Best practices when configuring an HTTP Proxy Server for splunkd
Best practices when configuring an HTTP Proxy Server for splunkd

You can set up an HTTP proxy server for splunkd so that all HTTP/S traffic originating from splunkd flows through the proxy server.

Points to Remember

1. Splunk supports only non-TLS proxying. Proxy servers listening directly on HTTPS are not supported.

2. Verify your proxy settings for accuracy and make sure they comply with your organization's network policies.

3. For performance issues with the proxy server, see the performance tuning tips below.

Performance Tuning with Apache Server

If you have a large number of clients communicating through the proxy server, you might see a performance impact for those clients. In the case of performance impact:

- Check that the proxy server is adequately provisioned in terms of CPU and memory resources.
- Use the different multi-processing modules (MPM) and tune the following settings depending on the requirements of your environment. Check the Apache documentation for additional information.

```
ServerLimit  <Upper limit on configurable number of processes>
StartServers  <Number of child server processes created at startup>
MaxRequestWorkers  <Maximum number of connections that will be processed simultaneously>
MinSpareThreads  <Minimum number of idle threads available to handle request spikes>
MaxSpareThreads  <Maximum number of idle threads>
ThreadsPerChild  <Number of threads created by each child process>
```

Performance Profiling with Squid Server

If you have a large number of clients communicating through the proxy server, you might see a performance impact for those clients. Please make sure that the proxy server is adequately provisioned in terms of CPU & Memory resources. Please check the Squid profiling documentation for additional information.