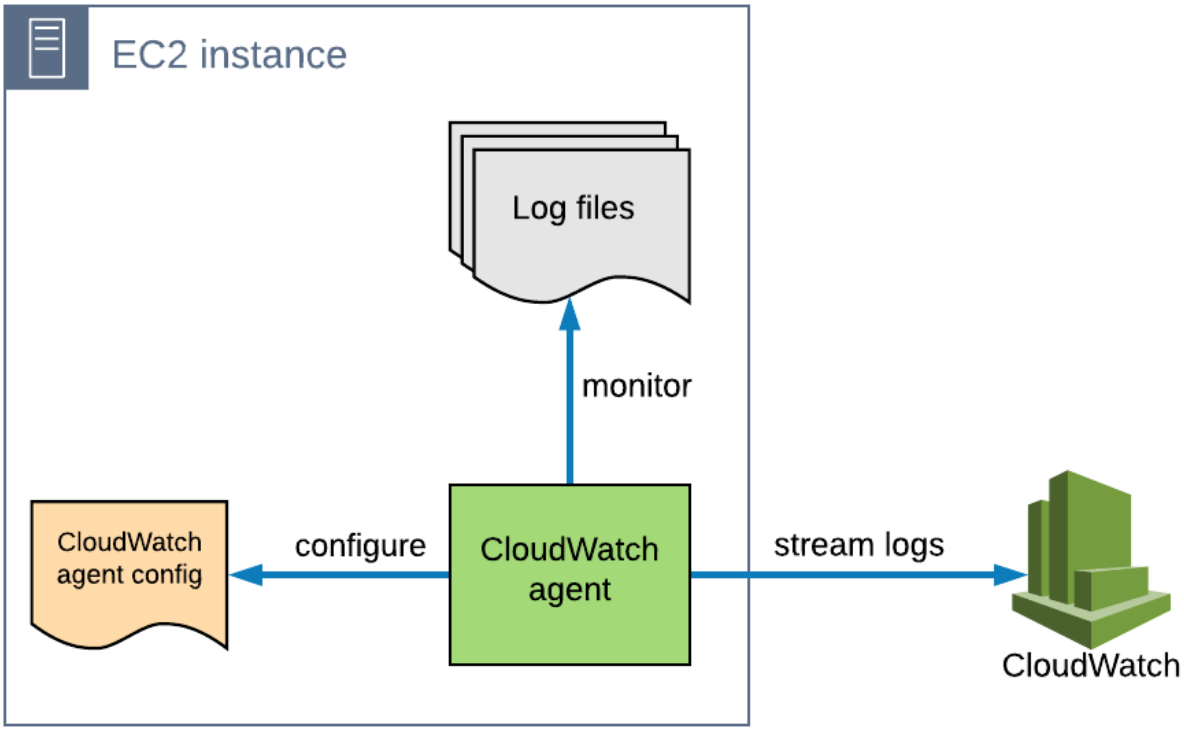
Understanding the CloudWatch agent

The best way to ship logs from an EC2 instance is to use the CloudWatch agent. This is a process that runs on the instance and can be configured to ship any logs (and metrics) to CloudWatch:



To get the agent working, you have to follow these steps, which are all covered in today's working example in the next section:

1. **role setup**: configure a role attached to the EC2 instance to include the *CloudWatchAgentServerPolicy* managed policy. This allows the agent to push the logs to CloudWatch.
2. **agent installation**: the agent can be installed using *rpm* (Red Hat package manager) and can be downloaded from an Amazon provided S3 bucket
3. **configuration:** a JSON file must be supplied which defines the logs to be collected along with which log group they should be streamed to. The CloudWatch agent then sends log events to log streams it creates, following a naming convention that you specify.

Setting up the CloudWatch agent: a working example

To demonstrate how to use the CloudWatch agent to stream logs, we'll setup:

1. an EC2 instance
2. a CloudWatch agent on that instance that streams the */var/log/secure* log file to CloudWatch. This log contains authentication information such as user logins and password changes.