Splunk4Admins

Splunk Cloud Admin Config Service

splunk>
a CISCO company

Forward-looking statements

This presentation may be deemed to contain forward-looking statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. Any statements that are not statements of historical fact (including statements containing the words “will,” “believes,” “plans,” “anticipates,” “expects,” “estimates,” “strives,” “goal,” “intends,” “may,” “endeavors,” “continues,” “projects,” “seeks,” or “targets,” or the negative of these terms or other comparable terminology, as well as similar expressions) should be considered to be forward-looking statements, although not all forward-looking statements contain these identifying words. Readers should not place undue reliance on these forward-looking statements, as these statements are management’s beliefs and assumptions, many of which, by their nature, are inherently uncertain, and outside of management’s control. Forward-looking statements may include statements regarding the expected benefits to Cisco, Splunk and their respective customers from the completed transaction, the integration of Splunk’s and Cisco’s complementary capabilities and products to create an end-to-end platform designed to unlock greater digital resilience for customers, our expectations regarding greater resiliency and better product outcomes, including for security and observability, plans for future investment, our development and use of AI and the role that our innovation plays as our customers adopt AI. Statements regarding future events are based on Cisco’s current expectations, estimates, and projections and are necessarily subject to associated risks related to, among other things, (i) the ability of Cisco to successfully integrate Splunk’s market opportunities, technology, personnel and operations and to achieve expected benefits, (ii) Cisco’s ability to implement its plans, forecasts and other expectations with respect to Splunk’s business and realize expected synergies, (iii) the outcome of any legal proceedings related to the transaction, (iv) the effects on the accounting relating to the acquisition of Splunk, (v) legislative, regulatory, and economic developments, (vi) general economic conditions, and (vii) the retention of key personnel. Therefore, actual results may differ materially and adversely from the anticipated results or outcomes indicated in any forward-looking statements. For information regarding other related risks, see the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent reports on Form 10-Q filed with the SEC on February 20, 2024 and November 21, 2023, respectively. The parties undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk>

Enroll in Today's Workshop

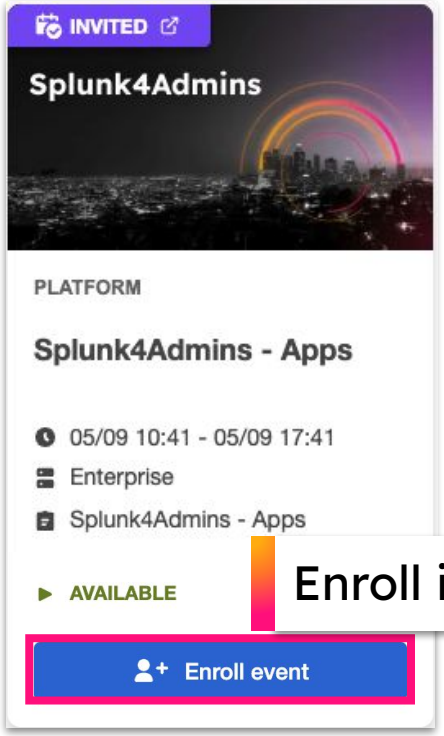
Tasks

1. Get a splunk.com account if you don't have one yet:
   https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event:
   https://splunk.show/<uniqueID>
3. Download the hands-on lab guide:
   https://splk.it/S4A-ACS-Lab-Guide

   Contains step-by-step instructions for all of today's exercises!

1. Download a copy of today's slide deck:
   https://splk.it/S4A-ACS-Attendee

Goal



Enroll in today's event

Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?

Workshop Agenda

- Who?|What?|Why?
- Expectations
- What is Splunk Cloud Admin Config Service?
- How does Admin Config Service work?
- What capabilities does Admin Config Service provide?
- How is Admin Config Service different from the Splunk Cloud GUI?
- Setup - Lab[1]
  - Splunk Cloud instance
  - Admin Config Service (acs) tool
  - Curl
- Scripts
- Labs - 2 3 4 5 6 7 8 9
- Summary

Audience

Who is this Workshop for?

- Those who are interested in how to interact via command line tools with Splunk Cloud …
  - Splunk Admins managing Splunk Cloud stacks
  - “Required”: Power User Certified
  - “Required”: Splunk Admin enabled
  - Preferred: Splunk Admin Certified

Expectations for Workshop

Splunk Cloud Admin Config Service - hereafter known as '**acs**'

- Last roughly 60 - 75 minutes
- A survey of available activities using the acs REST interface
- Experience the install of the 'acs' tool
- Configure the 'acs' tool to interact with a Splunk Cloud instance
- Execute multiple use cases to experience how the tool can be used to interact with and manage Splunk Cloud instances

What is Splunk Cloud “ACS”?

From Splunk Docs -
The Admin Config Service (ACS) is a cloud-native API that provides programmatic self-service administration capabilities for Splunk Cloud Platform . It allows Splunk Cloud Platform administrators to perform common administrative tasks without assistance from Splunk Support.

- An API accessible via REST on all Splunk Cloud stacks
- A trackable alternative to the interactive GUI (can use GUI)
  - All of the positives of REST (scalability, flexibility, accessibility, …)
  - Negatives (complexity, lack of standardization, security, …)
- RESTful endpoints that provide direct access to Splunk Cloud configuration settings
- Provides capabilities that previously required Support

About the Admin Config Service (ACS) API	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSIntro
What is REST?	https://restfulapi.net/

Workshop Agenda

- Who?|What?|Why?
- Expectations
- What is Splunk Cloud Admin Config Service?
- How does Admin Config Service work?
- What capabilities does Admin Config Service provide?
- How is Admin Config Service different from the Splunk Cloud GUI?
- Setup - Lab[1]
  - Splunk Cloud instance
  - Admin Config Service (acs) tool
  - Curl
- Scripts
- Labs - 2 3 4 5 6 7 8 9
- Summary

How does ACS work?

REST!

- Predefined endpoints available from Splunkd
- A user with appropriate permissions
- A token associated with that user
- Some form of client that can interact with REST endpoints
  - curl/wget/Invoke-WebRequest (and many others)
  - Python (or other script/programmatic) access
  - ACS tool from Splunk - what will be used in the labs
- Interacts with "https://admin.splunk.com" on every call
- Always uses https for access to any resources
- Responds with JSON

Admin Config Service (ACS) API endpoint reference	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSusage
Basic setup and usage concepts for the Admin Config Service (ACS) API	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSusage

Issues with ACS

Gotchas

- Stack type matters - Victoria vs. Classic, but most new are Victoria
  - Classic: can operate against a specific search head (Premium vs. general SH)
- Outbound traffic from management node needs to be permitted
- SAML users may need ‘Authentication Extensions’ enabled (instructions at docs.splunk.com
- Passwords may need to be either escaped or single-quoted on CLI
- ‘acs’ --h is extremely useful, acs <sub-command> <action> --h even more so

Admin Config Service (ACS) API endpoint reference	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSusage
Basic setup and usage concepts for the Admin Config Service (ACS) API	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSusage

Capabilities with ACS

What can be done?

- Manage a stack with change tracking (wrap in a script that outputs directly to Splunk, syslog, or REST call against a change management solution, or splunk the history file)
- Allows asynchronous execution of tasks

- Configure IP allow lists
- Configure outbound ports
- Enable private connectivity
- Export apps
- Manage app permissions
- Manage authentication tokens
- Manage DDSS self storage locations
- Manage HTTP Event Collector (HEC) tokens
- Manage indexes
- Manage limits.conf configurations
- Manage maintenance windows
- Manage maintenance window change freeze
- Manage private apps and add-ons
- Manage restarts
- Manage Splunkbase apps
- Manage users, roles, and capabilities
- Provision Enterprise Managed Encryption Keys (EMEK)
- Retry failed operations
- Set up Unified Identity with Single Sign On for Splunk Observability Cloud

About the Admin Config Service (ACS) API	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSIntro

Differences – ACS vs. SC GUI

Splunk GUI is primary, but.

- Capabilities for ACS are circumscribed and limited (but growing)
- More in Splunk Cloud GUI, but non-trackable via any Change Management System
- Example - Premium App management is in the GUI, but not ACS
- There are differences between the Classic and Victoria experiences
  - Victoria - All Apps everywhere, app export
  - Classic- only against the Adhoc, not for Premium
  - FedRAMP prior to specific versions
- Endpoints being added constantly

Workshop Agenda

- Who?|What?|Why?
- Expectations
- What is Splunk Cloud Admin Config Service?
- How does Admin Config Service work?
- What capabilities does Admin Config Service provide?
- How is Admin Config Service different from the Splunk Cloud GUI?
- Setup - Lab[1]
  - Splunk Cloud instance
  - Admin Config Service (acs) tool
  - Curl
- Scripts
- Labs - 2 3 4 5 6 7 8 9
- Summary

Configure ACS

Splunk Cloud: User

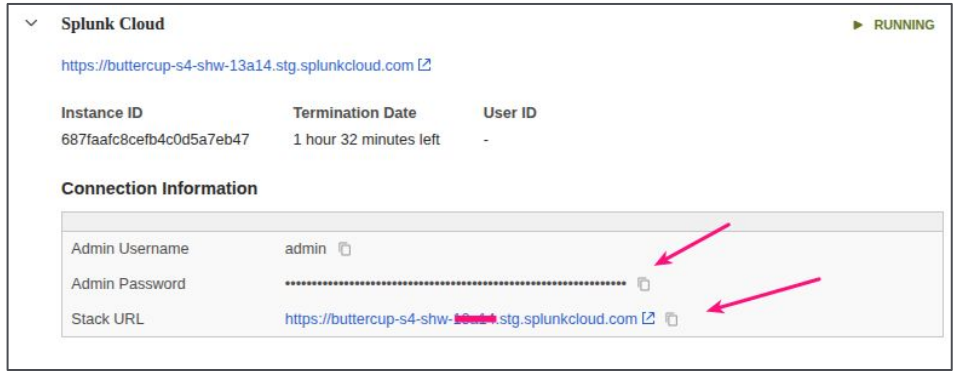
- If needed, create a specific user
  - Debatable as to which is better, have admins use their individual Splunk user, or generate specific users for specific taskings. Both may be appropriate
  - Scripted management should use administrative users only with passwords managed appropriately
  - SAML users require special handling
- Create a token for authentication during exchange
  - A token ensures authentication and authorization and ensures appropriate enforcement
  - Can be multiple tokens per use, with the ‘Audience’ field to differentiate between the uses
  - Ensures end-to-end encryption
  - Should be rotated on a specified cycle (whatever the security team defines)

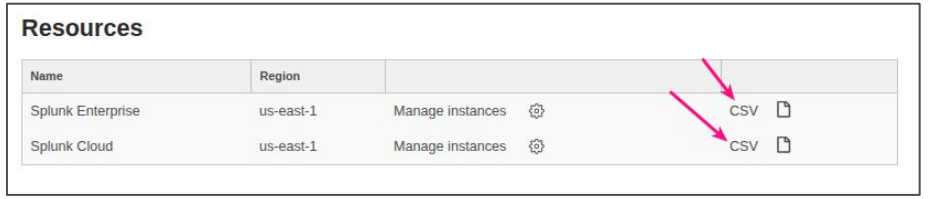
Create authentication tokens (Splunk Cloud)	https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/CreateAuthTokens
Configure user for managing Splunk Cloud via ACS	https://docs.splunk.com/Documentation/SplunkCloud/9.3.2408/Config/ACSCLI#:~:text=and%20password%20values.-,Set%20login%20credentials,-Some%20ACS%20CLI
Configure authentication extensions to interface with your SAML identity provider	https://docs.splunk.com/Documentation/Splunk/latest/Security/ConfigureauthextensionsforSAMLtokens

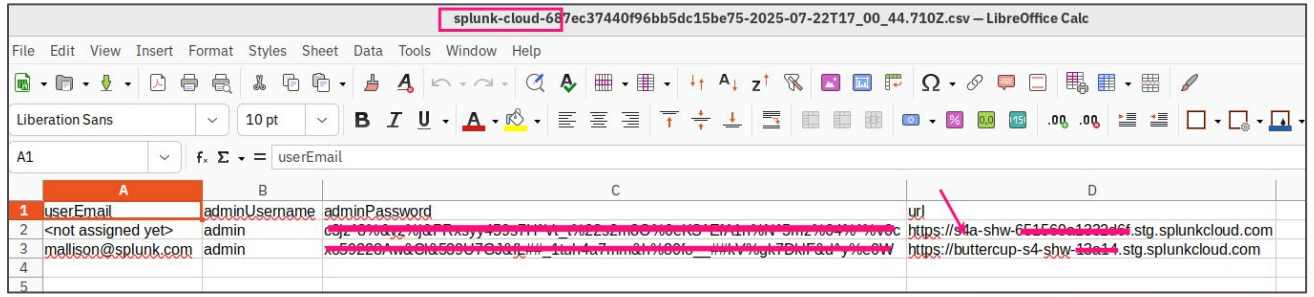
Configure ACS

Find your Cloud instances

- From the link sent out
- ‘Instances Information’ ‘Splunk Cloud’ dropdown
- Or ‘Resources’ CSV





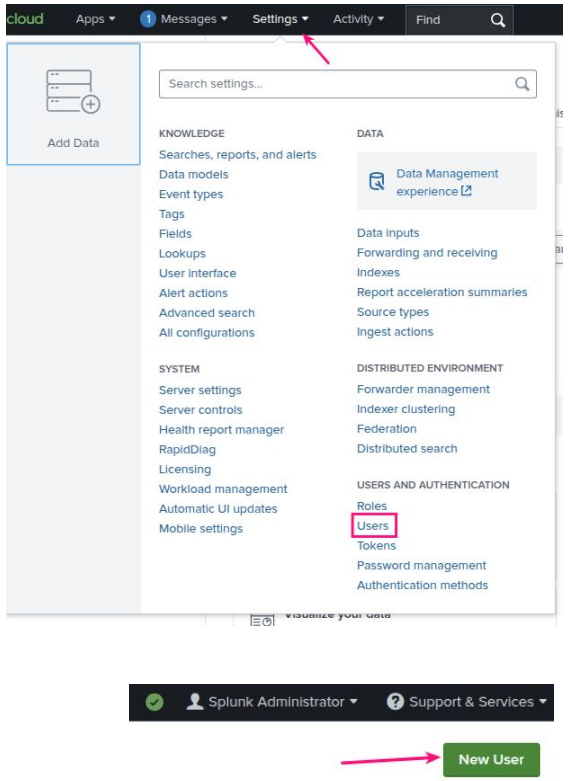


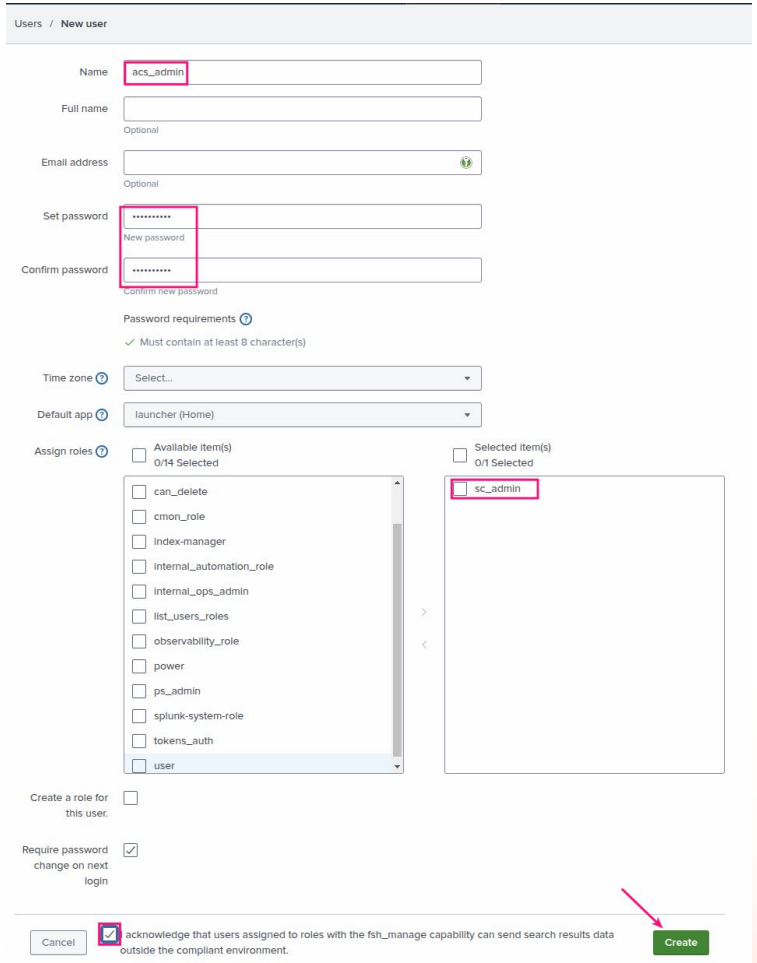
Create a user in Splunk Cloud GUI	https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/Addandeditusers#Create_a_user
Configure user for managing Splunk Cloud via ACS	https://docs.splunk.com/Documentation/SplunkCloud/9.3.2408/Config/ACSCLI#:~:text=and%20password%20values.-,Set%20login%20credentials,-Some%20ACS%20CLI

Configure ACS

Splunk Cloud: User

- Access the Splunk Cloud GUI of your assigned instance
- Create a user configured with roles with appropriate privileges
  - ‘sc_admin’ will always have all that is required
  - If the user will be doing specific tasks requires fewer, ‘least required privileges’ should be applied
  - Can be tuned for customized roles



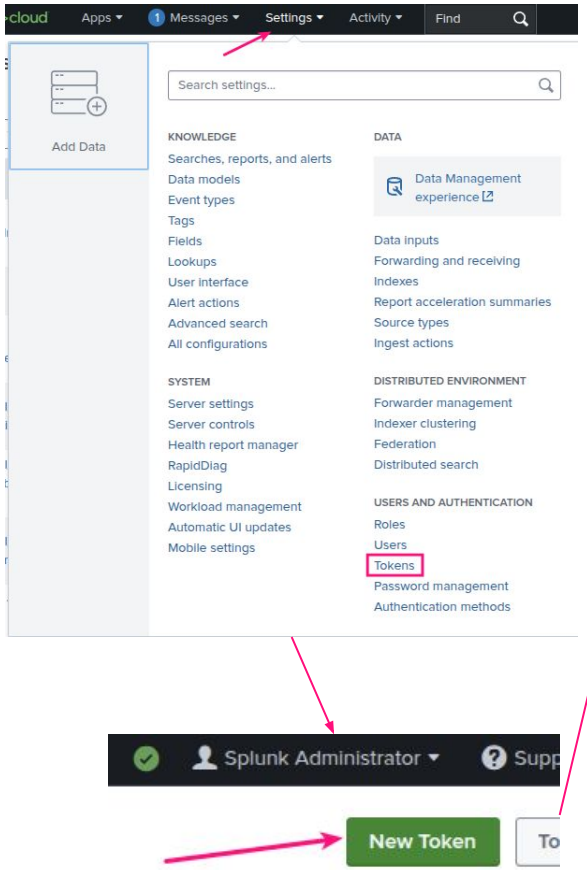


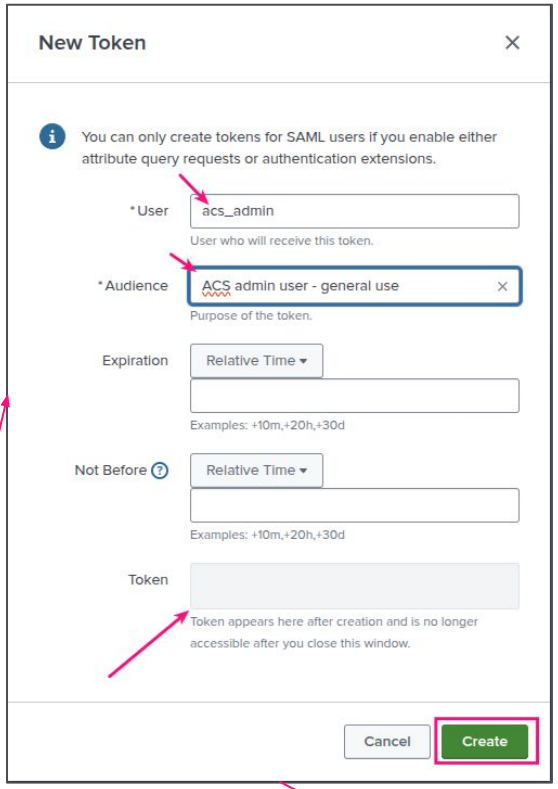
Create a user in Splunk Cloud GUI	https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/Addandeditusers#Create_a_user
Configure user for managing Splunk Cloud via ACS	https://docs.splunk.com/Documentation/SplunkCloud/9.3.2408/Config/ACSCLI#:~:text=and%20password%20values.-,Set%20login%20credentials,-Some%20ACS%20CLI

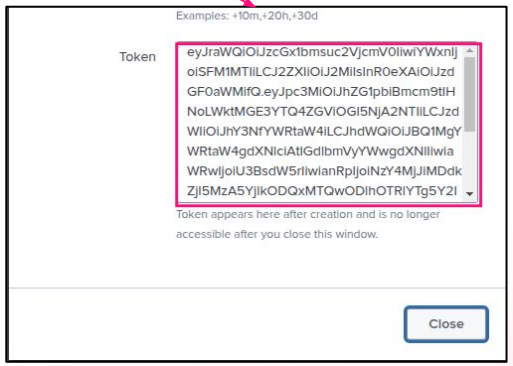
Configure ACS

Splunk Cloud: Token

- Access the Splunk Cloud GUI of your assigned instance
- Create a token for use by the ACS client
- Provide an audience to help understand why the token exists
- Be sure to capture the token before ‘close’ is clicked





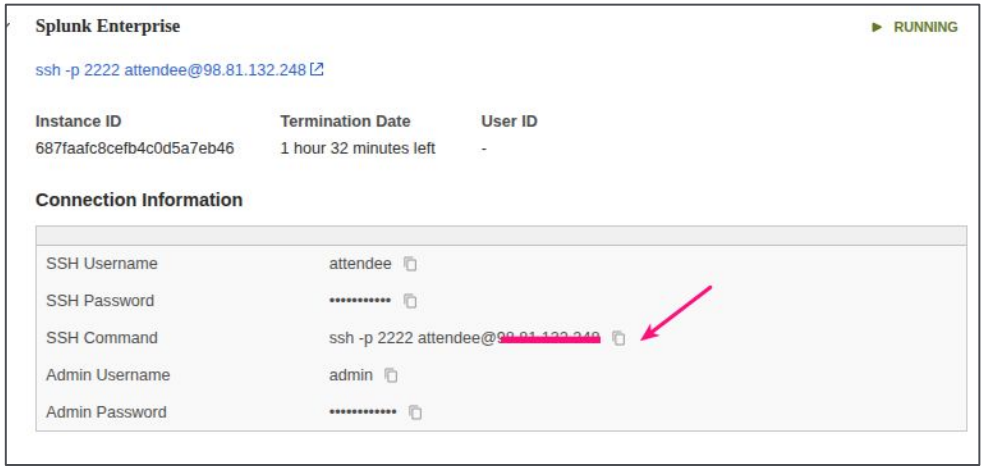


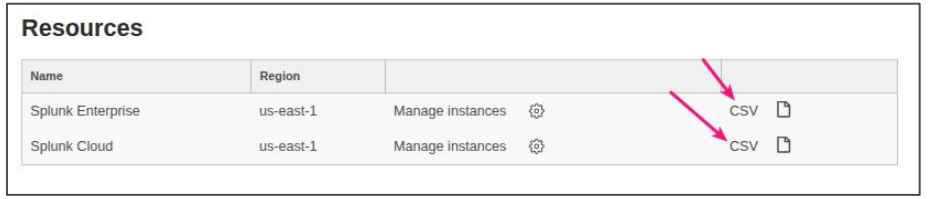
Create authentication tokens in the Splunk Cloud GUI	https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/CreateAuthTokens
Conifgure user for managing Splunk Cloud via ACS	https://docs.splunk.com/Documentation/SplunkCloud/9.3.2408/Config/ACSCLI#:~:text=and%20password%20values.-,Set%20login%20credentials,-Some%20ACS%20CLI

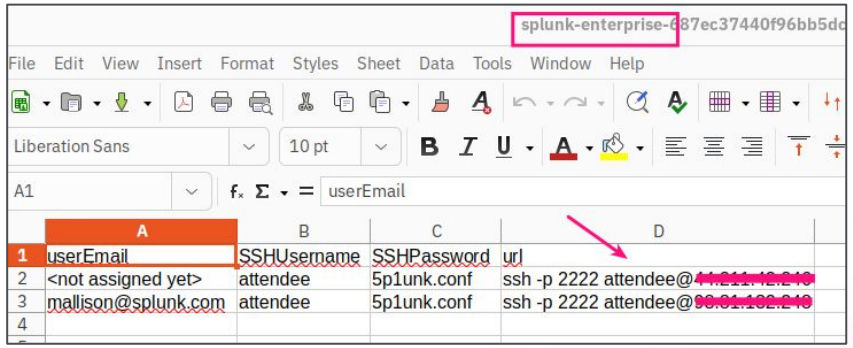
Configure ACS

Find your Cloud instances

- From the link sent out
- ‘Instances Information’
  ‘Splunk Enterprise dropdown
- Or ‘Resources’ CSV







Create a user in Splunk Cloud GUI	https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/Addandeditusers#Create_a_user
Configure user for managing Splunk Cloud via ACS	https://docs.splunk.com/Documentation/SplunkCloud/9.3.2408/Config/ACSCLI#:~:text=and%20password%20values.-,Set%20login%20credentials,-Some%20ACS%20CLI

Install and Configure ACS

Client

- All major OSes supported, Windows, MacOS, linux
- Tool called ‘acs’
- Hosted via homebrew
  - Requirements: git (nice to have - gcc, build-essential)
- Designed for MacOS, ported to linux (can be used in WSL)
- Native client for Windows available
- No GUI client on any OS

Administer Splunk Cloud Platform using the ACS CLI	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI
Homebrew on Linux	https://docs.brew.sh/Homebrew-on-Linux
Install Homebrew on linux (and MacOS)	https://brew.sh/

Install ACS in the lab

```
> brew update
> brew tap splunk/tap
> brew install acs
```

Lab 1

Splunk-built Client

- Labs use linux
- t3.micro AWS instance (smaller kept OOM'ing)
- Homebrew is a requirement
- Execute three steps to install ACS from homebrew (already setup)

- Requirements for homebrew
  - git
- Helps to have *gcc* and *build-essential*, but not specifically for homebrew

Install ACS onto a linux machine	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#:~:text=Install%20or%20upgrade%20on%20Mac%20or%20Linux

Configure ACS

Splunk-built client

```
> export SPLUNKCLOUD_STACK_NAME=<your_stack_here>
> acs config add-stack ${SPLUNKCLOUD_STACK_NAME}
> acs config use-stack ${SPLUNKCLOUD_STACK_NAME}
> acs login --token-user=acs_admin
```

Lab 1

- Execute three steps to configure for access to stack

```
attendee@ip-172-31-86-2:~$ export SPLUNKCLOUD_STACK_NAME="s4a-acs-02"
acs config add-stack ${SPLUNKCLOUD_STACK_NAME}
acs config use-stack ${SPLUNKCLOUD_STACK_NAME}
acs login --token-user=acs_admin

Stack added: s4a-acs-02, Type: victoria

Please run "acs config use-stack" to use this stack for further CLI operations.

current-stack is now set to s4a-acs-02

Please run "acs login" command to create and cache token to authenticate against ACS for further commands on this stack.
Enter Username: acs_admin
Enter Password:
Token successfully cached to authenticate against ACS for further operations
Populating stack type...
{
    "user": "acs_admin",
    "audience": "acs_admin",
    "id": "7e718b4018ac830572b435359a341e5084742bf30dac3d3c1bac249d10043105",
    "token": "eyJraWQiOiJzcbx1bmsuc2VjcmV0IiwiYWxnIjoiSFM1MTIiLCJ2ZXIiOiJ2MiIsInR0eXAiOiJzdGF0aWMifQ.eyJpc3MiOiJhY3NfYWRtaW4gA
nRpIjoiN2U3MThiNDAxOGFjODMwNTcyYjQzNTM1OWEzNDF1NTA4NDc0MmJmMzBkYWMzZDNjMWJhYzI0OWQxMDA0MzEwNSIsImlhdCI6MTczODEwNjA4MiwiZXhwIjo
ktUkMUHn3TNdFWLQ",
    "status": "enabled",
    "expiresOn": "2025-02-27T23:14:42Z",
    "notBefore": "2025-01-28T23:14:42Z"
}

attendee@ip-172-31-86-2:~$
```

Configure ACS to manage a Splunk Cloud stack	https://docs.splunk.com/Documentation/SplunkCloud/9.3.2408/Config/ACSCLI#:~:text=server%20override%20flag.-,Configure%20the%20ACS%20CLI,-Before%20you%20can

Help with ACS

Splunk-built client

- Help!

```
attendee@ip-172-31-86-240:~$ acs
API for managing splunk cloud stacks.
The Admin Config Service (ACS) is a cloud-native API that provides programmatic self-servi
ce administration capabilities for Splunk Cloud Platform.
Splunk Cloud Platform administrators can use the ACS API to perform common administrative
tasks without assistance from Splunk Support.
Example usage:
Begin by setting up and logging into an ACS stack:   "acs setup <stack-name>"
Alternatively, to perform these actions one at a time, begin by running the "acs config" c
ommand:
Add a stack to CLI config:                           "acs config add-stack <stack-name>"
Switch to using this stack for further operations:   "acs config use-stack <stack-name>"
Login to the stack to cache authentication info:     "acs login"
Run further commands for ACS APIs, for ex:           "acs token", "acs apps", etc

Exit Codes:
       1 - General Error
       2 - HTTP Request completed with unsuccessful return code.

Usage:
  acs [command]

Available Commands:
  apps                Manage apps
  capabilities        Manage capabilities
  completion          Generate the autocompletion script for the specified shell
  config              Configure the Admin Config Service CLI
  deployment          Manage task deployment
  hec-token           Manage HEC tokens
  help                Help about any command
```

```
> acs
```

‘acs’	Execute just the basic command for top-level help
Command error codes	Response codes to the execution of the ‘acs’ command, not the HTTP response code
Available sub-commands	The sub-commands that specify an action to be executed against the defined stack

- The sub-commands correlate to the available REST endpoints
- We will explore one, but each have unique and different requirements, and therefore different usage and parameters

Useful ACS assistance on the command line	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Run_ACS_CLI_operations

Help with ACS

```
> acs hec-token
```

Splunk-built client

- Help for a specific sub-command

```
attendee@ip-172-31-86-240:~$ acs hec-token
The HTTP Event Collector (HEC) lets you send data and application events to your Splunk
 deployment over HTTP protocol using token-based authentication.
You can use the Admin Config Service (ACS) CLI to create and manage HEC tokens for your
 Splunk Cloud Platform deployment programmatically.
The ACS CLI is available for HEC token management on Splunk Cloud Platform deployments
on Victoria Experience only.
If your Splunk Cloud Platform deployment is on Classic Experience, you can alternativel
y use Splunk Cloud Classic endpoints for HEC token management, please refer to Splunk d
ocumentation for more details.

To manage HEC tokens using the ACS API, you must:
- Have the sc_admin (Splunk Cloud Platform Administrator) role.
- Have Splunk Cloud Platform version 8.1.2101 or higher.

WARNING: It can take several seconds for HEC token CRUD requests to complete.

Usage:
  acs hec-token [command]

Available Commands:
  bulk-create Create HEC tokens in bulk
  bulk-delete Delete HEC tokens in bulk
  bulk-update Update HEC tokens in bulk
  create      Create a new HEC token
  delete      Delete a HEC token
  describe    Describe an individual HEC token
  list        List existing HEC tokens in your environment
  update      Update an existing HEC token

Flags:
  -h, --help   help for hec-token

Global Flags:
  -f, --format string   Controls the output format of the CLI.
                        The "pretty" format is optimized for interactive use.
                        The "structured" format is more parsable for automation. (defau
lt "pretty")
      --server string   Override server URL (default "https://staging.admin.splunk.com"
)
  -v, --verbose         Configures the client to print detailed messages. Extra message
s printed in verbose mode respect the current format setting.

Use "acs hec-token [command] --help" for more information about a command.
```

‘acs hec-token’	Help for the sub-command hec-token
Action commands for sub-command	The available actions for the hec-token subcommand
Formatting options	The output from each of the commands can be controlled and either use a “pretty” format that forms the JSON output in a people readable way, while the structured is for programmatic output without “prettyfying” strings such as “\n” that interrupt programmatic processing

Useful ACS assistance on the command line	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Run_ACS_CLI_operations

Help with ACS

```
> acs hec-token create --help
```

Splunk-built client

- Help for a specific sub-command

```
attendee@ip-172-31-86-240:~$ acs hec-token create --help
Create a new HEC token. You must specify a unique token name and a default index.
You can optionally specify an existing token.
You can also optionally specify the useACK option, as a boolean value (true/false), to
enable or disable indexer acknowledgement.
Splunk Cloud Platform currently supports indexer acknowledgement for Amazon Web Service
s (AWS) Kinesis Firehose only.
Make sure the specified default index exists on your system. Specifying an index that d
oes not exist can cause data loss.

Once the request completes successfully, ACS will reply with the new HEC token. Note th
at it can take several seconds for the token creation request to complete.

Usage:
  acs hec-token create [flags]

Flags:
      --name string                 HEC token name (required)
      --default-index string        default index
      --default-source string       default source
      --default-source-type string  default source type
      --disabled                    specify '--disabled=true to disable
      --default-host string         default host
      --token string                existing token
      --use-ack                     specify '--use-ack=true' to enable indexer acknowl
edgement
      --allowed-indexes strings     allowed indexes
  -h, --help                        help for create

Global Flags:
  -f, --format string   Controls the output format of the CLI.
                        The "pretty" format is optimized for interactive use.
                        The "structured" format is more parsable for automation. (defau
lt "pretty")
      --server string   Override server URL (default "https://staging.admin.splunk.com"
)
  -v, --verbose         Configures the client to print detailed messages. Extra message
s printed in verbose mode respect the current format setting.
```

‘acs hec-token create –help’	Help for the action command ‘create’ for hec-token
Configuration options for action command	Not all are required, but ‘name’ is. Some commands operate with defaults, some not. In this case, ‘hec-token create –name token-name’ just creates the token without any additional parameters.
Formatting options	The output from each of the commands can be controlled and either use a “pretty” format that forms the JSON output in a people readable way, while the structured is for programmatic output without “prettyfying” strings such as “\n” that interrupt programmatic processing

Useful ACS assistance on the command line	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Run_ACS_CLI_operations

Workshop Agenda

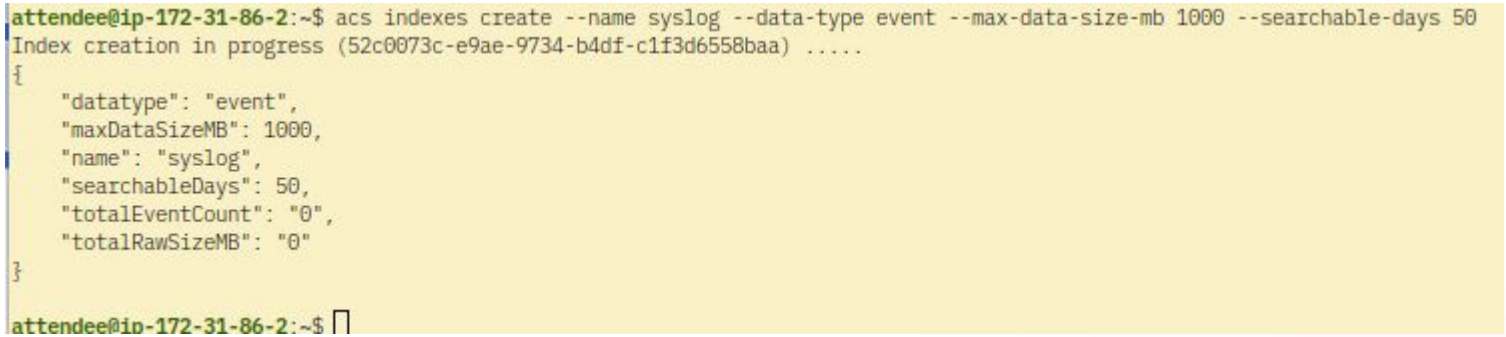
- Who?|What?|Why?
- Expectations
- What is Splunk Cloud Admin Config Service?
- How does Admin Config Service work?
- What capabilities does Admin Config Service provide?
- How is Admin Config Service different from the Splunk Cloud GUI?
- Setup - Lab[1]
  - Splunk Cloud instance
  - Admin Config Service (acs) tool
  - Curl
- Scripts
- Labs - 2 3 4 5 6 7 8 9
- Summary

Lab: Create indexes

```
> acs indexes create --name syslog
--data-type event
--max-data-size-mb 1000
--searchable-days 50
```

Splunk-built client

- Straightforward command - don't need to know the endpoint, just the service to be modified
- The relevant information regarding the index (name, type, size, searchable days, DDAA or DDSS)
- Index information (name=syslog, type=event, size=1000Mb, searchable days=50)



Manage indexes via ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Manage_indexes

Lab: Create indexes

```
> curl
'https://staging.admin.splunk.com/s4a-acs-02/ad
minconfig/v2/indexes' --header 'Authorization:
Bearer eyJr …' | jq
```

Lab 1

Curl

- Bare client
  - Requires all of the Splunk Cloud setup, including acquiring the user token
- Least footprint on a local machine, but requires the most knowledge

```
attendee@ip-172-31-86-240:~$ curl 'https://staging.admin.splunk.com/s4a-acs-02/adminconfig/v2/indexes'
 --header 'Authorization: Bearer eyJraWQiOiJzcGx1bmsuc2VjcmV0IiwiYWxnIjoiSFh…iLCJ2ZXIiOiJ2MiIsInR0e
XAiOiJzdGF0aWMifQ.eyJpc3MiO…ZG1pbiBmcm9tIHNoLWktMDVkNWUzODBiZDY3MTU0ODUiLCJzdWIiOiJhY3…RtaW4iLCJh
dWQiOiJVc2VyIHRvIHJ1biBBQ1MgcmVtb3RlIGNvbW1hbmRzIiwiaWRwIjoiU3BsdW5rIiwianRpIjoiODcxM2UyZGU0NzQ4MzQzN…
YwMGJiZGFlODQ4NDlmYmNjZTk3OGYxYWY1N2RkNjA4ZGE…NWVkYzIwMjU5ZjAyYSIsImlhdCI6MTczODM0ODEwNywiZXhwIjoxNzQw
OTQwMTA3LCJuYnIiOjE3MzgzNDgxMDd9.mdPa2CJDHV5xAc3MAn34…1xB6D2OcBitoIwsWDpwD5OaTaREr2pyTNVHUW00AfGxWHnM
-S9v_XOY_lS3xILIw' | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   619  100   619    0     0    190      0  0:00:03  0:00:03 --:--:--   190
[
  {
    "datatype": "event",
    "maxDataSizeMB": 0,
    "name": "history",
    "searchableDays": 7,
    "totalEventCount": "0",
    "totalRawSizeMB": "0"
  },
  {
    "datatype": "event",
    "maxDataSizeMB": 0,
    "name": "lastchanceindex",
    "searchableDays": 1095,
    "totalEventCount": "0",
    "totalRawSizeMB": "0"
  },
```

URL to ‘admin’ with stack in ‘URL’ with appropriate endpoint, here ‘indexes’	Using a non-production staging stack in our example and exercises. Normally omit ‘staging’.
The --header contains the token	Authorization token contained in the header. Must have ‘Authorization: Bearer ‘ prior to the token. Must finish with the closing single quote
Piped through ‘jq’ permits easier human reading, un-necessary for programmatic interaction	The commonly installed ‘jq’ permits pretty-printing. Usable here to make the output more readable

Manage indexes via ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Manage_indexes

Lab: Create IP Allow list

Splunk-built client

```
> acs ip-allowlist create search-api --subnets <your_admin_host_ip>/24
> acs ip-allowlist describe search-api
```

- Need to get appropriate external IP networks from networking
- Several different allow lists
  - search-api
  - hec
  - s3s
  - search-ui
  - idm-ui
  - idm-api

```
attendee@ip-172-31-86-2:~$ acs ip-allowlist create search-api --subnets 18.212.166.0/24
IP allow list subnets creation request submitted successfully for feature:search-api
Note that it can take several minutes for the subnet update to be applied to your Splunk Cloud Platform stack.
To verify the status of your stack after subnet update request, please run the "acs status current-stack" command.
{
    "warnings": [
        "IP allow list subnets creation request submitted successfully. Note that it can take several minutes for the subnet update to be applied to your Splunk Cloud Platform stack."
    ]
}
```

```
attendee@ip-172-31-86-2:~$ acs ip-allowlist describe search-api
{
    "subnets": [
        "[redacted]/24"
    ]
}
```

Manage IP Allow lists via ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Configure_IP_allow_lists

Lab: Manage HEC token

Splunk-built client

```
> acs hec-token create –name syslog_hec_sys01
> acs hec-token create –name syslog_hec_sys02
```

- Create and manage HEC tokens programmatically
- Allows constant and continuous rolling of HEC tokens
- Permits external organizations to manage their own

```
attendee@ip-172-31-82-162:~$ acs hec-token create --name syslog_hec_sys01
Hec creation in progress (efd01505-a2b8-94f3-a7eb-233dbe07e308) ...

{
    "http-event-collector": {
        "spec": {
            "allowedIndexes": null,
            "defaultHost": "",
            "defaultIndex": "",
            "defaultSource": "",
            "defaultSourcetype": "",
            "disabled": false,
            "name": "syslog_hec_sys01",
            "useAck": false
        },
        "token": "7F04BCBE-8EDE-4633-83D1-4844DF13F2EA"
    }
}
```

```
attendee@ip-172-31-82-162:~$ acs hec-token create --name syslog_hec_sys02
A deployment task is still in progress. Please try again later. Please refer https://docs.splunk
.com/Documentation/SplunkCloud/latest/Config/ACSerrormessages for general troubleshooting tips.
{
    "code": "424-dependency-incomplete",
    "message": "A deployment task is still in progress. Please try again later. Please refer htt
ps://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSerrormessages for general troubl
eshooting tips."
}

Error: Create hec token failed: POST request to "https://staging.admin.splunk.com/s4a-acs-02/adm
inconfig/v2/inputs/http-event-collectors" failed, code: 424 Failed Dependency
```

```
attendee@ip-172-31-82-162:~$ acs hec-token create --name syslog_hec_sys02
Hec creation in progress (03a70b9b-11e7-9eff-a5cb-edfcf11d749a) ...

{
    "http-event-collector": {
        "spec": {
            "allowedIndexes": null,
            "defaultHost": "",
            "defaultIndex": "",
            "defaultSource": "",
            "defaultSourcetype": "",
            "disabled": false,
            "name": "syslog_hec_sys02",
            "useAck": false
        },
        "token": "2814263D-55F5-414A-B22B-17F4EAC6C716"
```

Manage HEC tokens using ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Manage_HTTP_Event_Collector_.28HEC.29_tokens

Lab: Manage HEC token

```
> acs hec-token bulk-create –file
./addtional_syslog_tokens.json
```

Lab 5

Splunk-built client

- Bulk creation of HEC tokens

Basic install, just the name
Somewhat more complicated, including a default index
More complicated, with the ‘allowedIndexes’ including multiple allowed indexes in a JSON array
Showing multiple possible additions, a fail …

- In bulk creation, the token is not part of the default output
- Must be retrieved via a ‘hec-token describe’ call

Manage HEC tokens in bulk using ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Create_HEC_tokens_in_bulk

Lab: Manage HEC token

```
> acs hec-token bulk-create –file
./addtional_syslog_tokens.json
```

Lab 5

Splunk-built client

- Bulk creation of HEC tokens

```
attendee@ip-172-31-82-162:~$ acs hec-token bulk-create --file ./additional_syslog_tokens.json

HEC creation (syslog_token_sys01) in progress (e6b7510b-5296-97be-bb02-93ed7ee3ed00) ...
{
    "identifier": "syslog_token_sys01",
    "requestID": "e6b7510b-5296-97be-bb02-93ed7ee3ed00",
    "statusCode": 202,
    "message": "Token creation request submitted successfully. Note that it can take several minutes for the token creation to be applied to your Splunk Clou
d Platform stack.",
    "response": "{\"http-event-collector\":{\"spec\":{\"name\":\"syslog_token_sys01\"}}}\n",
    "content-type": "application/json; charset=UTF-8"
}
HEC creation (syslog_token_sys02) in progress (d5d00965-abbc-959e-8f51-8cc9bffd765d) ...
{
    "identifier": "syslog_token_sys02",
    "requestID": "d5d00965-abbc-959e-8f51-8cc9bffd765d",
    "statusCode": 202,
    "message": "Token creation request submitted successfully. Note that it can take several minutes for the token creation to be applied to your Splunk Clou
d Platform stack.",
    "response": "{\"http-event-collector\":{\"spec\":{\"name\":\"syslog_token_sys02\"}}}\n",
    "content-type": "application/json; charset=UTF-8"
}
HEC creation (syslog_token_sys03) in progress (ae1b3379-39f3-9e01-8f84-d85fae5ab9f2) ...
{
    "identifier": "syslog_token_sys03",
    "requestID": "ae1b3379-39f3-9e01-8f84-d85fae5ab9f2",
    "statusCode": 202,
    "message": "Token creation request submitted successfully. Note that it can take several minutes for the token creation to be applied to your Splunk Clou
d Platform stack.",
    "response": "{\"http-event-collector\":{\"spec\":{\"name\":\"syslog_token_sys03\"}}}\n",
    "content-type": "application/json; charset=UTF-8"
}
HEC creation (syslog_token_sys04) failed (e3e3d909-d33b-9252-b9d9-ef76ba919255) ...
{
    "identifier": "syslog_token_sys04",
    "requestID": "e3e3d909-d33b-9252-b9d9-ef76ba919255",
    "statusCode": 400,
    "message": "syslog_finance in allowedIndexes is an internal index or is not a valid index. Please refer https://docs.splunk.com/Documentation/SplunkCloud
/latest/Config/ACSerrormessages for general troubleshooting tips.",
    "response": "{\"code\":\"400-bad-request\",\"message\":\"syslog_finance in allowedIndexes is an internal index or is not a valid index. Please refer http
s://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSerrormessages for general troubleshooting tips.\"}\n",
    "content-type": "application/json; charset=UTF-8"
}
Bulk Creation Results (success=3, failures=1, skipped=0)
Report for hec_bulk_create is saved at: /home/attendee/.acs/reports/s4a-acs-02/hec_bulk_create_1738198899.json
Error: Bulk create HEC token failed: POST request to "https://staging.admin.splunk.com/s4a-acs-02/adminconfig/v2/inputs/http-event-collectors" failed, code:
400 Bad Request
```

Basic install, just the name	Success!
Somewhat more complicated, including a default index	Success!
More complicated, with the ‘allowedIndexes’ including multiple allowed indexes in a JSON array	Success!
Showing multiple possible additions, a fail …	FAIL, why? The index doesn’t exit!

Manage HEC tokens in bulk using ACS https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Create_HEC_tokens_in_bulk

Lab: Manage HEC token

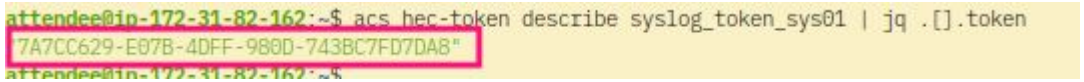
```
> acs hec-token describe
syslog_token_sys01
> acs hec-token describe
syslog_token_sys01 | jq
.[].token
```

Lab 5

Splunk-built client

- Bulk creation of HEC tokens

- Use ‘describe’ to extract the actual token contents
- The shell command ‘jq’ is available on nearly all of the production distributions
- Capture the token output for integration into other commands



Manage HEC tokens in bulk using ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Create_HEC_tokens_in_bulk
JSON on the command line with jq	https://shapeshed.com/jq-json/

Workshop Agenda

- Who?|What?|Why?
- Expectations
- What is Splunk Cloud Admin Config Service?
- How does Admin Config Service work?
- What capabilities does Admin Config Service provide?
- How is Admin Config Service different from the Splunk Cloud GUI?
- Setup - Lab[1]
  - Splunk Cloud instance
  - Admin Config Service (acs) tool
  - Curl
- Scripts
- Labs - 2 3 4 5 6 7 8 9
- Summary

Lab: Manage Roles

Splunk-built client

```
> acs roles create --name "index-syslog"
--srch-indexes-allowed "syslog"
> acs roles create --name "index-syslog"
--srch-indexes-allowed "syslog1"
```

- Create a role

```
attendee@ip-172-31-86-240:~$ acs roles create --name "index-syslog" --srch-indexes-allowed "syslog"
{
    "cumulativeRTSrchJobsQuota": 100,
    "cumulativeSrchJobsQuota": 50,
    "defaultApp": "",
    "imported": {
        "capabilities": [],
        "rtSrchJobsQuota": 0,
        "srchDiskQuota": 0,
        "srchFilter": "",
        "srchIndexesAllowed": [],
        "srchIndexesDefault": [],
        "srchJobsQuota": 0,
        "srchTimeEarliest": -1,
        "srchTimeWin": -1,
        "roles": []
    },
    "name": "index-syslog"
    "capabilities": [],
    "rtSrchJobsQuota": 6,
    "srchDiskQuota": 100,
    "srchFilter": "",
    "srchIndexesAllowed": [
        "syslog"
    ],
    "srchIndexesDefault": [],
    "srchJobsQuota": 3,
    "srchTimeEarliest": -1,
    "srchTimeWin": -1
}
```

- Create a role to access a specific index (syslog)
- Will generate errors if a resource (index) is unavailable, so watch for >400 in the response

```
attendee@ip-172-31-86-240:~$ acs roles create --name "index-syslog1" --srch-indexes-allowed "syslog1"
cannot set index name 'syslog1': index does not exist. Please refer https://docs.splunk.com/Documentatio
n/SplunkCloud/latest/Config/ACSerrormessages for general troubleshooting tips.
{
    "code": "400-bad-request"
    "message": "cannot set index name 'syslog1': index does not exist. Please refer https://docs.splunk.
com/Documentation/SplunkCloud/latest/Config/ACSerrormessages for general troubleshooting tips."
}

Error: Create role failed: POST request to "https://staging.admin.splunk.com/s4a-acs-02/adminconfig/v2/r
oles" failed, code: 400 Bad Request
```

Useful ACS assistance on the command line	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Run_ACS_CLI_operations
Manage users, roles, and capabilities in Splunk Cloud Platform	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ManageRoles

Lab: Manage Roles

Splunk-built client

```
> acs roles update index-syslog
--srch-indexes-allowed wineventlog
```

- Update a role

```
attendee@ip-172-31-86-240:~$ acs roles update index-syslog
--srch-indexes-allowed wineventlog

{
    "cumulativeRTSrchJobsQuota": 100,
    "cumulativeSrchJobsQuota": 50,
    "defaultApp": "",
    "imported": {
        "capabilities": [],
        "rtSrchJobsQuota": 0,
        "srchDiskQuota": 0,
        "srchFilter": "",
        "srchIndexesAllowed": [],
        "srchIndexesDefault": [],
        "srchJobsQuota": 0,
        "srchTimeEarliest": -1,
        "srchTimeWin": -1,
        "roles": []
    },
    "name": "index-syslog",
    "capabilities": [],
    "rtSrchJobsQuota": 6,
    "srchDiskQuota": 100,
    "srchFilter": "",
    "srchIndexesAllowed": [
        "wineventlog"
    ],
    "srchIndexesDefault": [],
    "srchJobsQuota": 3,
    "srchTimeEarliest": -1,
    "srchTimeWin": -1
}
```

- Modify a role (index-syslog) to access a specific index (winventlog)
- Note what happened. The srchIndexesAllowed was over-written entirely. The list needs to be complete, it is not an add but a replace.

```
attendee@ip-172-31-86-240:~$ acs roles describe index-syslog
{
    "cumulativeRTSrchJobsQuota": 100,
    "cumulativeSrchJobsQuota": 50,
    "defaultApp": "",
    "imported": {
        "capabilities": [],
        "rtSrchJobsQuota": 0,
        "srchDiskQuota": 0,
        "srchFilter": "",
        "srchIndexesAllowed": [],
        "srchIndexesDefault": [],
        "srchJobsQuota": 0,
        "srchTimeEarliest": -1,
        "srchTimeWin": -1,
        "roles": []
    },
    "name": "index-syslog",
    "capabilities": [],
    "rtSrchJobsQuota": 6,
    "srchDiskQuota": 100,
    "srchFilter": "",
    "srchIndexesAllowed": [
        "wineventlog"
    ],
    "srchIndexesDefault": [],
    "srchJobsQuota": 3,
    "srchTimeEarliest": -1,
    "srchTimeWin": -1
}
```

```
attendee@ip-172-31-86-240:~$ acs roles update index-syslog
 --srch-indexes-allowed "wineventlog,syslog"
{
    "cumulativeRTSrchJobsQuota": 100,
    "cumulativeSrchJobsQuota": 50,
    "defaultApp": "",
    "imported": {
        "capabilities": [],
        "rtSrchJobsQuota": 0,
        "srchDiskQuota": 0,
        "srchFilter": "",
        "srchIndexesAllowed": [],
        "srchIndexesDefault": [],
        "srchJobsQuota": 0,
        "srchTimeEarliest": -1,
        "srchTimeWin": -1,
        "roles": []
    },
    "name": "index-syslog",
    "capabilities": [],
    "rtSrchJobsQuota": 6,
    "srchDiskQuota": 100,
    "srchFilter": "",
    "srchIndexesAllowed": [
        "syslog",
        "wineventlog"
    ],
    "srchIndexesDefault": [],
    "srchJobsQuota": 3,
    "srchTimeEarliest": -1,
    "srchTimeWin": -1
}
```

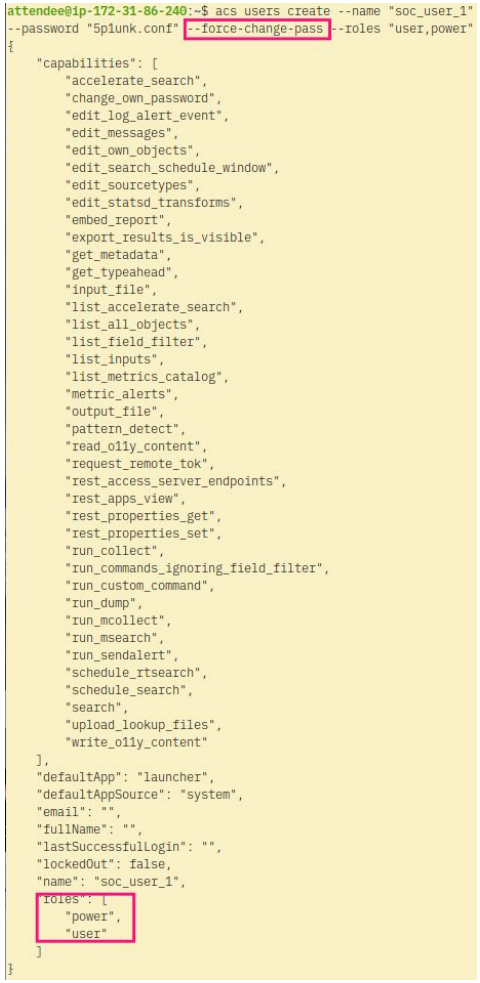
Useful ACS assistance on the command line	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Run_ACS_CLI_operations
Manage users, roles, and capabilities in Splunk Cloud Platform	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ManageRoles

Lab: Manage Users

Splunk-built client

- Create a user

```
> acs users create --name
"soc_user_1" –force-change-pass
--password "5p1unk.conf" --roles
"user,power"
```



- Create a user (soc_user_1), with the Workshop standard password, with otherwise default settings for capabilities, and the two roles “user” and “power” assigned
- Default behavior is to not force a password change, but the command line option --force-change-pass sets this bit to ensure a change at first login

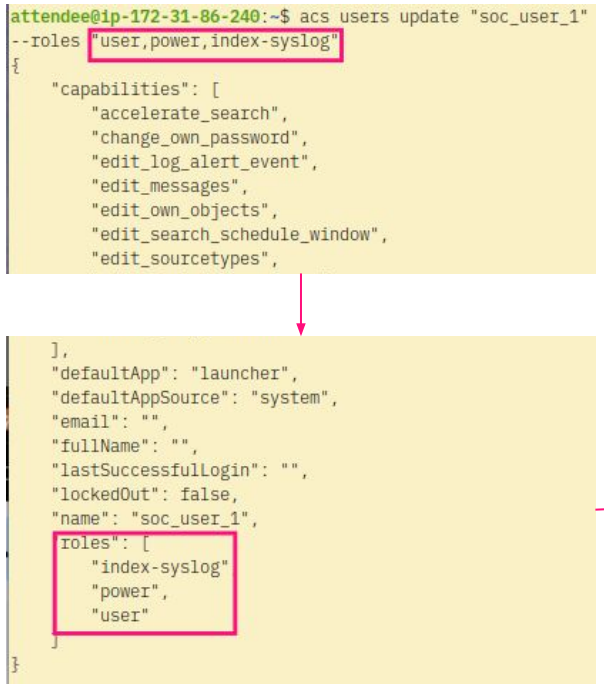
Useful ACS assistance on the command line	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Run_ACS_CLI_operations
Manage users, roles, and capabilities in Splunk Cloud Platform	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ManageRoles

Lab: Manage Users

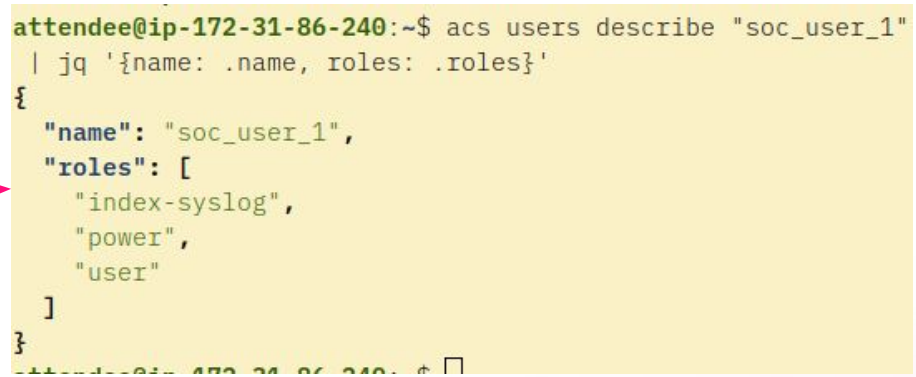
Splunk-built client

- Update a user

```
> acs users update "soc_user_1"
--password "5p1unk.conf"
–force-change-pass --roles "user,power"
> acs users describe "soc_user_1" | jq
'{name: .name, roles: .roles}'
```



- Modify a user (soc_user_1) to add another role (index-syslog, with both ‘syslog’ and ‘wineventlog’ as the accessible indexes)
- Be sure to define the entire string, this isn’t an “add” this is aways complete redefine



Useful ACS assistance on the command line	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Run_ACS_CLI_operations
Manage users, roles, and capabilities in Splunk Cloud Platform	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ManageRoles
JSON on the command line with jq	https://shapeshed.com/jq-json/

Lab: Add App - private

Splunk-built client

- Add a private app

```
attendee@ip-172-31-86-240:~$ acs apps install private --app-package SA_hywels_dashboards222.tar.g
z --acs-legal-ack=Y
Authenticating with the Splunk API service using your splunk.com credentials.
Enter Username: [redacted]
Enter Password:
Successfully authenticated user and assigned a token
Inspecting your private app...
Submitted app for inspection (requestId='92aadfb3-531b-4c01-82d1-7755238a1437')
Waiting for inspection to finish...
processing.....success
Vetting completed, summary:
{
    "error": 0,
    "failure": 0,
    "skipped": 1,
    "manual_check": 0,
    "not_applicable": 117,
    "warning": 1,
    "success": 77
}
Vetting successful
Installing the app...
{
    "label": "Hywels Dashboards",
    "name": "SA_hywels_dashboards",
    "package": "SA_hywels_dashboards-2.2.2.tar.gz",
    "status": "installed",
    "version": "2.2.2"
}
```

```
> acs apps install private
--app-package
SA_hywels_dashboards222.tar.gz
--acs-legal-ack=Y
```

Lab 8

- Add a private app
- All apps installed into a Splunk Cloud app MUST be vetted
- During the process of installation, a valid Splunk.com login is required
- Note the “processing.....success” is the submission to the vetting process, not the success of the vetting
- For Victoria experience stacks, the apps must be installed on each separate search head

Manage private apps using ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Manage_private_apps
Manage private apps in Splunk Cloud Platform with ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ManageApps

Lab: Add App - private

Splunk-built client

```
> acs apps install private
--acs-legal-ack=Y
--app-package
SC_Fail_SA_hywels_dashboards222
.tar.gz --acs-legal-ack=Y
```

- Add a private app - with a fail …

```
attendee@ip-172-31-86-240:~$ acs apps install private --acs-legal-ack=Y  --app-package
SC_Fail_SA_hywels_dashboards222.tar.gz
Authenticating with the Splunk API service using your splunk.com credentials.
Enter Username: [redacted]
Enter Password:
Successfully authenticated user and assigned a token
Inspecting your private app...
Submitted app for inspection (requestId='a437e856-4c36-4c77-8a70-02f26cfdfca7')
Waiting for inspection to finish...
processing......success
Vetting completed, summary:
{
    "error": 0,
    "failure": 0,
    "skipped": 0,
    "manual_check": 0,
    "not_applicable": 117,
    "warning": 2,
    "success": 77
}
Vetting successful
Installing the app...
This app has failed AppInspect validation. Fix the issues in the report, and retry AppI
nspect validation. Please refer https://docs.splunk.com/Documentation/SplunkCloud/lates
t/Config/ACSerrormessages for general troubleshooting tips.
{
    "code": "400-bad-request",
    "message": "This app has failed AppInspect validation. Fix the issues in the report
, and retry AppInspect validation. Please refer https://docs.splunk.com/Documentation/S
plunkCloud/latest/Config/ACSerrormessages for general troubleshooting tips."
}

Error: Install App failed: POST request to "https://staging.admin.splunk.com/s4a-acs-02
/adminconfig/v2/apps" failed, code: 400 Bad Request
```

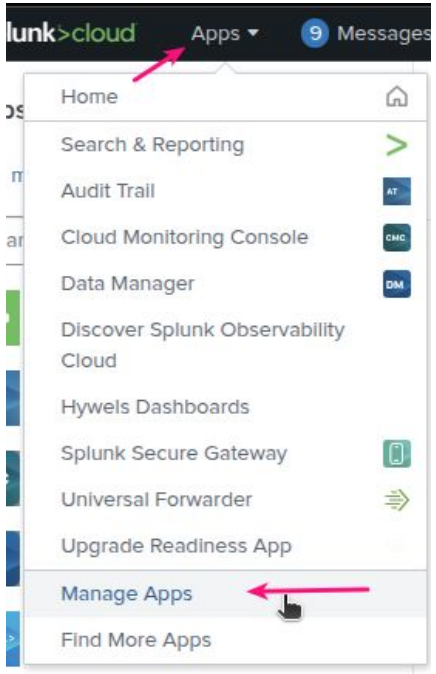
- Confusingly, says ‘processing……success’
- … however the vetting failed, see the return code - 400.
- Have to go out to the stack to determine what happened
- Be aware that older versions of the Splunk Cloud stacks only support up to 30 apps

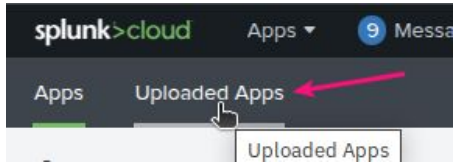
Manage private apps using ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Manage_private_apps
Manage private apps in Splunk Cloud Platform with ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ManageApps

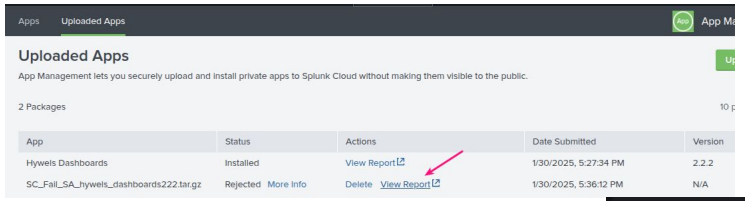
Lab: Add App - private

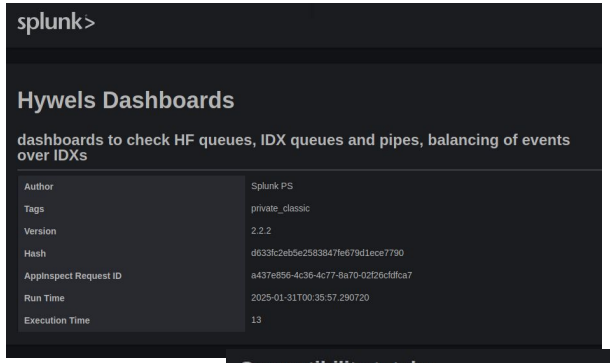
Splunk-built client

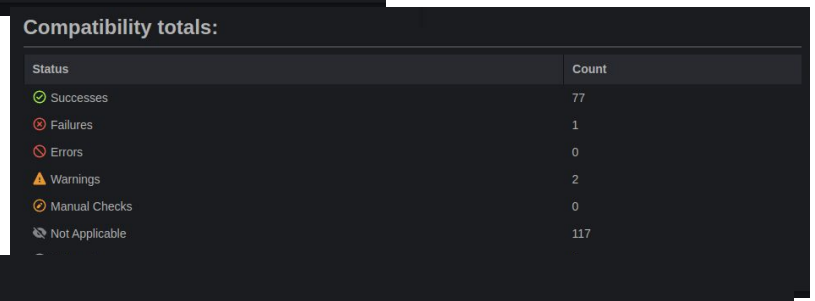
- Add a private app - with a fail …

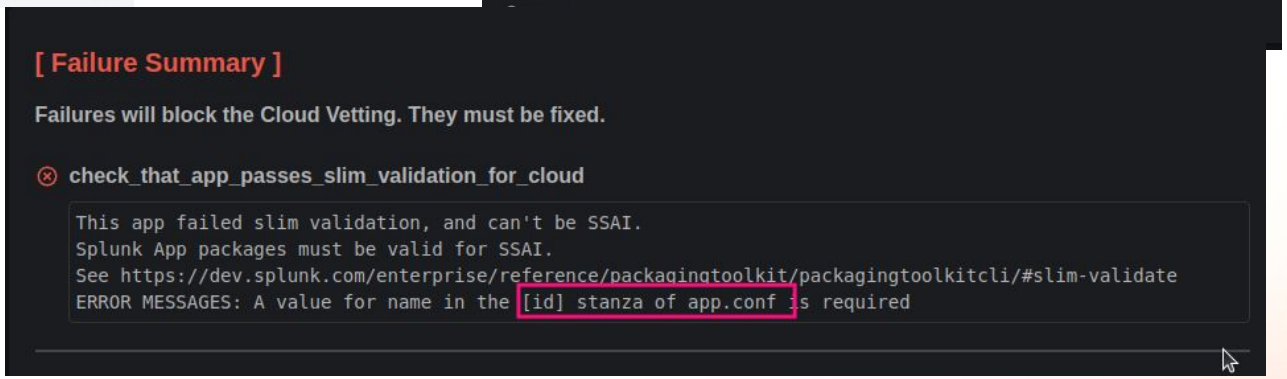












Manage private apps using ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Manage_private_apps
Manage private apps in Splunk Cloud Platform with ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ManageApps
Manage private apps on your Splunk Cloud Platform deployment	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/PrivateApps

Workshop Agenda

- Who?|What?|Why?
- Expectations
- What is Splunk Cloud Admin Config Service?
- How does Admin Config Service work?
- What capabilities does Admin Config Service provide?
- How is Admin Config Service different from the Splunk Cloud GUI?
- Setup - Lab[1]
  - Splunk Cloud instance
  - Admin Config Service (acs) tool
  - Curl
- Scripts
- Labs - 2 3 4 5 6 7 8 9
- Summary

Lab: Add App - Splunkbase

Splunk-built client

```
> acs apps install splunkbase
--splunkbase-id 833
```

- Add a Splunkbase app

```
attendee@ip-172-31-86-240:~$ acs apps install splunkbase --splunkbase-id 833
Authenticating with the Splunk API service using your splunk.com credentials.
Enter Username: [redacted]
Enter Password:
Retrieving license for Splunkbase app: 833

URL of the third-party license for the app to acknowledge your acceptance of any risks:
https://www.splunk.com/en_us/legal/splunk-general-terms.html
Enter 'Y' to accept: Y

Installing the app...
App installation in progress (8e2d8fa1-eb0f-922a-a885-7abc1a431962)....
App install succeeded
{
    "appID": "Splunk_TA_nix",
    "label": "Splunk Add-on for Unix and Linux",
    "name": "Splunk_TA_nix",
    "package": "",
    "splunkbaseID": "833",
    "stateChangeRequiresRestart": false,
    "status": "installed",
    "version": "9.2.0"
}
```

- Must use a valid Splunk.com login
- Must understand the numbering convention. Find the app in Splunkbase, the URL includes the ID
- Must provide the license URL one way or another and then accept (or deny)
- Output provides feedback
- Error, similar to the other commands, provides a “400”
- For Victoria experience stacks, the apps must be installed on each separate search head

Manage Splunkbase app using ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Manage_Splunkbase_apps
Manage Splunkbase app using ACS API	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ManageSplunkbaseApps
Splunk Add-on for Unix and Linux	https://splunkbase.splunk.com/app/833

Summary

Splunk Admin Config Service

- A way for customers to provide many self-service actions that otherwise would require interaction with Splunk Cloud support
- Provides a REST endpoint that can be accessed via any tool that can hit an endpoint (curl, podman, the ‘acs’ tool Splunk has provided
- Provides access to many services that are unavailable in Splunk Cloud GUI but in ACS, some not in ACS but in the GUI
- Provides GIT tracking
- The exercises provided examples for many actions, but many more are available, use Splunk docs and

Links

About the Admin Config Service (ACS) API	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSIntro
What is REST?	https://restfulapi.net/
Admin Config Service (ACS) API endpoint reference	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSREF
Configure authentication extensions to interface with your SAML identity provider	https://docs.splunk.com/Documentation/Splunk/latest/Security/ConfigureauthextensionsforSAMLtokens
Manage ACS API access with capabilities	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/RBAC#Manage_ACS_endpoint_access_with_capabilities
About the Admin Config Service (ACS) API	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSIntro
What is REST?	https://restfulapi.net/
Admin Config Service (ACS) API endpoint reference	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSREF
Basic setup and usage concepts for the Admin Config Service (ACS) API	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSusage
Introduction to the Splunk ACS Github Action CI/CD Starter	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Introduction_to_the_Splunk_ACS_Github_Action_CI%2F%2FCD_Starter
Administer Your Splunk Cloud Stacks Easily and Efficiently with ACS Helper for Splunk	Introduction to the Splunk ACS Github Action CI/CD Starter
Start Managing Your Deployment with Splunk Cloud's Admin Configuration Service (ACS)	https://community.splunk.com/t5/Splunk-Tech-Talks/Start-Managing-Your-Deployment-with-Splunk-Cloud-s-Admin/ba-p/599981
Creating allows lists with the Splunk Cloud Platform Admin Configuration Service (ACS) API	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Creating_allows_lists_with_the_Splunk_Cloud_Platform_Admin_Configuration_Service_API
Using Admin Config Service (ACS) in Splunk Cloud Platform FedRAMP environments	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Using_Admin_Config_Service_(ACS)_in_Splunk_Cloud_Platform_FedRAMP_environments#
Configure user for managing Splunk Cloud via ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#:~:text=and%20password%20values.-,Set%20login%20credentials,-Some%20ACS%20CLI
Create authentication tokens (Splunk Cloud)	https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/CreateAuthTokens

Administer Splunk Cloud Platform using the ACS CLI	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI
Homebrew on Linux	https://docs.brew.sh/Homebrew-on-Linux
Install Homebrew on linux (and MacOS)	https://brew.sh/
Install ACS onto a linux machine	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#:~:text=Install%20or%20upgrade%20on%20Mac%20or%20Linux
Configure ACS to manage a Splunk Cloud stack	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#:~:text=server%20override%20flag.-,Configure%20the%20ACS%20CLI,-Before%20you%20can
Useful ACS assistance on the command line	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Run_ACS_CLI_operations
Manage indexes via ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Manage_indexes
Manage IP Allow lists via ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Configure_IP_allow_lists
Manage HEC tokens using ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Manage_HTTP_Event_Collector_.28HEC.29_tokens
Manage HEC tokens in bulk using ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Create_HEC_tokens_in_bulk
JSON on the command line with jq	https://shapeshed.com/jq-json/
Manage users, roles, and capabilities in Splunk Cloud Platform	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ManageRoles
Manage private apps using ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ACSCLI#Manage_private_apps
Manage private apps in Splunk Cloud Platform with ACS	https://docs.splunk.com/Documentation/SplunkCloud/latest/Config/ManageApps
Create a user in Splunk Cloud GUI	https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/Addandeditusers#Create_a_user

Thank you

splunk> a CISCO company