



Alerts on Splunk

By: Ryan Stewart

What is an Alert?

Alerts are predefined searches that activate when specific conditions are fulfilled. These can be scheduled to run at specified intervals or set to operate in real-time. Caution is advised when configuring real-time alerts to prevent overloading your Splunk server.

****Exercise:****

Utilize the same search request as in the report section and save it as an alert.

Save As Alert

Settings

Title

Title

Description

Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run every week

On

Monday

at

6:00

Expires

24

hour(s)

Trigger Conditions

Trigger alert when

Number of Results

is greater than

0

Trigger

Once

For each result

Throttle ?

Trigger Actions

+ Add Actions

Cancel

Save

