Monitoring API transactions

Your software uses APIs to connect services and pass data back and forth between uniquely managed systems, but that connectivity and interdependence creates vulnerabilities. As a site owner, you've decided that the benefit of relying on the third-party service outweighs the risk of these types of failures. However, in order to accurately assess the risk and have visibility into the impact of these services over time, it's crucial that you monitor the part of your site's user flow that relies on an API. You want to build out robust and flexible performance tests for your API transactions.

How to use Splunk software for this use case

Depending on what information you have available, you might find it useful to identify some or all of the following:

- Request headers in API checks
- HTTP basic authentication to an API
- API key authentication
- Ticket-based API authentication
- Data validation for API responses

Next steps

These API checks are only a few of the many ways you can implement robust monitoring for an API. You may also want to consider:

- Writing performance tests in a way that allows a system to call an API and not receive data. When writing code with lots of local calls, a wrapper that calls to an external API often goes unnoticed with the context of an application. If your test is designed to alert when no data is present, this will help make sure you don’t miss critical errors.
- Building a synthetic, external monitor to test pulling data from your own API and put alerting in place so that your engineers know right away if there’s any type of issue that might put you close to breaching your service level agreements.
- Testing availability. Is this API endpoint up? Is it returning an error?
- Testing response time. How quickly is the API returning responses? Is the response time degrading over time? Is the response time worse in production than in pre-production?
- Testing multi-step processes. Can you successfully save and reuse a variable from this API? Does authentication work as expected? Can you complete a transaction with data from this API?

These additional Splunk resources might also help you understand and implement this use case:

- Splunk Docs: API Check Overview
- White Paper: APIs in action