



# Splunk Enterprise 7.3 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 YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Course Prerequisites

---

- Required:
  - Splunk Fundamentals 1
  - Splunk Fundamentals 2

# Course Goals

---

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

# System Administrator vs Data Administrator

---

- The Splunk System Administrator is primarily responsible for system management efforts which include:
  - Install, configure, and manage Splunk components
  - Install and manage Splunk apps
  - Manage Splunk licensing
  - Manage Splunk indexes
  - Manage Splunk users and authentication
  - Manage Splunk configuration files
  - Monitor MC and respond to system health alerts
- The Splunk Data Administrator is primarily responsible for data onboarding and management efforts which include:
  - 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

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Course Outline

---

Module 1: Splunk Deployment Overview

Module 2: License Management

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

Module 10: Introduction to Splunk Clusters

---

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Module 1: Splunk Deployment Overview

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

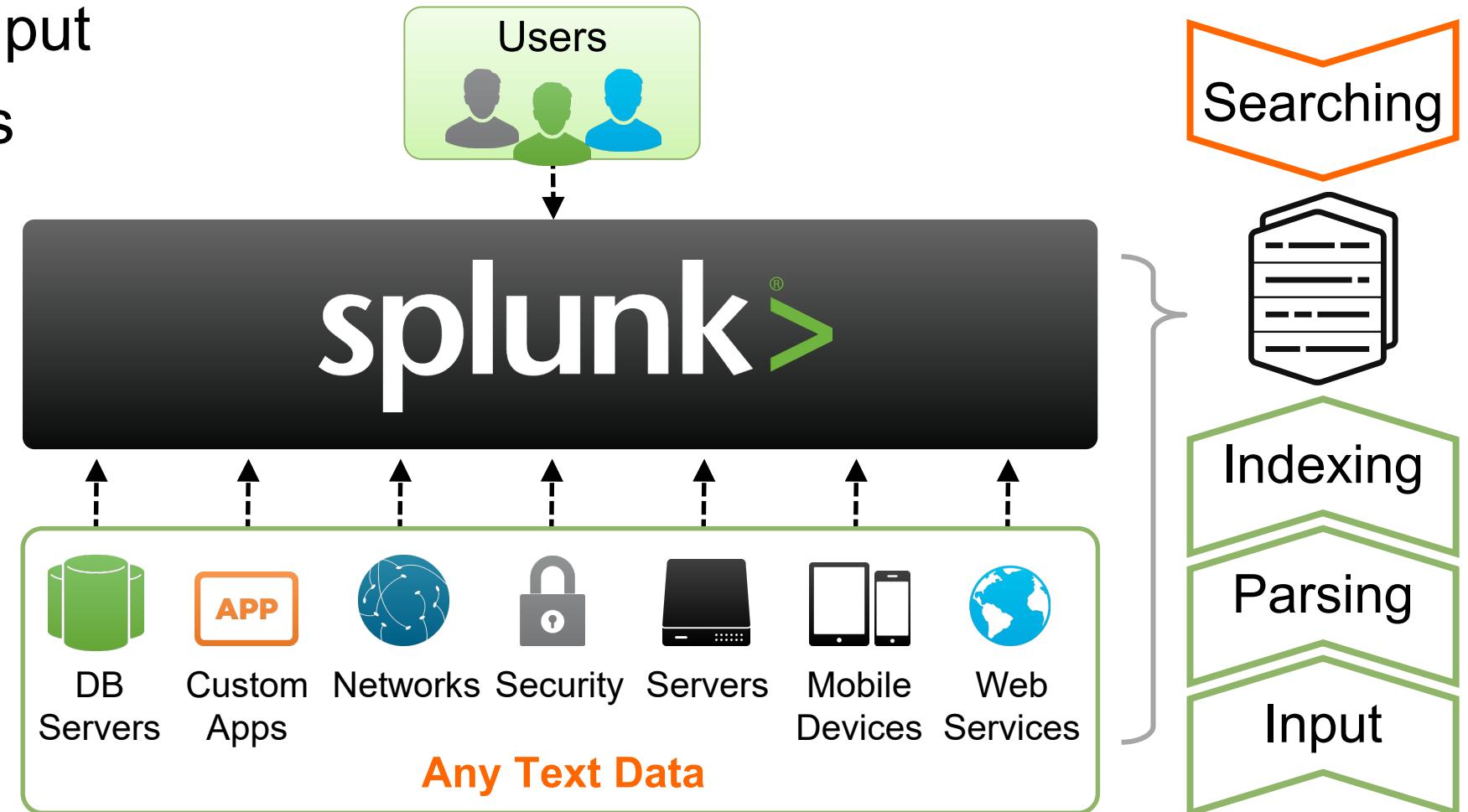
# Module Objectives

---

- Provide an overview of Splunk
- Identify Splunk Enterprise components
- Identify the types of Splunk deployments
- Describe the Splunk System Administrator role
- List the steps to install Splunk
- Use Splunk CLI commands
- Enable the Monitoring Console (MC)

# Splunk Overview

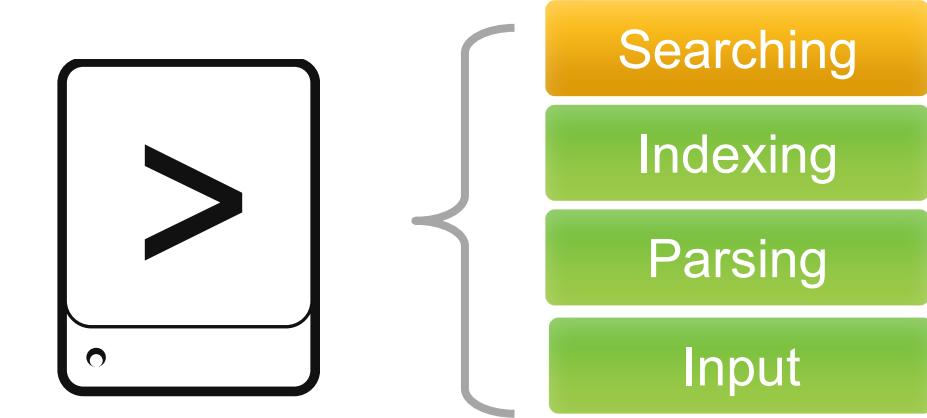
- Splunk can be deployed in a variety of configurations
- Scales from a single server to a distributed infrastructure
  - Accepts any text data as input
  - Parses the data into events
  - Stores events in indexes
  - Searches and reports
  - Authenticates users



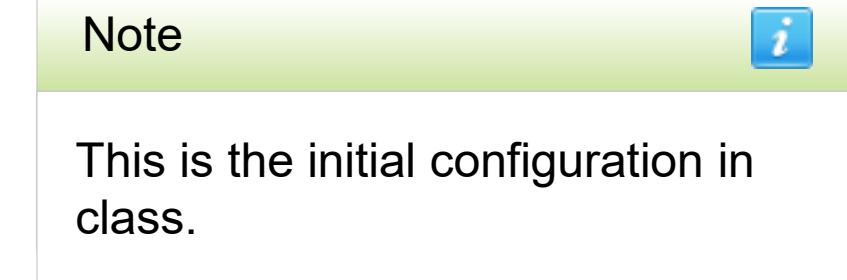
Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Splunk Deployment – Standalone

- Single server
  - All functions in a single instance of Splunk
  - For testing, proof of concept, personal use, and learning
  - This is what you get when you download Splunk and install with default settings



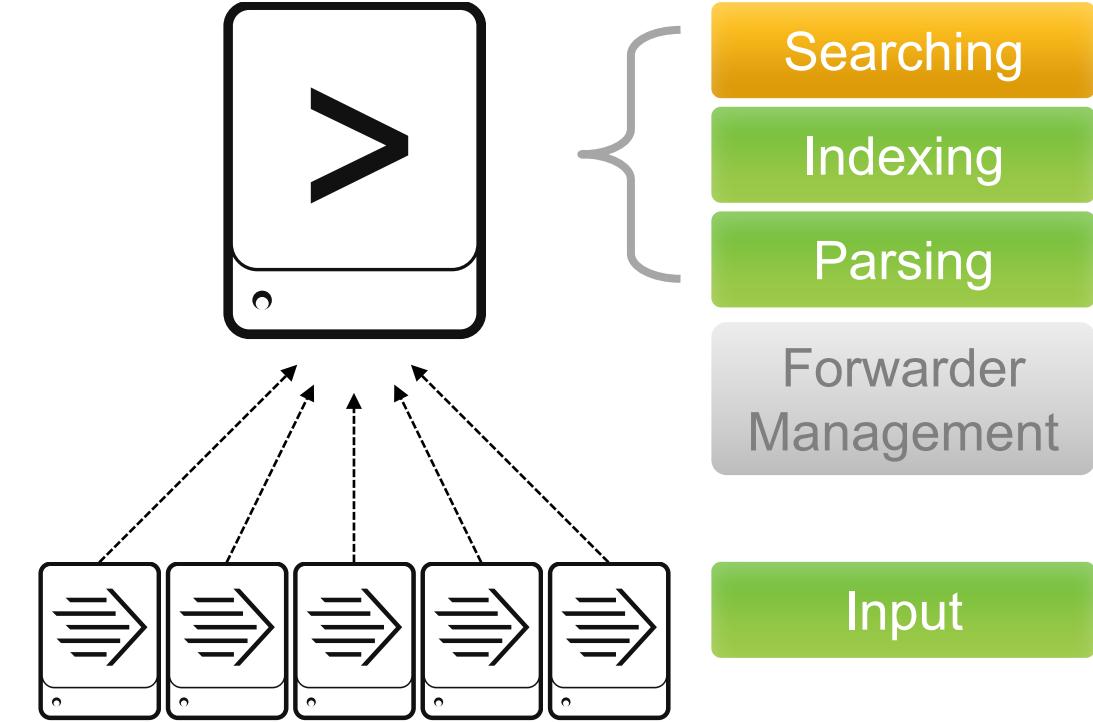
- Recommendation
  - Have at least one test/development setup at your site



Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Splunk Deployment – Basic

- Splunk server
  - Similar to server in standalone configuration
  - Manage deployment of forwarder configurations
- Forwarders
  - Forwarders collect data and send it to Splunk servers
  - Install forwarders at data source (usually production servers)



Note

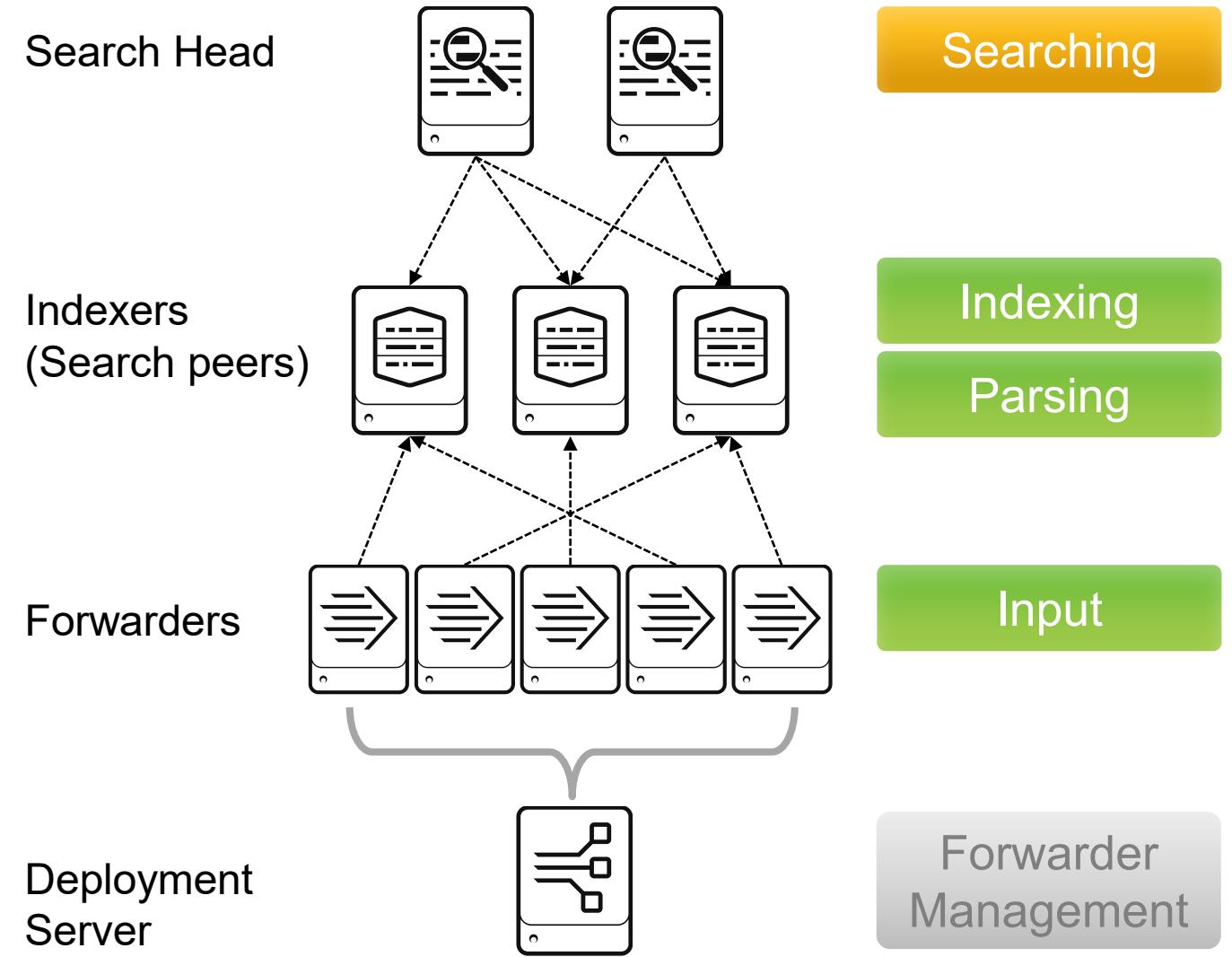
Your lab environment will evolve to include a separate forwarder.

# Splunk Deployment – Distributed

- Splunk can be distributed and scaled in a variety of ways
  - More indexers to handle more inputs
  - More indexers AND search heads to handle more searching
- Manage forwarder configurations from a dedicated Deployment Server

Note

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



# Splunk Core Components and Processes

Searching

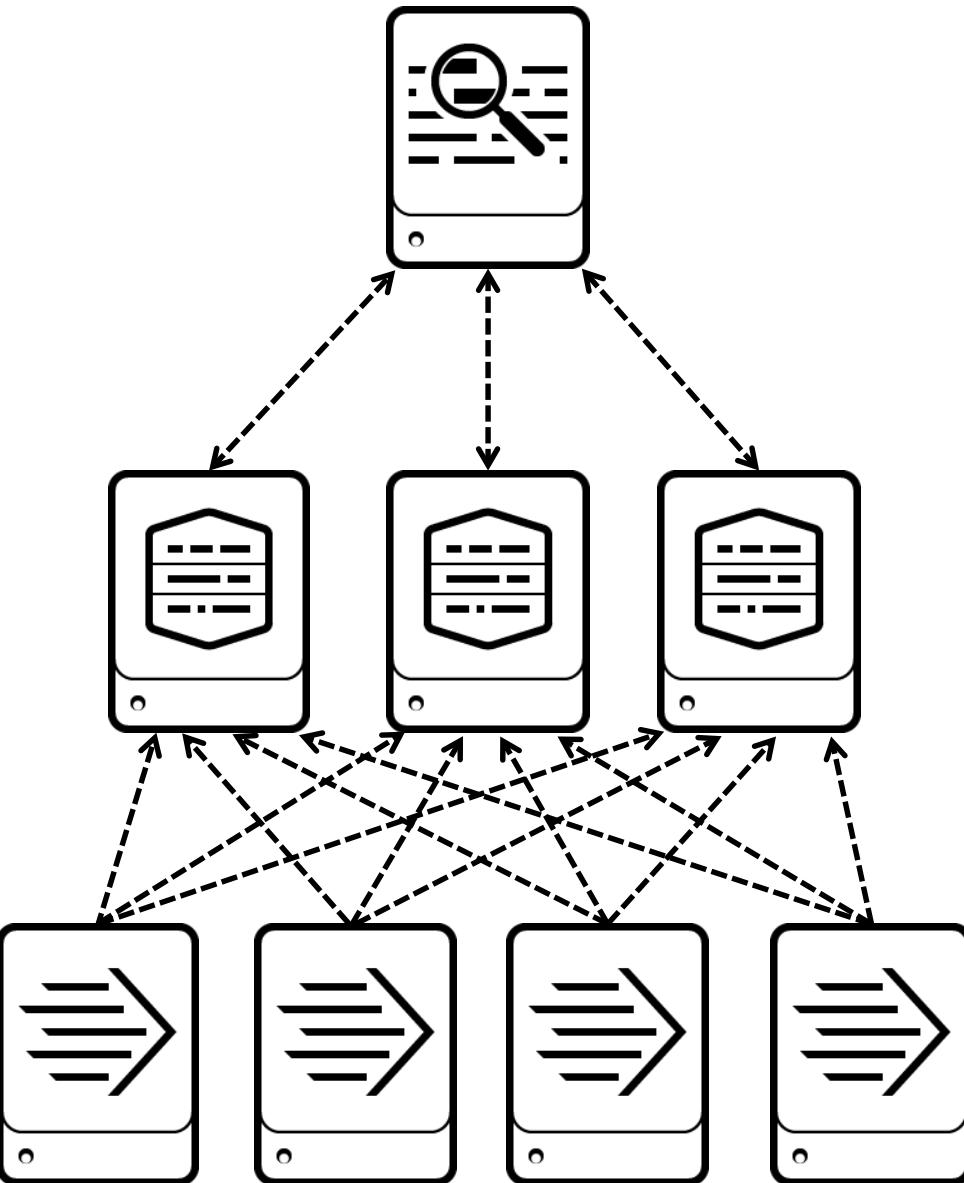


- Allow users to submit search requests using SPL
- Distribute search requests to the indexers
- Consolidate results and render visualizations of results
- Search time knowledge objects are stored on the search heads  
Examples include: field extractions, alerts, and dashboards

Indexing

Parsing

Inputs



- Reside on dedicated machines
- Receive, index, and store incoming data from forwarders
- Search data in response to requests received from the search heads

- Splunk instances that monitor configured inputs and forward the data to the index
- Best practice data collection method
- Requires minimal resources and typically installed on the machines that produce the data

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Splunk Installation Overview

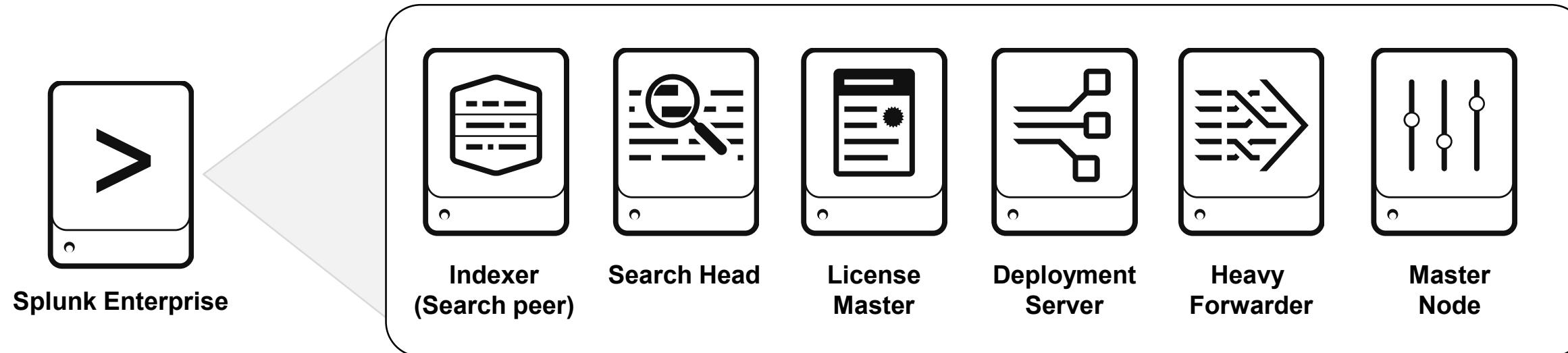
---

- What software do you install?
- Pre-installation checklist
  - Start-up account
  - Time synchronization
  - Splunk ports
  - Linux setting recommendations
  - Server hardware recommendations
- Installation
  - Splunk directory structure
- Post-installation configuration
  - Run Splunk at boot
  - Configure system settings
  - Optionally, enable Monitoring Console

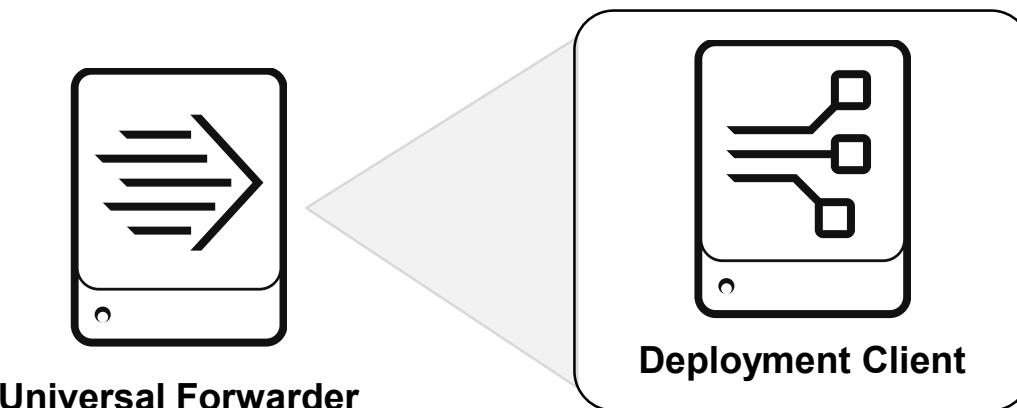
Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# What Software Do You Install?

- Included in the Splunk Enterprise software package



- Included in the Universal Forwarder software package



Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Installation

---

- Download Splunk Enterprise from [www.splunk.com/download](http://www.splunk.com/download)
- Installation: (as account running Splunk)
  - \*NIX – un-compress the `.tar.gz` file in the path you want Splunk to run from
    - ▶ Also available as `rpm`, `deb`
  - Windows – execute the `.msi` installer and follow the wizard steps
- Complete installation instructions at:  
[docs.splunk.com/Documentation/Splunk/latest/Installation/Chooseyourplatform](http://docs.splunk.com/Documentation/Splunk/latest/Installation/Chooseyourplatform)
- After installation:
  - Splunk starts automatically on Windows
  - Splunk must be manually started on \*NIX until **boot-start** is enabled

# Run Splunk at Boot – \*NIX

- Splunk on \*NIX does not auto-start at boot time (default)
- Run as root if allowed :

```
# ./splunk enable boot-start
```

- This modifies the \*NIX boot-up configuration
  - Modifies **/etc/init.d** depending on your \*NIX flavor
- If cannot run as root, pass the **-user** parameter

```
# ./splunk enable boot-start -user bob
```

- On **systemd** distributions, you can configure Splunk to let **systemd** control it

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

# Run Splunk at Boot – Windows

---

- On Windows, the installer configures Splunk software to start at machine startup
  - Runs as **splunkd** service and starts child processes
  - The service starts and stops like any Windows services
  - Can be disabled if needed

# Startup Account

---

- **Best practice:** Do not run Splunk as *super-user*
  - For example, **root** on \*NIX, **administrator** on Windows
- Create a user account that is used to run Splunk
  - For input, Splunk must be able to access data sources
    - ▶ On \*NIX, `/var/log` is not typically open to non-root accounts
  - On \*NIX, non-root accounts cannot access ports < 1024
  - On Windows
    - ▶ Use a domain account if Splunk has to connect to other servers
      - ▶ Otherwise, use a local machine account that can run services
  - Make sure the Splunk account can access scripts used for inputs and alerts

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Time Synchronization

---

- **Best practice:** Use a time synchronization service such as NTP
- Splunk searches depend on accurate time
  - Correct event timestamping is essential
- It is imperative that your Splunk indexer and production servers have standardized time configuration
  - Clock skew between hosts can affect search results

# Splunk Default Ports

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

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Linux Setting Recommendations

- Increase `ulimit` settings
  - The following OS parameters need to be increased to allow for a large number of buckets/forwarders/users

[docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/ulimitErrors](https://docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/ulimitErrors)

core file size	ulimit -c 1073741824 (1 GB) (unlimited)
open files	ulimit -n 48 x default (48 x 1024 = 49,152) (65536)
max user processes	ulimit -u 12 x default (12 x 1024 = 12,288) (258048)

- Turn Transparent Huge Pages (THP) off on Splunk Enterprise servers

[docs.splunk.com/Documentation/Splunk/latest/ReleaseNotes/SplunkandTHP](https://docs.splunk.com/Documentation/Splunk/latest/ReleaseNotes/SplunkandTHP)

# Reference Servers Hardware

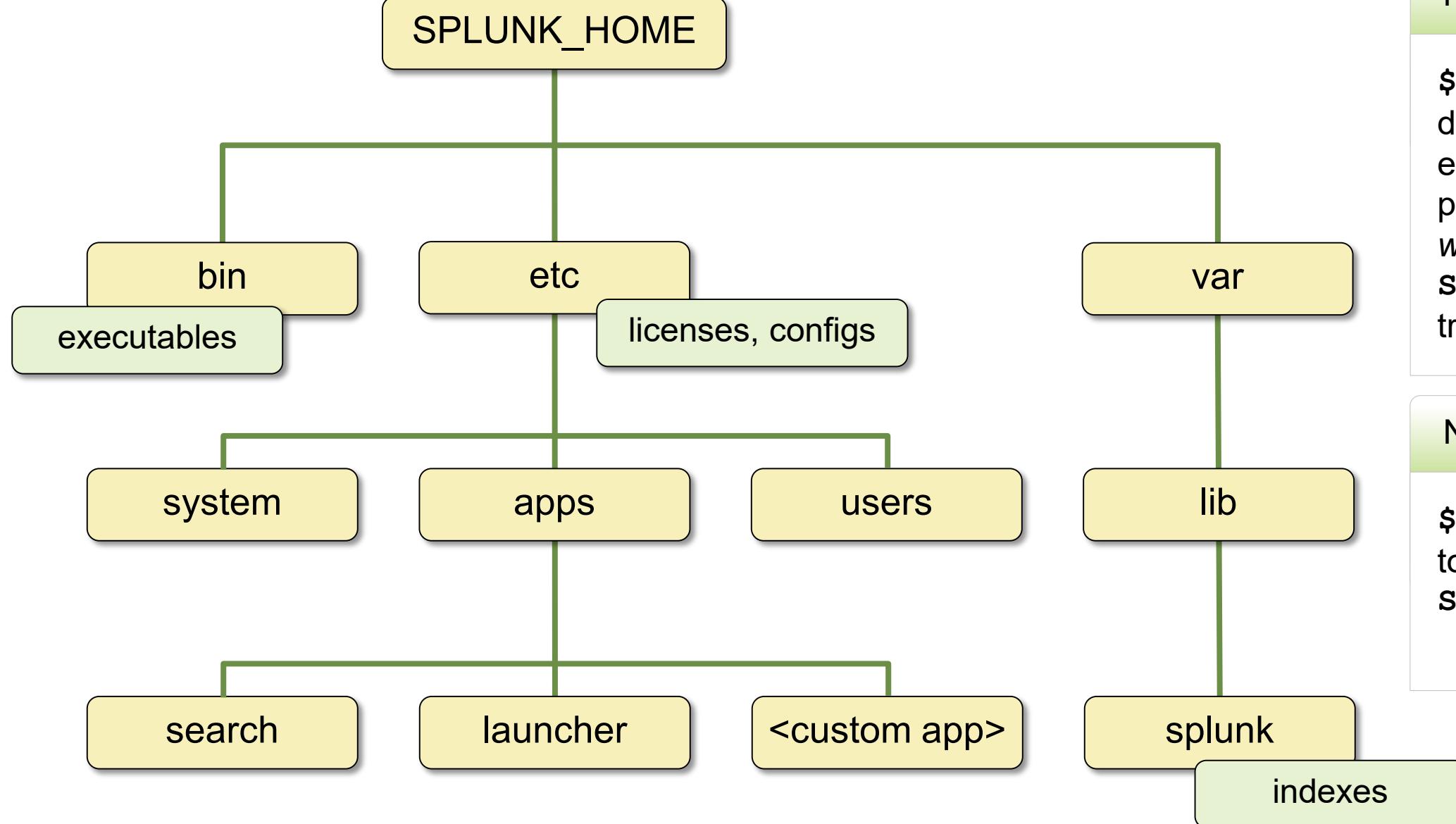
	<b>Indexer</b>	<b>Search Head</b>
OS		Linux or Windows 64-bit distribution
Network		1Gb Ethernet NIC Optional second NIC for a management network
Memory		12 GB RAM
CPU	Intel 64-bit chip architecture <b>12 CPU cores</b> Running at 2+ GHz	Intel 64-bit chip architecture <b>4 CPUs, quad-core per CPU</b> Running at 2+ GHz
Disk	Disk subsystem capable of 800 IOPS RAID 10	2 x 10K RPM 300GB SAS drives - RAID 1

- Hardware requirements and sizing are discussed in detail in Architecting and Deploying Splunk class

[docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware](https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware)

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Splunk Directory Structure



## Note



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

## Note



`$SPLUNK_DB` is used in this training to refer to `SPLUNK_HOME/var/lib/splunk`

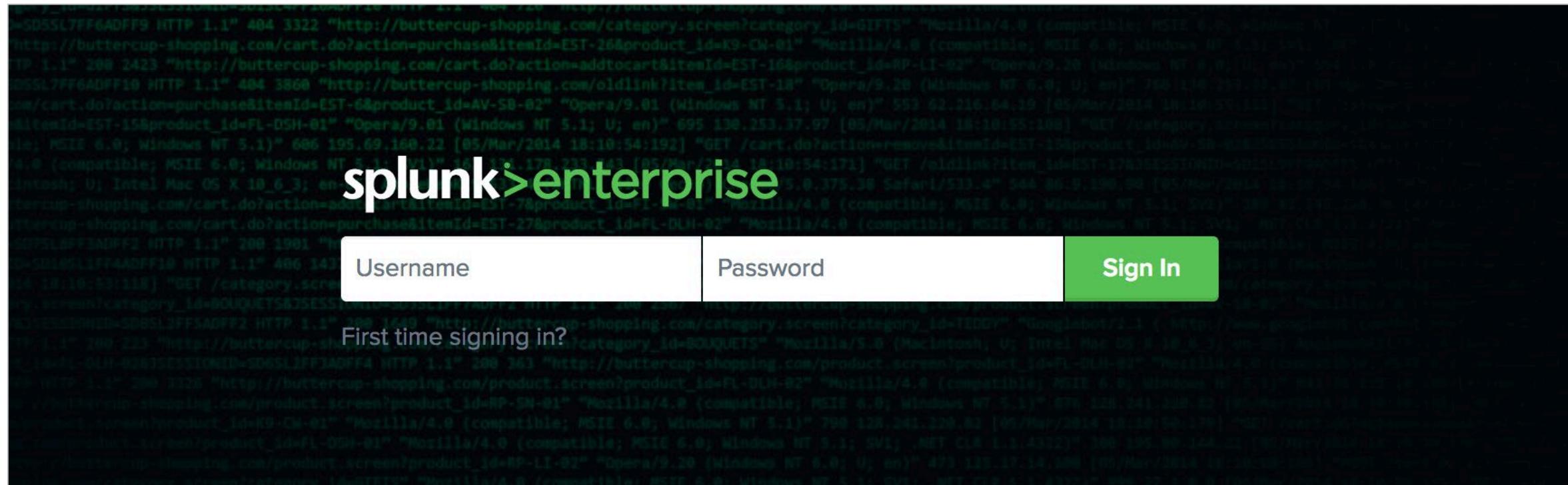
# splunkd

---

- 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

# Splunk Web

- Splunk Web is browser-based user interface
  - Provides both a search and management front end for **splunkd** process
- Runs on port 8000 by default
  - **http://<server\_name>:<port>**



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Splunk Web – Server Settings

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

The screenshot shows the Splunk Web interface. At the top is a dark navigation bar with icons for Admin, Messages, Settings (which has a red circle with the number 1), Activity, Help, and Find. Below the navigation bar is a light-colored sidebar with three main sections: Add Data, Explore Data, and Monitoring Console. The Add Data section has an icon of a database and a plus sign, and contains links for Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; and All configurations. The Explore Data section has an icon of a magnifying glass over a grid, and contains links for Indexer clustering; Forwarder management; Distributed search; and Access controls. The Monitoring Console section has an icon of three vertical bars, and contains links for Server controls; Instrumentation; and Licensing. 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; Distributed search); and USERS AND AUTHENTICATION (Access controls).

Used to set server configuration and server options

## Server settings

Manage system settings including ports, host name, index path, and more.

3 **General settings**

Login background

Email settings

Server logging

Deployment client

Search preferences

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Describing General Settings

- ① Identifies this server to other Splunk servers
- ② Identifies the installation path **SPLUNK\_HOME**
- ③ Identifies the splunkd port
- ④ Identifies the IP address used for SSO authentication configurations

**General settings**  
[Server settings](#) » General settings

1	Splunk server name *	splunk_server
2	Installation path	/opt/splunk
3	Management port *	8089
4	SSO Trusted IP	<p>Port that Splunk Web uses to communicate with the splunkd process. This port is also used for distributed search.</p> <p>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.</p>

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Describing General Settings – Splunk Web

- ⑤ Enables Splunk Web
- ⑥ Enables HTTPS for Splunk Web
- ⑦ Identifies the Splunk Web port
- ⑧ **App server ports** (8065) is the python-based application server to listen on. Set to "0" only if you want to run Splunk Web in legacy mode (not compatible with SHC)
- ⑨ Sets the Splunk Web session timeout

**Splunk Web**

⑤	Run Splunk Web	<input checked="" type="radio"/> Yes	<input type="radio"/> No
⑥	Enable SSL (HTTPS) in Splunk Web?	<input type="radio"/> Yes	<input checked="" type="radio"/> No
⑦	Web port *	8000	
⑧	App server ports	8065	
⑨	Session timeout *	1h	

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

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

# Describing General Settings – Index/KV Store

- 10 Default host name which is the default value for the host field for inputs forwarded (indexed) from this server
- 11 Identifies the path to the existing indexes (read-only in UI)
- 12 Sets the minimum free disk space setting the datastore location can fall before Splunk stops indexing
- 13 Defines the port used by the KV Store to communicate with splunkd

Index settings	
10	Default host name ip-10-0-0-201 Sets the host field value for all events coming from this server.
11	Path to indexes <code>/opt/splunk/var/lib/splunk</code>
12	Pause indexing if free disk space (in MB) falls below * 5000
KV Store	
13	Port * 8191 Port that splunkd uses to connect to the KV Store server.

# Restarting the Server from Splunk Web

The screenshot illustrates the steps to restart the Splunk server:

- Step 1:** In the top navigation bar, click the **Messages** icon (Admin dropdown with a red circle containing '1'). A message box appears: **Splunk must be restarted for changes to take effect.** **Click here to restart from Server controls.**
- Step 2:** Click the link in the message box: **Click here to restart from Server controls.**
- Step 3:** On the **Server controls** page, click the **Restart Splunk** button (green button with a red circle containing '3').

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

You can also restart by selecting **Settings > Server controls** or from the CLI. (`splunk restart`)

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# The Splunk Command Line Interface (CLI)

- **splunk** is an executable command in the **bin** directory
  - Same syntax is used on all supported platforms

Command	Operation
<b>splunk help</b>	Display a usage summary
<b>splunk help &lt;object&gt;</b>	Display the details of a specific object
<b>splunk [start   stop   restart]</b>	Manages the Splunk processes
<b>splunk start --accept-license</b>	Automatically accept the license without prompt
<b>splunk status</b>	Display the Splunk process status
<b>splunk show splunkd-port</b>	Show the port that the <b>splunkd</b> listens on
<b>splunk show web-port</b>	Show the port that Splunk Web listens on
<b>splunk show servername</b>	Show the servername of this instance
<b>splunk show default-hostname</b>	Show the default host name used for all data inputs

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Monitoring Console (MC)

- Splunk collects a lot of data about itself
- MC is a Splunk admin-only app used to monitor and investigate Splunk performance, resource usage, and more

The image shows two screenshots of the Splunk Monitoring Console (MC) interface. The left screenshot displays the navigation bar with options like Admin, Messages, Settings, Activity, Help, and Find. Below the navigation is a sidebar with links for Add Data, Explore Data, and Monitoring Console. A green arrow points from the 'Monitoring Console' link in the sidebar to the right screenshot. The right screenshot shows the main monitoring dashboard for Splunk Enterprise Server 7.1.0. It features a large index rate metric of 1.47 KB/s, concurrent searches (0 results found), and CPU usage at 1.70%. A note box on the right states: "You will use MC to monitor your activities as you learn more about Splunk components."

Generated for YongHyeok Jeong (yh.jeong@time-gate.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**
  - You must **Apply Changes** to initialize the MC and after any change

The screenshot shows the Splunk Enterprise 7.3 System Administration interface. The top navigation bar includes links for Overview, Health Check, Indexing, Search, Resource Usage, Forwarders (highlighted with a red circle 1), Settings (highlighted with a red circle 1), Run a Search, Admin, Messages, Activity, Help, Find, and a search bar. A dropdown menu from the Settings link is open, showing options: General Setup (highlighted with a red circle 2), Forwarder Monitoring Setup, Alerts Setup, Overview Preferences, and Health Check Items. On the left, a 'Setup' sidebar displays the current topology of the deployment and offers Mode selection between Standalone (selected) and Distributed. The main content area shows 'This instance' details for 'splunkXX'. A callout box highlights the 'Server roles' column, which lists 'Indexer', 'License', 'Master', and 'Search Head'. A note states: 'Only available in distributed mode.' A yellow callout box labeled 'The default server roles' points to the 'Server roles' column. In the top right, there are 'Reset All Settings' and 'Apply Changes' buttons (highlighted with a red circle 3).

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Enabling MC Platform Alerts

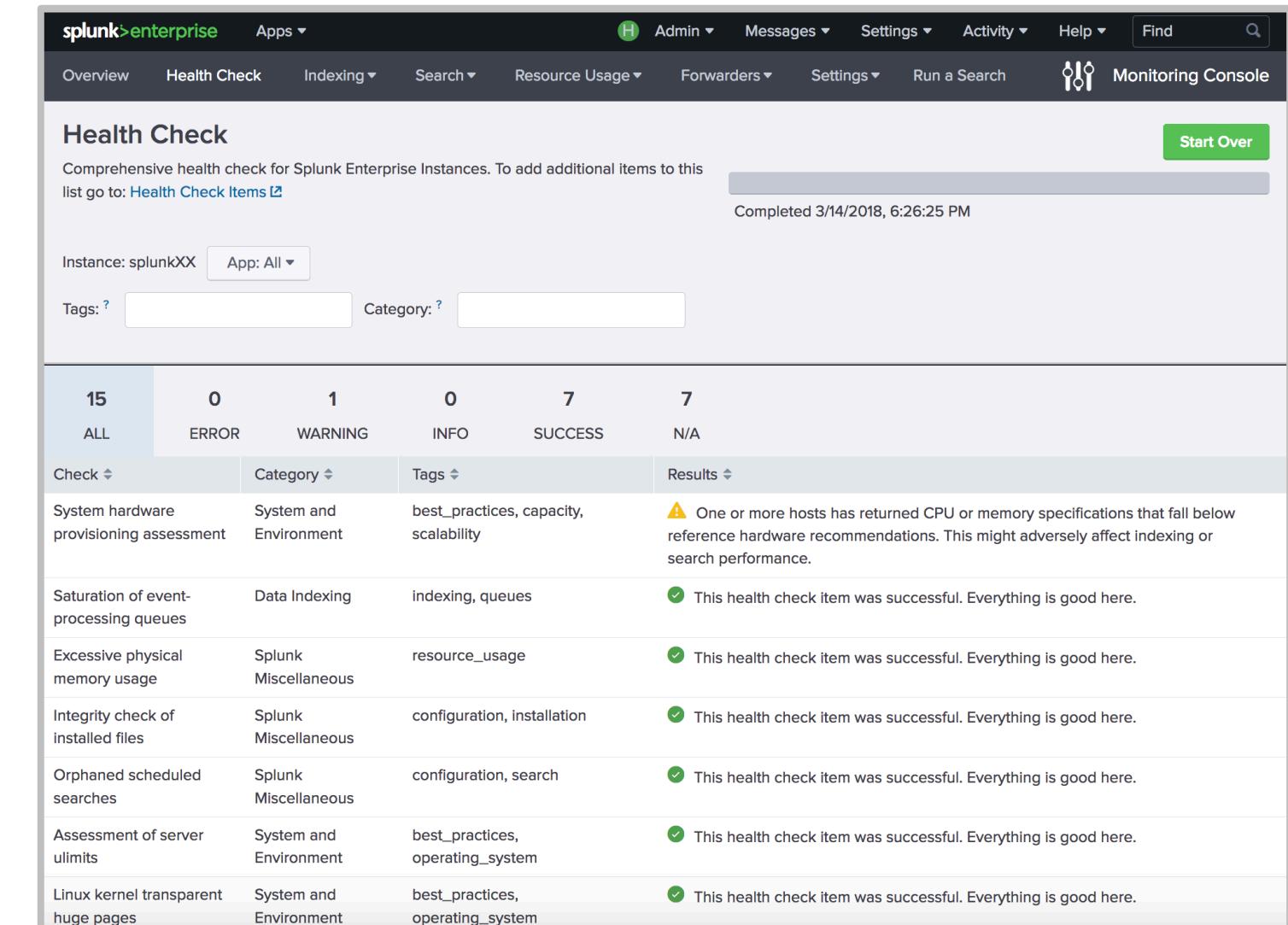
- Effective operation of your Splunk environment is timely identification and notification of critical conditions
  - Any item over 80% mark can't be good
- MC **Alerts Setup** provides a number of preconfigured platform alerts
  - Platform alerts are disabled by default
  - Tweak parameters such as alert schedule, suppression time, and alert actions

The screenshot shows the Splunk Enterprise Monitoring Console interface. The top navigation bar includes links for Admin, Messages, Settings, Activity, Help, Find, and Monitoring Console. A context menu is open over the 'Alerts Setup' link in the top right, showing options like General Setup, Forwarder Monitoring Setup, Alerts Setup (which is selected and highlighted in blue), Overview Preferences, and Health Check Items. The main content area is titled 'Platform Alerts Setup' and displays a list of 8 alerts. Each alert has a name, a brief description, and status columns for Edit, Advanced Edit, Enable, and Status (all currently set to Disabled). The alerts listed are:

- DMC Alert - Abnormal State of Indexer Processor
- DMC Alert - Critical System Physical Memory Usage
- DMC Alert - Expired and Soon To Expire Licenses
- DMC Alert - Missing forwarders
- DMC Alert - Near Critical Disk Usage
- DMC Alert - Saturated Event-Processing Queues
- DMC Alert - Search Peer Not Responding
- DMC Alert - Total License Usage Near Daily Quota

# MC Health Check Items

- In addition to platform alerts, MC comes with preconfigured health checks
- Each health check is an ad hoc search that runs sequentially
  - **Monitoring Console > Health Check**
- Health checks can be disabled, modified, created, and exported
  - **Settings > Health Check Items**



The screenshot shows the Splunk Enterprise Monitoring Console interface. The top navigation bar includes links for Overview, Health Check (which is currently selected), Indexing, Search, Resource Usage, Forwarders, Settings, and Activity. A search bar and a 'Find' button are also present. The main content area is titled 'Health Check' and displays a summary of the results: 15 total items, 0 errors, 1 warning, 0 info, 7 successes, and 7 N/A items. Below this, a table lists individual health check items with their status, category, tags, and a detailed description of the result.

Check	Category	Tags	Results
System hardware provisioning assessment	System and Environment	best_practices, capacity, scalability	<span style="color: orange;">⚠ One or more hosts has returned CPU or memory specifications that fall below reference hardware recommendations. This might adversely affect indexing or search performance.</span>
Saturation of event-processing queues	Data Indexing	indexing, queues	<span style="color: green;">✓ This health check item was successful. Everything is good here.</span>
Excessive physical memory usage	Splunk Miscellaneous	resource_usage	<span style="color: green;">✓ This health check item was successful. Everything is good here.</span>
Integrity check of installed files	Splunk Miscellaneous	configuration, installation	<span style="color: green;">✓ This health check item was successful. Everything is good here.</span>
Orphaned scheduled searches	Splunk Miscellaneous	configuration, search	<span style="color: green;">✓ This health check item was successful. Everything is good here.</span>
Assessment of server ulimits	System and Environment	best_practices, operating_system	<span style="color: green;">✓ This health check item was successful. Everything is good here.</span>
Linux kernel transparent huge pages	System and Environment	best_practices, operating_system	<span style="color: green;">✓ This health check item was successful. Everything is good here.</span>

# More Resources

---

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

# Module 1 Knowledge Check

---

- Which installer will you use to install the Search Head?
- True or False. When you install Splunk on a Windows OS, 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 a Windows OS, you also have to configure the boot-start?

False. You only need to do that on a Linux installation

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

True.

# Lab Exercise 1 – Configure Splunk

---

**Time:** 25 minutes

**Tasks:**

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

# Module 2: License Management

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Identify license types
- Describe license violations
- Add and remove licenses

# Splunk License Types

---

- **Enterprise trial license**
  - Downloads with product
  - Features same as Enterprise except for 500 MB per day limit
  - Only valid for 60 days, after which one of the other 3 license types must be activated
  - **Sales trial license** is a trial Enterprise license of varying size and duration
- **Enterprise license**
  - Purchased from Splunk
  - Full functionality for indexing, search head, deployment server, etc.
  - Sets the daily indexing volume
  - No-enforcement license, allows users to keep searching even if you are in a license violation period

# Splunk License Types (cont.)

---

- **Free license**
  - Disables alerts, 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
- Splunk license comparison:

[https://www.splunk.com/en\\_us/products/splunk-enterprise/free-vs-enterprise.html](https://www.splunk.com/en_us/products/splunk-enterprise/free-vs-enterprise.html)

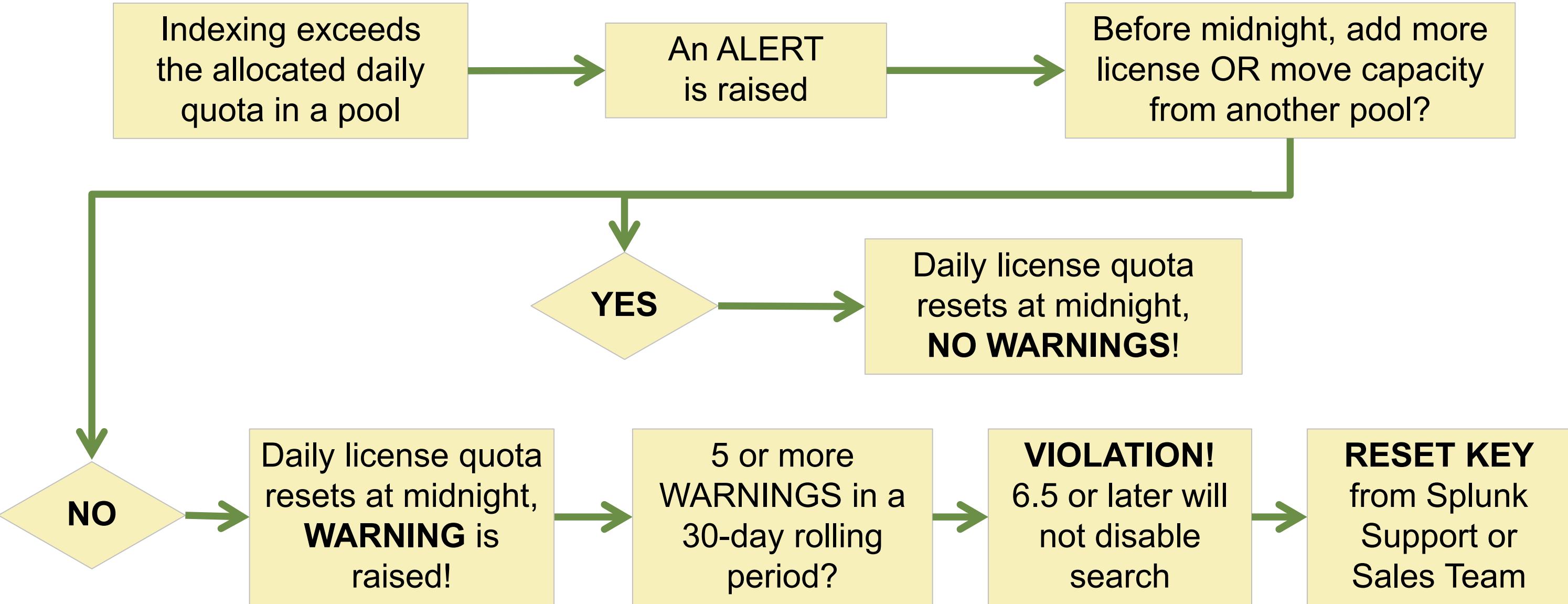
Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# License Warnings and Violations

---

- If the indexing exceeds the allocated daily quota in a pool, an alert is raised in Messages (pool warning) on any page in Splunk Web
  - The daily license quota resets at midnight
- 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*
- Splunk Enterprise 6.5.0 and later provides warnings but it does not disable search during the violation period
  - Prior versions of Splunk would disable search

# License Warnings and Violations (cont.)



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

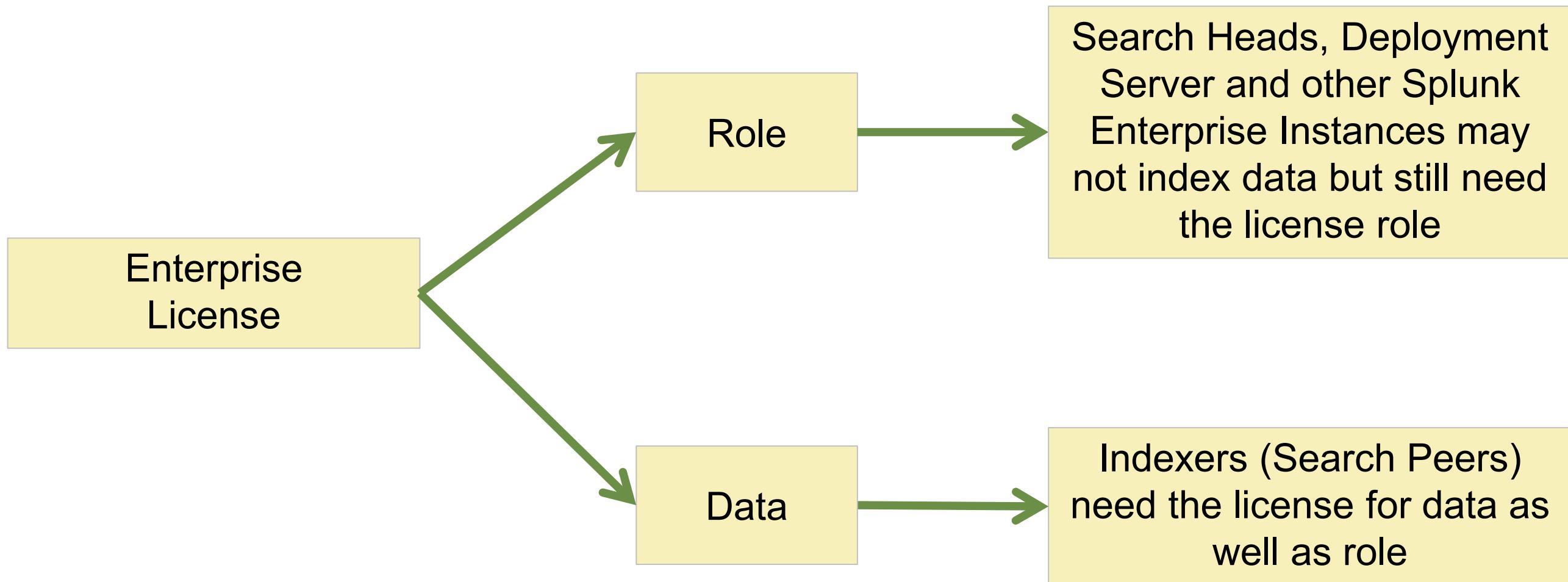
# What Counts As Daily License Quota?

---

- All data from all sources that is indexed
  - It is the data (full size) that flows through the parsing pipeline, per day
  - It is not the amount of storage used by the indexes
- What does not count against your license daily quota?
  - Replicated data (Index Clusters)
  - Summary indexes
  - Splunk internal logs (\_internal, \_audit, etc. indexes)
  - Structural components of an index (metadata, tsidx, etc.)
- Metrics data counts against a license at a fixed 150 bytes per metric event
  - Draws from the same license quota as event data

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Roles and Data



# 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

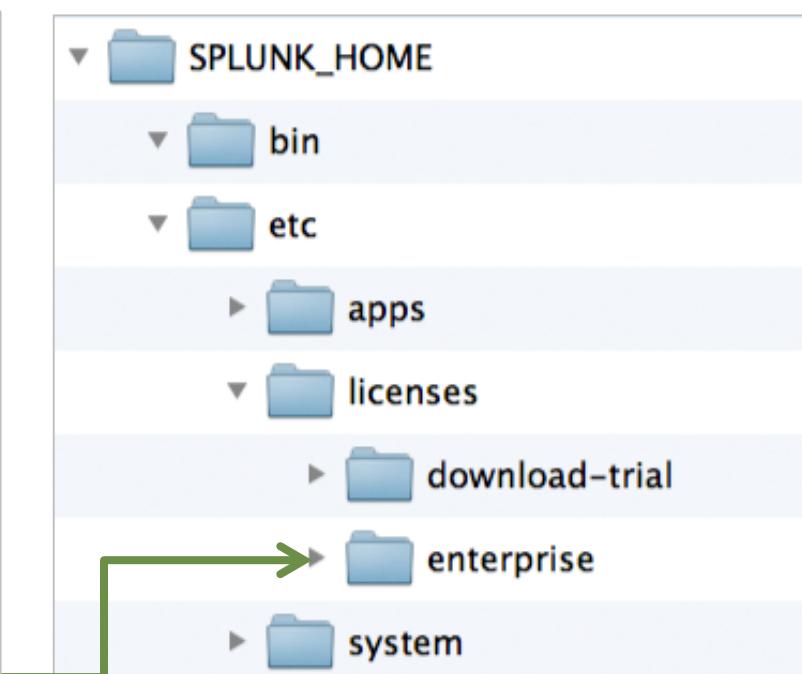
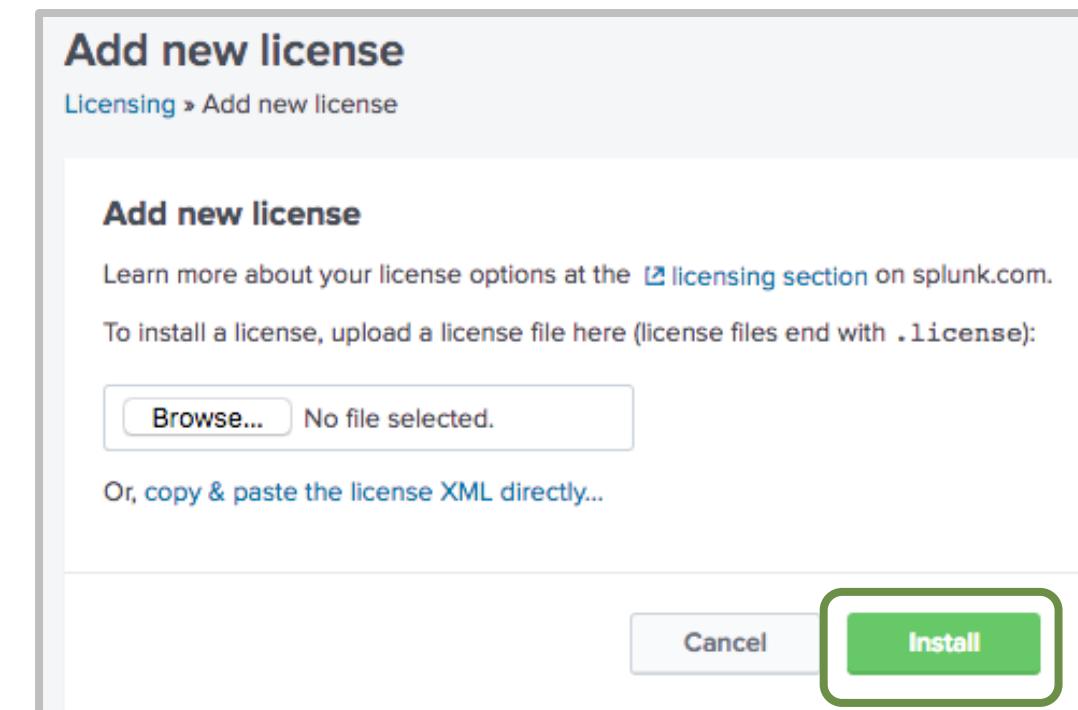
The screenshot shows the Splunk Licensing interface. At the top, it says "This server is acting as a master license server" with a "Change to slave" button. A red circle labeled "1" is over the "Change to slave" button. Below that, it says "Enterprise license group" with a "Change license group" button. A red circle labeled "2" is over the "Change license group" button. There are "Add license" and "Usage report" buttons. A red circle labeled "3" is over the "Usage report" button. Under "Alerts", there is a section for "Current" with two items: "1 pool warning reported by 1 indexer" and "1 pool quota overage warning reported by 1 indexer". A red circle labeled "4" is over the "Learn more" link for the first item. Under "Permanent", there is one item: "2 pool quota overage warnings reported by 1 indexer" (last updated 19 hours ago). A red circle labeled "5" is over the "Learn more" link for this item. Below that, the "Splunk Enterprise Sales Trial stack" is shown with its details: Licenses (Splunk Enterprise Sales Trial), Volume (200 MB), Expiration (Apr 14, 2018 1:50:34 PM), and Status (valid). A red circle labeled "6" is over the "Edit | Delete" link for the stack.

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Adding a License

- Can use CLI or Splunk Web (upload or copy/paste)
  - License group change requires a restart
- Licenses are stored under  
**SPLUNK\_HOME/etc/licenses**
- Multiple licenses of the same type are stacked  
(added together)

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



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Viewing Alerts

**Alerts**

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

**Current**

- 1 pool warning reported by 1 indexer      Correct by midnight to avoid violation [Learn more](#)
- 1 pool quota overage warning reported by 1 indexer      Correct by midnight to avoid violation [Learn more](#)

**Permanent**

- 2 pool quota overage warnings reported by 1 indexer      16 hours ago



## Pool quota overage alerts (3)

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](#)

Severity	Time	Message	Indexer	Pool	Stack	Category
●	Correct by midnight to avoid violation <a href="#">Learn more</a>	This pool is over poolsz=157286400 bytes, please correct before midnight		auto_generated_pool_enterprise	enterprise	pool_over_quota
●	Mar 30, 2018 12:00:00 AM (16 hours ago)	This pool has exceeded its configured poolsize=157286400 bytes. A warning has been recorded for all members	ip-10-0-0-203	auto_generated_pool_enterprise	enterprise	pool_over_quota
●	Mar 24, 2018 12:00:00 AM (6 days ago)	This pool has exceeded its configured poolsize=157286400 bytes. A warning has been recorded for all members	ip-10-0-0-203	auto_generated_pool_enterprise	enterprise	pool_over_quota

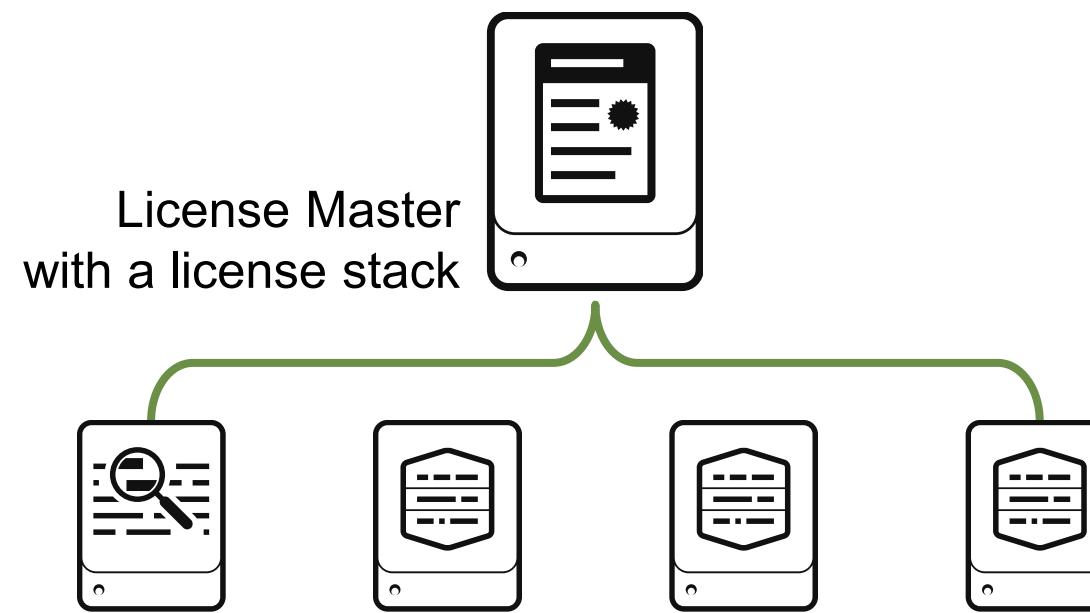
[Show messages for all alert types](#)

[« return to overview](#)

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Change to Slave

Change an instance to slave by entering the master license server URI



**Change master association**

This server, **myindexer2**, is currently acting as a master license server.

Designate this Splunk instance, **myindexer2**, 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**

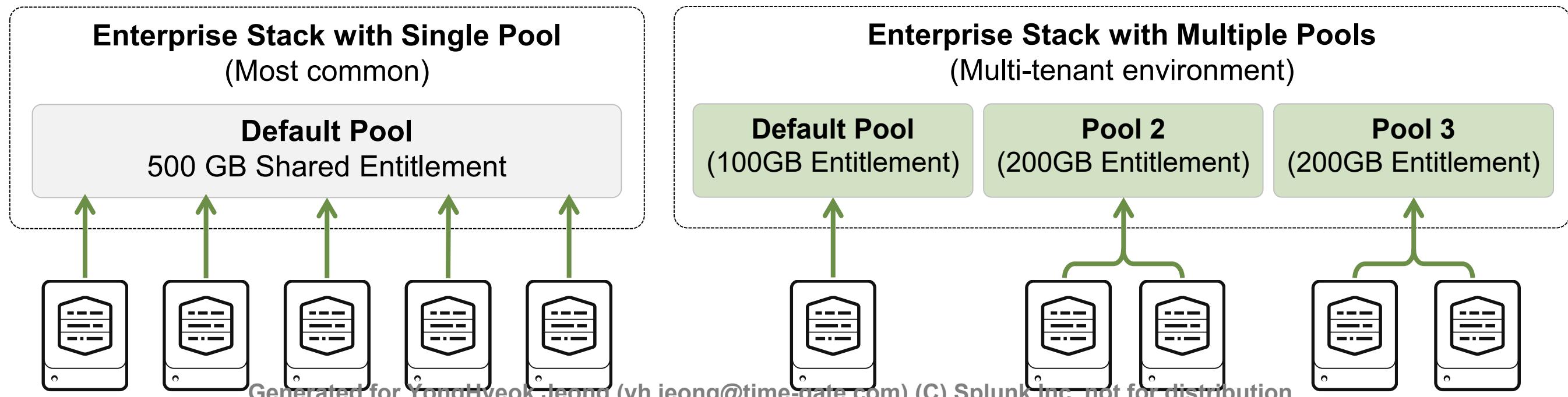
For example: [https://splunk\\_license\\_server:8089](https://splunk_license_server:8089)  
Use https and specify the management port.

**Cancel** **Save**

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# License Pooling

- **Pools** allow licenses to be subdivided and assigned to a group of indexers
  - Can be created for a given stack
  - Warnings and violations occur per pool
- Example: Master has a stack for a total 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

The screenshot displays two main panels of the Splunk Enterprise interface. On the left, the 'Splunk Enterprise Sales Trial stack' is shown, listing a single license entry: 'Splunk Enterprise Sales Trial' with a volume of 200 MB and an expiration date of Apr 14, 2018 1:50:34 PM, marked as 'valid'. Below this, the 'Effective daily volume' is listed as 200 MB. On the right, the 'Platform Alerts Setup' page is displayed, showing two alerts: 'DMC Alert - Expired and Soon To Expire Licenses' and 'DMC Alert - Total License Usage Near Daily Quota'. A context menu is open over the first alert, with 'General Setup' selected. Arrows point from the highlighted license row in the license stack to the 'Edit' and 'Delete' buttons in the pool section, and from the 'Edit' button in the pool section to the 'Edit' button in the alert context menu.

Generated for YongHyeok Jeong (yh.jeong@time-gate.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 (or set as a slave to a License Master with an Enterprise License) even though you have not configured 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 (or set as a slave to a License Master with an Enterprise License) even though you have not configured any inputs.

**True.**

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

**False. If the indexing exceeds the allocated daily quota in a pool, an alert is raised. If it is not fixed by midnight then the alert 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.**

# Lab Exercise 2 – Splunk License Management

---

**Time:** 10 minutes

**Tasks:**

- Add licenses
- Modify the license pool
- Enable MC Alert

# Module 3: Splunk Apps

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

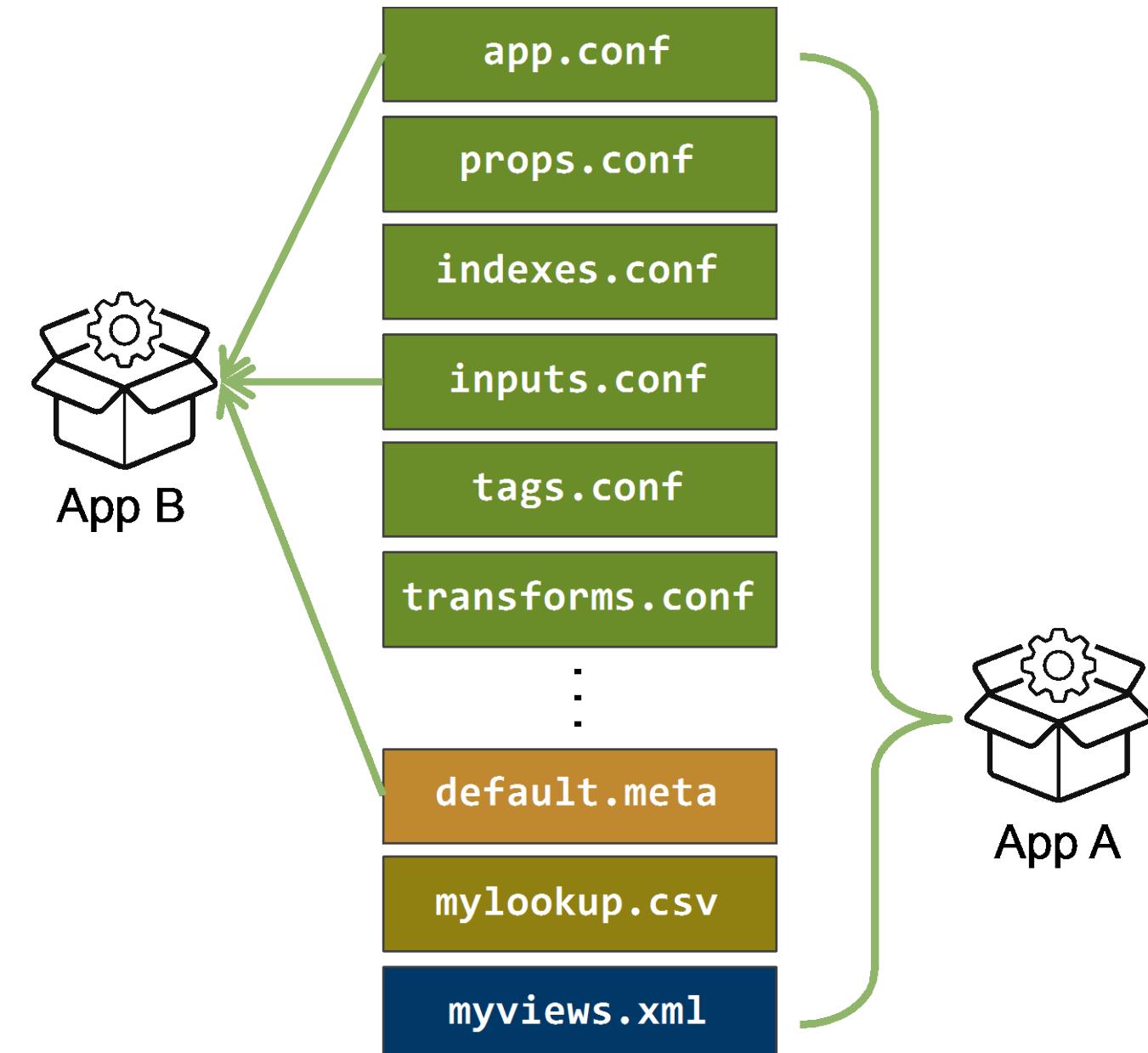
# Module Objectives

---

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

# What is an App?

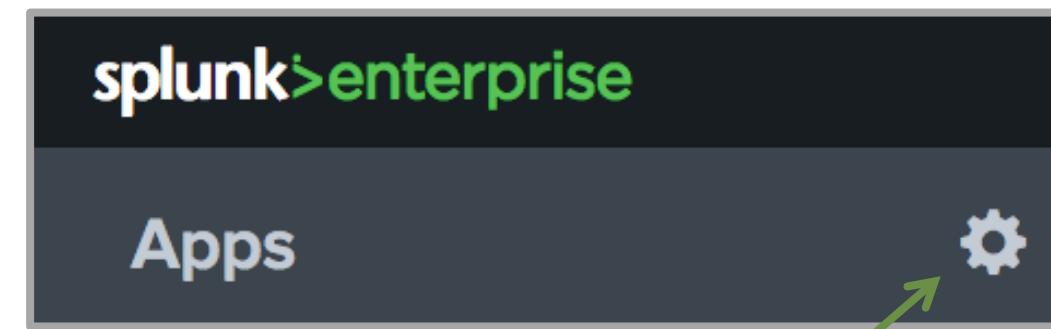
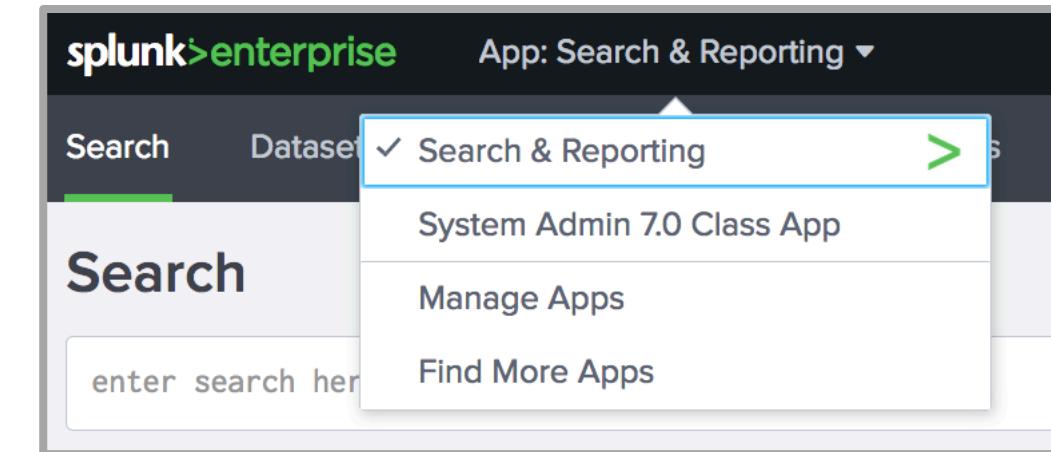
- An app is a collection of:
  - Configuration files
  - Scripts, web assets, etc.
- Most apps are focused on:
  - A specific type of data from a vendor, operating system, or industry
  - A specific business need
- Apps may be installed on any Splunk instance
- Splunk includes a number default apps



Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# View All Installed Apps

- Within an app, use the dropdown menu and select **Apps: app name > Manage Apps**
- On the **Home** view (launcher app), click the Manage Apps icon
- Apps can be visible or hidden
  - Several apps are installed by default that are hidden or disabled
    - Internal apps used by Splunk should not be modified
    - Legacy apps
    - Sample apps
- Apps are installed under **SPLUNK\_HOME/etc/apps**



Manage Apps icon

# Managing Apps

Apps

Showing 1-18 of 18 items

Add apps

Browse more apps | Install app from file | Create app

filter

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	<a href="#">App   Permissions</a>	Disabled   Enable	<a href="#">Launch app</a>   <a href="#">Edit properties</a>   <a href="#">View objects</a>
SplunkLightForwarder	SplunkLightForwarder		Yes	No	<a href="#">App   Permissions</a>	Disabled   Enable	<a href="#">Edit properties</a>   <a href="#">View objects</a>
System Admin 7.0 Class App	admin70	1.0	Yes	Yes	<a href="#">App   Permissions</a>	Enabled   Disable	<a href="#">Edit properties</a>   <a href="#">View objects</a>
Log Event Alert Action	alert_logevent	7.1.0	Yes	No	<a href="#">App   Permissions</a>	Enabled   Disable	<a href="#">Edit properties</a>   <a href="#">View objects</a>
Webhook Alert Action	alert_webhook	7.1.0	Yes	No	<a href="#">App   Permissions</a>	Enabled   Disable	<a href="#">Edit properties</a>   <a href="#">View objects</a>
Apps Browser	appsbrowser	7.1.0	Yes	No	<a href="#">App   Permissions</a>	Enabled	<a href="#">Edit properties</a>   <a href="#">View objects</a>
framework	framework		Yes	No	<a href="#">App   Permissions</a>	Enabled   Disable	<a href="#">Edit properties</a>   <a href="#">View objects</a>
Getting started	gettingstarted	1.0	Yes	Yes	<a href="#">App   Permissions</a>	Disabled   Enable	
introspection_generator_addon	introspection_generator_addon	7.1.0	Yes	No	<a href="#">App   Permissions</a>	Enabled   Disable	<a href="#">Edit properties</a>   <a href="#">View objects</a>
Home	launcher		Yes	Yes	<a href="#">App   Permissions</a>	Enabled	<a href="#">Launch app</a>   <a href="#">Edit properties</a>   <a href="#">View objects</a>
learned	learned			No	<a href="#">App   Permissions</a>	Enabled   Disable	<a href="#">Edit properties</a>   <a href="#">View objects</a>
legacy	legacy			No	<a href="#">App   Permissions</a>	Disabled   Enable	
sample data	sample data			No	<a href="#">App   Permissions</a>	Disabled   Enable	
Search & Reporting	search			Yes	<a href="#">App   Permissions</a>	Enabled	<a href="#">Launch app</a>   <a href="#">Edit properties</a>   <a href="#">View objects</a>
Splunk Archiver App	splunk_archiver	1.0	Yes	No	<a href="#">App   Permissions</a>	Enabled   Disable	<a href="#">Edit properties</a>   <a href="#">View objects</a>   <a href="#">View details on Splunkbase</a>

Controls access by Splunk role that can use/modify an app

Enable or disable an app (restart may be required)

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# App Permissions

- A user's role with **read** permission can see the app and use it
- A user's role with **write** permission can add/delete/modify knowledge objects used in the app
  - By default, the **user** role does not have write permissions within the **search** app

**App permissions**

Users with read access can only save objects for themselves, or for other users they have explicit permission to share with.

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

**Sharing for config file-only objects**

Set permissions for configurations that have been copied over from config files.

Objects defined in config files only (not in the UI) should appear here.

This app only (system)  All apps

# Installing an App from Splunkbase

- From the **Apps** page, click **Browse more apps**
- Or, click **Apps > Find More Apps**
  - Splunk Web will access **splunkbase.splunk.com**
  - Search for the app you want to install
  - Select **Install** (most apps are free)
    - You must provide your **splunk.com** user ID and password
    - The app is installed into a sub-directory below **SPLUNK\_HOME/etc/apps**
    - Some apps require a restart
- Or, go directly to **splunkbase.splunk.com** and download the app as a file to your local computer



# Installing an App From a File

---

- Download the app from splunkbase
  - The file format may be: `.tar.gz`, `.tgz`, `.zip`, or `.spl` file
- Install the app:
  - From Splunk Web, click **Install app from file**, OR
  - Use CLI, OR

```
splunk install app path-to-appfile
```
  - Extract the app in the proper location

```
cd SPLUNK_HOME/etc/apps
tar -xf path-to-appfile
```
- Apps may require a `splunkd` restart
- Configure the app according to its documentation

# Apps on Forwarders?

---

- Universal forwarders don't have a web interface, but they can still benefit from an app
- An add-on is a subset of an app
  - Usually contains data collection but no GUI components (reports or dashboards)
- To install an add-on or app on a forwarder
  - Install the app using the CLI on the forwarder
  - Or, use a deployment server to deploy the app

# Deleting an App

---

- When you delete an app, all of its related configuration files and scripts are deleted from a Splunk server
  - User's private app artifacts remain untouched
- To delete an app:
  - **splunk remove app <app\_folder>**
  - Or, navigate to **SPLUNK\_HOME/etc/apps** and delete the app's folder and all its contents
  - Restart the Splunk server
- It can be reinstalled later
- Safer to disable it or move the app's files to another location

# 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's role 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.

# Lab Exercise 3 – Install an App

---

**Time:** 10 minutes

**Tasks:**

- Download an app
- Install the app
- Change the app's permissions
- Verify if the app's dashboard displays reports

# Module 4: Splunk Configuration Files

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

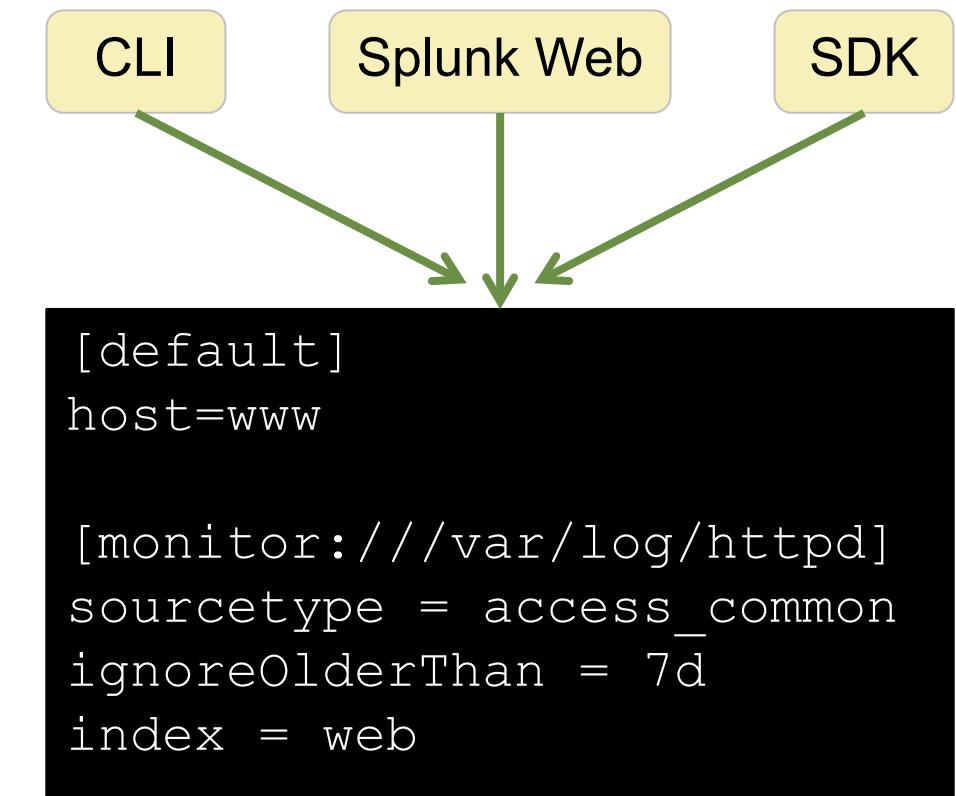
# Module Objectives

---

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

# Splunk Configuration Files

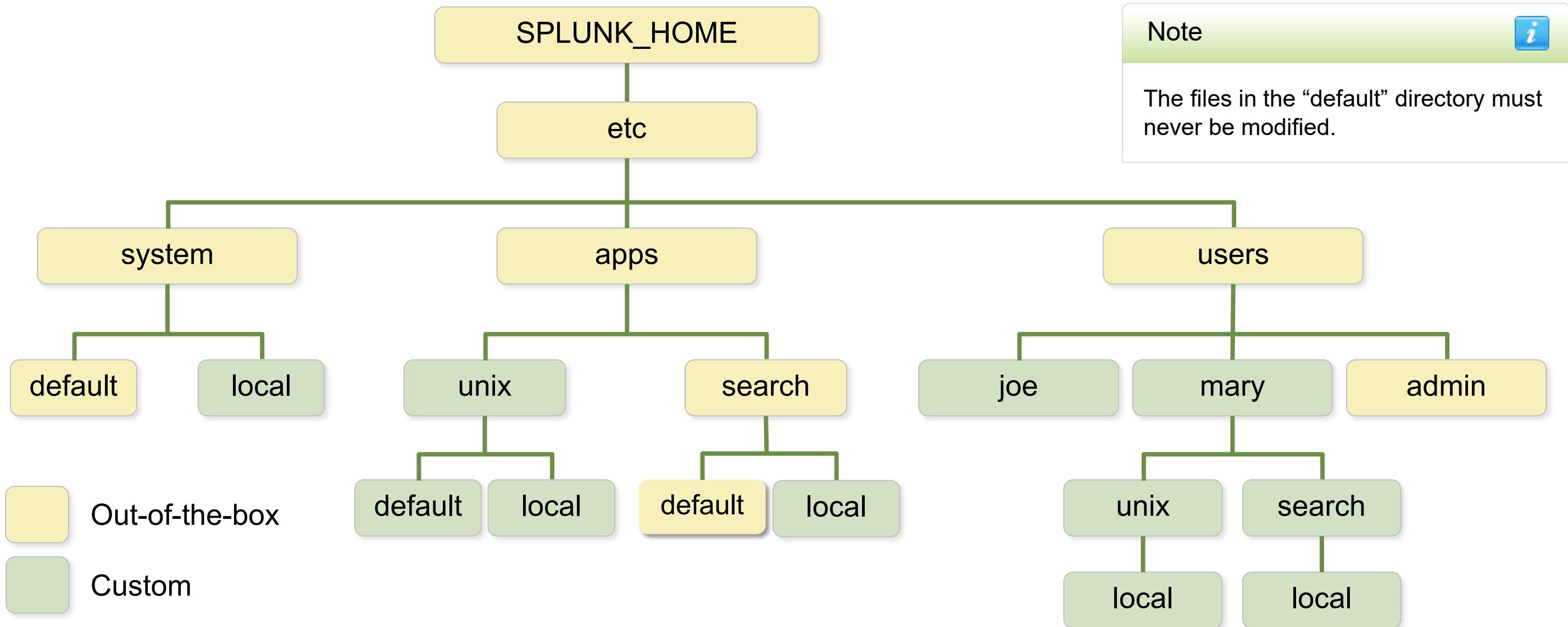
- Each configuration file governs a particular aspect of Splunk functionality
- Configuration changes are saved in **.conf** files under **SPLUNK\_HOME/etc/**
  - **.conf** files are text files using a stanza and name/value (attribute) format
  - The syntax is case-sensitive
- You can change settings using Splunk Web, CLI, SDK, app install, and/or direct edit
- All **.conf** files have documentation and examples:
  - **SPLUNK\_HOME/etc/system/README**
    - ▶ **\*.conf.spec**
    - ▶ **\*.conf.example**
  - ▶ Splunk documentation: [docs.splunk.com](https://docs.splunk.com)



**inputs.conf**

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Configuration Directories



<http://docs.splunk.com/Documentation/Splunk/latest/Admin>Listofconfigurationfiles>

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

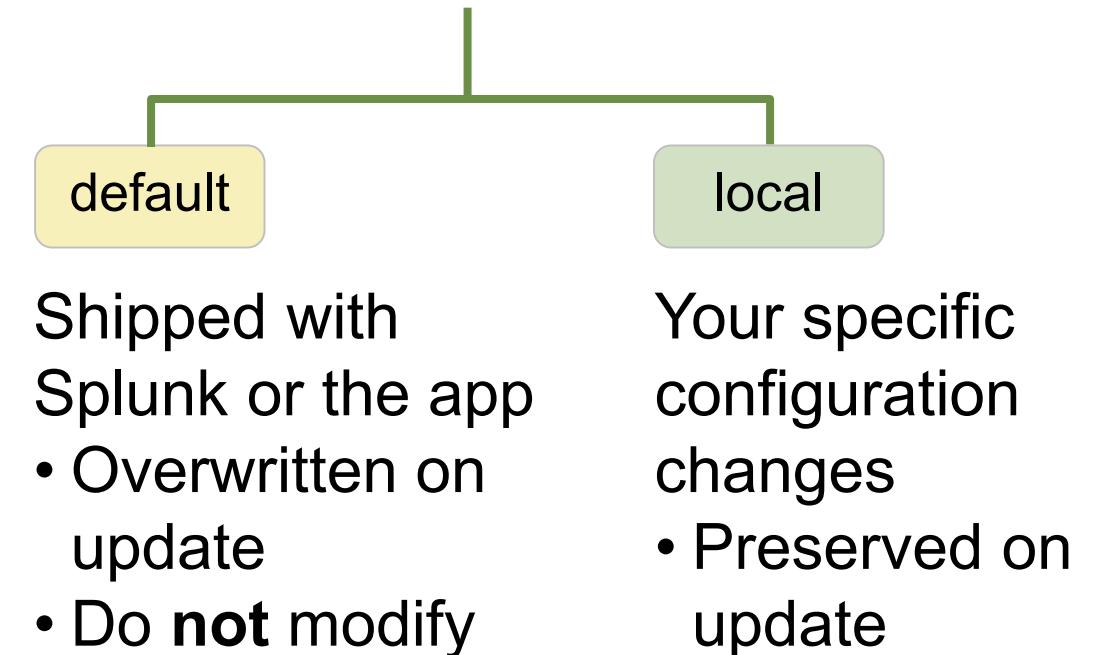
# Commonly Used Splunk Configuration Files

Component	<code>inputs.conf</code>	<code>props.conf</code>	<code>outputs.conf</code>
<b>Universal Forwarder</b> 	Defines what data to collect	Limited parsing such as character encoding, refine MetaData, event breaks*	Defines where to forward the data
<b>Indexer</b> 	Defines what data to collect including data coming from forwarders	Refine MetaData at event level, event breaks, time extraction, TZ, data transformation	Does not need an <code>outputs.conf</code> as the Indexer does not forward the data
<b>Search Head</b> 	Defines what data to collect including Splunk logs	Field Extractions (search time), Lookups, etc.	Defines where to forward the data. You may want to send the data to the Indexer especially the internal logs

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Default vs. Local Configuration

- Splunk ships with default .conf files
  - Stored in the **default** directories
- Only modify configuration files in a **local** directory
- Avoid storing configurations in **SPLUNK\_HOME/etc/system**
  - Manage your configs in the appropriate app under **etc/apps/<appname>/local**
  - If you don't have an app you need to create one



# Index Time vs. Search Time

Index time	Global context	User-independent and background tasks such as inputs, parsing, indexing, etc.
Search time	App/User context	User-related activity, such as searching

- The priority of layered configurations are based on the context

For example:

- **Global context**: a network input to collect syslog data
- **App/User context**: Mary's private report in the Search app
- For a list of configuration files and their context, go to:

[docs.splunk.com/Documentation/Splunk/latest/Admin/Wheretofindtheconfigurationfiles](https://docs.splunk.com/Documentation/Splunk/latest/Admin/Wheretofindtheconfigurationfiles)

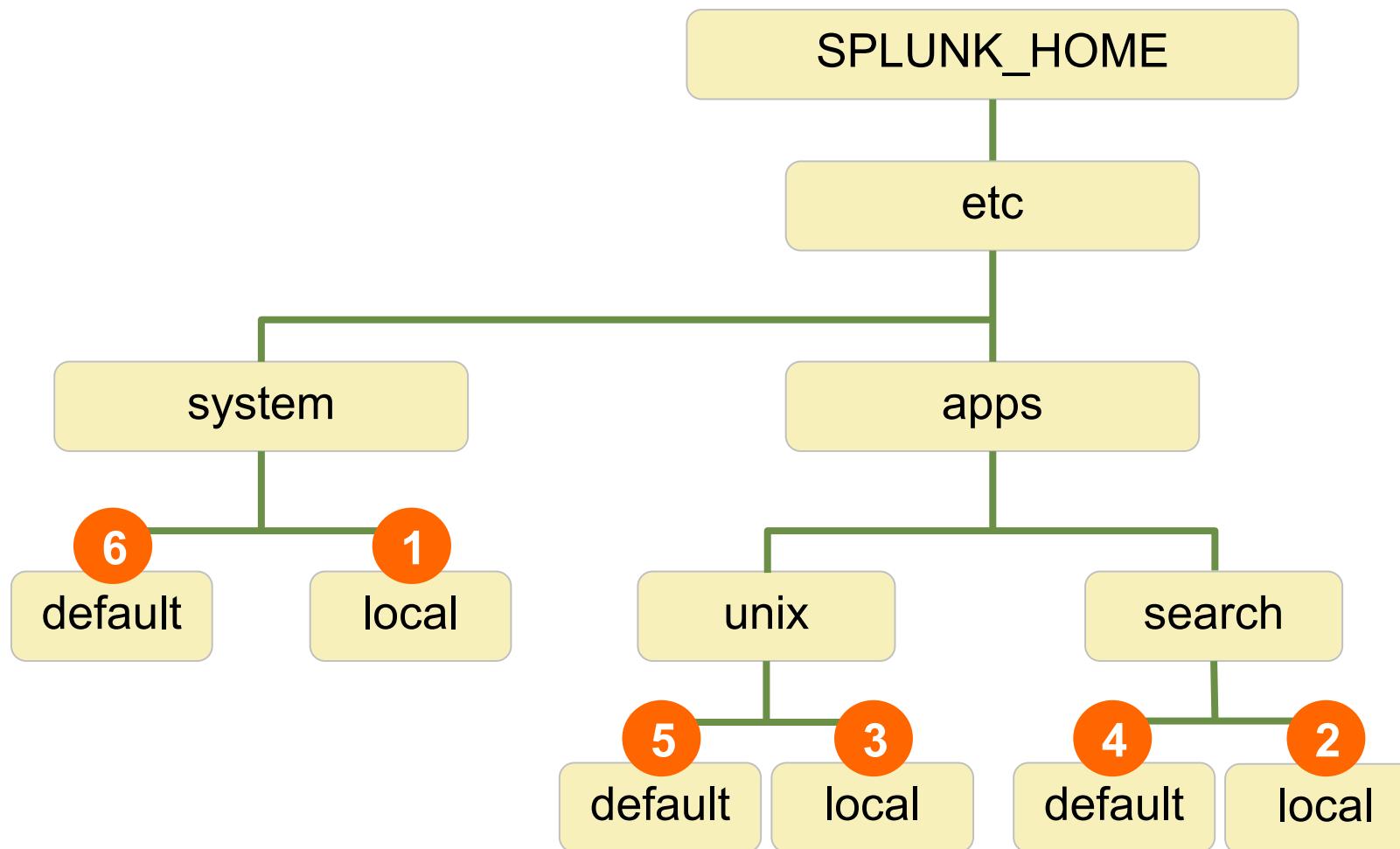
Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Index Time Merging of Configurations

---

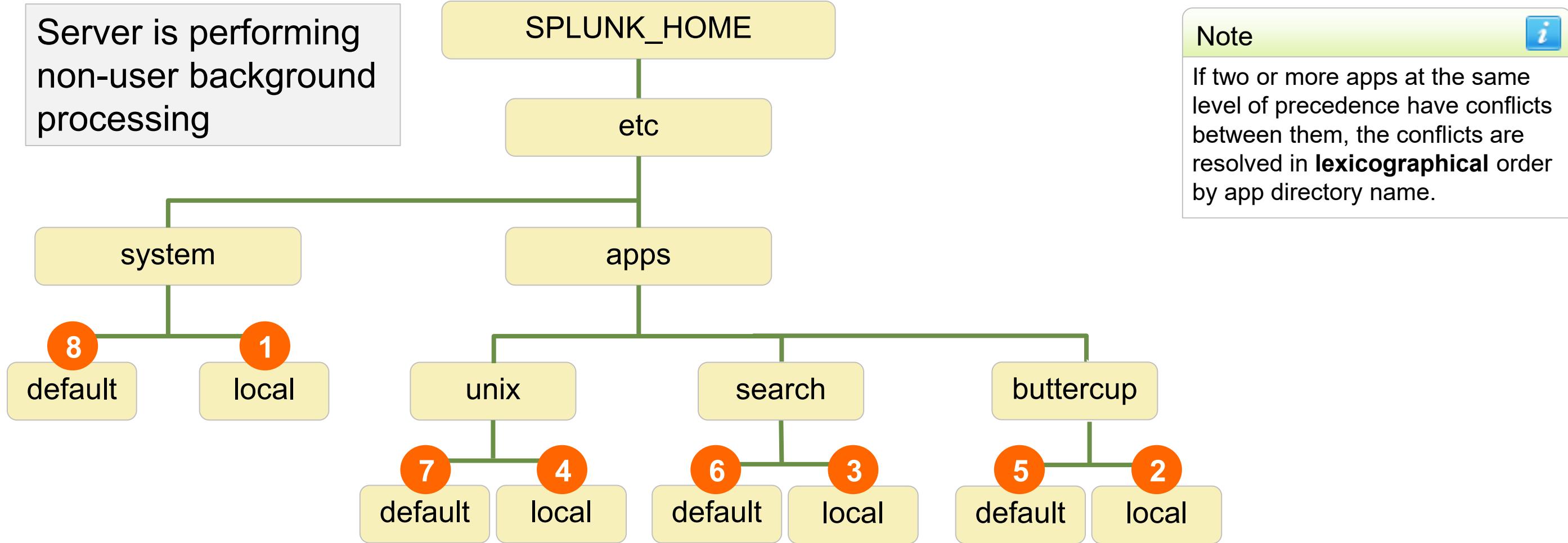
- When Splunk starts, configuration files are merged together into a single run time model for each file type
  - Regardless of the number of `inputs.conf` files in various apps or the system path, only one master inputs configuration model exists in memory at runtime
- If there are no duplicate stanzas or common settings between the files, the result is the union of all files
- If there are conflicts, the setting with the highest precedence is used
  - Remember that `local` always takes precedence over `default`

# Index Time Precedence Order



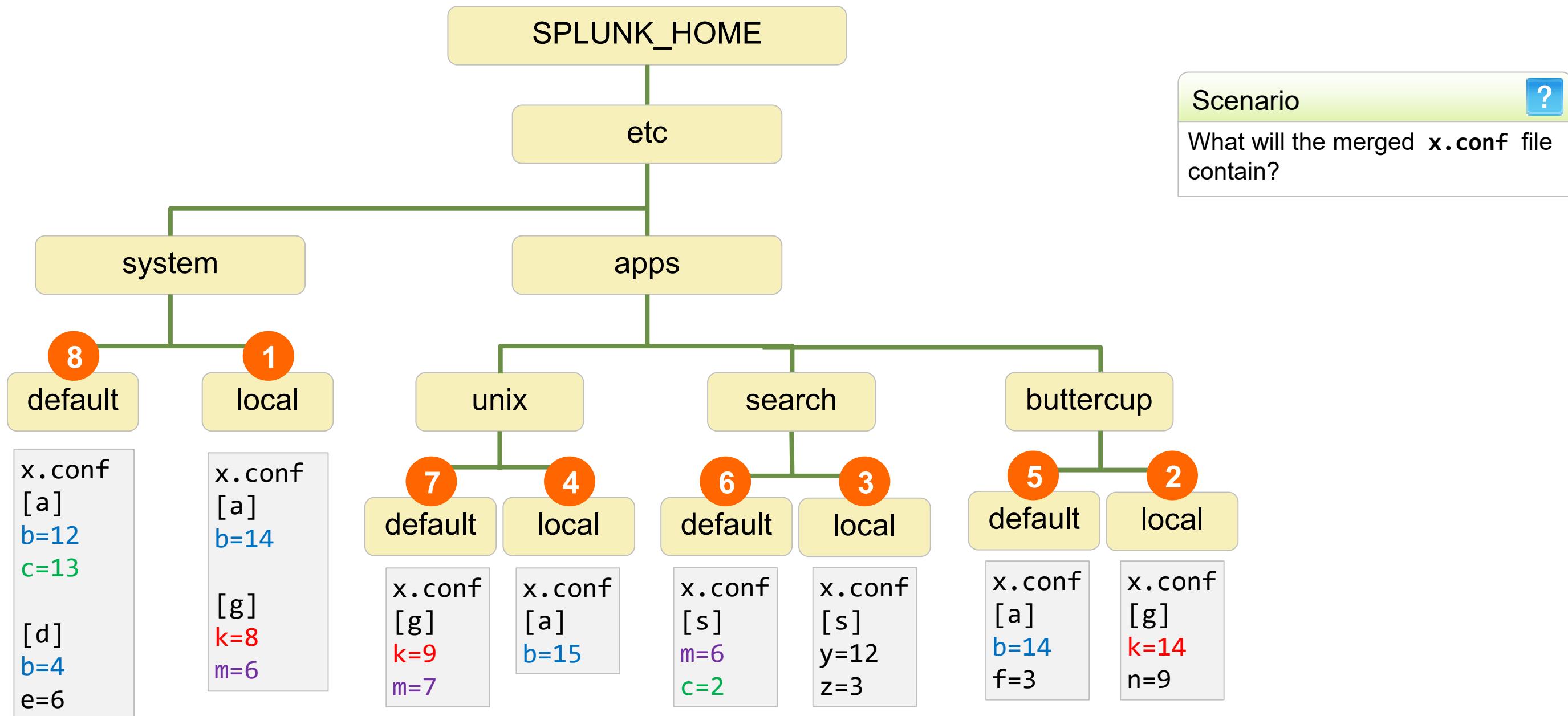
1. etc/system/local
2. etc/apps/search/local
3. etc/apps/unix/local
4. etc/apps/search/default
5. etc/apps/unix/default
6. etc/system/default

# Index Time Precedence – Adding an App



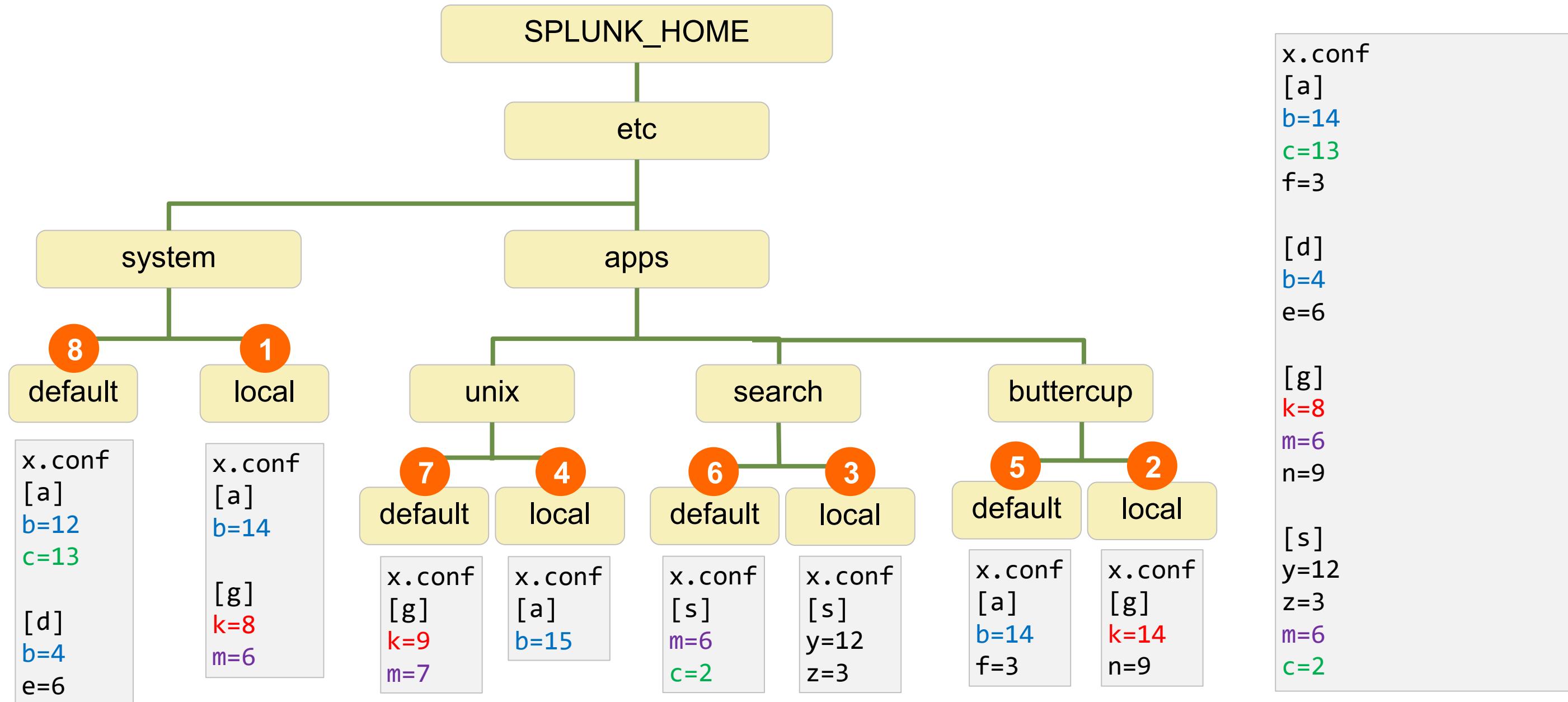
Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Index Time Precedence – Scenario



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

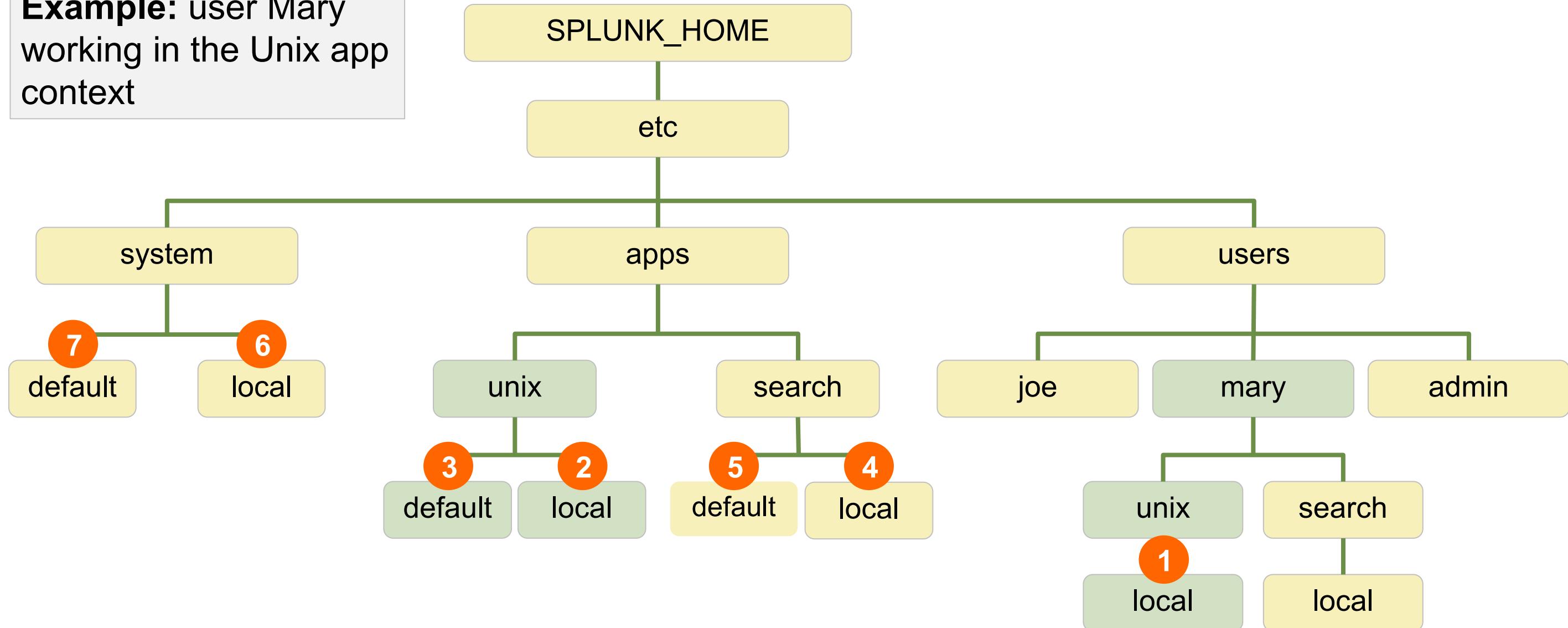
# Index Time Precedence – Scenario (cont.)



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

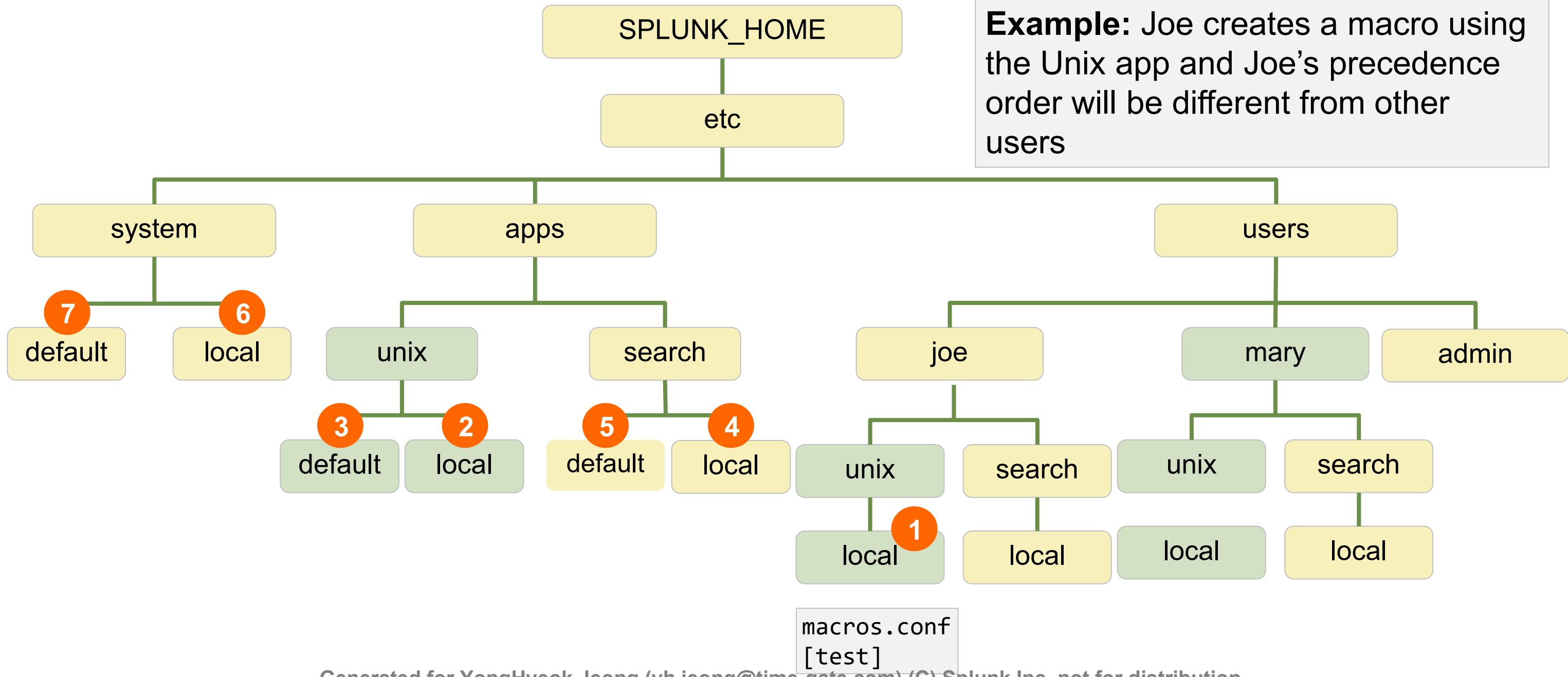
# Search Time Precedence Order

**Example:** user Mary working in the Unix app context



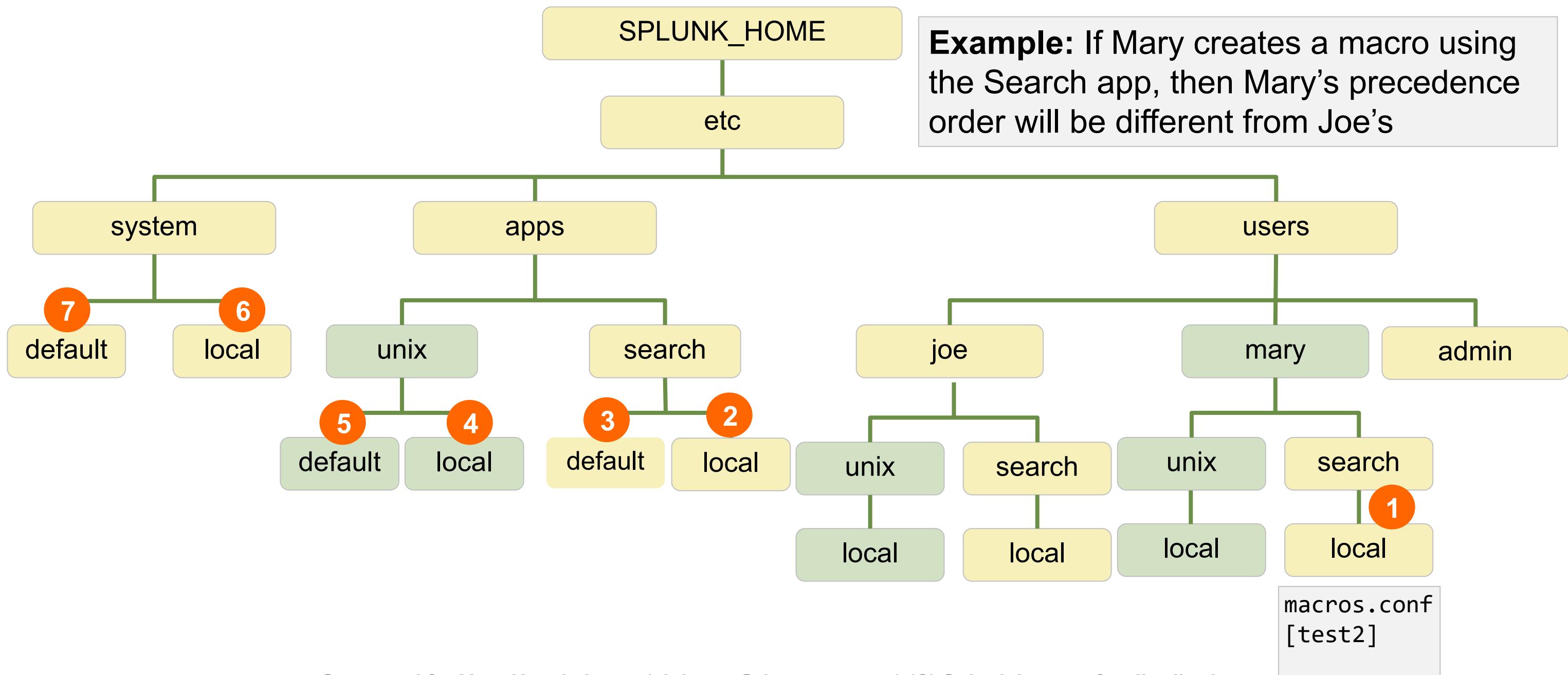
Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Search Time Precedence Order (Joe)



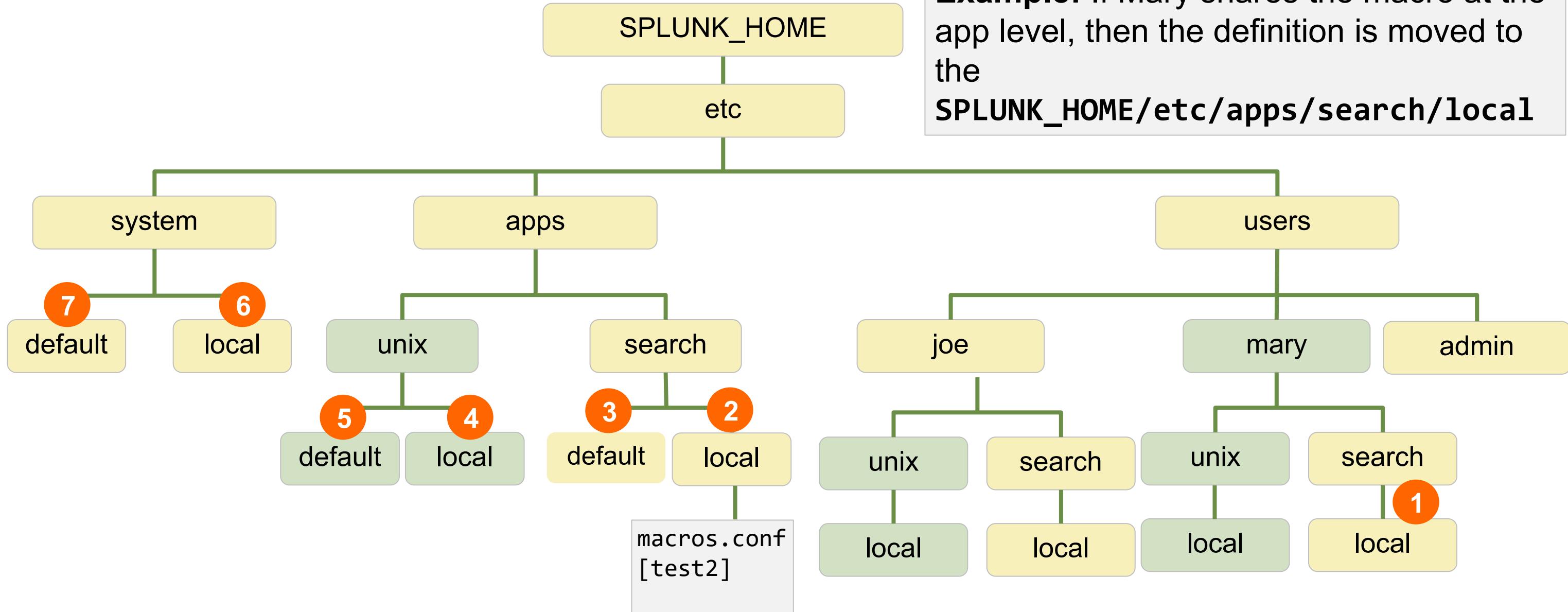
Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Search Time Precedence Order (Mary)



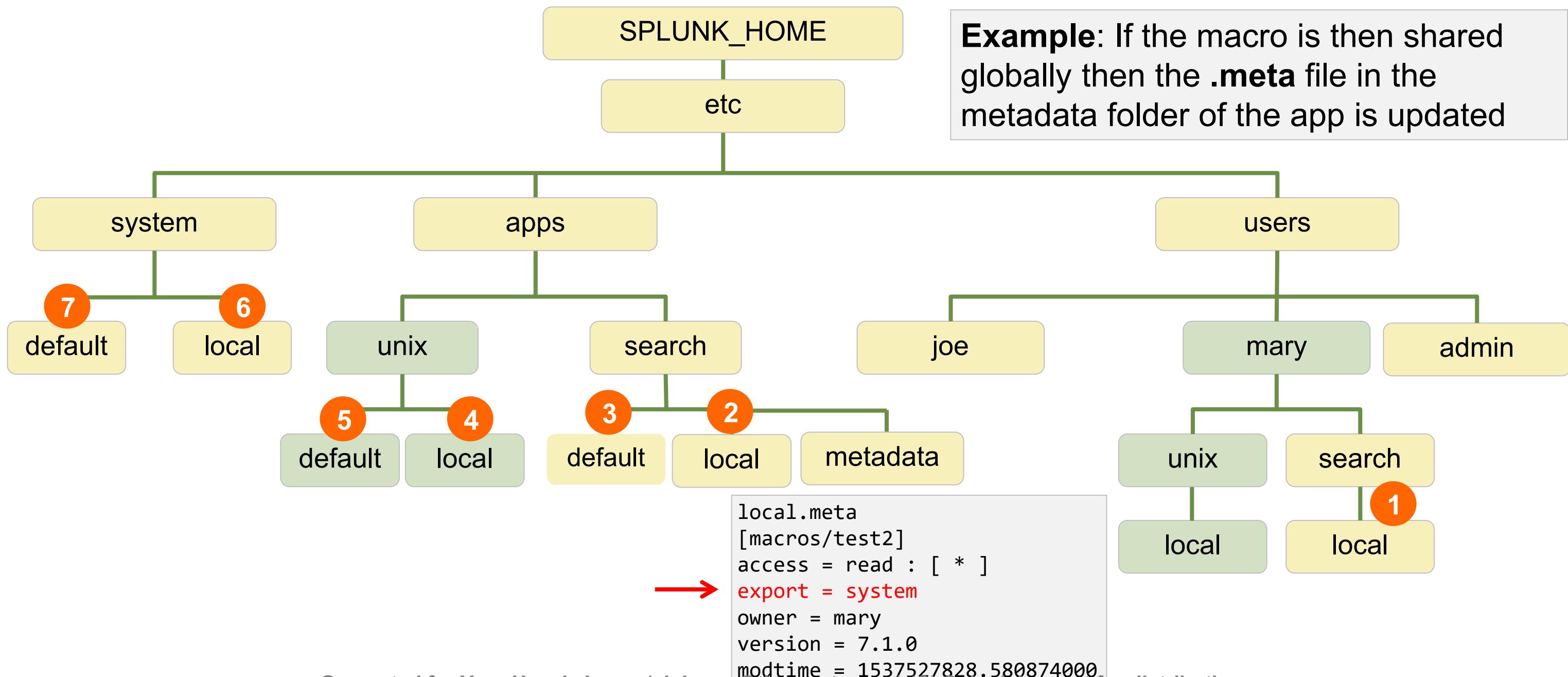
Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Search Time Precedence Order (Sharing KOs)



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Search Time Precedence Order (Sharing KOs) — (cont.)



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Configuration Validation Command **btool**

---

- **splunk btool** *conf-name list* [options]
  - Shows on-disk configuration for requested file
  - Run **splunk btool check** each time Splunk starts
  - Useful for checking the configuration scope and permission rules
    - 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](https://docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/Usebtooltotroubleshootconfigurations)

# btool Example

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  
etc/system/local/inputs.conf  
etc/system/default/inputs.conf  
etc/apps/search/local/inputs.conf

[monitor:///var/log/secure.log]  
host = myIndexer  
index = default  
sourcetype = linux\_secure

## etc/system/local/inputs.conf

```
[monitor:///var/log/secure.log]  
host=myIndexer
```

## etc/apps/search/local/inputs.conf

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

# Overriding Defaults

- There are default settings in `SPLUNK_HOME/etc/system/default` and `SPLUNK_HOME/etc/apps/search/default`
- The correct method to override these settings is to do so in the `local` directory at the same scope
  - Only add the items you are overriding — do not make a copy of the entire configuration file
- Example:
  - To disable a default attribute `TRANSFORMS` for `[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 SH.

# Instances, Phases and Configuration Files

## Phases and processes running on various instances

	Input (inputs.conf)	Forward (outputs.conf)	Parse (props.conf)	License	Search
Universal Forwarder		Forwarder	**		
Heavy Forwarder		Forwarder	Parser		
Indexer	File Monitor Network Input Scripted Input Internal Logs Other	Receiver	Parser	License Slave	Search Peer
Search Head		Receiver*	Parser	License Slave	Search Head
		Forwarder***	Parser ****	License Master	
Other		Forwarder		License Master	

\* Indexers “can” forward as well as receive, but we will not consider it in this course

\*\* For a very specific, limited case, the UF can run the parsing processor

\*\*\* Search Heads may be set to forward their data

\*\*\*\* Search Time Parsing happens here, fields extractions at search time for example

^ Inputs may be configured in `inputs.conf` or other configuration files like `wmi.conf`

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Module 4 Knowledge Check

---

- Which configuration file tells a Splunk instance to ingest data?
- True or False. When Splunk starts, configuration files are merged together into a single run time model for each file type.
- True or False. **btool** shows on-disk configuration for requested file

# Module 4 Knowledge Check – Answers

---

- Which configuration file tells a Splunk instance to ingest data?  
**inputs.conf**
- True or False. When Splunk starts, configuration files are merged together into a single run time model for each file type.  
**True.**
- True or False. **btool** shows on-disk configuration for requested file.  
**True.**

# Lab Exercise 4 – Examine User Configuration Files

---

**Time:** 10 minutes

**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 YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

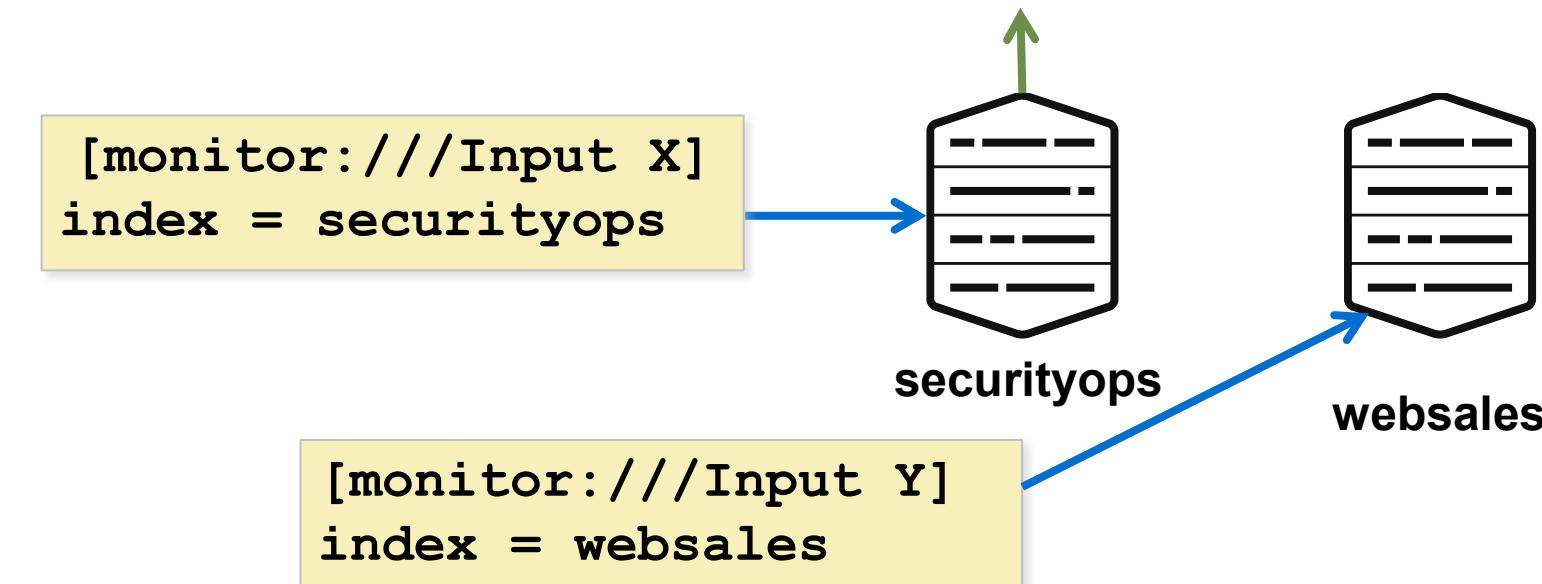
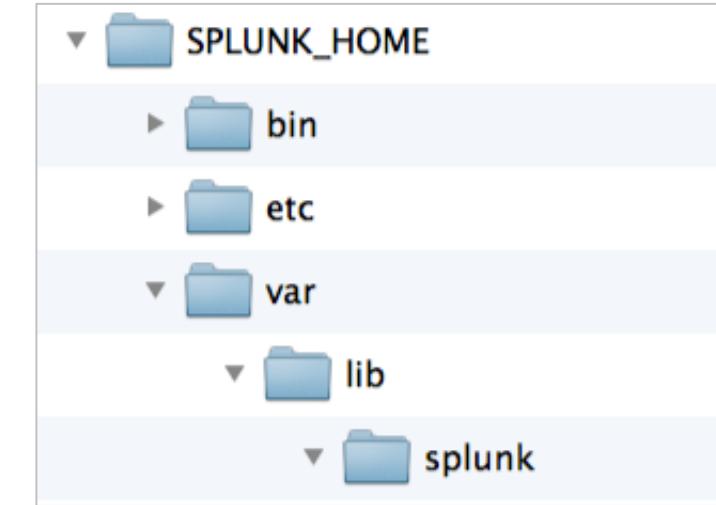
# Module Objectives

---

- Learn how Splunk indexes function
- Understand the types of index buckets
- Create new indexes
- Explain the advantages of using multiple indexes
- Monitor indexes with MC

# What are Indexes?

- Splunk stores the input data as events in indexes
  - **SPLUNK\_HOME/var/lib/splunk**
  - Set in **Settings > Server Settings > General Settings**
  - Can override on a per-index basis
- The system admin can:
  - Create new indexes
  - Control which indexes users can access
- Splunk users can specify the index to search
- Splunk ships with some indexes already installed



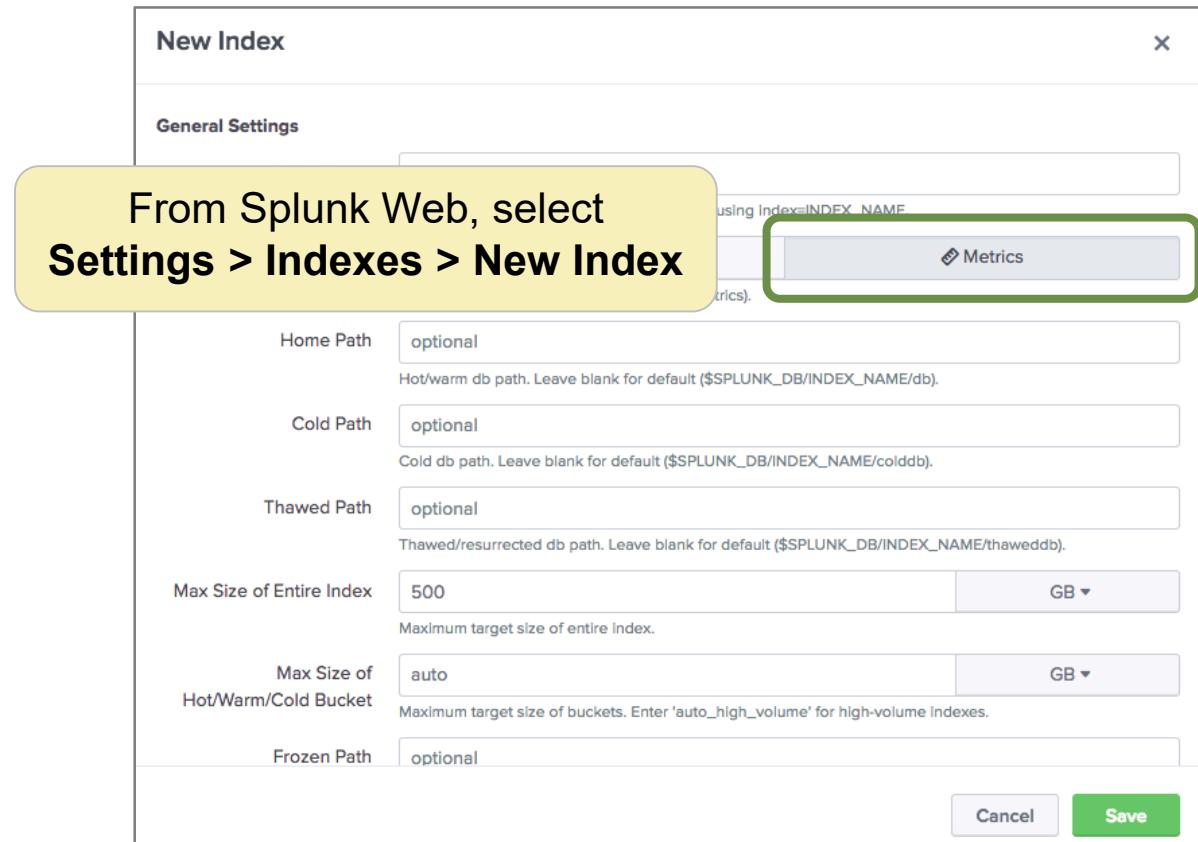
# Preconfigured Indexes

---

- Splunk ships with several indexes preconfigured
  - \_internal** – Splunk indexes its own logs and metrics from its processing here
  - \_audit** – Splunk stores its audit trails and other optional auditing information
  - \_introspection** – tracks system performance, Splunk resource usage data, and provides MC with performance data
  - \_thefishbucket** – contains checkpoint information for file monitoring inputs
- summary** – default index for summary indexing system
- main** – default index for inputs, located in the **defaultdb** directory

# Metrics Indexing

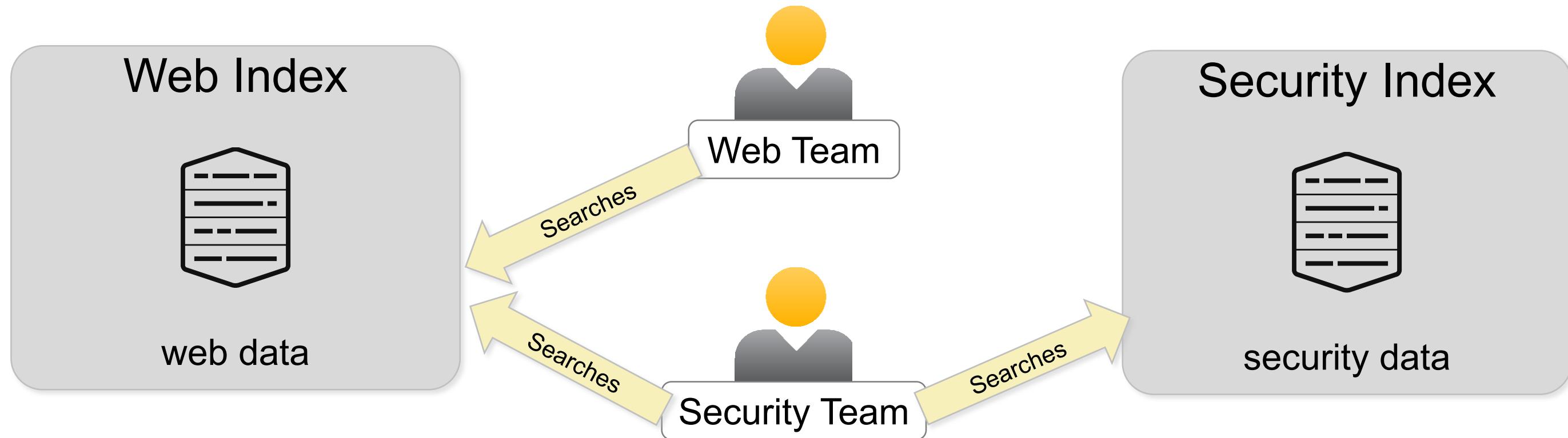
- Splunk supports metrics by including an index format for metrics and certain types of log collection
- Supports the following inputs
  - The StatsD extension over UDP/TCP
  - Plain StatsD extension with dimensions over UDP/TCP
  - Collected over HTTPs using HTTP Event Collector (HEC)
  - CSV format files and custom source type
- Event-based indexes are not the same as metrics-based indexes
  - An event index cannot be converted into a metrics index (or vice-versa)
  - Metrics events are not searchable
    - ▶ Only works with indexed fields/mstats



```
[metrics_index]
coldPath = $Splunk_DB/metrics_index/colddb
homePath = $Splunk_DB/metrics_index/db
thawedPath = $Splunk_DB/metrics_index/thaweddb
maxTotalDataSizeMB = 512000
datatype = metric
```

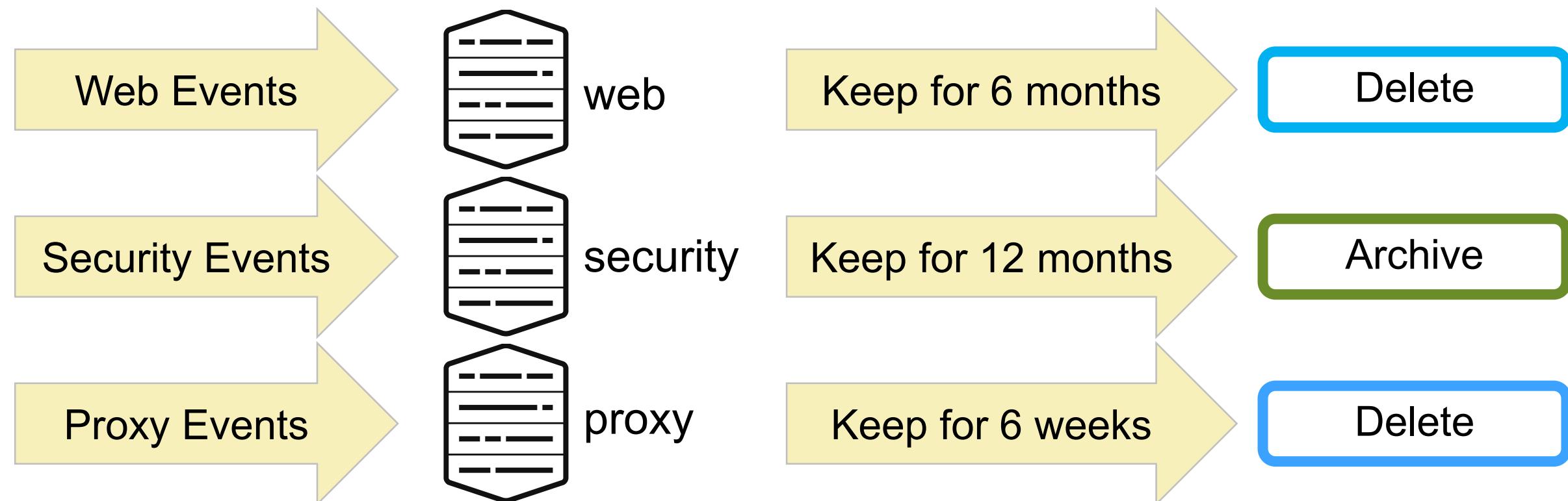
# Why Create Indexes?

Access control – segregate events into separate indexes to limit access by Splunk role



# Why Create Indexes? (cont.)

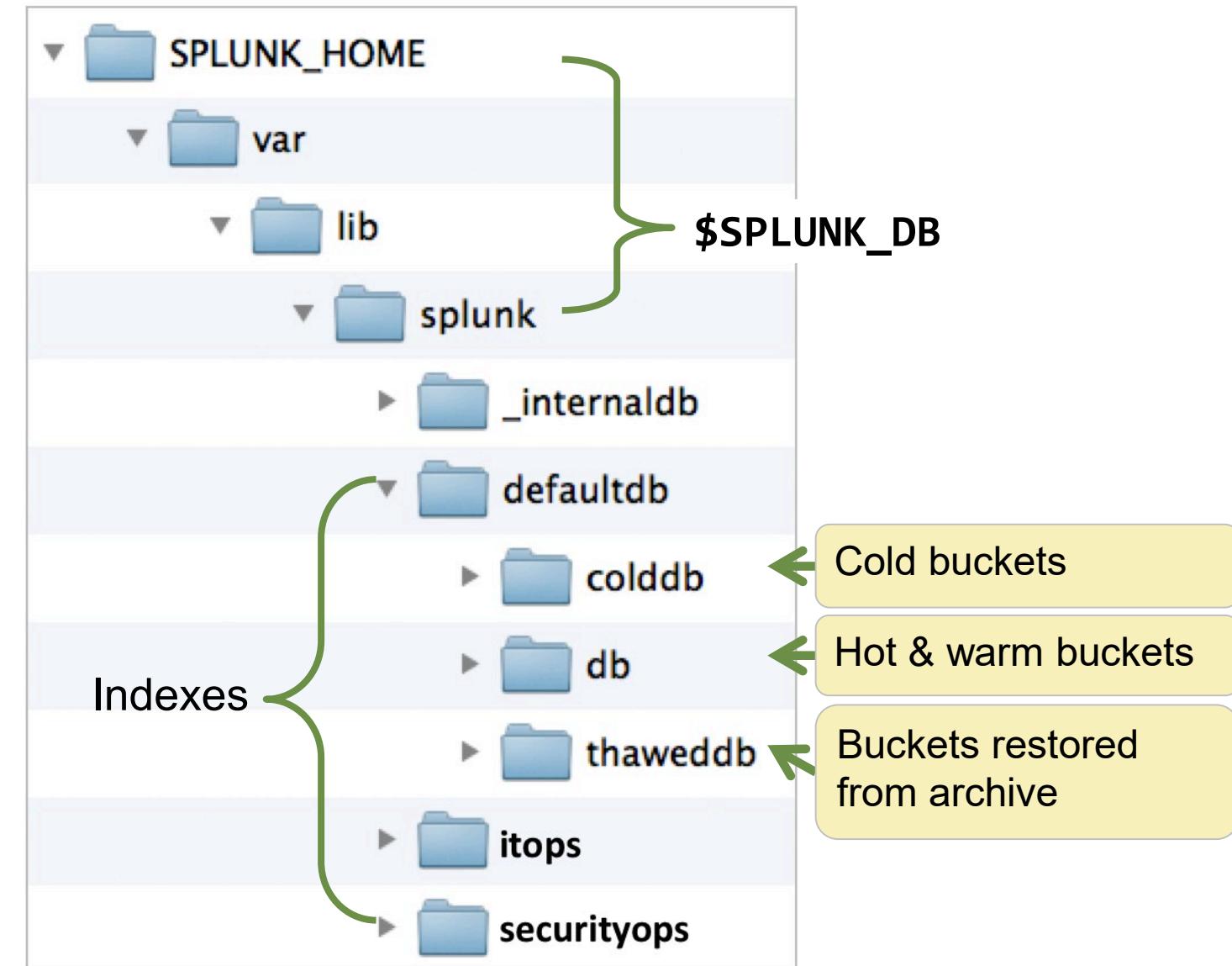
- Retention
  - Policy is set per index
  - Separate events into different indexes based on desired retention time



Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Buckets

- An index stores events in buckets
- A bucket is a directory containing a set of raw data and associated index files
- Buckets have a maximum data size and a time span
  - Both can be configured

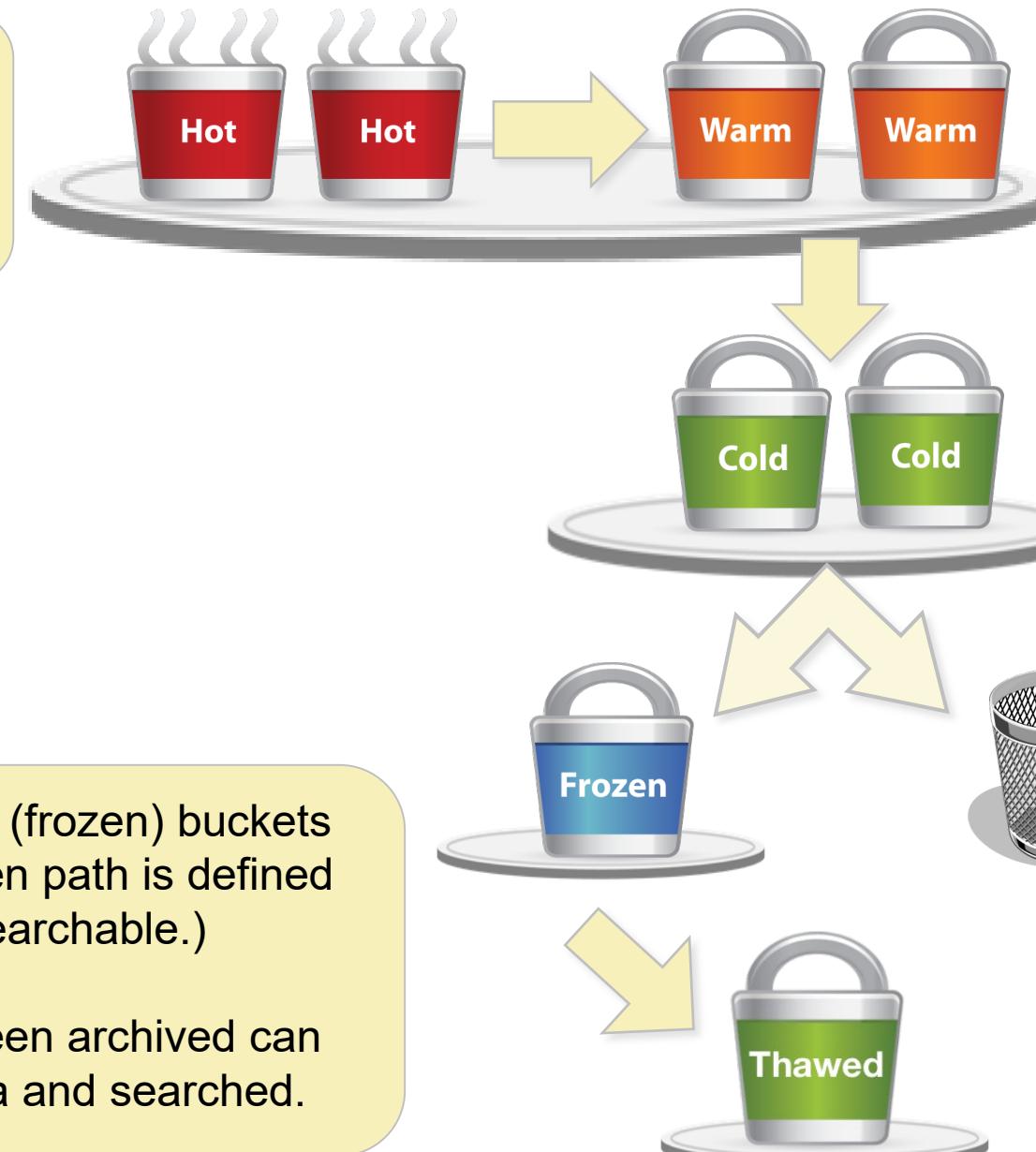


[wiki.splunk.com/Deploy:UnderstandingBuckets](https://wiki.splunk.com/Deploy:UnderstandingBuckets)

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Data Flow Through an Index

1 Hot buckets are the newest buckets open for writes (readable). Events stream to hot buckets split by time.



2 Transition to warm (read-only) when size or time limits are hit.

3 Cold buckets contain the oldest data still in the index (read-only) and can reside on separate partition.

4 Delete is the default action after buckets roll from cold.

One can optionally archive (frozen) buckets in 3rd party store. If a frozen path is defined the data is archived (not searchable.)

Older buckets that have been archived can be loaded into thawed area and searched.

# Hot Buckets

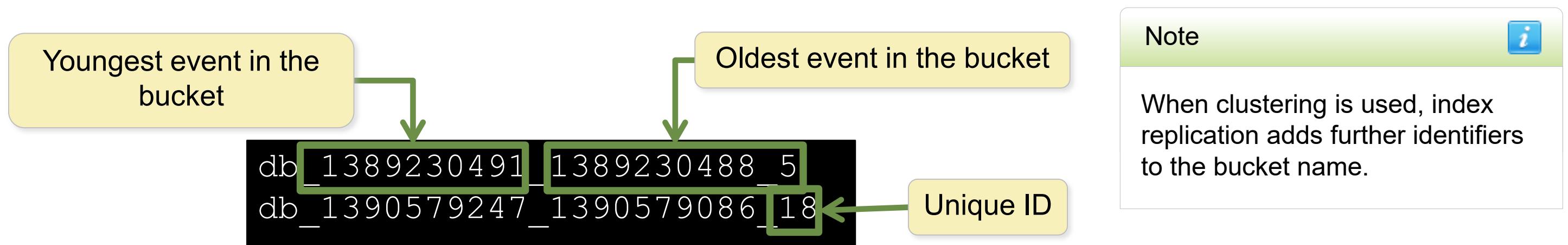
- After data is read and parsed, it goes through the license meter and the resulting event is written into a hot bucket
- When hot buckets reach their max size or time span, they are closed and converted to warm status
  - Hot buckets also roll to warm automatically when the indexer is restarted
  - Hot and warm buckets are stored in the `db` directory for the index
  - Hot buckets are renamed when rolled to warm

Hot Bucket names

hot\_v1\_0  
hot\_v1\_1

# Warm and Cold Bucket Names

- Warm bucket names identify the time range of the events contained in that bucket
- When a warm bucket rolls to cold, the entire bucket is moved, maintaining its name
- At search time, Splunk scans the time range on a bucket name to determine whether or not to open the bucket and search its events



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

Splunk Enterprise 7.3 System Administration

Copyright © 2019 Splunk, Inc. All rights reserved

| 28 June 2019

# Freezing: Data Expiration

---

- The oldest bucket is deleted from an index when:
  - The index's maximum size is reached
  - The bucket's age exceeds the retention time limit
    - ▶ All the events in the bucket have expired
- Splunk will never exceed the maximum overall size of an index
  - Buckets may be deleted even if they have not reached the time limit
- You can optionally configure the frozen path
  - Splunk moves the bucket's raw data to this location 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
    - If events have many searchable terms, the index components are larger
    - If the data contains fewer searchable terms and less variety, the index is smaller
- **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**

<http://docs.splunk.com/Documentation/Splunk/latest/Capacity/Estimateyourstoragerequirements>

# Calculating Index Storage

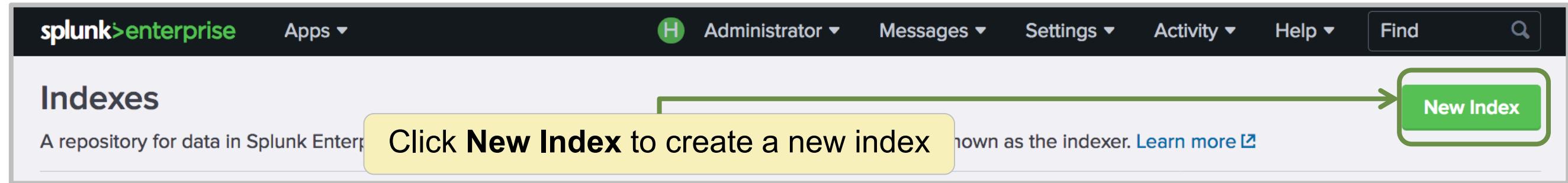
- Limiting size on disk is the most common method of controlling index growth

A screenshot of a user interface for managing index storage. It features a large input field with the value "500" and a dropdown menu next to it labeled "GB". Below the input field is a descriptive text: "Maximum target size of entire index."

- Allocate disk space to meet data retention needs
  - Daily Rate \* Compression Factor \* Retention Period (in days) + Padding
- Example: 5 GB/day of security data searchable for 6 months (with compression factor of .5)
  - **900 GB** (5 GB x 180 days) \* .5 (CF) + **50 GB** (padding) = **500 GB**
  - On average, data moves to frozen in this index after ~6 months

# Adding an Index

- Splunk admins can create indexes from Splunk Web or CLI
  - Splunk Web
    - ▶ **Settings > Indexes > New Index**



- CLI
  - ▶ **splunk add index <index\_name>**

<http://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setupmultipleindexes>

# Adding an Index With Splunk Web

**New Index**

**General Settings**

Index Name	itops	1 Name of index, alphanumeric, hyphens, underscores (cannot begin w/ underscore “_”)
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.		
Index Data Type	<input checked="" type="radio"/> Events	<input type="radio"/> Metrics
The type of data to store (event-based or metrics).	2 Select <b>Events</b> (default) or <b>Metrics</b>	
Home Path	/mnt/ssd/splunk/itops/db	3 Directory path names for index location (created if they don't exist)
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).	<ul style="list-style-type: none"><li>• <b>Home Path</b> - Most recent buckets (hot and warm buckets)</li></ul>	
Cold Path	/mnt/san/splunk/itops/colddb	<ul style="list-style-type: none"><li>• <b>Cold Path</b> – Buckets aged out of hot/warm (cold buckets)</li></ul>
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).	<ul style="list-style-type: none"><li>• <b>Thawed Path</b> - Buckets copied in from archive</li></ul>	
Thawed Path	optional	Default for each \$SPLUNK_DB/ <i>indexname</i> / [db colddb thaweddb]
Data Integrity Check	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.	4 Enable data integrity check (optional)	

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Adding an Index With Splunk Web (cont.)

Max Size of Entire Index  5 Overall index size (default = 500 GB). This setting overrides all other size and retention settings

Max Size of Hot/Warm/Cold Bucket  6 Set max Hot/Warm/Cold Bucket size

- default = auto (750 MB)
- Use **auto\_high\_volume** when daily volume is >10 GB
- Or, provide a specific size

Frozen Path  7 Optionally, specify the path to archive the raw data buckets. Default is to delete when size/time retention is met

App  8 Select where the **indexes.conf** file should be saved (App Context)  
**SPLUNK\_HOME/etc/apps/App/local/indexes.conf**

Storage Optimization

Tsidx Retention Policy  Enable Reduction  Disable Reduction 9 Optional – Configure TSIDX Retention Policy

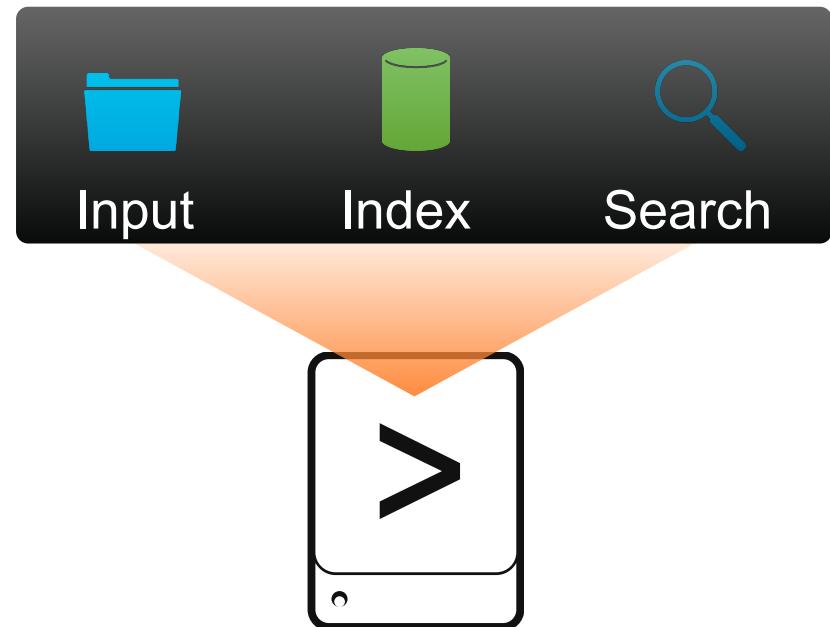
- By default TSIDX reduction is disabled and the indexer retains all TSIDX files for the life of the buckets
- When enabled, the default retention period is 7 days
- Edit Reduce tsidx files older than field to modify default retention period

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

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Input Staging (Index Testing)

- Production data is usually on a remote system and is not on the indexer
  - Normally data comes from one or more Splunk forwarders
- For testing, you can use Splunk Web to sample a log file on a test server
- Use **Add Data** to do this on the test server
  - Check to see if **sourcetype** and other settings are applied correctly
  - If not, delete the test data, change your test configuration, and try again



**Note** i

You will add data to the index you create in the lab exercise. More details about Adding Data can be found in the Splunk Enterprise Data Admin course or Appendix B.

# 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. When hot buckets roll to warm they are renamed.

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

True.

# Lab Exercise 5 – Add Indexes

---

**Time:** 10 minutes

**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 YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Manage indexes with Splunk Web
- Describe **indexes.conf** options
- Customize index retention policies
- Back up indexes
- Delete events from an index
- Restore frozen buckets

# Managing Indexes with Splunk Web

From the Splunk Web, select **Settings > Indexes**

Indexes

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	7 MB	488.28 GB	52.7K	3 days ago	a few seconds ago	\$SPLUNK_DB/audit/db	N/A	✓ Enabled
_internal	Edit	Delete	Disable	Events	system	100 MB	488.28 GB	1.03M	3 days ago	a few seconds ago	\$SPLUNK_DB/_internaldb/db	N/A	✓ Enabled
_introspection	Edit	Delete	Disable	Events	system	224 MB	488.28 GB	197K	3 days ago	a few seconds ago	\$SPLUNK_DB/_introspection/db	N/A	✓ Enabled
_telemetry	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	7	3 days ago	a day ago	\$SPLUNK_DB/_telemetry/db	N/A	✓ Enabled
_thefishbucket	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/fishbucket/db	N/A	✓ Enabled
history	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/historydb/db	N/A	✓ Enabled
itops	Edit	Delete	Disable	Events	search	1 MB	100 GB	4.27K	a month ago	16 minutes ago	volume:one/itops/db	N/A	✓ Enabled
main	Edit	Delete	Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/defaultdb/db	N/A	✓ Enabled
securityops	Edit	Delete	Disable	Events	search	8 MB	500 GB	54.5K	3 months ago	5 minutes ago	\$SPLUNK_DB/securityops/db	N/A	✓ Enabled
splunklogger	Edit	Delete	Enable	Events	search	1 MB	488.28 GB	0			\$SPLUNK_DB/splunklogger/db	N/A	✗ Disabled
summary	Edit	Delete	Disable	Events	search	1 MB	488.28 GB	0			\$SPLUNK_DB/summarydb/db	N/A	✓ Enabled
test	Edit	Delete	Disable	Events	admin72	8 MB	50 GB	55.5K	6 years ago	a day ago	\$SPLUNK_DB/test/db	N/A	✓ Enabled
websales	Edit	Delete	Disable	Events	admin72	8 MB	50 GB	55.5K	3 months ago	2 minutes ago	\$SPLUNK_DB/websales/db	N/A	✓ Enabled

Click New Index to launch the New Index dialog box New Index

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

Custom indexes can be enabled/disabled or deleted

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

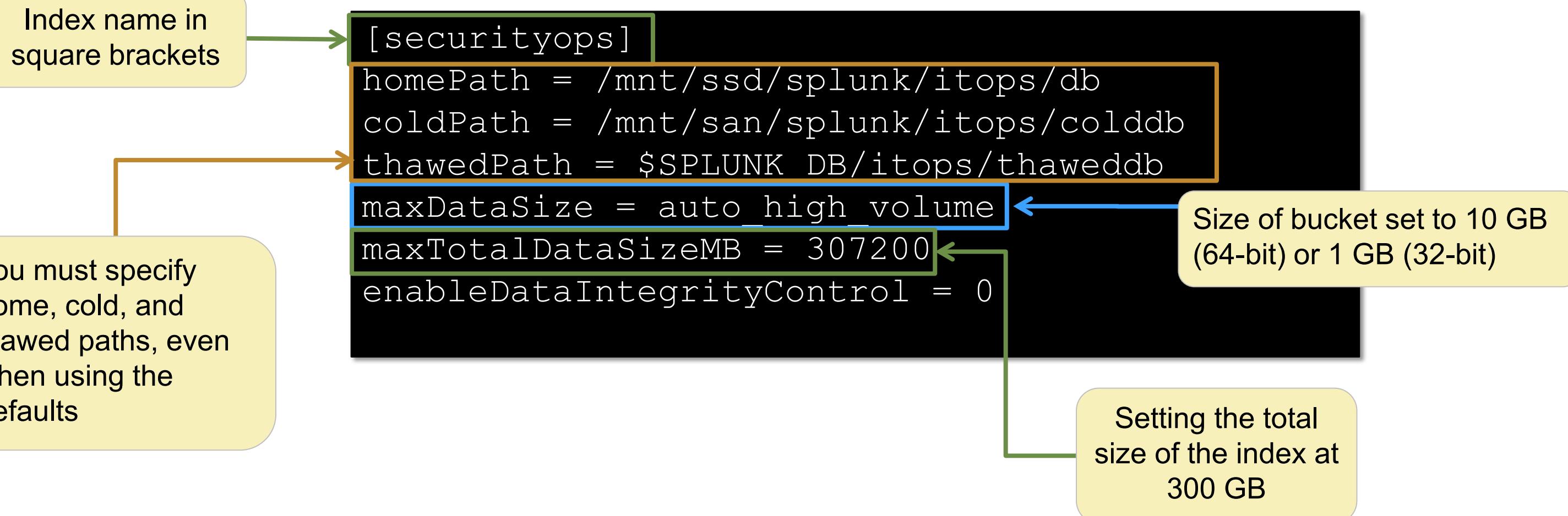
# Index Data Integrity Check

---

- Provides an ability to validate that data has not been tampered with after indexing  
[docs.splunk.com/Documentation/Splunk/latest/Security/Dataintegritycontrol](https://docs.splunk.com/Documentation/Splunk/latest/Security/Dataintegritycontrol)
- When enabled, produces calculated hash files for auditing and legal purposes
  - Works on index level (including clustering)
  - Does not protect in-flight data from forwarders
  - To prevent data loss, use the indexer acknowledgment capability (useACK)
- To verify the integrity of an index/bucket:  
**-splunk check-integrity -bucketPath [bucket\_path] [verbose]**  
**-splunk check-integrity -index [index] [verbose]**
- To re-generate hash files:  
**-splunk generate-hash-files [-bucketPath|-index]**  
**[bucket\_path|index]**

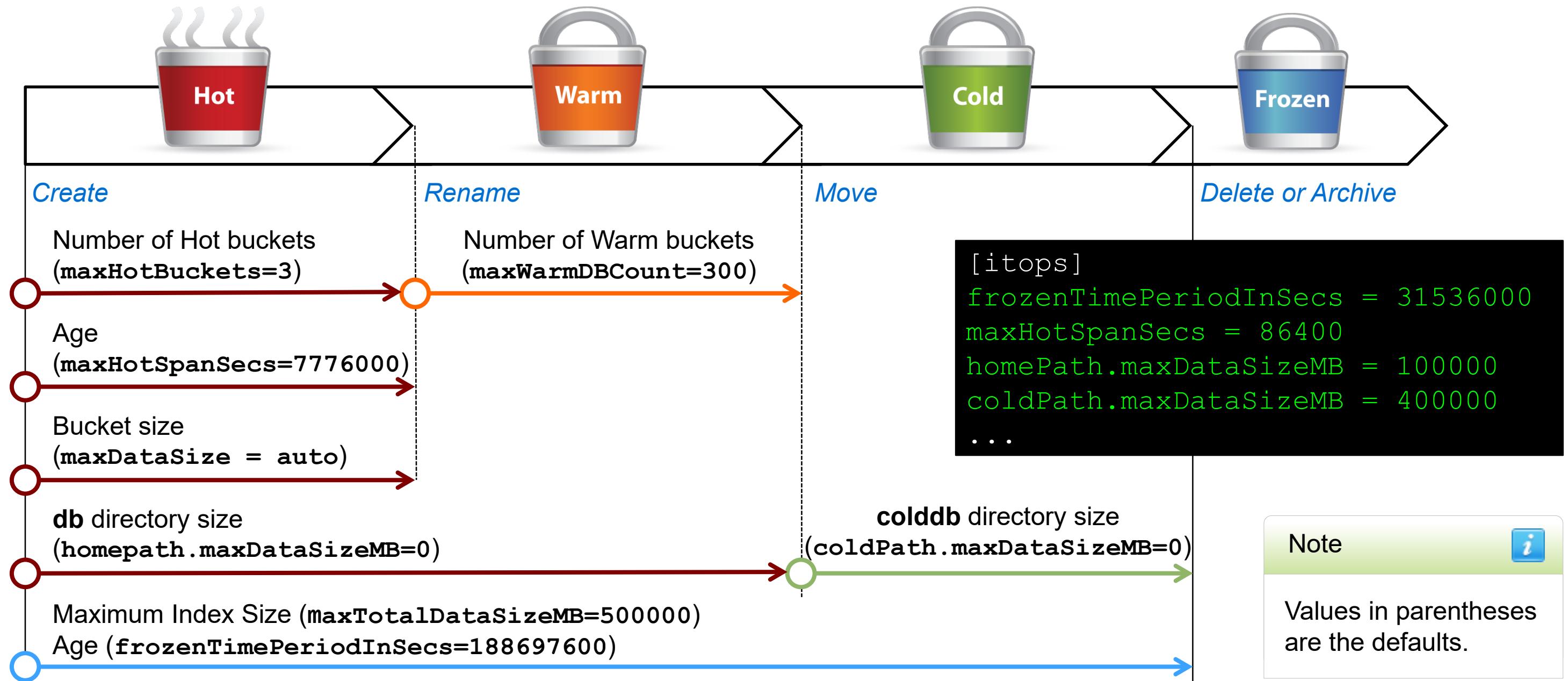
# indexes.conf

The index stanza is created in `local/indexes.conf` of the selected app



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# indexes.conf Options



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Index Definitions and Data

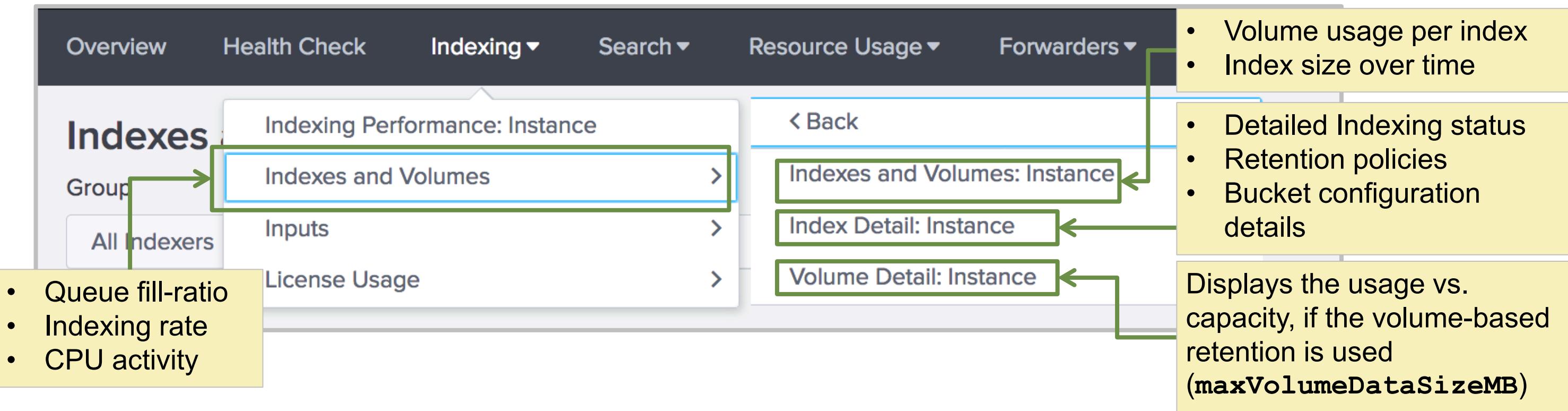
INDEX	
<b>Index Definition (indexes.conf)</b>	SPLUNK_HOME/etc/system/local SPLUNK_HOME/etc/apps/... SPLUNK_HOME/etc/apps/<app_name1>/local SPLUNK_HOME/etc/apps/<app_name2>/local
<b>Data (Buckets)</b>	SPLUNK_HOME/var/lib/splunk/<index_name>/db SPLUNK_HOME/var/lib/splunk/<index_name>/colddb SPLUNK_HOME/var/lib/splunk/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

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Viewing Indexing Activity and Health

- **Monitoring Console (MC)**

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



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Monitoring Indexes with MC

## Indexes and Volumes: Instance

Index Type      Group      Instance

Event Indexes Only      All Indexers      Indexer

All Index Types \*      Search produced no results.

The "All Index Types" option is not compatible with indexers running Splunk Enterprise 6.6 or earlier, where only event indexes exist.

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

Select views: All   Snapshot   Historical

### Snapshots

0.49

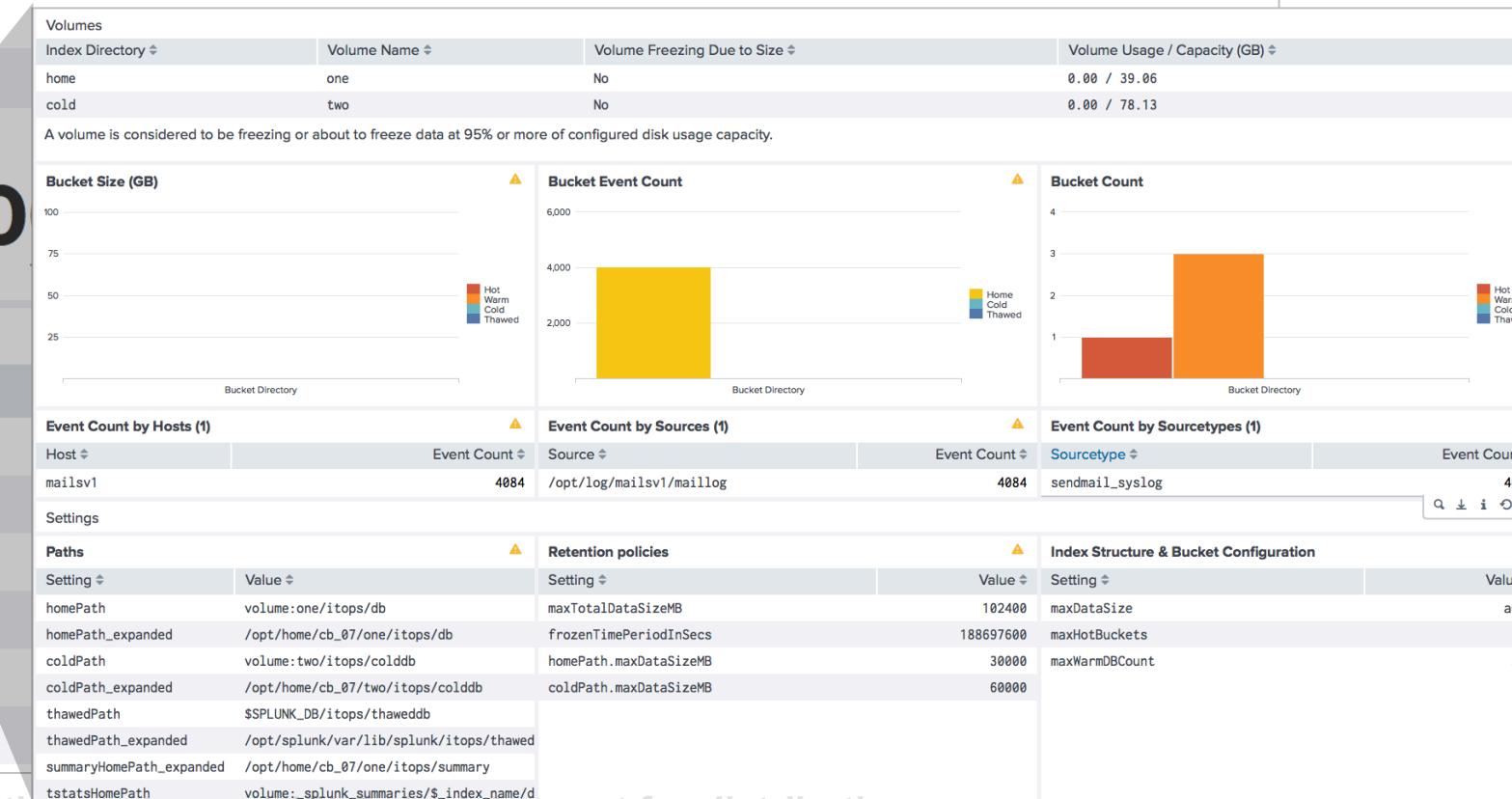
Total Index Size  
Select an index to see more details

2,0

Indexes (11)

Index	Data Type	Data Age vs Frozen Age (days)	Index Usage (GB)
_audit	event	3 / 2184	0.01 / 488.28
_internal	event	3 / 30	0.09 / 488.28
_introspection	event	3 / 14	0.20 / 488.28
_telemetry	event	3 / 730	0.00 / 488.28
itops	event	33 / 2184	0.00 / 100.00
main	event	0 / 2184	0.00 / 488.28

From the MC menu, select **Indexing > Indexes and Volumes > Indexes and Volumes: Instance Index**



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Configuring High-volume Indexes

- To set more advanced/specific options, edit the stanza in `indexes.conf`
- New indexes default to 3 hot buckets at a time
  - If it is likely that an index will receive events that are not in time-sequence order, increase the number of available hot buckets
- High-volume indexes should have up to 10 hot buckets
  - Set with the `maxHotBuckets` key
- **Best practice** for high-volume indexes:
  - Examine and copy settings of `main` index stanza and adjust for your 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

- Example: Purge HR data when it is more than 90 days old, but no sooner
- Issues to consider:
  - Splunk freezes entire buckets, not individual events
  - If a bucket spans more than one day, you can't 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 changing.

# Buckets on Different Storage Systems

- **Best Practice:** Use a high performance file system to store indexes
  - The bucket time span and storage type can affect search performance
- You can use multiple storage systems for buckets
  - Specify separate volumes for hot/warm and cold buckets during index creation
  - Hot and warm buckets should be on the fastest storage
  - Cold buckets can be located on a slower, less expensive storage (or SAN/NAS)

[wiki.splunk.com/Deploy:BucketRotationAndRetention](https://wiki.splunk.com/Deploy:BucketRotationAndRetention)



Generated for YongHyeok Jeong (yh.jeong@time-gate.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 if a retention based on size is desired

```
[volume:fast]
path = /mnt/ssd/
maxVolumeDataSizeMB = 500000

[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 YongHyeok Jeong (yh.jeong@time-gate.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 is empty, it will drop such events
- Defaults to empty

## indexes.conf Global Settings

```
lastChanceIndex = <index name>  
...
```

# What to Back Up

---

- Indexed events – Splunk indexes
  - **SPLUNK\_HOME/var/lib/splunk/**
  - Or the directories where you placed your indexes (see **indexes.conf** for details)
- The monitored source data files (optional)
- **SPLUNK\_HOME/etc** for config and other important files
  -  **apps**
  -  **users**
  -  **system/local**
  -  **licenses**
  -  **init.d**
  -  **passwd**
  - and more

# Backup Recommendation

---

- Use the incremental backup of your choice
  - Warm and cold buckets of your indexes
  - Configuration files
  - User files
- Hot buckets cannot be backed up without stopping Splunk
  - Use the snapshot capability of underlying file system to take a snapshot of hot, then back up the snapshot
  - Schedule multiple daily incremental backups of warm
    - Works best 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
  - \*NIX: `cp -rp <source> <target>`
  - Windows: `xcopy <source> <target> /s /e /v /o /k`  
(or, 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

---

- If you have unwanted events in an index
  - Splunk does not have an index editor
  - First, you should address your configuration to omit/modify future incoming events
- What are your options for events already in the index?
  - Let the events age-out normally (whole bucket ages out)
  - Use the **delete** command to make the unwanted events not show up in searches
  - Following options are NOT recommended in production:
    - ▶ Run **splunk clean** command to delete **ALL** events from the index
    - ▶ Delete the index

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Deleting Events

- The **delete** command marks all returned events by the search as deleted
- After you are certain you've targeted only the data you want to delete, pipe the **delete** command



## Note

This is a "virtual" delete. Splunk marks the events as deleted and they never show in searches again. However, they continue to take up space on disk.

# Deleting Events (cont.)

---

- Splunk recommends creating a native account with the **can\_delete** role specifically set up for deletions
  - **DO NOT** give this capability to other roles
  - By default, the admin role does not have this ability
- The delete operator triggers a roll of hot buckets to warm in the affected indexes
- The delete command **CANNOT** be undone
  - Subsequent searches do not return the marked events
  - Double check your search includes ONLY the events you want to delete
  - Does not reclaim disk space

# Cleaning Out an Index

---

- To flush indexed events and reset an index, use the CLI **clean** command

- DATA WILL BE PERMANENTLY DESTROYED

- Typically used on test/dev systems, not for production systems

- Command syntax:

**splunk clean** [eventdata|userdata|all] [-index name]

- **eventdata** – delete indexed events and metadata on each event

- **userdata** – delete user accounts

- **all** – everything - including users, saved searches, and alerts

- ALWAYS SPECIFY AN INDEX TO AVOID TEARS

**WARNING!** If no index is specified, the default is to clean (destroy) all indexed events from all indexes!

# The Fishbucket – Re-indexing Data

- The **fishbucket** index stores the checkpoint information for monitor inputs
- To reset the individual input checkpoint, use the **btprobe** command:

```
splunk cmd btprobe -d SPLUNK_HOME/var/lib/splunk/  
fishbucket/splunk_private_db --file <source> --reset
```

- Requires stopping the forwarder or indexer
- Other options:
  - **splunk clean eventdata -index \_thefishbucket**
    - Force re-indexing of all file monitors in the indexer
    - Resetting the monitor checkpoint re-indexes the data and results in more license usage
  - **rm -r ~/splunkforwarder/var/lib/splunk/fishbucket**
    - Manually delete the **fishbucket** on forwarders

Generated for Yong-Hyeok Jeong (yjhjeong@time-gate.com) (c) Splunk Inc. Not for distribution

# Restoring a Frozen Bucket

---

- To thaw a frozen bucket:
  - Copy the bucket directory from the frozen directory to the index's **thaweddb** directory
  - Run **splunk rebuild <path to thawed bucket directory>**
    - Does not count against license
  - Restart Splunk
- Events in **thaweddb** are searchable along with other events
  - They will not be frozen, nor do they count against the index max size
  - Delete the thawed bucket directory when no longer needed and restart Splunk

# Further Reading

---

- [docs.splunk.com/Documentation/Splunk/latest/Indexer/HowSplunkstoresindexes](https://docs.splunk.com/Documentation/Splunk/latest/Indexer/HowSplunkstoresindexes)
- [docs.splunk.com/Documentation/Splunk/latest/Indexer/Setlimitsondiskusage](https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setlimitsondiskusage)
- [docs.splunk.com/Documentation/Splunk/latest/Indexer/Automatearchiving](https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Automatearchiving)
- [wiki.splunk.com/Deploy:BucketRotationAndRetention](https://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 will have to 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.**

# Lab Exercise 6 – Splunk Index Management

---

**Time:** 10 minutes

**Tasks:**

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

# Module 7: Splunk User Management

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

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

# Managing Users and Roles

- Users and roles define user privileges
- To have access to a Splunk instance, a user must have:
  - A Splunk user account
  - Assignment to one or more Splunk roles
- Click **Settings > Access controls**

The screenshot shows the 'Access controls' page in Splunk. At the top, it says 'Access controls' and 'Specify authentication method, manage user settings, and manage roles.' Below this, there are four main sections: 'Authentication method' (blue link), 'Users' (blue link with '+ Add new' button), 'Roles' (blue link with '+ Add new' button), and 'Password Policy Management' (blue link).

# Adding Users in Splunk

---

- You can create user accounts directly in Splunk
  - Example: `admin` user
- Passwords are stored in `SPLUNK_HOME/etc/passwd`
- Use a blank password file to completely disable native authentication BUT
  - In all authentication scenarios, best practice is to keep a failsafe account here with a VERY strong password
- You can have a mix of Splunk and LDAP or other users
  - Splunk native authentication always takes precedence over others

# Adding Native Users

- Required:
  - Username and password
- Optional:
  - Full name and email address (defaults to none)
  - Time zone (defaults to search head time zone)
  - Default app (defaults to role default app, or home if no role default app)
  - Role(s)
    - ▶ Defaults to **user**
  - Change password on first login requirement
    - ▶ Defaults to enabled

**Create User**

Name	<input type="text"/>																								
Full name	optional																								
Email address	optional																								
Set password	New password																								
Confirm password	Confirm new password																								
Password must contain at least ? 0 1 character																									
Time zone ?	-- Default System Timezone -- ▾																								
Default app ?	launcher (Home) ▾																								
Assign to roles ?	<table border="1"><tr><td>Available item(s)</td><td><input type="button" value="add all »"/></td><td>Selected item(s)</td><td><input type="button" value="« remove all"/></td></tr><tr><td>admin</td><td></td><td>user</td><td></td></tr><tr><td>can_delete</td><td></td><td></td><td></td></tr><tr><td>power</td><td></td><td></td><td></td></tr><tr><td>splunk-system-role</td><td></td><td></td><td></td></tr><tr><td>user</td><td></td><td></td><td></td></tr></table>	Available item(s)	<input type="button" value="add all »"/>	Selected item(s)	<input type="button" value="« remove all"/>	admin		user		can_delete				power				splunk-system-role				user			
Available item(s)	<input type="button" value="add all »"/>	Selected item(s)	<input type="button" value="« remove all"/>																						
admin		user																							
can_delete																									
power																									
splunk-system-role																									
user																									
Create a role for this user <input type="checkbox"/>																									
Require password change <input checked="" type="checkbox"/> on first login																									

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Identifying Roles

- Five built-in user roles:
  - **admin**, **power**, and **user**
    - ▶ Users can be assigned these roles
  - **can\_delete**
  - **splunk-system-role**
    - ▶ Special role that allows system services to run without a defined user context
- Administrators can add custom user roles

The screenshot shows a table titled "Roles" with a green "New Role" button in the top right corner. The table has columns for Name, Actions, Native capabilities, Inherited capabilities, and Default App. The "Default App" column for the "splunk-system-role" row contains the value "search".

Name	Actions	Native capabilities	Inherited capabilities	Default App
admin	<a href="#">View Capabilities</a>   <a href="#">Delete</a>	80	27	
can_delete	<a href="#">View Capabilities</a>   <a href="#">Delete</a>	2	0	
power	<a href="#">View Capabilities</a>   <a href="#">Delete</a>	6	21	search
splunk-system-role	<a href="#">View Capabilities</a>   <a href="#">Delete</a>	0	107	
user	<a href="#">View Capabilities</a>   <a href="#">Delete</a>	21	0	

# Defining Custom User Roles

Give the role a name and select a default app

**New Role**

Name \* ?

**Resources**  Inheritance  Capabilities  Indexes

Default app

Restrict search terms  
Can include only source, host, index, event type, source type, search term, or regular expression.  
Example: "host=web\*" OR source="/var/log/\*"

Restrict search time range  
Set a time window, in seconds, for searches for this role. For example, set to '60' to restrict searches for this role to 1 minute before the most recent time specified in the search. You can set the time window to '0' to make it infinite, or '-1' to disable it. Inherited roles can override this setting.

Restrict searches on certain fields, sources, hosts, etc

Default is -1 (no restriction)

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Defining Custom User Roles (cont.)

## Optional user-level and role-level limits

New Role X

User-level concurrent search job limit  
  
Set the maximum number of concurrent search jobs for each user of this role.

User-level concurrent real-time search job limit  
  
Set the maximum number of concurrent real-time search jobs for each user of this role. This count is independent of the standard search job limit.

Role-level concurrent search job limit  
  
Set the maximum number of cumulative concurrent search jobs for this role.

Role-level concurrent real-time search job limit  
  
Set the maximum number of cumulative concurrent real-time search jobs for this role. This count is independent from the standard search job limit.

Total search job disk quota  
  
Set the total disk space, in megabytes, that search jobs under a certain role can use. For example, '100' limits total disk usage by a role's search jobs to 100 MB.

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Describing Role Inheritance

- A new role can be based on one or more existing roles
- The new role inherits capabilities and index access
  - Inherited index access is not visible in the user interface
- You cannot disable inherited capabilities or access

The screenshot shows a user interface for managing roles. At the top, there are four tabs: 'Resources', 'Inheritance' (which is highlighted with a red box), 'Capabilities', and 'Indexes'. Below the tabs, there is a descriptive text: '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.' Underneath this text is a search bar labeled 'Role name' with a 'filter' button. A list of roles follows, each with a checkbox next to it:

- admin
- can\_delete
- power
- splunk-system-role
- user

# Assigning Capabilities

The **Source** dropdown filters the displayed role capabilities.

Capabilities inherited from other roles are selected.

Capability Name	filter	Source
accelerate_datamodel		Show native only
accelerate_search		Show native only
admin_all_objects		Show native only
apps_backup		Show native only
apps_restore		Show native only
change_authentication		Show native only
change_own_password		Show native only
delete_by_keyword		Show native only

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Role Index Search Options

- The **Indexes** tab controls which indexes the users in this role can access
  - If the **Included** checkbox for that index is not selected, users cannot search or even see this index
  - The **Default** checkbox defines the index when a user does not specify "`index=<index_name>`"
- Indexes inherited from a parent role are searchable and cannot be disabled

The screenshot shows the 'New Role' configuration page in Splunk. The 'Indexes' tab is selected, indicated by a red box. A yellow callout box points to the 'Included' checkbox for the '\_internal' index, with the text 'The dropdown filters the index list.' A dropdown menu is open next to the 'Included' checkbox, listing five options: 'Show selected', 'Show unselected', 'Show inherited', 'Show native', and 'Show all' (which is checked). The table lists various indexes with their 'Included' and 'Default' status.

Index Name	filter	Included	Default
All non-internal indexes		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
All internal indexes		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
_audit		<input type="checkbox"/>	<input type="checkbox"/>
_internal		<input type="checkbox"/>	<input type="checkbox"/>
_introspection		<input type="checkbox"/>	<input type="checkbox"/>
_telemetry		<input type="checkbox"/>	<input type="checkbox"/>
_thefishbucket		<input type="checkbox"/>	<input type="checkbox"/>
history		<input type="checkbox"/>	<input type="checkbox"/>

# Implications of Inheritance

---

- If you create a new role that inherits from another role, such as **user**:
  - The new role has all the capabilities of the inherited role
  - The new role inherits the index settings
  - You cannot turn off capabilities or index access that was inherited from the original role
- If you want a role that is "like" **user** but with some capabilities turned off:
  1. Make a new role that does not inherit from any other role
  2. Turn on all of the same capabilities as in User, except those you want turned off
  3. Assign the appropriate indexes to the new role

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# authorize.conf

- Roles can also be modified/added using **authorize.conf**
- Do not edit or delete roles in  
**SPLUNK\_HOME/etc/system/default/authorize.conf**
- Edit roles in local version  
**SPLUNK\_HOME/etc/system/local** or **SPLUNK\_HOME/etc/apps**

## authorize.conf

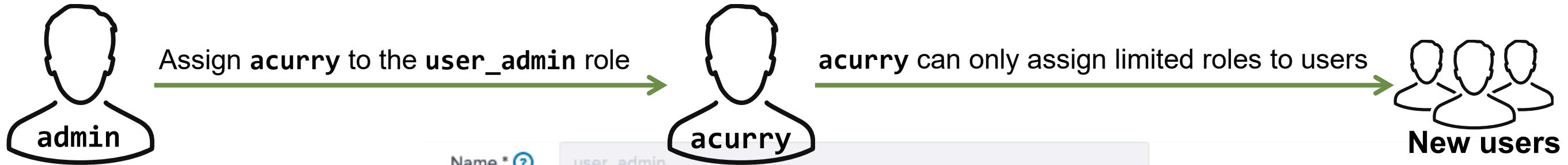
```
[role_user]
srchIndexesAllowed = main;websales
srchIndexesDefault = websales
srchMaxTime = 8640000
```

# `edit_roles_grantable` Capability

---

- Example: I want to separate and delegate administration tasks between sys admins and data admins without granting full **admin** role
- Issues to consider:
  - With `edit_roles` and `edit_user` capabilities, users can promote themselves to full **admin** role
  - Want to restrict grantable capabilities only to the level sub-admins currently have
- Configuration option:
  - Add the `edit_roles_grantable` capability to the **sub-admin** role
    - Can only create roles with subset of the capabilities that the current user role has
    - Must use in conjunction with the `edit_user` capability

# Example: edit\_roles\_grantable Capability



Add new role **user\_admin**

- Inheritance:
  - **power**
  - **user**
- Capabilities:
  - **edit\_roles\_grantable**
  - **edit\_user**

Source	Capability Name
inherited	accelerate_search
inherited	change_own_password
native	edit_roles_grantable
inherited	edit_search_schedule_window
inherited	edit_sourcetypes
inherited	edit_statsd_transforms
native	edit_user
inherited	embed_report

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Password Policy Management

- Password management options for administrators
  - Only applies to native Splunk users
    - ▶ Does not apply to SAML or LDAP passwords
  - Provides options for password rules, expiration, lockout, and history

From Splunk Web, select **Settings > Access controls > Password Policy Management**

**Access controls**  
Specify authentication method, manage user settings, and manage roles.

**Authentication method**

**Users** + Add new

**Roles** + Add new

**Password Policy Management**

<http://docs.splunk.com/Documentation/Splunk/latest/Security/Passwordbestpracticesforadministrators>

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Unlocking Users

- Users that have been locked out or have forgotten their password, can be unlocked or reset in Splunk Web or CLI
  - Using Splunk Web, select **Settings > User**

Name	Actions			Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Status
acurry	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>			LDAP	Amanda			launcher	system	securityops	<span style="color: green;">✓ Active</span>
admin	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>			Splunk	Administrator	changeme@example.com		launcher	system	admin	<span style="color: green;">✓ Active</span>
ayoung	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Delete</a> <a href="#">Unlock</a> ← <span style="color: green;">Splunk</span>							launcher	system	power	<span style="color: red;">🔒 Locked</span>

- Using CLI

```
splunk/bin/splunk edit user <lockeduser> -locked-out false  
-auth <admin:password>
```

# Admin Passwords

- An Admin password is **required** during installation and to start Splunk 7.1 for the first time
  - To create a password during startup

```
splunk/bin/splunk start --accept-license --answer-yes  
--no-prompt --seed-passwd <ch@ngeM3>
```

- To generate a random password during startup

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

<http://docs.splunk.com/Documentation/Splunk/latest/Security/Secureyouradminaccount>

# Splunk Authentication Options

- User accounts can be defined as:
  - Native Splunk accounts
  - LDAP or Active Directory
  - SAML
  - Scripted access to PAM, RADIUS, or other user account systems
- Saves the settings in **authentication.conf**

**Authentication method**

Access controls > Authentication method

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

Internal  Splunk Authentication (always on)

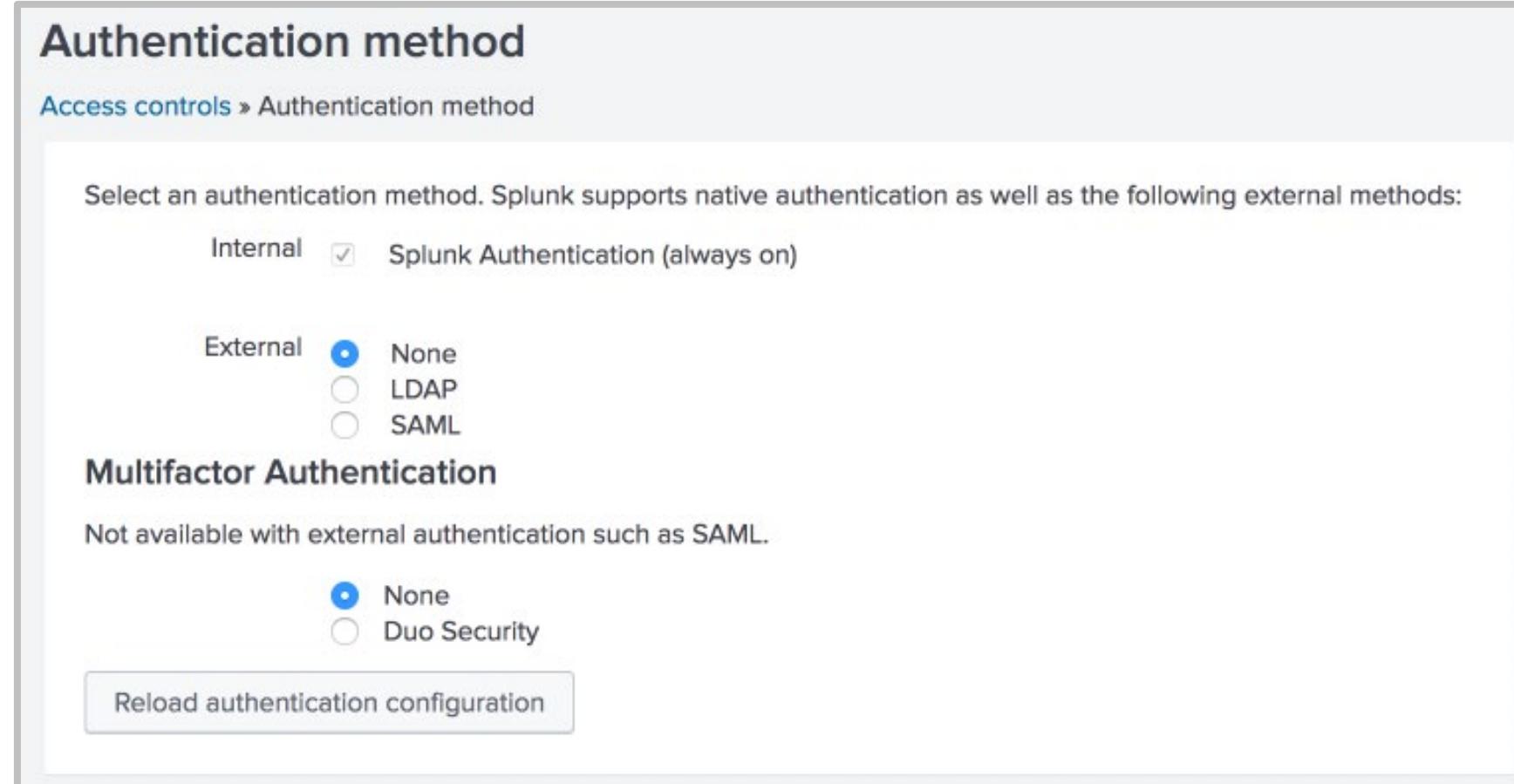
External  None  
 LDAP  
 SAML

**Multifactor Authentication**

Not available with external authentication such as SAML.

None  
 Duo Security

Reload authentication configuration



Note



More details in Appendix A

# 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

The screenshot shows two Splunk web pages related to LDAP group mappings:

**splunkAdmins** (Left Page):

- Available Roles:** admin, can\_delete, power, splunk-system-role, user.
- Selected Roles:** admin.
- Action Buttons:** "add all >" and "< clear all".
- Text Overlay:** "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

**LDAP Groups** (Right Page):

- Header:** Access controls > Authentication method > LDAP strategies > LDAP Groups
- Table Headers:** LDAP Group Name, LDAP Strategy, Group type, Roles.
- Data:** Showing 1-4 of 4 items
- Table Rows:**

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
- Text Overlay:** After completing the mapping for all LDAP groups, the mapped roles are shown here.

Generated for YongHyeok Jeong (yh.jeong@time-gate.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

Access Control » Users

13 Users filter 10 per page ▾

< Prev 1 2 Next >

Name	Actions	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Status
acurry	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>	LDAP	Amanda		launcher	system		securityops	✓ Active
admin	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>	Splunk	Administrator	changeme@example.com	launcher	system		admin	✓ Active
blu	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>	LDAP	Bao Lu		launcher	system		user	✓ Active
coryf	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>	LDAP			launcher	system		admin	✓ Active
dhalo	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>				launcher	system		user	✓ Active
emaxwell	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Delete</a>	Splunk			launcher	system		power	✓ Active
gvoronoff	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>	LDAP	Gabriel Voronoff		launcher	system		admin	✓ Active

Click to edit the user settings

Generated for YongHyeok Jeong (yh.jeong@time-gate.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. You will have to create a new role that does NOT inherit from the user role, turn on all of the same capabilities as in user role, except those you want turned off**
- True or False. You can unlock a user from the CLI.  
**True.**

# Lab Exercise 7 – Add Roles and Users

---

**Time:** 15 minutes

**Tasks:**

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

# Module 8: Configuring Basic Forwarding

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Module Objectives

---

- Identify forwarder configuration steps
- List Splunk forwarder types
- Configure the forwarder
- Identify forwarder configuration files

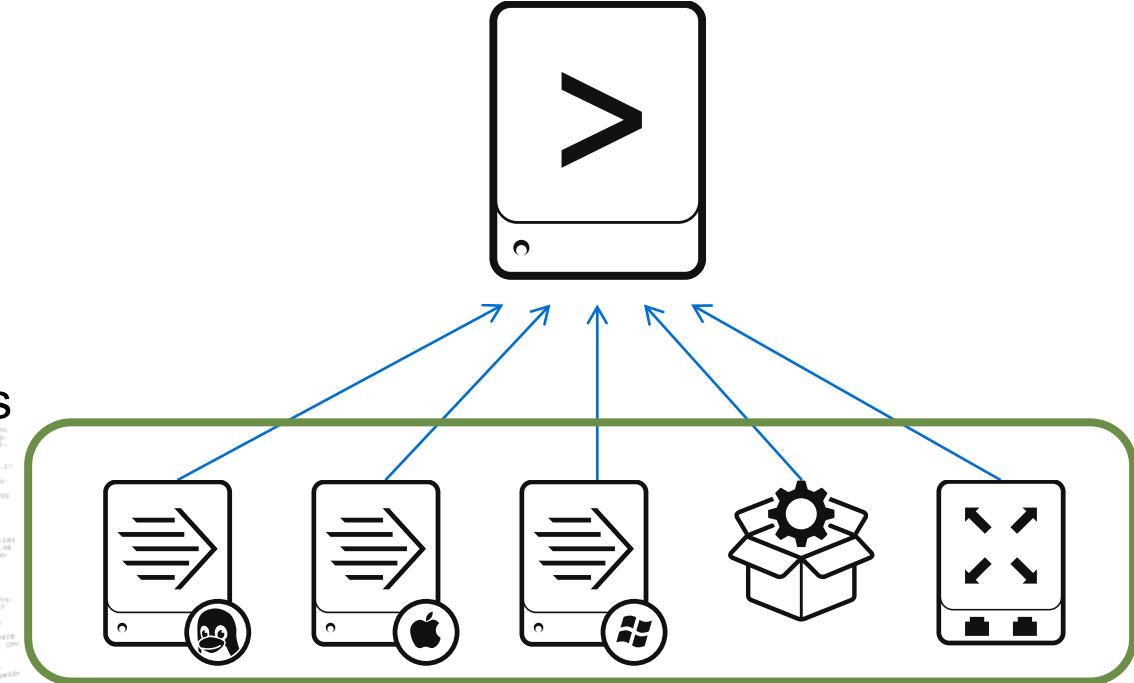
# Got Data?



- Computers
- Network devices
- Virtual Machines
- Internet of Things (IoT)
- Communication devices
- Sensors
- Databases
- **Any source**



- Logs
- Configurations
- Messages
- Call Detail Records
- Clickstream
- Alerts
- Metrics
- Scripts
- Changes
- Tickets
- **Any data**

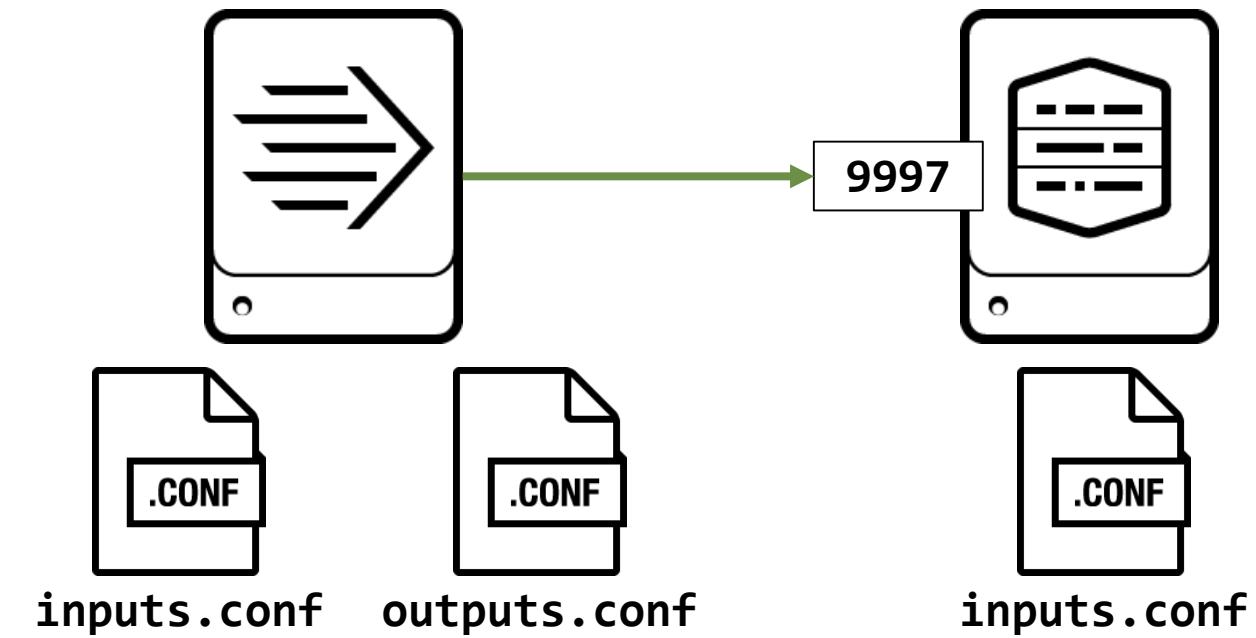


Indexes any data from any source

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Forwarders and Indexers

- In a production environment
  - Splunk indexers run on dedicated servers
  - The data you want is on remote machines
- Install Splunk **forwarders** on the remote machines to
  - Gather the data
  - Send it across the network to the Splunk indexer(s)
- Indexers listen on a **receiving port** for the forwarded data



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Deployment Server/Forwarder Management

---

- In larger or production environments, forwarders can be managed remotely
- Splunk Deployment Server provides a Forwarder Management interface
  - A centralized configuration management tool to manage forwarder configuration
  - Allows forwarders to be managed in groups (server classes)
- In this class, we will set up a single forwarder manually for testing
- Deployment server is discussed in detail in the Splunk Enterprise Data Administration class

# Forwarder Configuration Steps

---

1. Set up a receiving port on each indexer
  - It is only necessary to do this once
2. Download and install Universal Forwarder
3. Set up forwarding on each forwarder
  - Either manually or using Deployment Server
4. Add inputs on forwarders, using one of the following:
  - Forwarder management
  - CLI
  - Edit `inputs.conf` manually

# 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**
- Using CLI:  
**splunk enable listen <port>**
- The configuration is saved in **inputs.conf** as:  
**[splunktcp://portNumber]**

**Forwarding and receiving**

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

[Forwarding defaults](#)

[Configure forwarding](#) + Add new

**Receive data**  
Configure this instance to receive data forwarded from other instances.

[Configure receiving](#) + Add new

**Configure receiving**

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port \*

For example, 9997 will receive data on TCP port 9997.

Cancel Save

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

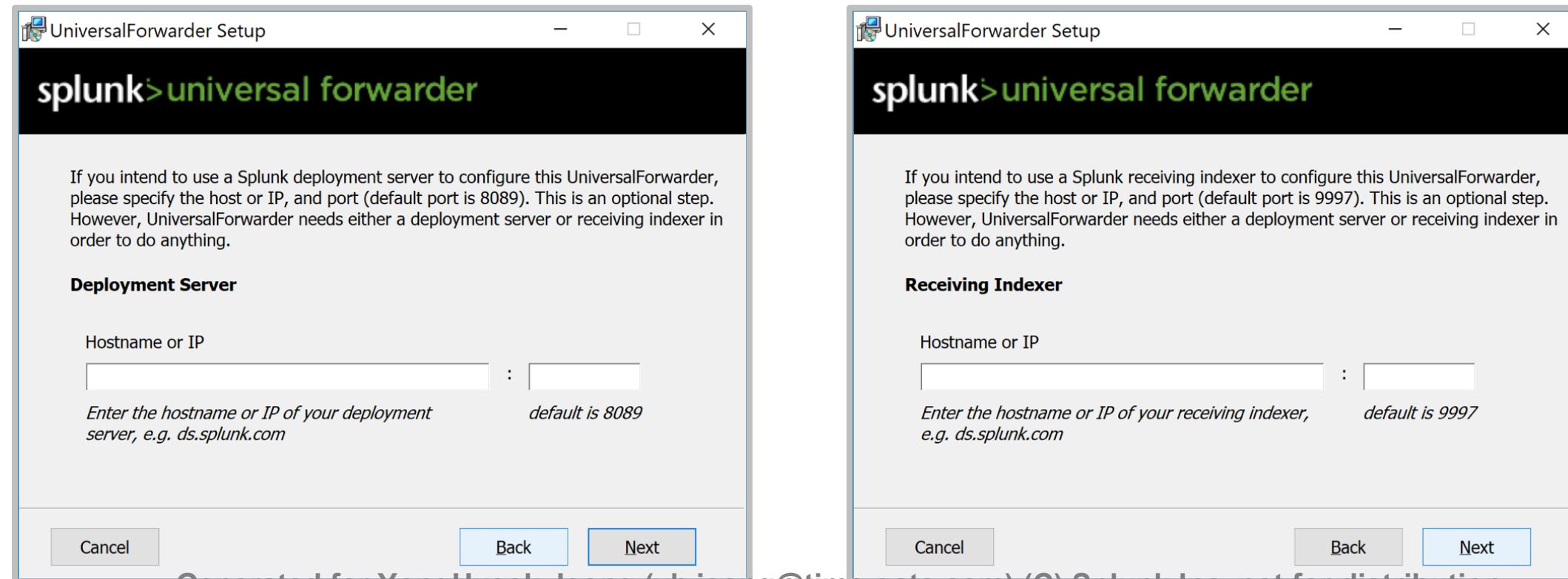
# Installing Universal Forwarder

---

- \*NIX: unpack the `.tgz` or `.tgz.z` in the desired location
- Windows: execute the `.msi` or use the command line
  - Installed as a service
- **SPLUNK\_HOME** is the installation directory, defaults to  
`/opt/splunkforwarder` or  
`c:\Program Files\SplunkUniversalForwarder`
- Same `splunk` command-line interface in **SPLUNK\_HOME/bin**
  - Same commands for start/stop, restart, etc.
  - An **admin** account and password are required
- When installing large numbers of forwarders, use an automated method

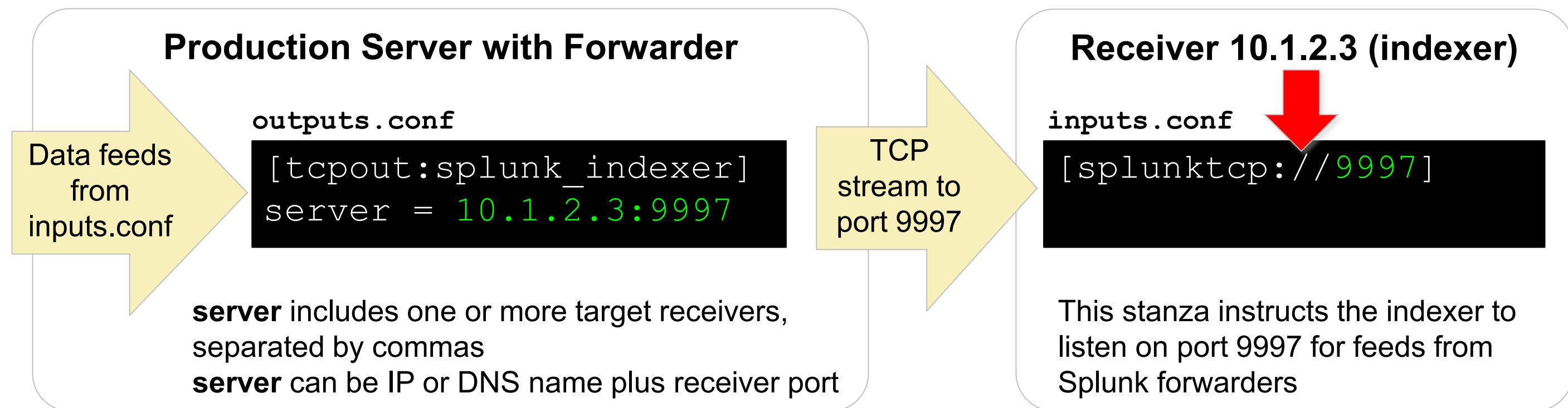
# Using the Interactive Windows Installer

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



# Forwarder Configuration Files

- Forwarders require **outputs.conf**
  - **outputs.conf** points the forwarder to the receiver(s)
  - Can specify additional options for load balancing, SSL, compression, alternate indexers, and indexer acknowledgement



# Defining Target Indexers on the Forwarder

- Execute on the forwarder for each destination indexer:

**splunk add forward-server indexer:receiving-port**

- For example, **splunk add forward-server 10.1.2.3:9997** configures the **outputs.conf** as:

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

[tcpout-server://10.1.2.3:9997]

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

[docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Configureforwardingwithoutputs.conf](https://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Configureforwardingwithoutputs.conf)

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Configuration and Connection Validation

---

- After running **splunk add forward-server**, the forwarder should be communicating with the indexer
  - Splunk forwarder logs are automatically sent to the indexer's **\_internal** index
- To check the configuration:
  - On the indexer, run **splunk display listen**
  - On the forwarder, run **splunk list forward-server**
- To check for successful connection:
  - On the indexer, search  
**index=\_internal host=forwarder\_hostname**
- To remove the target indexer setting:
  - On the forwarder, run  
**splunk remove forward-server indexer:port**

# Module 8 Knowledge Check

---

- True or False. You have to 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.
- The command **splunk add forward-server indexer:receiving-port** will create stanza(s) in which config file?

# Module 8 Knowledge Check – Answers

---

- True or False. You have to configure a separate receiving port on the indexer for each universal forwarder.  
**False. You do not **have** to create a separate port for each UF.**
- 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.**
- The command **splunk add forward-server indexer:receiving-port** will create stanza(s) in which config file?  
**outputs.conf**

# Lab Exercise 8 – Basic Forwarder Configuration

---

**Time:** 20 minutes

**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 and the `inputs.conf` file on the indexer

# Module 9: Distributed Search

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

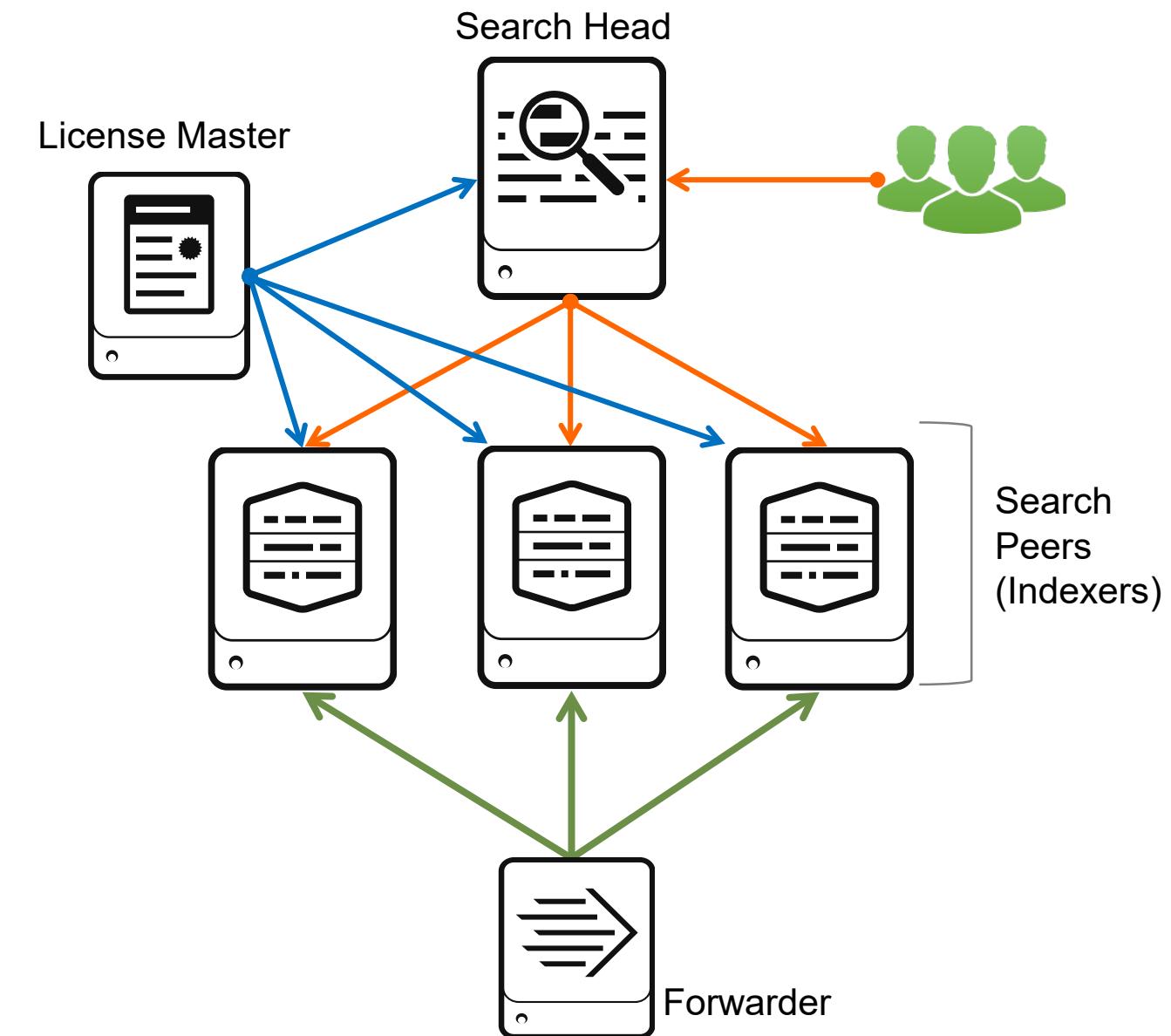
# Module Objectives

---

- Describe how distributed search works
- Explain the roles of the search head and search peers
- Configure a distributed search group
- List search head scaling options

# Distributed Search

- Production servers with universal forwarders send data to indexers
- Indexers (peers) store their portion of the data
- Users log on to the search head and run reports
  - The search head dispatches searches to the peers
  - Peers run searches in parallel and return their portion of results
  - The search head consolidates the individual results and prepares reports



# Setting Up Distributed Search

- Install Splunk on each search head and peers (indexers)
- Set up the same indexes on all peers
- All search heads and peers should use a license master
- Add a user to each peer with a role that has the **edit\_user** capability
  - Used only for authenticating a search head to the peers
- On the search head, configure search peers by selecting:  
**Settings > Distributed search**
  - Distributed search is turned **on** by default, so just add search peers

**Distributed search**  
Perform a search across multiple Splunk indexers.

[Distributed search setup](#)

[Search peers](#) [+ Add new](#)

# Adding Search Peers

- Select **Settings > Distributed search > Search peers > Add new**
- Enter the **servername:port** for a search peer
- Enter a username and password of an account on the search peer
  - The account must have the **edit\_user** capability
  - You should create an account on each peer for this purpose

**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**

# Knowledge Bundles and Replication

---

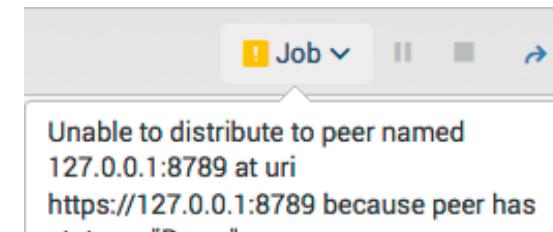
- Knowledge bundles are distributed to search peers by the search head when a distributed search is initiated
- They contain the knowledge objects required by the indexers for searching
- Knowledge bundles' locations:
  - `$SPLUNK_HOME/var/run`** on the search head
  - `$SPLUNK_HOME/var/run/searchpeers`** on the search peer
- Replication status of knowledge bundles can be viewed from **Replication Status** column of the Splunk Web home page  
**Settings > Distributed search > Search peers**

# Peer Failure

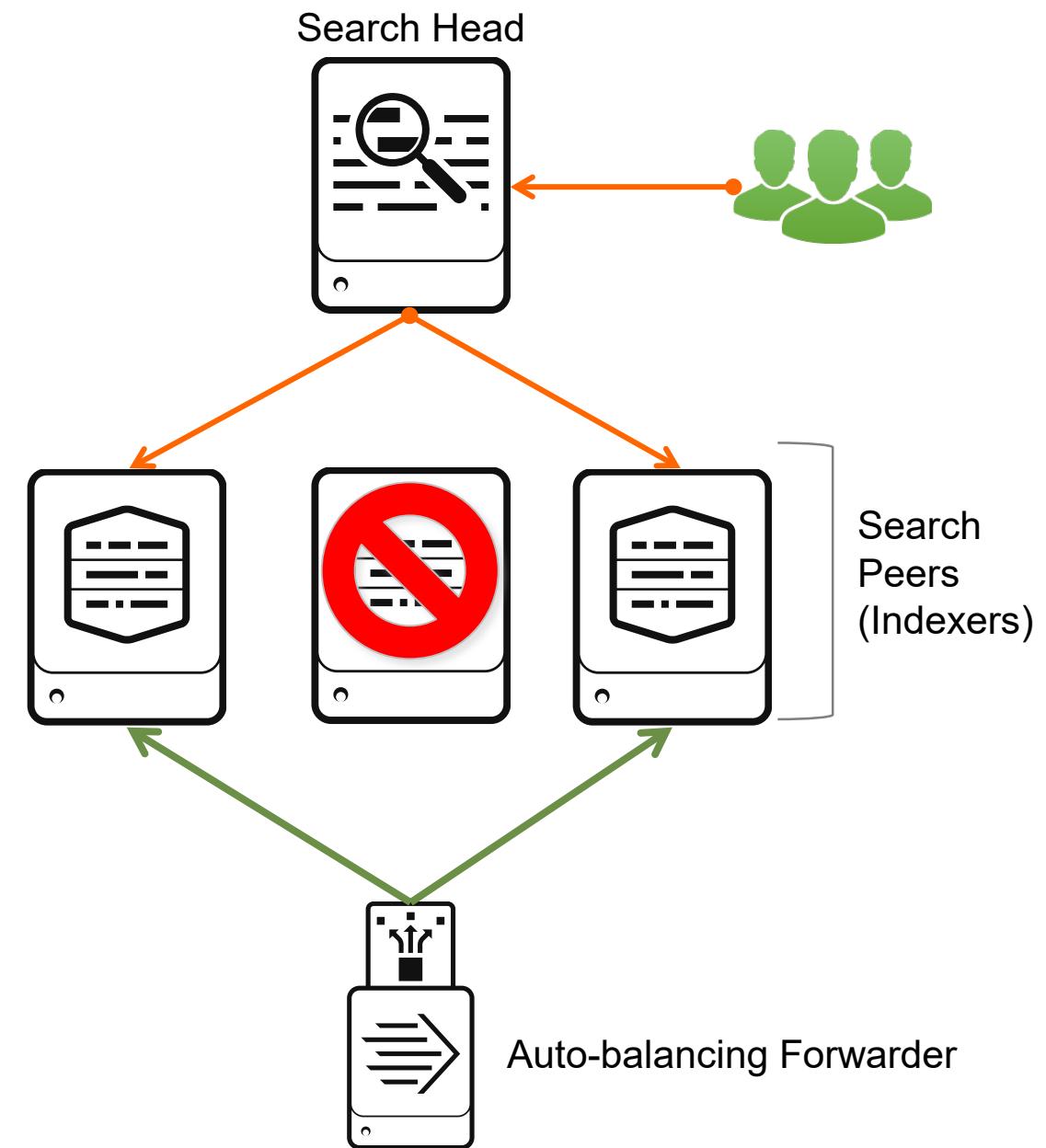
- When an indexer goes down:
  - The forwarder automatically uses only the available indexers
  - The offline indexer does not participate in searches
  - The remaining indexers handle all indexing and searches
- If a peer goes down during a job, a notification is sent to the user that the job is potentially incomplete

 Search results may be incomplete: the search process on peer myindexer2 ended prematurely. search's <a href="https://127.0.0.1:8789/services/search/jobs/remote\_mysearchhead\_139207 a possible crash log in the myindexer2's \$SPLUNK\_HOME/var/log/splunkd directory.

- If a peer is already down, a message indicates which peer is down



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution



# Viewing Search Peer Status with MC

- The **Search Activity: Instance** dashboard in the MC provides a graphical view of the status of your search peers
  - Median resource usage (Memory, CPU)
  - Top 10 Memory-Consuming Searches
  - Aggregate Search Runtime

The screenshot shows the Splunk Enterprise interface with the 'Search' tab selected in the top navigation bar. A dropdown menu is open under the 'Search' tab, listing several options: 'Search Activity: Instance' (which is highlighted with a blue border), 'Search Usage Statistics: Instance' (which has a checked checkbox next to it), 'KV Store: Instance', and 'Scheduler Activity: Instance'. A green callout bubble points to the 'Search Activity: Instance' option with the text 'Select Search > Search Activity: Instance'.

# Search Peer Quarantine

---

- If a search peer is experiencing performance issues, it can be quarantined from participating in future searches
  - Allows you to perform live troubleshooting by not stopping the search peer
  - It is prevented from performing new searches but continues to attempt to service any currently running searches
  - Only affects the relationship between search peer and search head
- From the search head, run the following CLI command:  
`splunk edit search-server -auth <user>:<password> <host:<port> -action quarantine`
- To use Splunk Web: **Settings > Distributed search > Search peers**

# Use Cases for Multiple Search Heads

---

- Access control
  - Control who can access which indexes using what apps
  - Dedicate a search head for each functional area – IT Ops, Security, or 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

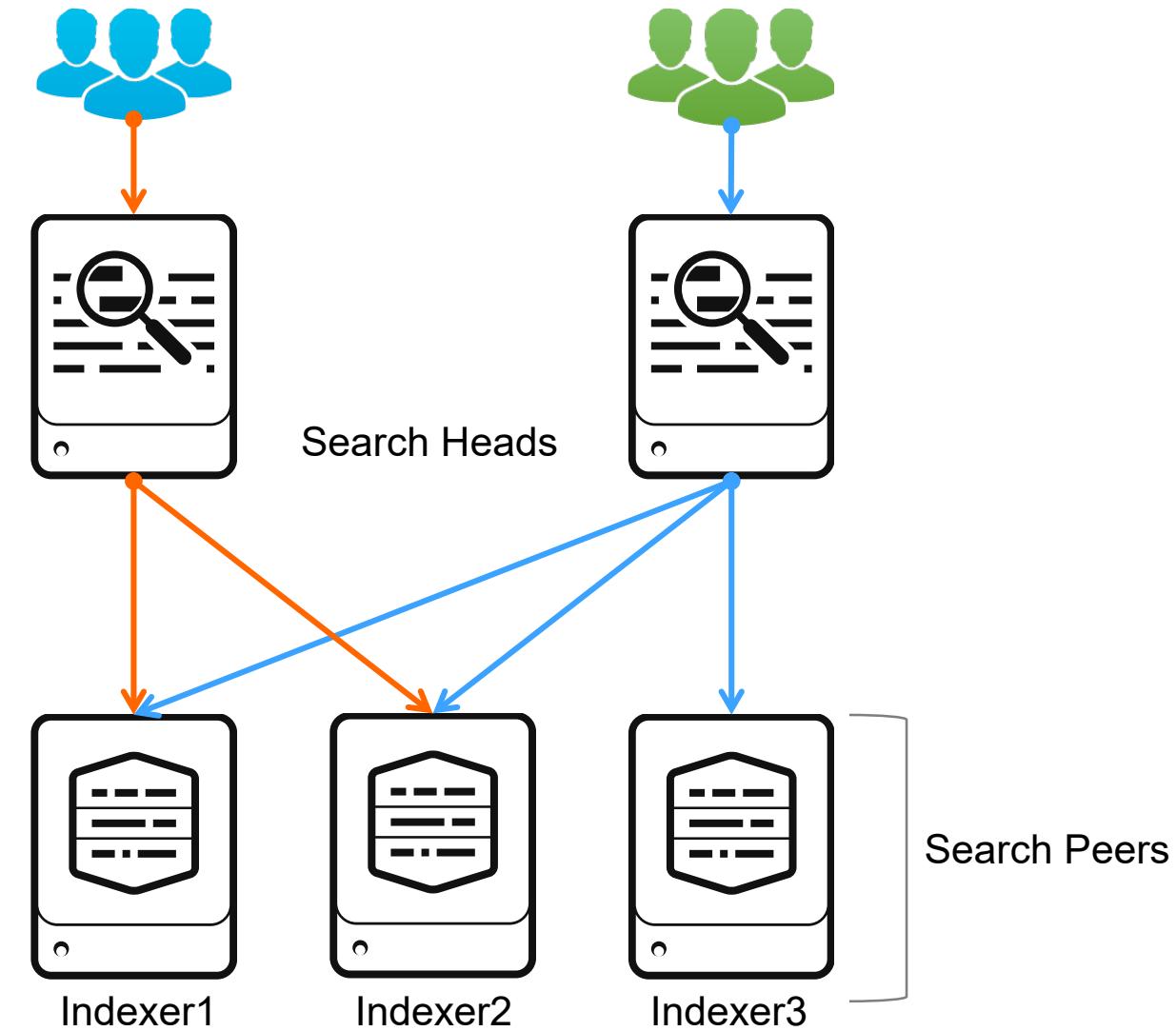
# How Many Search Heads?

---

- One dedicated search head can handle around 8 to 12 simultaneous searches (ad hoc or scheduled)
  - Exact numbers depend on types of searches and the hardware of the search head; especially number of CPU cores
- Search heads can be added to the distributed group at any time
- Search heads can be **dedicated** or **clustered**
  - Dedicated search heads don't share knowledge objects (separate small teams)
  - Search head cluster shares a common set of knowledge objects (large teams)

# Dedicated Search Heads

- More than one search head can be configured for the same set of search peers
- Each search head
  - Contains its own unique set of reports, dashboards, etc.
  - Is dedicated to one team of users who want to have unique knowledge objects for their own use
- Good when you have teams of different people who don't share knowledge objects



# Distributed Search Best Practice

- Forward all search head indexes to the search peer (indexer) layer
  - Simplifies the process of managing indexes
  - Can diagnose from other search heads if one goes down
  - Allows other search heads to access all summary indexes

The screenshot shows the Splunk Forwarding and receiving interface. On the left, there's a sidebar with 'Forwarding and receiving' and 'Forward data'. Below that are two buttons: 'Forwarding defaults' (highlighted with a green border) and 'Configure forwarding'. A green arrow points from the 'Forwarding defaults' button to a modal window titled 'Forwarding defaults'. Inside the modal, there's a radio button group for 'Store a local copy of forwarded events?' with 'No' selected (indicated by a red circle with '1'). Below it is a note: 'This saves a copy of all indexed data on this Splunk instance and forwards copies to other instances.' At the bottom right of the modal is a 'Save' button (also highlighted with a red circle with '1'). Another green arrow points from the 'Configure forwarding' button to a 'Configure forwarding' section at the bottom of the page. This section has a '+ Add new' button (highlighted with a red circle with '2') and a green arrow pointing to the generated configuration file on the right.

**outputs.conf**

```
[indexAndForward]
index = false

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

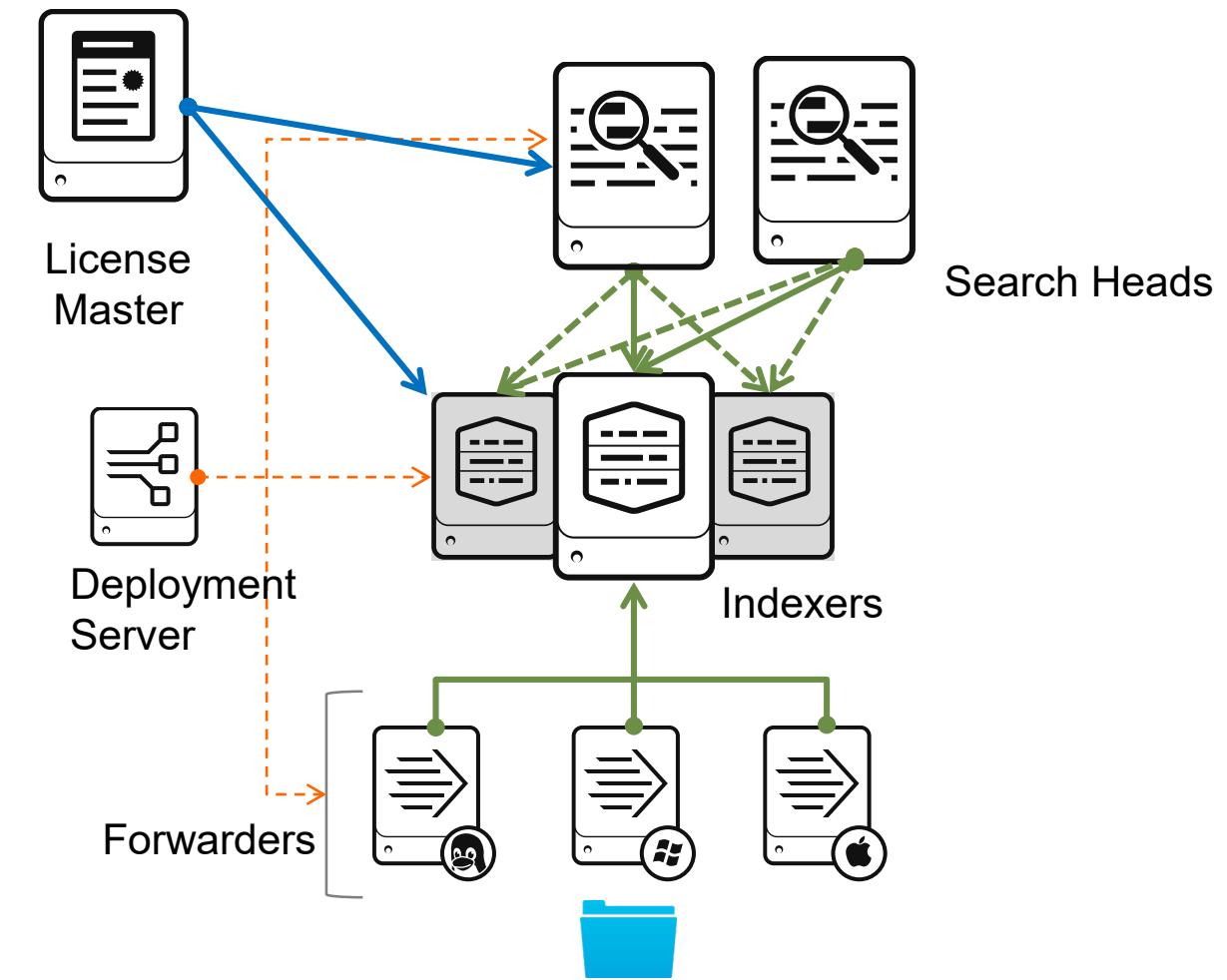
[tcpout:default-autolb-group]
server=idx1:9997, idx2:9997
```

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Best Practices

- Splunk recommends that you dedicate a host for each role
  - You can enable multiple Splunk server roles on a server with caveats (discussed in the Architecting Splunk Deployments course)
- Disable Web on instances that don't need the web interface

```
./splunk disable webserver
```
- Deployment Server can be used to manage Splunk Instance remotely (more details in the Splunk Enterprise Data Admin course)



# Module 9 Knowledge Check

---

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

# Lab Exercise 9 – Distributed Search

---

**Time:** 10 minutes

**Tasks:**

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

# Module 10: Introduction to Splunk Clusters

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Module Objectives

---

Introduce Splunk clustering concepts

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

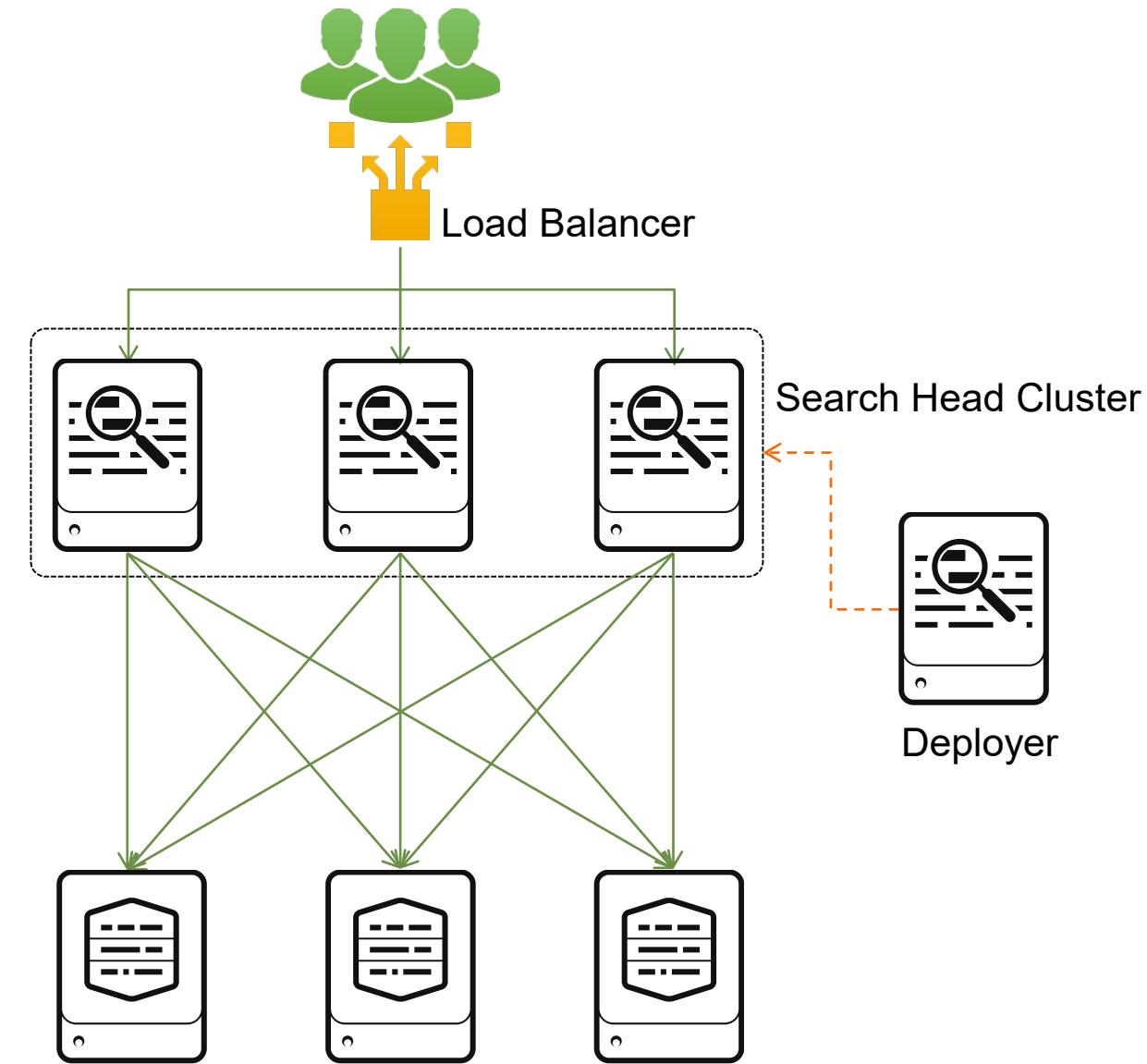
# Splunk Clustering

---

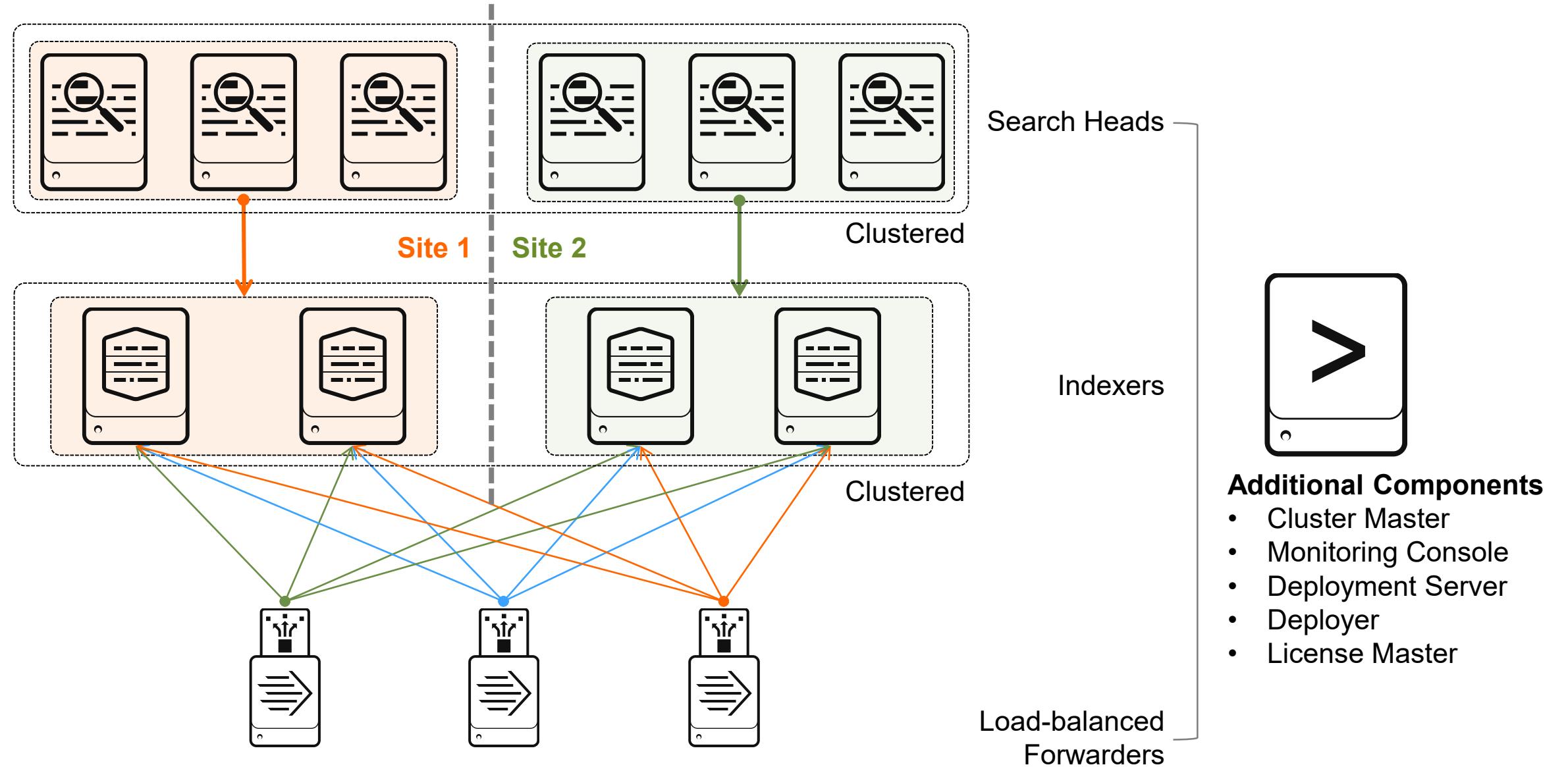
- Splunk provides two types of clustering: search head clustering and indexer clustering
- Search head clustering
  - Replicates knowledge objects across search heads
- Indexer clustering
  - Replicates buckets (data) across indexers
  - Can be configured as single-site or multi-site
  - Allows you to balance growth, speed of recovery, and overall disk usage
- Requires only Splunk enterprise license
- Splunk Clustering is discussed in detail in **Splunk Cluster Administration** class

# 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
- Can configure an external (non-Splunk) load balancer to provide transparent access to the cluster



# Splunk Cluster Overview



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Index Replication

---

- Splunk indexers can function as a **cluster**
  - Indexers in a cluster replicate buckets amongst themselves
- Index replication allows for rapid failure recovery
- Fully configurable replication allows you to balance speed of recovery and overall disk usage
  - Index replication requires additional disk space
- Allows for Auto Indexer Discovery
  - Forwarders “discover” the available indexers instead of hard-coding **outputs.conf**
- Does not require additional license quota
- Discussed in detail in **Splunk Cluster Administration** class

# Further Reading: Clustering

---

- Basic clustering concepts for advanced users

[docs.splunk.com/Documentation/Splunk/latest/Indexer/Basicconcepts](https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Basicconcepts)

- Configure the search head

[docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCconfigurationoverview](https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCconfigurationoverview)

- Indexer discovery

[docs.splunk.com/Documentation/Splunk/latest/Indexer/indexerdiscovery](https://docs.splunk.com/Documentation/Splunk/latest/Indexer/indexerdiscovery)

# Module 10 Knowledge Check

---

- What are the two types of clustering provided by Splunk?

# Module 10 Knowledge Check – Answers

---

- What are the two types of clustering provided by Splunk?

Indexer clustering and search head clustering.

# Course Wrap-up

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Support Programs

---

## • Community

- **Answers:** [answers.splunk.com](https://answers.splunk.com)  
Post specific questions and get them answered by Splunk community experts.
- **Splunk Docs:** [docs.splunk.com](https://docs.splunk.com)  
These are constantly updated. Be sure to select the version of Splunk you are using.
- **Wiki:** [wiki.splunk.com](https://wiki.splunk.com)  
A community space where you can share what you know with other Splunk users.
- **IRC Channel:** #splunk on the EFNet IRC server Many well-informed Splunk users “hang out” here.

## • Global Support

Support for critical issues, a dedicated resource to manage your account – 24 x 7 x 365.

- **Phone:** **(855) SPLUNK-S or (855) 775-8657**
- **Web:** [http://www.splunk.com/index.php/submit\\_issue](http://www.splunk.com/index.php/submit_issue)

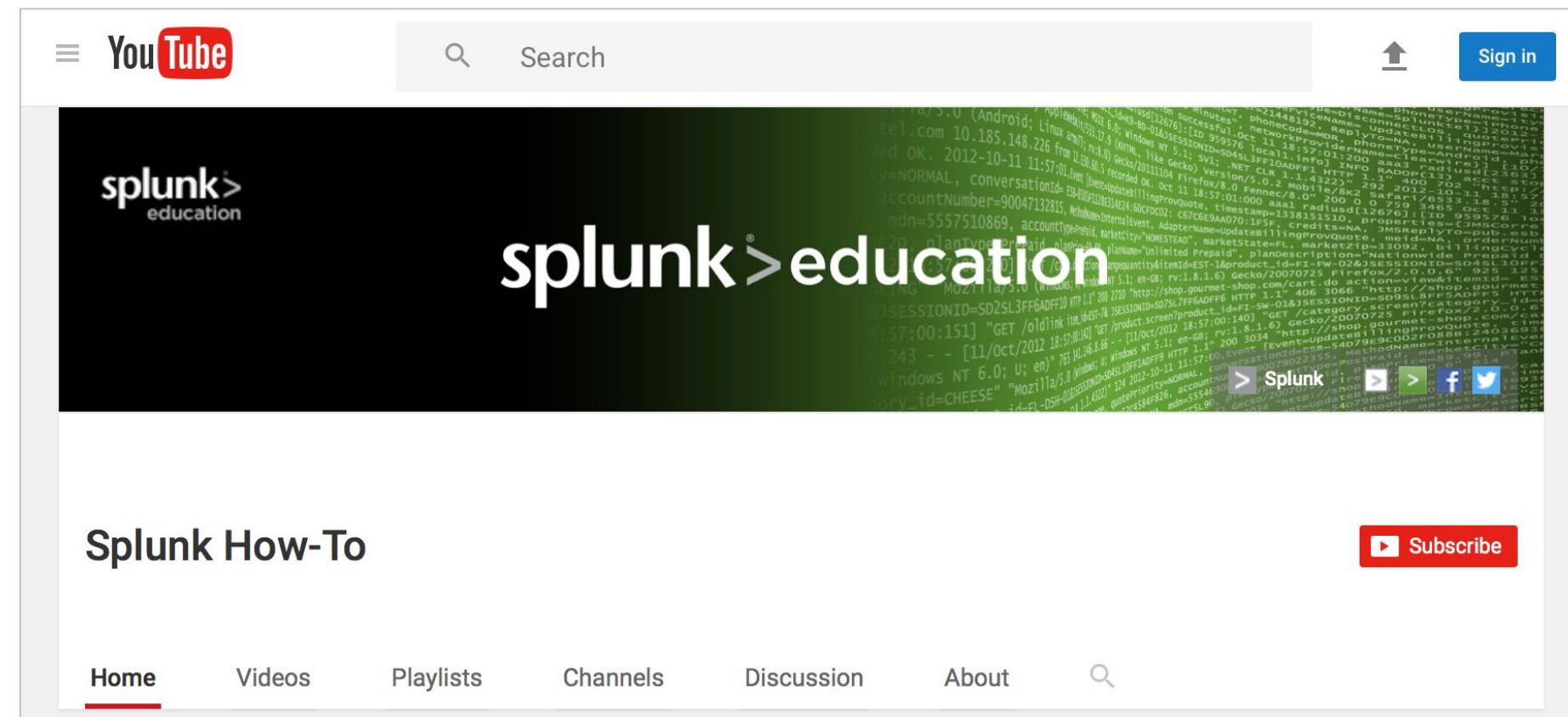
## • Enterprise Support

Access your customer support team by phone and manage your cases online 24 x 7  
(depending on support contract).

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# YouTube: The Splunk How-To Channel

- In addition to our roster of training courses, check out the Splunk Education How-To channel: <http://www.youtube.com/c/SplunkHowTo>
- This site provides useful, short videos on a variety of Splunk topics



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# What's Next?

---

- Splunk Certification program

[https://www.splunk.com/en\\_us/training/faq-training.html](https://www.splunk.com/en_us/training/faq-training.html)

- Program information

<https://www.splunk.com/pdfs/training/Splunk-Certification-Candidate-Handbook.pdf>

- Exam registration

<https://www.splunk.com/pdfs/training/Exam-Registration-Tutorial.pdf>

- If you have further questions, send an email to:  
[certification@splunk.com](mailto:certification@splunk.com)



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

splunk® > .conf19

.conf19

October 21-24, 2019

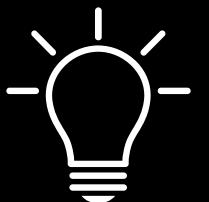
Splunk University

October 19-21, 2019

Las Vegas, NV

The Venetian Sands Expo

4 Days of Innovation



350 Education Sessions



20 Hours of Networking



sign up for notifications @ [conf.splunk.com](http://conf.splunk.com)

# Thank You

---



Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Appendix A: Splunk Authentication Management

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

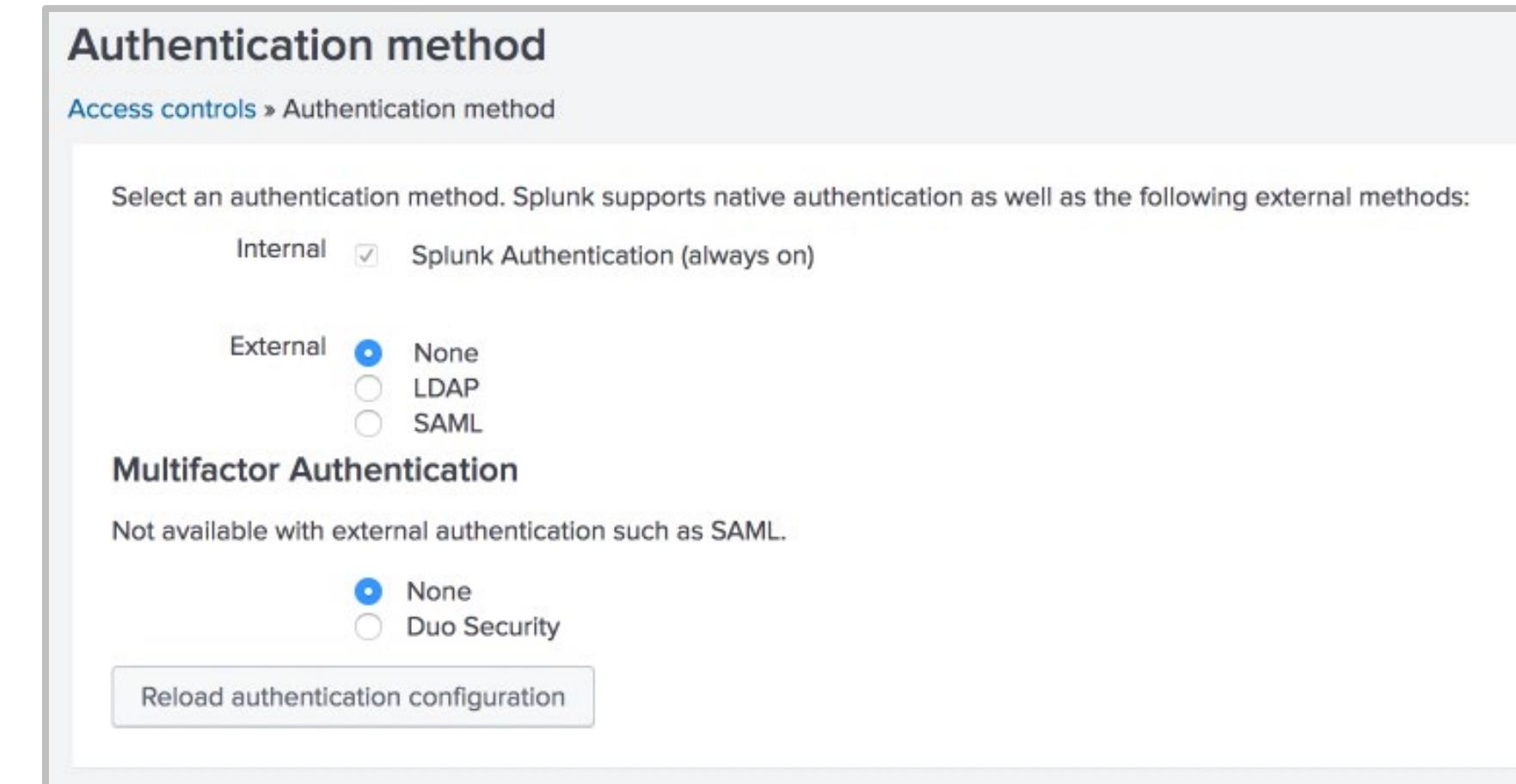
# Module Objectives

---

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

# Splunk Authentication Options

- User accounts can be defined as:
  - Native Splunk accounts
  - LDAP or Active Directory
  - SAML
  - Scripted access to PAM, RADIUS, or other user account systems
- Saves the settings in **authentication.conf**



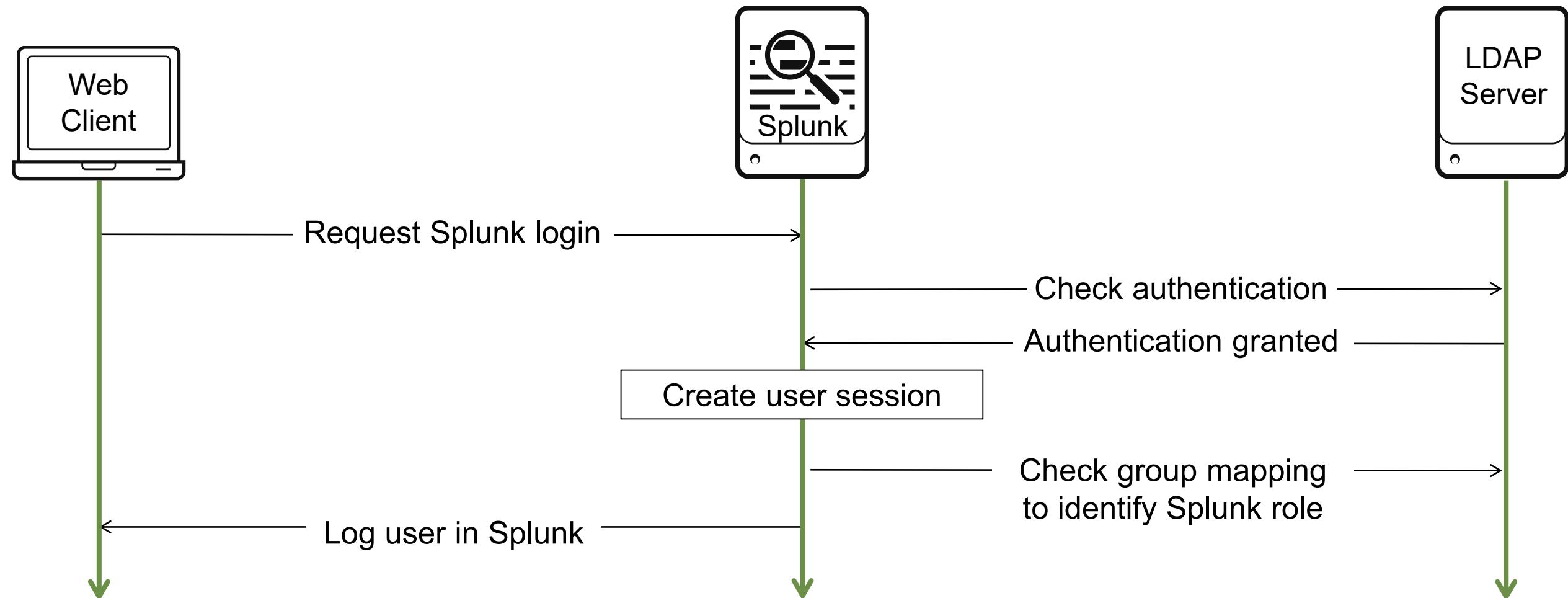
# Directory Server Integration

---

- **Best practice:** integrate Splunk with a directory server
  - Works with multiple LDAP servers, including OpenLDAP and Active Directory
  - You can configure from Splunk Web or CLI
- User accounts stored in directory server
  - Enforces LDAP user account and password policies
  - Users use the same user name and password in Splunk that they use elsewhere
  - LDAP groups must be mapped to Splunk roles
    - ▶ Or, this can be done manually in Splunk

# LDAP Authentication

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



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Creating an LDAP Strategy

1. Select **LDAP**
2. Click **Configure Splunk to use LDAP**
  - The list of current LDAP strategies displays
    - A strategy is a connection to one or more LDAP nodes on an LDAP server
  - Can define multiple LDAP servers
3. Click **New** to add a new LDAP strategy
  - Name the strategy and fill out the form

The image shows two screenshots of the Splunk web interface. The top screenshot is titled 'Authentication method' under 'Access controls > Authentication method'. It displays a list of authentication methods: 'Internal' (checked) and 'Splunk Authentication (always on)', and 'External' (radio buttons for 'None', 'LDAP' (selected), and 'SAML'). A green arrow labeled '1' points to the 'External' section. Another green arrow labeled '2' points to the 'Configure Splunk to use LDAP' link. A third green arrow labeled '3' points to the 'New LDAP' button in the bottom right corner of the 'LDAP strategies' screen. The bottom screenshot is titled 'LDAP strategies' under 'Access controls > Authentication method > LDAP strategies'. It shows a message: 'There are no configurations of this type. Click the "New LDAP" button to create a new configuration.' The 'New LDAP' button is highlighted with a green circle and an arrow.

# LDAP Strategy Settings

- Normally the configuration is based on the information given to you by the LDAP administrators
  - LDAP connection settings
  - User settings
    - Determine which part of the LDAP directory stores Splunk users
  - Group settings & Dynamic group settings
    - Determine which node in the directory contains your group definitions
  - 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

## LDAP strategies

Access controls » Authentication method » LDAP strategies

Successfully saved "AD\_splunkers". Successfully performed a bind to the LDAP server.

Showing 1-1 of 1 item

LDAP strategy name	Host	Port	Connection order	Status	Actions
AD_splunkers	10.0.0.150	389	1	Enabled   Disable	<a href="#">Map groups</a>   <a href="#">Clone</a>   <a href="#">Delete</a>

| « Back to strategies

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

Select **Map groups** to define relationships between LDAP groups and Splunk roles

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

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Mapping LDAP Groups to Roles (cont.)

**splunkAdmins**

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

Available Roles

- admin
- can\_delete
- power
- splunk-system-role
- user

Selected Roles

- admin

« clear all

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

**LDAP Groups**

Access controls > Authentication method > LDAP strategies > LDAP Groups

Showing 1-4 of 4 items

filter

25 per page ▾

| « Back to strategies

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

- 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

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

# 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

Access Control » Users

13 Users filter 10 per page ▾

< Prev 1 2 Next >

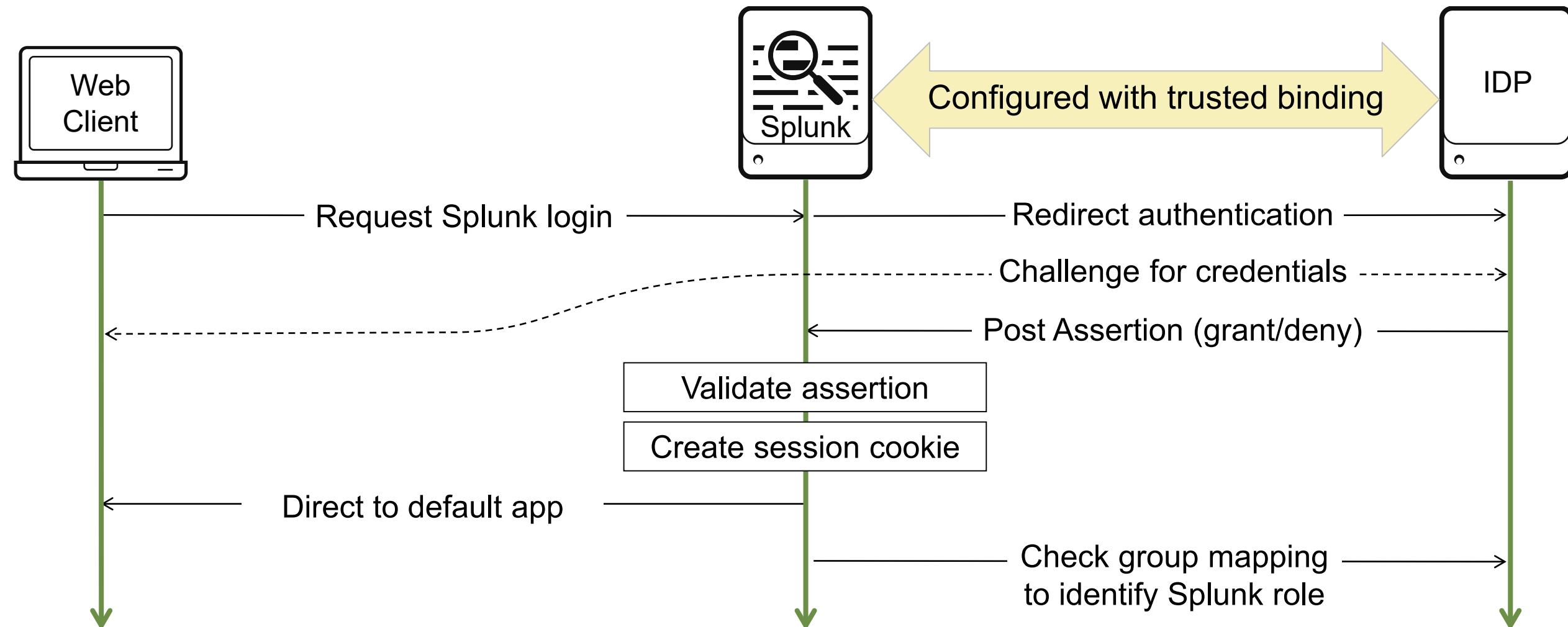
Name	Actions	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Status
acurry	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>	LDAP	Amanda		launcher	system		securityops	<span>✓ Active</span>
admin	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>	Splunk	Administrator	changeme@example.com	launcher	system		admin	<span>✓ Active</span>
blu	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>	LDAP	Bao Lu		launcher	system		user	<span>✓ Active</span>
coryf	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>				launcher	system		admin	<span>✓ Active</span>
dhalo	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>				launcher	system		user	<span>✓ Active</span>
emaxwell	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Delete</a>	Splunk			launcher	system		power	<span>✓ Active</span>
gvoronoff	<a href="#">View Capabilities</a> <a href="#">Edit</a> <a href="#">Clone</a>	LDAP	Gabriel Voronoff		launcher	system		admin	<span>✓ Active</span>

Click to edit the user settings

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

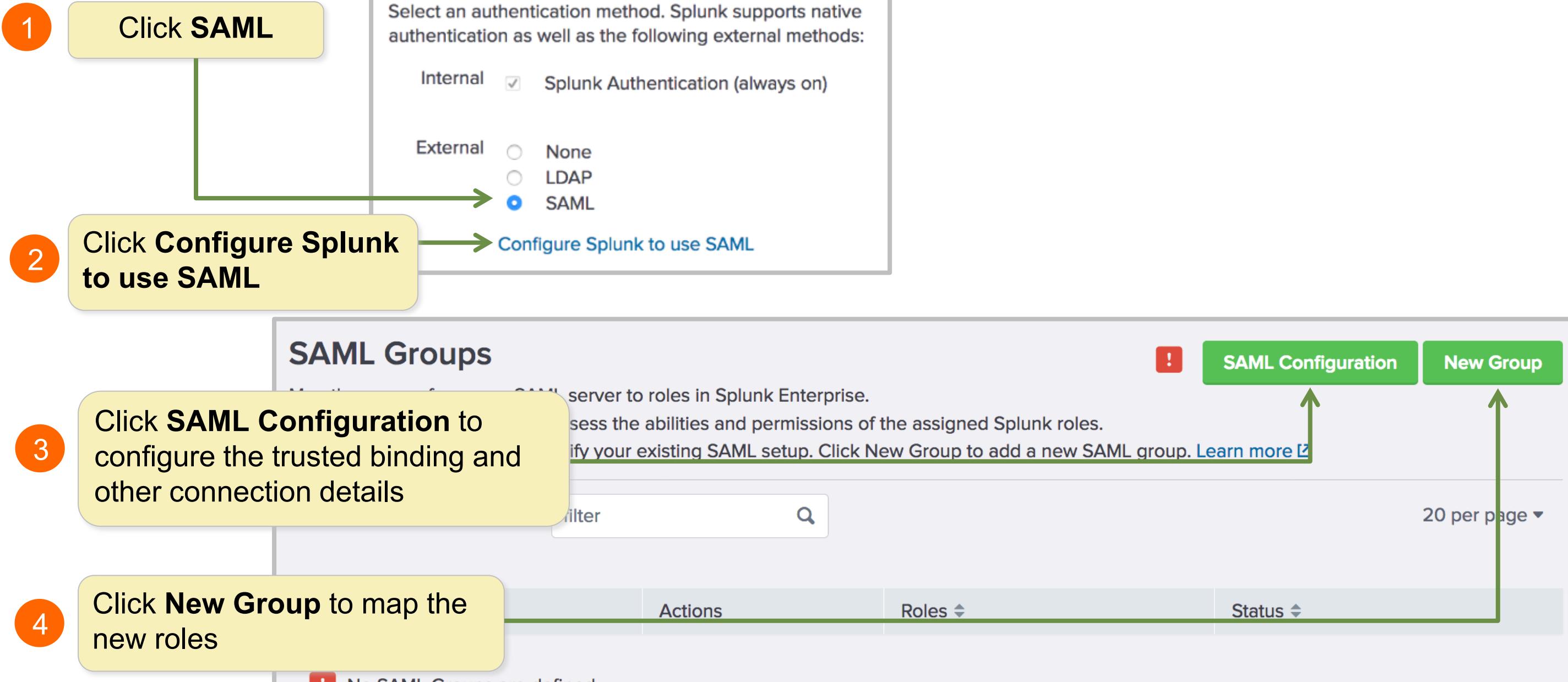
# SAML 2.0 Single Sign On

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



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Configuring SAML



Generated for YongHyeok Jeong (yh.jeong@time-gate.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.

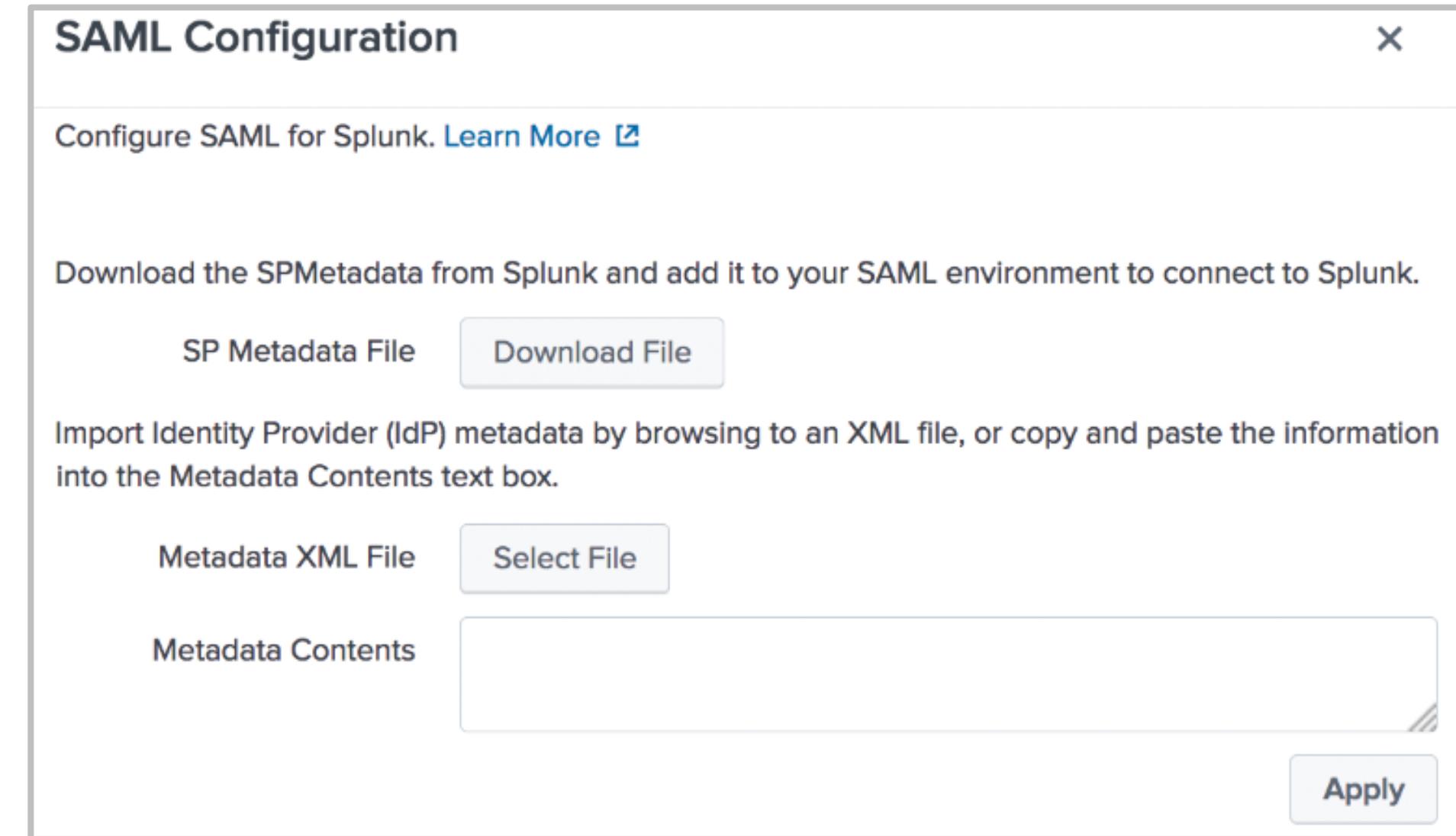
SP Metadata File [Download File](#)

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 YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Configuring SAML – General Settings

- Contact your SAML administrator for the following configuration information:
  - Sign on/Log off URLs
    - ▶ These are the protected endpoints on the IdP which Splunk sends authentication requests
  - Certificate information

**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 ?

Issuer Id ?

Entity ID ?

Sign AuthnRequest

Verify SAML response ?

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Configuring SAML – Query and Alias Settings

- Attribute Query Requests
  - Attribute query URL
    - ▶ Endpoint on the IdP to which queries over SOAP are sent
  - Sign attribute query request/response
    - ▶ Username/Password
- Aliases
  - Role
  - RealName
  - Mail

▼ Attribute Query Requests

Attribute query requests are required for scheduled searches.

Attribute query URL ?

Sign attribute query request

Sign attribute query response

Username

Password .....

▼ Alias

Role alias

RealName alias

Mail alias

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Configuring SAML – Advanced Settings

- Advanced Settings
  - Name Id Format
    - ▶ Leave this empty or pick the correct format configured on the IdP from the dropdown list
  - Domain name/IP of load balancer
  - Redirect/load balancer port
  - Redirect URL after logout
  - SSO/SLO Binding
    - ▶ Protocol binding used for the SAML sign on/log off requests sent to the IdP

**Advanced Settings**

Name Id Format ?	dropdown
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

# 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

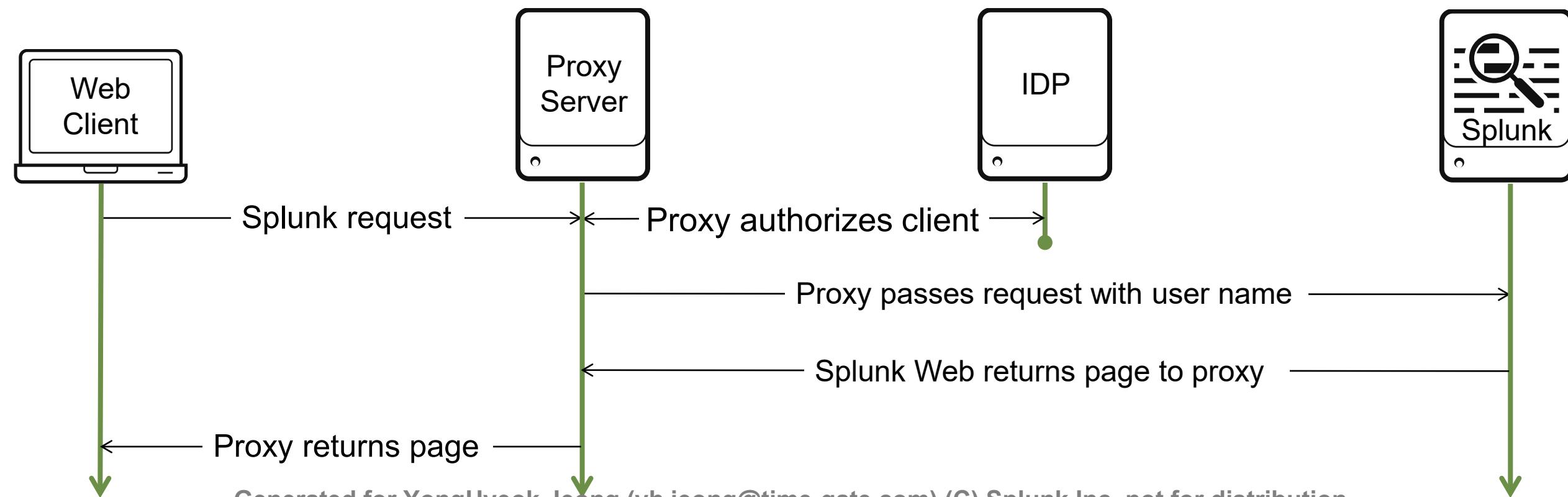
Create New SAML Group

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

# 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](https://docs.splunk.com/Documentation/Splunk/latest/Security/HowSplunkSSOworks)



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

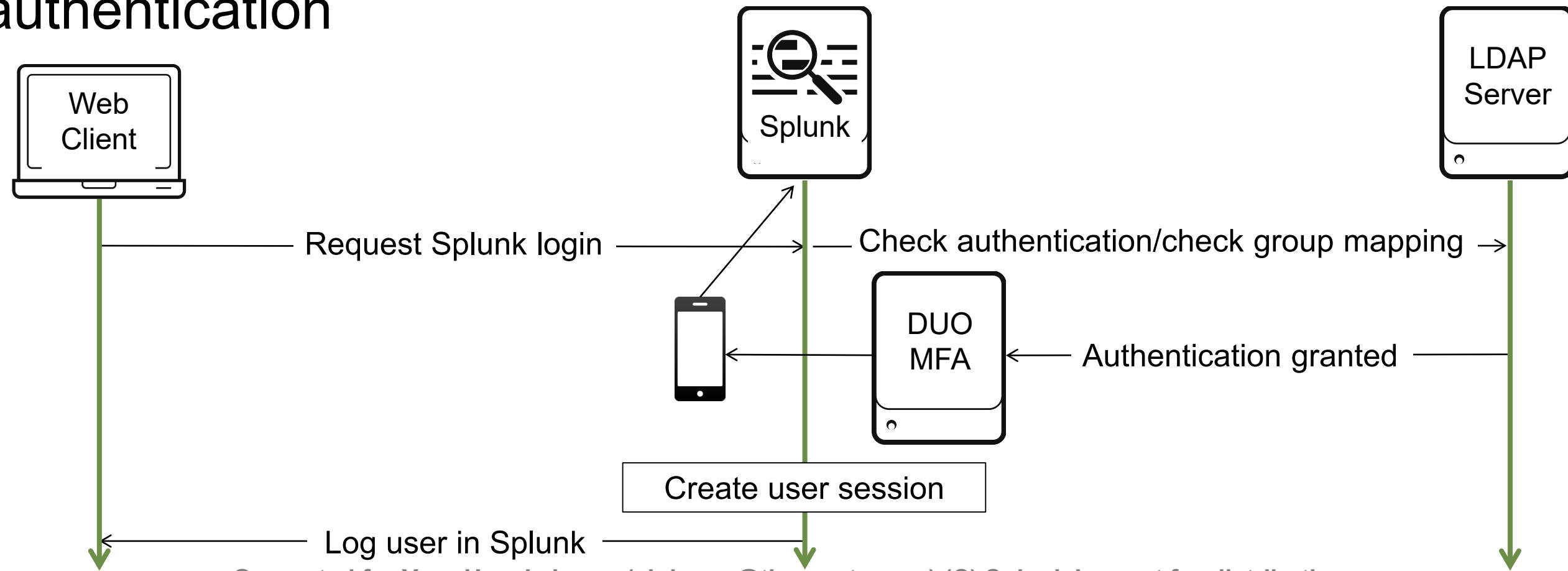
# Scripted Authentication

---

- There are other types of authentication systems that Splunk can integrate with using scripts
- For the most up-to-date information on scripted authentication, see the README file in:  
**SPLUNK\_HOME/share/splunk/authScriptSamples/**
  - The directory includes 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 YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Configuring Duo MFA

Create an account for your Splunk configuration on the Duo website

**Note:** see <https://duo.com>

From your search head:

1. Select **Duo Security**
2. Click **Configure Duo Security**

**Authentication method**  
Access controls » Authentication method

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

Internal  Splunk Authentication (always on)

External  None  
 LDAP  
 SAML

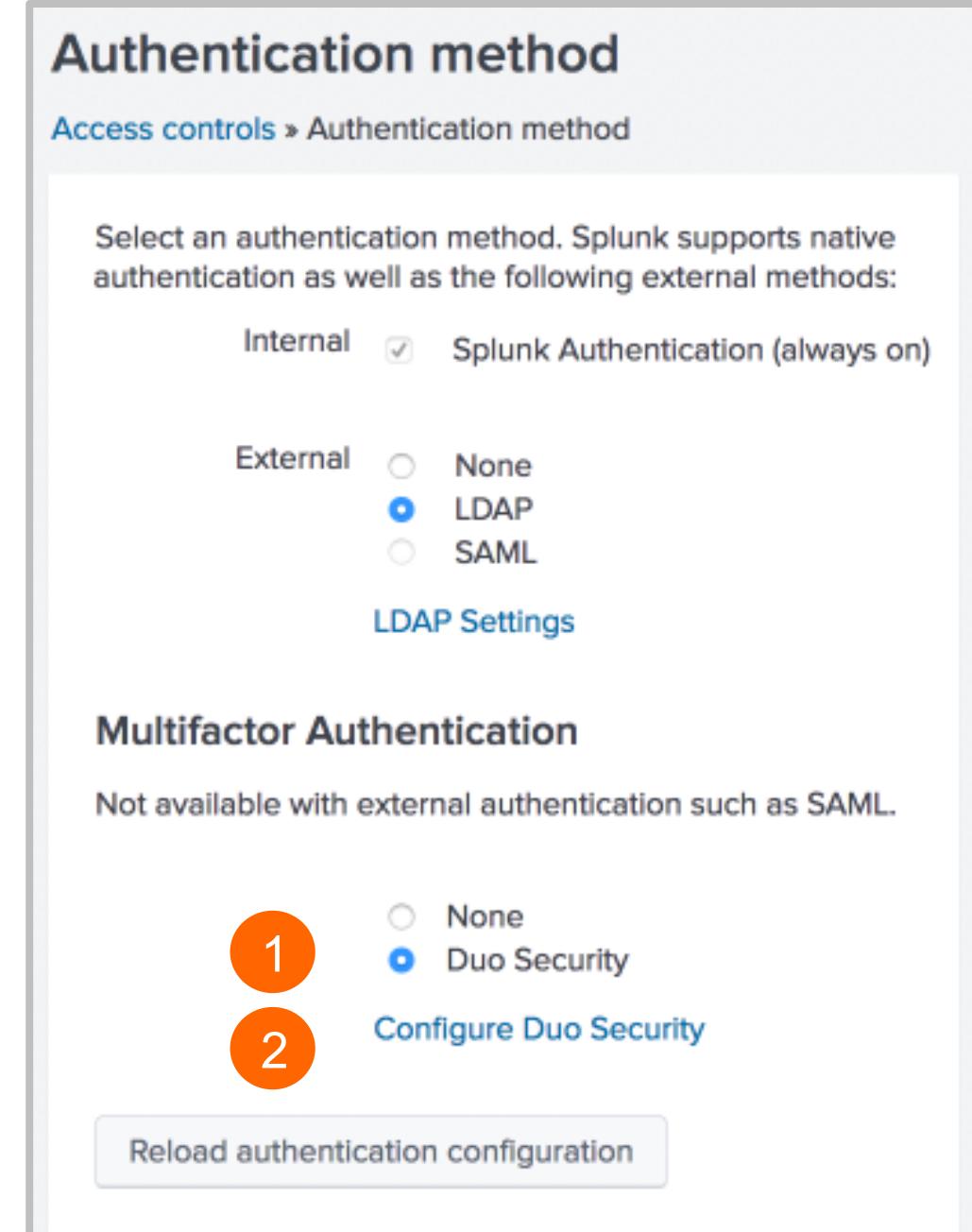
[LDAP Settings](#)

**Multifactor Authentication**  
Not available with external authentication such as SAML.

1  None  
 Duo Security

2 [Configure Duo Security](#)

[Reload authentication configuration](#)



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Configuring Duo MFA (cont.)

3. Enter the following info (provided by the 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

Access controls > Authentication method > 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.

Canc 6 Save

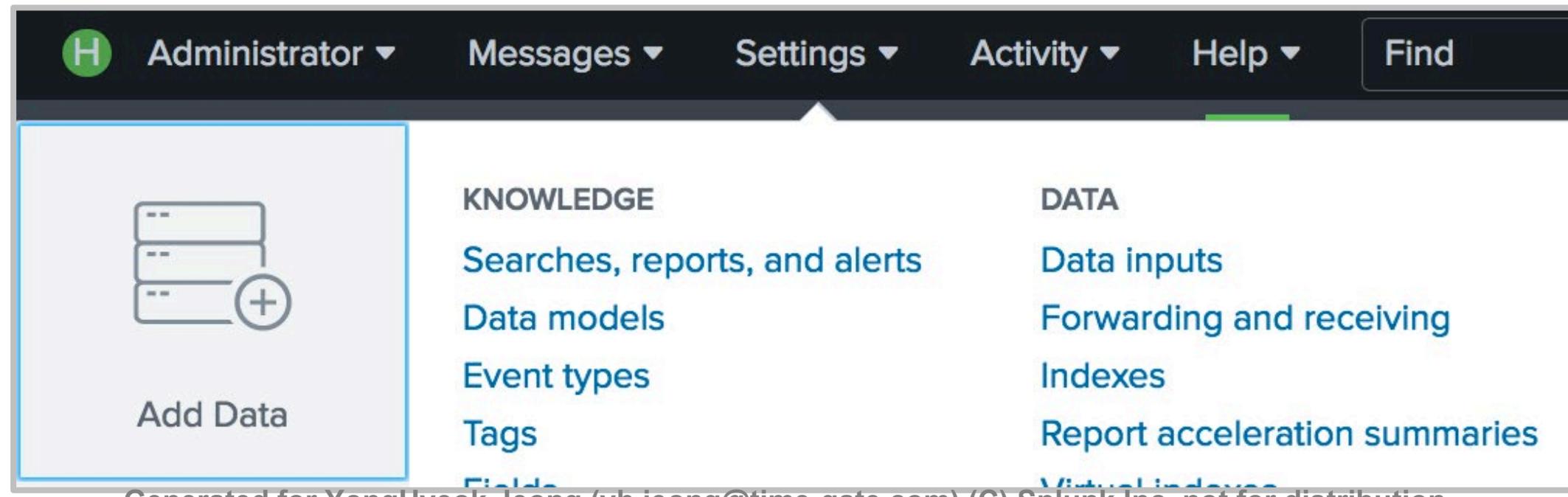
Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Appendix B: Adding Data

Generated for YongHyeok Jeong ([yh.jeong@time-gate.com](mailto:yh.jeong@time-gate.com)) (C) Splunk Inc, not for distribution

# Adding an Input with Splunk Web

- Splunk admins have a number of ways to start the **Add Data** page
  - Click the **Add Data** icon
    - ▶ On the admin's **Home** page
    - ▶ On the **Settings** panel
  - Select **Settings > Data inputs > Add new**



# Select Source

Add Data       Select Source   Set Source Type   Input Settings   Review   Done   < Back   **Next >**

**1** Select the **Files & Directories** option to configure a monitor input

**2** To specify the source:

- Enter the absolute path to a file or directory, or
- Use the Browse button

**3** Select Continuously Monitor for ongoing monitoring; creates a stanza in **inputs.conf**

For one time indexing (or testing); the Index Once option does not create a stanza in **inputs.conf**

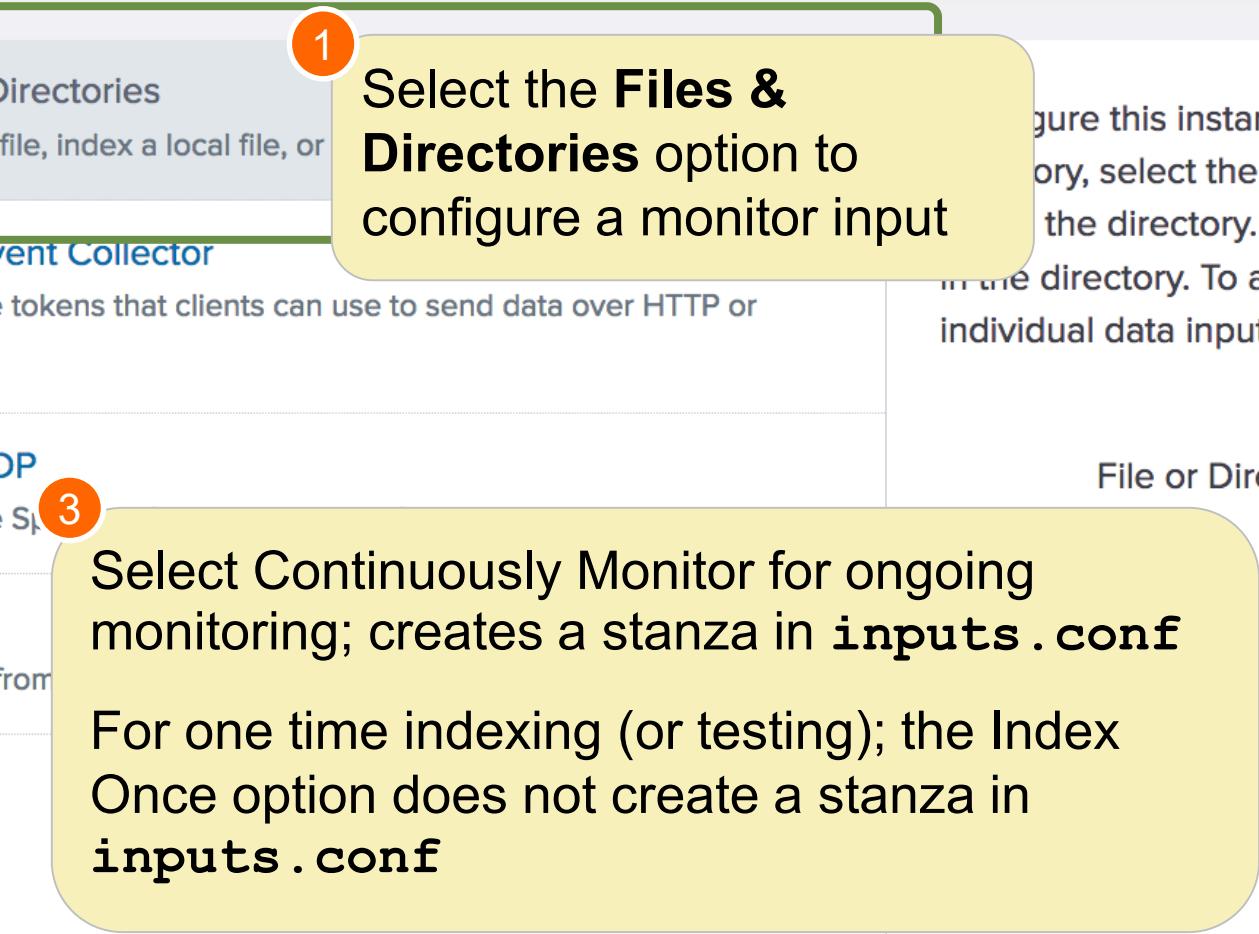
File or Directory ? /opt/log/www2/access.log      Browse

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

Continuously Monitor      Index Once

Whitelist ?

Blacklist ?



Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Set Source Type (Data Preview)

Add Data

Select Source Set Source Type Input Settings Review Done

< Back Next >

## Set Source Type

This page lets you see how Splunk 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 create a new one by clicking "Save As".

Source: /opt/log/www2/access.log

If Splunk recognizes the data, a pretrained sourcetype will be assigned

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 >

Event Breaks

Timestamp

Advanced

Data Preview displays how your processed events will be indexed.

Time Event

Time	Event
12/15/17 12:29:22.000 AM	24.185.15.226 - - [15/Dec/2017:00:29:22] "POST /product.screen?productId=DC-S G-G02&JSESSIONID=SD10SL9FF1ADFF4960 HTTP 1.1" 200 2656 "http://www.yahoo.com" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:12.0) Gecko/20100101 Firefox/12.0" 267
12/15/17 12:29:28.000 AM	24.185.15.226 - - [15/Dec/2017:00:29:28] "GET /category.screen?categoryId=NUL L&JSESSIONID=SD10SL9FF1ADFF4960 HTTP 1.1" 406 542 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-16" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:12.0) Gecko/20100101 Firefox/12.0" 974

Generated for YongHyeok Jeong (yh.jeong@time-gate.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 instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. [Learn More](#)

**Host**

When Splunk 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**

Splunk 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 your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

App Context: Search & Reporting (search)

Host field value: splunk01

Index: securityops | Create a new index

- The app context determines where your input configuration is saved
- In this example, it will be saved in: **SPLUNK\_HOME/etc/apps/search/local**

- By default, the default host name in **General settings** is used
- You will learn about other options in the Splunk Enterprise Data Administration class

Select the index where this input should be stored  
To store in a new index, first create the new index

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# Review

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

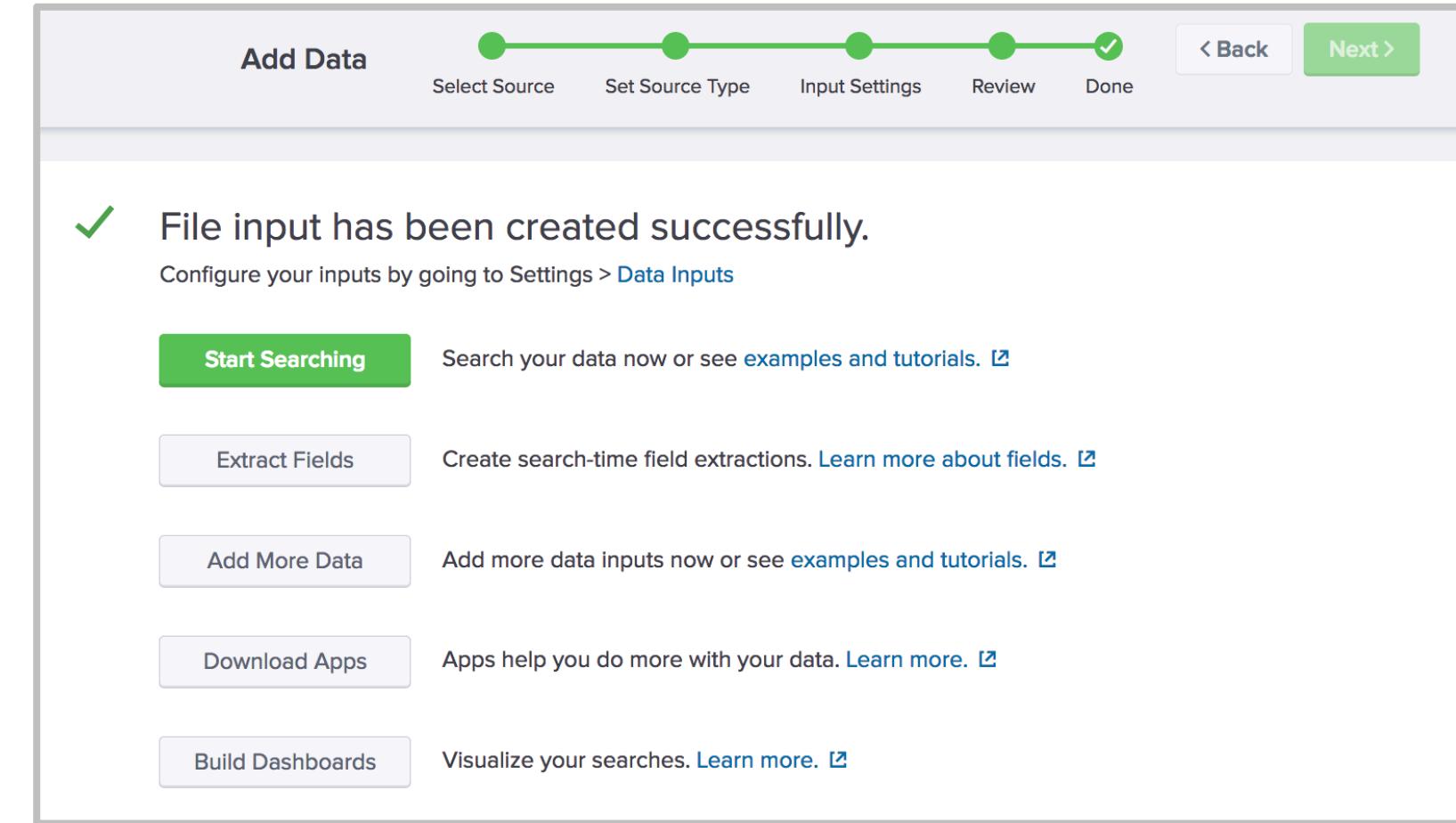
The screenshot shows the 'Add Data' wizard in the 'Review' step. The top navigation bar includes 'Add Data' on the left, a progress bar with five steps ('Select Source', 'Set Source Type', 'Input Settings', 'Review', 'Done') where the first four are green and the last one is grey, and buttons for '<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

Input Type .....	File Monitor
Source Path .....	/opt/log/www2/access.log
Continuously Monitor .....	Yes
Source Type .....	access_combined_wcookie
App Context .....	search
Host .....	splunk01
Index .....	securityops

Generated for YongHyeok Jeong (yh.jeong@time-gate.com) (C) Splunk Inc, not for distribution

# What Happens Next?

- Indexed events are available for immediate search
  - However, it may take a minute for Splunk to *start* indexing the data
- You are given other options to do more with your data
- The input configuration is saved in:  
**etc/apps/<app>/local/inputs.conf**



# Verify your Input

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

