

Humio is a leading Observability platform that you likely know can handle containerized and cloud-based events. But did you know Humio makes it easy to capture Windows server event logs? We do this by leveraging [WinLogBeat by Elastic](#) to ingest any Windows Event log into Humio.

WinLogBeat is a native Windows event-log shipping agent usually installed as a windows service. We can use WinLogBeat to collect and transmit event logs to one or more destinations including Humio.

In this article, we will take you through setting up the Open Source version of WinLogBeat on a Windows host and configuring it to publish logs and events to a Humio Repository using Humio Community Edition. We will then show some example queries that will show the immediate value by tracking Setup events as applied to the monitored host.

Setup Humio

To use Humio, you will need a Humio account. If you don't have one, you can sign up for the Community Edition [here](#). Typically, your new account will be activated in two business days. You'll get an email with your login information:

Your Humio Community account has been activated. You're all set and ready to go.

To log in, go to

<https://cloud.community.humio.com>

Your license

- 16 GB/day data ingest
- 7-day retention
- 5 Users
- 1 Repository

You can then log in with your identity provider of choice.

Log in



Log in with Google



Log in with GitHub

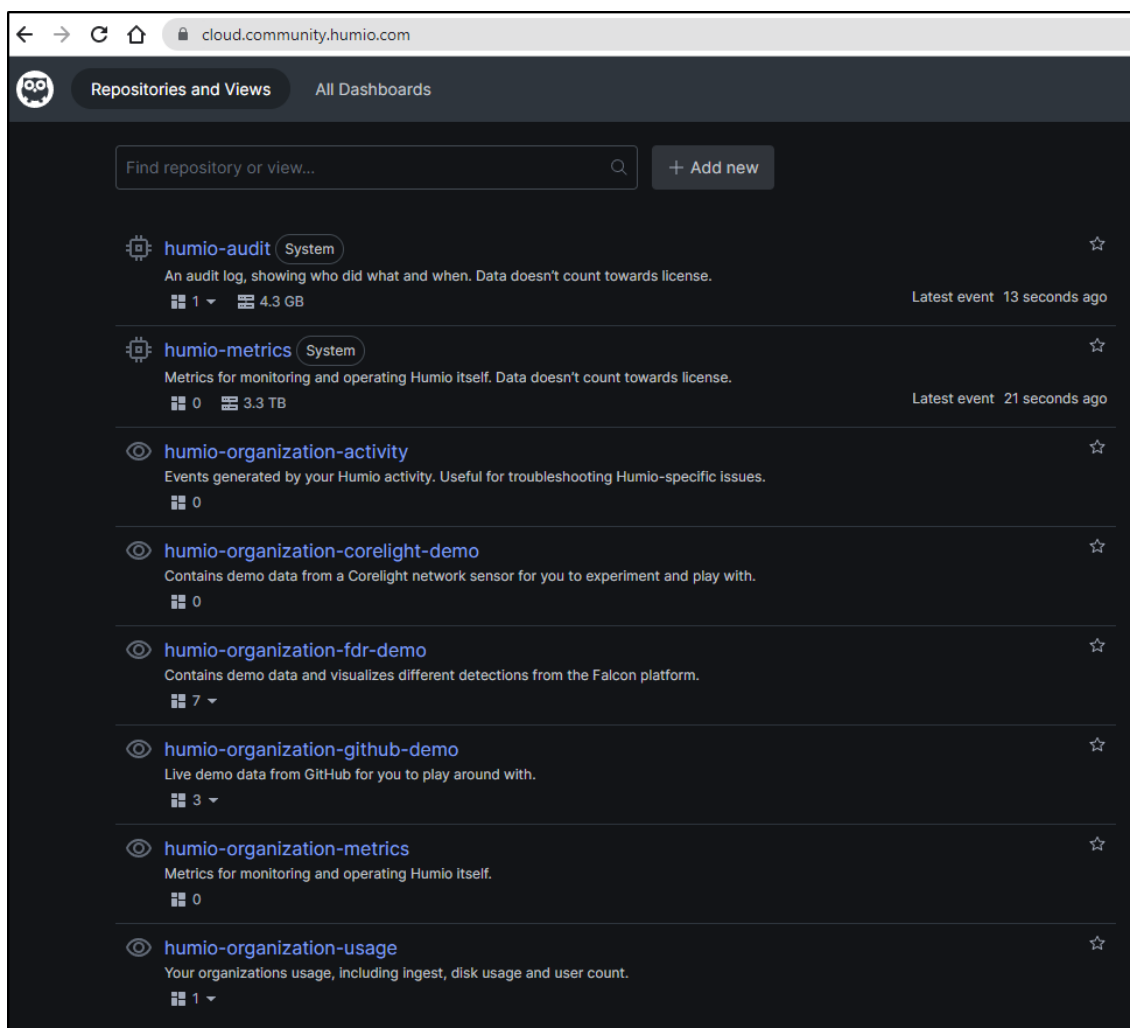


Log in with Bitbucket

Don't have an account yet?
[Sign up for a free Community account](#)

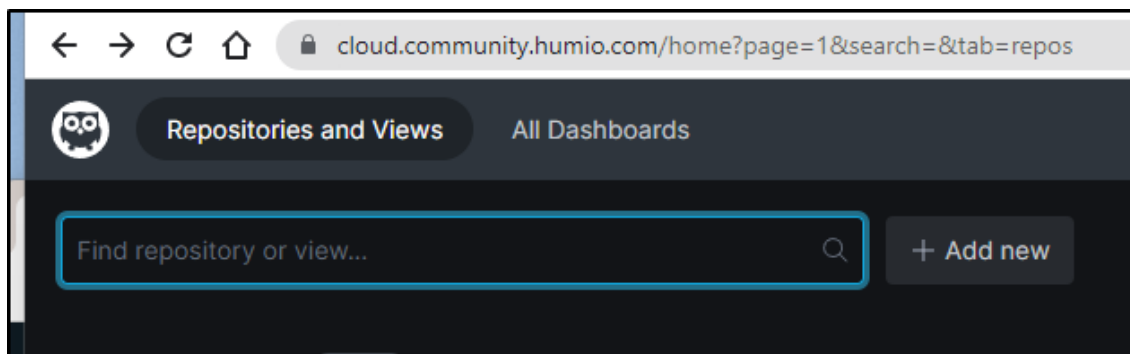
By logging in, I agree to be bound by the [CrowdStrike-Humio Software as a Service Terms and Conditions](#), and acknowledge the CrowdStrike [Privacy Notice](#).

From there, you can view all of your Humio repositories.

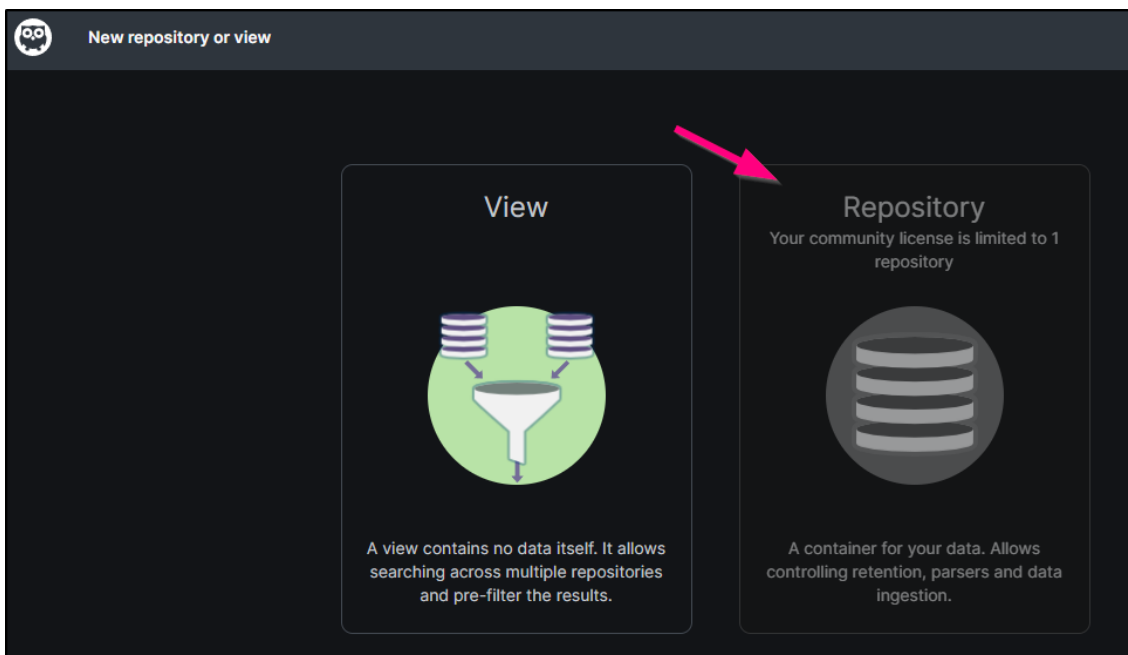


Create a new Humio repository

We'll need to create a repository. Once created, we can get a token for the repository. Click **+ Add New** to create a repository.



Select **Repository** to add a repository.



Note: Community Edition allows only one repository. If you already have an existing repository, you'll need to remove it before you can add a new one.

Installing WinLogBeat

The version of WinLogBeat that works with Humio is the Open Source Edition (OSS). Elastic also provides a "Standard" edition, however that is designed only to work with their own products.

Installing WinLogBeat OSS

We'll go to the ["Past Releases" section of Elastic.co Downloads](#) and chose the latest Download that starts with "Winlogbeat OSS".

Because of some known issues with 8.0 and above, we can opt to get the latest 7.* version, in this case it is [Winlogbeat OSS 7.17.5](#)

Winlogbeat OSS 7.17.5

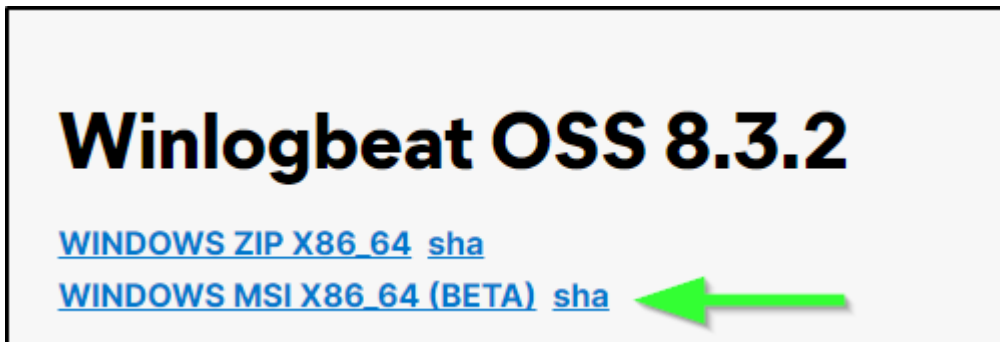
[WINDOWS ZIP 32-BIT](#) [sha](#)

[WINDOWS ZIP X86_64](#) [sha](#)

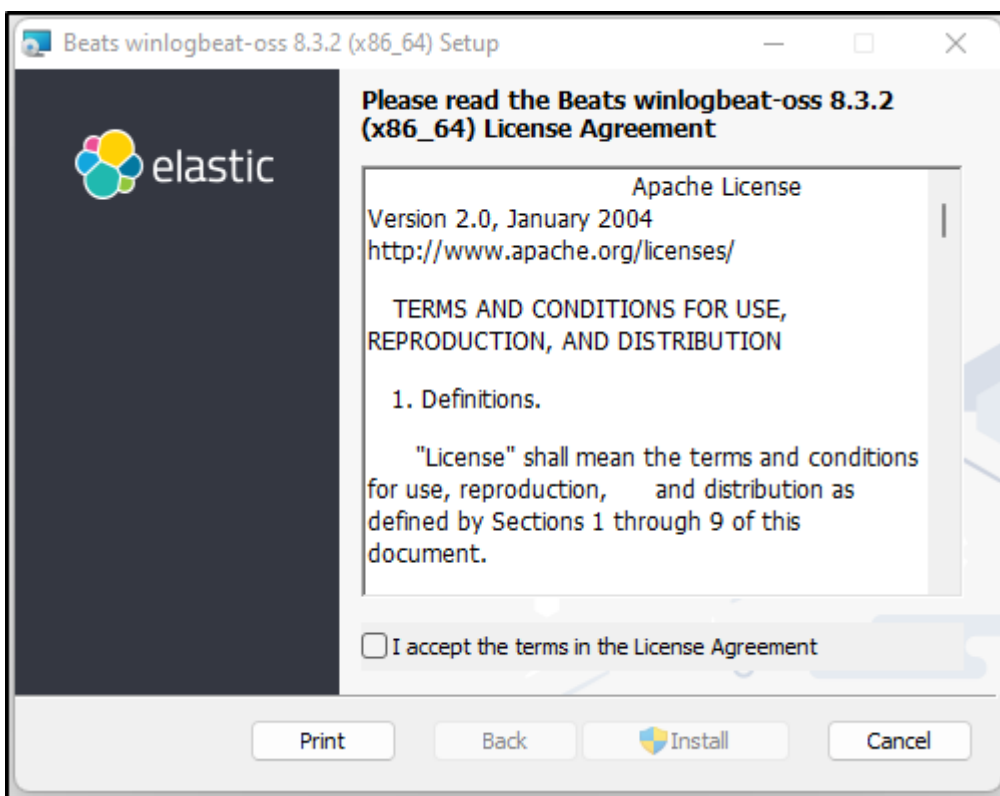
[WINDOWS MSI 32-BIT \(BETA\)](#) [sha](#)

[WINDOWS MSI X86_64 \(BETA\)](#) [sha](#)

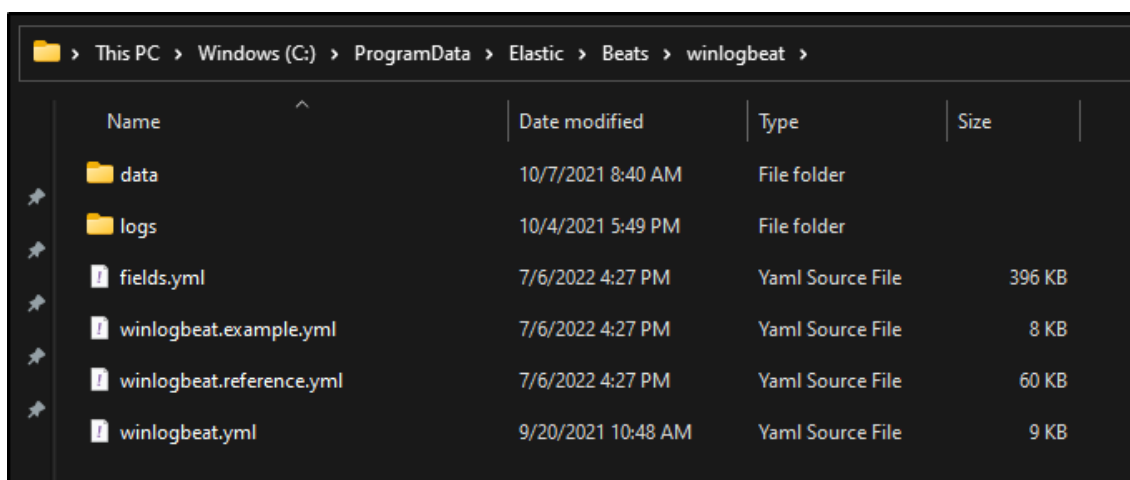
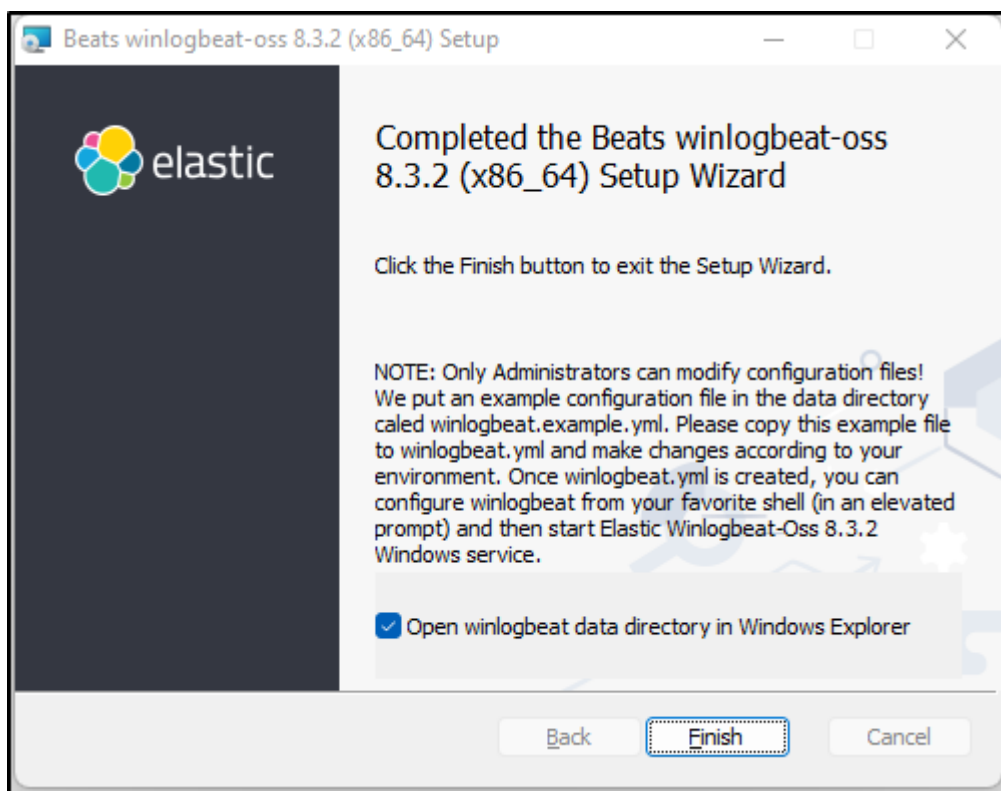
We can use the new beta MSI package for an easier install



We'll then follow the installer flow to accept the terms of the Apache license provided they are acceptable to you.

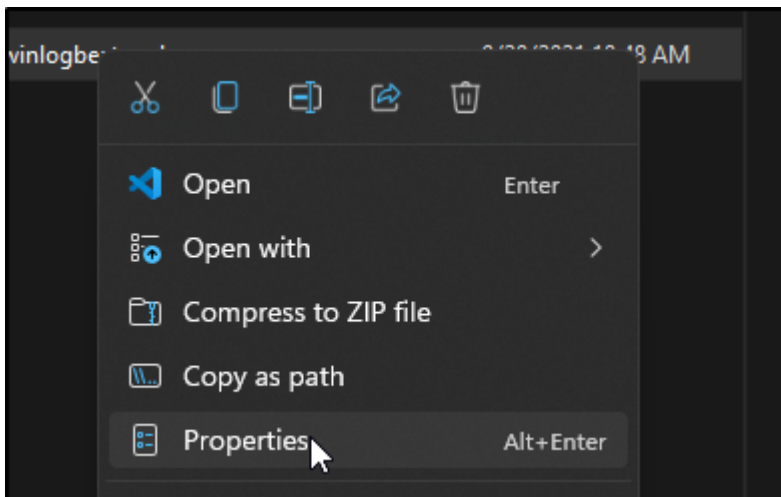


When the installer is done, we can check the box to automatically open the data directory for Winlogbeat

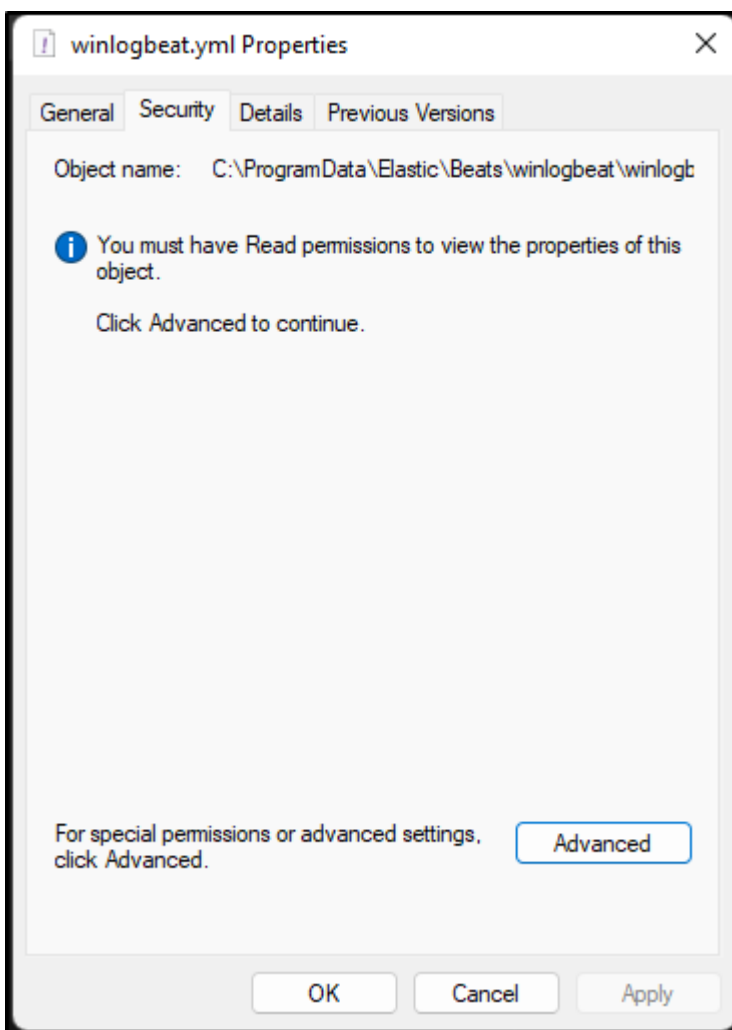


To open the file for editing, I needed to fix the file permissions to allow me to read and edit the winlogbeat.yml file

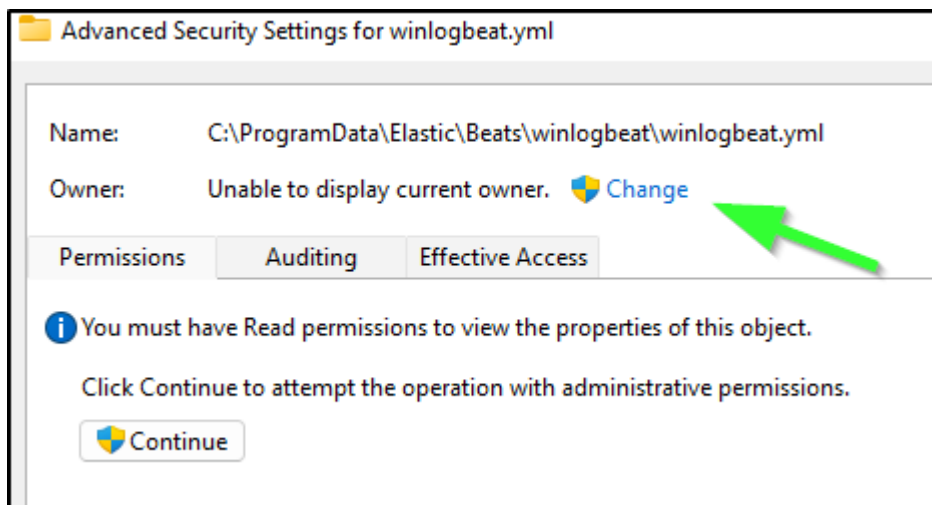
Right-click the file and choose properties



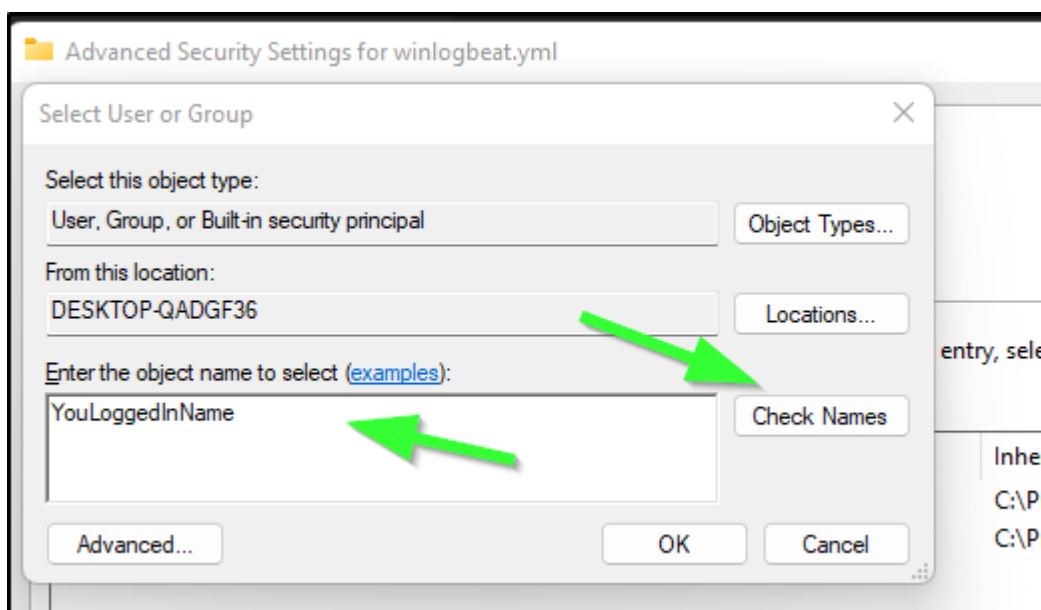
Under the Security tab, if the issue still exists, you'll note that it says "You must have Read permissions to view the properties of this object". choose advanced



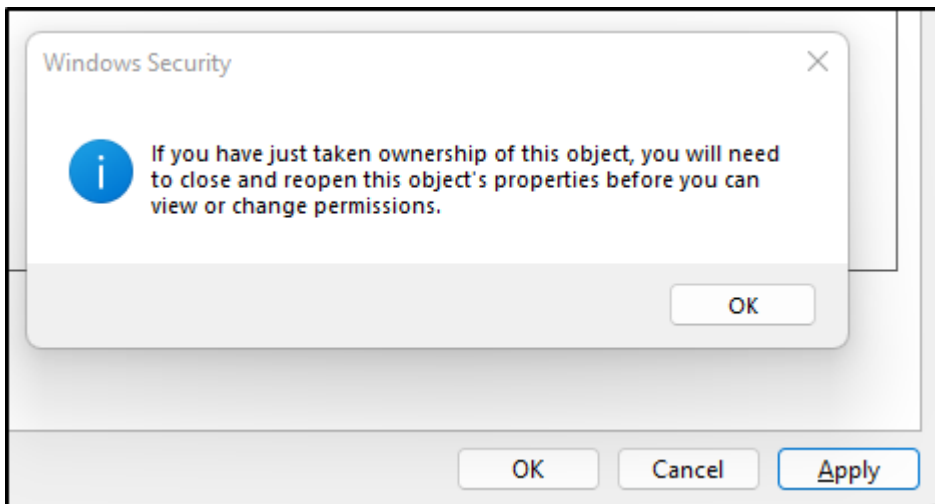
I chose Change on the Owner section of the Advanced dialog



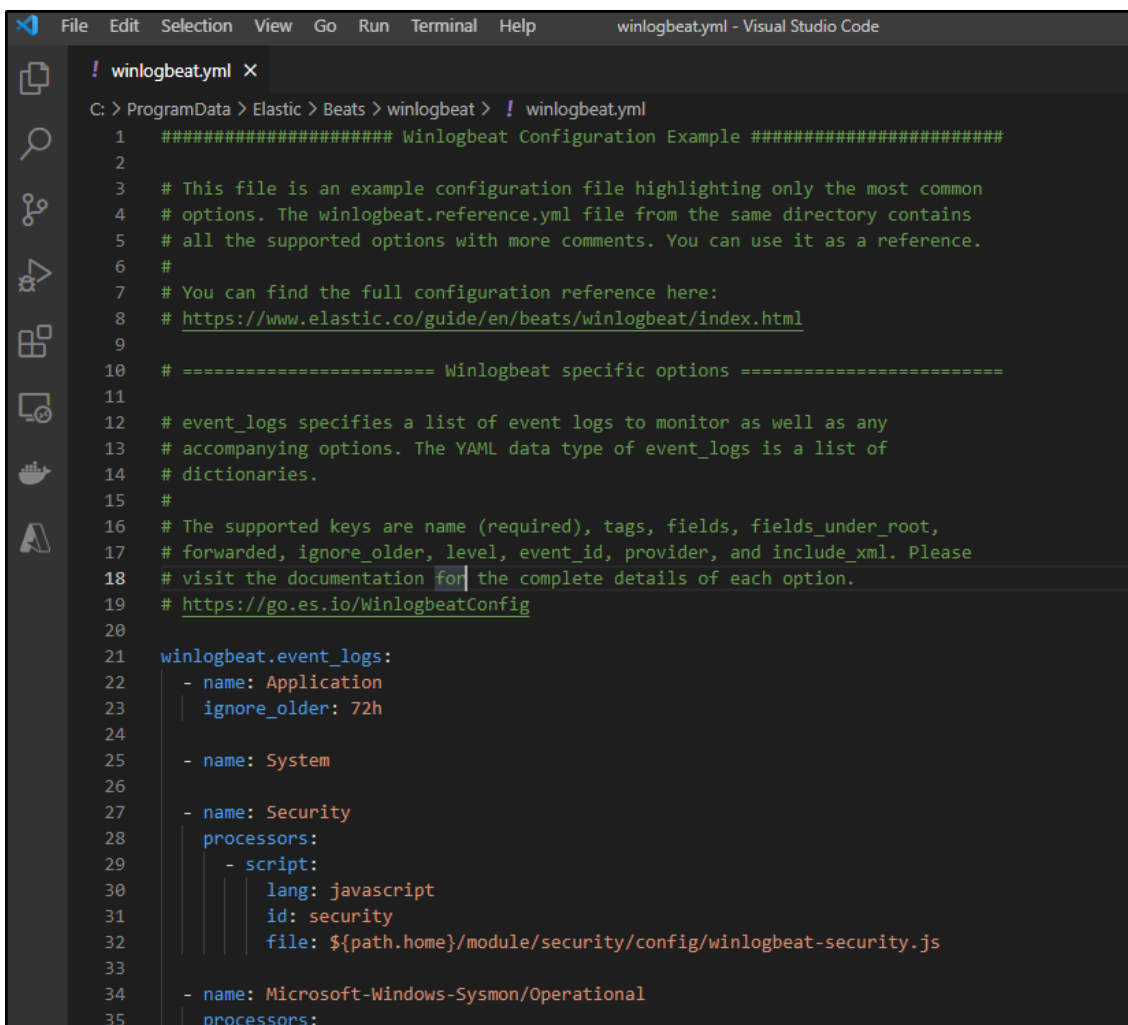
Then put in my User ID and clicked **Check Names** (which then filled it in)



I was then prompted to re-open the object



If you have sorted out your user permissions, you should be able to open the file in an editor like Visual Studio Code

A screenshot of the Visual Studio Code editor. The title bar shows "winlogbeat.yml - Visual Studio Code". The menu bar includes File, Edit, Selection, View, Go, Run, Terminal, and Help. The left sidebar shows icons for Explorer, Search, Source Control, Run and Debug, Extensions, Output, and Task View. The main editor area shows the content of the file "winlogbeat.yml". The file path in the Explorer is "C: > ProgramData > Elastic > Beats > winlogbeat > ! winlogbeat.yml". The file content is a YAML configuration file for Winlogbeat. It starts with a comment block explaining the file's purpose and providing links to documentation. It then defines the "winlogbeat.event_logs" section with a list of event logs to monitor: "Application", "System", "Security", and "Microsoft-Windows-Sysmon/Operational". The "Security" log has specific processors defined, including a script processor for security events. The "Sysmon/Operational" log also has processors defined.

```
! winlogbeat.yml X
C: > ProgramData > Elastic > Beats > winlogbeat > ! winlogbeat.yml
1  ##### Winlogbeat Configuration Example #####
2
3  # This file is an example configuration file highlighting only the most common
4  # options. The winlogbeat.reference.yml file from the same directory contains
5  # all the supported options with more comments. You can use it as a reference.
6  #
7  # You can find the full configuration reference here:
8  # https://www.elastic.co/guide/en/beats/winlogbeat/index.html
9
10 # ===== Winlogbeat specific options =====
11
12 # event_logs specifies a list of event logs to monitor as well as any
13 # accompanying options. The YAML data type of event_logs is a list of
14 # dictionaries.
15 #
16 # The supported keys are name (required), tags, fields, fields_under_root,
17 # forwarded, ignore_older, level, event_id, provider, and include_xml. Please
18 # visit the documentation for the complete details of each option.
19 # https://go.es.io/winlogbeatConfig
20
21 winlogbeat.event_logs:
22   - name: Application
23     ignore_older: 72h
24
25   - name: System
26
27   - name: Security
28     processors:
29       - script:
30         lang: javascript
31         id: security
32         file: ${path.home}/module/security/config/winlogbeat-security.js
33
34   - name: Microsoft-Windows-Sysmon/Operational
35     processors:
```

We need to verify that we are pulling in the Application, System and Security logs

```
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h

  - name: System

  - name: Security
```

We can scroll down to the commented-out section for Elasticsearch

```
158 # ----- Elasticsearch Output -----
159 #output.elasticsearch:
160   # Array of hosts to connect to.
161   #hosts: ["localhost:9200"]
162
163   # Protocol - either `http` (default) or `https`.
164   #protocol: "https"
165
166   # Authentication credentials - either API key or username/password.
167   #api_key: "id:api_key"
168   #username: "elastic"
169   #password: "changeme"
170
```

We will want to use our Humio Elastic ingestion endpoint. For community edition;

```
hosts: ["https://cloud.community.humio.com/api/v1/ingest/elastic-bulk"]
```

and for Enterprise customers in the US

```
hosts: ["https://cloud.us.humio.com/api/v1/ingest/elastic-bulk"]
```

and in the EU

```
hosts: ["https://cloud.humio.com/api/v1/ingest/elastic-bulk"]
```

Note: You can see all endpoint URLs in [Humio Endpoints Documentation](#)

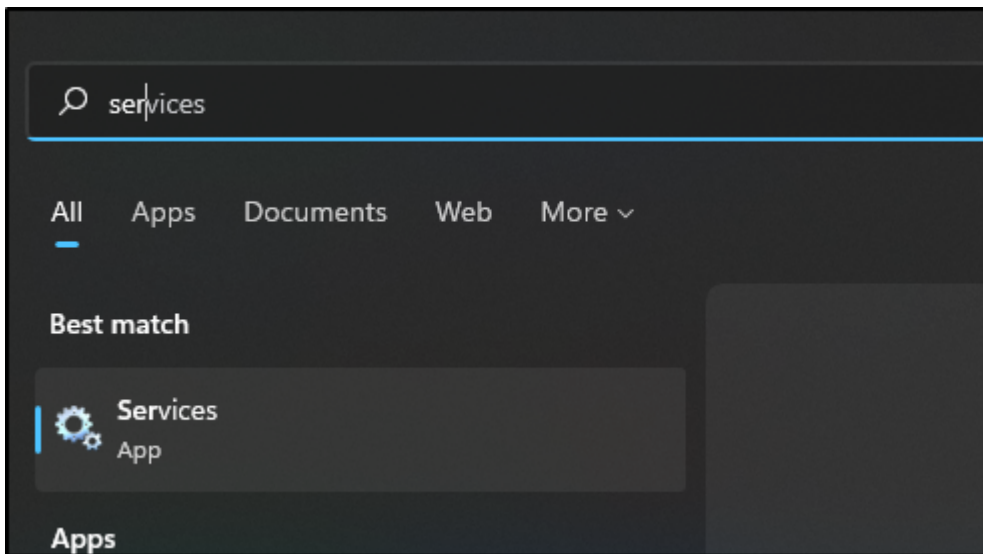
The password will be your Humio Repository ingest token

```
password: "*****"
```

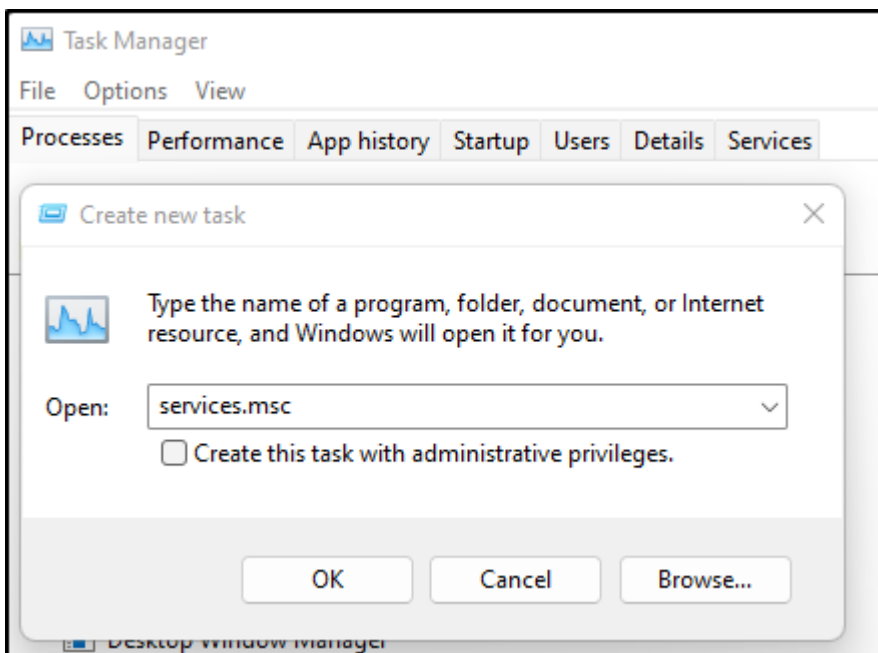
Lastly, ensure we are using the HTTPS endpoint:

```
protocol: "https"
```

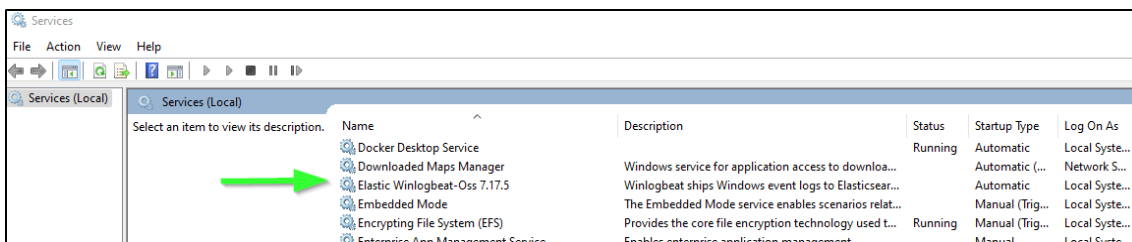
Once saved, we can open up Services by either searching for Services



or going to the Task Manager, choosing File/Run New Task and entering "services.msc"



And there we should find the Winlogbeat service



Right-click and chose start.

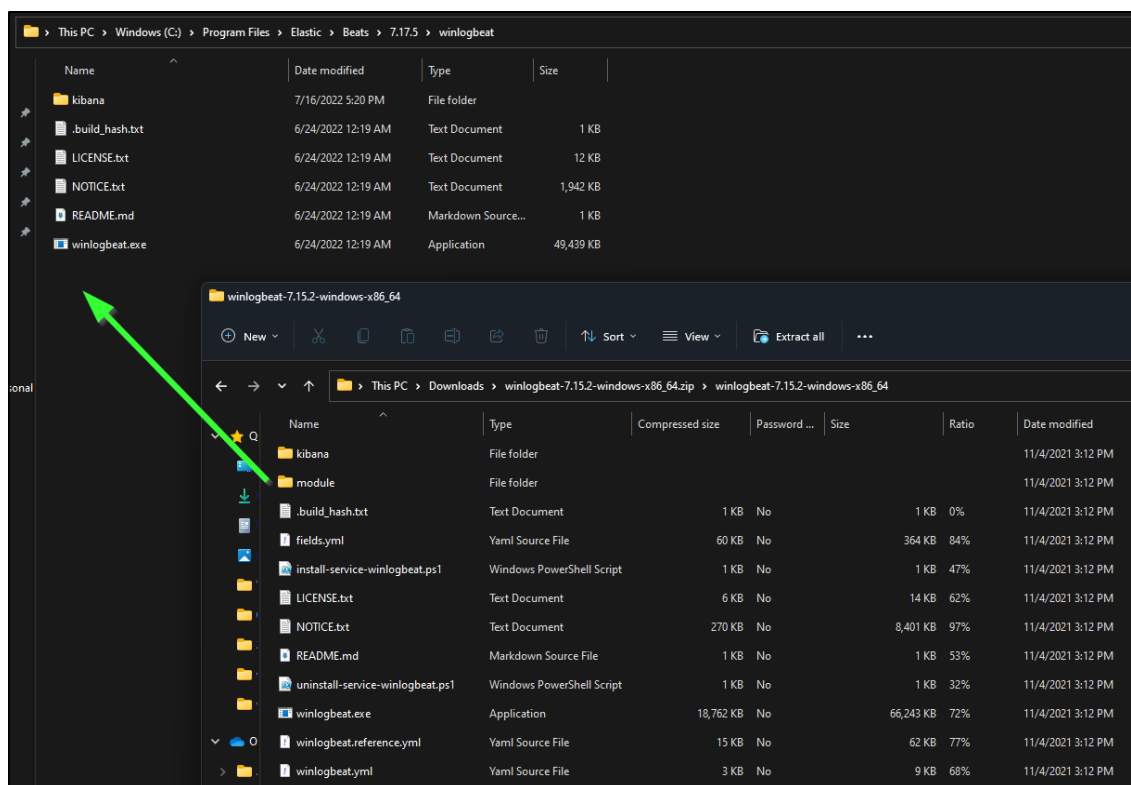
Validating Configurations

If you have troubles starting Winlogbeat, it could be the configuration YAML file. You can test the file using the winlogbeat command prompt with the option of `config test *`

For example, here I errantly had two configured outputs:

```
C:\ProgramData\Elastic\Beats\winlogbeat>"C:\Program
Files\Elastic\Beats\7.17.5\winlogbeat.cmd" test config winlogbeat.yml
Exiting: error unpacking config data: more than one namespace configured accessing
'output' (source:'C:\ProgramData\Elastic\Beats\winlogbeat\winlogbeat.yml')
```

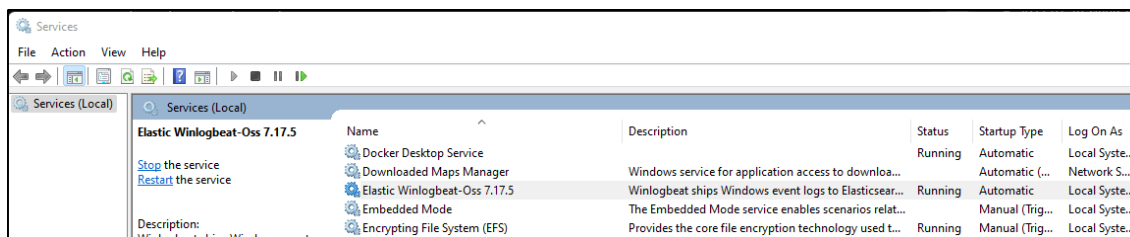
In another case, I found the MSI did *not* install the required modules folders. If these should still be absent, you can pull them from the Zip file download and copy them to the binary folder of WinLogbeat



If your installation is setup proper, and your YAML is valid, the `test config` should give a result of "Config OK"

```
C:\ProgramData\Elastic\Beats\winlogbeat>"C:\Program
Files\Elastic\Beats\7.17.5\winlogbeat.cmd" test config winlogbeat.yml
Config OK
```

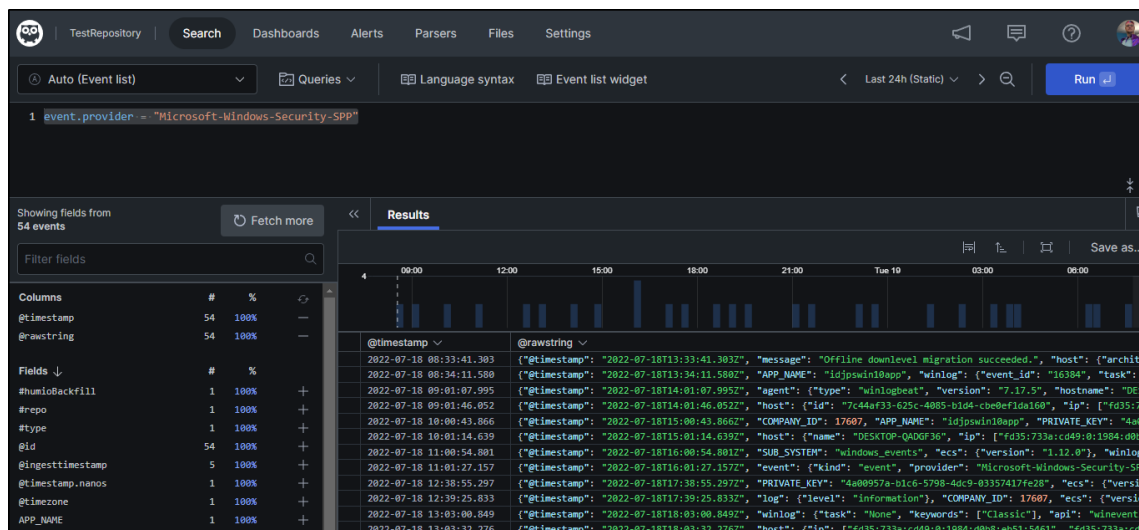
When started, you should see the Service is running



Seeing Results

We can now login to Humio.com and see results populate in our TestRepository.

For instance, we can trim our search results to just the Windows Security SPP entries using the query `event.provider = "Microsoft-Windows-Security-SPP"`

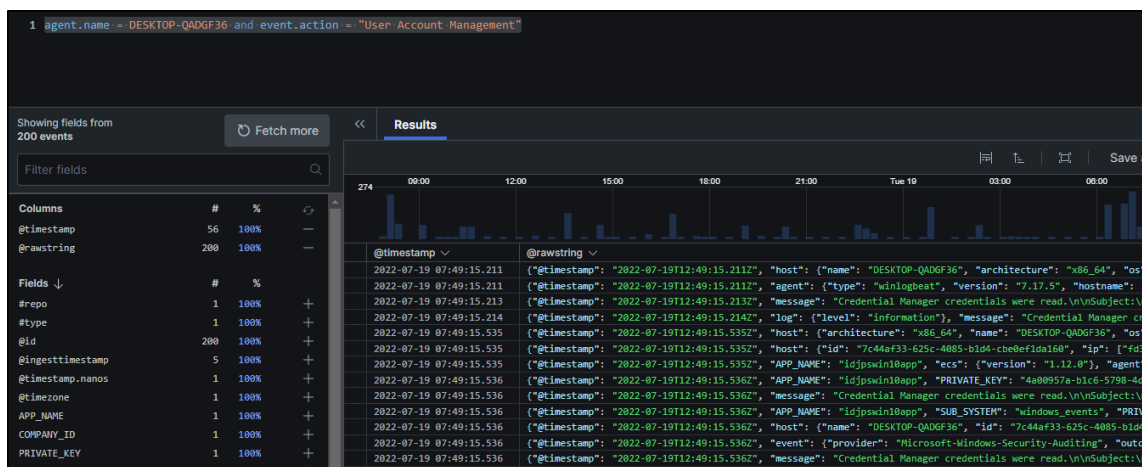


Looking at a give result, we can see some of the many fields Humio collects on our behalf

2022-07-18 12:39:25.833	{ "@timestamp": "2022-07-18T17:39:25.833Z", "log": { "level": "information" }, "COMPANY_ID": 17607, "ecs": { "vers
2022-07-18 13:03:00.849	{ "@timestamp": "2022-07-18T18:03:00.849Z", "winlog": { "task": "None", "keywords": ["Classic"], "aoi": "winevent

Fields	Message	JSON
Filter fields, separate by comma		
Navigate events with Alt-Ctrl-↑/↓		
2022-07-18T12:39:25.833-05:00		
@timestamp	1658165965833	(2022-07-18 17:39:25 UTC)
@timestamp.nanos	0	
@timezone	Z	
agent.ephemeral_id	b66b002f-0f0b-4159-8948-3755d0f572ea	
agent.hostname	DESKTOP-QADGF36	
agent.id	20de2246-597a-4e9a-8bb9-7393c70a71e6	
agent.name	DESKTOP-QADGF36	
agent.type	winlogbeat	
agent.version	7.17.5	
APP_NAME	idjpswin10app	
COMPANY_ID	17607	
ecs.version	1.12.0	
event.action	None	
event.code	16384	
event.created	2022-07-19T12:46:39.339Z	
event.kind	event	
event.provider	Microsoft-Windows-Security-SPP	
host.architecture	x86_64	
host.hostname	DESKTOP-QADGF36	
host.id	7c44af33-625c-4085-b1d4-cbe0ef1da160	
host.ip[0]	fd35:733a:cd49:0:1984:d0b8:eb51:5461	
host.ip[10]	169.254.110.180	
host.ip[11]	fe80::19f8:5fcb:39fe:fe5d	
host.ip[12]	169.254.254.93	
host.ip[13]	fe80::28e4:6262:e7d6:c458	
host.ip[14]	169.254.196.88	
host.ip[15]	fe80::d9bc:867e:a956:cbaa	
host.ip[16]	169.254.203.170	
host.ip[17]	fe80::1d6:808b:4bb5:a0be	

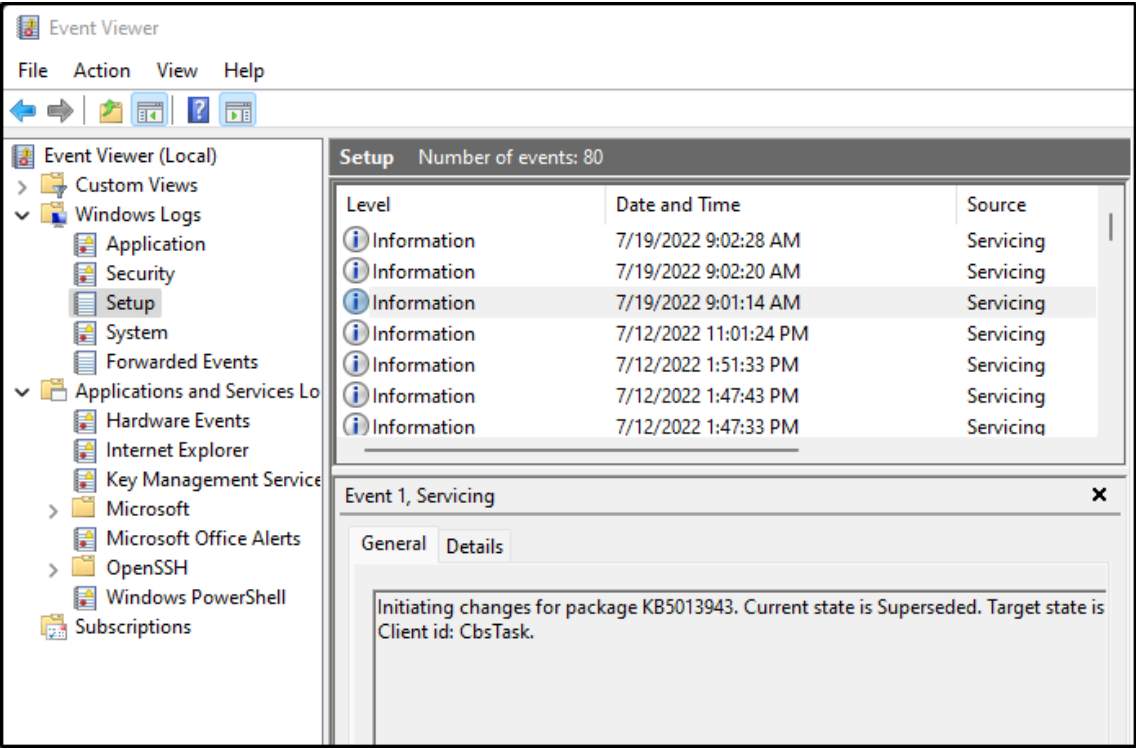
For instance, we may wish to just lookup User Event Management activities on a given host. We could do that with the query `agent.name = (Hostname)` and `event.action = "User Account Management"`



An example: Collecting Setup Events from Windows

Say we wished to track Windows Setup events.

We can open the Event Viewer to see the name of the Log we wish to capture



Seeing it is "Setup", we can update our WinLogbeat config YAML file to add a line for that log

```
*winlogbeat.yml - Notepad

File Edit View
F E V

##### Winlogbeat Configuration Example #####

# This file is an example configuration file highlighting only the most common
# options. The winlogbeat.reference.yml file from the same directory contains
# all the supported options with more comments. You can use it as a reference.
#
# You can find the full configuration reference here:
# https://www.elastic.co/guide/en/beats/winlogbeat/index.html

# ===== Winlogbeat specific options =====

# event_logs specifies a list of event logs to monitor as well as any
# accompanying options. The YAML data type of event_logs is a list of
# dictionaries.
#
# The supported keys are name (required), tags, fields, fields_under_root,
# forwarded, ignore_older, level, event_id, provider, and include_xml. Please
# visit the documentation for the complete details of each option.
# https://go.es.io/WinlogbeatConfig

winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h

  - name: System

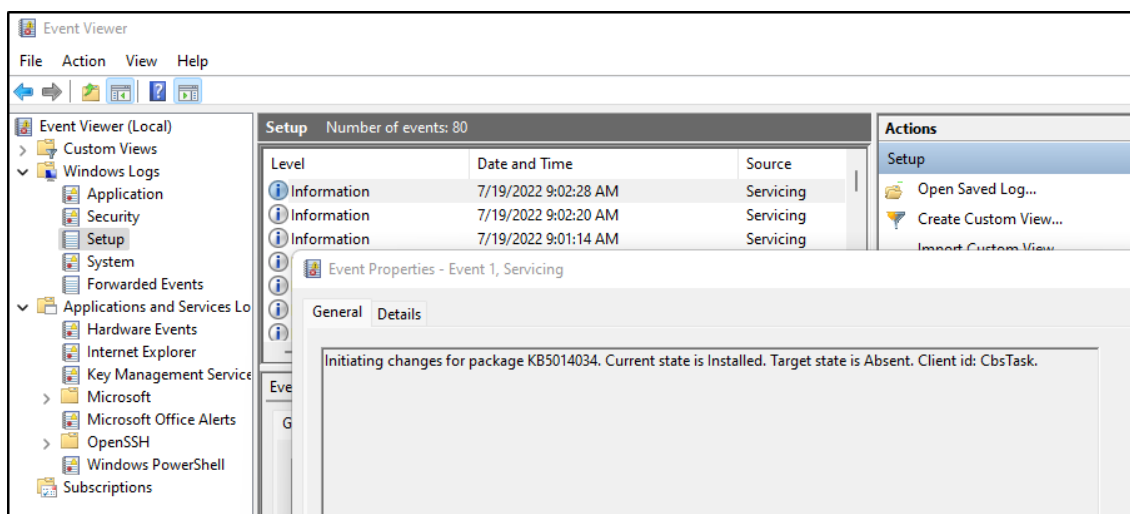
  - name: Setup

  - name: Security
    processors:
      - script:
        lang: javascript
        id: security
        file: ${path.home}/module/security/config/winlogbeat-security.js
```

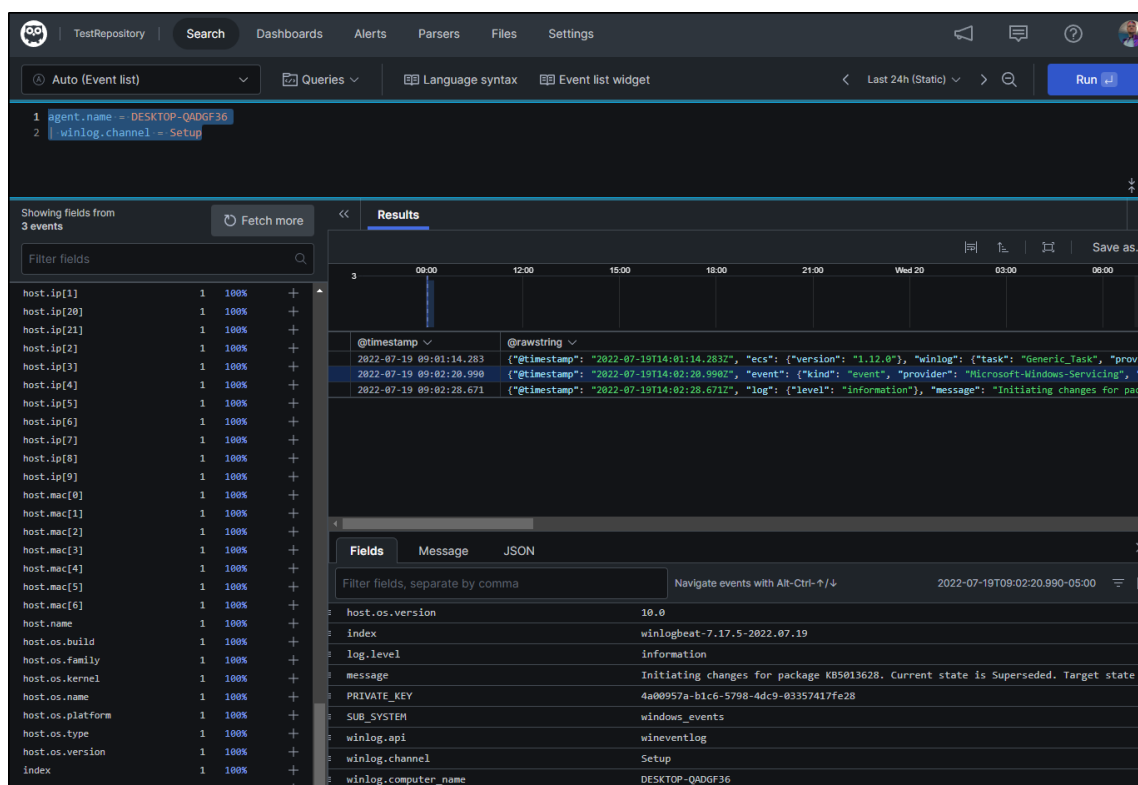
Then right-click and chose restart on the WinLogBeat service to have the changes take effect

Services (Local)			
Elastic Winlogbeat-Oss 7.17.5			
Stop the service Restart the service Description: Winlogbeat ships Windows event logs to Elasticsearch or Logstash	Name	Description	Status
	Docker Desktop Service		Running
	Downloaded Maps Manager	Windows service for application access to downloa...	
	Elastic Winlogbeat-Oss 7.17.5	Winlogbeat ships Windows event logs to Elasticsear...	Running
	Embedded Mode	The Embedded Mode service enables scenarios relat...	
	Encrypting File System (EFS)	Provides the core file encryption technology used t...	Running
	Enterprise App Management Service	Enables enterprise application management.	
	Extensible Authentication Protocol	The Extensible Authentication Protocol (EAP) servic...	
Fax			
Enables you to send and receive faxes, utilizing fax r...			

We can verify this is working by looking at our Windows Event viewer for a recent Setup event



and using the Humio Query `agent.name = (HOST NAME) | winlog.channel = Setup` we can see the results in our Humio Repository



Adding more Logs

We can see the full list of logs we could add by using the Powershell command `Get-WinEvent -ListLog *` | `Format-Table -Property LogName` in an Administrative Powershell Prompt

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Get-WinEvent -ListLog * | Format-Table -Property LogName

LogName
-----
Windows PowerShell
System
Security
OALerts
Key Management Service
Internet Explorer
HardwareEvents
Application
Windows Networking Vpn Plugin Platform/OperationalVerbose
Windows Networking Vpn Plugin Platform/Operational
SMSApi
Setup
RemoteDesktopServices-RemoteFX-SessionLicensing-Operational
RemoteDesktopServices-RemoteFX-SessionLicensing-Admin
OpenSSH/Operational
OpenSSH/Admin
Network Isolation Operational
Microsoft-WindowsPhone-Connectivity-WiFiConnSvc-Channel
Microsoft-Windows-ZTraceMaps/Operational
Microsoft-Windows-WWAN-SVC-Events/Operational
Microsoft-Windows-WPD-MTPClassDriver/Operational
```

Summary

In this article we showed how easy it is to add Windows monitoring to Humio by using the freely available WinLogBeat log shipper on your Windows Hosts. We walked through the installation and configuration of WinLogBeat Open-Source Edition. This included troubleshooting and YAML configuration validation steps. We then verified the installation by ingesting Application, System and Security Events. Lastly, we walked through how to add another Event Log, "Setup" to track and display Setup events in our Humio Repository.

Links for more Information

- [Humio Documentation on WinLogBeat](#)
- [Troubleshooting WinLogBeat and Logstash](#)
- [Elastic setup guide on WinLogBeat](#)