

AWS

CloudTrail

what is it?

CloudTrail is concerned with the **'who?'**

- Who made the API call?
- Which IP address has done something?
- How did a user access a bucket?

CloudTrail is turned on by default and sends logs to an S3 bucket for further analysis.

when to use it?

- CloudTrail can help with auditing and allows us to start with the problem, and trackback to where the problem began.
- It's timestamps a record of 'who' and lets us follow the trail to find the cause of any problems.
- CloudTrail is free of charge BUT the storing of the logs on S3 is not. Check out the Monthly Cost Calculator to find out how much you will be charged given your use case.