Users who haven't accessed AWS for an extended time

You might want to know which users are not actively using your AWS cloud infrastructure when doing the following:

- Managing an Amazon Web Services environment

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- Splunk Enterprise or Splunk Cloud Platform
- AWS description data
- Splunk Add-on for Amazon Web Services

Example

To better control access to your cloud infrastructure, you want to review who has access and how frequently or infrequently they have accessed the system. You also want to see accounts created for employees who are no longer with the company or no longer in the organization where cloud access is needed.

To optimize the search shown below, you should specify an index and a time range.

1. Ensure that your deployment is ingesting AWS data through one of the following methods:
   - Pulling the data from Splunk via AWS APIs. At small scale, pull via the AWS APIs will work fine.
   - Pushing the data from AWS into Splunk via Lambda/Firehose to Splunk HTTP event collector. As the size and scale of either your AWS accounts or the amount of data to be collected grows, pushing data from AWS into Splunk is the easier and more scalable method.

2. Run the following search:

```plaintext
sourcetype="aws:description" source="*:iam_users" |dedup Arn sortBy -_time |spath output=AccessKeys path=AccessKeys{} |eval AccessKeys=mvfilter(match(AccessKeys,":\"Status\": \"Active\",\"\")}) |fields account_id UserName AccessKeys PasswordLastUsed |mvexpand AccessKeys |rex field=AccessKeys ":\"LastUsedDate\": \"(?<LastUsedDate>[\^\"]\")" |eval ak_used_day=strptime(LastUsedDate,"%FT%T"), ps_used_day=strptime(PasswordLastUsed,"%FT%T"), recent_used_day=max(ak_used_day,ps_used_day), diff_days=((now() - recent_used_day) / 86400) |stats min(diff_days) AS no_used_days BY UserName, account_id |eval no_used_days=round(no_used_days)
```

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.
| where (no_used_days > 30)  
| eval insight="User unused for extended period of time. (".no_used_days." days since last access)"
| sort - no_used_days
| table account_id UserName insight

## 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.

### Splunk Search

```
sourcetype="aws:description"  
source="*:iam_users"
```

**Explanation**

Search only your iam users and filter by description data.

```
dedup Arn sortby -_time
```

**Explanation**

Remove duplicate instances by Amazon resource name (Arn) and sort the remaining results with the most recent instances first.

```
spath output=AccessKeys path=AccessKeys{}
```

**Explanation**

Parse the JSON data and obtain the list of access keys configured for each user.

```
eval AccessKeys=mvfilter(match(AccessKeys, \\"Status\": \\"Active\", \\")")
```

**Explanation**

Filter the list to return only active access keys by matching on "Status: Active" in the AccessKeys JSON text.

```
|fields account_id UserName AccessKeys PasswordLastUsed
```

**Explanation**

Show only the fields listed.

```
mvexpand AccessKeys
```

**Explanation**

Create a row for each access key record for each user.

```
rex field=AccessKeys \\"LastUsedDate\": \\("\"\")"(?<LastUsedDate>\"\")"
```

**Explanation**

Extract and parse the timestamp for the last time the access key was used.

```
eval ak_used_day=strptime(LastUsedDate,"%FT%T"),  
ps_used_day=strptime(PasswordLastUsed,"%FT%T"),  
recent_used_day=max(ak_used_day,ps_used_day),
```

**Explanation**

Determine the most recent access time for each user and filter the results to only users who have not accessed AWS in 30 or more days.

---

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.
Splunk Search

diff_days=((now() - recent_used_day) / 86400)

|stats min(diff_days) AS no_used_days BY UserName, account_id

|eval no_used_days=round(no_used_days)

|where (no_used_days > 30)

|eval insight="User unused for extended period of time. (.no_used_days." days since last access)"

|sort - no_used_days

|table account_id UserName insight

---

**Result**

Sample results for this search are shown in the table below. The user name and the amount of time since last seen is displayed. To prevent accidental misconfigurations or security concerns, a good practice is to revoke access for users who access cloud infrastructure on an infrequent basis.

<table>
<thead>
<tr>
<th>account_id</th>
<th>UserName</th>
<th>insight</th>
</tr>
</thead>
<tbody>
<tr>
<td>63605715280</td>
<td>yzhu</td>
<td>User unused for extended period of time. (1684 days since last access)</td>
</tr>
<tr>
<td>63605715280</td>
<td>zhouz</td>
<td>User unused for extended period of</td>
</tr>
</tbody>
</table>

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.
<table>
<thead>
<tr>
<th>account_id</th>
<th>UserName</th>
<th>insight</th>
</tr>
</thead>
<tbody>
<tr>
<td>63605715280</td>
<td>yang_cao</td>
<td>User unused for extended period of time. (1451 days since last access)</td>
</tr>
<tr>
<td>63605715280</td>
<td>yfu</td>
<td>User unused for extended period of time. (1383 days since last access)</td>
</tr>
</tbody>
</table>

The AWS app does a similar search for lack of use by users and provides additional insight for lack of password policy, IAM access key rotation, and password reuse not prevented. These can be found by navigating to Insights > IAM Insights > Insights Filter.