

# So you want to do some logging. . . (PT. 4 Importing Logs from a Domain Controller and Sysmon)

 [blog.iso365down.com/so-you-want-to-do-some-logging-pt-4-importing-logs-from-a-domain-controller-and-sysmon-7bcac9407c62](https://blog.iso365down.com/so-you-want-to-do-some-logging-pt-4-importing-logs-from-a-domain-controller-and-sysmon-7bcac9407c62)

HanSolo71

December 10, 2023

Now that we have a working Graylog instance, its time to start importing data. Our first data will come from our domain controller(s) and the Microsoft Sysinternals Sysmon instance we will be installing and configuring on the domain controller(s).



Gather as much data from as many sources as you can

This is going to be one of my longer blog posts with a lot of moving parts. By the end of this blog we will have configured and discussed the following items.

- Index Set(s)
- Basic Log Types
- Microsoft Sysinternals Sysmon
- Graylog Sidecar

## Index Set(s)

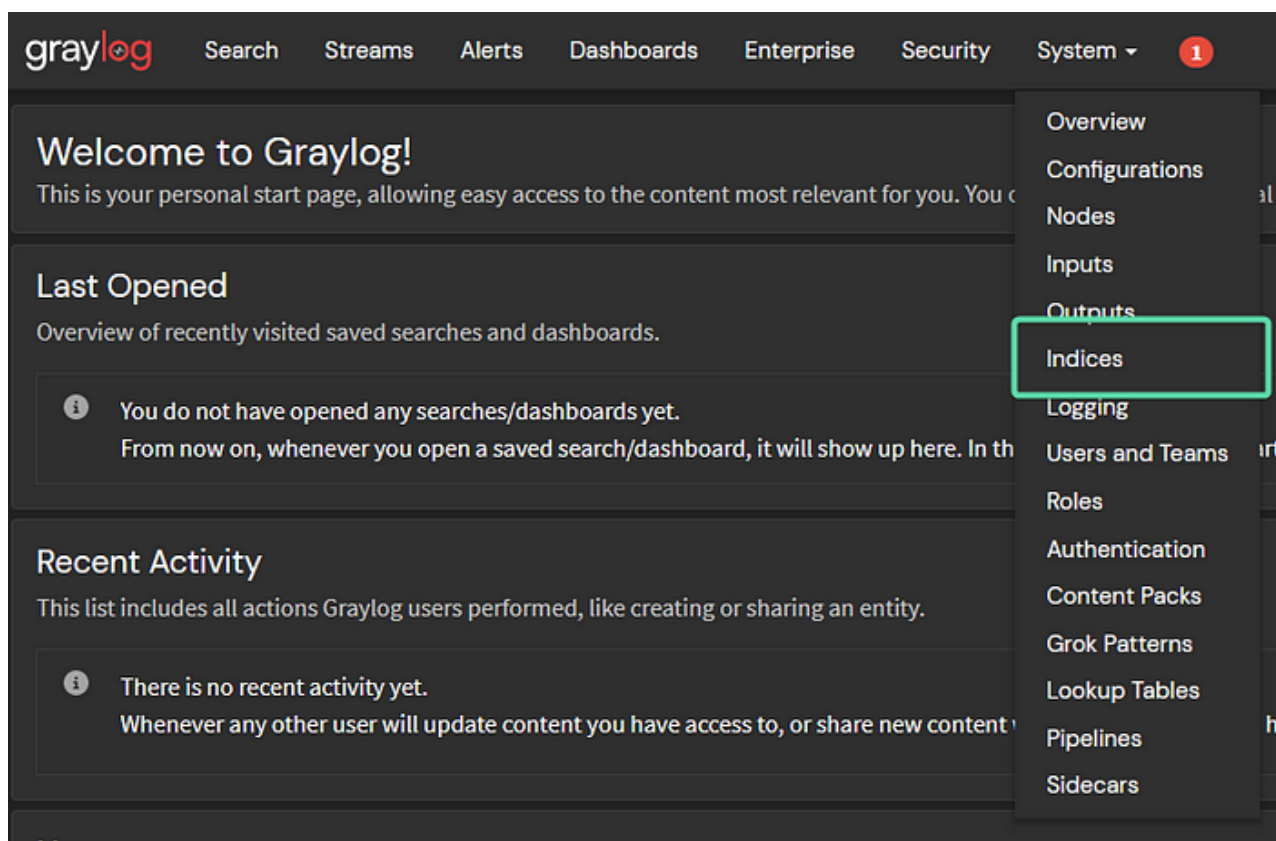
---

Before moving forward lets make some new index sets. Index sets serve a couple purposes.

- Break data up into different data sets for performance and parallelization
- Provide different retention strategies for different data types
- Customize index settings based on data type and needs

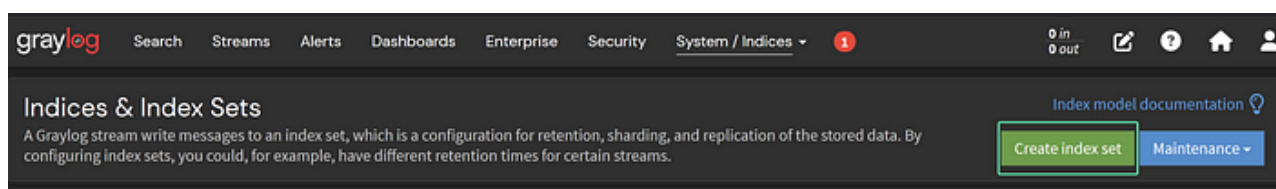
For this demo we will be breaking our up indexes based on our where our data originates. Each part of the blog series going forward will include a section were we create a new index set for the new data we are importing.

To make a new index set, use the top menu and select **System > Indices**.



To make a new index set, use the top menu and select

Then select **Create index set**.



Time to make our first index sets

Because we are focusing on configuring Graylog for the first time with a basic combined Graylog and Opensearch instance we do not need to worry about shard, replica, or segment settings.

We will only need to worry about *Title* and *Index prefix* fields for along with rotation strategy.

Rotation strategy defines how Graylog determines when it is time to rotate a index. Rotating indexes serves to purposes. In distributed systems it can help with performance as different indexes can be served by different nodes.

In all systems it also defines how long data is stored.

- Index Time Size Optimizing
- Index Time
- Index Size
- Index Message Count

Because I am focused on compliance and compliance cares about data retention, this blog will only use index time as a rotation strategy.

## Active Directory Logs

---

Title the active directory index and create unique prefix

We will want our Active Directory logs in their own index set as Active Directory is the heart of authentication in many environments. With that in mind, its best to have longer retention times on these logs.

An attacker may lay low in an environment slowly making changes to provide access and backdoor. Without long term logs it may not be possible to determine all of the changes made by an attacker and what systems they accessed.

Because of this I recommend having at least a 90 day storage for Active Directory Logs.

### Index Rotation Configuration

**Graylog uses multiple indices to store documents in. You can configure the strategy it uses to determine when to rotate the currently active write index.**

**Select rotation strategy** Index Time

**Rotation period (ISO8601 Duration)** P1D a day  
 How long an index gets written to before it is rotated. (i.e. "P1D" for 1 day, "PT6H" for 6 hours).

**Empty index set** ☒ Rotate empty index set  
 Apply the rotation strategy even when the index set is empty (not recommended).

### Index Retention Configuration

**Graylog uses a retention strategy to clean up old indices.**

**Select retention strategy** Delete Index

**Max number of indices** 90  
 Maximum number of indices to keep before **deleting** the oldest ones

Create index set Cancel

These setting will create a new index every day and delete the oldest index when index 91 is created

To do this, we will use a rotation strategy of **Index Time** with a duration of **P1D**. We want to set the retention strategy to **Delete Index** and set the max number of indices to 90.

These setting will create a new index every day and delete the oldest index when index 91 is created

## Windows Generic ETW Logs

Generic Windows ETW logs could consist of anything from system messages, hardware alerts, OS errors, or application logs. If we don't create a index for a specific type of Windows ETW log they will end up in this index.

<b>Title</b>	Windows Generic ETW Logs Descriptive name of the index set.
<b>Description</b>	Windows Generic ETW Logs Add a description of this index set.
<b>Index prefix</b>	etw A <b>unique</b> prefix used in Elasticsearch indices belonging to this index set. The prefix must start with a letter or number, and can only contain letters, numbers, '-', '_' and '+'.  <input type="text"/>

Title the ETW Logs and give them a unique prefix

Depending on the environment you may want to keep logs longer than the 30 days I have chosen

The screenshot shows the 'Index Rotation Configuration' and 'Index Retention Configuration' sections of the Graylog web interface. The 'Index Rotation Configuration' section includes a help message, a 'Select rotation strategy' dropdown set to 'Index Time', a 'Rotation period (ISO8601 Duration)' field set to 'P1D' with a 'a day' unit selector, and an 'Empty index set' checkbox labeled 'Rotate empty index set' which is checked. The 'Index Retention Configuration' section includes a help message, a 'Select retention strategy' dropdown set to 'Delete Index', and a 'Max number of indices' field set to '30'. At the bottom of the retention section are 'Update index set' and 'Cancel' buttons.

**Index Rotation Configuration**

Graylog uses multiple indices to store documents in. You can configure the strategy it uses to determine when to rotate the currently active write index.

**Select rotation strategy** Index Time

**Rotation period (ISO8601 Duration)** P1D a day  
How long an index gets written to before it is rotated. (i.e. "P1D" for 1 day, "PT6H" for 6 hours).

**Empty index set** ☒ Rotate empty index set  
Apply the rotation strategy even when the index set is empty (not recommended).

**Index Retention Configuration**

Graylog uses a retention strategy to clean up old indices.

**Select retention strategy** Delete Index

**Max number of indices** 30  
Maximum number of indices to keep before **deleting** the oldest ones

Update index set Cancel

30 days of generic ETW logs should be enough for most environments

## Microsoft Sysinternals Sysmon Logs

Microsoft Sysinternals Sysmon is a tool for Windows systems (Although a beta for Linux exists now) to monitor and log all kinds of activity on a system that could be useful to a security investigation. This is included but not limited to per MS.

- Logs process creation with full command line for both current and parent processes.
- Records the hash of process image files using SHA1 (the default), MD5, SHA256 or IMPHASH.
- Multiple hashes can be used at the same time.
- Includes a process GUID in process create events to allow for correlation of events even when Windows reuses process IDs.
- Includes a session GUID in each event to allow correlation of events on same logon session.
- Logs loading of drivers or DLLs with their signatures and hashes.
- Logs opens for raw read access of disks and volumes.
- Optionally logs network connections, including each connection's source process, IP addresses, port numbers, hostnames and port names.
- Detects changes in file creation time to understand when a file was really created. Modification of file create timestamps is a technique commonly used by malware to cover its tracks.

- Automatically reload configuration if changed in the registry.
- Rule filtering to include or exclude certain events dynamically.
- Generates events from early in the boot process to capture activity made by even sophisticated kernel-mode malware.

Sysmon is loud, creating a crazy amounts of logs. Because of this I highly recommend it has its own Index with a short time-to-live until you validate how much data Sysmon will create in your environment.

<b>Title</b>	Sysmon Logs
	Descriptive name of the index set.
<b>Description</b>	Sysmon Logs
	Add a description of this index set.
<b>Index prefix</b>	sysmon
	A <b>unique</b> prefix used in Elasticsearch indices belonging to this index set. The prefix must start with a letter or number, and can only contain letters, numbers, '_', '-' and '+'.

Title sysmon logs and give the the index a unique prefix

### Index Rotation Configuration

**i** Graylog uses multiple indices to store documents in. You can configure the strategy it uses to determine when to rotate the currently active write index.

<b>Select rotation strategy</b>	Index Time
<b>Rotation period (ISO8601 Duration)</b>	P1D <span>a day</span>
	How long an index gets written to before it is rotated. (i.e. "P1D" for 1 day, "PT6H" for 6 hours).
<b>Empty index set</b>	<input checked="" type="checkbox"/> Rotate empty index set
	Apply the rotation strategy even when the index set is empty (not recommended).

### Index Retention Configuration

**i** Graylog uses a retention strategy to clean up old indices.

<b>Select retention strategy</b>	Delete Index
<b>Max number of indices</b>	7
	Maximum number of indices to keep before <b>deleting</b> the oldest ones

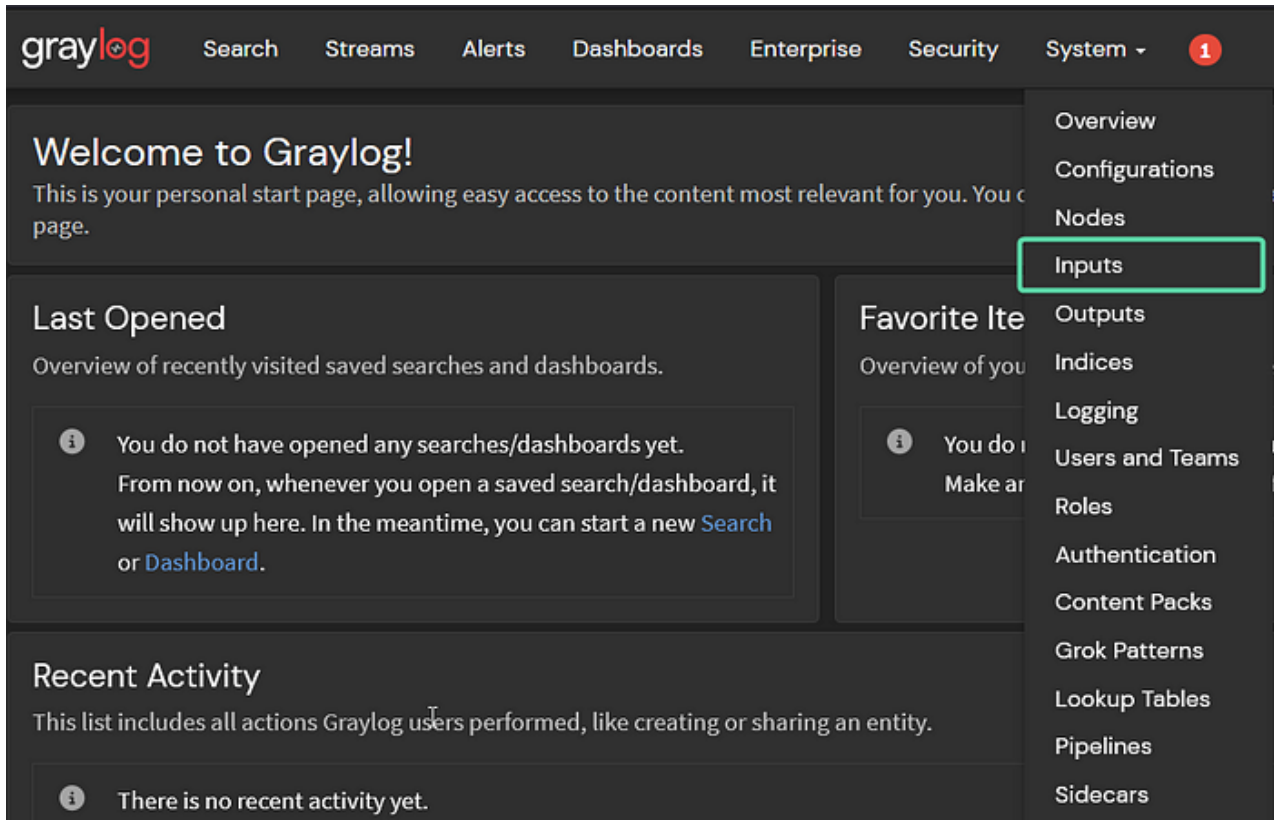
Set the number of indices as low as you want starting out. This blog is starting at 7 days.

## Graylog Sidecar



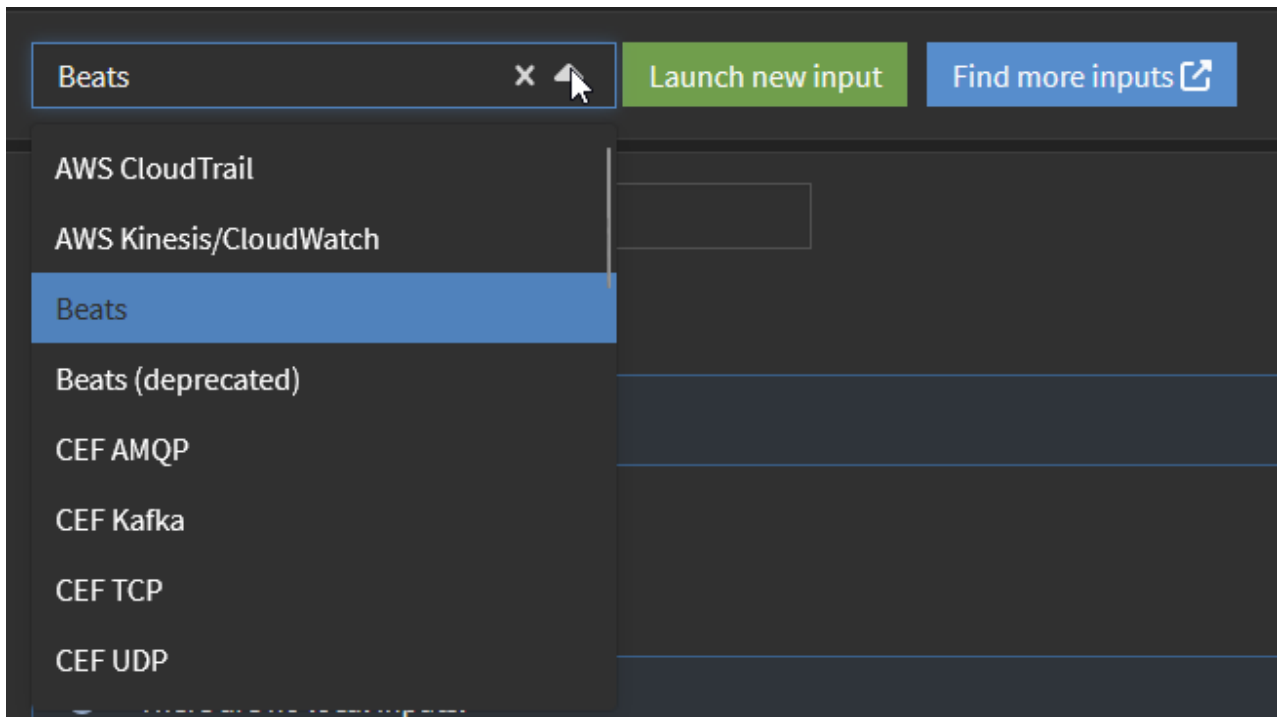
Graylog Sidecar is the name of one of the agents Graylog can use to import data from various remote systems. Another popular alternative is NXLog. For this blog we will be focusing on using as much of the built in Graylog infrastructure as possible.

Before we can install Sidecar we will need to create a network location for Sidecar to send its data. To do this from the top menu select **System > Inputs**



From the top menu select

Create a new beat input by selecting **Beats** from the available inputs.



Create a new beat input by selecting from the available inputs.

With a single server setup we can configure all of our inputs to be global inputs. Along with this we need to set the address we will bind to and the port we will bind to. For this example we are binding on available addresses (0.0.0.0) and the port is 5044.

A screenshot of the Sysmon configuration form for a new input. The form has a dark background. At the top, there is a checkbox labeled 'Global' which is checked. Below it, the text 'Should this input start on all nodes' is displayed. The 'Title' field contains 'Windows Beats'. The 'Bind address' field contains '0.0.0.0'. Below this field, the text 'Address to listen on. For example 0.0.0.0 or 127.0.0.1.' is shown. The 'Port' field contains '5044' and has a small up/down arrow icon to its right.

Name the input, set your bind address and port

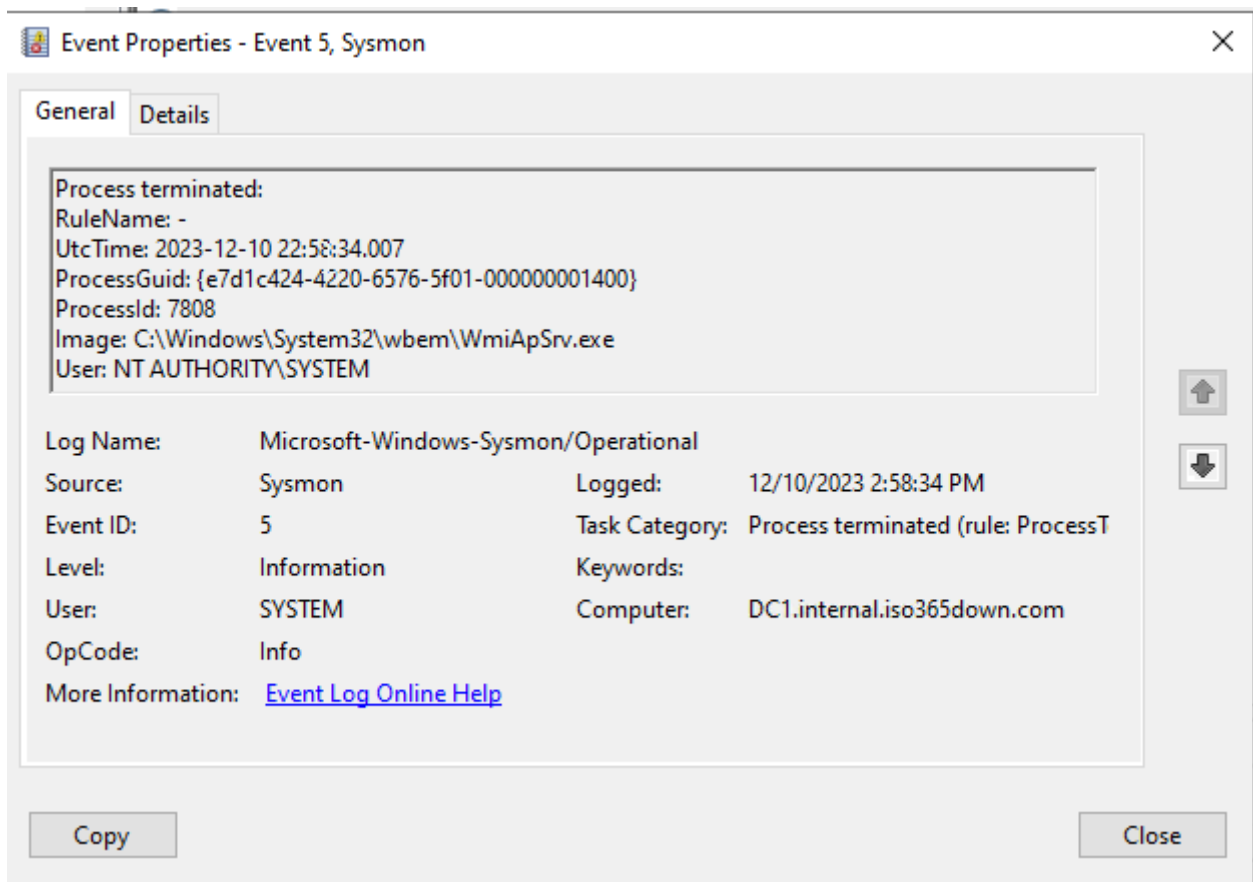
## Installing Sysmon

Now lets install Sysmon. Download sysmon from the included link and install on your Domain Controller with the following command.

```
.\Sysmon64 -accepteula - -h md5 -n -l
```



Once sysmon is installed and started you can verify it is working by visiting **Event Viewer > Applications and Services > Microsoft > Windows > Sysmon**. If working you should see some data in this ETW directory.



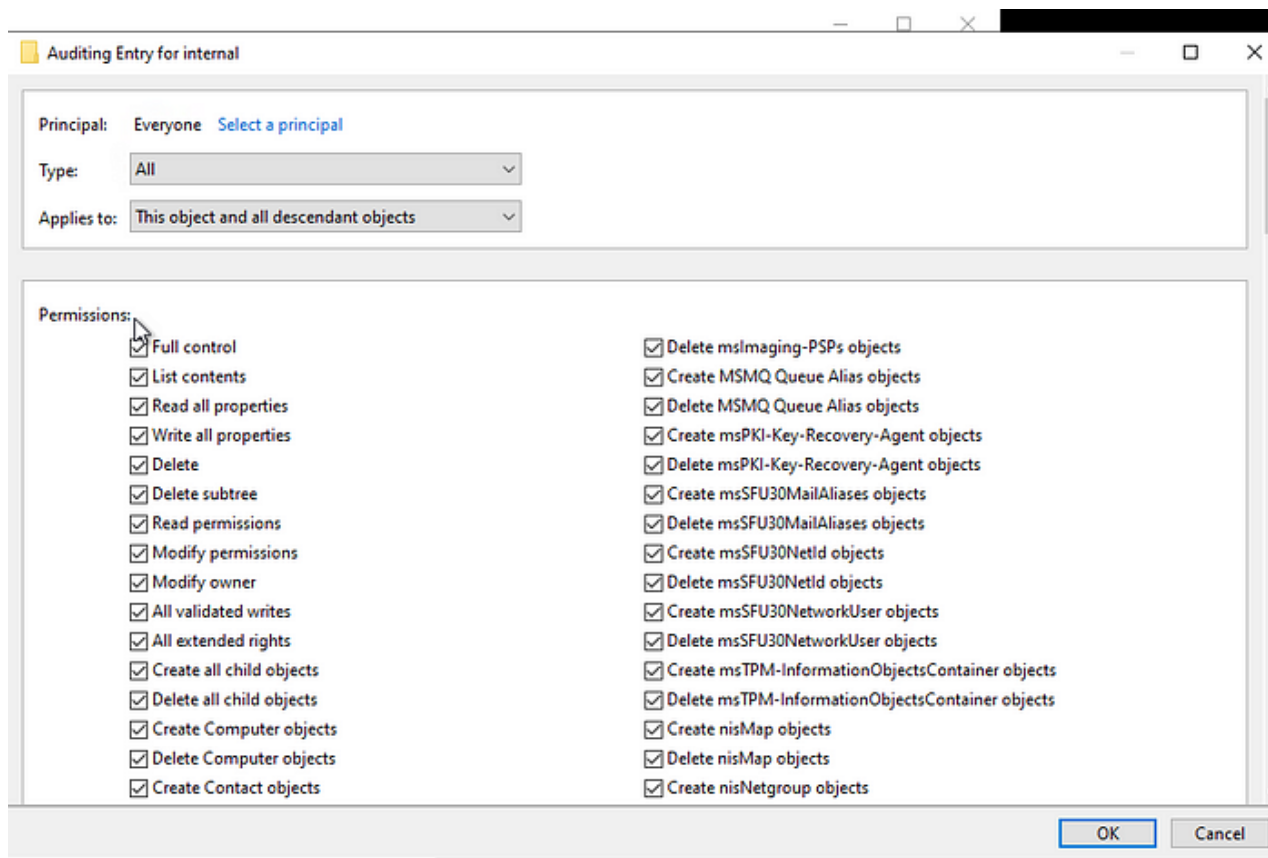
Sysmon Logs

## Enabling AD Logging

Lets extend Active Directories default configuring to give us more data about what is happening.

Open **Active Directory Users and Computers > Active Directory Users and Computers > Domain.name.com > Properties > Security > Advanced > Auditing**

Create a new Audit entry with a principle of *Everyone* and make sure it applies to *this object and all decedent objects*. Make sure to select **Full Control and Read all properties**.

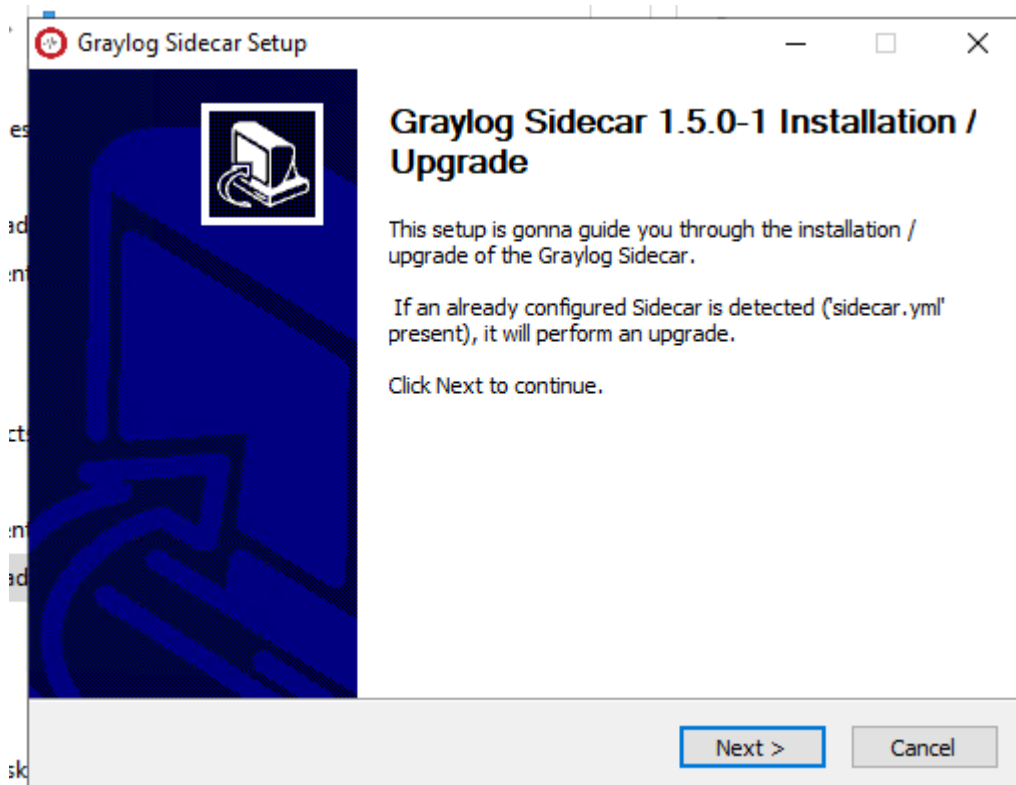


Adding Auditing to AD

## Windows Graylog Sidecar Install

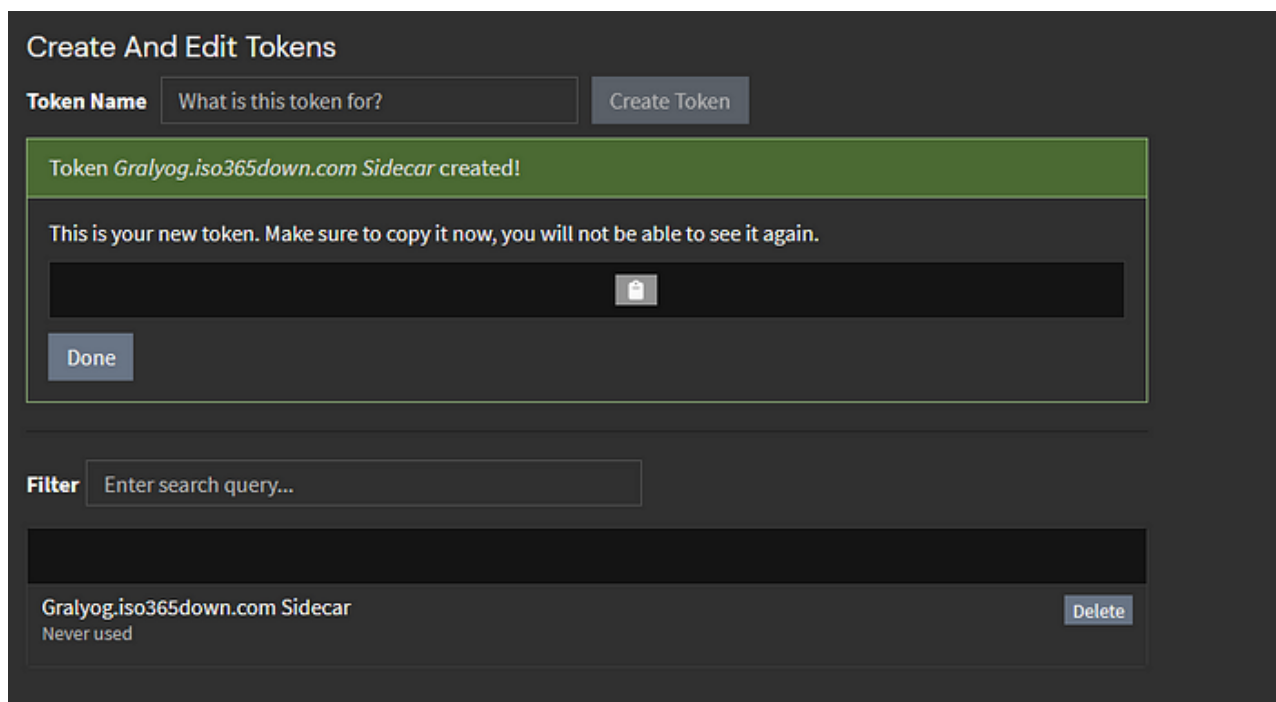
Because we are using Graylog 5.2.2 we can use the Graylog Sidecar 1.5.0 code. It can be downloaded .

After downloading on our domain controller go ahead and start the installation.



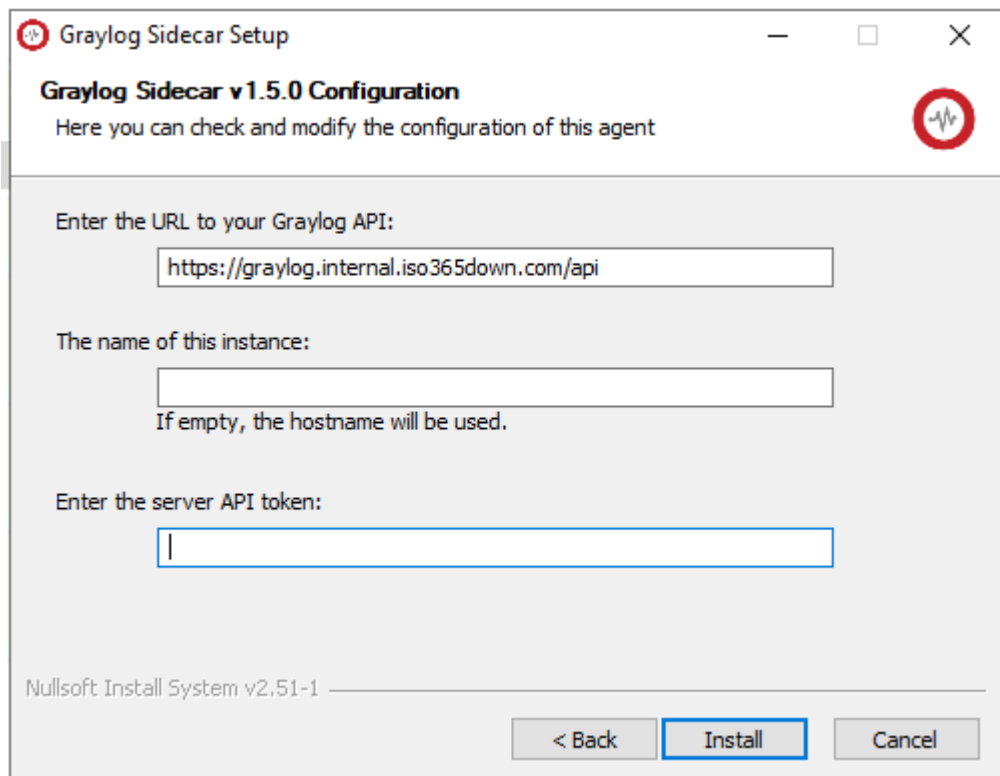
Installing the sidecar

We will also want to gather our API Token this can be found or created in **System > Sidecar > Create or reuse a token for the graylog-sidecar user.**



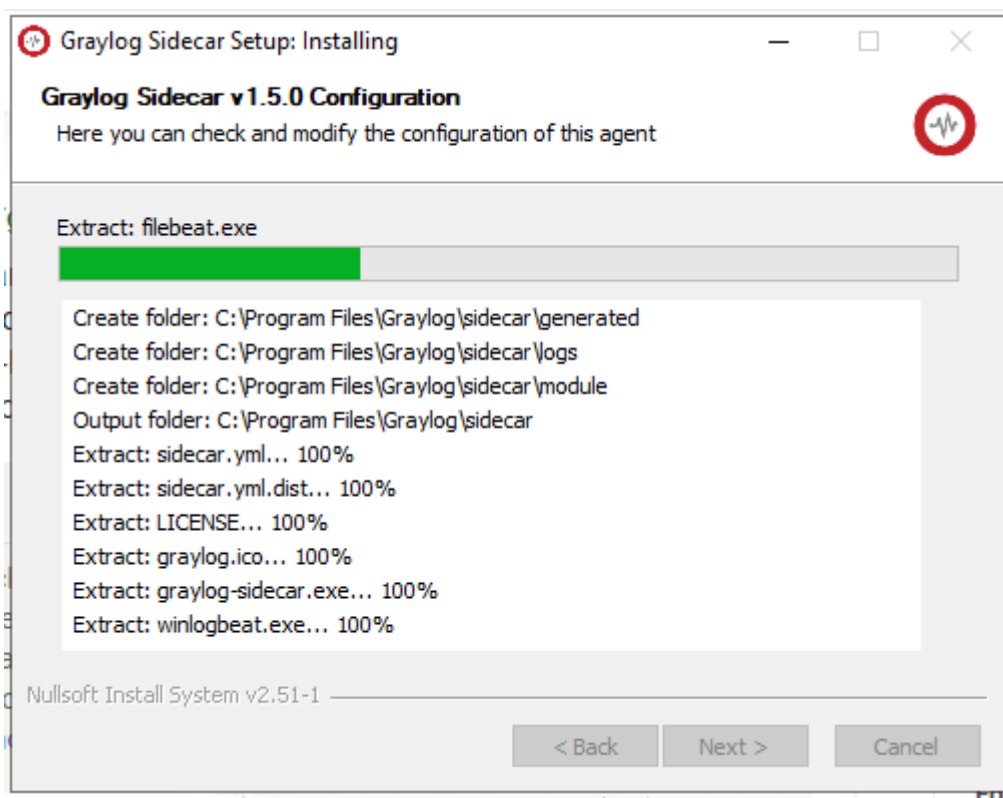
Don't forget to copy and save your token

Make sure you point the system at your graylog instance using a <https://FQDN/api>.



Make sure you use the FQDN you setup

And let it install.



If things are working you should see two things immediately happen. First you will start seeing network I/O

## Throughput / Metrics

1 minute average rate: 0 msg/s

Network IO: ▼2.0KiB ▲0B (total: ▼5.2MiB ▲966.0B)

Active connections: 0 (536 total)

Empty messages discarded: 0

[Show details](#)

Network I/O

Second if you browse back to your sidecar settings under **System > Sidecars** you will see your newly installed system running.

### Sidecars Overview

The Graylog sidecars can reliably forward contents of log files or Windows EventLog from your servers.  
Do you need an API token for a sidecar? [Create or reuse a token for the graylog-sidecar user](#)

Find sidecars [?](#) [Hide inactive sidecars](#) Show 10 Rows ▼

Name ↑	Status ↓	Operating System ↓	Last Seen ↓	Node Id ↓	Sidecar Version ↓	
DC1	Running	Windows	a few seconds ago	8acd4836-797f-458b-85db-b758042a1305	1.5.0	<a href="#">Manage sidecar</a> <a href="#">Show messages</a>

Our new system.

Go ahead and select **Manage sidecar** and edit *winlogbeat* with the following configuration.

```
# Needed for Graylog
fields_under_root:true
fields.collector_node_id:${sidecar.nodeName}
fields.gl2_source_collector:${sidecar.nodeId}

[]
```

## Testing our Data

If you go to your search you will now see data flowing into Graylog.

**Received by**  
Windows Beats on 41fd6254 / graylog.intera  
l.thedownings.org

**message**  
An account was successfully logged on.

**Stored in index**  
graylog\_0

**Routed into streams**

- Default Stream

**Subject:**

Security ID: S-1-0-0  
Account Name: -  
Account Domain: -  
Logon ID: 0x0

**Logon Information:**

Logon Type: 3  
Restricted Admin Mode: -  
Virtual Account: No  
Elevated Token: Yes

**Impersonation Level:** Impersonation

**New Logon:**

Security ID: S-1-5-18  
Account Name: DC1\$  
Account Domain: INTERNAL.ISO365DOWN.COM  
Logon ID: 0x55F550  
Linked Logon ID: 0x0  
Network Account Name: -  
Network Account Domain: -  
Logon GUID: {b577a85d-cdee-b540-4a48-d9ff22a66310}

**Process Information:**

Process ID: 0x0  
Process Name: -

We have logs!

## Sending our Data to the Proper Index

Now that we have lots of different types of data coming into Graylog we will want to start sending it to the various index sets we created earlier.

## Sysmon

Find a sysmon message and keep record of the message ID and index it came from.

2023-12-10 19:53:36.489
DC1

Process Create:  
RuleName: -  
UtcTime: 2023-12-11 00:53:35.429  
ProcessGuid: {e7d1c424-5d8f-6576-4e00-000000001b00}  
ProcessId: 3204

05893037-97ac-11ee-9e47-5254004e74ba
Permalink Show surrounding messages - Test against stream - Copy ID Copy message

**Timestamp**  
2023-12-10 19:53:36.489

**beats\_type**  
winlogbeat

**Received by**  
Windows Beats on 41fd6254 / graylog.intera  
l.thedownings.org

**message**  
Process Create:  
RuleName: -  
UtcTime: 2023-12-11 00:53:35.429  
ProcessGuid: {e7d1c424-5d8f-6576-4e00-000000001b00}  
ProcessId: 3204  
Image: C:\Windows\Sysmon64.exe  
FileVersion: 15.11  
Description: System activity monitor  
Product: Sysinternals Sysmon  
Company: Sysinternals - www.sysinternals.com  
OriginalFileName: -  
CommandLine: C:\Windows\Sysmon64.exe  
CurrentDirectory: C:\Windows\system32\  
User: NT AUTHORITY\SYSTEM  
LogonGuid: {e7d1c424-5d8f-6576-e703-000000000000}  
LogonId: 0x3e7  
TerminalSessionId: 0  
IntegrityLevel: System  
Hashes: MD5=4167707AA71EF596BE07CA0C25FBF094

**Stored in index**  
graylog\_0

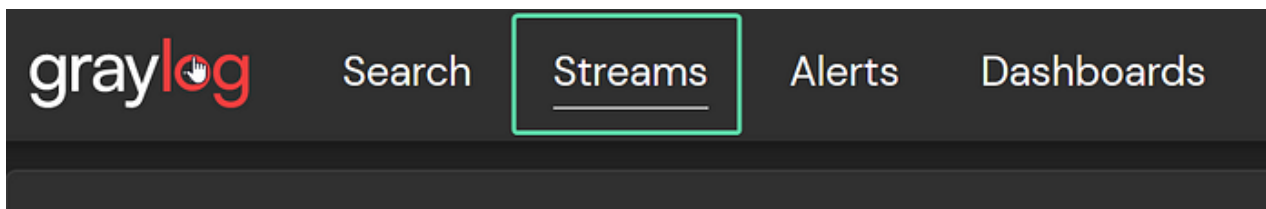
**Routed into streams**

- Default Stream

Note the message ID and index

Now go to **Streams** in the top menu





Enter the streams configuration

Create a new stream named Sysmon and make sure to route the messages to the Sysmon Log index set and remove the messages from the default stream.

The image shows a modal window titled 'Editing Stream' with a close button (X) in the top right corner. The form contains the following fields and options:

- Title**: A text input field containing 'Sysmon'. Below it is a placeholder text: 'A descriptive name of the new stream'.
- Description (Opt.)**: A text input field containing 'Sysmon'. Below it is a placeholder text: 'What kind of messages are routed into this stream?'.
- Index Set**: A dropdown menu showing 'Sysmon Logs'. To the right of the dropdown are a close button (X) and a dropdown arrow.
- Below the Index Set dropdown is a text line: 'Messages that match this stream will be written to the configured index set.'
- A checked checkbox with the label 'Remove matches from 'Default Stream''.
- Below the checkbox is a text line: 'Don't assign messages that match this stream to the 'Default Stream'.'
- At the bottom right are two buttons: 'Cancel' (gray) and 'Update stream' (green).

Name the stream, set the index set it will send data to, and remove the data from the default stream

The newly created stream needs rules configured to send data to it. To do this select **More > Manage Rules**.

Taking the Message ID and Index we saved earlier, load a the message to test against. Search for the field `winlogbeat_event_provider` and make a rule matching the field name `Microsoft-Windows-Sysmon`.

Edit Stream Rule

Field

winlogbeat\_event\_provider

Type

match exactly

Value

Microsoft-Windows-Sysmon

☐ Inverted

Description (Opt.)

Result: winlogbeat\_event\_provider **must** match exactly Microsoft-Windows-Sysmon

Cancel

Update Rule

The server will try to convert to strings or numbers based on the matcher type as well as it can.

[Take a look at the matcher code on GitHub](#)

Regular expressions use Java syntax. ?

Check that your message now matches the rule you have created.



If it is, you are done.

## Windows ETW Logs

We want to move logs coming from the *Application*, *System*, and *Security* logs to go to the Windows ETW Logs. For this rule set we want to ensure we select **A message must match at least one of the following rules**. Otherwise a message would need to be in all three message groups to get routed to our Windows ETW Index

2. Manage stream rules

Add stream rule

☐ A message must match all of the following rules
 ☒ A message must match at least one of the following rules

Please load a message in Step 1 above to check if it would match against these rules.

winlogbeat\_winlog\_channel **must** match exactly Application

winlogbeat\_winlog\_channel **must** match exactly System

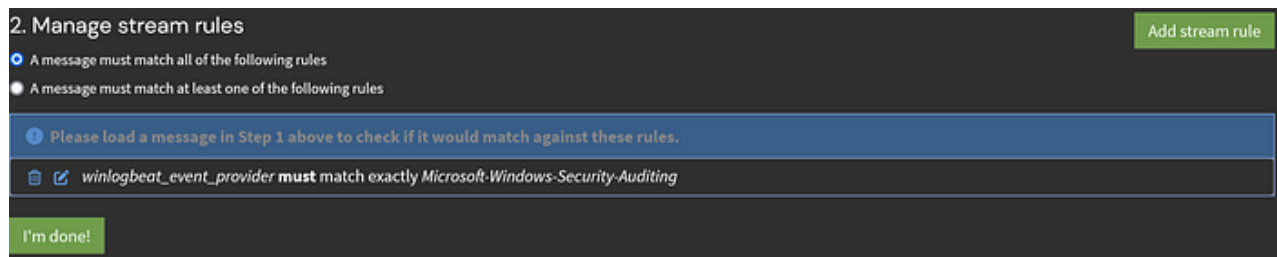
winlogbeat\_winlog\_channel **must** match exactly Security

## Active Directory Logs

Logs from Active Directory are important for security investigations and as such should have a longer retention period than other types of data. By routing our active directory audit logs into the Active Directory Logs index we are able to save logs for 90 days.

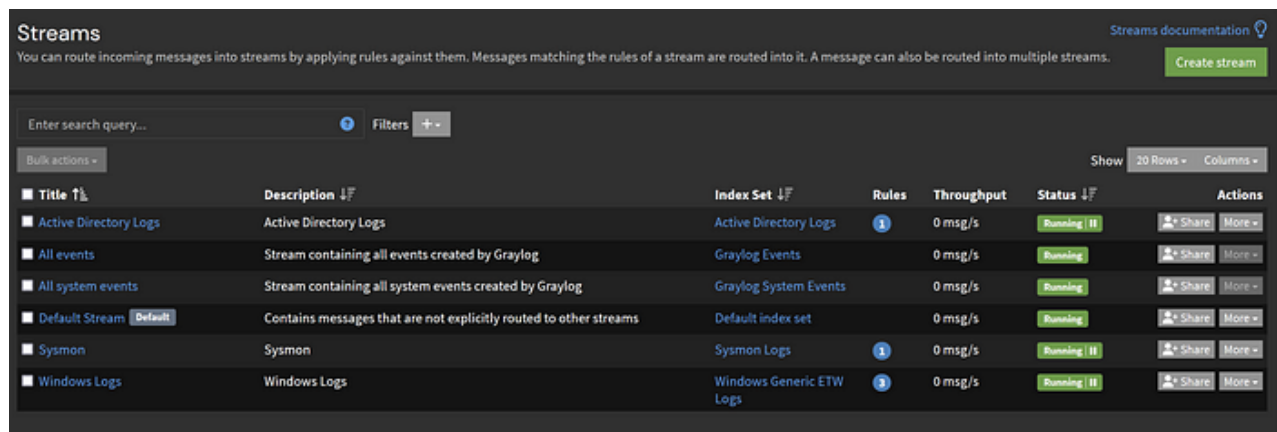
The rule needed for this is simple.

`winlogbeat_event_provider` **must** match exactly `Microsoft-Windows-Security-Auditing`



match exactly

Make sure to start each stream and you should start seeing messages flowing into the indices we created.



Title	Description	Index Set	Rules	Throughput	Status	Actions
Active Directory Logs	Active Directory Logs	Active Directory Logs	1	0 msg/s	Running II	Share More
All events	Stream containing all events created by Graylog	Graylog Events		0 msg/s	Running	Share More
All system events	Stream containing all system events created by Graylog	Graylog System Events		0 msg/s	Running	Share More
Default Stream <small>Default</small>	Contains messages that are not explicitly routed to other streams	Default index set		0 msg/s	Running	Share More
Sysmon	Sysmon	Sysmon Logs	1	0 msg/s	Running II	Share More
Windows Logs	Windows Logs	Windows Generic ETW Logs	2	0 msg/s	Running II	Share More

Don't forget to start your Streams

We can now search logs from Active Directory, Sysmon, and Windows itself.

Our next part will be on adding logging from SMB shares to our stack.



Time to see what you can find