

# Creating Scheduled Reports and Alerts

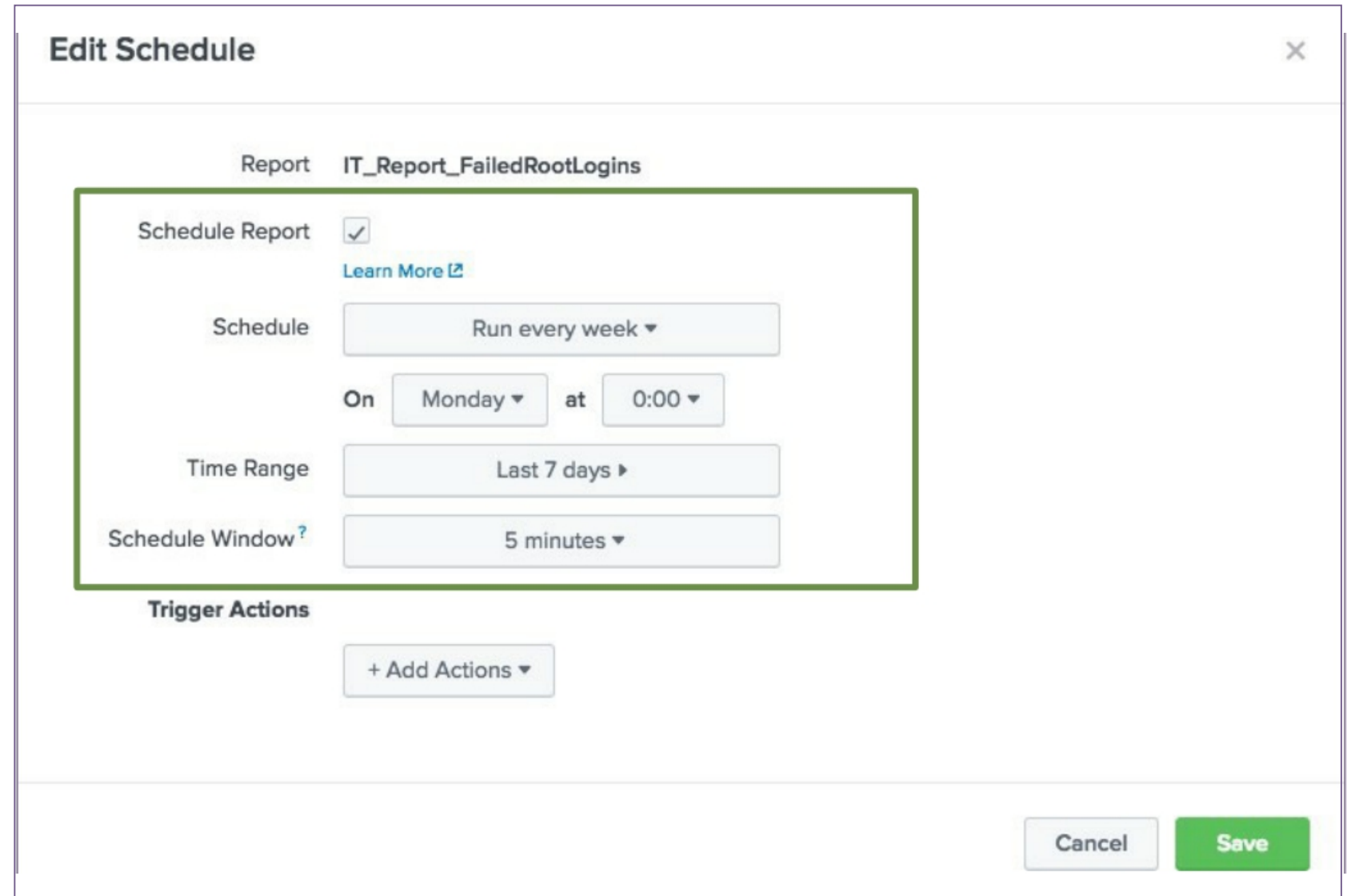
# Why Scheduled Reports?

Scheduled Reports are useful for:

- Monthly, weekly, daily executive/managerial roll up reports
- Dashboard performance
- Automatically sending reports via email

# Creating a Scheduled Report – Define Schedule

- Schedule Report – select this checkbox
- Schedule – select the frequency to run the report
  - Run every hour
  - Run every day
  - Run every week
  - Run every month
  - Run on Cron Schedule



The screenshot shows the 'Edit Schedule' dialog box for the report 'IT\_Report\_FailedRootLogins'. A green box highlights the scheduling configuration section. The 'Schedule Report' checkbox is checked, with a 'Learn More' link below it. The 'Schedule' dropdown is set to 'Run every week'. The 'On' dropdown is set to 'Monday' and the 'at' dropdown is set to '0:00'. The 'Time Range' dropdown is set to 'Last 7 days'. The 'Schedule Window' dropdown is set to '5 minutes'. Below this section is the 'Trigger Actions' section with a '+ Add Actions' button. At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

Report IT\_Report\_FailedRootLogins

Schedule Report ☒ [Learn More](#)

Schedule Run every week ▼

On Monday ▼ at 0:00 ▼

Time Range Last 7 days ▶

Schedule Window? 5 minutes ▼

Trigger Actions

+ Add Actions ▼

Cancel Save

# Creating a Scheduled Report – Add Actions

- **Log Event** – creates an indexed, searchable log event
- **Output results to lookup** – sends results of search to CSV lookup file
- **Output results to telemetry endpoint** – sends usage metrics back to Splunk (if your company has opted-in to program)
- **Run a script** – runs a previously created script
- **Send email** – sends an email with results to specified recipients
- **Webhook** – sends an HTTP POST request to specified URL

The screenshot shows the 'Edit Schedule' dialog box in Splunk. The report is named 'IT\_Report\_FailedRootLogins'. The 'Schedule Report' checkbox is checked, with a 'Learn More' link below it. The 'Schedule' dropdown is set to 'Run every week'. The 'On' dropdown is set to 'Monday' and the 'at' dropdown is set to '6:00'. The 'Time Range' dropdown is set to 'Last 7 days'. The 'Schedule Window' dropdown is set to '5 minutes'. Below these settings is a section titled 'Trigger Actions' with a '+ Add Actions' button. A list of actions is shown, including 'Log Event', 'Output results to lookup', 'Output results to telemetry endpoint', 'Run a script', and 'Send email'. The 'Log Event' action is highlighted. At the bottom right of the dialog are 'Cancel' and 'Save' buttons. The background shows a log viewer with entries for failed password attempts.

# Managing Reports – Embed

- To access the report results from a webpage, click Edit > Embed
  - Before a report can be embedded, it must be scheduled

**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.

1 Reports

All
Yours
This App's

i	Title ^	Actions	Next Scheduled Time ▾	Owner ▾	App ▾	Sharing ▾
>	IT_Report_FailedRootLogins	Open in Search Edit ▾	None	student1	class_Fund1	Private

- Edit Description
- Edit Permissions
- Edit Schedule
- Edit Acceleration
- Clone
- Embed**
- Delete

### Enable Report Embedding

Are you sure you want to enable embedding for report *IT\_Report\_FailedRootLogins*? An embedded report can be viewed by anyone with access to the web page(s) in which it is inserted.

Cancel **Enable Embedding**

### Embed

⚠ Embedded Report will not have data until the scheduled search runs.

Copy and paste this code into your HTML-based web page.

```
<iframe height="636" width="480" frameborder="0" src="http://34.212.105.44/en-US/embed?s=%2FservicesNS%2Fstudent1%2Fclass_Fund1%2Fsaved%2Fsearches%2FIT_Report_FailedRootLogins&oid=fVkJUe...></iframe>
```

Disable embedding if you no longer want to share this report outside of Splunk.

Disable Embedding **Done**

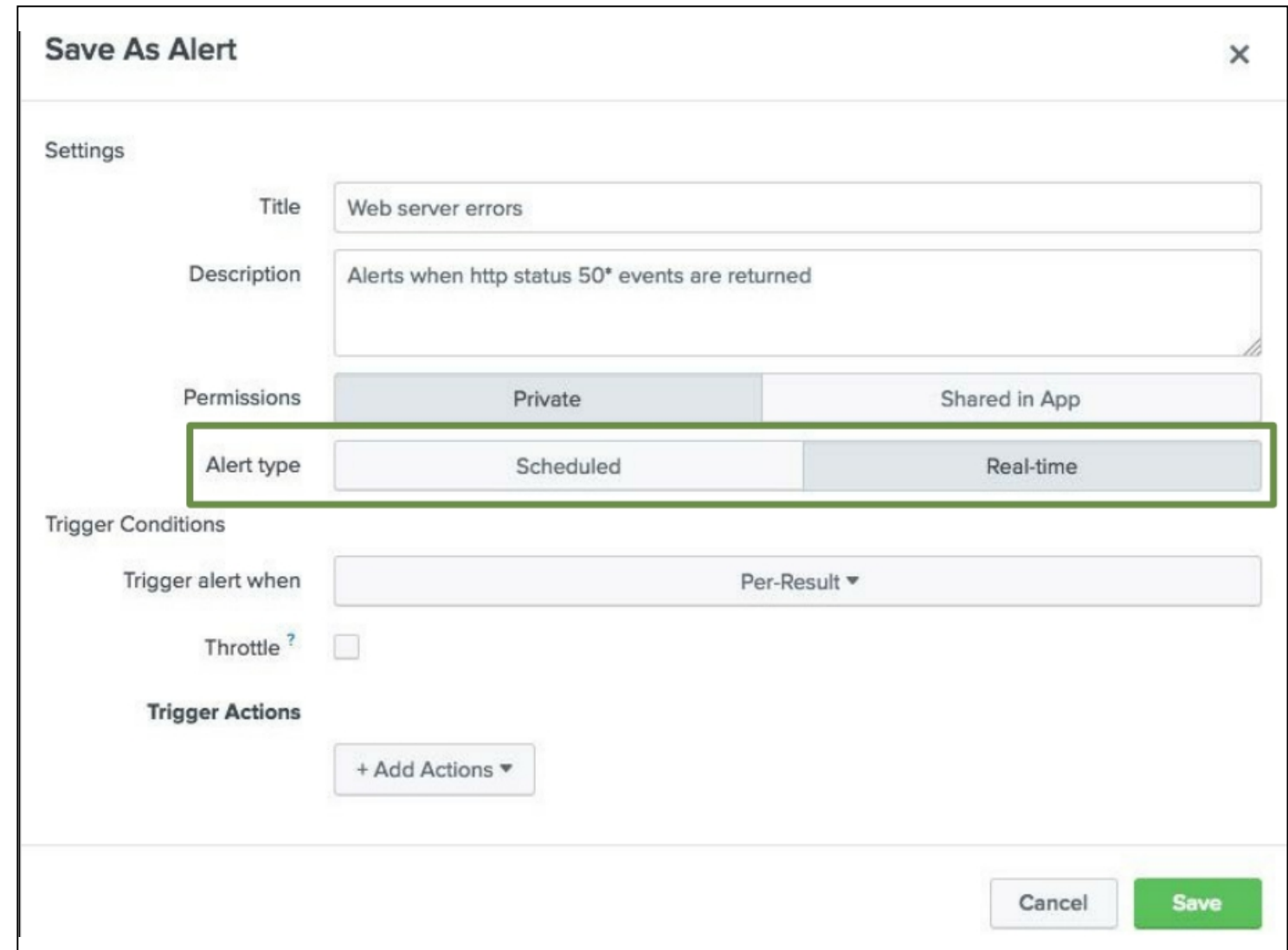
# What Are Alerts?

- Splunk alerts are based on searches that can run either:
  - On a regular scheduled interval
  - In real-time
- Alerts are triggered when the results of the search meet a specific condition that you define
- Based on your needs, alerts can:
  - Create an entry in Triggered Alerts
  - Log an event
  - Output results to a lookup file
  - Send emails
  - Use a webhook
  - Perform a custom action

# Choosing Real-time or Scheduled Alert Type

Choose an **Alert type** to determine how Splunk searches for events that match your alert

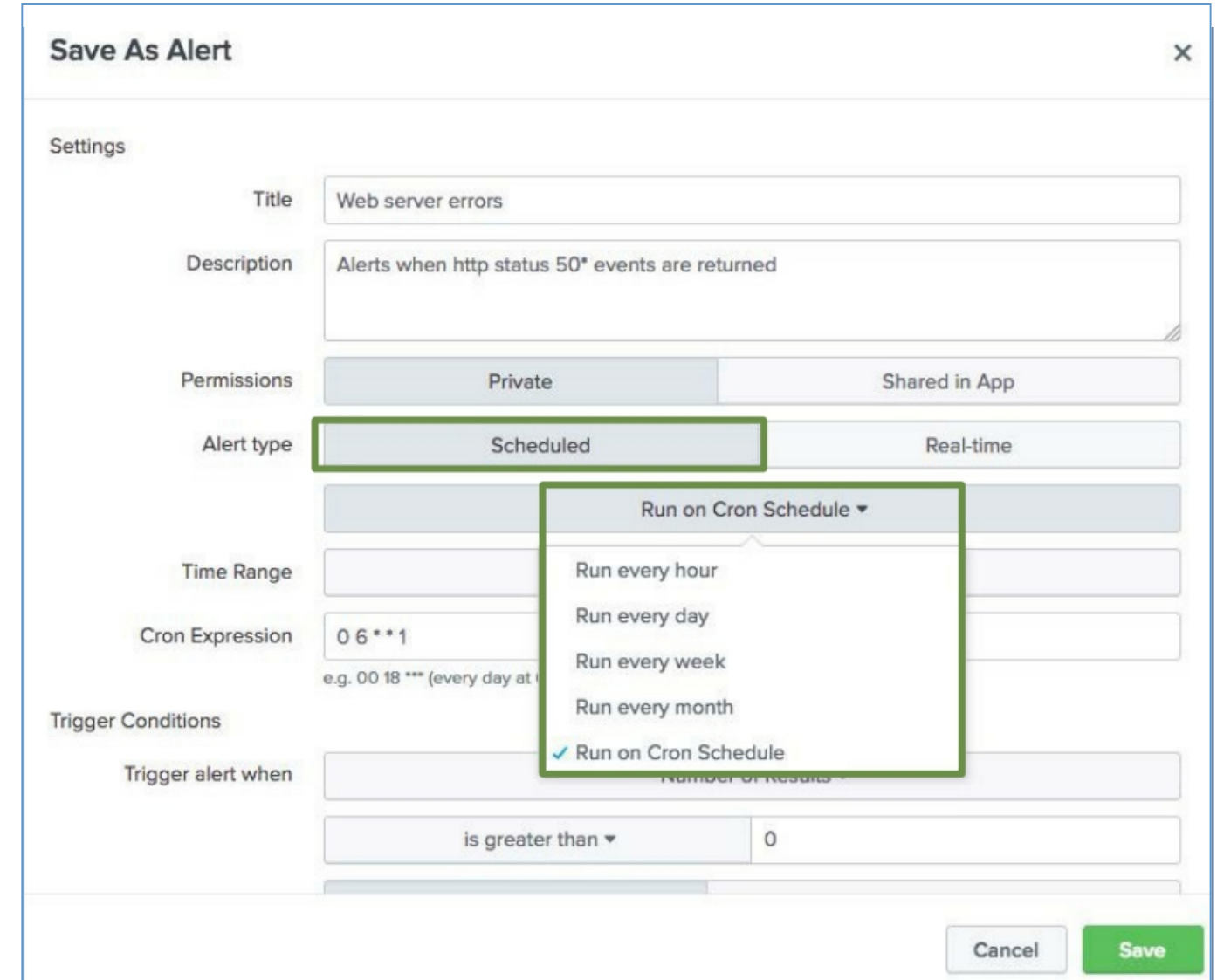
- **Scheduled** alerts
  - Search runs at a defined interval
  - Evaluates trigger condition when the search completes
- **Real-time** alerts
  - Search runs constantly in the background
  - Evaluates trigger conditions within a window of time based on the conditions you define



The screenshot shows the 'Save As Alert' dialog box in Splunk. The 'Settings' section includes fields for 'Title' (Web server errors) and 'Description' (Alerts when http status 50\* events are returned). The 'Permissions' section shows 'Private' and 'Shared in App' options. The 'Alert type' section has two radio buttons: 'Scheduled' (selected) and 'Real-time'. The 'Trigger Conditions' section includes a 'Trigger alert when' dropdown set to 'Per-Result', a 'Throttle' checkbox, and a '+ Add Actions' button. The 'Cancel' and 'Save' buttons are at the bottom right.

# Setting the Alert Type – Scheduled

- From the frequency menu, choose to run the search every hour, day, week, month, or on a cron schedule
  - For the scheduled interval options, select the time the search will run
  - For cron schedule, define the cron expression



The screenshot shows the 'Save As Alert' dialog box with the following fields and options:

- Title:** Web server errors
- Description:** Alerts when http status 50\* events are returned
- Permissions:** Private (selected) / Shared in App
- Alert type:** Scheduled (selected) / Real-time
- Time Range:** (empty)
- Cron Expression:** 0 6 \* \* 1  
e.g. 00 18 \*\*\* (every day at 18:00)
- Trigger Conditions:**
  - Trigger alert when: (empty)
  - is greater than ▼ 0

The 'Alert type' dropdown menu is open, showing the following options:

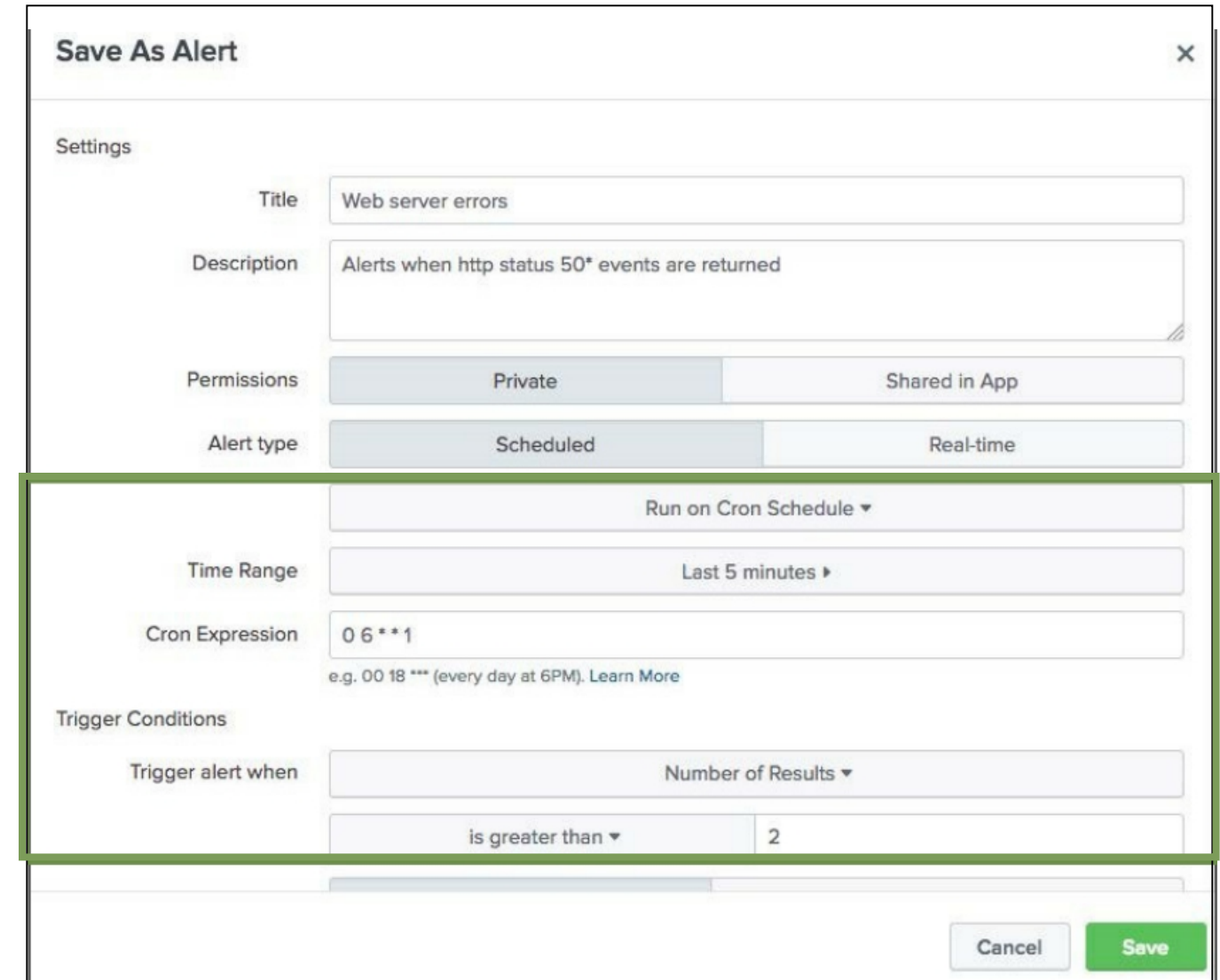
- Run on Cron Schedule ▼ (selected)
- Run every hour
- Run every day
- Run every week
- Run every month
- Run on Cron Schedule (checked)

Buttons: Cancel, Save



# Setting Trigger Conditions – Scheduled

- For the cron schedule, choose a Time Range and enter a Cron Expression
- Set trigger conditions for scheduled alerts (same steps outlined for real-time alerts)
  - The alert examines the complete results set after the search is run



The screenshot shows a 'Save As Alert' dialog box with the following settings:

- Title:** Web server errors
- Description:** Alerts when http status 50\* events are returned
- Permissions:** Private (selected), Shared in App
- Alert type:** Scheduled (selected), Real-time
- Run on Cron Schedule:** (selected)
- Time Range:** Last 5 minutes (selected)
- Cron Expression:** 0 6 \* \* 1  
e.g. 00 18 \*\*\* (every day at 6PM). [Learn More](#)
- Trigger Conditions:**
  - Trigger alert when:** Number of Results (selected)
  - is greater than:** 2

At the bottom right, there are 'Cancel' and 'Save' buttons.

# Setting Trigger Conditions – Real-time

- Trigger conditions allow you to capture a larger data set, then apply more stringent criteria to results before executing the alert
- You can set alerts to trigger:
  - **Per-Result** – triggers when a result is returned
  - **Number of Results** – define how many results are returned before the alert triggers
  - **Number of Hosts** – define how many unique hosts are returned before the alert triggers
  - **Number of Sources** – define how many unique sources are returned before the alert triggers
  - **Custom** – define custom conditions using the search language

The screenshot shows a 'Save As Alert' dialog box with the following settings:

- Title:** Web server errors
- Description:** Alerts when http status 50\* events are returned
- Permissions:** Private (selected), Shared in App
- Alert type:** Scheduled, Real-time (selected and highlighted with a green border)
- Trigger Conditions:**
  - Trigger alert when: Per-Result ▼
  - Per-Result** (checked with a green checkmark): Triggers whenever search returns a result.
  - Number of Results:** Triggers based on a number of search results during a rolling-window of time.
  - Number of Hosts:** Triggers based on a number of hosts during a rolling-window of time.
  - Number of Sources:** Triggers based on a number of sources during a rolling-window of time.
  - Custom:** Triggers based on a custom condition during a rolling-window time.

Buttons: Cancel, Save

# Alert Actions – Trigger Conditions: Once

- **Once** executes actions *one time* for all matching events within the scheduled time and conditions
  - Example: If your alert is scheduled to run every **5 minutes**, and 40 results are returned, the alert only triggers and executes actions one time
- Select the Throttle option to suppress the actions for results within a specified time range

The screenshot shows the 'Save As Alert' configuration window. The 'Alert type' is set to 'Scheduled'. The 'Time Range' is 'Last 5 minutes'. The 'Cron Expression' is '0 6 \* \* 1' with an example 'e.g. 00 18 \*\*\* (every day at 6PM)' and a 'Learn More' link. Under 'Trigger Conditions', 'Trigger alert when' is 'Number of Results', which is 'is greater than' '2'. The 'Trigger' is set to 'Once' (highlighted with a green box). Below this, the 'Throttle' checkbox is checked, and 'Suppress triggering for' is set to '10' 'minute(s)' (this entire section is also highlighted with a green box). At the bottom, there is a '+ Add Actions' button and 'Cancel' and 'Save' buttons.

# Alert Actions – Trigger Conditions: For Each Result

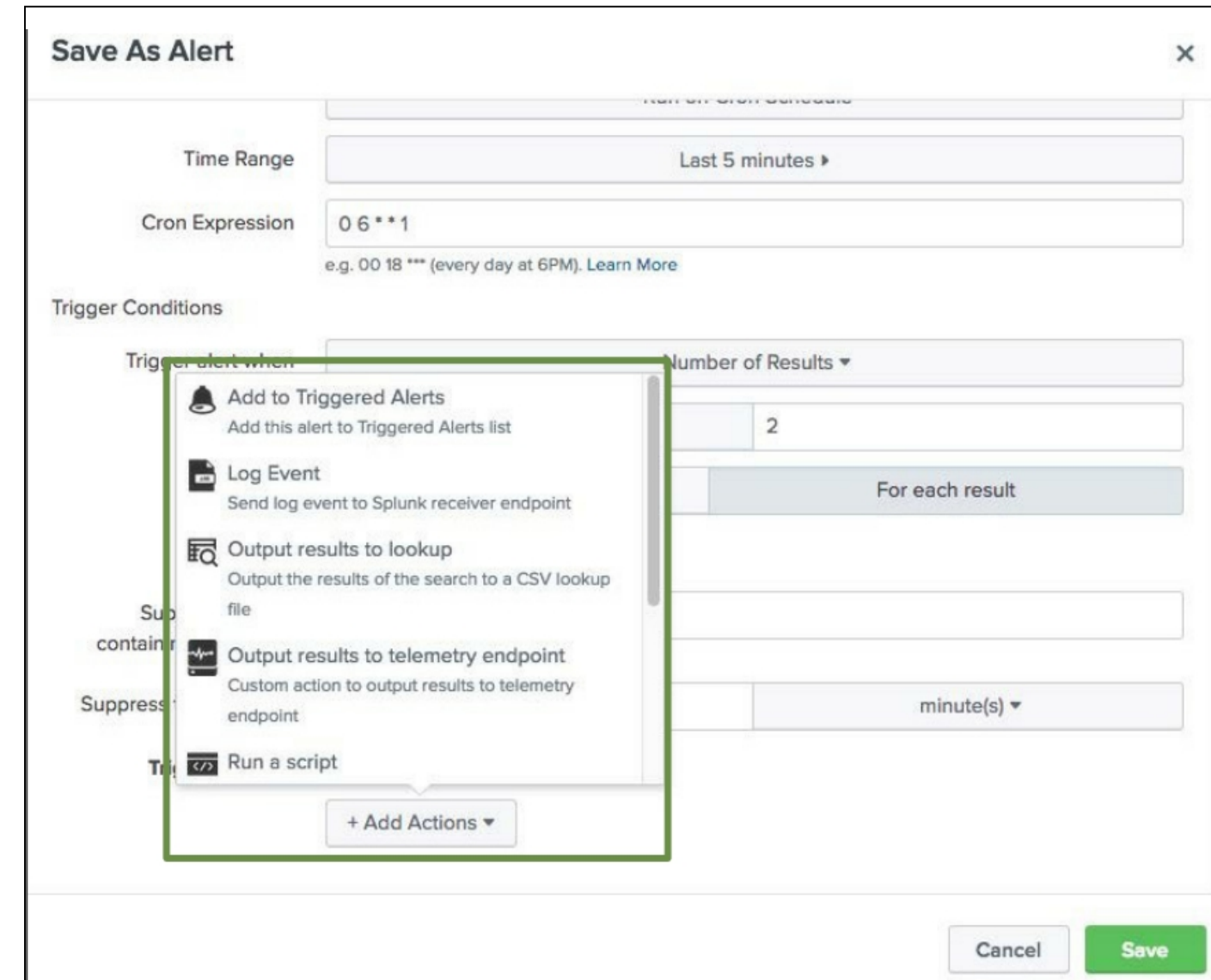
- **For each result** – executes the alert actions once *for each result* that matches the conditions
- Select the Throttle option to suppress the actions for results that have the same field value within a specified time range
  - Certain situations can cause a flood of alerts, when really you only want one
- In this example:
  - The search runs every 5 minutes
  - 70 events are returned in a 5 minute window—50 events with status=**500**, 20 with status=**503**
  - Since *For each result* is selected, **two actions** trigger—one for each status

The screenshot shows the 'Save As Alert' configuration window. The 'Alert type' is set to 'Scheduled'. The 'Run on Cron Schedule' dropdown is selected. The 'Time Range' is set to 'Last 5 minutes'. The 'Cron Expression' is '0 6 \* \* 1', with a note 'e.g. 00 18 \*\*\* (every day at 6PM). Learn More'. Under 'Trigger Conditions', 'Trigger alert when' is set to 'Number of Results', which is 'is greater than' 2. The 'Trigger' is set to 'For each result'. The 'Throttle' checkbox is checked. The 'Suppress results containing field value' is set to 'status'. The 'Suppress triggering for' is set to '10' minutes.

Alert type	Scheduled	Real-time
Run on Cron Schedule	Run on Cron Schedule ▼	
Time Range	Last 5 minutes ▶	
Cron Expression	0 6 * * 1 e.g. 00 18 *** (every day at 6PM). <a href="#">Learn More</a>	
Trigger Conditions	Trigger alert when	
	Number of Results ▼	
	is greater than ▼	2
Trigger	Once	For each result
Throttle ?	<input checked="" type="checkbox"/>	
Suppress results containing field value	status	
Suppress triggering for	10	minute(s) ▼

# Add Trigger Actions

- Add to Triggered Alerts – adds the alert to the Activity > Triggered alerts list
- All actions available for scheduled reports are also available for alerts:
  - Log Event
  - Output results to lookup
  - Output results to telemetry endpoint
  - Run a script
  - Send email
  - Webhook



The screenshot shows the 'Save As Alert' dialog box in Splunk. The 'Time Range' is set to 'Last 5 minutes' and the 'Cron Expression' is '0 6 \* \* 1'. The 'Trigger Conditions' section is highlighted with a green box, showing a list of actions: 'Add to Triggered Alerts', 'Log Event', 'Output results to lookup', 'Output results to telemetry endpoint', and 'Run a script'. The 'Add to Triggered Alerts' action is selected. The 'Number of Results' is set to 2, and the 'For each result' option is selected. The 'Suppress' section is also visible, with a 'minute(s)' dropdown set to 1. The 'Cancel' and 'Save' buttons are at the bottom right.



# Alert Actions – Add to Triggered Alerts

Choose an appropriate severity for the alert

Save As Alert

e.g. 00 18 \*\*\* (every day at 6PM). Learn More

Trigger Conditions

Trigger alert when

Number of Results

is greater than

2

Trigger

Once

For each result

Throttle ?

☒

Suppress results containing field value

status

Suppress triggering for

10

minute(s)

Trigger Actions

+ Add Actions

When triggered

Add to Triggered Alerts

Remove

Severity

Medium

Info

Low

Medium

High

Critical

App

CLASS: Fundamentals 1 (class\_F...

Owner

student...

Severity

All

Alert

All

<prev

next>

Showing 1-12 of 12 results

Time	Fired alerts	App	Type	Severity	Mode	Actions
<input type="checkbox"/> 2018-01-11 00:26:29 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/> 2018-01-11 00:26:28 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/> 2018-01-11 00:26:24 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/> 2018-01-11 00:26:23 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/> 2018-01-11 00:26:19 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>

# Alert Actions – Send Email

Customize the content of email alerts

- To - enter the email address(es) of the alert recipients
- Priority – select the priority
- Subject – edit the subject of the email (the \$name\$ token is the title of the alert)
- Message – provide the message body of the email
- Include – select the format of the alert
- Type – select the format of the text message

The screenshot shows the 'Save As Alert' dialog box with the 'Send email' action selected. The configuration fields are as follows:

- When triggered:** Send email (with a 'Remove' link)
- To:** (Empty text box) Comma separated list of email addresses. [Show CC and BCC](#)
- Priority:** Normal (dropdown menu)
- Subject:** Splunk Alert: \$name\$
- Message:** The alert condition for '\$name\$' was triggered. The email subject, recipients and message can include tokens that insert text based on the results of the search. [Learn More](#)
- Include:**
  - ☒ Link to Alert
  - ☒ Link to Results
  - ☐ Search String
  - ☐ Inline **Table** (dropdown)
  - ☐ Trigger Condition
  - ☐ Attach CSV
  - ☐ Trigger Time
  - ☐ Attach PDF
- Type:** HTML & Plain Text (selected) | Plain Text

Buttons at the bottom: Cancel, Save

# Viewing Triggered Alerts

- If you elected to list in triggered alerts, you can view the results by accessing **Activity > Triggered Alerts**
- Click **View results** to see the matching events that triggered the alert
- Click **Edit search** to modify the alert definition

The screenshot displays the Splunk Enterprise interface for viewing triggered alerts. The top navigation bar includes the Splunk logo, 'enterprise', and various menu items like 'Apps', 'student1', 'Messages', 'Settings', 'Activity', and 'Help'. Below the navigation bar, there's a filter section with 'App' (CLASS: Fundamentals 1), 'Owner' (student...), 'Severity' (All), and 'Alert' (Jobs). A dropdown menu for 'Alert' is open, showing 'Jobs' and 'Triggered Alerts' (highlighted with a green box). The main content area shows a table of triggered alerts with columns: Time, Fired alerts, App, Type, Severity, Mode, and Actions. The table contains three rows of alerts, all for 'Web server errors' in the 'class\_Fund1' app, triggered at 00:26:29, 00:26:28, and 00:26:24 UTC. Each row has links for 'View results', 'Edit search', and 'Delete'.

Time	Fired alerts	App	Type	Severity	Mode	Actions
2018-01-11 00:26:29 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2018-01-11 00:26:28 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
2018-01-11 00:26:24 UTC	Web server errors	class_Fund1	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>



# Other Resources

- Splunk App Repository  
<https://splunkbase.splunk.com/>
- Splunk Answers  
<http://answers.splunk.com/>
- Splunk Blogs  
<http://blogs.splunk.com/>
- Splunk Wiki  
<http://wiki.splunk.com/>
- Splunk Docs  
<http://docs.splunk.com/Documentation/Splunk>
- Splunk User Groups  
<http://usergroups.splunk.com/>