SSL certificates nearing expiration

SSL certificates that are allowed to expire can often lead to outages or, at a minimum, a poor user experience while browsing the site.

Data required

Web server data

Procedure

1. Verify that you installed the SSL Certificate Lookup Add-on. For more information, see About installing Splunk add-ons.

2. Run the following search. You can optimize it by specifying an index and adjusting the time range.

```
| makeresults
| eval dest="<domain to check>"
| lookup sslcert_lookup dest
| eval seconds_till_expiry = ssl_end_time - now(), duration_till_expiry = tostring(seconds_till_expiry, "duration")
| table dest seconds_till_expiry duration_till_expiry ssl_is_valid ssl_issuer_common_name
```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the specifics of your environment.

<table>
<thead>
<tr>
<th>Splunk Search</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>makeresults</td>
</tr>
<tr>
<td></td>
<td>lookup sslcert_lookup dest</td>
</tr>
<tr>
<td></td>
<td>eval seconds_till_expiry = ssl_end_time - now(), duration_till_expiry = tostring(seconds_till_expiry, &quot;duration&quot;)</td>
</tr>
<tr>
<td></td>
<td>table dest seconds_till_expiry duration_till_expiry ssl_is_valid ssl_issuer_common_name</td>
</tr>
</tbody>
</table>
Next steps

The SPL in this procedure uses `makeresults` and `eval` commands to specify the domain to check; however, other more scalable options are also viable. For instance you could:

- Create a lookup with a list of domains to periodically check and begin the SPL with `| inputlookup <your_domain_lookup_file>`
- Use raw results from a Splunk search, such as the data coming from the Website Monitor app to identify the domains to check

To alert when an SSL certificate is nearing or past expiration, you can use the SPL in this procedure to configure a Core Splunk alert. You can filter the results based on the number of seconds before the SSL certificate is expiring. For instance, adding `| where seconds_till_expiry < (60*60*24)` will alert when an SSL certificate is set to expire within the next 24 hours.

Finally, you might be interested in other processes associated with the Managing web server performance use case.