Splunk® Enterprise Securing Splunk Enterprise 7.3.0

Use authentication tokens

Generated: 12/29/2019 1:44 am
Use authentication tokens

If you have been assigned an authentication token, you can access a Splunk platform instance using Representational State Transfer (REST) calls. This method lets you access the instance and make web requests without having to authenticate with credentials.

You must possess a valid token that has been given to you from an administrator who maintains the instance. The token cannot be expired, as expired tokens are unusable. Administrators can delay when the validity of a token starts, meaning that the token cannot be used until its validity begins.

You cannot use a token on any instance other than the instance where the administrator granted you the token. For example, if you have a token for server1, and need access to server2, you must ask the administrator for server2 to give you access to a token there. There is an exception on search head clusters: if an administrator grants you token-based access to a search head cluster, that token is valid for all search head cluster nodes.

You lose access to the instance through the token if any of the following occurs:

- The token expires. You can ask the administrator to issue a new token to regain access.
- The administrator disables the token. The administrator must reenable the token before you can use it again.
- The administrator deletes the token. You can ask the administrator to issue a new token to regain access.
- The administrator disables token authentication, either temporarily or permanently.
- The administrator deletes your account.
- You lock out or disable your Active Directory account on a Splunk platform instance that uses LDAP to connect to Active Directory.

Confirm that the administrator sends you the full token when they assign it to you. You must have the full token to authenticate with it through REST. If you do not, the Splunk platform rejects those authentication requests as if you had entered incorrect credentials.

Use an authentication token to make REST calls to an instance

After you receive a valid token for the instance you want to use, you can use the token to make calls to REST endpoints on the instance. Your access is the same
as what you have if you logged in with credentials.

The type of web request you make depends on the endpoint you want to access and what you want to do with the endpoint. For more information on REST endpoints and how to use them, see the REST API User Manual and the REST API Reference Manual for information on REST and using REST endpoints.

Understand the ramifications of making REST calls using tokens. Tokens are only a method of authentication, not a safeguard against making potentially dangerous changes to a Splunk platform instance. If you have questions or concerns about using tokens, contact your administrator.

Currently, tokens are available only for making REST calls to a Splunk Enterprise instance. You cannot use tokens to authenticate using the CLI or Splunk Web. You must use credentials for these authentication methods.

Use your REST web client or command line tool to make an HTTP GET, POST, or DELETE request on an endpoint. When you make the request, include the management port of the instance:

curl -X GET -H "Authorization: Bearer <token>" https://<instance host name or IP address>:<management port>/services/authentication/users/<user>

If the operation succeeds, the command prints a response in XML that contains the information that the instance generated upon accessing the endpoint.

An authentication failure appears as follows:

<?xml version="1.0" encoding="UTF-8"?>
<response>
  <messages>
    <msg type="WARN">call not properly authenticated</msg>
  </messages>
</response>

Insufficient permissions to access the endpoint appear as follows:

<response>
  <messages>
    <msg type="ERROR">You (user=<user>) do not have permission to perform this operation (requires capability: <capability> [or <capability>...]</msg>
</response>
Examples

These examples presume that you have properly configured your SSL certificates. If you have not, then the commands will not work. As a temporary measure to test connectivity to SSL, you can use the -k argument for curl to bypass certificate review. Do not do this long term, as certificates are a key part of maintaining security in SSL.

The following example accesses the /apps/local endpoint to retrieve a list of local Splunk applications on the instance:

<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>
<feed xmlns="http://www.w3.org/2005/Atom"
xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
<title>localapps</title>
<id>https://10.224.100.135:34740/services/apps/local</id>
<updated>2019-02-13T23:05:24+00:00</updated>
<generator build="7d447048a453" version="7.3.0"/>
<author>
    <name>Splunk</name>
</author>
<link href="/services/apps/local/_new" rel="create"/>
<link href="/services/apps/local/_reload" rel="_reload"/>
<opensearch:totalResults>18</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
    <title>alert_logevent</title>
    ...
</entry>
...
</feed>

The following example accesses the authorization/roles endpoint to get information about the roles that have been configured on the instance:

<?xml-version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>
<feed xmlns="http://www.w3.org/2005/Atom"
xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
<title>roles</title>
...
<id>https://10.224.100.135:34740/services/authorization/roles</id>  
<updated>2019-02-13T23:10:41+00:00</updated>  
<generator build="7d447048a453" version="7.3.0"/>  
<author> <name>Splunk</name>  
</author>  
<link href="/services/authorization/roles/_new" rel="create"/>  
<opensearch:totalResults>5</opensearch:totalResults>  
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>  
<opensearch:startIndex>0</opensearch:startIndex>  
<s:messages/>  
<entry>  
<title>admin</title>  
...  
</entry>  
...  
</feed>