Request headers in API checks

Request headers may be a critical part of requirements for an active monitoring test’s configuration in order to effectively simulate a transaction.

Request headers can include rules and settings to define how an HTTP transaction should operate. There is a standard set of supported request header types that have specific names and purposes. Some common examples of request headers are:

- Authorization. Send credentials for basic HTTP authentication to give permission for access.
- Cache-Control. Tell the browser how long a resource is eligible to be cached and reused.
- Content-Type. Tell a server the MIME type of the body of a request so that the server knows how to parse the data.
- Cookie. Set a cookie to be stored in the browser so we can track state or sessions.

Some developers may also implement custom request headers with custom names. It’s common to see custom request headers with a prefix of “X,” for example: X-Http-Method-Override could override the request method from something like POST to another method like PUT or DELETE.

Procedure

To monitor the availability, response time, and data quality for transactions with APIs, use Splunk’s API check to set request headers with each request as part of a transaction.

Consider a scenario where you need to POST username and password credentials to access some information. After you’re logged in at that endpoint, you need to store and set a session ID in order to pre-populate other components specific to our session.

When building the steps for an API check, click + Add a Request Header to supply one or more headers at each request step.

Next steps

You can add more functional steps to this transaction or add an Assert step to confirm that the session ID is set as
expected.

You might be interested in other processes associated with the Monitoring API transactions use case.