Creating allows lists with the Splunk Cloud Platform Admin Configuration Service API

Today's infrastructure exists in a dynamic and rapidly changing environment. New compute sources and networks come online quickly, and Splunk Cloud admins have to keep pace to ensure that this data flows into their Splunk Cloud deployment. Traditional IP allow lists can be leveraged to permit one or more IP addresses from accessing Splunk. However, as an admin, you'd like a faster way to quickly add or remove IPs or entire subnets from your Splunk environment.

This solution is applicable to 8.x Splunk Cloud environments.

An authentication token is required for administrative access to the ACS API. ACS leverages JSON Web Token (JWT) support. A Splunk JWT must be presented in all ACS requests. The lifespan of the JWT can vary, ranging anywhere from a few minutes to 60 days. Any customer using Splunk version 8.0.2007 or higher can create and distribute these credentials. For more information on setting up and managing tokens in your environment, see the Splunk documentation.

The Admin Configuration Service API is equipped with a rich set of features that extend well beyond the user interface. Starting with IP allow lists, ACS is a RESTful API that equips Splunk Cloud admins with a steady stream of capabilities that remove friction and provide full control over their deployments. ACS streamlines a number of common IP allow list use cases, shown in the following table.

<table>
<thead>
<tr>
<th>Use case</th>
<th>Splunk resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>API access</td>
<td>Search head</td>
</tr>
<tr>
<td>HEC-based ingestion</td>
<td>Indexer</td>
</tr>
<tr>
<td>Forwarder-based ingestion</td>
<td>Indexer</td>
</tr>
<tr>
<td>UI access (if applicable)</td>
<td>Search head</td>
</tr>
<tr>
<td>UI access (if applicable)</td>
<td>Inputs data manager</td>
</tr>
<tr>
<td>IDM API access</td>
<td>Inputs data manager</td>
</tr>
</tbody>
</table>

The examples below leverage the Postman API client. ACS can be leveraged by Curl or any equivalent API client.

1. To retrieve a comprehensive description of the REST APIs, perform a GET call to the ACS endpoint at https://admin.splunk.com.
2. Assign your Splunk deployment details to specific variables such as stack, baseURL, and feature. A feature can include any of the predefined IP allow list blocks. For the full set of feature types, see the ACS documentation.

3. Assigned your Splunk JWT to a token variable and pass this value in your authorization header.

4. Perform a GET call for a listing of all subnets for a feature type. For example, you can request all in-use subnets for HEC or Splunk forwarding (S2S). For more information, see the documentation Splunk Cloud Admin Guide: Configure IP Allow lists.

5. To add new subnets to your Splunk deployment, perform a POST call. ACS can accept one or more subnets in JSON format, as shown in the following image. Although the URI is the same, it’s good practice to check the feature type before any submissions, especially if the feature is assigned to a variable in Postman. The first octet in this example was replaced with a ‘#’. ACS expects subnets to be expressed in standard CIDR notation.

![JSON format for adding subnets](image)

A 200 response code indicates that the request has successfully passed all ACS validation (for example, the public IP is valid and not on the Bogon list) and is in the queue to be applied to your Splunk deployment.

6. The time between a submission and update to your deployment is typically within a few minutes. To query the status of the change set, perform a GET call that passes only your Splunk deployment (stack) name.

![GET call to query change set status](image)

7. Review the ACS responses:
   - Ready. All changes have been applied to your deployment
   - Pending. There are some changes that have not been applied to your deployment
   - Failed. The changes failed in your deployment. Contact Splunk Support to open a case if you encounter successive failures.

If you need to remove an allow list, the DELETE request mirrors the format of the POST (add subnet allow list) call shown in step 5 of this procedure.

---

Next steps

These additional Splunk resources might help you understand and implement these recommendations:

- Blog: Splunk Cloud Self-Service: Announcing The new Admin Config Service API
- Splunk Docs: Configure IP allow list for Splunk Cloud Platform
- Splunk Docs: Splunk Cloud Admin Manual

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.