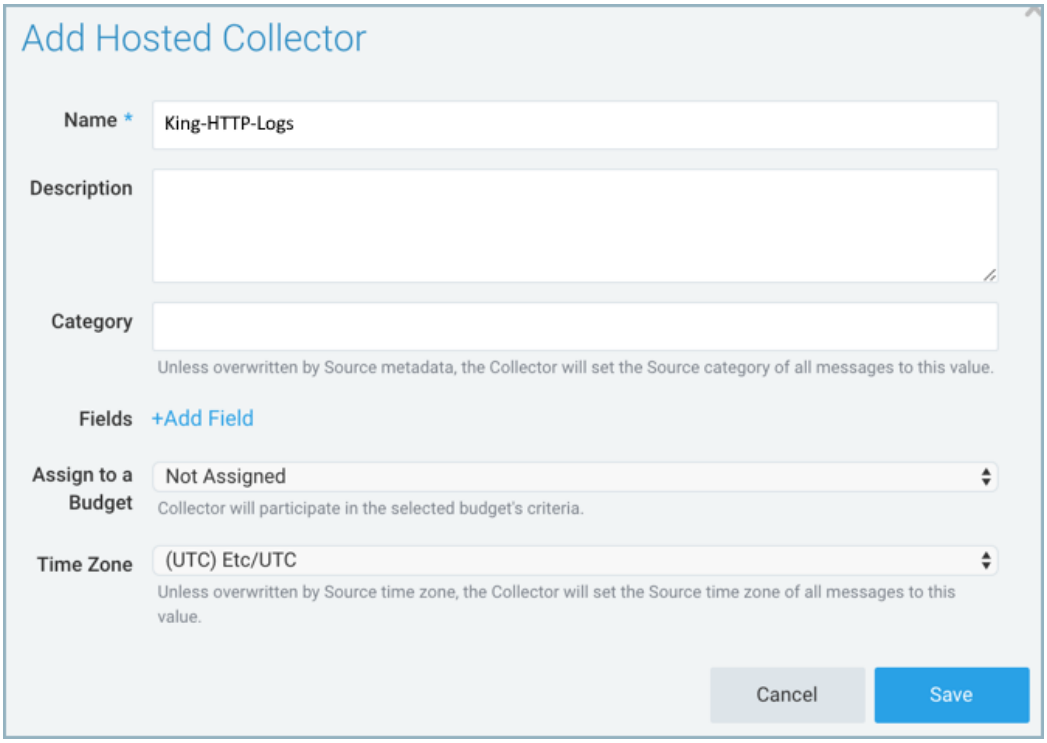
12.1 Procedure

12.1.1 Configure an HTTP Logs and Metrics Source in Sumo Logic

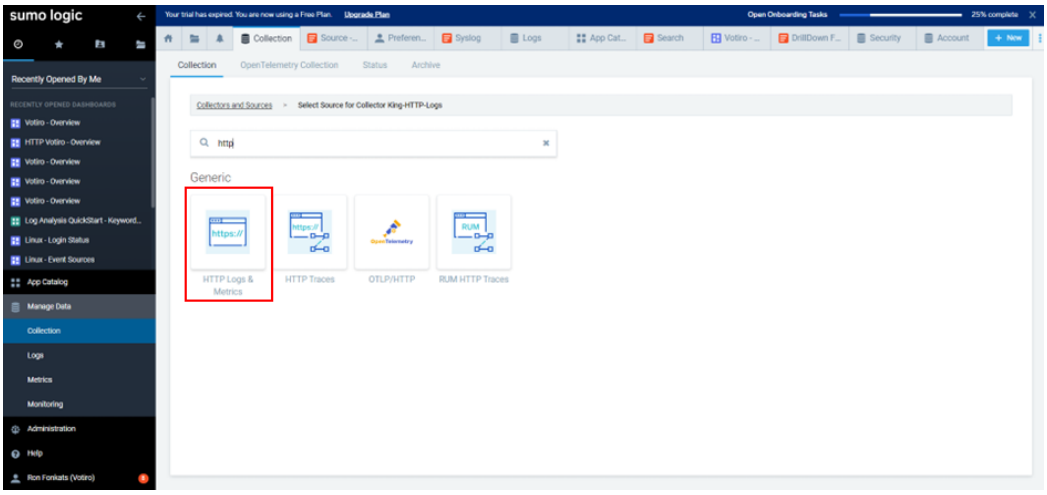
1. In Sumo Logic, select **Manage Data > Collection > Collection**.
2. Click **Add Collector**.
3. In the **Select Collector Type** window, select **Hosted Collector**.



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



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

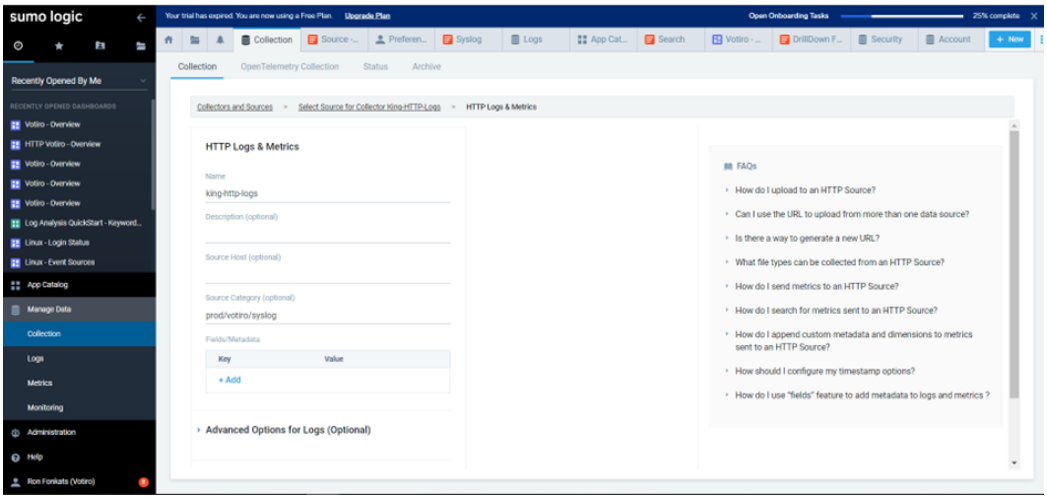


6. In the **HTTP Logs & Metrics** screen:

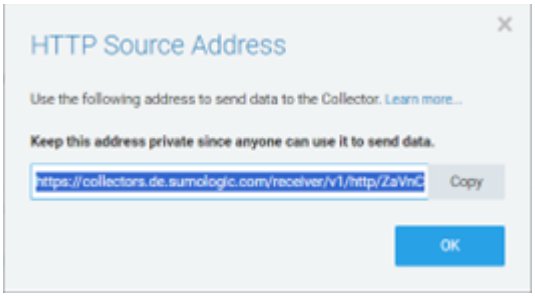
   a. Type a **Name**.

   b. Set the **Source Category** to **prod/votiro/syslog**.

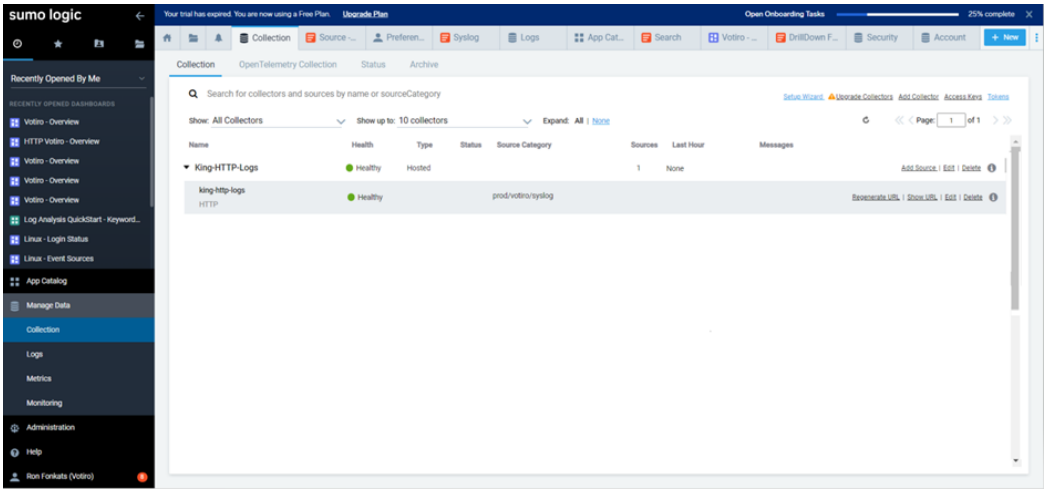
   c. Click **Save**.



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



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



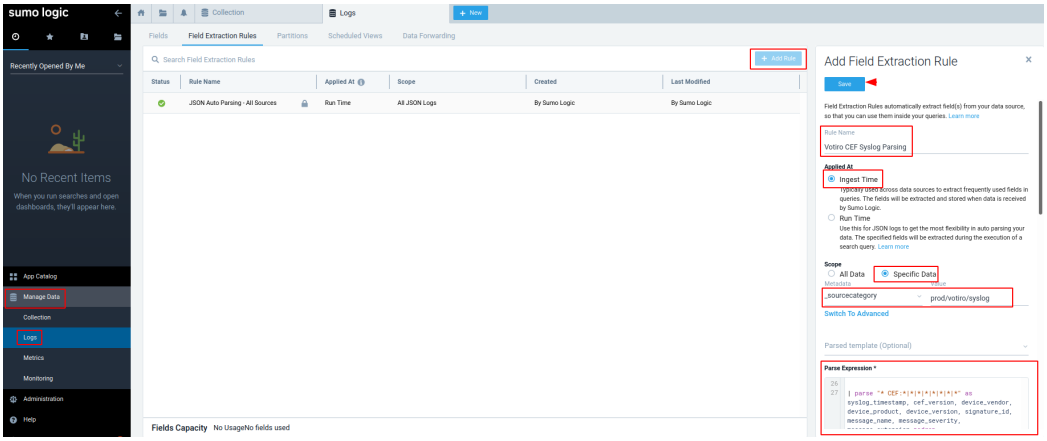
12.1.2 Create the Field Extraction Rules at Ingest Time

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

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

```
| parse regex "companyName=(?<company_name>.*?)\s\w*[=]|$" nodrop
| parse regex "correlationId=(?<correlation_id>.*?)\s\w*[=]|$" nodrop
| parse regex "itemId=(?<item_id>.*?)\s\w*[=]|$" nodrop
| parse regex "fileName=(?<file_name>.*?)\s\w*[=]|$" nodrop
| parse regex "fileType=(?<file_type>.*?)\s\w*[=]|$" nodrop
| parse regex "fileHash=(?<file_hash>.*?)\s\w*[=]|$" nodrop
| parse regex "fileSize=(?<file_size>.*?)\s\w*[=]|$" nodrop
| parse regex "passwordProtected=(?<password_protected>.*?)\s\w*[=]|$"
nodrop
| parse regex "AVResult=(?<av_result>.*?)\s\w*[=]|$" nodrop
| parse regex "threatCount=(?<threat_count>.*?)\s\w*[=]|$" nodrop
| parse regex "blockedCount=(?<blocked_count>.*?)\s\w*[=]|$" nodrop
| parse regex "fileModification=(?<file_modification>.*?)\s\w*[=]|$"
nodrop
| parse regex "sanitizationResult=(?<sanitization_result>.*?)\s\w*[=]|$"
nodrop
| parse regex "sanitizationTime=(?<sanitization_time>.*?)\s\w*[=]|$"
nodrop
| parse regex "connectorType=(?<connector_type>.*?)\s\w*[=]|$" nodrop
| parse regex "connectorName=(?<connector_name>.*?)\s\w*[=]|$" nodrop
| parse regex "connectorId=(?<connector_id>.*?)\s\w*[=]|$" nodrop
| parse regex "policyName=(?<policy_name>.*?)\s\w*[=]|$" nodrop
| parse regex "exceptionId=(?<exception_id>.*?)\s\w*[=]|$" nodrop
| parse regex "incidentURL=(?<incident_url>.*?)\s\w*[=]|$" nodrop
| parse regex "messageId=(?<message_id>.*?)\s\w*[=]|$" nodrop
| parse regex "subject=(?<subject>.*?)\s\w*[=]|$" nodrop
| parse regex "from=(?<from>.*?)\s\w*[=]|$" nodrop
| parse regex "recipients=(?<recipients>.*?)\s\w*[=]|$" nodrop
| parse "* CEF:*|*|*|*|*|*|*|*" as syslog_timestamp, cef_version, device_
vendor, device_product, device_version, signature_id, message_name,
message_severity, message_extension nodrop
| fields - message_extension, cef_version
```

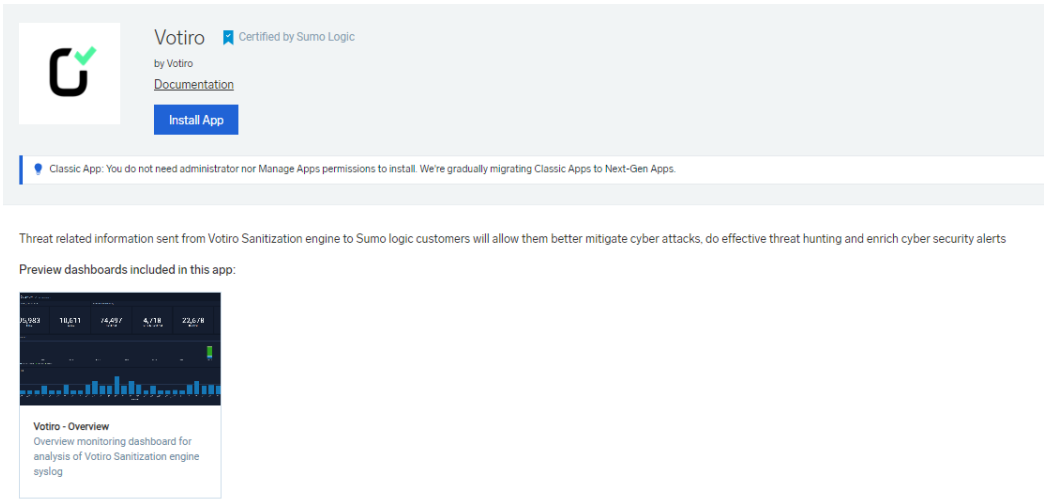
9. Paste the copied rules into the **Parse Expression *** field.



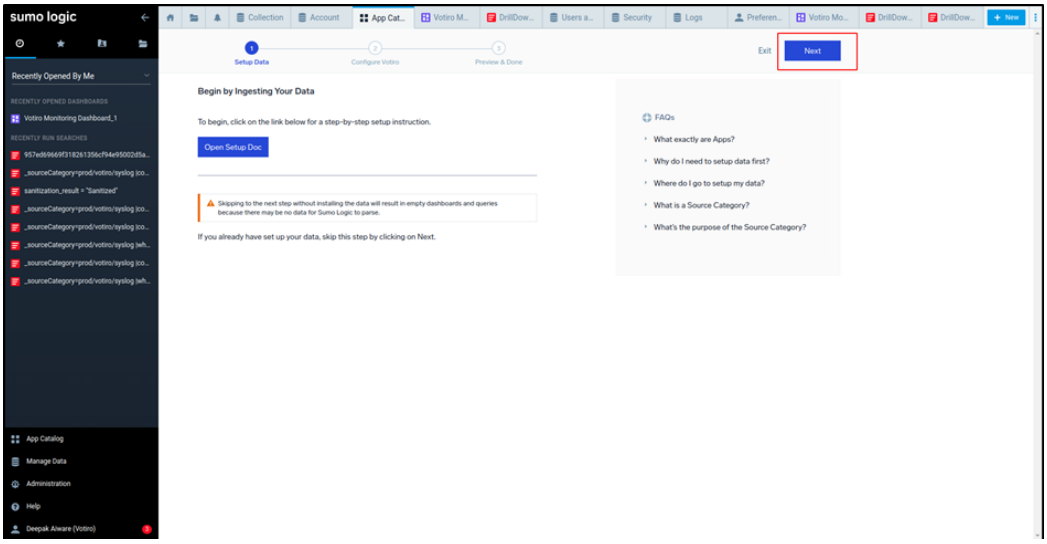
10. Click on the **Save** button.

12.1.3 Install the Votiro App

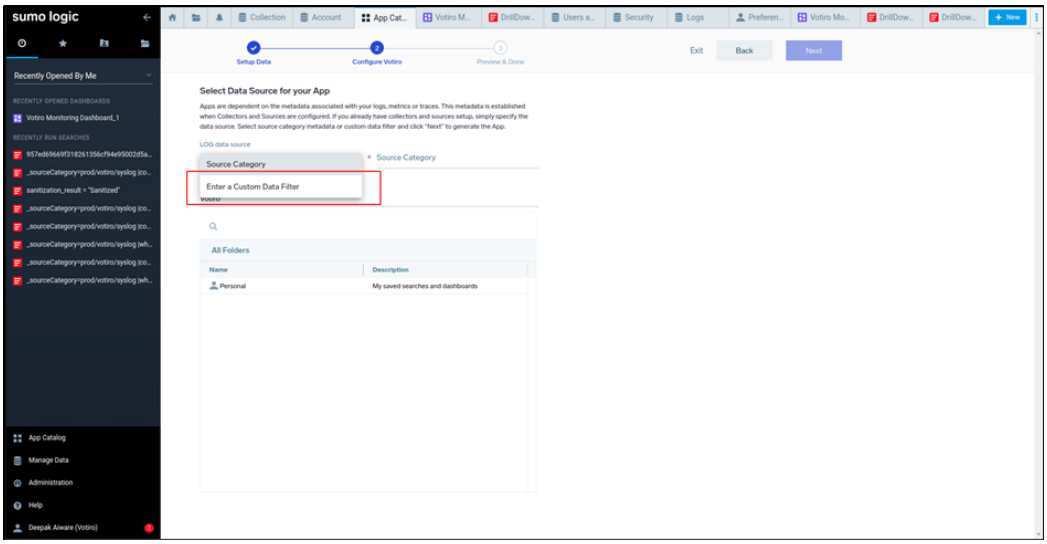
1. Navigate to the **App Catalog** on the Sumo Logic tenant and search for **Votiro**.



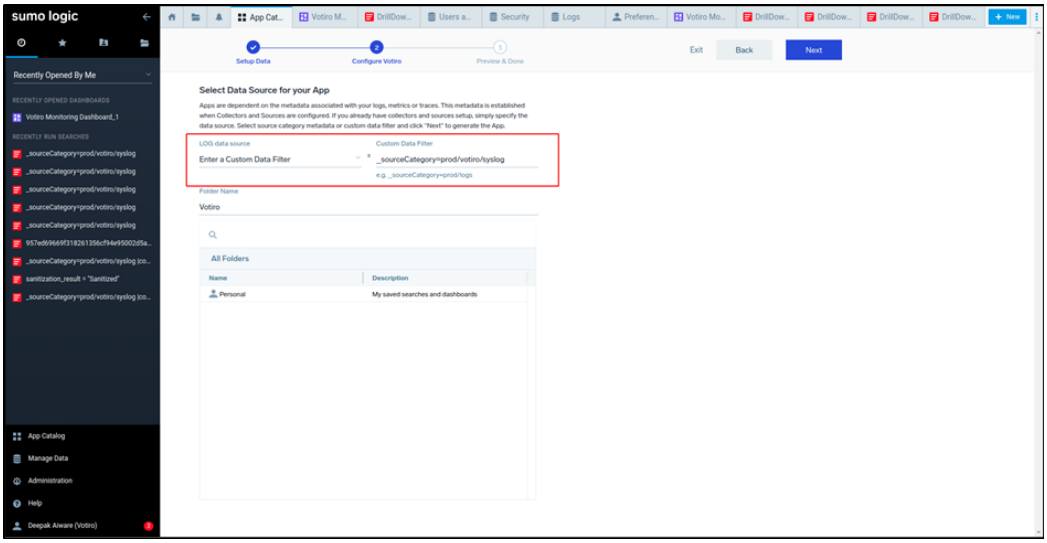
2. Click on **Install App**.
3. After configuring the **collector**, **syslog source** and **extraction rules**, click on **Next**.



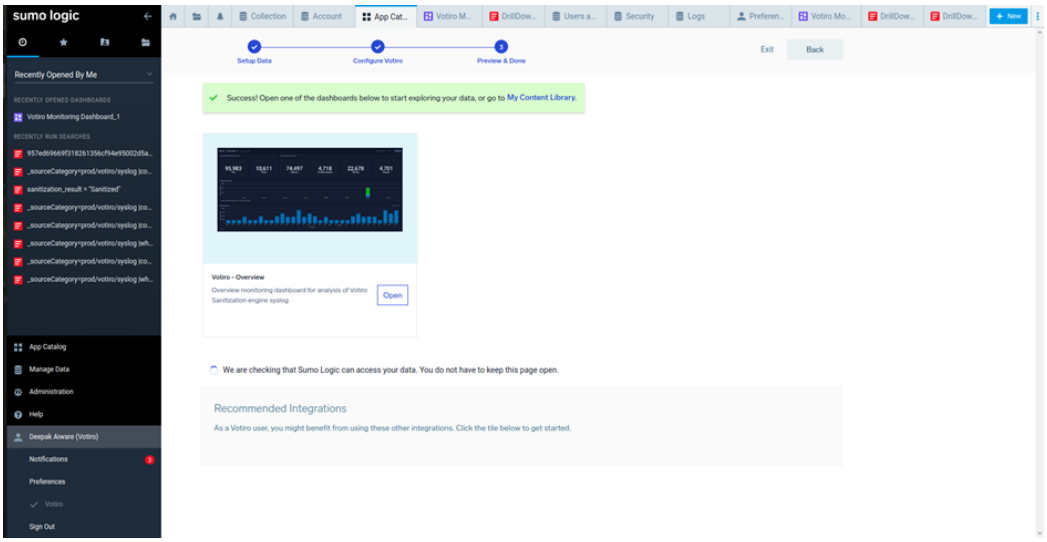
4. Under **LOG data source**, in the **Source Category** field, select **Enter a Custom Data Filter** as you did in the above mentioned steps - use the one that you already created.



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

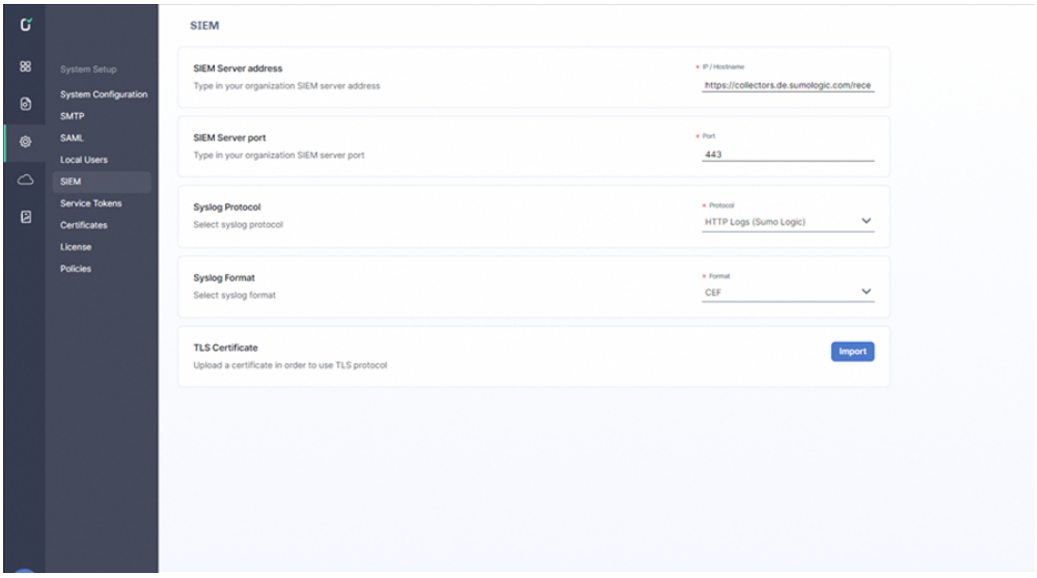


6. Click on **Next**. The Setup completes and a Success message appears and a dashboard is displayed.



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

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



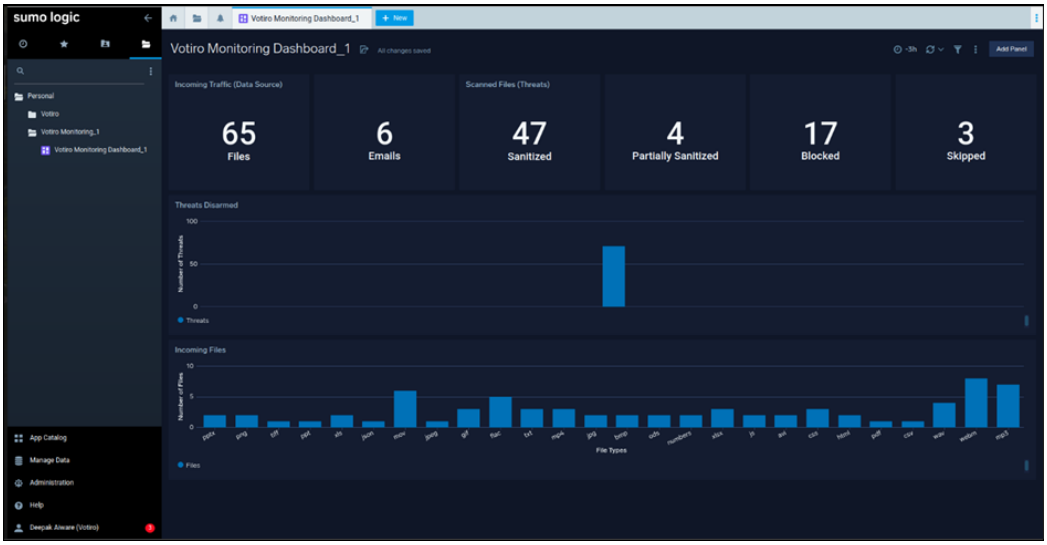
12.1.5 Verify the Integration

To check if the integration was successful:

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

3.a Votiro Dashboard

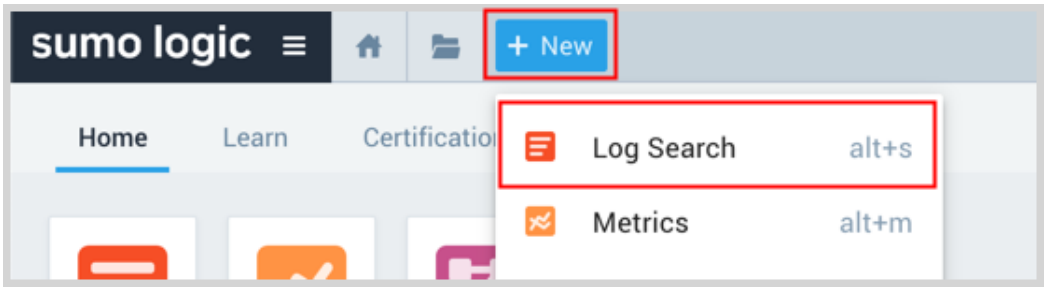
On the Sumo Logic website, open the newly imported folder **Votiro Monitoring Dashboard**. Data coming from the configured source should be shown on this dashboard.



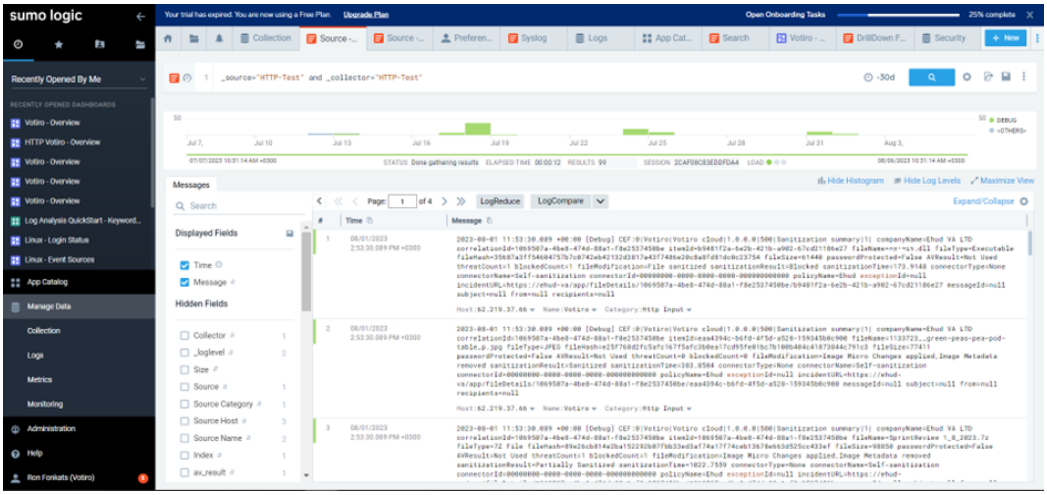
3.b Search Ingested Data inside Sumo Logic

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

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



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.

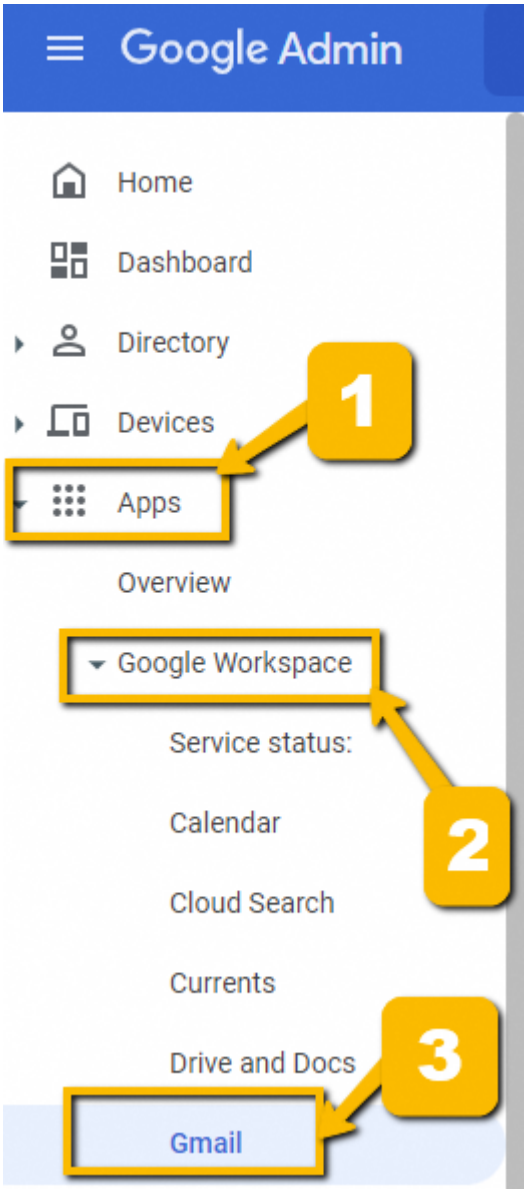

sumo logic
Recently Opened By Me
Votiro - Overview
HTTP Votiro - Overview
Log Analysis QuickStart - Keyword...
Linux - Login Status
Linux - Event Sources
App Catalog
Manage Data
Collection
Logs
Metrics
Monitoring
Administration
Help
Ron Forkats (Votiro)
_source="HTTP-Test" and _collector="HTTP-Test"
Messages
Displayed Fields
Time
Message
Hidden Fields
Collector
_loglevel
Size
Source
Source Category
Source Host
Source Name
Index
av_result

13 How to Integrate Votiro Cloud with Google Workspace

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

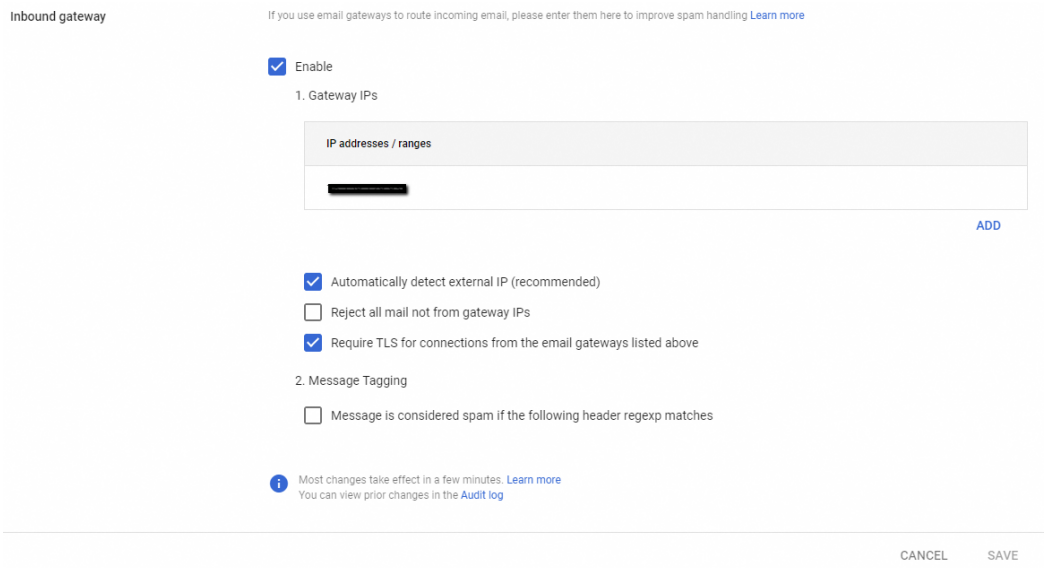
13.1 Procedure

1. Sign in to the 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**

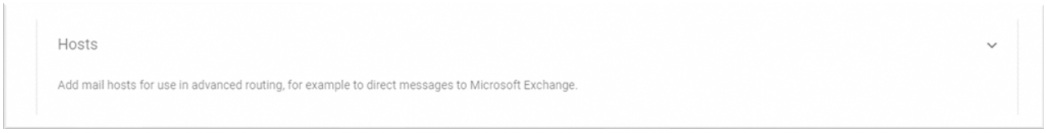
4. Move the cursor over **Inbound gateway** and click the pencil button to edit the settings:



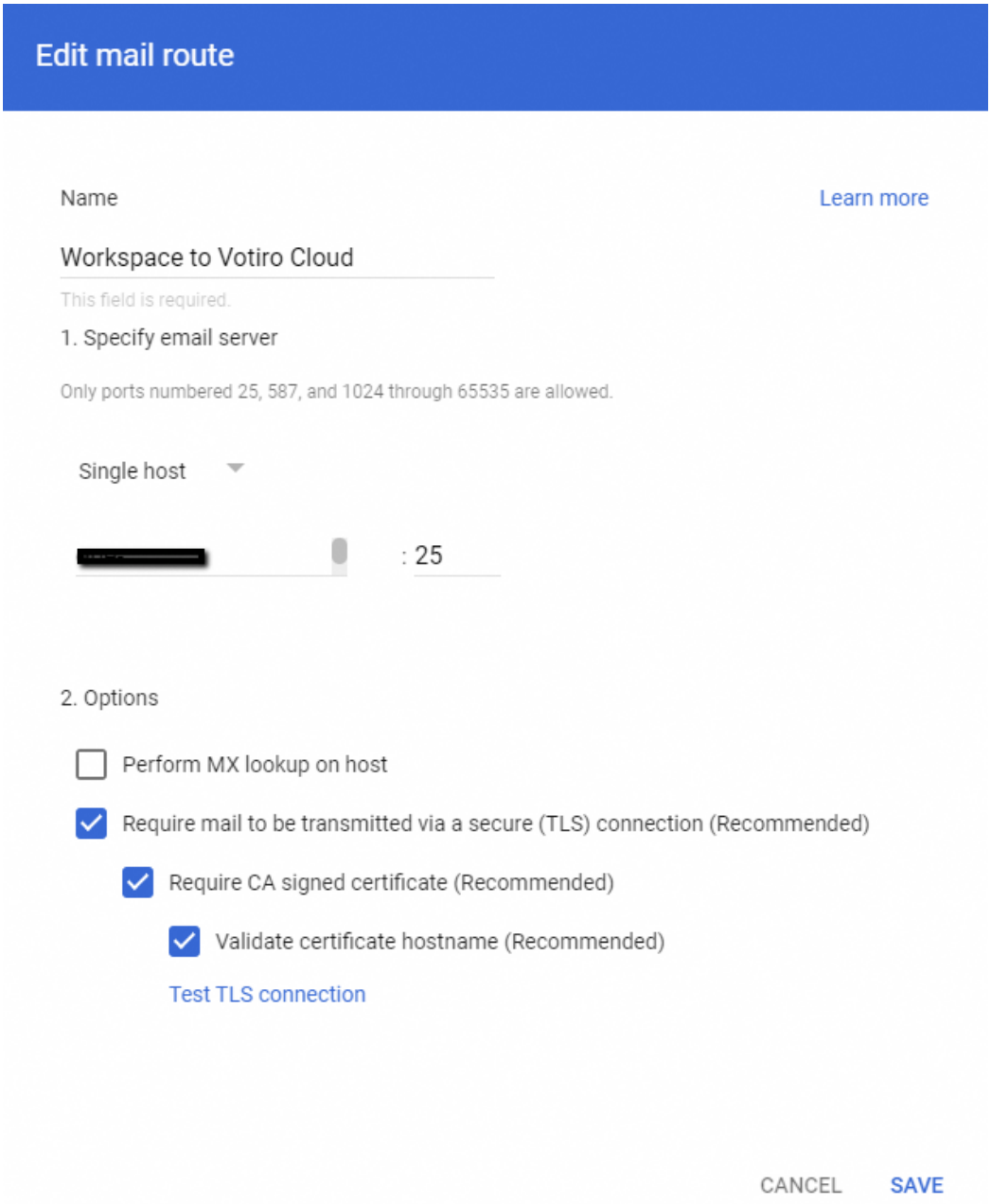
5. Enter the IP address provided by Votiro.
6. Verify that the following boxes are checked:
   - **Automatically detect external IP (recommended)**
   - **Require TLS for connections from the email gateways listed above**
7. Click **SAVE**.

13.1.1 Create a Host

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

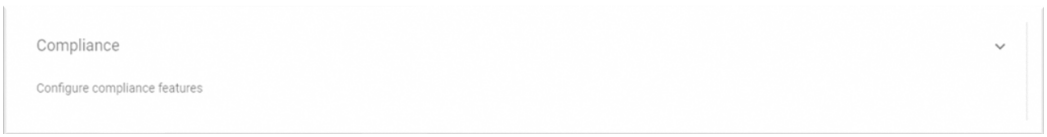


9. Click **Add route**.
   a. Type a name, for example: “Workspace to Votiro Cloud”.
   b. Select **Single host** and type the host name provided by Votiro.
   c. Check **Require mail to be transmitted via secure (TLS) connection (Recommended)**.
   d. Check **Require CA signed Certificate (Recommended)**.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

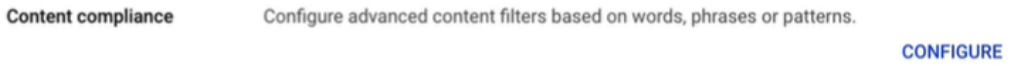


13.1.2 Configure content compliance rule for emails received from Votiro Cloud

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



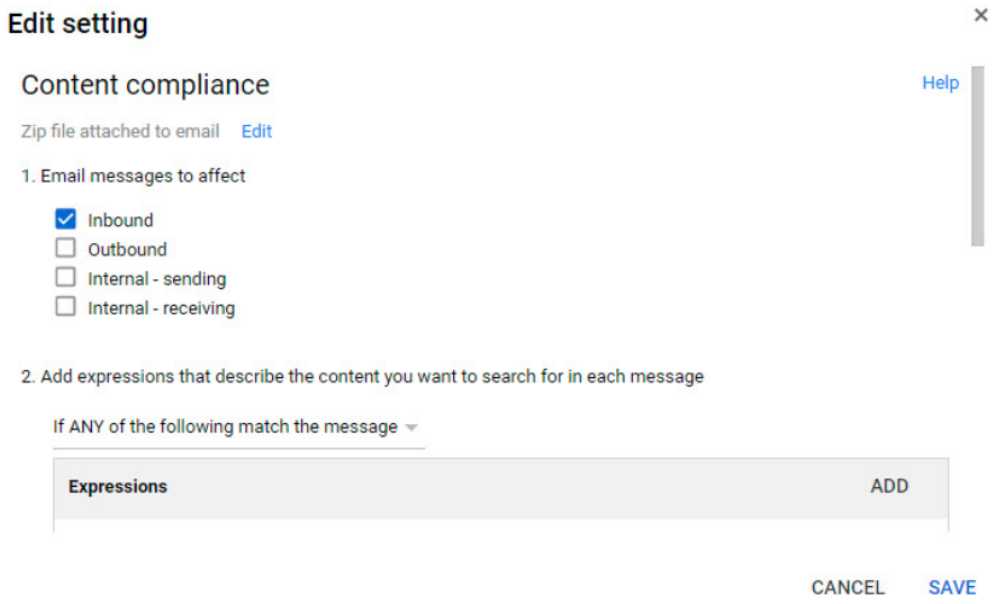
11. Under **Content compliance**, select **CONFIGURE**.



a. Specify a name, for example “Votiro Cloud to Workspace”

b. For **Email messages to affect**, check **Inbound.**

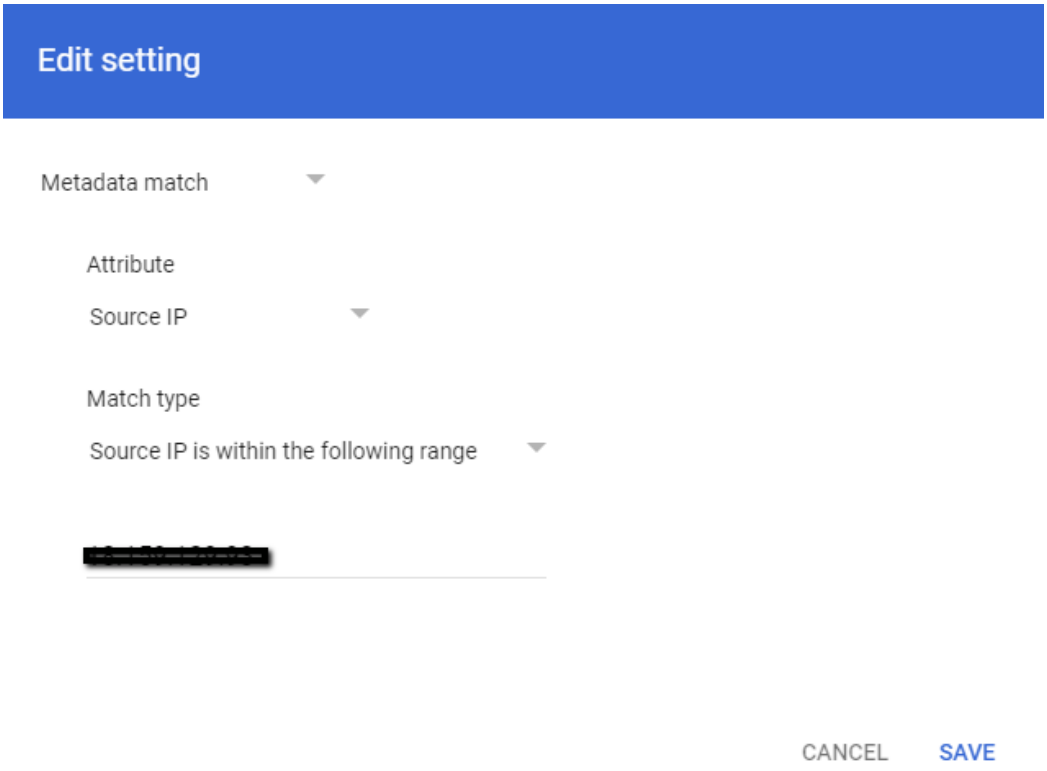
c. For **Add expressions that describe the content you want to search for in each message**, select **If ANY of the following match the message** and click **ADD**.



d. Select **Metadata match**, **Attribute**, **Source IP** and **Match type**.

e. Select **Source IP is within the following range** and enter the IP address provided by Votiro.

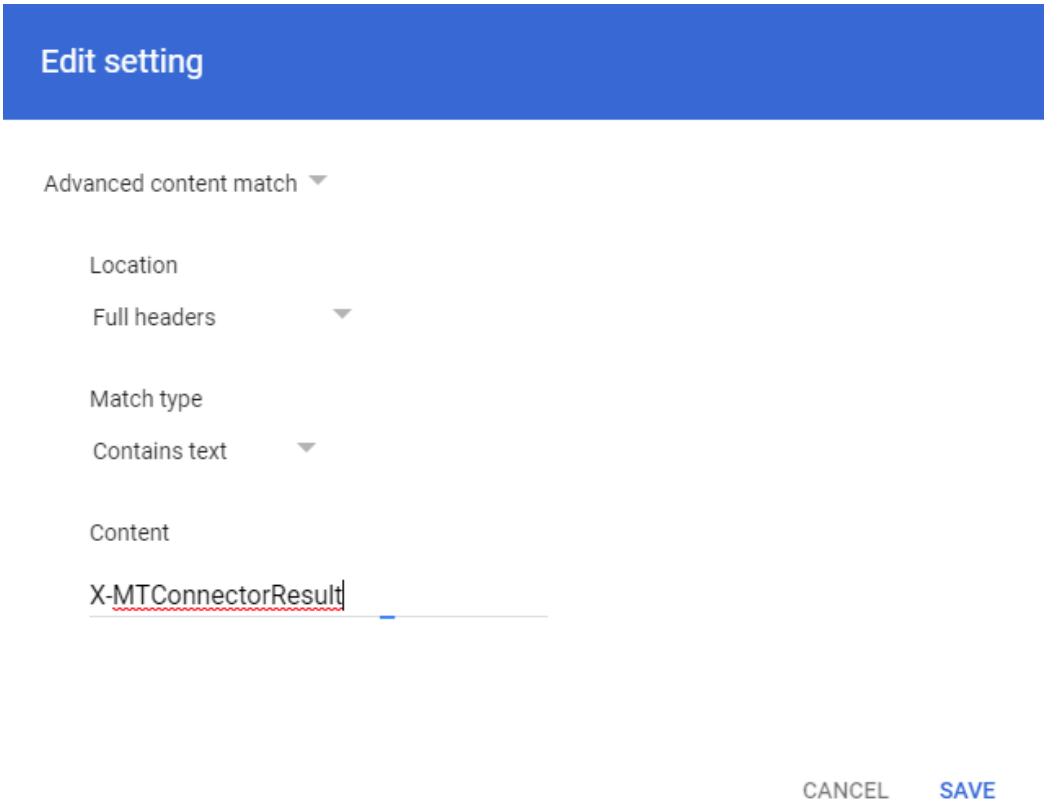
f. Click **SAVE**.



g. Add another expression, select **Advanced content match**, **Location**, **Full headers**, **Match type**, **Contains text**.

h. In **Content**, enter "X-MTConnectorResult".

i. Click **SAVE**.



j. For 3 - If the above expressions match, do the following: Under **Route** select **Change route** and make sure **Normal routing** is selected.

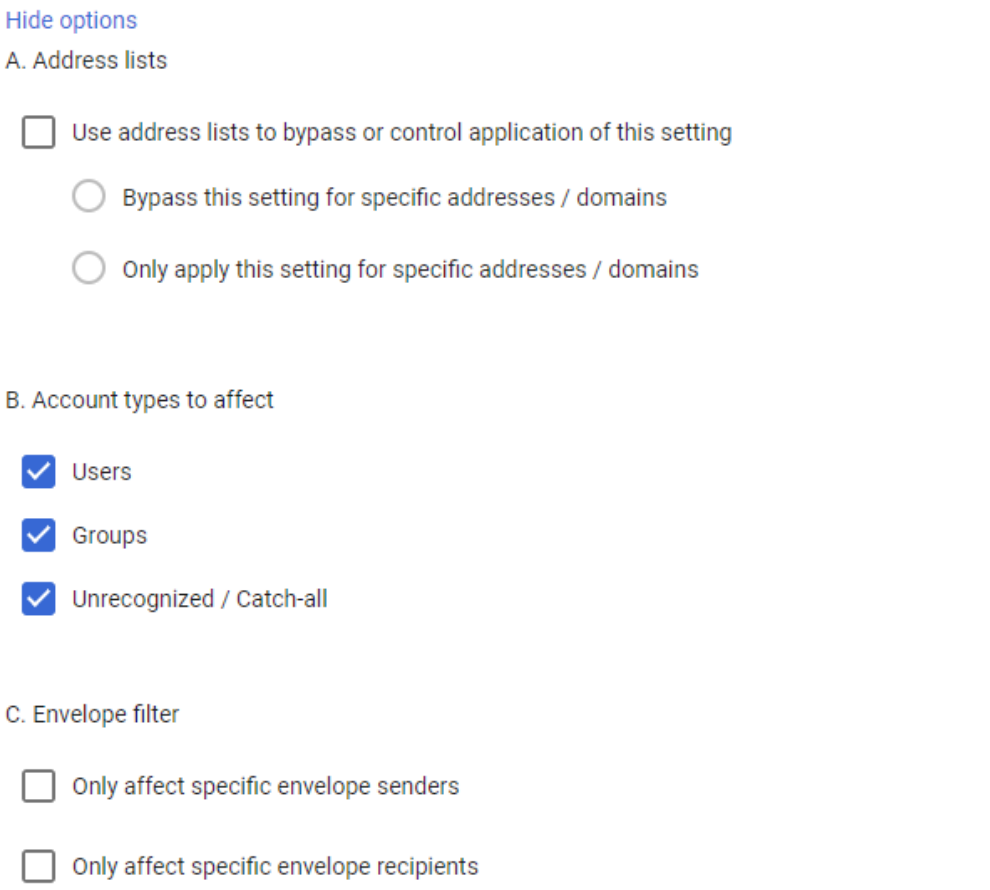
k. Under Encryption, check **Require secure transport (TLS).**

l. Click **Show options**.

   i. Under **Account types to affect**, check the following boxes:

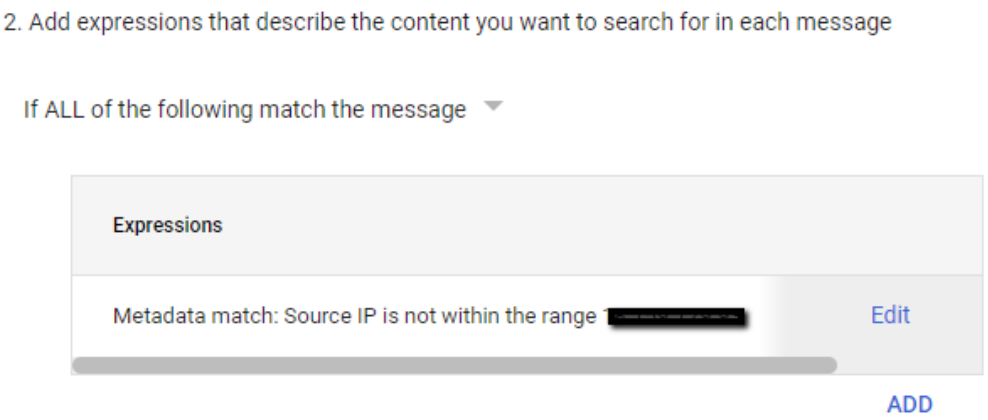
      - **Users**
      - **Groups**
      - **Unrecognized / Catch-all**

   ii. Click **SAVE**.



13.1.3 Configure Content compliance rule for emails sent to Votiro Cloud

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



d. For 3 - If the above expressions match, do the following: Under **Route**, select **Change route** and make sure "Workspace to Votiro Cloud" is selected.

e. Under **Encryption**, check **Require secure transport (TLS)**.

f. Click **Show options**.

i. Under **Account types to affect**, check the following boxes:

- **Users**
- **Groups**
- **Unrecognized / Catch-all**

ii. Click **SAVE**

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

13. After the rules are successfully configured:

a. Send a test email.

b. Under Reporting > Email Log Search, see if the message was routed through Votiro's Cloud instance.

c. Verify you're able to see the sanitized email in Votiro's dashboard.

14 How to Integrate Votiro Cloud with Sumo Logic

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

14.1 System Requirements

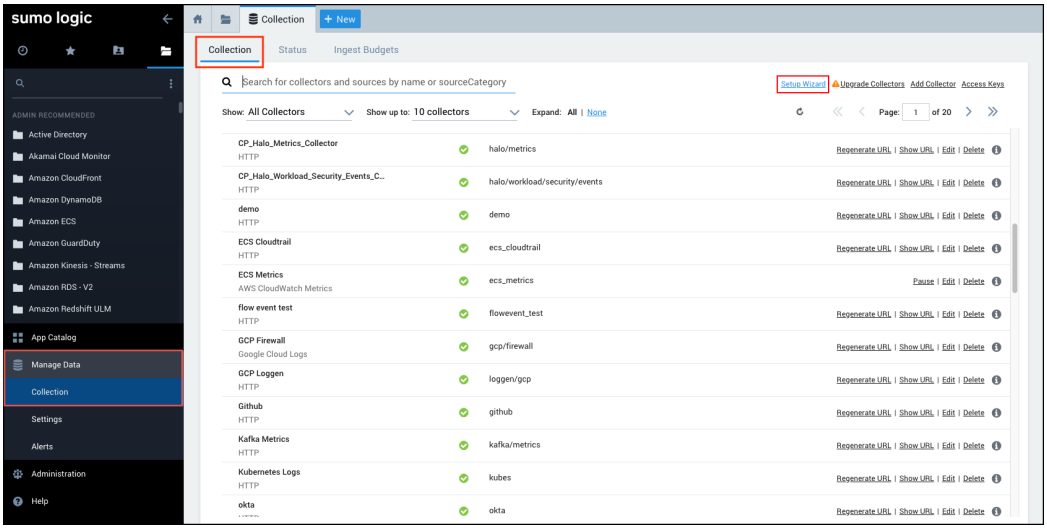
The specifications listed below are for installation of "installed collector" for sending data to the Sumo Logic server.

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

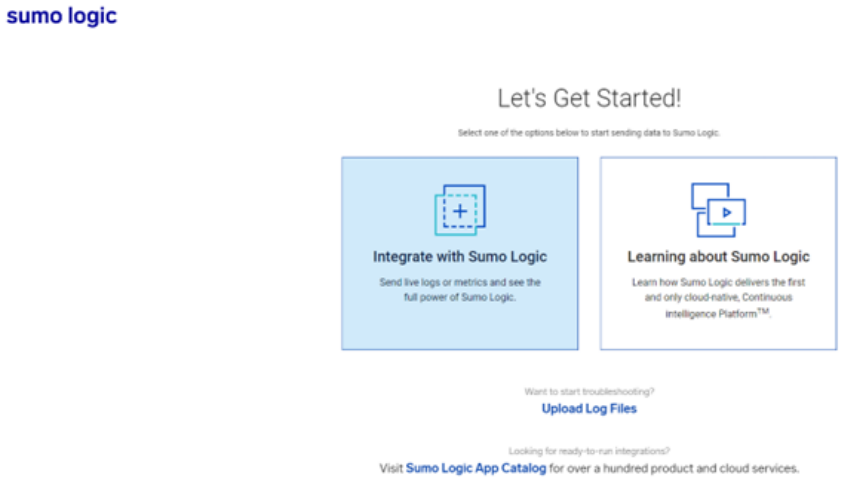
14.2 Procedure

14.2.1 Configure the Sumo Logic Syslog Collection

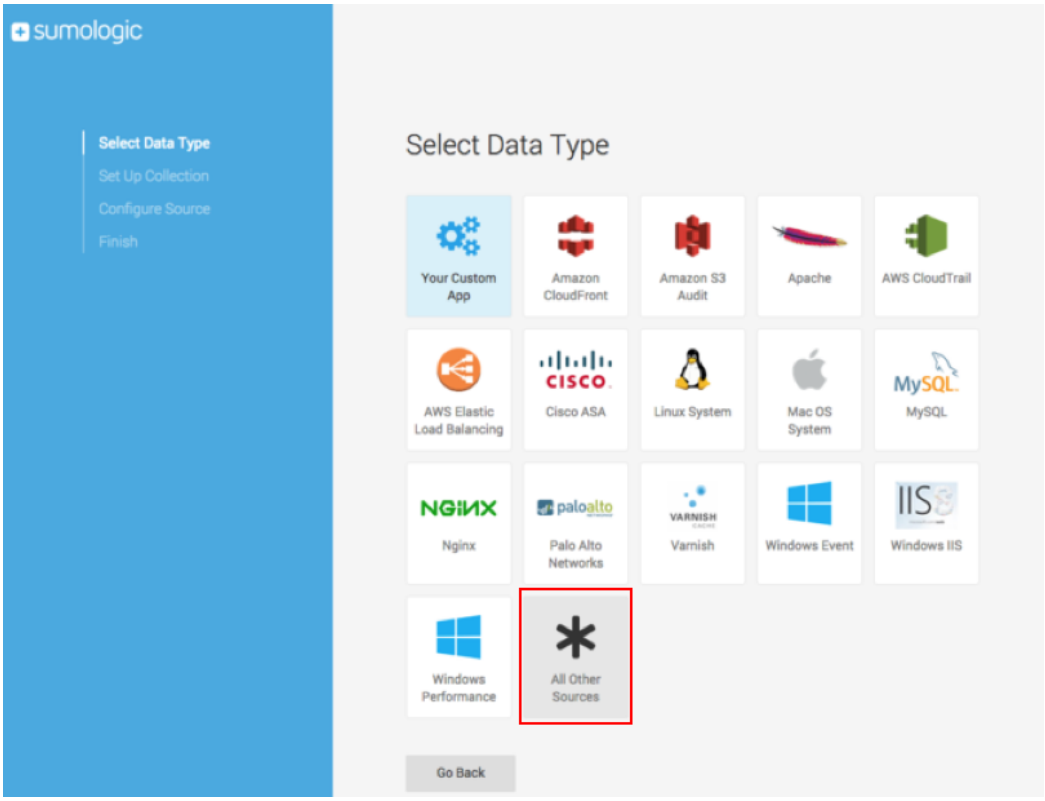
1. In Sumo Logic select **Manage Data > Collection > Collection**.
2. Click on **Setup Wizard**.



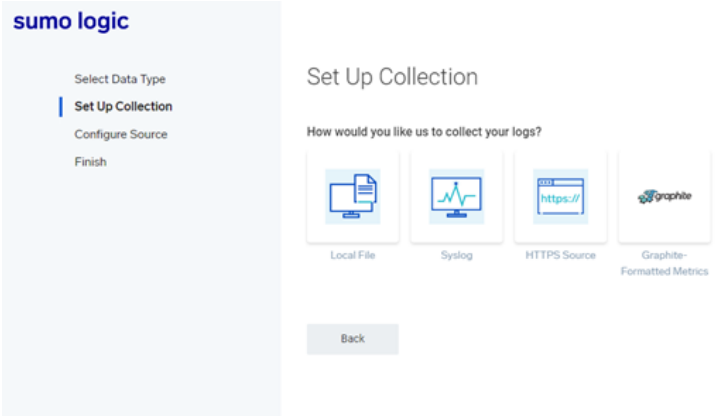
3. Click on **Integrate with Sumo Logic**.



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



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

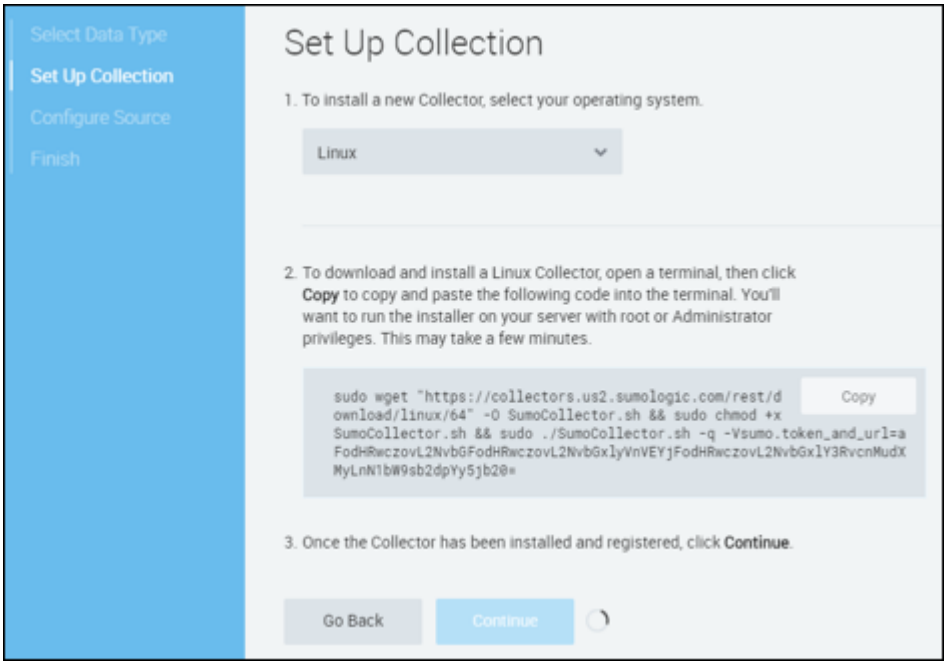


6. Under **Set Up Collection**:

   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**:

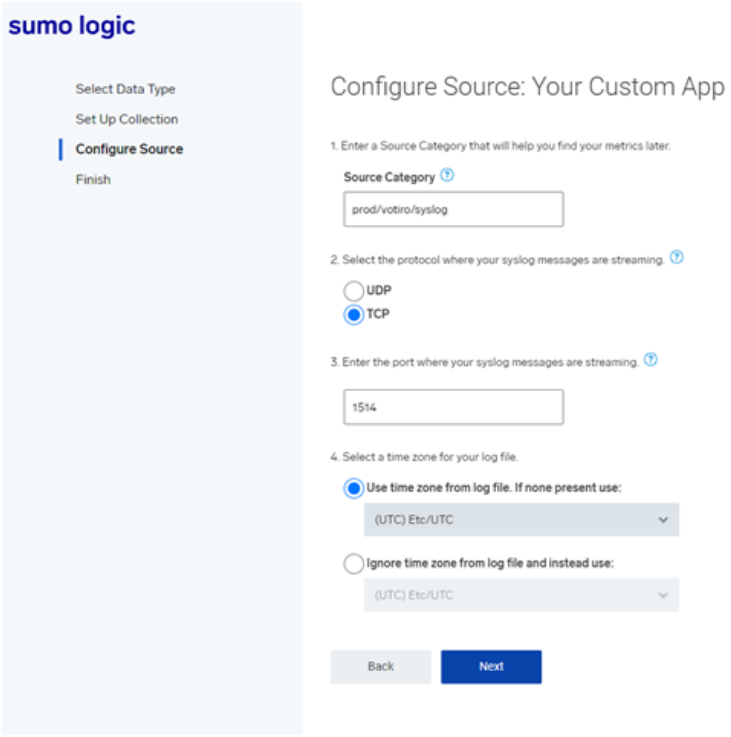
   a. In **1. Enter a Source Category...** field, type the value: **prod/votiro/syslog**.

   b. In **2. Select the protocol...**, select **TCP**.

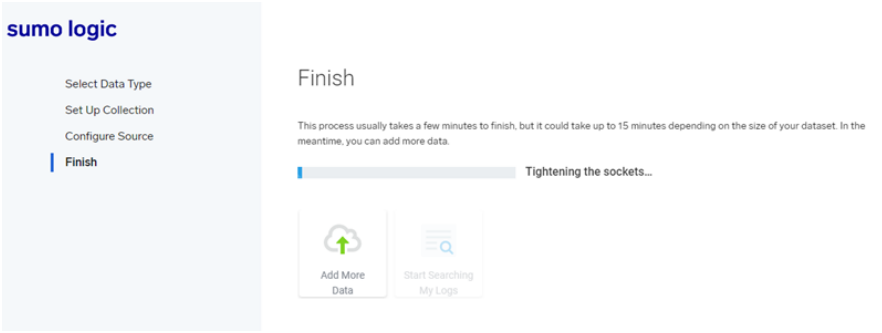
   c. In **3. Enter the port...**, type the value **1514**.

   d. In **4. Select a time zone...**, select **UTC**.

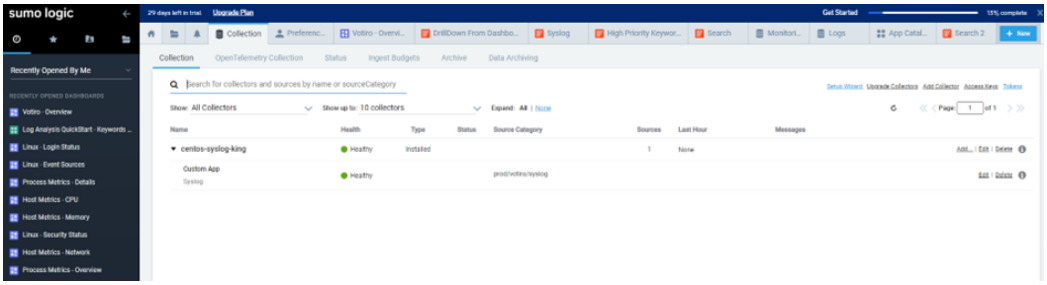
e. Click on **Next**.



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**.



14.2.2 Create the Field Extraction Rules at Ingest Time

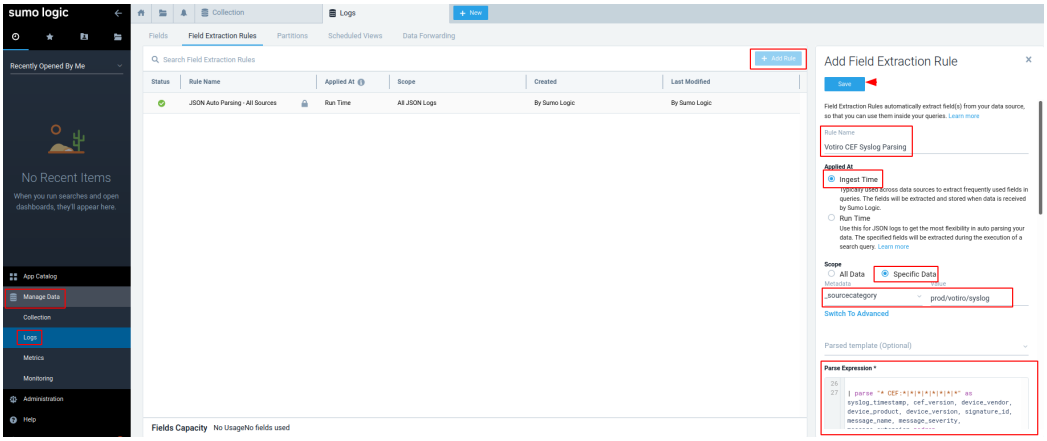
When configuring the Votiro App, the Sumo Logic Admin should perform the following procedure to create field extraction rules at ingest time:

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

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

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

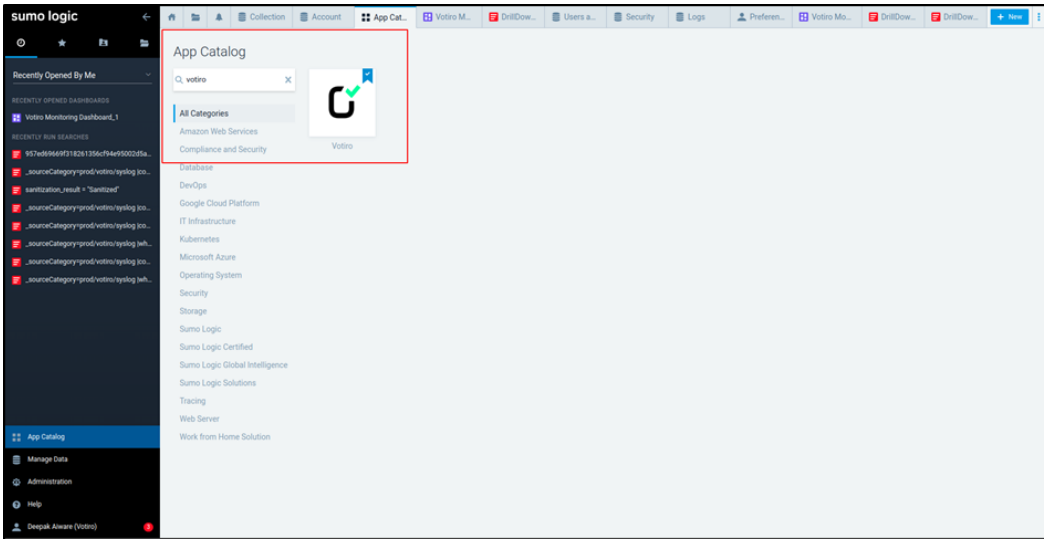
9. Paste the copied rules into the **Parse Expression *** field.



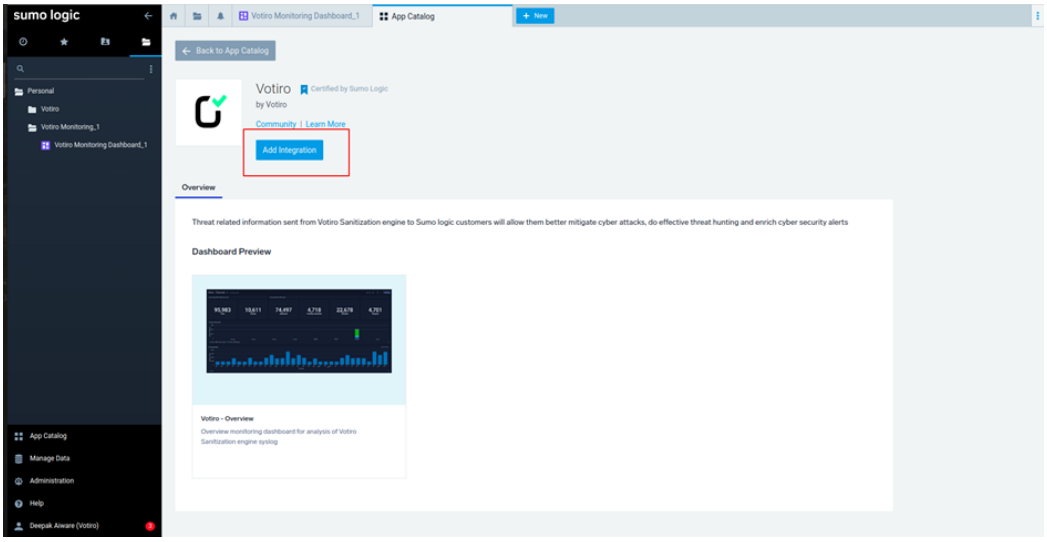
10. Click on the **Save** button.

14.2.3 Install the Votiro App

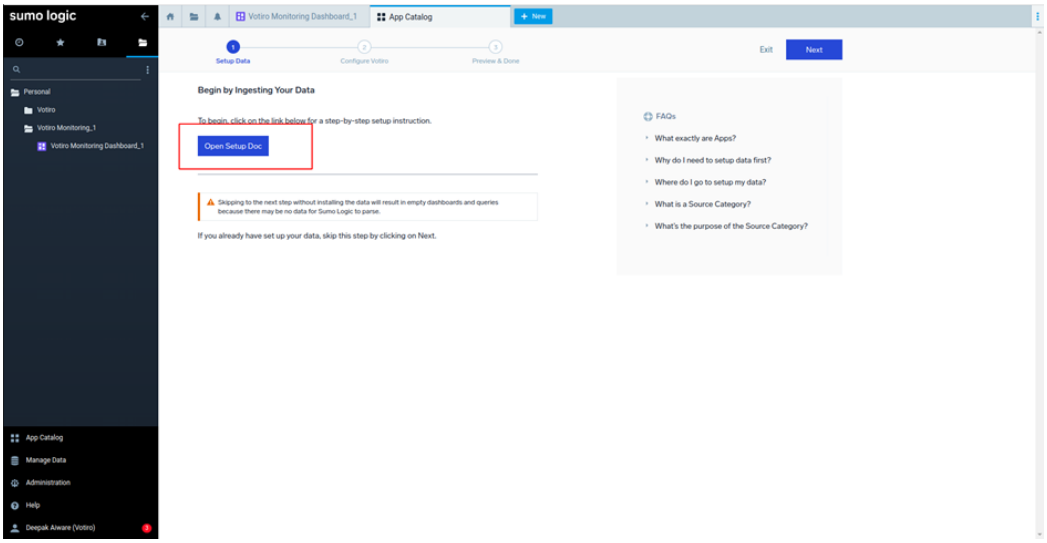
1. Navigate to the **App Catalog** on the Sumo Logic tenant and search for **Votiro**.



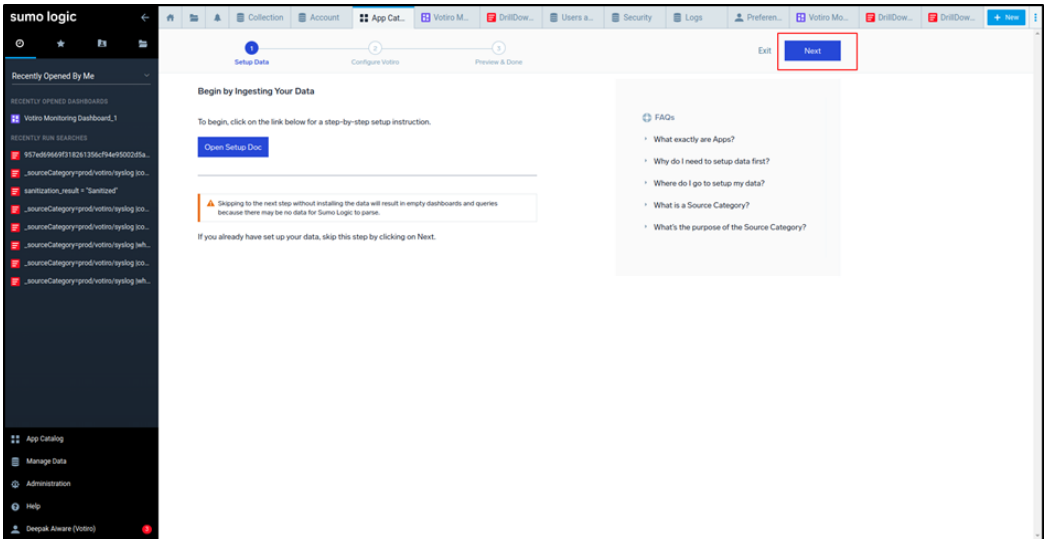
2. Click on **Add Integration**.



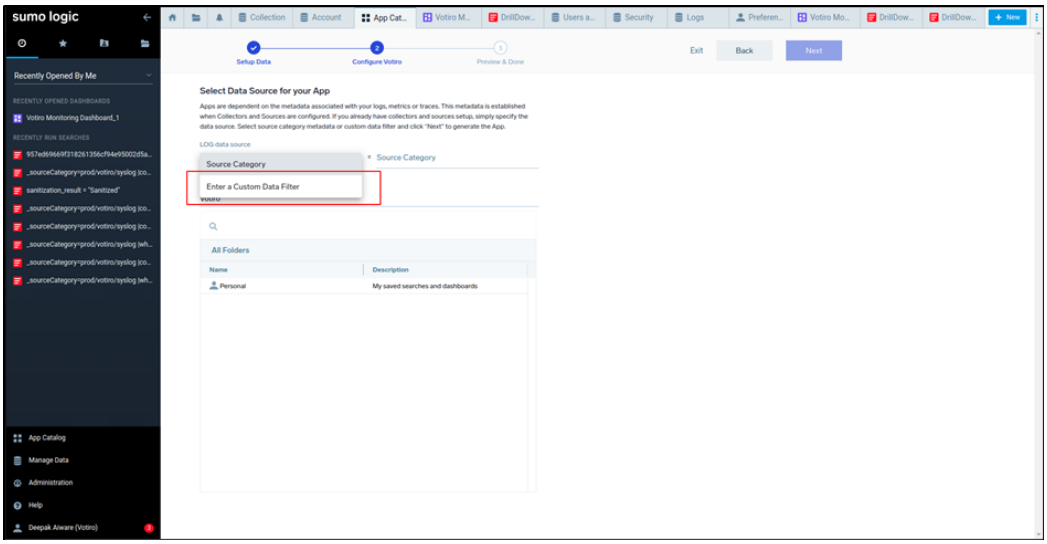
3. Click on **Open Setup Doc**. This will take you to the documentation on the Sumo Logic Github page.



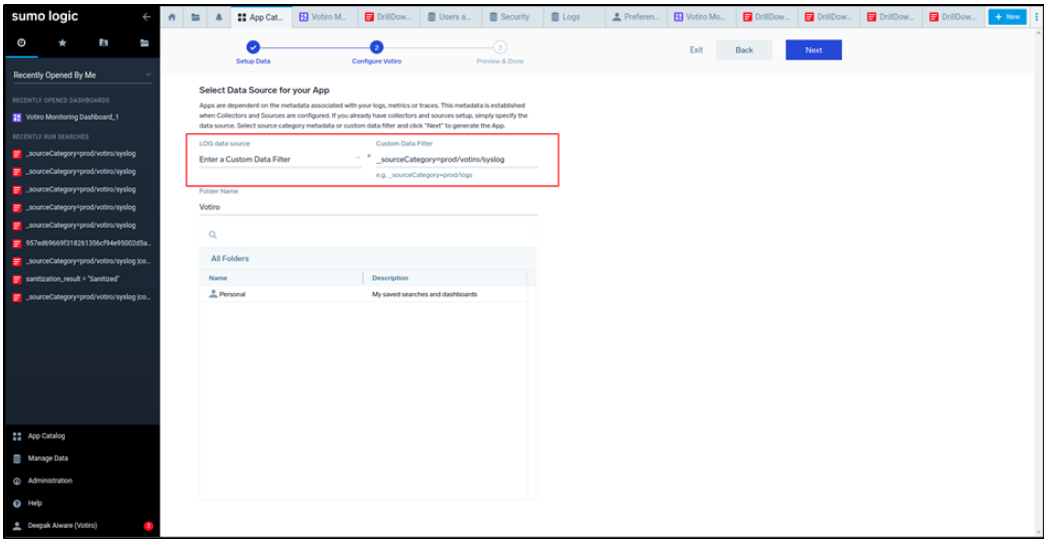
4. After configuring the **collector**, **syslog source** and **extraction rules** with the help of the Setup Doc, click on **Next**.



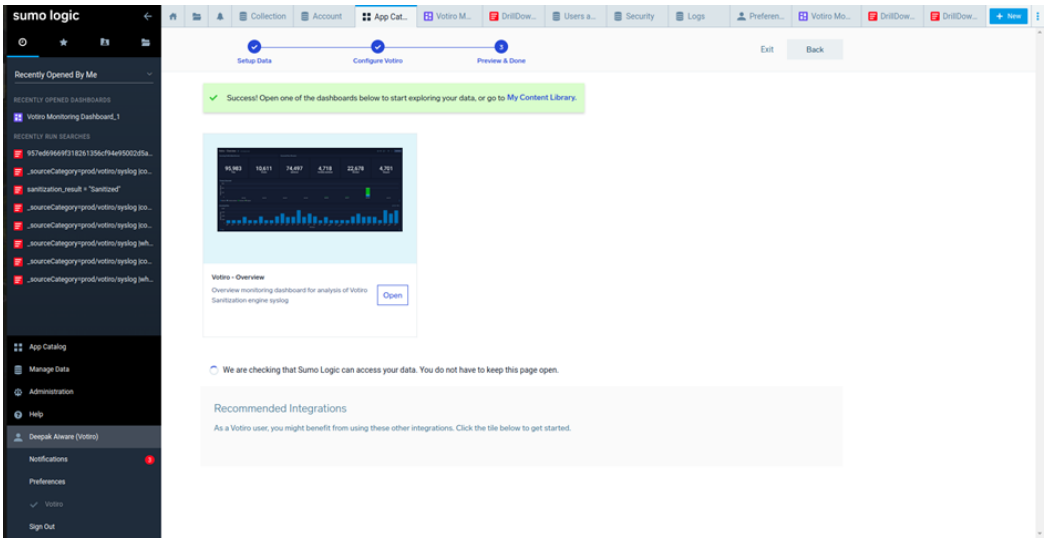
5. Under **LOG data source**, in the **Source Category** field, select **Enter a Custom Data Filter** as you did in the above mentioned steps - use the one that you already created.



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

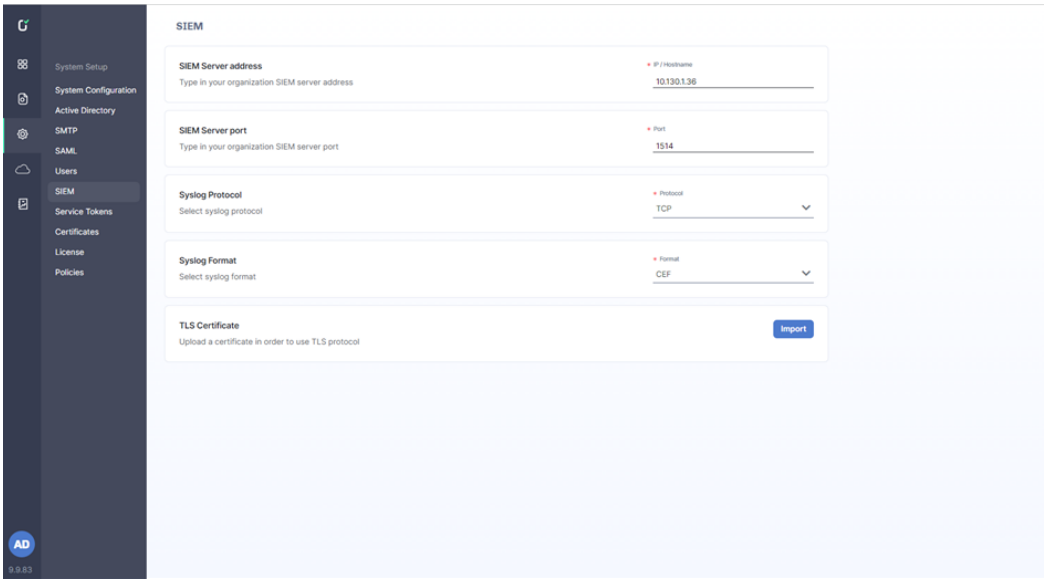


7. Click on **Next**. The Setup completes, a Success message appears and a dashboard is displayed.

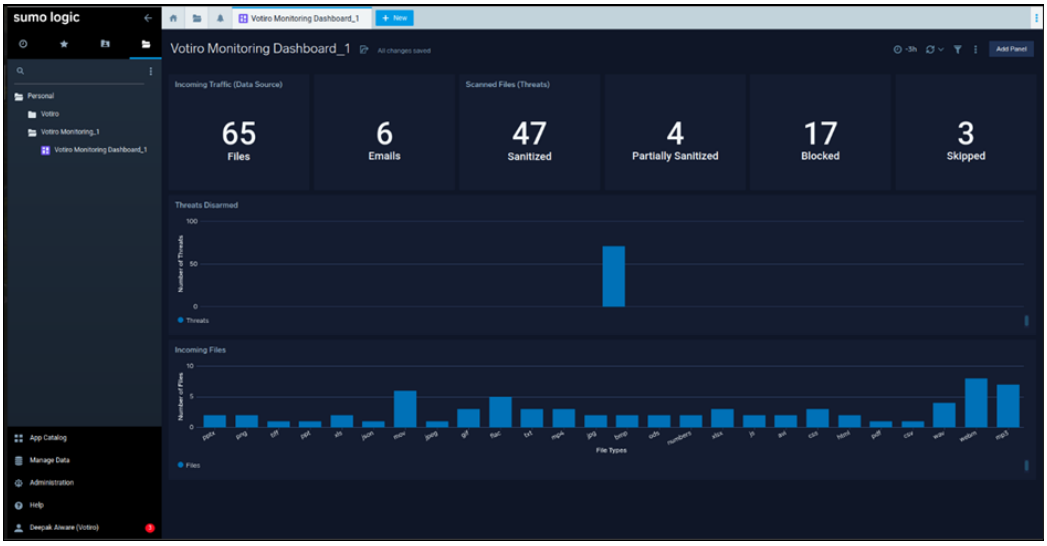


14.2.4 Integrate Votiro Management Console with Sumo Logic Syslog Collector

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



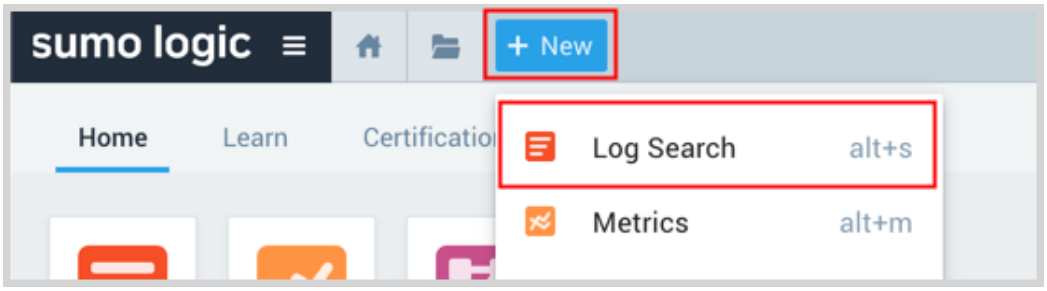
4. On the Sumo Logic website, open the newly imported folder **Votiro Monitoring Dashboard**. Data coming from the configured source should be shown on this dashboard.



14.2.5 Search Ingested Data inside Sumo Logic

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

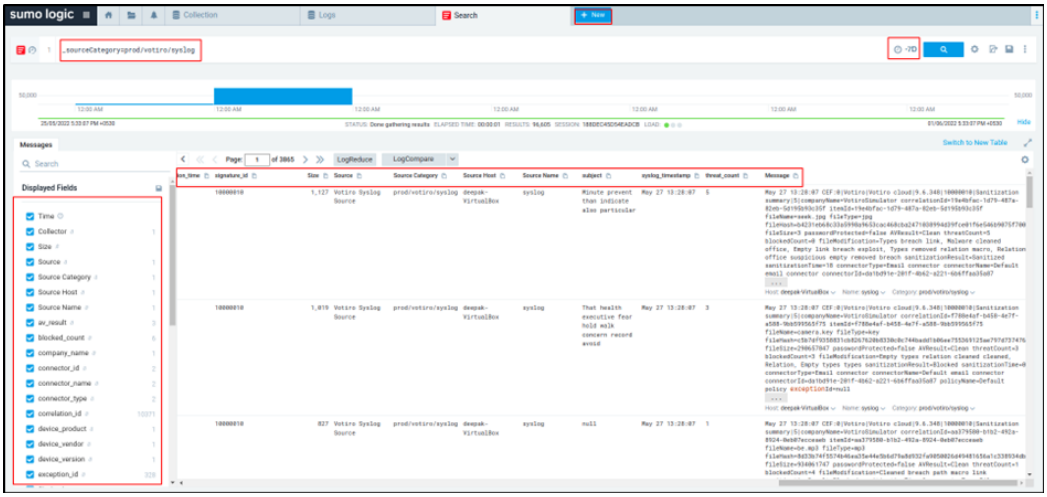
1. Login to the tenant.
2. Click **+ New -> Log Search**.



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.



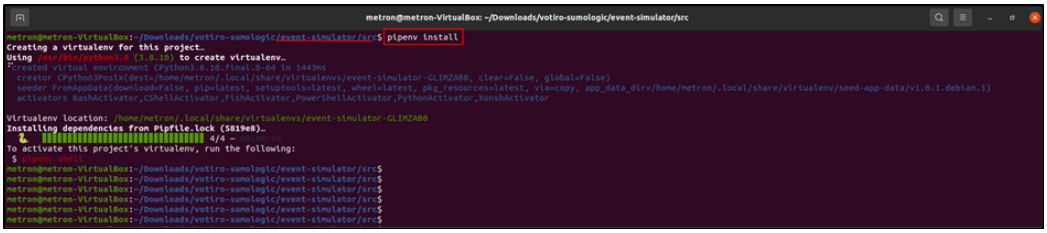
14.2.6 Event Simulator

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

Prerequisites

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

  ```
  pipenv install
  ```



Using the simulator

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

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

   The *<target_port>* and *<target_ip>* should be of the target machine for which the Configuration was done. For example:

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

15 Performing a Health Check

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

```
#./healthcheck
```

The expected results are:

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

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

16 How to Send Files to Votiro via Postman

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

16.1 Prerequisites

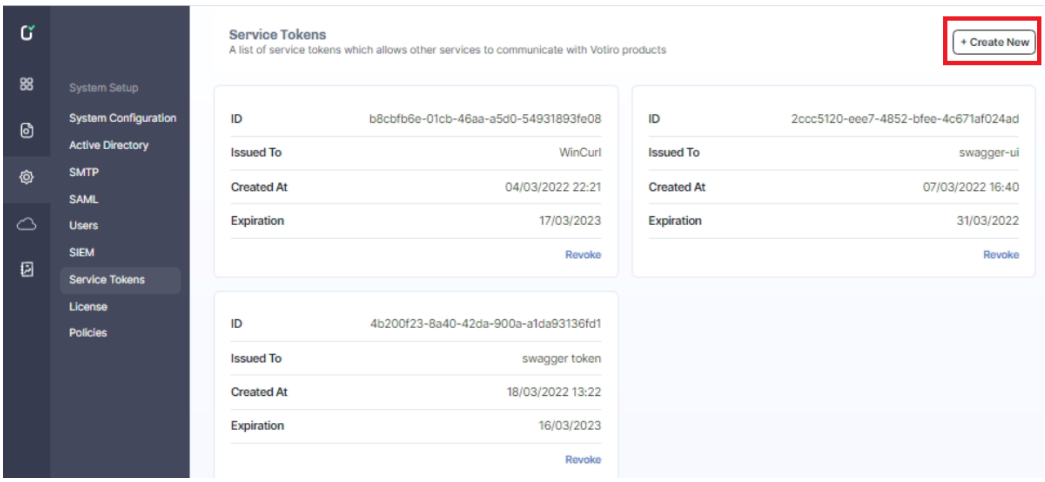
Install Postman by downloading one of the following:

- The Postman app from Download Postman.
- The Postman portable app from Postman™ portable.

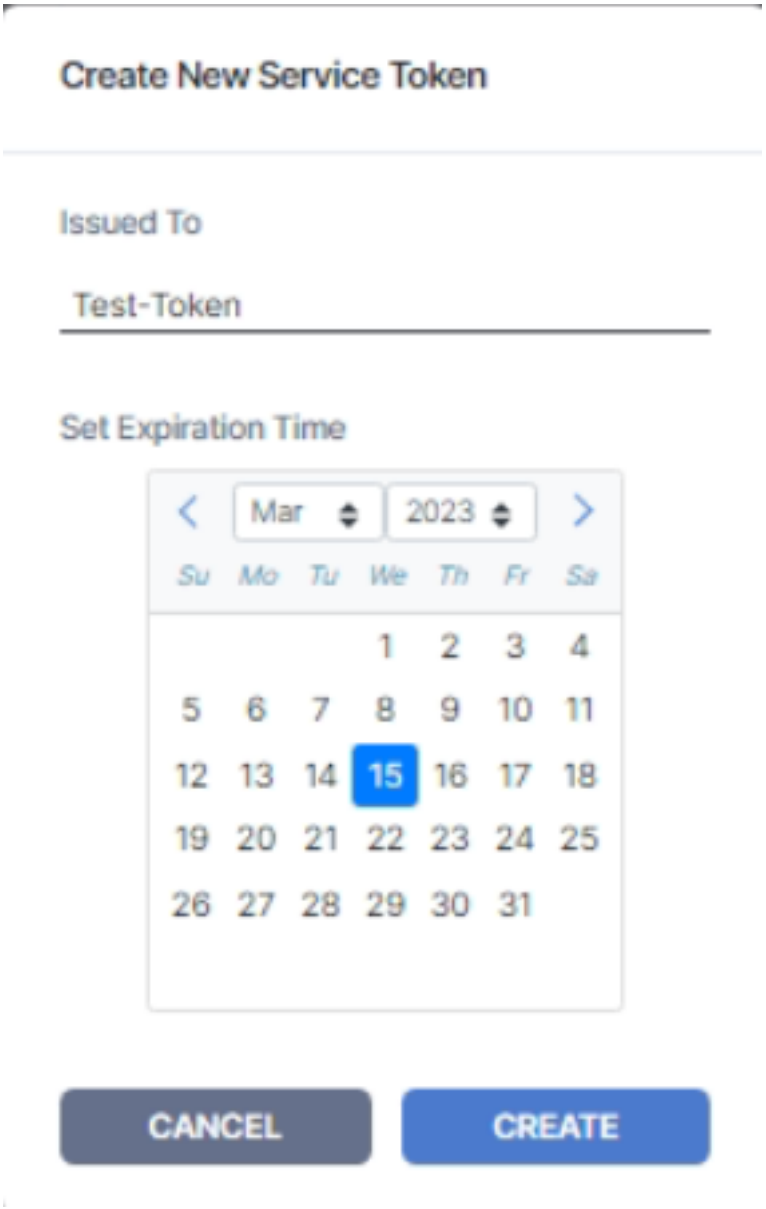
16.2 Procedure

16.2.1 Generating a Service Token

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



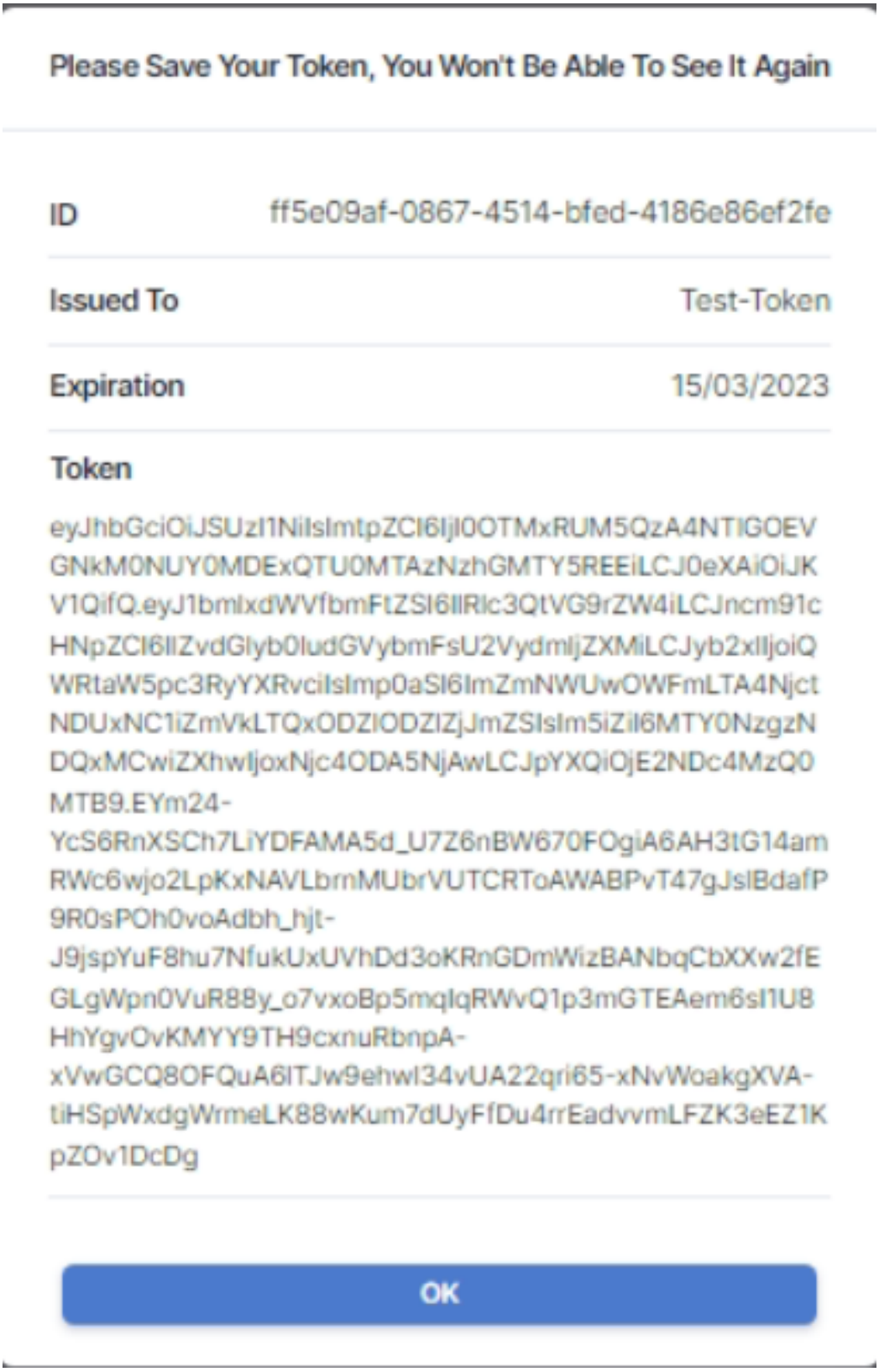
2. Create a name for the new token, set an expiration date and press **CREATE**:



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

WARNING!

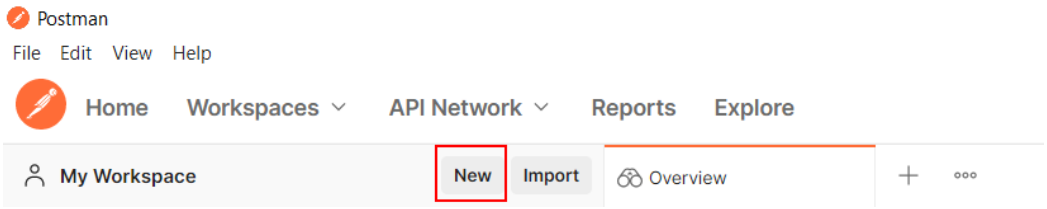
Save the token string. This page will only appear once.



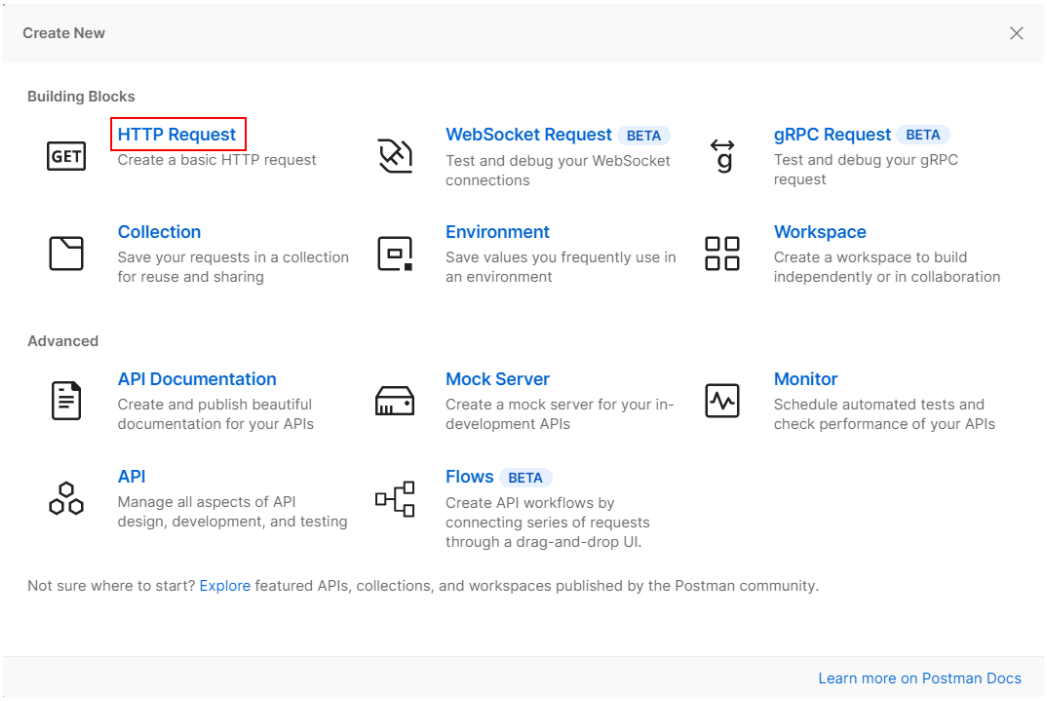
4. Press **OK** to close the Token window.

16.2.2 Postman Setup

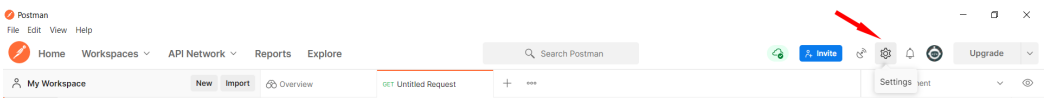
1. In the Postman app, go to **Workspaces** > **My Workspace** and press **New**:



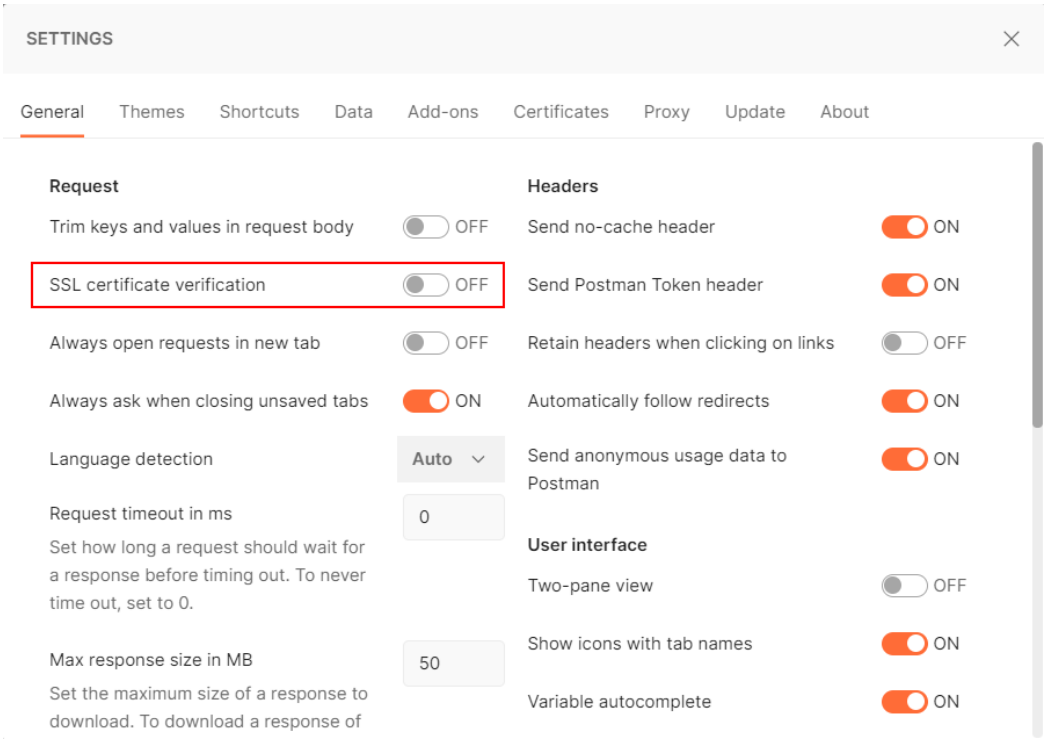
2. The **Create New** window opens. Select **HTTP Request**:



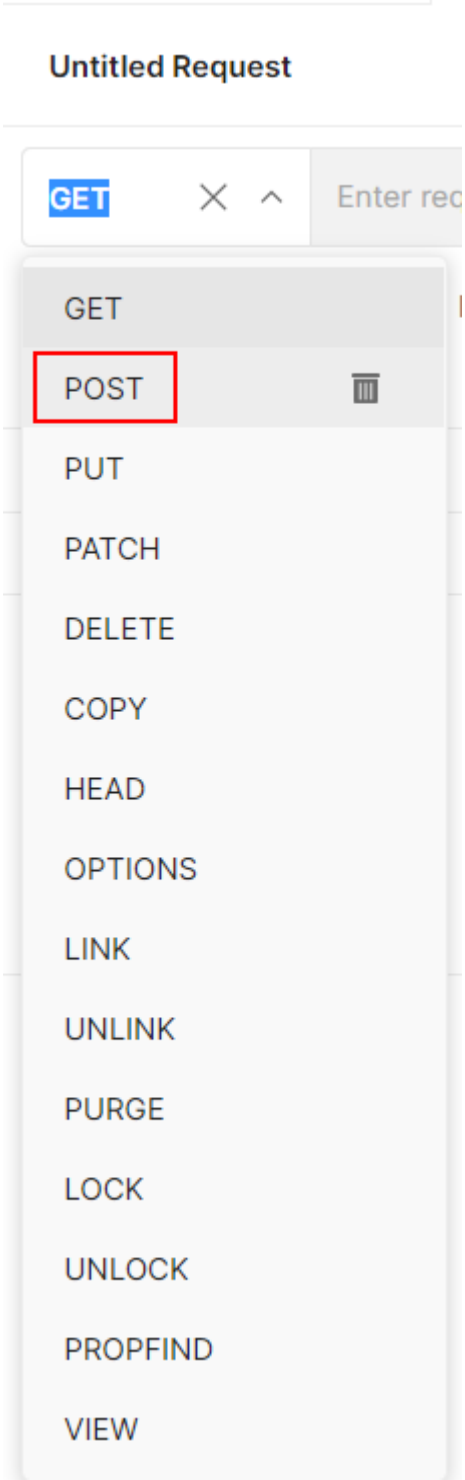
3. Press the Settings icon:



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**:



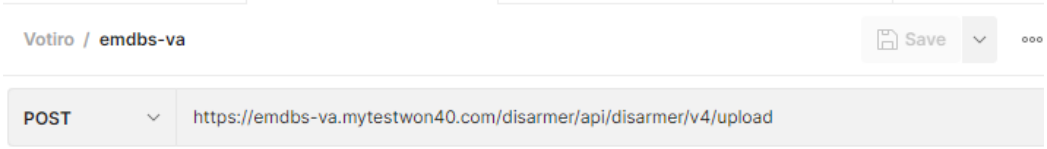
5. Close the **Settings** window.
6. Under the **Untitled Request** dropdown box, select **POST**:



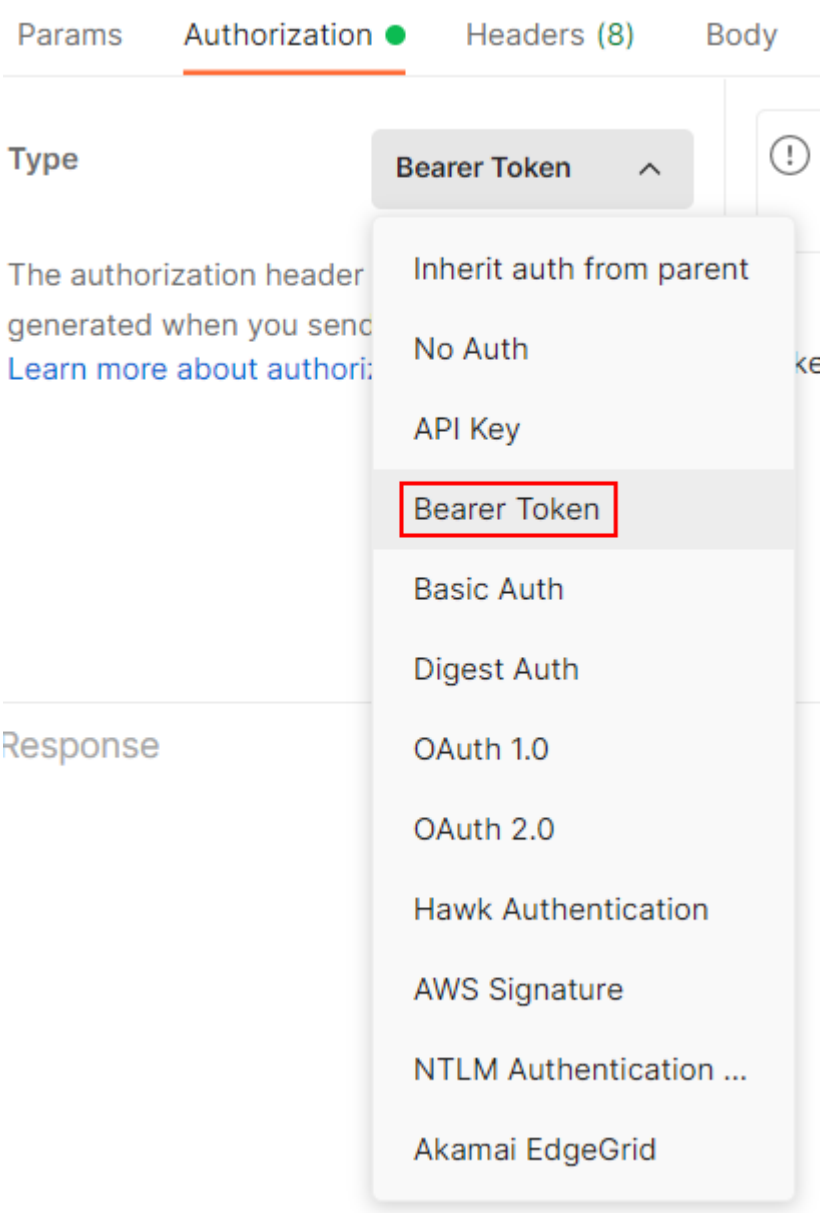
7. In the **Enter request URL** box, enter your VA FQDN in the following format:

   `https://<VA-FQDN>/disarmer/api/disarmer/v4/upload`

For example:

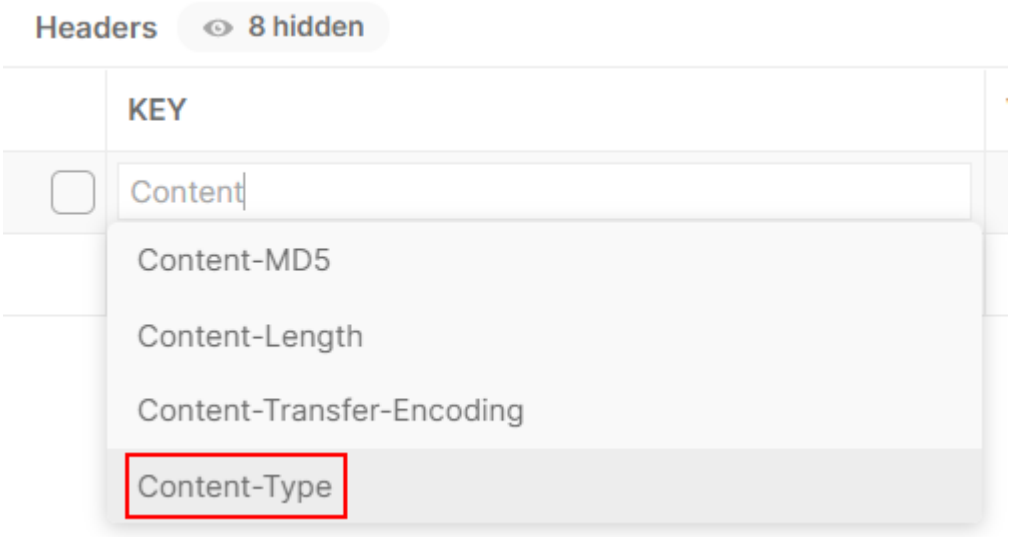


8. Select the **Authorization** tab and under the **Type** dropdown, select **Bearer Token**:

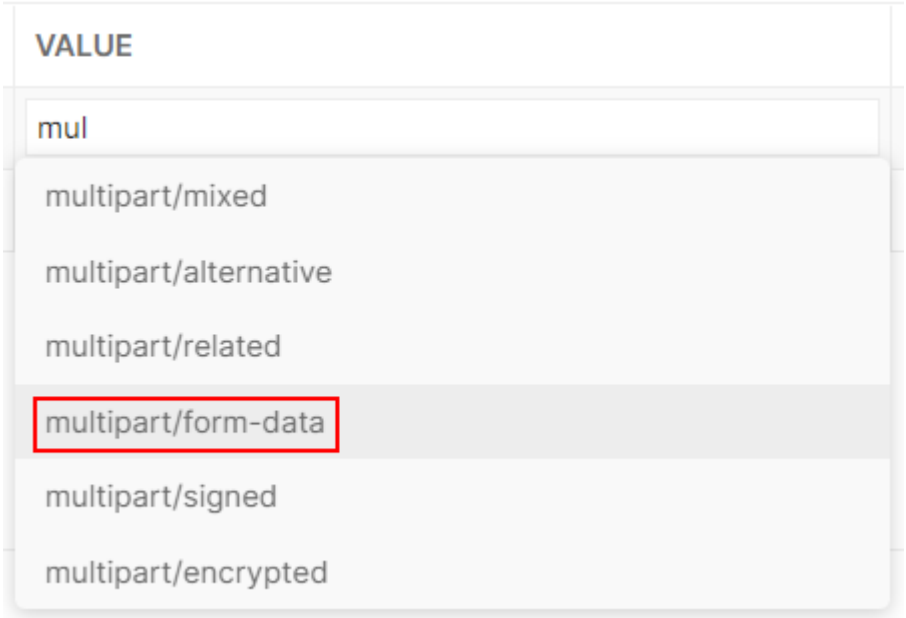


9. Select the **Headers** tab.

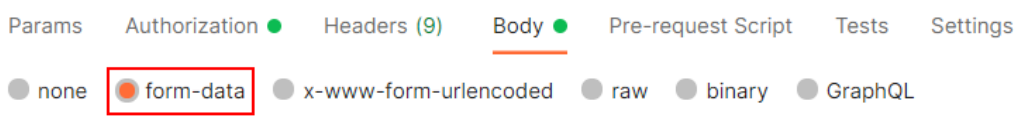
10. In the first row of the **Key** column, start to type **Content** until a dropdown list appears. Then select **Content-Type** from the dropdown list:



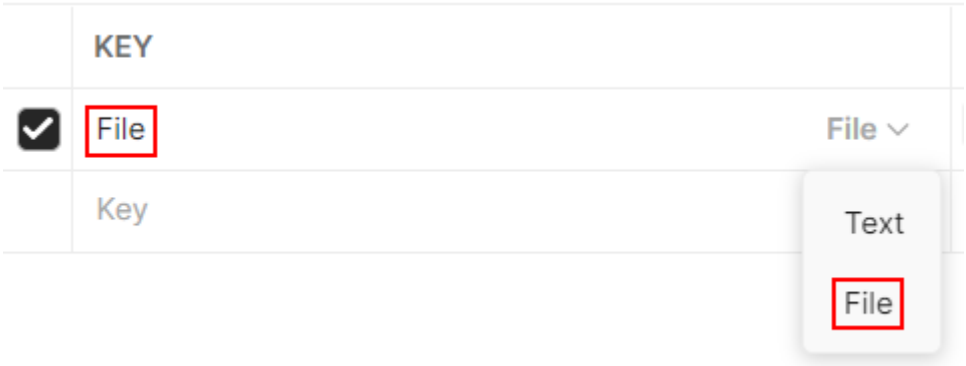
11. In first row of the **Value** column, start to type **multipart** until a dropdown list appears. Then select **multipart/form-data** from the dropdown list:



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



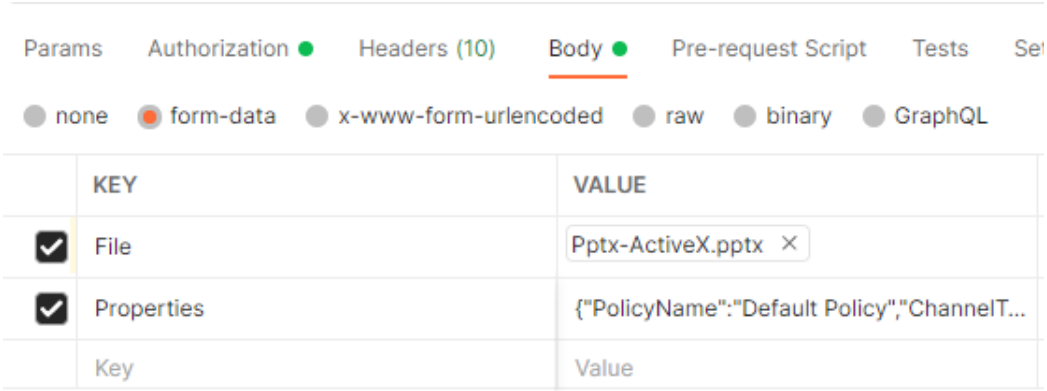
13. In the first row of the **KEY** column, type **File**, and select **File** from the hidden dropdown list:



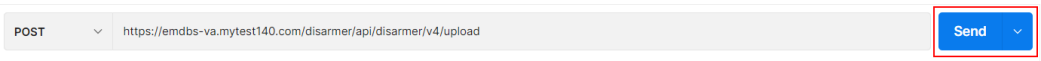
14. In the first row of the **VALUE** column, press **Select Files** and select the desired file from the browser window that opens.
15. In the second row of the **KEY** column, type **Properties**.
16. In the second row of the **VALUE** column, enter the following:

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

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

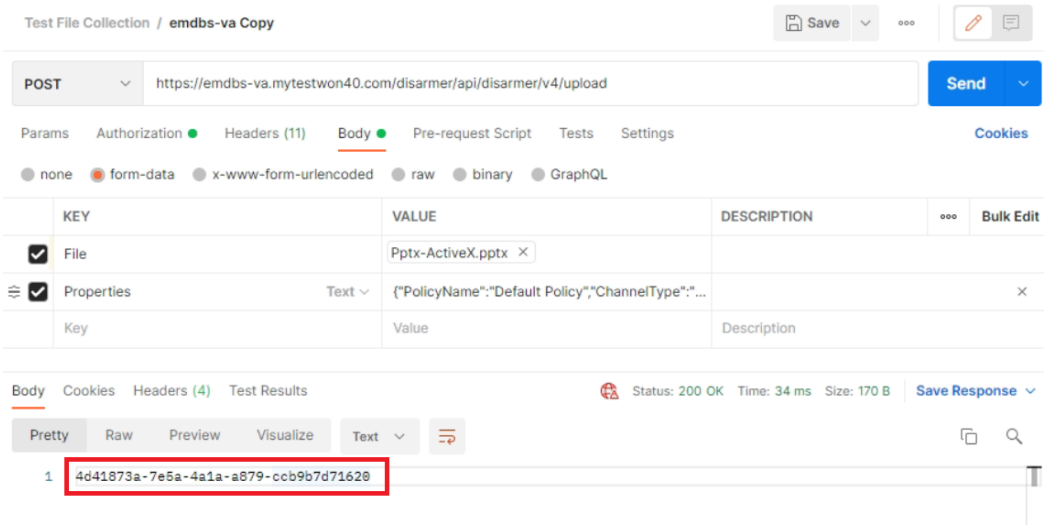


18. Press the **Send** button:

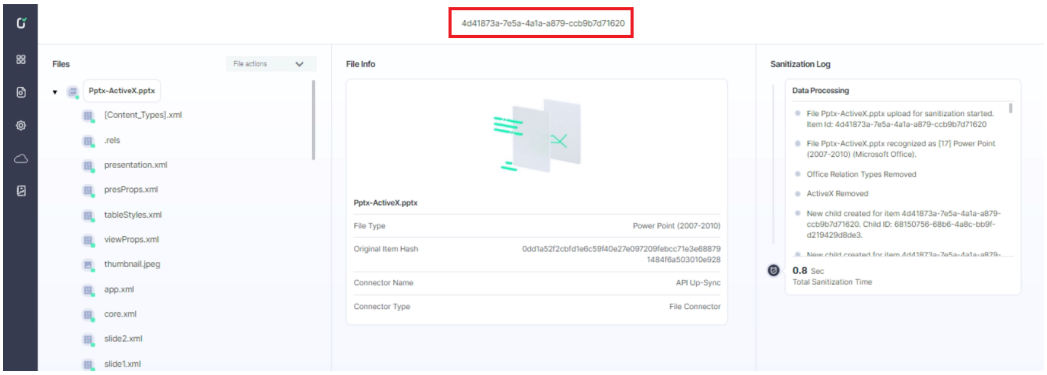


19. You should get a HTTP/200 response and a GUID string in the body. This will be the Correlation ID of the file that you have submitted.

For example:



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



17 How to Sync with an NTP Server

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

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

17.1 Solution

Obtain a list of servers, using the following command:

```
# cat /etc/ntp.conf | grep server
```

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

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

- External NTP server.
- Internal NTP server.

17.2 External NTP Server

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

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

   ```
   *.centos.pool.ntp.org
   ```

17.3 Internal NTP Server

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

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

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

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

   ```
   # vi /etc/ntp.conf
   ```

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

```
# Use public servers from the 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
```

17.4 Verify Time of Syncronization for each Node

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

```
# timedatectl
```

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

18 How to Troubleshoot NTP using Chrony in VA

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

18.1 Solution

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

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

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

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

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

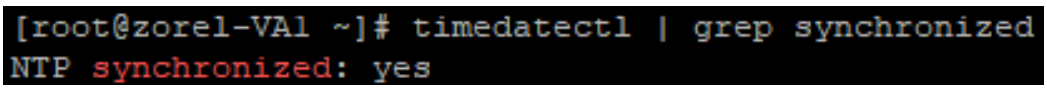
     ```
     systemctl stop ntpd.service
     ```

     ```
     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:

   - 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
       ```

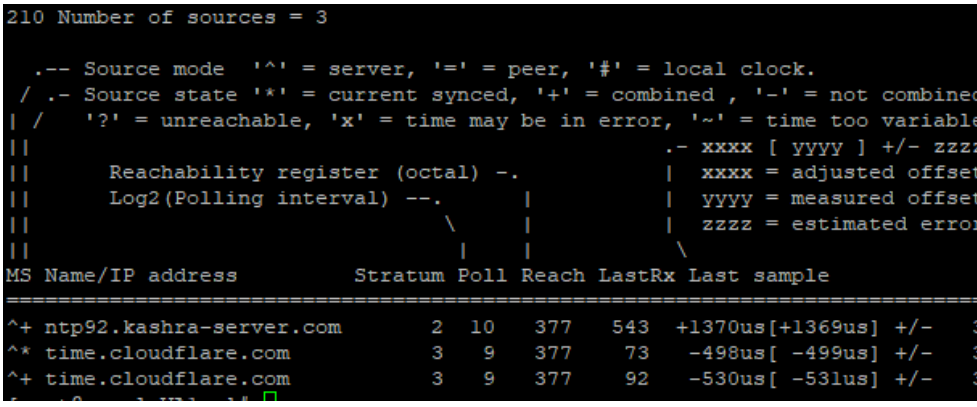
- If the service is running, run the following command to verify the synchronization of the local system with the reference server:

  ```
  chronyc tracking
  ```

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

  ```
  chronyc sources -v
  ```

  For example:



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

  ```
  chronyc sourcestats
  ```

- To edit the chrony configuration, run the command:

  ```
  vi /etc/chrony.conf
  ```

For example, with public servers:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.centos.pool.ntp.org iburst
server 1.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
server 3.centos.pool.ntp.org iburst

# Record the rate at which the system clock gains/losses time.
driftfile /var/lib/chrony/drift

# Allow the system clock to be stepped in the first three updates
# if its offset is larger than 1 second.
makestep 1.0 3

# Enable kernel synchronization of the real-time clock (RTC).
rtcsync

# Enable hardware timestamping on all interfaces that support it.
#hwtimestamp *

# Increase the minimum number of selectable sources required to adjust
# the system clock.
#minsources 2

# Allow NTP client access from local network.
#allow 192.168.0.0/16

# Serve time even if not synchronized to a time source.
#local stratum 10

# Specify file containing keys for NTP authentication.
#keyfile /etc/chrony.keys

# Specify directory for log files.
logdir /var/log/chrony

# Select which information is logged.
#log measurements statistics tracking
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/chrony.conf" 38L, 1108C
```

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

18.2 Troubleshooting Example: NTP not synchronized with external server

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

```
[root@dmzcdreml02 ~]# 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@dmzcdreml02 ~]# 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@dmzcdreml02 ~]# chronyc sources -v
210 Number of sources = 2

  .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
 / .- Source state '*' = current synced, '+' = combined , '-' = not combined,
| /   '?' = unreachable, 'x' = time may be in error, '~' = time too variable.
||                                                 .- xxxx [ yyyy ] +/- zzzz
||      Reachability register (octal) -.           |  xxxx = adjusted offset,
||      Log2(Polling interval) --.      |          |  yyyy = measured offset,
||                                \     |          |  zzzz = estimated error.
||                                 |    |           \
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^? dmzdc01.dmz.local             2   6   377    32  +1814ms[+1814ms] +/-  10.8s
^? dmzdc02.dmz.local             1   7   377    59  +1816ms[+1816ms] +/-  10.8s
[root@dmzcdreml02 ~]# chronyc tracking
Reference ID    : 00000000 ()
Stratum         : 0
Ref time (UTC)  : Thu Jan 01 00:00:00 1970
System time     : 0.000000015 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.

19 How to Upgrade Votiro Cloud

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

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

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

19.1 Upgrade Installation

19.1.1 Before You Begin

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

19.1.2 Procedure

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

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

   For example:

   ```
   yum install wget -y && mkdir -p /root/upgrade && cd upgrade
   wget -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.

19.1.3 Verification of Upgrade

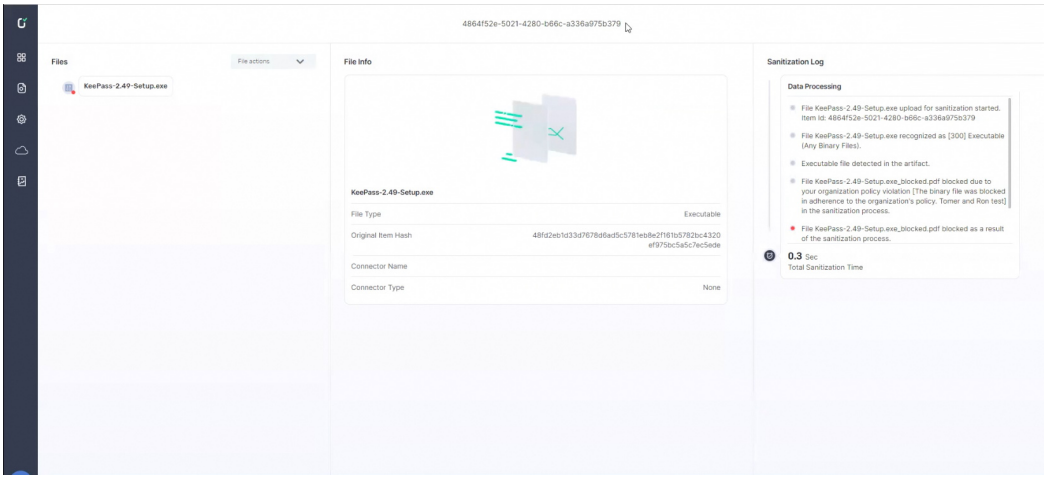
To verify that the upgrade has completed successfully, wait a few minutes, then login to the Management Dashboard. The version number you have upgraded to is displayed.

20 How to Use Kibana to Troubleshoot Votiro Incidents

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

20.1 Example of Votiro Incident

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



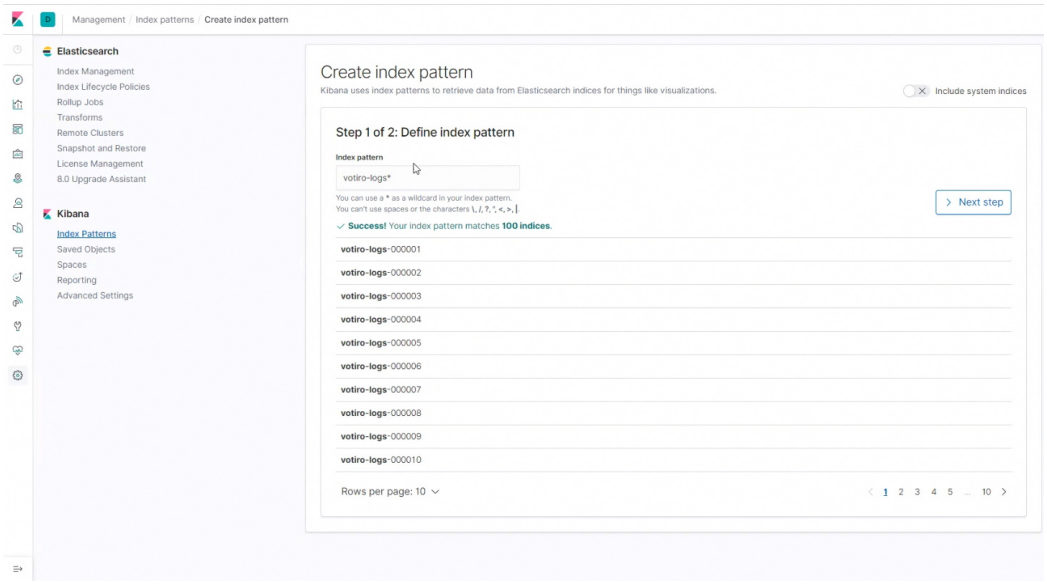
This screen shows the results of Votiro Cloud processing a file named KeePass-2.49-Setup.exe. The **File Info** pane displays some of the file properties and the **Sanitization Log** pane displays highlights of the file **Data Processing**.

20.2 Procedure

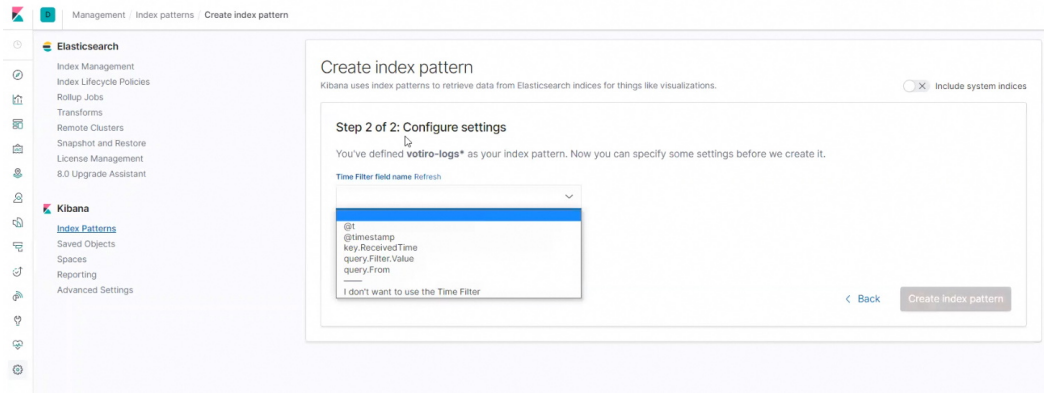
20.2.1 Create and Configure an Index Pattern

To begin, you must define a Kibana index pattern.

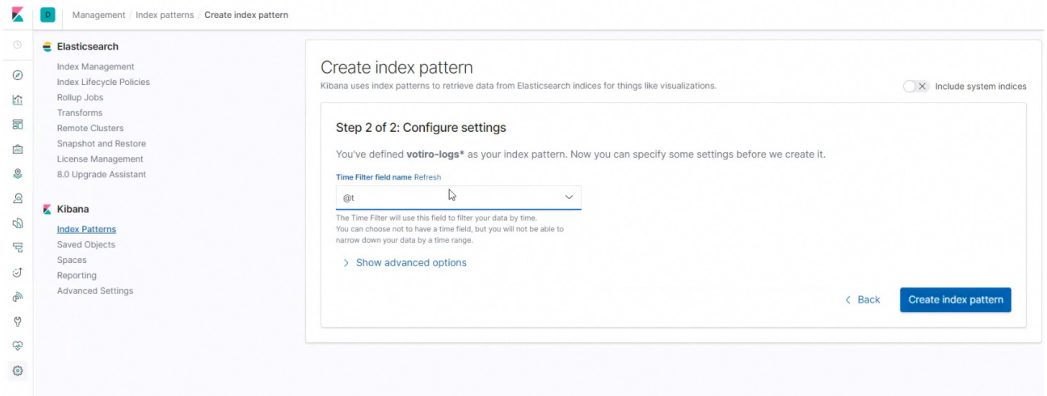
1. Login to the Kibana Discover interface with the credentials provided to you by Votiro Support.
2. Select **Create index pattern**. **Step 1 of 2 Define index pattern** appears.
3. Type **votiro-logs*** (or similar) as the Index pattern. Kibana displays a list matching the index pattern:



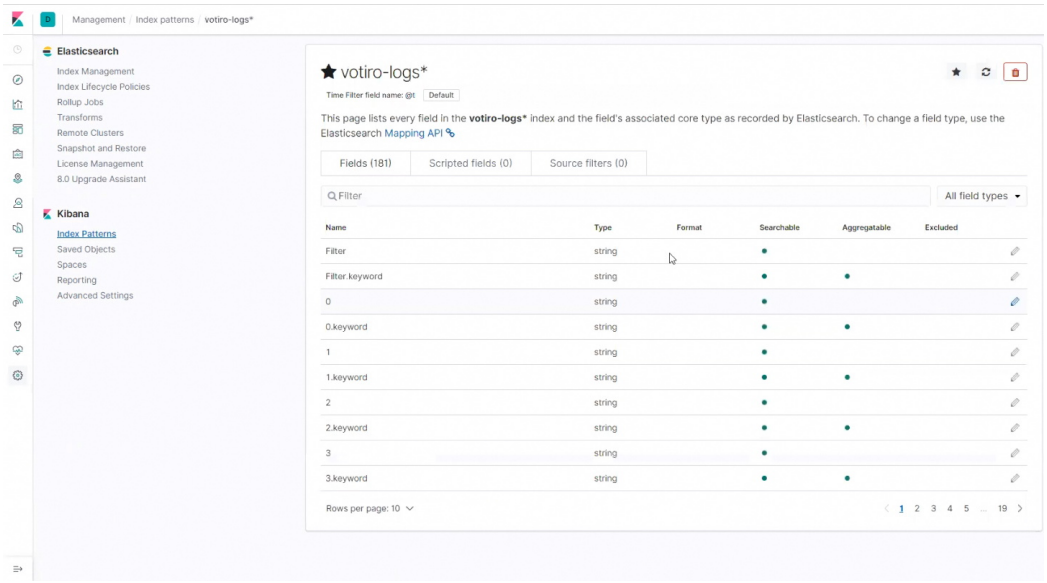
4. Click on **Next step**. **Step 2 of 2 Configure settings** appears.



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*):

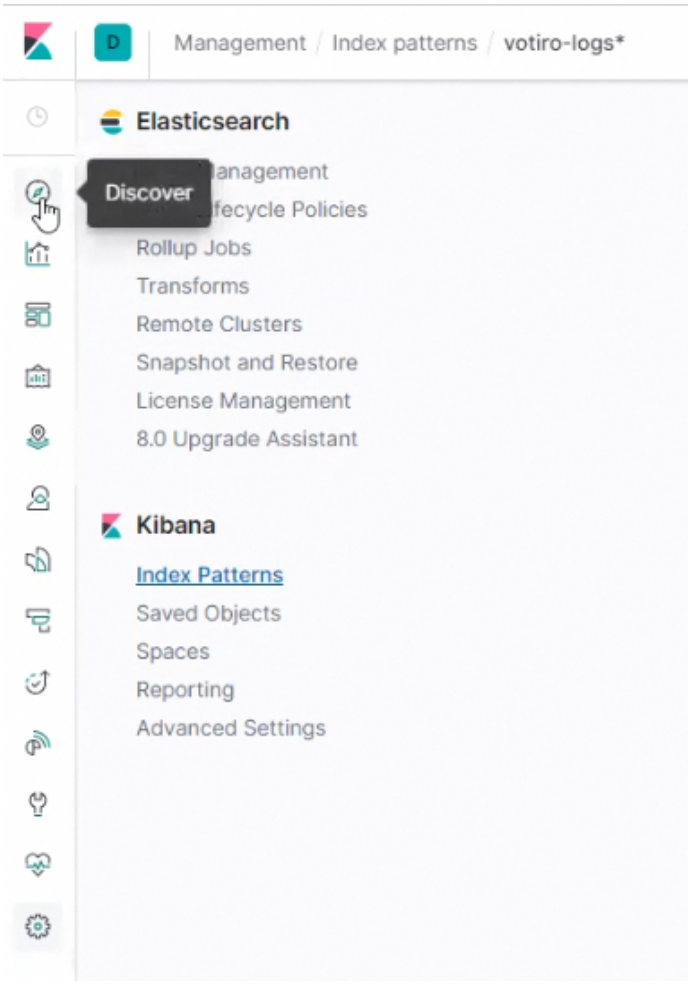


20.3 Analyze the Data

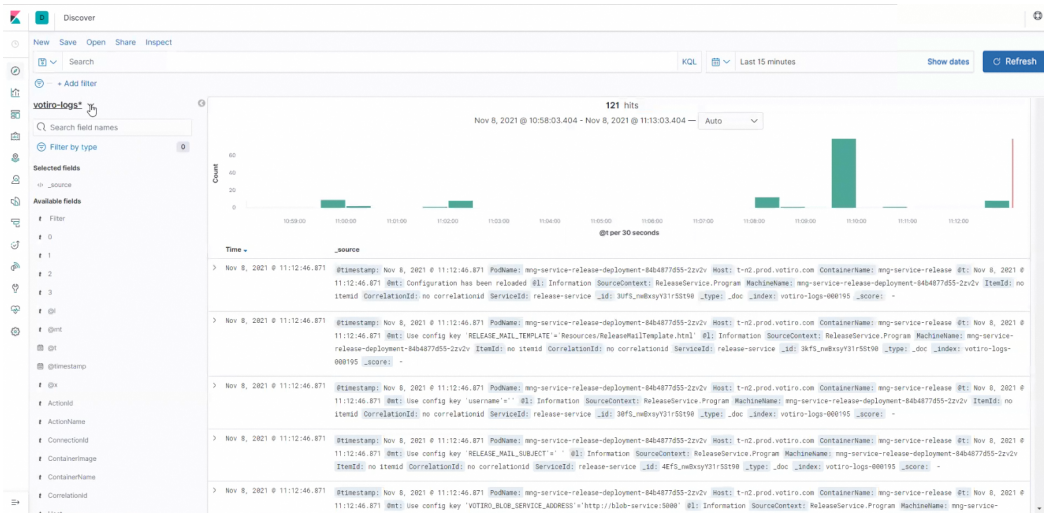
After the index pattern is created and configured, apply it to the data in Kibana's Discover mode to yield useful results by additional filtering of the data.

20.3.1 Discover

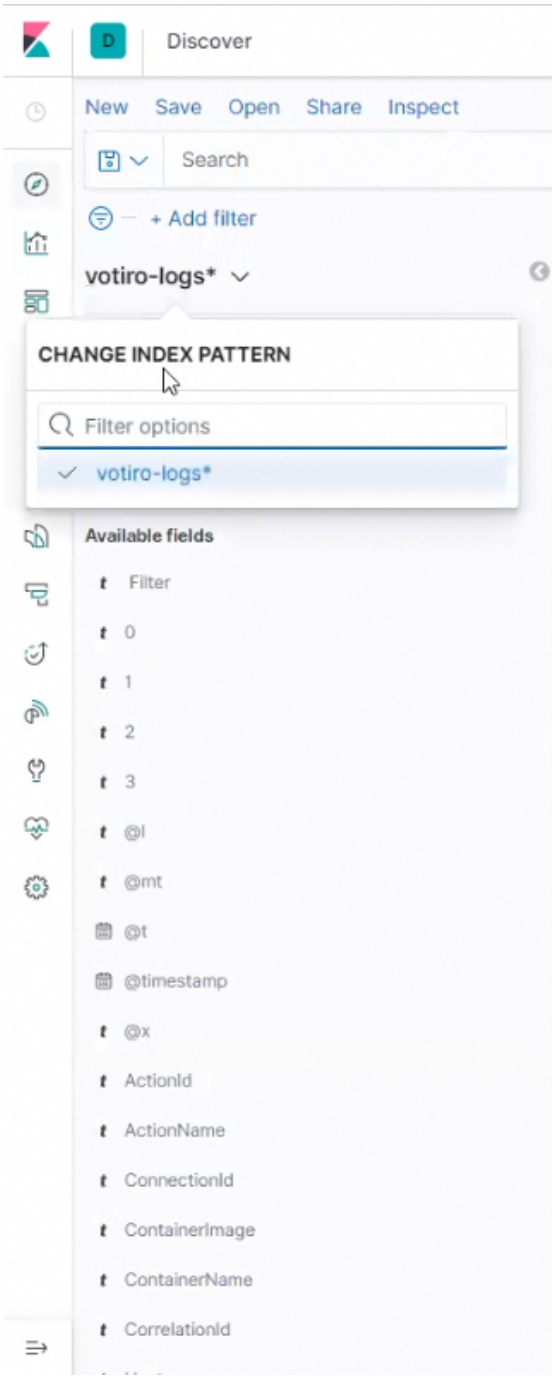
1. Click on the Discover icon on the left side of the screen:



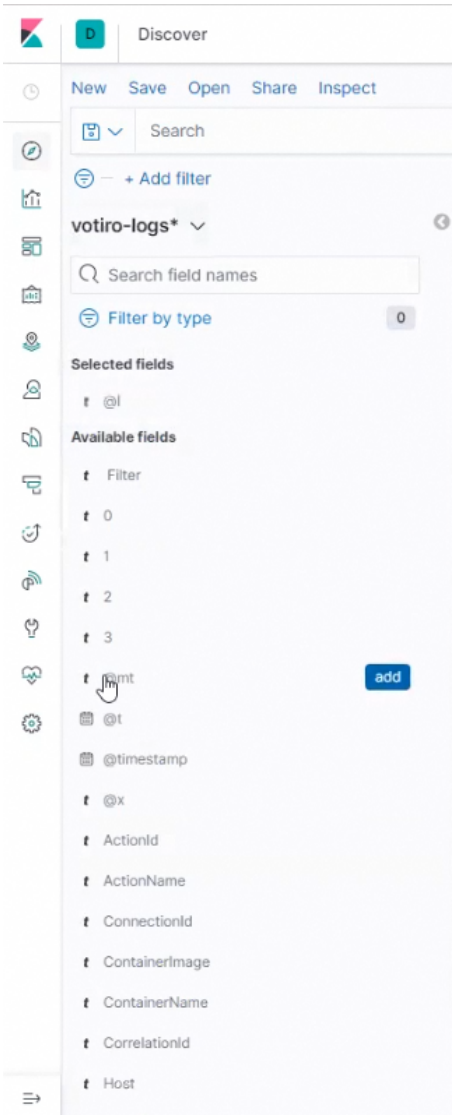
2. Kibana displays all hits that match the time filter criteria within the time range indicated (in this example, for the last 15 minutes):



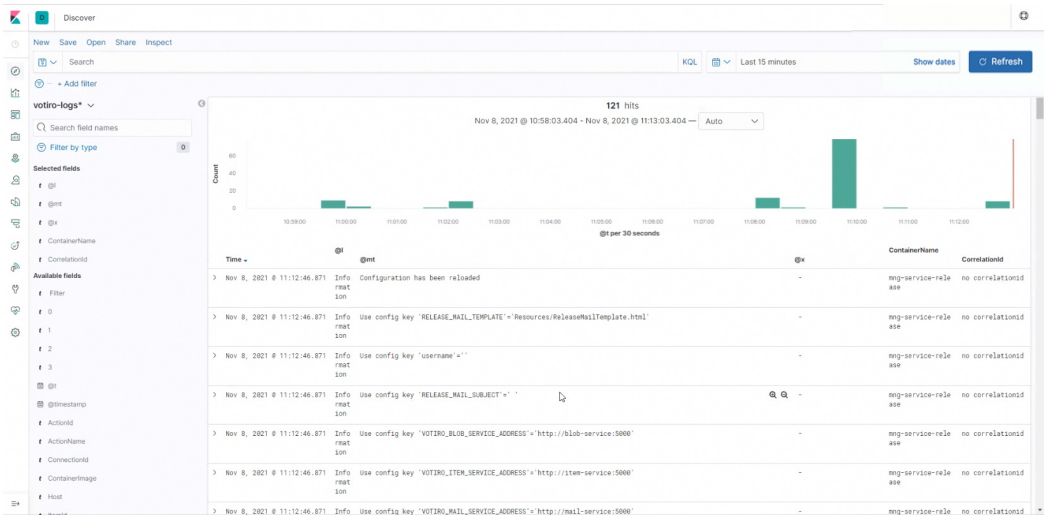
3. To further filter the results, click on ˅ next to the index pattern (votiro-logs* by default) in the left side of the screen. The **CHANGE INDEX PATTERN** window opens:



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:



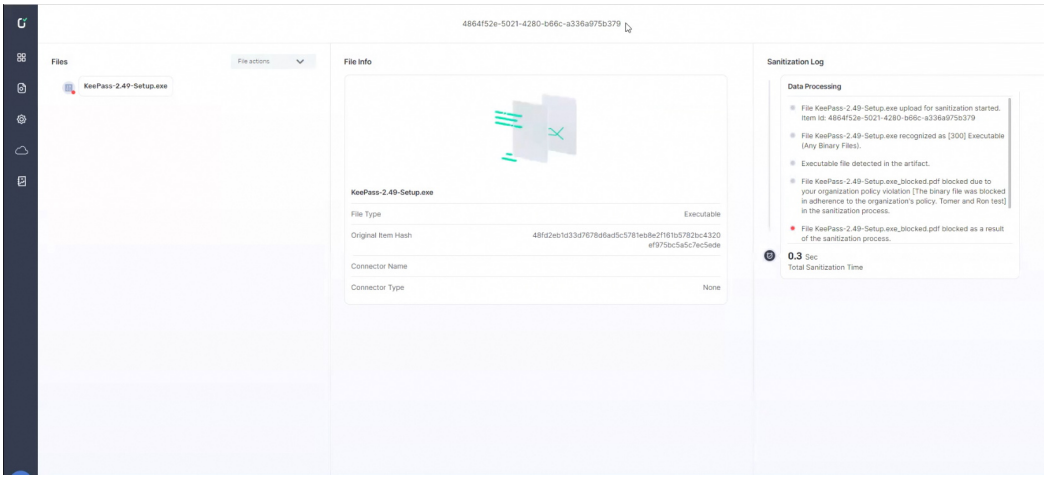
5. In the example below, the following fields are added:
   - **@l** - level
   - **@mt** - message template
   - **@x** - exception
   - **ContainerName**
   - **CorrelationId**
6. The display of hits is now updated to show only the selected fields:



20.3.2 Votiro Explore Incident & File Info

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

1. Open the Votiro Explore Incident:



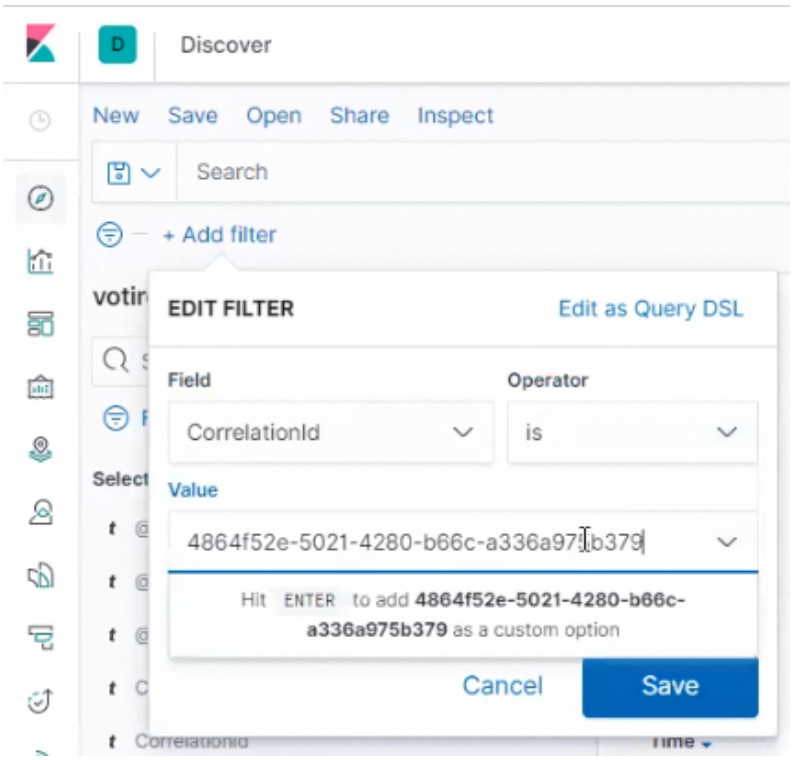
2. Copy to the clipboard the file ID at the top of the screen, in this example:

4864f52e-5021-4280-b66c-a336a975b379

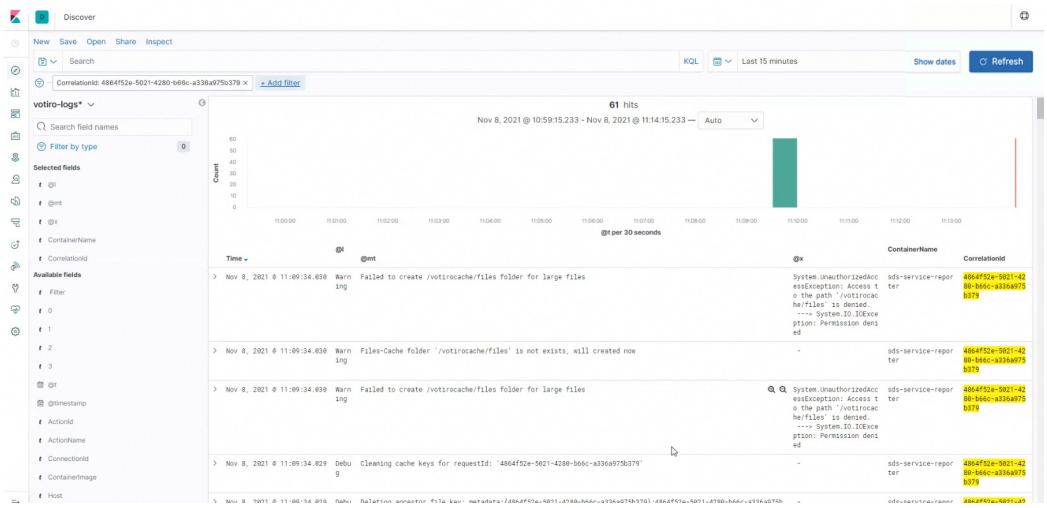
20.3.3 File Sanitization Analysis

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

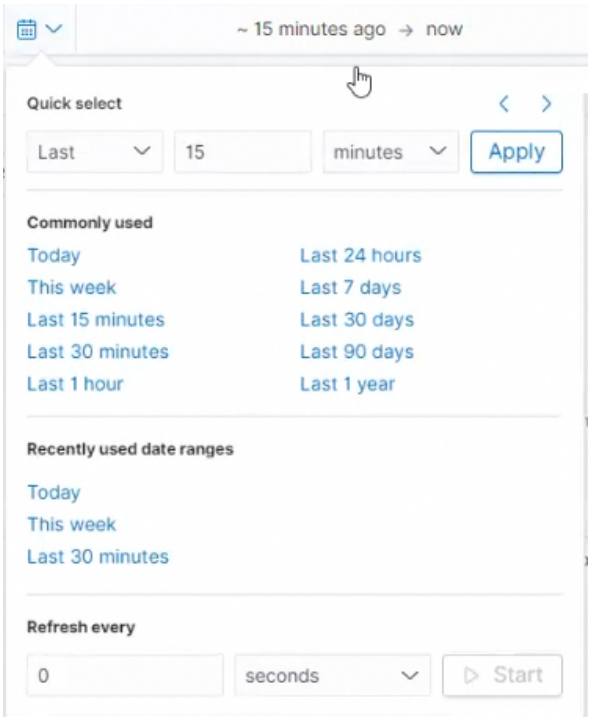
5. In the **Value** field, paste the file ID from the clipboard .



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



7. 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.

21 Message Size Limits in Exchange

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

21.1 Symptoms

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

21.2 Solution

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

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

21.3 Limitations

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

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

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

22 MSSP User Guide

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

Examples of MSSP use cases supported by Votiro include:

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

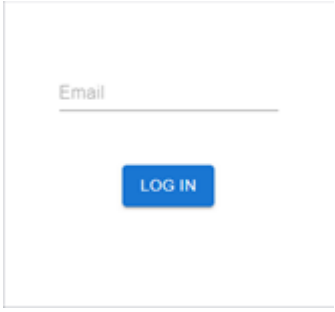
22.1 MSSP Tenant Management

1. **Login**

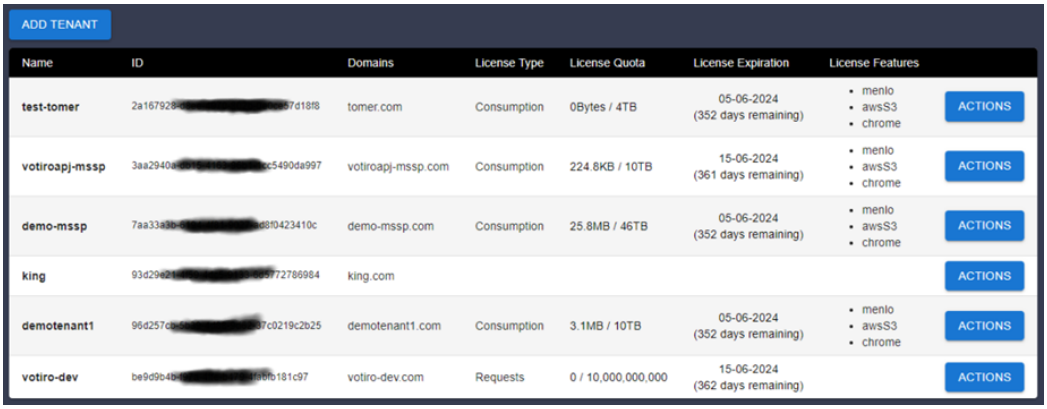
   To login to MSSP Tenant Management, use the following URL address:

   “https://{clusterName}/portal/#/votiro/login”

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



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



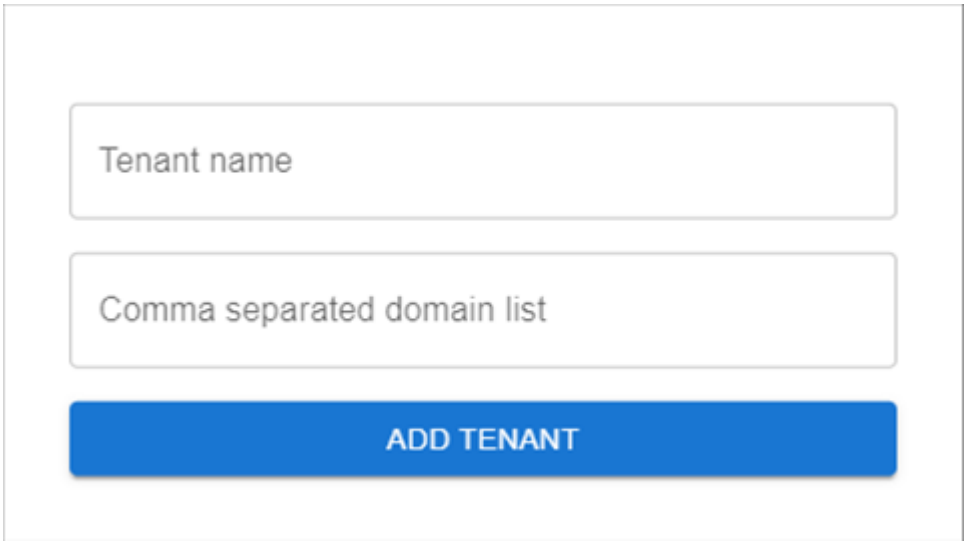
The MSSP admin can use the Tenant Management screen to:

- Add a customer tenant

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

2. **Add a customer tenant**

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



Enter:

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

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

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

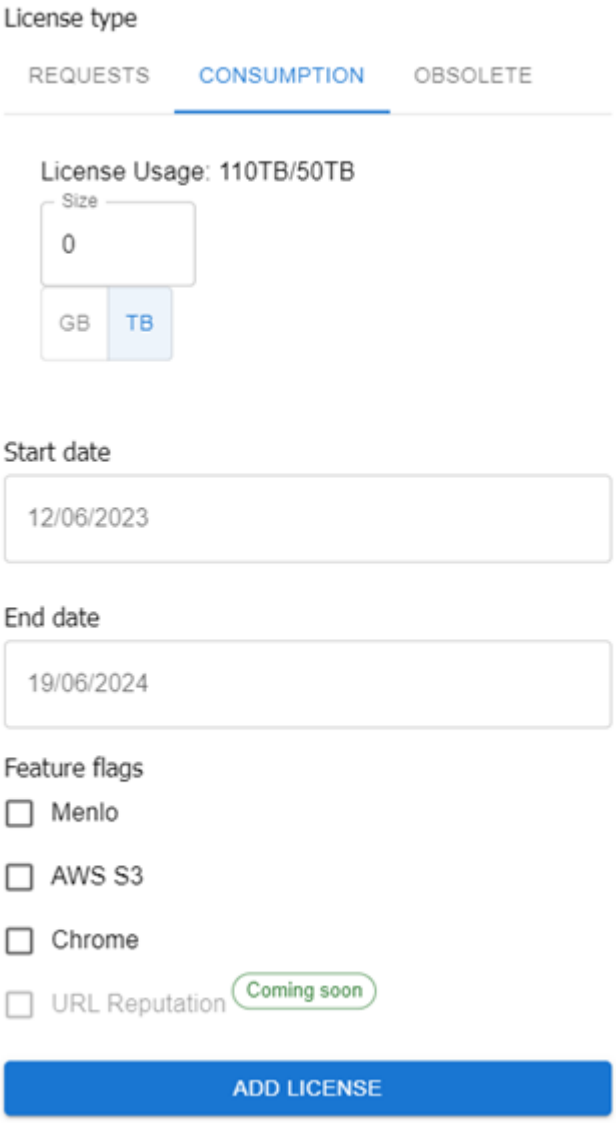
The following information is displayed on the Tenant Management screen for each tenant:

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

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

4. **Import a license**

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



Enter or select:

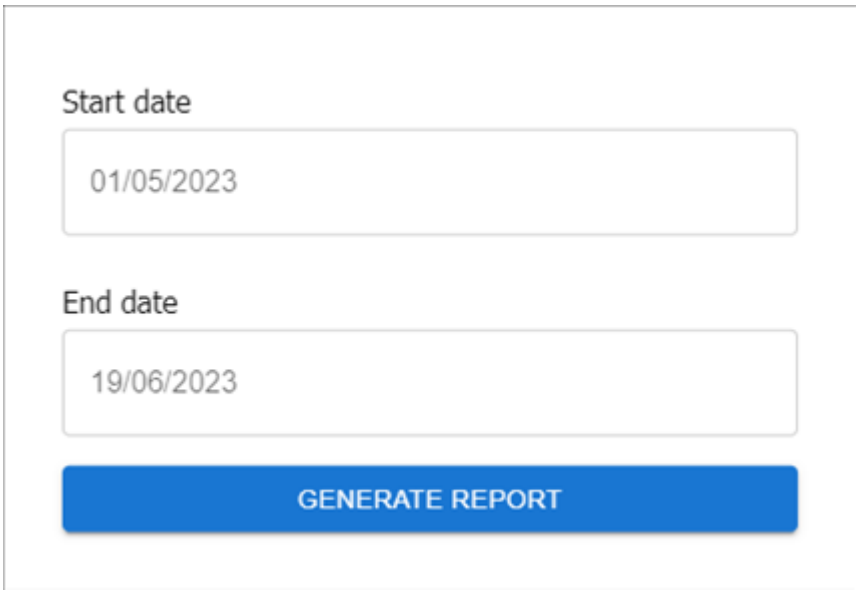
- License type
- License Usage
- Start date
- End date
- Feature flags (if needed)

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

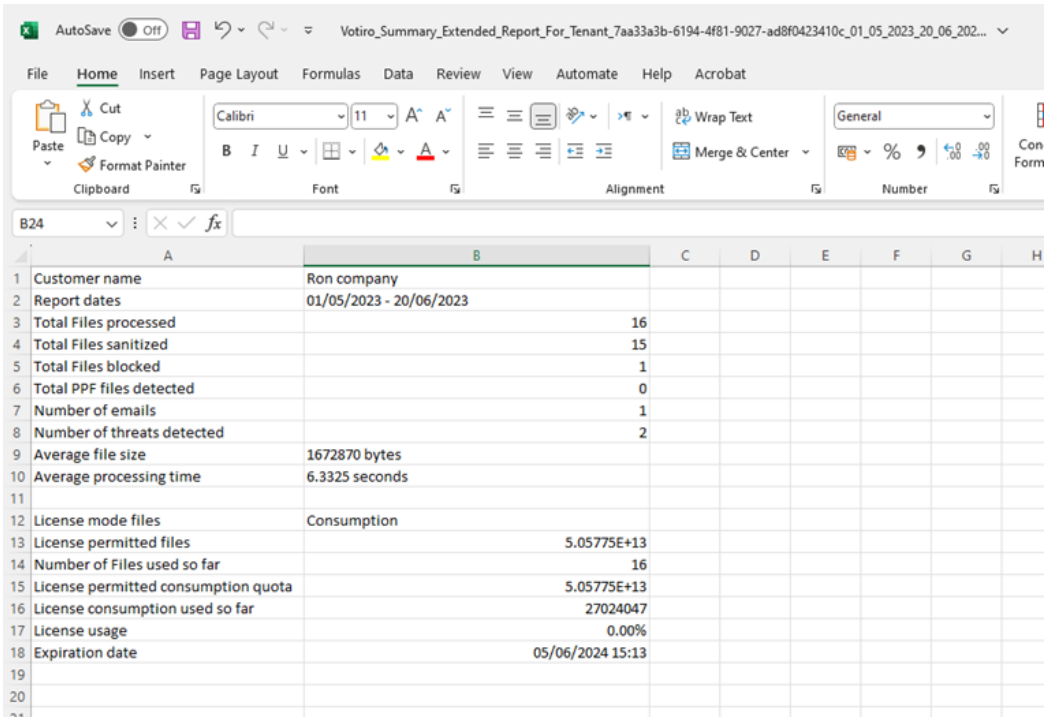
- Votiro MSSP Tenant Management screen
- Customer tenant Management console license page

5. **Download Analytics Report**

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



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



	A	B	C	D	E	F	G	H
1	Customer name	Ron company						
2	Report dates	01/05/2023 - 20/06/2023						
3	Total Files processed	16						
4	Total Files sanitized	15						
5	Total Files blocked	1						
6	Total PPF files detected	0						
7	Number of emails	1						
8	Number of threats detected	2						
9	Average file size	1672870 bytes						
10	Average processing time	6.3325 seconds						
11								
12	License mode files	Consumption						
13	License permitted files	5.05775E+13						
14	Number of Files used so far	16						
15	License permitted consumption quota	5.05775E+13						
16	License consumption used so far	27024047						
17	License usage	0.00%						
18	Expiration date	05/06/2024 15:13						
19								
20								

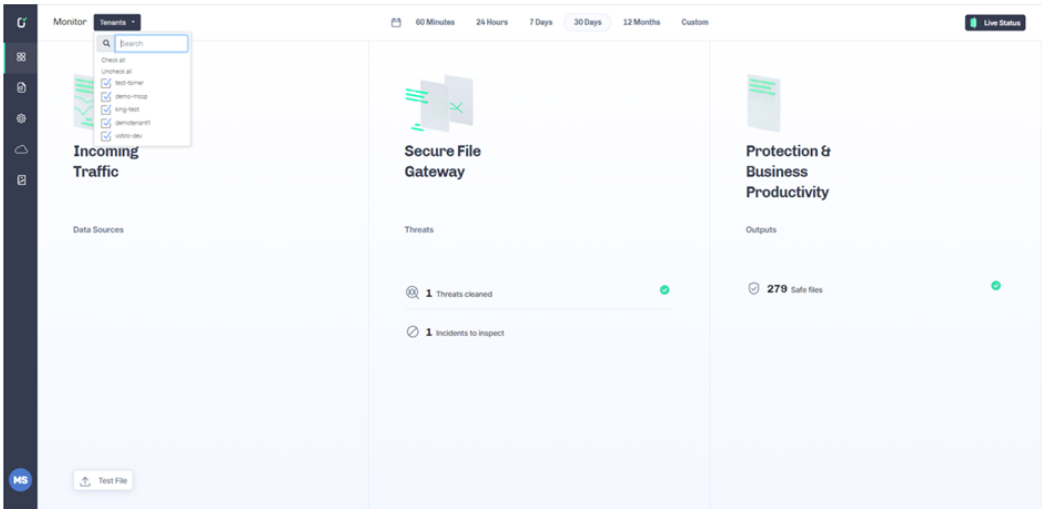
6. **Delete a customer tenant**

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

22.2 Monitoring Tenant Activity

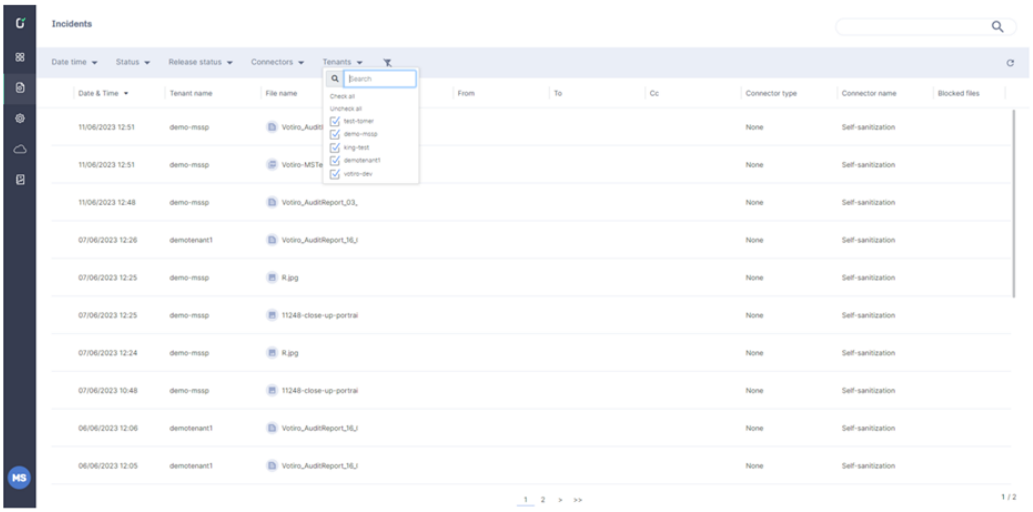
1. **MSSP Dashboard**

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



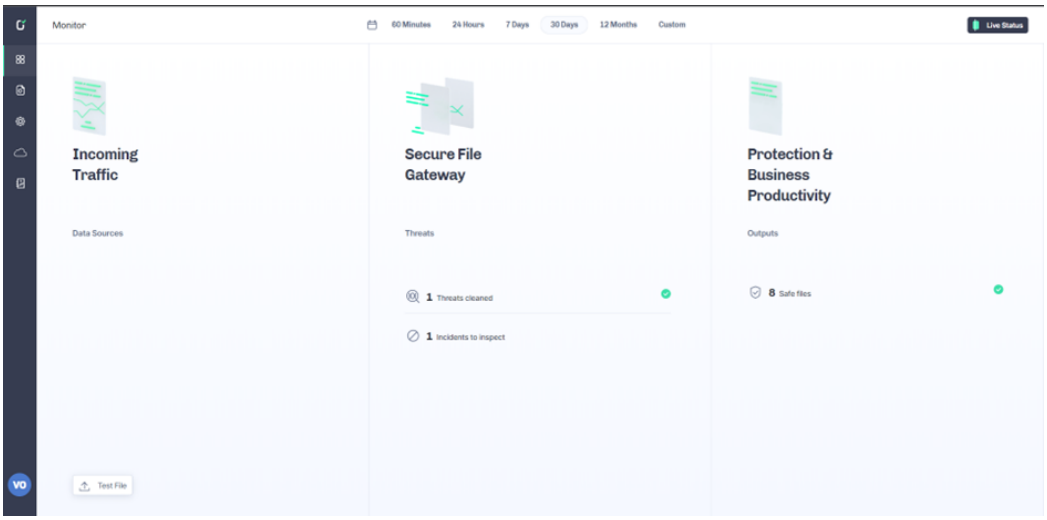
2. **MSSP Incidents**

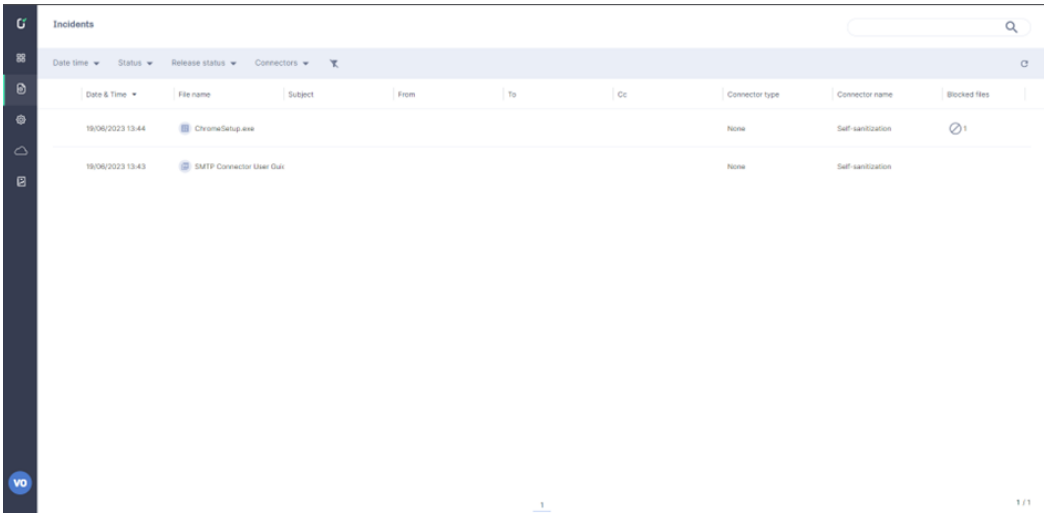
   The MSSP user can view and filter incidents data by customer tenant selection in the **Tenants** column.



3. **MSSP Customer's Dashboard**

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



4. **MSSP Customer's Incidents**

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