So you want to do some logging. . . (PT. 5 Windows File Share Logs)

blog.iso365down.com/so-you-want-to-do-some-logging-pt-5-windows-file-share-logs-3a31a664dde8

HanSolo71

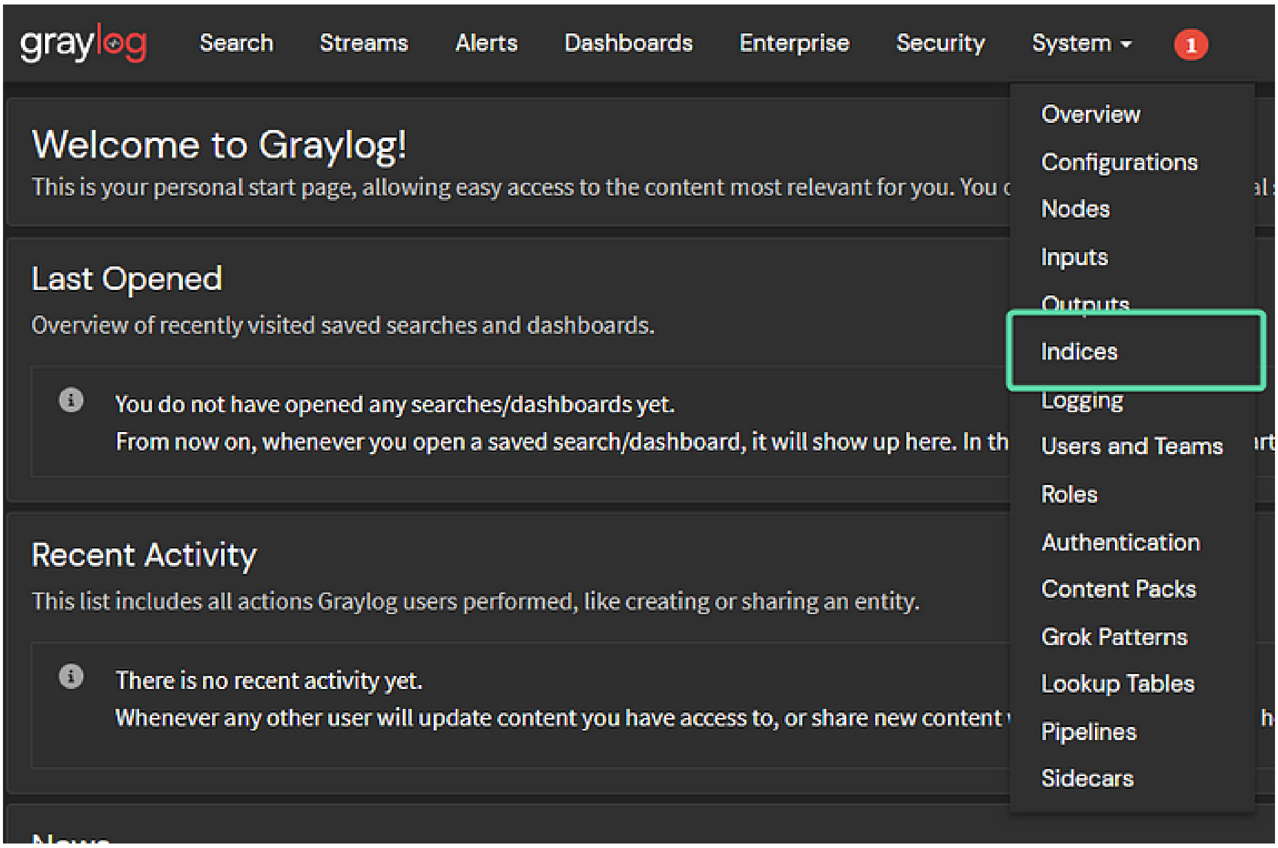
December 16, 2023

Gotta track those files

Creating a New Index

Before moving forward we will want to create a new index in Graylog. Logs from file servers can be very chatty and you may want to change retention based on storage needs.

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



Welcome to Graylog!

This is your personal start page, allowing easy access to the content most relevant for you. You c

Last Opened

Overview of recently visited saved searches and dashboards.

You do not have opened any searches/dashboards yet.
From now on, whenever you open a saved search/dashboard, it will show up here. In th

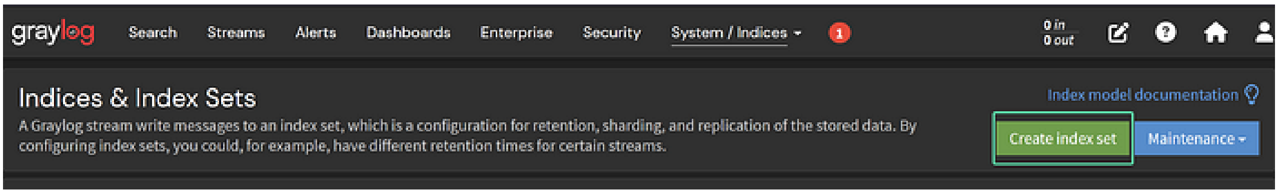
Recent Activity

This list includes all actions Graylog users performed, like creating or sharing an entity.

There is no recent activity yet.
Whenever any other user will update content you have access to, or share new content

Time for a new index!

Then select **Create index set.**

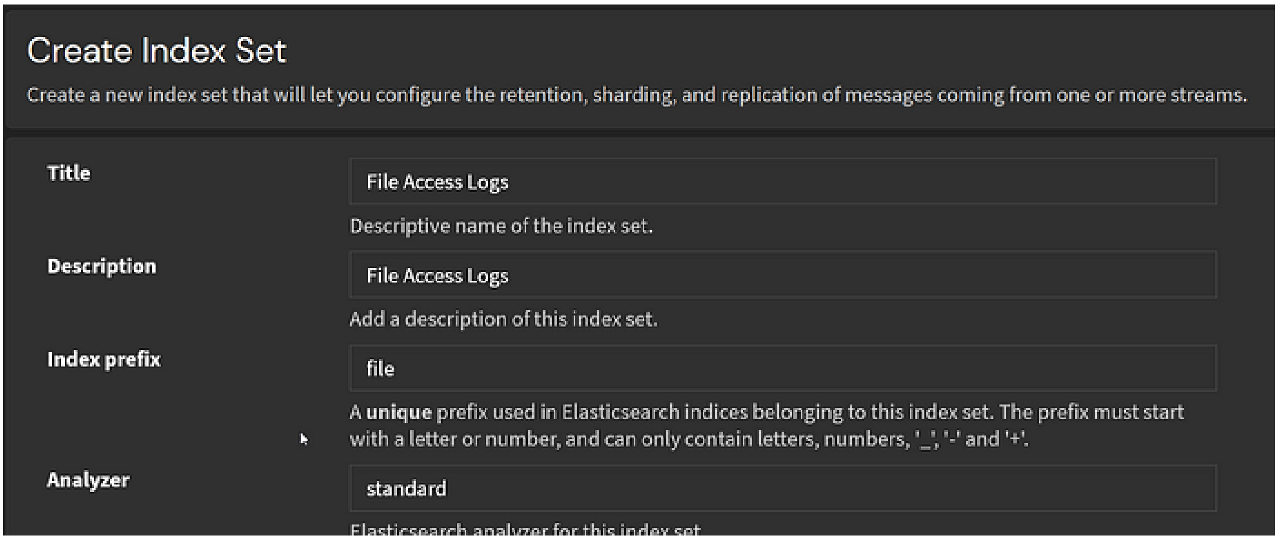


Indices & Index Sets

A Graylog stream write messages to an index set, which is a configuration for retention, sharding, and replication of the stored data. By configuring index sets, you could, for example, have different retention times for certain streams.

Make the new index

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



Create Index Set

Create a new index set that will let you configure the retention, sharding, and replication of messages coming from one or more streams.

Title: File Access Logs
Descriptive name of the index set.

Description: File Access Logs
Add a description of this index set.

Index prefix: file
A **unique** 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 '+'.

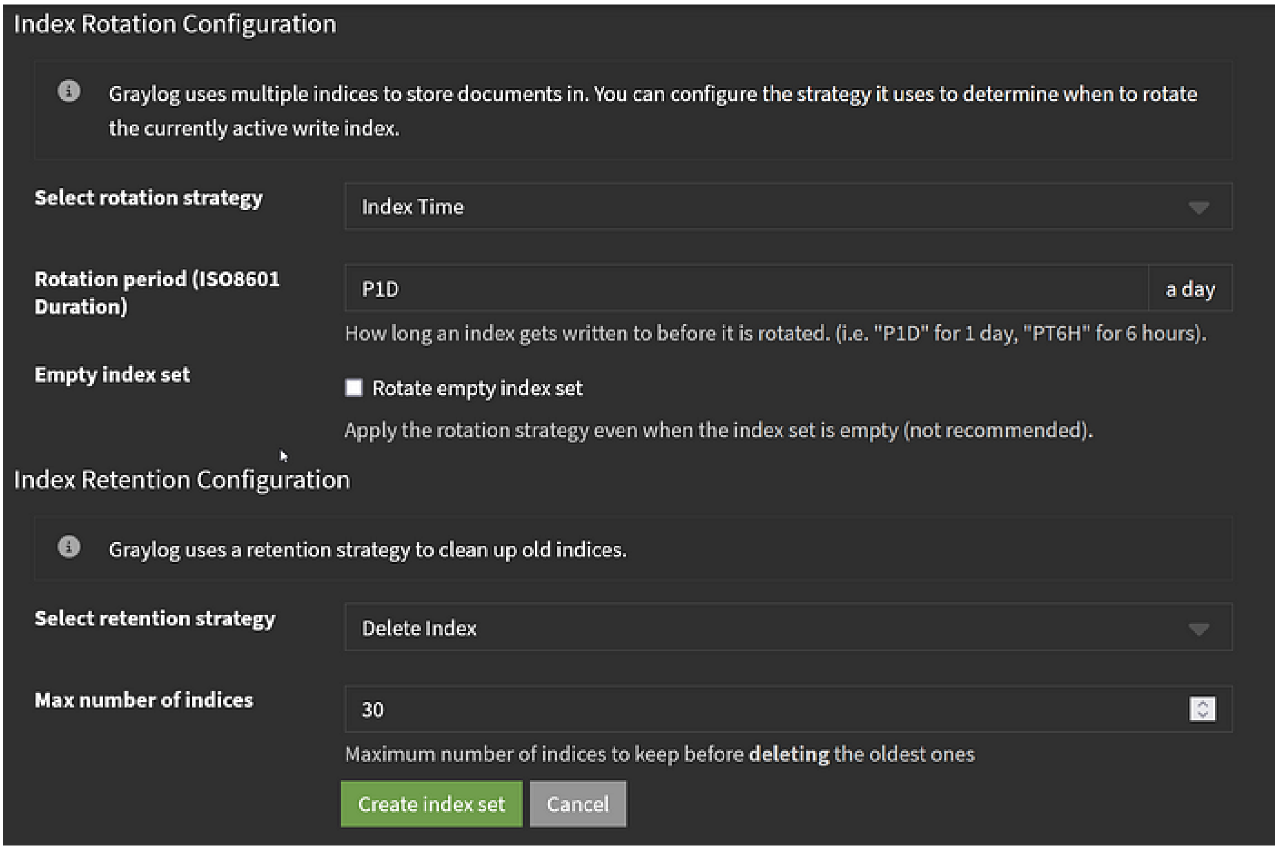
Analyzer: standard
Elasticsearch analyzer for this index set.

Title the File Share Logs and give them a unique prefix

We want to keep our file access logs for 30 days.

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 30.

These setting will create a new index every day and delete the oldest index when index 31 is created



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

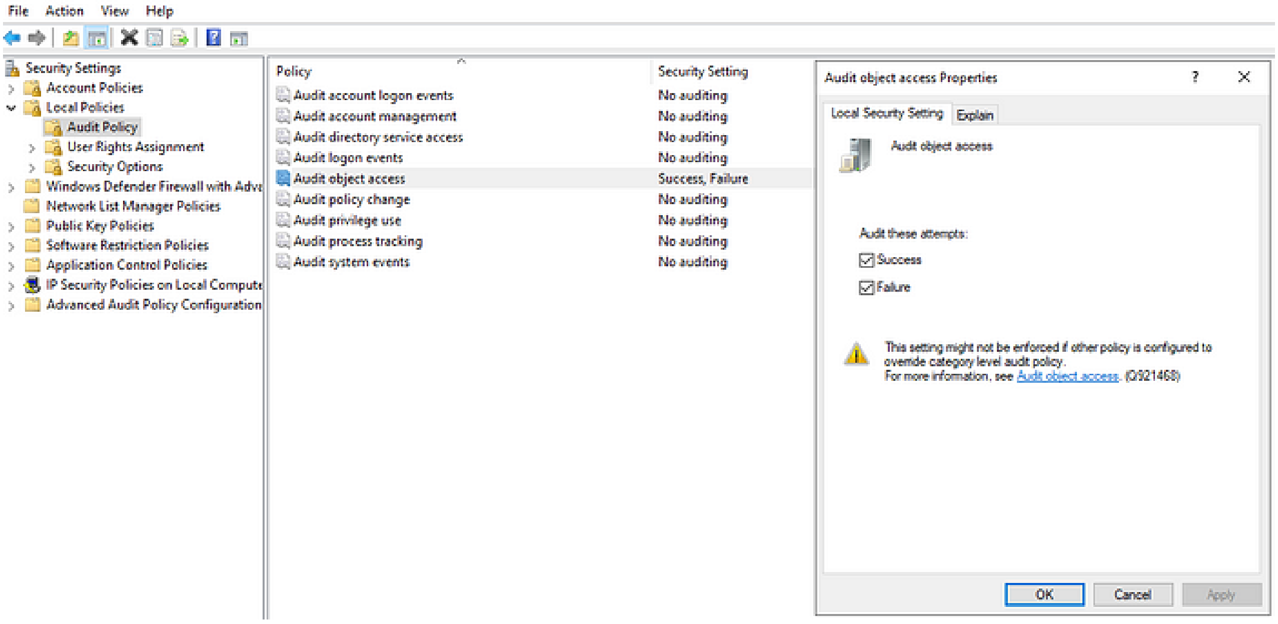
Maximum number of indices to keep before **deleting** the oldest ones

These setting will create a new index every day and delete the oldest index when index 31 is created

Enabling File Auditing in the OS

Before adding any auditing rules to our files we will need to enable **Audit Object Access.** This can be done from **Group Policy** centrally or **Local Security policy** locally.

To start we will want to edit the **Security Policy.** Browse to **Security Settings > Local Polices > Audit Policies.** From there enable **Audit Object Access** on both **Success and Failure.**


File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Local Security Setting
Explain
OK
Cancel
Apply

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	Success, Failure
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Audit object access Properties

Audit object access

Audit these attempts:

☑ Success

☑ Failure

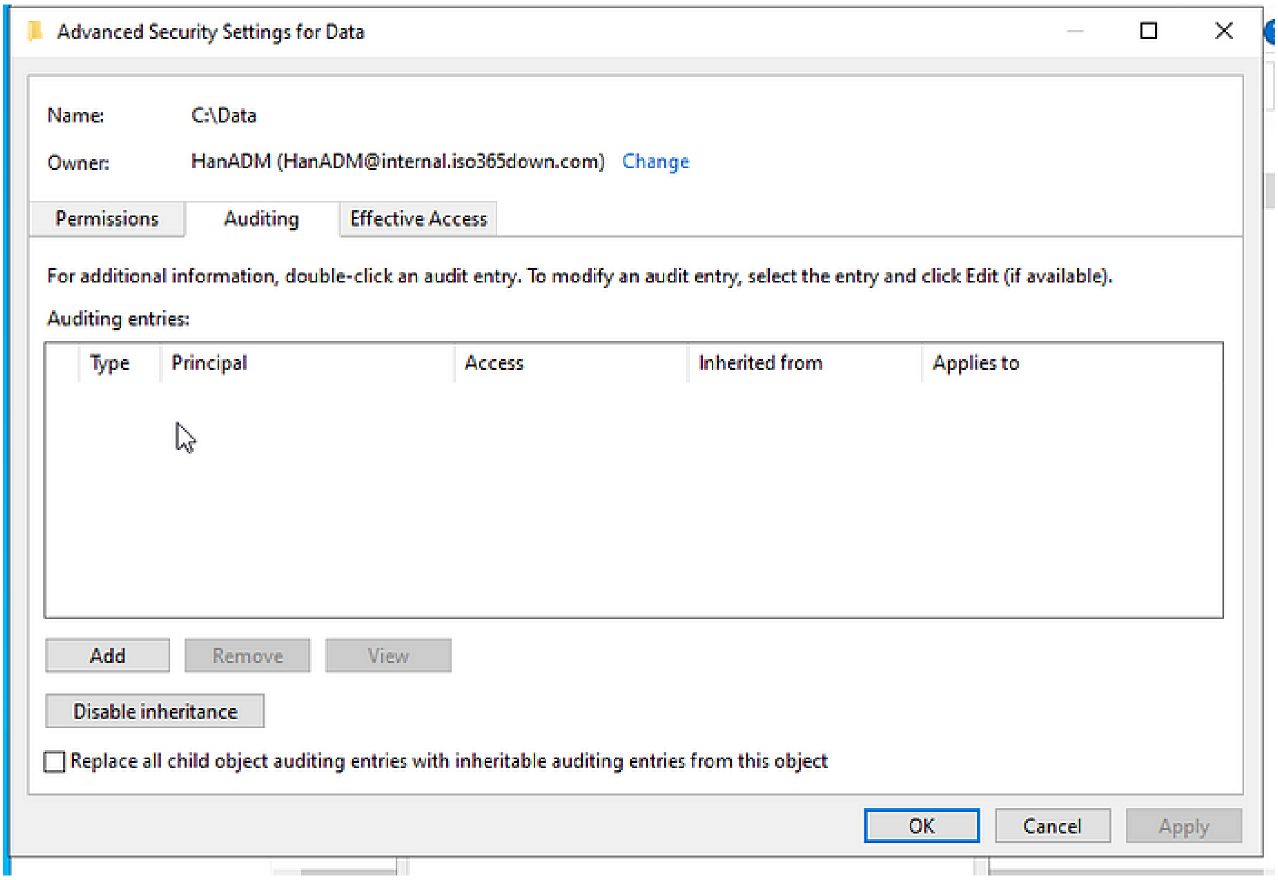
This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit object access. (Q921468)

Enabling Object Access Auditing

Enabling Auditing on our Files

Now we need to enable auditing on files and folders.

To do this, log into any system hosting files whose access you would like to audit. Find the directory you would like to audit, right click and select **properties**, then browse to the **security tab.** Select **advanced** and then view the **Auditing** tab.



Advanced Security Settings for Data

Name: C:\Data

Owner: HanADM (HanADM@internal.iso365down.com) Change

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

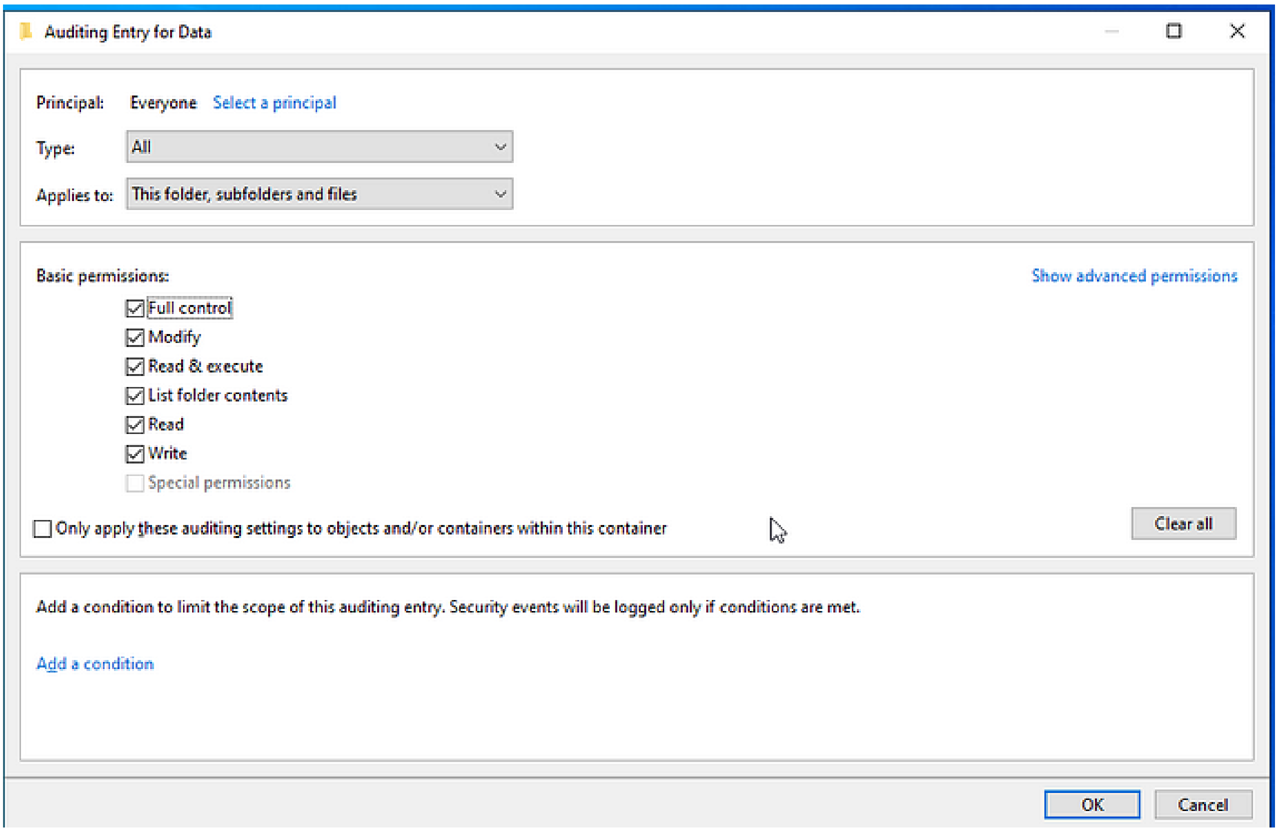
Auditing entries:

Type	Principal	Access	Inherited from	Applies to

☐ Replace all child object auditing entries with inheritable auditing entries from this object

Unless configured the auditing tab will be empty

Add a new auditing entry. This entry will have a principle of **everyone**, audit on **all** actions, and **apply to this folder, subfolders, and files.** We will also want to audit all actions so selection **Full Control.**



Auditing Entry for Data

Principal: Everyone Select a principal

Type: All

Applies to: This folder, subfolders and files

Basic permissions:

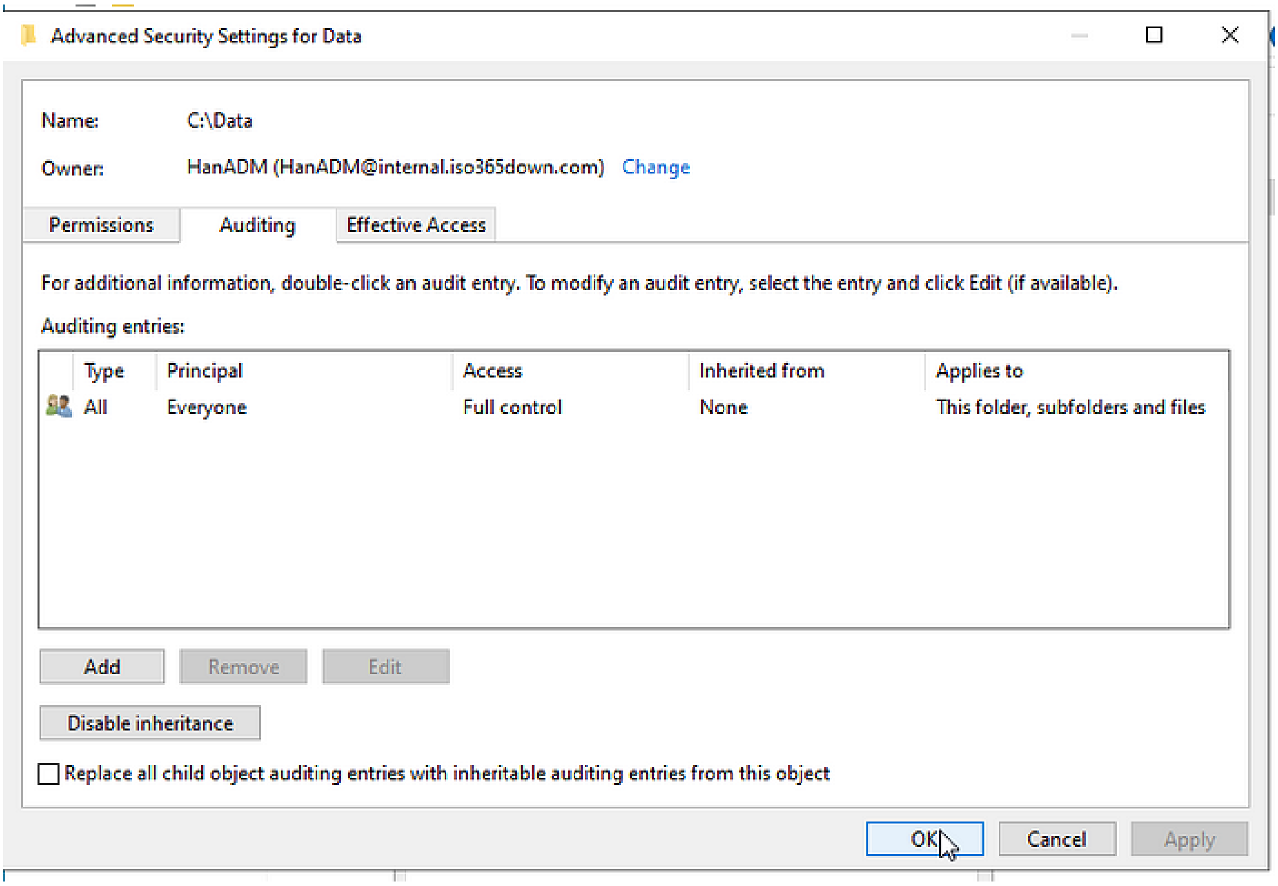
☑ Full control
☑ Modify
☑ Read & execute
☑ List folder contents
☑ Read
☑ Write
□ Special permissions

□ Only apply these auditing settings to objects and/or containers within this container

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

Auditing all actions, anyone takes on a folder

If successful the Auditing tab will now appear as with a new entry for **everyone.**



Advanced Security Settings for Data

Name: C:\Data

Owner: HanADM (HanADM@internal.iso365down.com) Change

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
All	Everyone	Full control	None	This folder, subfolders and files

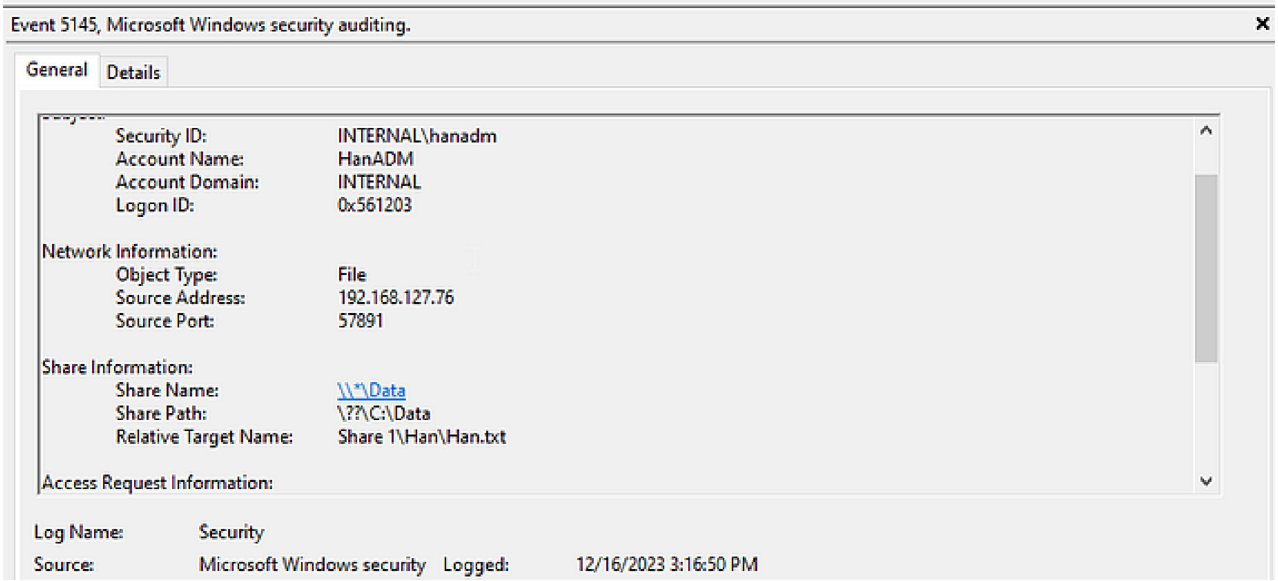
□ Replace all child object auditing entries with inheritable auditing entries from this object

We can now audit various actions that may be done to files

Validating we have logs

Before we install the Graylog Sidecar lets validate our audit rules work.

If we open **Even Viewer > Windows Logs > Security** we can now see users accessing various files.



Event 5145, Microsoft Windows security auditing.

```
        Security ID:            INTERNAL\hanadm
        Account Name:           HanADM
        Account Domain:         INTERNAL
        Logon ID:               0x561203

Network Information:
        Object Type:            File
        Source Address:         192.168.127.76
        Source Port:            57891

Share Information:
        Share Name:             \\*\Data
        Share Path:             \??\C:\Data
        Relative Target Name:   Share 1\Han\Han.txt

Access Request Information:
```

Log Name: Security

Source: Microsoft Windows security Logged: 12/16/2023 3:16:50 PM

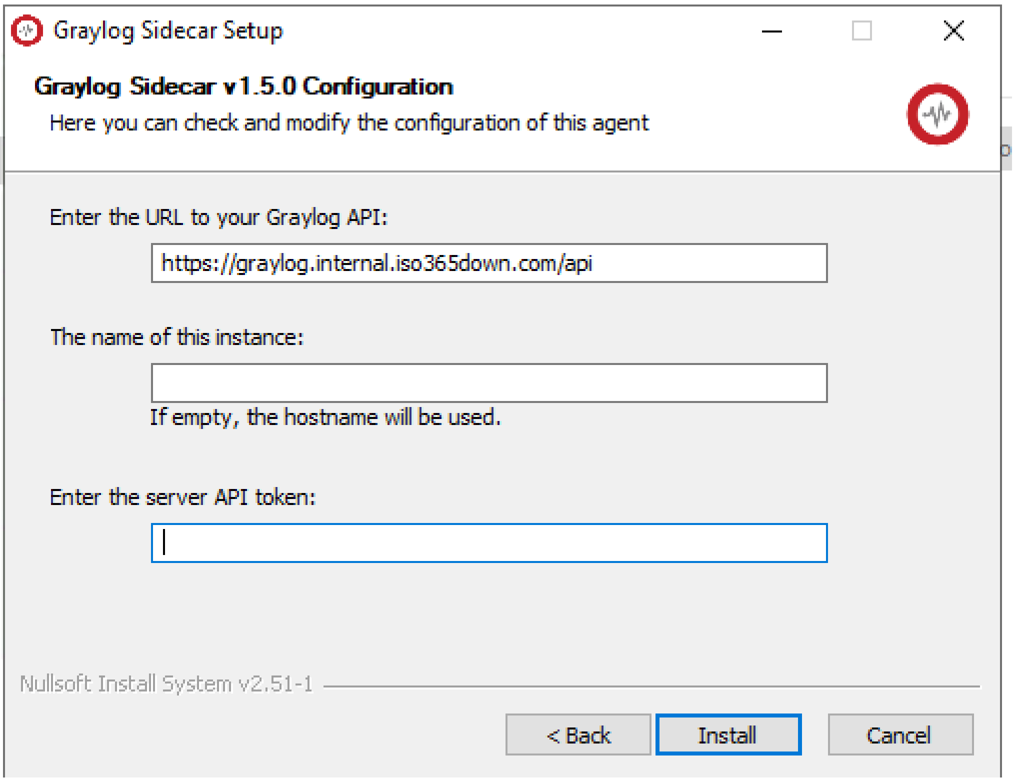
Audit Logs For Files

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 **.**

Using the API key we generated in part 4, install the Graylog collector and point it at our Graylog instance.

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



Graylog Sidecar v1.5.0 Configuration

Here you can check and modify the configuration of this agent

Enter the URL to your Graylog API: https://graylog.internal.iso365down.com/api

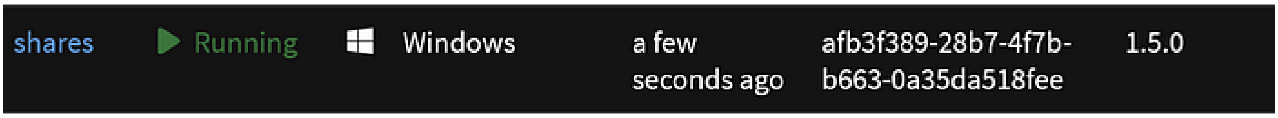
The name of this instance:

If empty, the hostname will be used.

Enter the server API token:

Make sure you use the FQDN of the Graylog Server

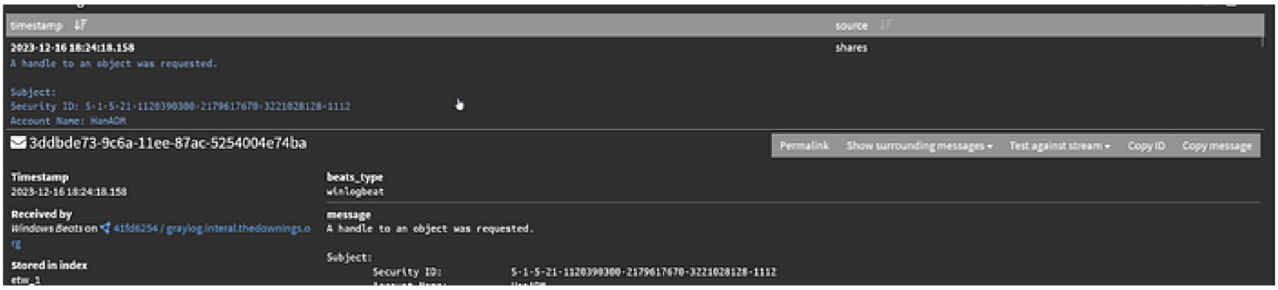
And let it install and validate it is showing up in Graylog.



```
shares   Running   Windows   a few seconds ago   afb3f389-28b7-4f7b-b663-0a35da518fee   1.5.0
```

The new agent up and running

Validate your see data being ingested. Save this **message ID and the index it is stored in.**



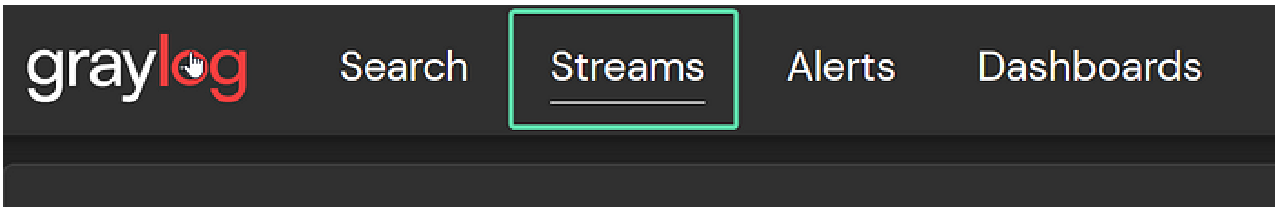
```
2023-12-16 18:24:18.158                                   shares
A handle to an object was requested.

Subject:
Security ID: S-1-5-21-1120390300-2179617670-3221028128-1112
Account Name: HanADM

3ddbde73-9c6a-11ee-87ac-5254004e74ba

Timestamp                         beats_type
2023-12-16 18:24:18.158           winlogbeat

Received by                       message
Windows Beats on 41fd6254 / graylog.interal.thedownings.org     A handle to an object was requested.

                                  Subject:
Stored in index                       Security ID:      S-1-5-21-1120390300-2179617670-3221028128-1112
etw_1
```

Data from our SMB Share server flowing in

With data flowing in, lets create a new data stream to send this new data to the proper index.

Creating a New Data Stream

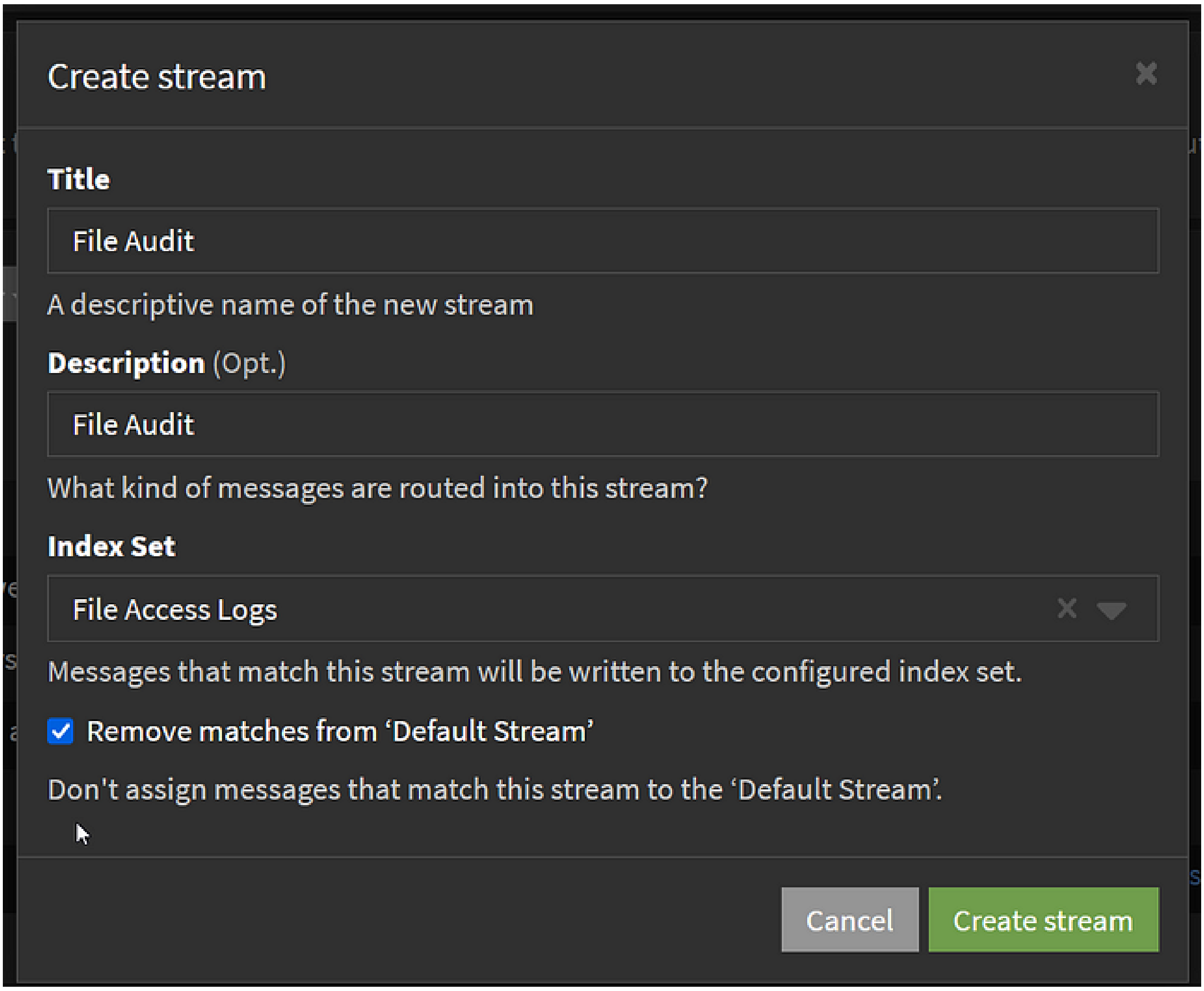
Start by going to **Streams** in the top menu



Creating a new stream

Enter the streams configuration

Create a new stream named File Audit Logs and make sure to route the messages to the File Audit Access index set and remove the messages from the default stream.



Create stream

Title

File Audit

A descriptive name of the new stream

Description (Opt.)

File Audit

What kind of messages are routed into this stream?

Index Set

File Access Logs

Messages that match this stream will be written to the configured index set.

☑ Remove matches from 'Default Stream'

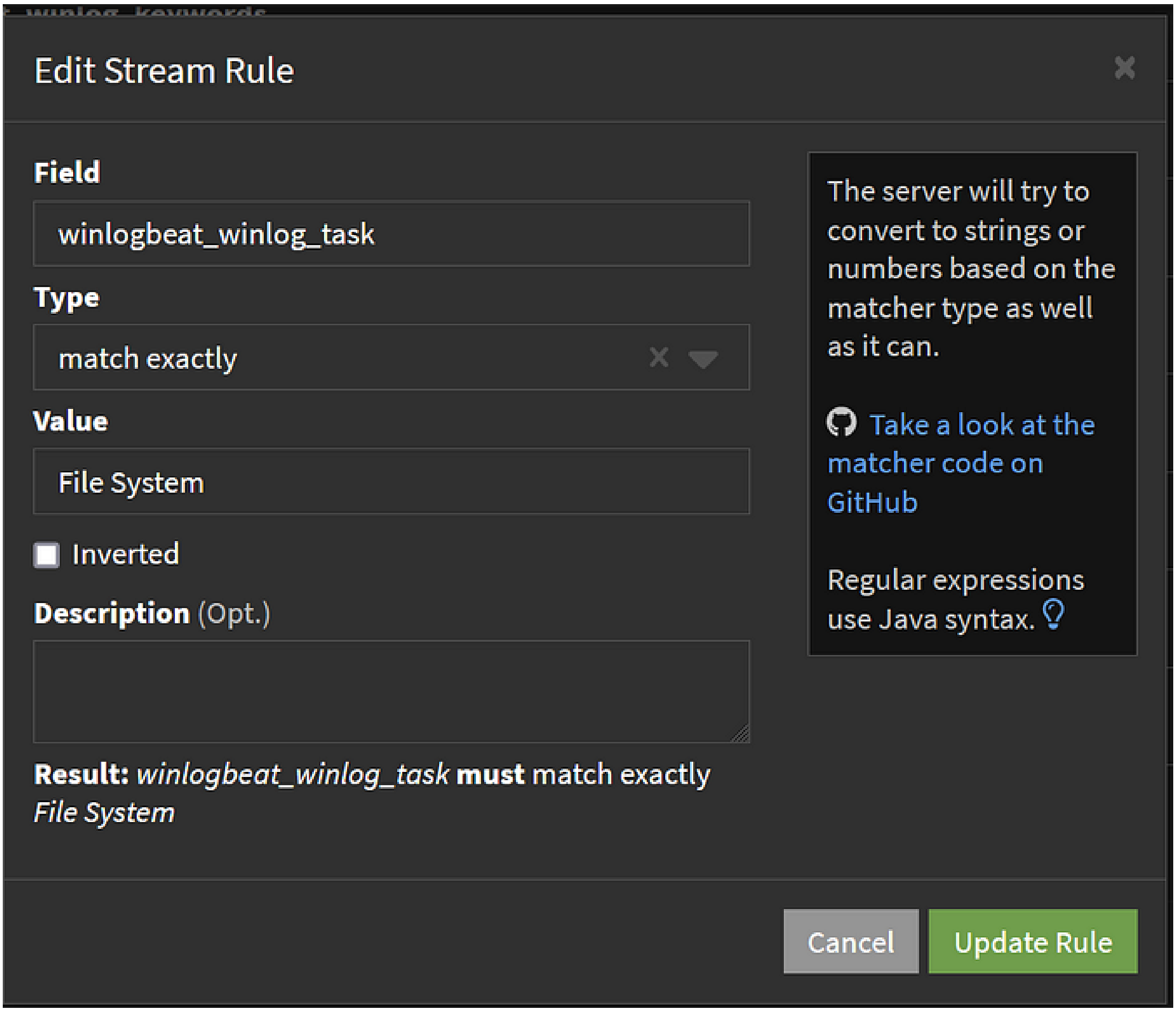
Don't assign messages that match this stream to the 'Default Stream'.

Creating our new stream

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_winlog_task* and make a rule matching the field name *File System.*



Edit Stream Rule

Field

winlogbeat_winlog_task

Type

match exactly

Value

File System

□ Inverted

Description (Opt.)

Result: *winlogbeat_winlog_task* **must** match exactly *File System*

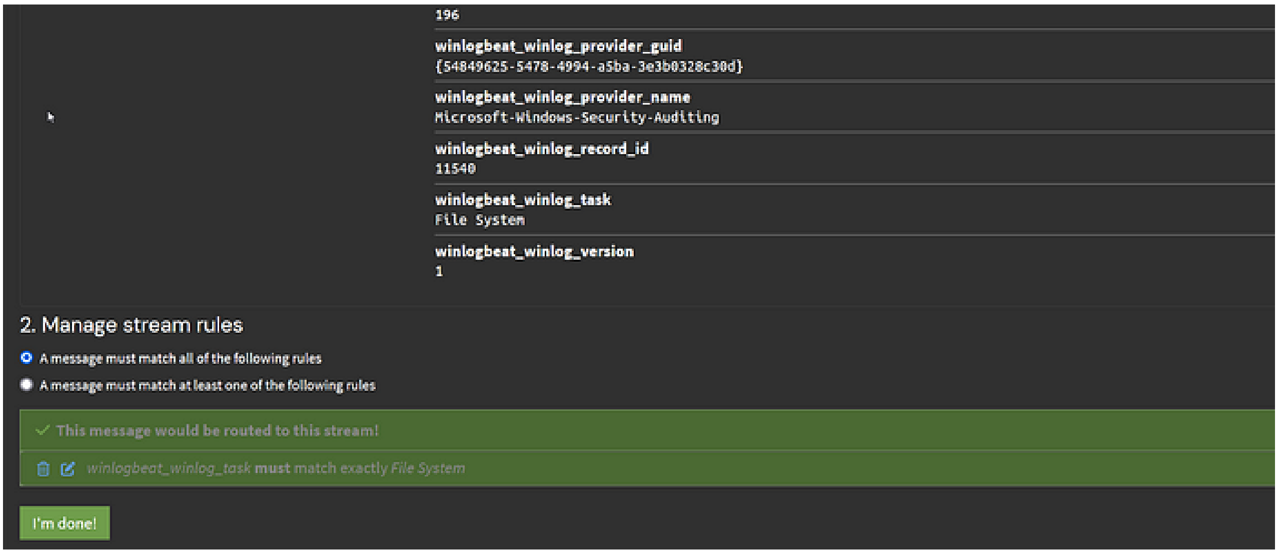
The server will try to convert to strings or numbers based on the matcher type as well as it can.

Take a look at the matcher code on GitHub

Regular expressions use Java syntax.

Creating our stream rule

Test the stream rule against the message we selected and make sure the rule matches.



```
196
winlogbeat_winlog_provider_guid
{54849625-5478-4994-a5ba-3e3b0328c30d}
winlogbeat_winlog_provider_name
Microsoft-Windows-Security-Auditing
winlogbeat_winlog_record_id
11540
winlogbeat_winlog_task
File System
winlogbeat_winlog_version
1
```

2. Manage stream rules

● A message must match all of the following rules

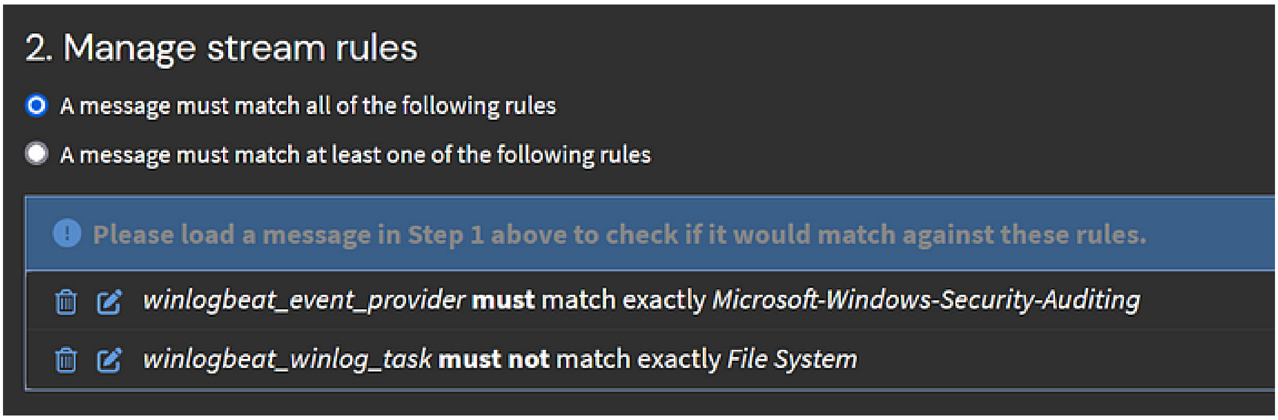
○ A message must match at least one of the following rules

✓ This message would be routed to this stream!

winlogbeat_winlog_task **must** match exactly *File System*

Our message matches!

To prevent copies of messages being made in secondary and tertiary indexes, it is best practice to ensure that we update older rules to remove File Systems Logs from their streams.



2. Manage stream rules

● 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_event_provider **must** match exactly *Microsoft-Windows-Security-Auditing*

winlogbeat_winlog_task **must not** match exactly *File System*

Removing File System Logs from Active Directory Index

During the next part of the series we will be looking into importing IIS logs.