Splunk Reports

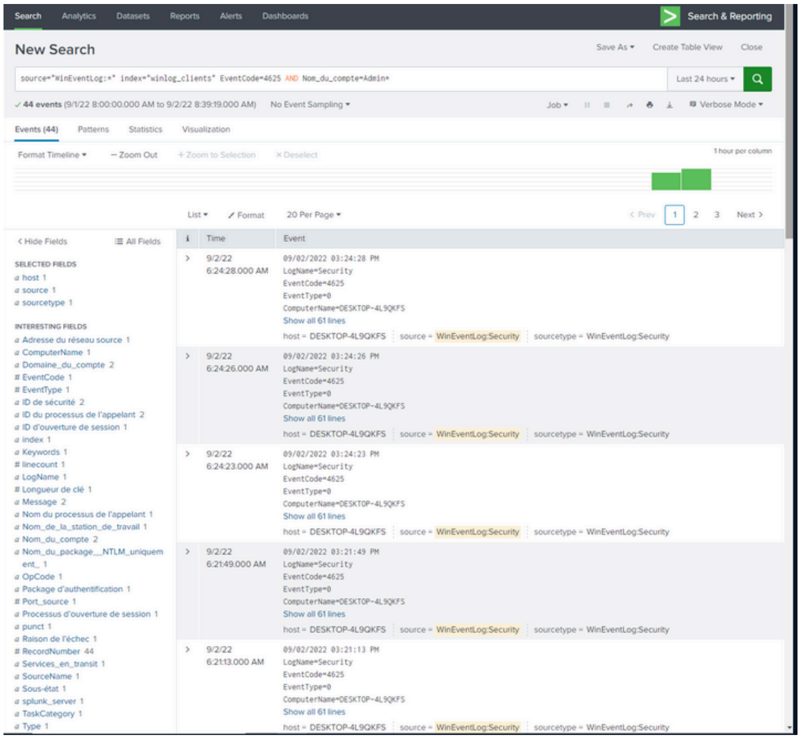
By: Ryan Stewart

What is a Report?

Reports essentially capture saved search results. They can be scheduled for regular execution or run on-demand.

Exercise:

For this exercise, we will use a simple request to find failed connections associated with accounts containing "admin." The request is as follows:



```
source="WinEventLog:*" index="winlog_clients" EventCode=4625 AND Nom_du_compte=Admin*
```

✓ 44 events (9/1/22 8:00:00.000 AM to 9/2/22 8:39:19.000 AM)

```
9/2/22 6:24:28.000 AM
09/02/2022 03:24:28 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=DESKTOP-4L9QKFS
Show all 61 lines
host = DESKTOP-4L9QKFS   source = WinEventLog:Security   sourcetype = WinEventLog:Security

9/2/22 6:24:26.000 AM
09/02/2022 03:24:26 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=DESKTOP-4L9QKFS
Show all 61 lines
host = DESKTOP-4L9QKFS   source = WinEventLog:Security   sourcetype = WinEventLog:Security

9/2/22 6:24:23.000 AM
09/02/2022 03:24:23 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=DESKTOP-4L9QKFS
Show all 61 lines
host = DESKTOP-4L9QKFS   source = WinEventLog:Security   sourcetype = WinEventLog:Security

9/2/22 6:21:49.000 AM
09/02/2022 03:21:49 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=DESKTOP-4L9QKFS
Show all 61 lines
host = DESKTOP-4L9QKFS   source = WinEventLog:Security   sourcetype = WinEventLog:Security

9/2/22 6:21:13.000 AM
09/02/2022 03:21:13 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=DESKTOP-4L9QKFS
Show all 61 lines
host = DESKTOP-4L9QKFS   source = WinEventLog:Security   sourcetype = WinEventLog:Security
```

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

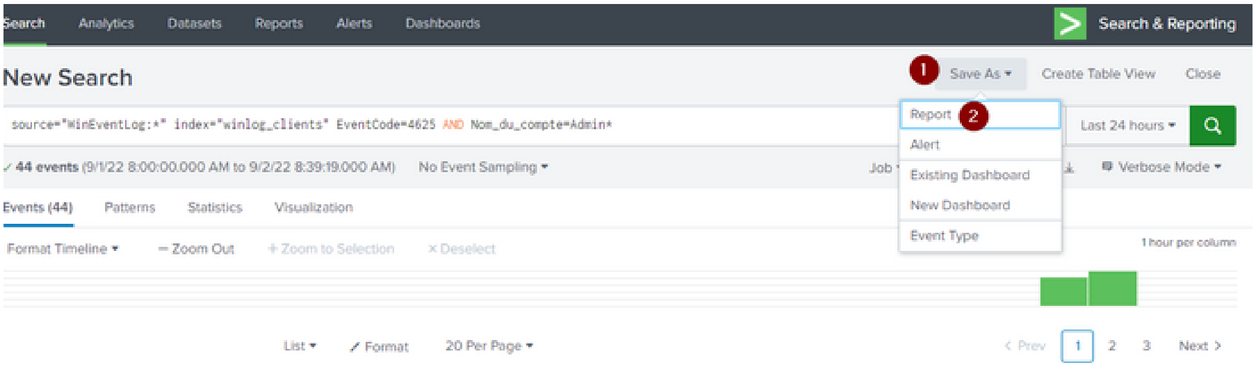
INTERESTING FIELDS
- a Adresse du réseau source 1
- a ComputerName 1
- a Domaine_du_compte 2
- # EventCode 1
- # EventType 1
- a ID de sécurité 2
- a ID du processus de l'appelant 2
- a ID d'ouverture de session 1
- a index 1
- a Keywords 1
- # linecount 1
- a LogName 1
- # Longueur de clé 1
- a Message 2
- a Nom du processus de l'appelant 1
- a Nom_de_la_station_de_travail 1
- a Nom_du_compte 2
- a Nom_du_package__NTLM_uniquement_ 1
- a OpCode 1
- a Package d'authentification 1
- # Port_source 1
- a Processus d'ouverture de session 1
- a punct 1
- a Raison de l'échec 1
- # RecordNumber 44
- a Services_en_transit 1
- a SourceName 1
- a Sous-état 1
- a splunk_server 1
- a TaskCategory 1
- a Type 1

- Try entering your request in the search bar.

- Go to the "Save As" menu and select.

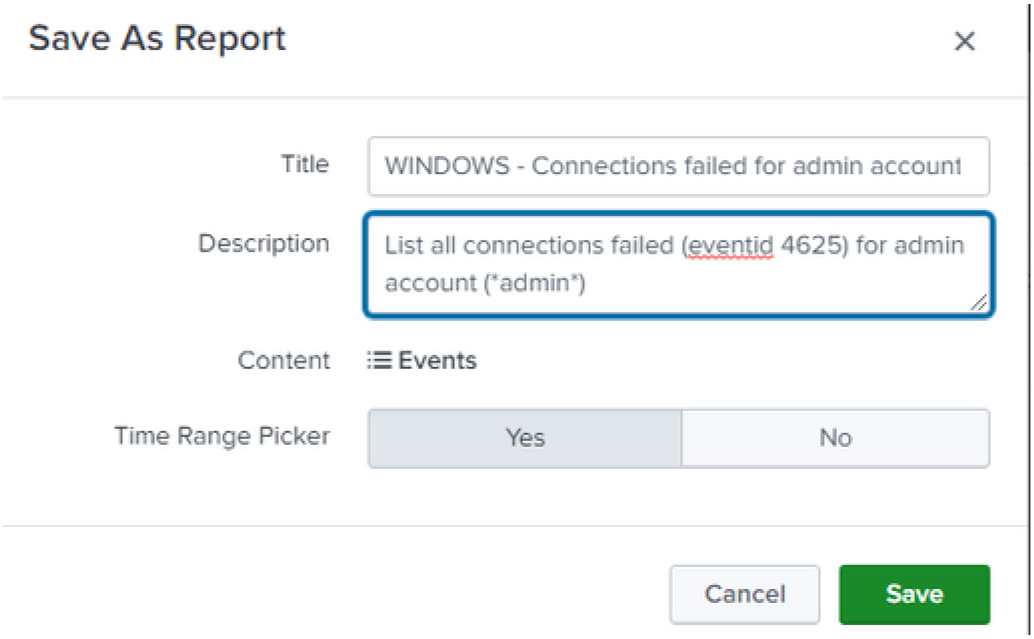
- Provide a title and description for your report.

- Save and proceed to View.



```
source="WinEventLog:*" index="winlog_clients" EventCode=4625 AND Nom_du_compte=Admin*
```

✓ 44 events (9/1/22 8:00:00.000 AM to 9/2/22 8:39:19.000 AM) No Event Sampling



Save As Report

Title: WINDOWS - Connections failed for admin account

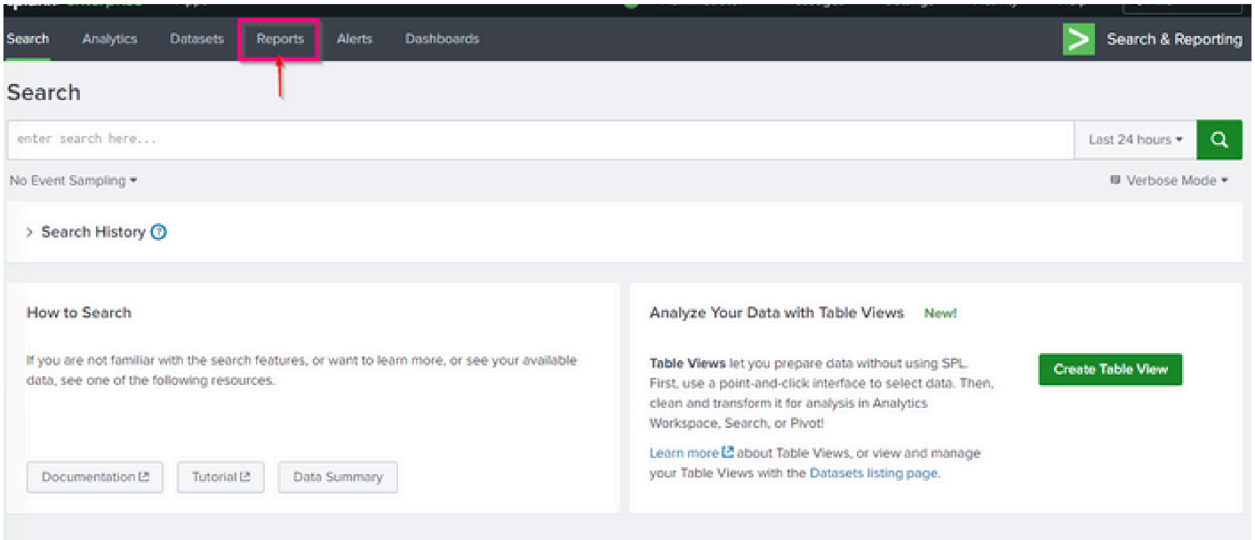
Description: List all connections failed (eventid 4625) for admin account (*admin*)

Content: Events

Time Range Picker: [✓ Yes] No

Edit or Delete an Existing Report:

- Navigate to the Reports section from the Search App.



How to Search

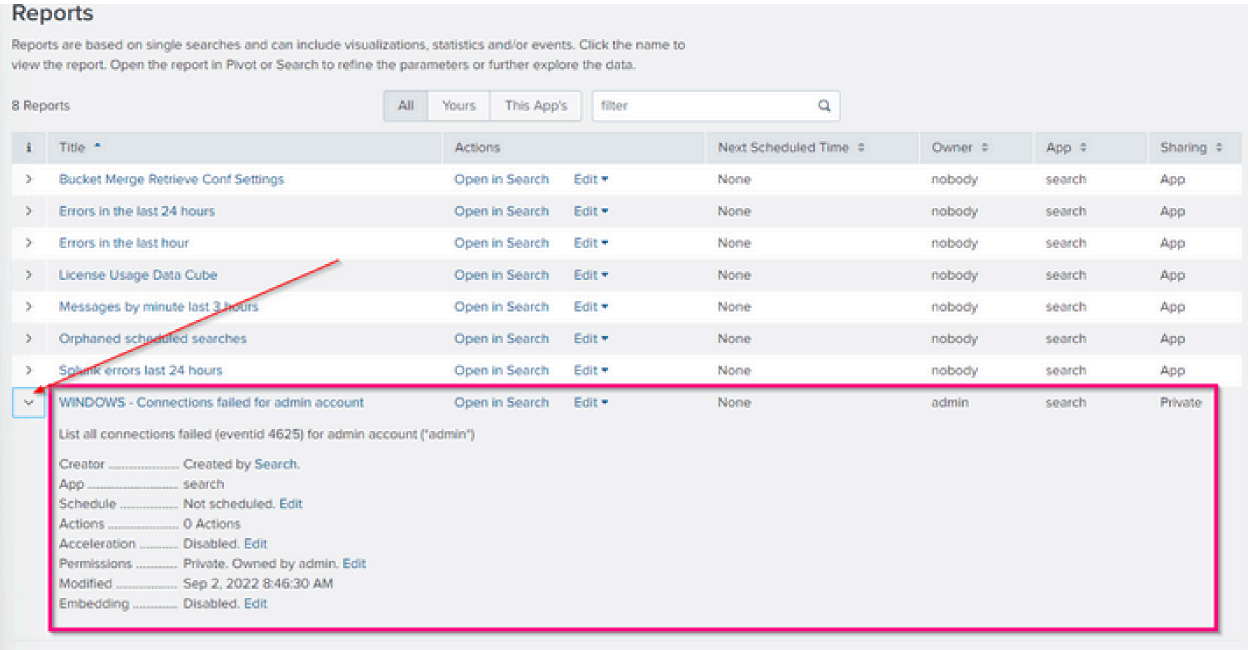
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Analyze Your Data with Table Views

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

- Locate the report created a few minutes ago.



Reports

Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Pivot or Search to refine the parameters or further explore the data.

8 Reports

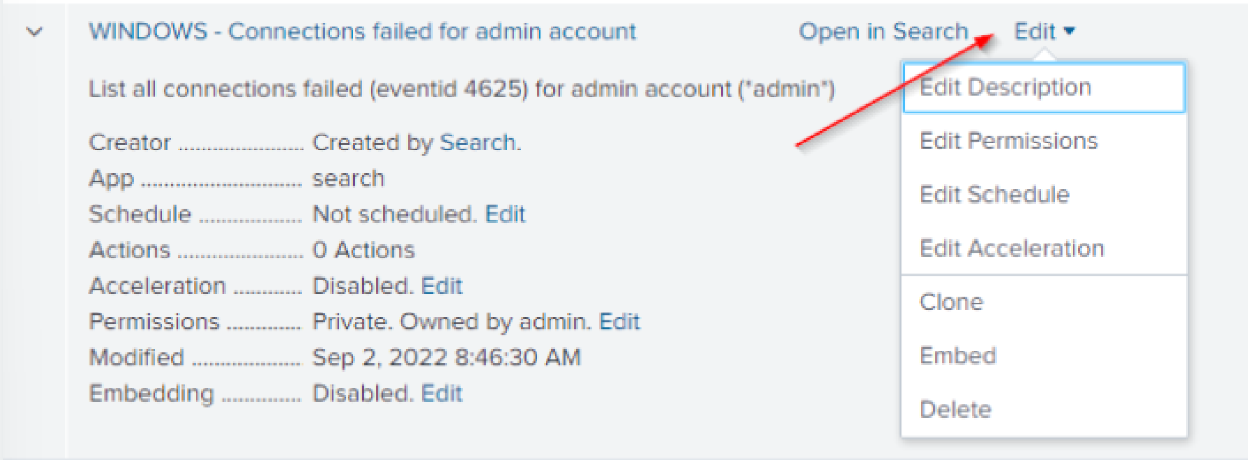
i	Title ▴	Actions		Next Scheduled Time ⇕	Owner ⇕	App ⇕	Sharing ⇕
›	Bucket Merge Retrieve Conf Settings	Open in Search	Edit ▾	None	nobody	search	App
›	Errors in the last 24 hours	Open in Search	Edit ▾	None	nobody	search	App
›	Errors in the last hour	Open in Search	Edit ▾	None	nobody	search	App
›	License Usage Data Cube	Open in Search	Edit ▾	None	nobody	search	App
›	Messages by minute last 3 hours	Open in Search	Edit ▾	None	nobody	search	App
›	Orphaned scheduled searches	Open in Search	Edit ▾	None	nobody	search	App
›	Splunk errors last 24 hours	Open in Search	Edit ▾	None	nobody	search	App
⌄	WINDOWS - Connections failed for admin account	Open in Search	Edit ▾	None	admin	search	Private

List all connections failed (eventid 4625) for admin account ("admin")

Creator .... Created by Search.
App .... search
Schedule .... Not scheduled. Edit
Actions .... 0 Actions
Acceleration .... Disabled. Edit
Permissions .... Private. Owned by admin. Edit
Modified .... Sep 2, 2022 8:46:30 AM
Embedding .... Disabled. Edit

- Access information about your report.

- Select the Edit button.



WINDOWS - Connections failed for admin account

List all connections failed (eventid 4625) for admin account ("admin")

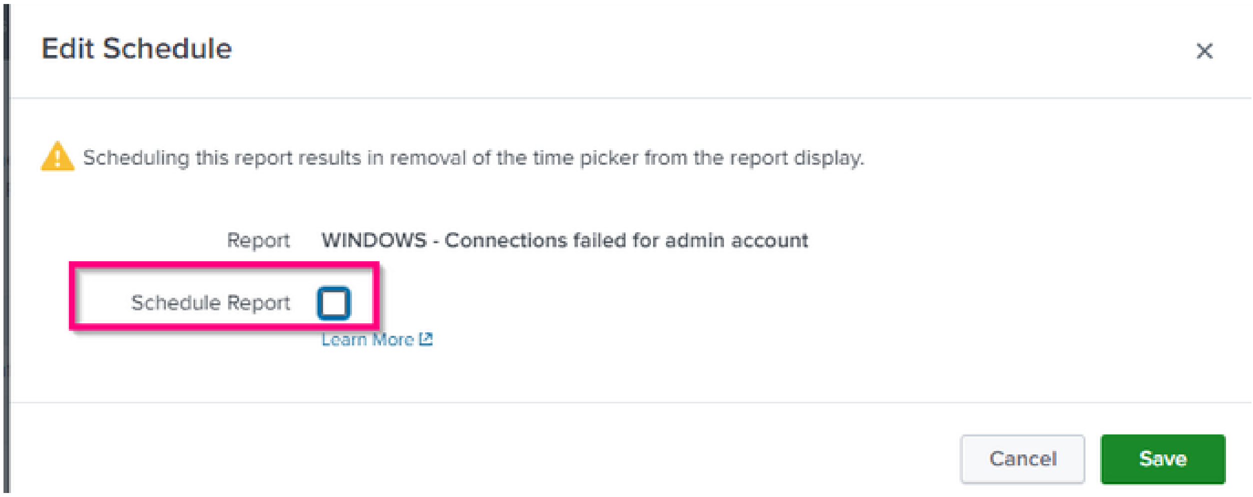
Creator .... Created by Search.
App .... search
Schedule .... Not scheduled. Edit
Actions .... 0 Actions
Acceleration .... Disabled. Edit
Permissions .... Private. Owned by admin. Edit
Modified .... Sep 2, 2022 8:46:30 AM
Embedding .... Disabled. Edit

Exercise:

Now, let's schedule this report for execution every day at 8 AM to capture connections that failed the previous day.

- Choose "Edit Schedule."

- Enable "Schedule Report."

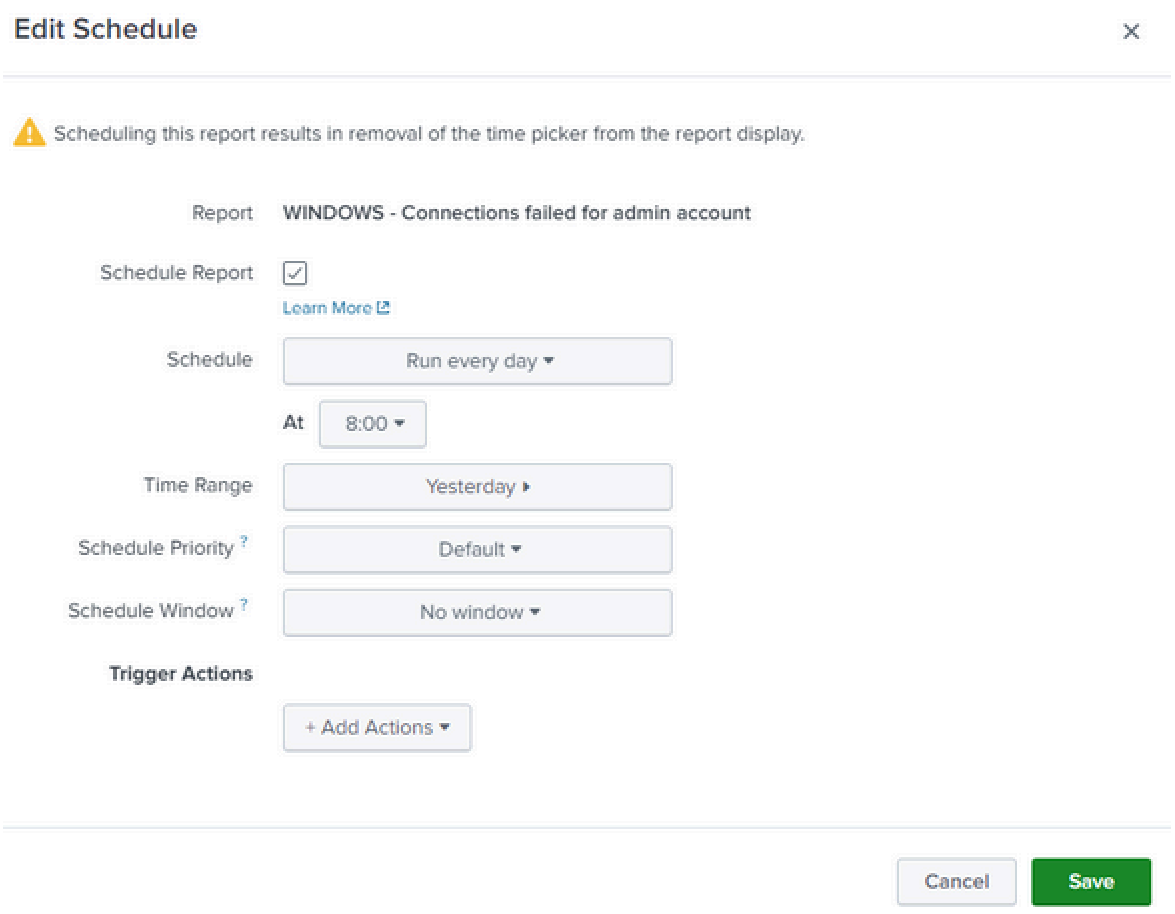


Edit Schedule

⚠ Scheduling this report results in removal of the time picker from the report display.

Report WINDOWS - Connections failed for admin account

Schedule Report □



Edit Schedule

⚠ Scheduling this report results in removal of the time picker from the report display.

Report WINDOWS - Connections failed for admin account

Schedule Report ☑

Schedule: Run every day

At 8:00

Time Range: Yesterday

Schedule Priority: Default

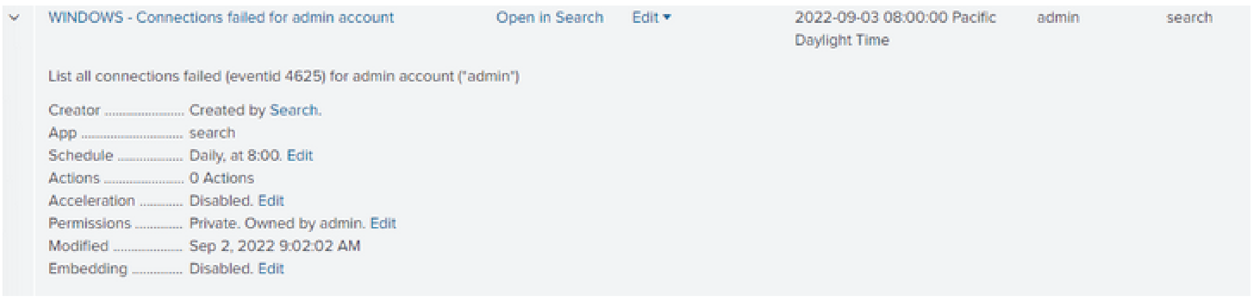
Schedule Window: No window

Trigger Actions

- Configure the schedule settings.

IIn the future we can explore possibilities such as **sending emails** or launching scripts when your report is generated.

- Save and review the information in your report.



WINDOWS - Connections failed for admin account | Open in Search | Edit | 2022-09-03 08:00:00 Pacific Daylight Time | admin | search

List all connections failed (eventid 4625) for admin account ("admin")

```
Creator ..................... Created by Search.
App ......................... search
Schedule .................... Daily, at 8:00. Edit
Actions ..................... 0 Actions
Acceleration ................ Disabled. Edit
Permissions ................. Private. Owned by admin. Edit
Modified .................... Sep 2, 2022 9:02:02 AM
Embedding ................... Disabled. Edit
```

Questions Progress:

Can you send an email when a report is generated? YES!