



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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

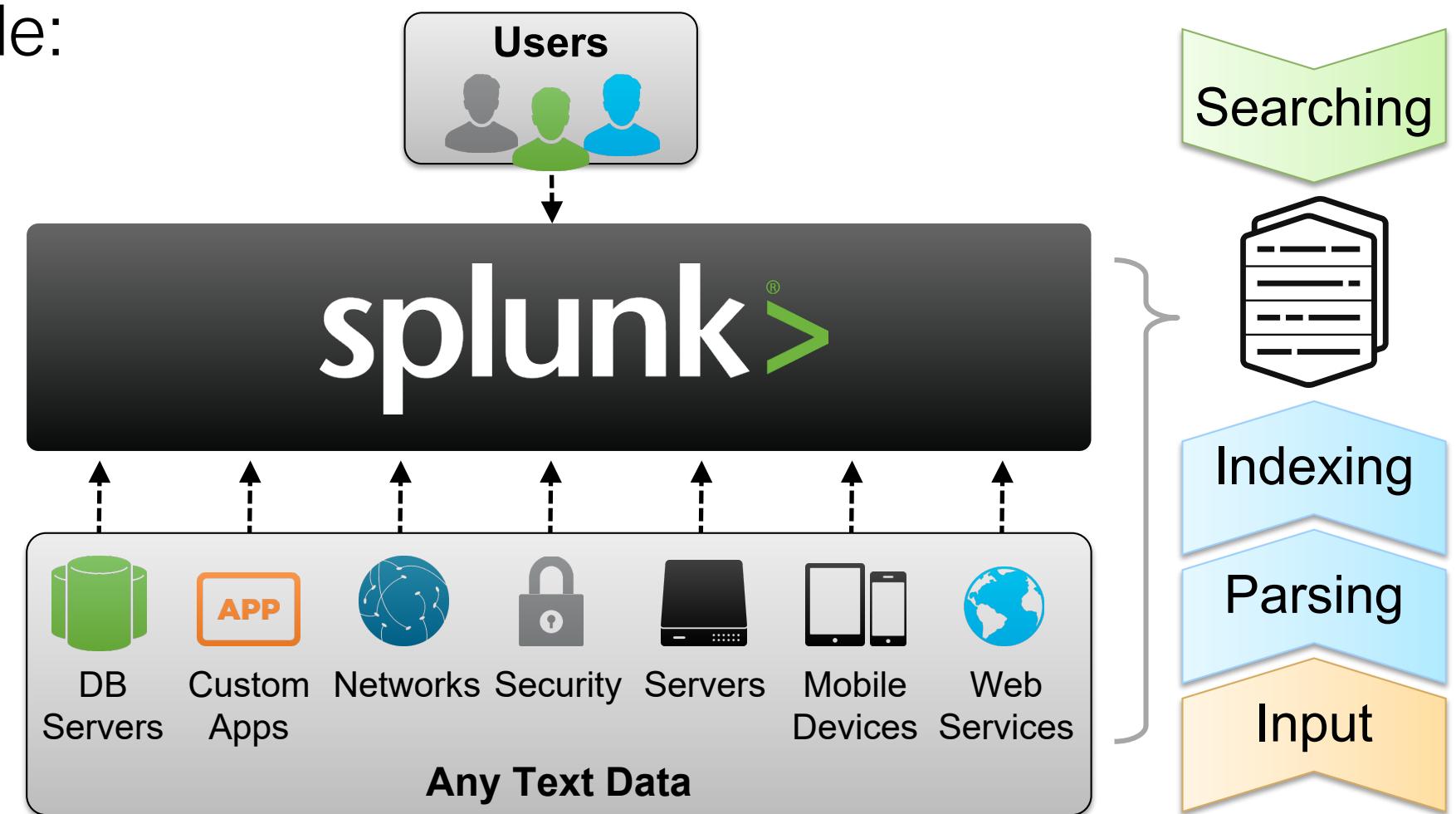
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

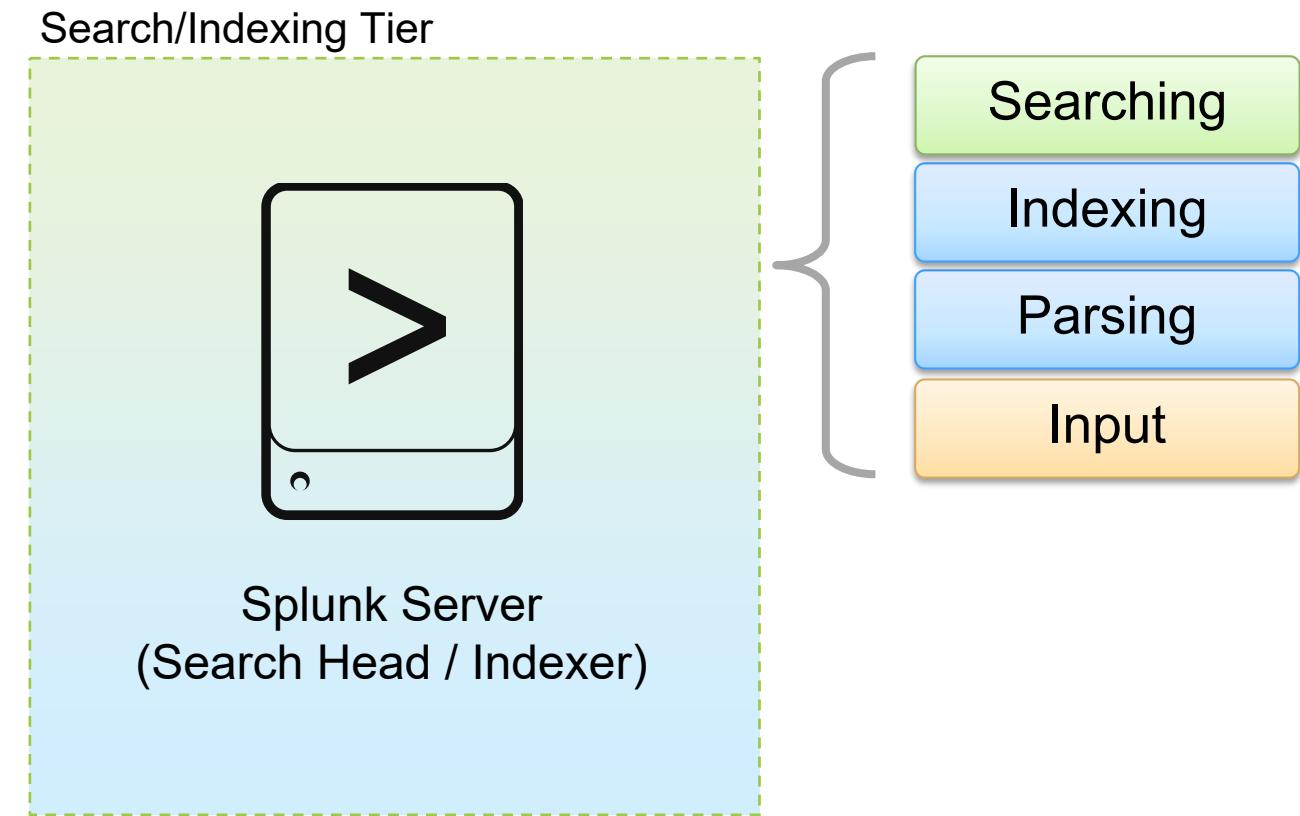
- Splunk can be deployed in a variety of configurations
- Scales from a single server to a distributed infrastructure
- Four stages of Splunk include:
 - Input any text data
 - Parse the data into events
 - Index and store events
 - Search and report



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

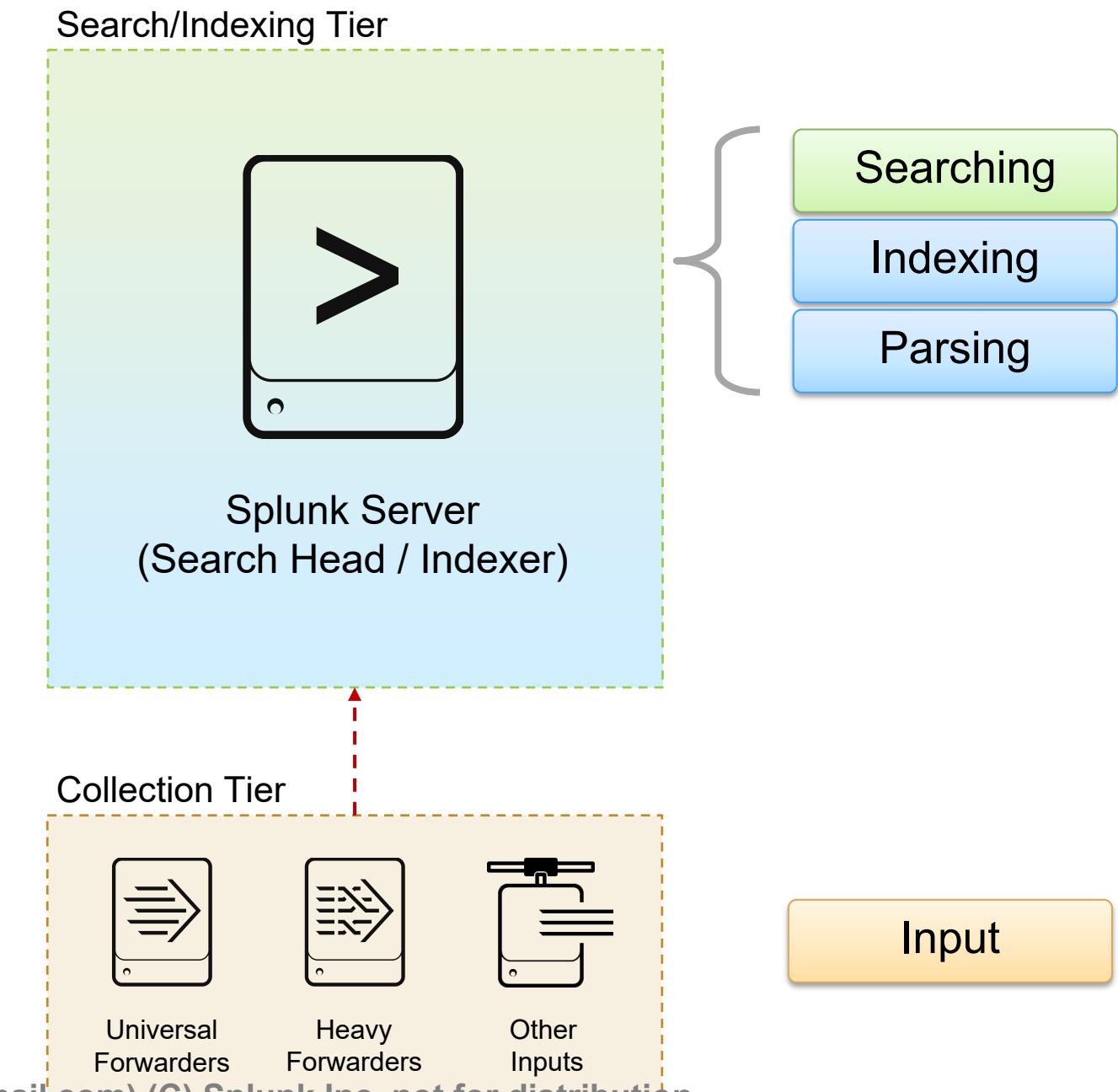
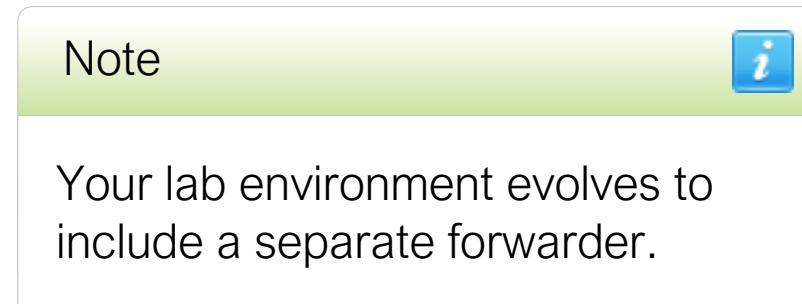


This is the initial configuration in class.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Single Server With Inputs

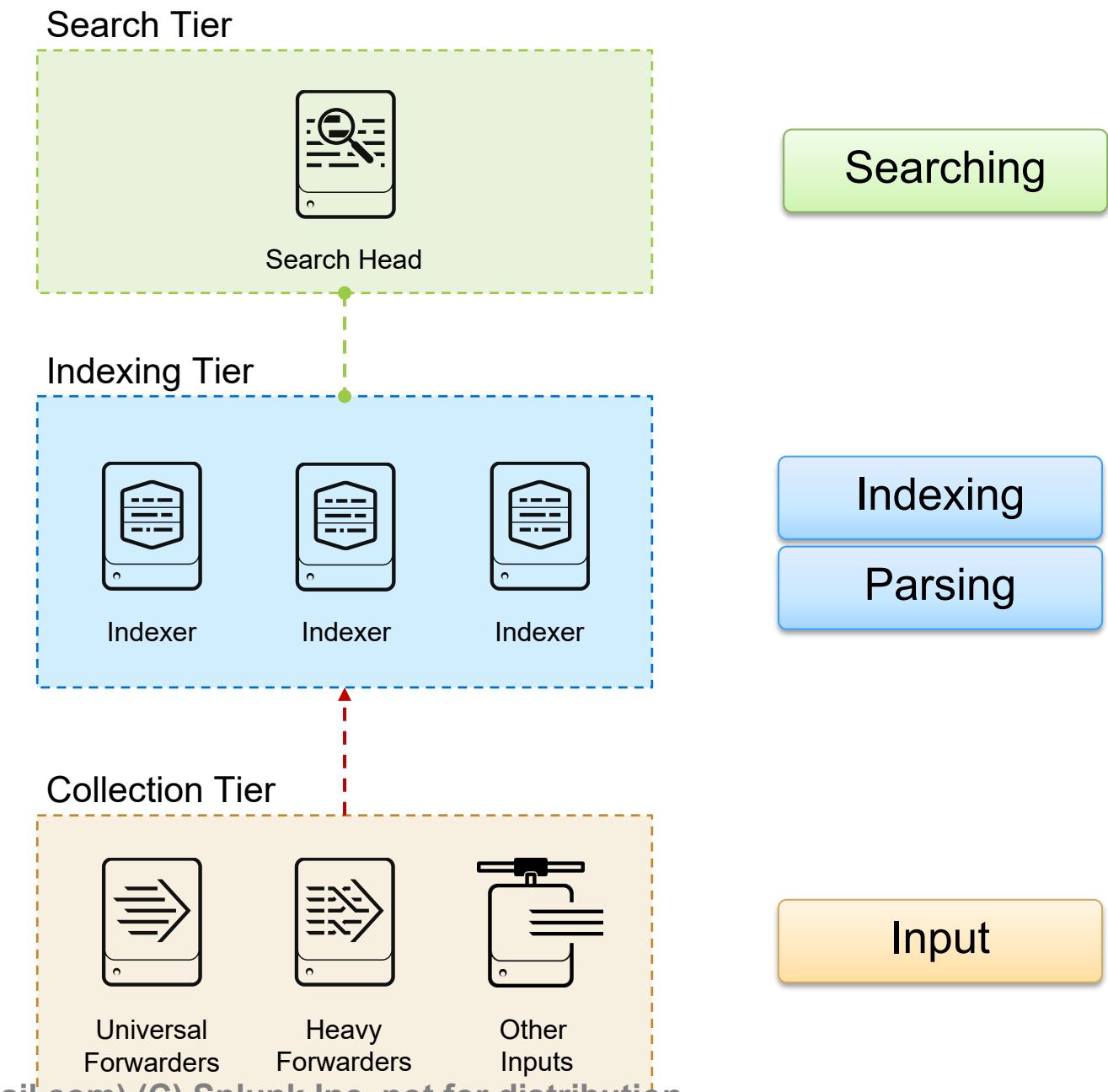
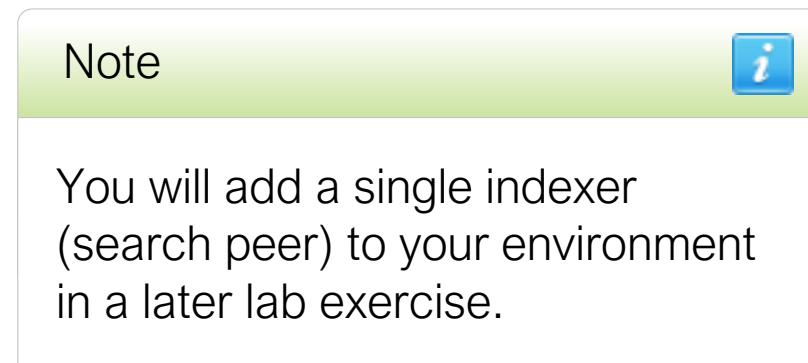
- Deploying a basic Splunk server
 - Similar to standalone configuration
 - Manage deployment of forwarder configurations
- Deploying Forwarders
 - Install Splunk forwarder at data source (usually production servers)
 - Collect data and send it to Splunk servers



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Distributed Non-Cluster Environment

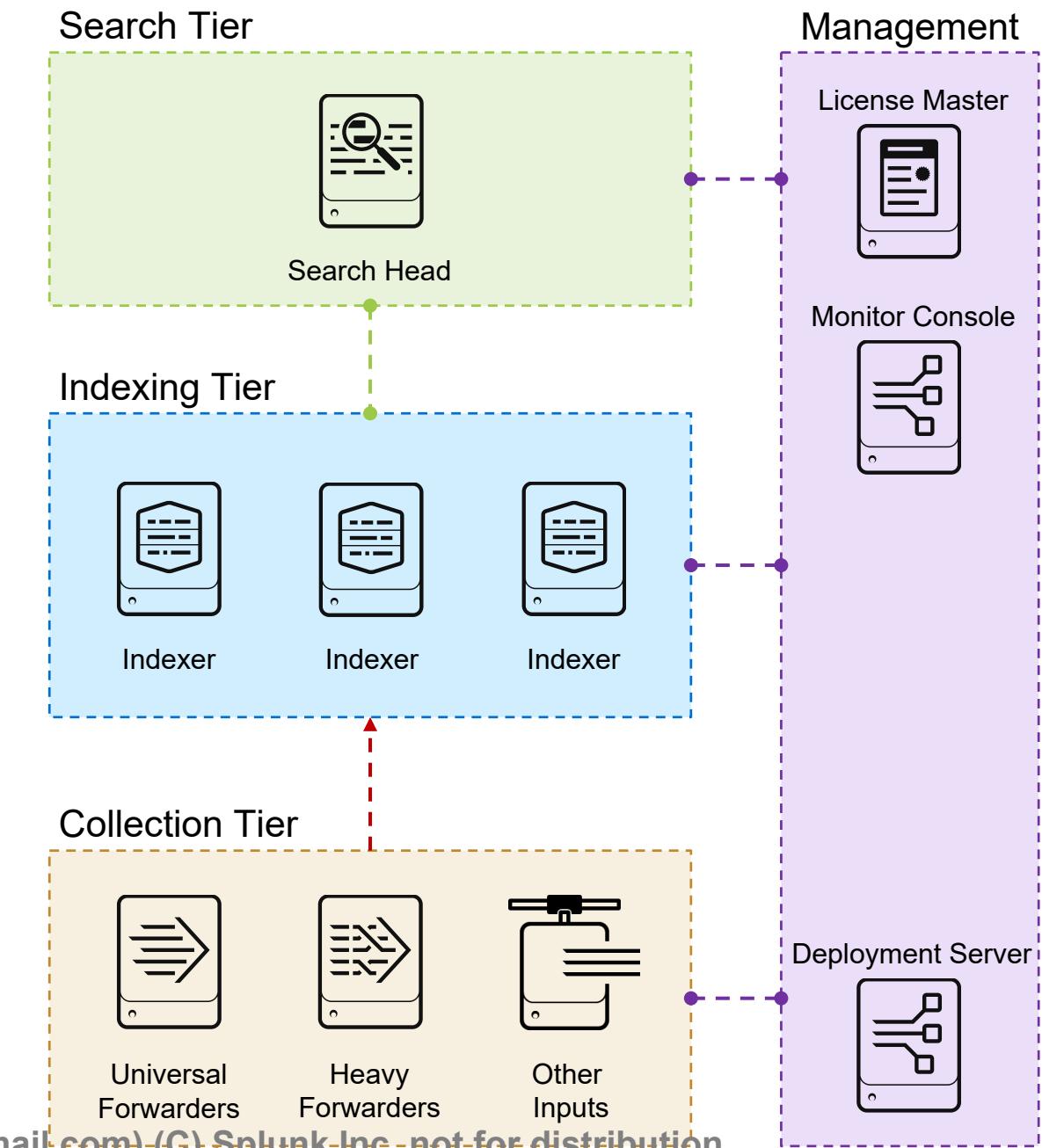
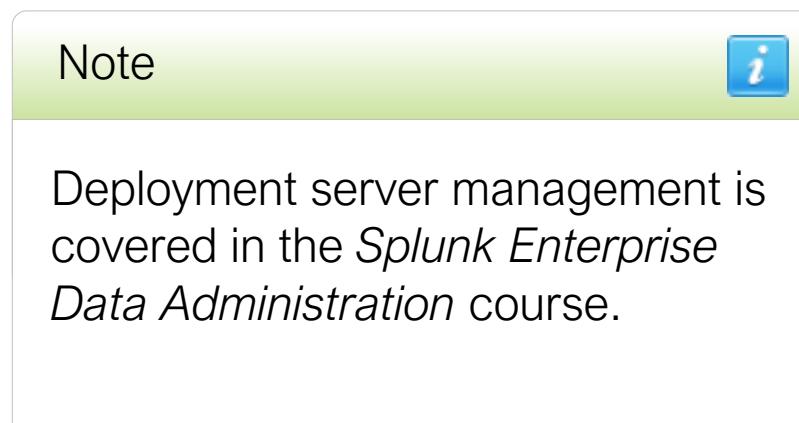
- Scale Splunk in various ways
 - Add indexers to handle more inputs
 - Add indexers and search heads to handle more searching



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Distributed Non-Cluster Environment (2)

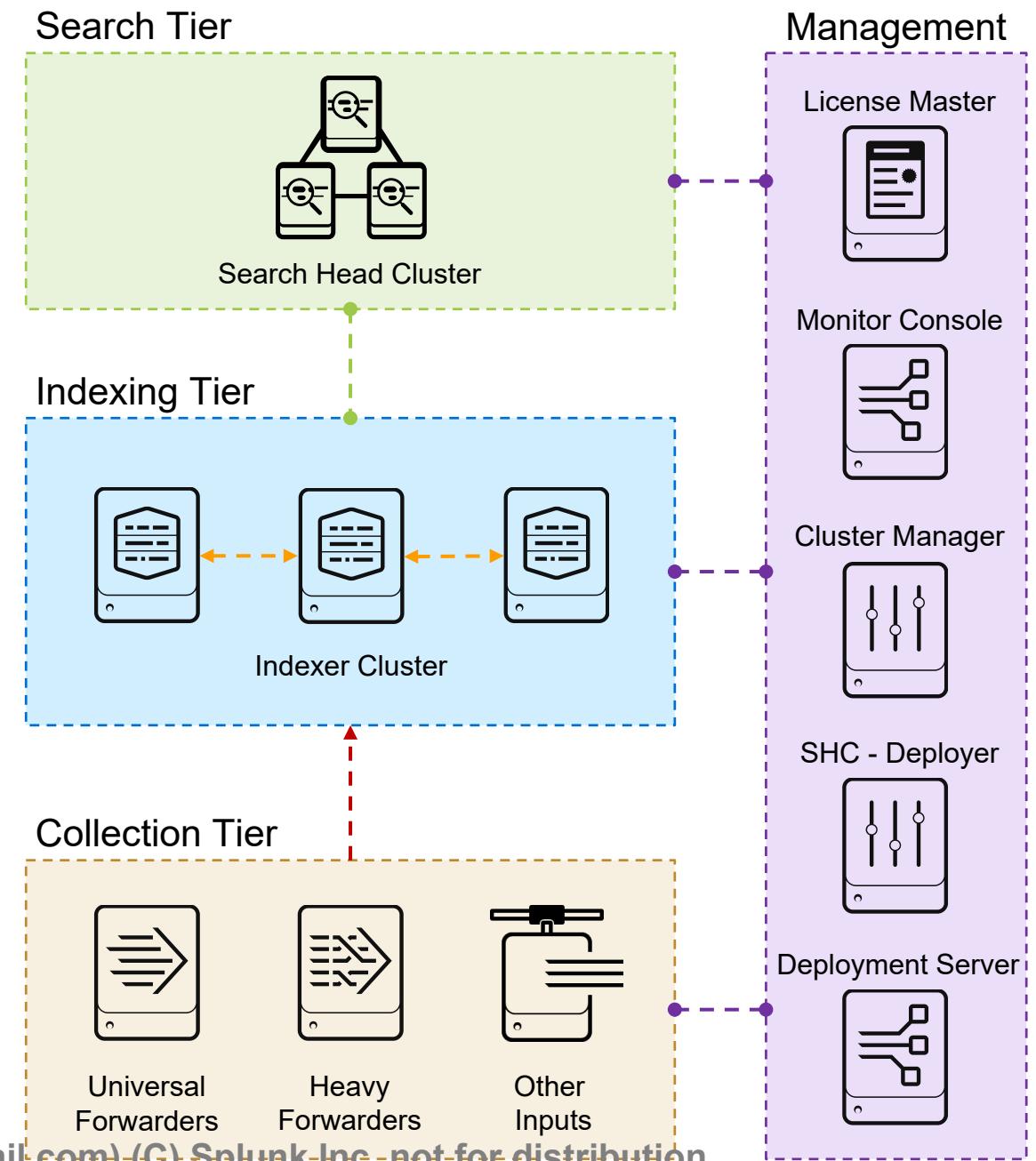
- Centralize management using dedicated servers for various functions including:
 - Deployment server for forwarder management
 - License Master
 - Monitoring Console



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

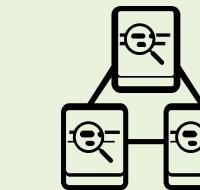


Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Splunk Core Components and Processes

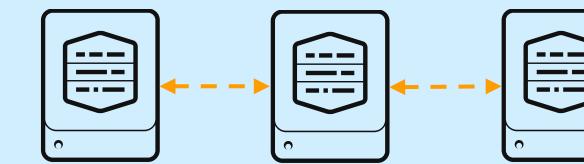
- Allow users to submit search requests using SPL
- Distribute search requests to the indexers
- Consolidate results and render visualizations of results
- Store search-time knowledge objects (such as field extractions, alerts, and dashboards)

Search Tier



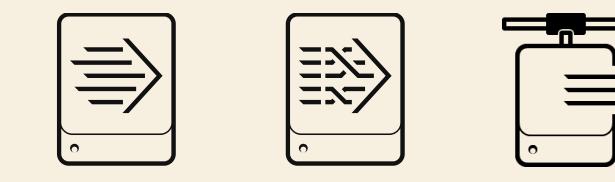
Search Head Cluster

Indexing Tier



Indexer Cluster

Collection Tier



Universal
Forwarders

Heavy
Forwarders

Other
Inputs

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

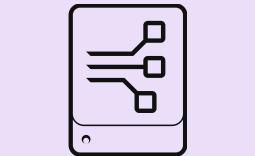
- Monitor configured inputs and forward the data to the indexers (best practice data collection method)
- Requires minimal resources and typically installed on the machines that produce the data

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

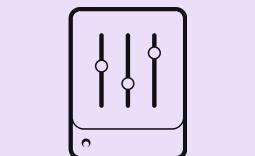
Management



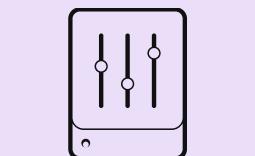
Monitor Console



Cluster Manager



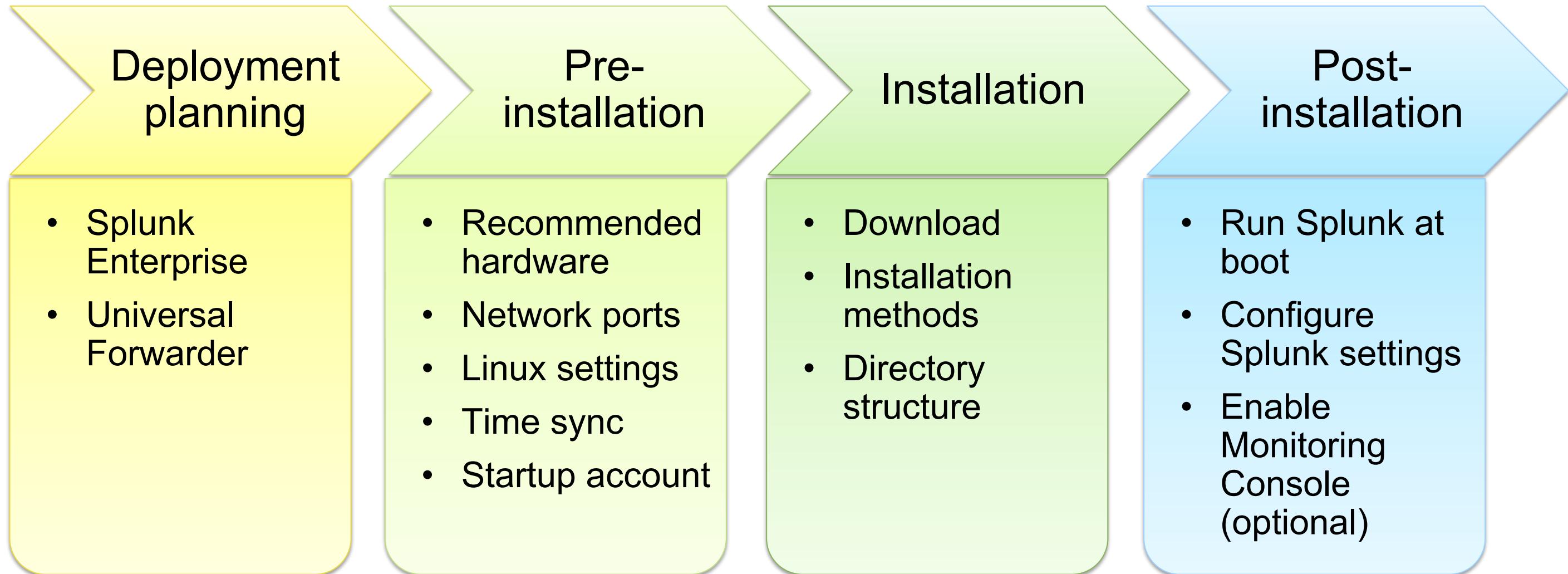
SHC - Deployer



Deployment Server

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

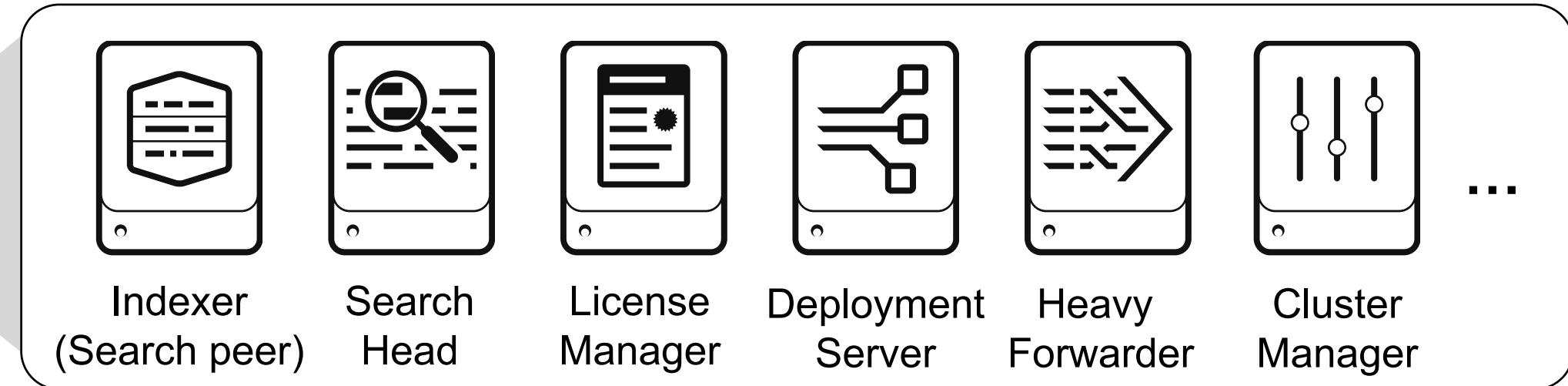
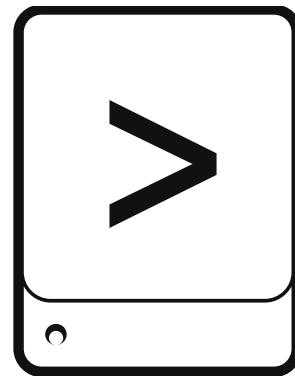
Splunk Installation Overview



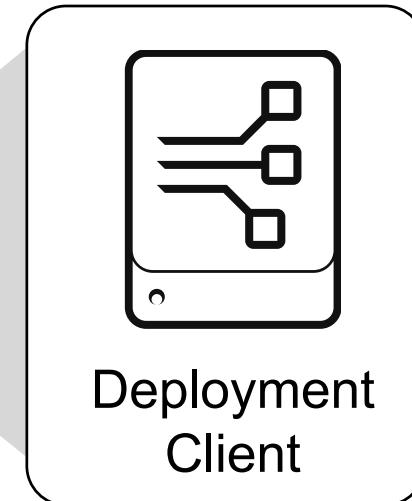
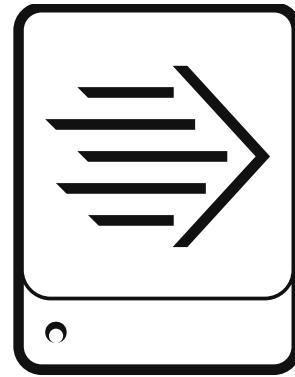
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Software in Splunk Enterprise packages

**Splunk
Enterprise
package**



**Universal
Forwarder
package**



Note



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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

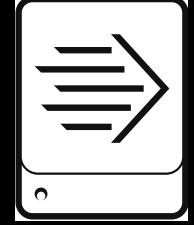
Server Hardware Recommendations

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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	-

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

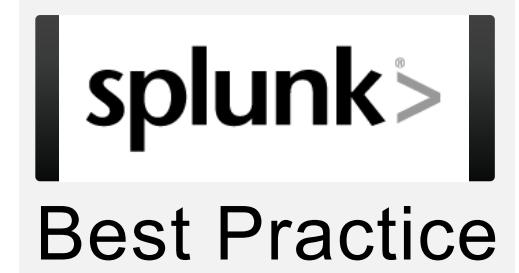
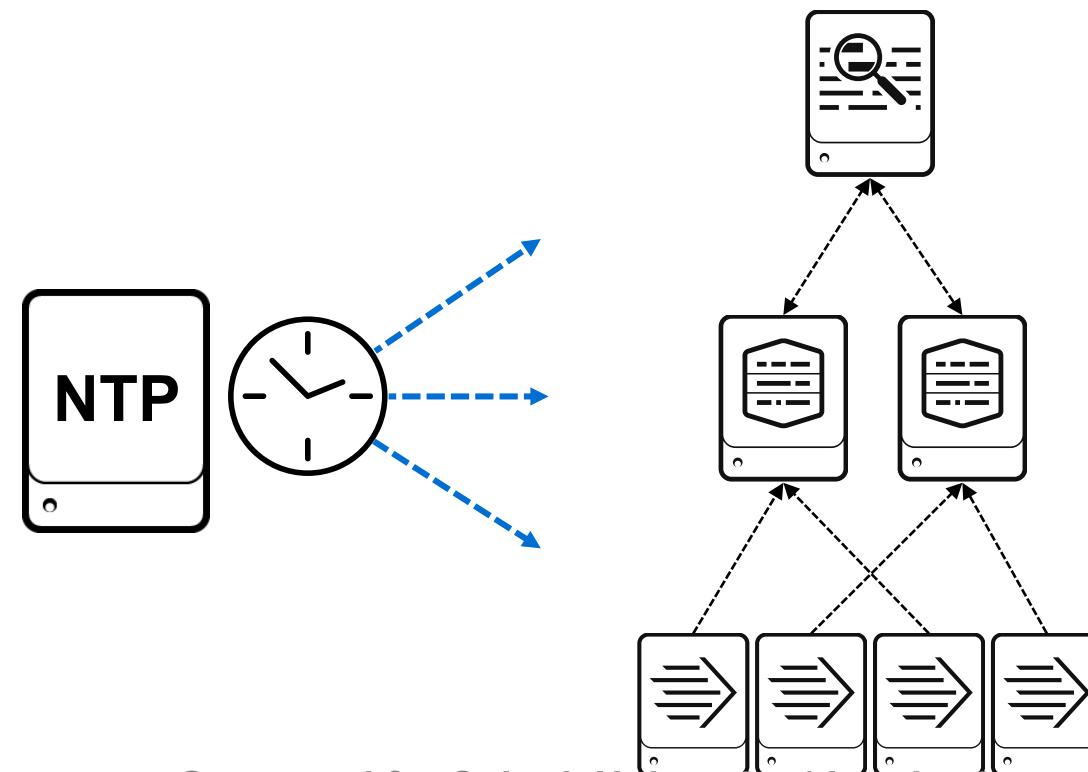
Linux Setting Recommendations

- 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)



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

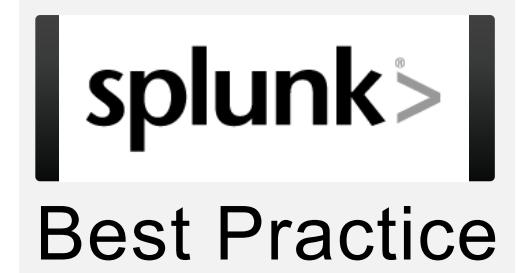
Startup Account

- Do not run Splunk as *super-user*

*NIX	<ul style="list-style-type: none">• Avoid the root account
Windows	<ul style="list-style-type: none">• 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)



Installing Splunk Enterprise Server

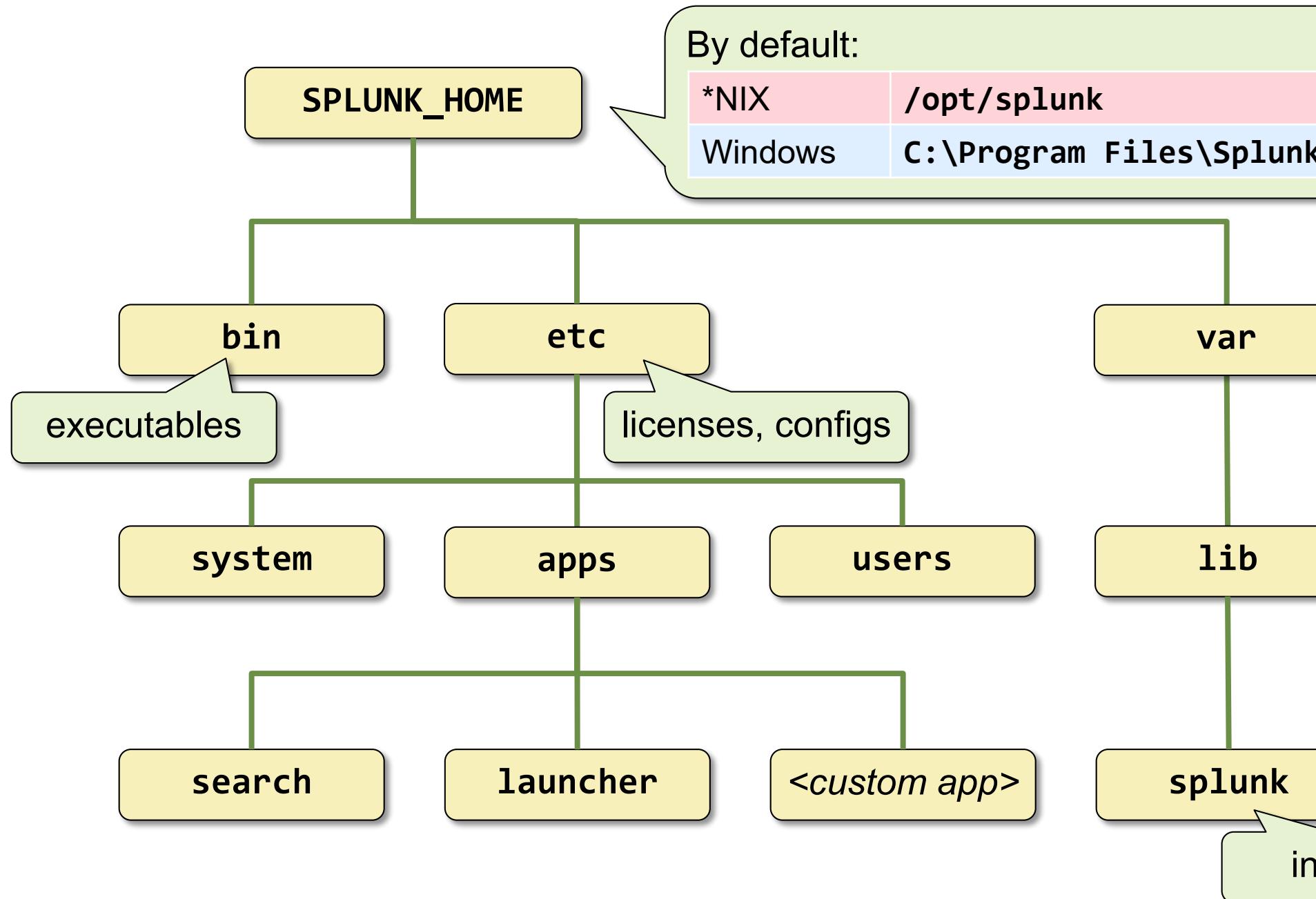
	*NIX	Windows
Download	https://www.splunk.com/download	
Install	<ul style="list-style-type: none">Un-compress .tar.gz file in the path you want Splunk to run fromAlso available as rpm, deb	Execute the .msi installer and follow the wizard steps
Post-Install	<ul style="list-style-type: none">Splunk starts manuallyEnable boot-start to have Splunk start automatically	Splunk starts automatically

Installation instructions at:

docs.splunk.com/Documentation/Splunk/latest/Installation/Chooseyourplatform

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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**



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

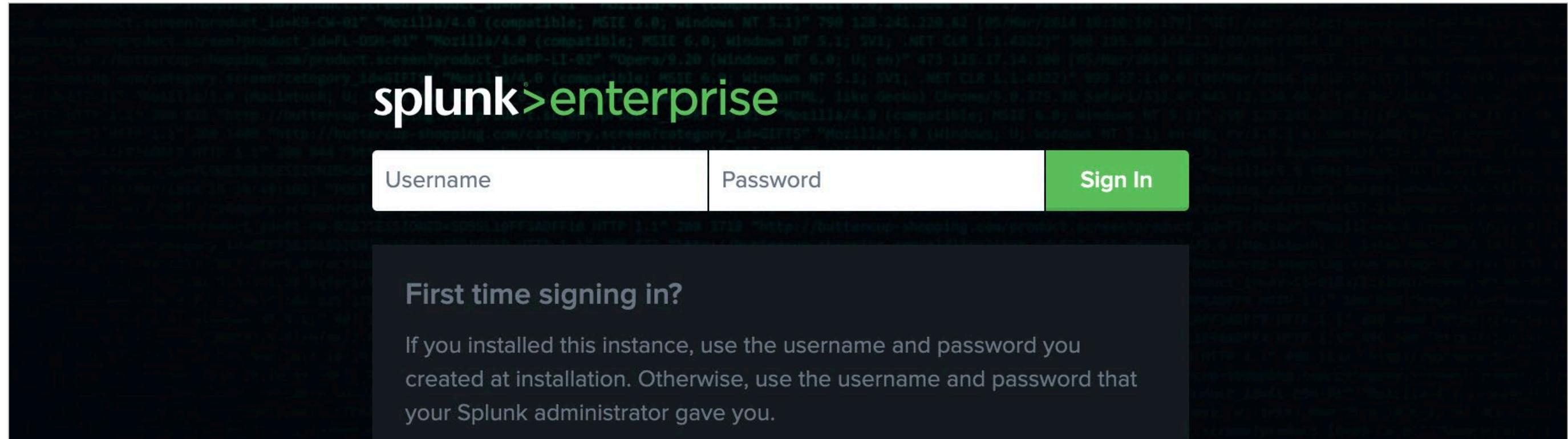
The **splunkd** Process

- 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)



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Splunk Web – Server Settings

The screenshot shows the Splunk Web interface. At the top is a navigation bar with links for Administrator, Messages, Settings, Activity, Help, and Find. Below the navigation bar is a sidebar with icons for Add Data, Explore Data, Monitoring Console, and a System section containing 'Server settings' (which is highlighted with a red circle labeled '1'), 'Server controls', 'Health report manager', 'RapidDiag', 'Instrumentation', 'Licensing', and 'Workload management'. The main content area is divided into several sections: KNOWLEDGE (Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; All configurations), DATA (Data inputs; Forwarding and receiving; Indexes; Report acceleration summaries; Virtual indexes; Source types), DISTRIBUTED ENVIRONMENT (Indexer clustering; Forwarder management; Data Fabric; Federated search; Distributed search), USERS AND AUTHENTICATION (Roles; Users; Tokens; Password Management; Authentication Methods). A large orange callout box on the right side of the slide points to the 'Server settings' link in the sidebar.

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

Server settings

Manage system settings including ports, host name, index path, email server, and s

3

General settings

Used to set server configuration and server options

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Describing General Settings

General settings

Server settings » General settings

Splunk server name *	splunk01	Identifies this server to other Splunk servers
Installation path	/opt/splunk	Splunk installation path: SPLUNK_HOME
Management port *	8089	splunkd port
	Port that Splunk Web uses to communicate with the splunkd process. This port is also used for distributed search.	
SSO Trusted IP		IP address used for SSO authentication configurations
	The IP address to accept trusted logins from. Only set this if you are using single sign-on (SSO) with a proxy server for authentication.	

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Describing General Settings – Splunk Web

Splunk Web

Run Splunk Web Yes No

Enable SSL (HTTPS) in Splunk Web? Yes No

Web port * 8000

App server ports 8065

Port number(s) for the python-based application server to listen on. Use comma-separated list to specify more than one port number.

Session timeout * 1h

Set the Splunk Web session timeout. Use the same notation as relative time modifiers, for example 3h, 100s, 6d.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Describing General Settings – Index/KV Store

Index settings

Default host name	splunk01	Default host field for inputs forwarded from this server
Path to indexes	/opt/splunk/var/lib/splunk	Path to the existing indexes: SPLUNK_DB (read-only in UI)
Pause indexing if free disk space (in MB) falls below *	5000	Minimum free disk space required or Splunk pauses indexing

KV Store

Port *	8191	Port that splunkd uses to connect to the KV Store server.
--------	------	---

Cancel **Save**

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Restarting the Server from Splunk Web

The screenshot shows the Splunk Web interface with the following elements:

- Header:** splunk>enterprise, Apps ▾, Admin... ▾, **1 Messages ▾** (highlighted with a green box and orange circle with '1'), Settings ▾, Activity ▾, Help ▾, Find, and a magnifying glass icon.
- Server settings:** Successfully updated "settings".
- Message Overlay:** A yellow warning message: "Splunk must be restarted for changes to take effect." with a link "Click here to restart from Server controls." (highlighted with a blue box and orange circle with '2').
- Server controls:** General settings, Note, and Restart Splunk.
- Note:** Any changes to **General settings** generate a message. Clicking the indicator opens a message, prompting you to restart.
- Restart Splunk:** Click the button below to restart Splunk. (highlighted with a green box and orange circle with '3').

A green arrow points from the "Note" section back to the "General settings" link in the message overlay.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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/

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

The screenshot shows the Splunk Monitoring Console (MC) interface. The left sidebar includes links for Add Data, Explore Data, and Monitoring Console (which is highlighted with a green border). The main dashboard displays various monitoring metrics and status information.

Splunk Enterprise Server 8.2.0
Linux, 7.5 GB Physical Memory, 2 CPU Cores
Mode: Standalone

INDEXING RATE
5.58 KB/s (Total)

LICENSE USAGE
Today 0%

DISK USAGE
Disk 12%

CONCURRENT SEARCHES
1 Searches

CONCURRENT SEARCHES BY TYPE

CPU USAGE

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Enabling MC in Standalone Mode

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

The screenshot shows the Splunk Enterprise Monitoring Console interface. The top navigation bar includes links for Overview, Summary, Health Check, Indexing, Search, Resource Usage, Forwarders, Settings (which is highlighted with a red circle labeled 1), and Run a Search. The right side of the header has links for Administrator, Messages, Settings, Activity, Help, Find, and a search icon.

The main content area is titled "Setup" and displays the current topology of the Splunk Enterprise deployment. It includes tabs for Mode (Standalone is selected and highlighted with a green box), and sections for This instance and Other instances. The "This instance" section shows details for "splunk02": Instance (host) is "splunk02", Instance (serverName) is "splunk02", Machine is "ip-10-0-0-202", and Server roles are listed as "Indexer", "License", "Master", "KV Store", and "Search Head". A callout bubble labeled "Default server roles" points to the "Server roles" section.

A dropdown menu is open from the "Settings" link in the header, with "General Setup" selected (highlighted with a red circle labeled 2). Other options in the menu include "Forwarder Monitoring Setup", "Alerts Setup", "Overview Preferences", and "Health Check Items".

At the bottom right of the page, there are two buttons: "Reset All Settings" and "Apply Changes" (highlighted with a red circle labeled 3). A callout bubble labeled "Edit monitoring of server roles" points to the "Actions" button for the "splunk02" instance.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

splunk>enterprise Apps ▾

Admin ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Overview Health Check Indexing ▾ Search ▾ Resource Usage ▾ Forwarders ▾ Settings ▾ Run a Search Monitoring Console

Platform Alerts Setup

Manage Monitoring Console platform alerts. [Learn More](#)

8 Alerts filter

Name	Actions	Status
DMC Alert - Abnormal State of Indexer Processor One or more of your indexers is reporting an abnormal state.	Edit Advanced Edit Enable	Disabled
DMC Alert - Critical System Physical Memory Usage One or more instances has exceeded 90% memory usage.	Edit Advanced Edit Enable	Disabled
DMC Alert - Expired and Soon To Expire Licenses You have licenses that expired or will expire within 2 weeks.	Edit Advanced Edit Enable	Disabled
DMC Alert - Missing forwarders One or more forwarders are missing.	Edit Advanced Edit Enable	Disabled
DMC Alert - Near Critical Disk Usage You have used 80% of your disk capacity.	Edit Advanced Edit Enable	Disabled
DMC Alert - Saturated Event-Processing Queues One or more of your indexer queues is reporting a fill percentage, averaged over the last 15 minutes, of 90% or more.	Edit Advanced Edit Enable	Disabled
DMC Alert - Search Peer Not Responding One or more of your search peers is currently down.	Edit Advanced Edit Enable	Disabled
DMC Alert - Total License Usage Near Daily Quota You have used 90% of your total daily license quota.	Edit Advanced Edit Enable	Disabled

Disabled by default

MC Health Check

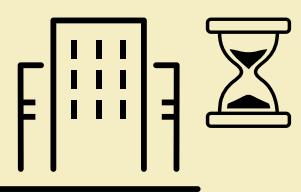
- Series of ad hoc searches that run sequentially:
 - Monitoring Console > Health Check
- Comes preconfigured but can be disabled, modified, created, and exported using:
 - Settings > Health Check Items

The screenshot shows the Splunk Enterprise Health Check interface. At the top, there's a navigation bar with links for Overview, Summary, Health Check (which is selected), Indexing, Search, Resource Usage, Forwarders, Settings, and Run a Search. Below the navigation is a sub-header for 'Health Check' with a sub-instruction to 'Add additional items to this list go to: [Health Check Items](#)'. It displays the instance as 'splunk02' and the app as 'All'. There are filters for 'Tags' and 'Category'. The main area is a table with the following data:

Check	Category	Tags	Results
System hardware provisioning assessment	System and Environment	best_practices, capacity, scalability	⚠ One or more hosts has returned CPU or
Assessment of server ulimits	System and Environment	best_practices, operating_system	⚠ One or more Splunk instances are runni
Event-processing issues	Data Collection	event_breaking, indexing, timestamp_extraction	✓ This health check item was successful.
Expiring or expired licenses	Data Indexing	licensing	✓ This health check item was successful.
Indexing status	Data Indexing	buckets, indexing	✓ This health check item was successful.
License warnings and violations	Data Indexing	indexing, licensing	✓ This health check item was successful.
Saturation of event-processing queues	Data Indexing	indexing, queues	✓ This health check item was successful.
Search scheduler skip ratio	Data Search	scheduler, searches_skipped	✓ This health check item was successful.
Excessive physical memory usage	Splunk Miscellaneous	resource_usage	✓ This health check item was successful.
Integrity check of installed files	Splunk Miscellaneous	configuration, installation	✓ This health check item was successful.
KV Store status	Splunk Miscellaneous	kv_store	✓ This health check item was successful.
Orphaned scheduled searches	Splunk Miscellaneous	configuration, search, searches_skipped	✓ This health check item was successful.
Near-critical disk usage	System and Environment	capacity, disk_space, searches_skipped, storage	✓ This health check item was successful.
Linux kernel transparent huge pages	System and Environment	best_practices, operating_system	✓ This health check item was successful.
Missing forwarders	Data Indexing	batchreader, forwarding, tailreader	▬ This health check item is not applicable

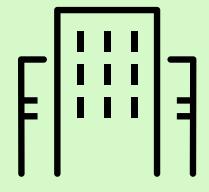
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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



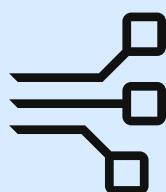
Enterprise license

- 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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

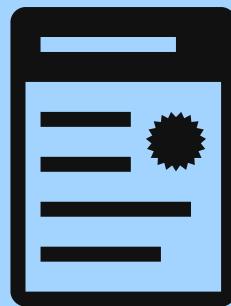
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Measuring Daily License Quota



Counts for daily license quota

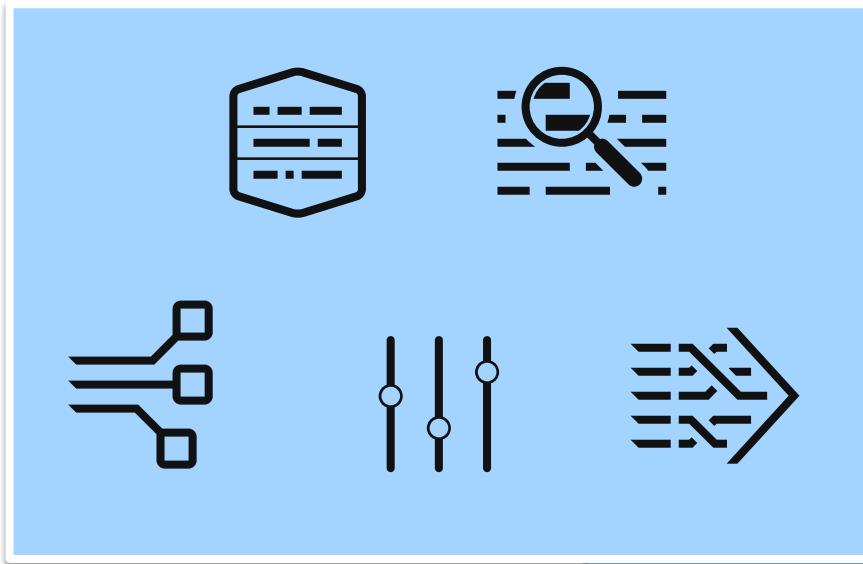
- All data from all sources that is indexed
- **For events:** Measured as the data (full size) that flows through the parsing pipeline per day
- **For metrics:** Measurement capped at 150 bytes per metric event



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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

The screenshot shows the Splunk Licensing interface with several numbered callouts:

1. A button to "Change to slave" from a "master license server".
2. A section for the "Enterprise license group" with a "Change license group" button.
3. Buttons for "Add license" and "Usage report".
4. A section for "Alerts" with a message about license enforcement and a link to learn more.
5. A section for the "Splunk Enterprise Sales Trial stack" with a "Learn more" link.
6. An "Edit | Delete" button for a license pool entry.

Below these sections, there is a table for managing license stacks:

Licenses	Volume	Expiration	Status
Splunk Enterprise Sales Trial Notes	200 MB	May 9, 2021, 6:59:59 AM	valid
Effective daily volume			200 MB
Pools	Indexers	Volume used today	
auto_generated_pool_enterprise		0 MB / 200 MB	
No indexers have reported into this pool today			
+ Add pool			

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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)

The diagram illustrates the process of adding a license. On the left, a screenshot of the Splunk Web interface shows the 'Add new license' page. It includes a 'Choose File' input field with 'No file chosen', a note about XML direct paste, and 'Cancel' and 'Install' buttons. A green arrow points from the 'Install' button to the 'licenses' folder in the file system tree on the right. The file system tree shows the directory structure: SPLUNK_HOME/bin, SPLUNK_HOME/etc/apps, SPLUNK_HOME/etc/licenses (which contains download-trial and enterprise), and SPLUNK_HOME/system.

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Viewing License Alerts

Alerts

This deployment is subject to license enforcement. Search is disabled after 45 warnings over a 60-day window [Learn more](#)

Licensing alerts notify you of excessive indexing warnings and licensing misconfigurations. [Learn more](#)

From Splunk Web, select
Licensing > License Alerts

Current

- 1 cle_pool_over_quota message reported by 1 indexer Correct by midnight to avoid warning [Learn more](#)
- 1 pool warning reported by 1 indexer Correct by midnight to avoid warning [Learn more](#)

Permanent

- No licensing violations

All licensing alerts (2)

License alerts notify you of excessive indexing warnings and licensing misconfigurations. If you receive too many warnings, your indexer will be in violation of the license and you will not be able to search. [Learn more](#)

Current:

Severity	Time	Message	Indexer	Pool	Stack	Category
●	Correct by midnight to avoid violation Learn more	This pool contains slave(s) with 0 warning(s)	splunk02	auto_generated_pool_enterprise	enterprise	pool_warning_count
●	Correct by midnight to avoid violation Learn more	This pool is over poolsz=157286400 bytes, please correct before midnight		auto_generated_pool_enterprise	enterprise	cle_pool_over_quota

Permanent:

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Changing an Instance to Use a License Master

Change master association

This server, **splunk02**, is currently acting as a master license server.

- Designate this Splunk instance, **splunk02**, as the master license server

Choosing this option will:

- Point the local indexer at the local master license server
- Disconnect the local indexer from any remote license server

- Designate a different Splunk instance as the master license server

Choosing this option will:

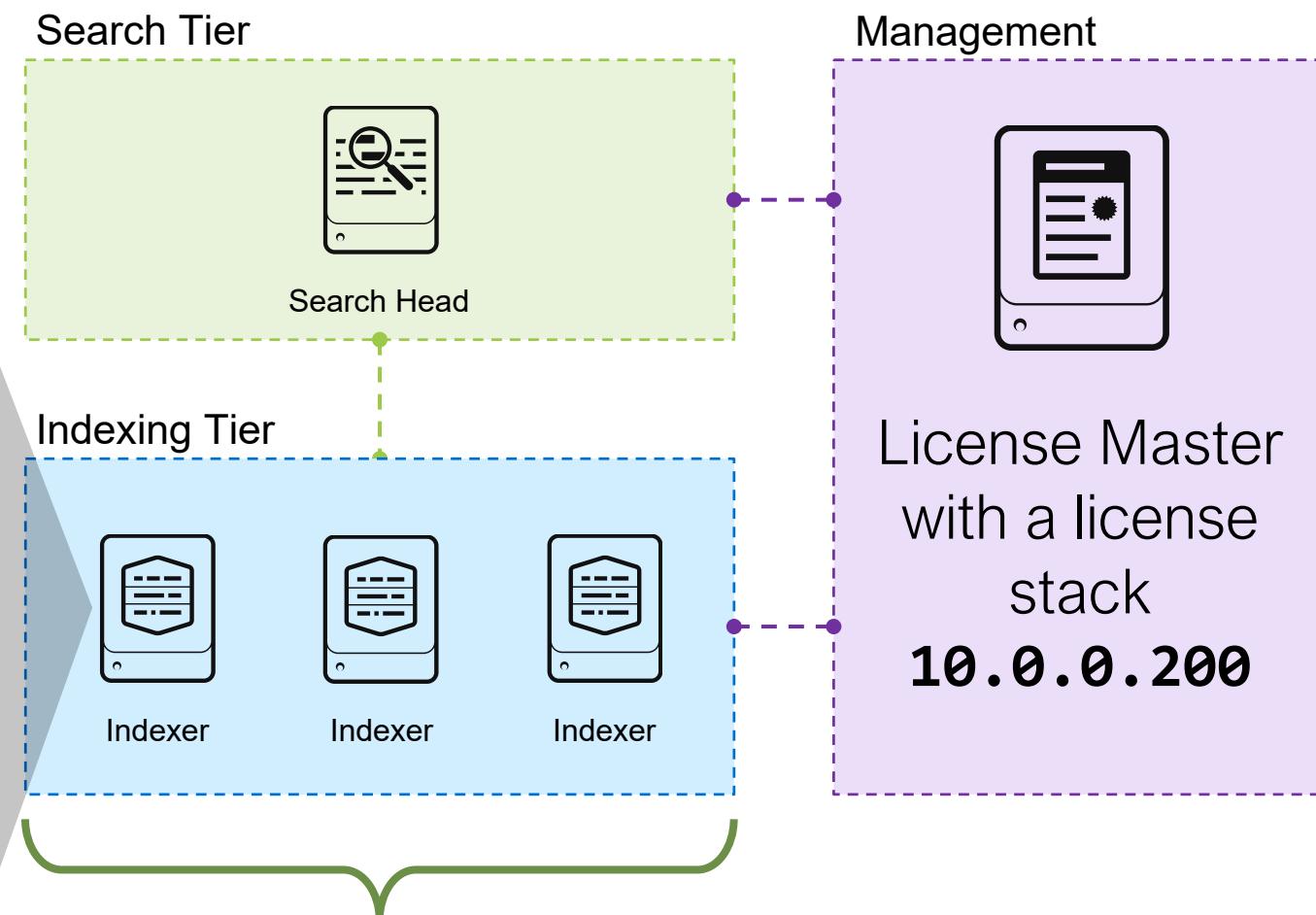
- Deactivate the local master license server
- Point the local indexer at license server specified below
- Discontinue license services to remote indexers currently pointing to this server

Master license server URI

`https://10.0.0.200:8089`

For example: `https://splunk_license_server:8089`

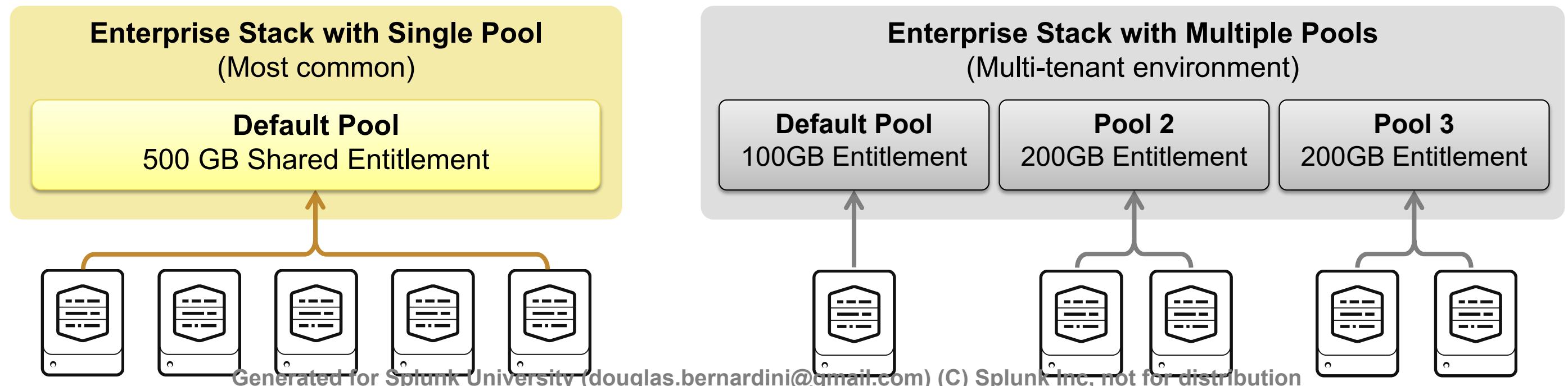
Use https and specify the management port.



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Splunk Enterprise Sales Trial stack [Learn more](#)

Licenses	Volume	Expiration
Splunk Enterprise Sales Trial Notes	200 MB	May 9, 2021, 6:59:59 AM
Effective daily volume	200 MB	
Pools	Indexers	Volume used today
auto_generated_pool_enterprise		0 MB / 200 MB

No indexers have reported into this pool today

+ Add pool

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Set

Overview Summary Health Check Indexing ▾ Search ▾ Resource Usage ▾ Forwarders ▾ Settings ▾

Platform Alerts Setup

Manage Monitoring Console platform alerts. [Learn More](#)

2 Alerts X

Name
DMC Alert - Expired and Soon To Expire Licenses
You have instances with licenses that expired or will expire within 2 weeks. No other valid licenses are installed.
DMC Alert - Total License Usage Near Daily Quota
You have used 90% of your total daily license quota.

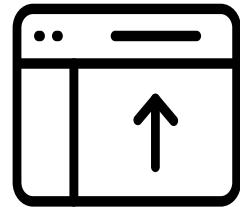
General Setup
Forwarder Monitoring Setup
✓ Alerts Setup
Overview Preferences
Health Check Items

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Ingest-Based versus Infrastructure-Based Pricing

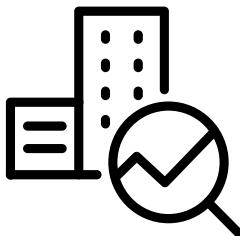
Ingest-Based Pricing

- 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



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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 collects 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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

The screenshot shows the Splunk Web interface with a navigation bar at the top. The 'Administrator' dropdown has a yellow warning icon. The 'Messages' dropdown shows 17 messages. The 'Find' button is also visible. The main content area is titled 'Health of Splunk Deployment'. It contains sections for 'splunkd' (File Monitor Input, BatchReader-0, Ingestion Latency, TailReader-0), 'Index Processor' (Buckets, Disk Space, Index Optimization), and 'Indexer Clustering' (Cluster Bundles, Data Durability, Data Searchable). A 'RapidDiag' link is highlighted with a green box and an arrow pointing to it. Another green box highlights the 'Index Processor' section. On the right side, there's a 'Indexers' section with 'Root Cause(s)' and 'Unhealthy Instances' listed, along with a 'Generate Diag' button. A third green box highlights the 'Indexing Ready' status under 'Index Processor'.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Module 3: Splunk Apps

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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)



app.conf

props.conf

indexes.conf

inputs.conf

tags.conf

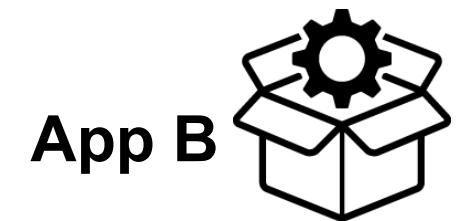
transforms.conf

...

default.meta

mylookup.csv

myviews.xml



app.conf

inputs.conf

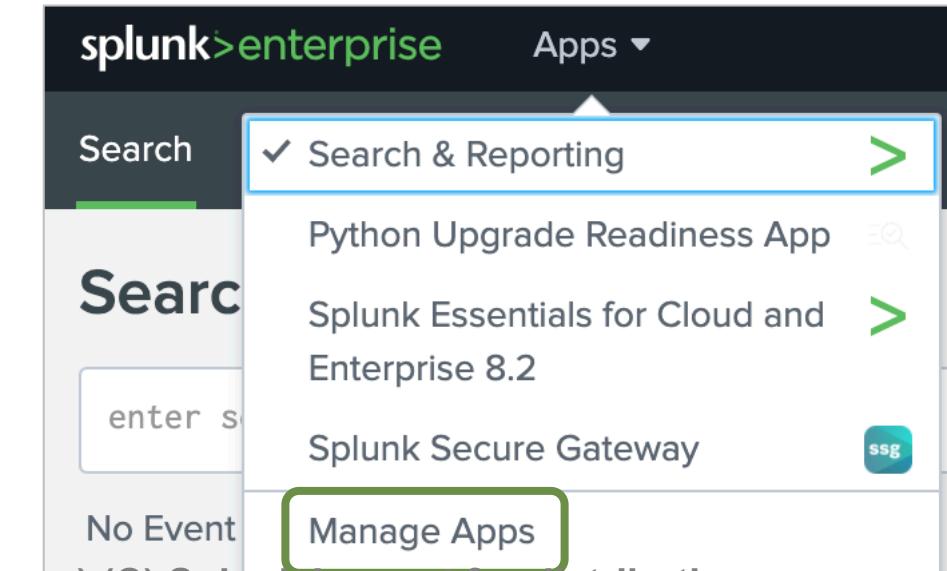
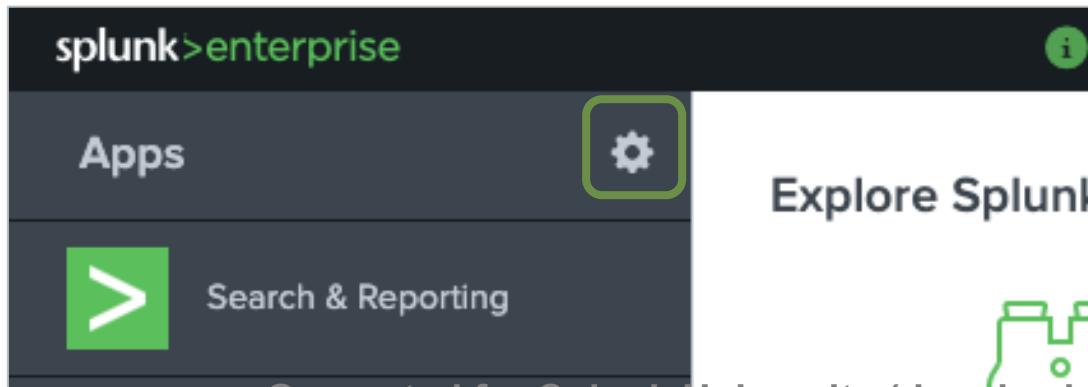
default.meta

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:

Within an app

On the Home view



Managing Apps

Apps							Add apps	Browse more apps	Install app from file	Create app
Showing 1-23 of 23 items										
Name	Folder name	Version	Update checking	Visible	Sharing	Status				
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	Enable or disable app (restart may be required)			
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable				
Log Event Alert Action	alert_logevent	8.2.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects			
Webhook Alert Action	alert_webhook	8.2.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects			
Apps Browser	appsbrowser	8.2.0	Yes	No	App Permissions	Enabled	Edit properties View objects			
introspection_generator_addon	introspection_generator_addon	8.2.0	Yes	No	App Permissions	Enabled Disable	Edit properties View objects			
journald_input	journald_input		Yes	No	App Permissions	Enabled Disable	Edit properties View objects			
Home	launcher				App Permissions	Enabled	Launch app Edit properties View objects			
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View objects			
legacy	legacy		Yes	No	App Permissions	Disabled Enable				
Python Upgrade Readiness App	python_upgrade_readiness_app	1.0.0	Yes	Yes	App Permissions	Enabled Disable	Launch app Edit properties View objects			
sample data	sample_app		Yes	No	App Permissions	Disabled Enable				

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

App permissions

Users with read access can only save objects for themselves, and

Roles	Read	Write
Everyone	<input checked="" type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input checked="" type="checkbox"/>
securegateway	<input type="checkbox"/>	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

Apply selected role permissions to:

[Learn more](#)

This app only (Search & Reporting) All apps (system)

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

The screenshot shows the Splunk Python Upgrade Readiness App interface. At the top, there's a navigation bar with 'splunk>enterprise' and 'Apps'. Below it, a search bar and a 'Search & Reporting' button are highlighted. A green arrow points down from the 'Search & Reporting' button to the main content area. The main content area has a title 'Python Upgrade Readiness App' and a sub-section 'About This App' which describes the app's purpose. It also shows 'Scan Results' with counts for failed and passed public and private apps. A green arrow points down from the 'Scan Results' section to the 'Private Apps' section. The 'Private Apps' section lists 'Citrix System Log Add-On for Splunk' with a 'Fail' status. A green box highlights the 'Details' section, which states 'This app is not compatible with Python 3.' Below this, 'Version' is listed as 1.0.1, 'Application Path' as '/opt/splunk/etc/apps/citrix-system-log-add-on', and 'Required Action' as 'Update this app or uninstall it. If you do nothing, the app will fail.' An 'Issue' is noted: 'File path designates Python 2 library.' A table titled 'Incompatible File Paths' lists two entries: 1. /opt/splunk/etc/apps/citrix-system-log-add-on/bin/citrix_system_log_records.py and 2. /opt/splunk/etc/apps/citrix-system-log-add-on/bin/citrix_system_log_add_on/aob_py2/decorator.py. Buttons for 'Dismiss App', 'Email Result', and 'Export Result' are shown at the bottom of the app details.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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	✓	✓

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Module Objectives

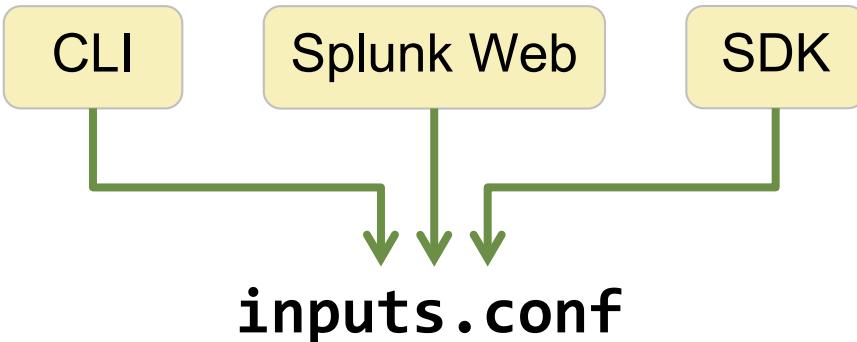
- Describe Splunk configuration directory structure
- Understand configuration layering process
 - Index time process
 - Search time process
- Use **btool** to examine configuration settings

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/**



```
[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
```

Host
Tell Splunk how to set the value of the host field in your events from
Set host constant value
Specify method for getting host
Host field value **splunk01**

Source type
Tell Splunk what kind of data this is so you can group it with other
can specify what you want if Splunk gets it wrong.
Set the source type Manual
When this is set to automatic
sourcetypes placeholder nam
Source type * **access_combined_wcookie**

Index
Set the destination index for this source.
Index **itops**

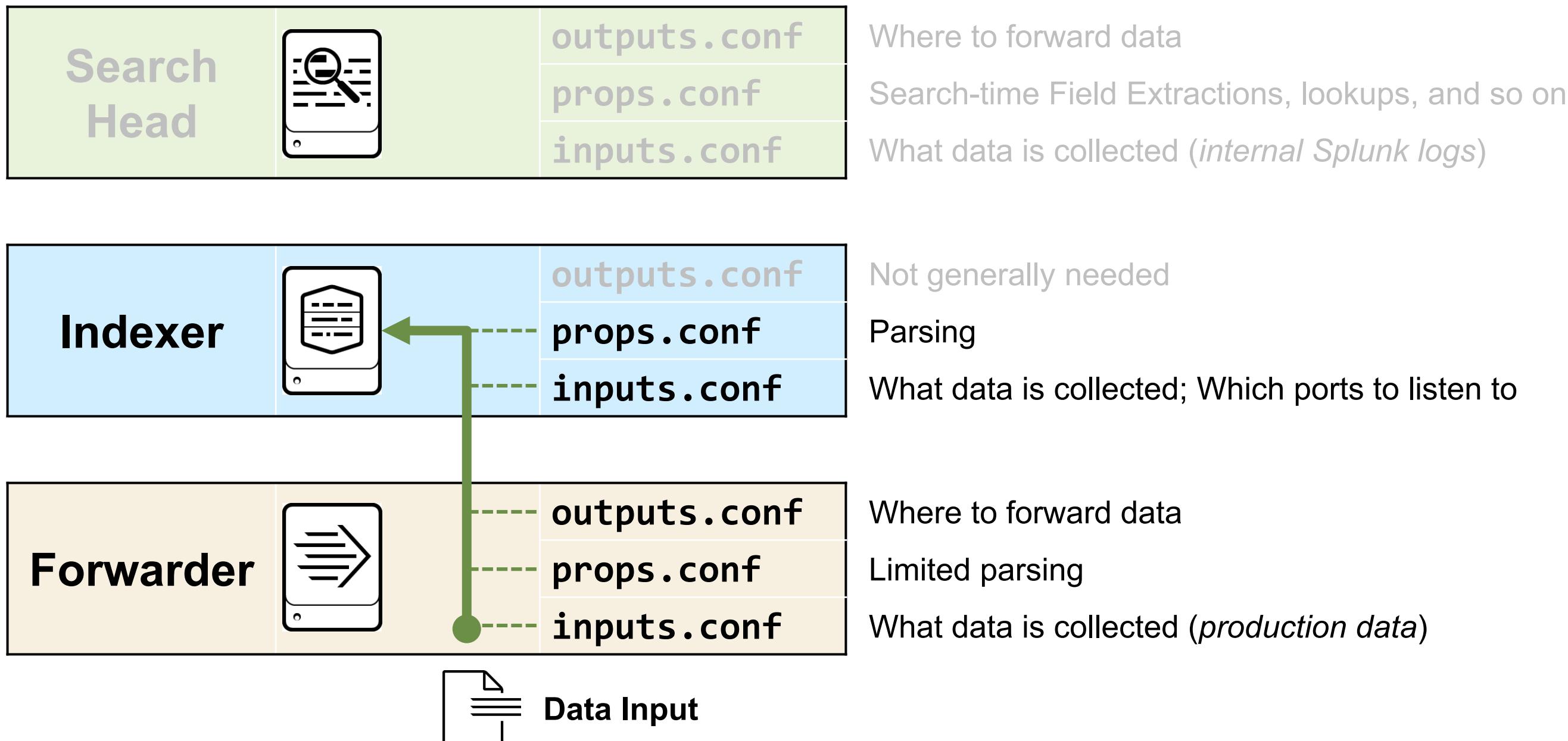
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Commonly Used Splunk Configuration Files

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

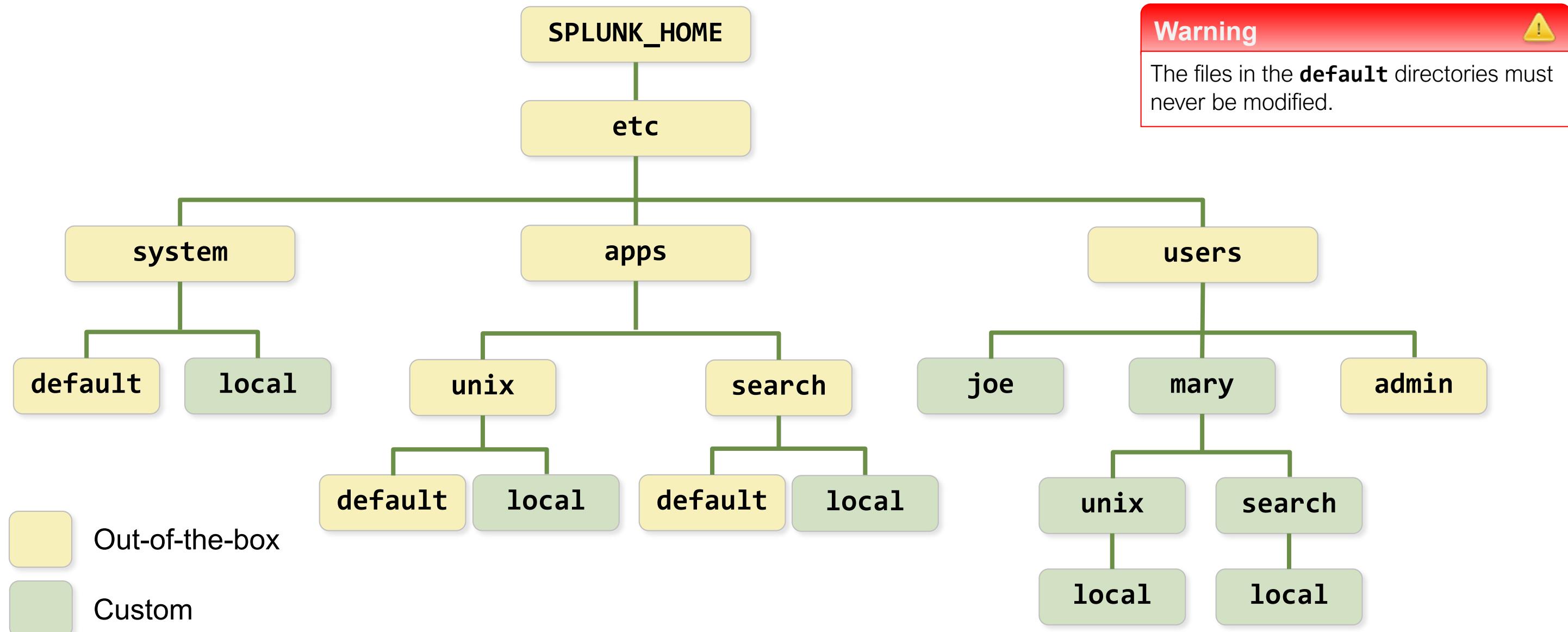
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Configuration Files Used During Data Input



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Configuration Directories

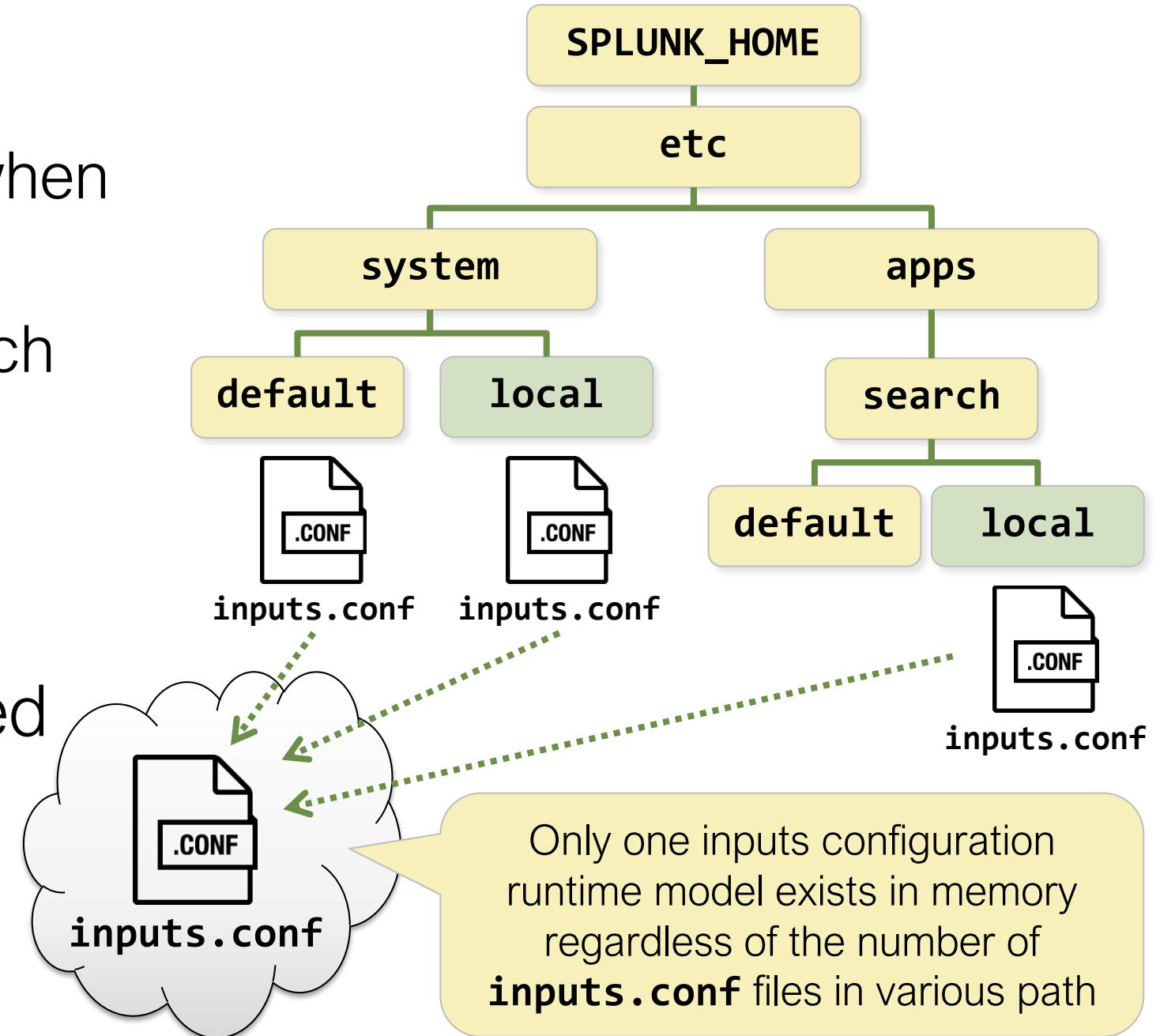


docs.splunk.com/Documentation/Splunk/latest/Admin>Listofconfigurationfiles

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

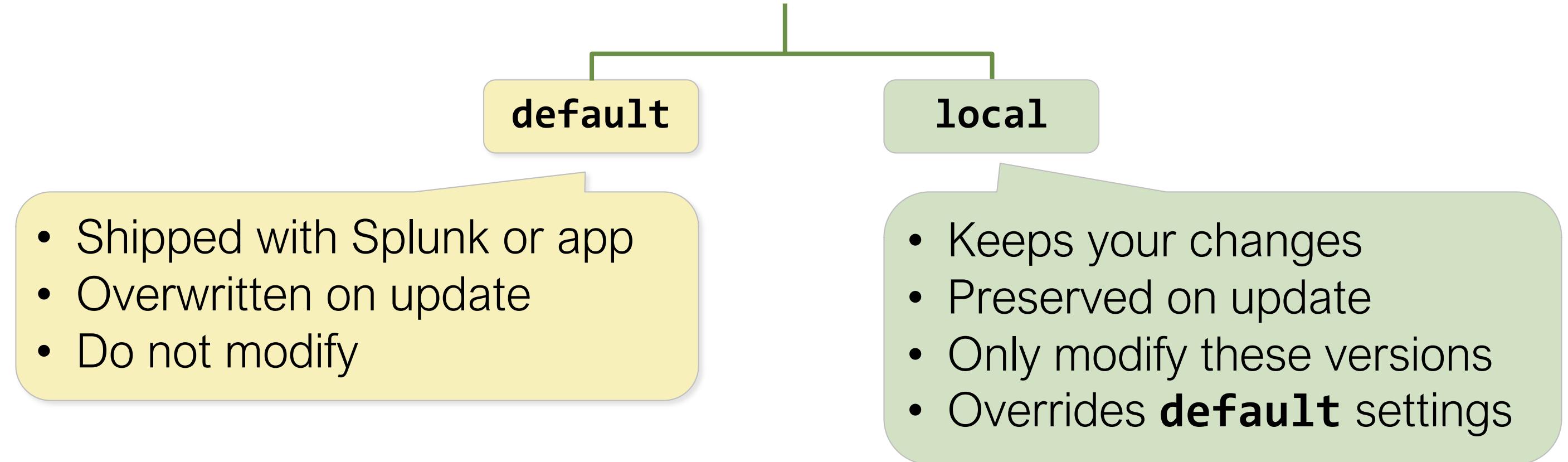
Merging of Configuration Files

- 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)



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Default versus Local Configuration



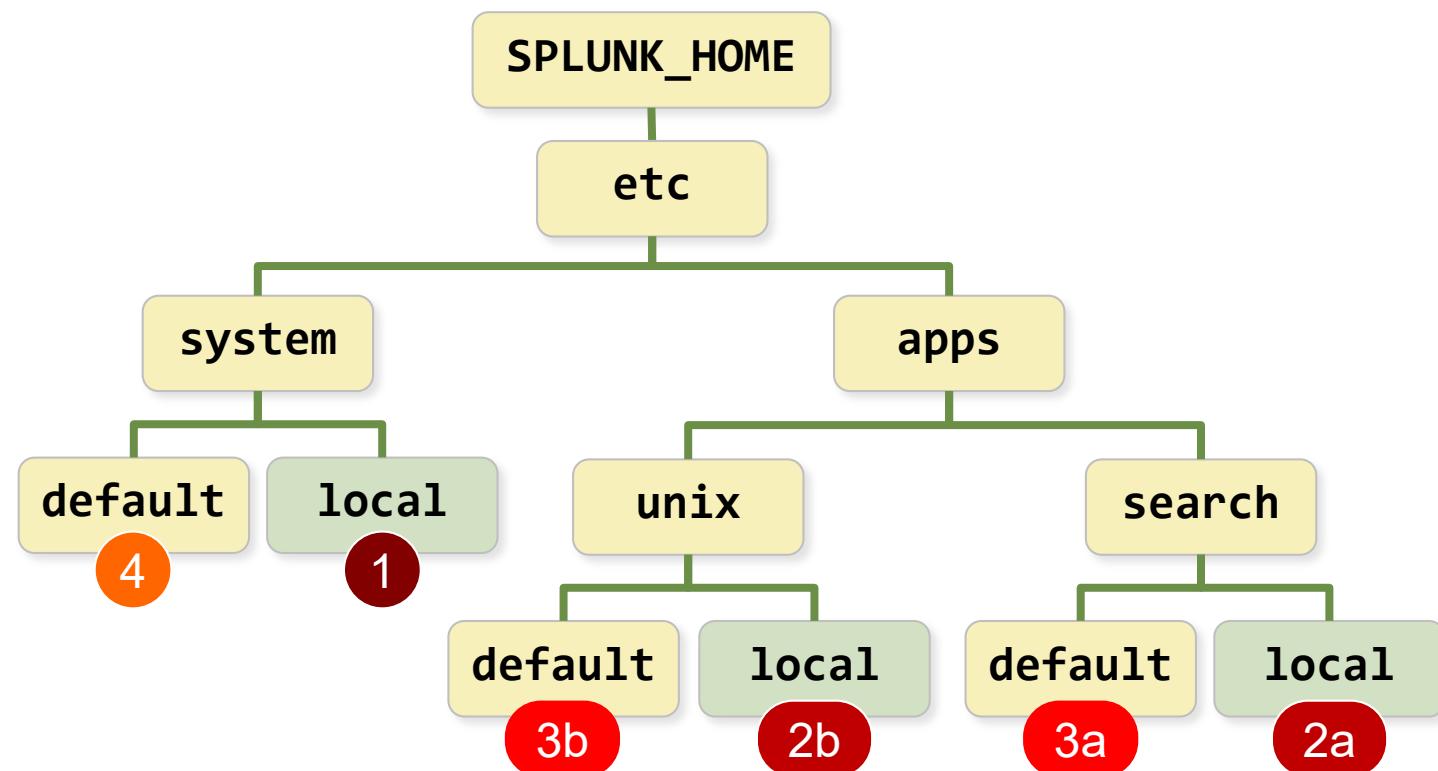
File Context and Index-time versus Search-time

	Global Context	App/User Context
<i>Used during:</i>	Index-time	Search-time
<i>Used by:</i>	<ul style="list-style-type: none">• User-independent tasks• Background tasks• Input, parsing, indexing	<ul style="list-style-type: none">• User-related activity• Searching• Search-time processing
<i>Example use-case:</i>	A network input to collect syslog data	Mary's private report in the Search app
<i>Example files:</i>	inputs.conf outputs.conf props.conf	macros.conf savedsearches.conf props.conf

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Index-Time Precedence (Global Context)



Precedence order

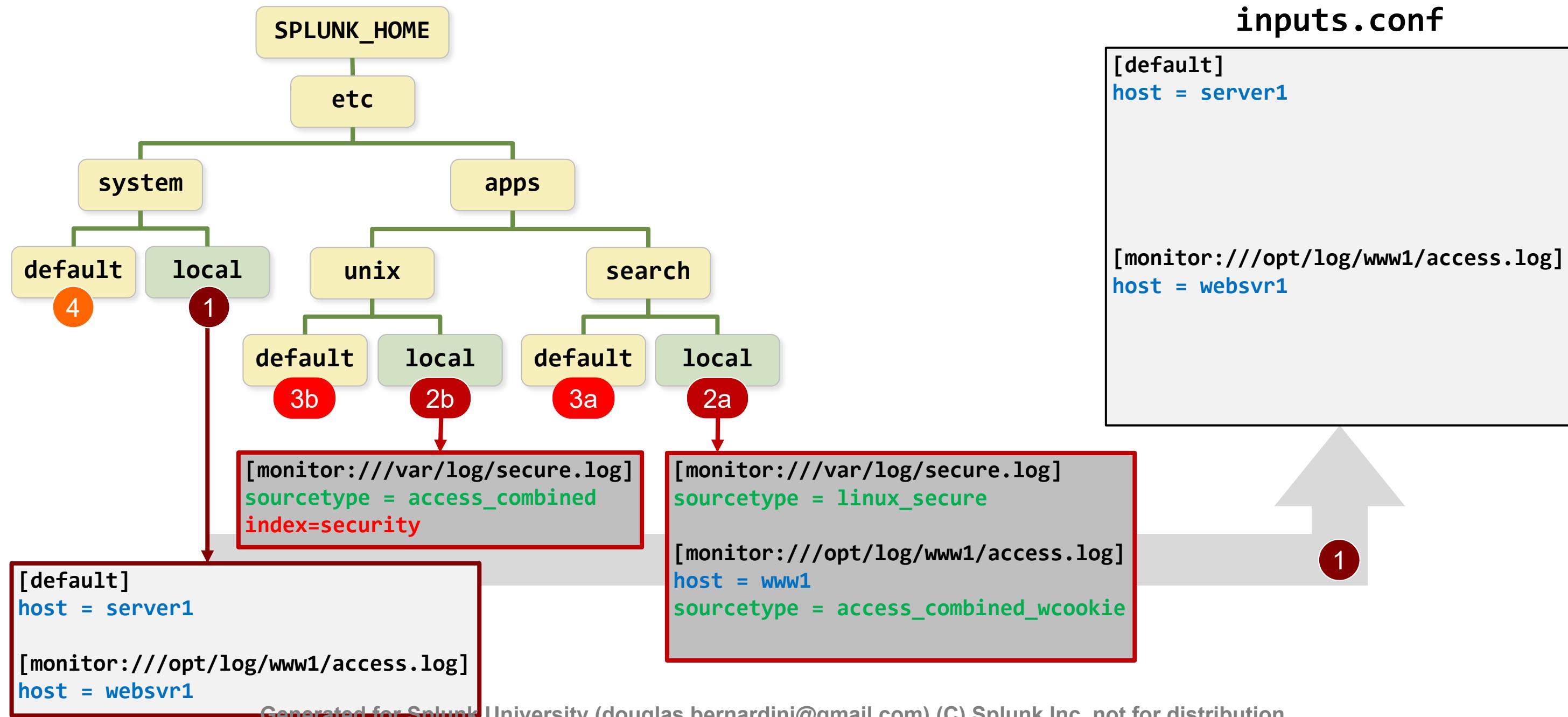
- 1 System local directory
`etc/system/local`
- 2 App local directories*
`etc/apps/appname/local`
- 3 App default directories*
`etc/apps/appname/default`
- 4 System default directory
`etc/system/default`

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)



`inputs.conf`

```
[default]
host = server1

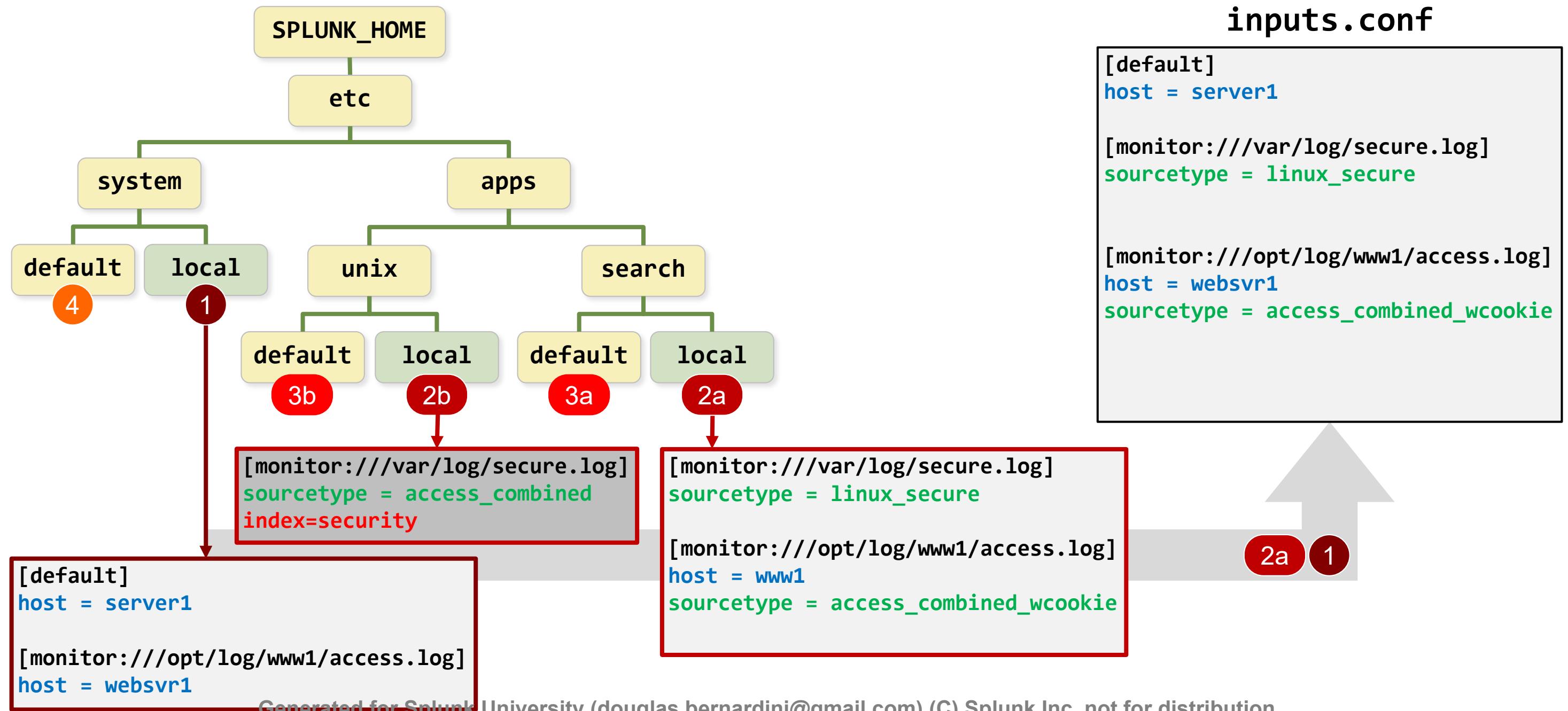
[monitor:///opt/log/www1/access.log]
host = websvr1
```

```
[default]
host = server1
```

```
[monitor:///opt/log/www1/access.log]
host = websvr1
```

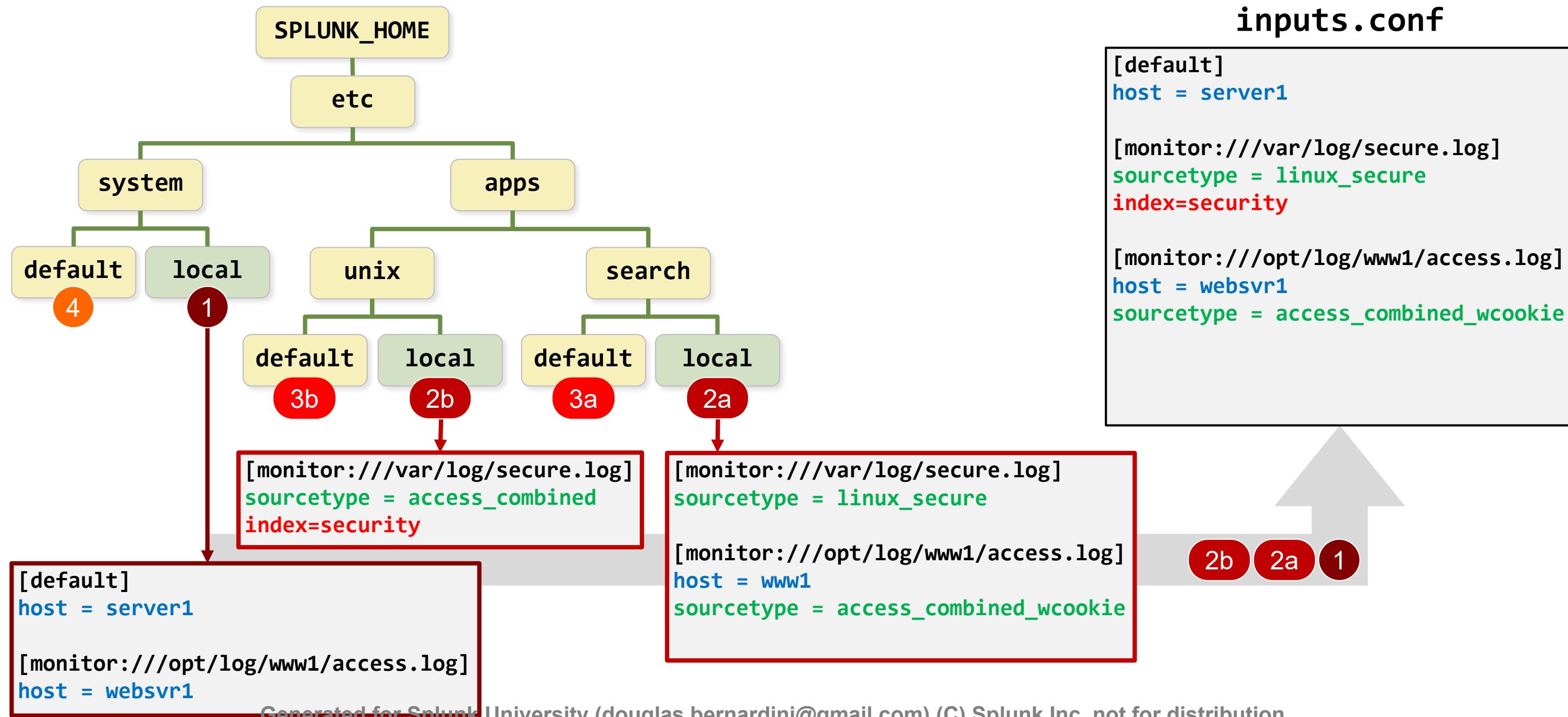
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Example of Index-Time Precedence (2)



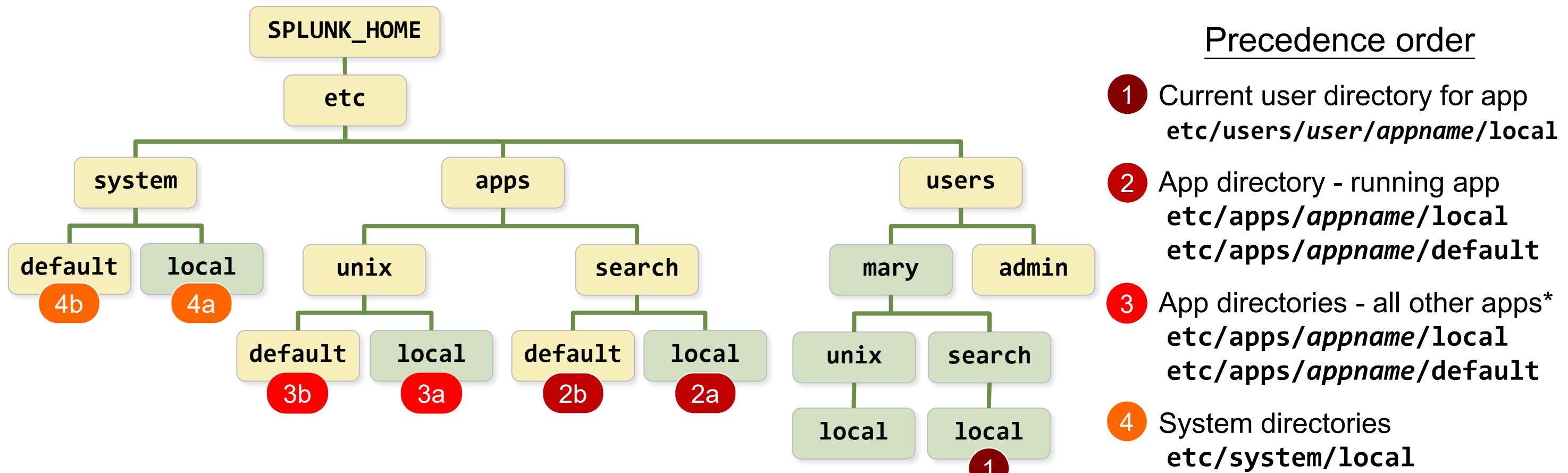
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Example of Index-Time Precedence (3)



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Search-Time Precedence (App/User Context)



Note

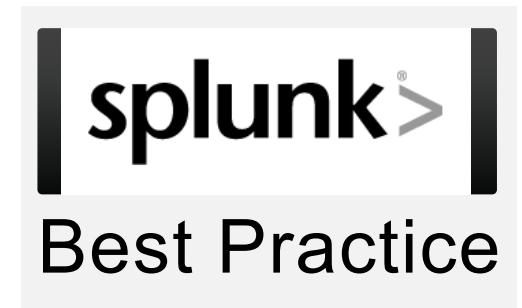


* If objects from the app are exported globally with `.meta` file setting, evaluate all other app directories using *reverse lexicographical* order. (Files in apps directory "B" have higher priority than directory "A".)

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Module Objectives

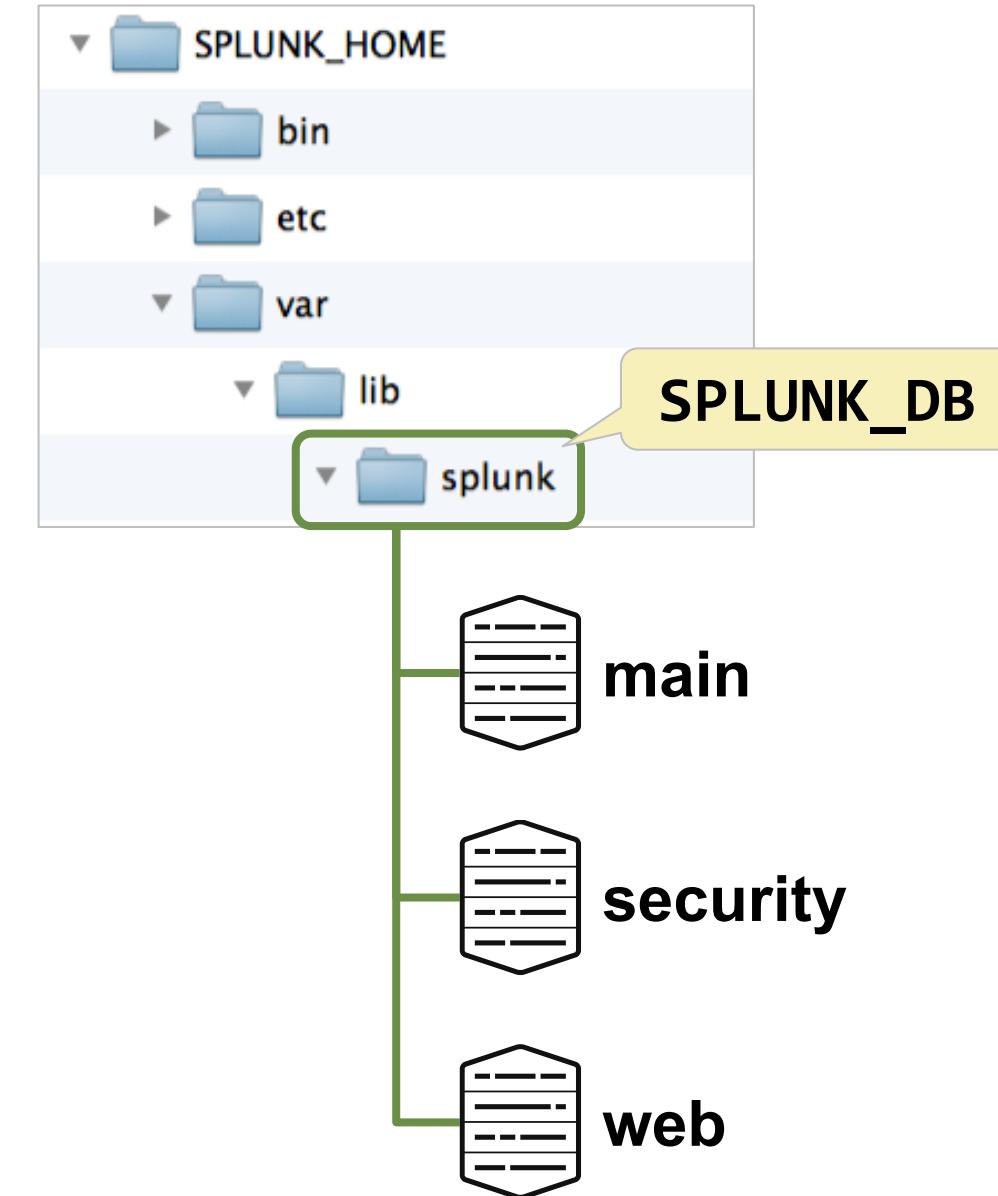
- Learn how Splunk indexes function
- Identify the types of index buckets
- Add and work with indexes
- Overview of metrics index

What are Indexes?



Splunk Indexes

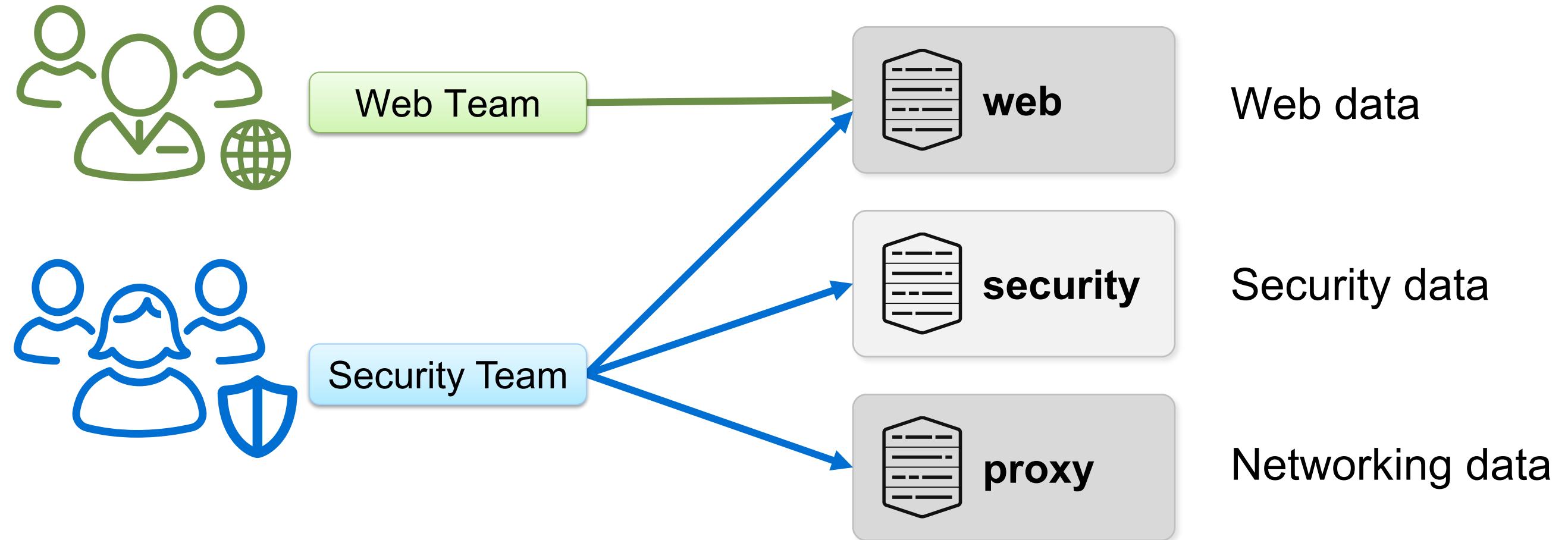
- Store input data as events
- Included with Splunk (**main**, **_internal**)
- Can be created by a Splunk administrator
- Can be used to limit scope of a search
- Allow the ability to limit access by user
- Found by default under **SPLUNK_DB**
(SPLUNK_HOME/var/lib/splunk)



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Indexes and Access Control

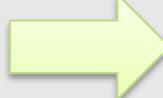
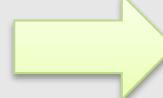
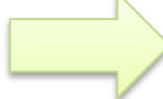
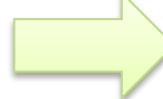
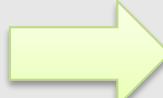
- Access control is set per index
- Segregate events into indexes to limit access by Splunk role



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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 

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Preconfigured Indexes (Partial List)

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

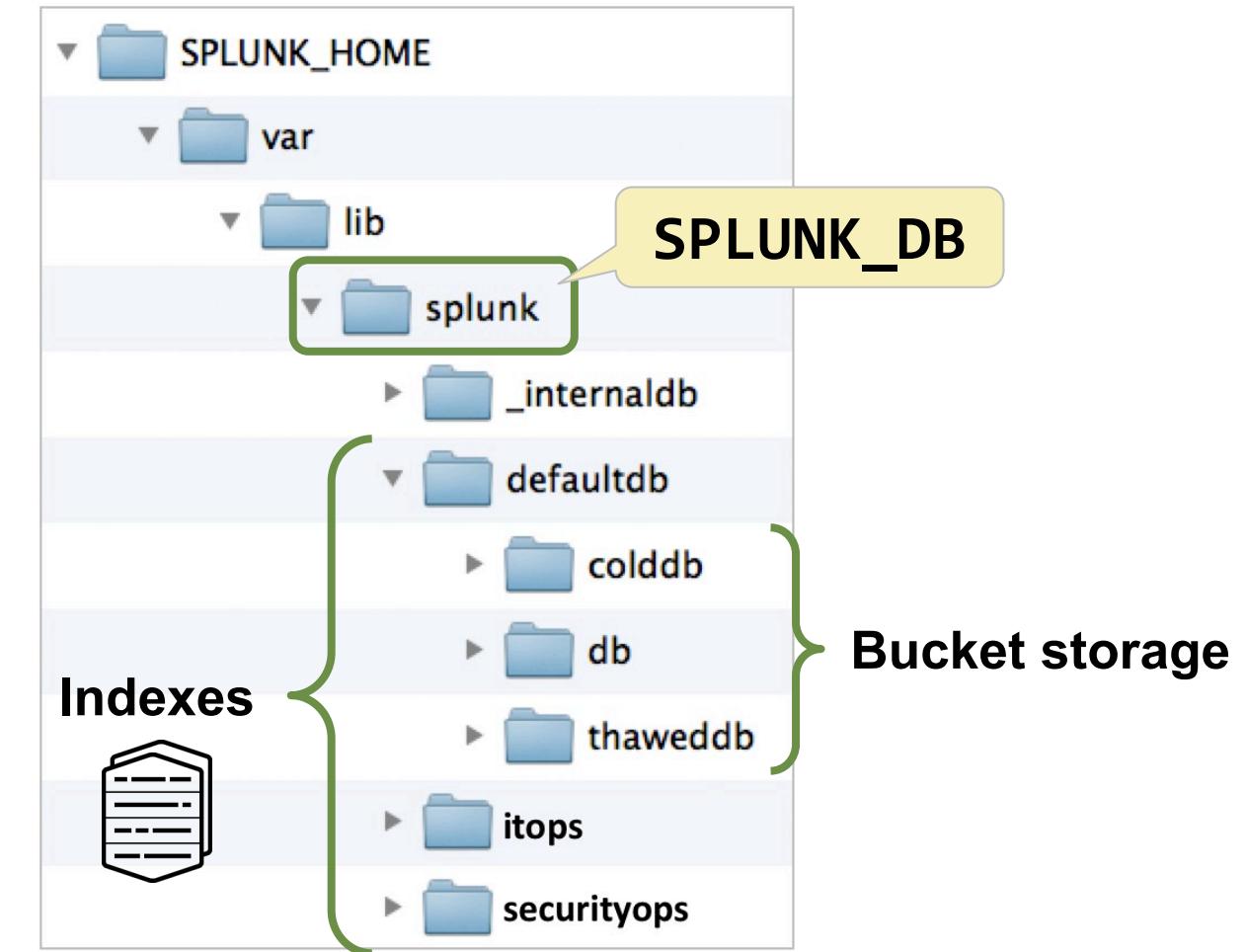
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

What are Buckets?



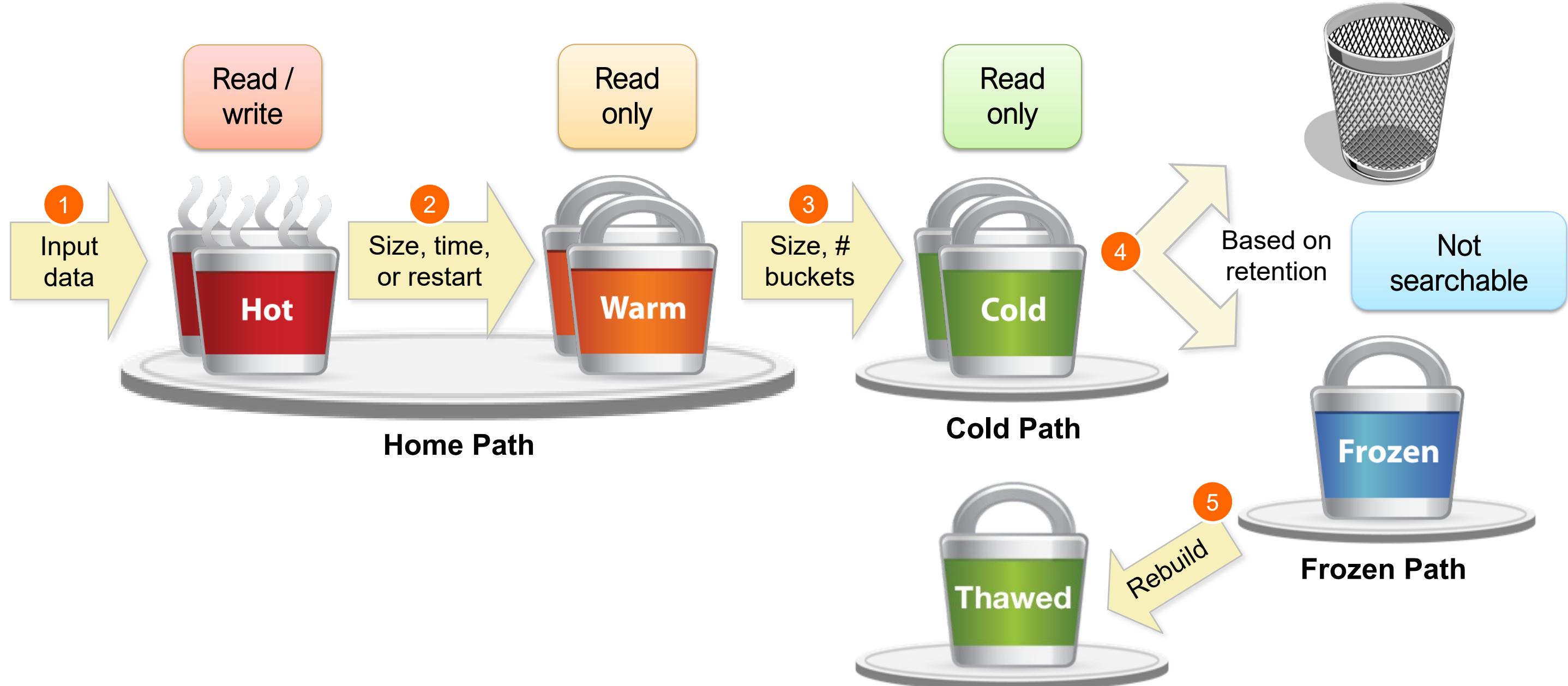
Buckets

- 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>



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

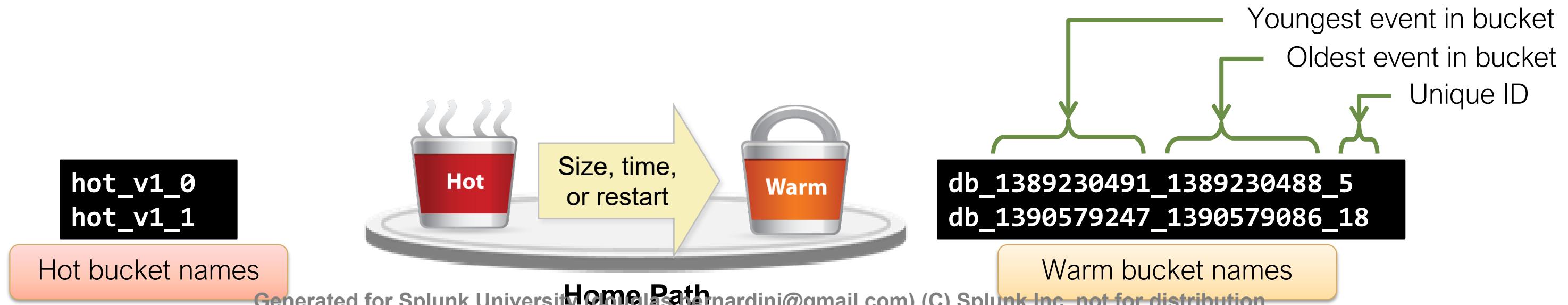
Data Flow Through an Index



Generated for Splunk University (douglas.bernardini@gmail.com) (c) Splunk Inc, not for distribution

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



Generated for Splunk University (douglasbernardini@gmail.com) (C) Splunk Inc, not for distribution

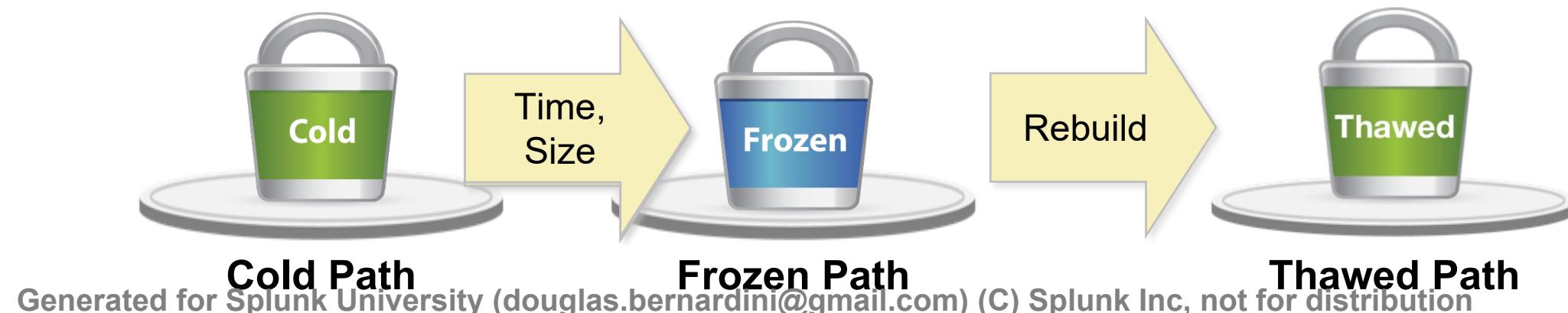
Warm and Cold Buckets

- 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



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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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:

Max Size of Entire Index GB ▾

Maximum target size of entire index.

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Adding an Index

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

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. [Learn more](#)

- 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

New Index ×

General Settings

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

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type Events Metrics Events is the default index data type

The type of data to store (event-based or metrics).

Home Path Locations of buckets:

Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path

Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path

Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check Enable Disable Optional data integrity check

Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Adding an Index With Splunk Web (cont.)

The screenshot shows the 'Storage Optimization' section of the Splunk Web configuration interface. It includes fields for 'Max Size of Entire Index' (500 GB), 'Max Size of Hot/Warm/Cold Bucket' (auto_high_volume GB), 'Frozen Path' (optional), and an 'App' dropdown set to 'Search & Reporting'. A 'Save' button is at the bottom right.

Overall index size (default = 500 GB)

Max Size of Entire Index
500 GB ▾
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket
auto_high_volume GB ▾
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path
optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App Search & Reporting ▾

Storage Optimization

Tsidx Retention Policy
Enable Reduction Disable Reduction
Warning: Do not enable reduction without understanding the full implications. It is extremely difficult to rebuild reduced buckets. [Learn More ↗](#)

Reduce tsidx files older than
Age is determined by the latest event in a bucket. Days ▾

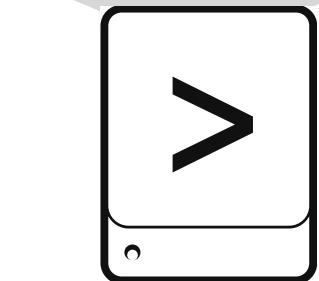
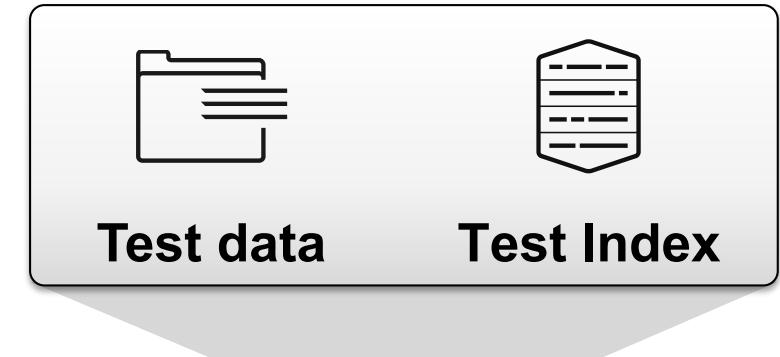
TSIDX Retention Policy (optional):

- Disabled by default; TSIDX files are not compressed
- When enabled, TSIDX files are compressed after this time

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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



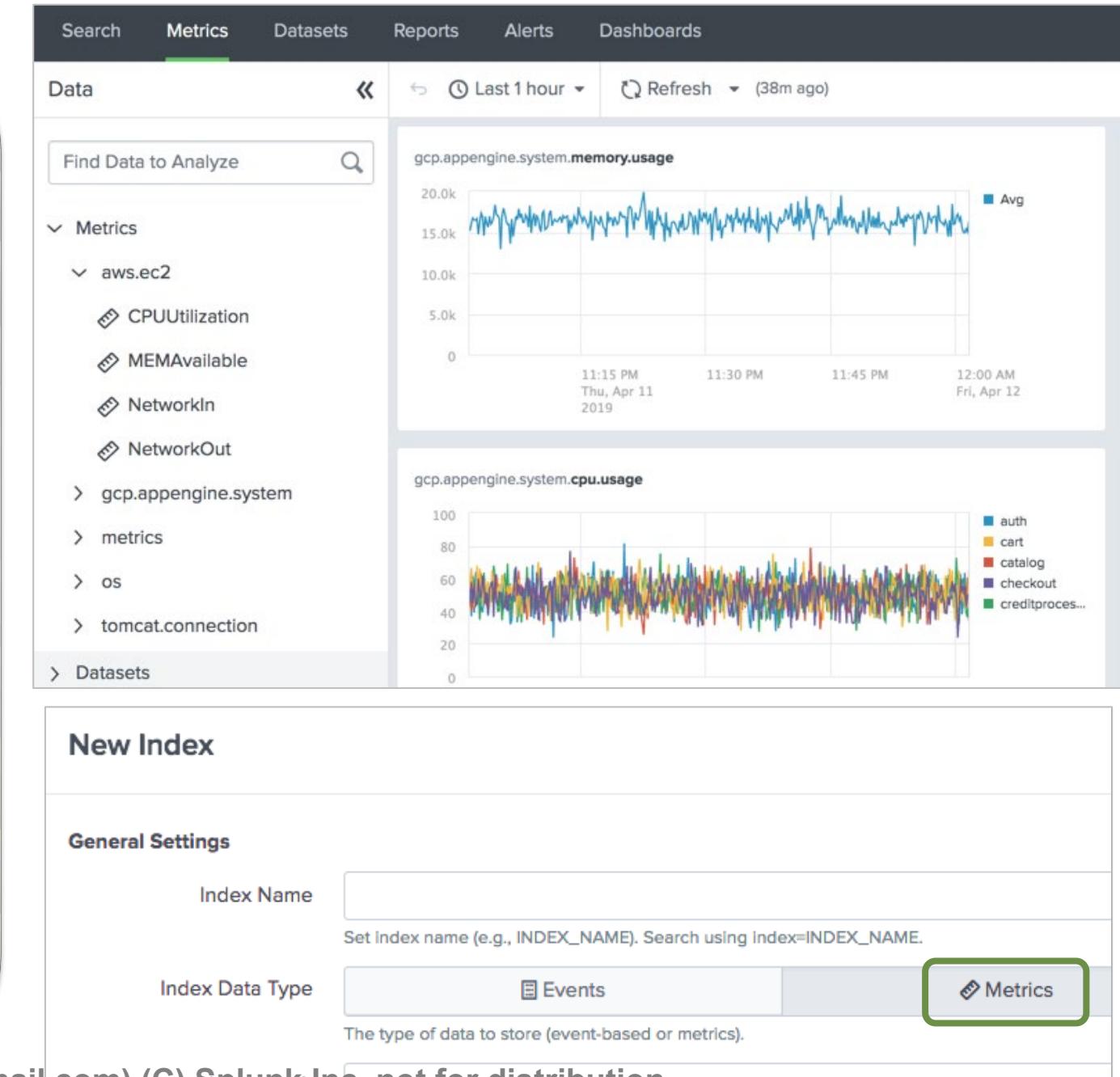
Test server

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



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Indexes

New Index

A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. [Learn more](#)

13 Indexes

filter

20 per page ▾

Name	Actions		Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status	
_audit	Edit	Delete	Disable	Events	system	4 MB	488.28 GB	39.5K	a day ago	a few seconds ago	\$SPLUNK_DB/audit/db	N/A	Enabled
_internal	Edit	Delete	Disable	Events	system	46 MB	488.28 GB	675K	a day ago	a few seconds ago	\$SPLUNK_DB/_internaldb/db	N/A	Enabled
_introspection	Edit	Delete	Disable	Events	system	84 MB	488.28 GB	107K	a day ago	a few seconds ago	\$SPLUNK_DB/_introspection/db	N/A	Enabled
_metrics	Edit	Delete	Disable	Metrics	system	42 MB	488.28 GB	638K	a day ago	a few seconds ago	\$SPLUNK_DB/_metrics/db	N/A	Enabled
_metrics_rollup	Edit	Delete	Disable	Metrics	custom	1 MB	488.28 GB	0			\$SPLUNK_DB/_metrics_rollup/db	N/A	Enabled
_telemetry	Edit	Delete	Disable	Events	system	488.28 GB	11	a day ago	18 minutes ago	\$SPLUNK_DB/_telemetry/db	N/A	Enabled	
_thefishbucket	Edit	Delete	Disable	Events	system	488.28 GB	0			\$SPLUNK_DB/fishbucket/db	N/A	Enabled	
history	Edit	Delete	Disable	Events	system	488.28 GB	0			\$SPLUNK_DB/historydb/db	N/A	Enabled	
main	Edit	Delete	Disable	Events	system	488.28 GB	100,000,000	5 years ago	2 minutes ago	\$SPLUNK_DB/defaultdb/db	N/A	Enabled	
securityops	Edit	Delete	Disable	Events	admin82	10 MB	50 GB	54K			\$SPLUNK_DB/securityops/db	N/A	Enabled
splunklogger	Edit	Delete	Enable	Events	admin82	488.28 GB	3 months ago			\$SPLUNK_DB/splunklogger/db	N/A	Disabled	
summary	Edit	Delete	Disable	Events	admin82	488.28 GB	3 months ago			\$SPLUNK_DB/summarydb/db	N/A	Enabled	
websales	Edit	Delete	Disable	Events	admin82	50 GB	54K	3 months ago	6 minutes ago	\$SPLUNK_DB/websales/db	N/A	Enabled	

Click index name or Edit to launch the **Edit Index** dialog box

Custom indexes can be enabled/disabled or deleted

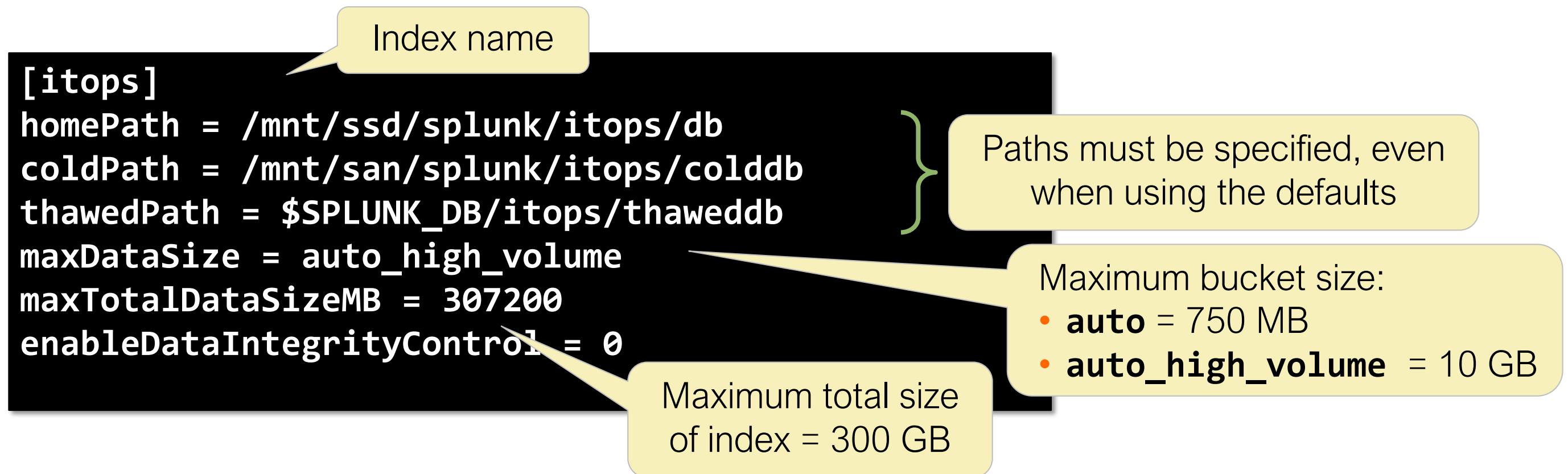
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Index Definitions and Data

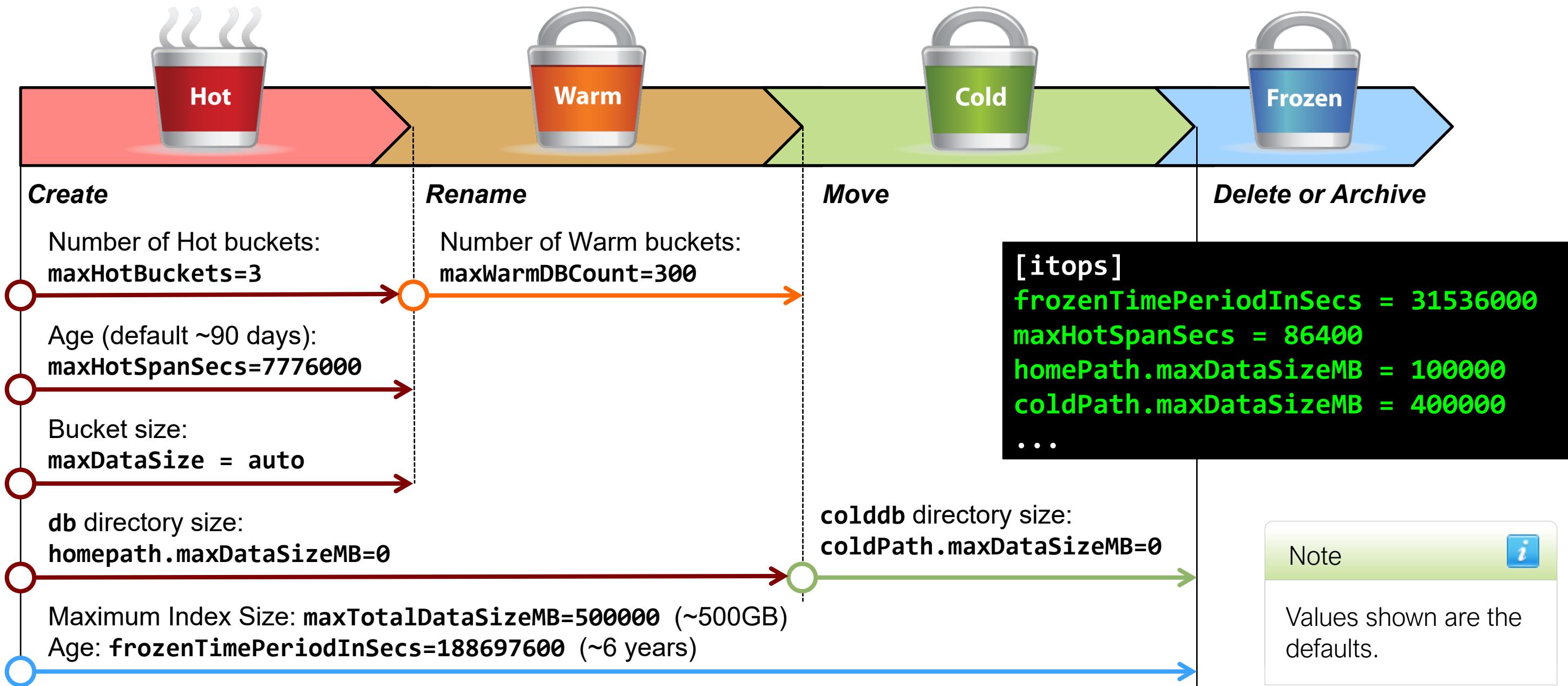
Index Definition (indexes.conf)	<code>SPLUNK_HOME/etc/system/default</code> <code>SPLUNK_HOME/etc/system/local</code> <code>SPLUNK_HOME/etc/apps/<app_name1>/local</code> <code>SPLUNK_HOME/etc/apps/<app_name2>/local</code> <code>SPLUNK_HOME/etc/apps/...</code>
Indexed Data (Buckets)	<code>SPLUNK_HOME/var/lib/splunk/<index_name>/db</code> <code>SPLUNK_HOME/var/lib/splunk/<index_name>/colddb</code> <code>SPLUNK_HOME/var/lib/splunk/<index_name>/thaweddb</code>

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

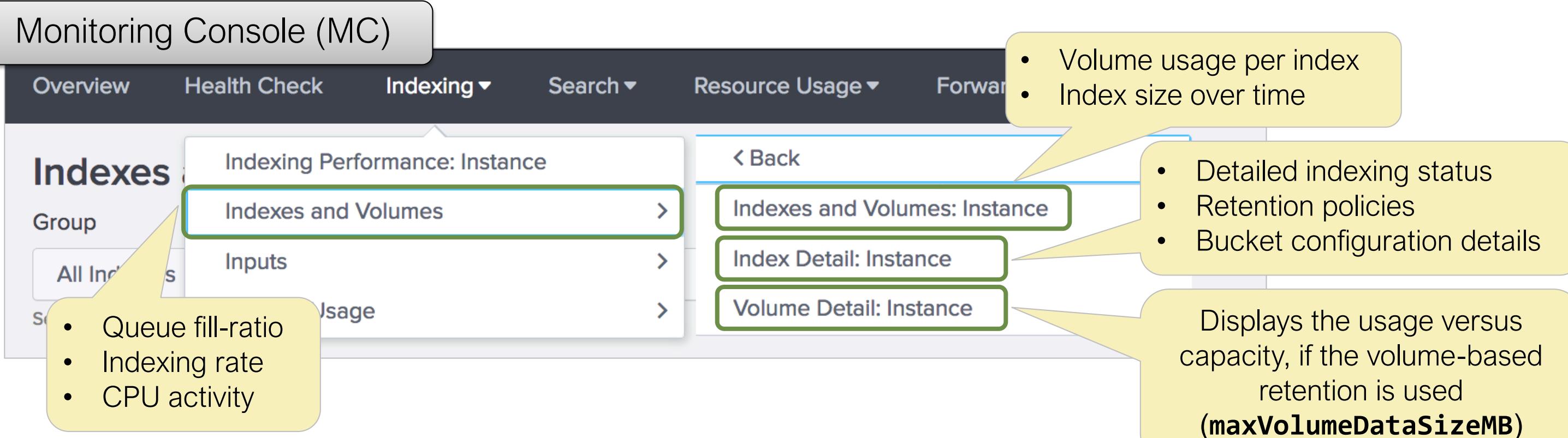


Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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 Console (MC)



Overview Health Check Indexing ▾ Search ▾ Resource Usage ▾ Forward

Indexes

Group
All Indices

Inputs

Usage

- Queue fill-ratio
- Indexing rate
- CPU activity

Indexing Performance: Instance

Indexes and Volumes >

Inputs

Usage

Volume Detail: Instance

Index Detail: Instance

Indexes and Volumes: Instance

< Back

- Volume usage per index
- Index size over time

- Detailed indexing status
- Retention policies
- Bucket configuration details

Displays the usage versus capacity, if the volume-based retention is used
(maxVolumeDataSizeMB)

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Monitoring Indexes with MC

Indexes and Volumes: Instance

Index Type Group Instance

Event Indexes Only All Indexers splunk02 Hide Filters

All Index Types * Search produced no results.

The "All Index Types" option is not compatible with indexers running Splunk Enterprise 6.6 or earlier, when selected.

Select views: All Snapshot Historical

Snapshots

0.22 GB Total Index Size

Indexes (9)

Index	Data Type	Data Age vs Frozen Age (days)	Index Usage (GB)
_audit	event	1 / 2184	0.00 / 488.28
_internal	event	1 / 30	0.04 / 488.28
_introspection	event	1 / 14	0.08 / 488.28
_telemetry	event	1 / 730	0.00 / 488.28
main	event	1806 / 2184	0.08 / 488.28
securityops	event	91 / 2184	0.01 / 500.00

Select an index to see more details

Volumes

Index Directory	Volume Name	Volume Freezing Due to Size	Volume Usage / Capacity
home	one	No	0.00 / 39.06
cold	two	No	0.00 / 78.13

A volume is considered to be freezing or about to freeze data at 95% or more of configured disk usage capacity.

Bucket Size (GB)

Bucket Event Count

Bucket Count

Event Count by Hosts (1)

Event Count by Sources (1)

Event Count by Sourcetype (1)

Paths

Retention policies

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

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

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



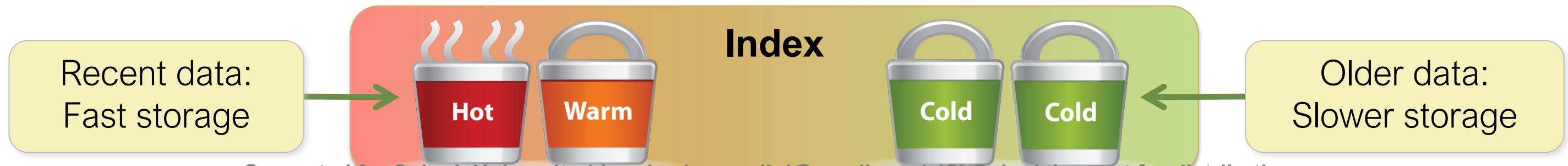
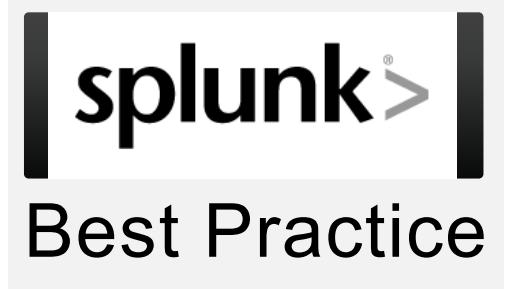
These options satisfy the strict data retention policy but may negatively impact performance.

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



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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
```

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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	<code>cp -rp <source> <target></code>
Windows	<code>xcopy <source> <target> /s /e /v /o /k</code> (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:



```
index=soc host=www1 source=access.log | delete
```

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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]

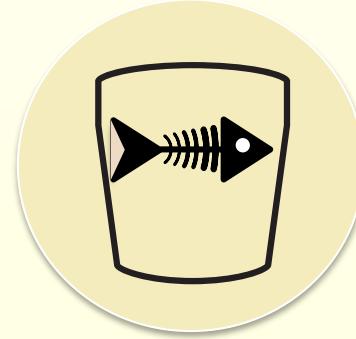
- **eventdata**: Delete indexed events and metadata on each event
- **userdata**: Delete user accounts
- **all**: Everything, including users, saved searches, and alerts

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!

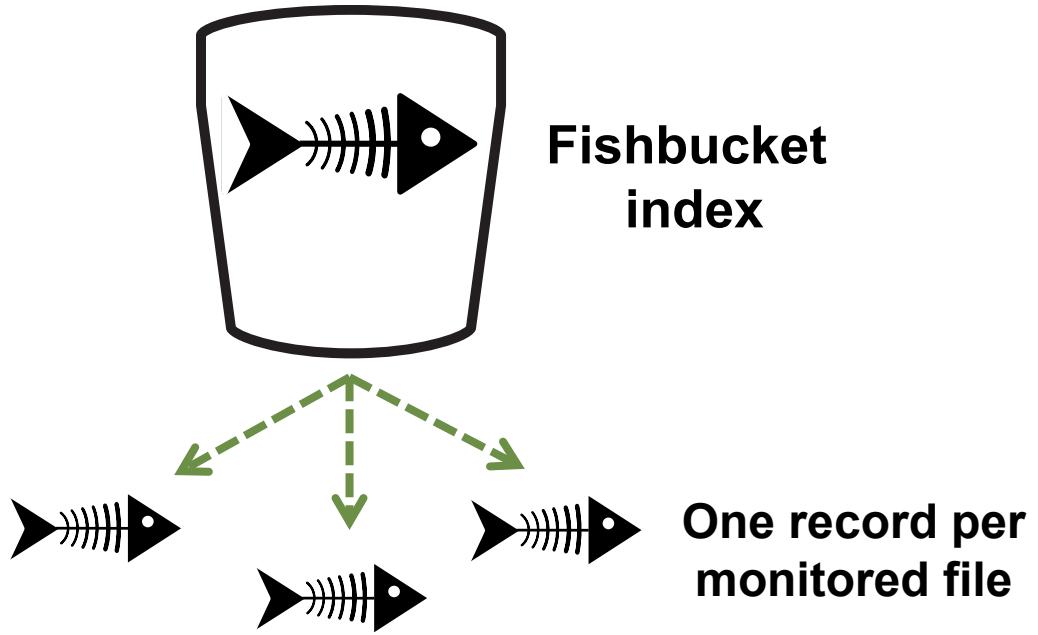
What is the Fishbucket?



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**

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution



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
```

Warning



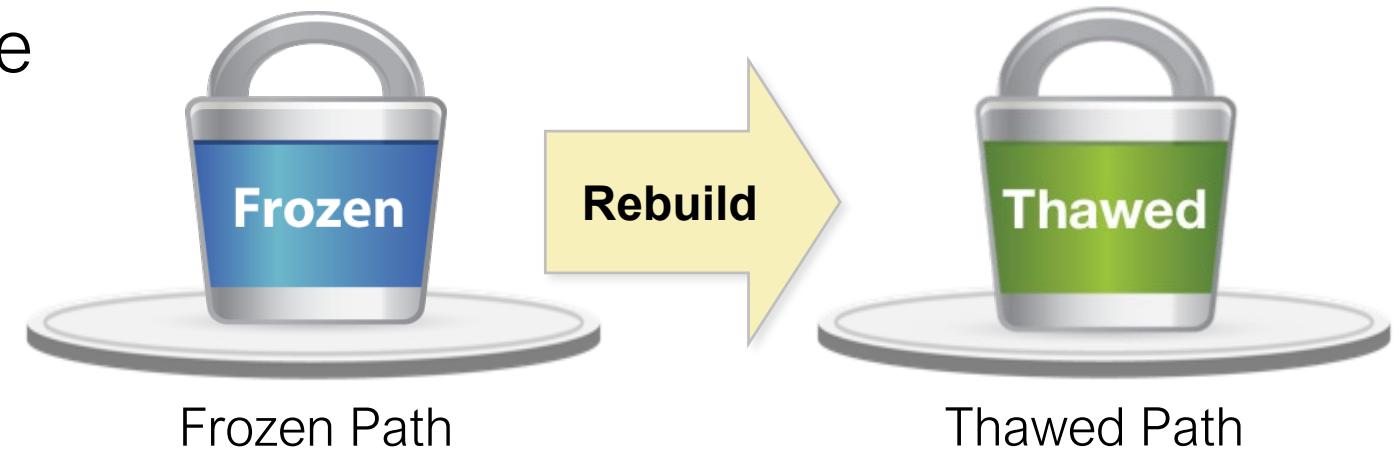
Resetting the fishbucket forces re-indexing of all file monitors affected. This results in more license usage.

3. Start Splunk

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

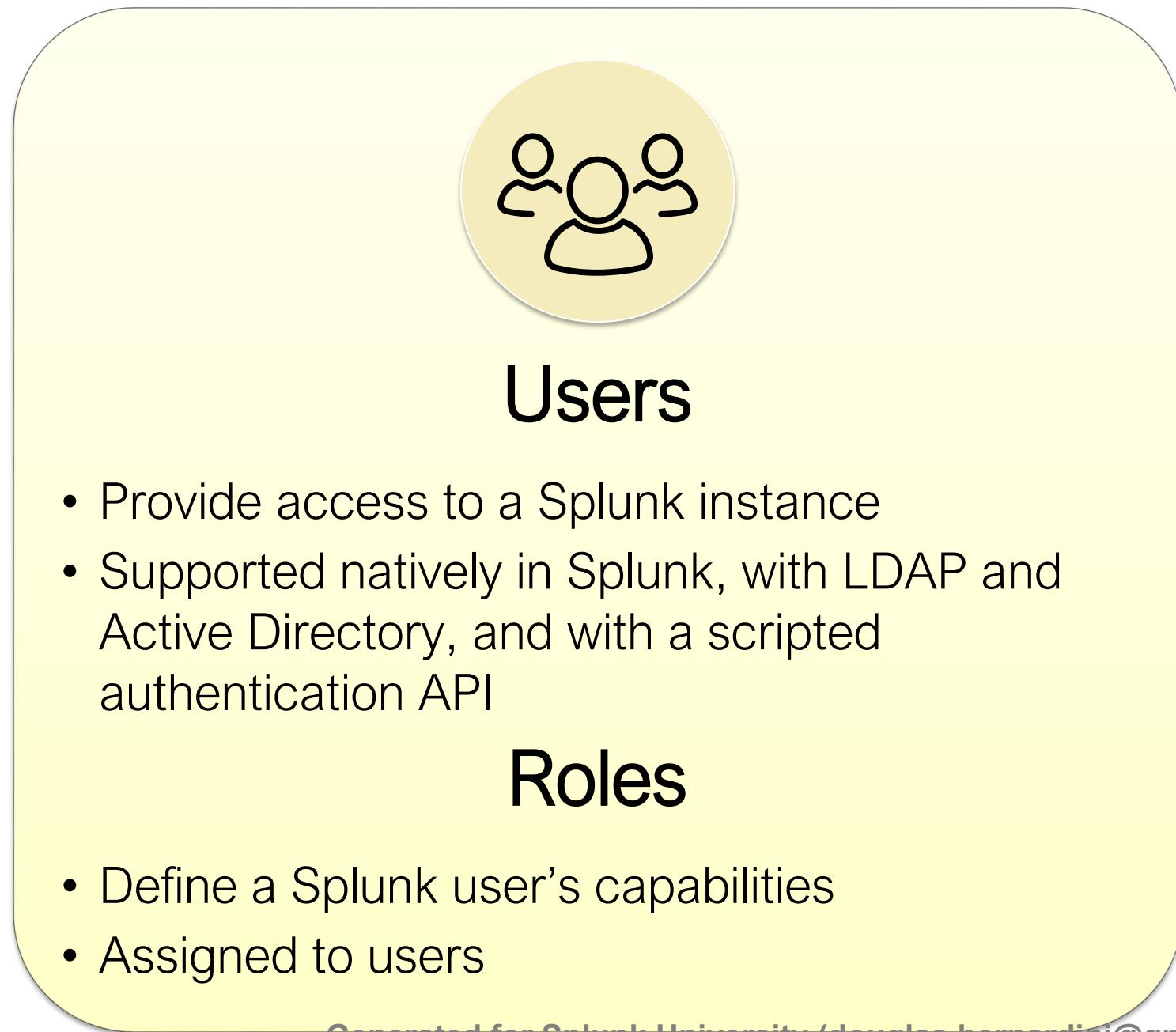
Module 7: Splunk User Management

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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



Web users



Web role

- Search the Web index

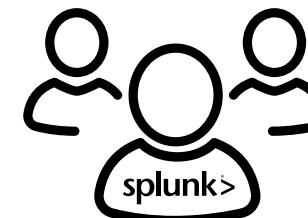
Security users



Security role

- Search the Web, Proxy and Security indexes

Splunk admins



Admin role

- Splunk administration
- Search all indexes

Managing Users and Roles

The screenshot shows the Splunk web interface with the following navigation bar:

- Administrator ▾
- Messages ▾
- Settings ▾** (highlighted with a green box)
- Activity ▾
- Help ▾
- Find

The main content area is divided into several sections:

- Add Data** (with a database icon):
 - Searches, reports, and alerts
 - Data models
 - Event types
 - Tags
 - Fields
 - Lookups
 - User interface
 - Alert actions
 - Advanced search
 - All configurations
- Explore Data** (with a magnifying glass icon):
 - Server settings
 - Server controls
 - Health report manager
 - RapidDiag
 - Instrumentation
 - Licensing
 - Workload management
- Monitoring Console** (with a monitoring icon):

The **Settings** menu (highlighted with a green box) contains the following sections:

- KNOWLEDGE**: Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; All configurations.
- DATA**: Data inputs; Forwarding and receiving; Indexes; Report acceleration summaries; Virtual indexes; Source types.
- DISTRIBUTED ENVIRONMENT**: Indexer clustering; Forwarder management; Data Fabric; Federated search; Distributed search.
- USERS AND AUTHENTICATION** (highlighted with a green rounded rectangle): Roles; Users; Tokens; Password Management; Authentication Methods.

A large yellow arrow points from the 'Users and Authentication' section in the Settings menu down to the same section in the main content area.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

User Authentication in Splunk

Native authentication

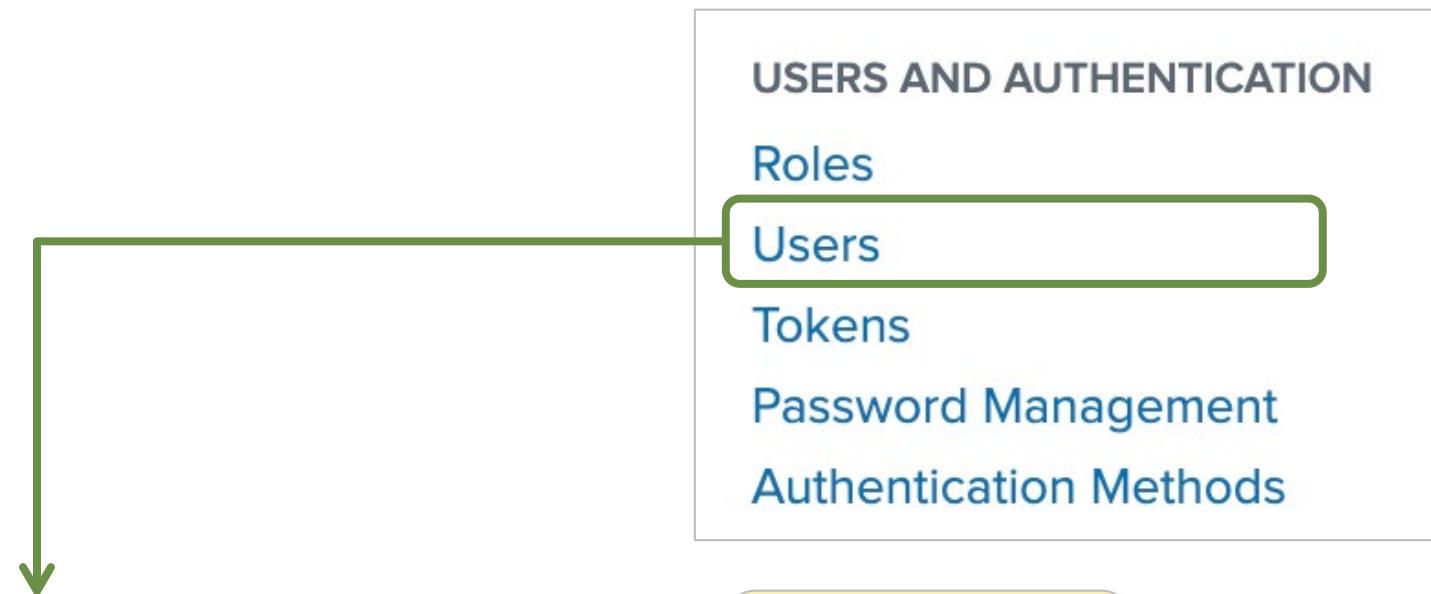
- Creating an account directly in Splunk (example: **admin** user)
- Stores passwords in **SPLUNK_HOME/etc/passwd**
- A blank **passwd** file disables native authentication
- Best Practice: Keep a failsafe account in the **passwd** file with a very strong password

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



Users										
13 Users		filter								
Name	Actions	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Last Login	Status
acurry		LDAP	Amanda		search	soc_analyst		soc_analyst	9/22/2020, 4:40:45 PM	✓ Active
admin	Edit ▾	Splunk	Administrator	02	launcher	system		admin	9/22/2020, 4:40:45 PM	✓ Active
blu	Edit	LDAP	Ron Lu		launcher	system		user		✓ Active
cory	Clone				launcher	system		admin		✓ Active
dha	View Capabilities	LDAP	Dwight Hale		launcher	system		user		✓ Active
ema	View Indexes				search	soc_analyst		soc_analyst	9/22/2020, 12:16:52 PM	✓ Active
gav	Search As	LDAP	Gabriel Veronoff	douglas.bernardini@gmail.com	launcher	system		admin		✓ Active

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Native Authentication: Adding Users

The screenshot shows the 'Create User' interface in Splunk. The 'Name' field is populated with 'acurry'. The 'Set password' and 'Confirm password' fields are also highlighted with a green border. A green arrow points from a 'New User' button to the 'Create User' window. Callout boxes explain the defaults for Time zone, Default app, and Assign roles.

Time zone: Defaults to search head time zone

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

Assign roles: Defaults to user role only

Fields and Options:

- Name: acurry
- Full name: Amanda Curry
- Email address: acurry@example.com
- Set password: (highlighted)
- Confirm password: (highlighted)
- Time zone: -- Default System Timezone --
- Default app: launcher (Home)
- Assign roles:
 - Available item(s): admin, can_delete, power, securegateway, splunk-system-role
 - Selected item: user
- Create a role for this user:
- Require password change on first login:

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Identifying Roles

Roles

6 Roles filter

Name	Actions	Native capabilities	Inherited capabilities	Default App
admin	Edit ▾	97	32	
can_delete	Edit ▾	4	0	
power	Edit ▾	9	23	
securegateway	Edit ▾	5	0	
splunk-system-role	Edit ▾	0	129	
user	Edit ▾	23	0	

New Role

USERS AND AUTHENTICATION

Roles

Users

Tokens

Password Management

Authentication Methods

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Creating User Roles: Inheritance

The screenshot shows the 'New Role' creation interface. The 'Name' field contains 'soc_analyst'. A yellow callout bubble says 'Create a name for the role'. The '1. Inheritance' tab is selected, highlighted with a green border. Below it, instructions say: 'Specify roles from which this role inherits capabilities and indexes. Inherited capabilities and indexes cannot be disabled. If multiple roles are specified, this role inherits capabilities and indexes from all selected roles.' A list of roles is shown with checkboxes: admin (unchecked), can_delete (unchecked), power (checked), securegateway (unchecked), splunk-system-role (unchecked), and user (unchecked). A green curly brace groups the 'power' checkbox and the inheritance instructions. A yellow callout bubble for 'Inheritance:' lists: '• Can be based on one or more existing roles' and '• Provides inherited capabilities and index access'. At the bottom are 'Cancel' and 'Create' buttons.

New Role

Name * soc_analyst

1. Inheritance 2. Capabilities 3. Indexes 4. Restrictions 5. Resources

Create a name for the role

Specify roles from which this role inherits capabilities and indexes. Inherited capabilities and indexes cannot be disabled. If multiple roles are specified, this role inherits capabilities and indexes from all selected roles.

Role name filter Showing all ▾

Role	Status
admin	<input type="checkbox"/>
can_delete	<input type="checkbox"/>
power	<input checked="" type="checkbox"/>
securegateway	<input type="checkbox"/>
splunk-system-role	<input type="checkbox"/>
user	<input type="checkbox"/>

Inheritance:

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

Cancel Create

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Creating User Roles: Capabilities

New Role

Name *

1. Inheritance 2. Capabilities 3. Indexes 4. Restrictions 5. Resources

Select specific capabilities for this role.

Capability Name	filter	Show
<input type="checkbox"/> accelerate_datamodel		inherited
<input checked="" type="checkbox"/> accelerate_search		inherited
<input type="checkbox"/> admin_all_objects		inherited
<input type="checkbox"/> apps_backup		inherited
<input type="checkbox"/> apps_restore		inherited
<input type="checkbox"/> change_authentication		inherited
<input checked="" type="checkbox"/> change_own_password		inherited
...		

Showing all ▾

- Show selected
- Show unselected
- Show native
- Show inherited
- Show all

Cancel Create

Source drop-down menu filters the displayed role capabilities

Capabilities inherited from other roles are pre-checked

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Creating User Roles: Indexes

New Role

Name *

1. Inheritance 2. Capabilities 3. Indexes 4. Restrictions 5. Resources

Wildcards
Instead of selecting individual indexes, you can create a Wildcard Index to dynamically capture all indexes that match the Wildcard. After you add a Wildcard Index, it appears in the Indexes table. Wildcard Indexes are limited to this role.

Enter a value that contains *** Add

Indexes
Enable both the "Included" and "Default" checkboxes for an index to make that index searchable by default for this role. You must save this role before you can see its inherited wildcards.

Index Name	Included	Default	Action
* (All non-internal indexes)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Show selected
_ (All internal)	<input type="checkbox"/>	<input type="checkbox"/>	Show unselected
_audit	<input type="checkbox"/>	<input type="checkbox"/>	Show native
_internal	<input type="checkbox"/>	<input type="checkbox"/>	Show inherited
introspection	<input type="checkbox"/>	<input type="checkbox"/>	Show wildcards

Note i

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Creating User Roles: Restrictions

New Role

Name * soc_analyst

1. Inheritance 2. Capabilities 3. Indexes 4. Restrictions **5. Resources**

Restrict searches

Create a search filter to set search restrictions for this role. You can enter a valid search filter or use the search filter generator to add queries.

Search filter generator

Indexed field and values time range
60 seconds

Increasing the time range beyond the default of 60 seconds can increase the time it takes to populate the "Indexed Fields" and "Values" text boxes.

Indexed fields

Select or type an indexed field

Search filter

(index::websales) AND (sourcetype::access_combined_wcookie)

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

Values Select one or more values
You can type in custom values that do not appear in the list, including wildcards. Example: "syslog_"

Concatenation option OR

Generated search filter OR

Add to search filter Reset Preview search filter results

Note: the search filter can only include:

- source type
- source
- host
- index
- event type
- search fields
- the operators "", "OR", "AND", "NOT"

Cancel Create

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Creating User Roles: Resources

New Role

Name *

1. Inheritance 2. Capabilities 3. Indexes 4. Restrictions **5. Resources**

This role

Default app Default app

Role search job limit

Set a limit for how many search jobs that all users with this role can run at the same time. [?](#)

Standard search limit

Real-time search limit

User search job limit

Set a limit for how many search jobs that a single user with this role can run at the same time. [?](#)

Standard search limit

Real-time search limit

Role search time window limit

Select a maximum time window for searches for this role. Inherited roles can override this setting.

Unset

Select the earliest searchable event time for this role. Inherited roles can override this setting.

Unset

Disk space limit

Set the maximum amount of disk space, in megabytes, that search jobs for a specific user with this role can use.

Standard search limit MB

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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)



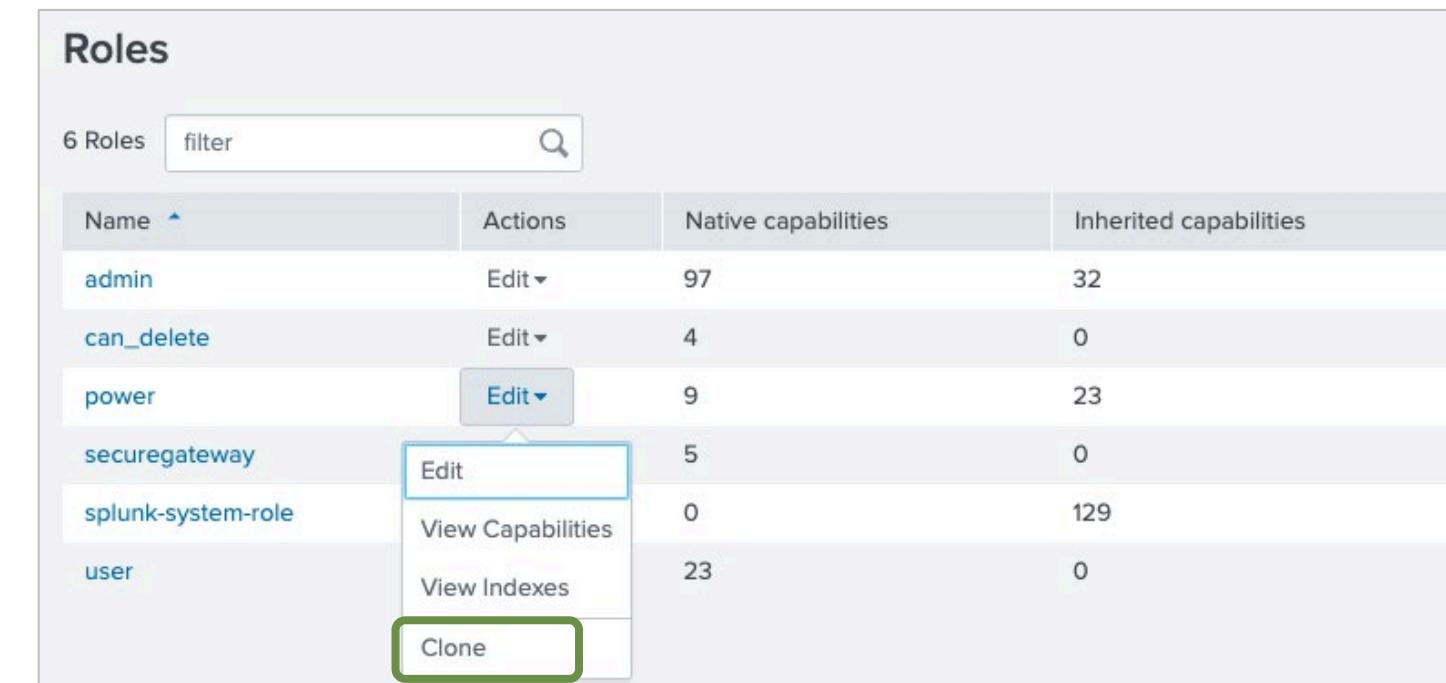
Role name

```
[role_webusers]
srchIndexesAllowed = main;websales
srchIndexesDefault = websales
srchMaxTime = 8640000
```

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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



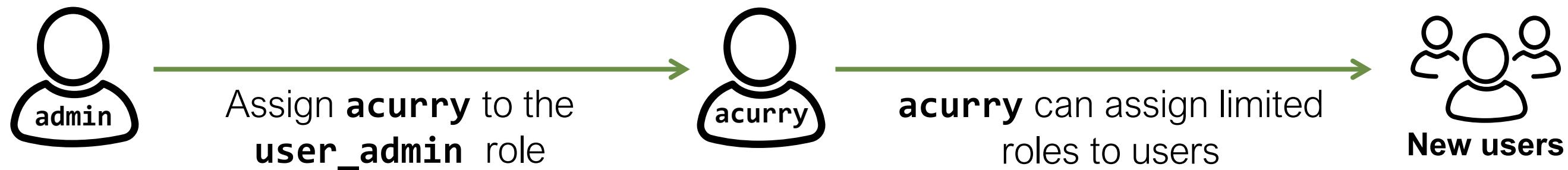
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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**)

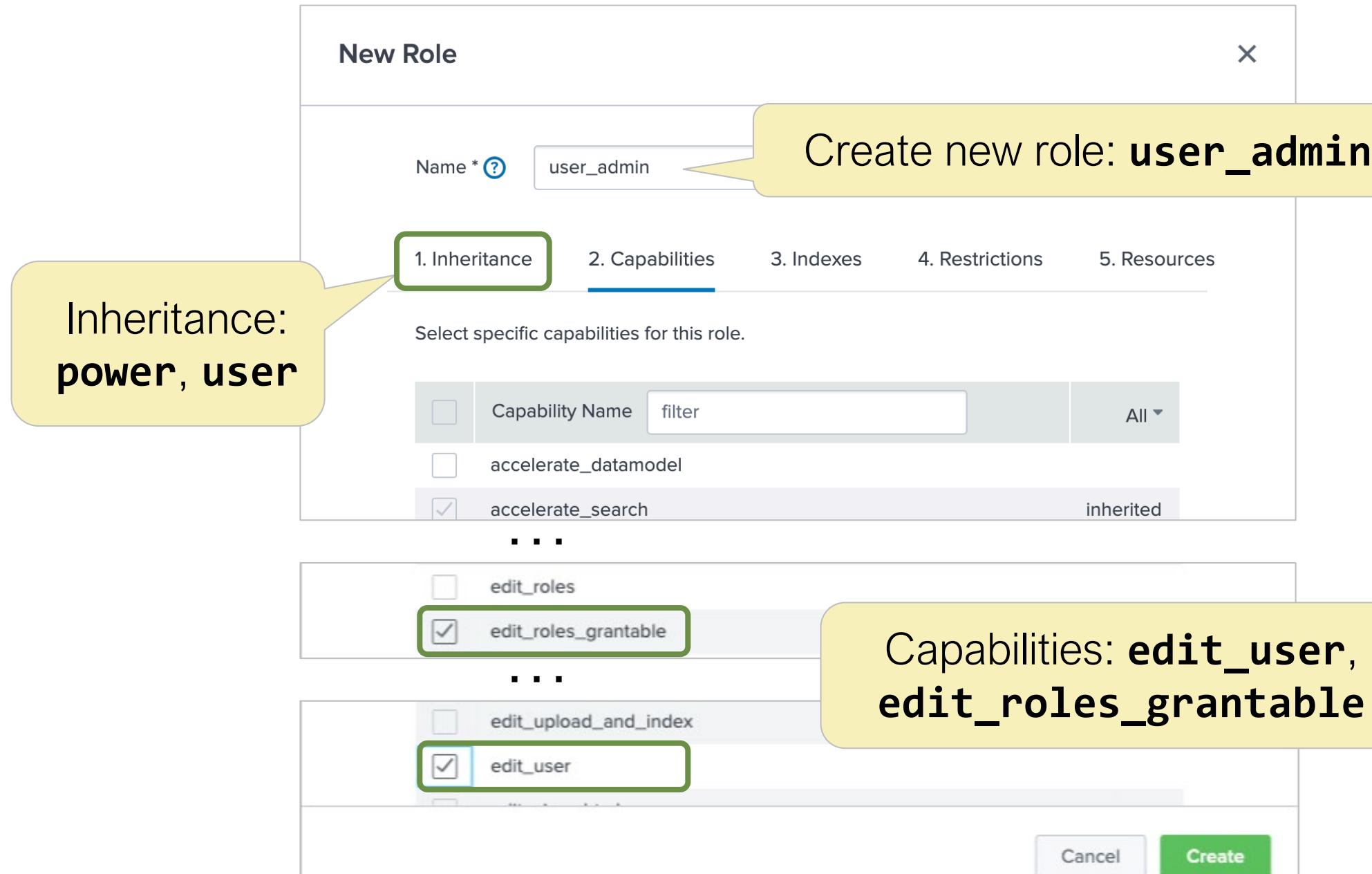


Issues to consider:

- 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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Assigning `edit_roles_grantable` Capability



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Password Policy Management

Password Policy Management

These Password Policy Management settings apply only to Internal Splunk Authentication, not to SAML or LDAP.

Password Rules

Minimum characters	1	Must be a number between 1 and 256. For better security, we recommend a number between 8 and 256.
Numerical	0	Minimum number of digits required.
Lowercase	0	Minimum number of lowercase letters required.
Uppercase	0	Minimum number of uppercase letters required.
Special character	0	Minimum number of printable ASCII characters.

Expiration

Days until password expires	90	Number of days until a password expires.
-----------------------------	----	--

USERS AND AUTHENTICATION

Roles

Users

Tokens

Password Management

Authentication Methods



- 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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Unlocking Users

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

Lockout

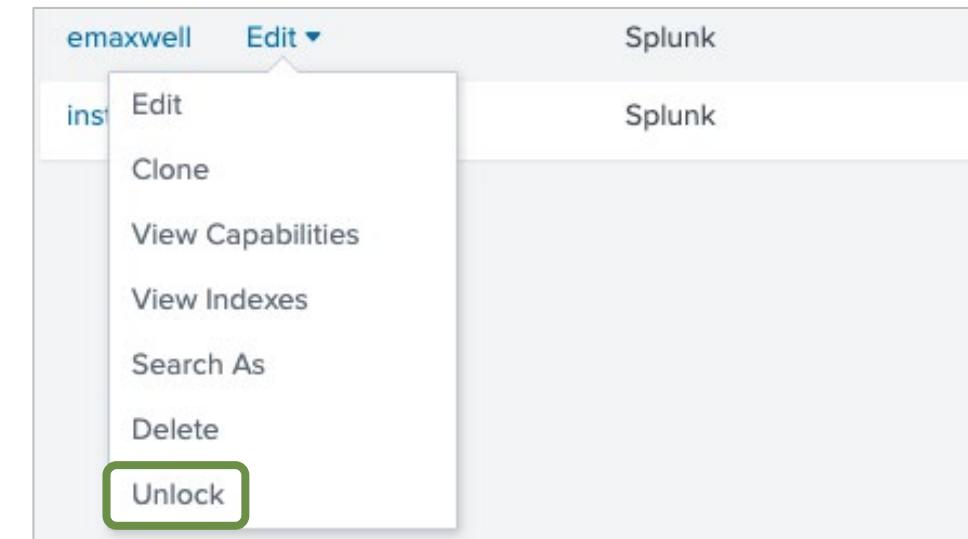
Failed login attempts
5
Number of unsuccessful login attempts that can occur before a user is locked out.

Lockout threshold in minutes
5
Number of minutes that must pass from the time of the first failed login until the failed login attempt counter resets.

Lockout duration in minutes
30
Number of minutes a user must wait before attempting login.

Enable Disable

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



- Using CLI:

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Authentication Methods

Select an authentication method. Splunk supports native authentication as well as the following external methods:

Internal Splunk Authentication (always on)

- External None
 LDAP
 SAML

Multifactor Authentication

Not available with external authentication such as SAML.

- None
 Duo Security
 RSA Security

[Reload authentication configuration](#)

USERS AND AUTHENTICATION

Roles

Users

Tokens

Password Management

Authentication Methods



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.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

splunkAdmins

Access controls > Authentication method > LDAP strategies > LDAP Groups > splunkAdmins

Available Roles	Selected Roles
<input type="checkbox"/> admin	<input checked="" type="checkbox"/> admin
<input type="checkbox"/> can_delete	
<input type="checkbox"/> power	
<input type="checkbox"/> splunk-system-role	
<input type="checkbox"/> user	

Click one or more role names to map them to this group

LDAP Users

CN=Gabriel Voronoff,OU=splunk,DC=buttercupgames,DC=local
CN=Kathleen Percy,OU=splunk,DC=buttercupgames,DC=local

add all >

< clear all

LDAP Groups

Access controls > Authentication method > LDAP strategies > LDAP Groups

Showing 1-4 of 4 items

LDAP Group Name	LDAP Strategy	Group type	Roles
splunkAdmins	AD_splunkers	static	admin
splunkBizDev	AD_splunkers	static	user
splunkITOps	AD_splunkers	static	power
splunkSOC	AD_splunkers	static	securityops

Mapped roles for LDAP groups

filter

25 per page

Back to strategies

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Module Objectives

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

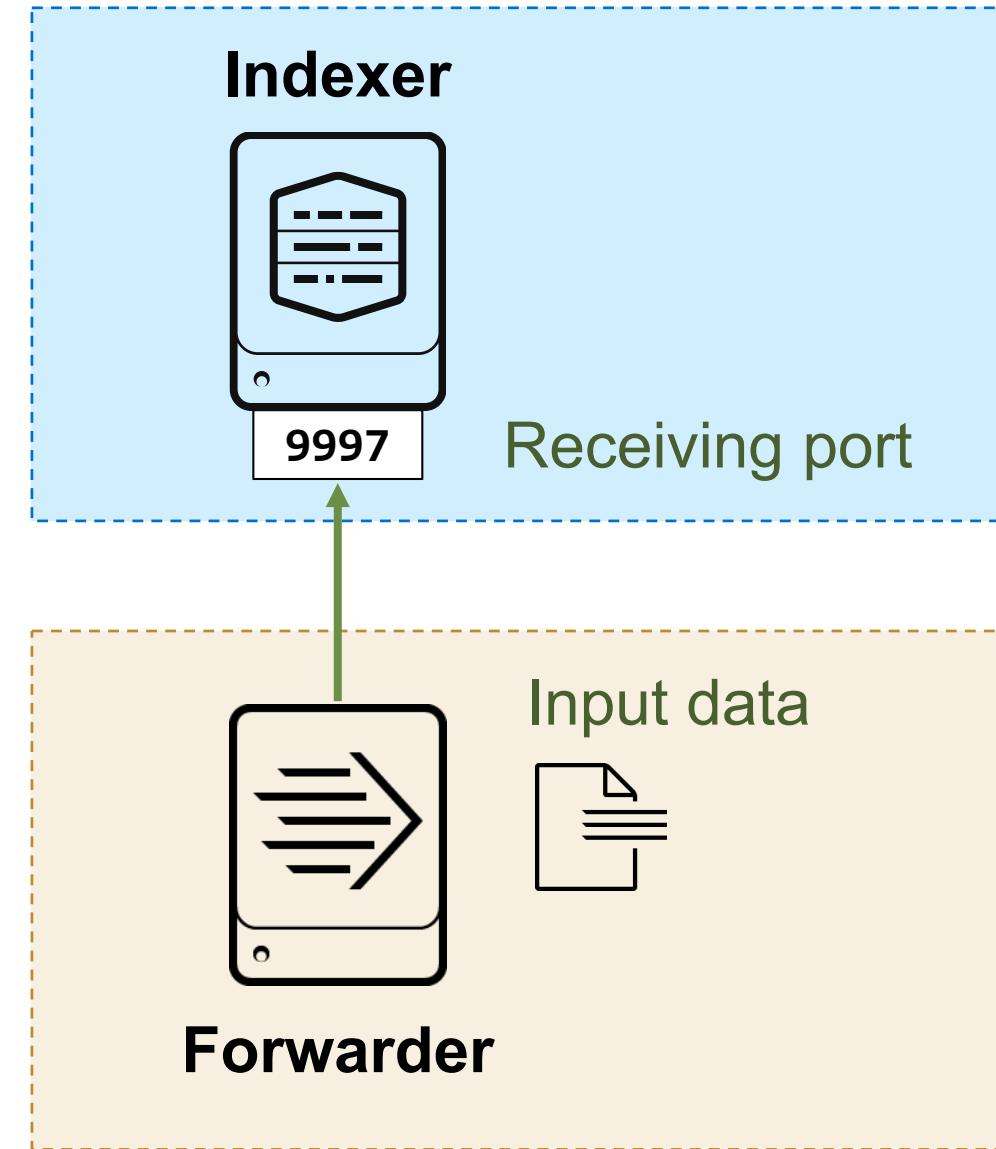
Forwarders and Indexers

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



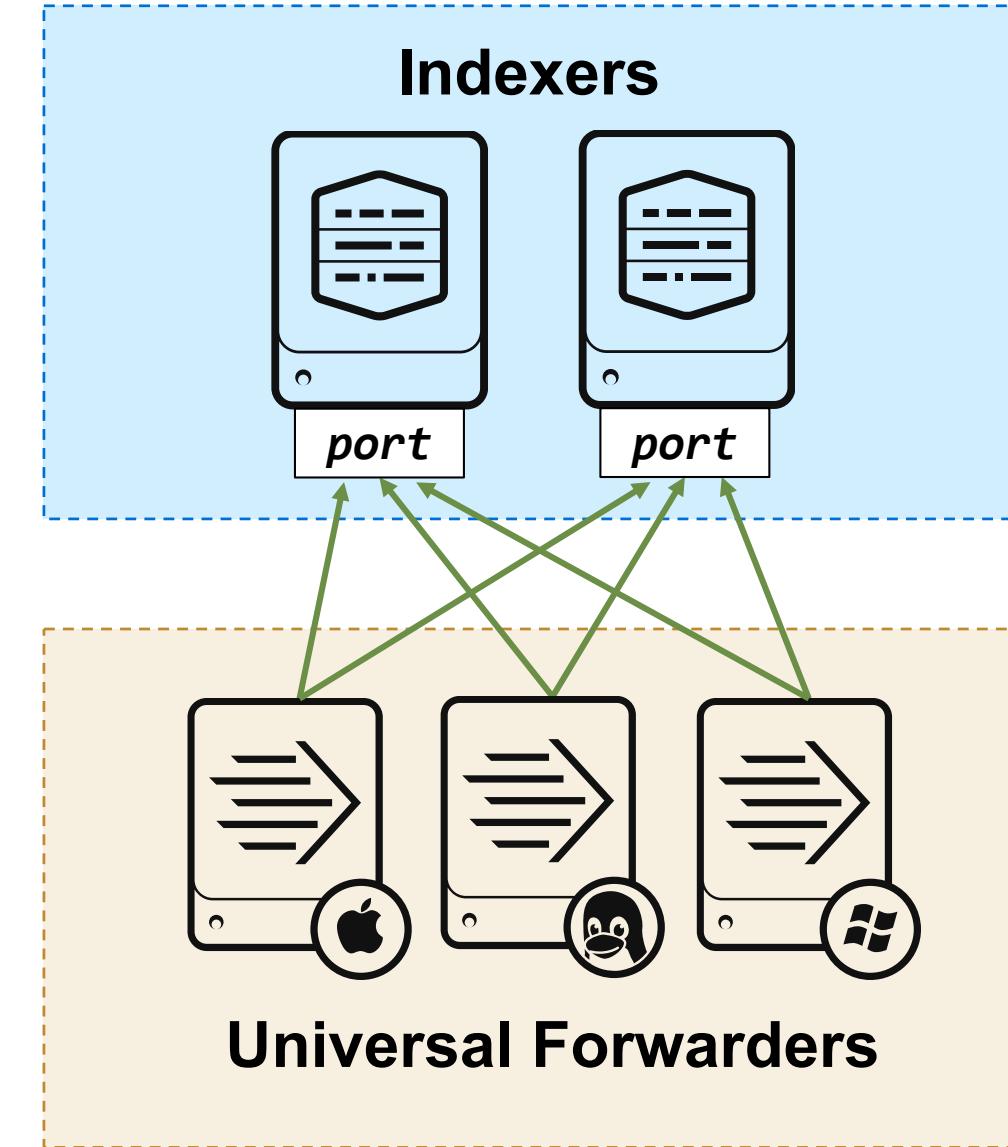
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Understanding Universal Forwarders



Universal Forwarders (UF)

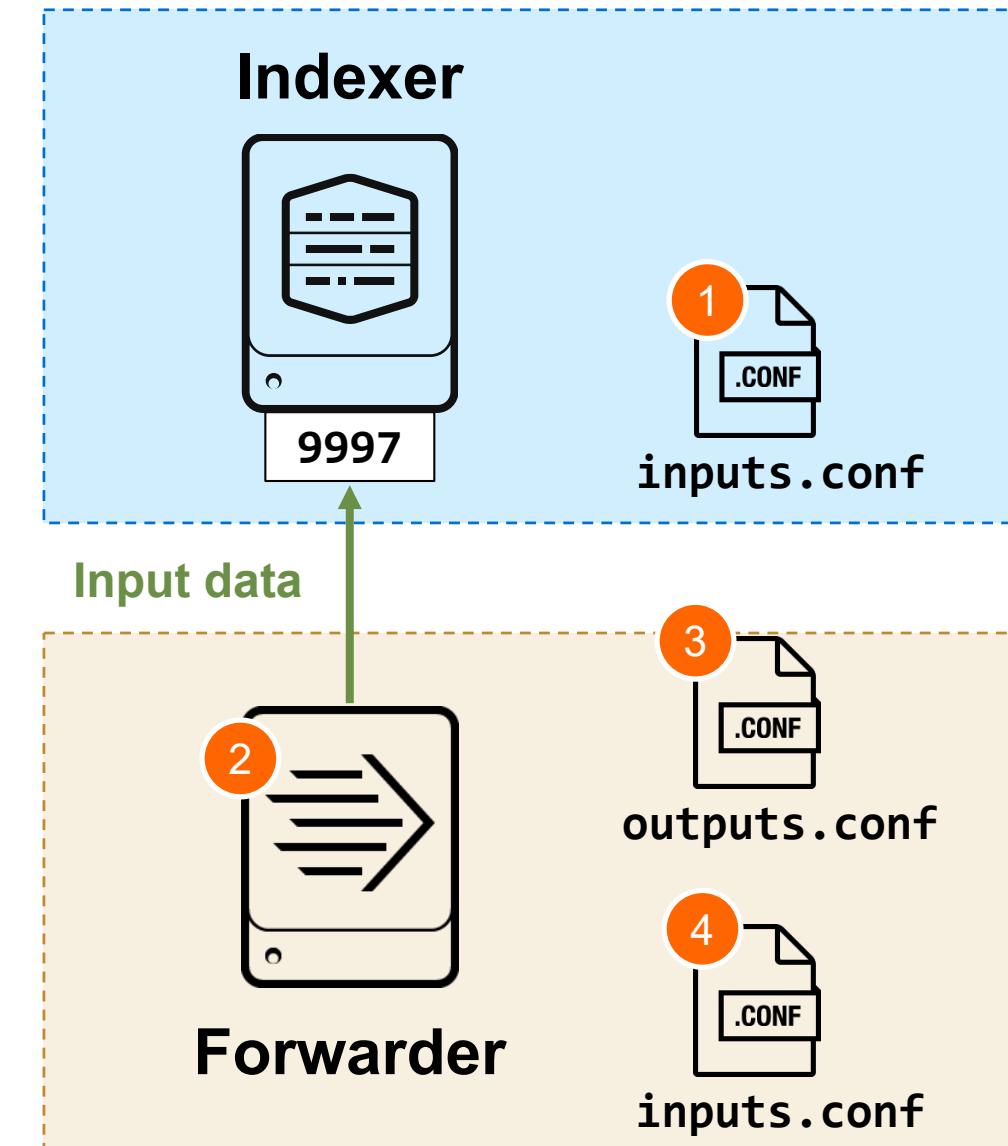
- Gathers data from a host
- Sends data over the network to receiving ports on receivers (usually an indexer)
- Provided as separate installation binary with a built-in license (no limits)
- Designed to run on production servers
(minimal CPU / memory use, bandwidth constrained to 256 KBps by default, no web interface, cannot search or index)



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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]

The screenshot shows the 'Forwarding and receiving' configuration page in Splunk Web. It has two main sections: 'Forward data' and 'Receive data'. In the 'Forward data' section, there is a 'Forwarding defaults' link and a 'Configure forwarding' link. In the 'Receive data' section, there is a 'Configure receiving' link and a '+ Add new' button. A green arrow points from the 'Listen on this port' input field in the 'Configure receiving' section to the '+ Add new' button in the 'Receive data' section.

Installing a Universal Forwarder

	*NIX	Windows
Download	www.splunk.com/en_us/download/universal-forwarder.html	
Install	<ul style="list-style-type: none">• Un-compress .tgz, .rpm, or .deb file in the path Splunk will run from• Default SPLUNK_HOME is: /opt/splunkforwarder	<ul style="list-style-type: none">• Execute .msi installer (or use the CLI)• Default SPLUNK_HOME is: C:\Program Files\SplunkUniversalForwarder

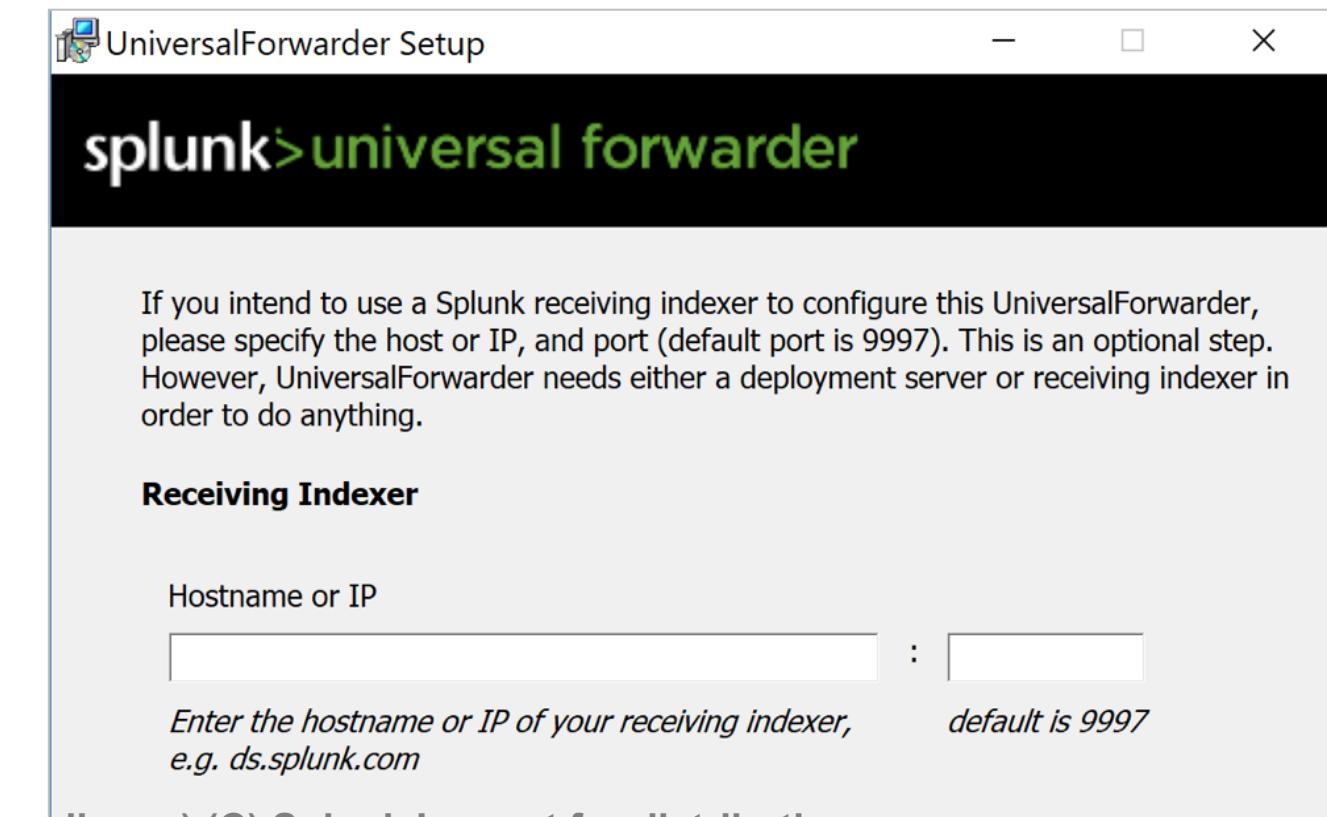
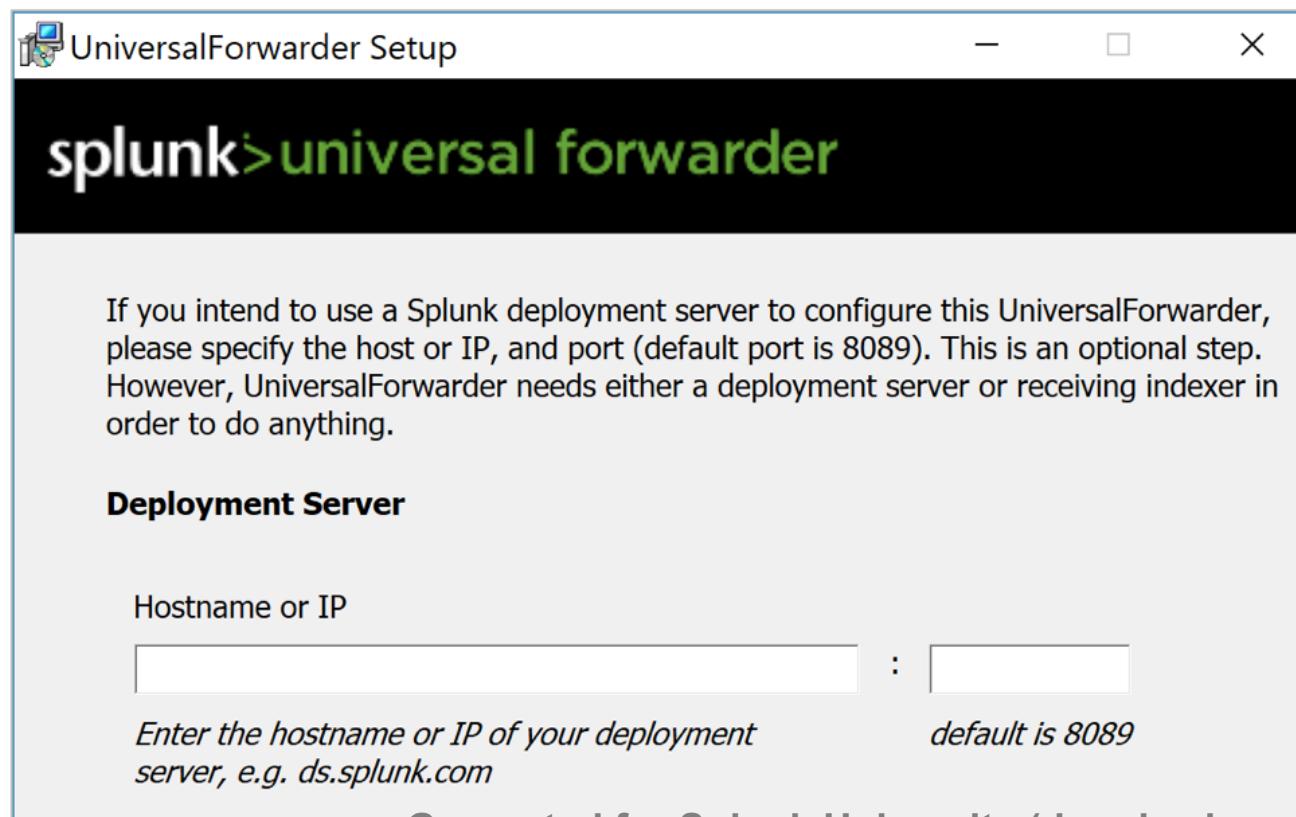
- Silent installation methods exist on all platforms
- Same **splunk** command-line interface in **SPLUNK_HOME/bin**
 - Same commands for start/stop, restart, etc.
 - An admin account and password are required

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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:

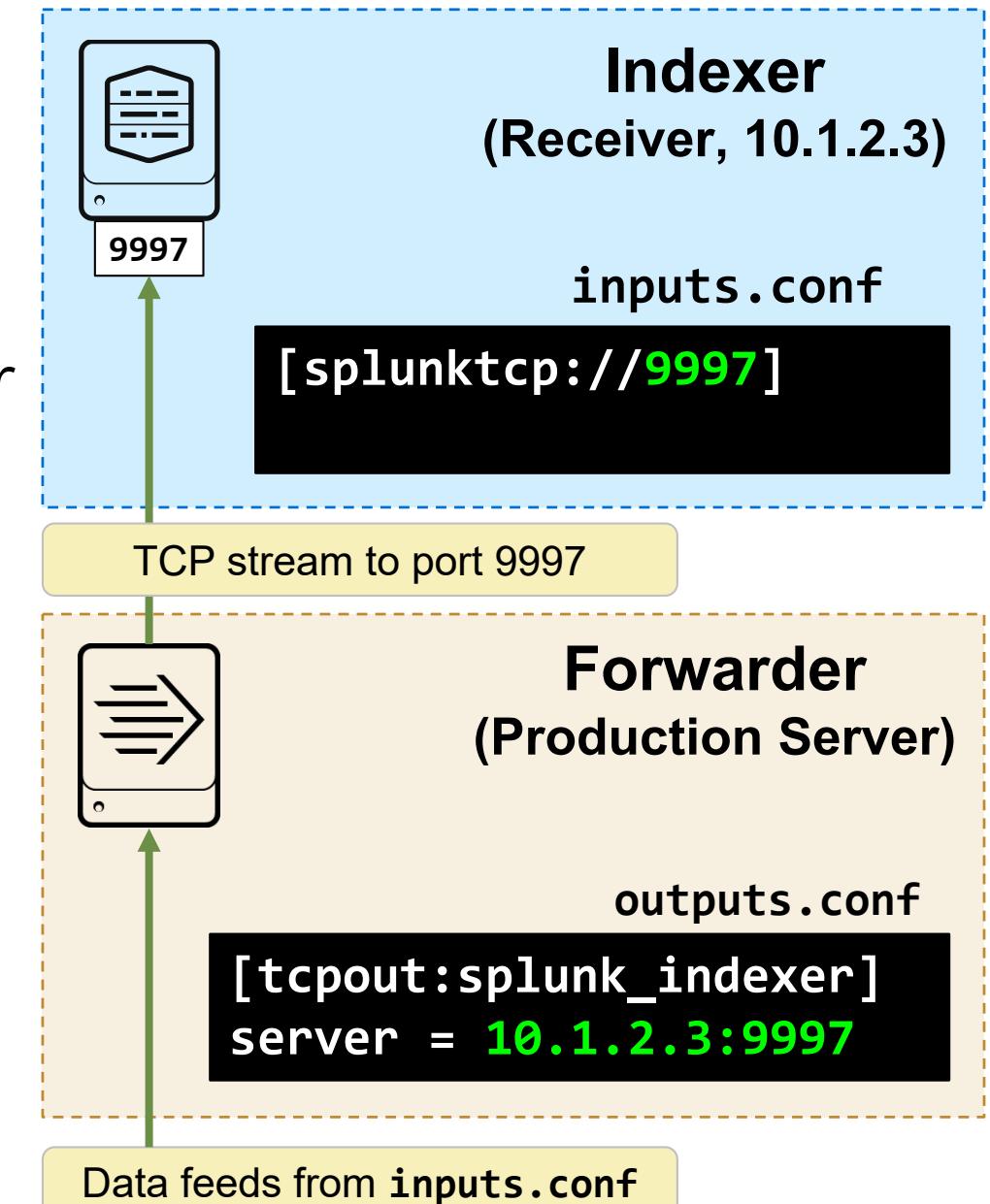
```
[tcpout]
defaultGroup = default-autolb-group

[tcpout-server://10.1.2.3:9997]

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

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

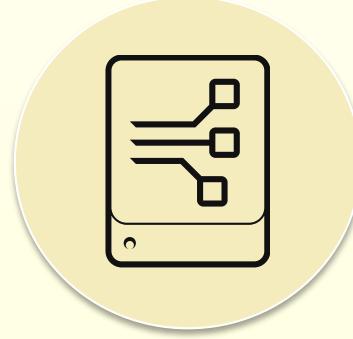


Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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



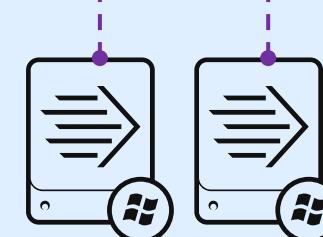
Deployment Server (DS)

- 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

Infrastructure servers



Windows UF servers



Linux UF servers

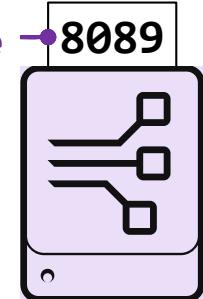


Note

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

Management Port

Manage



Deployment Server

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

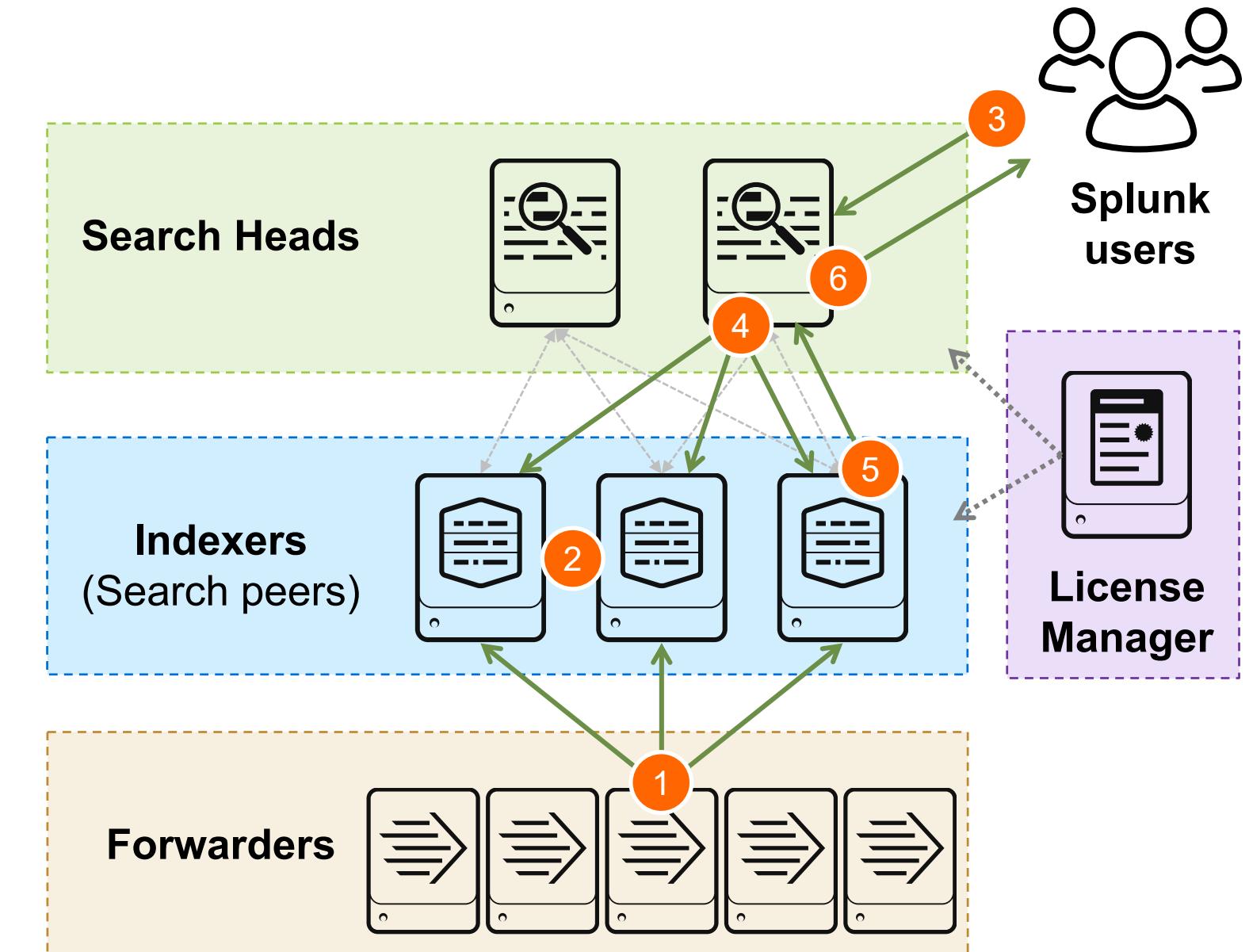
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Module Objectives

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

How Distributed Search Works

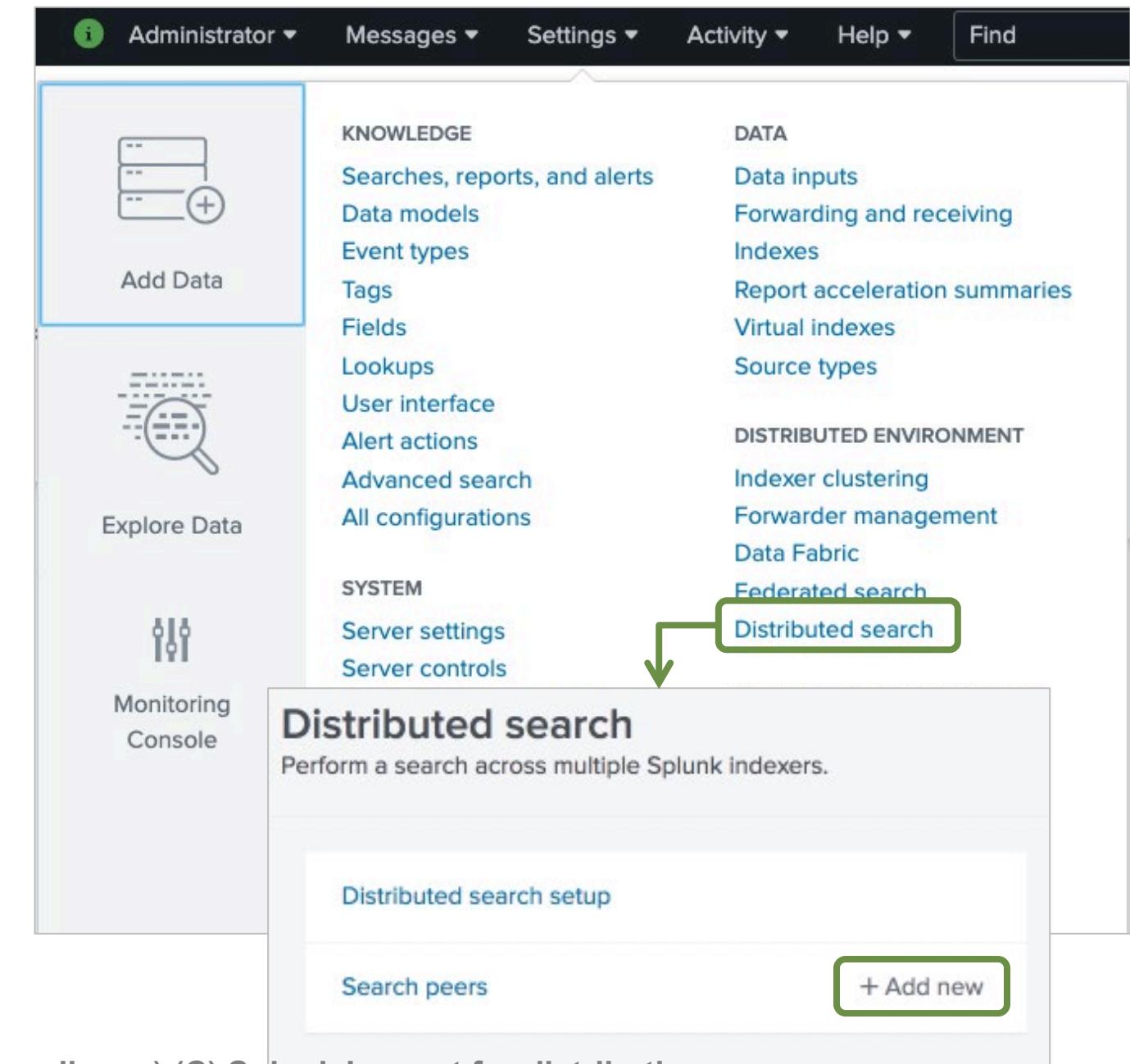
1. Universal forwarders (production servers) send data to indexers
2. Indexers (search peers) store their portion of the data
3. Users log on to the search head and run reports
4. The search head dispatches searches to the indexers
5. Indexers run searches in parallel and return their portion of results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



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Adding Indexers (Search Peers)

Add search peers

Use this page to explicitly add distributed search peers. Enable distributed search through the Distributed search setup page in Splunk Settings.

Peer URI *

Specify the search peer as `servername:mgmt_port` or `URI:mgmt_port`. You must prefix the URI with its scheme. For example: '`https://sp1.example.com:8089`'.

Distributed search authentication

To share a public key for distributed authentication, enter a username and password for an admin user on the remote search peer.

Remote username *

Remote password *

Confirm password

Cancel Save

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

User account with **`edit_user`** capability

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

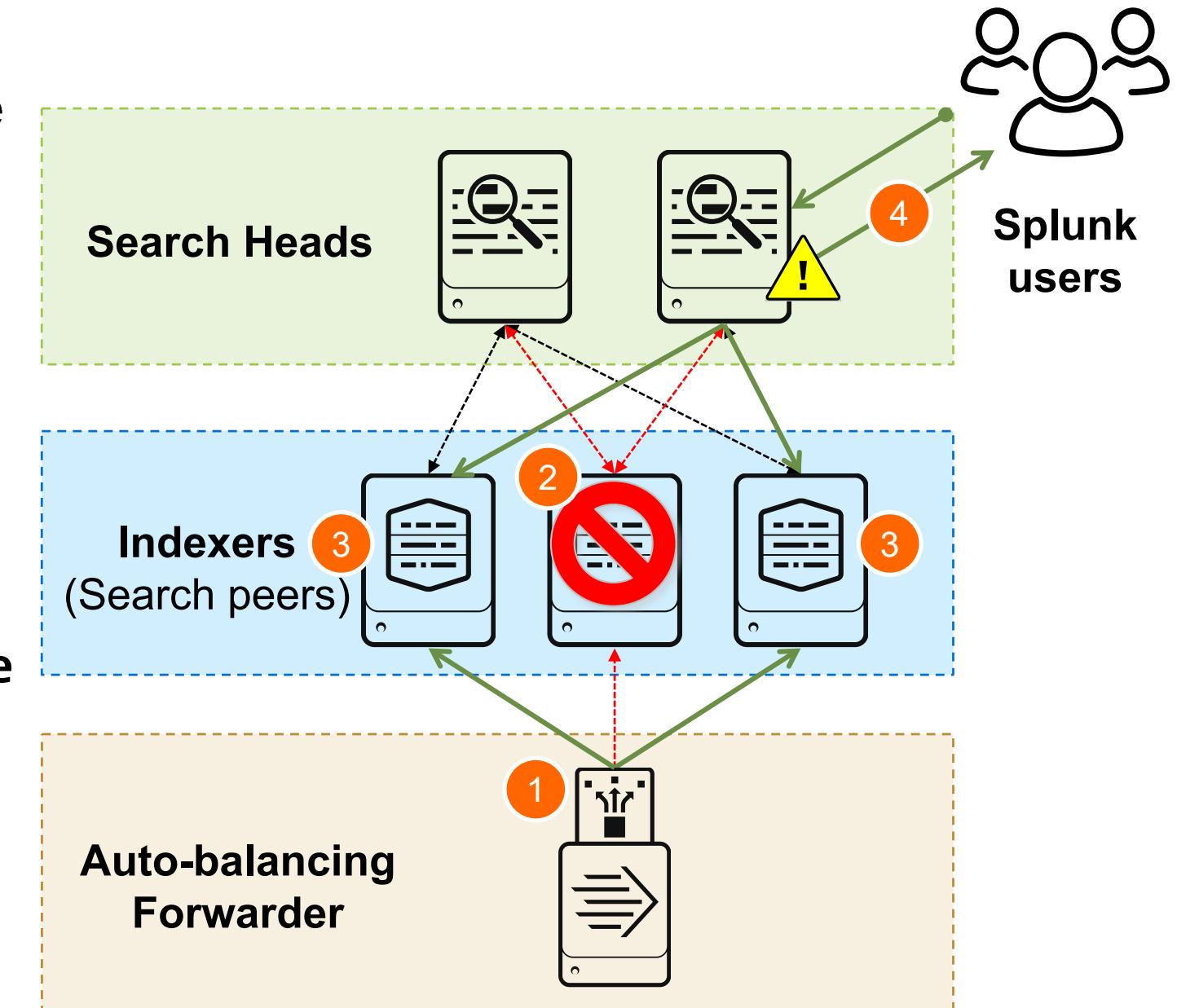
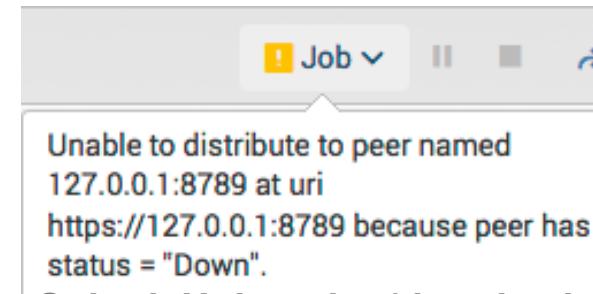
Knowledge Bundles and Replication

- 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:



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

The screenshot shows the Splunk Monitoring Console interface. The top navigation bar includes 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' search bar. The main menu has tabs for 'Overview', 'Summary', 'Health Check', 'Indexing', 'Search', 'Resource Usage', 'Forwarders', 'Settings', and 'Run a Search'. On the right, there's a 'Monitoring Console' icon. The central area is titled 'Search Activity: Instance'. It features a 'Role' section with 'Search Heads' selected and 'Indexers' as an option. Below this is a 'Group' section with 'All' selected. A dropdown menu is open over the 'Group' button, showing four options: 'Search Activity: Instance' (selected), 'Search Usage Statistics: Instance', 'KV Store: Instance', and 'Scheduler Activity: Instance'. There's also a 'Hide Filters' link. Underneath, there are buttons for 'Select views: All', 'Snapshot', and 'Historical'. A 'Snapshots' section displays 'Search Concurrency (Running/Limit)'. Below that are sections for 'Ad hoc + Scheduled Searches (0 Running)', 'Scheduled Searches (0 Running)', and 'Summarization'. Each section contains a large numerical value (e.g., 0/10, 0/5, 0/2) and a status indicator (Historical, Real-time). A green box highlights the 'Search Activity: Instance' dropdown, and a green arrow points from it down to the 'Search Concurrency' section.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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



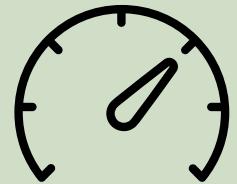
Access control

- 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

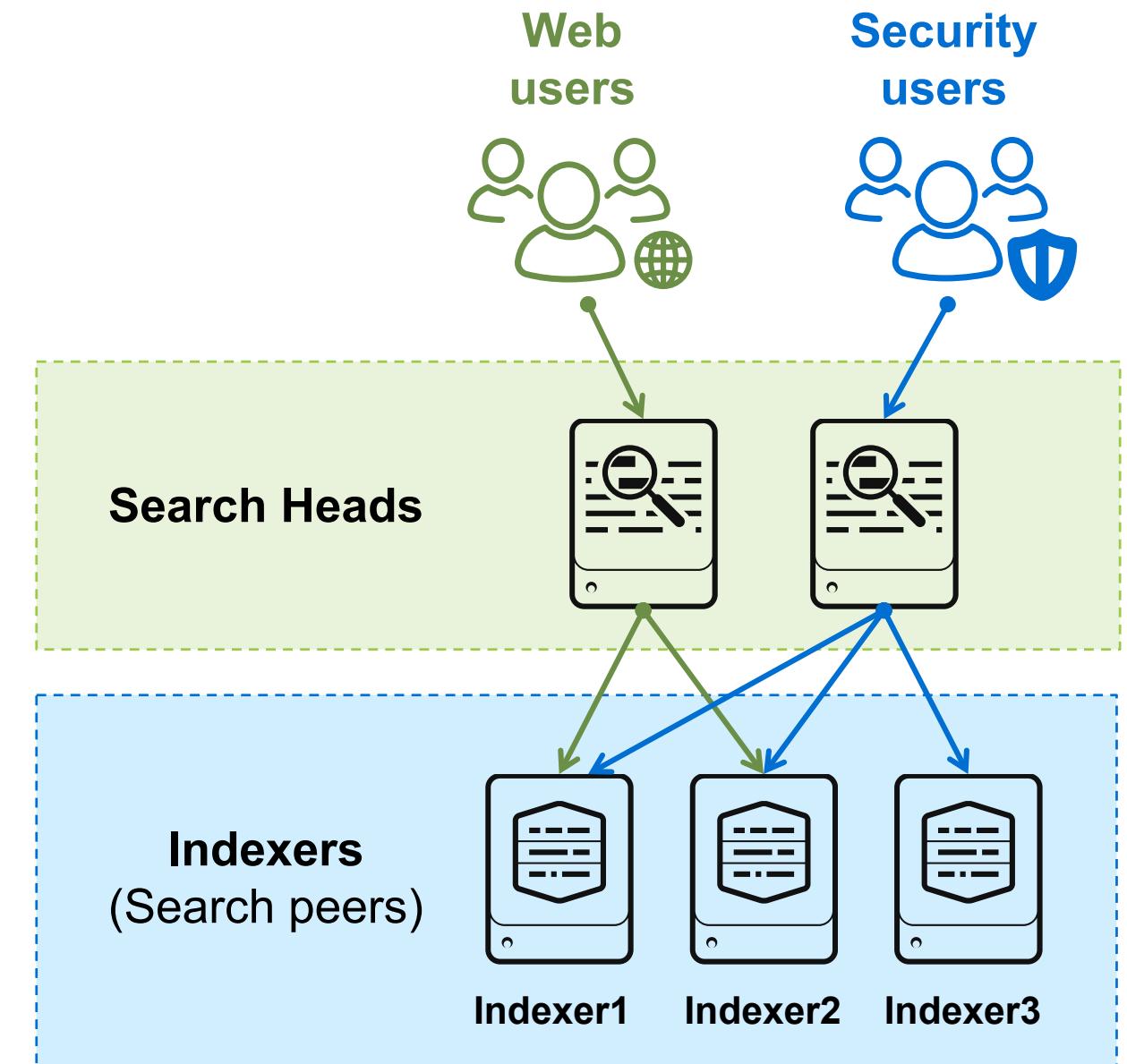
Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Determining the Number of Search Heads

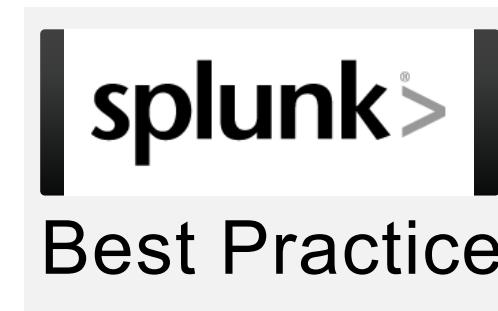
- Each search head handles ~8 - 12 simultaneous searches
 - Total includes both ad hoc and scheduled searches
 - Exact number depends on types of searches and search head hardware (especially CPU cores)
- Search heads can be added to the distributed group at any time
- Search heads can be:
 - **Dedicated:**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

Dedicated Search Heads

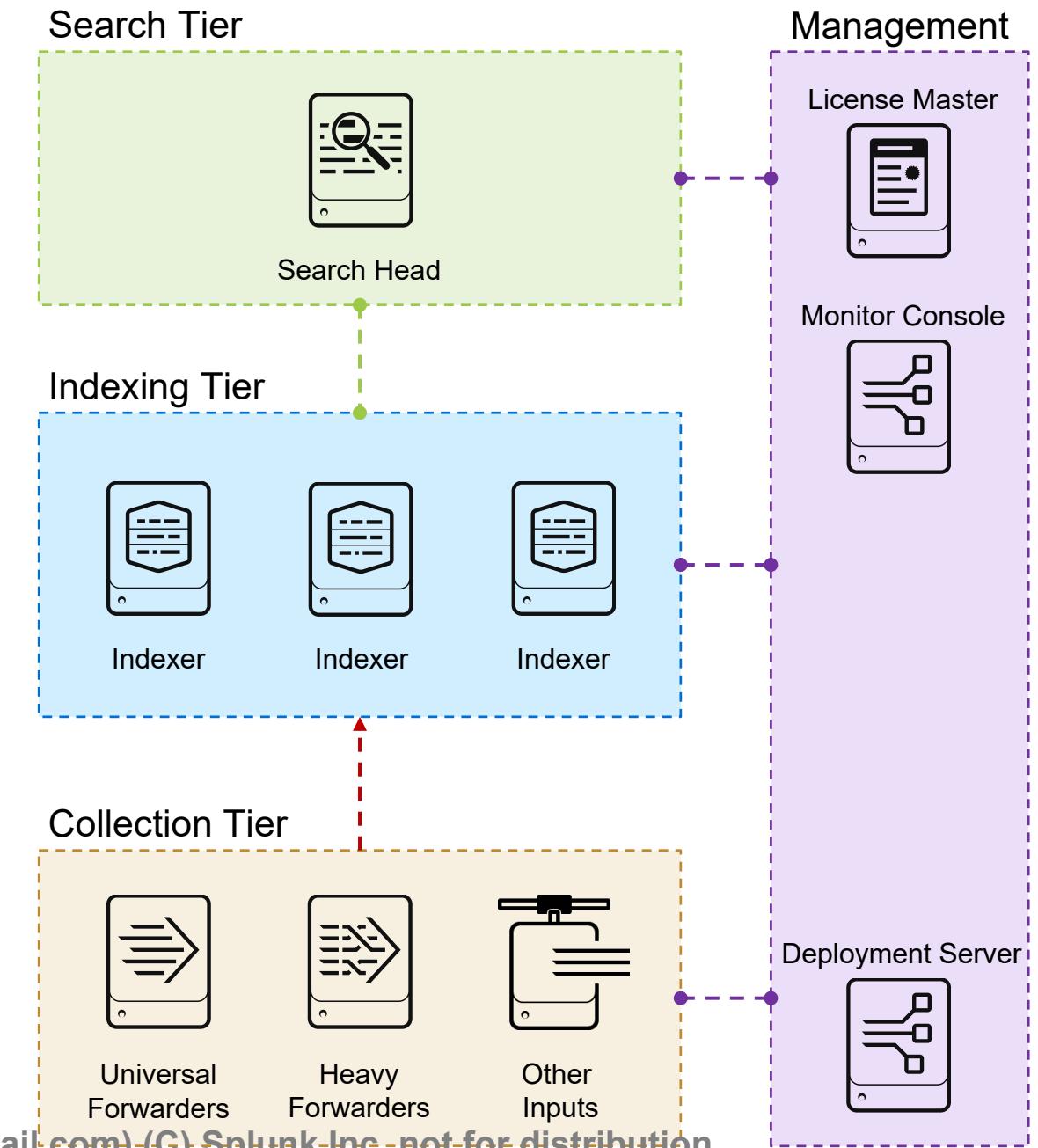
- Each search head
 - Contains its own unique set of reports, dashboards, and so on
 - Dedicated to a team of users with unique knowledge objects
- More than one search head can be configured for the same set of indexers (search peers)



Distributed Search Best Practices



- 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



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

The diagram illustrates the configuration of forwarding defaults in Splunk and its corresponding configuration in the `outputs.conf` file.

Forwarding and receiving

Forward data
Set up forwarding between two or more Splunk instances.

Forwarding defaults

Forwarding defaults
Forwarding and receiving » Forwarding defaults

Store a local copy of forwarded events?
 Yes No

This saves a copy of all indexed data on this Splunk instance and forwards copies to other instances.

Cancel **Save**

outputs.conf

```
[indexAndForward]
index = false

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

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

A green arrow points from the "Forwarding defaults" link in the first panel to the "Forwarding defaults" section in the second panel. A green arrow also points from the "Configure forwarding" button in the first panel to the "Forwarding defaults" section in the second panel. A red circle with the number 1 is on the "Save" button in the second panel. A red circle with the number 2 is on the "outputs.conf" heading in the third panel.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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**

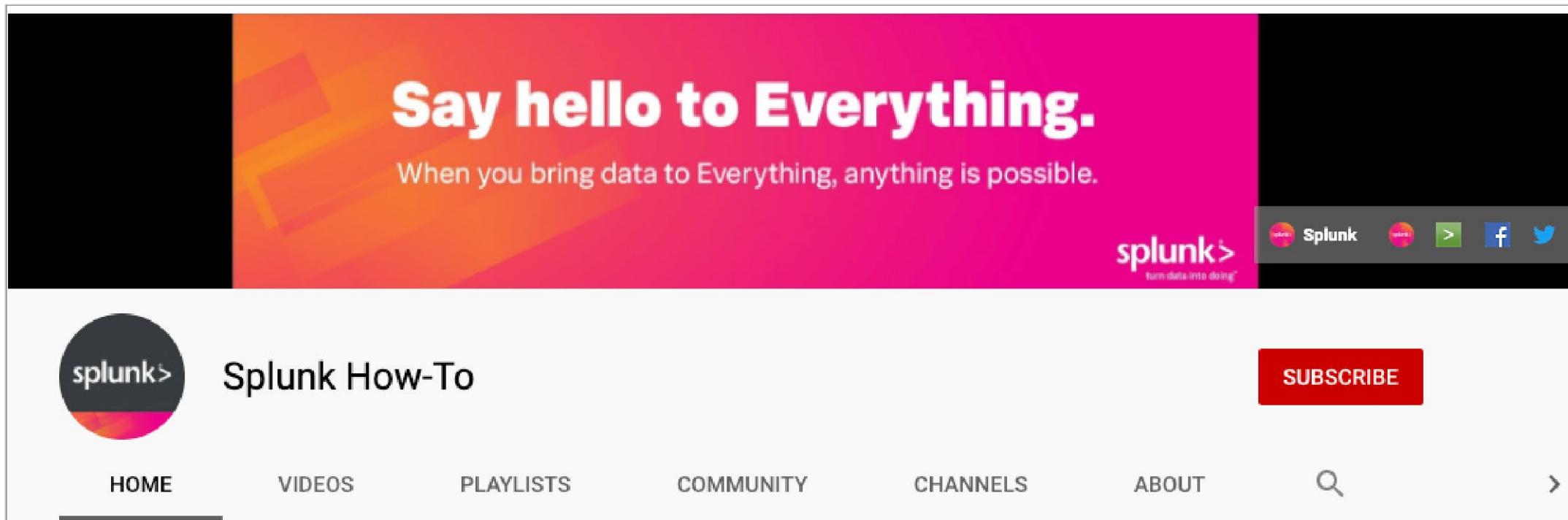
twitter.com/splunkdev

- **IRC Channel**

#splunk on the EFNet IRC server

Splunk How-To Channel

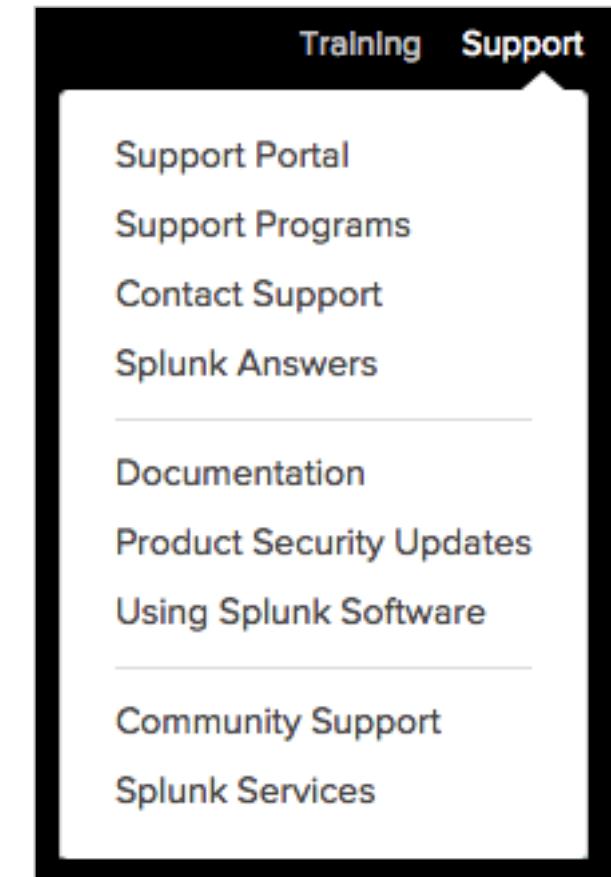
- Check out the Splunk Education How-To channel on YouTube:
splk.it/How-To
- Free, short videos on a variety of Splunk topics



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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)



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

splunk®>

.conf21

.conf21 Las Vegas
October 18–21

.conf21 Virtual
October 19–20

Splunk University
October 16–18

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution



Thank You



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Appendix A: Splunk Authentication Management

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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**

Authentication Methods

Select an authentication method. Splunk supports native authentication as well as the following external methods:

Internal Splunk Authentication (always on)

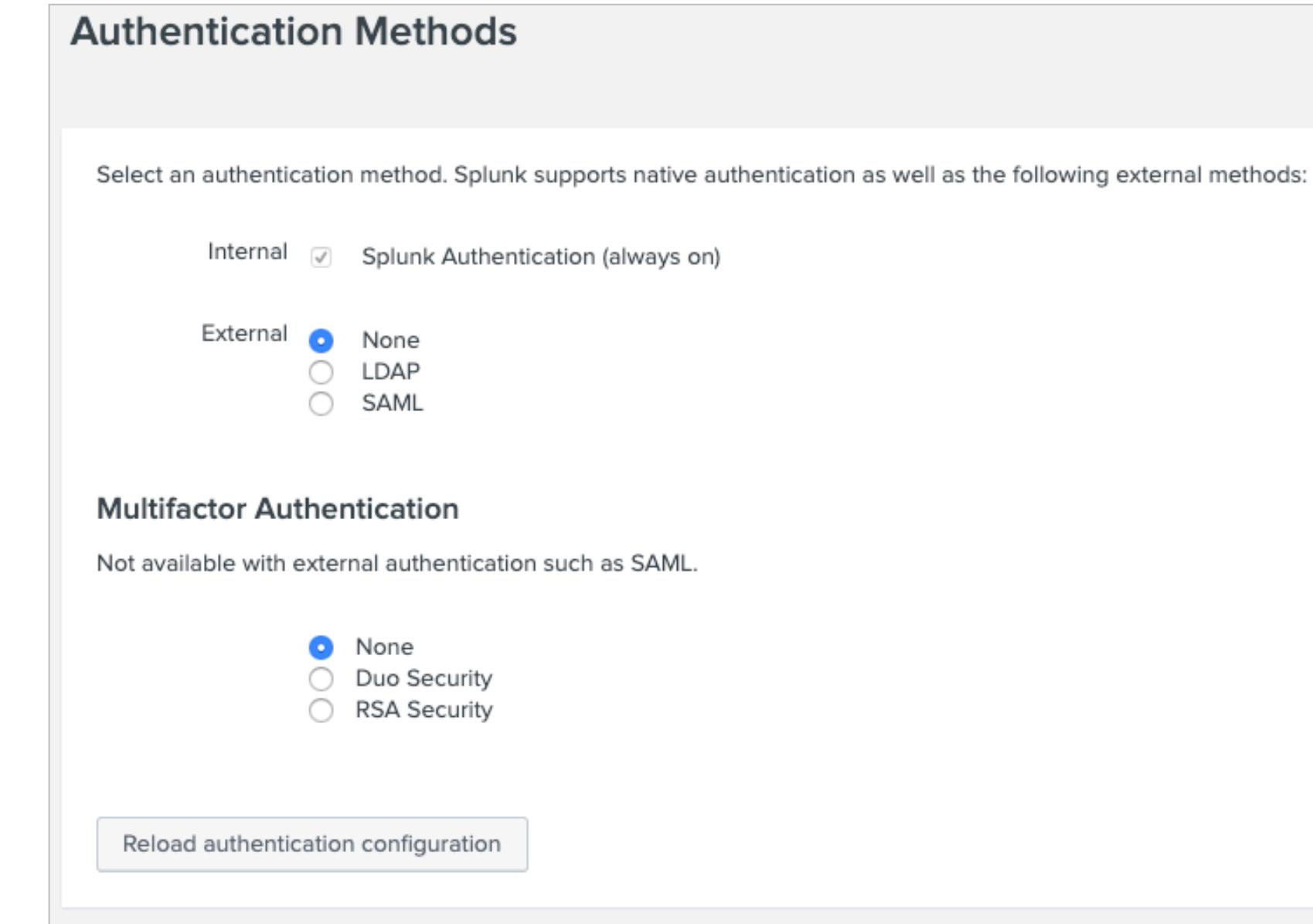
External None
 LDAP
 SAML

Multifactor Authentication

Not available with external authentication such as SAML.

None
 Duo Security
 RSA Security

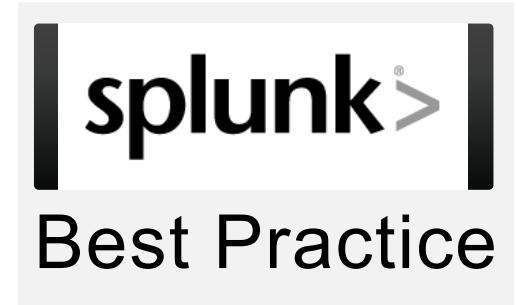
[Reload authentication configuration](#)



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

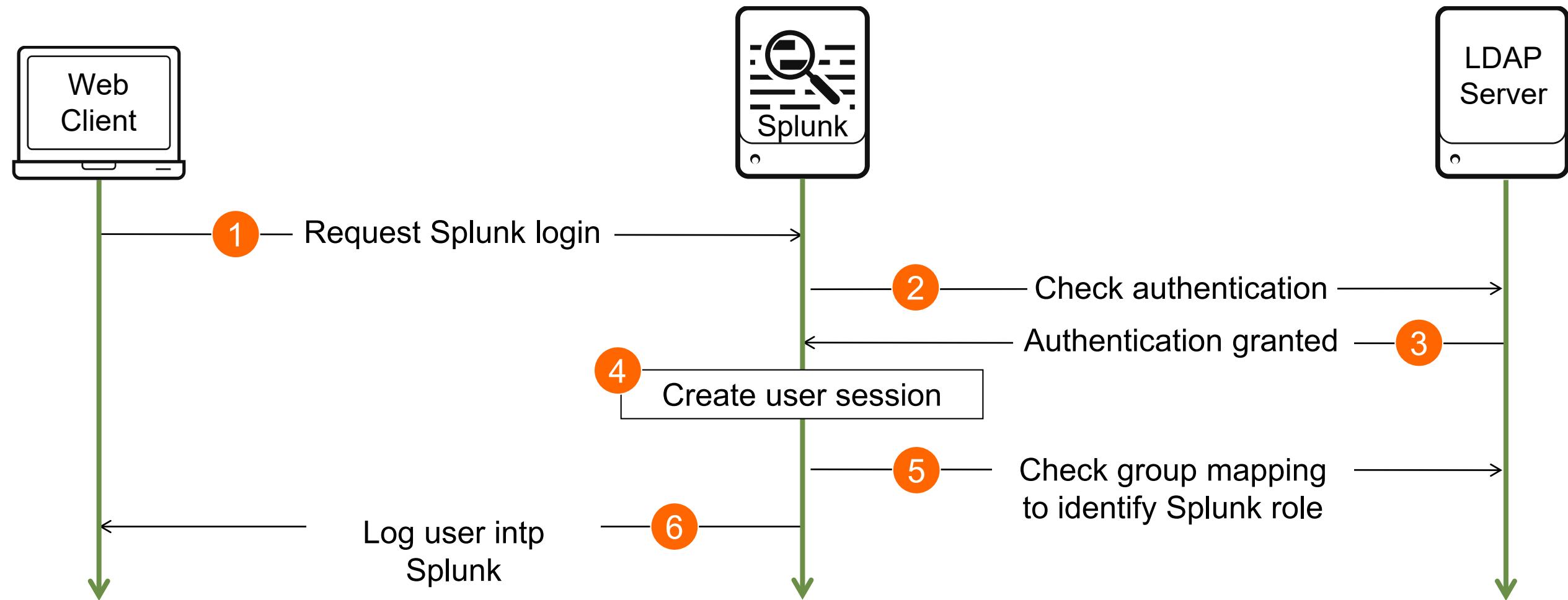
Directory Server Integration

- **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

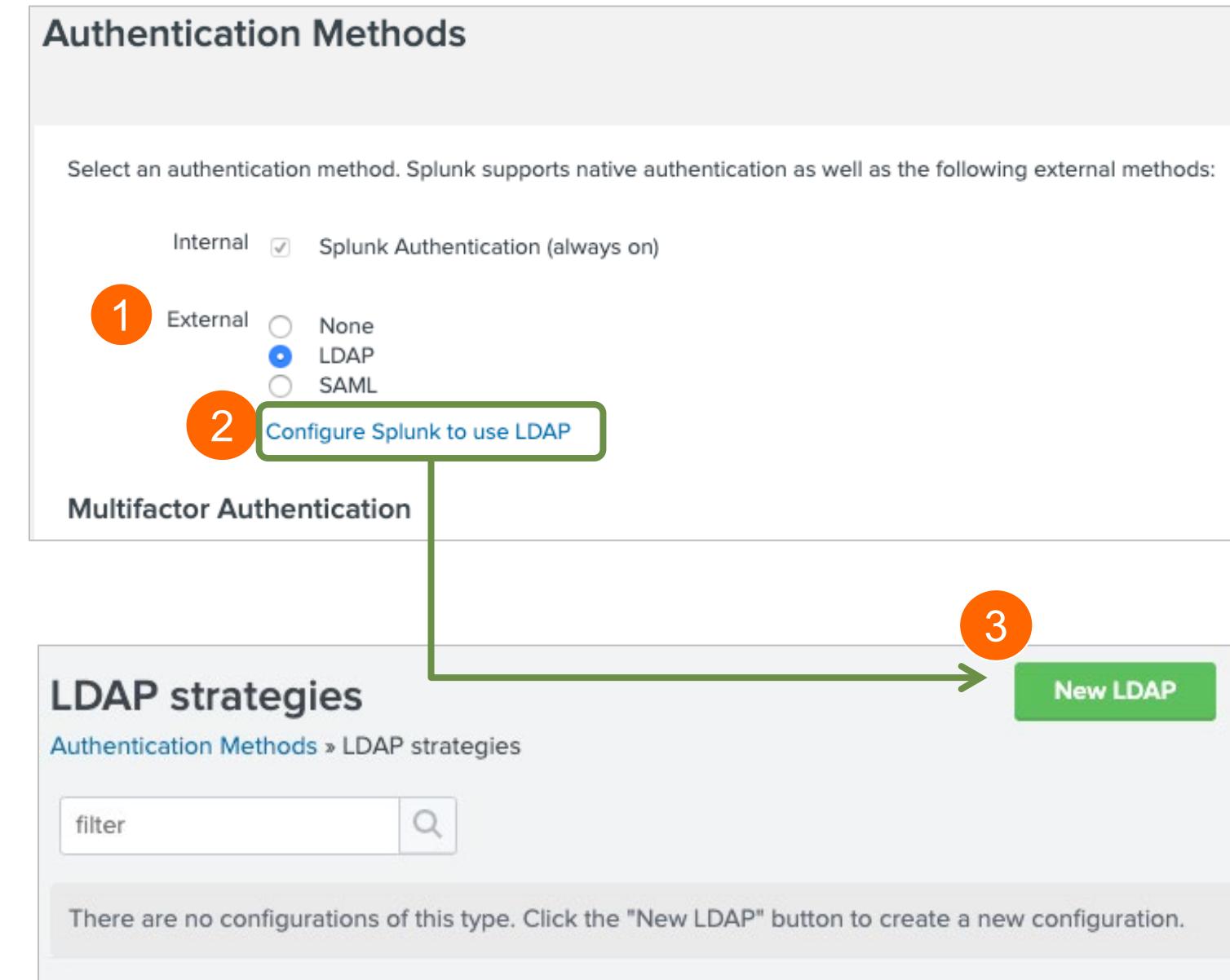
LDAP maintains the user credentials - user ID and password, plus other information - centrally and handles all authentication



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

The screenshot shows the Splunk interface for managing LDAP strategies. At the top, there is a green button labeled "New LDAP". Below it, a success message says "Successfully saved 'AD_splunkers'. Successfully performed a bind to the LDAP server." The main table lists one item: "AD_splunkers" with host "10.0.0.150" and port "389". The status is "Enabled". In the "Actions" column, there are links for "Map groups", "Clone", and "Delete", with "Map groups" being highlighted by a green box and arrow.

LDAP strategy name	Host	Port	Connection order	Status	Actions
AD_splunkers	10.0.0.150	389	1	Enabled Disable	Map groups Clone Delete

Below this, another table shows the mapping of LDAP groups to roles. It includes columns for "LDAP Group Name", "LDAP Strategy", "Group type", and "Roles". The "splunkAdmins" group is selected and highlighted with a green box and arrow. A callout box points to the "Map groups" link in the first table, stating: "Select to define relationships between LDAP groups and Splunk roles". Another callout box points to the "splunkAdmins" row, stating: "Click an LDAP group name to map it to one or more Splunk roles".

LDAP Group Name	LDAP Strategy	Group type	Roles
splunkAdmins	AD_splunkers	static	
splunkBizDev	AD_splunkers	static	
splunkITOps	AD_splunkers	static	
splunkSOC	AD_splunkers	static	

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Mapping LDAP Groups to Roles (cont.)

splunkAdmins
Authentication Methods » LDAP strategies » LDAP Groups » splunkAdmins

Available Roles

- admin
- can_delete
- power
- soc_analyst
- splunk-system-role
- user

Selected Roles

- admin

Click one or more role names to map them to this group

LDAP Users

CN=Cory Flintoff,OU=splunk,DC=buttercupgames,DC=local
CN=Gabriel Voronoff,OU=splunk,DC=buttercupgames,DC=local

```
graph LR; Admin[admin] --> AddAll[add all]; Admin --> Selected[admin]; Admin --> Callout1[Click one or more role names to map them to this group]; Admin --> Callout2[After completing the mapping for all LDAP groups, the mapped roles are shown here]; Admin --> LDAPUsers[CN=Cory Flintoff,OU=splunk,DC=buttercupgames,DC=local  
CN=Gabriel Voronoff,OU=splunk,DC=buttercupgames,DC=local]; Admin --> RolesTable[Roles]; Admin --> Callout3[After completing the mapping for all LDAP groups, the mapped roles are shown here];
```

LDAP Groups
Authentication Methods » LDAP strategies » LDAP Groups

Showing 1-4 of 4 items

LDAP Group Name	LDAP Strategy	Group type	Roles
splunkAdmins	AD_splunkers	static	admin
splunkBizDev	AD_splunkers	static	user
splunkITOps	AD_splunkers	static	power
splunkSOC	AD_splunkers	static	soc_analyst

- 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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

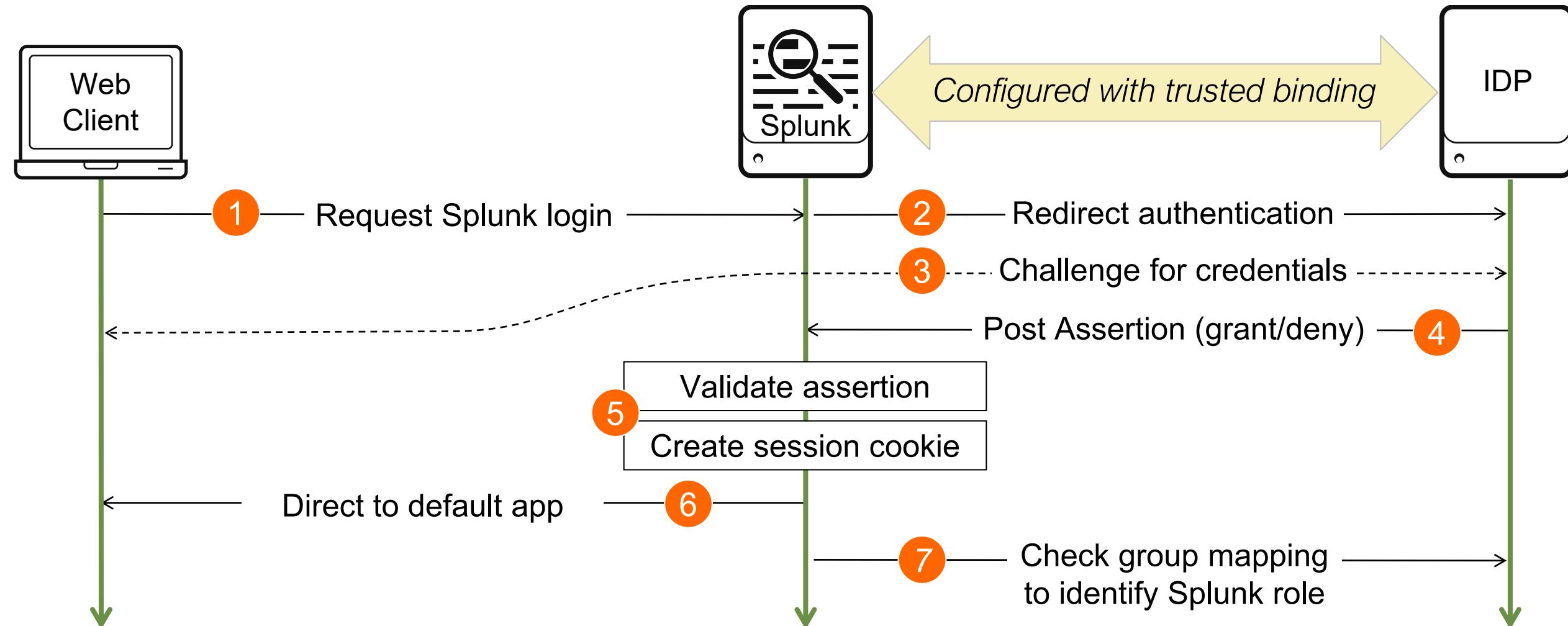
Users											Add new Splunk user	New User
13 Users											filter	10 per page ▾
Name ▾	Actions	Authentication system ▾	Full name ▾	Email address ▾	Time zone ▾	Default app ▾	Default app inherited from ▾	Roles ▾	Last Login ▾	Status ▾		
acurry		LDAP	Amanda			search	soc_analyst	soc_analyst		✓ Active		
admin	Edit ▾	Splunk	Administrator	02		launcher	system	admin	9/22/2020, 4:40:45 PM	✓ Active	< Prev	1 2 Next >
blu						launcher	system	user		✓ Active		
coryf		LDAP	Cory Flintoff			launcher	system	admin		✓ Active		
dhare		LDAP	Dwight Hale			launcher	system	user		✓ Active		
emaxwell	Edit ▾	Splunk				search	soc_analyst	soc_analyst	9/22/2020, 12:16:52 PM	✓ Active		
gvoronoff		LDAP	Gabriel Voronoff			launcher	system	admin		✓ Active		

Click to edit the user settings

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

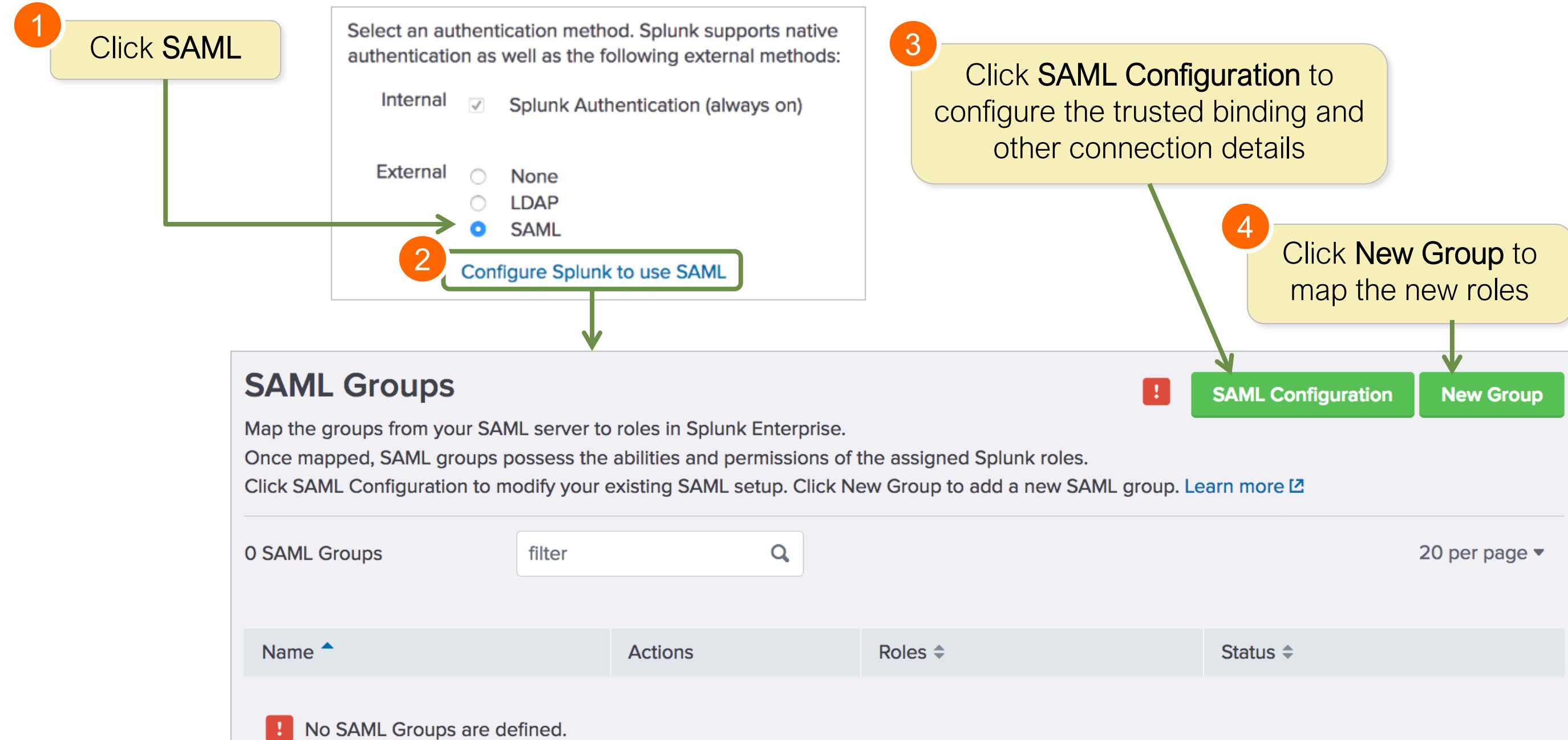
SAML 2.0 Single Sign On

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



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Configuring SAML



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Configuring SAML – Splunk Settings

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

SAML Configuration

Configure SAML for Splunk. [Learn More ↗](#)

Download the SPMetadata from Splunk and add it to your SAML environment to connect to Splunk.

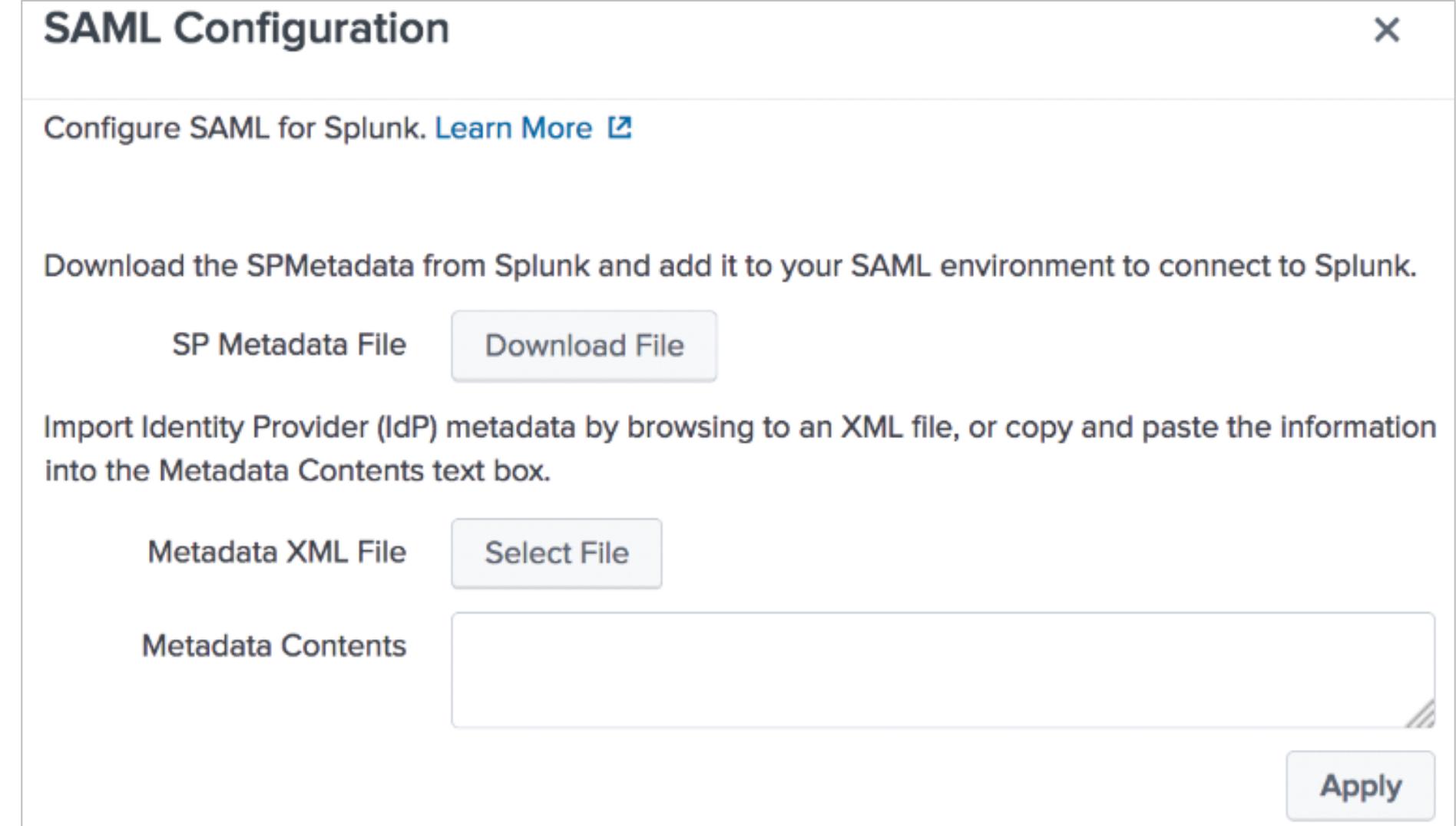
SP Metadata File [Download File](#)

Import Identity Provider (IdP) metadata by browsing to an XML file, or copy and paste the information into the Metadata Contents text box.

Metadata XML File [Select File](#)

Metadata Contents

[Apply](#)



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Configuring SAML – General Settings

Gather SAML configuration information

Protected endpoints on the IdP which Splunk sends authentication requests to

General Settings

Single Sign On (SSO) URL ?	
Single Log Out (SLO) URL ?	optional
IdP certificate path ?	optional Leave blank if you store IdP certificates under \$SPLUNK_HOME/etc/auth/idpCerts
IdP certificate chains ?	
Replicate Certificates ?	<input checked="" type="checkbox"/>
Issuer Id ?	
Entity ID ?	
Sign AuthnRequest	<input checked="" type="checkbox"/>

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Configuring SAML – Query and Alias Settings

Endpoint on the IdP to which queries over SOAP are sent

▼ Attribute Query Requests

Optional. Used only for vendors that support AQRs, such as IBM, CA, Ping Identity. Confirm with your provider. You must enable either AQRs or authentication extensions for SAML user tokens.

Attribute query URL [?](#)

Sign attribute query request

Sign attribute query response

Username

Password

▼ Alias

Role alias

RealName alias

Mail alias

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Advanced Settings		
Name Id Format ?	-----	
Fully qualified domain name or IP of the load balancer ?	optional	
Redirect port - load balancer port ?	optional	
Redirect to URL after logout ?	optional	
SSO Binding ?	HTTP Post	HTTP Redirect
SLO Binding ?	HTTP Post	HTTP Redirect

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

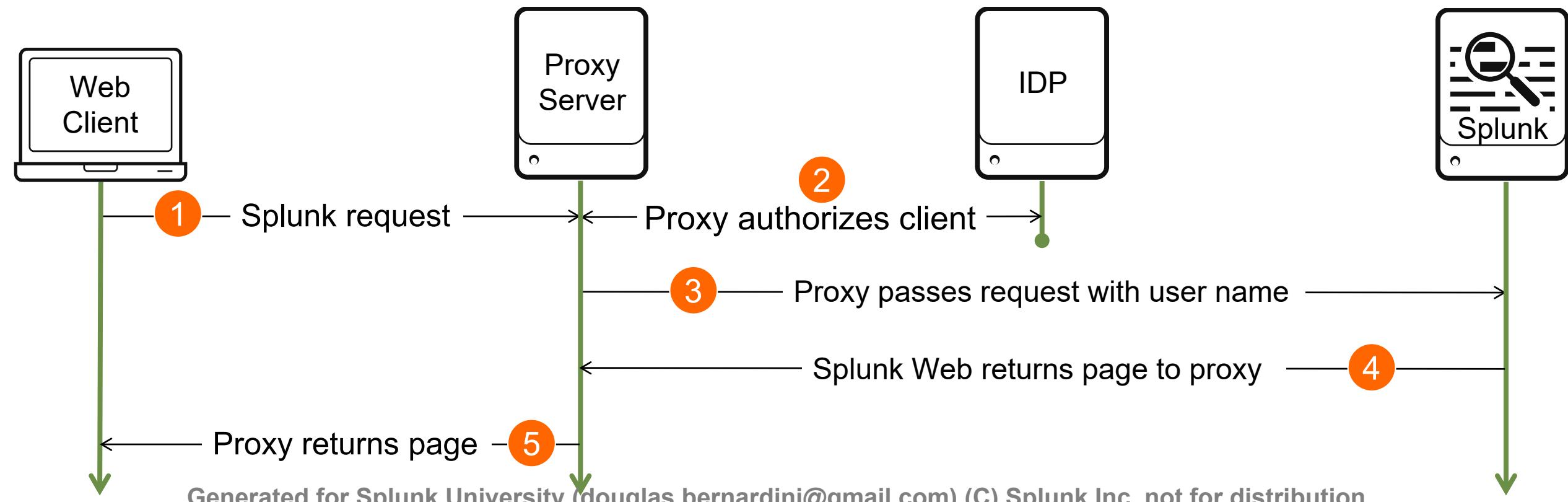
Create New SAML Group X

Group Name													
Splunk Roles	<table border="1"><thead><tr><th>Available item(s)</th><th>Selected item(s)</th></tr></thead><tbody><tr><td>admin</td><td>admin</td></tr><tr><td>can_delete</td><td>can_delete</td></tr><tr><td>power</td><td>power</td></tr><tr><td>securityops</td><td>securityops</td></tr><tr><td>splunk-system-role</td><td></td></tr></tbody></table>	Available item(s)	Selected item(s)	admin	admin	can_delete	can_delete	power	power	securityops	securityops	splunk-system-role	
Available item(s)	Selected item(s)												
admin	admin												
can_delete	can_delete												
power	power												
securityops	securityops												
splunk-system-role													
	add all » « remove all												

[Cancel](#) [Save](#)

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

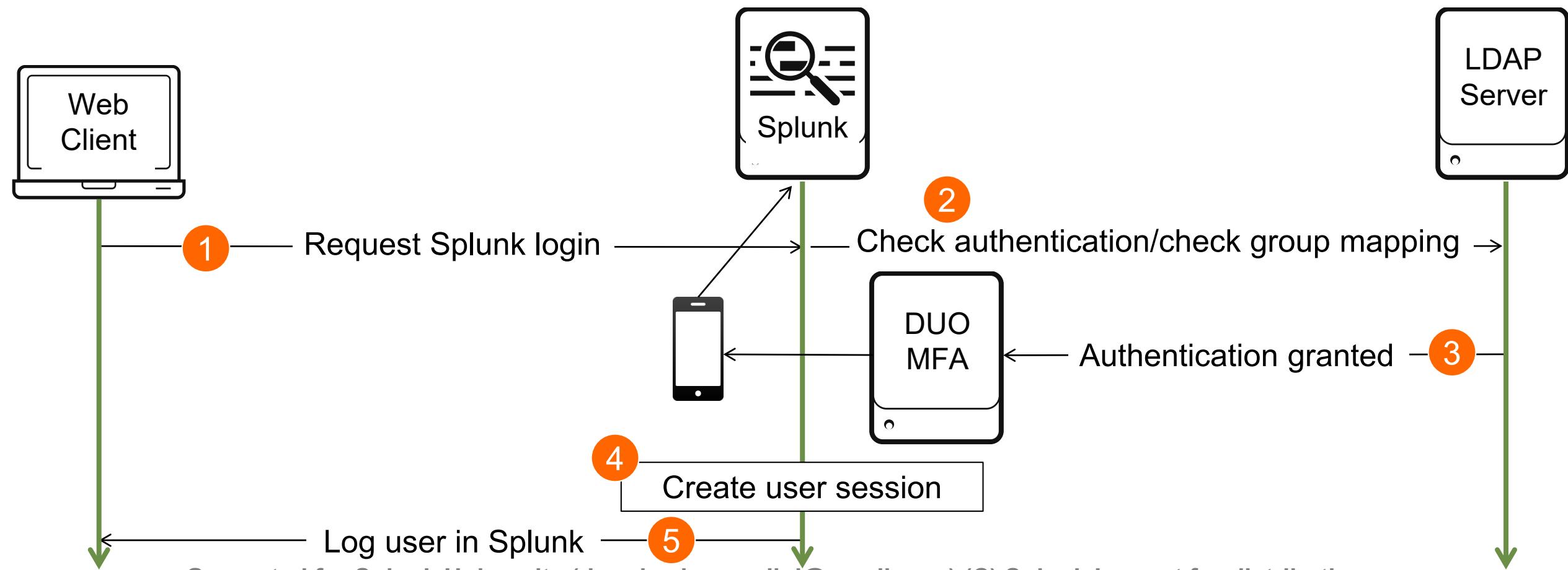


Scripted Authentication

- 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



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

The screenshot shows the 'Authentication Methods' section of the Splunk web interface. It includes a note about native authentication support and a table for selecting authentication methods. The 'Internal' row has a checked checkbox next to 'Splunk Authentication (always on)'. The 'External' row has three options: 'None' (radio button), 'LDAP' (radio button, highlighted with a blue dot), and 'SAML' (radio button). Below the table is a link to 'LDAP Settings'. The 'Multifactor Authentication' section notes that it's not available with external authentication like SAML. A callout with orange circles numbered 1 and 2 points to the 'Duo Security' radio button and the 'Configure Duo Security' button respectively. At the bottom is a 'Reload authentication configuration' button.

Authentication Methods	
Select an authentication method. Splunk supports native authentication as well as external authentication.	
Internal	<input checked="" type="checkbox"/> Splunk Authentication (always on)
External	<input type="radio"/> None <input checked="" type="radio"/> LDAP <input type="radio"/> SAML

[LDAP Settings](#)

Multifactor Authentication

Not available with external authentication such as SAML.

1 → Duo Security
2 [Configure Duo Security](#)

[Reload authentication configuration](#)

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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

Add new
Authentication Methods » Add new

3 Application Secret Key *
Should be 40 characters long. Splunk auto generates it, but you can create your own.

Integration Key *

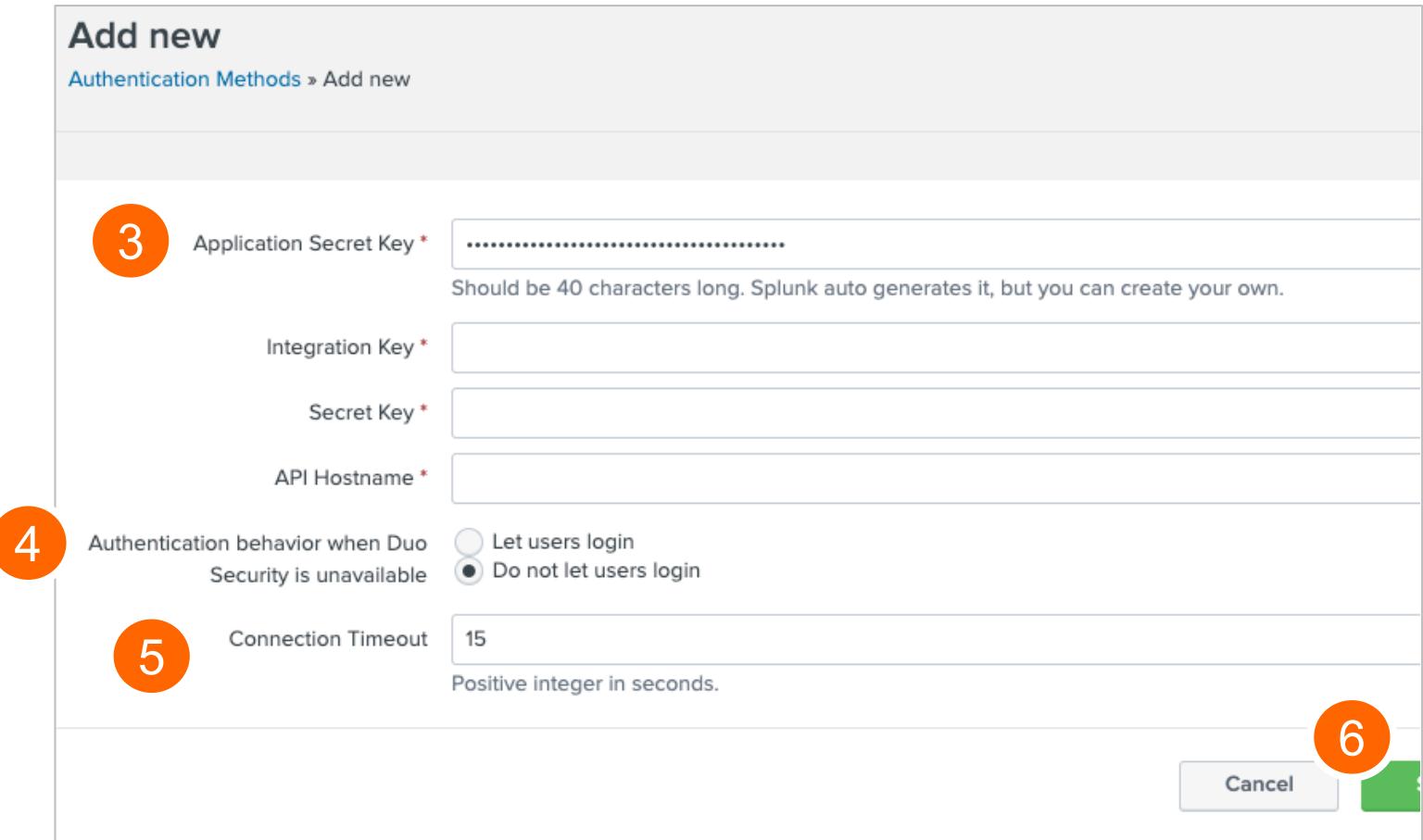
Secret Key *

API Hostname *

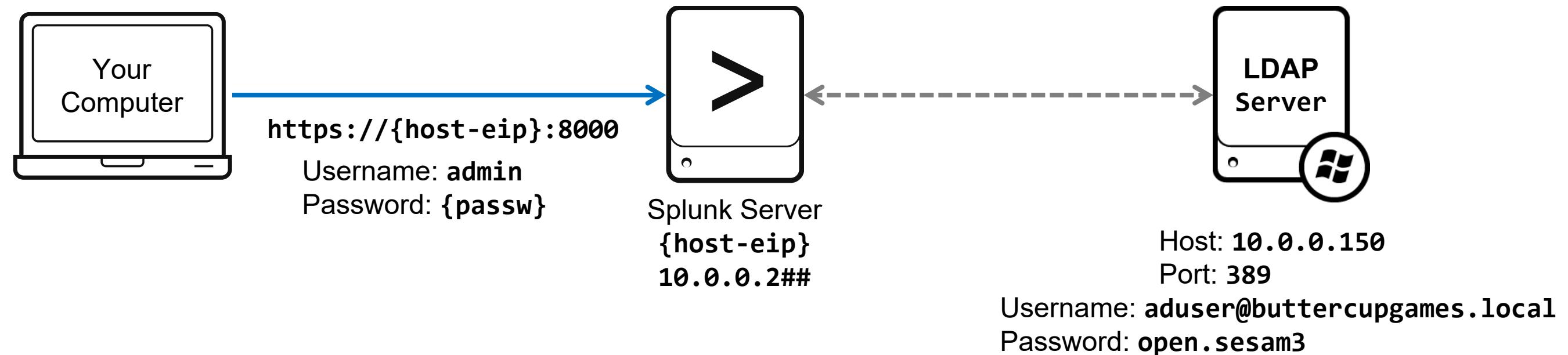
4 Authentication behavior when Duo Security is unavailable
 Let users login
 Do not let users login

5 Connection Timeout
15 Positive integer in seconds.

6 Cancel 



Lab Exercise A – Environment Diagram



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

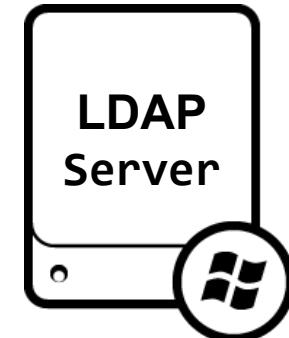
Appendix A Lab Exercise

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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Adding an Input with Splunk Web

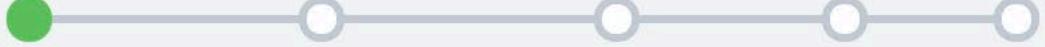
- Click the Add Data icon
 - On admin's Home page
 - On the Settings panel

- Or select:
 1. Settings
 2. Data inputs
 3. Add new

The screenshot shows the Splunk Web interface. At the top, there is a navigation bar with tabs: Administrator, Messages, Settings (highlighted with a red circle labeled 1), Activity, Help, and Find. Below the navigation bar is a main menu with several categories: KNOWLEDGE (Searches, reports, and alerts, Data models, Event types, Tags, Fields, Lookups, User interface), DATA (highlighted with a red circle labeled 2), and FORWARDING (Forwarding and receiving, Indexes, Report acceleration summaries, Virtual indexes, Source types). A large green arrow points from the 'Add Data' icon on the Home page to the 'Data inputs' link in the DATA category. In the 'Data inputs' section, there is a sub-section titled 'Local inputs' with two items: 'Files & Directories' (Index a local file or monitor an entire directory) and 'HTTP Event Collector'. At the bottom right of this section, there is a green button labeled '+ Add new' (highlighted with a red circle labeled 3).

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Select Source

Add Data  [Back](#) [Next >](#)

To configure a monitor input

Files & Directories 1

Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector

Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP

Configure the Splunk platform to listen on a network port.

Scripts

Get data from any API, service, or database with a script.

Systemd Journald Input for Splunk

This is the input that gets data from journald (systemd's logging component) into Splunk.

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. Then, Splunk monitors all objects within the directory. This includes all data sources in the directory. To add individual data inputs, click [Learn More](#).

Specify the source with absolute path to a file or directory, or use the **Browse** button

File or Directory ? 2 [Browse](#)

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Continuously Monitor 3 Index Once

Whitelist ? For ongoing monitoring

Blacklist ? • For one-time indexing
• Does not create a stanza in **inputs.conf**



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Set Source Type (Data Preview - 1)

Set Source Type

Tip: You can preview your data before indexing. If the events look correct and have the right timestamps, click "Save As" to automatically determine the source type. If you need to manually set the source type or fix proper event breaks and timestamps. If you cannot find an appropriate source type for your data, click "View Event Summary".

Automatically determined for major data types

1

Source type: access_combined_wcookie ▾

Save As

List ▾ Format 20 Per Page ▾

< Prev 1 2 3 4 5 6 7 8 ... Next >

	Time	Event
1	7/14/20 5:19:23.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:23] "POST /oldlink?itemId=EST-27&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 1391 "http://www.google.com" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 677
2	7/14/20 5:19:29.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:29] "GET /product.screen?productId=WC-SH-A01&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 1053 "http://www.buttercupgames.com/oldlink?itemId=EST-6" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 531
3	7/14/20 5:19:30.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:30] "GET /product.screen?productId=MB-AG-T01&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 1434 "http://www.buttercupgames.com/oldlink?itemId=EST-16" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 862
4	7/14/20 5:19:34.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:34] "POST /cart.do?action=changequantity&itemId=EST-15&productId=FI-AG-G08&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 3279 "http://www.buttercupgames.com/category.screen?categoryId=ARCADE" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 655
5	7/14/20 5:19:38.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:38] "GET /product.screen?productId=MB-AG-T01&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 2316 "http://www.buttercupgames.com/oldlink?itemId=EST-26" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 672

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Set Source Type (Data Preview - 2)

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: /opt/log/www1/access.log View Event Summary

Source type: access_combined_wcookie Save As

filter Q

List ▾ Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

	Time	Event
1	7/14/20 5:19:23.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:23] "POST /oldlink?itemId=EST-27&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 1391 "http://www.google.com" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 677
2	7/14/20 5:19:29.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:29] "GET /product.screen?productId=WC-SH-A01&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 1053 "http://www.buttercupgames.com/oldlink?itemId=EST-6" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 531
3	7/14/20 5:19:30.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:30] "GET /product.screen?productId=MB-AG-T01&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 1434 "http://www.buttercupgames.com/oldlink?itemId=EST-16" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 862
4	7/14/20 5:19:34.000 AM	-- [14/Jul/2020:05:19:34] "POST /cart.do?action=changequantity&itemId=EST-15&G08&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 3279 "http://www.buttercupgame.com/screen?categoryId=ARCADE" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 655
5	7/14/20 5:19:38.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:38] "GET /product.screen?productId=MB-AG-T01&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 2316 "http://www.buttercupgames.com/oldlink?itemId=EST-26" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 672

Optional choose a different source type 2

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Set Source Type (Data Preview - 3)

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: /opt/log/www1/access.log View Event Summary

Source type: access_combined_wcookie Save As

List ▾ Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

	Time	Event
1	7/14/20 5:19:23.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:23] "POST /oldlink?itemId=EST-27&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 1391 "http://www.google.com" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 677
2	7/14/20 5:19:29.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:29] "GET /product.screen?productId=WC-SH-A01&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 1055 "http://www.buttercupgames.com/oldlink?itemId=EST-6" "Mozilla/5.0 (Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 677
3	7/14/20 5:19:30.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:30] "GET /product.screen?productId=WC-SH-A01&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 1055 "http://www.buttercupgames.com/oldlink?itemId=EST-6" "Mozilla/5.0 (Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 677
4	7/14/20 5:19:34.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:34] "POST /cart.do?action=changequantity&itemId=EST-15&productId=FI-AG-G08&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 3279 "http://www.buttercupgames.com/category.screen?categoryId=ARCADE" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 655
5	7/14/20 5:19:38.000 AM	211.191.168.25 -- [14/Jul/2020:05:19:38] "GET /product.screen?productId=MB-AG-T01&JSESSIONID=SD3SL3FF2ADFF4954 HTTP 1.1" 200 2316 "http://www.buttercupgames.com/oldlink?itemId=EST-26" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 672

3 Data Preview displays how processed events will be indexed

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Set Source Type (Data Preview - Warning)

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks or your data, create a new one by clicking "Save As".

Source: /opt/log/www1/access.log

Source type: apache_error ▾

Save As

> Event Breaks

> Timestamp

> Advanced

List ▾ Format 20 Per Page ▾

1 7/14/20 5:57:03.000 AM

Event

188.173.152.100 -- [14/Jul/2020:05:57:03] "GET /category.screen?categoryId=ACCESSORIES&JSESSIONID=SD2SL6FF10ADFF4967 HTTP 1.1" 200 3994 "http://www.buttercupgames.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5" 106

188.173.152.100 -- [14/Jul/2020:05:57:10] "GET /oldlink?itemId=EST-15&JSESSIONID=SD2SL6FF10ADFF4967 HTTP 1.1" 200 2992 "http://www.buttercupgames.com/product.screen?productId=DC-SG-G02" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5" 359

188.173.152.100 -- [14/Jul/2020:05:57:16] "GET /oldlink?itemId=EST-7&JSESSIONID=SD2SL6FF10ADFF4967 HTTP 1.1" 400 3314 "http://www.buttercupgames.com/oldlink?itemId=EST-7" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5" 316

188.173.152.100 -- [14/Jul/2020:05:57:19] "GET /category.screen?categoryId=TEE&JSESSIONID=SD2SL6FF10ADFF4967 HTTP 1.1" 200 2715 "http://www.tee categoryId=TEE" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5" 879

188.173.152.100 -- [14/Jul/2020:05:57:23] "GET /pr SIONID=SD2SL6FF10ADFF4967 HTTP 1.1" 500 750 "http://n?categoryId=NULL" "Mozilla/5.0 (Windows NT 6.1; WOcko) Chrome/19.0.1084.52 Safari/536.5" 157

Show all 257 lines

Allows creation of a new source type for a specific source data

View Event Summary

< Prev 1 2 Next >

Warning If events are not separated correctly or have incorrect timestamps, select a different source type from the list or customize the source type settings.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Input Settings

Add Data

Select Source Set Source Type Input Settings Review Done

< Back Review >

Input Settings

Optionaly set additional input parameters for this data input as follows:

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for

App Context: Search & Reporting (search)

Host field value: splunk03

Index: itops

- 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

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Review

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

The screenshot shows the 'Add Data' wizard in the 'Review' step. The top navigation bar includes 'Add Data' on the left, a progress bar with five steps ('Select Source', 'Set Source Type', 'Input Settings', 'Review', 'Done') where the first four are green and the last one is grey, and buttons for '< Back' and 'Submit >' on the right.

Review

Input Type File Monitor
Source Path /opt/log/www1/access.log
Continuously Monitor Yes
Source Type access_combined_wcookie
App Context search
Host splunk03
Index itops

Note i

Confirm settings before proceeding.
It is easier to use < Back and make changes than to rectify later.

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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:

The screenshot shows the 'Add Data' wizard with the title 'Add Data' and a progress bar at the top. The steps are: Select Source, Set Source Type, Input Settings, Review, and Done. The 'Review' step is highlighted with a green checkmark. The main content area displays a success message: 'File input has been created successfully.' It also includes links to 'Start Searching', 'Extract Fields', 'Add More Data', 'Download Apps', and 'Build Dashboards'. Below these links are descriptions and 'Learn more' links for each option.

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

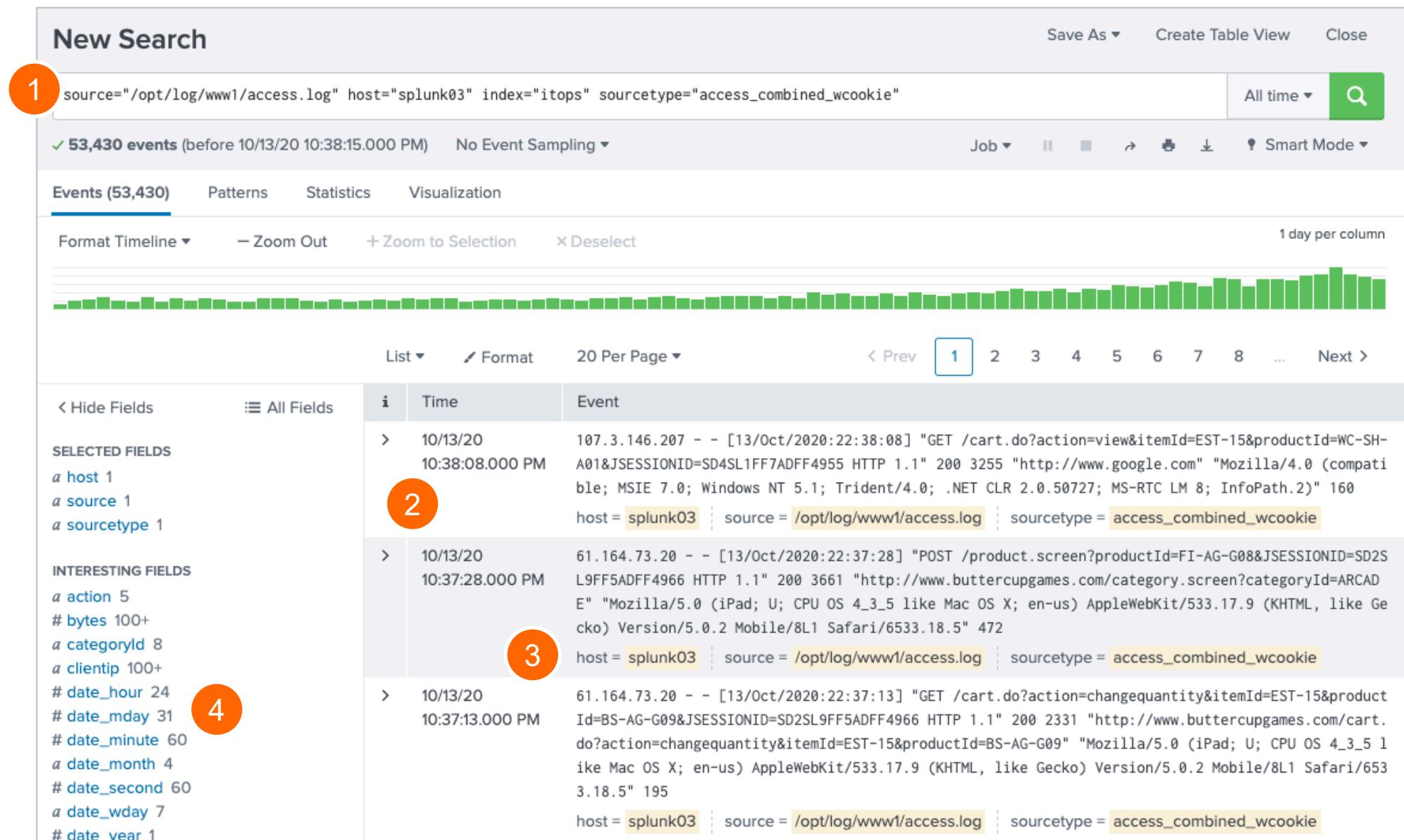
Note



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



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Appendix C: Introduction to Splunk Clustering

Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

Splunk Clustering

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

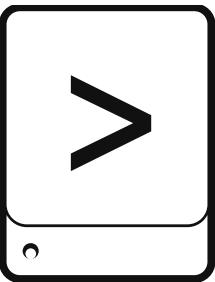
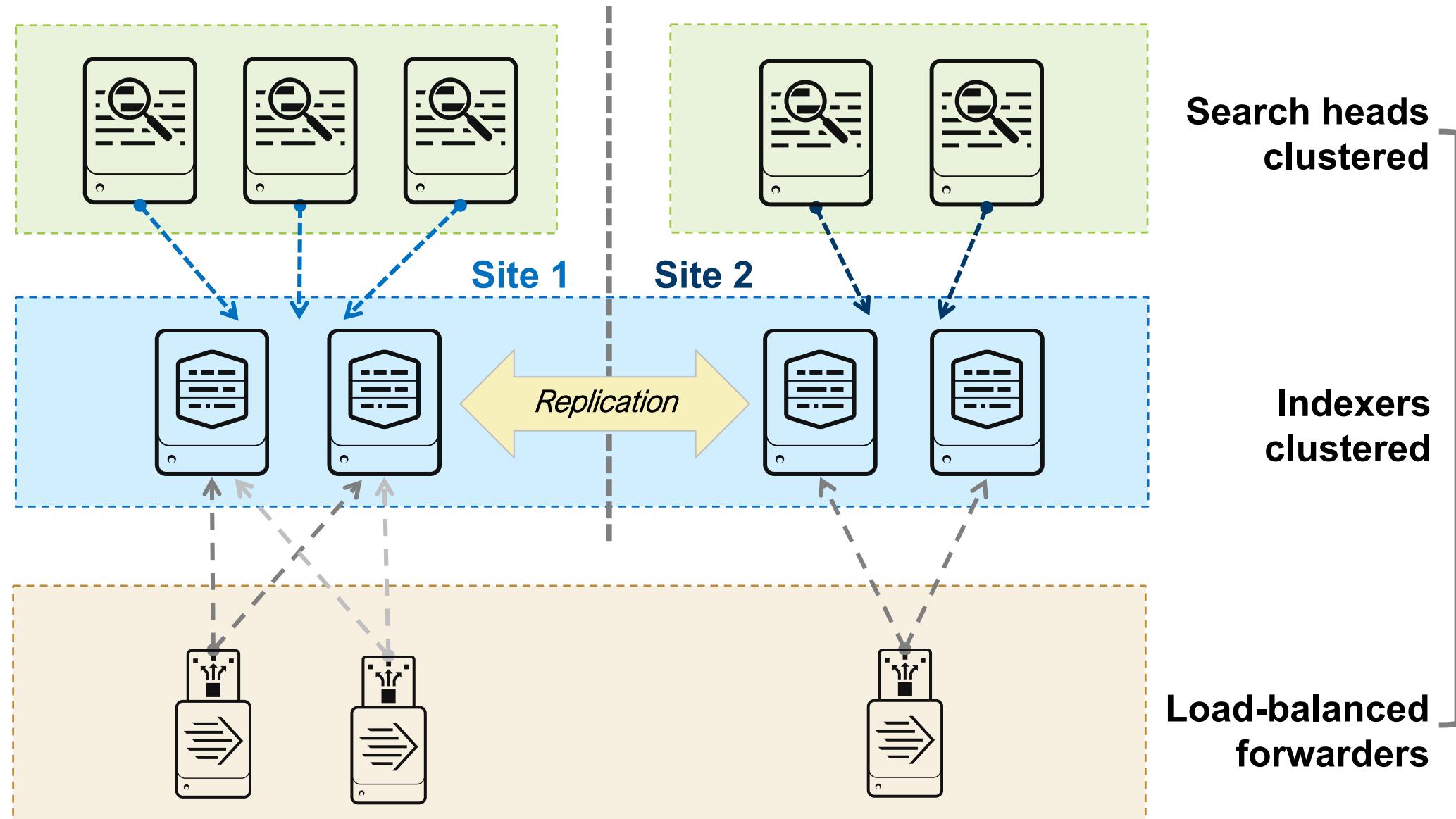
Search head
clustering

- 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

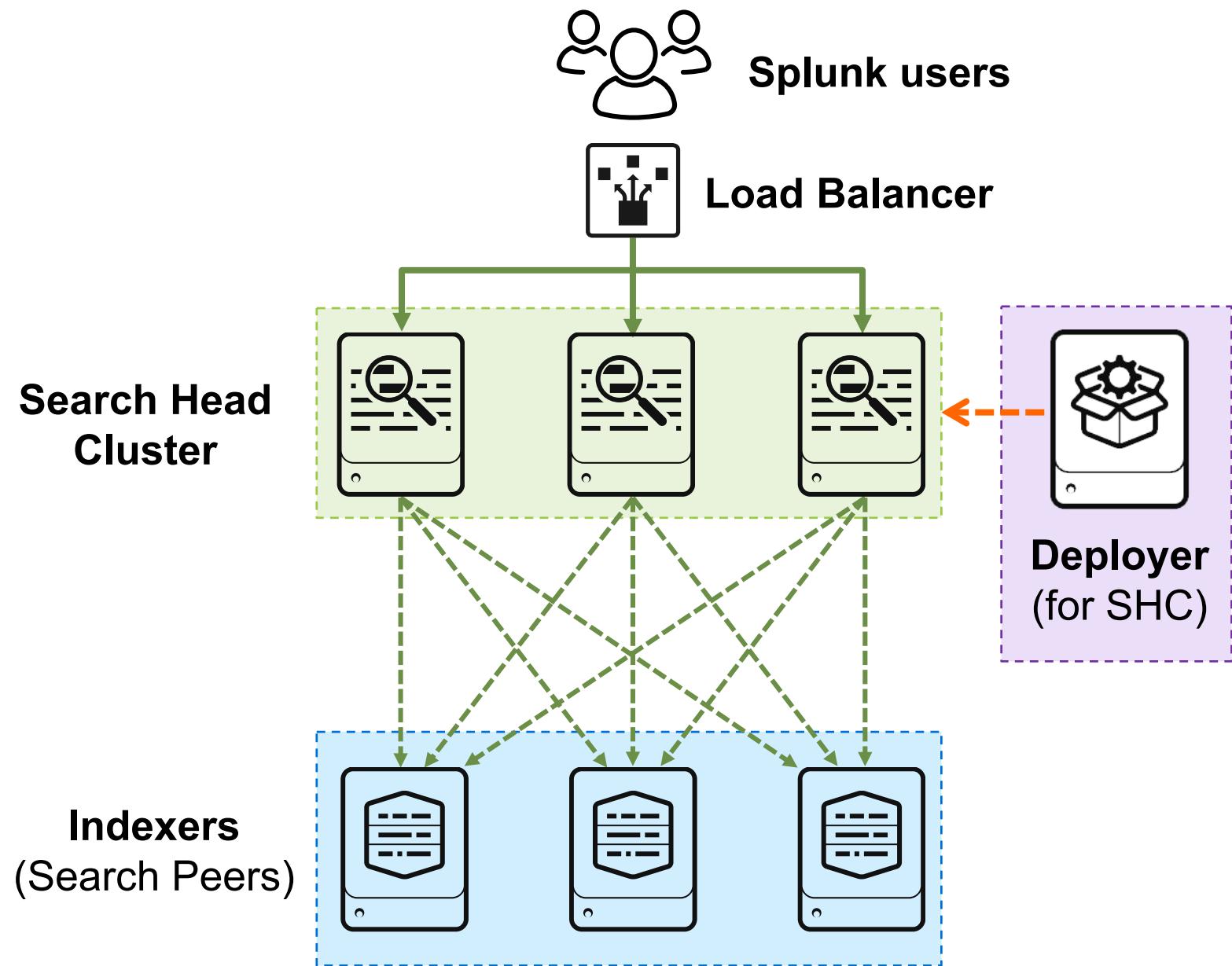
Splunk Cluster Overview



- Additional Components:
- Cluster Manager
 - Monitoring Console
 - Deployment Server
 - Deployer
 - License Manager

Search Head Cluster

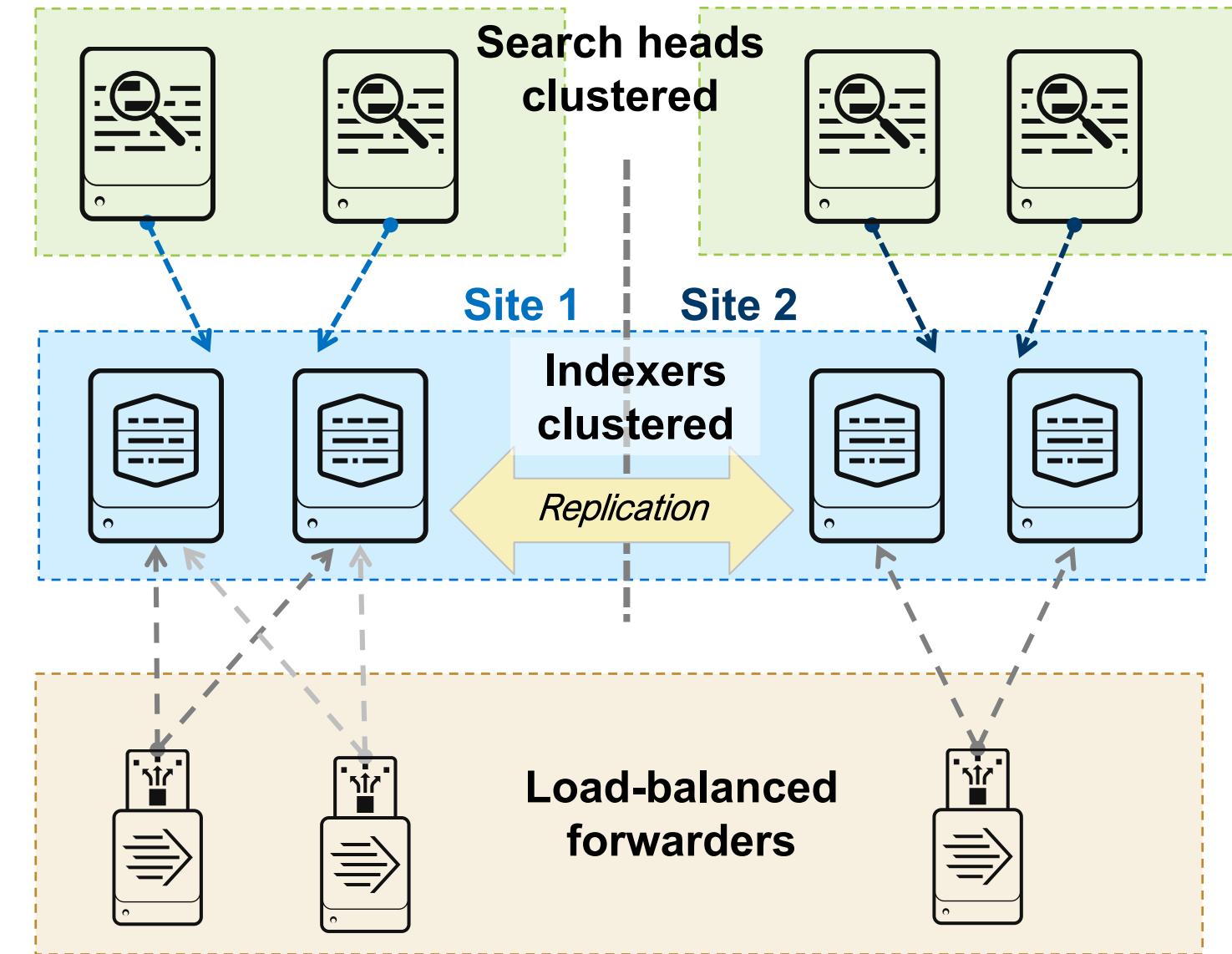
- Accommodates large enterprise use cases
 - Search head high-availability
 - Unified user experience across SHs
 - Search scaling foundation
 - Configuration sharing
 - Artifact replication
 - Job distribution
 - Alert management
 - Load balancing
- Supports external (non-Splunk) load balancers to provide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



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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**



Generated for Splunk University (douglas.bernardini@gmail.com) (C) Splunk Inc, not for distribution

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