Splunk Enterprise System Administration

Document Usage Guidelines

- Should be used only for enrolled students
- Not meant to be a self-paced document, an instructor is needed
- Do not distribute

Course Prerequisites

- Required:
  - Splunk Fundamentals 1
- Strongly recommended:
  - Splunk Fundamentals 2

Course Goals

- Identify Splunk components and understand the basics of a Splunk deployment
- Monitor Splunk operations and licensing
- Install a Splunk app
- Understand Splunk configuration files
- Create and manage Splunk indexes
- Create users and roles in Splunk
- Introduce distributed search

Course Outline

Module 1: Splunk Server Deployment

Module 2: Splunk Server Monitoring

Module 3: Splunk Apps

Module 4: Splunk Configuration Files

Module 5: Splunk Indexes

Module 6: Splunk Index Management

Module 7: Splunk User Management

Module 8: Configuring Basic Forwarding

Module 9: Distributed Search

System Administrator versus Data Administrator

Splunk System Administrator

System Management

- Install, configure, and manage Splunk components
- Install and manage Splunk apps
- Monitor Splunk operations
- Manage Splunk licensing
- Manage Splunk indexes
- Manage Splunk users and authentication
- Manage Splunk configuration files
- Monitor MC and respond to system health alerts

Splunk Data Administrator

Data Onboarding and Management

- Work with users requesting new data sources
- Document existing and newly ingested data sources
- Design and manage inputs for UFs/HFs to capture data
- Manage parsing, event line breaking, timestamp extraction
- Move configuration through non-production testing as required
- Deploy changes to production
- Manage Splunk configuration files

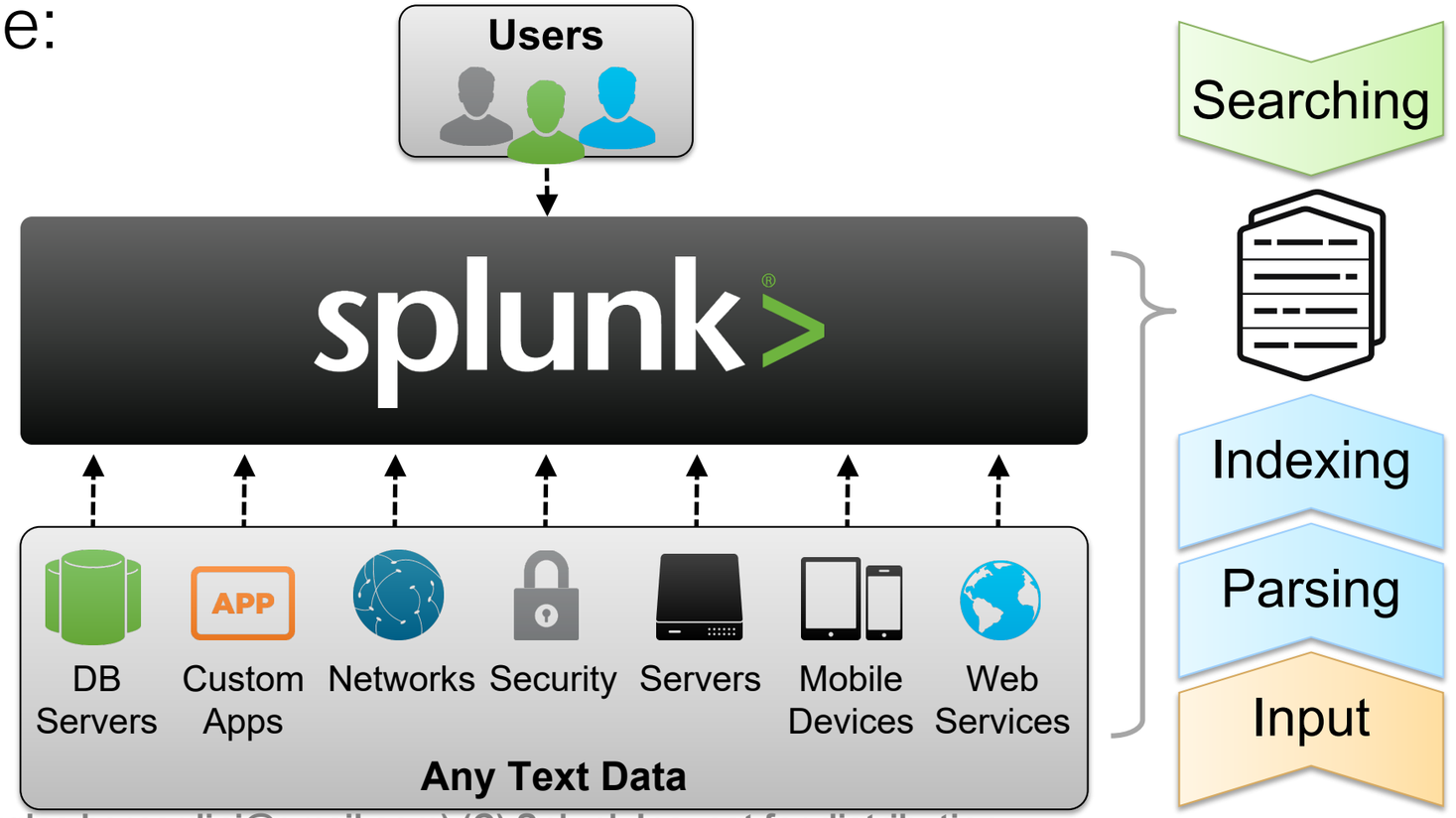
Module 1:
Splunk Server Deployment

Module Objectives

- Provide an overview of Splunk
- Identify Splunk Enterprise components
- Identify the types of Splunk deployments
- List the steps to install Splunk
- Use Splunk CLI commands

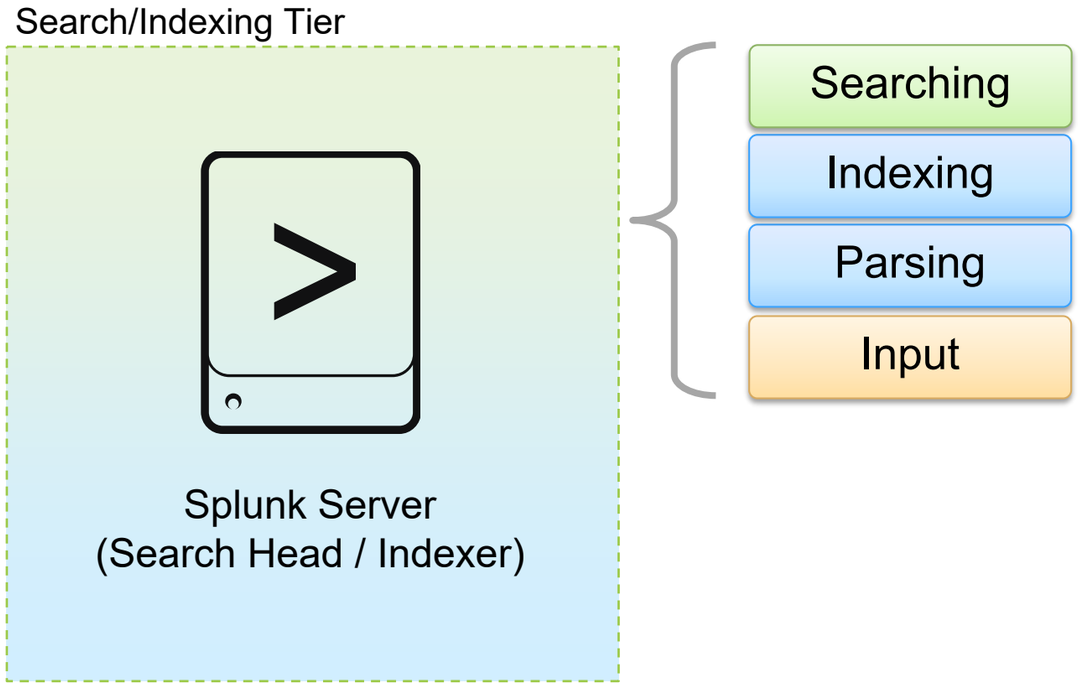
Splunk Overview

- Splunk can be deployed in a variety of configurations
- Scales from a single server to a distributed infrastructure
- Four stages of Splunk include:
  - **Input** any text data
  - **Parse** the data into events
  - **Index** and store events
  - **Search** and report



Simple Test Server

- Deploying a single, standalone server
  - All functions in a single Splunk instance
  - The result when you download and install Splunk with default settings
- Recommended use:
  - For testing, proof of concept, personal use, and learning
  - Consider having at least one test / development setup at your site

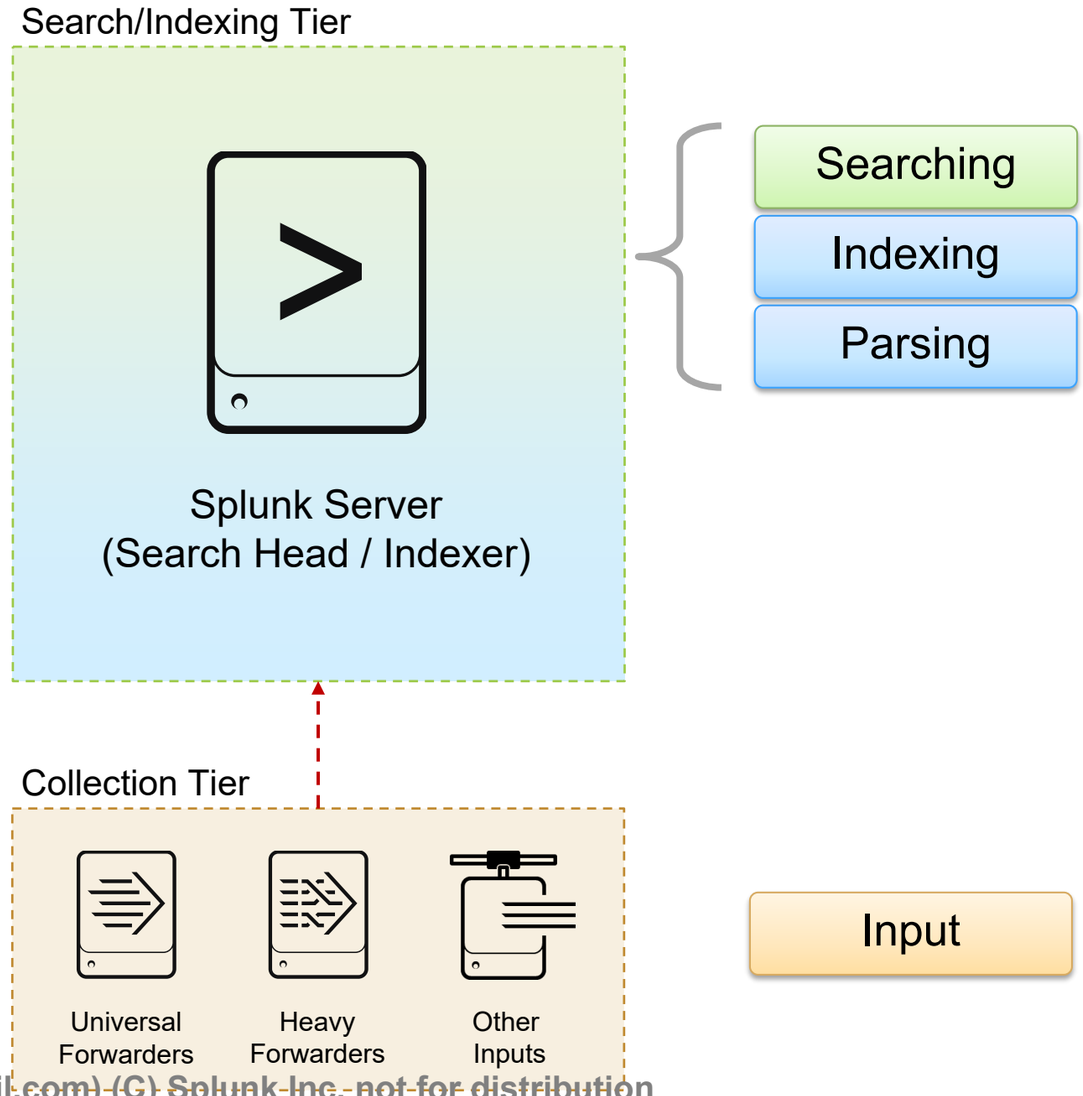


Note

This is the initial configuration in class.

Single Server With Inputs

- Deploying a basic Splunk server
  - Similar to standalone configuration
  - Manage deployment of forwarder configurations
- Deploying Forwarders
  - Install Splunk forwarder at data source (usually production servers)
  - Collect data and send it to Splunk servers

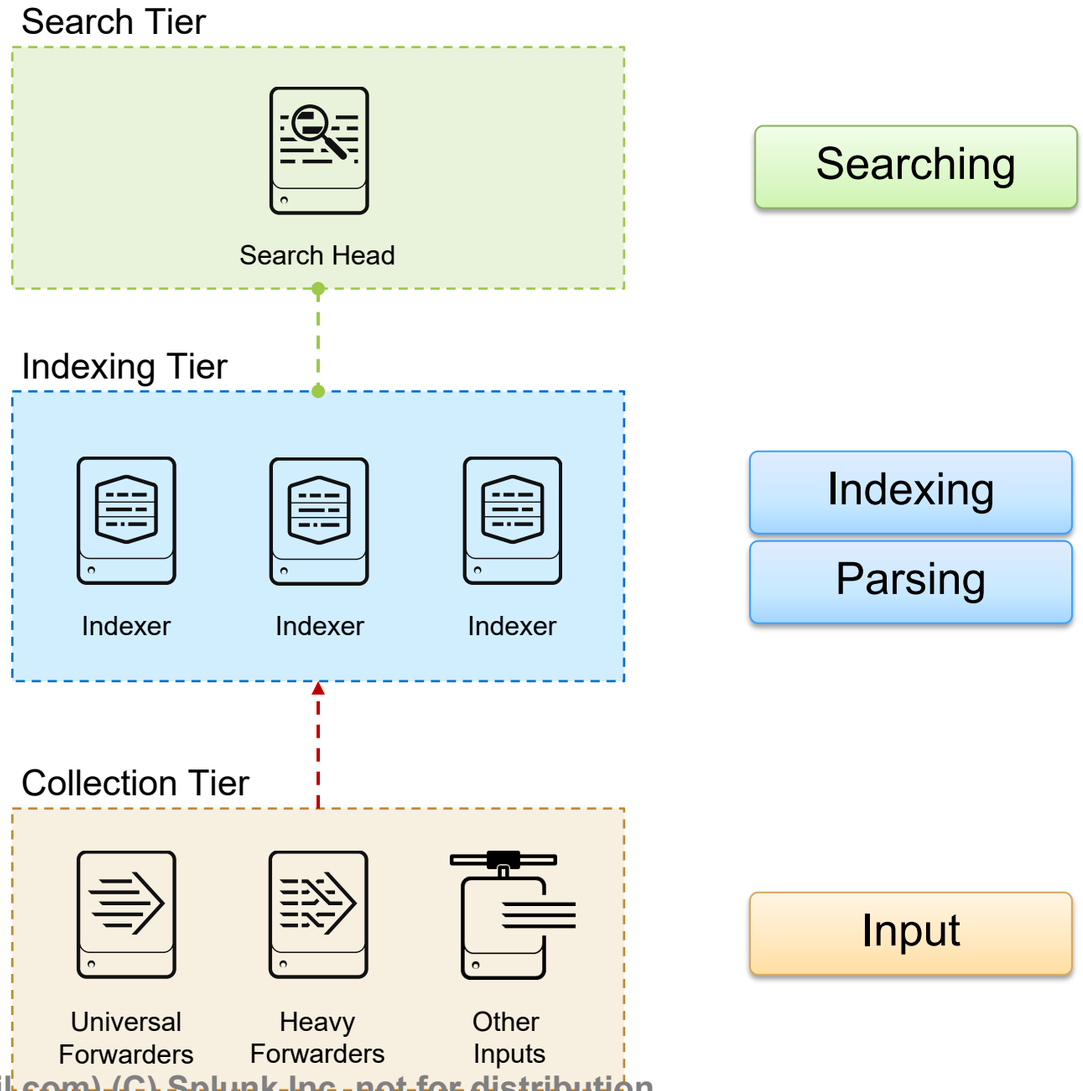


Note

Your lab environment evolves to include a separate forwarder.

Distributed Non-Cluster Environment

- Scale Splunk in various ways
  - Add indexers to handle more inputs
  - Add indexers and search heads to handle more searching

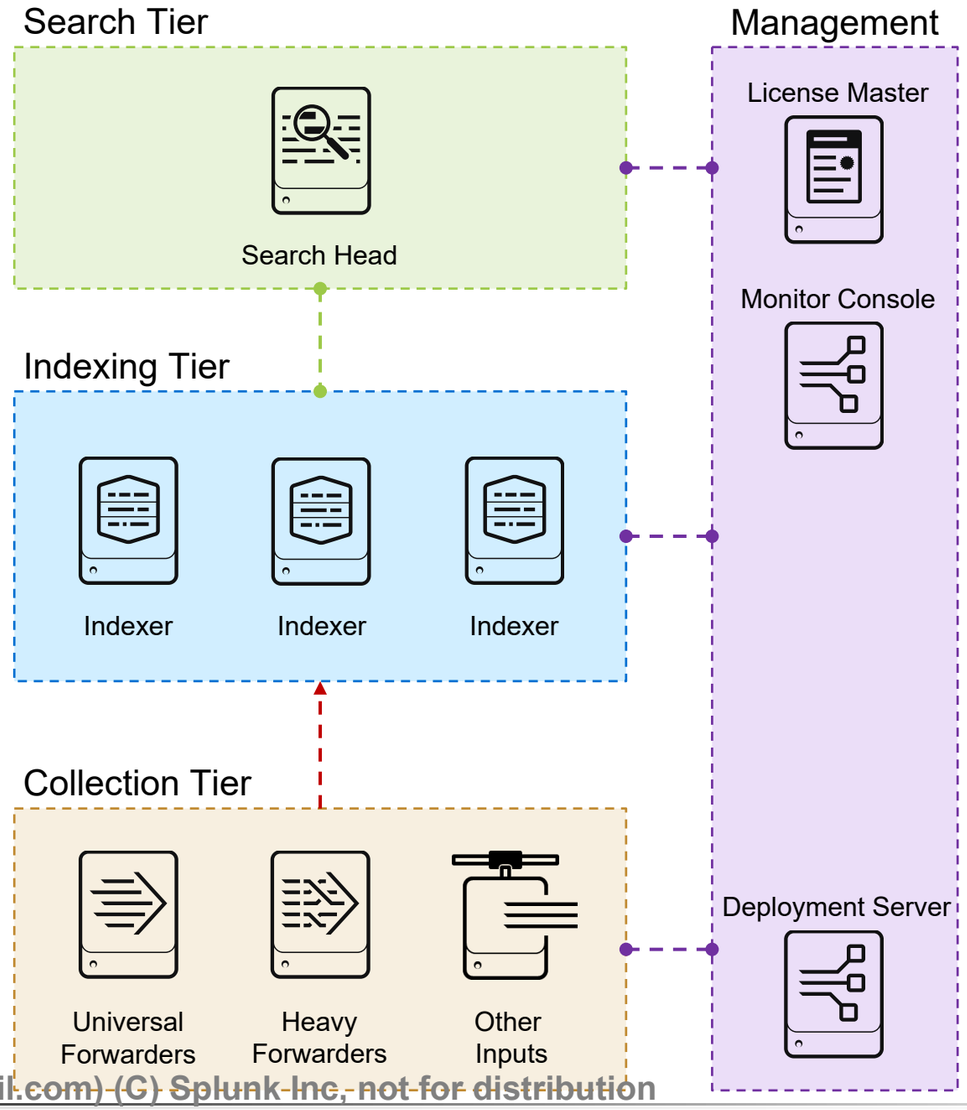


Note

You will add a single indexer (search peer) to your environment in a later lab exercise.

Distributed Non-Cluster Environment (2)

- Centralize management using dedicated servers for various functions including:
  - Deployment server for forwarder management
  - License Master
  - Monitoring Console



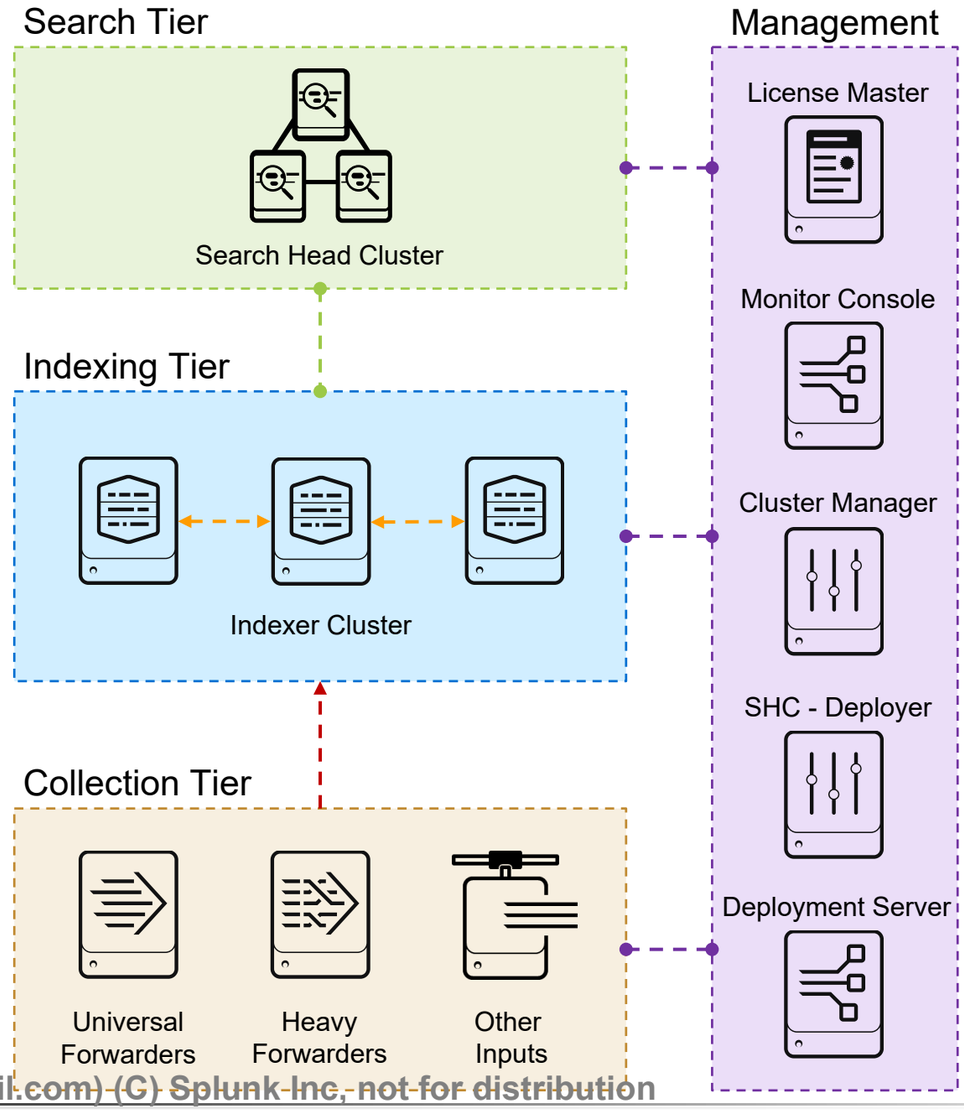
Note

Deployment server management is covered in the *Splunk Enterprise Data Administration* course.

 | 15 September 2021

Splunk Clustered Environment

- Search head clustering
  - Replicates knowledge objects
- Indexer clustering
  - Replicates data across indexers
  - Single-site or multi-site
  - Allows balance of growth, speed of recovery, and overall disk usage
- Does not require additional licenses
- Discussed in the *Splunk Cluster Administration* class



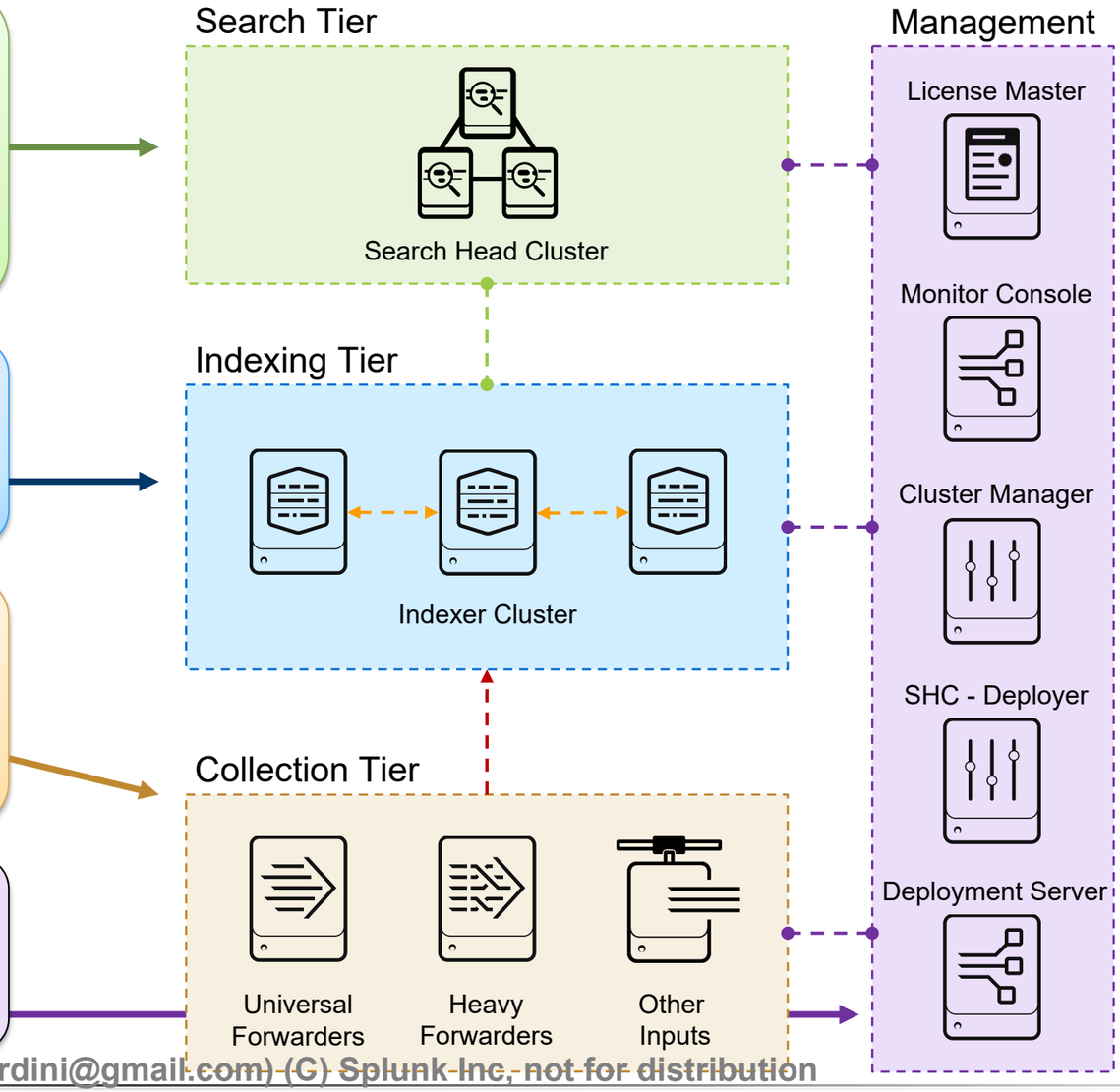
Splunk Core Components and Processes

- Allow users to submit search requests using SPL
- Distribute search requests to the indexers
- Consolidate results and render visualizations of results
- Store search-time knowledge objects (such as field extractions, alerts, and dashboards)

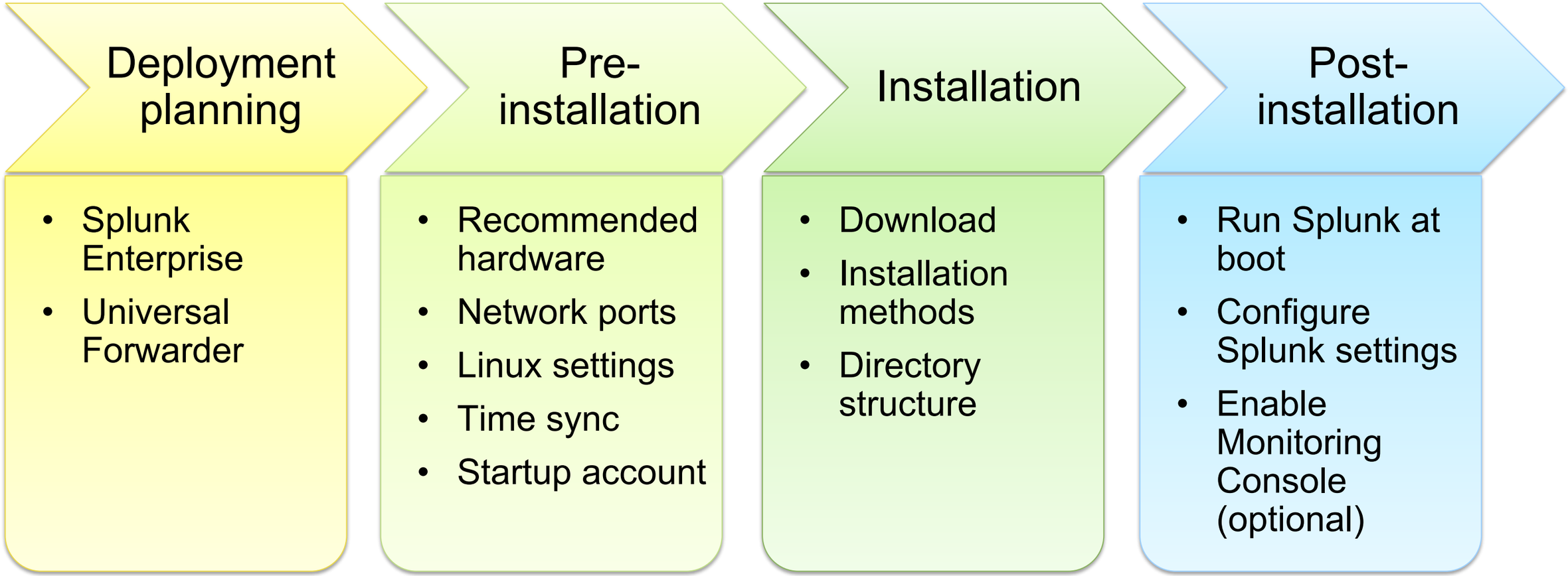
- Receive incoming data from forwarders
- Index and store data in Splunk indexes
- Search data in response to requests from search heads

- Monitor configured inputs and forward the data to the indexers (best practice data collection method)
- Requires minimal resources and typically installed on the machines that produce the data

- Centralizes configuration management for various functions including clustering, licensing, and clients
- Requires systems running Splunk Enterprise

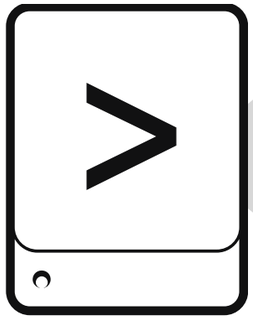


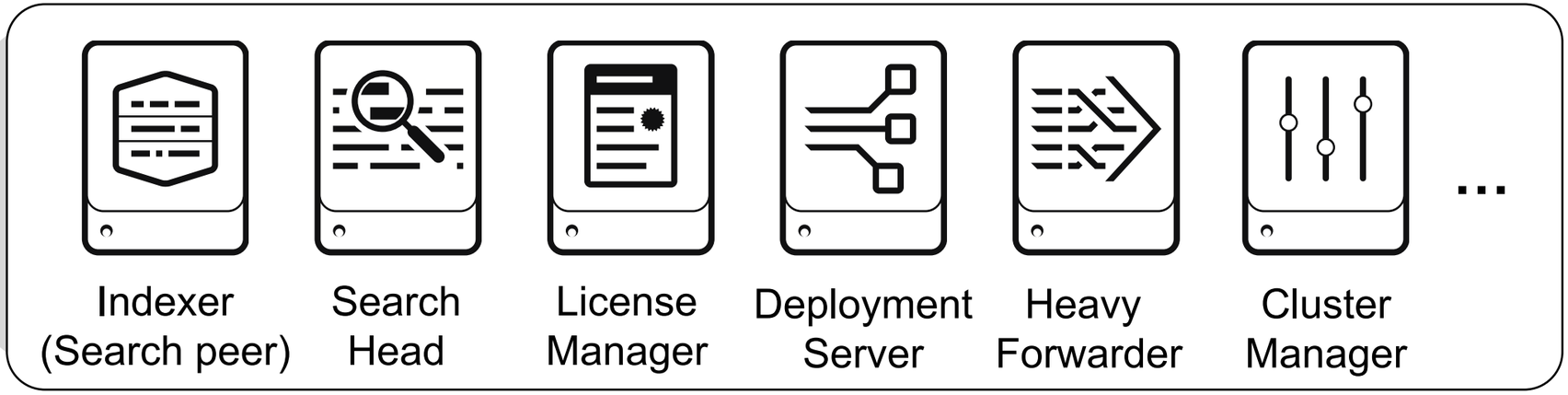
Splunk Installation Overview



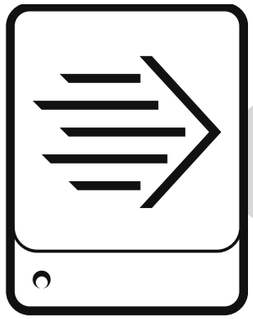
Software in Splunk Enterprise packages

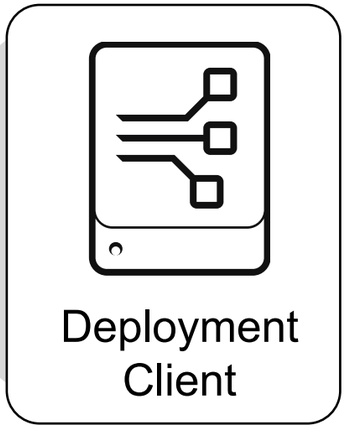
Splunk Enterprise package





Universal Forwarder package





Note

The System Administrator is responsible for installing and configuring Splunk components.

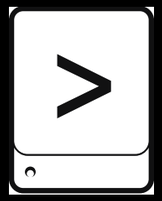
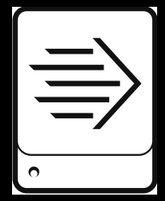
 | 15 September 2021

Server Hardware Recommendations

Component	Indexer	Search Head
OS	Linux or Windows 64-bit distribution	
Network	1Gb Ethernet NIC (optional 2nd NIC for a management network)	
Memory	12-128 GB RAM	12 GB RAM
CPU	x86 64-bit chip architecture **12-48 CPU cores** or **24-96 vCPU** (2+ GHz)	x86 64-bit chip architecture **16 CPU cores** or **32 vCPU** (2+ GHz)
Disk	Disk subsystem capable of **800+ IOPS** SSD subsystem for hot/warm buckets	2 x 10K RPM 300GB SAS drives, or better

- For more detailed information:
  - Attend the *Architecting and Deploying Splunk* class
  - docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware
  - docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements

Splunk Default Network Ports

Usage	Splunk Enterprise 	Universal Forwarder 
splunkd	**8089**	**8089**
Splunk Web	**8000**	-
Web app-server proxy	**8065**	-
KV Store	**8191**	-
S2S receiving port(s)	No default	-
Any network/http input(s)	No default	No default
Index replication port(s)	No default	-
Search replication port(s)	No default	-

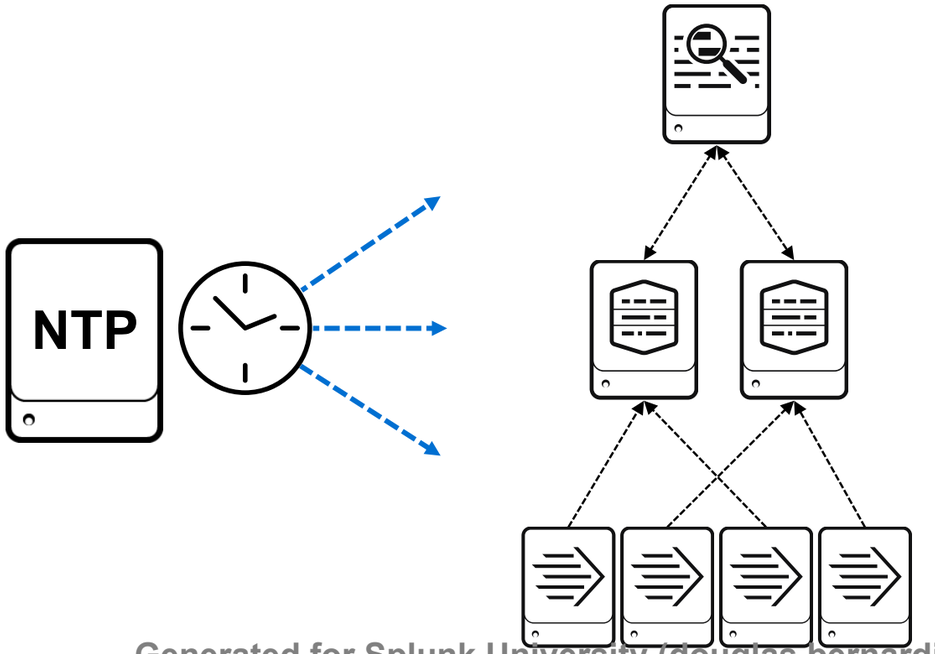
Linux Setting Recommendations

- Setting system resource limits
  - Use **`ulimit -a`** to view settings
  - Increase parameters on indexers and search heads, for example:
    - File descriptors (**`ulimit -n`**) >= 64k, based on buckets and searches
    - Max user processes (**`ulimit -u`**) >= 16k, based on forwarders / concurrent searches
    - Set in configuration files, according to whether Linux is **`initd`** or **`systemd`** -based
  - docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/ulimitErrors
  - docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements
- Turn Transparent Huge Pages (THP) off on Splunk Enterprise servers
  - docs.splunk.com/Documentation/Splunk/latest/ReleaseNotes/SplunkandTHP

```
# ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) unlimited
pending signals                 (-i) 30646
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files                      (-n) 8192
...
cpu time               (seconds, -t) unlimited
max user processes              (-u) 30646
```

Time Synchronization

- Ensure a standardized time configuration on Splunk servers
  - Splunk searches depend on accurate timestamps on events
  - Clock skew between hosts can affect search results
  - Popular protocol is NTP (Network Time Protocol)



splunk> Best Practice

Startup Account

- Do not run Splunk as ***super-user***

***NIX**	• Avoid the **root** account
Windows	• Avoid the **administrator** account • Use a domain account if Splunk must connect to other servers • Alternatively, use a local machine account that can run services

- Splunk user account must:
  - Read files and directories configured for monitoring by Splunk
    - *NIX: **`/var/log`** is not typically open to non-root accounts
  - Write to the Splunk Enterprise directory (**`SPLUNK_HOME`**)
  - Execute any scripts required (alerts or scripted input)
  - Bind to the network ports Splunk is listening on
    - *NIX: non-root accounts cannot access reserved ports (< 1024)

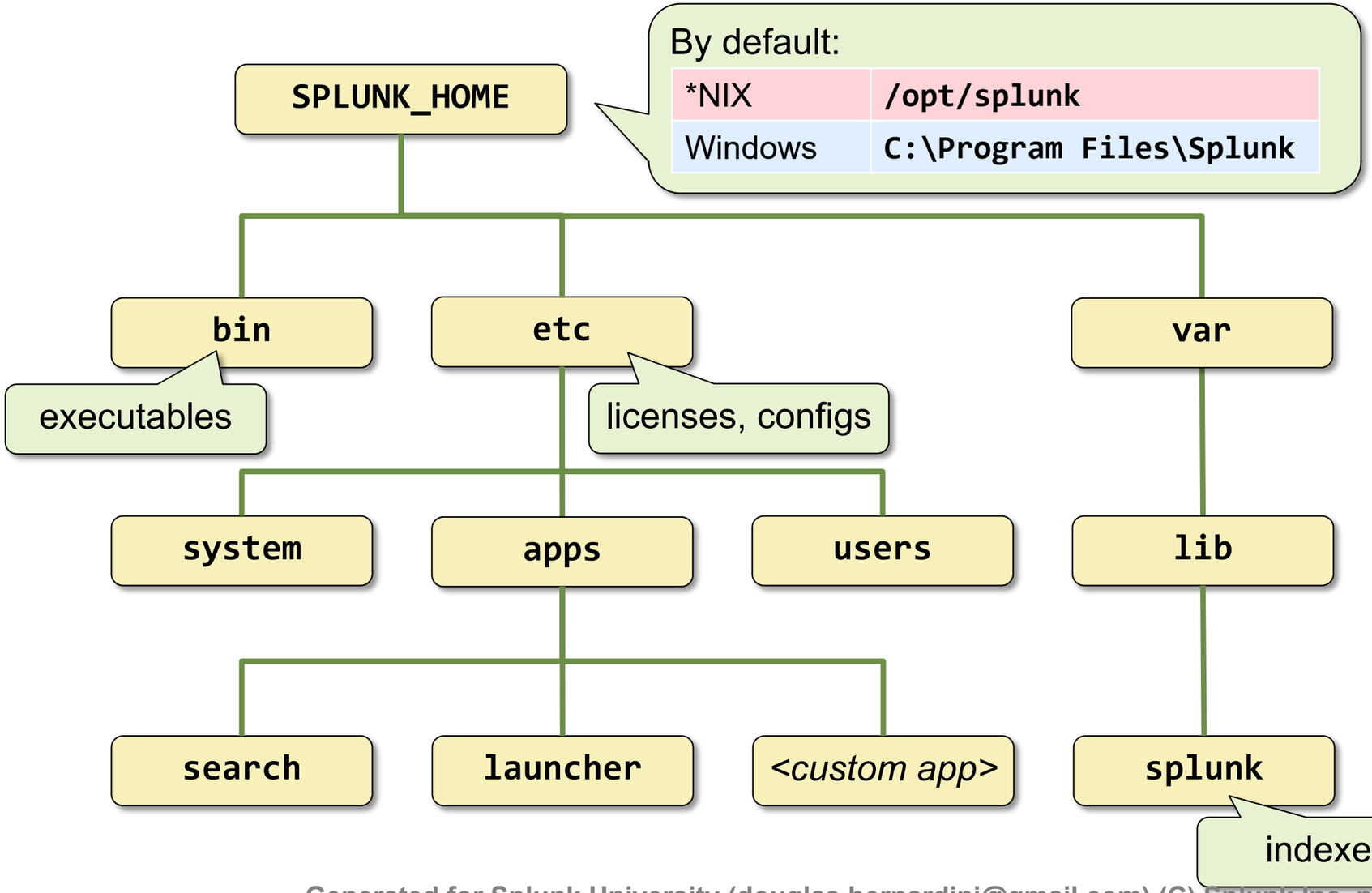
splunk> Best Practice

Installing Splunk Enterprise Server

	*NIX	Windows
Download	**https://www.splunk.com/download**	
Install	• Un-compress **`.tar.gz`** file in the path you want Splunk to run from • Also available as rpm, deb	Execute the **`.msi`** installer and follow the wizard steps
Post-Install	• Splunk starts manually • Enable **`boot-start`** to have Splunk start automatically	Splunk starts automatically

Installation instructions at:
docs.splunk.com/Documentation/Splunk/latest/Installation/Chooseyourplatform

Splunk Directory Structure



Note

$SPLUNK_HOME is used in Splunk documentation as a placeholder for "*the top directory where Splunk is installed*", **not** as an exported environment variable. In this training **SPLUNK_HOME** is used.

Note

$SPLUNK_DB by default refers to **SPLUNK_HOME/var/lib/splunk**

Running Splunk at Boot

Splunk on *NIX

- Does not auto-start at boot time, by default
- Enable auto-start on **`init.d`** -based distributions:

```
# splunk enable boot-start -user username
```

- Enable auto-start on **`systemd`** -based distributions:

```
# splunk enable boot-start -systemd-managed 1
```

Note

Splunk best practice is to run Splunk Enterprise as a non-root user.

Splunk on Windows

- Configured to auto-start at boot time by the installer
- Runs as **`splunkd`** and **`splunkweb`** services, and starts child processes
- Managed as any Windows service (can be set to Manual or Disabled)

docs.splunk.com/Documentation/Splunk/latest/admin/ConfigureSplunkToStartAtBootTime

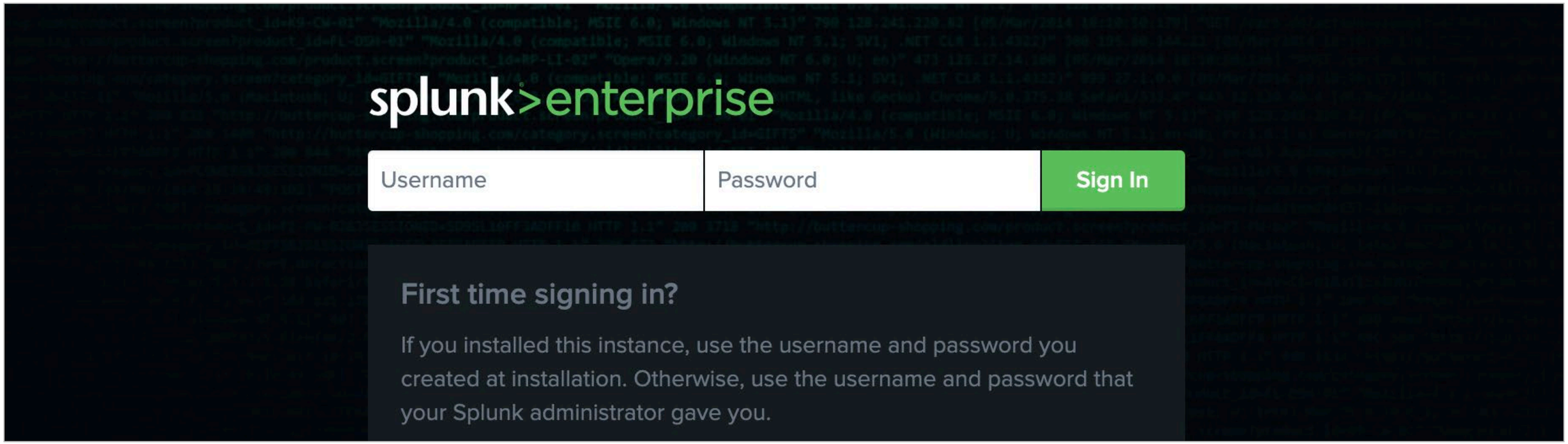
The **splunkd** Process

- Runs on port 8089 (default) using SSL
- Spawns and controls Splunk child processes (helpers)
  - Splunk Web proxy, KV store, and Introspection services
  - Each search, scripted input, or scripted alert
- Accesses, processes, and indexes incoming data
- Handles all search requests and returns results
- Viewed using the **splunk status** command:

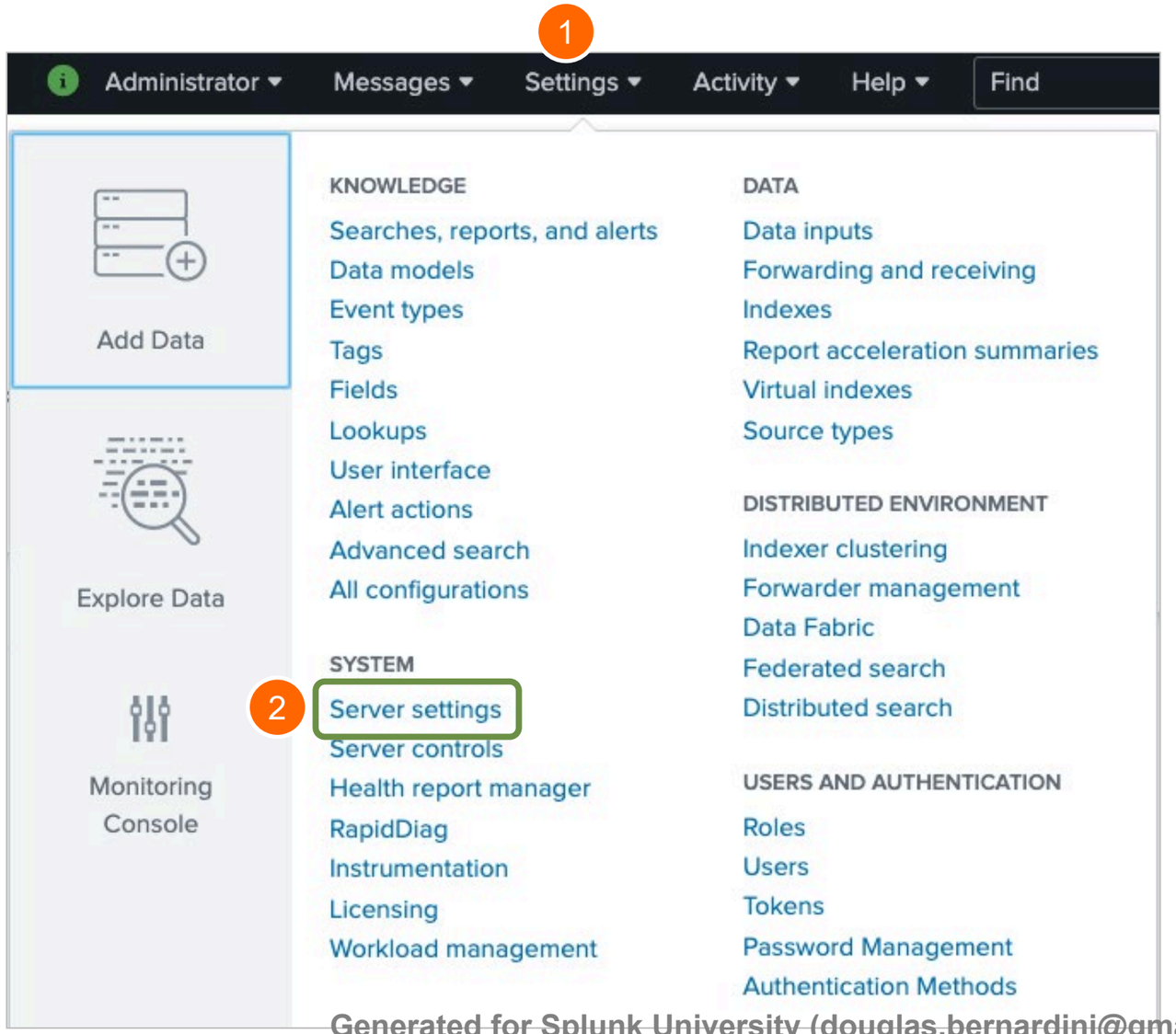
```
# splunk status
splunkd is running (PID: 2128).
splunk helpers are running (PIDs: 2135 2148 2205 2266).
```


Splunk Web

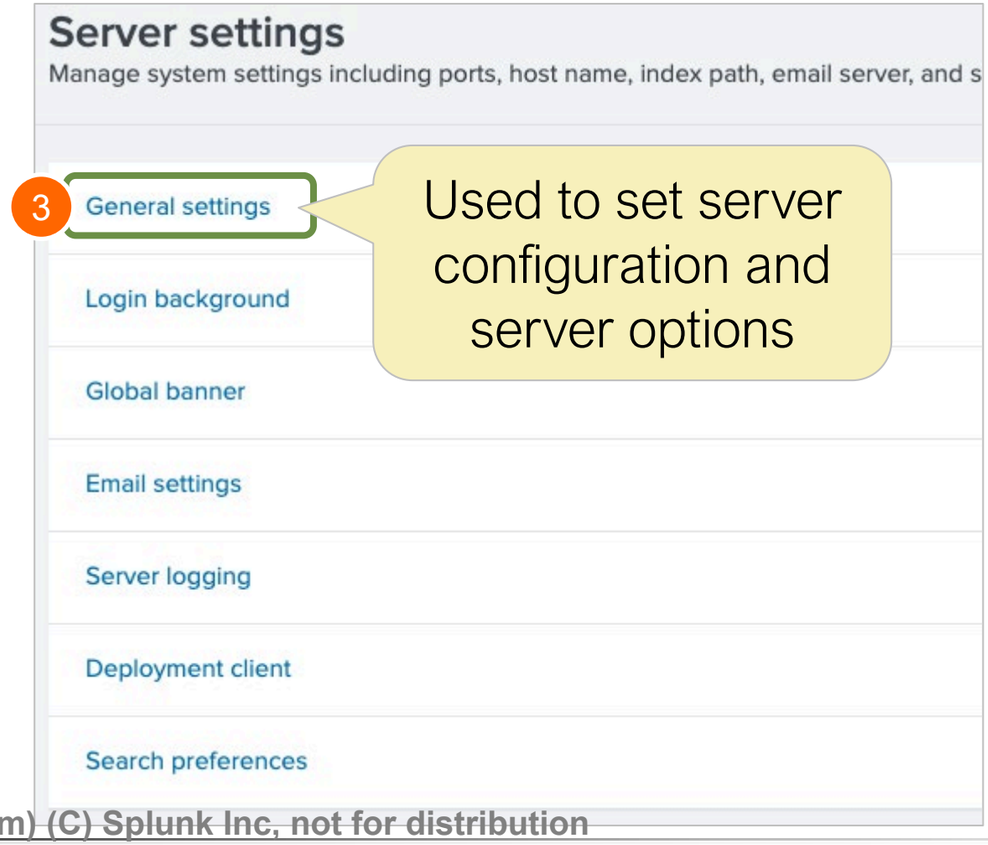
- Browser-based user interface
- Provides a search and management front end for **splunkd** process
- Found at **http://<*server_name*>:<*port*>** (default port 8000)



Splunk Web – Server Settings

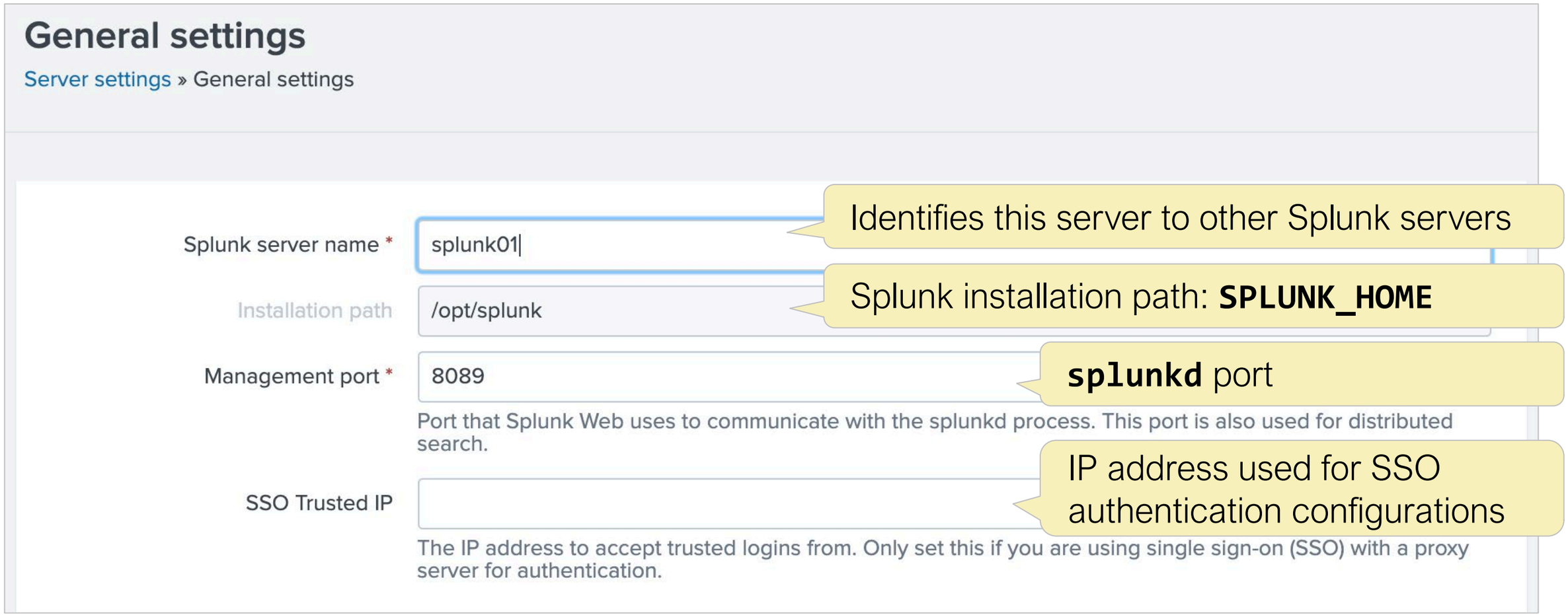


Select **Settings > Server settings > General settings**

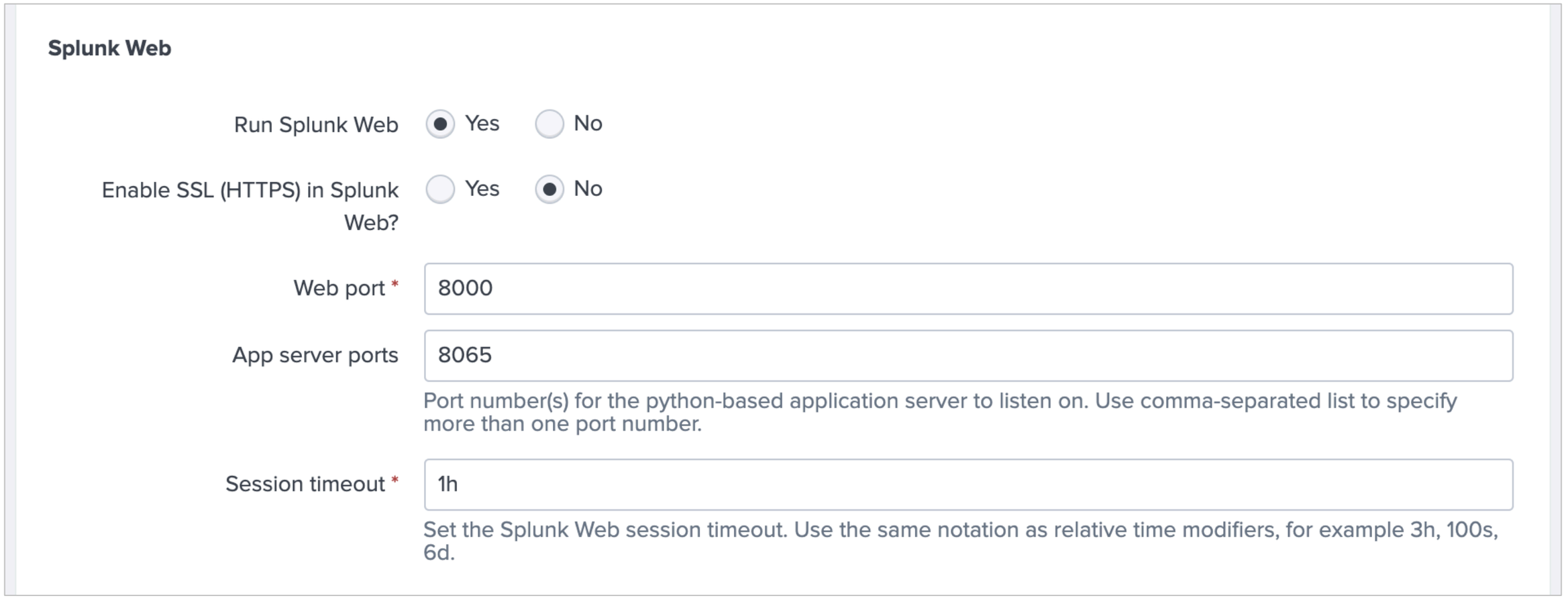


Used to set server configuration and server options

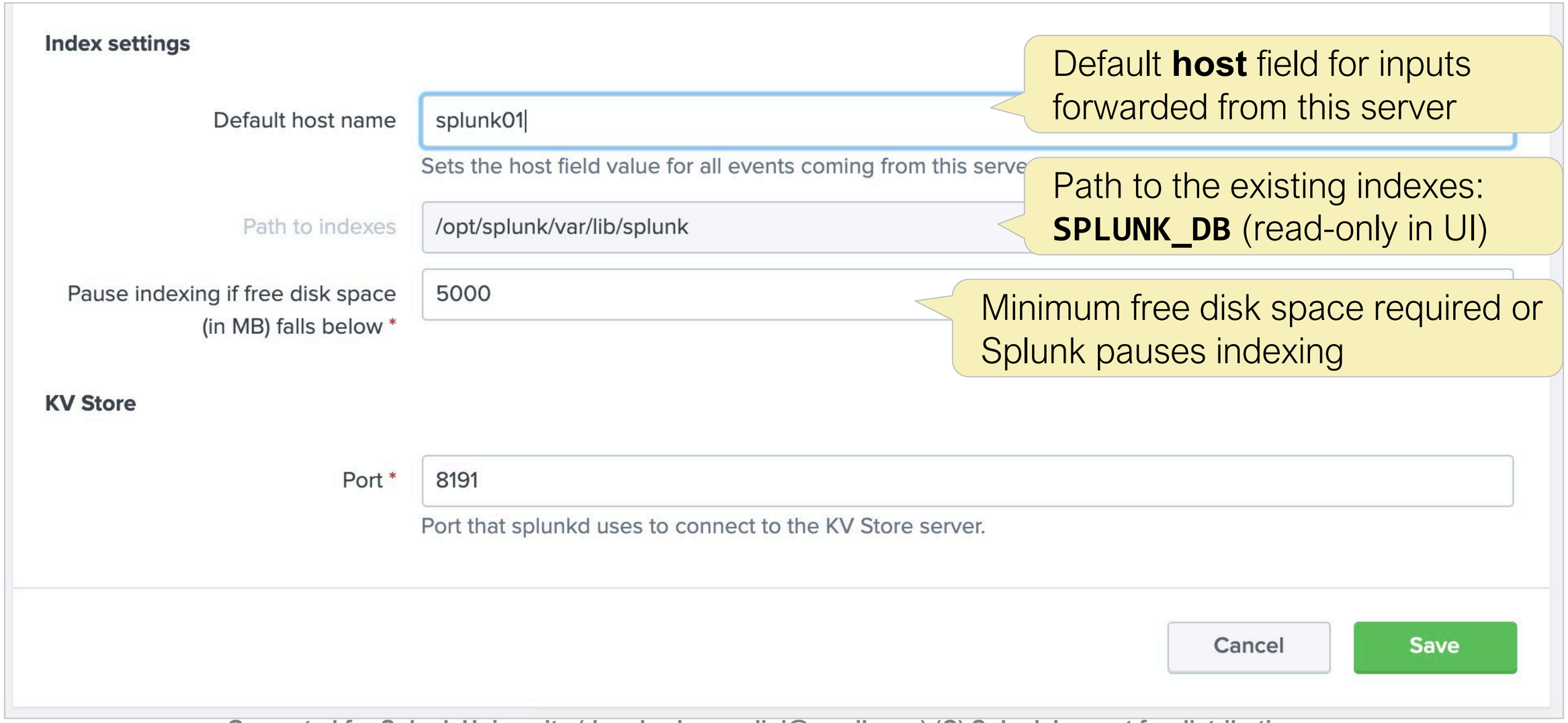
Describing General Settings



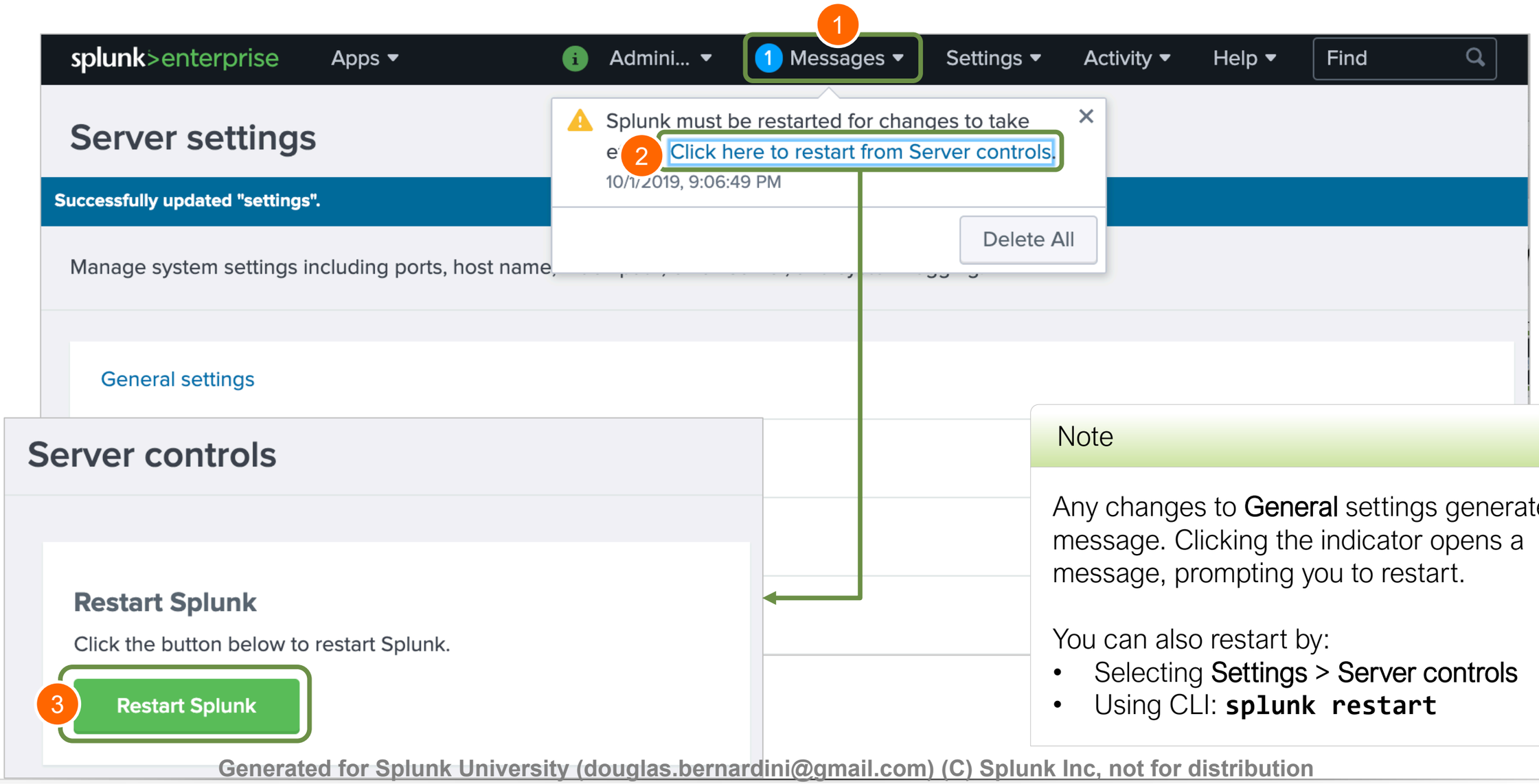
Describing General Settings – Splunk Web



Describing General Settings – Index/KV Store



Restarting the Server from Splunk Web



Note

Any changes to **General** settings generate a message. Clicking the indicator opens a message, prompting you to restart.

You can also restart by:

- Selecting **Settings** > **Server controls**
- Using CLI: **`splunk restart`**

 | 15 September 2021

Splunk Command Line Interface (CLI)

- Executable command (**splunk**) in the **SPLUNK_HOME/bin** directory
- Uses the same syntax on all supported platforms:

Command	Operation
splunk help	Display a usage summary
splunk help <object>	Display the details of a specific object
splunk [start | stop | restart]	Starts and stops the Splunk processes
splunk start –-accept-license	Automatically accept the license without prompt
splunk status	Display the Splunk process status
splunk show splunkd-port	Show the port that the **splunkd** listens on
splunk show web-port	Show the port that Splunk Web listens on
splunk show servername	Show the server name of this instance
splunk show default-hostname	Show the default host name used for all data inputs

More Resources

Splunk Documentation	http://docs.splunk.com/Documentation
Splunk App Repository	http://splunkbase.splunk.com/
Splunk Answers	http://answers.splunk.com/
Splunk Blogs	http://www.splunk.com/blog/
Splunk Wiki	http://wiki.splunk.com/
Splunk User Groups	http://usergroups.splunk.com/

Module 1 Knowledge Check

- Which installer will you use to install the Search Head?
- True or False. When you install Splunk on Windows, you also have to configure the boot-start.
- True or False. The default Splunk Web port is set to 8000

Module 1 Knowledge Check – Answers

- Which installer will you use to install the Search Head?

  Splunk Enterprise

- True or False. When you install Splunk on Windows, you also have to configure the boot-start.

  False. You only need to configure boot-start on Linux

- True or False. The default Splunk Web port is set to 8000

  True.

Module 1 Lab Exercise

Time: 15 minutes

Description: Configure a Splunk Server

Tasks:

- Log into Splunk Web
- Change Splunk server name
- Restart Splunk
- Use CLI to confirm the status and changes

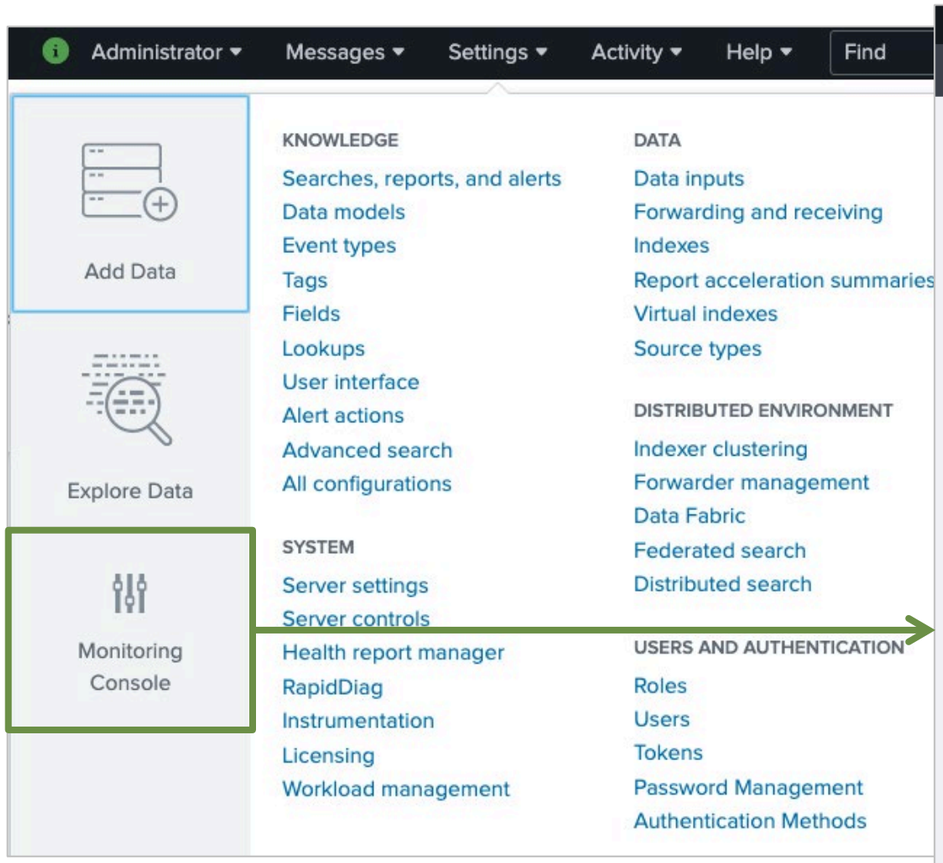
Module 2:
Splunk Server Monitoring

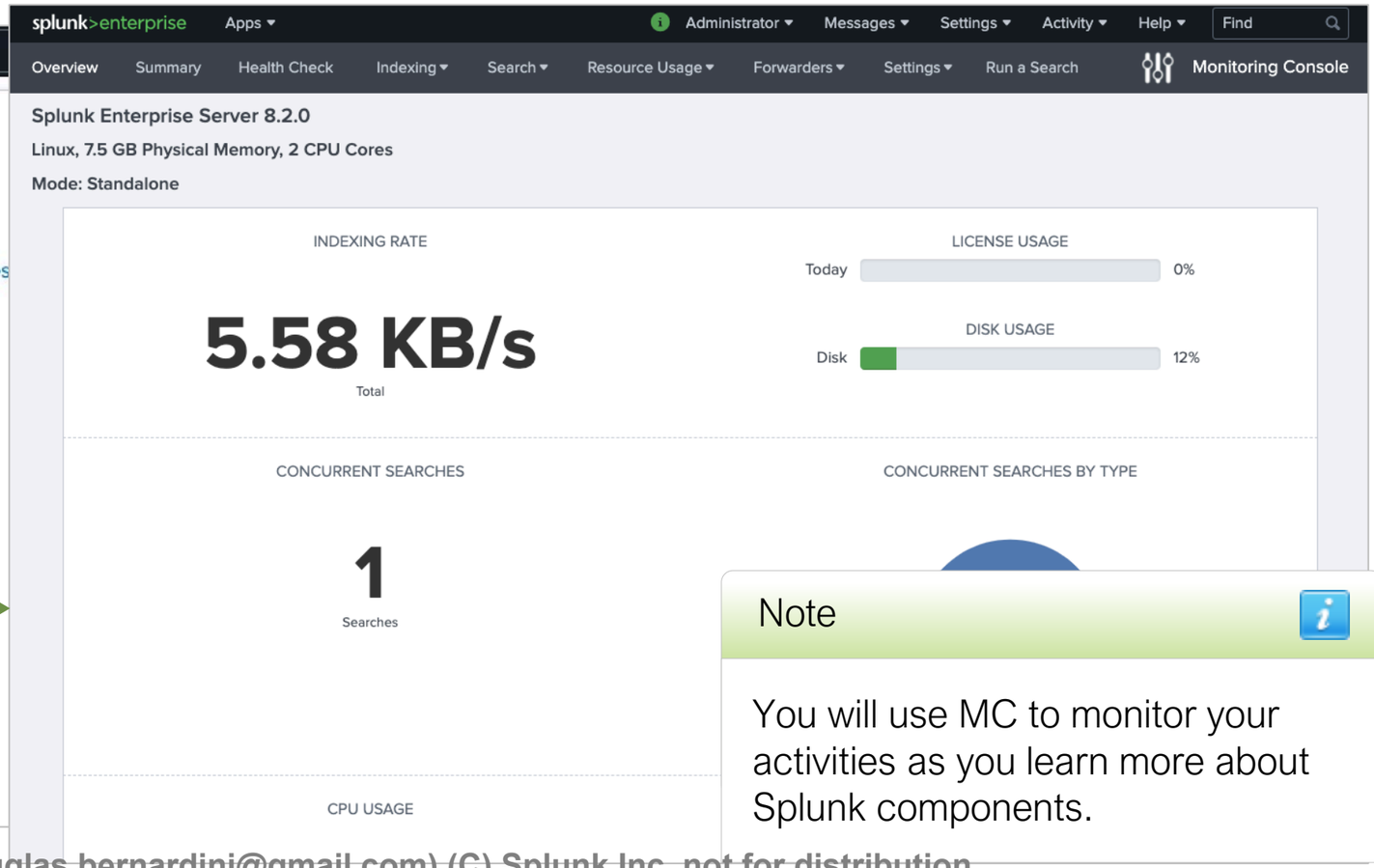
Module Objectives

- Enable the Monitoring Console (MC)
- Identify Splunk license types
- Describe license violations
- Add and remove licenses
- Use Splunk Diag

Monitoring Console (MC)

A Splunk admin-only app used to monitor and investigate data Splunk collects about itself, such as performance and resource usage





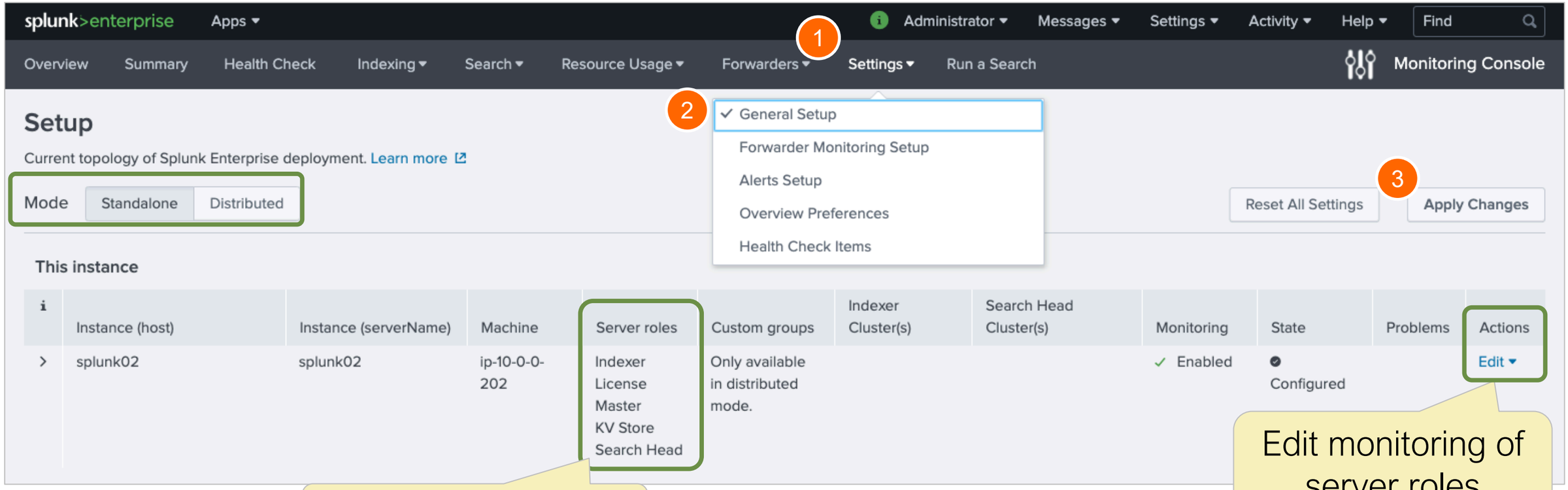
Note

You will use MC to monitor your activities as you learn more about Splunk components.

 | 15 September 2021

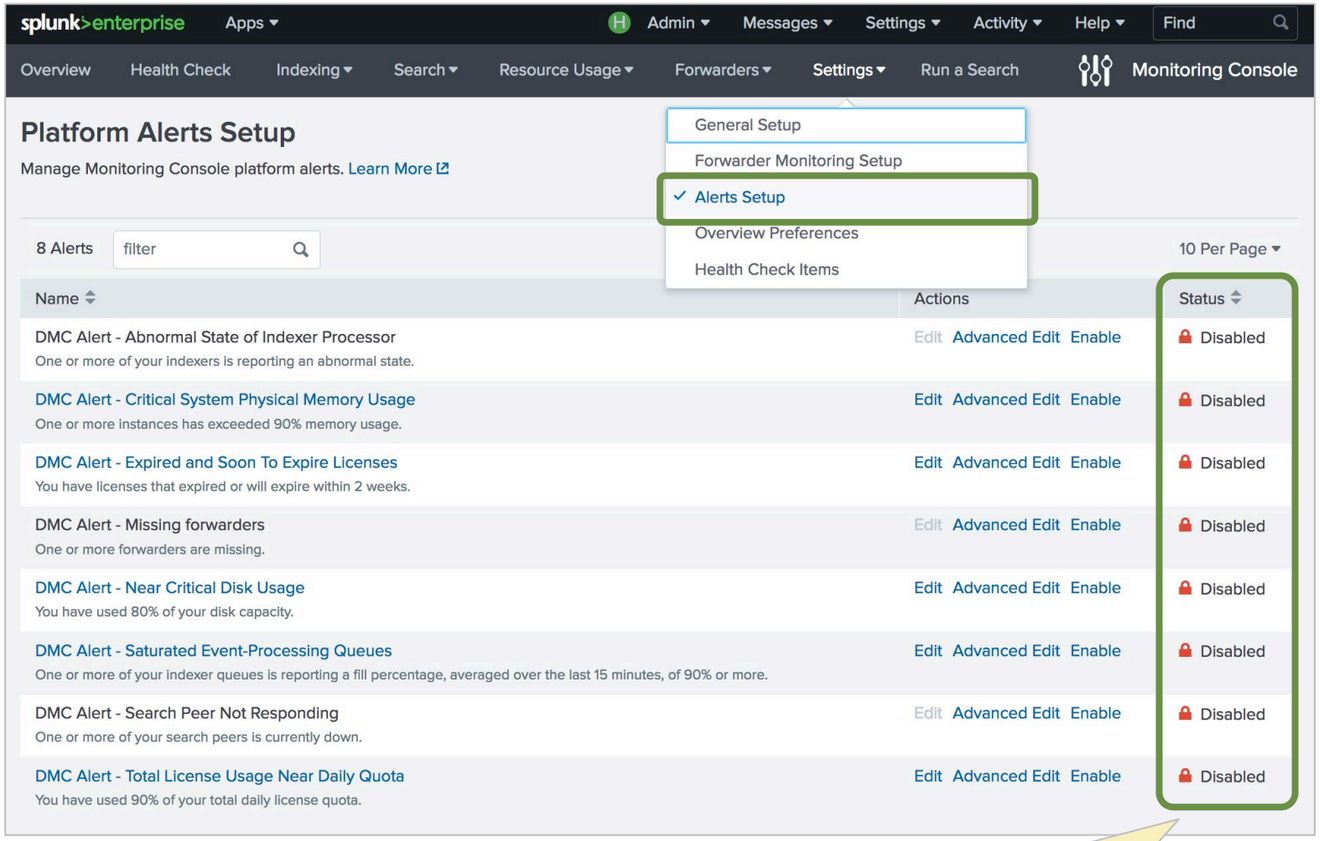
Enabling MC in Standalone Mode

- MC runs un-configured in standalone mode by default
- To enable, click **Settings > General Setup > Apply Changes**



Enabling MC Platform Alerts

- Timely notification of critical conditions helps effectively operate the Splunk environment
- MC **Alerts Setup** provides preconfigured platform alerts
  - Disabled by default
  - Customizable alert schedule, suppression time, and alert actions

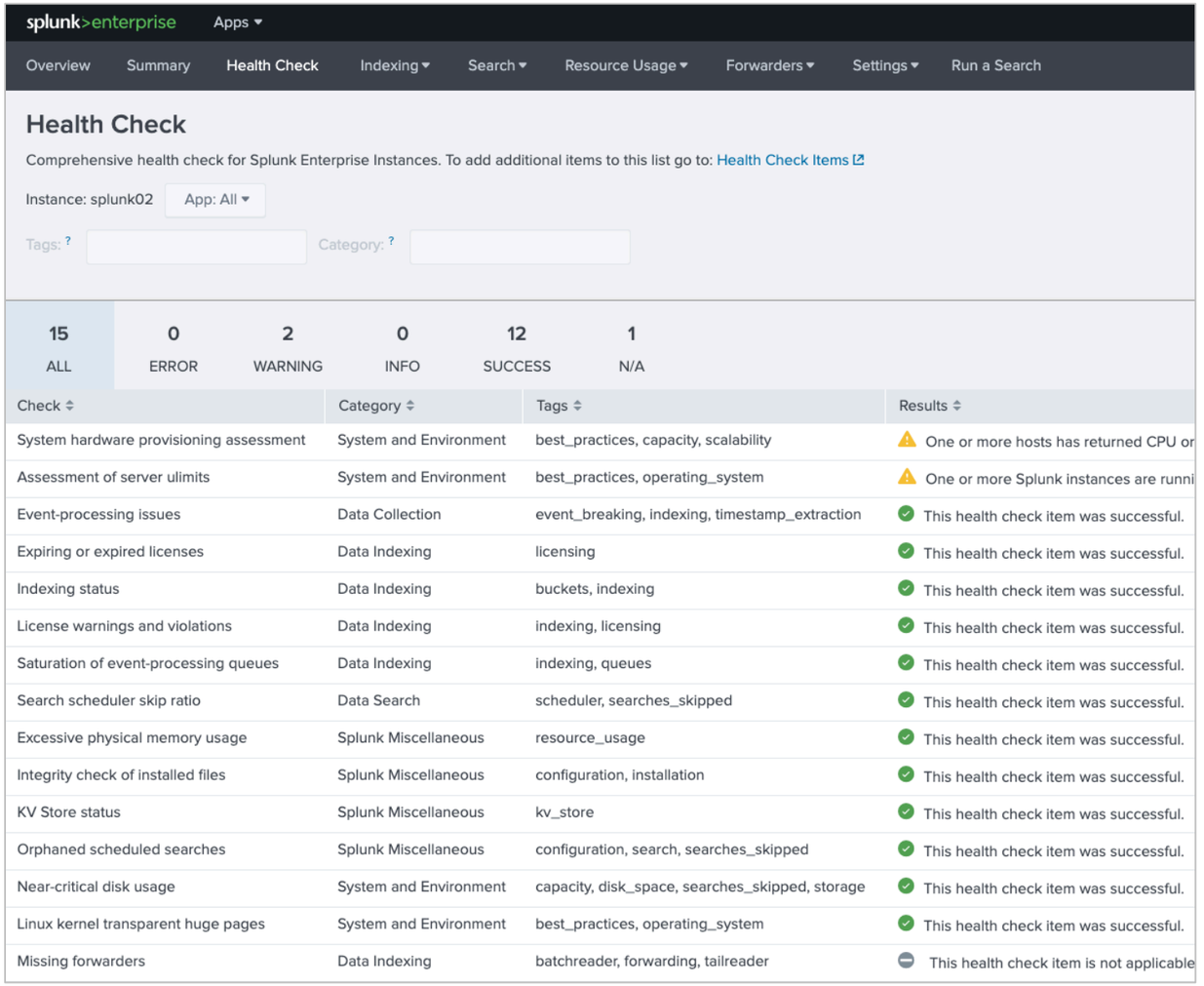


Disabled by default

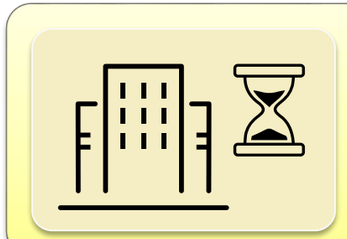
 | 15 September 2021

MC Health Check

- Series of ad hoc searches that run sequentially:
  - **Monitoring Console > Health Check**
- Comes preconfigured but can be disabled, modified, created, and exported using:
  - **Settings > Health Check Items**

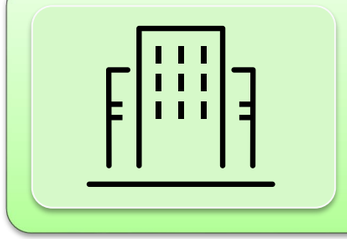


Splunk License Types



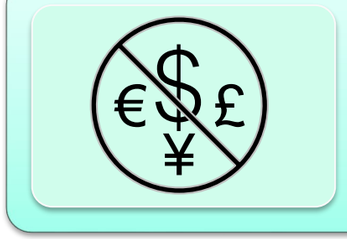
Enterprise trial license

- Comes with product; Valid for 60 days, after which another license type must be activated
- Same as **Enterprise license**, except for 500 MB/day limit
- A **Sales trial license** is a trial Enterprise license of varying size and duration



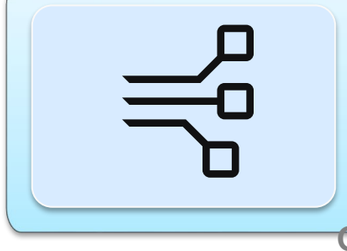
Enterprise license

- Purchased from Splunk; Sets the daily indexing volume amount or compute capacity
- Full functionality for indexing, search head, deployment server, and so on
- No-enforcement license: Allows searching even if you are in a license violation period *



Free license

- Disables alerts, scheduled searches, authentication, clustering, distributed search, summarization, and forwarding to non-Splunk servers
- Allows 500 MB/day of indexing and forwarding to other Splunk instances



Forwarder license

- Sets the server up as a heavy forwarder
- Applies to non-indexing forwarders
- Allows authentication, but no indexing

* Except for licenses < 100 GB/day starting in Splunk 8.1

License Alerts, Warnings and Violations

Alert

- Occurs when indexing exceeds the allocated daily quota in a pool
- Viewed in Splunk Web > **Messages** (as a "pool warning")
- Cleared at midnight when daily allocation is reset; may result in a Warning

Warning

- Occurs if an alert is triggered, and license capacity is not increased by midnight (by adding new license or moving capacity from another pool)
- Only occurs once per day

Violation

- Occurs after 5 warnings on an Enterprise license* in a rolling 30-day period
- Informational only, and does not affect indexing or searches**
- Requires a reset key from Splunk Support or Sales team

* 3 Warnings on a Free license

** Searches are disabled for licenses < 100 GB/day with 45 warnings in a rolling 60-day period

Measuring Daily License Quota

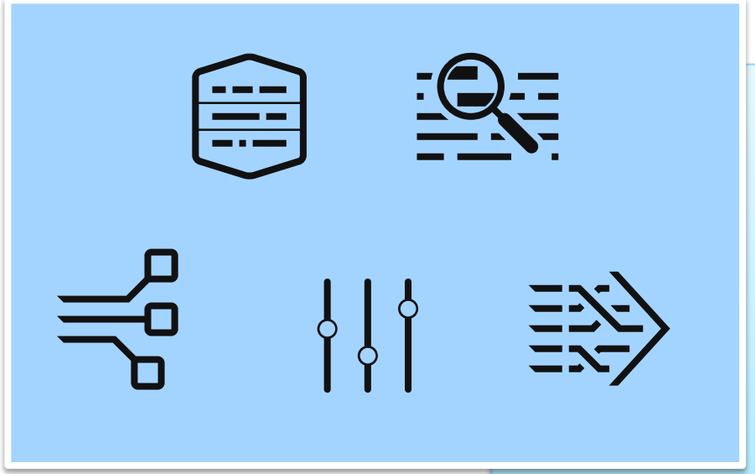
Counts for daily license quota

- All data from all sources that is indexed
- **For events**: Measured as the data (full size) that flows through the parsing pipeline per day
- **For metrics**: Measurement capped at 150 bytes per metric event

Does not count for daily license quota

- Replicated data (Index Clusters)
- Summary indexes
- Splunk internal logs (_internal, _audit, etc. indexes)
- Structural components of an index (metadata, tsidx, etc.)

License Requirements With Server Roles and Data



Server Roles

Search Heads, **Deployment Server** and other Splunk Enterprise instances require the license even if they are not ingesting data

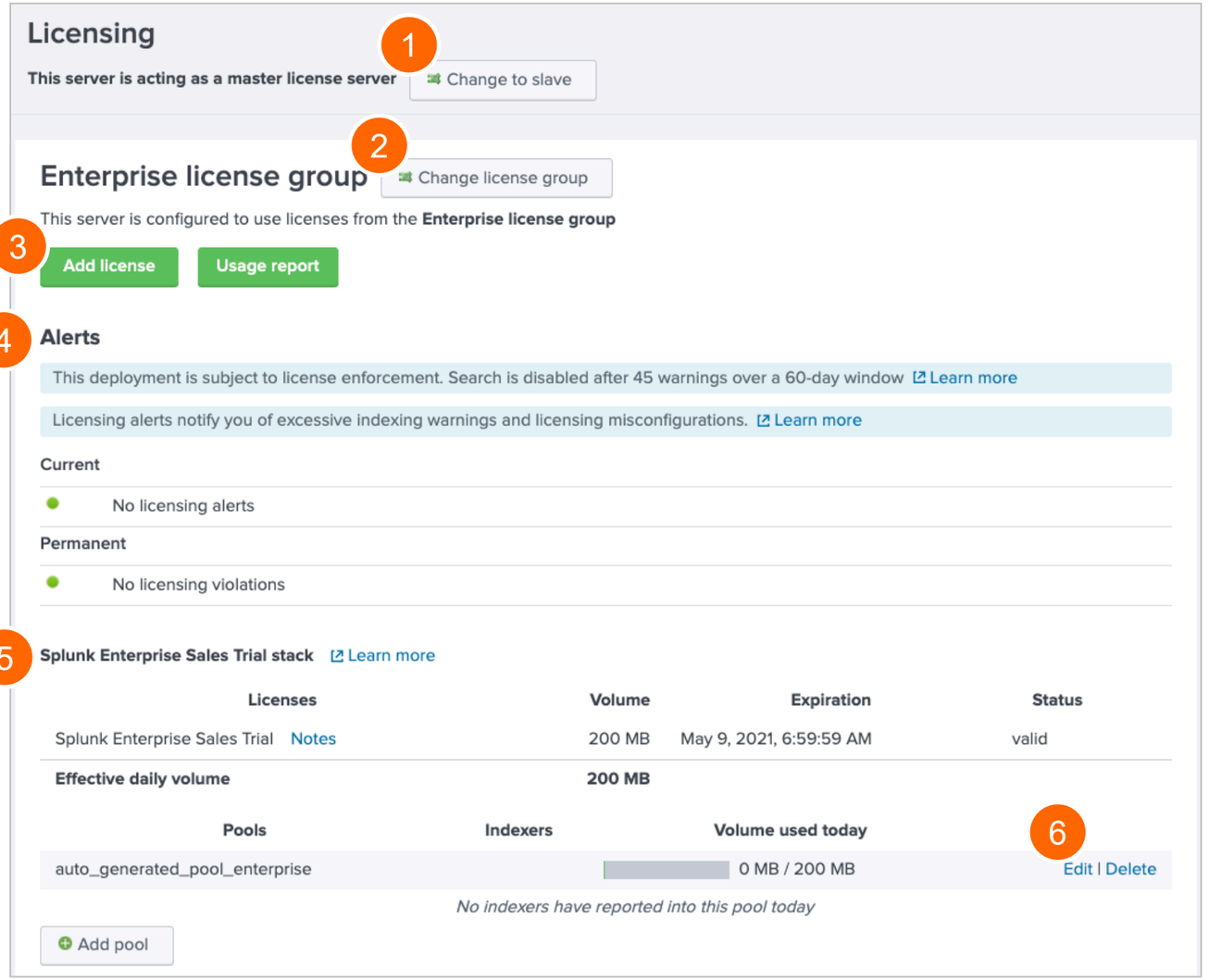
Data

Indexers (Search Peers) also need the license to determine the amount of ingested data allowed

Managing Licenses

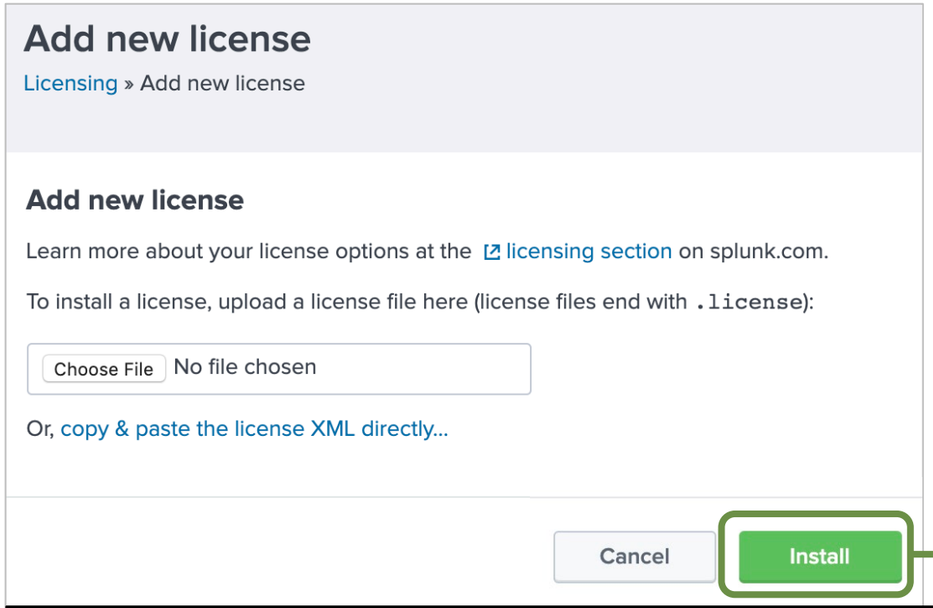
Select **Settings > Licensing**

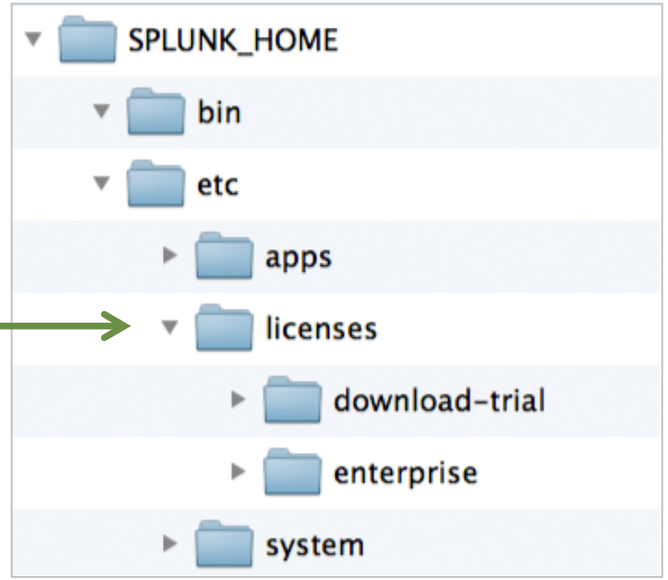
1. Designate the license server type: Master or slave
2. Change license group
3. Add a license
4. Check license alerts and violations
5. View stacks
6. Edit and add pools



Adding a License

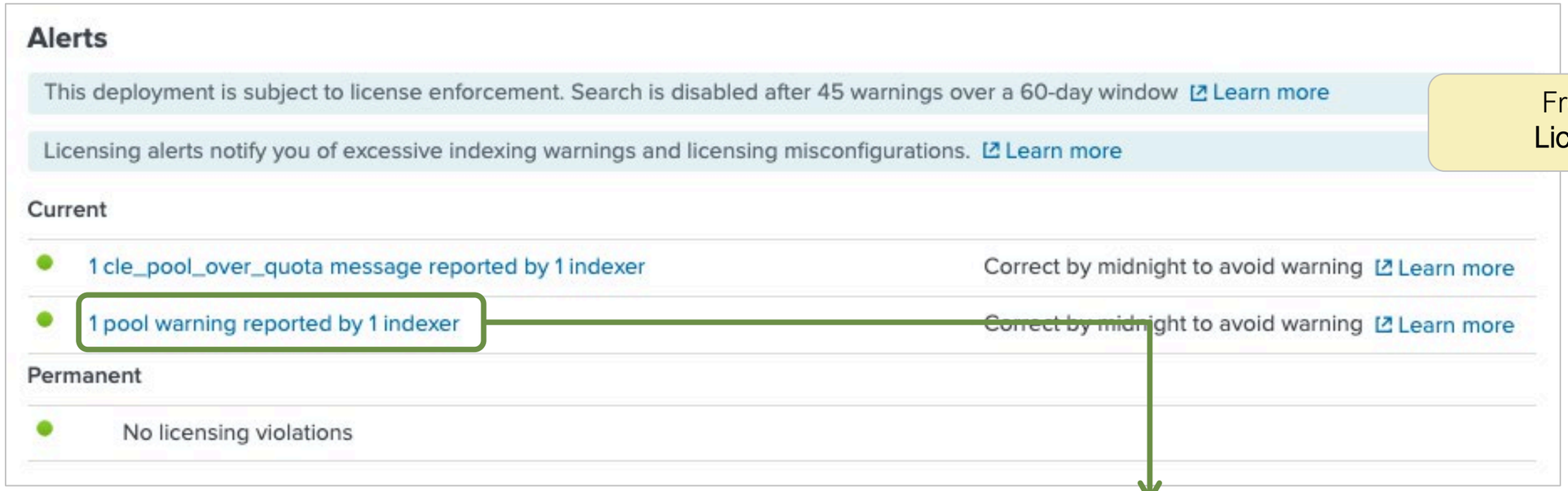
- Use CLI or Splunk Web (upload or copy/paste)
- Restart Splunk if license group changes are made
- Find licenses under **`SPLUNK_HOME/etc/licenses`**
  - Multiple licenses of the same type are “stacked” (added together)



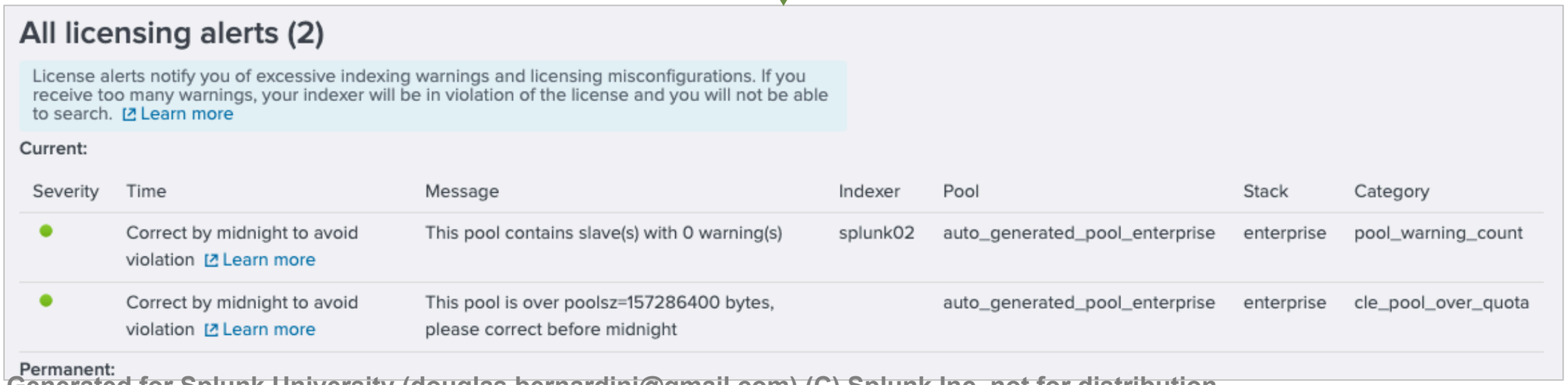



```
splunk add licenses <path_to_file>
```

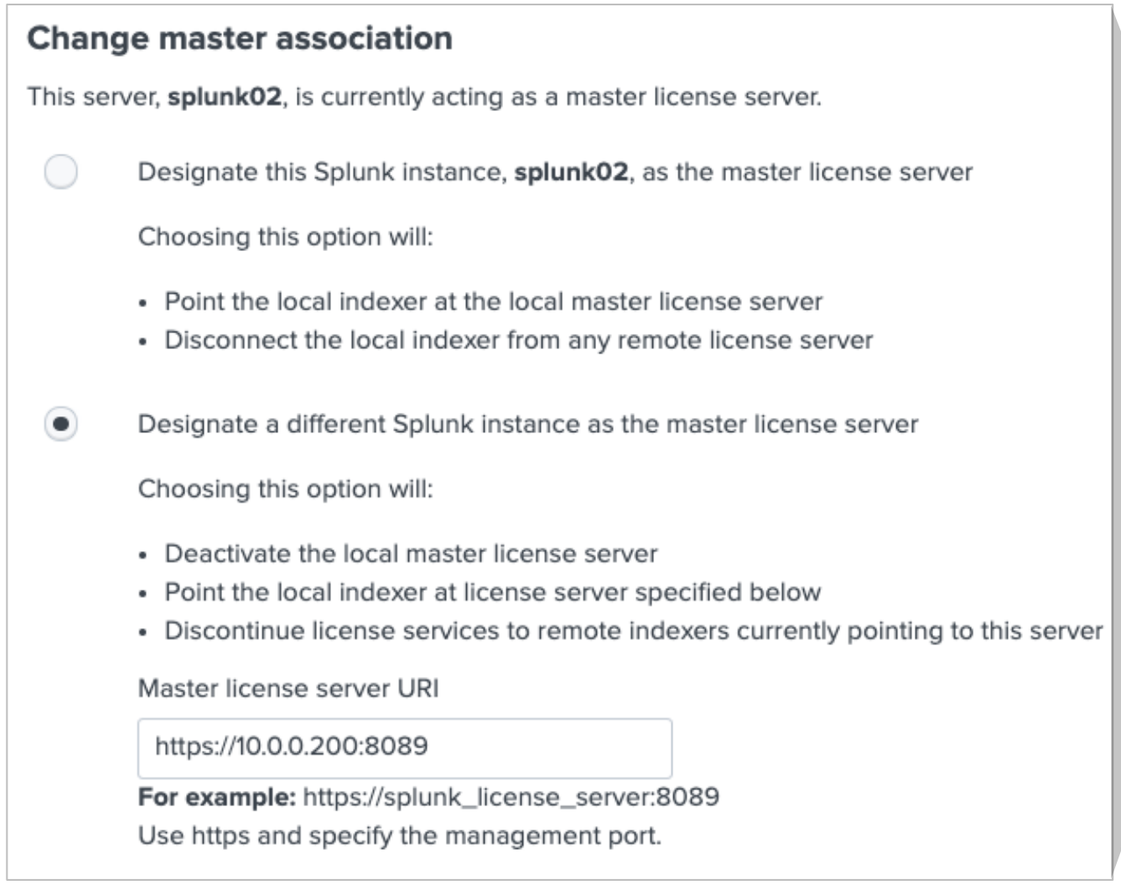
Viewing License Alerts

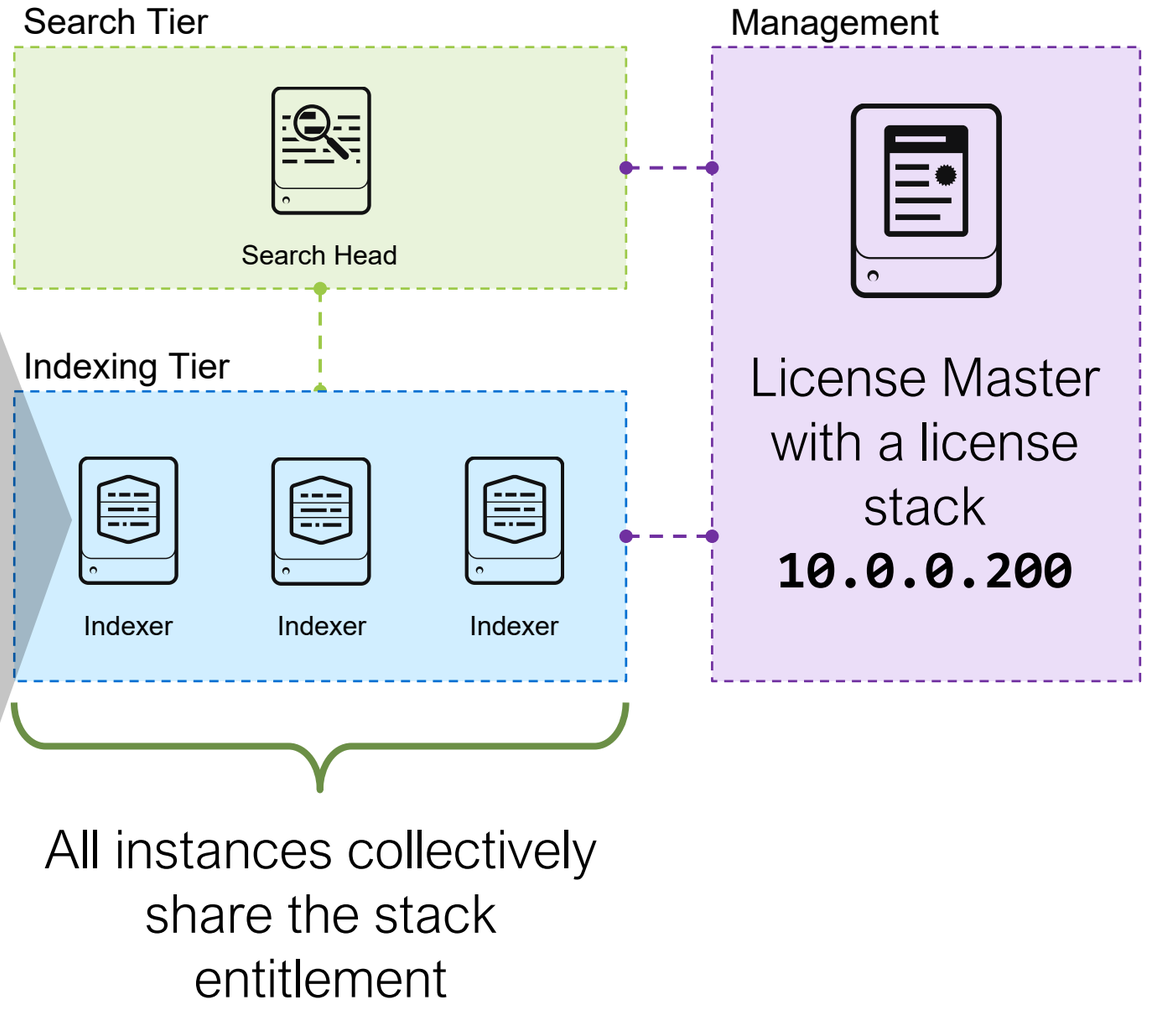


From Splunk Web, select
Licensing > License Alerts



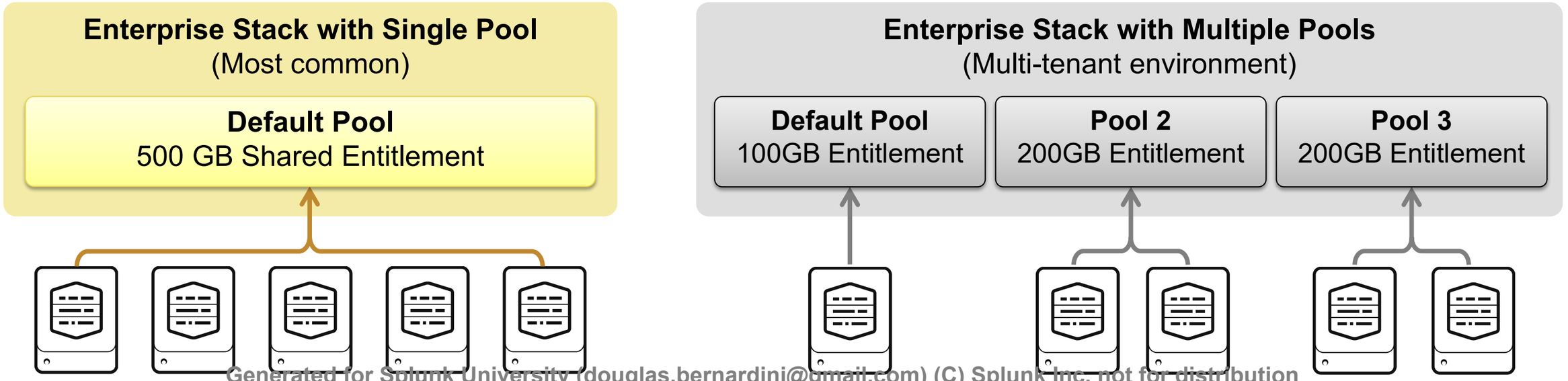
Changing an Instance to Use a License Master





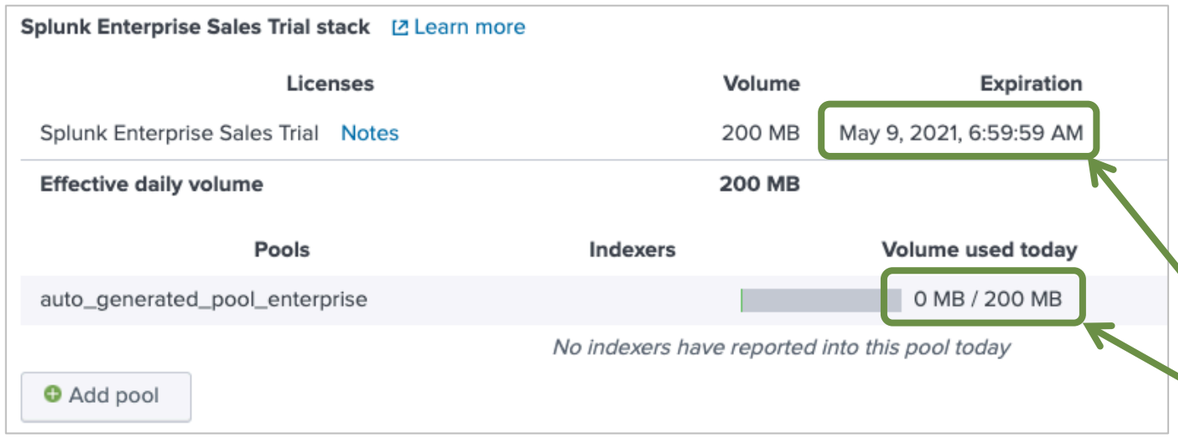
License Pooling

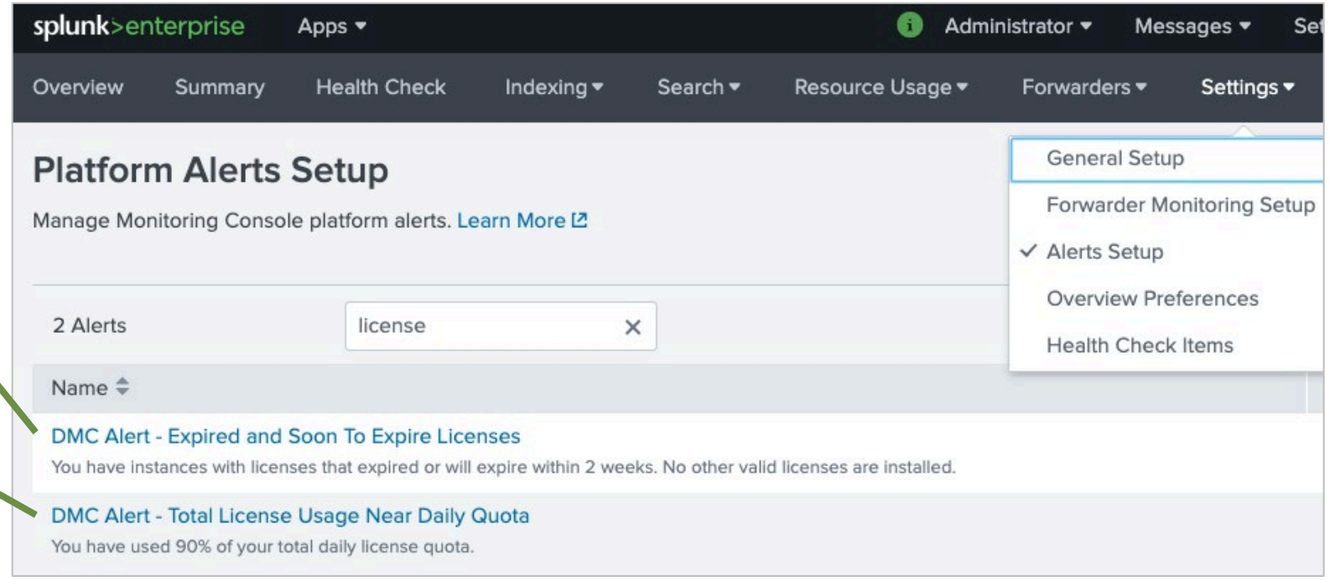
- Allows licenses to be subdivided and assigned to indexer groups
- Can be created for a given stack
- Provides warnings and violations per pool
- Examples of License Managers with total stack of 500GB



Managing License Warnings

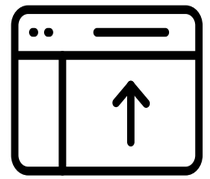
- DO NOT ignore license warnings
- Proactively monitor the consumption of your Splunk license
  - MC provides a couple of alerts
  - If possible, give yourself latitude by rearranging license pools





Ingest-Based versus Infrastructure-Based Pricing

Ingest-Based Pricing



- Based on data volume
- Traditional licensing method
- Cost effective for most environments and customers
- Monitored via MC and **Settings > Licensing** in Splunk Web

Infrastructure-Based Pricing

- Based on compute capacity
- Cost effective for some larger environments, providing more control over product expansion (search versus indexing)
- Monitored via MC in Splunk Web or Cloud Monitoring Console

What is a Splunk Diag?

- Gathers data and provides insight to your instance

Server specs	Configuration, OS version, file system, and current open connections
Splunk platform	Contents of **`SPLUNK_HOME/etc`** such as app configurations, Splunk log files, and index metadata

- Produces a **`tar.gz`** file and **`diag.log`**
- Does not retrieve customer or index data
  - Examine the file to ensure no proprietary data is included
- Can be Splunked!
  - Ingest the compressed file to view the information in Splunk

Diag Example

```
$ ./splunk diag
Collecting components: conf_replication_summary, consensus, dispatch, etc, file_validate, index_files,
index_listing, kvstore, log, profiler, searchpeers, suppression_listing
Skipping components: rest
Selected diag name of: diag-ip-10-0-0-202-2021-04-23_00-38-43
Starting splunk diag...
Logged search filtering is enabled.
Skipping REST endpoint gathering...
Determining diag-launching user...
Getting version info...
Getting system version info...
```

Reports the components it collect and skips

```
The following certificates were excluded from the diag output automatically.
      /opt/splunk/etc/apps/splunk_secure_gateway/lib/certifi/cacert.pem
      /opt/splunk/etc/apps/splunk_secure_gateway/lib/future/backports/test/https_sv
      /opt/splunk/etc/apps/splunk_secure_gateway/lib/future/backports/test/ssl_key.pem
      /opt/splunk/etc/apps/splunk_secure_gateway/lib/future/backports/test/badkey.pem
      /opt/splunk/etc/apps/splunk_secure_gateway/lib/future/backports/test/dh512.pem
```

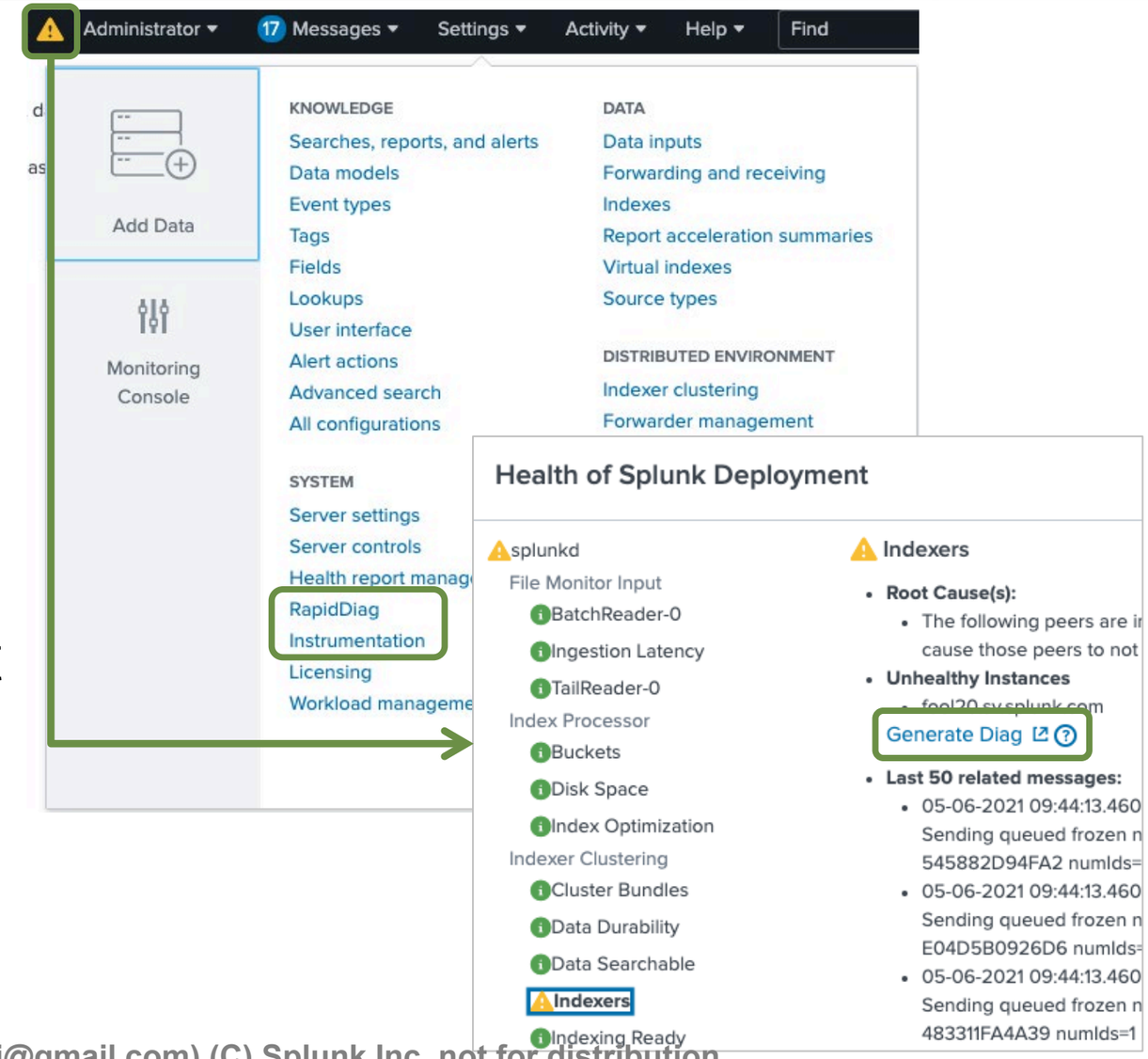
Reports certificates that were not auto-detected or skipped

```
Copying Splunk profiler files...
Copying Splunk dispatch files...
Copying Splunk consensus files...
Adding manifest files...
Adding cachemanager_upload.json...
Cleaning up...
Splunk diagnosis file created: /opt/splunk/diag-ip-10-0-0-202-2021-04-23_00-38-43.tar.gz
```

When complete, output is saved and file location is displayed

Splunk Diagnostics in Splunk Web

- **Instrumentation**
  - Runs diag in Splunk Web
- **RapidDiag**
  - Uses distributed search to run collections from instances
  - Leverages OS and Splunk tools
  - Directly uploads to Splunk Support using command line
  - Available under Health Report in some cases
  - Linux only in Splunk 8.2



Module 2 Knowledge Check

- True or False. Splunk provides separate licenses for metrics and events data.
- True or False. Search Heads also need an Enterprise License (directly or through a License Manager) even without configuring any inputs.
- True or False. If you exceed the daily license quota in a pool, your license will go into a violation.

Module 2 Knowledge Check – Answers

- True or False. Splunk provides separate licenses for metrics and events data.

  False. Metrics data draws from the same license quota as event data.

- True or False. Search Heads also need an Enterprise License (directly or through a License Manager) even without configuring any inputs.

  True.

- True or False. If you exceed the daily license quota in a pool, your license will go into a violation.

  False. Indexing that exceeds the allocated daily quota in a pool is an **alert**. An alert not fixed by midnight turns into a **warning**. 5 or more warnings on an enforced Enterprise license (or 3 warnings on a Free license) in a rolling 30-day period is a **violation**.

Module 2 Lab Exercise

Time: 15 minutes

Description: Splunk Server Monitoring

Tasks:

- Enable Monitoring Console (MC)
- Run a health check and Splunk diag in the MC
- Create a diag using the command line
- Add licenses
- Modify the license pool
- Enable and modify an MC Alert

Module 3: Splunk Apps

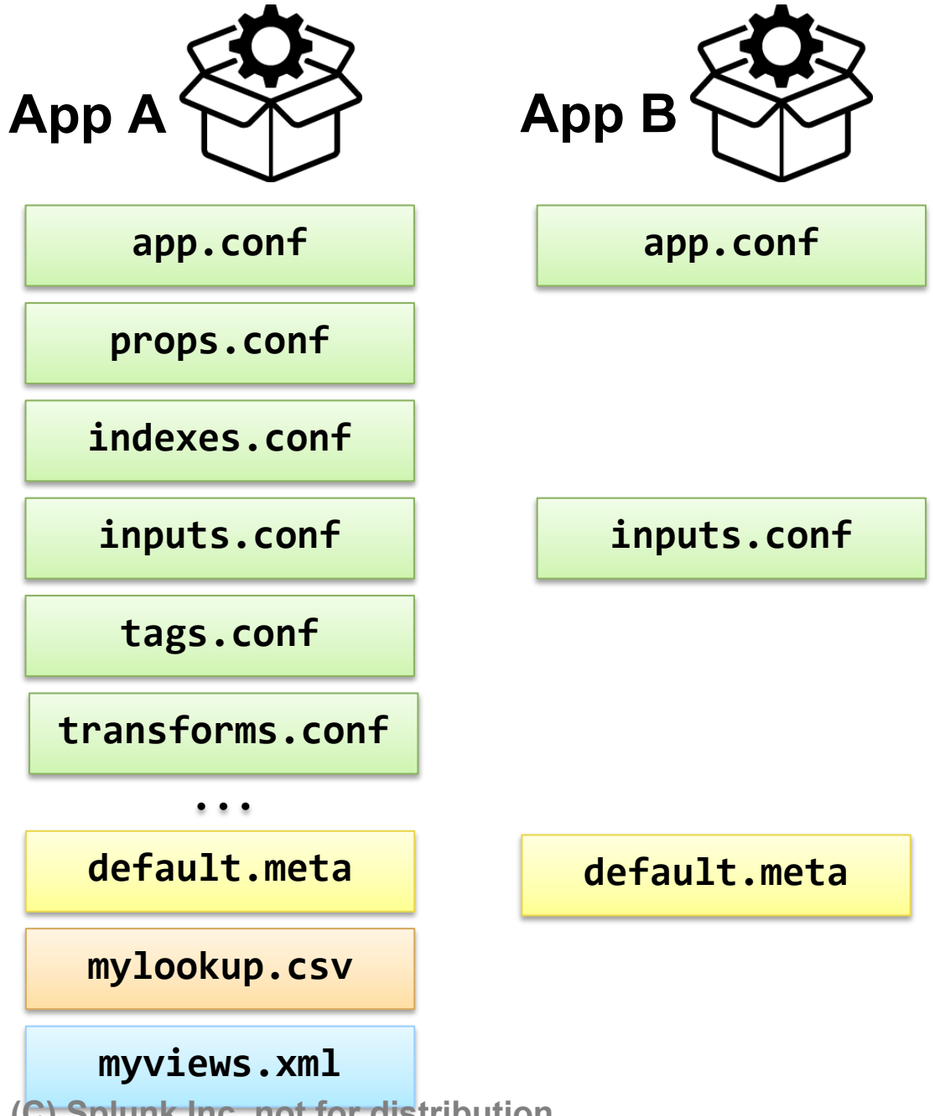
Module Objectives

- Describe Splunk apps and add-ons
- Install an app on a Splunk instance
- Manage app accessibility and permissions

What is an App?

Splunk App

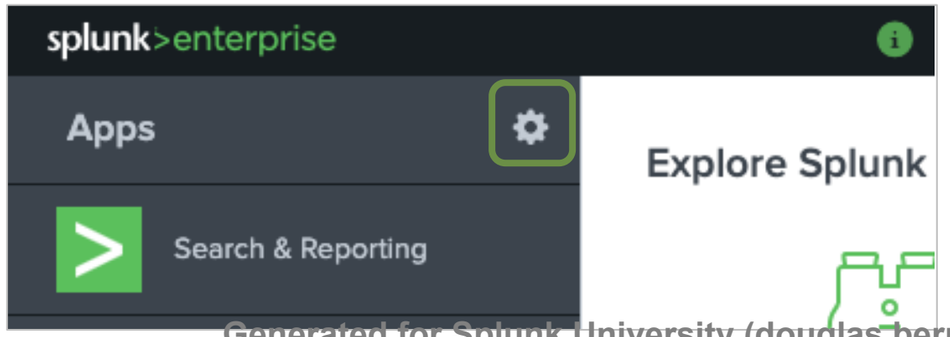
- Collection of configuration files, scripts, web assets, and so on
- May be focused on specific type of data, vendor, OS, industry, or business need
- May be installed on any Splunk instance
- May be included with Splunk (as a default app)



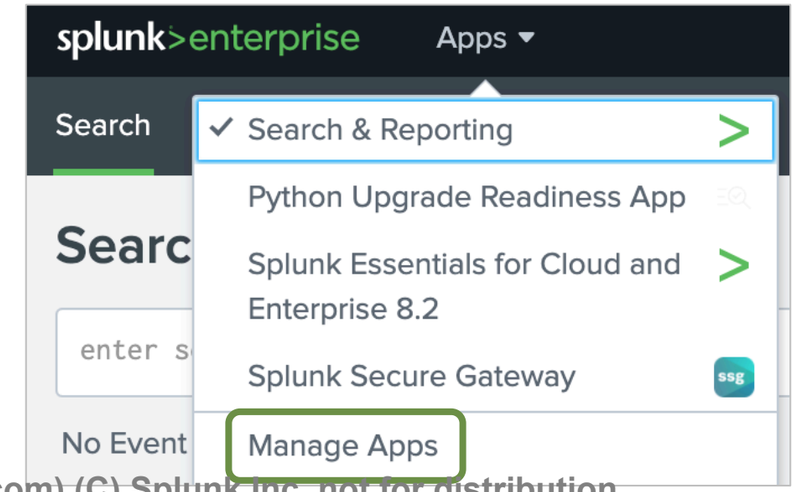
Viewing Installed Apps

- Apps are installed under **`SPLUNK_HOME/etc/apps`**
- Apps can be visible or hidden in Splunk Web
  - Several apps are installed by default
  - Internal apps used by Splunk should not be modified
- To manage apps in Splunk Web:

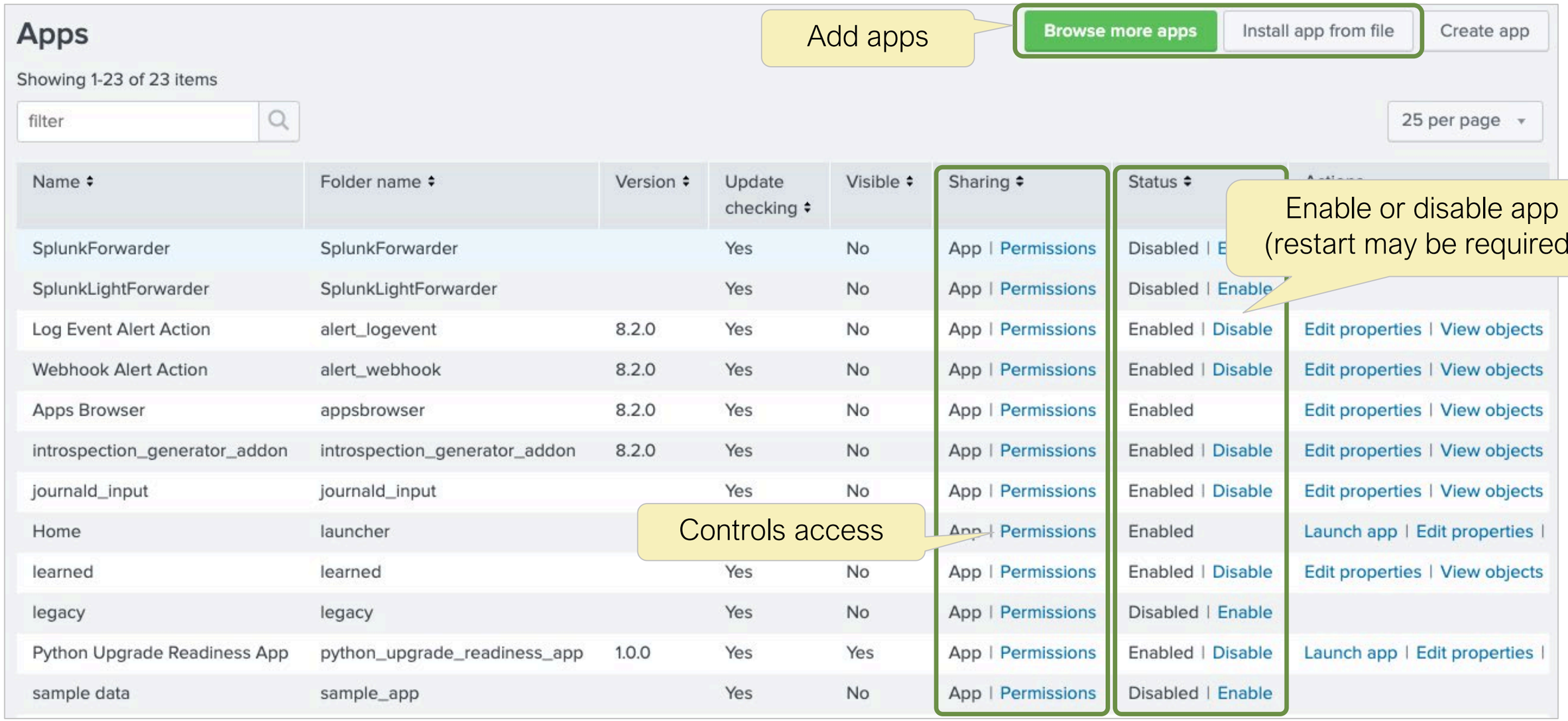
On the **Home** view



Within an app



Managing Apps



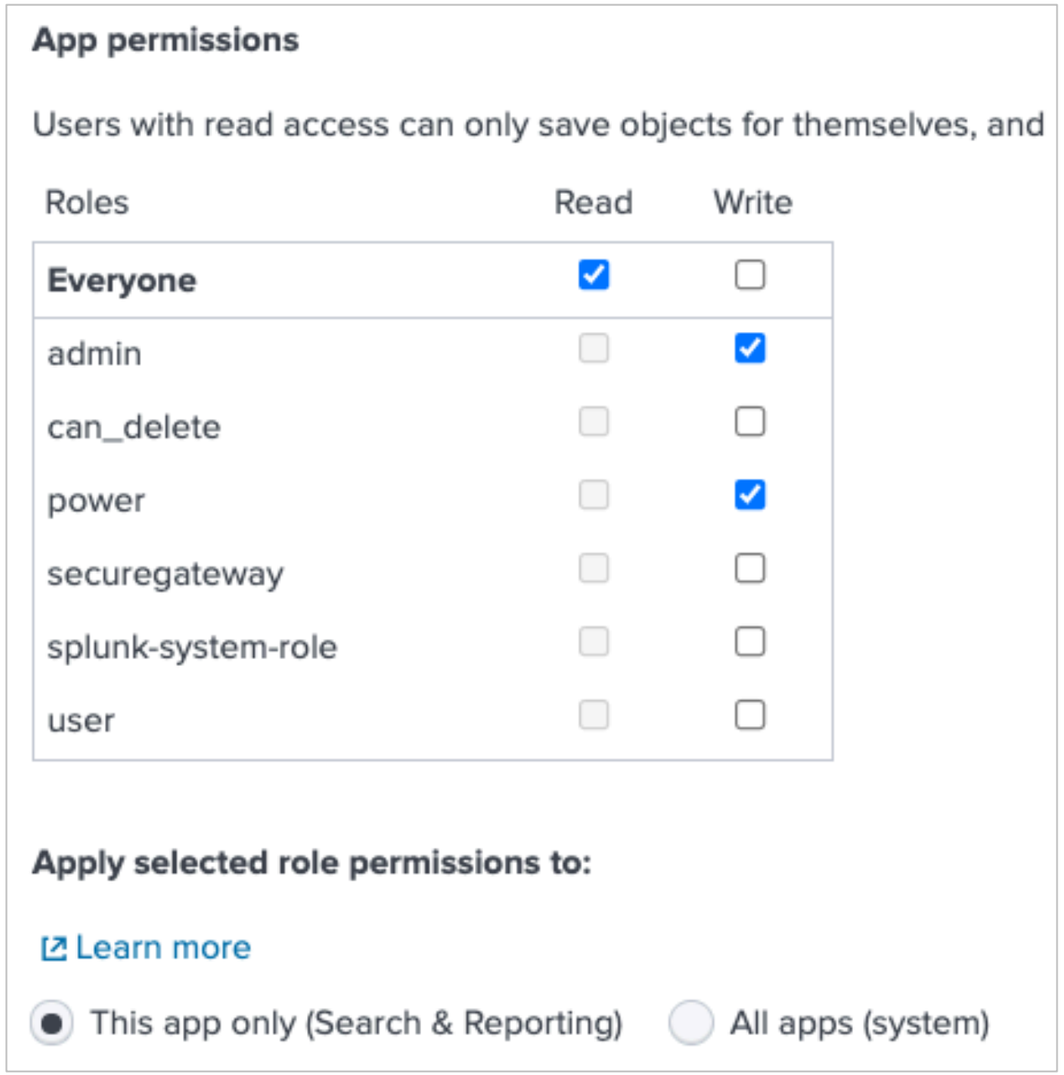
App Permissions

- User roles with **read** permission:
  - Can see the app and use it
  - Can add knowledge objects (KOs)
  - Can modify KOs they own
- User roles with **write** permission:
  - Can share KOs they own
  - Can delete KOs used in the app

Note

By default, the role "user" does not have write permissions within the search app.

Permissions on a KO generally take precedence over App permissions.



Installing an App from Splunkbase

1. From the **Apps** page, click **Browse more apps**, or click **Apps > Find More Apps**
   - Splunk Web will access http://splunkbase.splunk.com
2. Search for the app you want to install
3. Select **Install**
   - Most apps are free
   - Requires a splunk.com user ID and password
   - App is installed into **`SPLUNK_HOME/etc/apps`**
4. Restart Splunk, if required
5. Configure the app according to its documentation

Note

Anyone can sign up for a user account in splunk.com. A support contract is not required.

Installing an App From a File

1. Download the app from http://splunkbase.splunk.com
   - File format may be: **`.tar.gz`**, **`.tgz`**, **`.zip`**, **`.spl`**
2. Install the app using one of these methods:
   - **Splunk Web**: Click **Install app** from file
   - **Command line**:

```
# splunk install app <path-to-appfile>
```

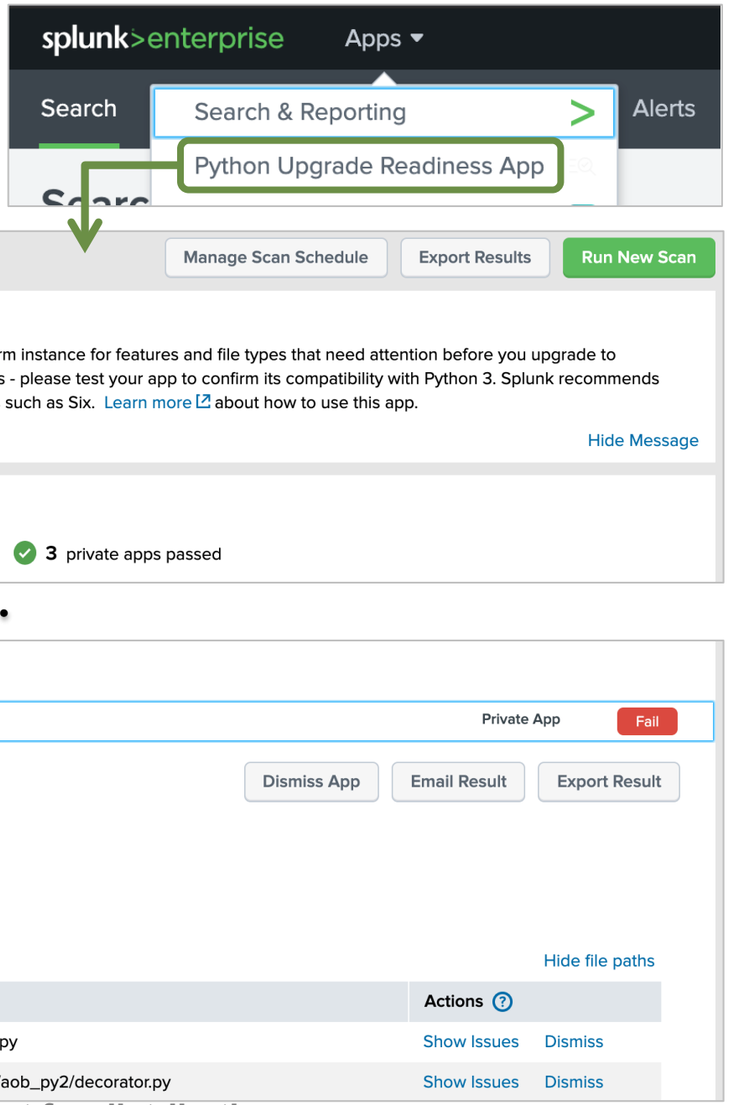
   - **Extract app** in proper location:

```
# cd SPLUNK_HOME/etc/apps
# tar -xf <path-to-appfile>
```

3. Restart Splunk, if required
4. Configure the app according to its documentation

Using the Python Upgrade Readiness App

- Scans Splunk 7.1 and later for app compatibility issues
  - Python 3 runtimes are default in Splunk 8.1+
- Installed by default starting in Splunk 8.2



What is an Add-on?

Splunk Add-on

- Reusable component supporting other apps
- Often used for data collection
- Any combination of configurations, scripts, data inputs, and so on
- Does **not** contain Splunk Web UI components (reports or dashboards)
- **Technology add-ons (TAs)**: specialized add-ons that help collect, transform, and normalize data feeds from specific sources

Description	Apps	Add-ons
Provides Splunk Web UI components (navigable interface, dedicated URL, visualize data)	✓	
Occupies a unique namespace within Splunk	✓	✓
Can be redistributed and shared using Splunkbase	✓	✓
Contains components intended for reuse by other apps		✓
Can depend on add-ons for correct operation	✓	✓

Apps / Add-ons on Forwarders

- Universal forwarders don't have a web interface, but may still benefit from an app
- Install the app on a forwarder using one of these methods:
  - **Command line** on the forwarder (**`splunk install app`**)
  - **Extract app** in proper location on the forwarder
  - **Use a deployment server** to deploy the app

Deleting an App

- Consider disabling or moving the app's files to another location
- When an app is deleted:
  - Configuration files and scripts are deleted from the Splunk server
  - User's private app artifacts remain untouched
  - The app can be reinstalled later
- To delete an app:
  1. Select one of these methods:
     - Run: **`splunk remove app <app_folder>`**
     - Navigate to **`SPLUNK_HOME/etc/apps`** and delete the app's folder and all its contents
  2. Restart the Splunk server

Warning

Deleting an app folder directly does not check for dependencies. Using the **`splunk remove app`** command is the preferred method.

Module 3 Knowledge Check

- True or False. Write permissions to an app means that the user's role is able to modify the app.
- True or False. Universal forwarders don't have a web interface, but they can still benefit from an app.

Module 3 Knowledge Check – Answers

- True or False. Write permissions to an app means that the user's role is able to modify the app.

  False. User roles with write permission can add/delete/modify knowledge objects used in the app

- True or False. Universal forwarders don't have a web interface, but they can still benefit from an app.

  True.

Module 3 Lab Exercise

Time: 10 minutes

Description: Install an App

Tasks:

- Explore Splunk apps on Splunkbase
- Download an app
- Install the class app
- Change the app permissions
- Verify if the app dashboard displays reports

Module 4:
Splunk Configuration Files

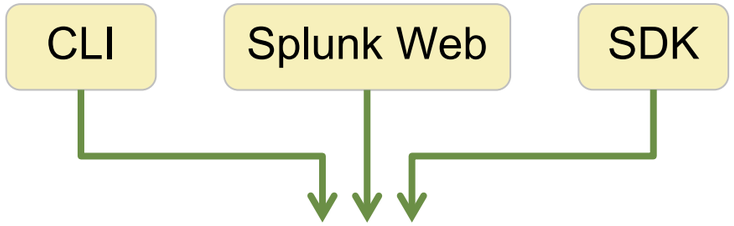
Module Objectives

- Describe Splunk configuration directory structure
- Understand configuration layering process
  - Index time process
  - Search time process
- Use **`btool`** to examine configuration settings

Splunk Configuration Files

Configuration Files (`.conf`)

- Govern an aspect of Splunk functionality
- Text files are generally case sensitive with **`[stanza]`** and **`attribute = value`** format
- Modified using Splunk Web, CLI, SDK, app install, or directly editing
- Saved under **`SPLUNK_HOME/etc`**
- Come with documentation and examples under **`SPLUNK_HOME/etc/system/README/`**



`inputs.conf`

```
[default]
host=www

[monitor:///var/log/httpd]
sourcetype = access_common
ignoreOlderThan = 7d
index = web
```

Note

For **`.conf`** file documentation and examples view **`SPLUNK_HOME/etc/system/README/`**:
- **`*.conf.spec`**
- **`*.conf.example`**

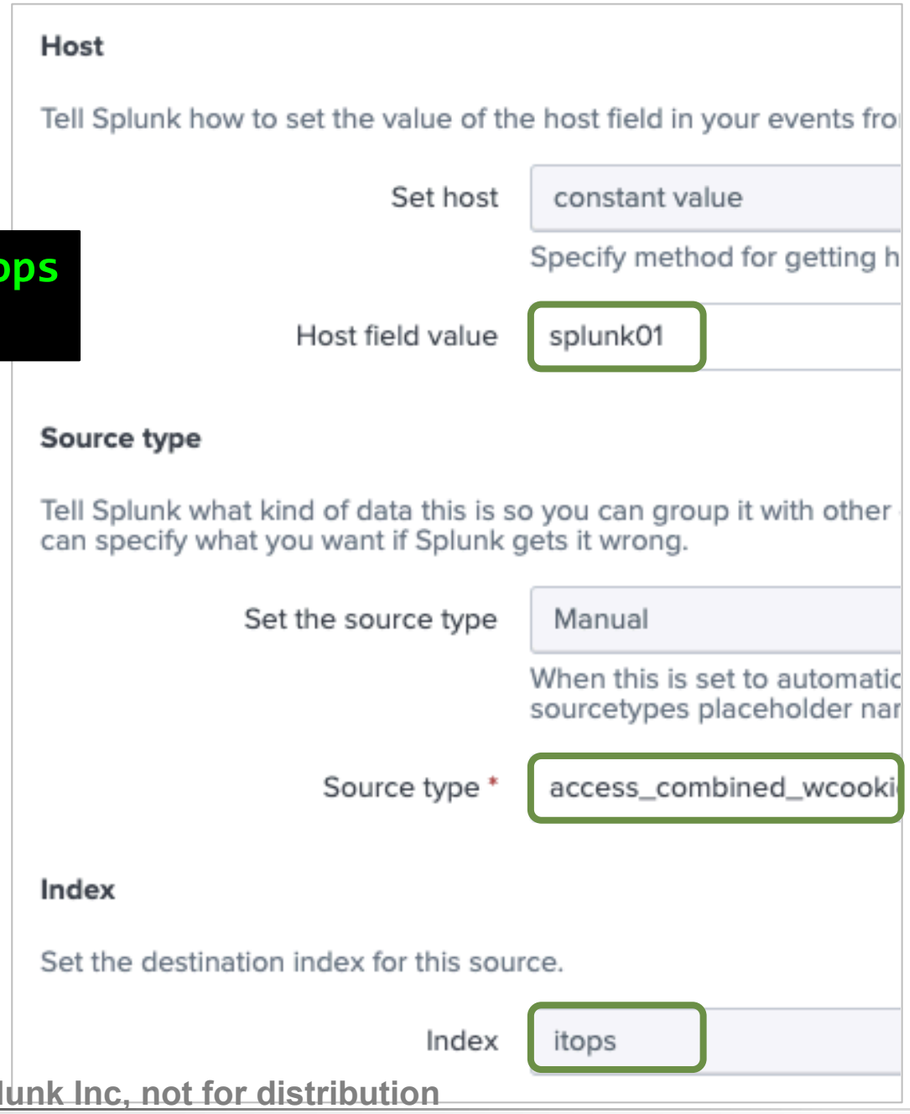
Methods for Modifying Splunk Configurations

- Splunk Web
- Splunk CLI

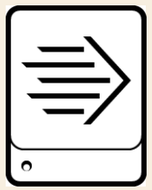
```
./splunk add monitor /opt/log/www1/access.log -index itops
   -sourcetype access_combined_wcookie -host splunk01
```

- Editing **.conf** files

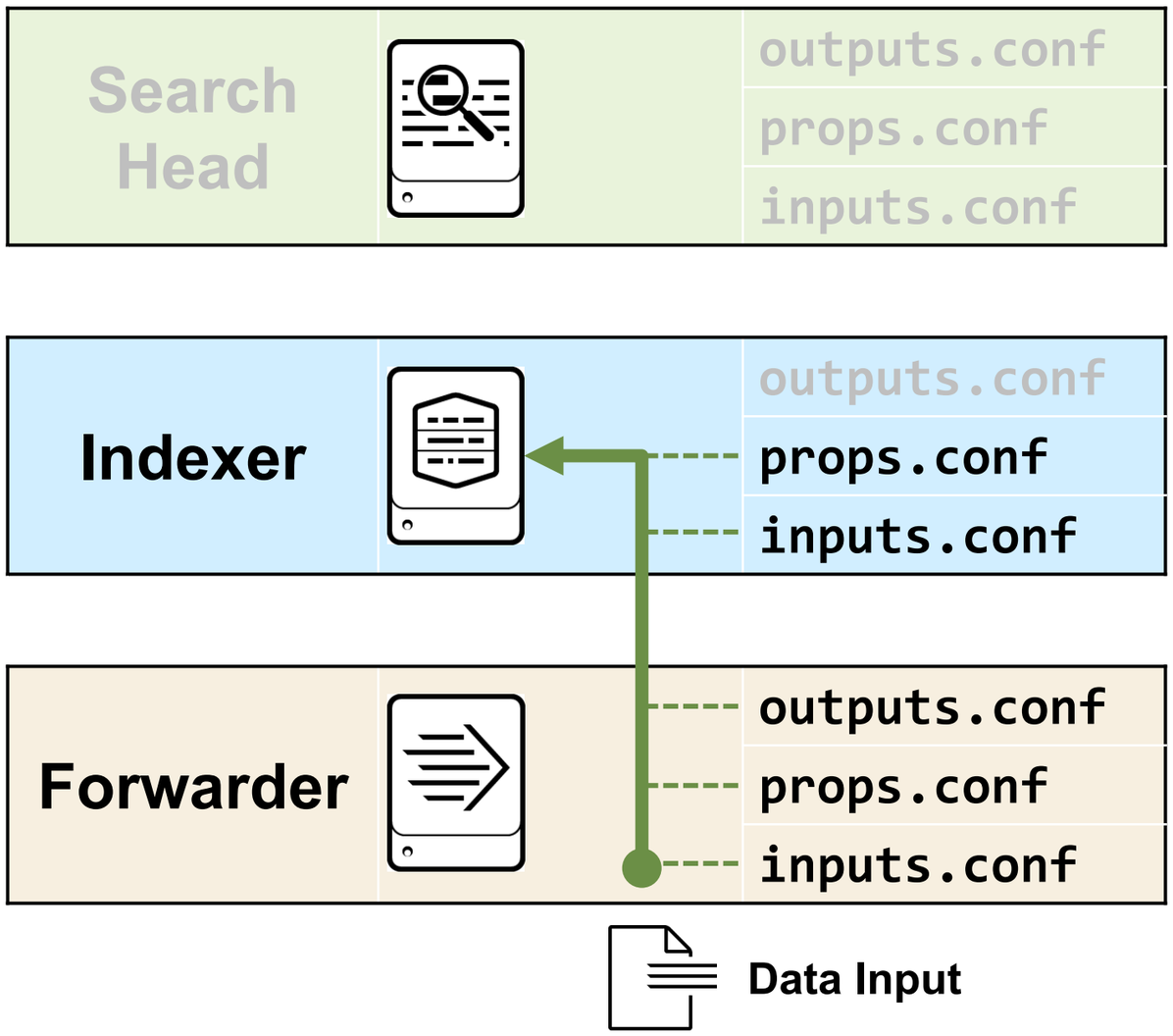
```
[monitor:///opt/log/www1/access.log]
disabled = false
host = splunk01
index = itops
sourcetype = access_combined_wcookie
```



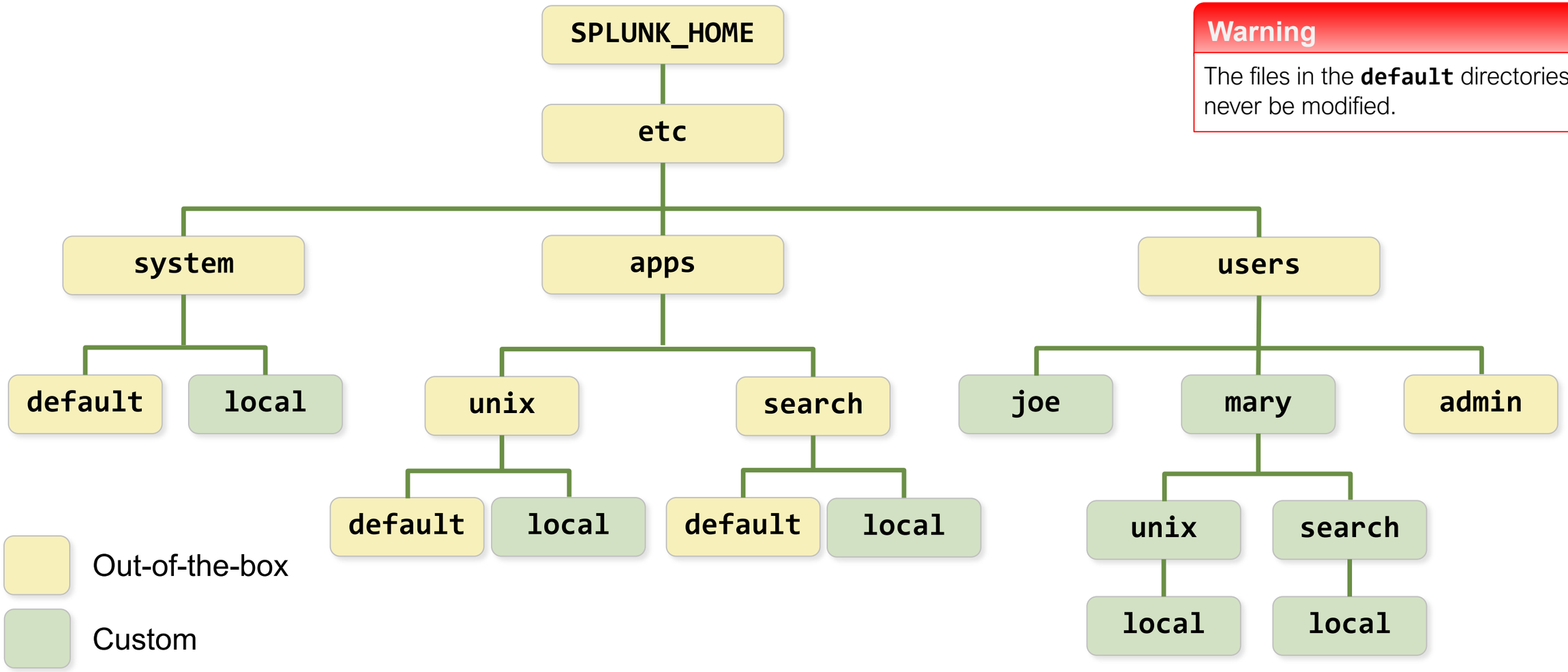
Commonly Used Splunk Configuration Files

Search Head		`outputs.conf`	Where to forward data
		`props.conf`	Search-time Field Extractions, lookups, and so on
		`inputs.conf`	What data is collected (*internal Splunk logs*)
Indexer		`outputs.conf`	Not generally needed
		`props.conf`	Parsing
		`inputs.conf`	What data is collected; Which ports to listen to
Forwarder		`outputs.conf`	Where to forward data
		`props.conf`	Limited parsing
		`inputs.conf`	What data is collected (*production data*)

Configuration Files Used During Data Input



Configuration Directories



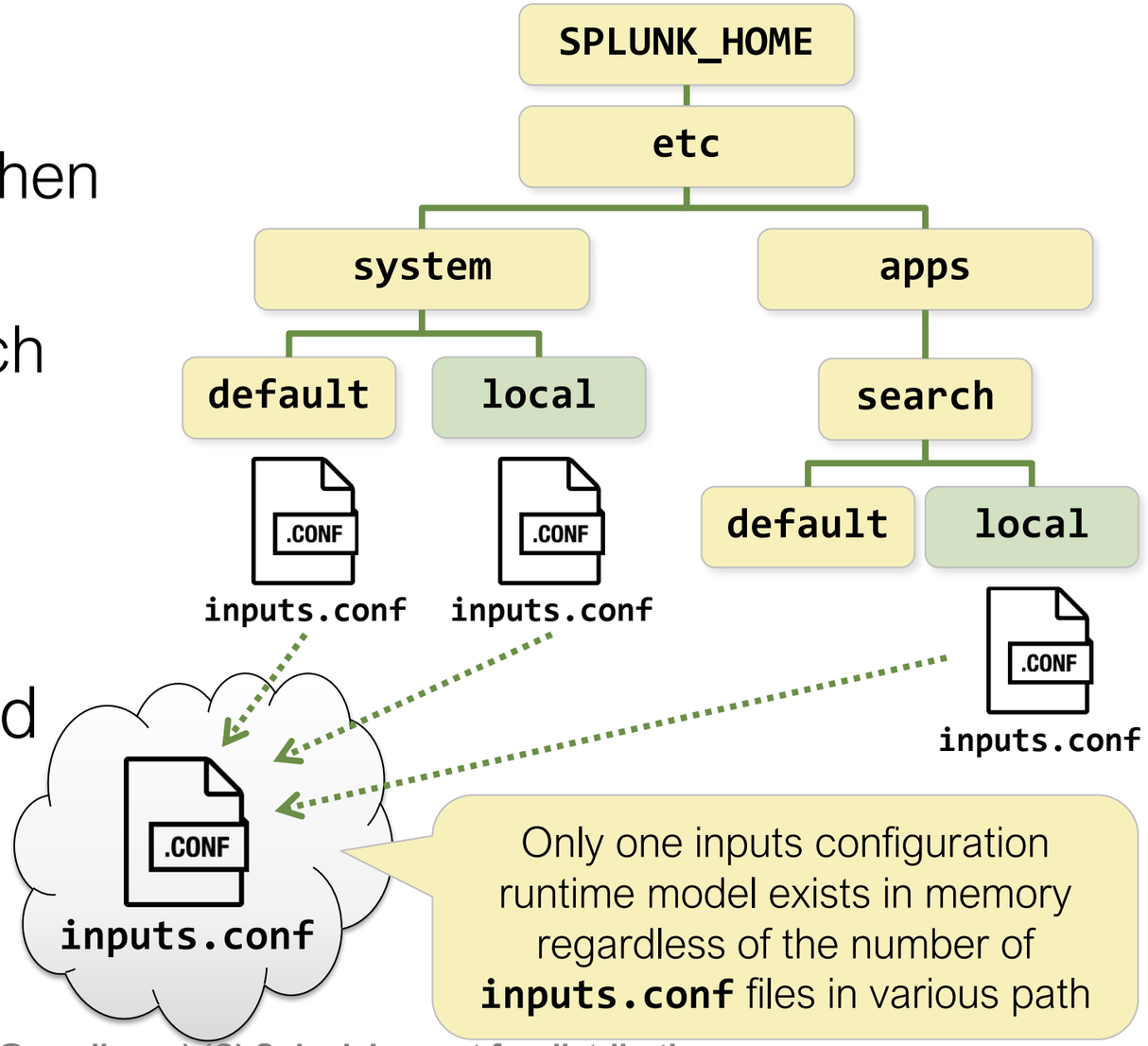
Warning

The files in the **default** directories must never be modified.

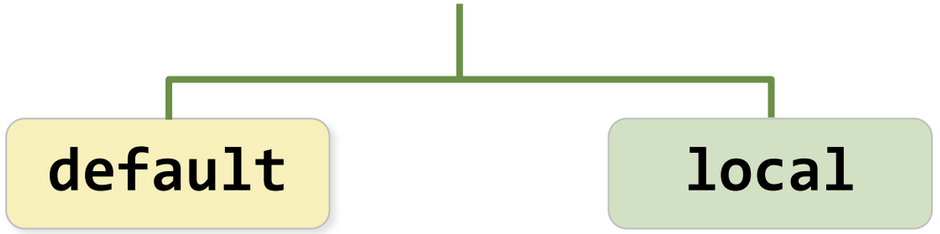
docs.splunk.com/Documentation/Splunk/latest/Admin/Listofconfigurationfiles

Merging of Configuration Files

- Splunk merges configuration files
  - Generally when Splunk starts, or when searches are run
  - Into a single run-time model for each file type
  - As a union of all files if no duplicates/conflicts exist
- In case of conflicts, priority is based on the context:
  - **Global context** (index-time)
  - **App/User context** (search-time)



Default versus Local Configuration



- Shipped with Splunk or app
- Overwritten on update
- Do not modify

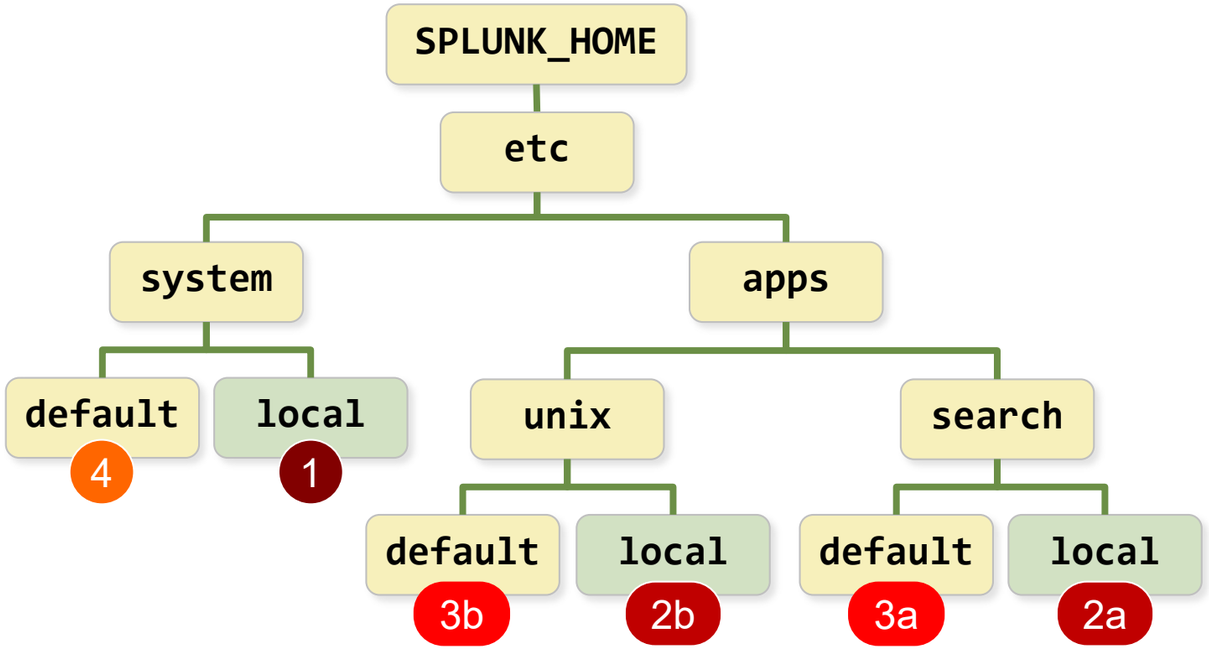
- Keeps your changes
- Preserved on update
- Only modify these versions
- Overrides **`default`** settings

File Context and Index-time versus Search-time

	Global Context	App/User Context
Used during:	**Index-time**	**Search-time**
Used by:	• User-independent tasks • Background tasks • Input, parsing, indexing	• User-related activity • Searching • Search-time processing
Example use-case:	A network input to collect syslog data	Mary's private report in the Search app
Example files:	**`inputs.conf`** **`outputs.conf`** **`props.conf`**	**`macros.conf`** **`savedsearches.conf`** **`props.conf`**

docs.splunk.com/Documentation/Splunk/latest/Admin/Wheretofindtheconfigurationfiles

Index-Time Precedence (Global Context)



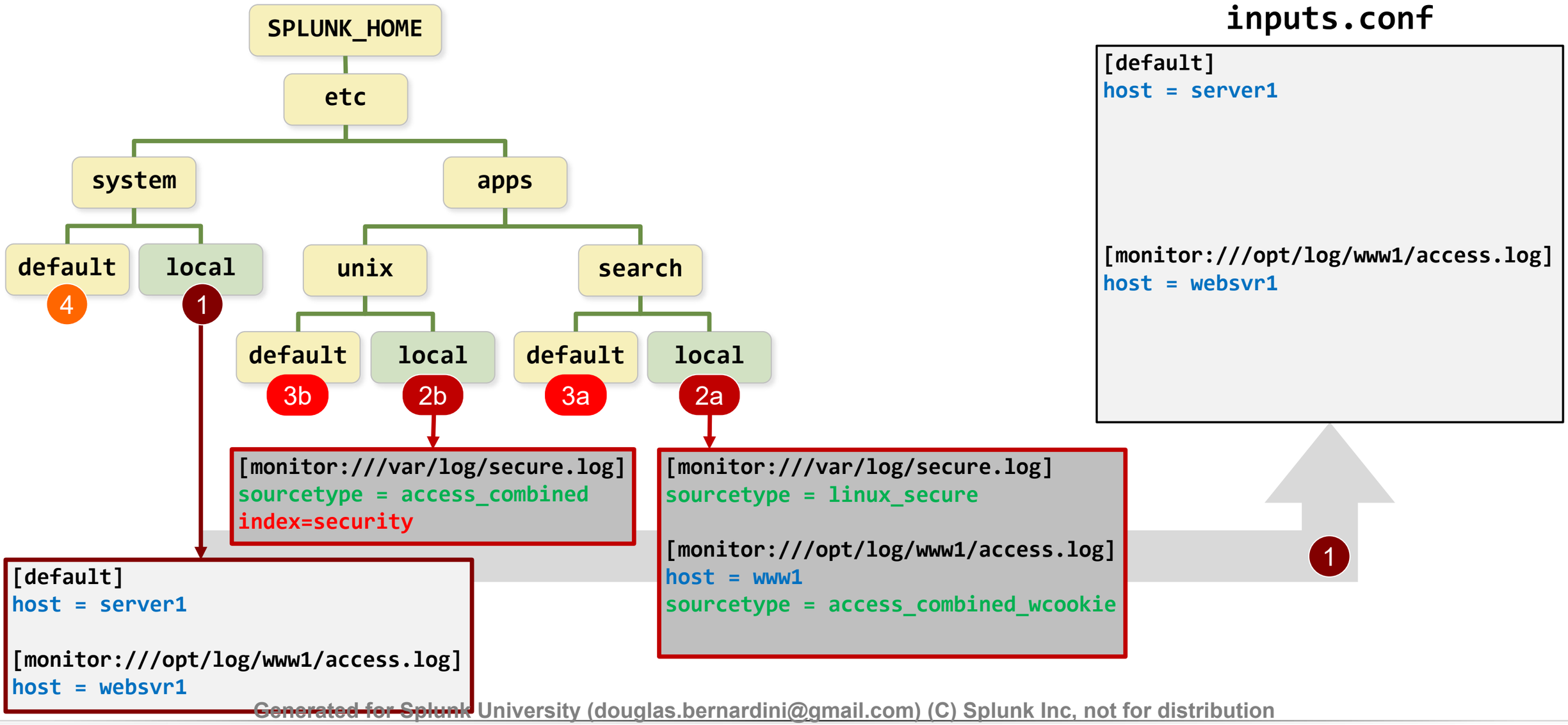
Precedence order

1. System local directory
   etc/system/local
2. App local directories*
   etc/apps/*appname*/local
3. App default directories*
   etc/apps/*appname*/default
4. System default directory
   etc/system/default

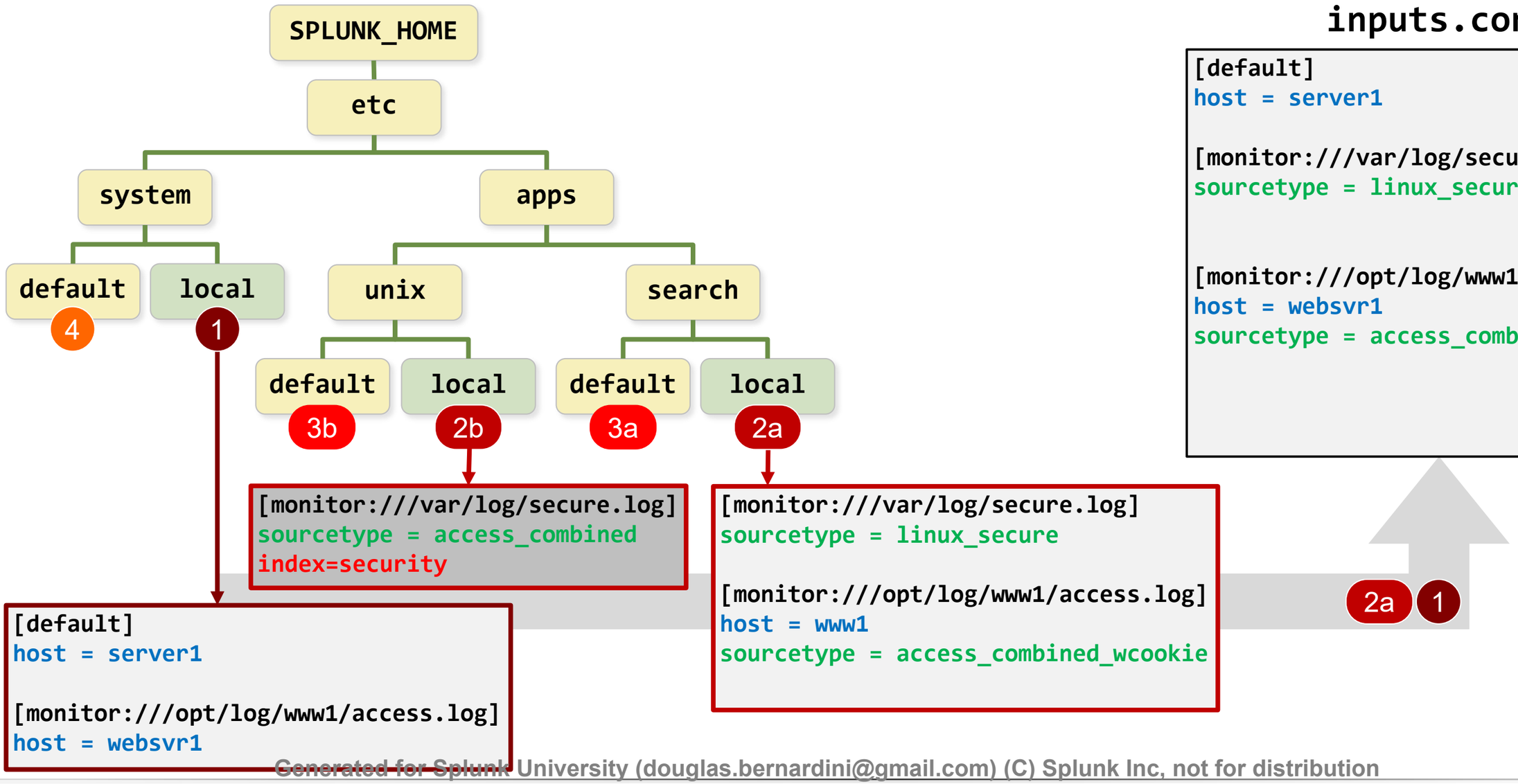
Note

* When determining priority of app directories in **global** context (for steps 2 and 3), Splunk uses *lexicographical* order. (Files in apps directory "A" have higher priority than files in apps directory "B".)

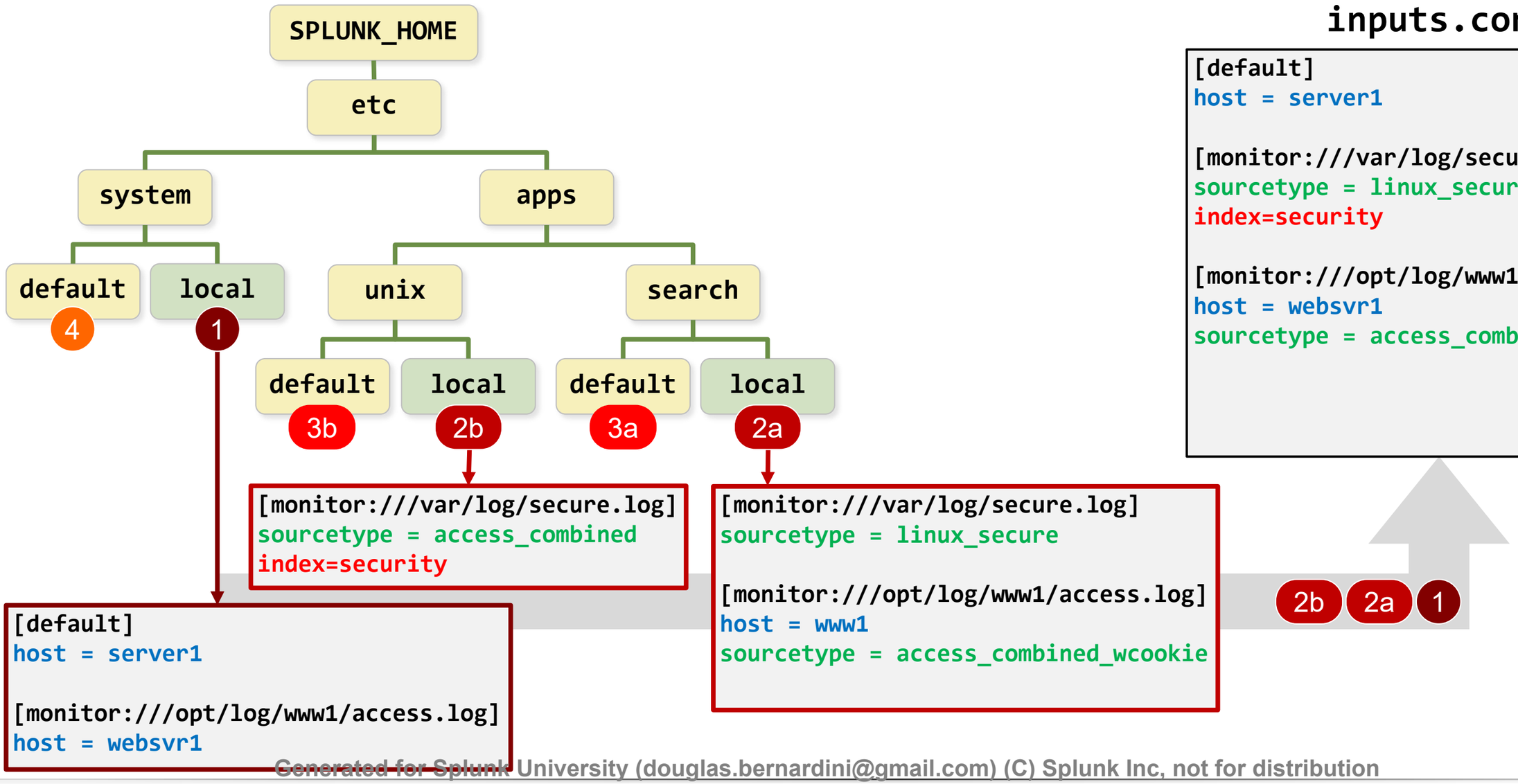
Example of Index-Time Precedence (1)



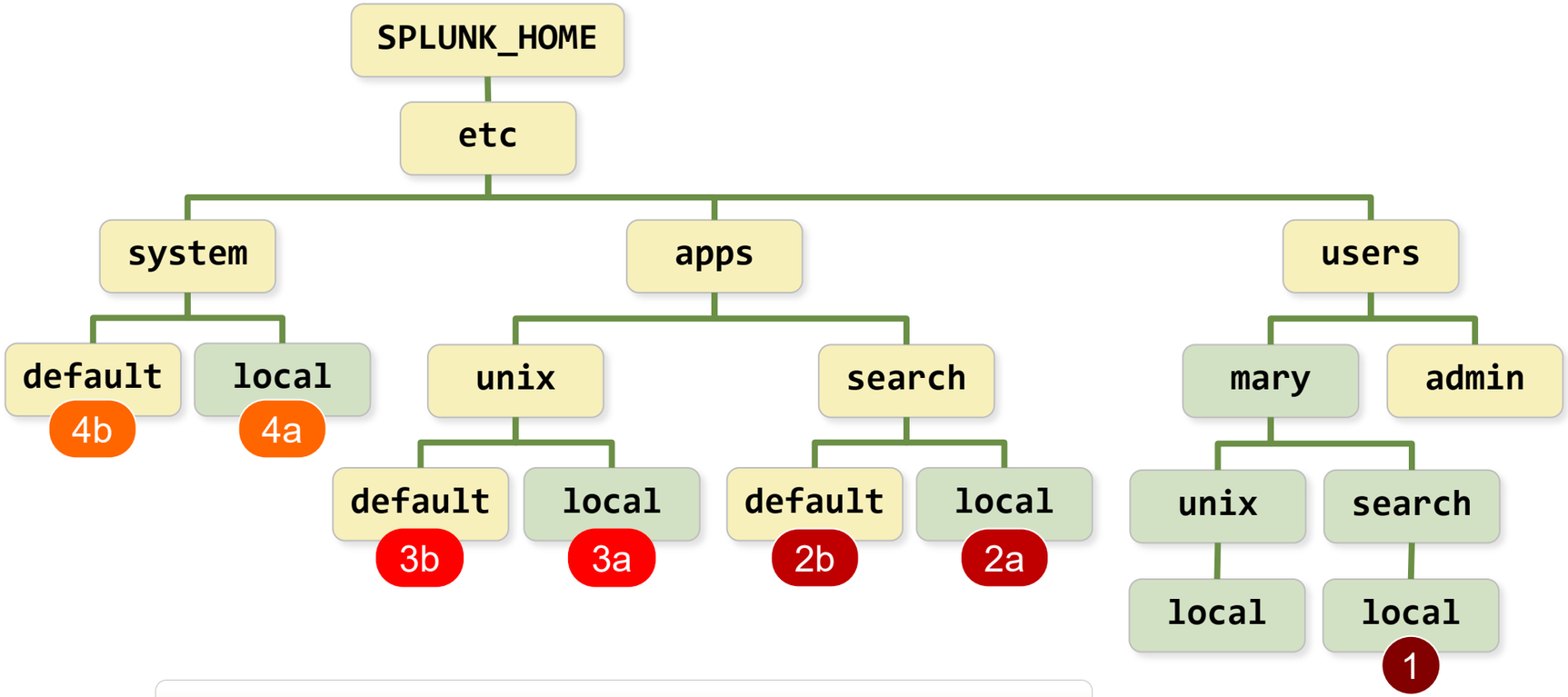
Example of Index-Time Precedence (2)



Example of Index-Time Precedence (3)



Search-Time Precedence (App/User Context)



Precedence order

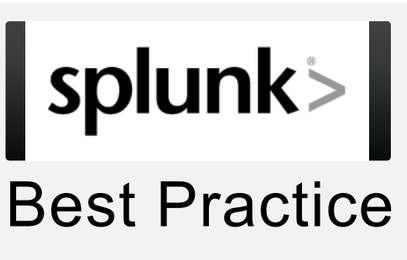
1. Current user directory for app
   etc/users/*user*/*appname*/local
2. App directory - running app
   etc/apps/*appname*/local
   etc/apps/*appname*/default
3. App directories - all other apps*
   etc/apps/*appname*/local
   etc/apps/*appname*/default
4. System directories
   etc/system/local
   etc/system/default

Note

* If objects from the app are exported globally with **.meta** file setting, evaluate all other app directories using *reverse lexicographical* order. (Files in apps directory "B" have higher priority than directory "A".)

Configuration Best Practices

- Avoid storing configurations in **`SPLUNK_HOME/etc/system/local`**
  - Local context settings will *always* take precedence
  - Attempting to override index-time settings in an app will fail
  - Managing these settings with a deployment server is impossible
- Create an app to manage system settings
  - Allows you to manage settings with a deployment server
  - Manage system configurations in an app (e.g. **`DC_app`**) under **`SPLUNK_HOME/etc/apps/<appname>/local`**
  - Refer to the *Splunk Enterprise Data Administration* course



Validating the Splunk configuration

Validating the on-disk configuration

- Performed with **`splunk btool`** CLI
- Syntax: **`splunk btool <conf_file> list`**
- Example: **`splunk btool inputs list`**

Validating the in-memory configuration

- Performed with **`splunk show config`** CLI or REST API
- Syntax: **`splunk show config <conf_file>`**
- Example: **`splunk show config inputs`**

Configuration Validation with **btool**

- **splunk btool <*conf-name*> list [*options*]**
  - Shows on-disk configuration for requested file
  - Useful for checking the configuration scope and permission rules
  - Run **splunk btool check** each time Splunk starts
    - Use **--debug** to display the exact **.conf** file location
    - Add **--user= <*user*> --app=<*app*>** to see the user/app context layering
- Examples:

```
splunk help btool
splunk btool check
splunk btool inputs list
splunk btool inputs list monitor:///var/log
splunk btool inputs list monitor:///var/log --debug
```

docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/Usebtooltotroubleshootconfigurations

Example using **btool**

Scenario: What are the **/var/log/secure.log** input configurations and where are they specified?

```
> splunk btool inputs list monitor:///var/log/secure.log --debug

  etc/apps/search/local/inputs.conf    [monitor:///var/log/secure.log]
  system/local/inputs.conf             host = server1
  etc/apps/unix/local/inputs.conf      index = security
  etc/apps/search/local/inputs.conf    sourcetype = linux_secure
```

etc/apps/unix/local/inputs.conf

```
[monitor:///var/log/secure.log]
sourcetype = access_combined
index = security
```

etc/apps/search/local/inputs.conf

```
[monitor:///var/log/secure.log]
sourcetype = linux_secure
```


Overriding Defaults

- Override settings in the **`local`** directory at the same scope
  - Do not modify the **`default`** directory version of the **`.conf`** file
  - Do not make a copy of the entire configuration file
  - Only include stanzas and settings you are overriding:
    - **Addition**: Add the new setting with its value
    - **Modification**: Place the existing setting with its new value
    - **Deletion**: Place the existing setting with a non-value
- Example: To disable the attribute **`TRANSFORMS`** for stanza **`[syslog]`**:

```
# etc/system/default/props.conf
[syslog]
TRANSFORMS = syslog-host
REPORT-syslog = syslog-extractions
...
```



```
# etc/system/local/props.conf
[syslog]
TRANSFORMS =
```

Reloading Configuration Files After Edit

- Changes made using Splunk Web or the CLI may not require restart
  - A message appears if restart is required (i.e. changing server settings)
- Changes made by editing **`.conf`** files are not automatically detected
- To force reload, go to **`http://servername:webport/debug/refresh`**
  - Reloads many of the configurations, including **`inputs.conf`**, but not all
- To reload all configurations, restart Splunk
  - Splunk Web: **Settings > Server controls > Restart Splunk**
  - CLI: **`splunk restart`**

Note

A Splunk refresh is only valid for standalone configuration or a search head.

Module 4 Knowledge Check

- Which configuration file tells a Splunk instance to ingest data?
- True or False. **`btool`** shows on-disk configuration for requested file
- True or False. The best place to add a parsing configuration on an indexer would be **`SPLUNK_HOME/etc/system/local`** directory as it has the highest precedence.

Module 4 Knowledge Check – Answers

- Which configuration file tells a Splunk instance to ingest data?

  inputs.conf

- True or False. **btool** shows on-disk configuration for requested file.

  True.

- True or False. The best place to add a parsing configuration on an indexer would be the **SPLUNK_HOME/etc/system/local** directory, as it has the highest precedence.

  False. Best practice is to put the configuration in an *app's* **local** directory (**SPLUNK_HOME/etc/apps/<*appname*>/local**).

Module 4 Lab Exercise

Time: 10 minutes

Description: Examine User Configuration files

Tasks:

- Run the same search as different users
- Check the search results and compare
- Use the **`btool`** command to investigate configurations

Module 5:
Splunk Indexes

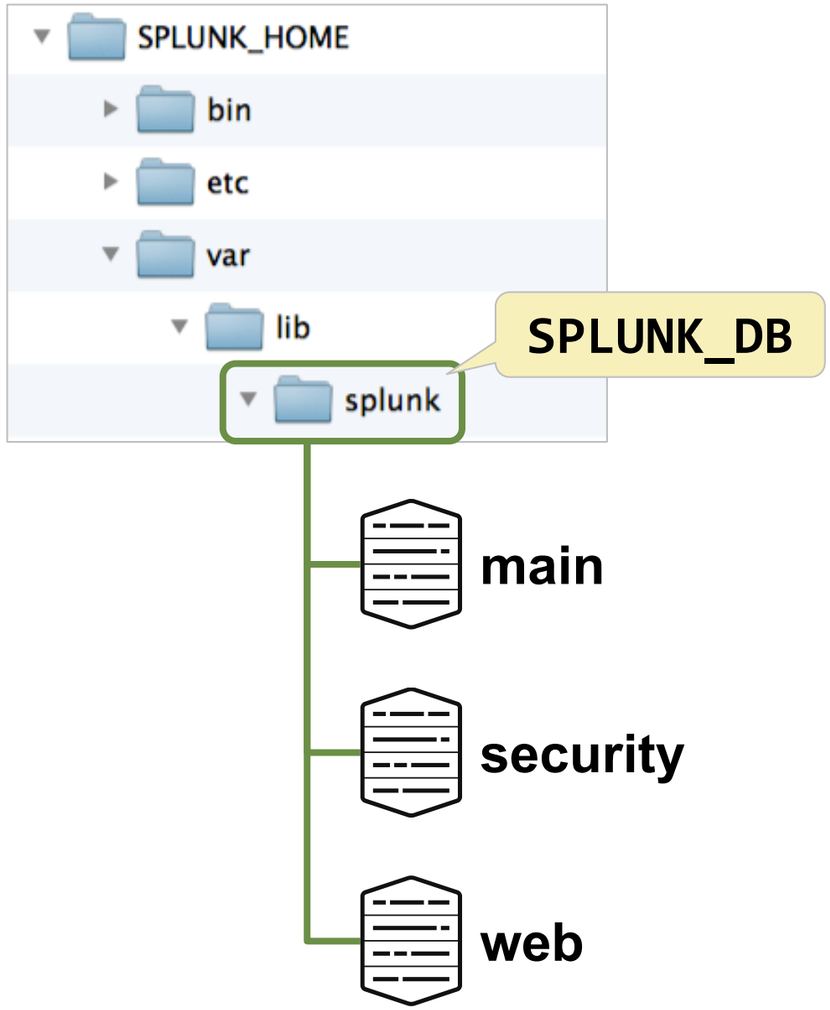
Module Objectives

- Learn how Splunk indexes function
- Identify the types of index buckets
- Add and work with indexes
- Overview of metrics index

What are Indexes?

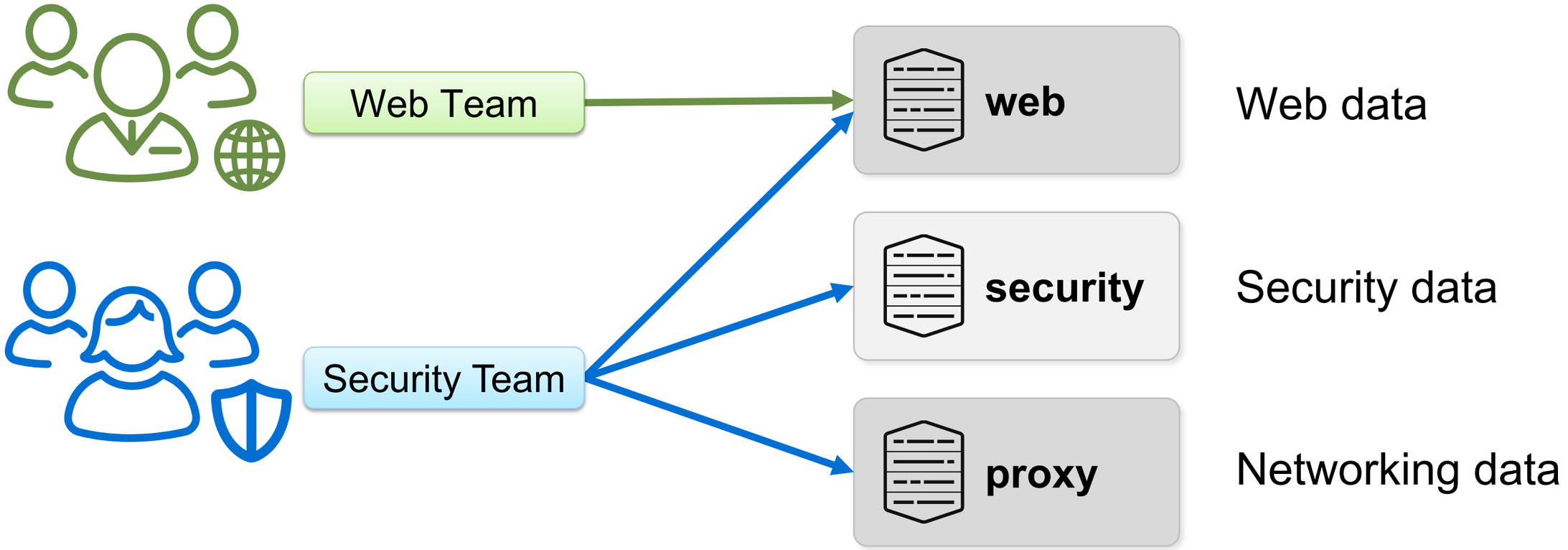
Splunk Indexes

- Store input data as events
- Included with Splunk (**`main`**, **`_internal`**)
- Can be created by a Splunk administrator
- Can be used to limit scope of a search
- Allow the ability to limit access by user
- Found by default under **`SPLUNK_DB`** (**`SPLUNK_HOME/var/lib/splunk`**)



Indexes and Access Control

- Access control is set per index
- Segregate events into indexes to limit access by Splunk role



Indexes and Retention

- Retention policy is set per index
  - Only one retention policy can be set per index
- Separate events into different indexes based on desired retention

Events	Index	Retention policy
Web events	**web**	Keep for 6 months → Delete
Security events	**security**	Keep for 12 months → Archive
Proxy events	**proxy**	Keep for 6 weeks → Delete

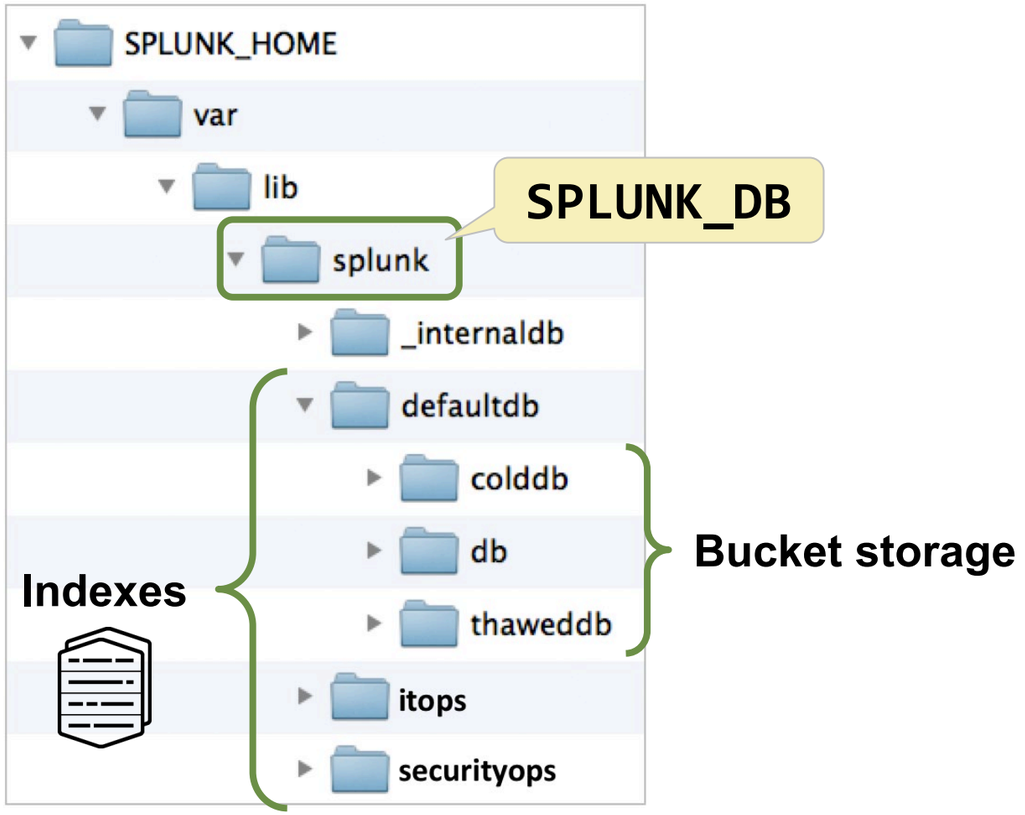
Preconfigured Indexes (Partial List)

Index name	Purpose
_internal	To index Splunk's own logs and metrics
_audit	To store Splunk audit trails and other optional auditing information
_introspection	To track system performance, Splunk resource usage data, and provide Monitoring Console (MC) with performance data
_thefishbucket	To contain checkpoint information for file monitoring inputs
summary	Default index for summary indexing system
main	Default index for inputs; located in the **defaultdb** directory

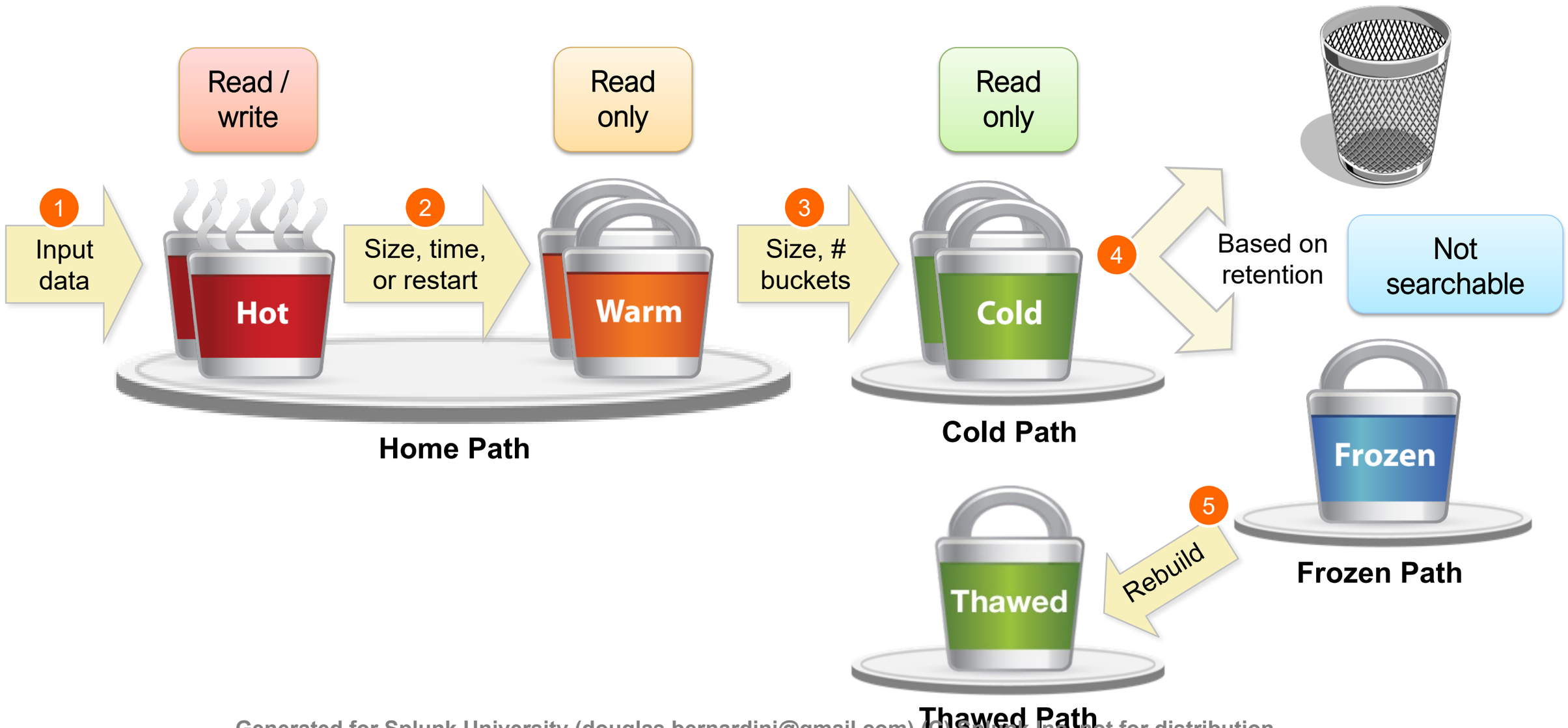
What are Buckets?

Buckets

- Part of an index that stores events
- A directory containing a set of raw data and associated index files
- Have a maximum data size and a time span, that can both be configured
- Discussed in detail: http://wiki.splunk.com/Deploy:UnderstandingBuckets

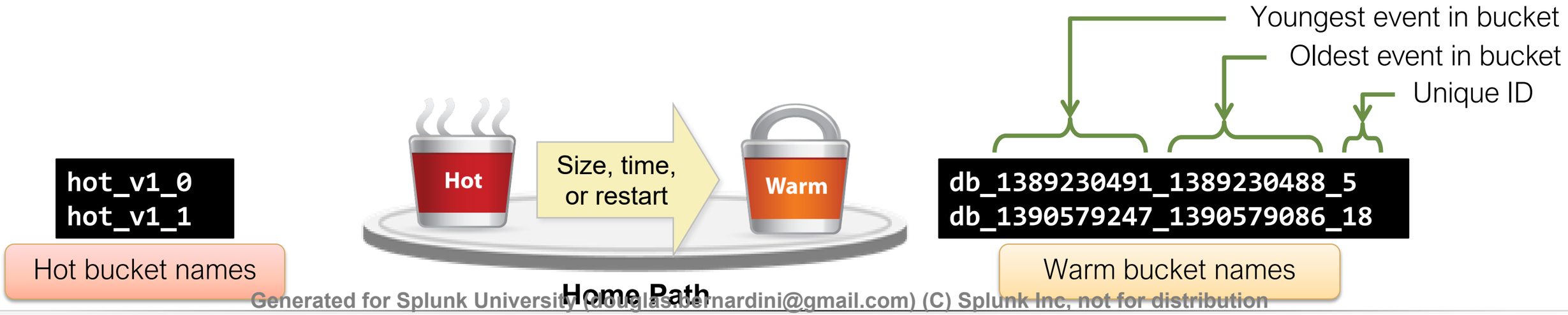


Data Flow Through an Index



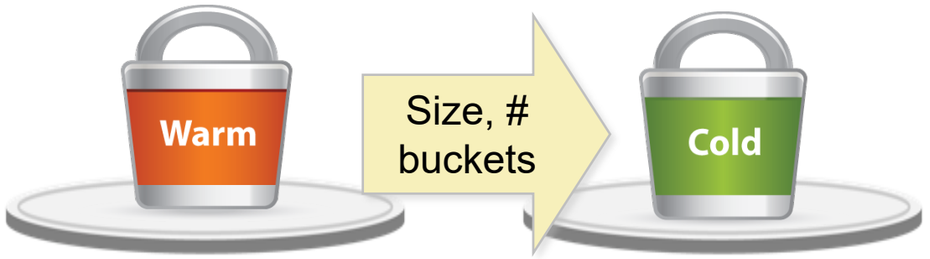
Hot and Warm Buckets

- Splunk input data is ingested: read, parsed, goes through the license meter, and is written to a hot bucket
- Hot and warm buckets are stored in the **Home Path**
- Hot buckets roll over to a warm bucket:
  - When they reach max size or time span, or when the indexer is restarted
  - By being renamed to identify the time range of the contained events



Warm and Cold Buckets

- Warm buckets roll over to a cold bucket:
  - When the **Home Path** maximum size (default: 0 / unconstrained) or the maximum warm bucket count (default: 300 buckets) is reached
  - By moving the oldest Warm bucket to the **Cold Path**
  - Preserving the bucket name
- At search time, Splunk scans the time range on a bucket name to determine whether to open the bucket and search its events




```
db_1389230491_1389230488_5
db_1390579247_1390579086_18
```

Cold bucket names

Retention, Deletion, and Frozen Buckets

- Oldest bucket is deleted when:
  - All events in the bucket exceed the time retention limit (default: 6 years)
  - Index's "**Max Size of Entire Index**" value is reached (default: ~500 GB)
    - Splunk never exceeds this size, and will delete buckets prior to the retention limit
- Optionally configure the **Frozen Path**
  - Splunk copies bucket's raw data here before deletion
  - Frozen buckets are not searchable
- Frozen data can be brought back (thawed) into Splunk if needed

Estimating Index Growth Rate

- Splunk compresses the event's raw data as it is indexed
  - Indexing components are added to each bucket
  - Events with many searchable terms → **Larger index**
  - Events with fewer searchable terms and less variety → **Smaller index**
- **Best practice**:
  - Get a good growth estimate
  - Input your data in a test/dev environment over a sample period
    - If possible, index more than one bucket of events
  - Examine the size of the index's **db** directory compared to the input
    - MC: **Indexing > Indexes and Volumes > Index Detail: Instance**

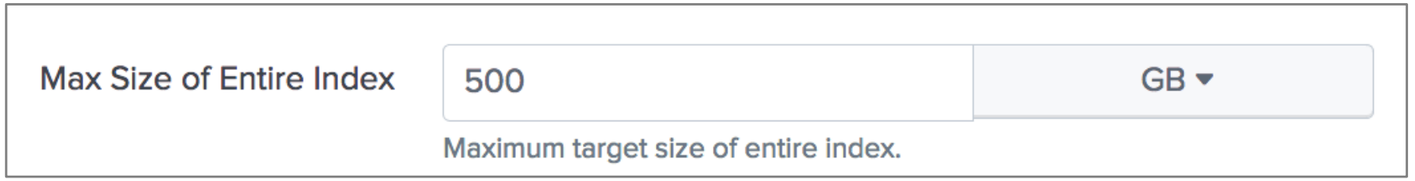
docs.splunk.com/Documentation/Splunk/latest/Capacity/Estimateyourstoragerequirements

Calculating Index Storage

- Limiting size on disk is the most common method of controlling index growth
- Allocate disk space to meet data retention needs, using:
  - **Daily rate** of input
  - **Retention period** (in days)
  - **Compression factor** (~50% = %15 raw data + 35% for Splunk indexing)
  - **Padding** (50 GB recommended)

Daily rate	x	Retention Period	x	Compress Factor	+	Padding	=	Total
5 GB/day	*	**180 days**	*	**0.5**	+	**50 GB**	=	**500 GB**

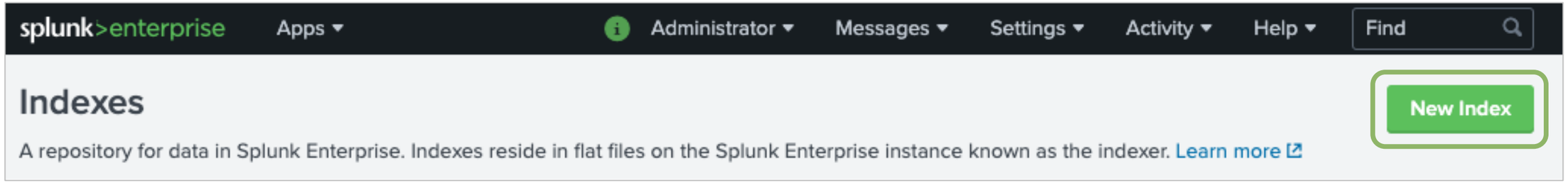
- Configure index:



- On average, data for this index is deleted or frozen after ~6 months

Adding an Index

- Requires administration rights
- Using Splunk Web:
  - **Settings > Indexes > New Index**

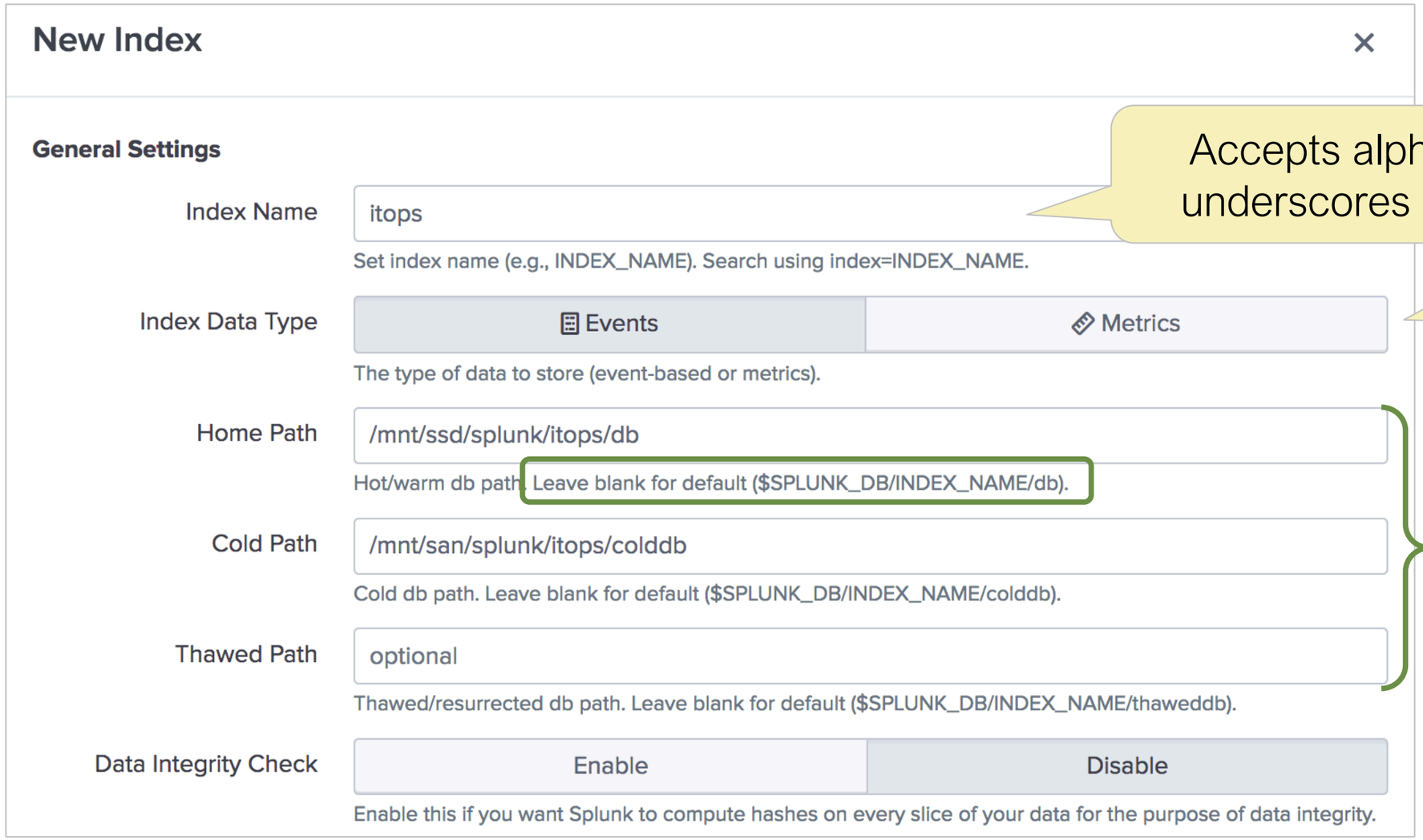


- Using command line:

  splunk add index <*index_name*> [-app <*app_context*>]

- Refer to:
  docs.splunk.com/Documentation/Splunk/latest/Indexer/SetupMultipleIndexes

Adding an Index With Splunk Web



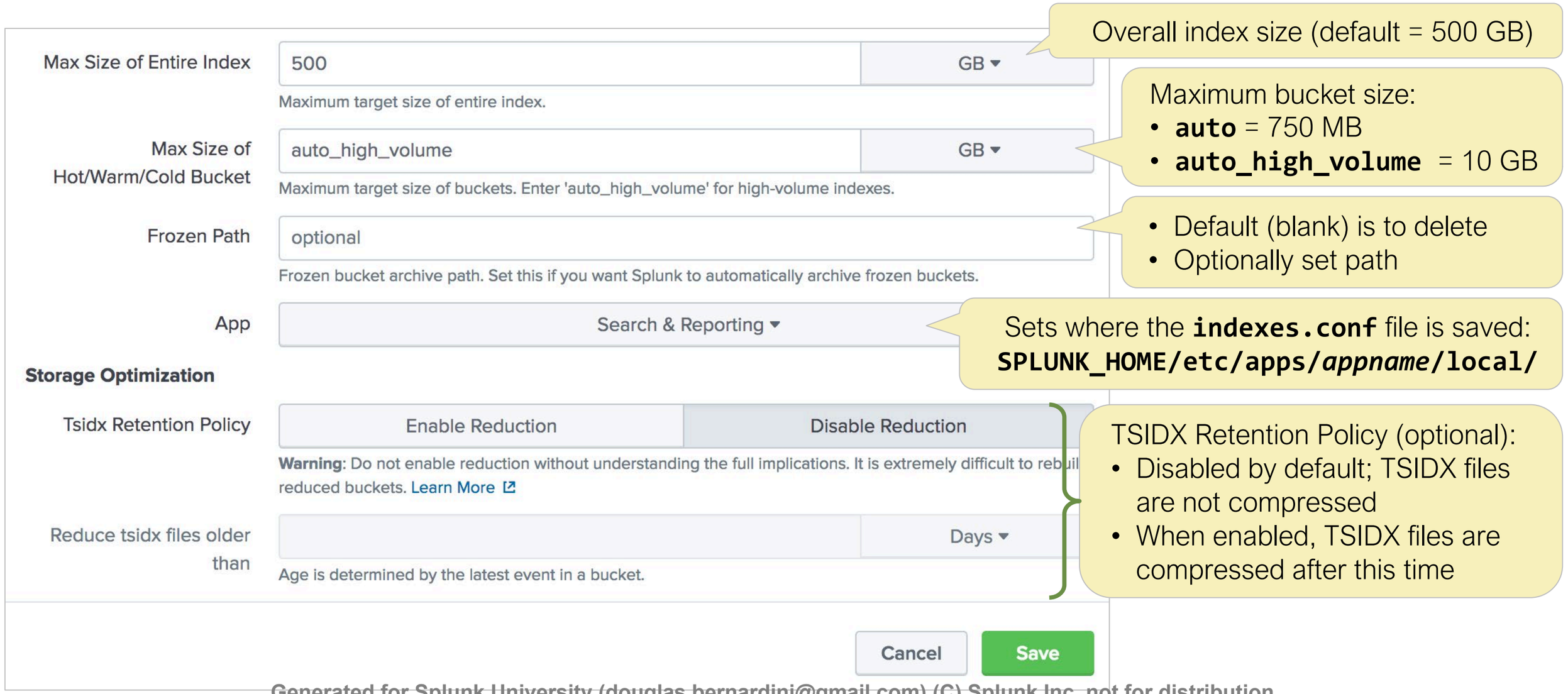
Accepts alphanumeric, hyphens, and underscores (except at the beginning)

Events is the default index data type

Locations of buckets:
- Hot + Warm
- Cold
- Thawed

Optional data integrity check

Adding an Index With Splunk Web (cont.)



Overall index size (default = 500 GB)

Maximum bucket size:
- **`auto`** = 750 MB
- **`auto_high_volume`** = 10 GB

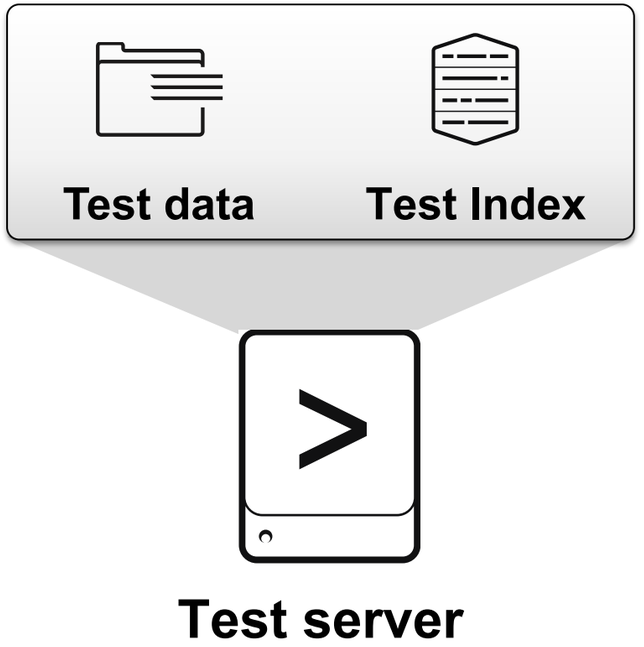
- Default (blank) is to delete
- Optionally set path

Sets where the **`indexes.conf`** file is saved:
`SPLUNK_HOME/etc/apps/`*`appname`*`/local/`

TSIDX Retention Policy (optional):
- Disabled by default; TSIDX files are not compressed
- When enabled, TSIDX files are compressed after this time

Initial Data Input Testing

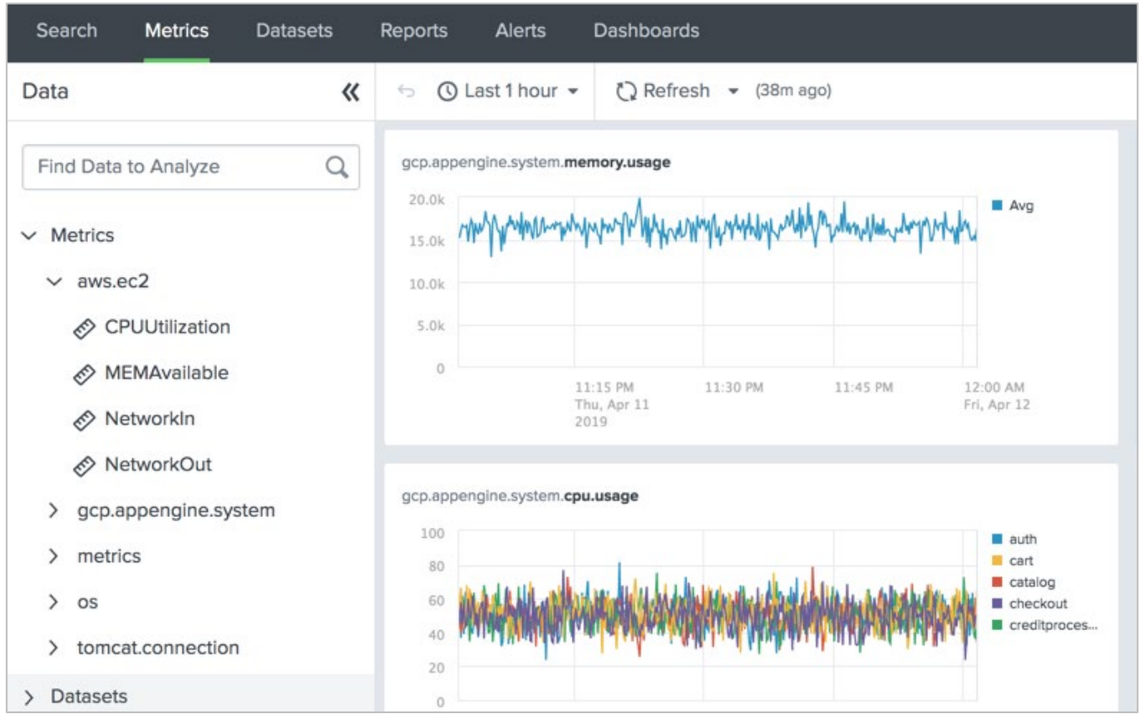
- Use a Splunk test server
  - Should be running same version as production
- Use test indexes
- Procedure:
  1. Copy production data to test server
  2. Use Splunk Web > **Add Data**
  3. Check to see if **sourcetype** and other settings are applied correctly
  4. Delete the test data, change your test configuration, and repeat as necessary

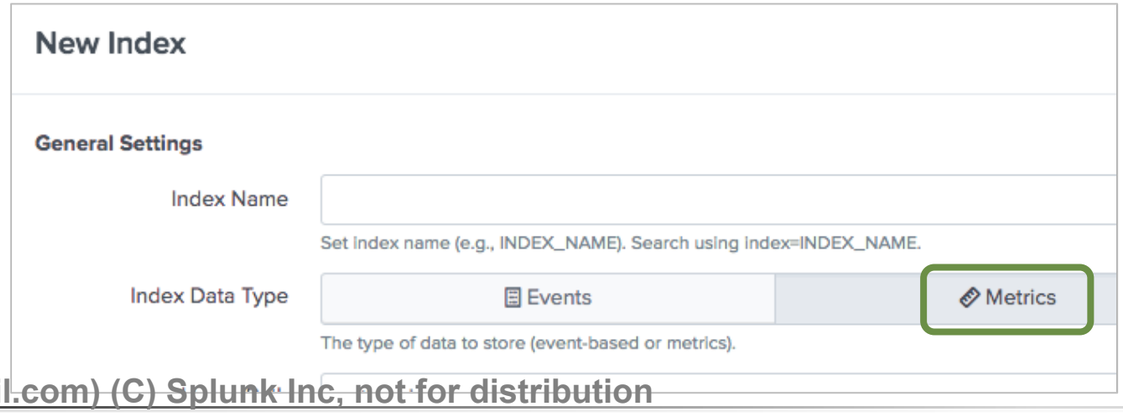


What are Metrics?

Metrics

- Set of structured and numeric measurements containing **timestamp**, **metric name**, **value**, and a **dimension**
- Uses a custom index type (“Metrics”), optimized for metric storage + retrieval
- Discussed in detail in the Working with Metrics in Splunk course





Module 5 Knowledge Check

- True or False. Splunk, by default, automatically sets the frozen path when you create an index.
- True or False. When hot buckets roll to warm, they go to a different directory.
- True or False. **`_introspection`** index tracks system performance and Splunk resource usage data.

Module 5 Knowledge Check – Answers

- True or False. Splunk, by default, automatically sets the frozen path when you create an index.

  False. Frozen path is not set by default. Data is set to delete by default.

- True or False. When hot buckets roll to warm, they go to a different directory.

  False, Hot and warm buckets stay in the same directory by default. When hot buckets roll to warm, they are renamed.

- True or False. **`_introspection`** index tracks system performance and Splunk resource usage data.

  True.

Module 5 Lab Exercise

Time: 10 minutes

Description: Add and test indexes

Tasks:

- Create a new index: **`securityops`**
- Add a file monitor input to send events to the **`securityops`** index

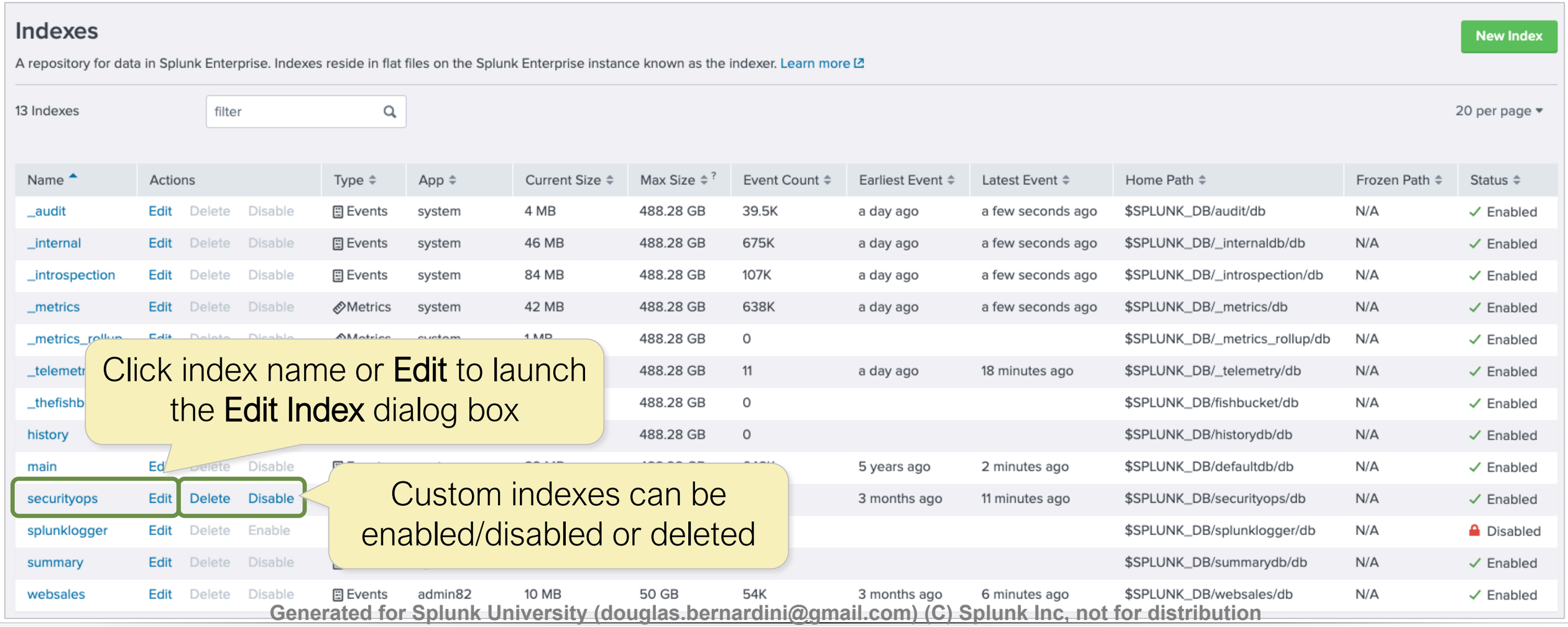
Module 6:
Splunk Index Management

Module Objectives

- Review Splunk Index Management basics
- Identify data retention recommendations
- Identify backup recommendations
- Move and delete index data
- Describe the use of the Fishbucket
- Restore a frozen bucket

Managing Indexes with Splunk Web

From Splunk Web: **Settings > Indexes**



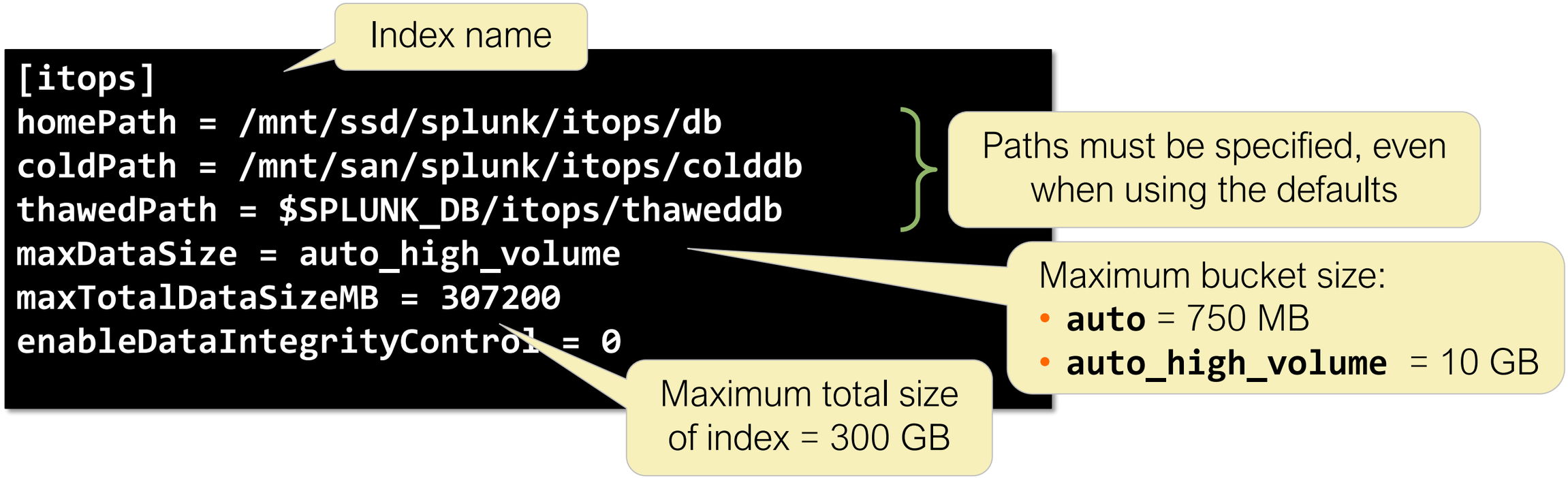
Index Definitions and Data

Index Definition (`indexes.conf`)	`SPLUNK_HOME/etc/system/default`
	`SPLUNK_HOME/etc/system/local`
	`SPLUNK_HOME/etc/apps/<app_name1>/local`
	`SPLUNK_HOME/etc/apps/<app_name2>/local`
	`SPLUNK_HOME/etc/apps/...`

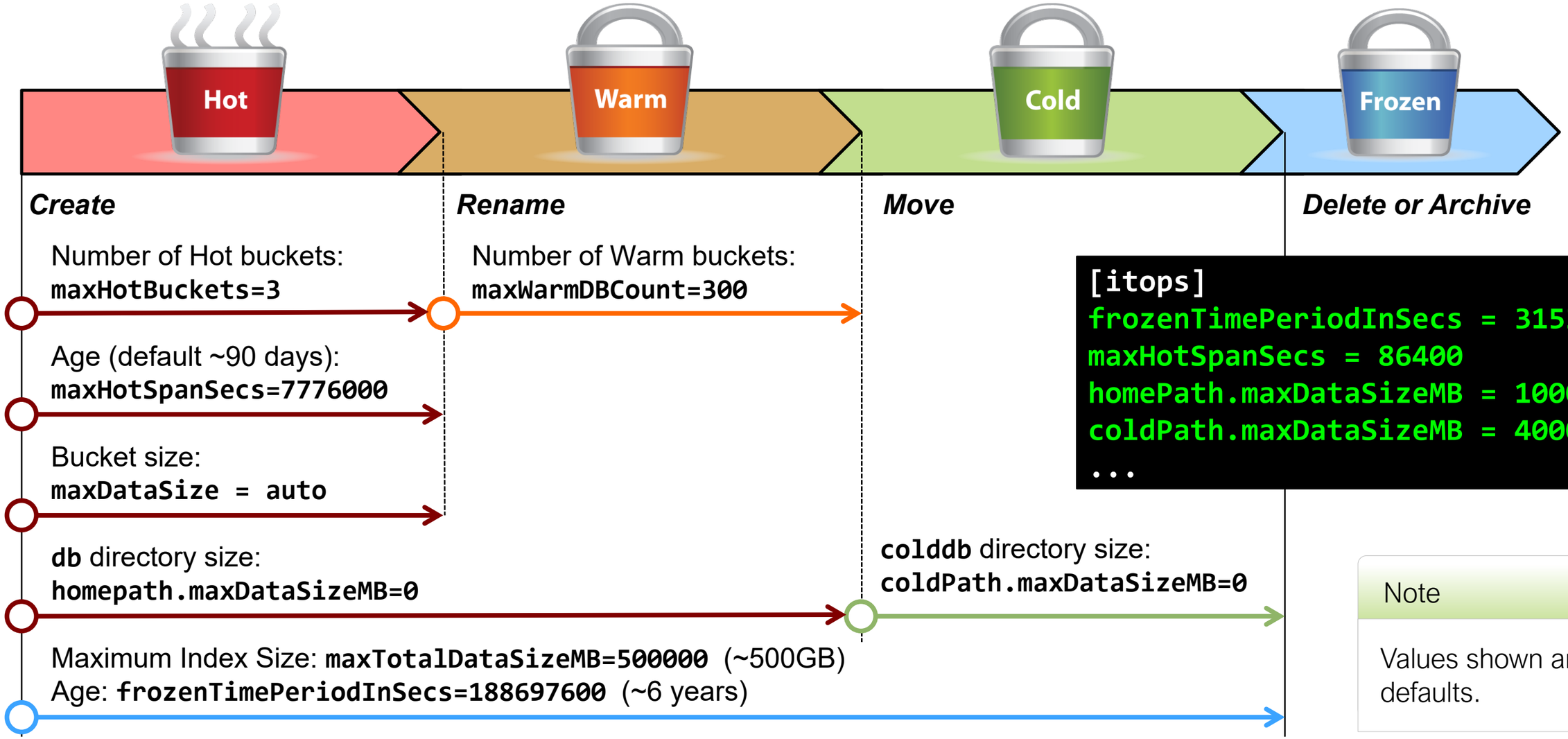
Indexed Data (Buckets)	`SPLUNK_HOME/var/lib/splunk/<index_name>/db`
	`SPLUNK_HOME/var/lib/splunk/<index_name>/colddb`
	`SPLUNK_HOME/var/lib/splunk/<index_name>/thaweddb`

The **indexes.conf** File

The index stanza is created in **indexes.conf** of the selected app (in **SPLUNK_HOME/etc/apps/<*appname*>/local/**)

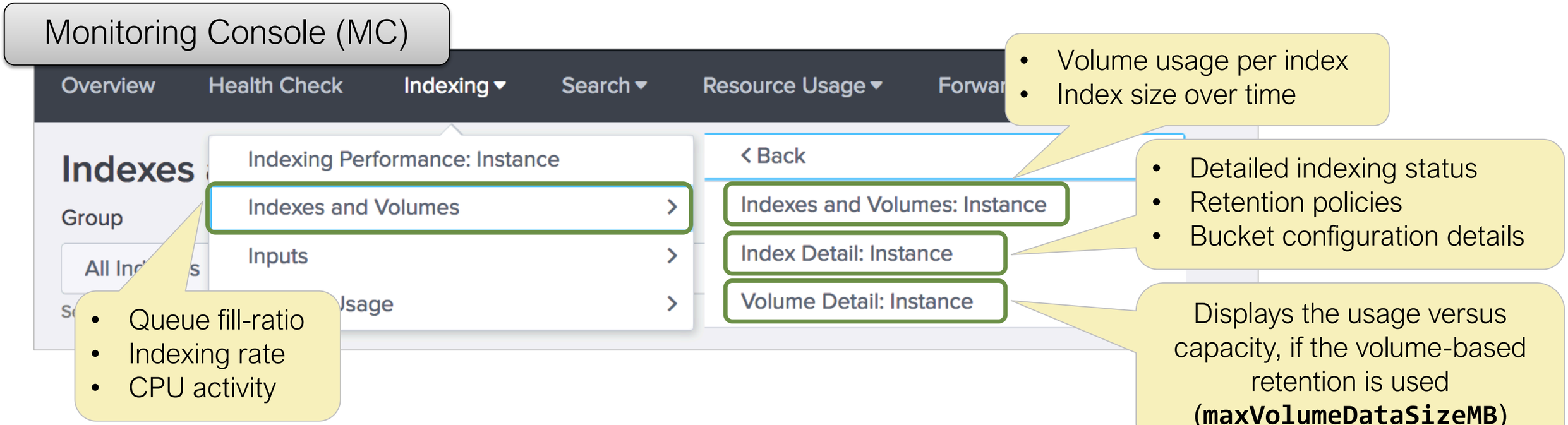


Additional **indexes.conf** Options

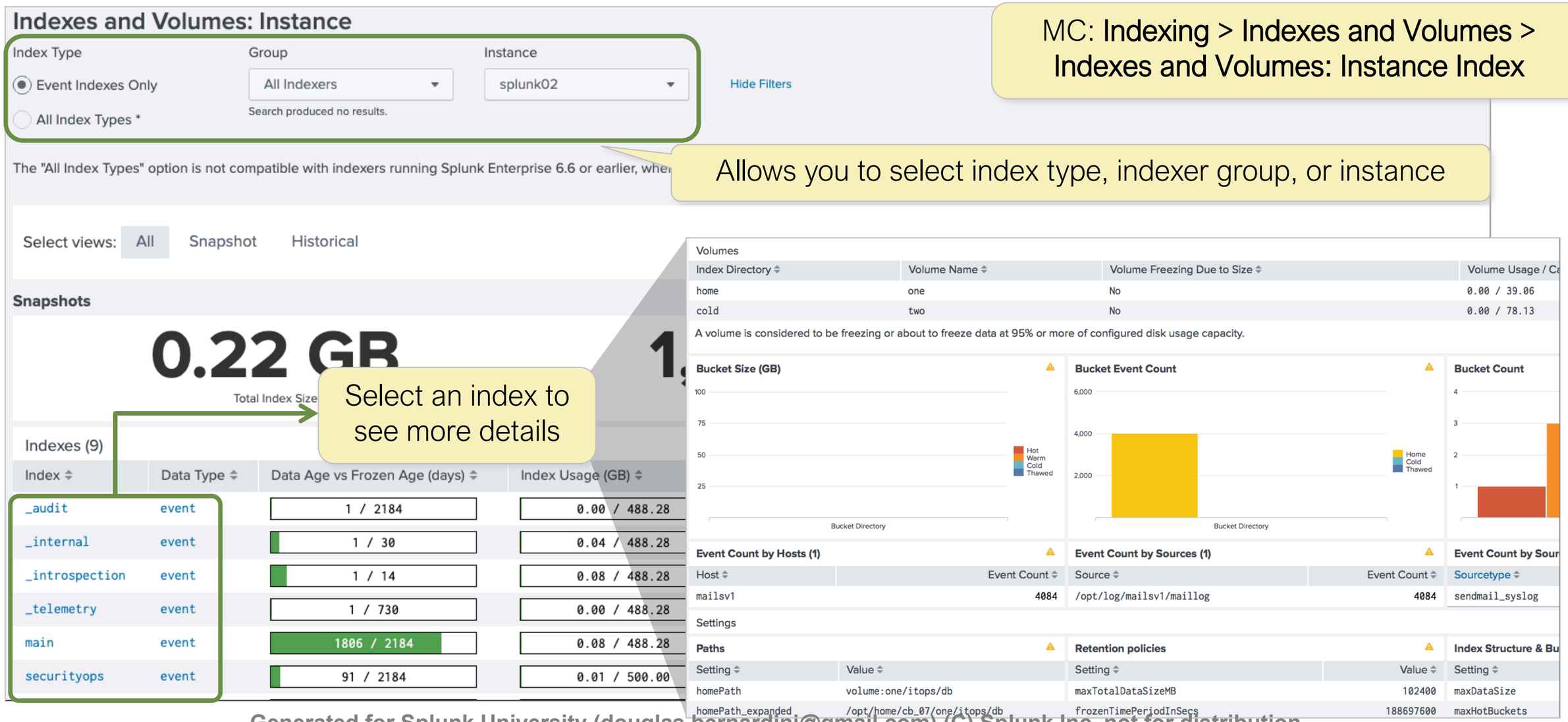


Viewing Indexing Activity and Health in the MC

- Provides comprehensive indexing activity details
- **Snapshot** shows averages over the previous 15 minutes
- **Historical** exposes trending and possible decaying health



Monitoring Indexes with MC



MC: Indexing > Indexes and Volumes > Indexes and Volumes: Instance Index

Allows you to select index type, indexer group, or instance

Select an index to see more details

Index Data Integrity Check

- Validates integrity of indexed data with SHA256-based hashes
- When enabled:
  - Produces hash files for auditing and legal purposes
  - Works on index level, including clustering
  - Does not protect in-flight data from forwarders (use SSL)
- Use the indexer acknowledgment capability (**`useACK`**) to prevent data loss
- Verify integrity of an index/bucket: **`splunk check-integrity …`**

docs.splunk.com/Documentation/Splunk/latest/Security/Dataintegritycontrol

Configuring High-volume Indexes

- Set specific options by editing the stanza in **`indexes.conf`**
- **Best practice** for high-volume indexes:
  - Change index default of 3 hot buckets to 10 hot buckets using the **`maxHotBuckets`** key
  - Examine and copy settings of **`main`** index stanza and adjust for use case

Warning

Incorrect retention settings can cause premature bucket rotation and even stop Splunk. It is advised to contact Splunk Professional Services before editing retention policies.

Strict Time-based Retention Policies

- Scenario: Purge HR data when it is more than 90 days old
- Issues to consider:
  - Splunk freezes entire buckets, not individual events
  - If a bucket spans more than one day, you can't strictly meet the 90 day requirement
- Configuration option:

  `frozenTimePeriodInSecs = 7776000` (~90 days)

  `maxHotSpanSecs = 86400` (~24 hours)

Warning

These options satisfy the strict data retention policy but may negatively impact performance.

Using small **`maxHotSpanSecs`** under indexer clustering is not recommended because it can produce many small buckets.

Monitor bucket size and the rate of accumulation (in terms of bucket count) closely after changes.

Buckets on Different Storage Systems

- Use a high-performance file system to store indexes
  - Bucket time span and storage type affects search performance
- Use multiple storage systems for buckets
  - Specify fastest storage for **Home path** (Hot/Warm buckets)
  - Specify slower, less expensive storage for **Cold path** (Cold buckets)
- Refer to: wiki.splunk.com/Deploy:BucketRotationAndRetention

splunk> Best Practice

Volume Stanzas in `indexes.conf`

- Example: Prevent data bursts in one index from triggering indexing issues elsewhere in the same volume
- Issues to consider:
  - Splunk cannot determine the maximum size for non-local volumes
  - Hot/warm and cold buckets can be in different volumes
  - If the volume runs out of space, buckets roll to frozen before **`frozenTimePeriodInSecs`**
- Configuration Options: Use volume reference for a retention based on size

```
[volume:fast]
path = /mnt/ssd/
maxVolumeDataSizeMB = 800000

[volume:slow]
path = /mnt/raid/
maxVolumeDataSizeMB = 4000000
```

```
[soc]
homePath = volume:fast/soc/db
homePath.maxDataSizeMB = 50000
coldPath = volume:slow/soc/colddb
coldPath.maxDataSizeMB = 200000
```


Last Chance Index

- Gives ability to define a last chance index for events destined for non-existent indexes
- If this setting is not defined or empty, Splunk drops such events
- Defaults to empty

indexes.conf Global Settings

```
lastChanceIndex = <index_name>
...
```


What to Back Up

- Splunk indexes
  - By default, stored in: **SPLUNK_HOME/var/lib/splunk/**
  - See **indexes.conf** if custom locations are used
- Monitored source data files (optional)
- Splunk configuration and important files in: **SPLUNK_HOME/etc**
  - **apps**
  - **users**
  - **system/local**
  - **licenses**
  - **init.d**
  - **passwd**

    and more

Backup Recommendation

- Use the incremental backup of your choice
  - Warm and cold buckets of your indexes
  - Configuration files
  - User files
- Hot buckets cannot be backed up without stopping Splunk
  - Use the snapshot capability of underlying file system to take a snapshot of hot, then back up the snapshot
  - Schedule multiple daily incremental backups of warm buckets for high data volumes

Moving an Index

1. Stop Splunk
2. Copy the entire index directory to new location while preserving permissions and all subdirectories

Linux	**`cp -rp <source> <target>`**
Windows	**`xcopy <source> <target> /s /e /v /o /k`** (or use **Robocopy**)

3. If this is a global change, unset the **`SPLUNK_DB`** environment variable and update **`SPLUNK_HOME/etc/splunk-launch.conf`**
4. Edit **`indexes.conf`** to indicate the new location
5. Start Splunk
6. After testing and verifying new index, the old one can be deleted

Removing Indexed Events

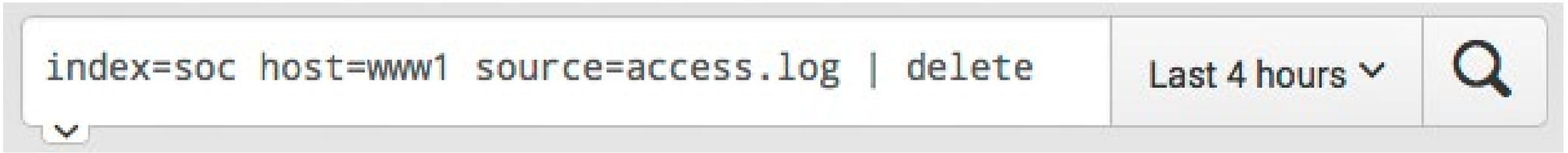
- Splunk does not provide the ability to modify the contents of an index
- Address your configuration to prevent undesired events from being ingested
- For undesired events already in the index, options are:
  - Let the events age out normally (whole bucket ages out)
  - Use the **`delete`** command so the unwanted events do not show up in searches
  - Run **`splunk clean`** command to delete **ALL** events from the index
  - Delete the index

Warning

These options should be used with extreme caution!

Deleting Events Using the **delete** Command

- Virtually deletes events by marking them as “deleted”
  - Prevents “deleted” events from showing in future searches
  - Does not reclaim disk space
  - Cannot be undone
- Can only be run by creating an account with **can_delete** role
  - Nobody, including **admin**, has this ability by default
- To use, ensure you’ve targeted only the events to be deleted, then pipe to the **delete** command:



Cleaning Out an Index

- To flush indexed events and reset an index, use the **`clean`** command
  - DATA WILL BE PERMANENTLY DESTROYED
  - Typically used on test/dev systems, not production systems
- Command syntax:

  `splunk clean [eventdata|userdata|all] [-index index_name]`
  - **`eventdata`**: Delete indexed events and metadata on each event
  - **`userdata`**: Delete user accounts
  - **`all`**: Everything, including users, saved searches, and alerts

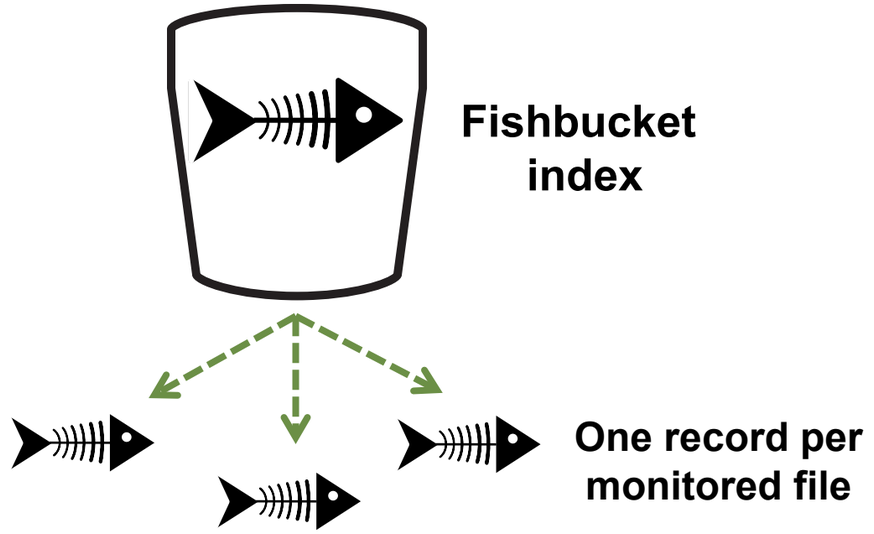
Warning

If no index is specified for the **`splunk clean`** command, the default is to clean (destroy) all indexed events from *all* indexes. Always specify an index!

What is the Fishbucket?

Fishbucket

- Allows Splunk to track monitored input files
- Contains file metadata which identifies a pointer to the file, and a pointer to where Splunk last read the file
- Exists on all Splunk instances
- Stored in a special subdirectory found at **`SPLUNK_DB/fishbucket`**



Includes:

- **Head**: Pointer to the file
- **Tail**: Pointer showing where Splunk last left off indexing in the file

Resetting Input File Monitors

1. Stop Splunk
2. Reset applicable file monitors
   - Individually for each source:

```
splunk cmd btprobe -d SPLUNK_DB/fishbucket/splunk_private_db
  --file <source> --reset
```

   - All sources (use only on test systems / with extreme caution):

```
splunk clean eventdata -index _thefishbucket
```

or

```
rm -r SPLUNK_DB/fishbucket
```

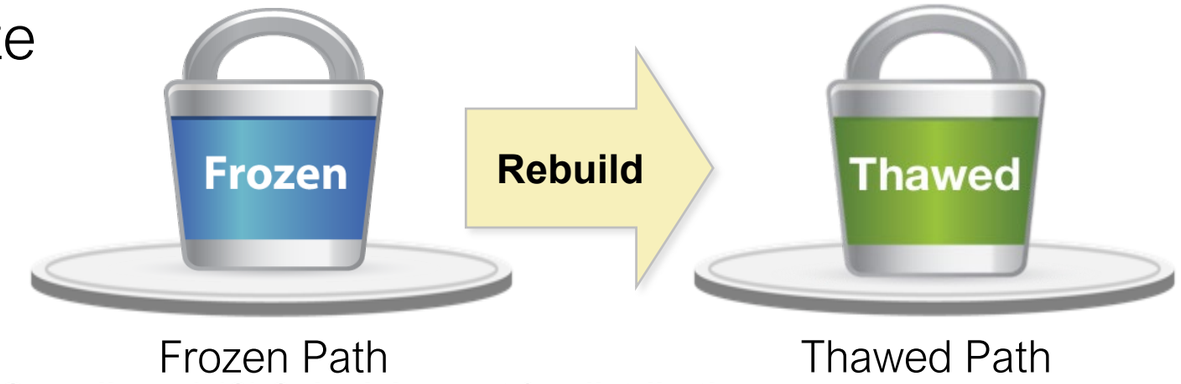
3. Start Splunk

Warning

Resetting the fishbucket forces re-indexing of all file monitors affected. This results in more license usage.

Restoring a Frozen Bucket

- To thaw a frozen bucket:
  1. Copy the bucket directory from the Frozen Path to the index's Thawed Path (**thaweddb**) directory
  2. Run **splunk rebuild <*Thawed_Path*>**
     - Does not count against Splunk license
  3. Restart Splunk
- Events in **thaweddb** are searchable along with other events
  - Will not be frozen again
  - Do not count against the index max size
- Delete the thawed bucket directory when no longer needed and restart Splunk



Further Reading

- docs.splunk.com/Documentation/Splunk/latest/Indexer/HowSplunkstoresindexes
- docs.splunk.com/Documentation/Splunk/latest/Indexer/Setlimitsondiskusage
- docs.splunk.com/Documentation/Splunk/latest/Indexer/Automatearchiving
- wiki.splunk.com/Deploy:BucketRotationAndRetention

Module 6 Knowledge Check

- True or False. Frozen buckets roll to Thawed automatically.
- True or False. When creating an Index from the web, it creates a stanza in **`inputs.conf`**.
- True or False. When running the **`splunk clean`** command, you can set a date range for the events you want to delete.

Module 6 Knowledge Check – Answers

- True or False. Frozen buckets roll to Thawed automatically.

  False. To thaw a frozen bucket, you start by copying the bucket directory from the frozen directory to the index's thaweddb directory and follow the steps mentioned on slide “Restoring Frozen Buckets.”

- True or False. When creating an Index from the web, it creates a stanza in **`inputs.conf`**.

  False. It creates a stanza in **`indexes.conf`**.

- True or False. When running the **`splunk clean`** command, you can set a date range for the events you want to delete.

  False. There is no option to set a date range.

Module 6 Lab Exercise

Time: 10 minutes

Description: Splunk Index Management

Tasks:

- Use the MC to view **`securityops`** index information
- Configure a time-based retention policy

Module 7:
Splunk User Management

Module Objectives

- Add Splunk users using native authentication
- Describe user roles in Splunk
- Create a custom role
- Manage users in Splunk

Defining Users and Roles

Users

- Provide access to a Splunk instance
- Supported natively in Splunk, with LDAP and Active Directory, and with a scripted authentication API

Roles

- Define a Splunk user's capabilities
- Assigned to users

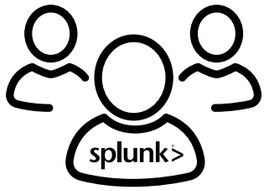
Web users → **Web role**

- Search the Web index

Security users → **Security role**

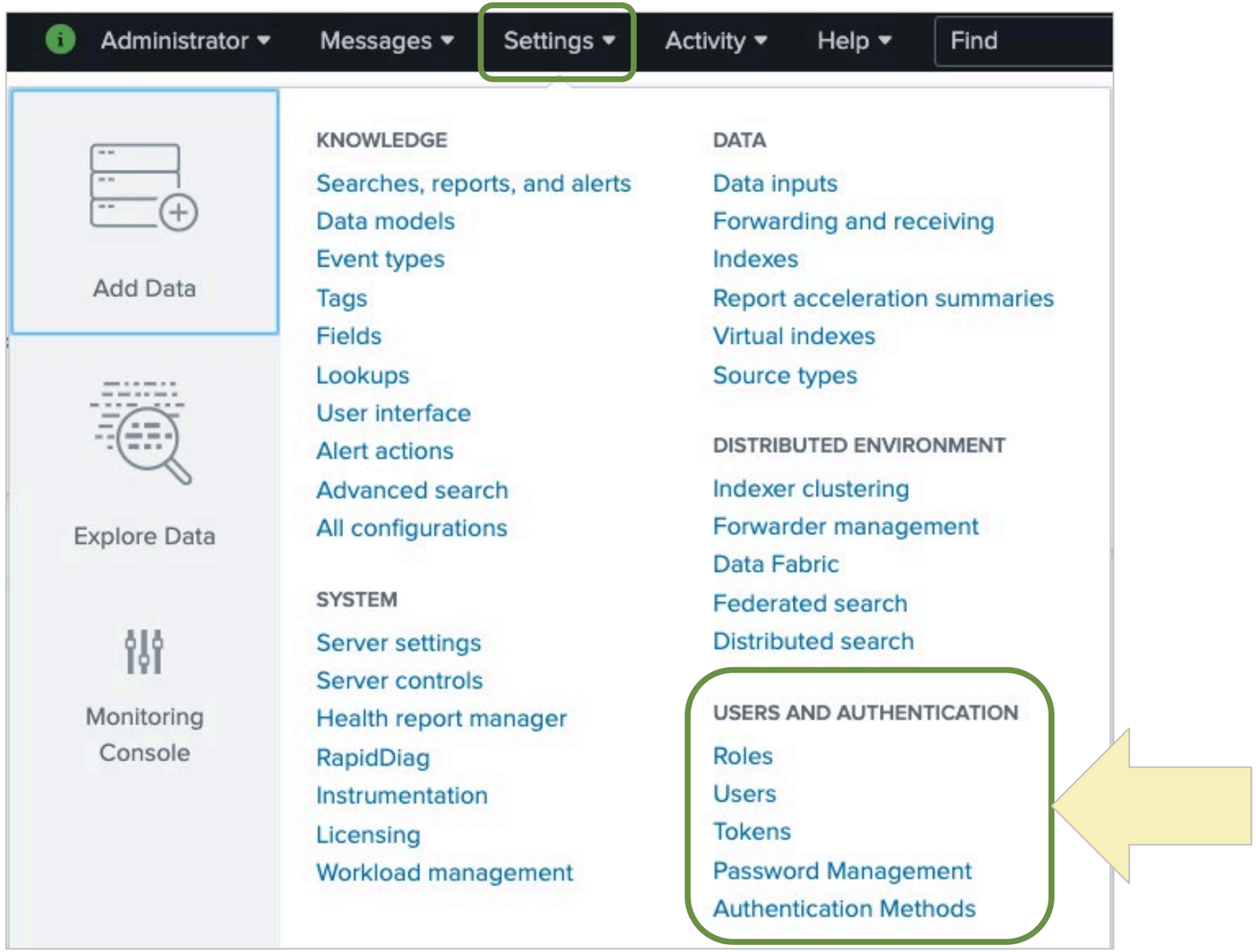
- Search the Web, Proxy and Security indexes

Splunk admins → **Admin role**



- Splunk administration
- Search all indexes

Managing Users and Roles



User Authentication in Splunk

Native authentication

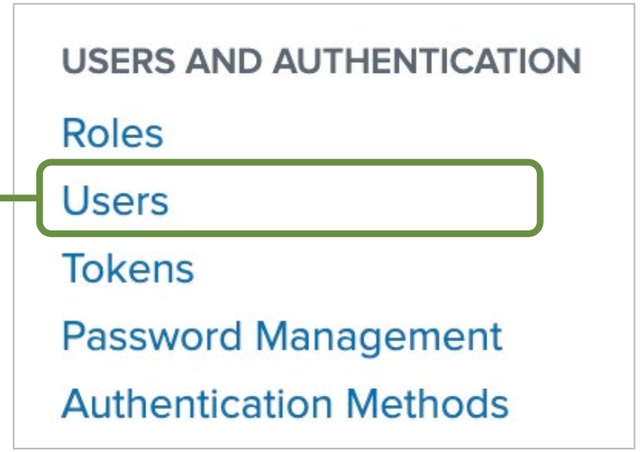
- Creating an account directly in Splunk (example: **admin** user)
- Stores passwords in **SPLUNK_HOME/etc/passwd**
- A blank **passwd** file disables native authentication
- Best Practice: Keep a failsafe account in the **passwd** file with a very strong password

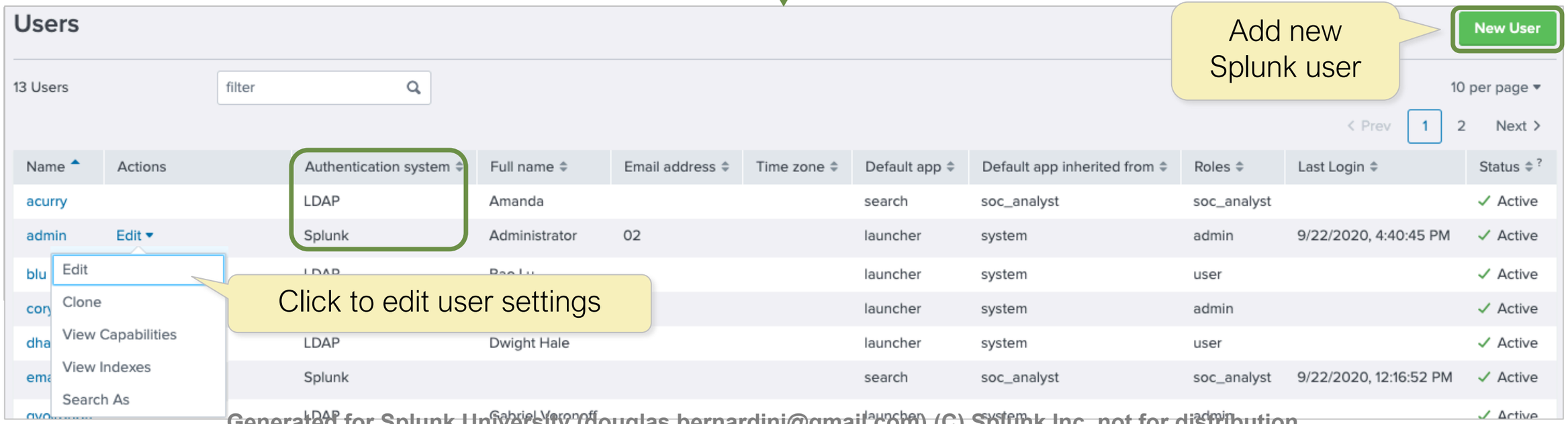
Other supported authentication

- Splunk integration with LDAP
- Scripted authentication API
- Splunk enforces precedence of native authentication over other models

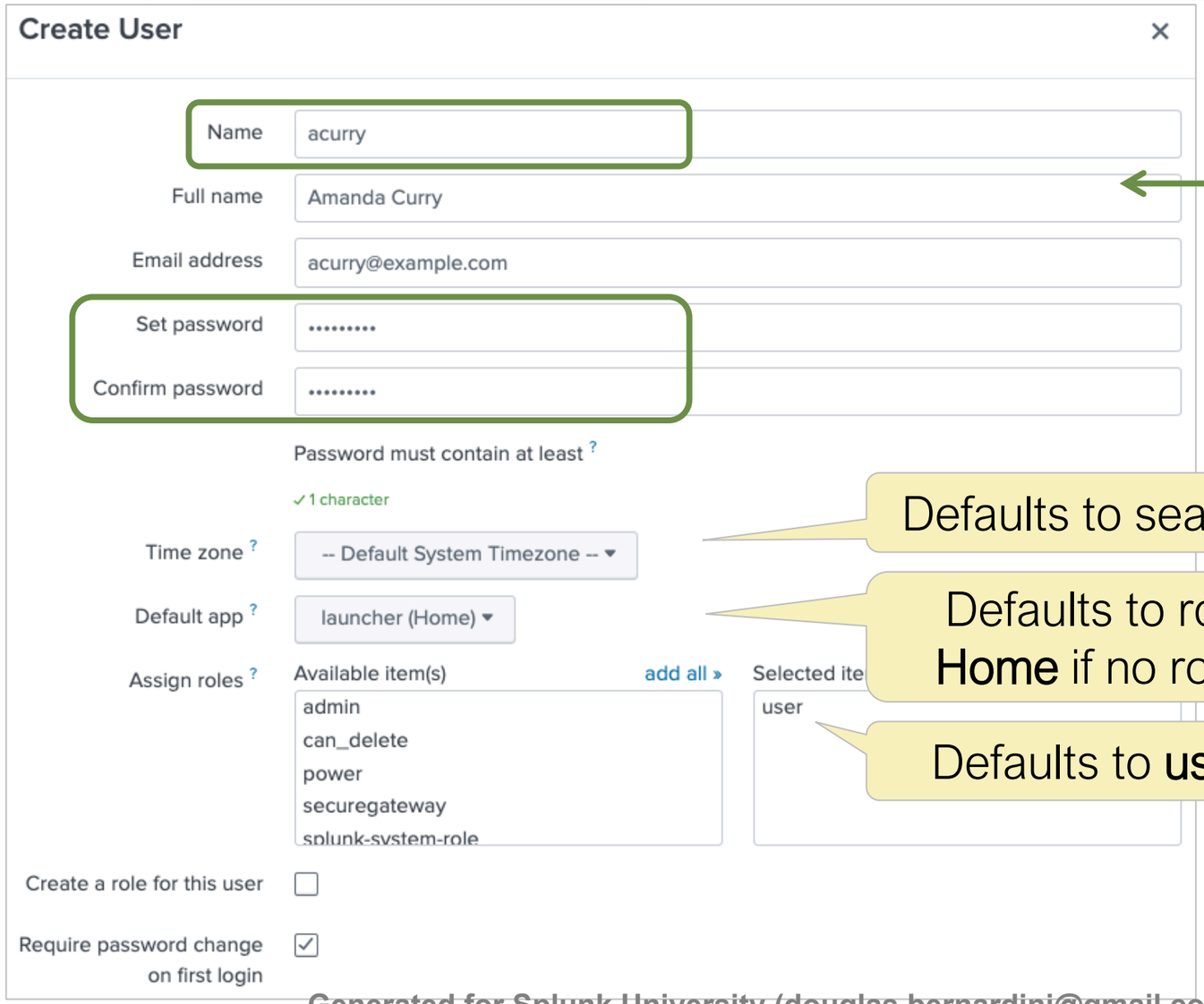
Viewing and Managing Users

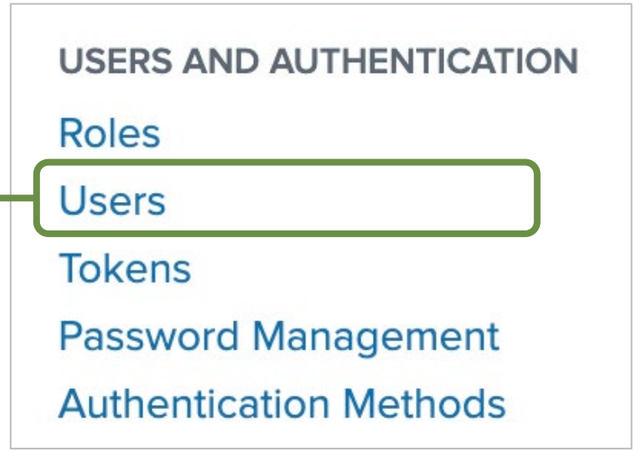
- Splunk native users can be edited or deleted
- Only time zone and default app can be changed on LDAP and other non-Splunk native users





Native Authentication: Adding Users



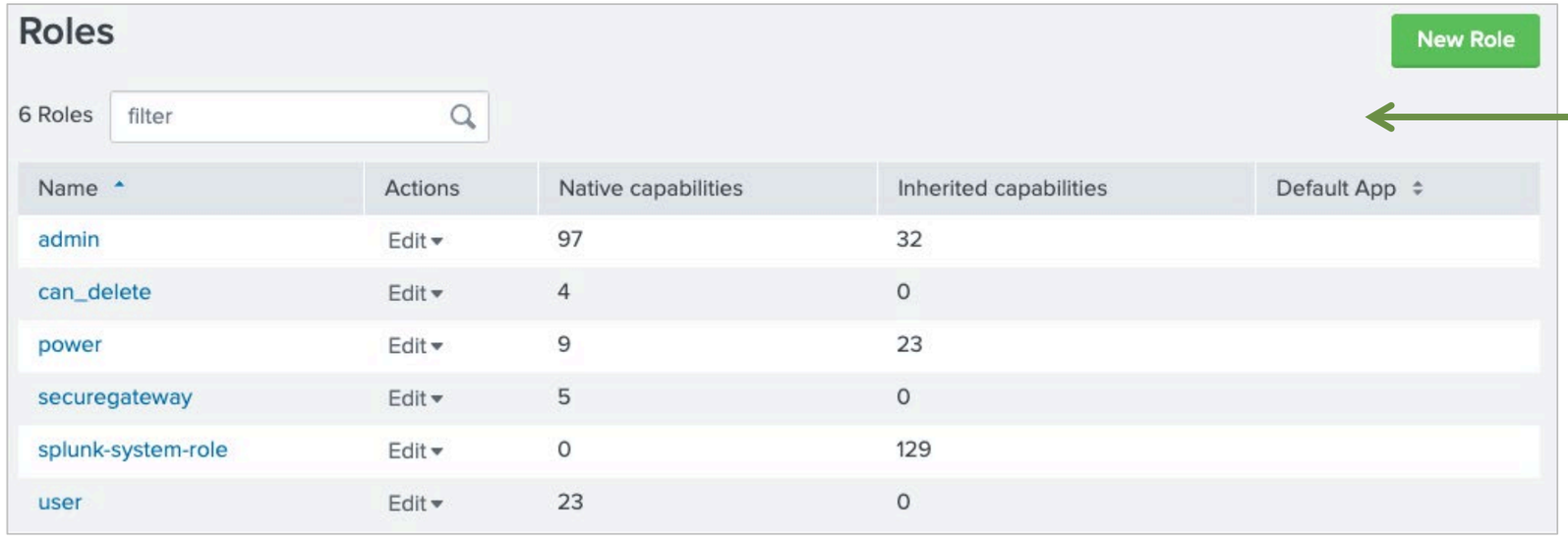


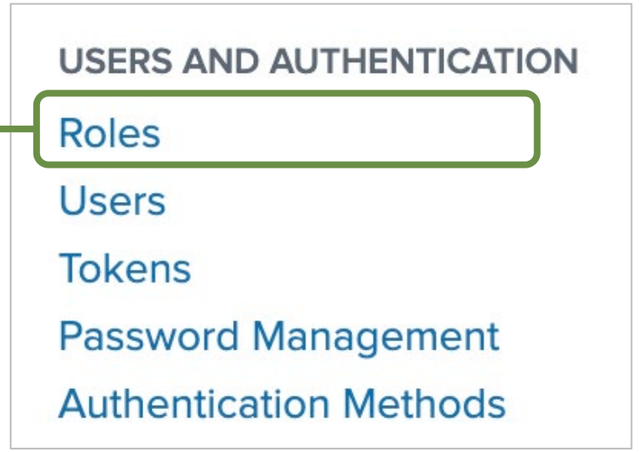
Defaults to search head time zone

Defaults to role's default app, or **Home** if no role default app is set

Defaults to **user** role only

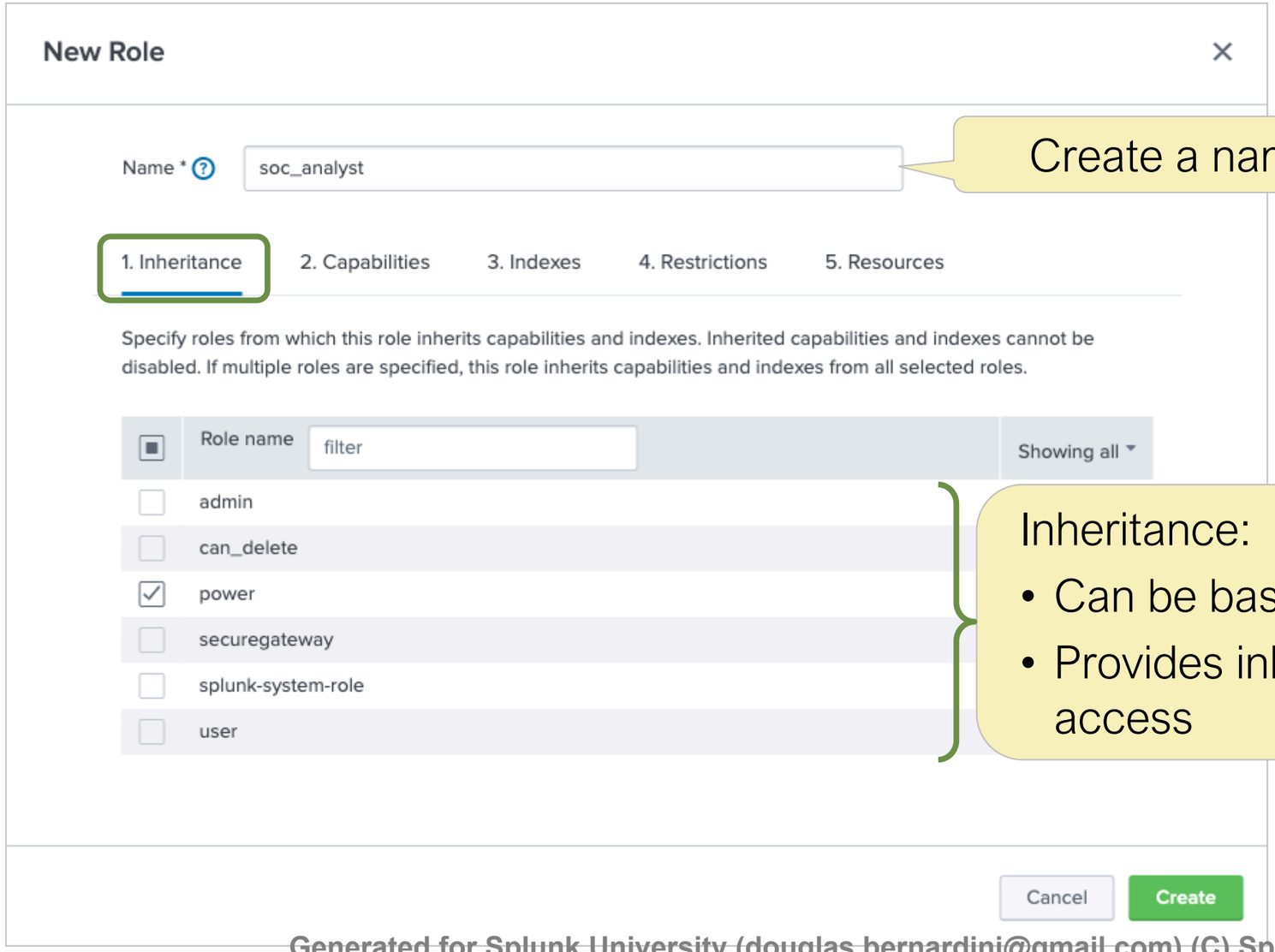
Identifying Roles





Built-in role	Overview of capabilities
admin	Has most capabilities; can create custom roles
power	Edit shared objects, saved searches, and alerts, tag events, and so on
user	Create, edit, and run own saved searches, edit own preferences, create and edit event types, and similar tasks
can_delete	Delete by keyword (necessary when using the **delete** search operator)
splunk-system-role	Allows Splunk system services to run without a defined user context
securegateway	Register devices or use features of Splunk Secure Gateway

Creating User Roles: Inheritance



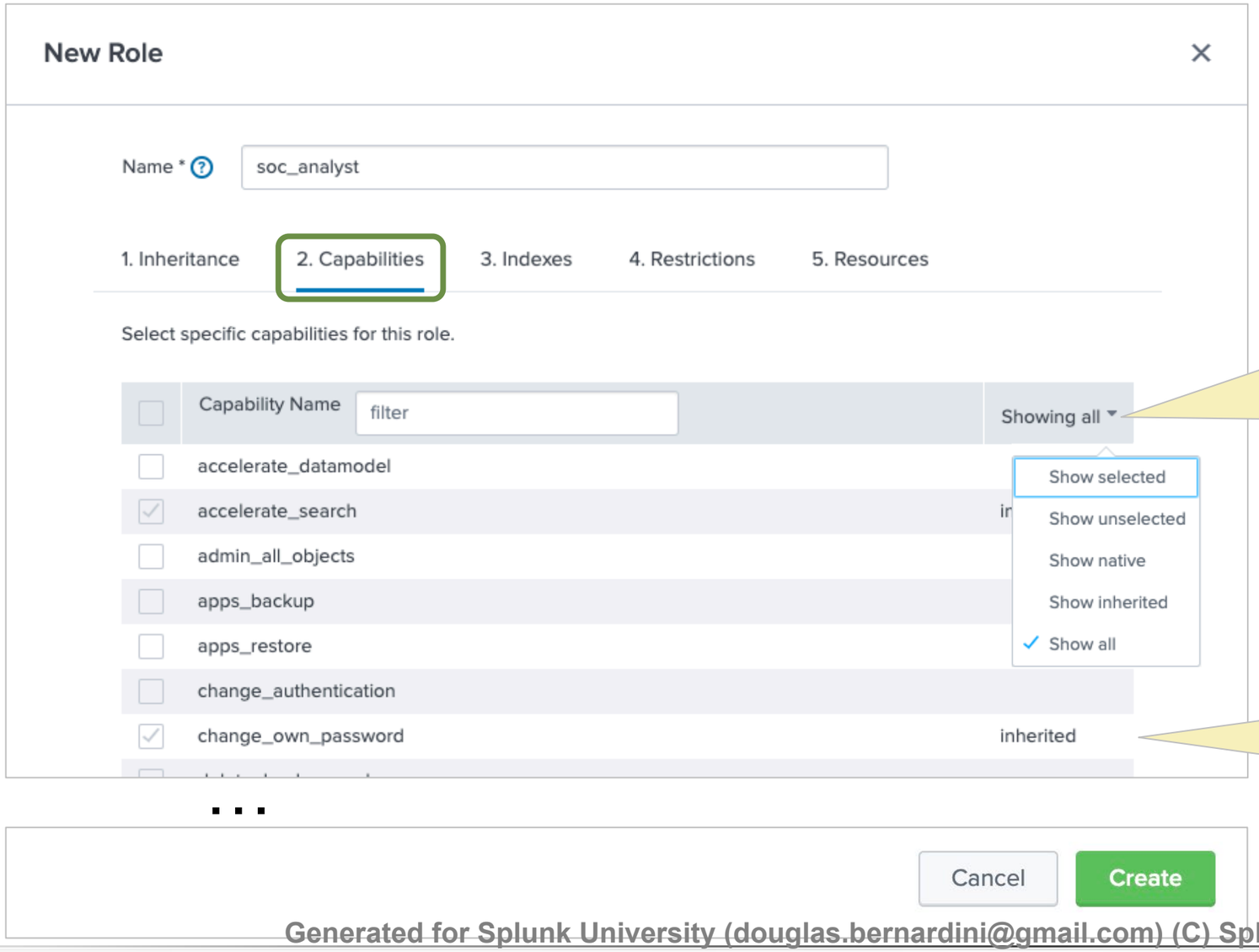
Create a name for the role

Inheritance:

- Can be based on one or more existing roles
- Provides inherited capabilities *and* index access

 | 15 September 2021

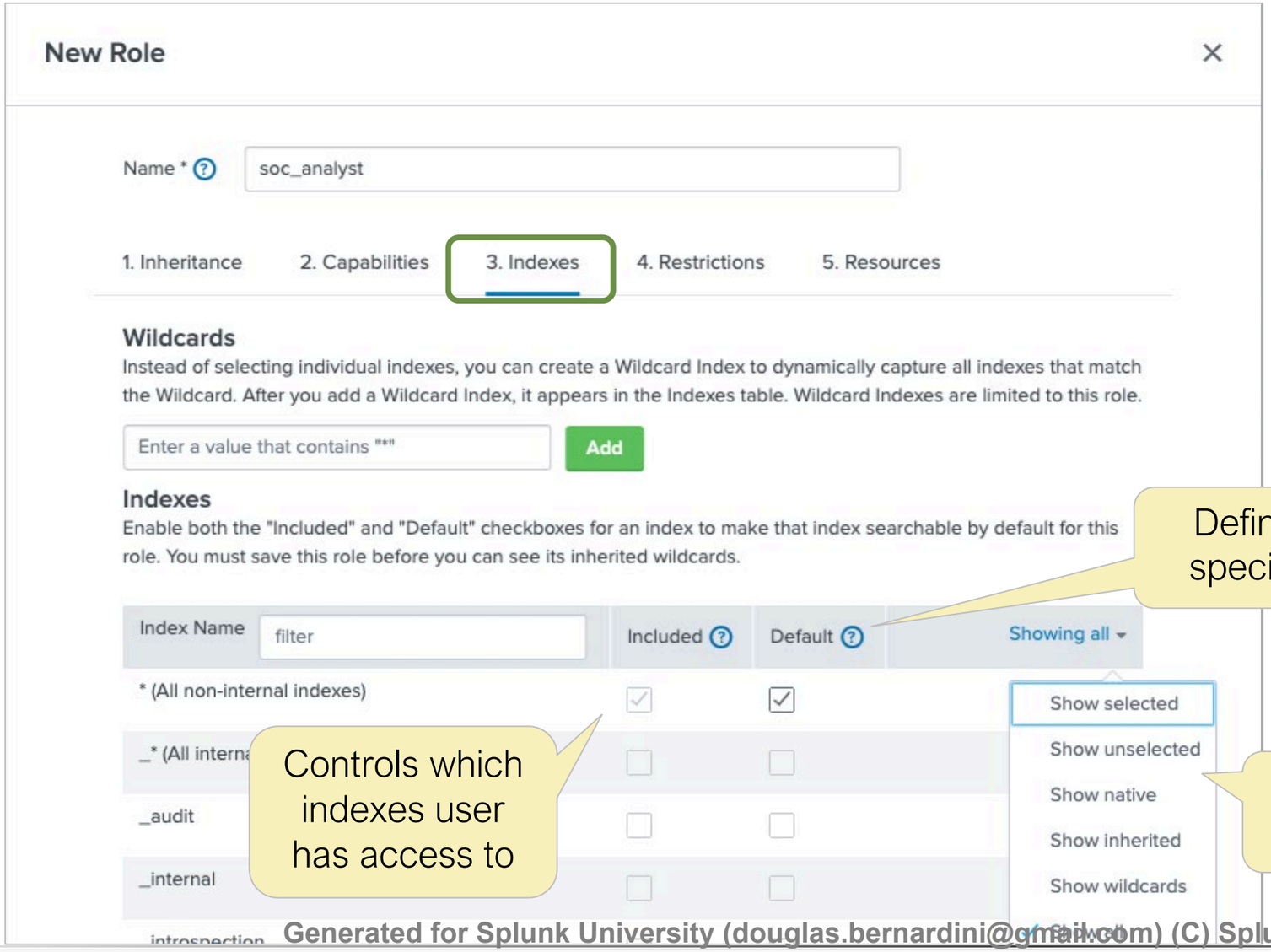
Creating User Roles: Capabilities



Source drop-down menu filters the displayed role capabilities

Capabilities **inherited** from other roles are pre-checked

Creating User Roles: Indexes



Note

Indexes inherited from a parent role are searchable and cannot be disabled. These appear as greyed out check boxes.

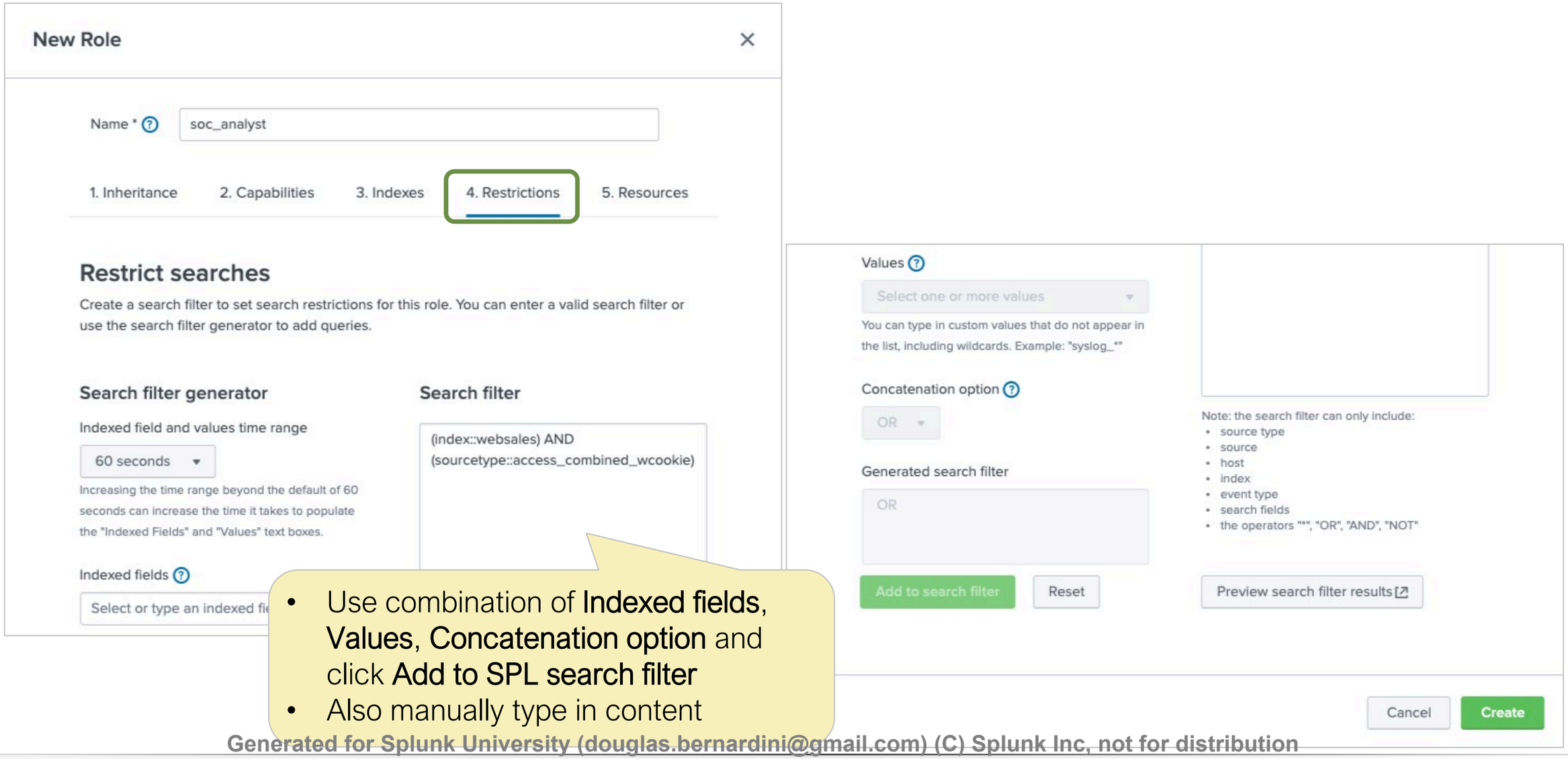
Defines indexes used when user does not specify "**index=<*index_name*>**" in search

Controls which indexes user has access to

Drop-down menu filters the index list

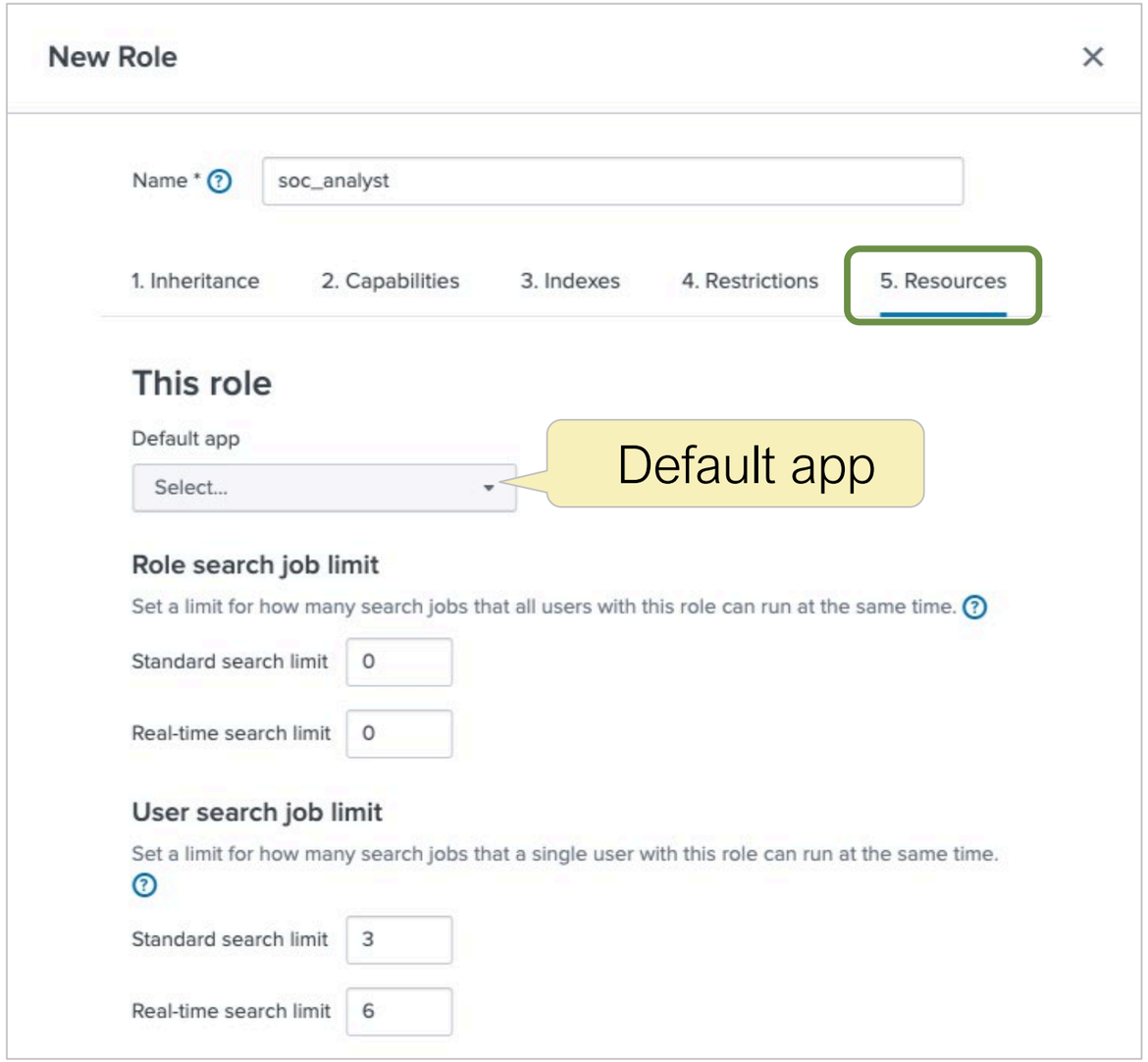
 | 15 September 2021

Creating User Roles: Restrictions

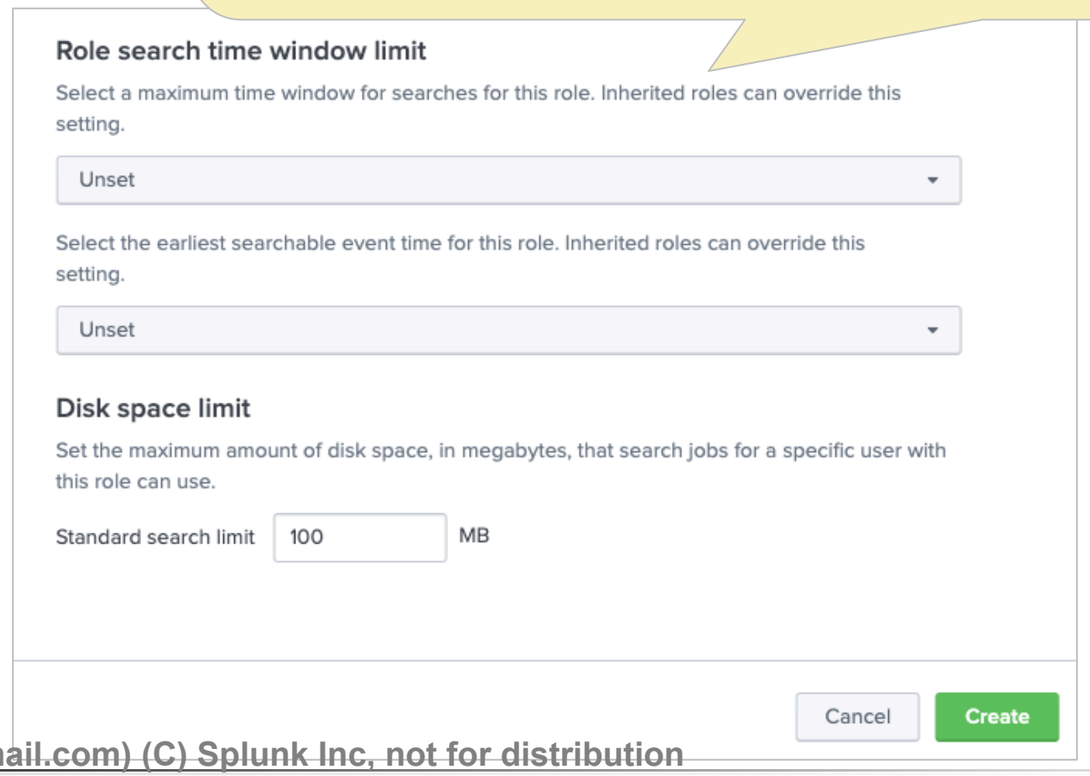


- Use combination of **Indexed fields**, **Values**, **Concatenation option** and click **Add to SPL search filter**
- Also manually type in content

Creating User Roles: Resources



- **Infinite** (0): No restrictions
- **Unset** (-1): Allows window limit to be overridden by inherited roles
- **Custom time**: Limit, in seconds



The **authorize.conf** File

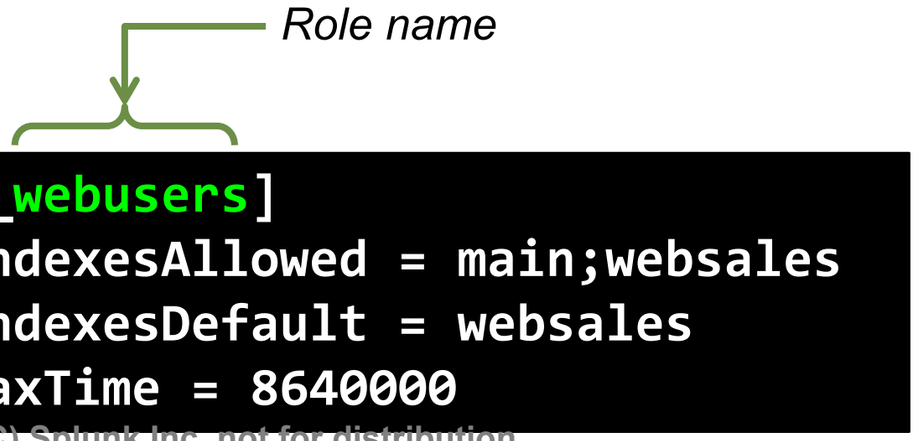
- Contains the Splunk role configuration
- Should not be modified from the **default** directory:

  SPLUNK_HOME/etc/system/default/authorize.conf

- Should only be modified from the **local** directories:

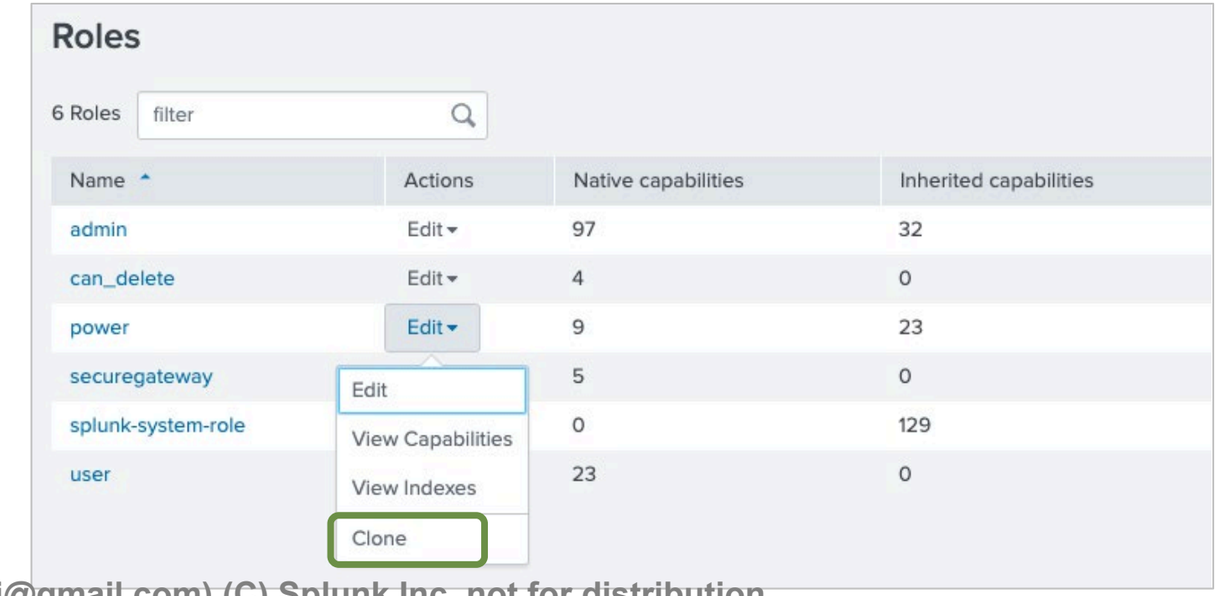
  SPLUNK_HOME/etc/system/local or
  SPLUNK_HOME/etc/apps/<*appname*>/local

authorize.conf
(example entries)



Creating a Copy of an Existing Role

- Using inheritance:
  - Create a new role and configure the **1. Inheritance** tab
  - Provides all the capabilities and index settings of the inherited role
  - Prevents disabling inherited capabilities or index access
- Without inheritance:
  1. Use **Edit > Clone** in Splunk Web
  2. Modify the new role as needed

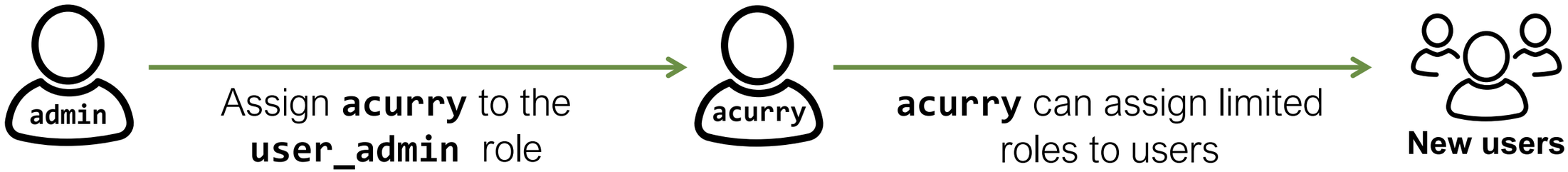


Example Scenario With **edit_roles_grantable**

Example scenario:

Separate and delegate user administration tasks

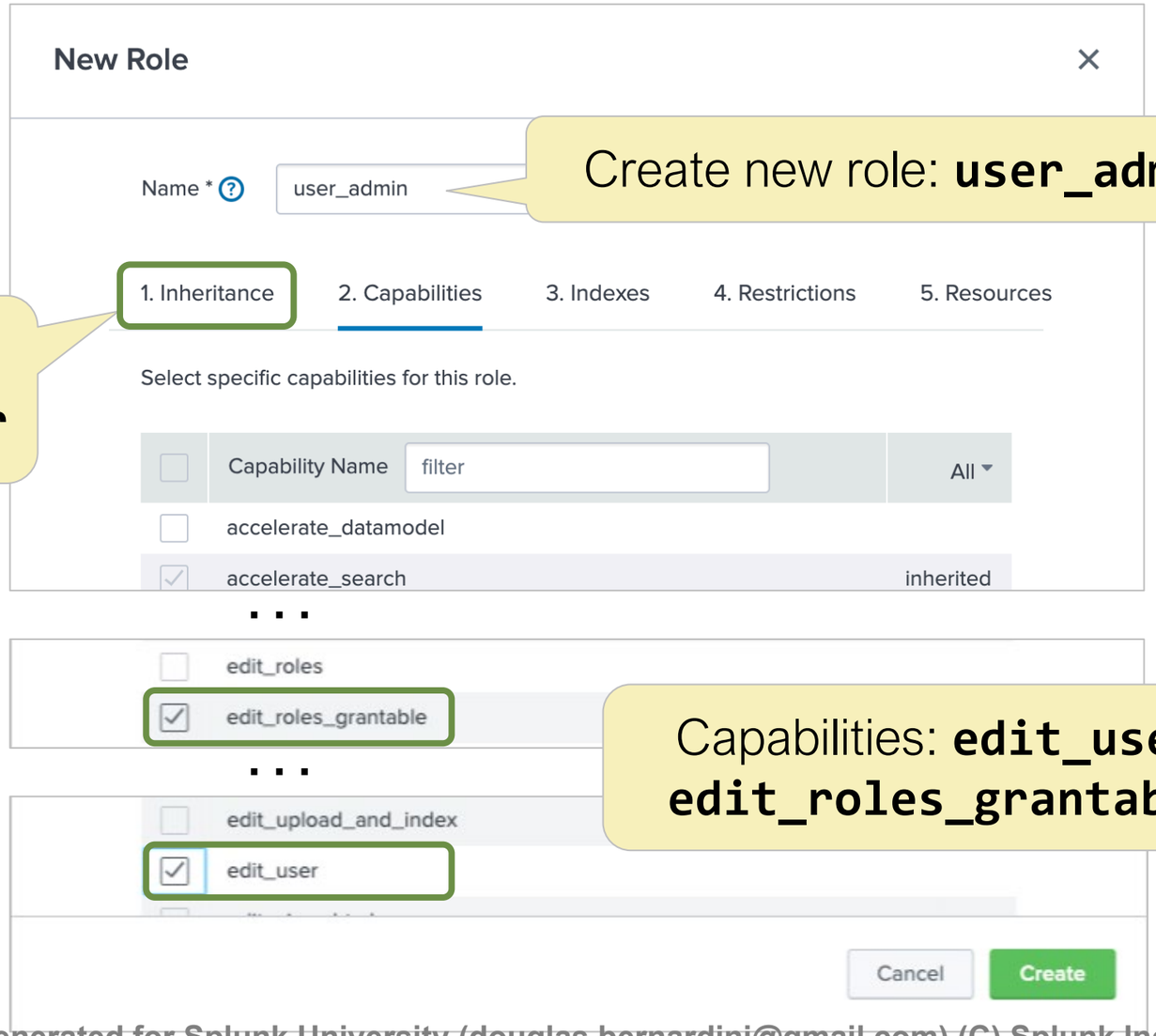
1. Create a new role of **user_admin**
   - New role can assign roles to other users
   - New role cannot grant the **admin** role to self or others
2. Assign **user_admin** role to Amanda Curry (user: **acurry**)



Issues to consider:

- Capabilities **edit_user** + **edit_roles** allows user to promote themselves to full admin
- Capabilities **edit_user** + **edit_roles_grantable** only allows user to assign a subset of roles they currently have

Assigning **edit_roles_grantable** Capability



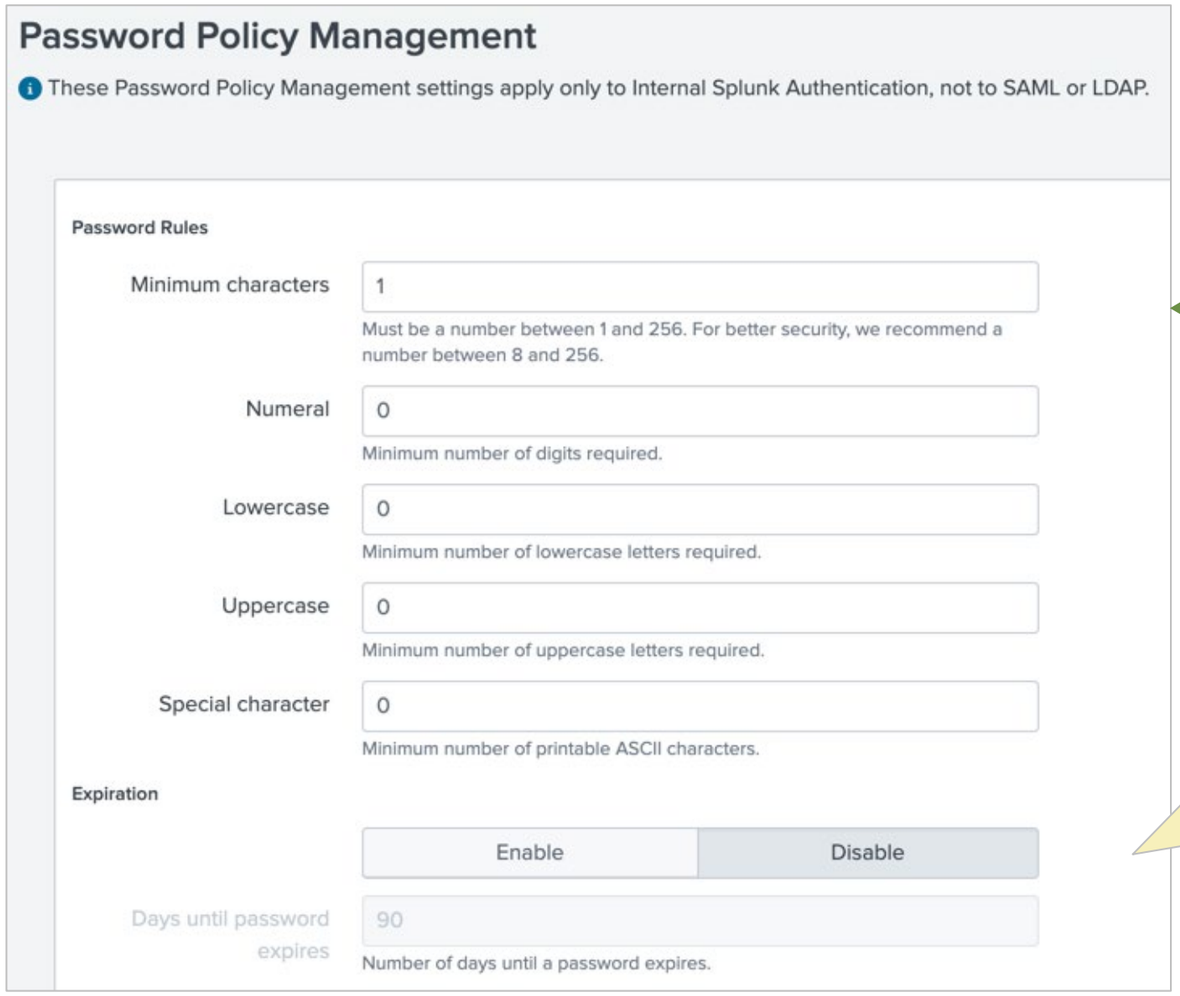
Create new role: **user_admin**

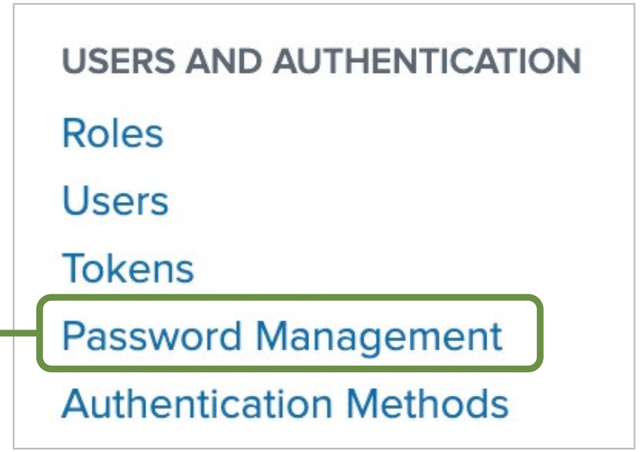
Inheritance: **power**, **user**

Capabilities: **edit_user**, **edit_roles_grantable**

 | 15 September 2021

Password Policy Management



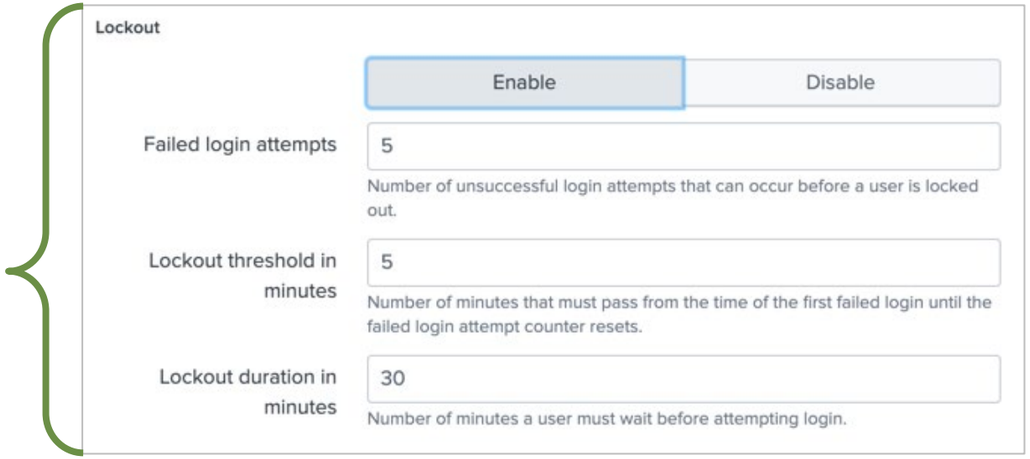


- Provides options for password rules, expiration, lockout, and history
- Only applies to native Splunk users (not SAML or LDAP passwords)

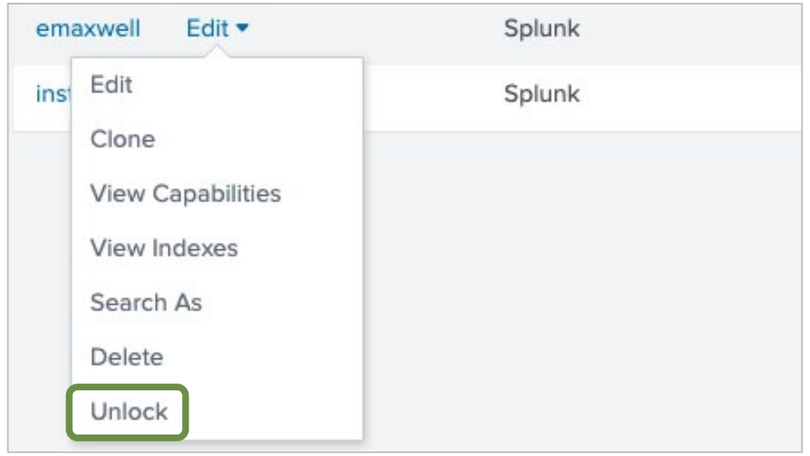
docs.splunk.com/Documentation/Splunk/latest/Security/Passwordbestpracticesforadministrators

Unlocking Users

- For users who have exceeded failed login attempts threshold
  - Configured in **Password Management**



- Using Splunk Web:
  - **Settings > Users,** then **Edit > Unlock**:



- Using CLI:

```
splunk edit user <locked_user> -locked-out false –auth <admin_user:password>
```

Admin Passwords

- An Admin password is **required** during installation and to start Splunk for the first time
- To create a password during startup:

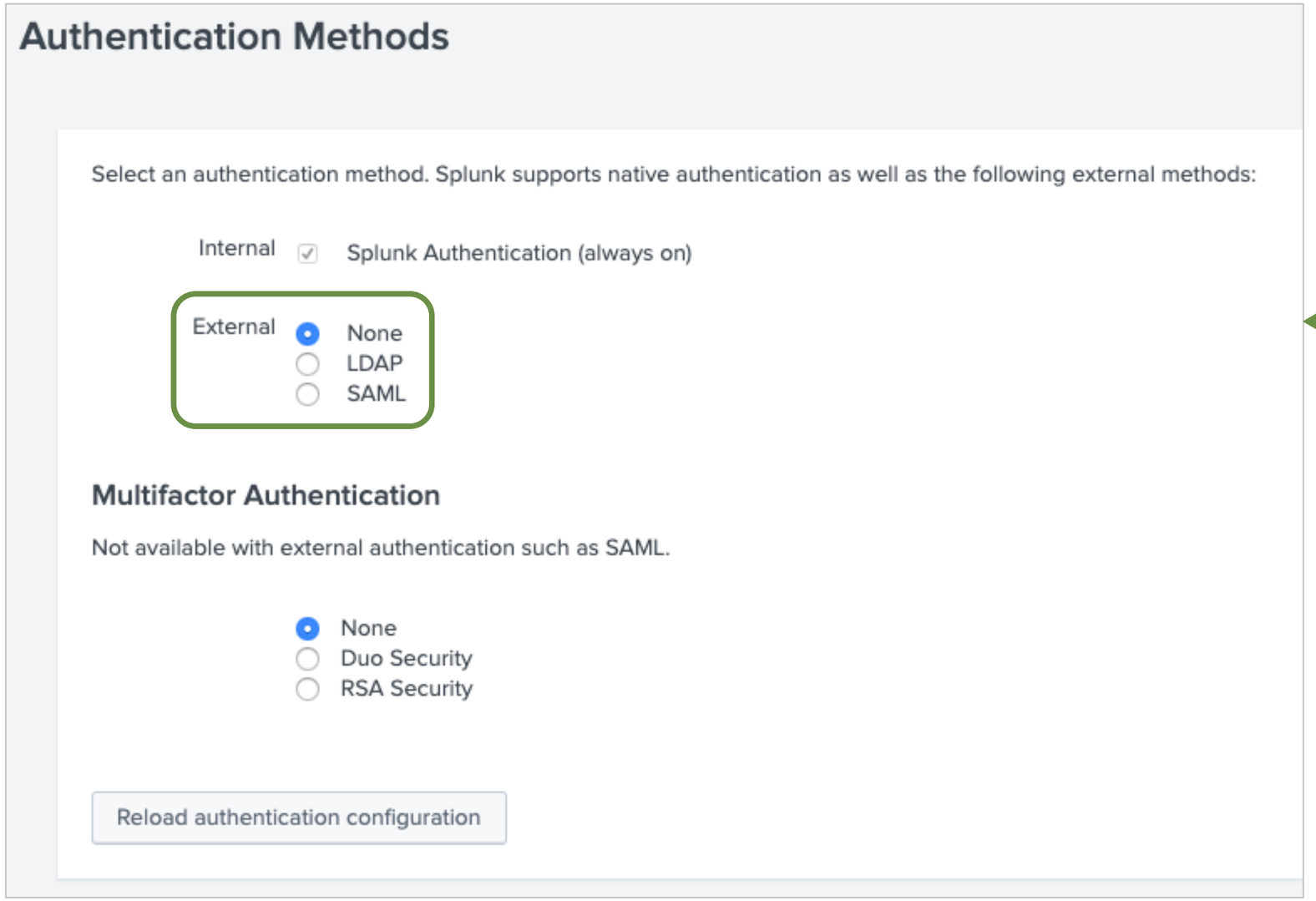
```
splunk start --accept-license --answer-yes --no-prompt --seed-passwd <password>
```

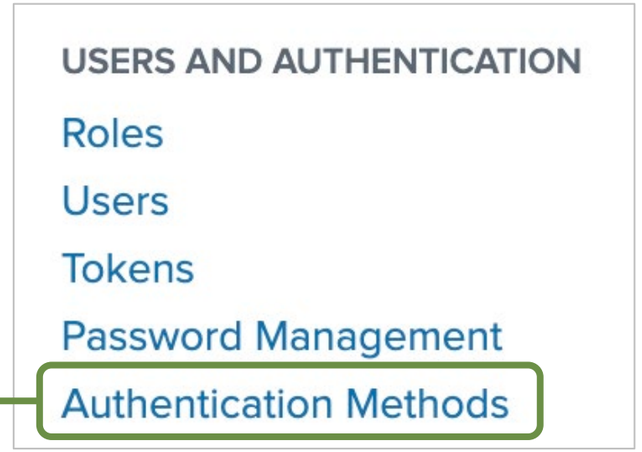
- To generate a random password during startup:

```
splunk start --accept-license --answer-yes --no-prompt --gen-and-print-passwd
```

docs.splunk.com/Documentation/Splunk/latest/Security/Secureyouradminaccount

Splunk Authentication Options





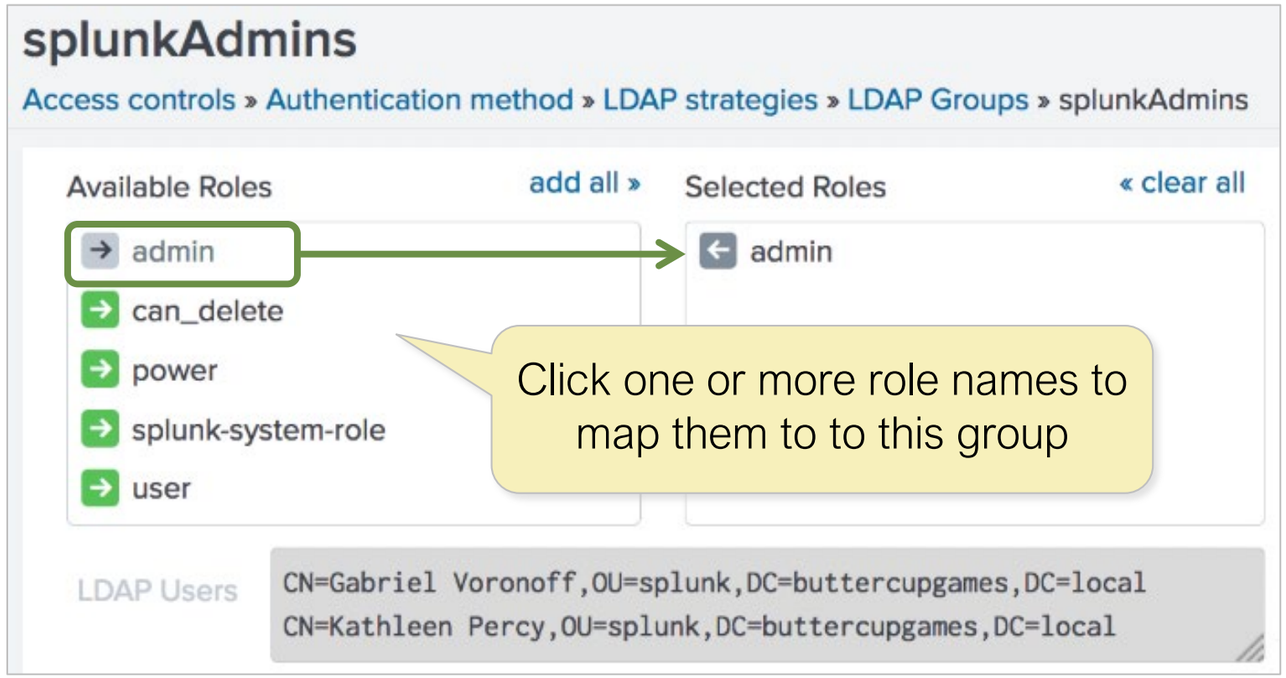
Note

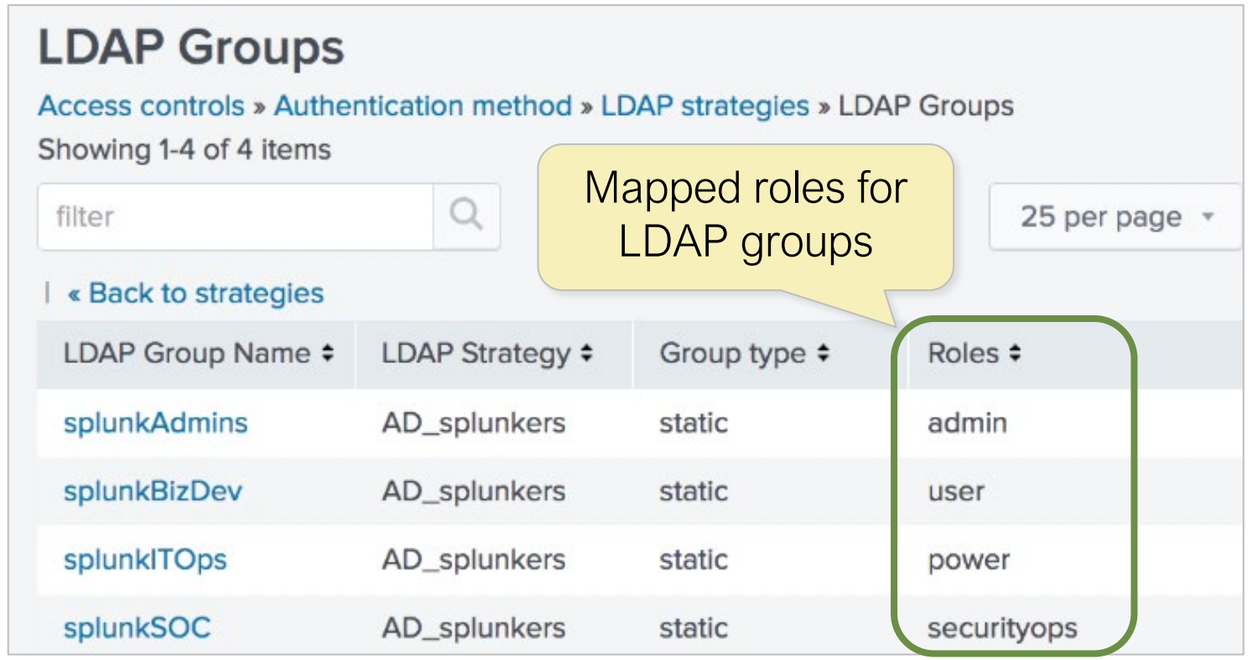
More details on using alternate authentication methods is provided in Appendix A.

Scripted access to PAM, RADIUS, or other user account systems are also supported.

Mapping LDAP/SAML Groups to Roles

- A user cannot log in unless they have a Splunk role
- Not all groups must be mapped
- Mappings can be changed at any time





Module 7 Knowledge Check

- True or False. If you are installing a Search Head and an Indexer, Splunk requires an admin account on each instance.
- True or False. If you want a role that is "like" **`user`** but with some capabilities turned off, you can create a new role that inherits from the **`user`** role and remove some of the capabilities.
- True or False. You can unlock a user from the CLI.

Module 7 Knowledge Check – Answers

- True or False. If you are installing a Search Head and an Indexer, Splunk requires an admin account on each instance.

  True.

- True or False. If you want a role that is "like" **`user`** but with some capabilities turned off, you can create a new role that inherits from the **`user`** role and remove some of the capabilities.

  False. Inheritance does *not* allow inherited capabilities to be turned off. Instead, clone the **`user`** role and modify it as desired.

- True or False. You can unlock a user from the CLI.

  True.

Module 7 Lab Exercise

Time: 15 minutes

Description: Manage Users and Roles

Tasks:

- Edit existing roles
- Create a new role and assign it to a user
- Verify the configurations

Module 8:
Configuring Basic Forwarding

Module Objectives

- Identify forwarder configuration steps
- Configure a Universal Forwarder
- Understand the Deployment Server

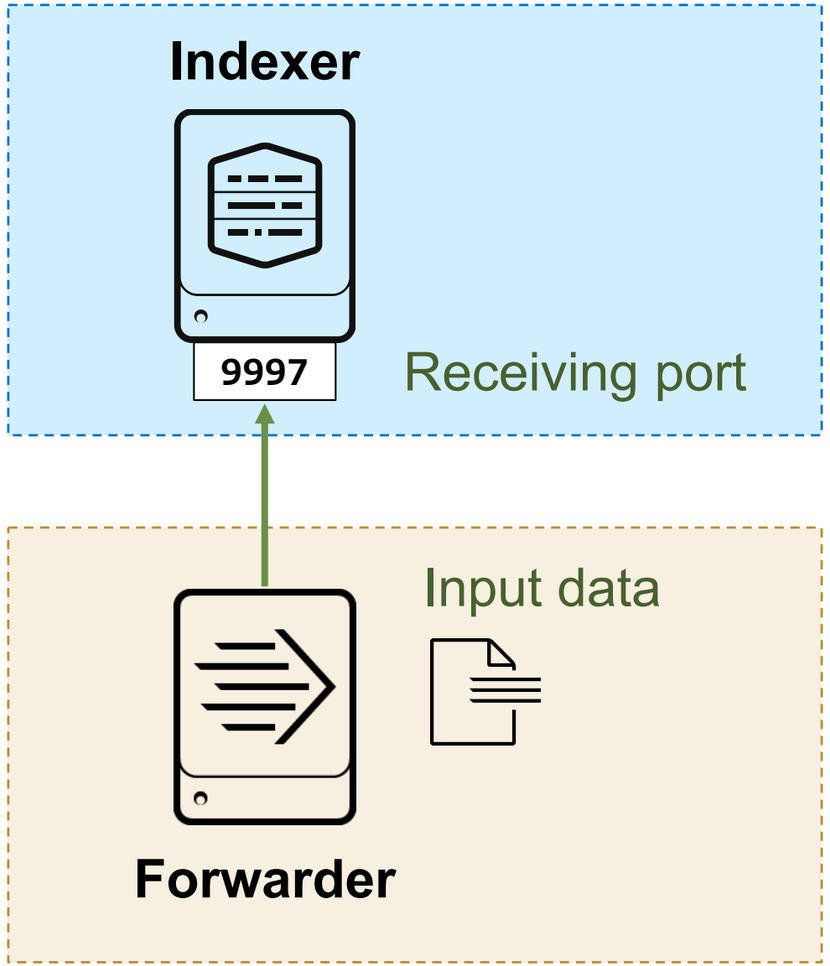
Forwarders and Indexers

Indexer

- Runs on dedicated servers
- Listens on receiving ports
- Stores and indexes the data

Forwarder

- Gathers the data
- Sends to indexers over network
  - Most production data is on remote servers

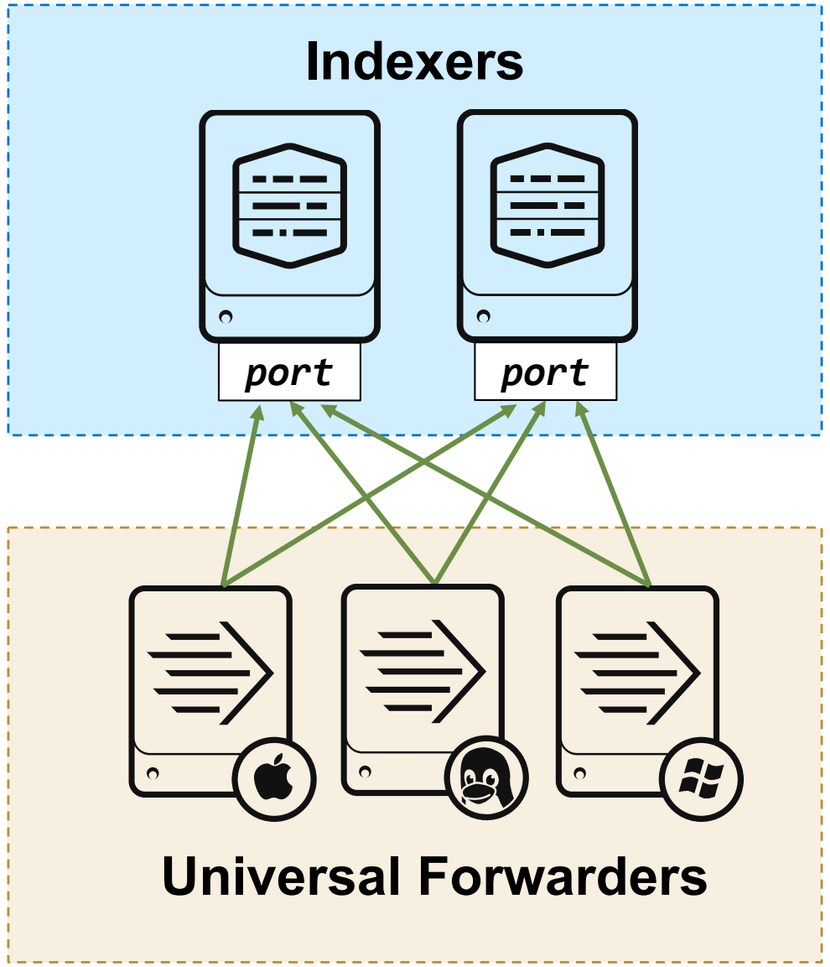


Understanding Universal Forwarders

Universal Forwarders (UF)

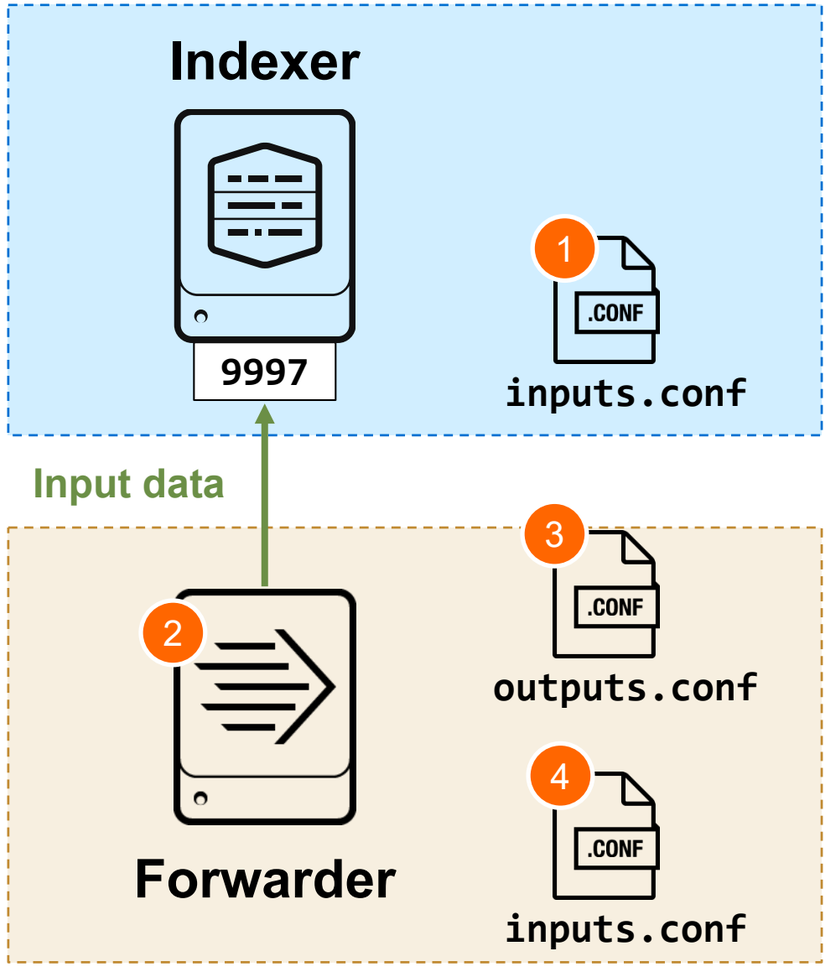
- Gathers data from a host
- Sends data over the network to receiving ports on receivers (usually an indexer)
- Provided as separate installation binary with a built-in license (no limits)
- Designed to run on production servers

  (minimal CPU / memory use, bandwidth constrained to 256 KBps by default, no web interface, cannot search or index)



Universal Forwarder Configuration Steps

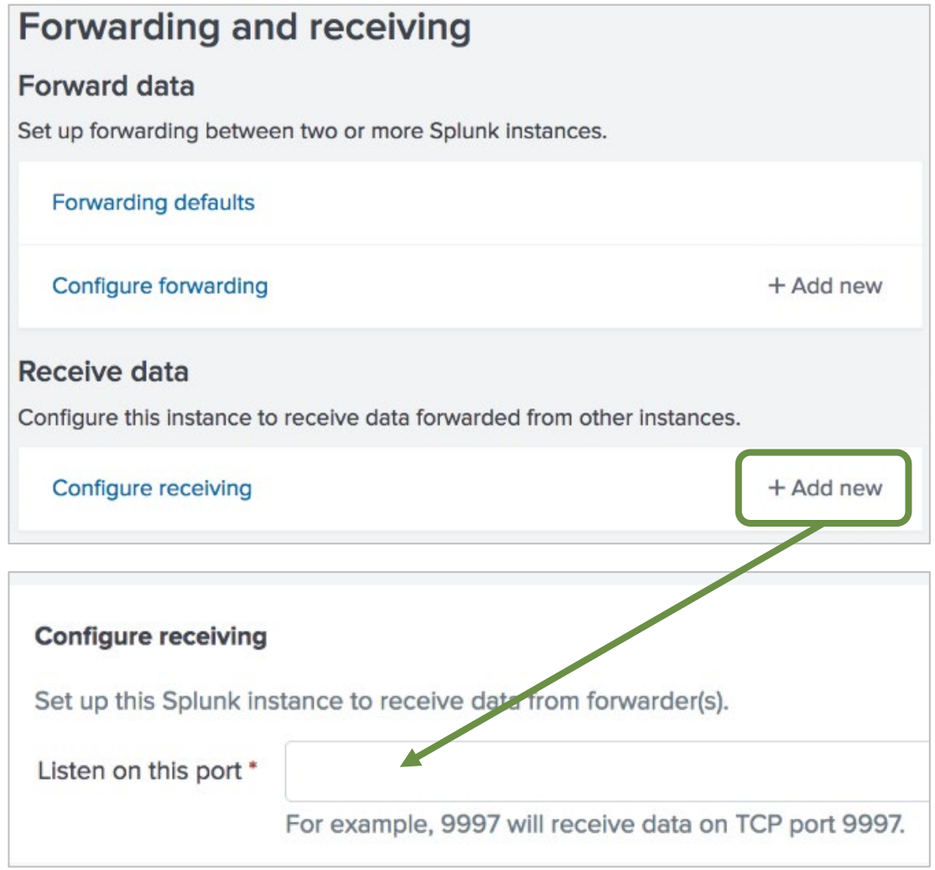
1. Set up a receiving port on each indexer
   - Task only needs to be performed once
2. Download and install Universal Forwarder
3. Set up forwarding on each forwarder
4. Add inputs on forwarders



Configure the Receiving Port on Each Indexer

- Using Splunk Web:
  1. Select **Settings > Forwarding and receiving**
  2. Next to **Configure receiving**, select **Add new**
  3. Enter a port number and click **Save**
  - Stored in most recently visited app: **`SPLUNK_HOME/etc/apps/<app>/local`**
- Using CLI:
  - Run **`splunk enable listen <port>`**
  - Stored in **`SPLUNK_HOME/etc/apps/search/local`**
- Manually in **`inputs.conf`** as:

  `[splunktcp://port]`



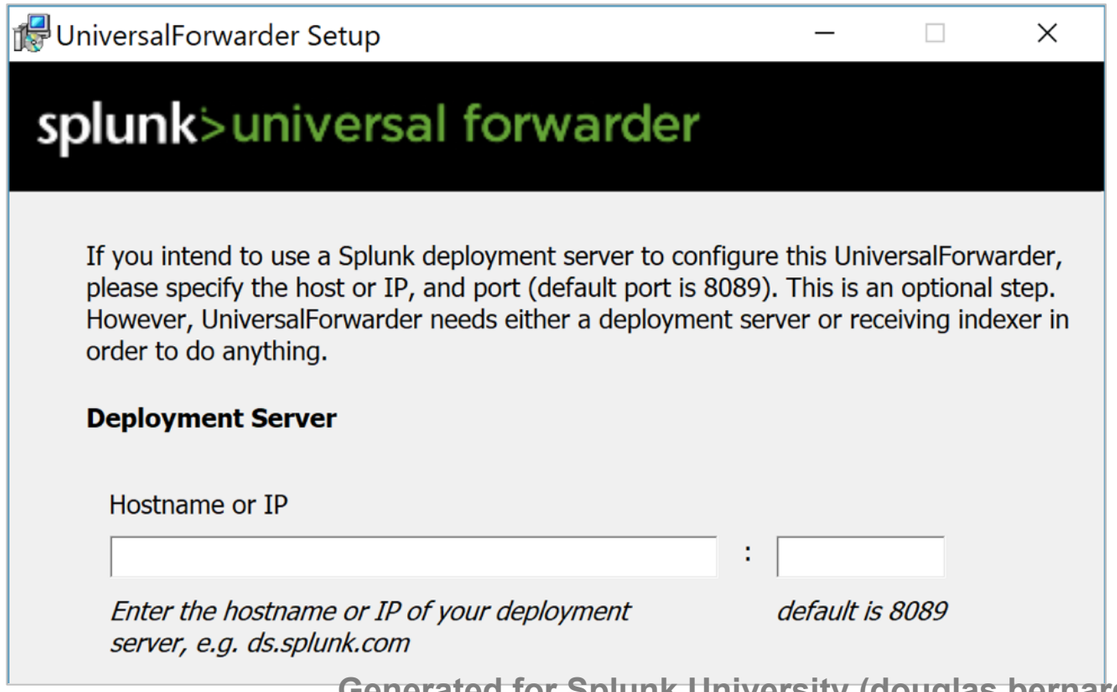
Installing a Universal Forwarder

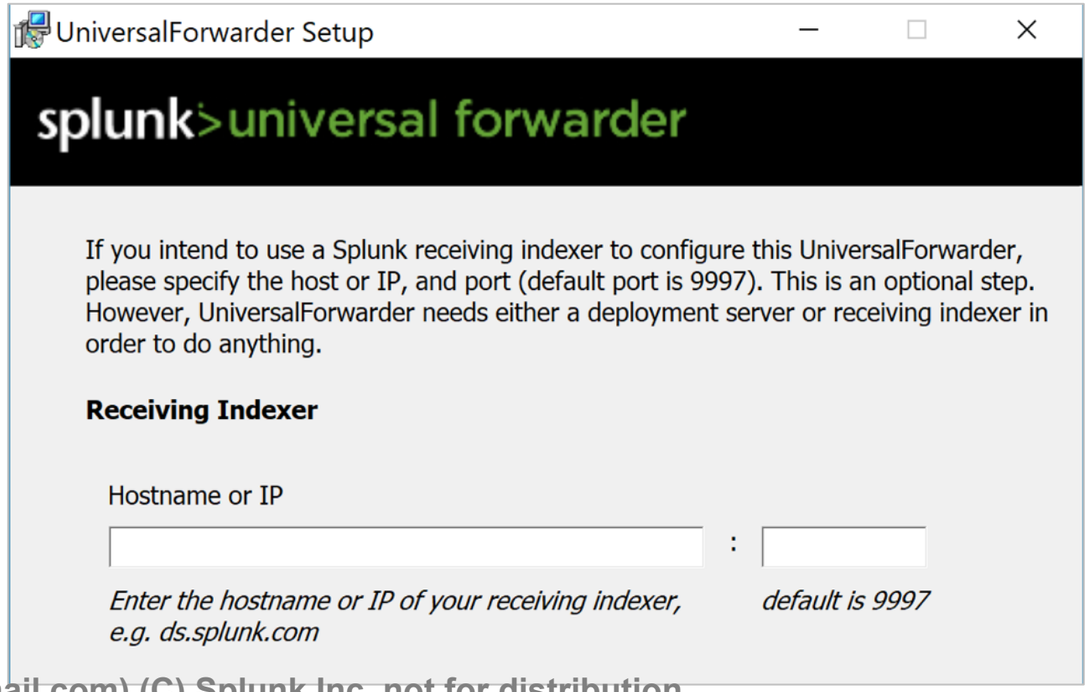
	*NIX	Windows
Download	www.splunk.com/en_us/download/universal-forwarder.html	
Install	• Un-compress **.tgz**, **.rpm**, or **.deb** file in the path Splunk will run from • Default **SPLUNK_HOME** is: **/opt/splunkforwarder**	• Execute **.msi** installer (or use the CLI) • Default **SPLUNK_HOME** is: **C:\Program Files\SplunkUniversalForwarder**

- Silent installation methods exist on all platforms
- Same **splunk** command-line interface in **SPLUNK_HOME/bin**
  - Same commands for start/stop, restart, etc.
  - An admin account and password are required

Using the Interactive Windows Installer

- Most forwarder settings can be configured using the installer wizard
  - Can run as a local or domain user without local administrator privileges
- CLI installation is available for scripted installations
  docs.splunk.com/Documentation/Forwarder/latest/Forwarder/InstallaWindowsuniversalforwarderfromthecommandline





Defining Target Indexers on the Forwarder

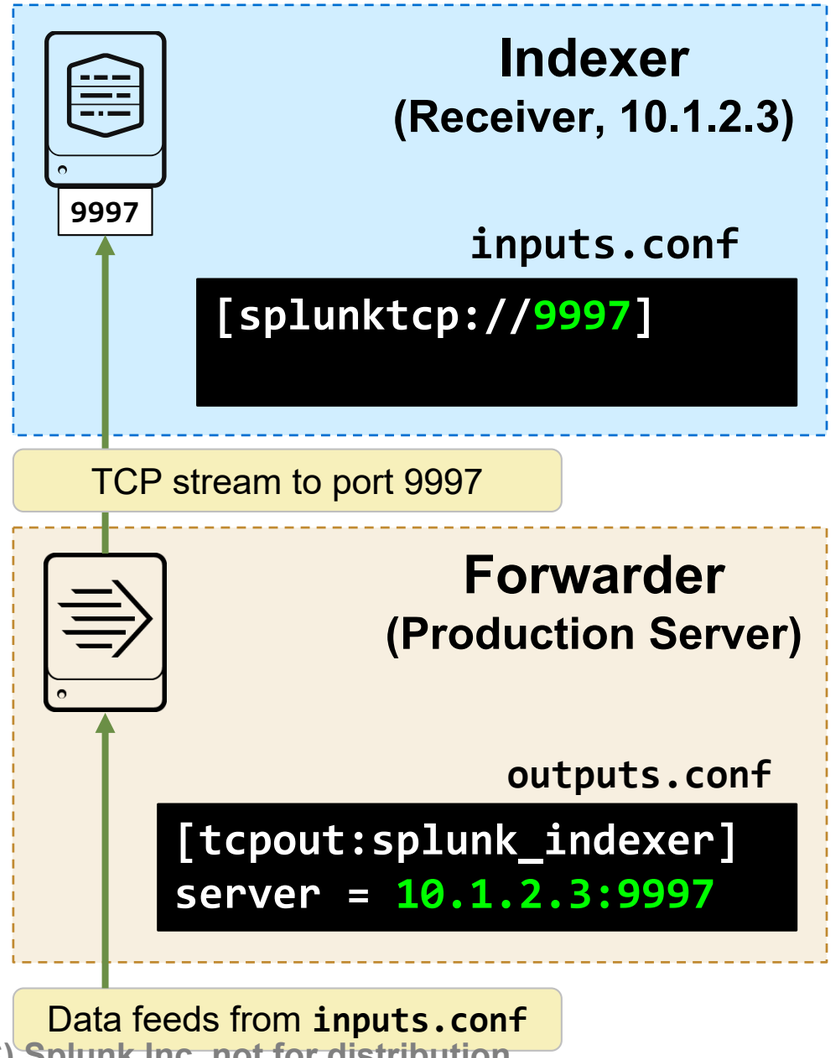
- To configure target indexers on forwarders, either:
  - Run **`splunk add forward-server <indexer:receiving_port>`**
  - Modify **`outputs.conf`**
- Splunk logs are automatically sent to indexer's **`_internal`** index
- Example: **`splunk add forward-server 10.1.2.3:9997`** configures **`outputs.conf`** as:

```
[tcpout]
defaultGroup = default-autolb-group

[tcpout-server://10.1.2.3:9997]

[tcpout:default-autolb-group]
disabled = false
server = 10.1.2.3:9997
```

docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Configureforwardingwithoutputs.conf

Forwarder **outputs.conf** File

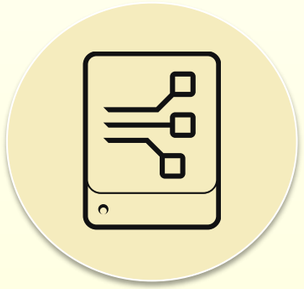
- Points the forwarder to the receivers
  - **splunktcp** stanza sets the indexer to listen on a port for feeds from Splunk forwarders
  - **server** sets a forwarder's destination to one or more receivers (IP or DNS name + receiver port), separated by commas
- Can specify additional options:
  - Load balancing
  - SSL
  - Compression
  - Alternate indexers
  - Indexer acknowledgement



Configuration Validation and Troubleshooting

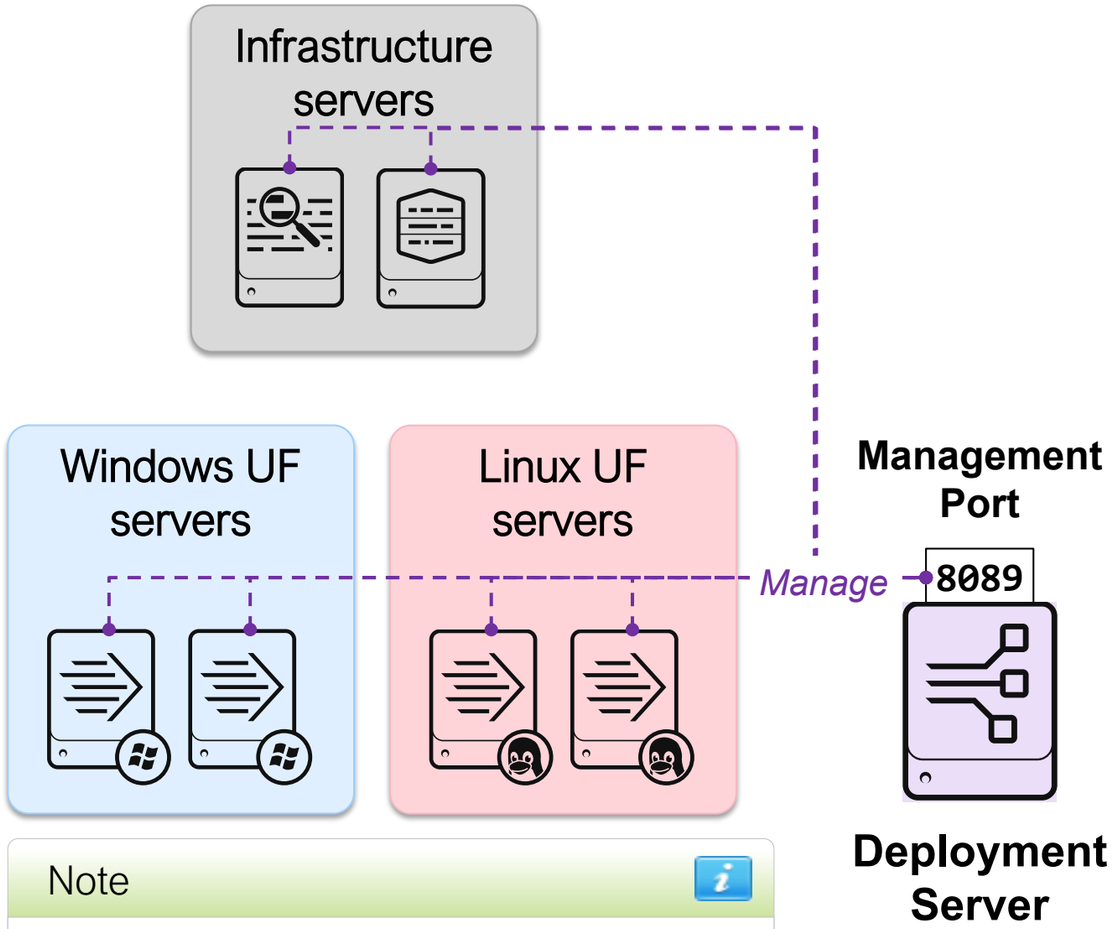
- To verify the configuration:
  - On forwarder, run: **`splunk list forward-server`**
  - On indexer, run: **`splunk display listen`**
- To verify successful connection:
  - On search head, search: `index=_internal host=<forwarder_hostname>`
- Troubleshooting forwarder connection
  - Check **`SPLUNK_HOME/var/log/splunk/splunkd.log`** on forwarder:
    `tail -f splunkd.log | egrep 'TcpOutputProc|TcpOutputFd'`

Understanding the Deployment Server



Deployment Server (DS)

- Built-in tool for centrally managing configuration packages as apps for clients
- Includes **Forwarder Management** as the graphical user interface
- Can restart remote Splunk instances
- Requires an Enterprise license and should be on a dedicated server



Note

This topic is covered in the *Splunk Enterprise Data Administration* course.

 | 15 September 2021

Module 8 Knowledge Check

- True or False. You must configure a separate receiving port on the indexer for each universal forwarder.
- True or False. When a UF is installed on Windows, the instance provides a GUI.
- Running **`splunk add forward-server <indexer:port>`** creates stanzas in which **`.conf`** file?

Module 8 Knowledge Check – Answers

- True or False. You must configure a separate receiving port on the indexer for each universal forwarder.

  False. Many forwarders can forward data to the same port on one indexer.

- True or False. When a UF is installed on Windows, the instance provides a GUI.

  False. Universal Forwarders do not have a GUI on Windows OS or any other OS.

- Running **`splunk add forward-server <indexer:port>`** creates stanzas in which **`.conf`** file?

  `outputs.conf`

Module 8 Lab Exercise

Time: 20 minutes

Description: Basic Forwarder Configuration

Tasks:

- Set up your Splunk indexer as the receiver
- Use CLI to configure and prepare your forwarder to send event data to the receiver
- Confirm the forwarder connection with the MC
- View the contents of the **`outputs.conf`** file on the forwarder

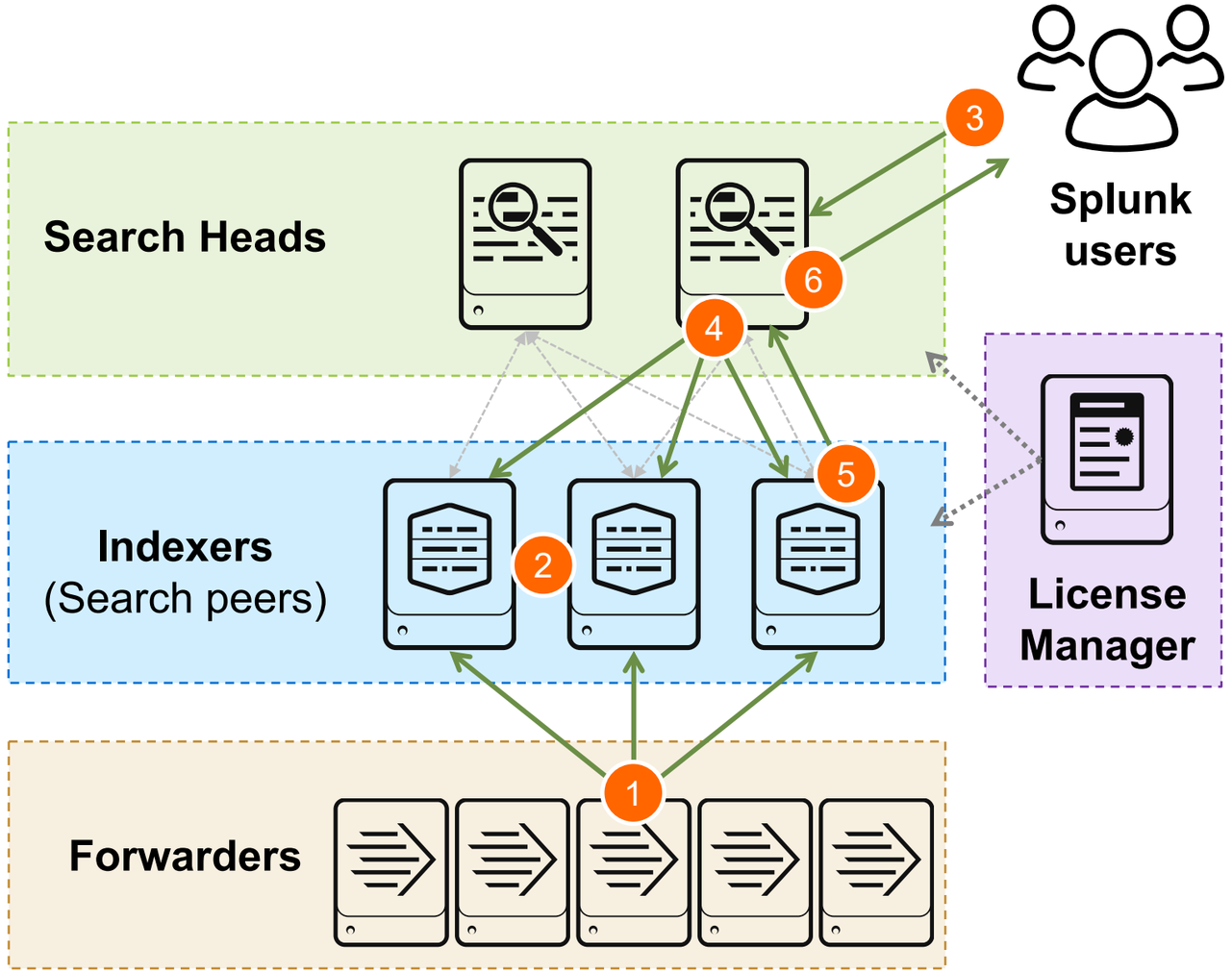
Module 9:
Distributed Search

Module Objectives

- Describe how distributed search works
- Define the roles of the search head and search peers

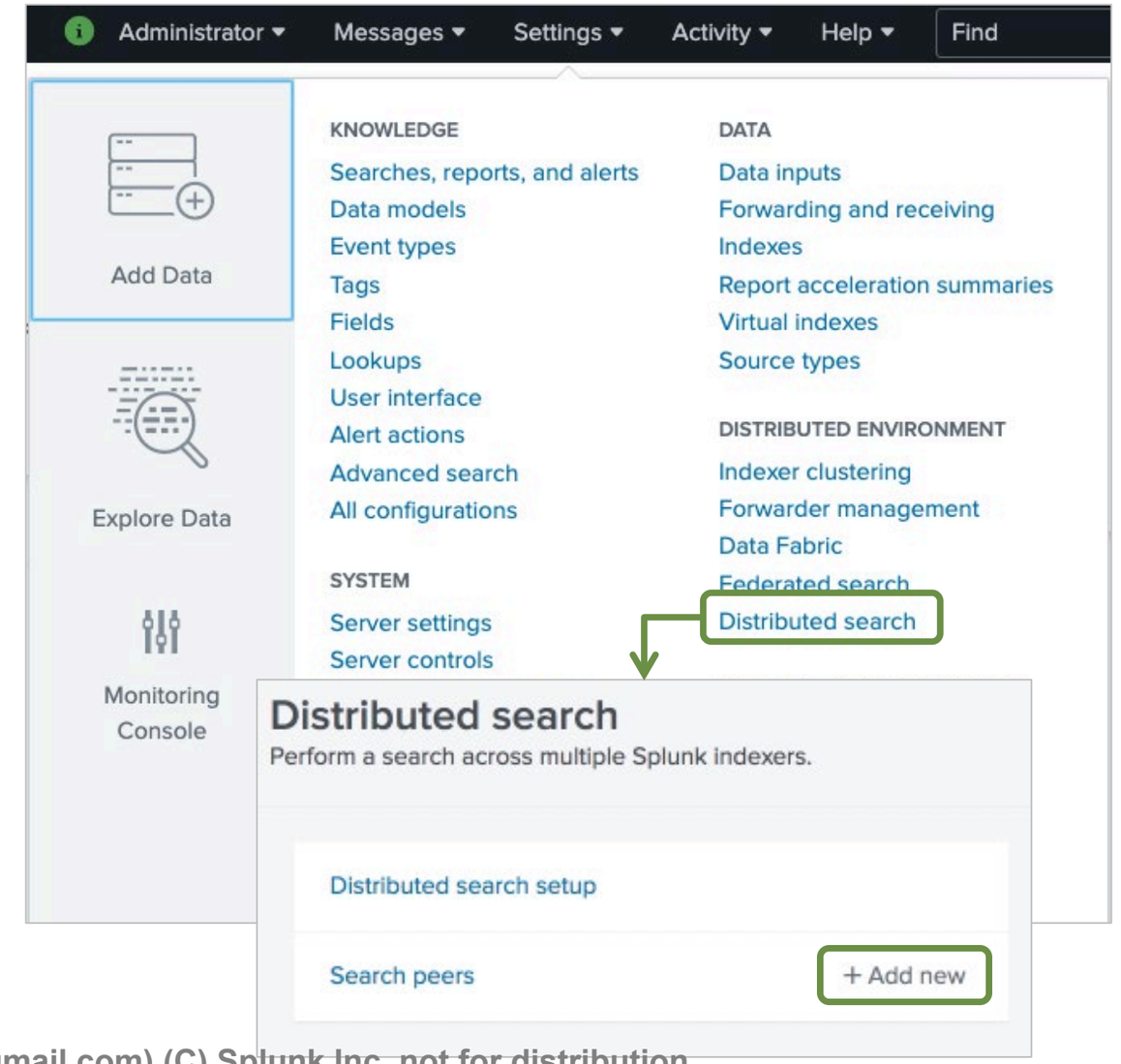
How Distributed Search Works

1. Universal forwarders (production servers) send data to indexers
2. Indexers (search peers) store their portion of the data
3. Users log on to the search head and run reports
4. The search head dispatches searches to the indexers
5. Indexers run searches in parallel and return their portion of results
6. The search head consolidates the individual results and prepares reports

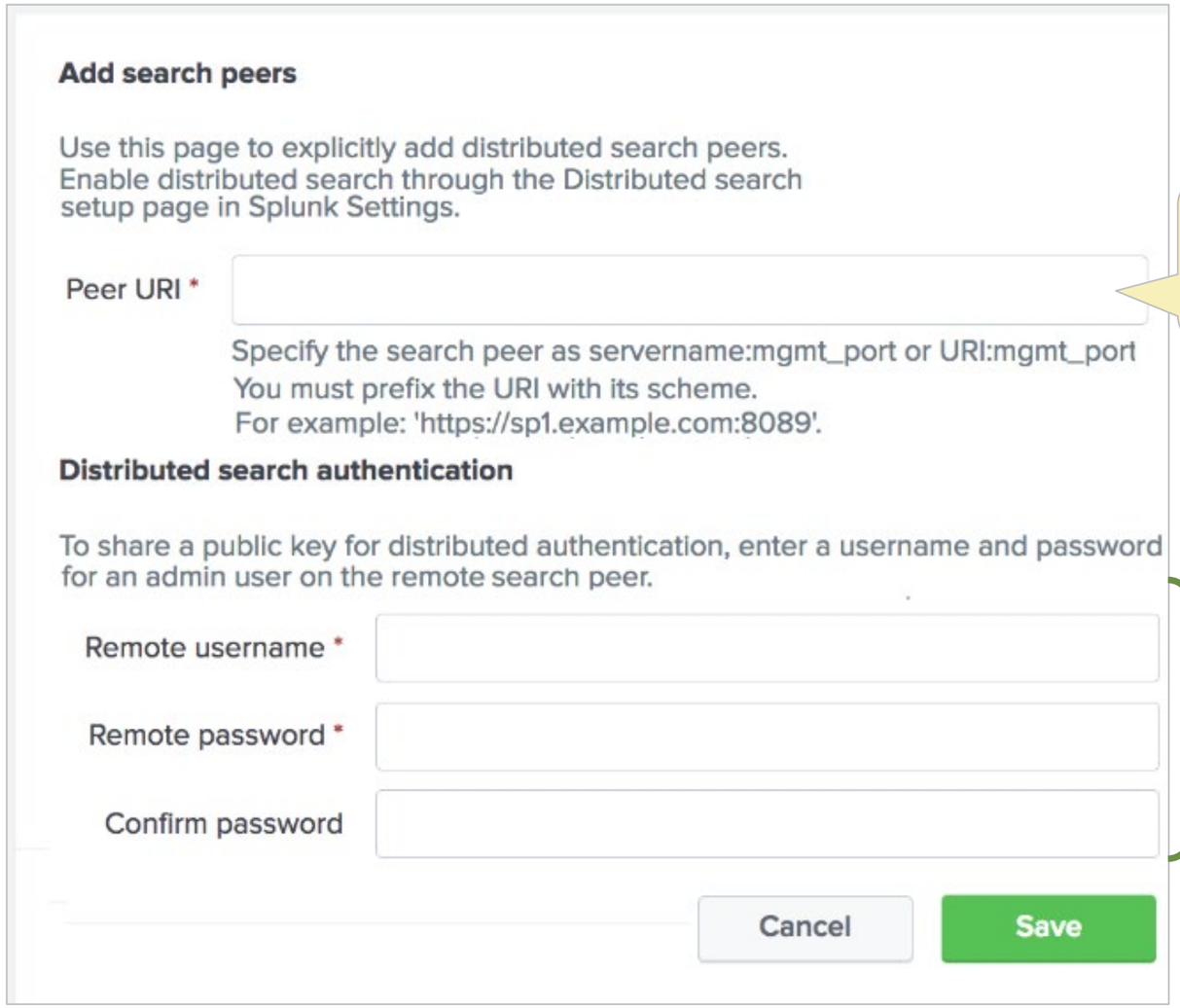


Setting Up Distributed Search

1. Install Splunk on each search head and indexer (search peer)
2. Set up the same indexes on all indexers
3. All search heads and indexers should use a License Manager
4. Add a user to each indexer with a role with **`edit_user`** capability
   - Used only for authenticating a search head to the indexer
5. On the search head, configure indexers by selecting: **Settings > Distributed search**
   - Distributed search is turned on by default, so just add search peers



Adding Indexers (Search Peers)



Enter the ***servername:port*** for the indexer

User account with **`edit_user`** capability

 | 15 September 2021

Knowledge Bundles and Replication

- Knowledge bundles
  - Distributed to indexers (search peers) by the search head when a distributed search is initiated
  - Contain the knowledge objects required by indexers for searching
  - Found in:

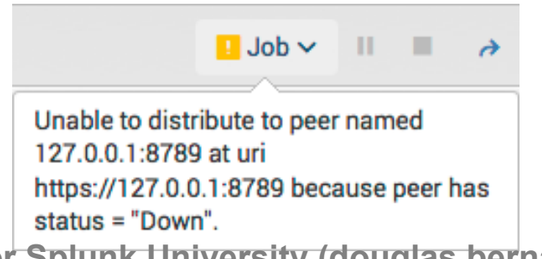
    `SPLUNK_HOME/var/run` on the search head

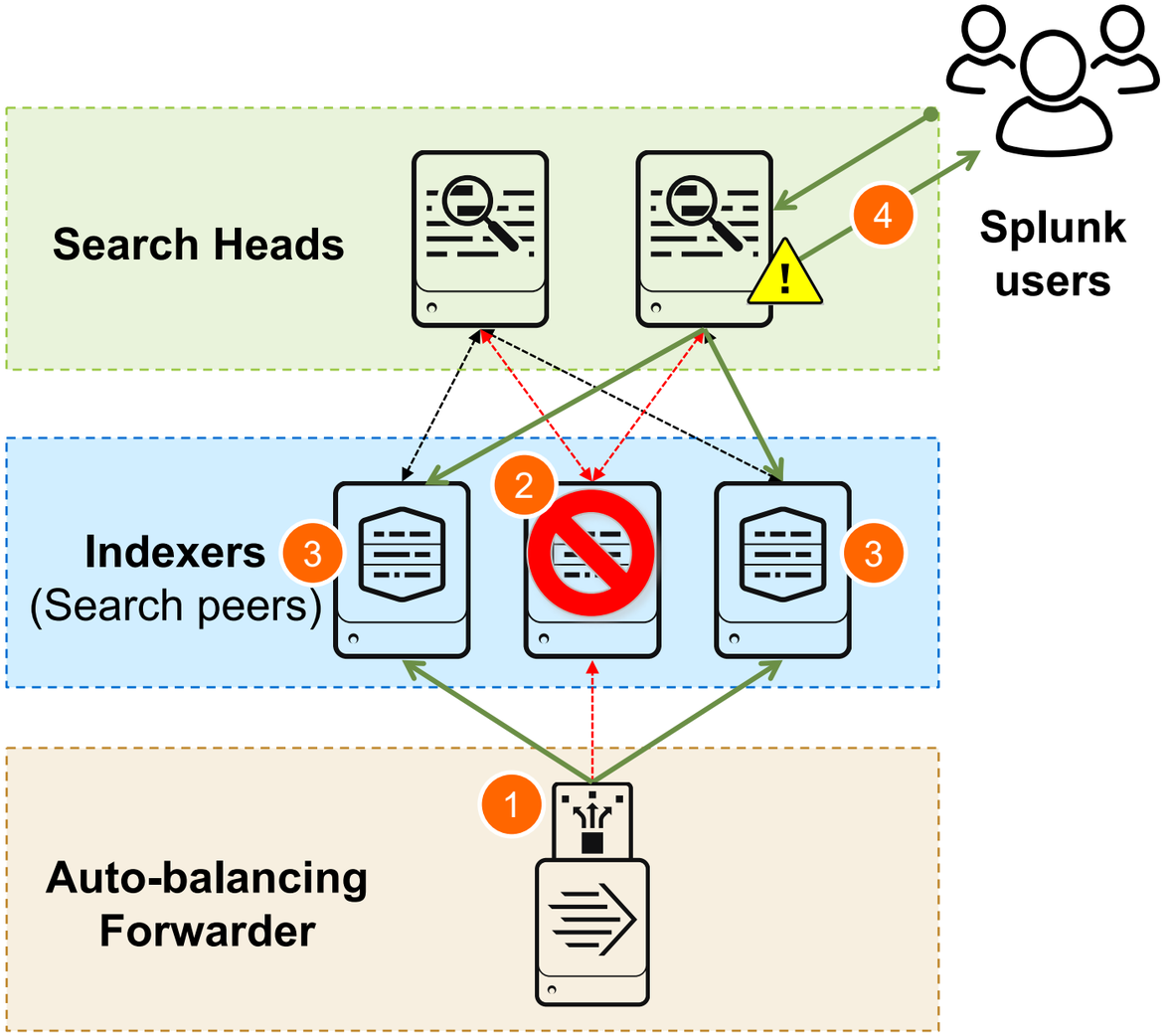
    `SPLUNK_HOME/var/run/searchpeers` on the indexer (search peer)
- Replication status of knowledge bundles
  - Splunk Web: **Settings** > **Distributed search** > **Search peers** under the **Replication Status** column

Indexer (Search Peer) Failure

- When an indexer goes down:
  1. Forwarders automatically use only available indexers
  2. Offline indexer does not participate in searches
  3. Remaining indexers handle all indexing and searches
  4. Notification is provided
- Notification message sent to user when an indexer goes down during a job:

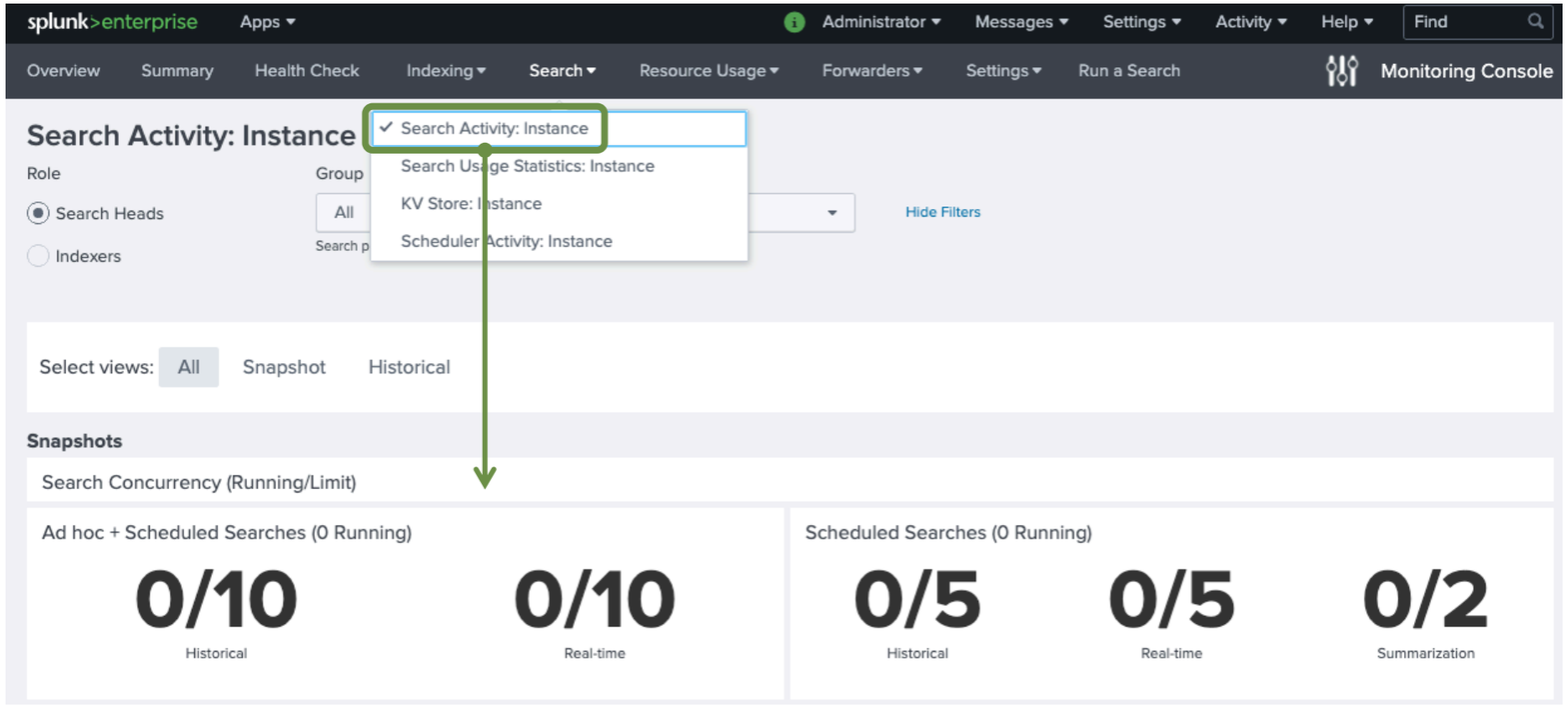
  `Search results may be incomplete: the search process on peer indexer_name ended prematurely.`
- Message shown when an indexer is already down:





Viewing Search Peer Status with MC

- Provides a graphical view of the status of indexers (search peers):
  - Median resource usage (Memory, CPU)
  - Top 10 memory-consuming searches
  - Aggregate search runtime



Search Peer Quarantine

- Quarantine of an indexer (search peer)
  - Used when an indexer is experiencing performance issues
  - Prevents indexer from participating in future searches
    - Attempts to complete any currently running searches
  - Allows live troubleshooting by not stopping the indexer
  - Only affects the relationship between indexer and search head
- Performed in Splunk Web: **Settings > Distributed search > Search peers**
- Performed from search head using CLI:

```
splunk edit search-server –auth <user:password> <host:port>
  -action quarantine
```

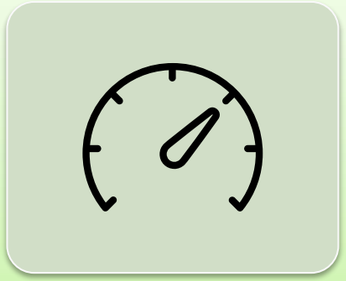

Use Cases for Multiple Search Heads

Access control

- Control who can access which indexes using what apps
- Dedicate search heads for functional areas: IT Ops, Security, or Business Intelligence (BI)

Manage geo-dispersed data

- Allow local offices to access their own data while maintaining centralized indexers



Performance enhancement

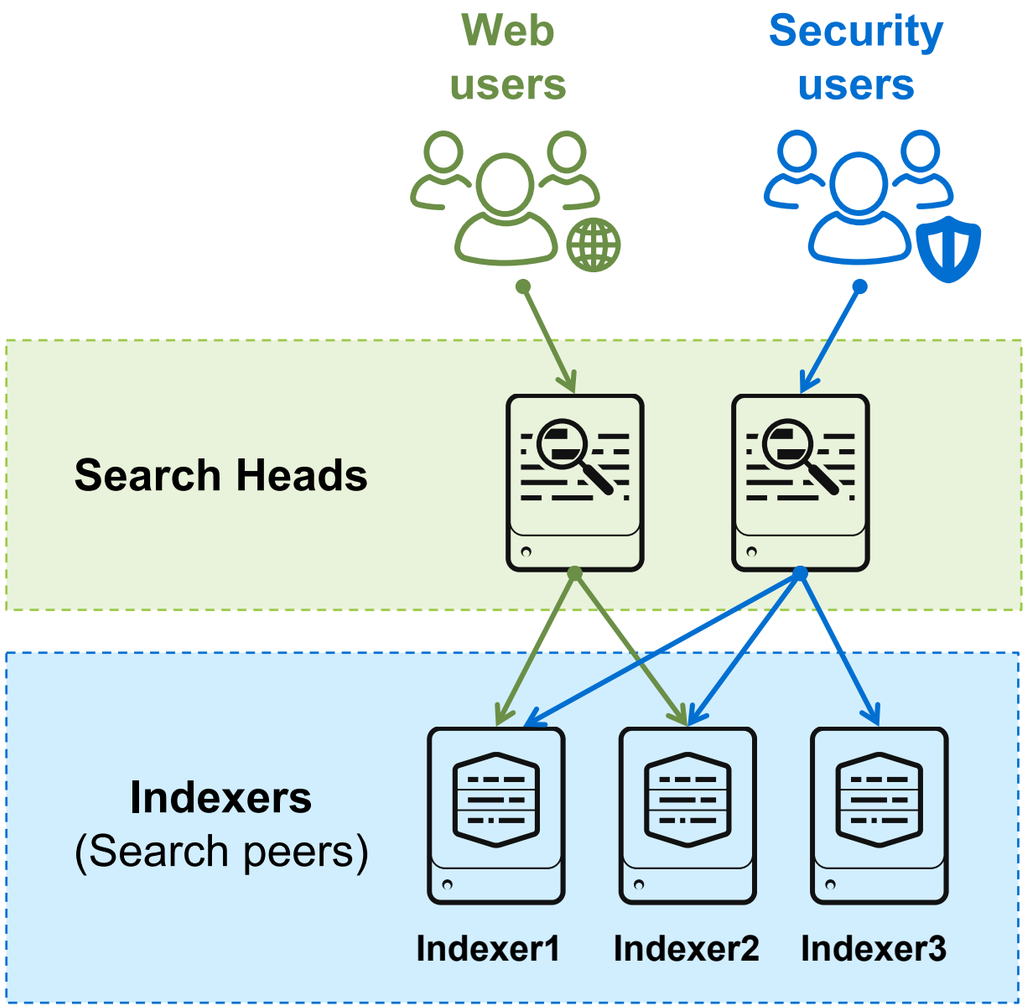
- Distribute indexing and search loads across multiple servers
- Facilitates horizontal scaling

Determining the Number of Search Heads

- Each search head handles ~8 - 12 simultaneous searches
  - Total includes both ad hoc and scheduled searches
  - Exact number depends on types of searches and search head hardware (especially CPU cores)
- Search heads can be added to the distributed group at any time
- Search heads can be:
  - **Dedicated**: Search heads don't share knowledge objects
  - **Clustered**: Share a common set of knowledge objects

Dedicated Search Heads

- Each search head
  - Contains its own unique set of reports, dashboards, and so on
  - Dedicated to a team of users with unique knowledge objects
- More than one search head can be configured for the same set of indexers (search peers)



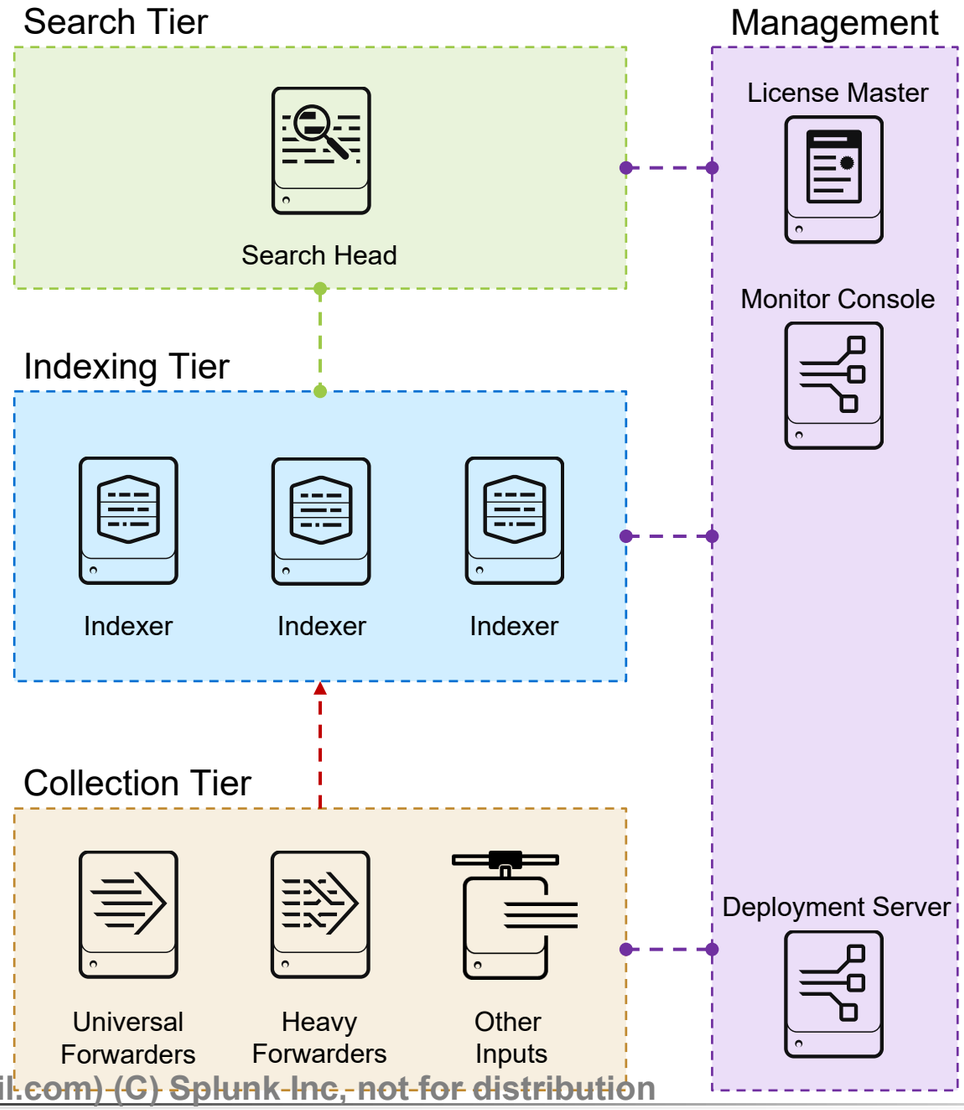
Distributed Search Best Practices

splunk> Best Practice

- Dedicate a host for each role
  - Combine server roles with caveats
  - Discussed in the *Architecting Splunk Deployments* course
- Disable Splunk Web on instances that don't require it

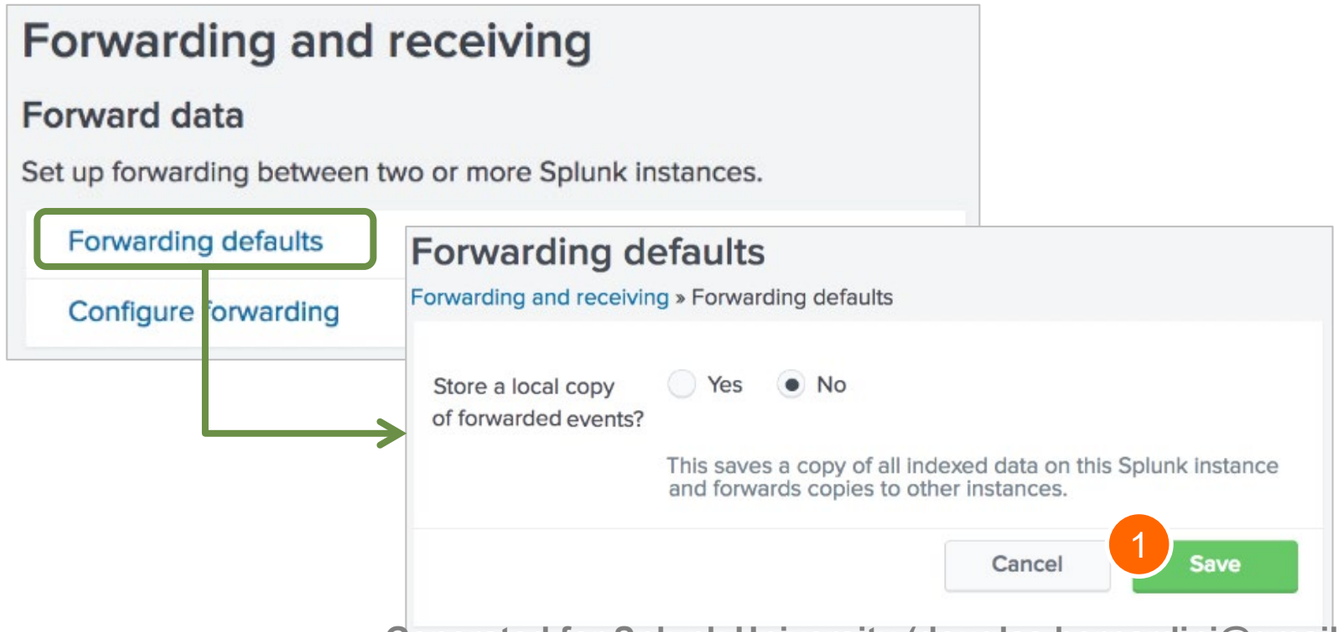
```
splunk disable webserver
```

- Use Deployment Server
  - Discussed in the *Splunk Enterprise Data Administration* course



Distributed Search Best Practices (cont.)

- Forward any data being indexed by the search heads to indexers
  - Centralizes data on indexers, which simplifies management
  - Allows diagnosis from other search heads if one goes down
  - Allows other search heads to access all summary indexes



outputs.conf

2

```
[indexAndForward]
index = false

[tcpout]
defaultGroup = default-autolb-group
forwardedindex.filter.disable = true
indexAndForward = false

[tcpout:default-autolb-group]
server=idx1:9997,idx2:9997
```

Module 9 Knowledge Check

- True or False. When adding a Search Peer you must enter a username and password of an account on the search peer, with **`edit_roles`** capability.
- True or False. Knowledge bundles contain the knowledge objects required by the indexers for searching.
- True or False. A quarantined search peer is prevented from performing new searches but continues to attempt to service any currently running search

Module 9 Knowledge Check – Answers

- True or False. When adding a Search Peer you must enter a username and password of an account on the search peer, with **`edit_roles`** capability.

  False. The account must have **`edit_user`** capability.

- True or False. Knowledge bundles contain the knowledge objects required by the indexers for searching.

  True.

- True or False. A quarantined search peer is prevented from performing new searches but continues to attempt to service any currently running search.

  True.

Module 9 Lab Exercise

Time: 10 minutes

Description: Distributed Search

Tasks:

- Add a search peer to your search head
- Search for indexes and source types on the search peer

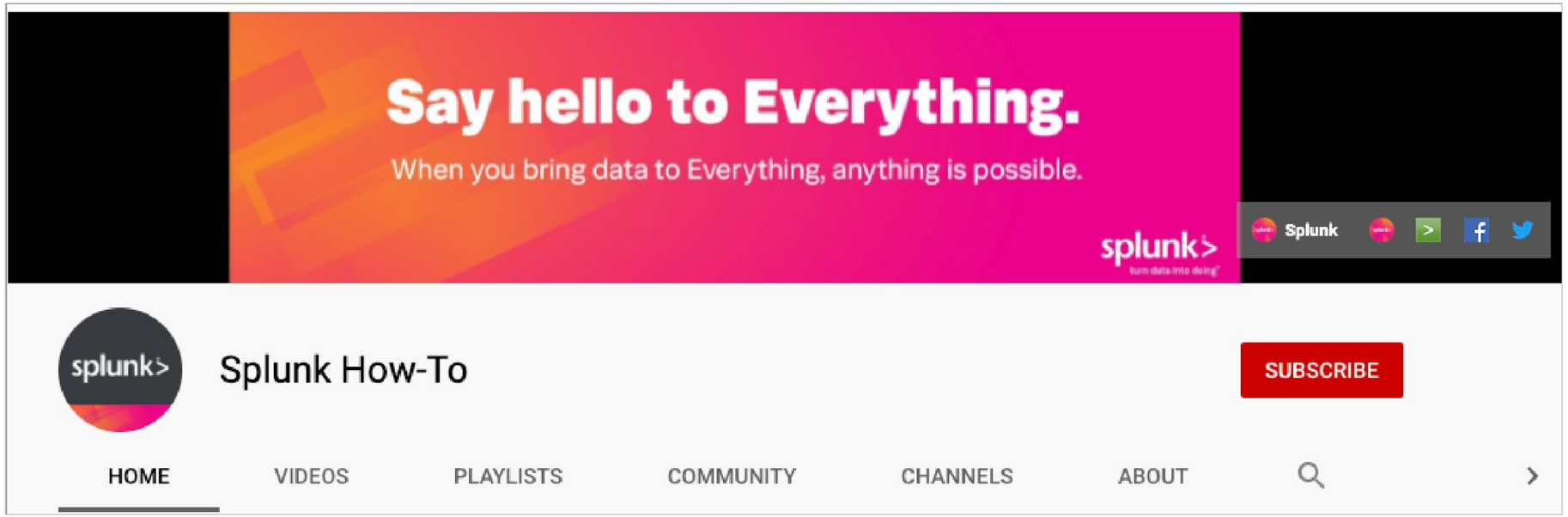
Course Wrap-up

Community

- Splunk Community Portal
  splunk.com/en_us/community.html
  - Splunk Answers
    answers.splunk.com
  - Splunk Apps
    splunkbase.com
  - Splunk Blogs
    splunk.com/blog/
  - Splunk Live!
    splunklive.splunk.com
  - .conf
    conf.splunk.com
- Slack User Groups
  splk.it/slack
- Splunk Dev Google Group
  groups.google.com/forum/#!forum/splunkdev
- Splunk Docs on Twitter
  twitter.com/splunkdocs
- Splunk Dev on Twitter
  twitter.com/splunkdev
- IRC Channel
  #splunk on the EFNet IRC server

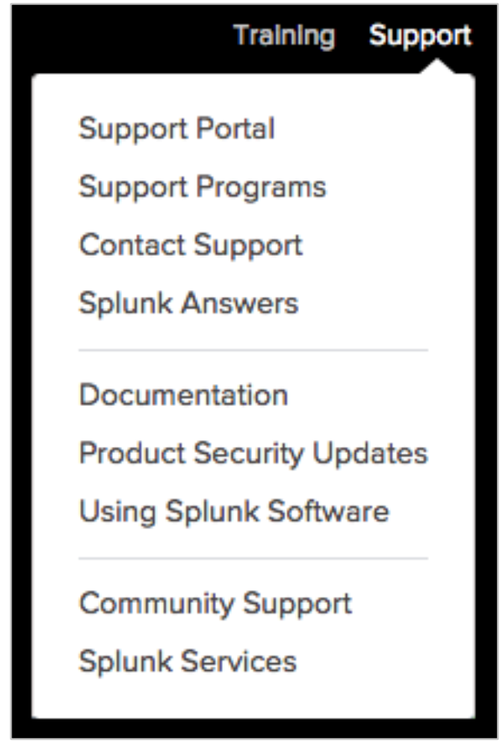
Splunk How-To Channel

- Check out the Splunk Education How-To channel on YouTube: splk.it/How-To
- Free, short videos on a variety of Splunk topics



Support Programs

- **Web**
  - Documentation: dev.splunk.com and docs.splunk.com
  - Wiki: wiki.splunk.com
- **Splunk Lantern**
  Guidance from Splunk experts
  - lantern.splunk.com
- **Global Support**
  Support for critical issues, a dedicated resource to manage your account – 24 x 7 x 365
  - Web: splunk.com/index.php/submit_issue
  - Phone: (855) SPLUNK-S or (855) 775-8657
- **Enterprise Support**
  - Access customer support by phone and manage your cases online 24 x 7 (depending on support contract)



splunk> .conf21

.conf21 Las Vegas

October 18–21

.conf21 Virtual

October 19–20

Splunk University

October 16–18

Thank You

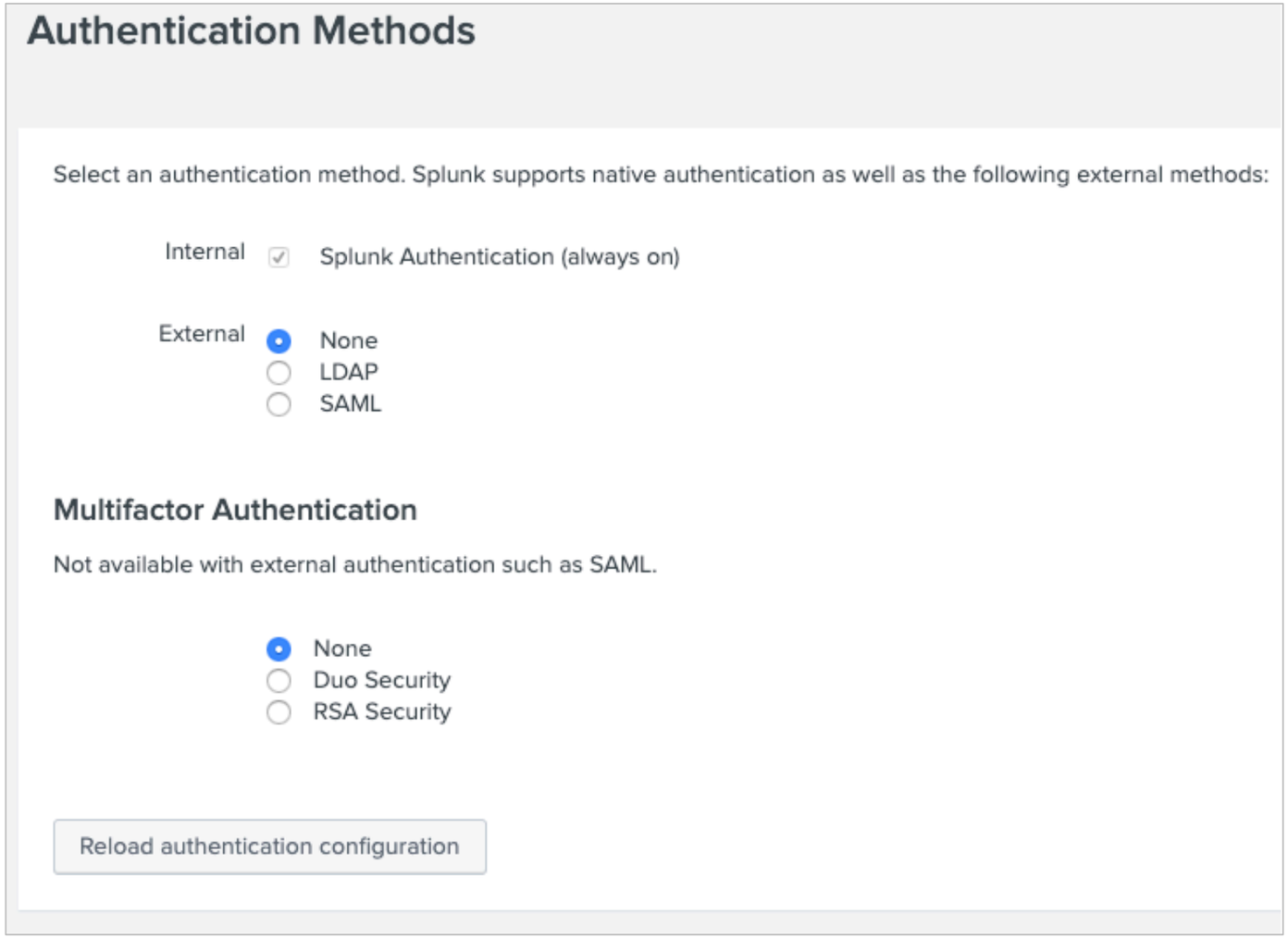
Appendix A:
Splunk Authentication Management

Module Objectives

- Overview of integrating Splunk with LDAP
- Overview of integrating Splunk with SAML
- Overview of integrating Splunk with Multifactor Authentication

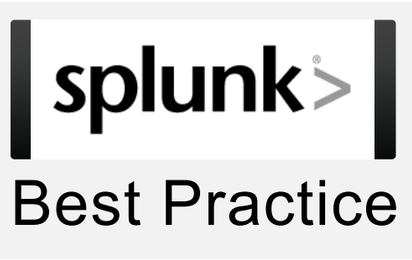
Splunk Authentication Options

- Supported user accounts:
  - Native Splunk accounts
  - LDAP or Active Directory
  - SAML
  - Scripted access to PAM, RADIUS, or other user account systems
- Settings are saved in **`authentication.conf`**



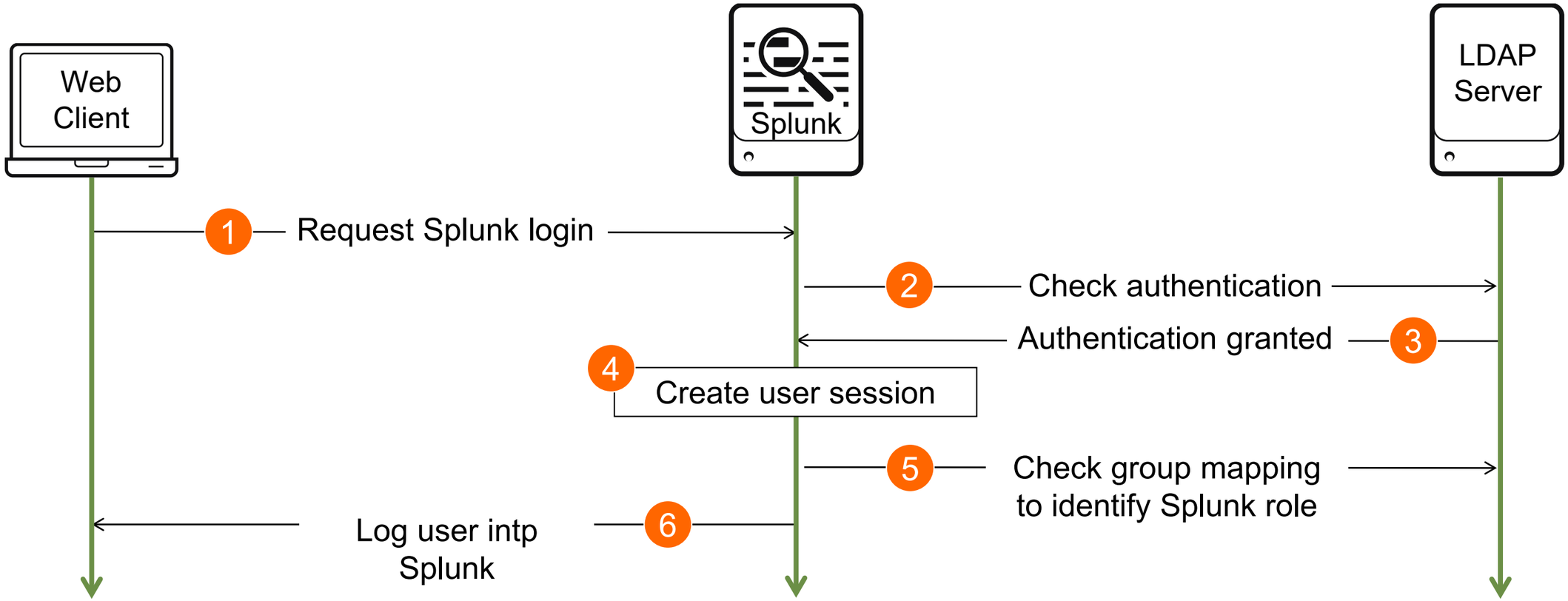
Directory Server Integration

- **Best practice:** Integrate Splunk with a directory server
  - Works with multiple LDAP servers, including OpenLDAP and Active Directory
  - Can be configured from Splunk Web or CLI
- User accounts stored in directory server
  - Enforces LDAP user account and password policies
  - Allows users to use same credentials in Splunk as used elsewhere
  - Allows mapping of LDAP groups to Splunk roles



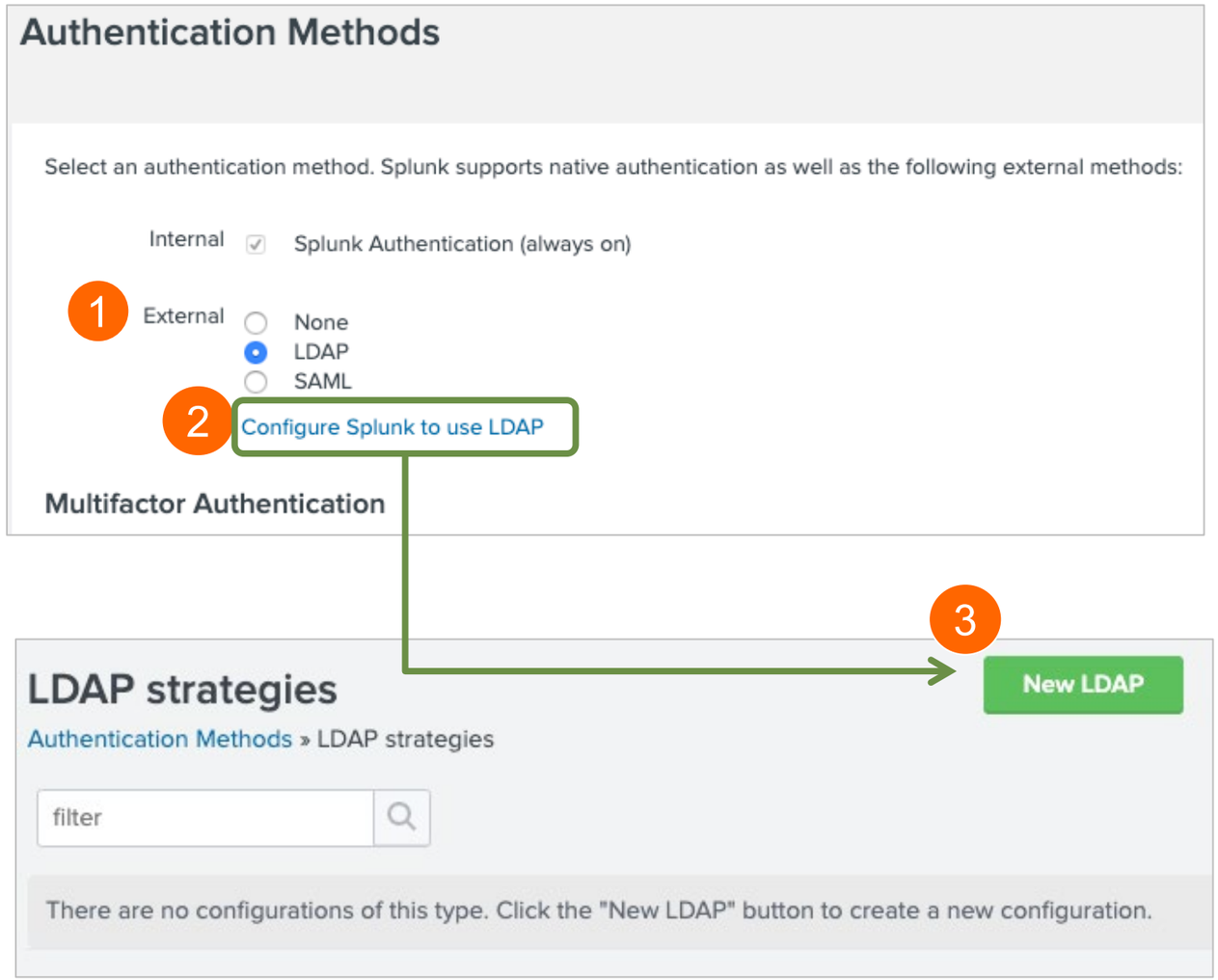
LDAP Authentication

LDAP maintains the user credentials - user ID and password, plus other information - centrally and handles all authentication



Creating an LDAP Strategy

1. Select **External** authentication method: **LDAP**
2. Click **Configure Splunk to use LDAP**
   - View the list of current LDAP strategies (connections to one or more LDAP nodes on an LDAP server)
   - Multiple LDAP servers can be defined
3. Click **New LDAP** to add a new LDAP strategy
   - Name the strategy and fill out the form

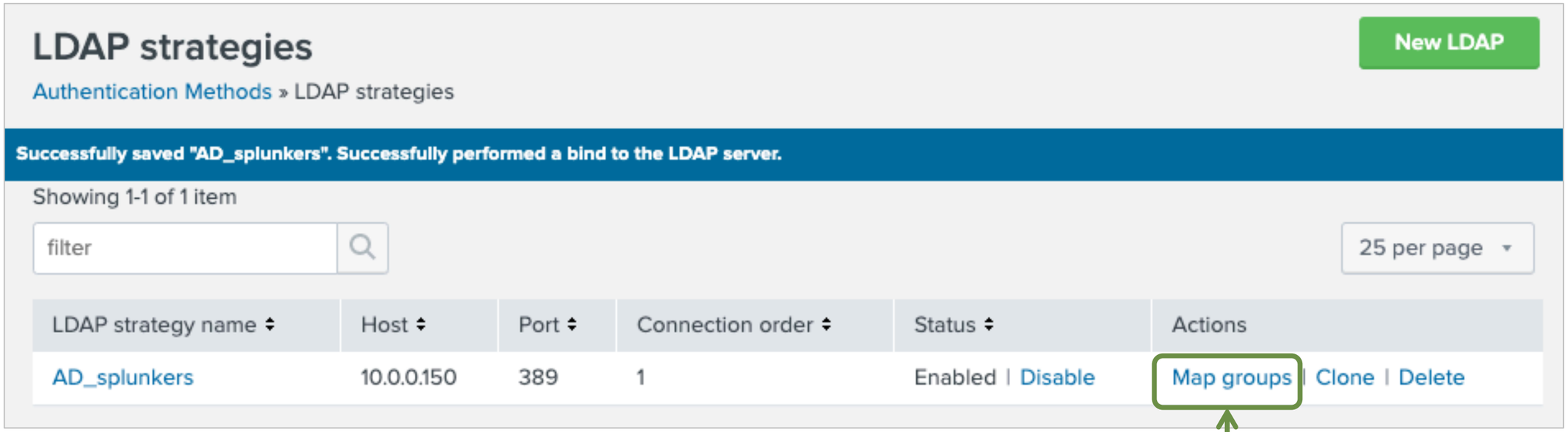


LDAP Strategy Settings

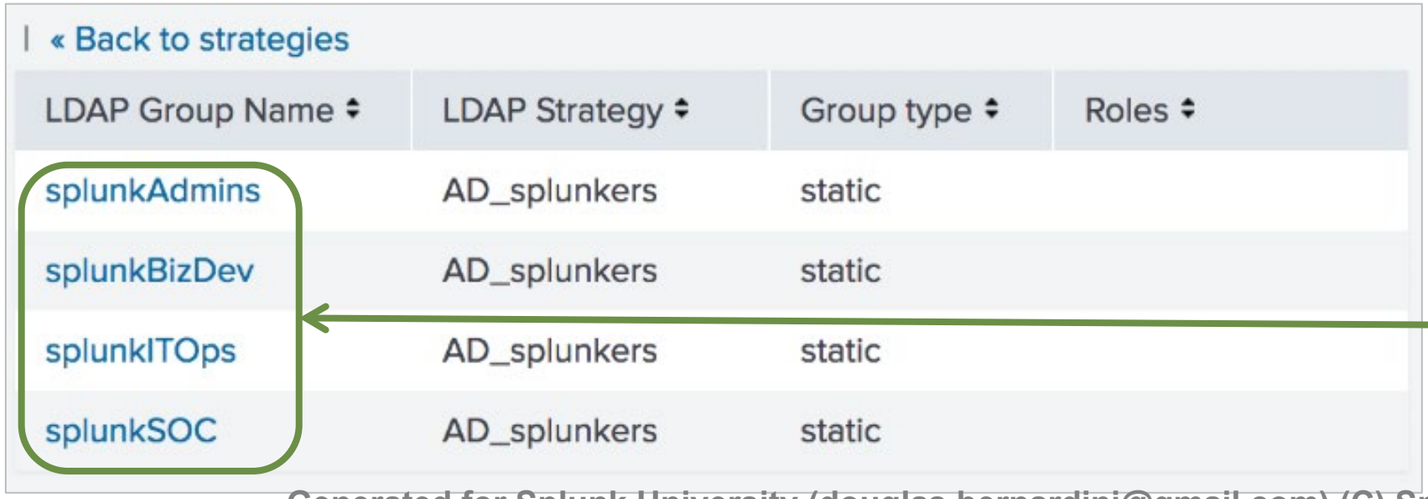
- Configuration is based on information from LDAP
  - LDAP connection settings
  - User settings
  - Group settings
  - Dynamic group settings
  - Advanced settings

```
host = 10.0.0.150
port = 389
SSLEnabled = 0
bindDN = adsuser@buttercupgames.local
bindDNpassword = <some_hashed_pw>

userBaseDN = OU=splunk,DC=buttercupgames,DC=local
userNameAttribute = samaccountname
realNameAttribute = displayname

groupBaseDN =
  OU=splunk,DC=buttercupgames,DC=local
groupNameAttribute = cn
groupMemberAttribute = member
nestedGroups = 0
groupMappingAttribute = dn

network_timeout = 20
sizelimit = 1000
timelimit = 15
```


Mapping LDAP Groups to Roles

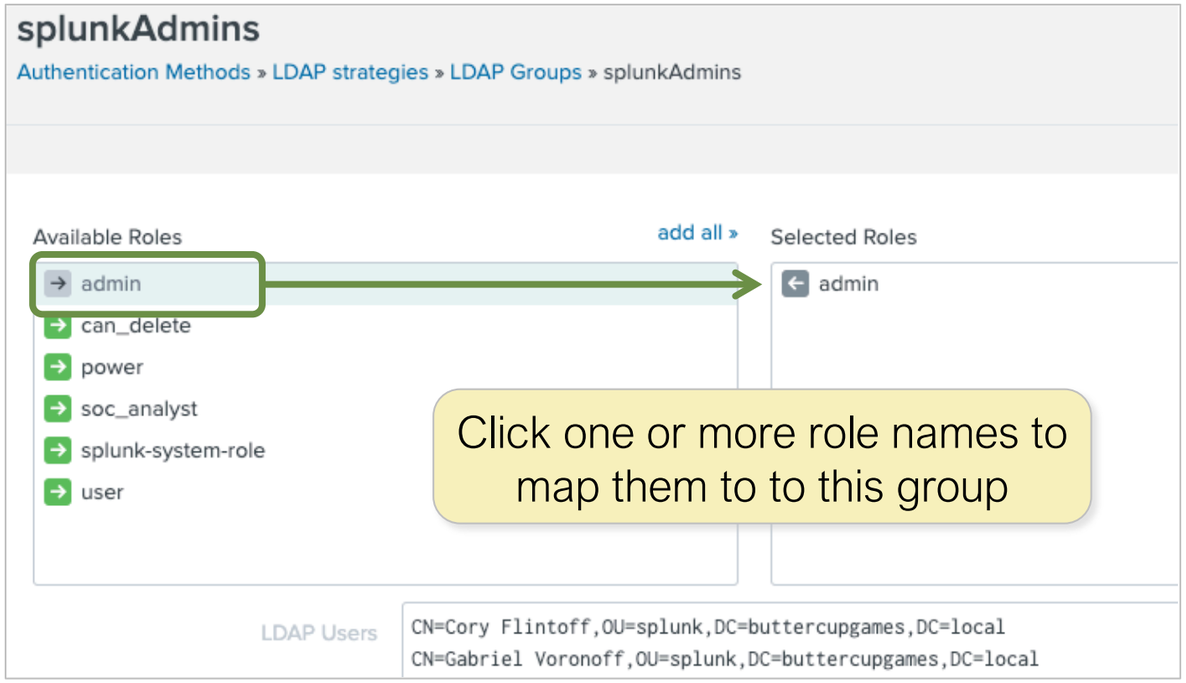


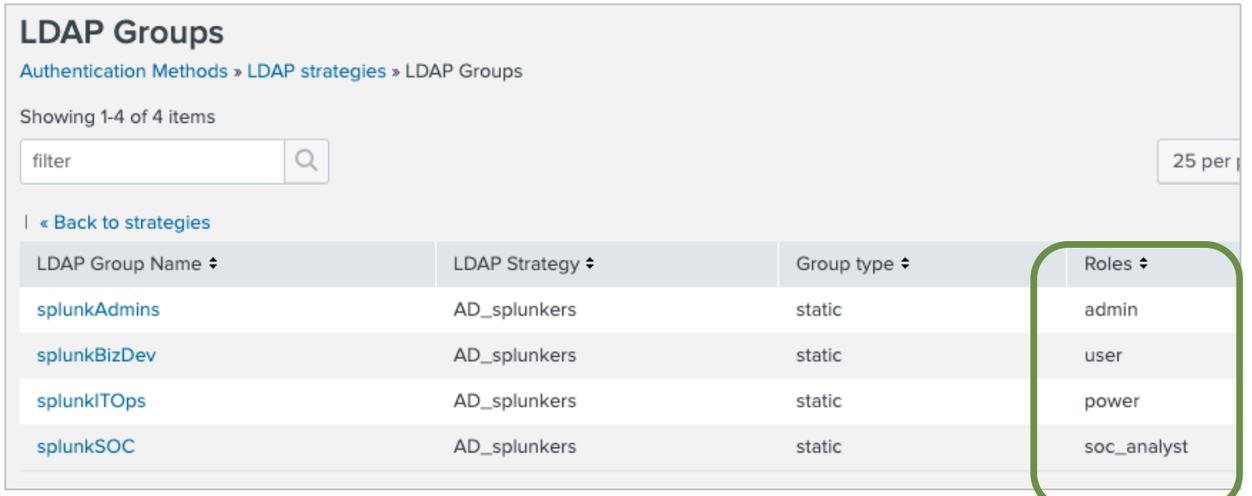
Select to define relationships between LDAP groups and Splunk roles



Click an LDAP group name to map it to one or more Splunk roles

Mapping LDAP Groups to Roles (cont.)



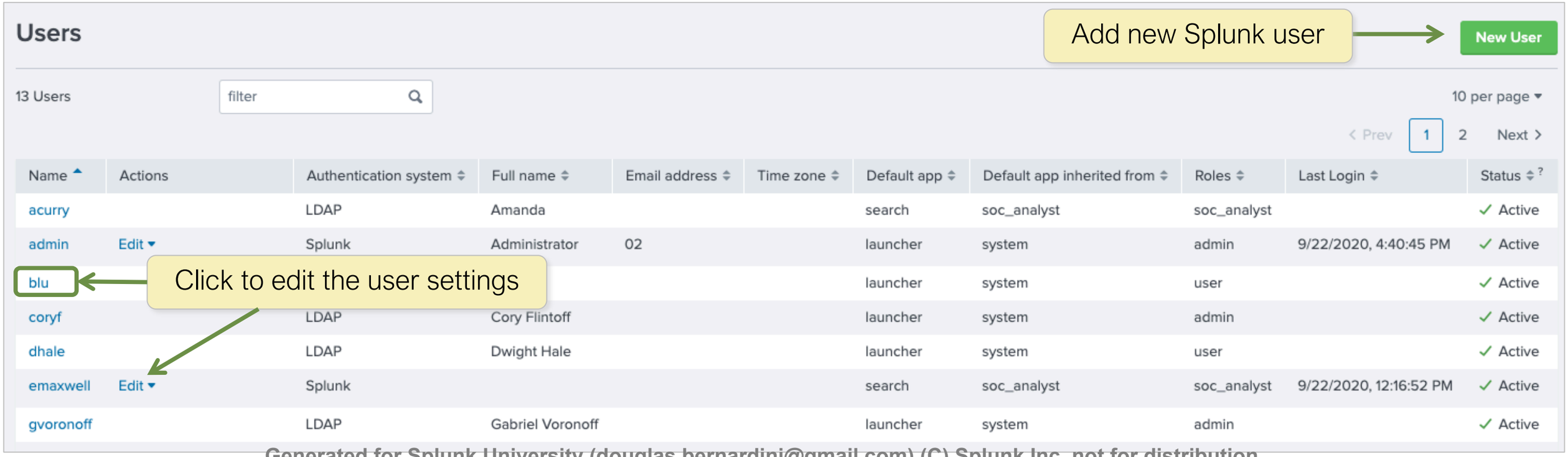


After completing the mapping for all LDAP groups, the mapped roles are shown here

- Not all groups must be mapped
- Mappings can be changed at any time
  - The LDAP server is rechecked each time a user logs into Splunk
  - A user cannot log in unless they have a Splunk role

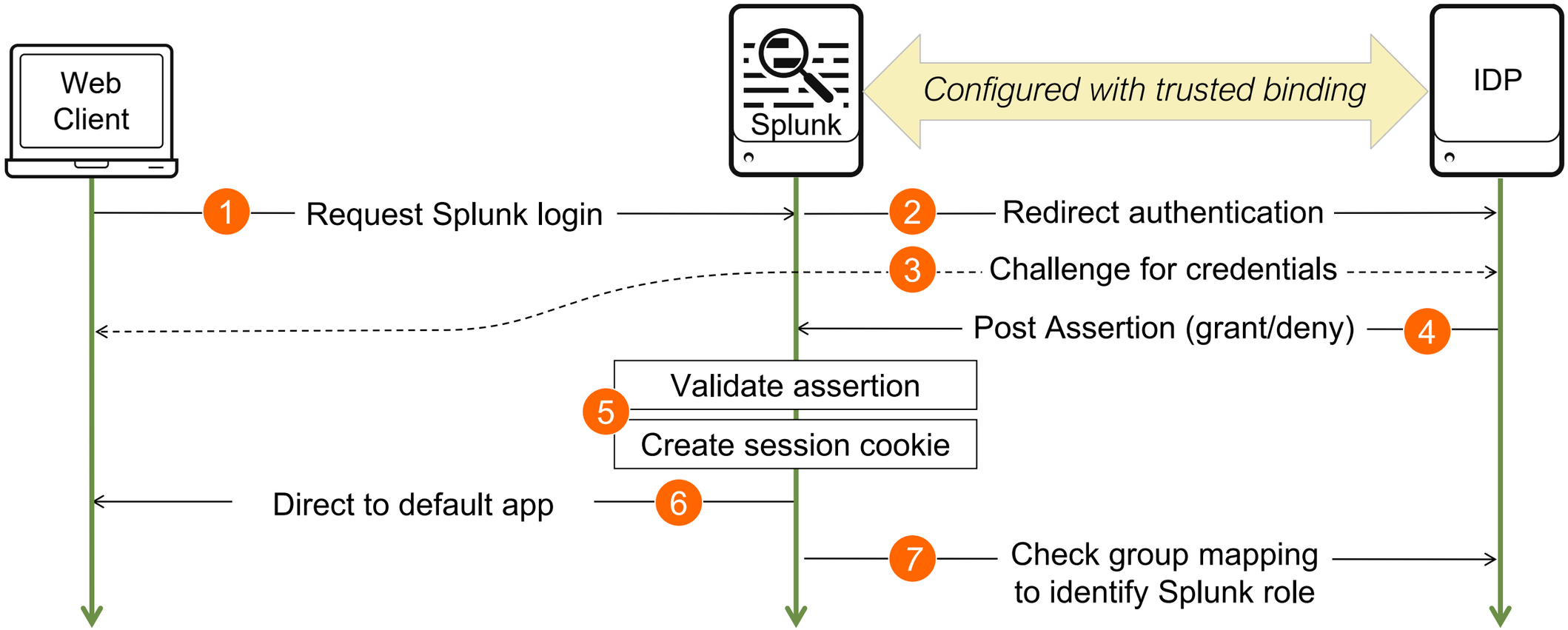
Managing Users in Splunk

- Splunk native users can be edited or deleted
- Only time zone and default app can be changed on LDAP or other users

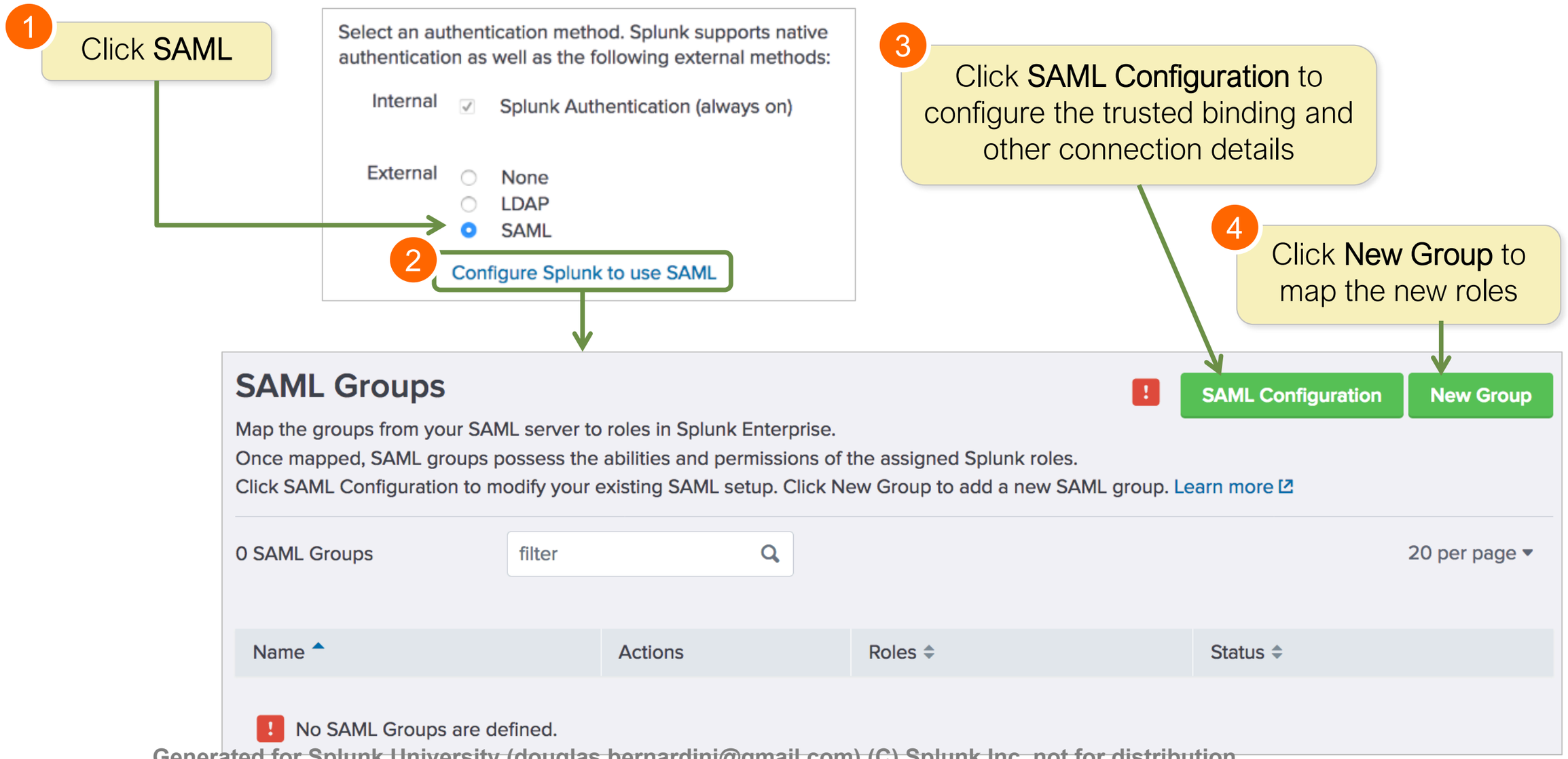


SAML 2.0 Single Sign On

Identity provider (IDP) maintains the user credentials and handles authentication

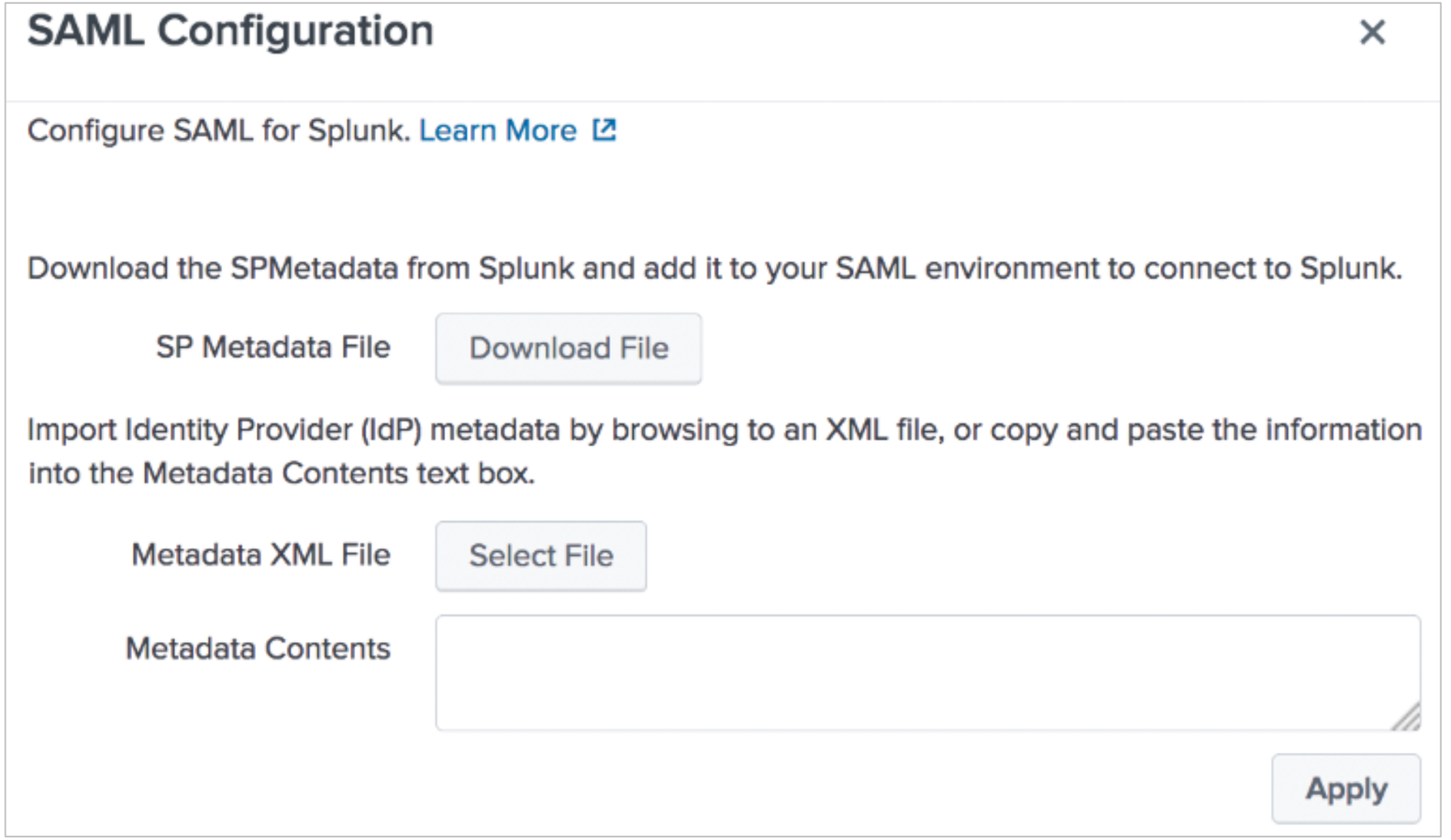


Configuring SAML



Configuring SAML – Splunk Settings

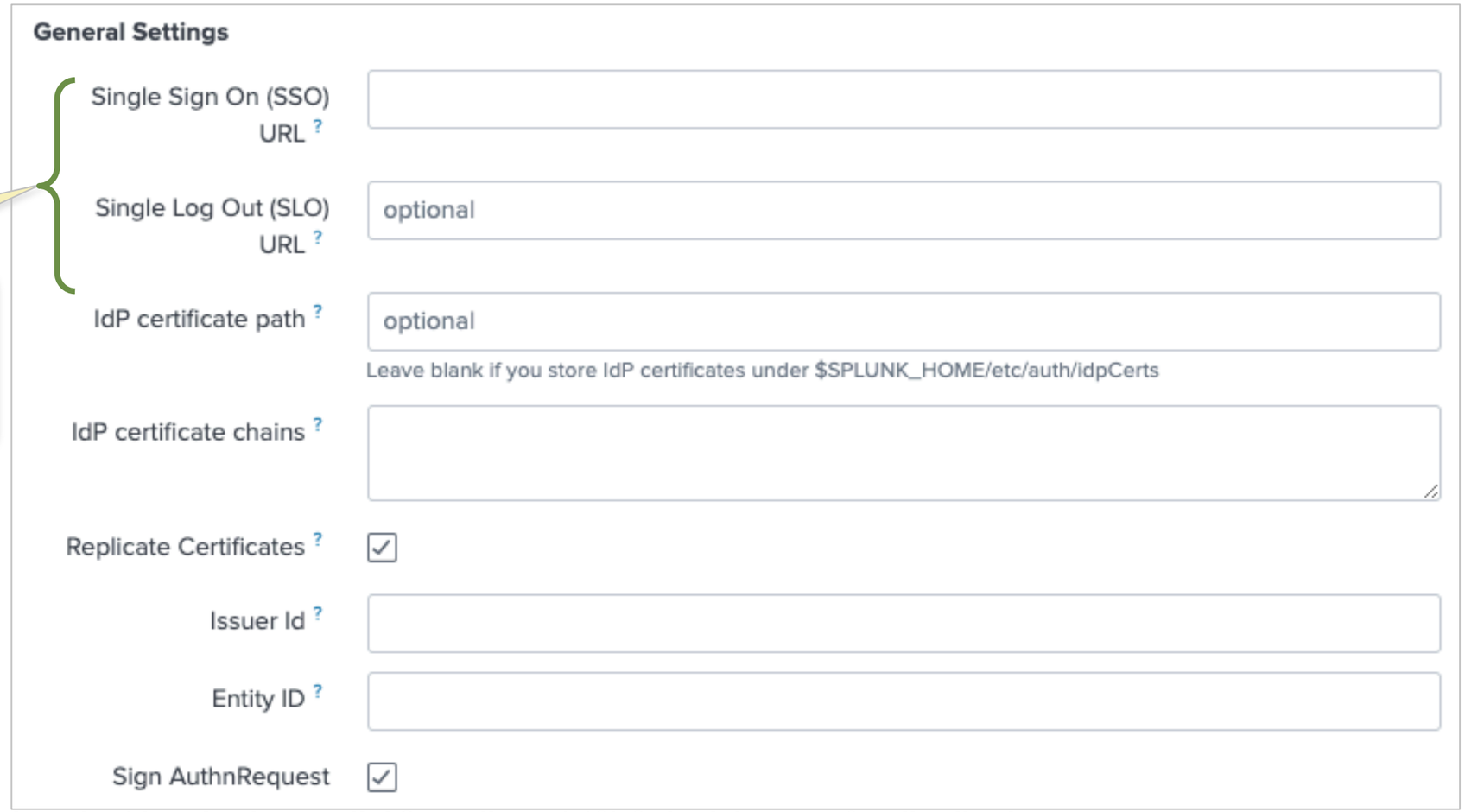
- Download the Splunk Service Provider Metadata file
- Import the IdP metadata into Splunk



Configuring SAML – General Settings

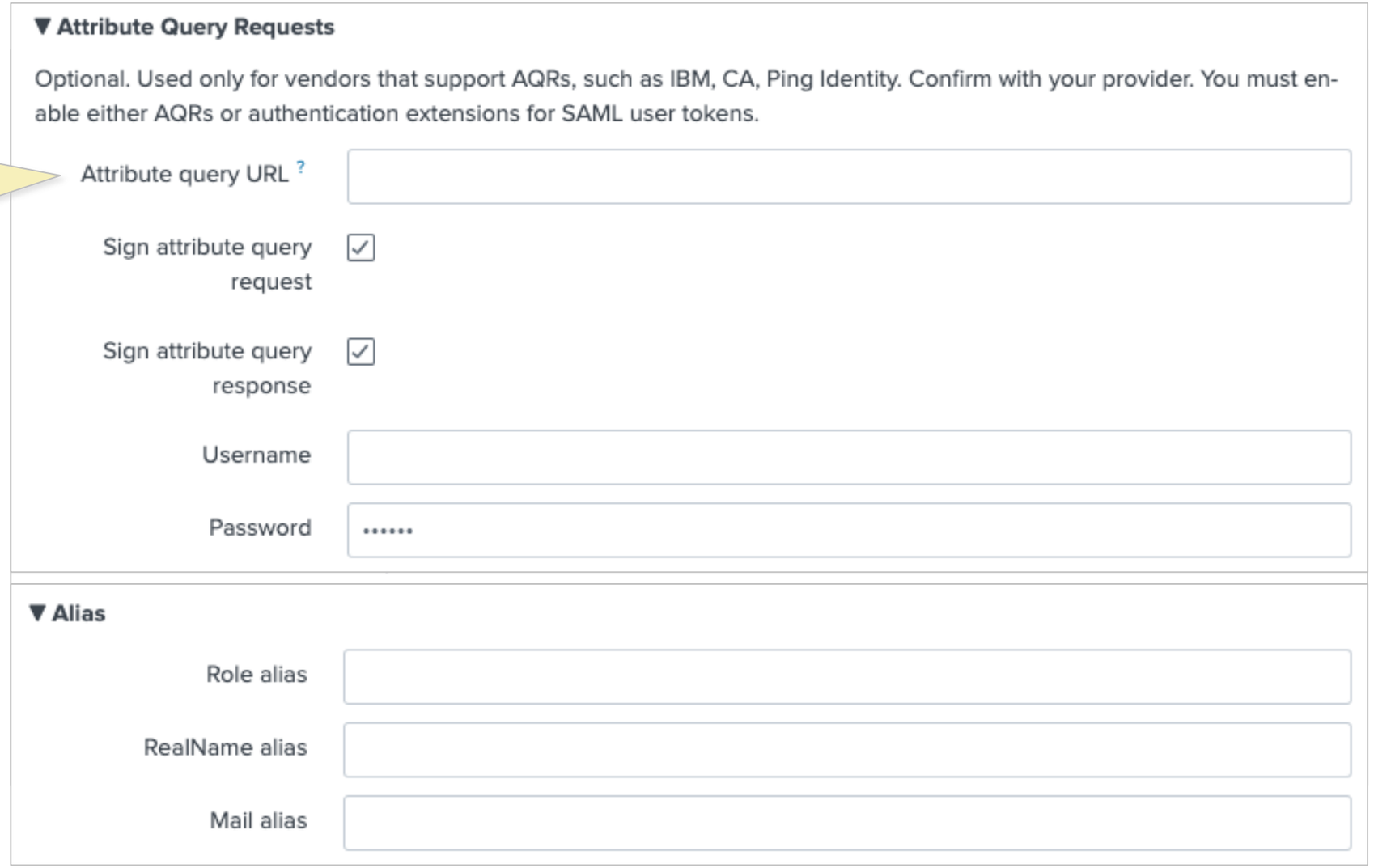
Gather SAML configuration information

Protected endpoints on the IdP which Splunk sends authentication requests to



Configuring SAML – Query and Alias Settings

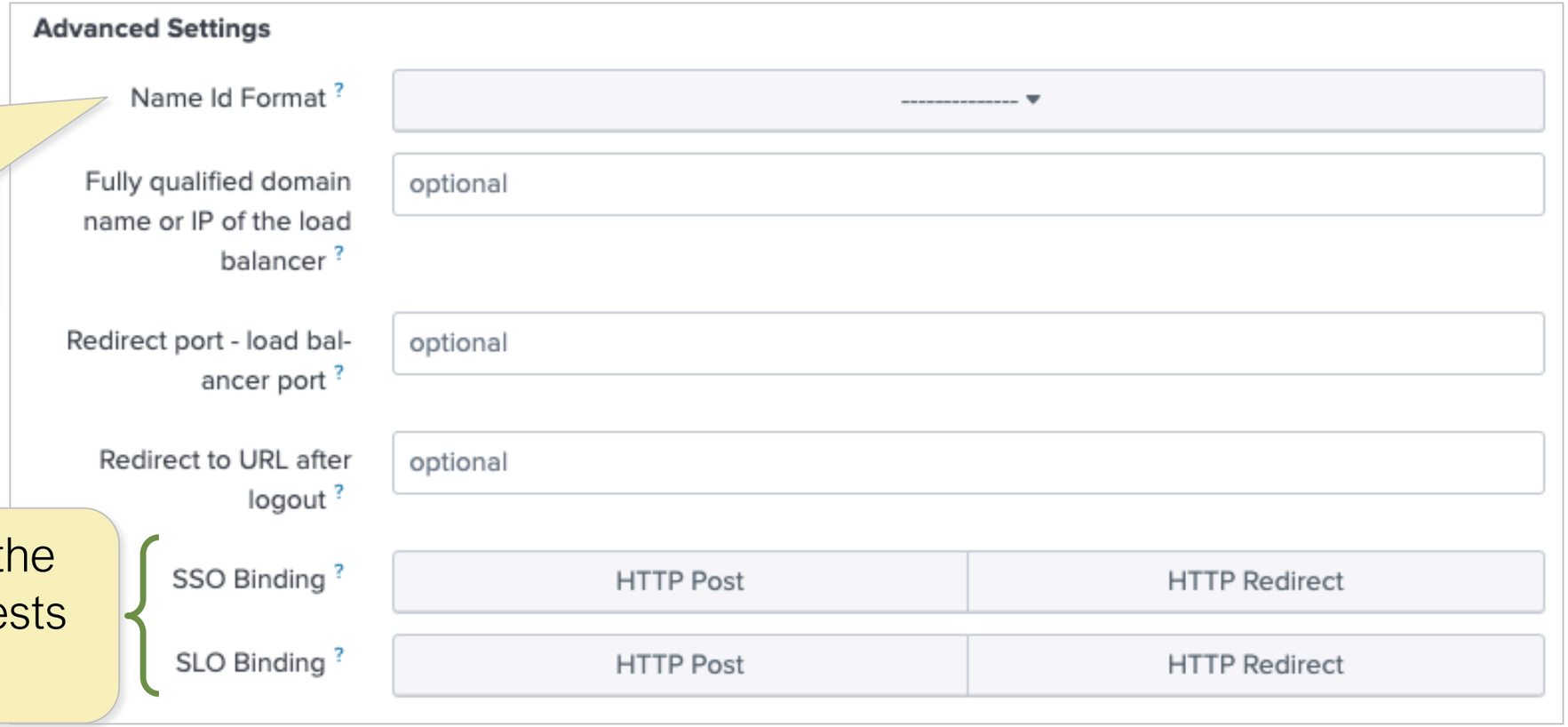
Endpoint on the IdP to which queries over SOAP are sent



Configuring SAML – Advanced Settings

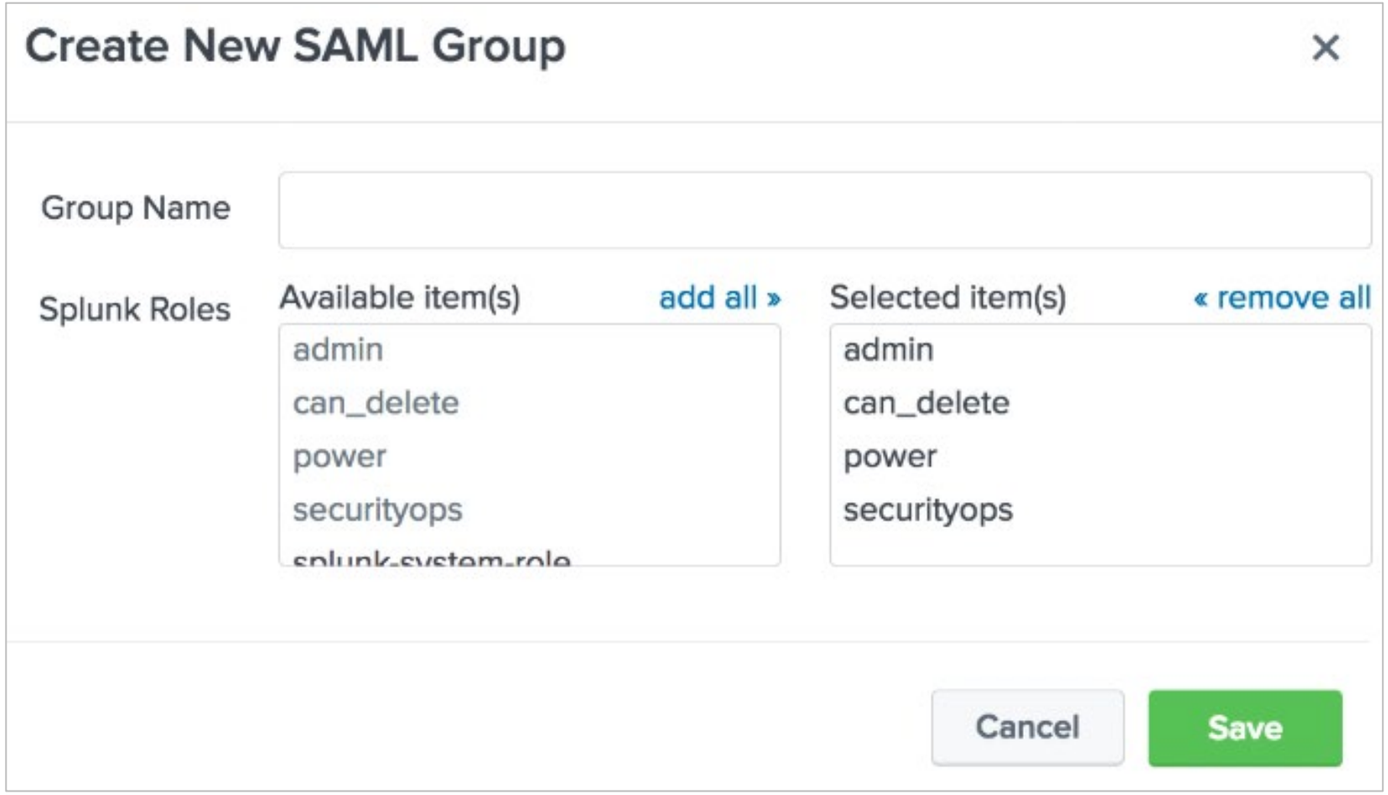
Leave this empty or pick the correct format configured on the IdP from the drop-down list

Protocol binding used for the SAML sign on/log off requests sent to the IdP



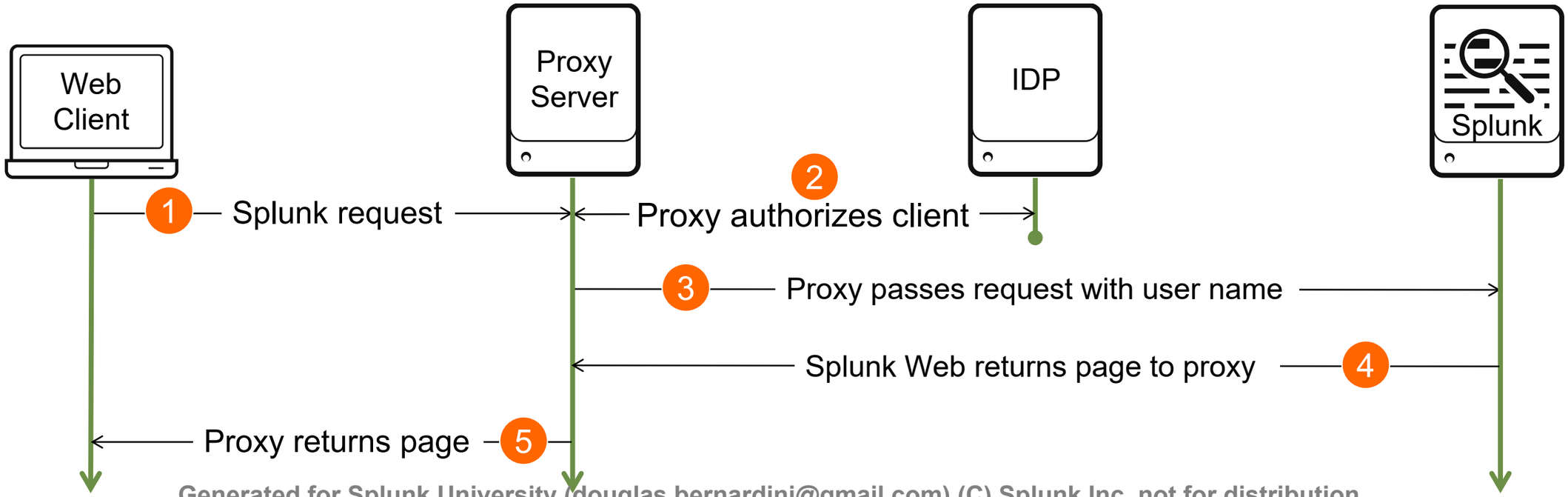
Creating SAML Groups

- Authorize groups on your SAML server to log into Splunk by mapping them to user roles
- Multiple groups can be mapped to a single user role
- A user must have a Splunk role in order to log in



Single Sign On with Reverse Proxy

- Splunk SSO allows you to use a web proxy to handle Splunk authentication
  - Authentication is moved to a web proxy, which passes along authentication to Splunk Web
  - Web proxy can use any method to authenticate (IDP in example)
- docs.splunk.com/Documentation/Splunk/latest/Security/HowSplunkSSOworks

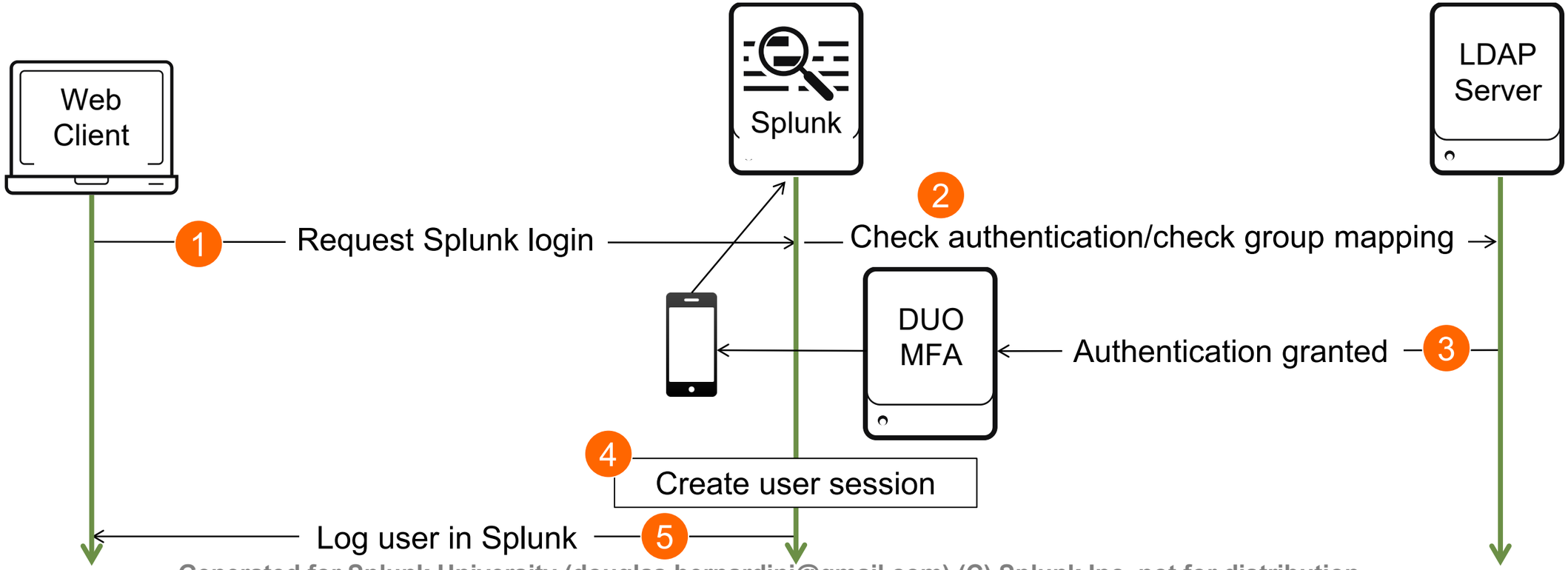


Scripted Authentication

- Splunk supports other authentication systems that can be integrated with scripts
- For up-to-date information on scripted authentication
  1. Navigate to **`SPLUNK_HOME/share/splunk/authScriptSamples/`**
  2. Read the **`README`** file
  3. View included sample authentication scripts

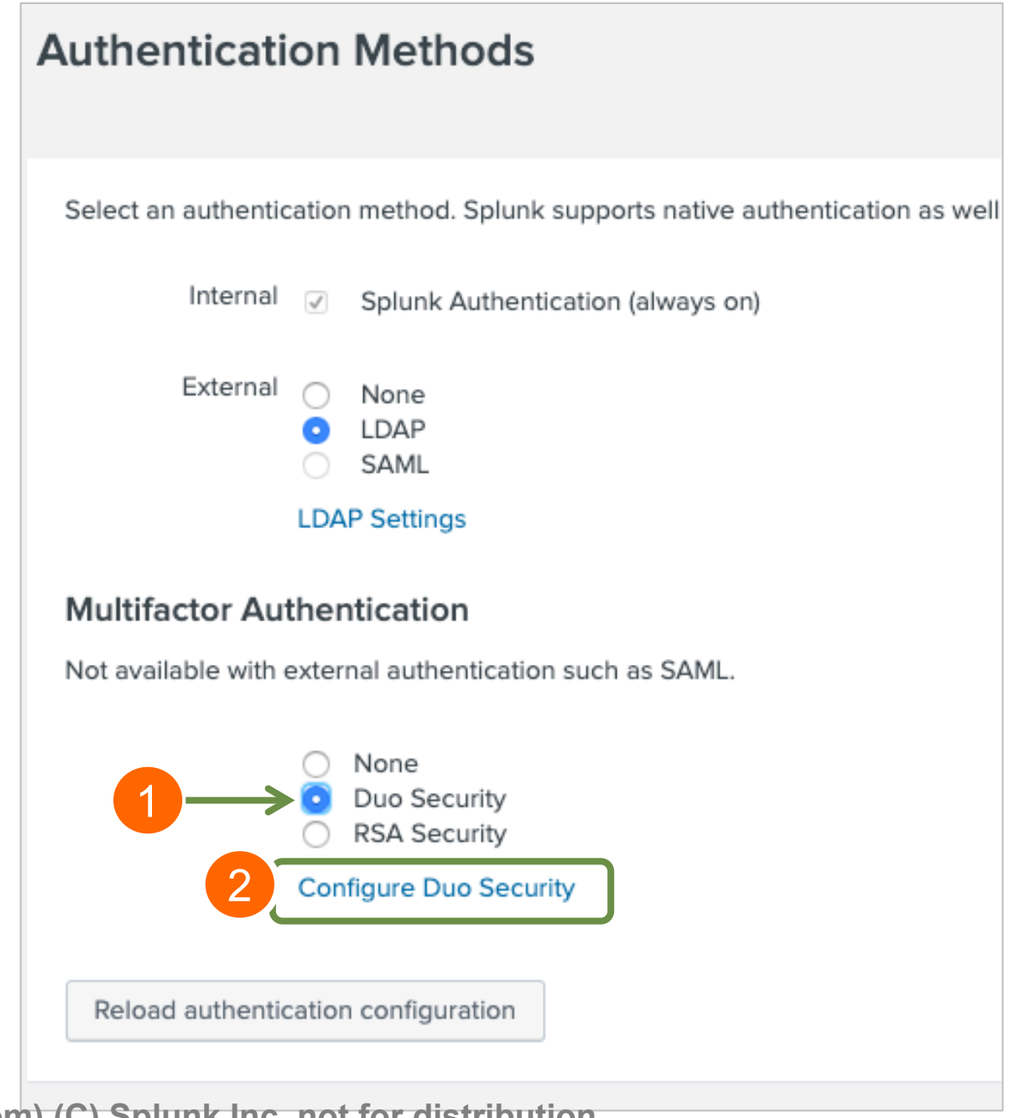
Duo Multi Factor Authentication

- Splunk supports Duo Security two-factor authentication logins
- LDAP maintains the user credentials including user ID and password, plus other information centrally and handles all authentication



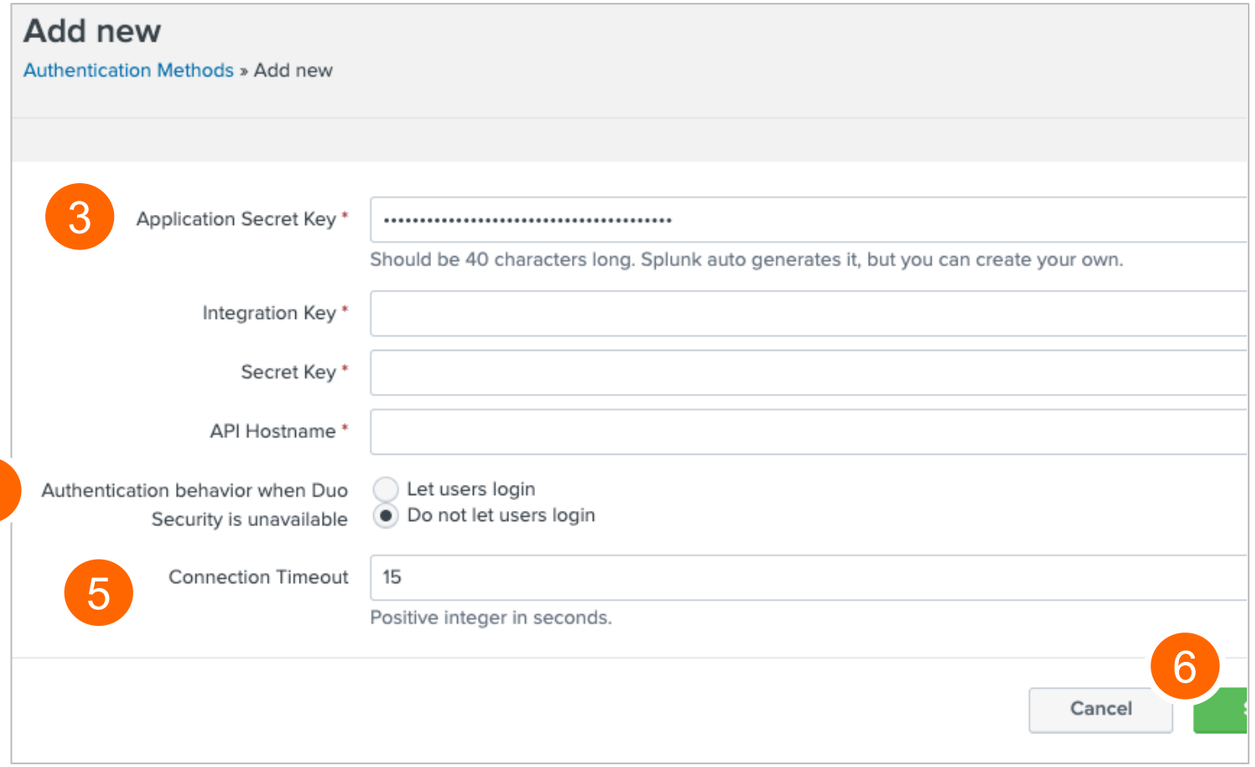
Configuring Duo MFA

- Create an account for your Splunk configuration on the Duo website
  - Refer to https://duo.com
- From your search head:
  1. Select Duo Security
  2. Click Configure Duo Security

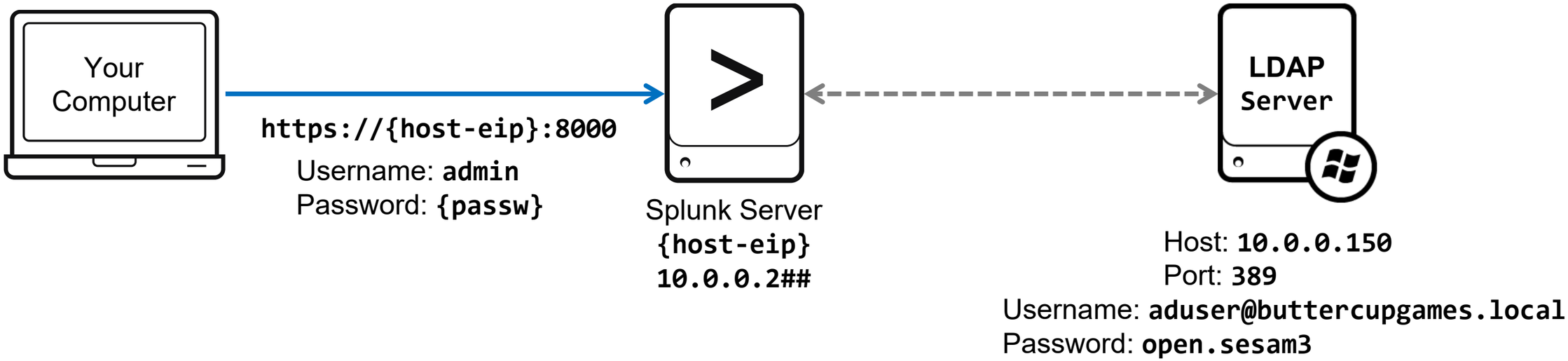


Configuring Duo MFA (cont.)

3. Enter the following info (provided by Duo administrator)
   - Application Secret Key
   - Integration Key
   - Secret Key
   - API Hostname
4. Authentication behavior if Duo is unavailable
5. Connection Timeout (in seconds)
6. Save



Lab Exercise A – Environment Diagram



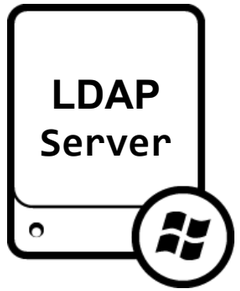
Appendix A Lab Exercise

Time: 10 minutes

Description: Configure Splunk to use LDAP

Tasks:

- Configure Splunk to use LDAP
- Map LDAP groups to Splunk roles
- Verify the LDAP configuration

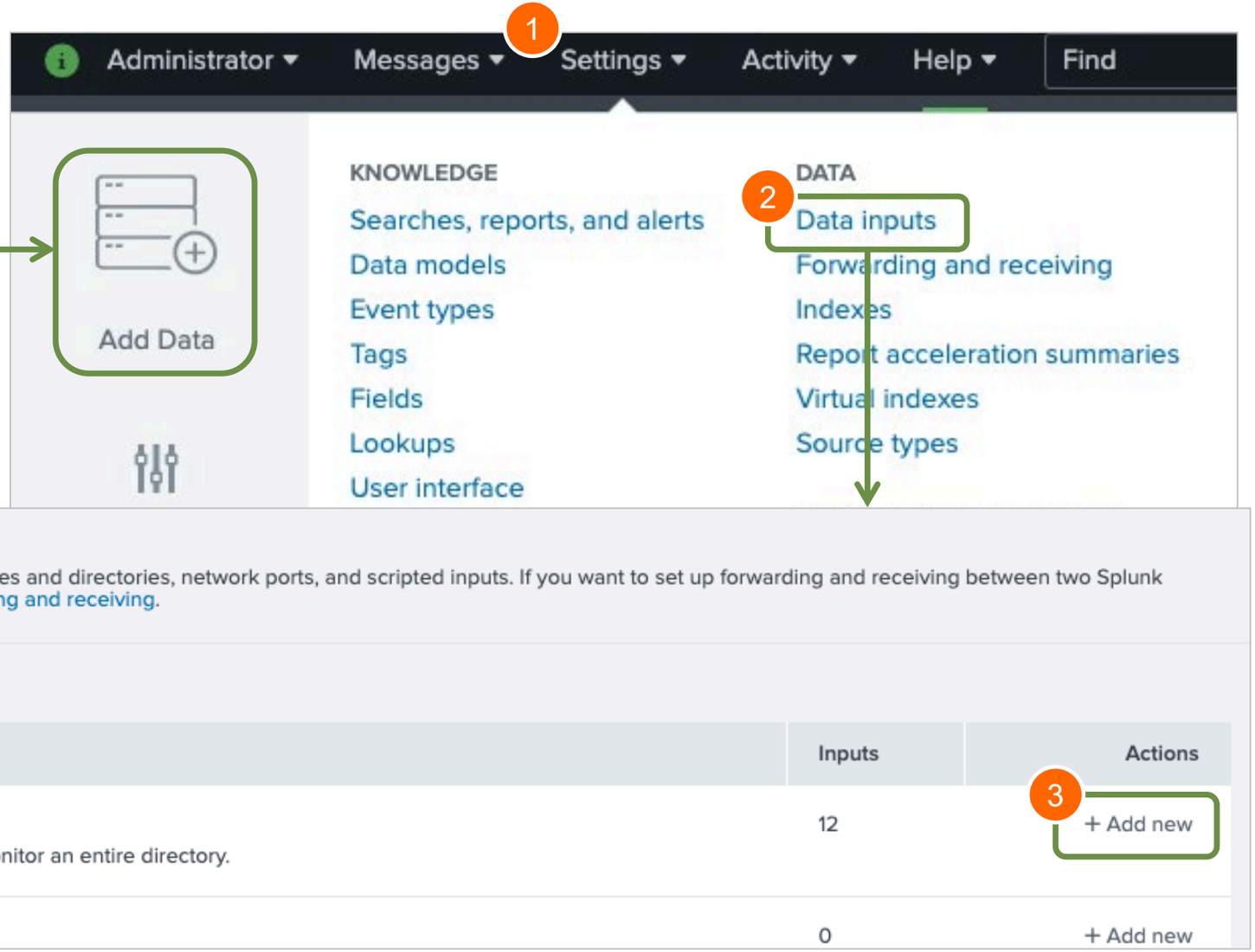


Host: **10.0.0.150**
Port: **389**
Username: **aduser@buttercupgames.local**
Password: **open.sesam3**

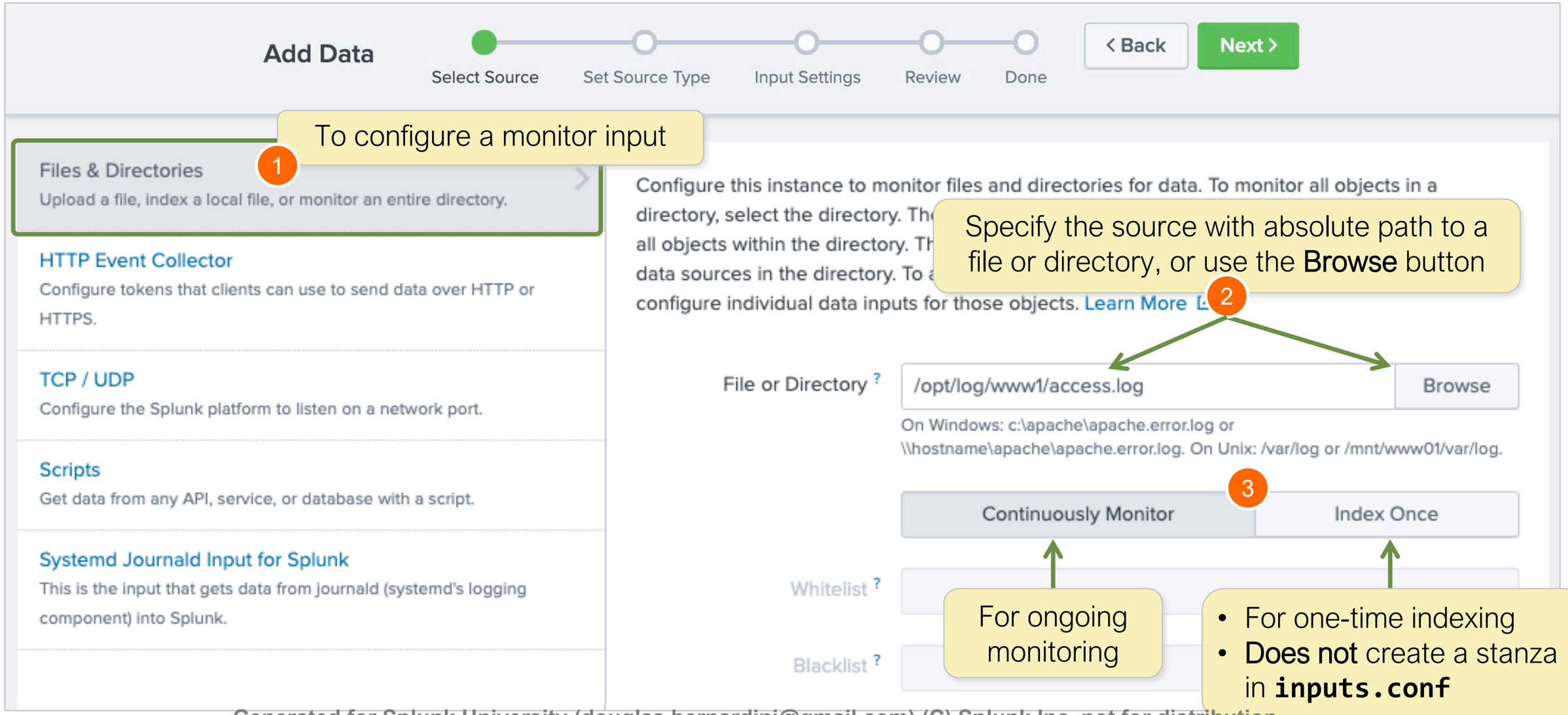
Appendix B: Adding Data

Adding an Input with Splunk Web

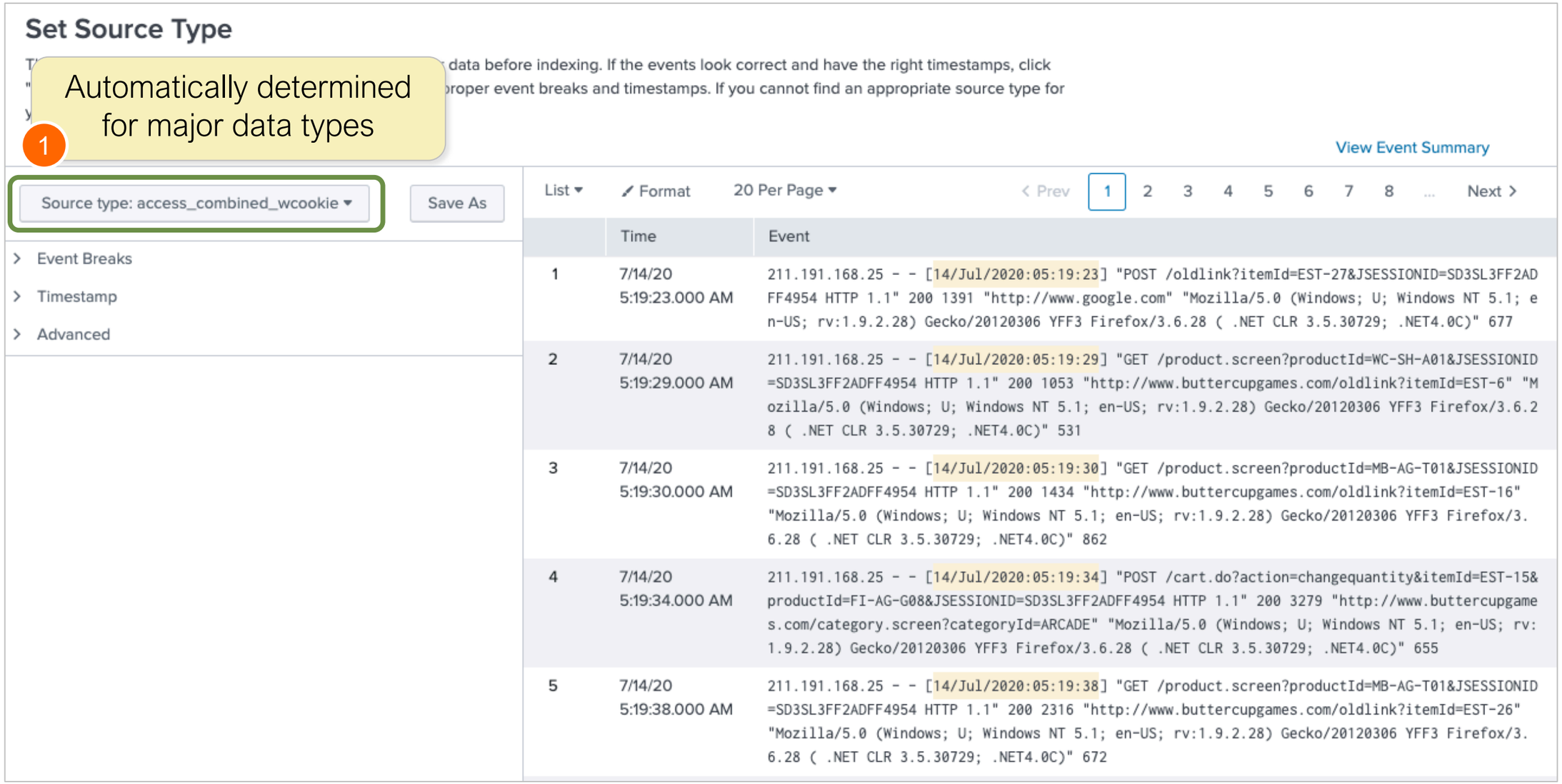
- Click the **Add Data** icon
  - On admin's **Home** page
  - On the **Settings** panel
- Or select:
  1. Settings
  2. Data inputs
  3. Add new



Select Source

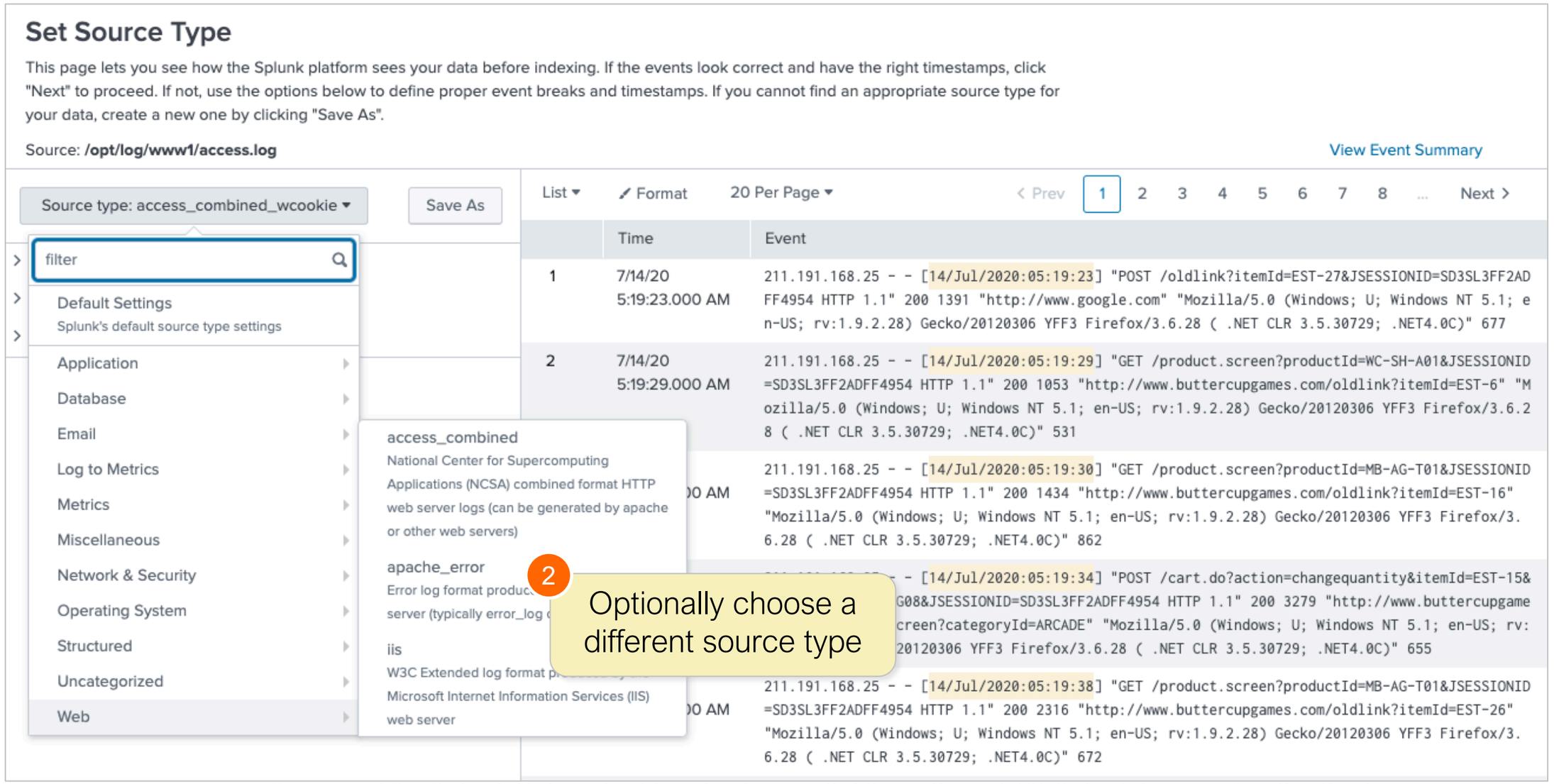


Set Source Type (Data Preview - 1)

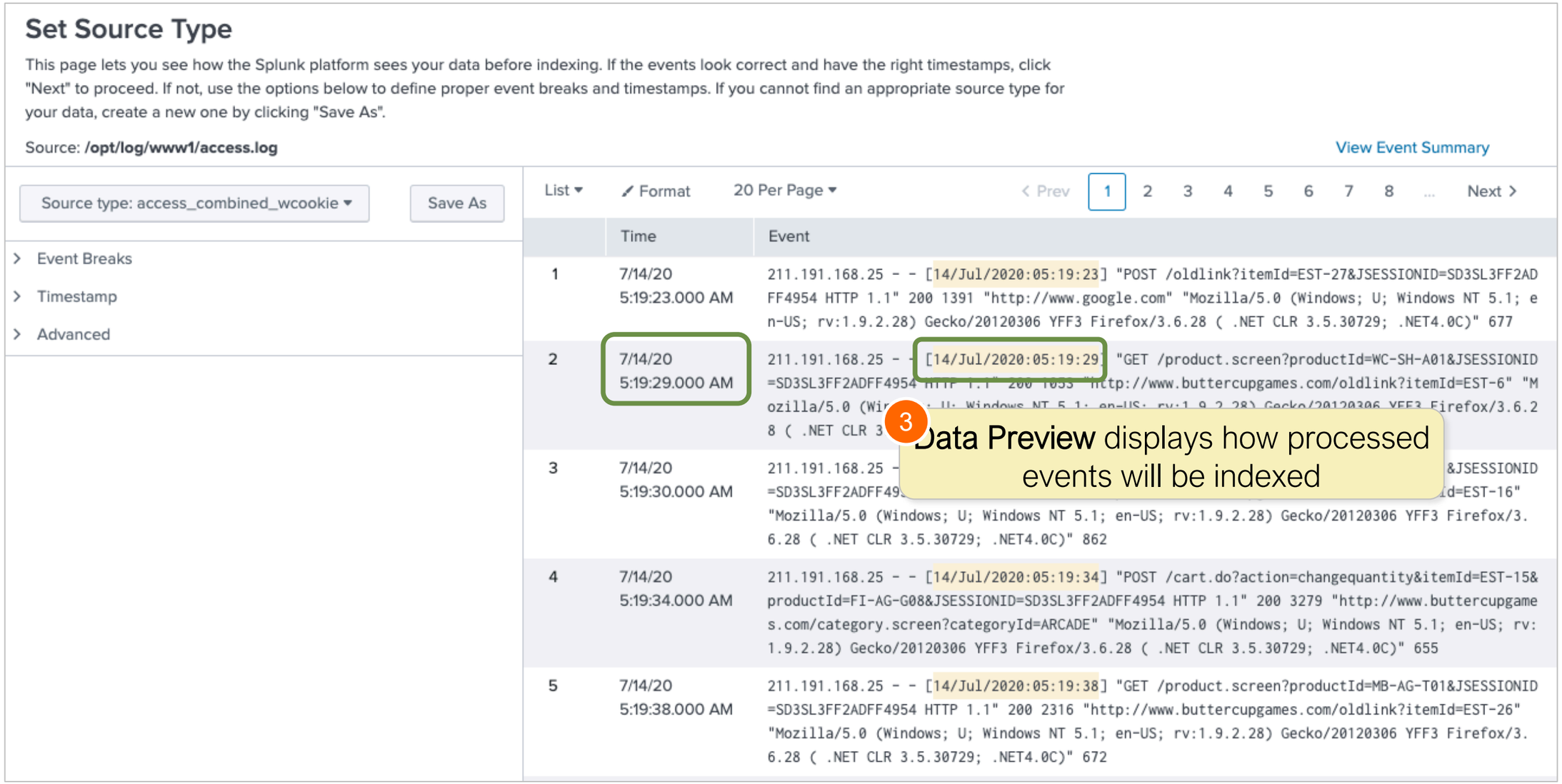


 | 15 September 2021

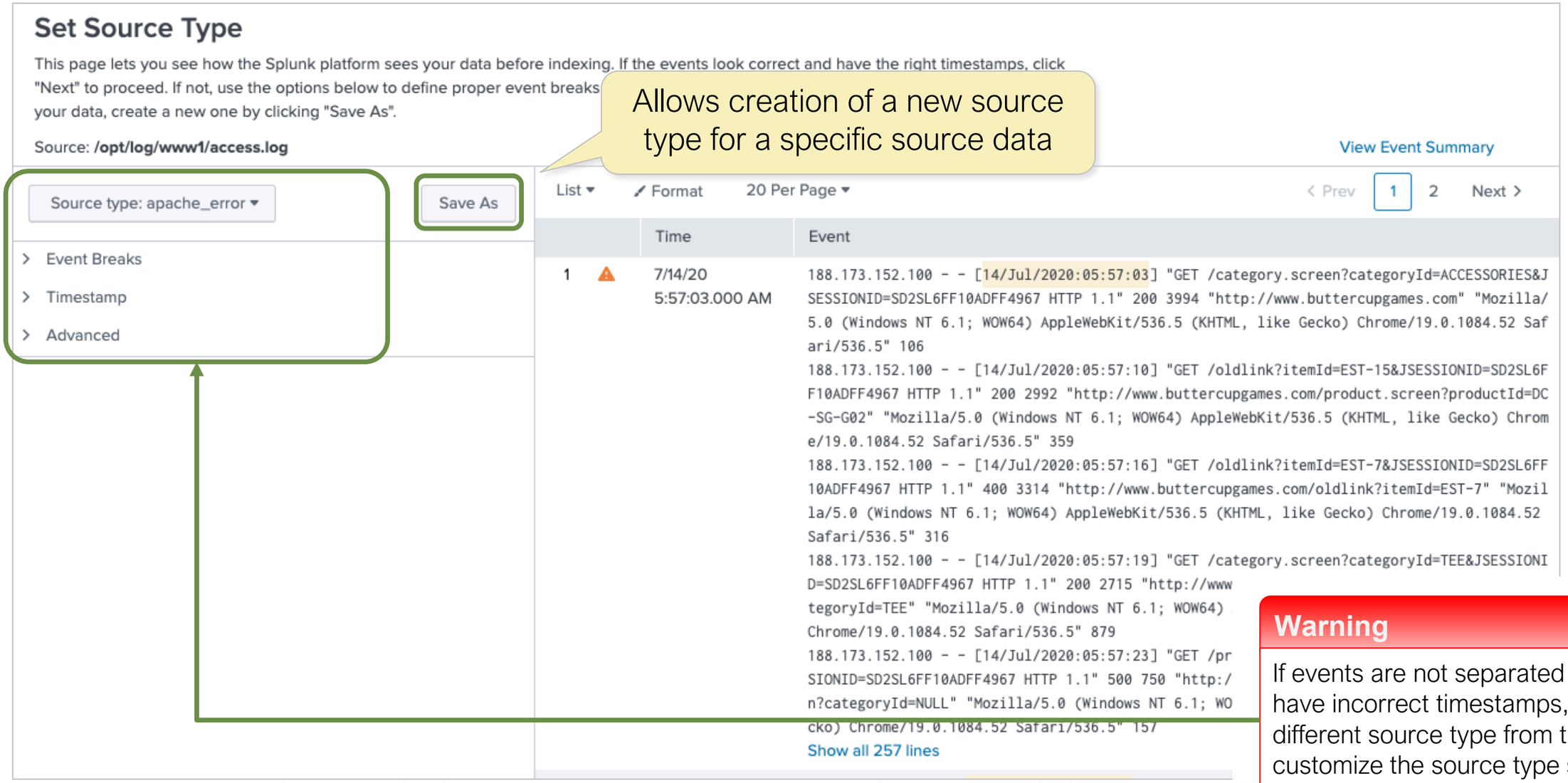
Set Source Type (Data Preview - 2)



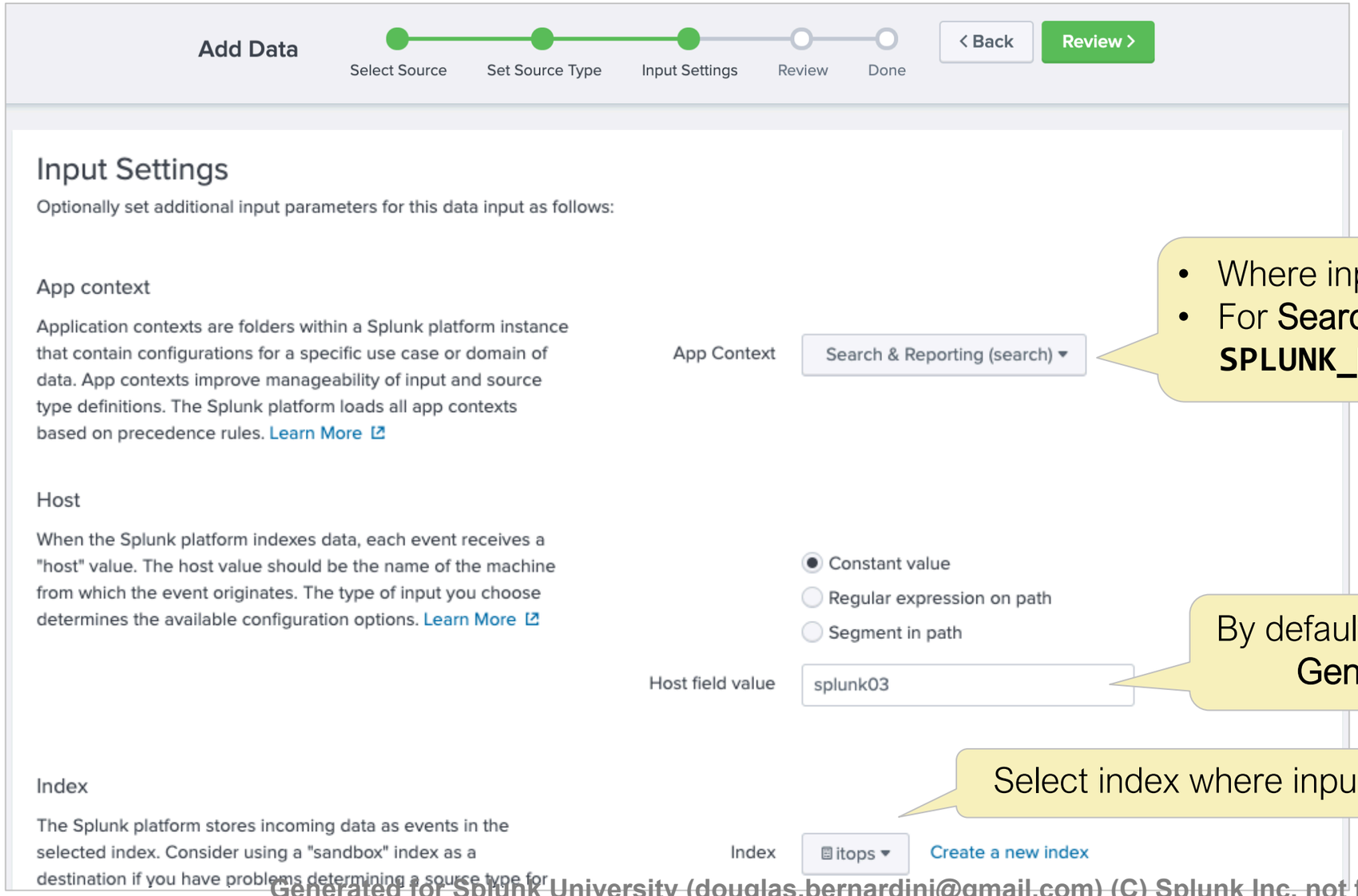
Set Source Type (Data Preview - 3)



Set Source Type (Data Preview - Warning)



Input Settings



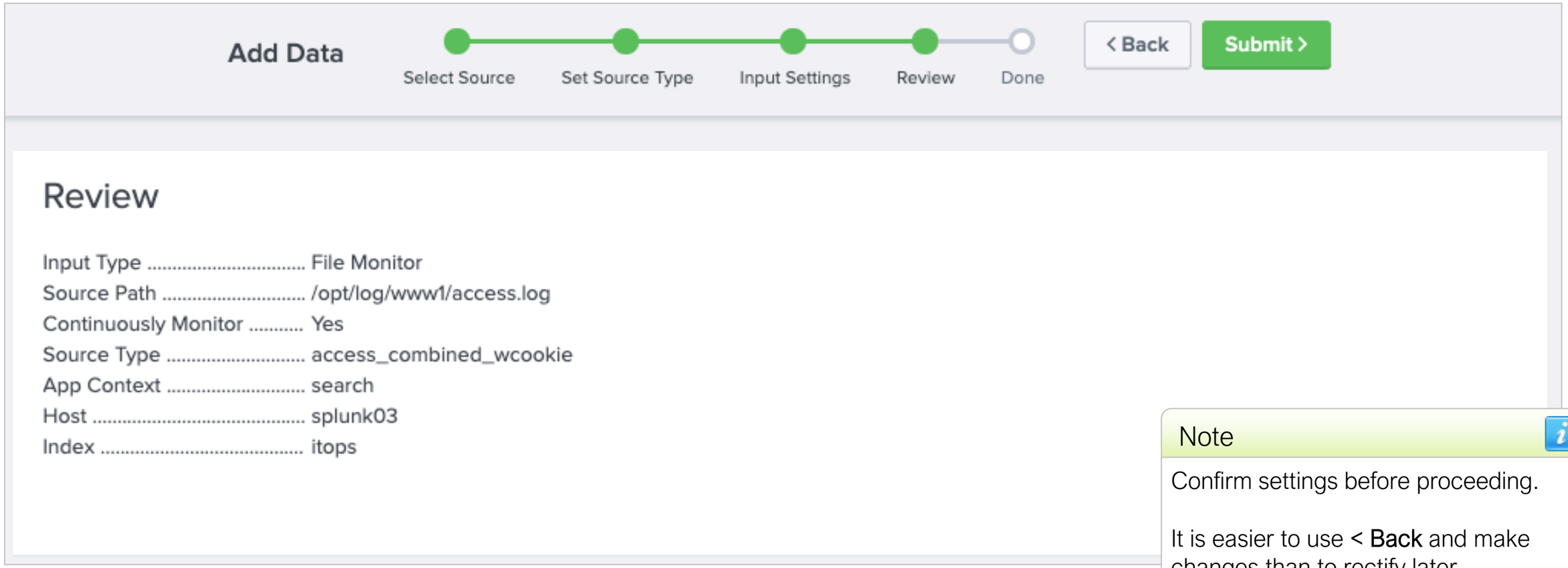
- Where input configuration is saved
- For **Search & Reporting (search)**: **`SPLUNK_HOME/etc/apps/search/local`**

By default the **default host name** in **General settings** is used

Select index where input will be stored

Review

Review the input configuration summary and click **Submit** to finalize



Note

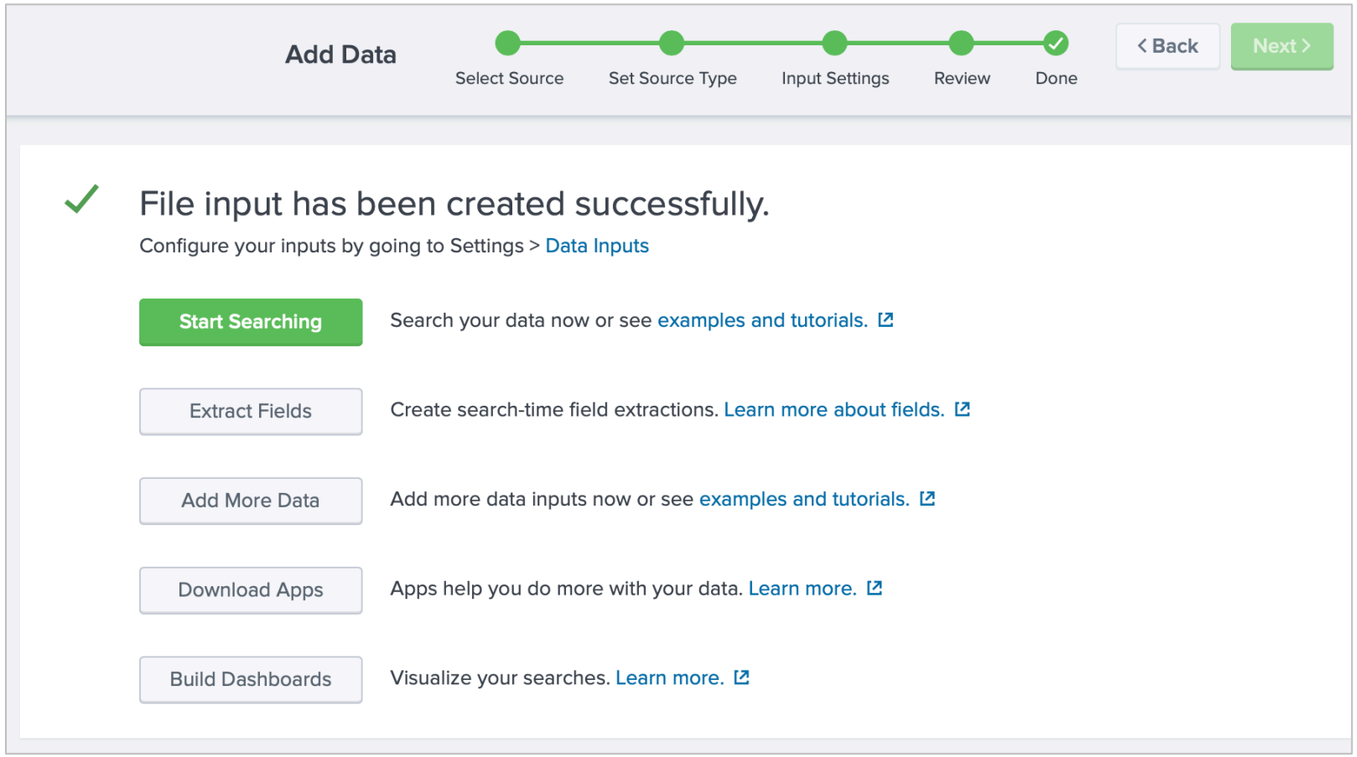
Confirm settings before proceeding.

It is easier to use < **Back** and make changes than to rectify later.

What Happens Next?

- Indexed events are available for immediate search
  - Splunk may take a minute to start indexing the data
- You are given other options to do more with your data
- Input configuration is saved in:

SPLUNK_HOME/etc/apps/<*app*>/local/inputs.conf

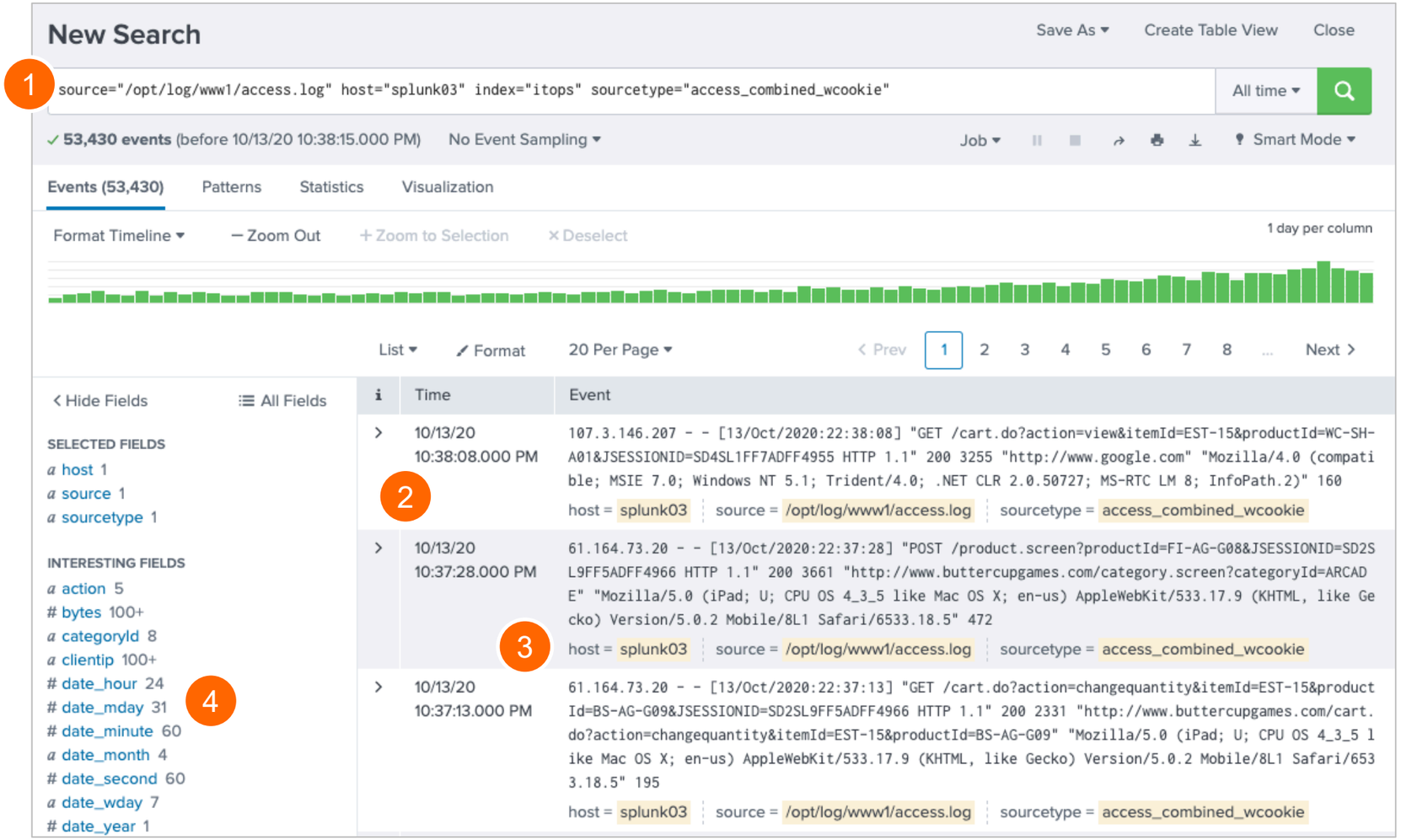


Note

Entries in the **`inputs.conf`** file are not created when **Upload** or **Index Once** is selected.

Verify your Input

1. Click **Start Searching** or search for **index=<*test_idx*>**
2. Verify events and timestamps
3. Confirm the **host**, **source**, and **sourcetype** field values
4. Check the auto-extracted field names



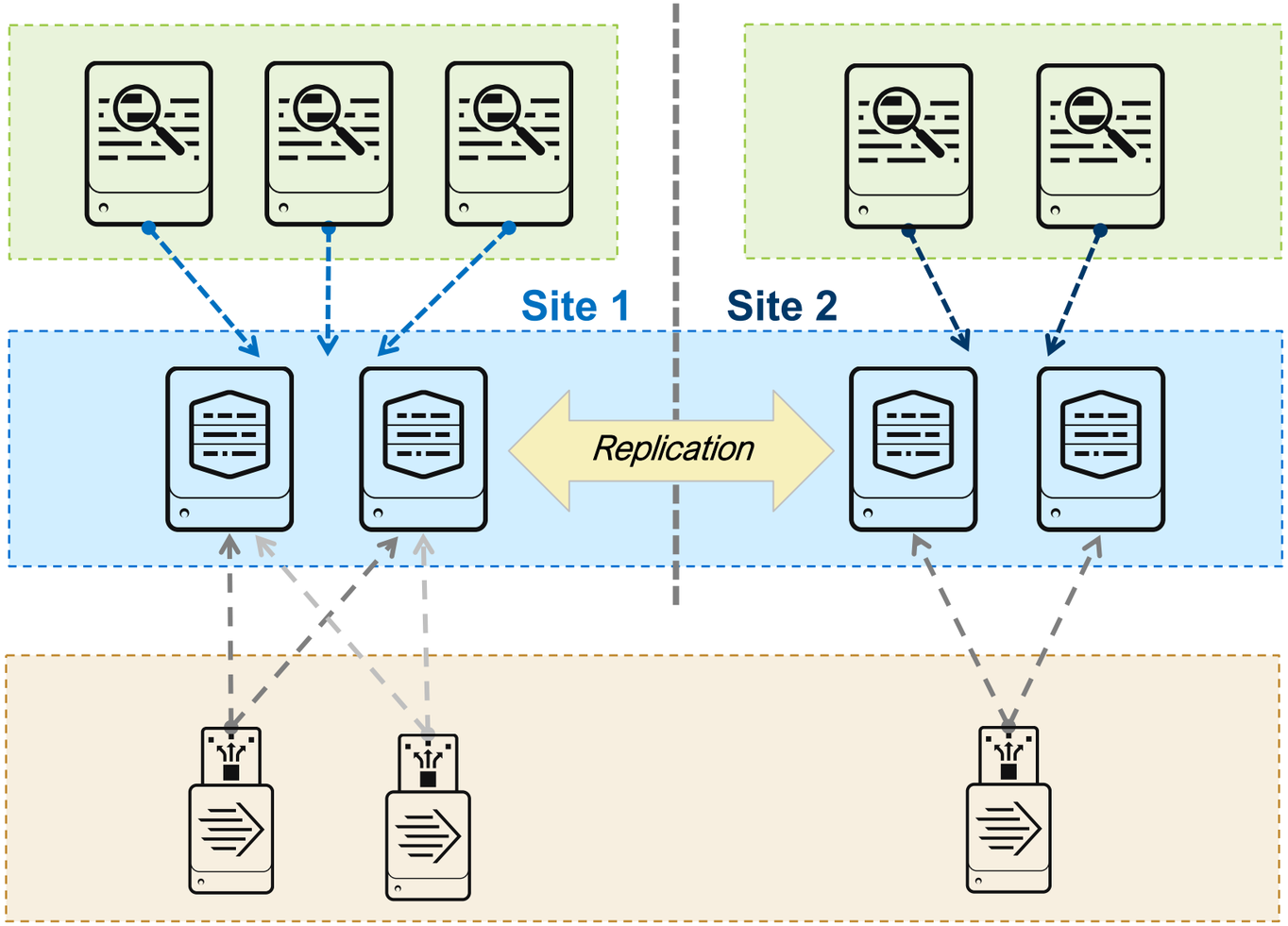
Appendix C:
Introduction to Splunk Clustering

Splunk Clustering

- Requires only Splunk enterprise license
- Discussed in detail in *Splunk Cluster Administration* class
- Supports two types of clusters:

Search head clustering	• Replicates knowledge objects across search heads
Indexer clustering	• Replicates buckets (data) across indexers • Can be configured as single-site or multi-site • Allows balance of growth, speed of recovery, and overall disk usage

Splunk Cluster Overview



Search heads clustered

Indexers clustered

Load-balanced forwarders

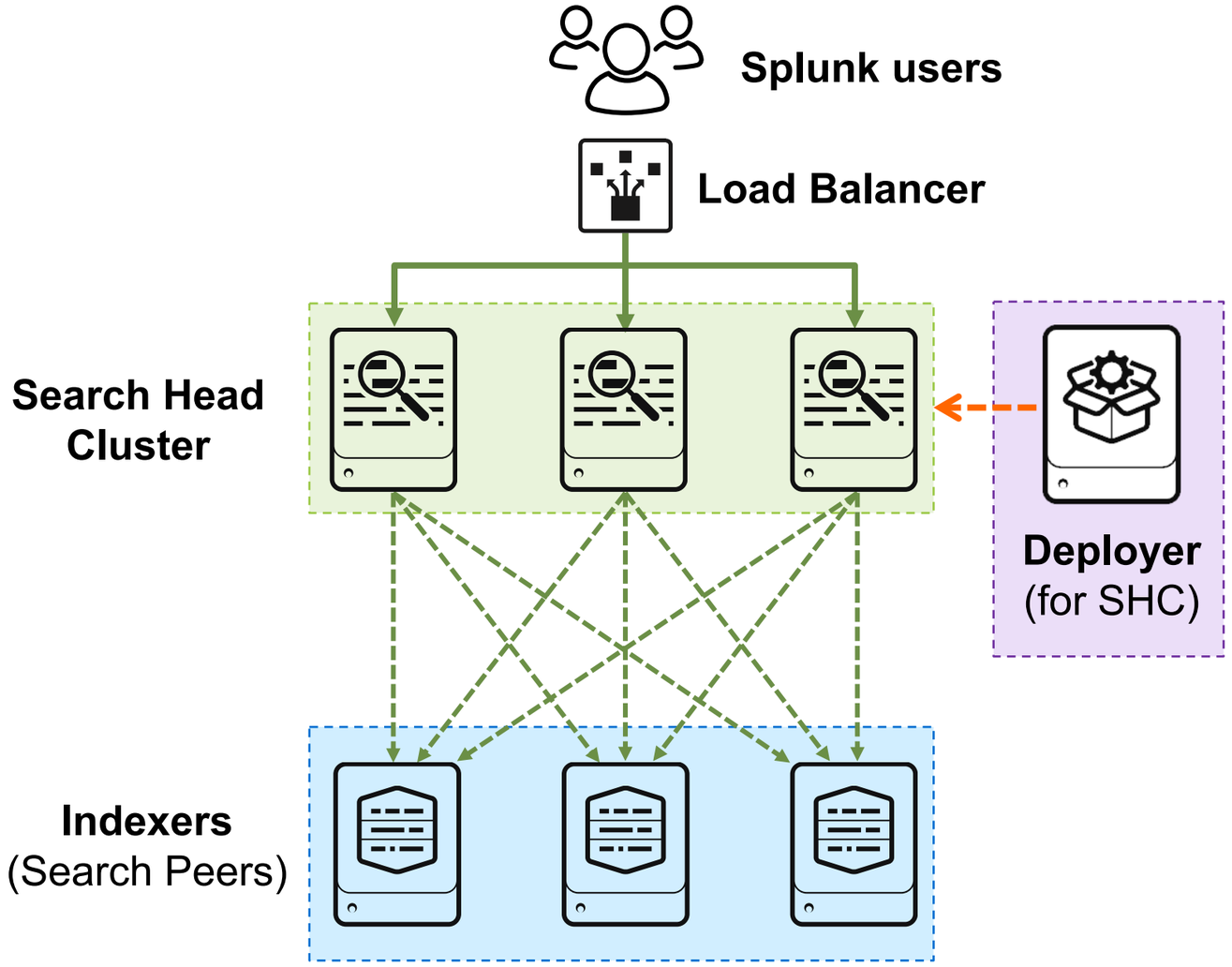
Additional Components:

- Cluster Manager
- Monitoring Console
- Deployment Server
- Deployer
- License Manager

 | 15 September 2021

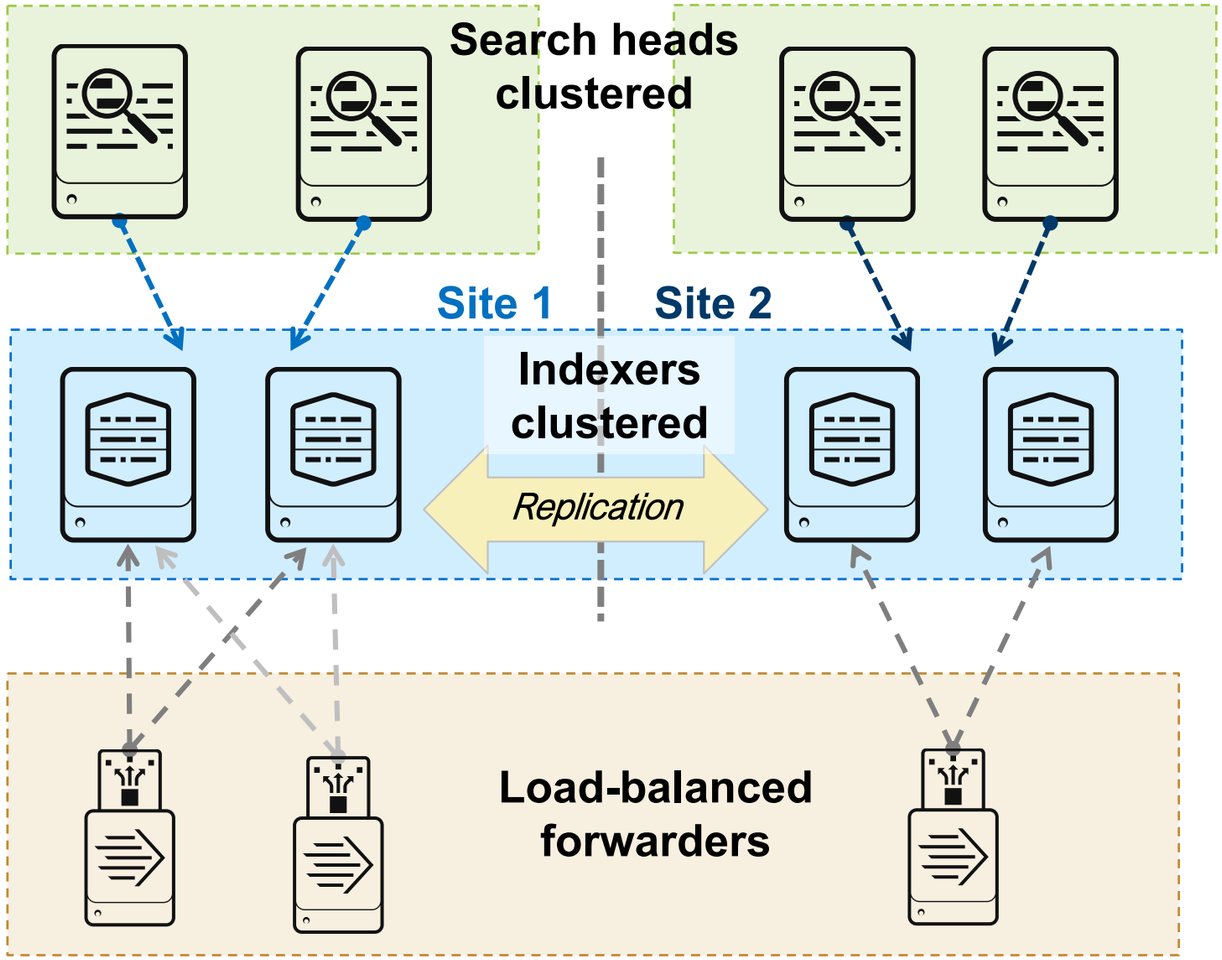
Search Head Cluster

- Accommodates large enterprise use cases
  - Search head high-availability
  - Unified user experience across SHs
  - Search scaling foundation
    - Configuration sharing
    - Artifact replication
    - Job distribution
    - Alert management
    - Load balancing
- Supports external (non-Splunk) load balancers to provide transparent access to the cluster



Indexer Clustering and Replication

- Allows for rapid failure recovery
- Replicates buckets amongst the indexers
- Fully configurable, allowing a balance between speed of recovery and overall disk usage
- Requires additional disk space
- Does not require additional license quota
- Allows for Auto Indexer Discovery
  - Forwarders "discover" the available indexers instead of hard-coding **`outputs.conf`**



Further Reading: Clustering

- Basic clustering concepts for advanced users

  docs.splunk.com/Documentation/Splunk/latest/Indexer/Basicconcepts

- Configure the search head

  docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCconfigurationoverview

- Indexer discovery

  docs.splunk.com/Documentation/Splunk/latest/Indexer/indexerdiscovery

