



Splunk Enterprise System Administration

Document Usage Guidelines

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.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 diag

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 and Splunk Diag

System Administrator vs Data Administrator

Splunk System Administrator

System Management

- 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

Splunk Data Administrator

Data Onboarding and Management

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

Module 1: Splunk Deployment Overview

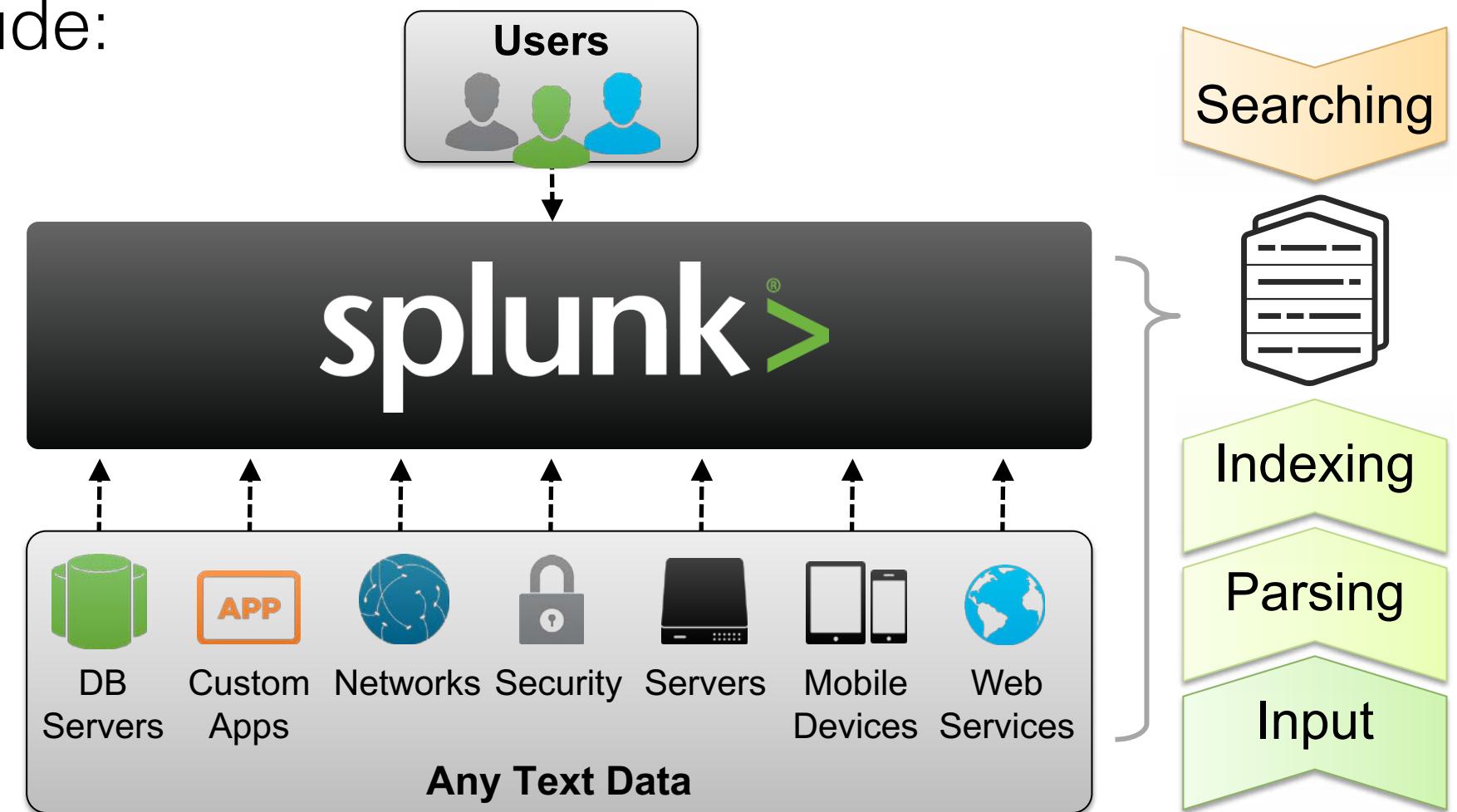
Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Module Objectives

- Provide an overview of Splunk
- Identify Splunk Enterprise components
- Identify the types of Splunk deployments
- List the steps to install Splunk
- Use Splunk CLI commands
- 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
- Four stages of Splunk include:
 - Input any text data
 - Parse the data into events
 - Index and store events
 - Search and report

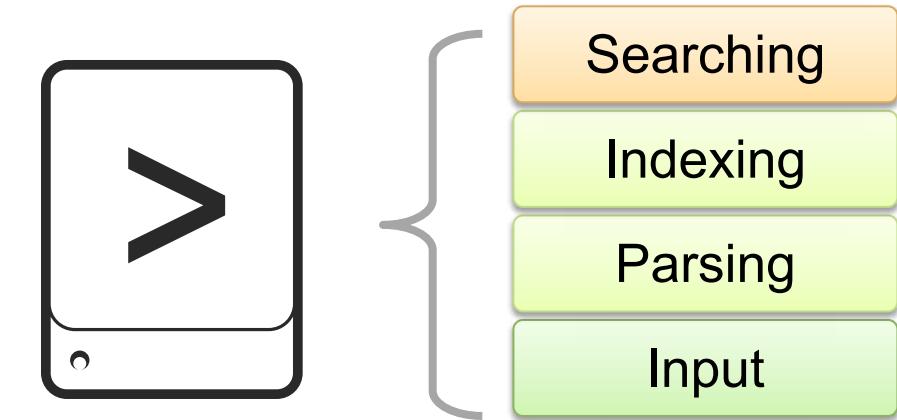


Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Splunk Deployment – Standalone

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

**Splunk
server
(standalone)**



Note

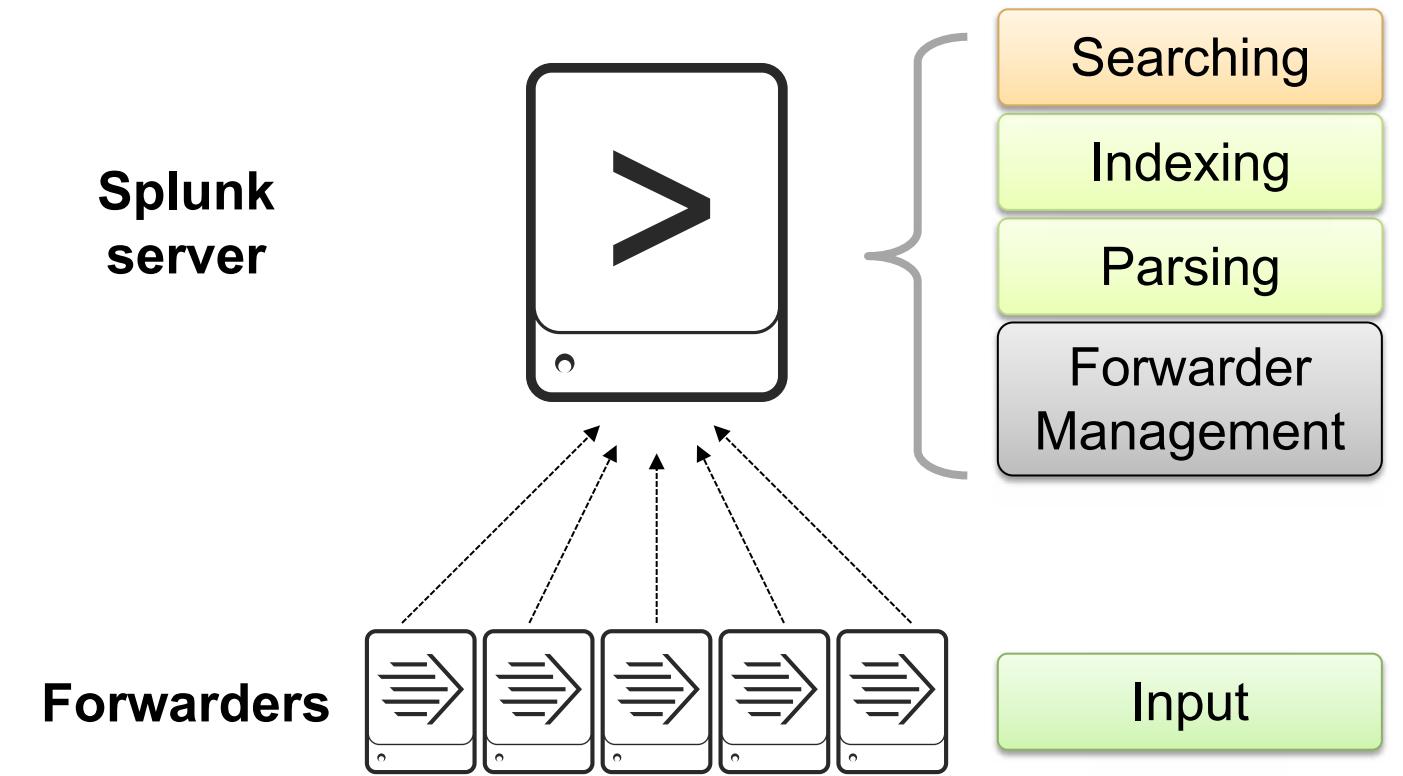


This is the initial configuration in class.

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Splunk Deployment – Basic

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



Note

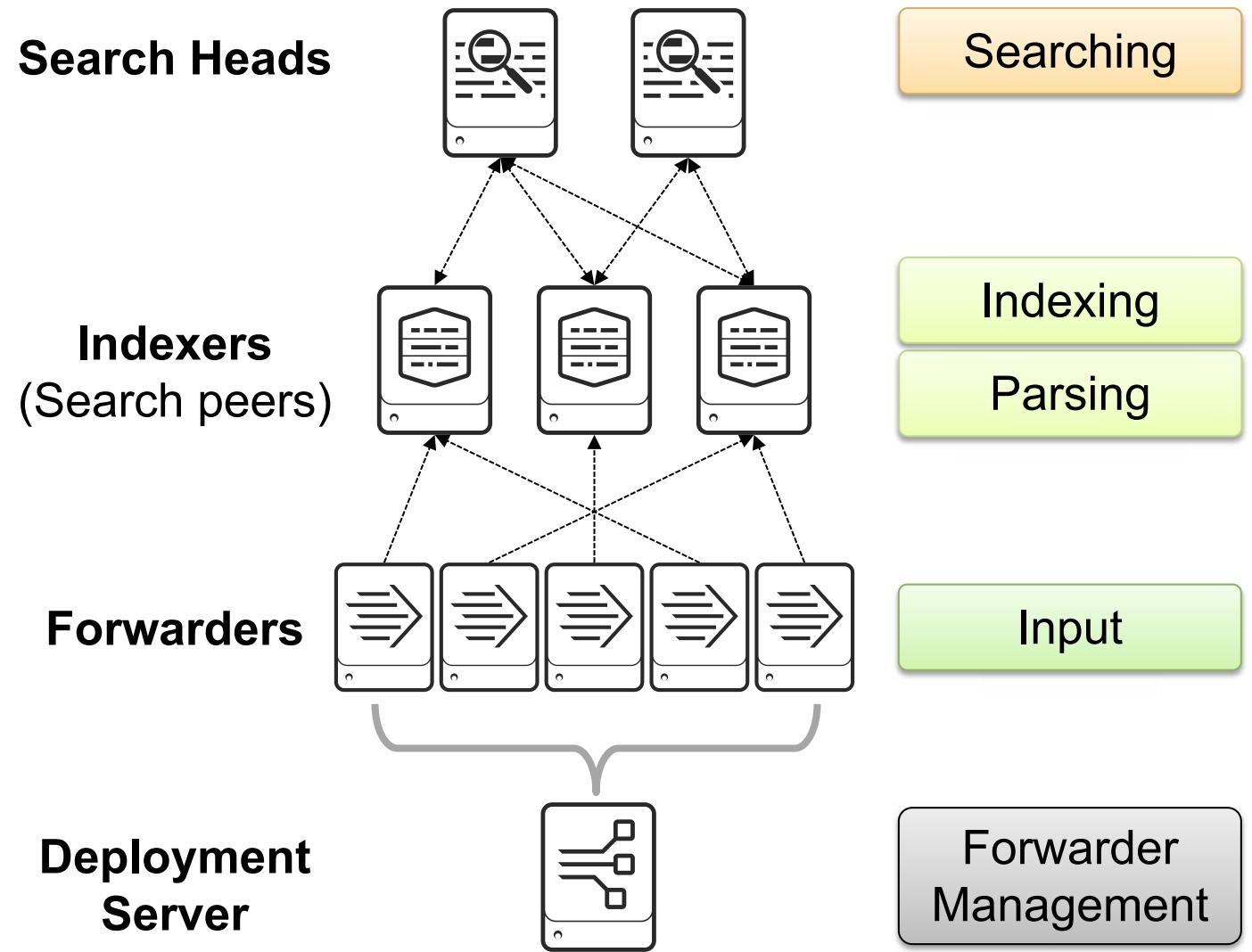
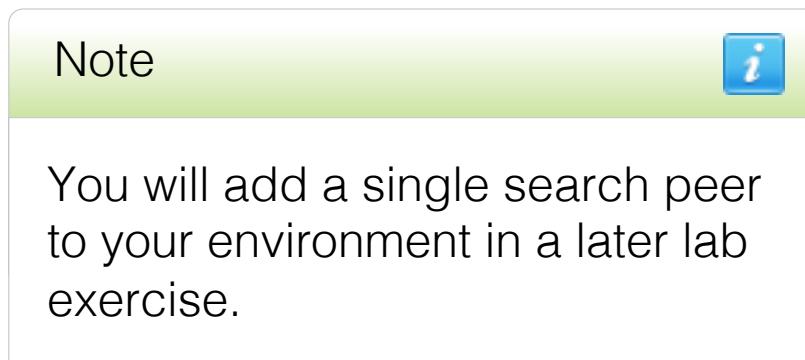


Your lab environment evolves to include a separate forwarder.

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Splunk Deployment – Distributed

- Scale Splunk in various ways
 - Add indexers to handle more inputs
 - Add indexers and search heads to handle more searching
- Manage forwarder configurations with a dedicated Deployment Server



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Splunk Core Components and Processes

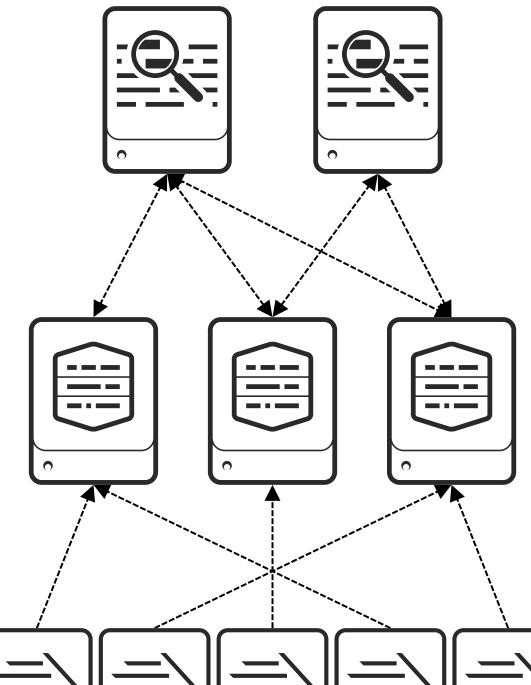
- Allow users to submit search requests using SPL
- Distribute search requests to the indexers
- Consolidate results and render visualizations of results
- Store search-time knowledge objects (such as field extractions, alerts, and dashboards)

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

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

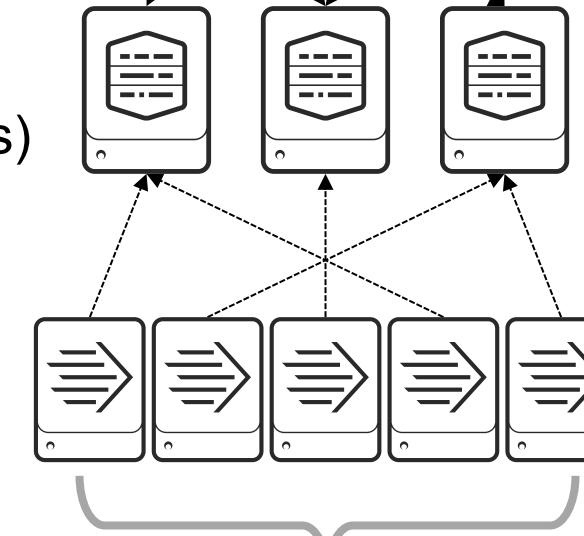
- Acts as a centralized configuration manager for any number of deployment clients
- Requires running on a Splunk Enterprise instance

Search Heads



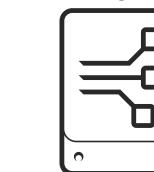
Searching

Indexers (Search peers)



Indexing
Parsing

Forwarders

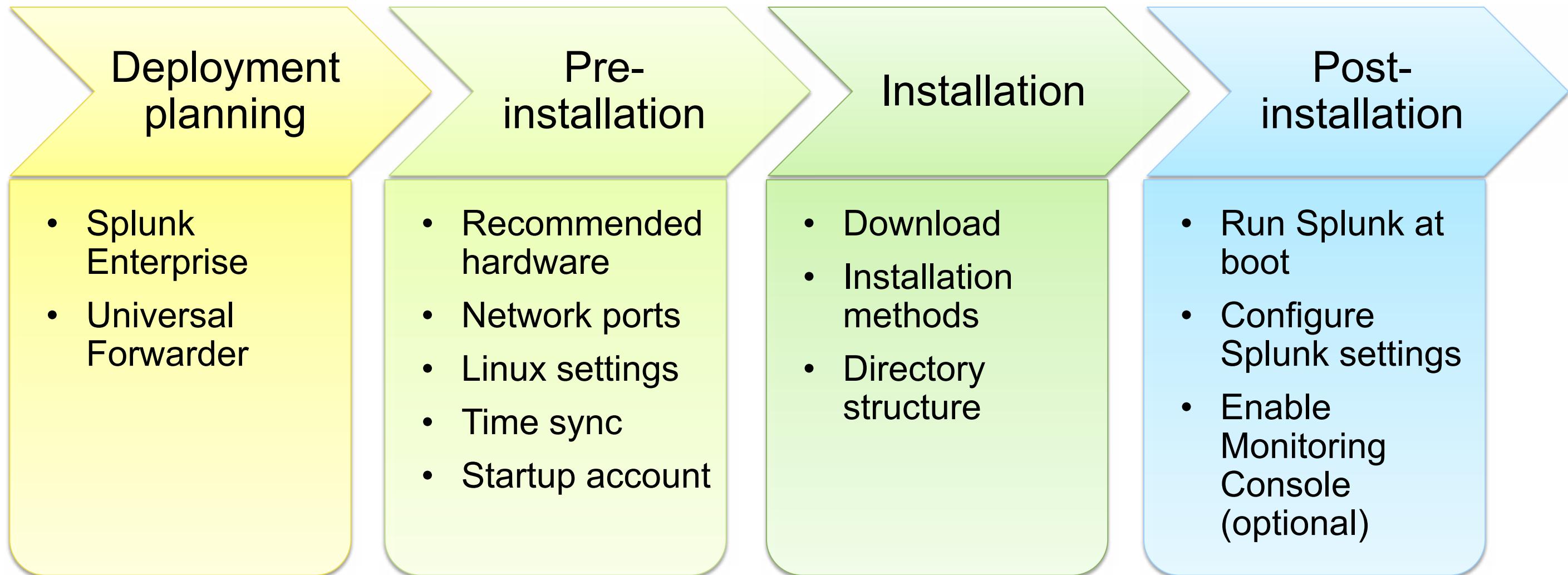


Deployment Server

Input

Forwarder
Management

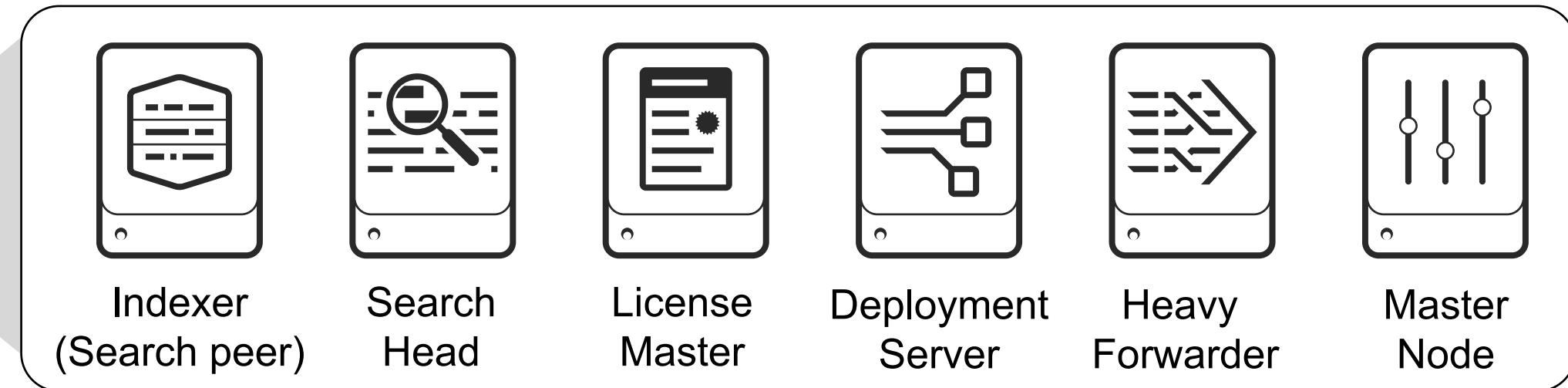
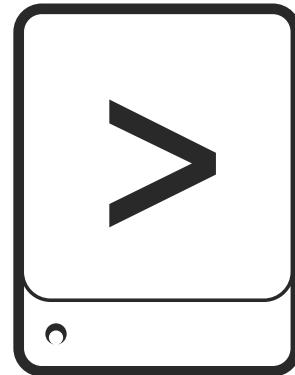
Splunk Installation Overview



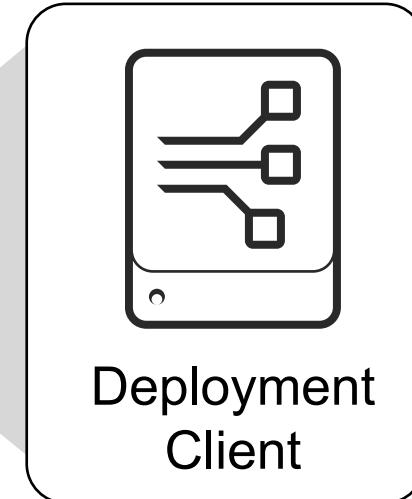
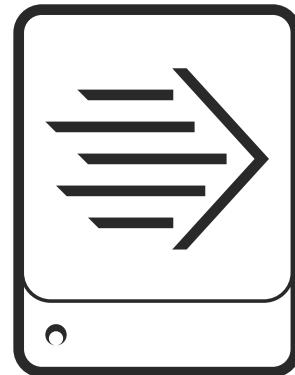
Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Software in Splunk Enterprise packages

**Splunk
Enterprise
package**



**Universal
Forwarder
package**



Note

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Server Hardware Recommendations

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

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Splunk Default Network Ports

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

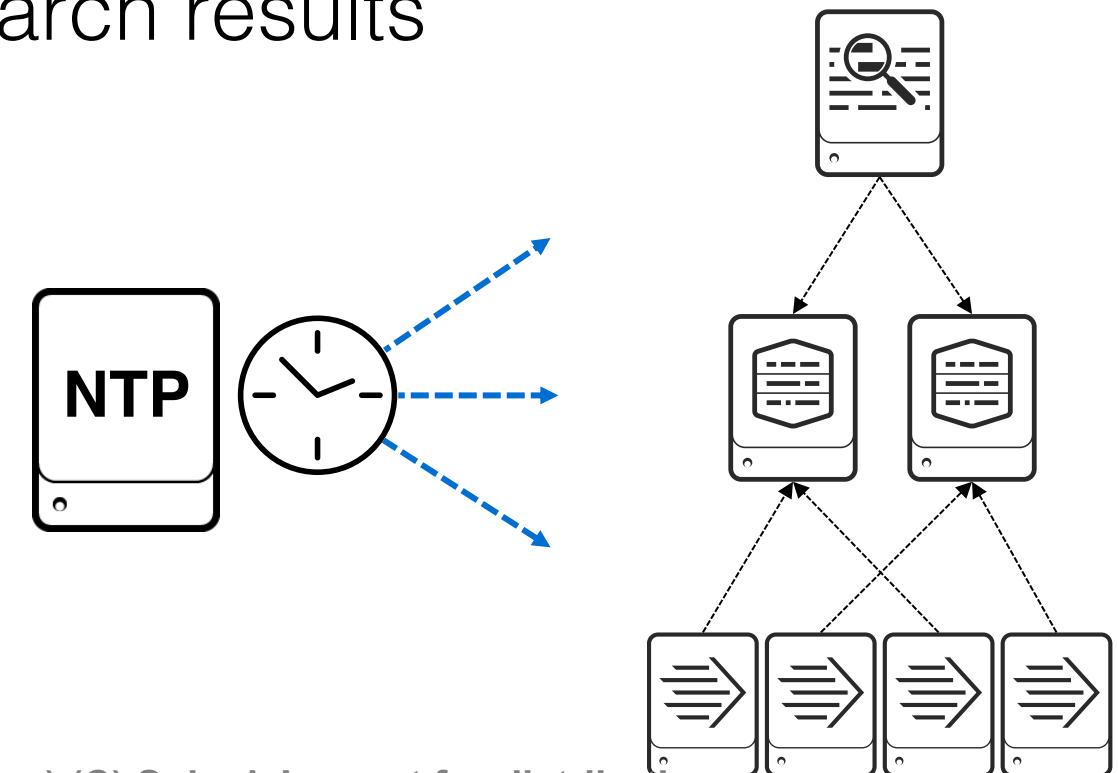
Linux Setting Recommendations

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

```
# ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority     (-e) 0
file size               (blocks, -f) unlimited
pending signals          (-i) 30424
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files              (-n) 8192
...
cpu time                (seconds, -t) unlimited
max user processes       (-u) 30424
```

Time Synchronization

- Best practice: Use a time synchronization service such as NTP
 - Splunk indexer and production servers should have standardized time configuration
 - Splunk searches depend on accurate timestamps on events
 - Clock skew between hosts can affect search results



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Startup Account

- Best practice: Do not run Splunk as *super-user*

*NIX	<ul style="list-style-type: none">• Avoid the root account
Windows	<ul style="list-style-type: none">• Avoid the administrator account• Use a domain account if Splunk must connect to other servers• Alternatively, use a local machine account that can run services

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Installing Splunk Enterprise Server

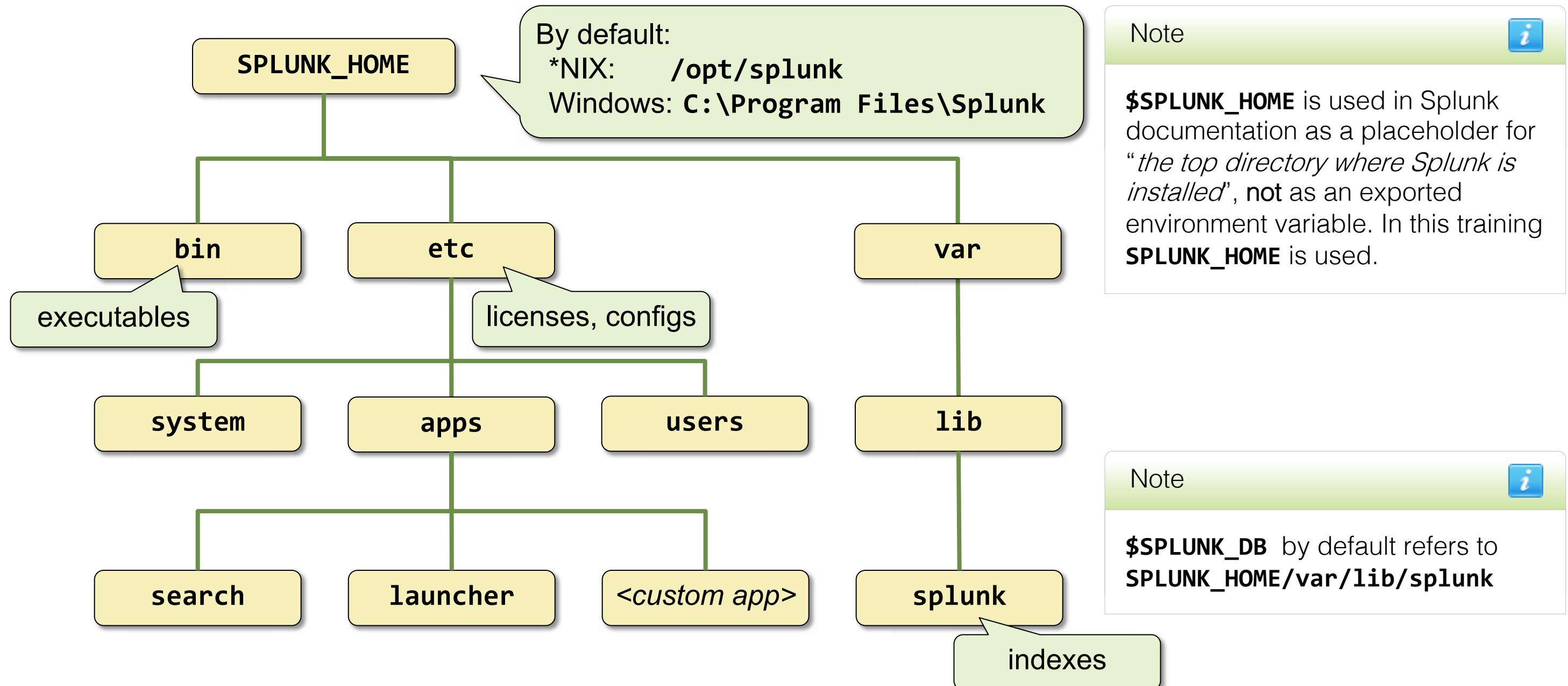
	*NIX	Windows
Download	http://www.splunk.com/download	
Install	<ul style="list-style-type: none">Un-compress .tar.gz file in the path you want Splunk to run fromAlso available as rpm, deb	Execute the .msi installer and follow the wizard steps
Post-Install	<ul style="list-style-type: none">Splunk starts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

Complete installation instructions at:

<http://docs.splunk.com/Documentation/Splunk/latest/Installation/Chooseyourplatform>

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Splunk Directory Structure



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Running Splunk at Boot

Splunk on *NIX

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

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

- Enable auto-start on **systemd** -based distributions:
- # splunk enable boot-start -systemd-managed 1

Note



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

Splunk on Windows

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

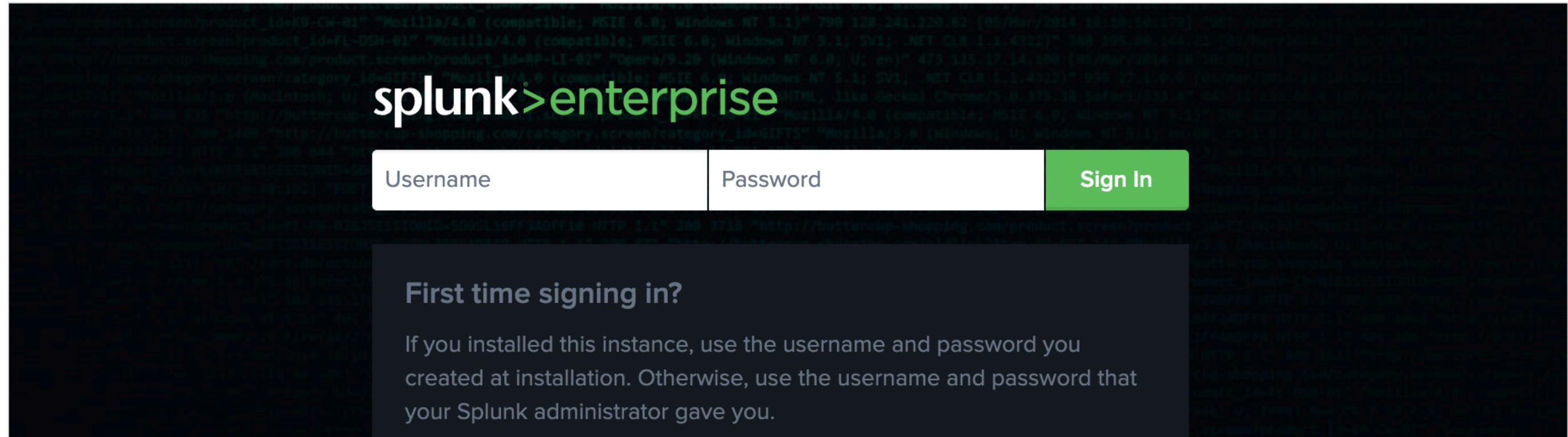
The **splunkd** Process

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

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

Splunk Web

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Splunk Web – Server Settings

The screenshot shows the Splunk Web interface. At the top is a navigation bar with tabs: Administrator, Messages, Settings (highlighted with a red circle containing the number 1), Activity, Help, and Find. Below the navigation bar is a sidebar with several sections:

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

In the bottom left of the sidebar, there are two sections: **SYSTEM** (containing Server settings, highlighted with a red circle containing the number 2) and **Monitoring Console**.

Select Settings > Server settings > General settings

The screenshot shows the 'Server settings' page. At the top, it says 'Manage system settings including ports, host name, index path, email server, and more'. Below this, the 'General settings' tab is selected (highlighted with a green box and a red circle containing the number 3). Other tabs include Login background, Email settings, Server logging, Deployment client, and Search preferences.

Used to set server configuration and server options

Generated for Balaram Guttula (balaram.krishn.guttula@pmchase.com) (C) Splunk Inc, not for distribution

Describing General Settings

General settings

Server settings » General settings

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Describing General Settings – Splunk Web

Splunk Web

Run Splunk Web	<input checked="" type="radio"/> Yes <input type="radio"/> No	Enables Splunk Web
Enable SSL (HTTPS) in Splunk Web?	<input type="radio"/> Yes <input checked="" type="radio"/> No	Enables HTTPS for Splunk Web
Web port *	8000	Identifies the Splunk Web port
App server ports	8065	Python-based application server port. Set to "0" to run Splunk Web in legacy mode (not compatible with SHC)
Session timeout *	1h	Sets the Splunk Web session timeout <small>Set the Splunk Web session timeout. Use the same value as the session timeout in the configuration file. For example, if you set the session timeout to 6d, set the session timeout in the configuration file to 6d.</small>

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Describing General Settings – Index/KV Store

Index settings	
Default host name	splunk01
	Sets the host field value for all events coming from this server.
Path to indexes	/opt/splunk/var/lib/splunk
	Identifies path to the existing indexes: SPLUNK_DB (read-only in UI)
Pause indexing if free disk space (in MB) falls below *	5000
	Sets minimum free disk space required; Splunk pauses indexing if this free disk space limit is reached
KV Store	
Port *	8191
	Port that splunkd uses to connect to the KV Store server.

Cancel **Save**

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Restarting the Server from Splunk Web

The screenshot shows the Splunk Web interface with the title bar "splunk>enterprise". The "Messages" tab is highlighted with a green border and has a red circle with the number "1" above it. A message box is displayed, containing an exclamation mark icon, the text "Splunk must be restarted for changes to take effect.", a blue button labeled "Click here to restart from Server controls.", and the timestamp "10/1/2019, 9:06:49 PM". The message box has a red circle with the number "2" on its left edge. Below the message box, there is a teal banner with the text "Successfully updated 'settings'." and a link to "Manage system settings including ports, host name, and more". A "Delete All" button is also visible.

The screenshot shows the "Server controls" page in Splunk Web. At the top, there is a note: "Any changes to **General** settings generate a message. Clicking the indicator opens a message, prompting you to restart." Below this, there are two main sections: "Restart Splunk" and "Clear restart message". The "Restart Splunk" section contains the text "Click the button below to restart Splunk." and a green button labeled "Restart Splunk" with a red circle containing the number "3" on its left edge. The "Clear restart message" section contains the text "Click the button below to clear restart message." and a green button labeled "Clear restart message".

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Splunk Command Line Interface (CLI)

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

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Monitoring Console (MC)

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

The screenshot shows the Splunk Enterprise interface with the 'Monitoring Console' selected in the left sidebar. The main dashboard displays various performance metrics:

- INDEXING RATE:** 4.83 KB/s
- LICENSE USAGE:** 0%
- DISK USAGE:** 12% (Disk)
- CONCURRENT SEARCHES:** 1
- CONCURRENT SEARCHES BY TYPE:** (partial view)
- CPU USAGE:** (partial view)

A note on the right side states: "You will use MC to monitor your activities as you learn more about Splunk components."

Left Sidebar (Administrator View):

- Add Data
- Explore Data
- Monitoring Console (selected)

Top Navigation: splunk>enterprise Apps ▾

Top Bar Buttons: Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Left Sidebar Submenu:

- KNOWLEDGE:** Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; All configurations
- DATA:** Data inputs; Forwarding and receiving; Indexes; Report acceleration summaries; Virtual indexes; Source types
- DISTRIBUTED ENVIRONMENT:** Indexer clustering; Forwarder management; Data Fabric; Distributed search
- SYSTEM:** Server settings; Server controls (highlighted); Health report manager; Instrumentation; Licensing; Workload management
- USERS AND AUTHENTICATION:** Roles; Users; Tokens; Password Management; Authentication Methods

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Enabling MC in Standalone Mode

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

The screenshot shows the Splunk Enterprise Monitoring Console interface. At the top, there's a navigation bar with links like Overview, Summary, Health Check, Indexing, Search, Resource Usage, Forwarders, Settings, and Activity. A user is logged in as Administrator.

In the main area, there's a "Setup" section with tabs for Overview, Summary, Health Check, Indexing, Search, Resource Usage, Forwarder Monitoring Setup, Alerts Setup, Overview Preferences, and Health Check Items. The "Forwarder Monitoring Setup" tab is highlighted with a blue border.

Below the setup section, there's a table titled "This instance" with columns for Instance (host), Instance (serverName), Machine, Server roles, Custom groups, Indexer Cluster(s), Search Head Cluster(s), Monitoring, State, Problems, and Actions. The "Standalone" mode is selected in the Mode dropdown.

A callout bubble labeled "Default server roles" points to the "Server roles" column in the table. Another callout bubble labeled "Edit monitoring of server roles" points to the "Actions" dropdown menu for the "splunk01" instance, which includes options like Edit and Delete.

Three numbered circles highlight specific steps:

- 1: Click on the Settings icon in the top navigation bar.
- 2: Click on the "General Setup" link in the dropdown menu.
- 3: Click the "Apply Changes" button.

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Enabling MC Platform Alerts

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

The screenshot shows the Splunk Enterprise Monitoring Console interface. The top navigation bar includes links for Admin, Messages, Settings, Activity, Help, Find, and a search bar. Below the navigation is a secondary menu with options like Overview, Health Check, Indexing, Search, Resource Usage, Forwarders, Settings, and Run a Search. The main content area is titled "Platform Alerts Setup" and describes managing monitoring console platform alerts. It shows 8 alerts listed, each with a brief description and three action buttons: Edit, Advanced, and Enable. A green box highlights the "Alerts Setup" link in the secondary menu. A yellow callout bubble on the right side of the page contains the text "Disabled by default".

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

Disabled by default

MC Health Check

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

The screenshot shows the Splunk Enterprise Monitoring Console interface. The top navigation bar includes links for Overview, Summary, Health Check (which is highlighted in green), Indexing, Search, Resource Usage, and a Monitoring Console icon. Below the navigation is a sub-menu with Forwarders, Settings, and Run a Search. The main content area is titled "Health Check" and displays a summary of the check results for instance "splunk01". It shows counts for ALL (15), ERROR (0), WARNING (2), INFO (0), SUCCESS (7), and N/A (6). There are two search filters: "App: All" and "Tags: ? Category: ?". A timestamp indicates the check was completed on 10/1/2019 at 2:20:15 PM. The results table lists seven health check items with their categories, tags, and status. The items are:

Check	Category	Tags	Status
System hardware provisioning assessment	System and Environment	best_practices, capacity, scalability	⚠️ One or more hosts has returned CPU or memory specifications that fall below reference hardware recommendations. This might adversely affect indexing or search performance.
Assessment of server ulimits	System and Environment	best_practices, operating_system	⚠️ One or more Splunk instances are running on a host that has one or more resource limits set below official recommendations.
Event-processing issues	Data Collection	event_breaking, indexing, timestamp_extraction	✅ This health check item was successful.
Saturation of event-processing queues	Data Indexing	indexing, queues	✅ This health check item was successful.
Excessive physical memory usage	Splunk Miscellaneous	resource_usage	✅ This health check item was successful.
Integrity check of installed files	Splunk Miscellaneous	configuration, installation	✅ This health check item was successful.

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

More Resources

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Module 1 Knowledge Check

- Which installer will you use to install the Search Head?
- True or False. When you install Splunk on 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 Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Module Objectives

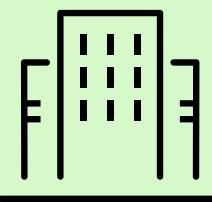
- Identify license types
- Describe license violations
- Add and remove licenses

Splunk License Types



Enterprise trial license

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



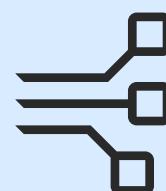
Enterprise license

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



Free license

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



Forwarder license

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Splunk License Comparison

https://www.splunk.com/en_us/software/features-comparison-chart.html

Features	Splunk Free	Splunk Enterprise
Maximum Daily Indexing Volume	500MB	Unlimited
Maximum Users	1	Unlimited
Universal Data Collection/ Indexing	✓	✓
Metrics Store	✓	✓
Data Collection Add-Ons	✓	✓
Monitoring and Alerting		✓
Dashboards and Reports	✓	✓

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

License Alerts, Warnings and Violations

- Alert**
 - Occurs when indexing exceeds the allocated daily quota in a pool
 - Viewed in Splunk Web > **Messages** (as a “pool warning”)
 - Cleared at midnight when daily allocation is reset; may result in a Warning
- Warning**
 - Occurs if an alert is triggered, and license capacity is not increased by midnight (by adding new license or moving capacity from another pool)
 - Only occurs once per day
- Violation**
 - Occurs after 5 warnings on an Enterprise license* in a rolling 30-day period
 - Informational only, and does not affect indexing or searches
 - Requires a reset key from Splunk Support or Sales Team

* 3 Warnings on a Free license

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Measuring Daily License Quota



Counts for daily license quota

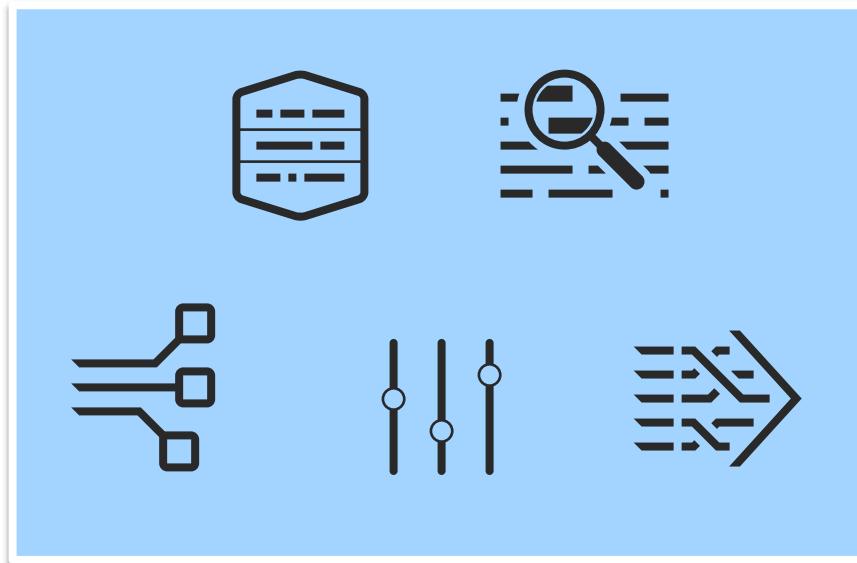
- All data from all sources that is indexed
- **For events:** Measured as the data (full size) that flows through the parsing pipeline per day
- **For metrics:** Measurement capped at 150 bytes per metric event



Does not count for daily license quota

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

License Requirements With Server Roles and Data



Server Roles

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



Data

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Managing Licenses

Select Settings > Licensing

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

The screenshot shows the Splunk Licensing interface. Step 1 highlights the 'Change to slave' button. Step 2 highlights the 'Enterprise license group' section. Step 3 highlights the 'Add license' and 'Usage report' buttons. Step 4 highlights the 'Alerts' section. Step 5 highlights the 'Splunk Enterprise Sales Trial stack' table. Step 6 highlights the 'Edit | Delete' link for a pool.

Licenses	Volume	Expiration	Status
Splunk Enterprise Sales Trial	200 MB	Nov 11, 2019, 7:59:59 AM	valid
Effective daily volume	200 MB		

Pools	Indexers	Volume used today
auto_generated_pool_enterprise		0 MB / 200 MB

No indexers have reported into this pool today

Add pool

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Adding a License

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

Add new license

Licensing » Add new license

Add new license

Learn more about your license options at the [licensing section](#) on splunk.com.

To install a license, upload a license file here (license files end with .license):

No file chosen

Or, [copy & paste the license XML directly...](#)

```
SPLUNK_HOME
  └── bin
  └── etc
    └── apps
    └── licenses
      └── download-trial
      └── enterprise
    └── system
```

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Viewing Alerts

Alerts

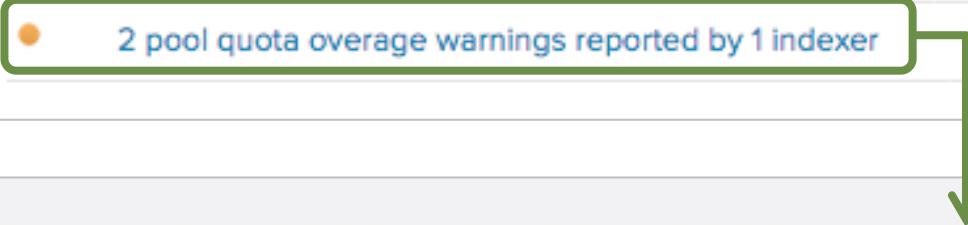
Licensing alerts notify you of excessive indexing warnings and licensing misconfigurations. [Learn more](#)

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)							
Severity	Time	Message	Indexer	Pool	Stack	Category	
●	Correct by midnight to avoid violation Learn more	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	

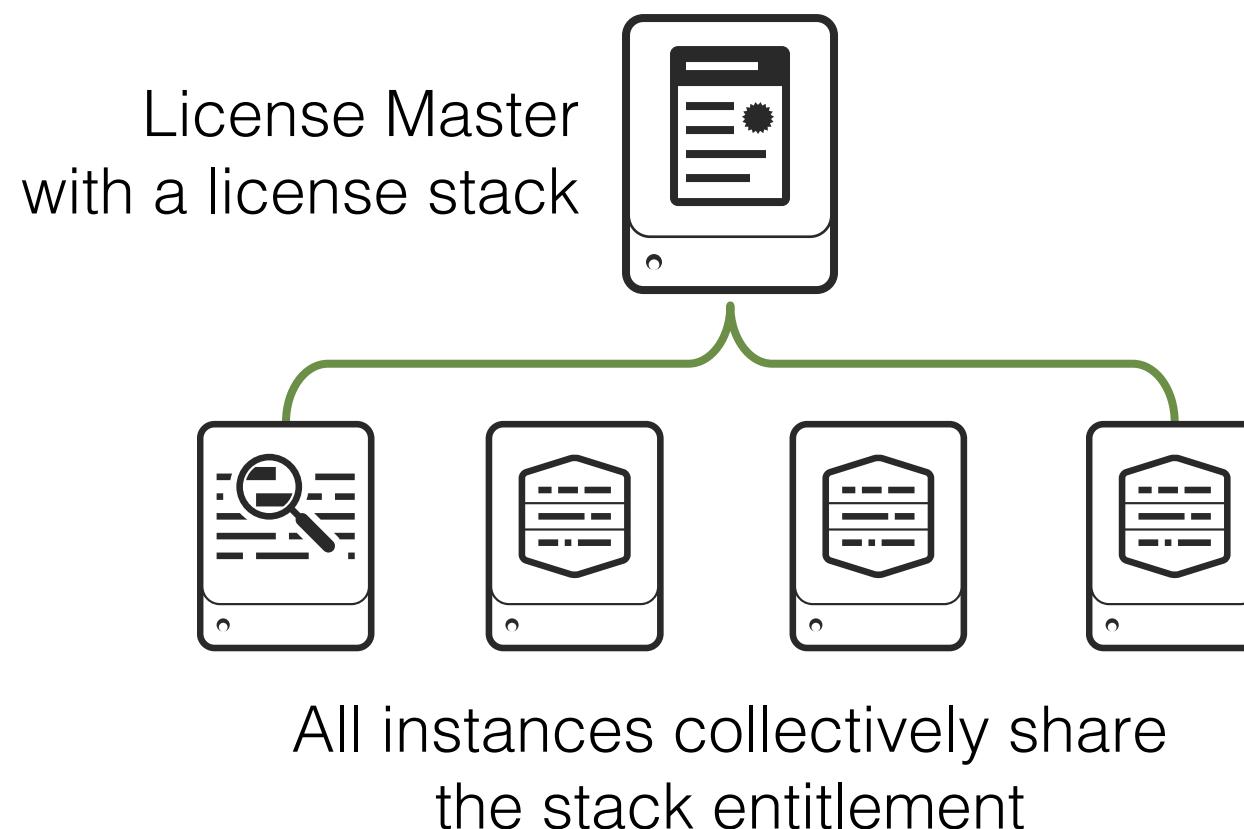
[Show messages for all alert types](#)

[« return to overview](#)

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Changing an Instance to a Slave

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



Change master association

This server, **splunk01**, is currently acting as a master license server.

Designate this Splunk instance, **splunk01**, as the master license server
Choosing this option will:

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

Designate a different Splunk instance as the master license server
Choosing this option will:

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

Master license server URI

`https://10.0.0.200:8089`

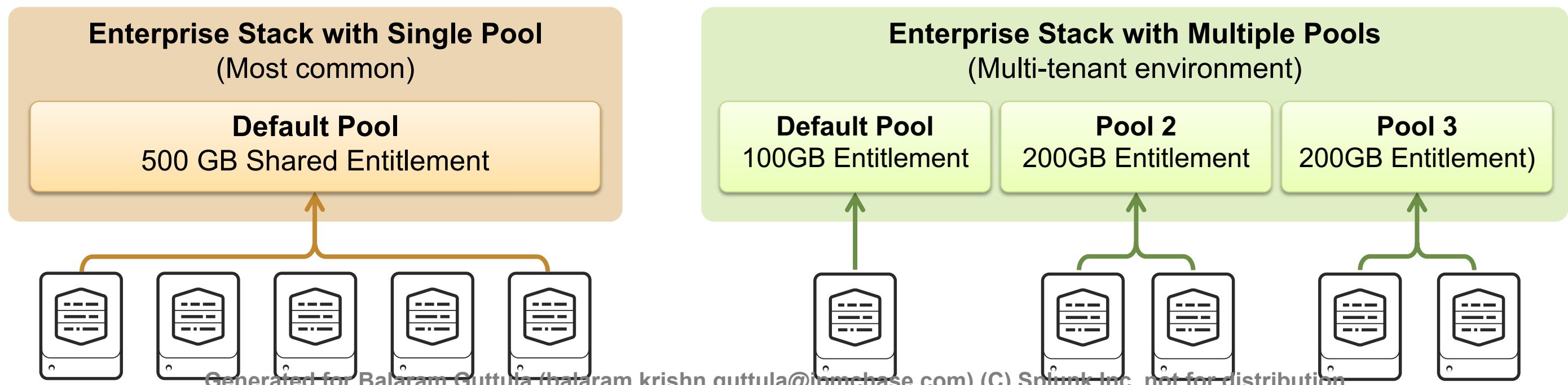
For example: `https://splunk_license_server:8089`
Use https and specify the management port.

Cancel **Save**

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.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
- Examples of License Masters with total stack of 500GB



Managing License Warnings

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

The screenshot displays two main panels of the Splunk Enterprise interface. On the left, the 'Splunk Enterprise Sales Trial stack' is shown, listing licenses, volumes, and expiration dates. A green arrow points from the 'Volume' column of the first row to the 'Edit | Delete' button in the 'Alerts' section of the 'Platform Alerts Setup' panel on the right. Another green arrow points from the 'Edit | Delete' button back to the 'Edit | Delete' button in the same row of the license table.

Splunk Enterprise Sales Trial stack

Licenses	Volume	Expiration	Status
Splunk Enterprise Sales Trial	200 MB	Apr 14, 2018 1:50:34 PM	valid
Effective daily volume	200 MB		

Platform Alerts Setup

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

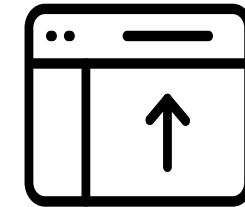
Name	Action	Enabled
DMC Alert - Expired and Soon To Expire Licenses	Edit Advanced Edit Disable	✓ Enabled
DMC Alert - Total License Usage Near Daily Quota	Edit Advanced Edit Disable	✓ Enabled

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Ingest- vs. Infrastructure-Based Pricing

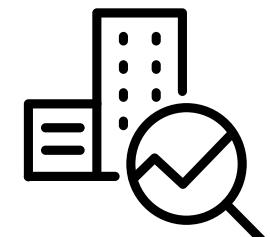
Ingest-Based Pricing

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



Infrastructure-Based Pricing

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.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 Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Module Objectives

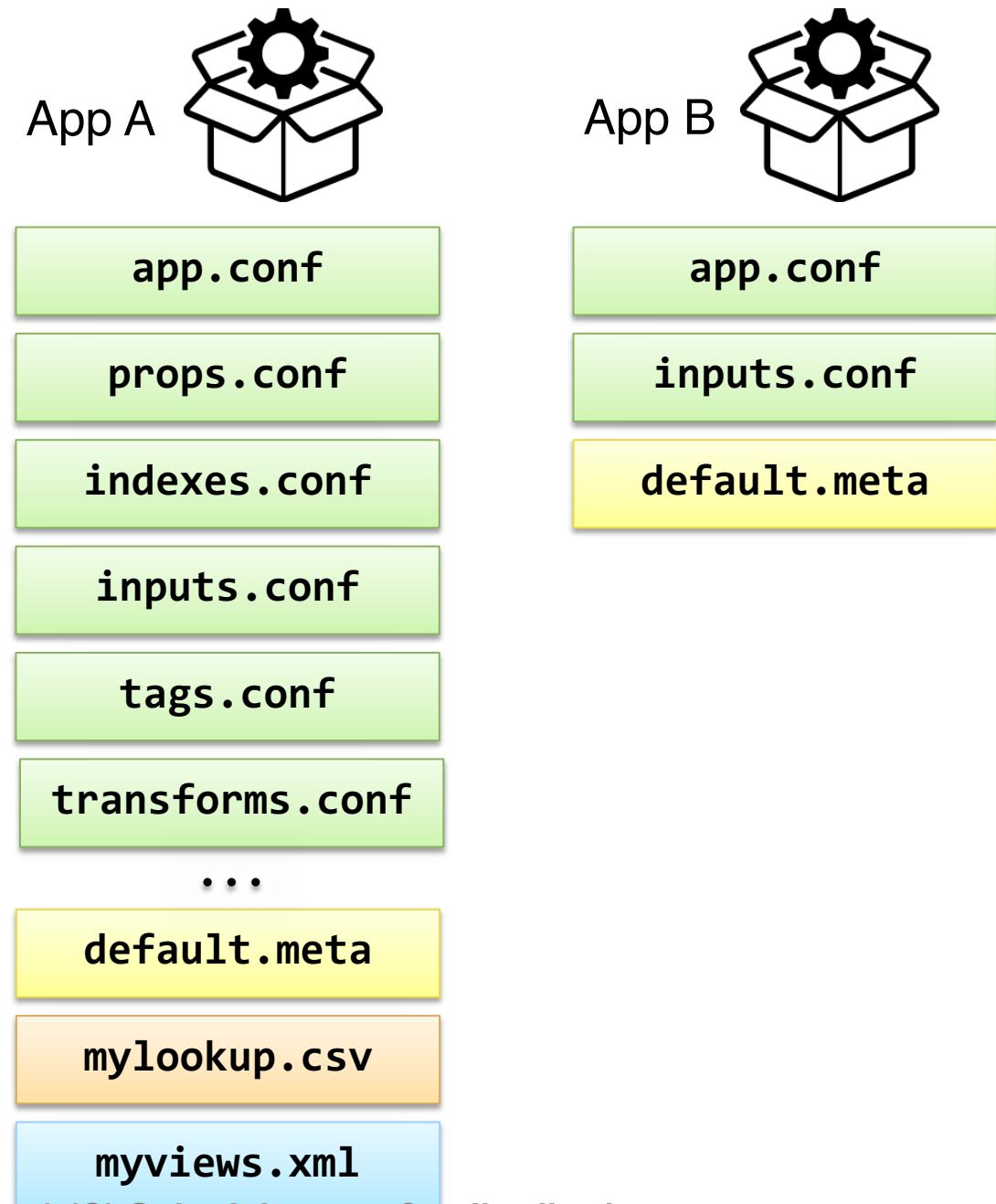
- Describe Splunk apps and add-ons
- Install an app on a Splunk instance
- Manage app accessibility and permissions

What is an App?



Splunk App

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

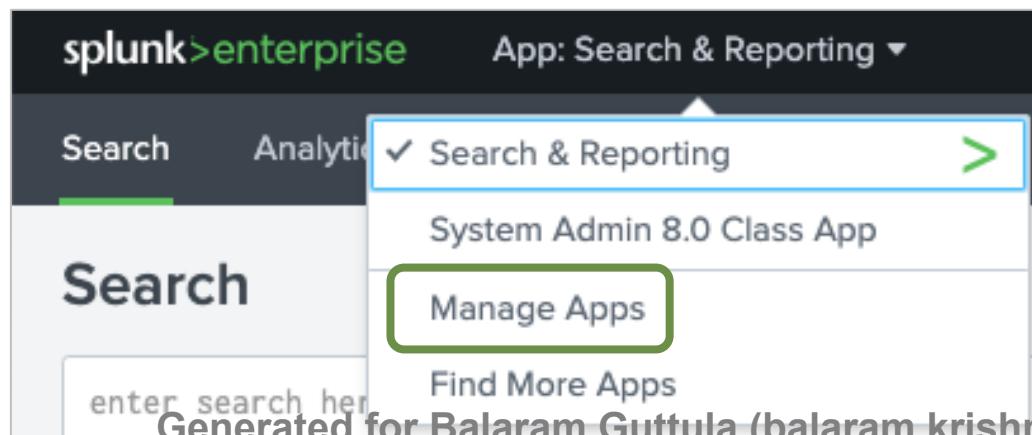


Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

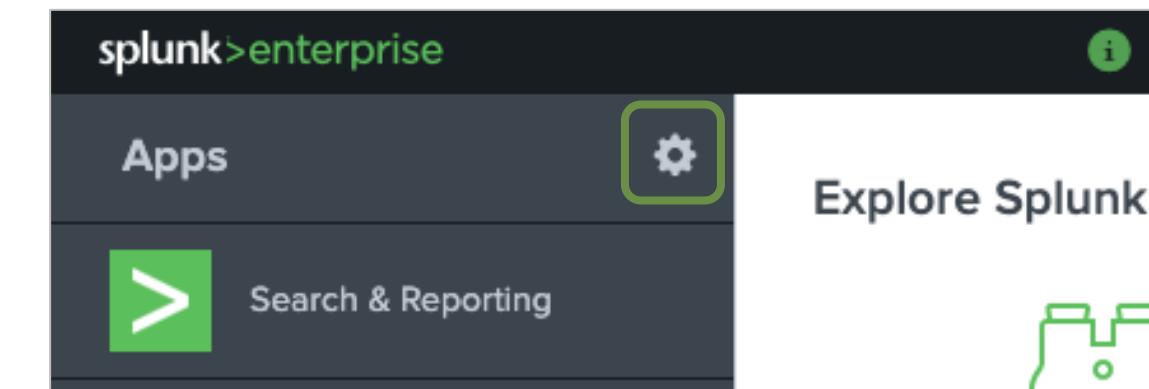
Viewing Installed Apps

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

Within an app, use the dropdown menu and select Apps: *app name* > Manage Apps



On the Home view (launcher app), click the Manage Apps icon



Managing Apps

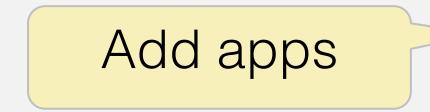
Apps

Showing 1-18 of 18 items

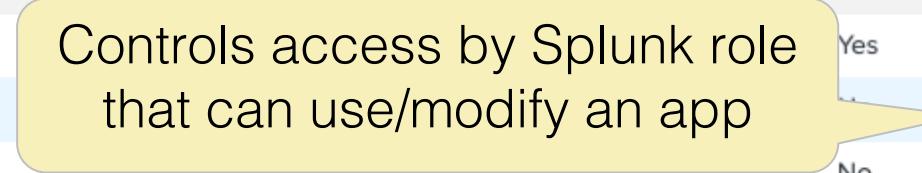
filter 

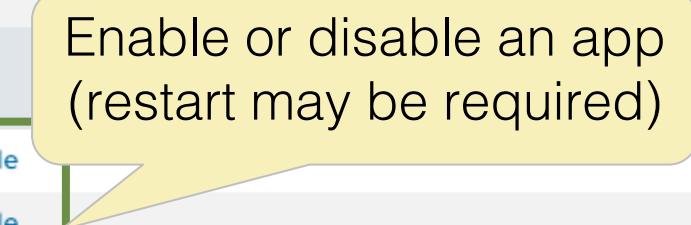
25 per page ▾

Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	Edit properties View objects
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	Edit properties View objects
Log Event Alert Action	alert_logevent	8.0.1	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Webhook Alert Action	alert_webhook	8.0.1	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Apps Browser	appsbrowser	8.0.1	Yes	No	App Permissions	Enabled	Edit properties View objects
introspection_generator_addon	introspection_generator_addon	8.0.1	Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Home	launcher		Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects
learned	learned		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
legacy	legacy		Yes	No	App Permissions	Disabled Enable	
sample data	sample_app		Yes	No	App Permissions	Disabled Enable	
Search & Reporting			Yes		App Permissions	Enabled	Launch app Edit properties View objects
Splunk Archiver App			Yes		App Permissions	Enabled Disable	Edit properties View objects View details on Splunkbase
Splunk Get Data In	splunk_gar	1.0.2	Yes	No	App Permissions	Enabled	Edit properties View objects
splunk_httpinput	splunk_httpinput		Yes	No	App Permissions	Enabled Disable	Edit properties View objects
Instrumentation	splunk_instrumentation	5.0.12	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects

Add apps 

[Browse more apps](#) [Install app from file](#) [Create app](#)

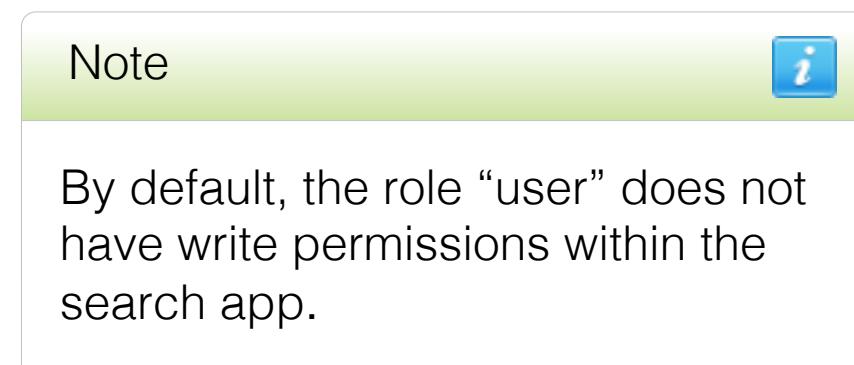
Controls access by Splunk role that can use/modify an app 

Enable or disable an app (restart may be required) 

Generated for Balaram Guttula (balaram.krishn.guttula@pmchase.com) (C) Splunk Inc, not for distribution

App Permissions

- User roles with **read** permission:
 - Can see the app and use it
- User roles with **write** permission:
 - Can add/delete/modify knowledge objects used in the app



App permissions

Users with read access can only save objects for themselves.

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

Apply selected role permissions to:

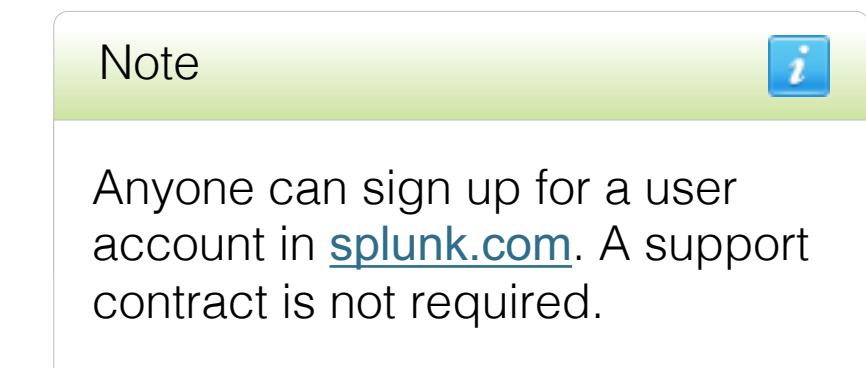
[Learn more](#)

This app only (search) All apps (system)

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Installing an App from Splunkbase

1. From the Apps page, click Browse more apps, or click Apps > Find More Apps
 - Splunk Web will access <http://splunkbase.splunk.com>
2. Search for the app you want to install
3. Select Install
 - Most apps are free
 - You must provide your [splunk.com](#) user ID and password
 - The app is installed into a sub-directory of **SPLUNK_HOME/etc/apps**
4. Restart Splunk, if required
5. Configure the app according to its documentation



Installing an App From a File

1. Download the app from <http://splunkbase.splunk.com>
 - File format may be: **.tar.gz, .tgz, .zip, .spl**
2. Install the app using one of these methods:
 - Splunk Web: Click Install app from file
 - Command line: **# splunk install app <path-to-appfile>**
 - Extract app in proper location: **# cd SPLUNK_HOME/etc/apps
tar -xf <path-to-appfile>**
3. Restart Splunk, if required
4. Configure the app according to its documentation

What is an Add-on?



Splunk Add-on

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

Difference	Apps	Add-ons
Navigation file required	✓	
Dedicated URL	✓	
Occupies a unique namespace within Splunk	✓	✓
Can be redistributed and shared using Splunkbase	✓	✓
Contains components not intended for reuse by other apps	✓	
Contains components intended for reuse by other apps		✓
Extends Splunk Web for exploring or visualizing data from a specific product or technology	✓	
Can depend on add-ons for correct operation	✓	✓

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Apps / Add-ons on Forwarders

- Universal forwarders don't have a web interface, but may still benefit from an app
- To install an add-on or app on a forwarder, use one of these methods:
 - Install the app using the CLI on the forwarder
 - Extract the app in the proper file system location
 - Use a deployment server to deploy the app

Deleting an App

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

Warning

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

Module 3 Knowledge Check

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

Module 3 Knowledge Check – Answers

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

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

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

True.

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 Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Module Objectives

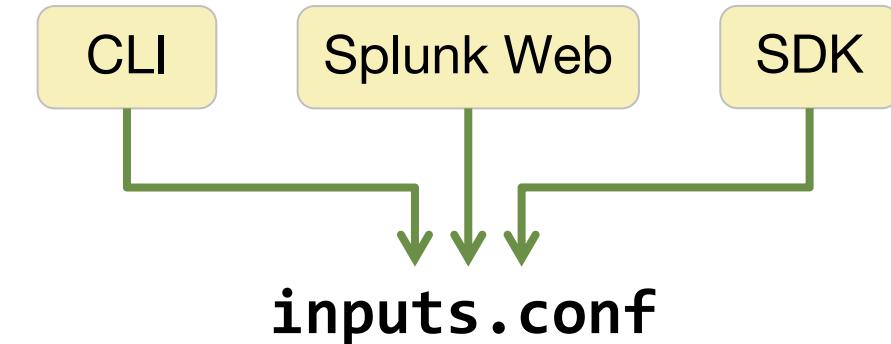
- Describe Splunk configuration directory structure
- Understand configuration layering process
 - Index time process
 - Search time process
- Use **btool** to examine configuration settings

Splunk Configuration Files



Configuration Files (.conf)

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



```
[default]  
host=www
```

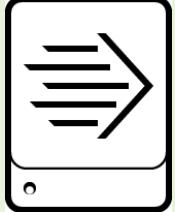
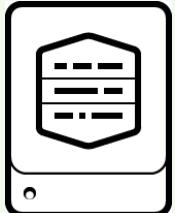
```
[monitor:///var/log/httpd]  
sourcetype = access_common  
ignoreOlderThan = 7d  
index = web
```

Note

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

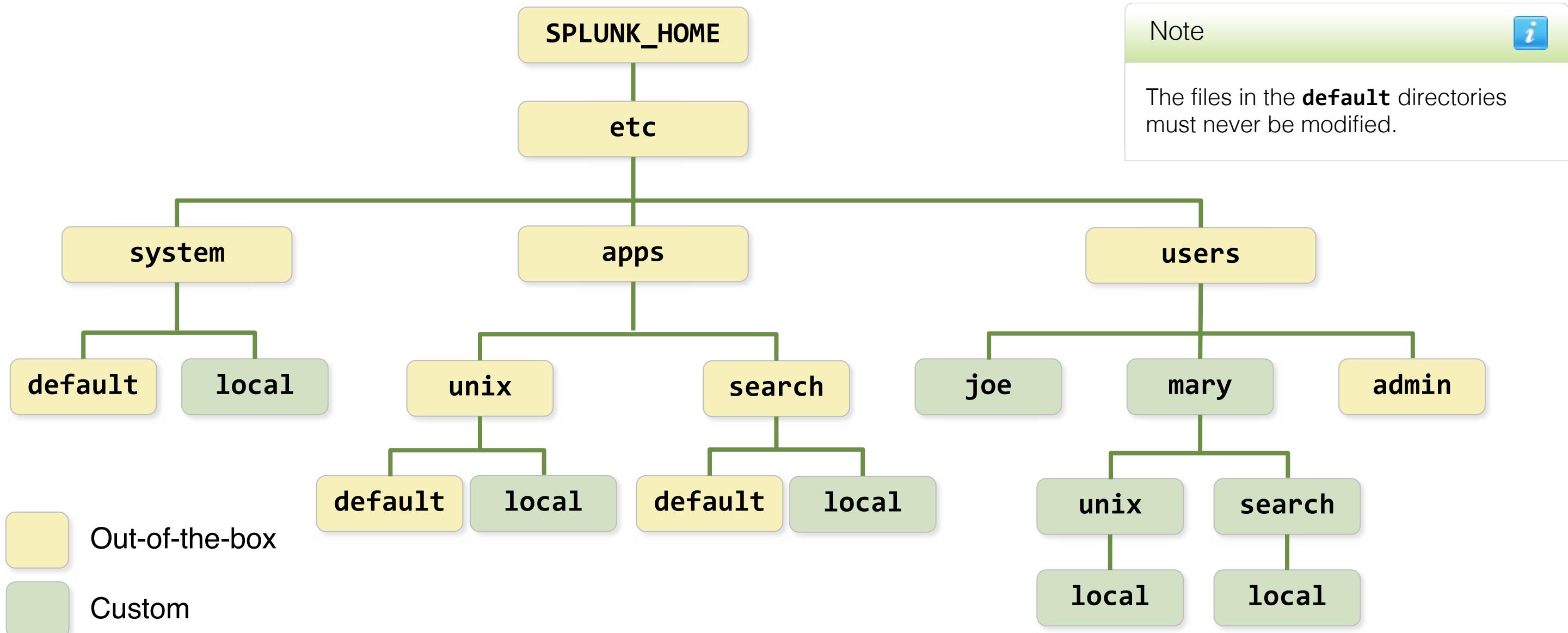
- `*.conf.spec`
- `*.conf.example`

Commonly Used Splunk Configuration Files

Component	inputs.conf	props.conf	outputs.conf
Universal Forwarder 	What data to collect (production logs)	Limited parsing (such as character encoding, refine MetaData, event breaks*)	Where to forward the data (generally to Indexers)
Indexer 	What data to collect; which ports to listen to	Refine MetaData at event level, event breaks, Time Extraction, TZ, data transformation	Not generally needed (generally Indexer does not forward data)
Search Head 	What data to collect (internal Splunk logs)	Field Extractions (search- time), lookups, and so on	Where to forward the data (such as the internal Splunk logs to an indexer)

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

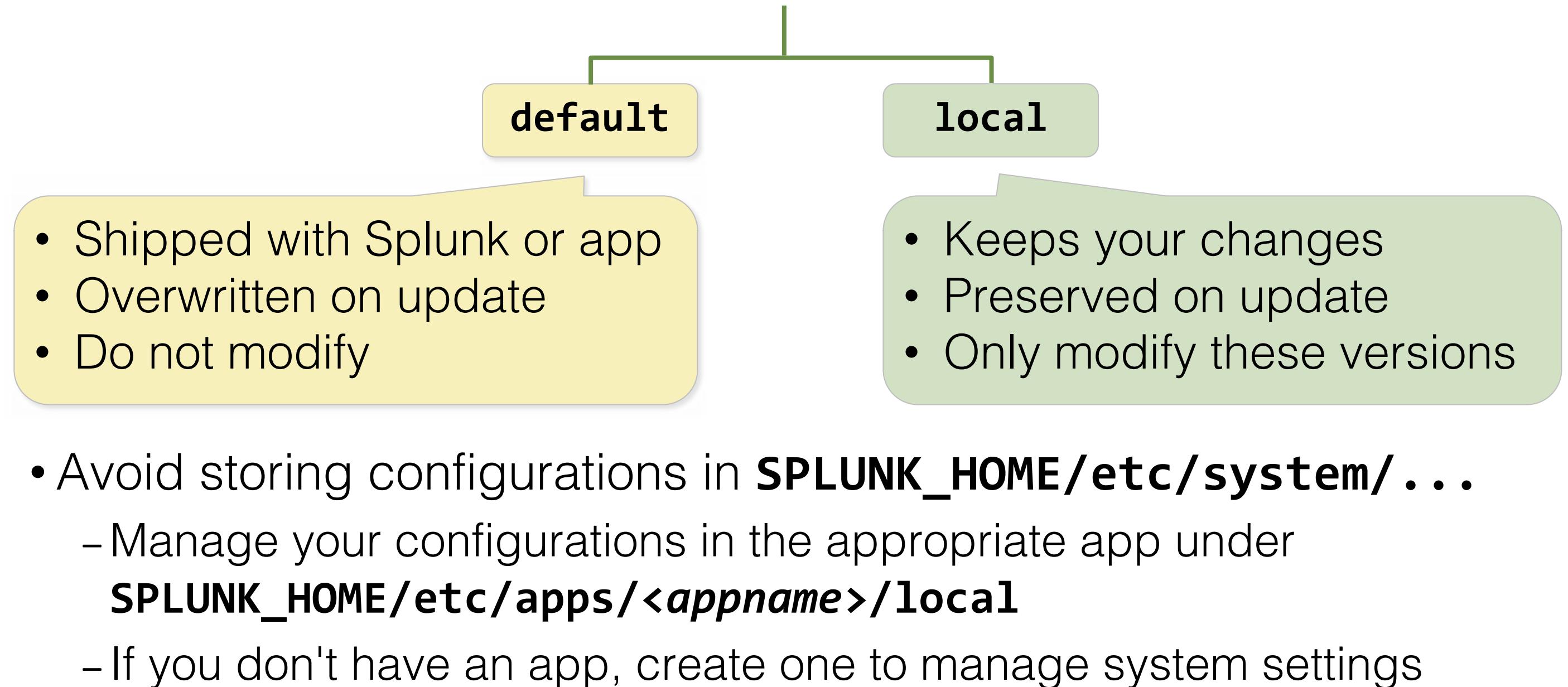
Configuration Directories



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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

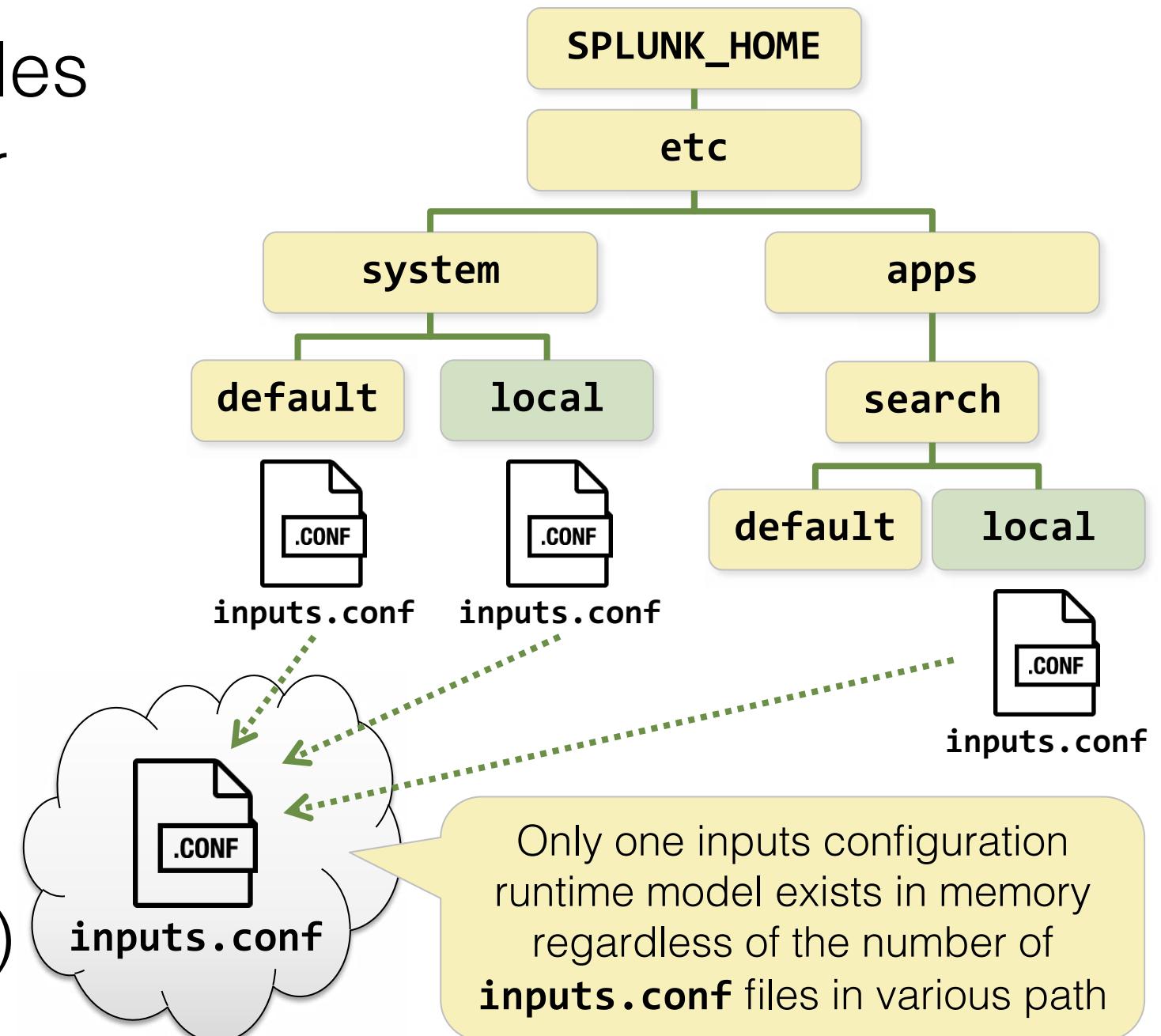
Default vs. Local Configuration



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Merging of Configuration Files

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



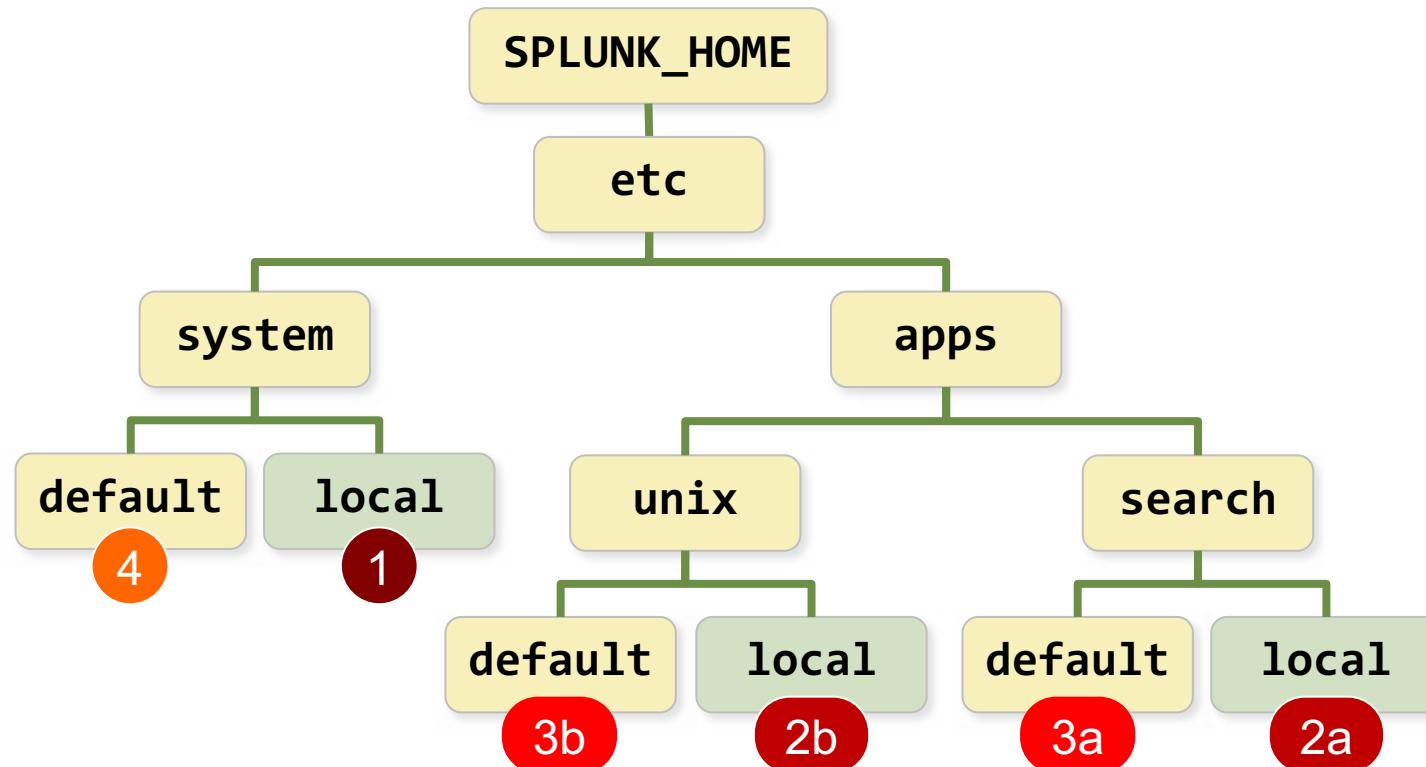
File Context and Index-time vs Search-time

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

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Index-Time Precedence (Global Context)



Precedence order

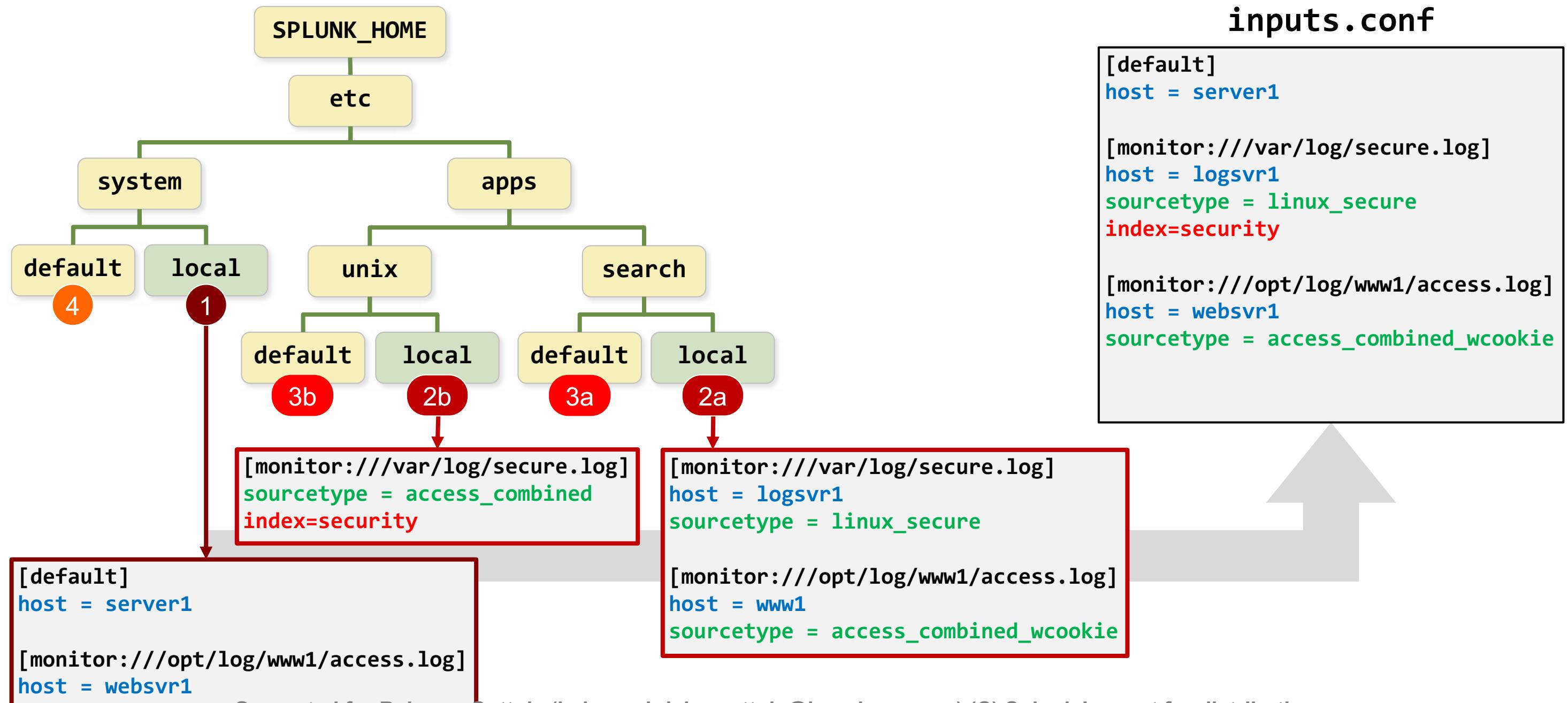
- 1 System local directory `etc/system/local`
- 2 App local directories* `etc/apps/appname/local`
- 3 App default directories* `etc/apps/appname/default`
- 4 System default directory `etc/system/default`

Note

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

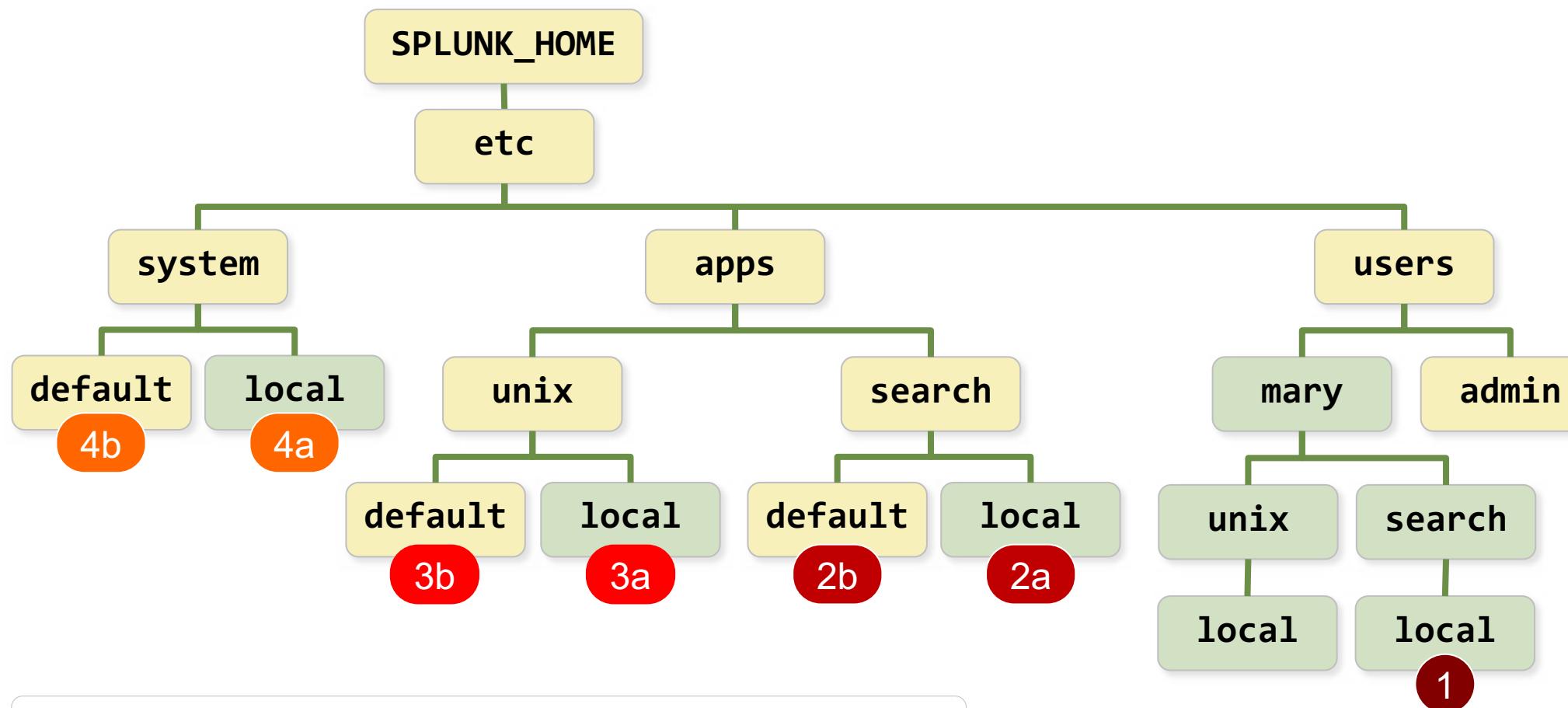
Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Example of Index-Time Precedence with `inputs.conf`



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Search-Time Precedence (App/User Context)



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

Precedence order

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

Validating the Splunk configuration

Validating the in-memory configuration

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

Validating the on-disk configuration

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

Configuration Validation with **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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Example using btool

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

```
> splunk btool inputs list monitor:///var/log/secure.log --debug  
  
etc/apps/search/local/inputs.conf      [monitor:///var/log/secure.log]  
etc/apps/search/local/inputs.conf      host = logsvr1  
etc/apps/unix/local/inputs.conf        index = security  
etc/apps/search/local/inputs.conf      sourcetype = linux_secure
```

etc/apps/unix/local/inputs.conf

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

etc/apps/search/local/inputs.conf

```
[monitor:///var/log/secure.log]  
host = logsvr1  
sourcetype = linux_secure
```

Overriding Defaults

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

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

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Reloading Configuration Files After Edit

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

Note



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

Module 4 Knowledge Check

- Which configuration file tells a Splunk instance to ingest data?
- True or False. 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 Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Module Objectives

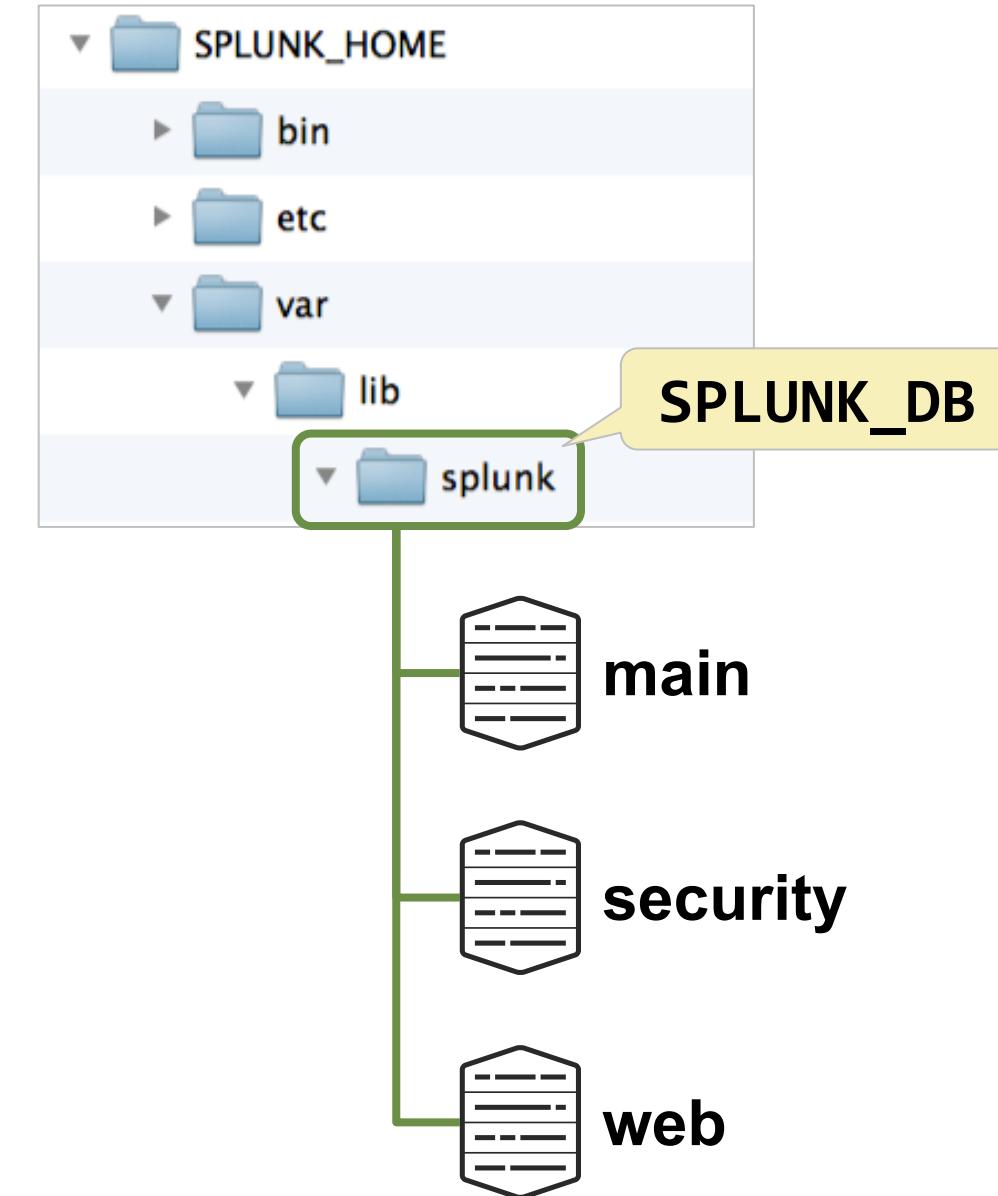
- Learn how Splunk indexes function
- Identify the types of index buckets
- Create new indexes
- Identify the advantages of using multiple indexes

What are Indexes?



Splunk Indexes

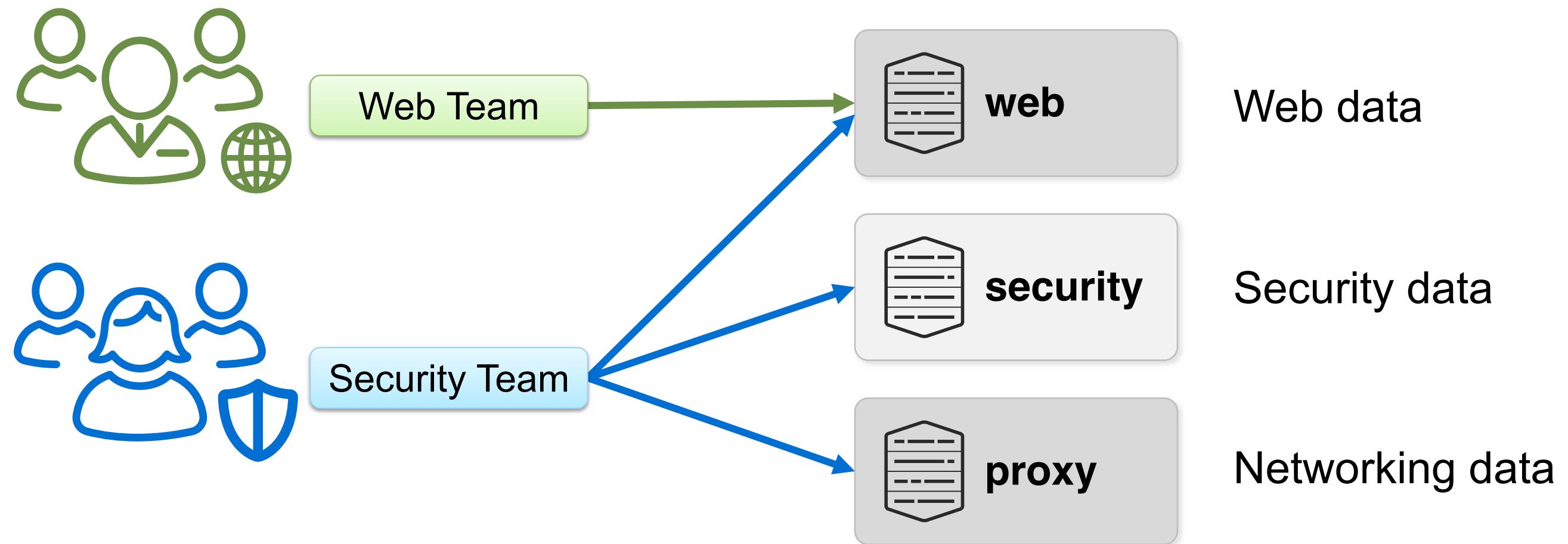
- Store input data as events
- Included with Splunk (**main**, **_internal**)
- Can be created by a Splunk administrator
- Can be used to limit scope of a search
- Allow the ability to limit access by user
- Found by default under **SPLUNK_DB**
(SPLUNK_HOME/var/lib/splunk)



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Indexes and Access Control

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Indexes and Retention

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

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

Generated for Balaram Guttula (balaram.krishn.guttula@jmpchase.com) (C) Splunk Inc, not for distribution

Preconfigured Indexes (Partial List)

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

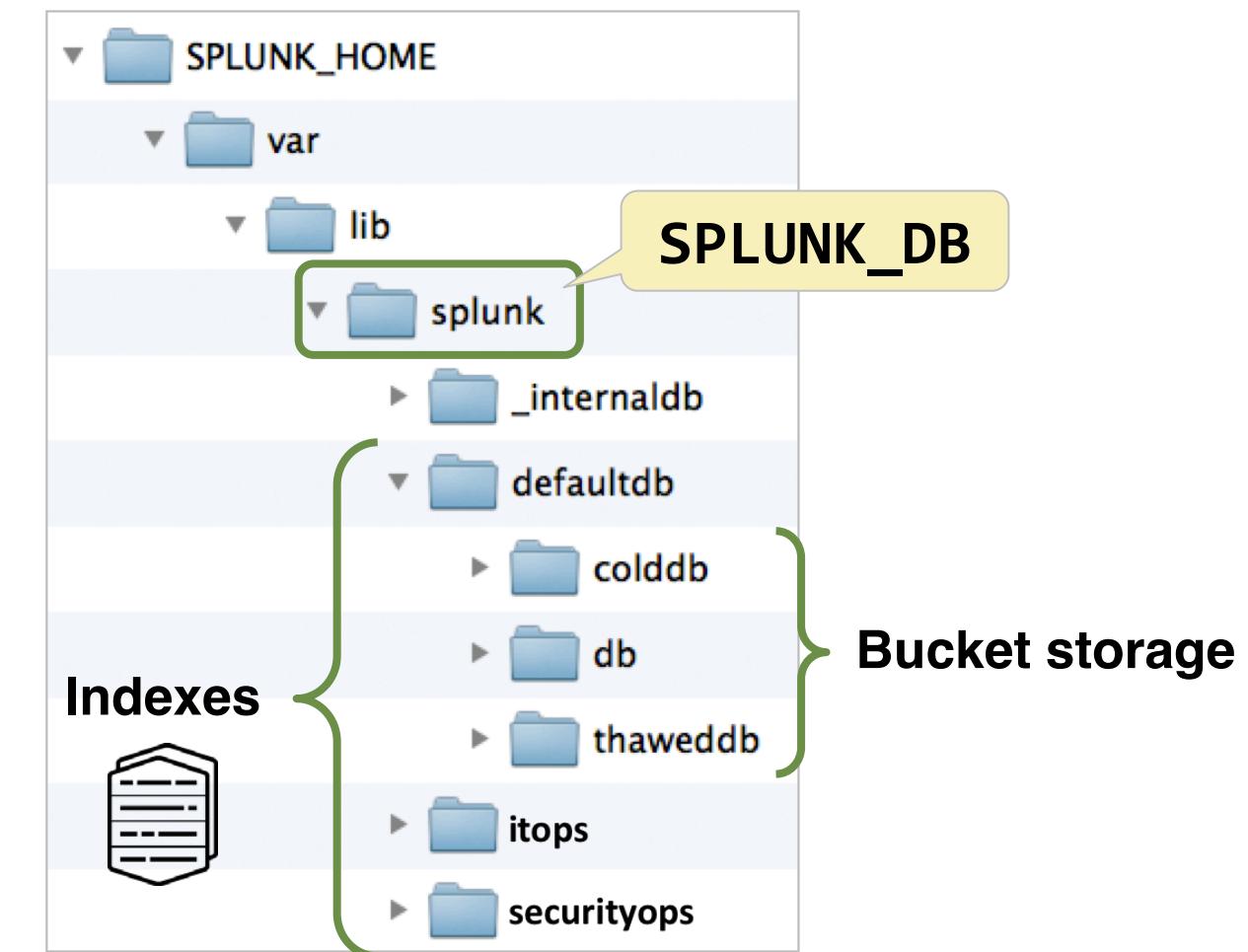
Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

What are Buckets?



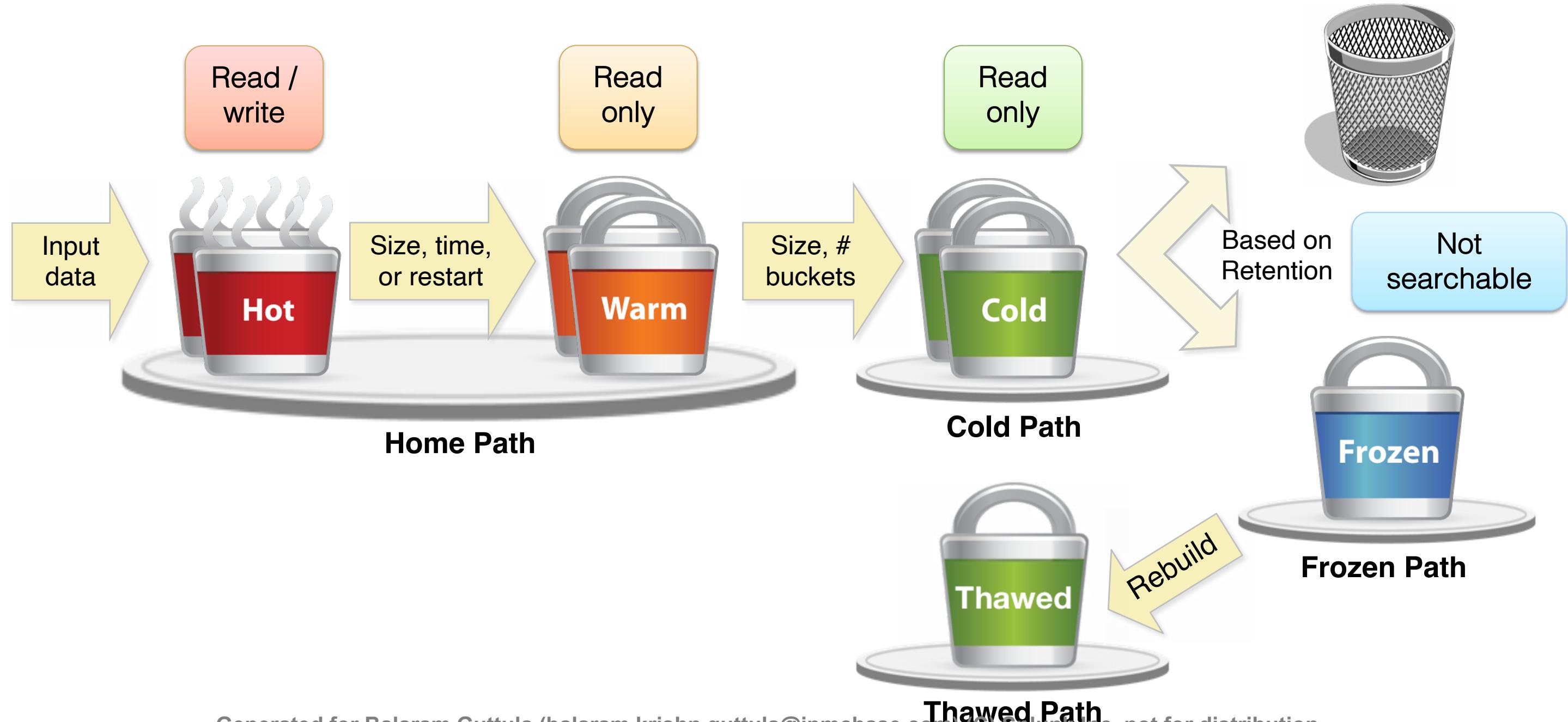
Buckets

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

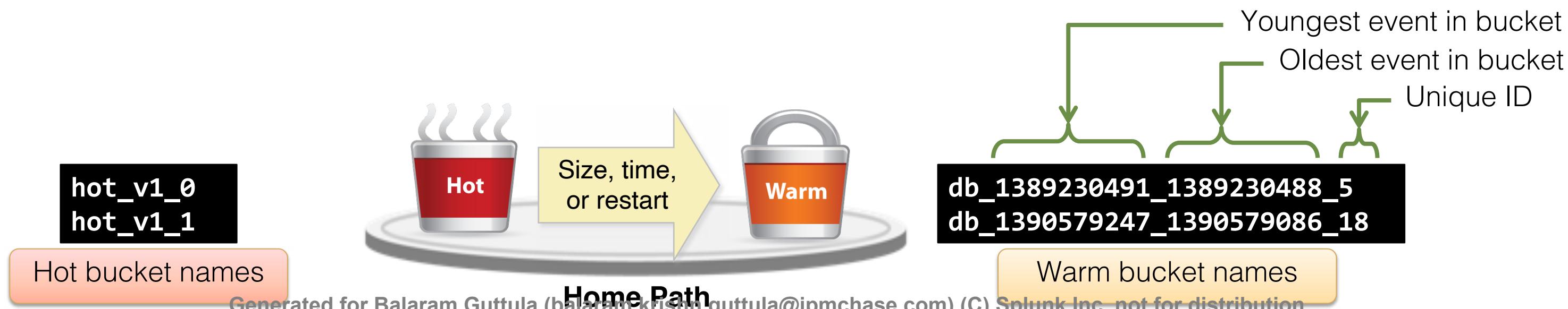
Data Flow Through an Index



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Hot and Warm Buckets

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



Warm and Cold Buckets

- Warm buckets roll over to a cold bucket:
 - When the Home Path maximum size (**homepath.maxDataSizeMB**) or the maximum warm bucket count (**maxWarmDBCount**) is reached
 - By moving the oldest Warm bucket to the Cold Path
 - Preserving the bucket name
- At search time, Splunk scans the time range on a bucket name to determine whether or not to open the bucket and search its events



Retention, Deletion, and Frozen Buckets

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



Estimating Index Growth Rate

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

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Calculating Index Storage

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

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

- Configure index:

Max Size of Entire Index GB ▾

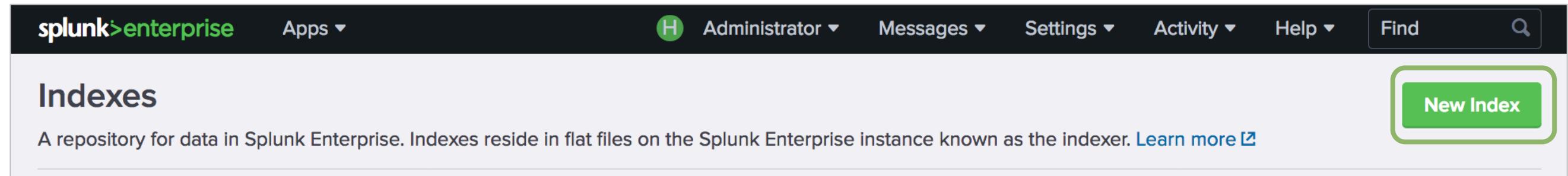
Maximum target size of entire index.

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Adding an Index

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



The screenshot shows the Splunk Web interface for managing indexes. The top navigation bar has the 'splunk>enterprise' logo, 'Apps', 'Administrator' (with a green profile icon), 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search icon. Below the navigation is a sub-navigation bar with 'Indexes' selected. A descriptive text box states: 'A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer.' A green button labeled 'New Index' is highlighted with a green border.

- Using command line:
splunk add index <index_name>
- Refer to:
docs.splunk.com/Documentation/Splunk/latest/Indexer/Setupmultipleindexes

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Adding an Index With Splunk Web

New Index ×

General Settings

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

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

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

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

Home Path Locations of Hot+Warm, Cold, and Thawed buckets

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

Cold Path

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

Thawed Path Optional data integrity check

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

Data Integrity Check Enable Disable

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Adding an Index With Splunk Web (cont.)

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

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

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

App Search & Reporting ▾

Storage Optimization

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

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

Overall index size (default = 500 GB)

Maximum bucket size:

- **auto** = 750 MB
- **auto_high_volume** = 10 GB

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

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

TSIDX Retention Policy (optional):

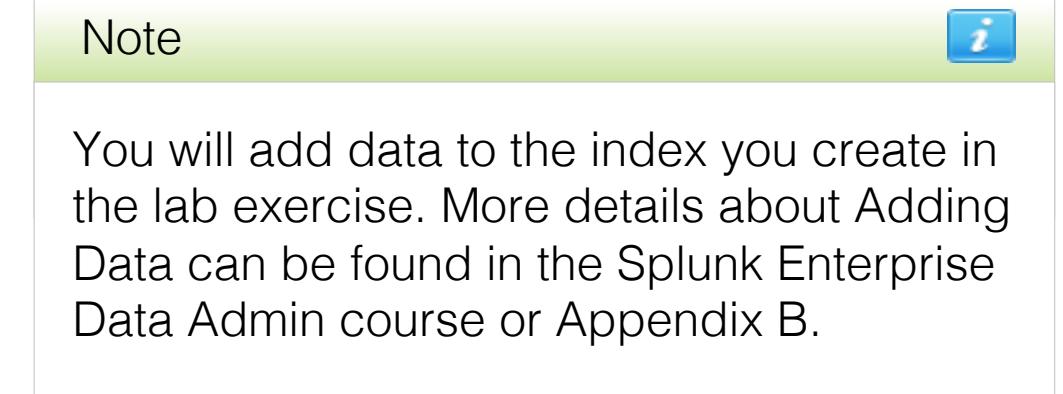
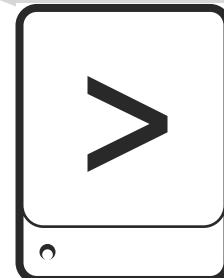
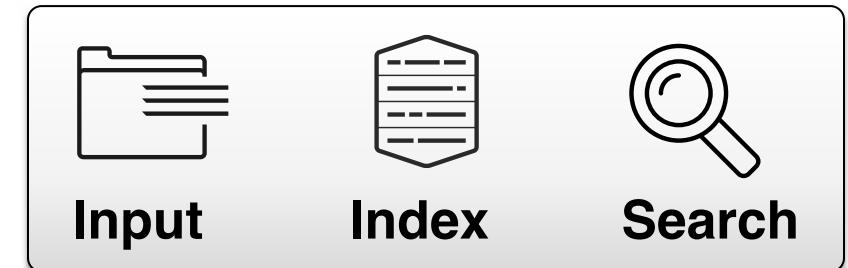
- Disabled by default; TSIDX files are not compressed
- When enabled, TSIDX files are compressed after this time

Cancel **Save**

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Testing Indexes with Input Staging

- Production data typically resides
 - On a forwarder (remote system)
 - Not on the indexer
- Test input data
 - Use Splunk Web > Add Data
 - Sample a log file on a test server
 - Check to see if **sourcetype** and other settings are applied correctly
 - Delete the test data, change your test configuration, and repeat as necessary

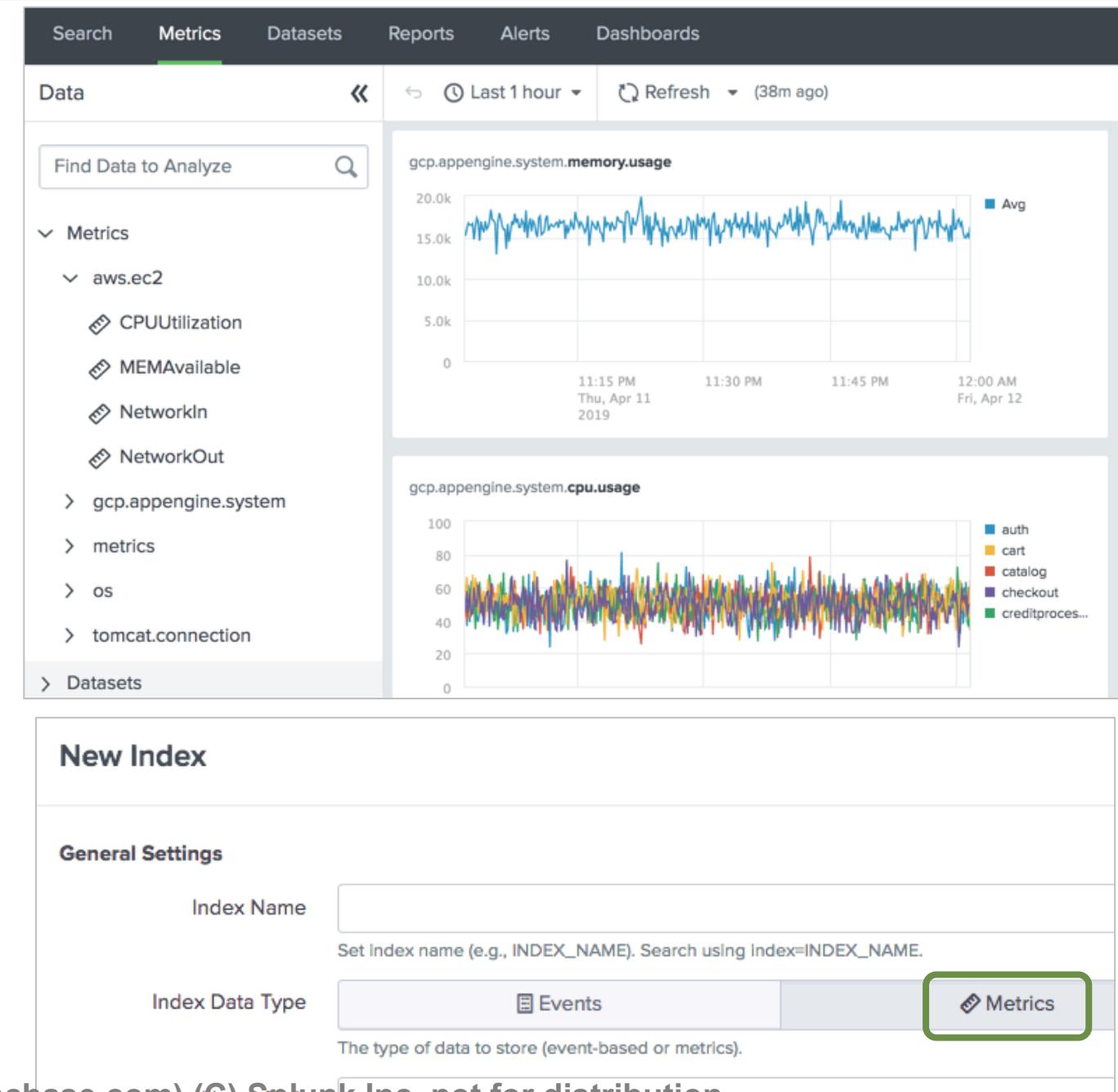


What are Metrics?



Metrics

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Module 5 Knowledge Check

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

Module 5 Knowledge Check – Answers

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

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

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

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

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

True.

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 Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Module Objectives

- Manage indexes with Splunk Web
- Describe **indexes.conf** options
- Monitor indexes with Monitoring Console (MC)
- 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

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	488.28 GB	197K	3 days ago	a few seconds ago	\$SPLUNK_DB/_introspection/db	N/A	✓ Enabled	
_telemetry	Edit Delete Disable	Events	system	488.28 GB	7	3 days ago	a day ago	\$SPLUNK_DB/_telemetry/db	N/A	✓ Enabled	
_thefishbucket	Edit Delete Disable	Events	system	488.28 GB	0			\$SPLUNK_DB/fishbucket/db	N/A	✓ Enabled	
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/historydb/db	N/A	✓ Enabled
itops	Edit Delete Disable	Events	system	1 MB	488.28 GB	0	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	system	1 MB	488.28 GB	0	3 months ago	5 minutes ago	\$SPLUNK_DB/securityops/db	N/A	✓ Enabled
splunklogger	Edit Delete Enable	Events	system	0 B	488.28 GB	0			\$SPLUNK_DB/splunklogger/db	N/A	✗ Disabled
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/summarydb/db	N/A	✓ Enabled
test	Edit Delete Disable	Events	search	173 MB	500 GB	752K	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

Launches the New Index dialog box

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

Custom indexes can be enabled/disabled or deleted

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

splunk® turn data into doing™

113

Splunk Enterprise System Administration
Copyright © 2020 Splunk, Inc. All rights reserved | 29 May 2020

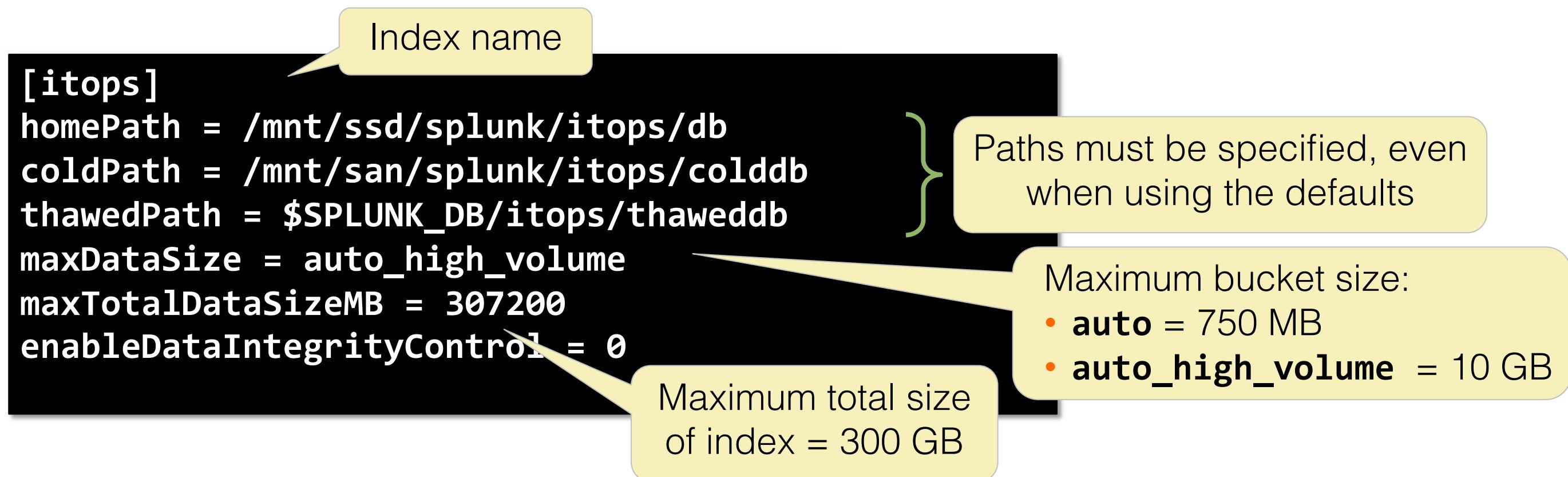
Index Data Integrity Check

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

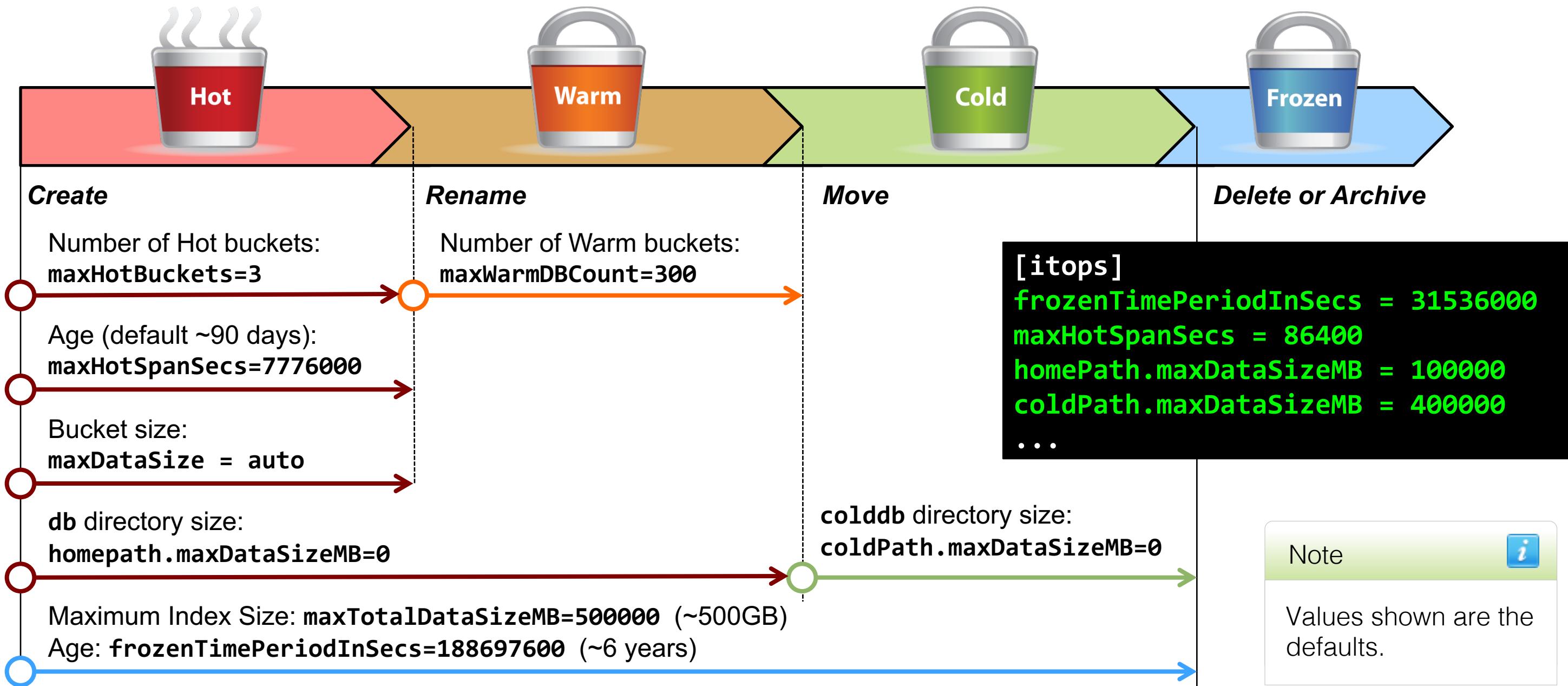
docs.splunk.com/Documentation/Splunk/latest/Security/Dataintegritycontrol

The `indexes.conf` File

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



Additional indexes.conf Options



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Index Definitions and Data

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Viewing Indexing Activity and Health in the MC

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

Monitoring Console (MC)

Overview Health Check Indexing ▾ Search ▾ Resource Usage ▾ Forward

Indexes

Group
All Indices

Inputs

Usage

- Queue fill-ratio
- Indexing rate
- CPU activity

Indexing Performance: Instance

Indexes and Volumes >

Index Detail: Instance

Volume Detail: Instance

- Volume usage per index
- Index size over time

- Detailed indexing status
- Retention policies
- Bucket configuration details

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.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

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

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

Volumes

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

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

Bucket Size (GB)

Bucket Event Count

Bucket Count

Event Count by Hosts (1)

Event Count by Sources (1)

Event Count by Sourcetype (1)

Paths

Retention policies

Settings

Generated for Balaram Guttula (balaram.krishn.guttula@pmchase.com) (C) Splunk Inc, not for distribution

Configuring High-volume Indexes

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

Warning 

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

Strict Time-based Retention Policies

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

frozenTimePeriodInSecs = 7776000 (~90 days)

maxHotSpanSecs = 86400 (~24 hours)

Warning



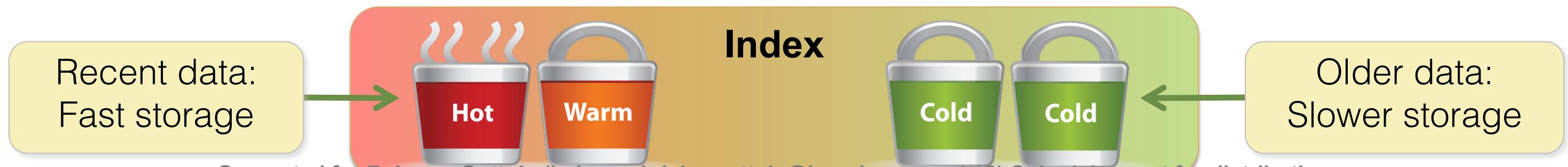
These options satisfy the strict data retention policy but may negatively impact performance.

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

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

Buckets on Different Storage Systems

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Volume Stanzas in indexes.conf

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

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

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

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Last Chance Index

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

indexes.conf Global Settings

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

What to Back Up

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Backup Recommendation

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

Moving an Index

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

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

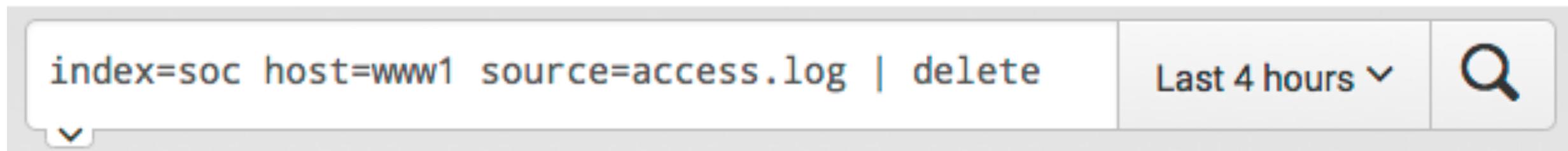
3. If this is a global change, unset the **SPLUNK_DB** environment variable and update **SPLUNK_HOME/etc/splunk-launch.conf**
4. Edit **indexes.conf** to indicate the new location
5. Start Splunk
6. After testing and verifying new index, the old one can be deleted

Removing Indexed Events

- Splunk does not provide the ability to modify the contents of an index
 - Address your configuration to prevent undesired events from being ingested
 - For undesired events already in the index, use one:
 - Let the events age-out normally (whole bucket ages out)
 - Use the **delete** command to make the unwanted events not show up in searches
 - Run **splunk clean** command to delete ALL events from the index
 - Delete the index
- These options should be used with extreme caution!

Deleting Events Using the **delete** Command

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



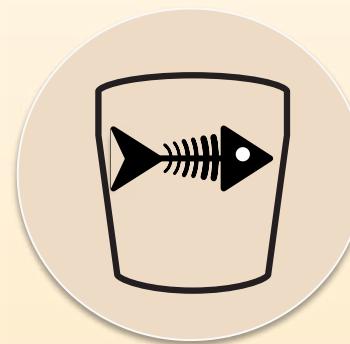
Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Cleaning Out an Index

- To flush indexed events and reset an index, use the **clean** command
 - **DATA WILL BE PERMANENTLY DESTROYED**
 - Typically used on test/dev systems, not production systems
- Command syntax:
splunk clean [eventdata|userdata|all] [-index index_name]
 - **eventdata**: Delete indexed events and metadata on each event
 - **userdata**: Delete user accounts
 - **all**: Everything, including users, saved searches, and alerts

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

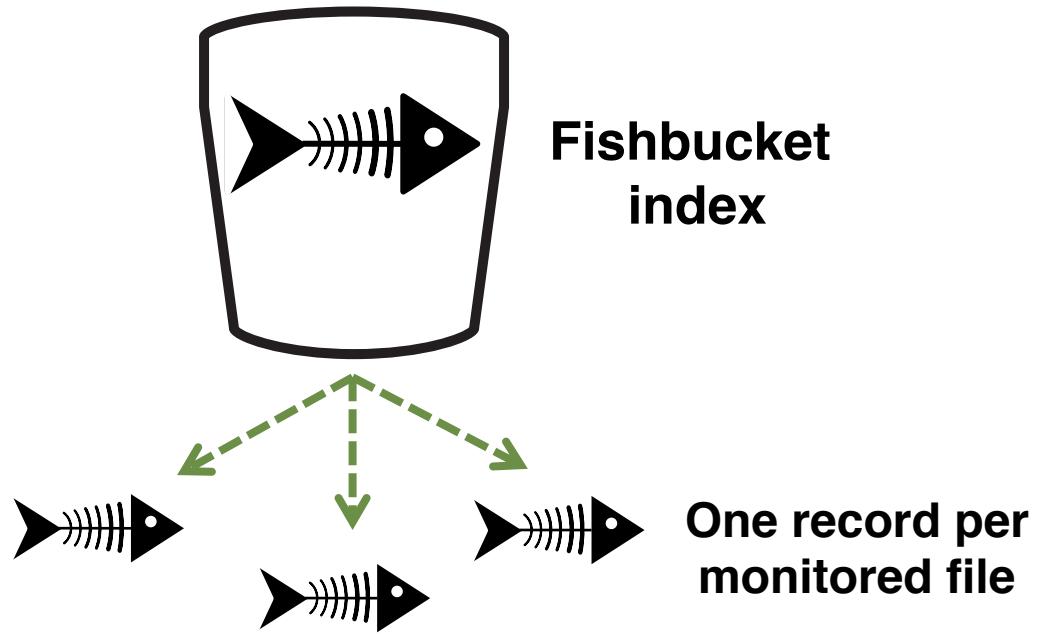
What is the Fishbucket?



Fishbucket

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution



Includes:

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

Resetting input file monitors

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

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

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

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

or

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

3. Start Splunk

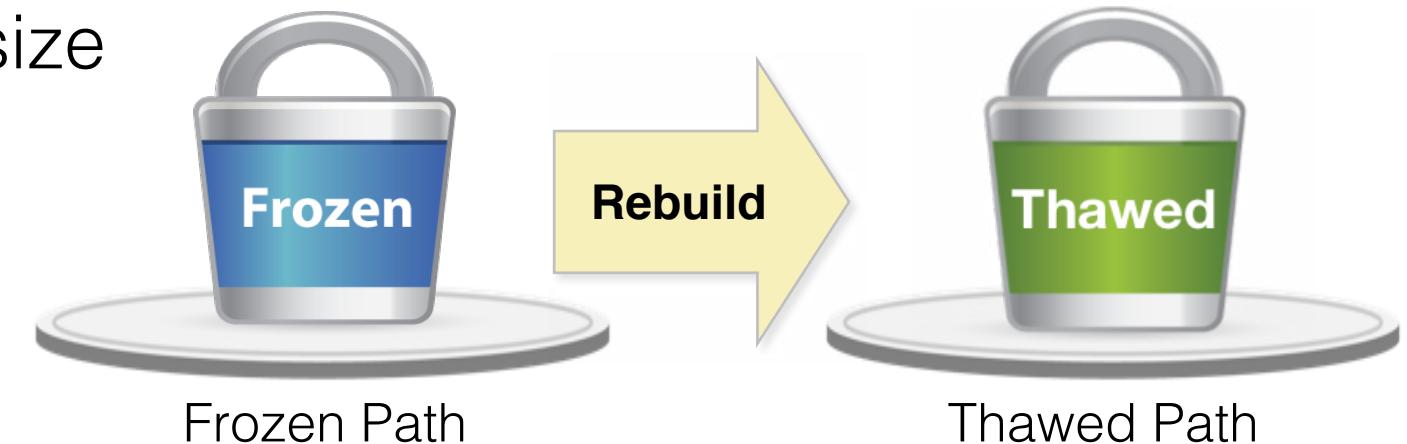
Warning



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

Restoring a Frozen Bucket

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Further Reading

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

Module 6 Knowledge Check

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

Module 6 Knowledge Check – Answers

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

False. To thaw a frozen bucket you 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 Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Module Objectives

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

Defining Users and Roles



Users

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

Roles

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

Web users



Web role

- Search the Web index

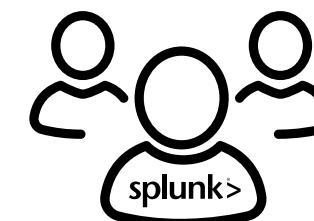
Security users



Security role

- Search the Web, Proxy and Security indexes

Splunk admins



Admin role

- Splunk administration
- Search all indexes

Managing Users and Roles

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

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

The main content area is divided into several sections:

- Add Data** (with a database icon):
 - Searches, reports, and alerts
 - Data models
 - Event types
 - Tags
 - Fields
 - Lookups
 - User interface
 - Alert actions
 - Advanced search
 - All configurations
- Explore Data** (with a magnifying glass icon):
- Monitoring Console** (with a monitoring icon):
 - Server settings
 - Server controls
 - Health report manager
 - Instrumentation
 - Licensing
 - Workload management
- KNOWLEDGE**: Searches, reports, and alerts; Data models; Event types; Tags; Fields; Lookups; User interface; Alert actions; Advanced search; All configurations.
- DATA**: Data inputs; Forwarding and receiving; Indexes; Report acceleration summaries; Virtual indexes; Source types.
- DISTRIBUTED ENVIRONMENT**: Indexer clustering; Forwarder management; Data Fabric; Distributed search.
- USERS AND AUTHENTICATION** (highlighted with a green rounded rectangle and a yellow arrow pointing to it):
 - Roles
 - Users
 - Tokens
 - Password Management
 - Authentication Methods

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

User Authentication in Splunk

Native authentication

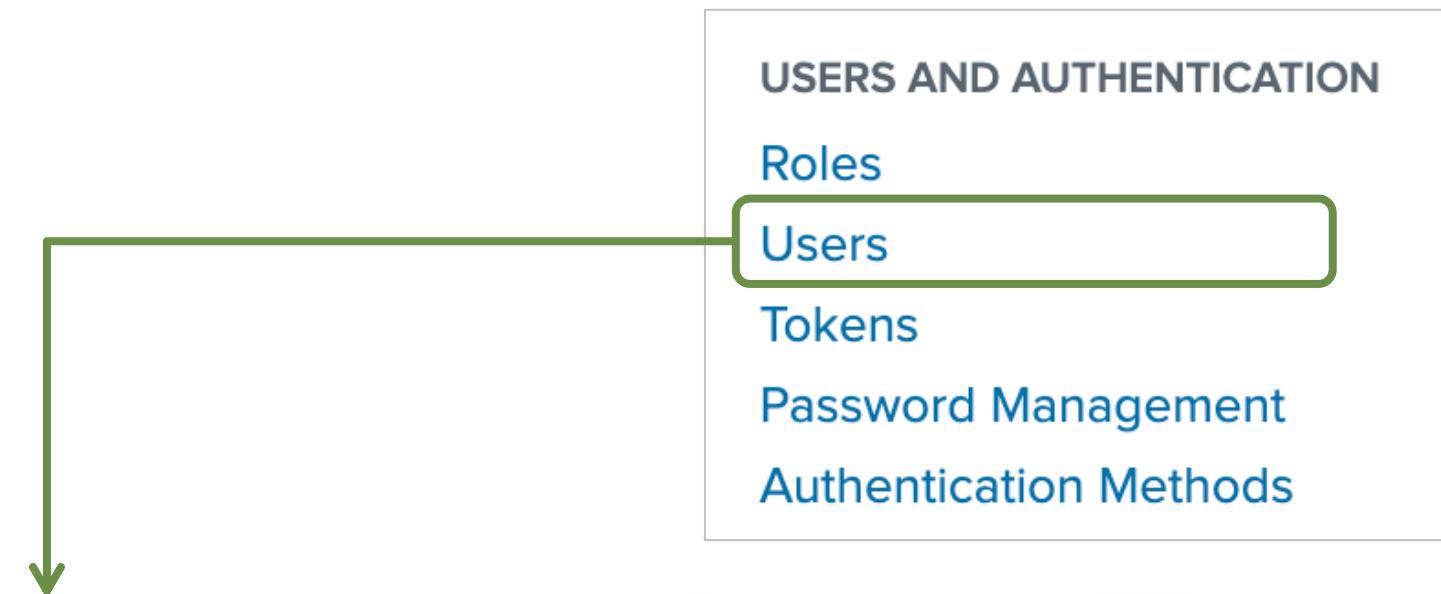
- Creating an account directly in Splunk (example: **admin** user)
- Stores passwords in **SPLUNK_HOME/etc/passwd**
- A blank **passwd** file disables native authentication
- Best Practice: Keep a failsafe account in the **passwd** file with a very strong password

Other supported authentication

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

Viewing and Managing Users

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



Users
Access Control » Users

13 Users filter 10 per page ▾

Name	Actions	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Status
acurry	View Capabilities Edit Clone	LDAP	Amanda		launcher	system		securityops	✓ Active
admin	View Capabilities Edit Clone	Splunk	Administrator	changeme@example.com	launcher	system		admin	✓ Active
blu	View Capabilities Edit Clone	LDAP	Bao Lu		launcher	system		user	✓ Active
coryf	View Capabilities Edit Clone	LDAP	cory Flintoff		launcher	system		admin	✓ Active
dhalo	View Capabilities Edit Clone				launcher	system		user	✓ Active
emaxwell	View Capabilities Edit Clone Delete				launcher	system		power	✓ Active

Add new Splunk user [New User](#)

Click to edit user settings

A yellow callout box labeled "Click to edit user settings" points to the "Edit" button for the "dhalo" user row. Another yellow callout box labeled "Add new Splunk user" points to the "New User" button in the top right corner of the table header.

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Native Authentication: Adding Users

Create User

Name acurry
Full name Amanda Curry
Email address acurry@example.com
Set password
Confirm password

Password must contain at least ?
✓ 1 character

Time zone ? -- Default System Timezone --
Default app ? launcher (Home)
Assign roles ? Available item(s) add all »
Selected item(s) user
admin
can_delete
power
splunk-system-role
user

Create a role for this user
Require password change on first login

USERS AND AUTHENTICATION

Roles
Users
Tokens
Password Management
Authentication Methods

New User

Defaults to search head time zone
Defaults to role's default app, or Home if no role default app is set
Defaults to user role only

```
graph LR; A[New User] --> B[Create User]; C[Time zone: -- Default System Timezone --]; D[Default app: launcher (Home)]; E[Available item(s): admin, can_delete, power, splunk-system-role, user]; F[Selected item(s): user]; G[Time zone: Defaults to search head time zone]; H[Default app: Defaults to role's default app, or Home if no role default app is set]; I[Assigned roles: Defaults to user role only]
```

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Identifying Roles

Roles

5 Roles filter

Name	Actions	Native capabilities	Inherited capabilities	Default App
admin	Edit▼	85	30	
can_delete	Edit▼	4	0	
power	Edit▼	7	23	
splunk-system-role	Edit▼	0	115	
user	Edit▼	23	0	

New Role 

USERS AND AUTHENTICATION

Roles

Users

Tokens

Password Management

Authentication Methods

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Creating User Roles: Inheritance

New Role

Name * ? soc_analyst

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

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

Role name filter All ▾

admin
 can_delete
 power
 splunk-system-role
 user

Cancel Create

Create a name for the role

Inheritance:

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

Generated for Balaram Guttula (balaram.krishn.guttula@jmpchase.com) (C) Splunk Inc, not for distribution

Creating User Roles: Capabilities

The screenshot shows the 'New Role' creation interface. The 'Name' field is set to 'soc_analyst'. The '2. Capabilities' tab is selected. A yellow callout points to a dropdown menu labeled 'All' which includes options: 'Show native', 'Show inherited', 'Show selected', 'Show unselected', and 'Show all' (which is checked). Another yellow callout points to the list of capabilities, stating 'Capabilities inherited from other roles are selected'. The list includes 'accelerate_search' (selected), 'change_own_password' (selected), and 'delete_by_keyword'. At the bottom are 'Cancel' and 'Create' buttons.

New Role

Name *

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

Select specific capabilities for this role.

Capability Name All ▾

- accelerate_datamodel
- accelerate_search
- admin_all_objects
- change_own_password
- delete_by_keyword

...
Cancel Create

Source dropdown filters the displayed role capabilities

Capabilities inherited from other roles are selected

Generated for Balaram Guttula (balaram.krishn.guttula@pmchase.com) (C) Splunk Inc, not for distribution

Creating User Roles: Indexes

New Role

Name * soc_analyst

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

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

Index Name	filter	Included	Default	All
All non-internal indexes		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Show selected
All internal indexes		<input type="checkbox"/>	<input type="checkbox"/>	Show unselected
_audit		<input type="checkbox"/>	<input type="checkbox"/>	Show inherited
_internal		<input type="checkbox"/>	<input type="checkbox"/>	Show native
_introspection		<input type="checkbox"/>	<input type="checkbox"/>	Show all
_metrics		<input type="checkbox"/>	<input type="checkbox"/>	
_telemetry		<input type="checkbox"/>	<input type="checkbox"/>	

Controls which indexes user has access to

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

Dropdown filters the index list

Note

Indexes inherited from a parent role are searchable and cannot be disabled

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Creating User Roles: Restrictions

New Role

Name * soc_analyst

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

Restrict searches

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

Search filter SPL generator

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

Indexed fields ?
Select or type an indexed field...

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

SPL Search filter

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

Concatenation option ?
OR ▾

Generated search filter SPL

Add to SPL search filter Reset Preview search filter results ▾

Note: the SPL search filter can only include:

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

Cancel Create

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Creating User Roles: Resources

New Role

Name *

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

This role

Default app Default app

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

Standard search limit

Real-time search limit

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

Standard search limit

Real-time search limit

Role search time window limit
Select a time window for searches for this role. Inherited roles can override this setting.

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

Standard search limit MB

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

The `authorize.conf` File

- Contains the Splunk role configuration
- Should not be modified from the **default** directory:
SPLUNK_HOME/etc/system/default/authorize.conf
- Should only be modified from the **local** directories:
SPLUNK_HOME/etc/system/local or
SPLUNK_HOME/etc/apps/<appname>/local

authorize.conf
(example entries)



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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Creating a copy of an existing role

- Using inheritance:
 - Create a new role and configure the **1. Inheritance** tab
 - Provides all the capabilities and index settings of the inherited role
 - Does not provide ability to turn off inherited capabilities or index access
- Without inheritance:
 1. Use **Edit > Clone** in Splunk Web:
 2. Make modifications to the new role

Roles				
5 Roles	filter	Actions	Native capabilities	Inherited capabilities
admin	Edit▼	85	30	
can_delete	Edit▼	4	0	
power	Edit▼	7	23	
splunk-system-role	Edit	0	115	
user	View Capabilities Clone	23	0	

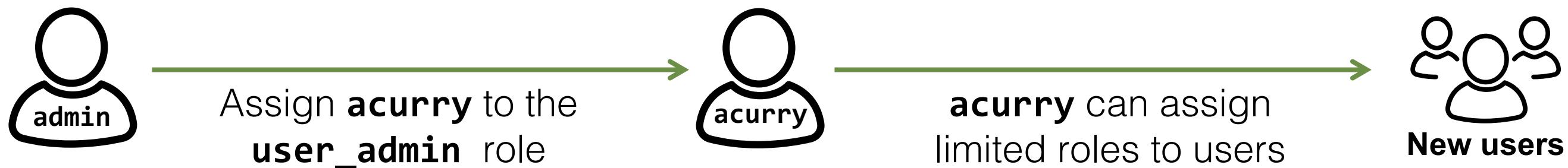
Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Example Scenario With `edit_roles_grantable`

Example scenario:

Separate and delegate user administration tasks

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

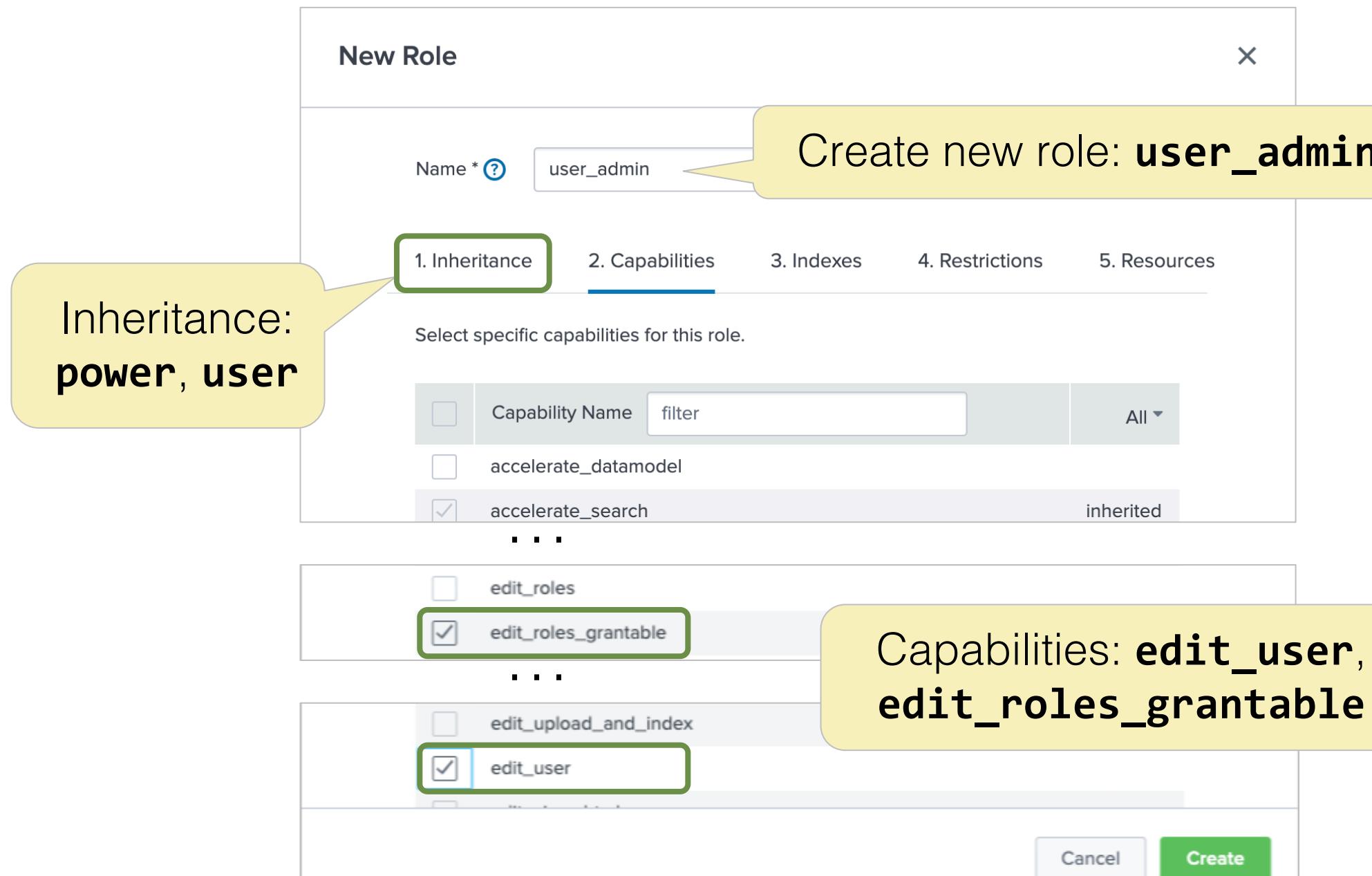


Issues to consider:

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Assigning `edit_roles_grantable` Capability



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Password Policy Management

Password Policy Management

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

Password Rules

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

Expiration

<input type="button" value="Enable"/> <input type="button" value="Disable"/>		
Days until password expires	90	Number of days until a password expires.

USERS AND AUTHENTICATION

Roles

Users

Tokens

Password Management

Authentication Methods



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

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Unlocking Users

- For users who have:
 - Forgotten their password
 - Exceeded failed login attempts threshold
(configured under Password Management)
- Using Splunk Web, select Settings > Users:

Lockout

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

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

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

Enable Disable

Name	Actions		Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Status
acury	View Capabilities Edit Clone		LDAP	Amanda		launcher	system		securityops	✓ Active
admin	View Capabilities Edit Clone		Splunk	Administrator	changeme@example.com	launcher	system		admin	✓ Active
ayoung	View Capabilities Edit Clone Delete Unlock		Splunk			launcher	system		power	🔒 Locked

- Using CLI:

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

Admin Passwords

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

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

- To generate a random password during startup:

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

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

Splunk Authentication Options

Authentication Methods

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

Internal Splunk Authentication (always on)

- External None
 LDAP
 SAML

Multifactor Authentication

Not available with external authentication such as SAML.

- None
 Duo Security
 RSA Security

[Reload authentication configuration](#)

USERS AND AUTHENTICATION

[Roles](#)

[Users](#)

[Tokens](#)

[Password Management](#)

[Authentication Methods](#)



Note



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

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Mapping LDAP/SAML Groups to Roles

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

splunkAdmins

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

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

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

LDAP Users

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

add all >

« clear all

LDAP Groups

Access controls > Authentication method > LDAP strategies > LDAP Groups

Showing 1-4 of 4 items

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

Mapped roles for LDAP groups

filter

« Back to strategies

25 per page

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.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

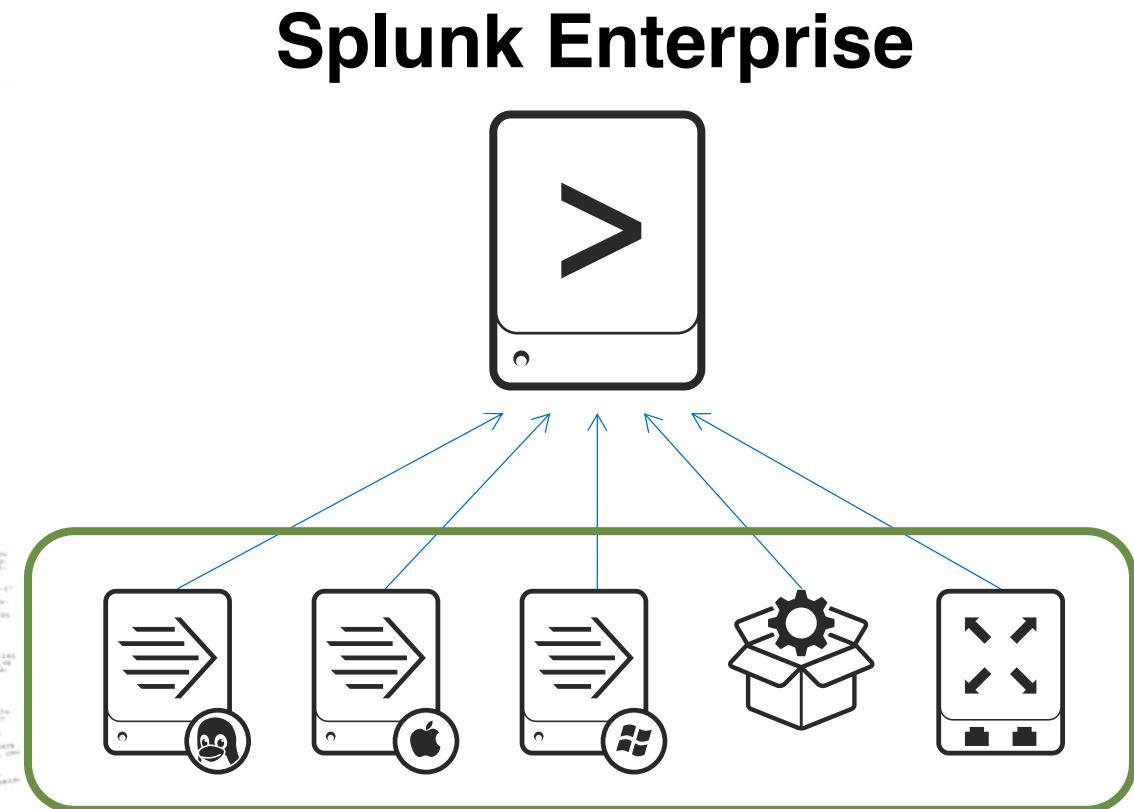
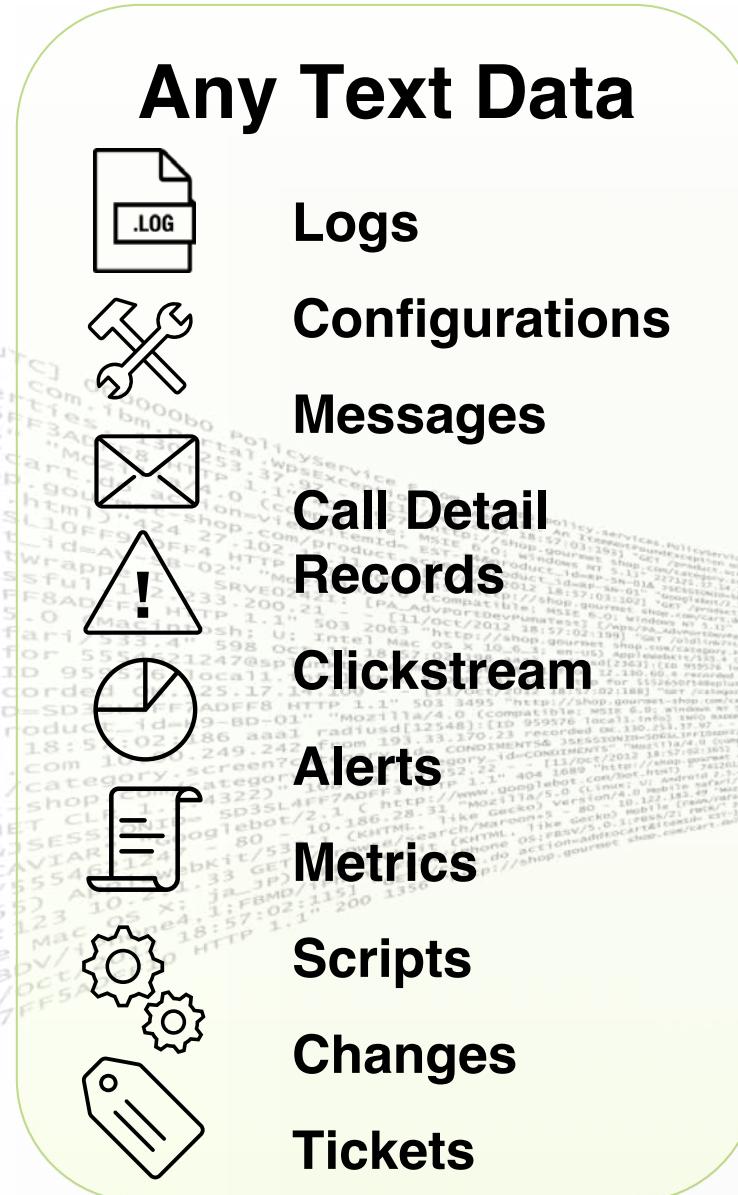
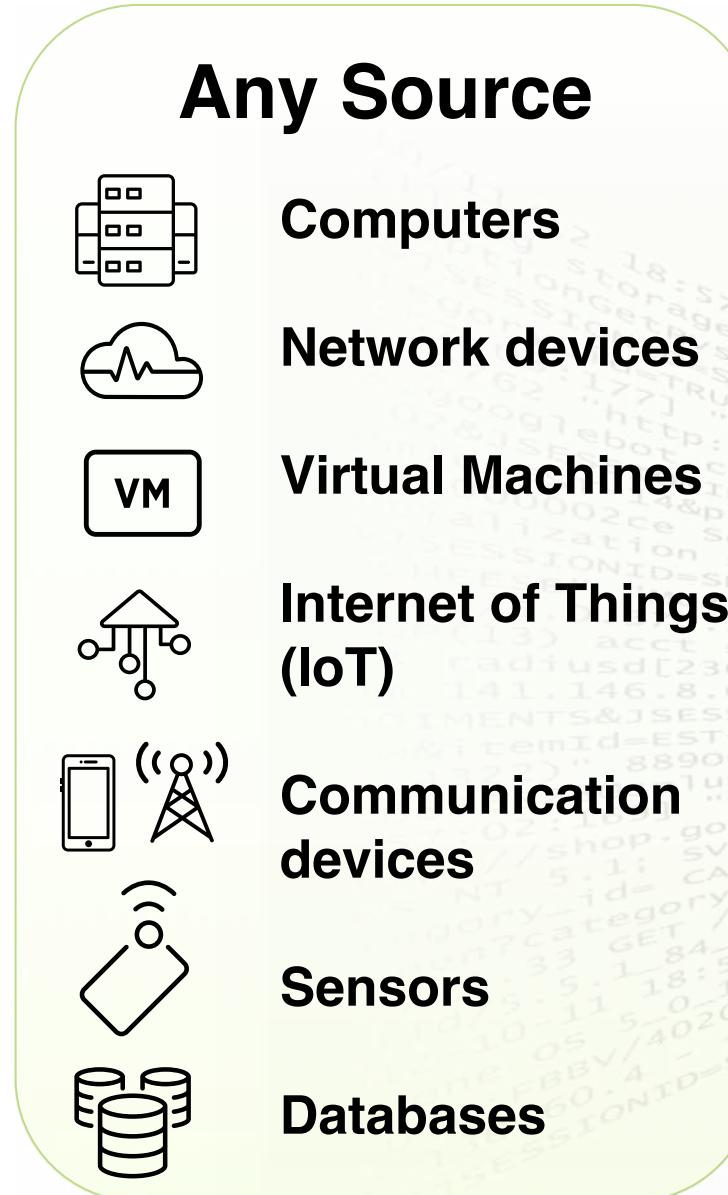
Module 8: Configuring Basic Forwarding

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Module Objectives

- Identify forwarder configuration steps
- Configure a Universal Forwarder
- Identify forwarder configuration files

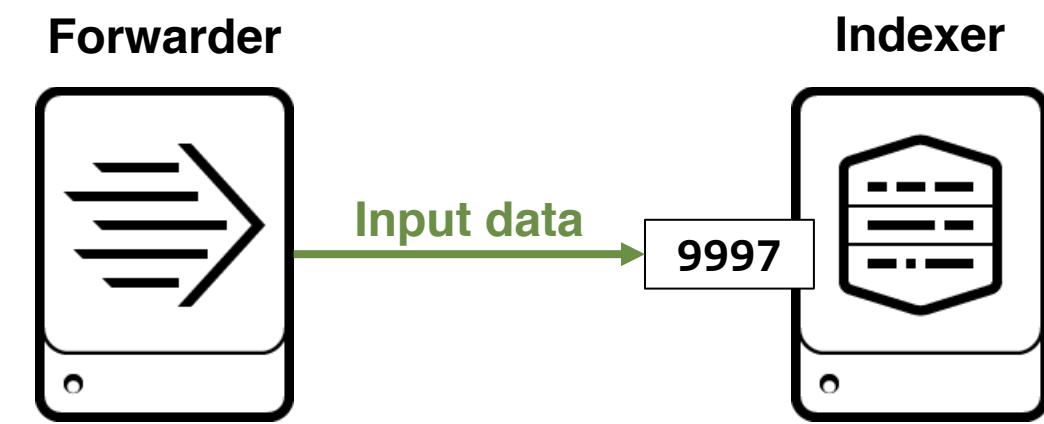
Forwarding Data to Splunk



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Forwarders and Indexers

- In production environments:
 - Indexers run on dedicated servers
 - Most input data is on remote servers
- Install **forwarders** on remote servers to
 - Gather the data
 - Send it over the network to indexers
- Configure indexers to listen on a receiving port for the forwarded data



Deployment Server for Forwarder Management

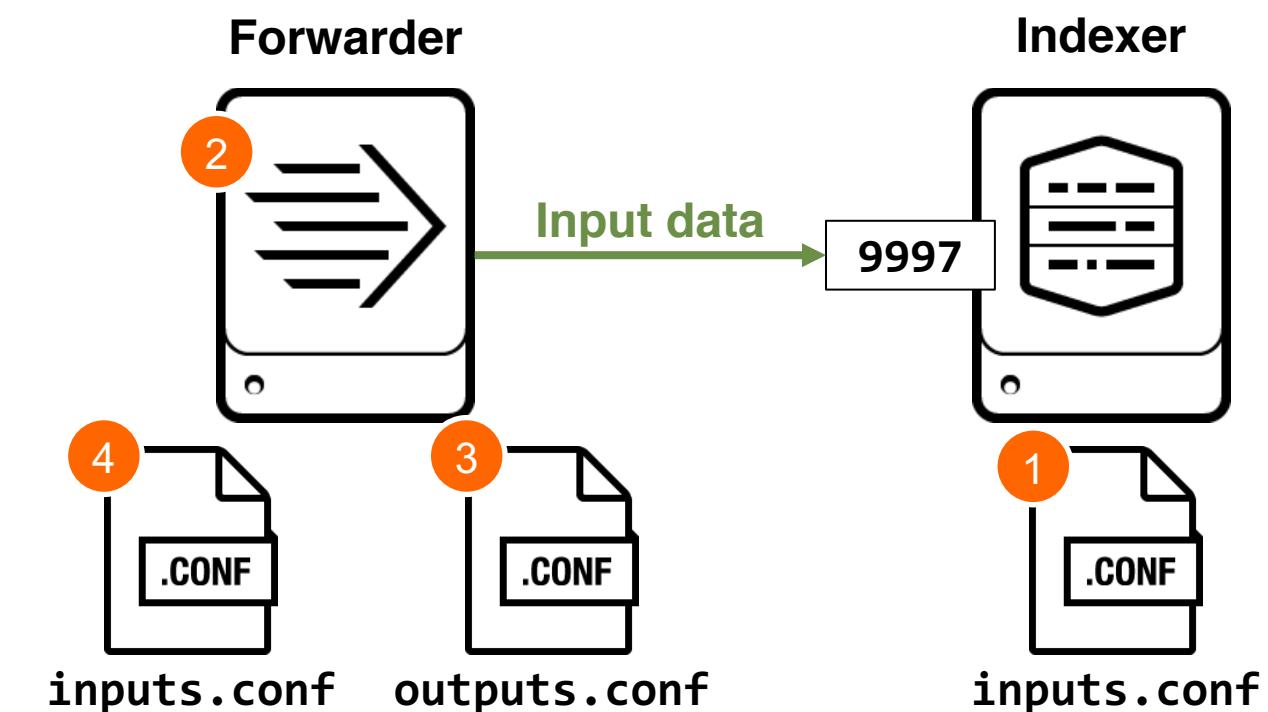
- Manages forwarders centrally and remotely
- Used in larger or production environments
- Provides a Forwarder Management interface
 - Centralized configuration management tool for forwarder configurations
 - Allows forwarders to be managed in groups (server classes)
- Discussed in detail in the *Splunk Enterprise Data Administration* class

Scenario	?
In this course's lab, you will set up a single forwarder manually for testing.	

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Universal Forwarder Configuration Steps

1. Set up a receiving port on each indexer
 - Task only needs to be performed once
2. Download and install Universal Forwarder
3. Set up forwarding on each forwarder, by either:
 - Editing **outputs.conf** manually
 - Using Deployment Server
4. Add inputs on forwarders, by either:
 - Editing **inputs.conf** manually
 - Using Deployment Server
 - Running Splunk commands (CLI)



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

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>

- Configuration is saved in **inputs.conf** as:

[splunktcp://port]

The screenshot shows the 'Forwarding and receiving' configuration page. It has two main sections: 'Forward data' and 'Receive data'. Under 'Forward data', there is a 'Forwarding defaults' link and a 'Configure forwarding' link with a '+ Add new' button. Under 'Receive data', there is a 'Configure receiving' link with a '+ Add new' button. A green arrow points from the '+ Add new' button on the 'Receive data' page to the 'Configure receiving' sub-page, which is displayed below. The sub-page title is 'Configure receiving' and it says 'Set up this Splunk instance to receive data from forwarder(s.)'. It has a field 'Listen on this port *' with a placeholder 'For example, 9997 will receive data on TCP port 9997.' and 'Save' and 'Cancel' buttons.

Installing Splunk Universal Forwarder

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

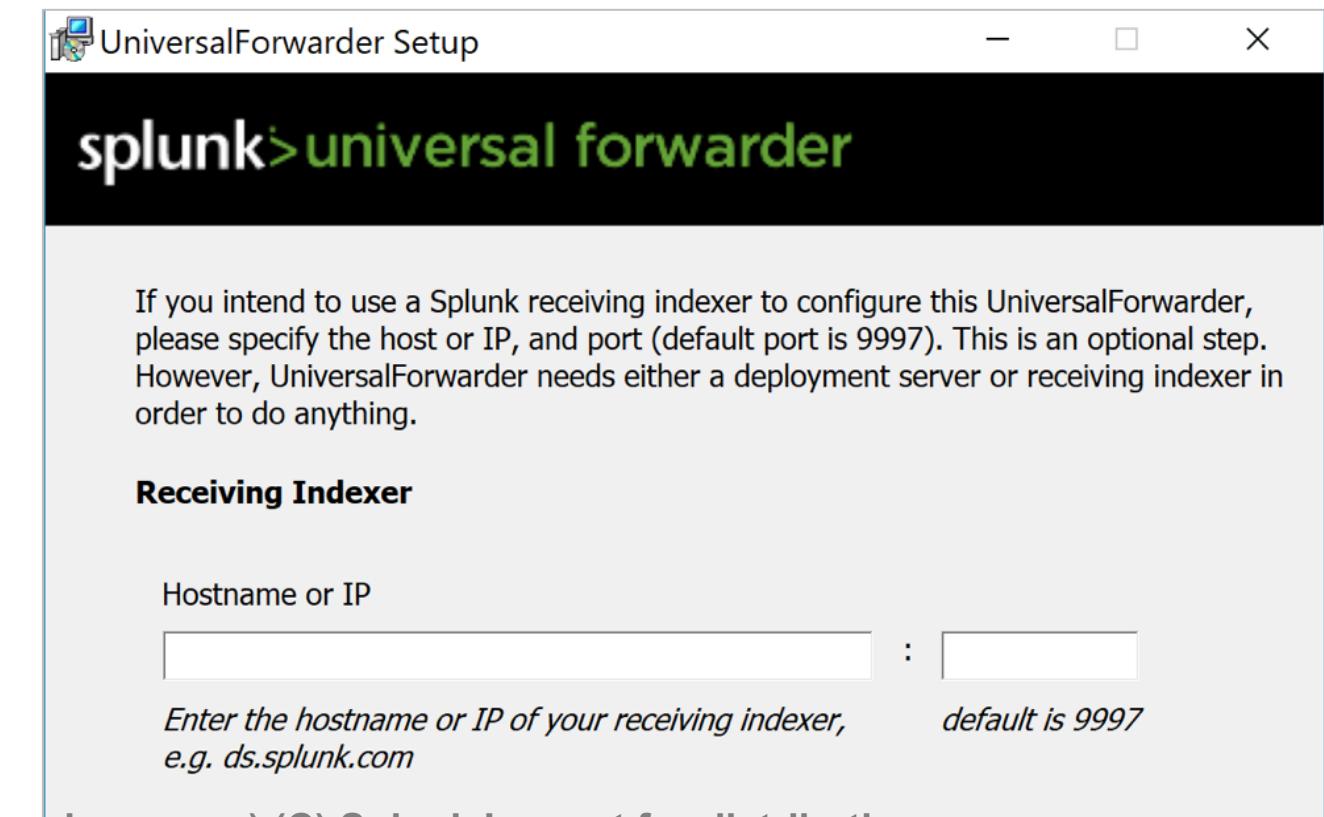
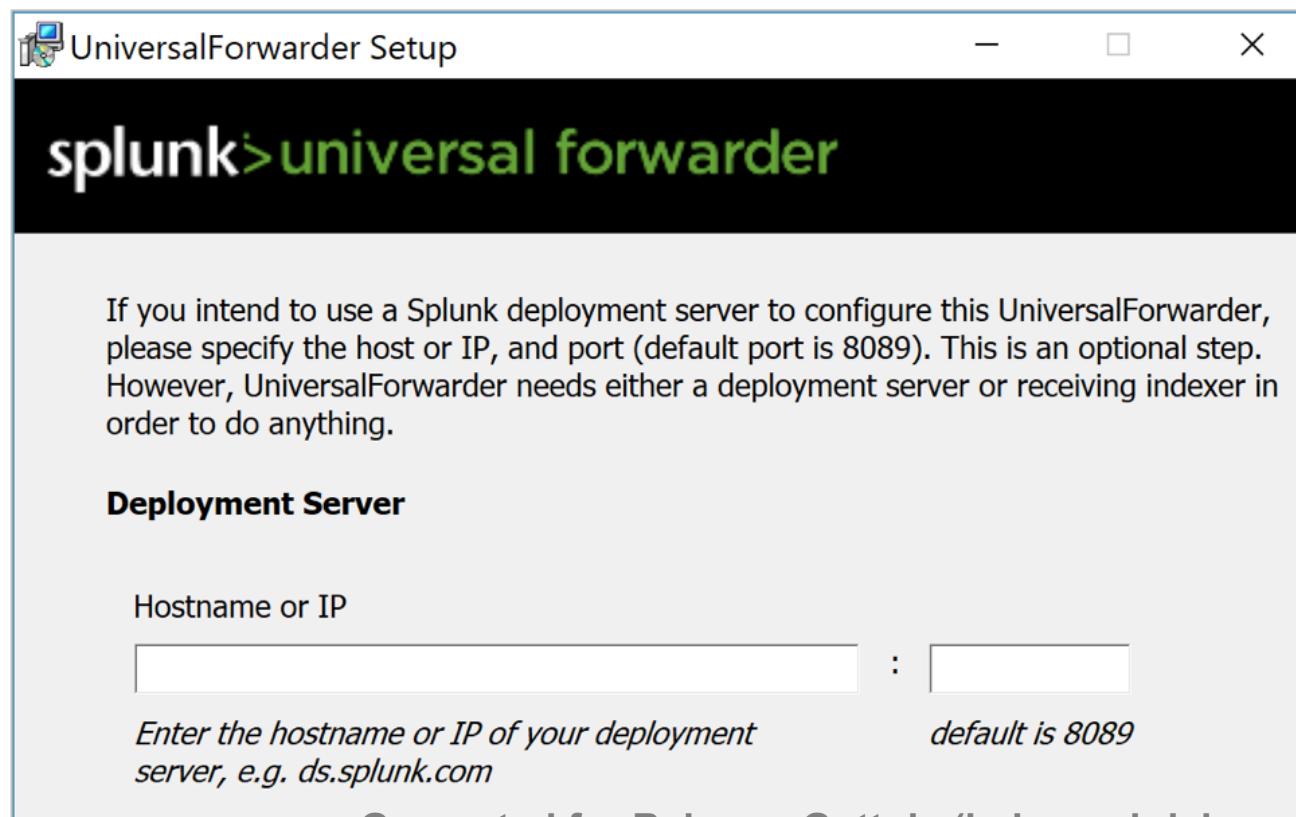
- Same **splunk** command-line interface in **SPLUNK_HOME/bin**
 - Same commands for start/stop, restart
 - Not all command options are supported
 - An admin account and password are required
- When installing large numbers of forwarders, use an automated method

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Using the Interactive Windows Installer

- Most forwarder settings can be configured using the installer wizard
 - Can run as a domain user without the domain user local administrator privileges
- CLI installation is available for scripted installations

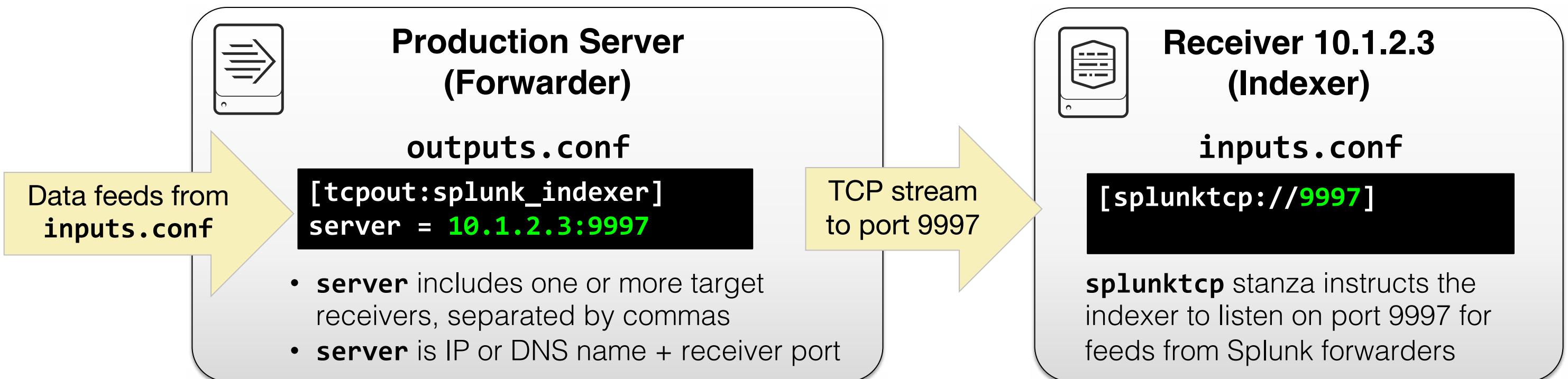
docs.splunk.com/Documentation/Forwarder/latest/Forwarder/InstallWindowsuniversalforwarderfromthecommandline



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Forwarder outputs.conf File

- Points the forwarder to the receivers
- Can specify additional options for load balancing, SSL, compression, alternate indexers, and indexer acknowledgement



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Configuration and Connection Validation

- After running **splunk add forward-server**:
 - Forwarder should be communicating with the indexer
 - Forwarder Splunk logs are automatically sent to indexer's **_internal** index
- To check the configuration:
 - On indexer, run: **splunk display listen**
 - On forwarder, run: **splunk list forward-server**
- To check for successful connection:
 - Search: **index=_internal host=<forwarder_hostname>**
- To remove the target indexer setting:
 - On 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.
- Running **splunk add forward-server <indexer:port>** creates stanzas in which **.conf** 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.

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

outputs.conf

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

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

Module 9: Distributed Search and Splunk Diag

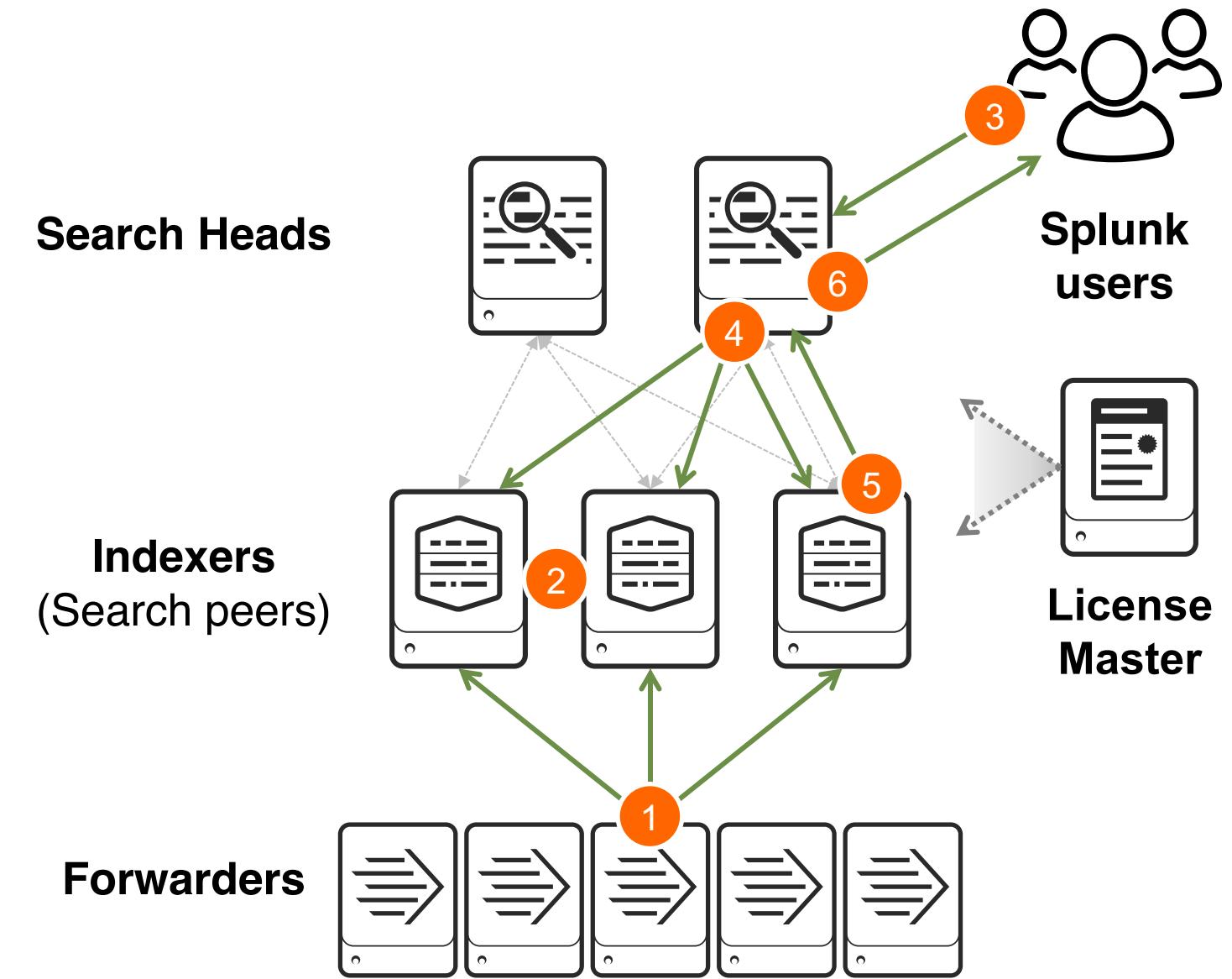
Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Module Objectives

- Describe how distributed search works
- Explain the roles of the search head and search peers
- List search head scaling options
- Describe Splunk diag
- Generate a Splunk diag

How Distributed Search Works

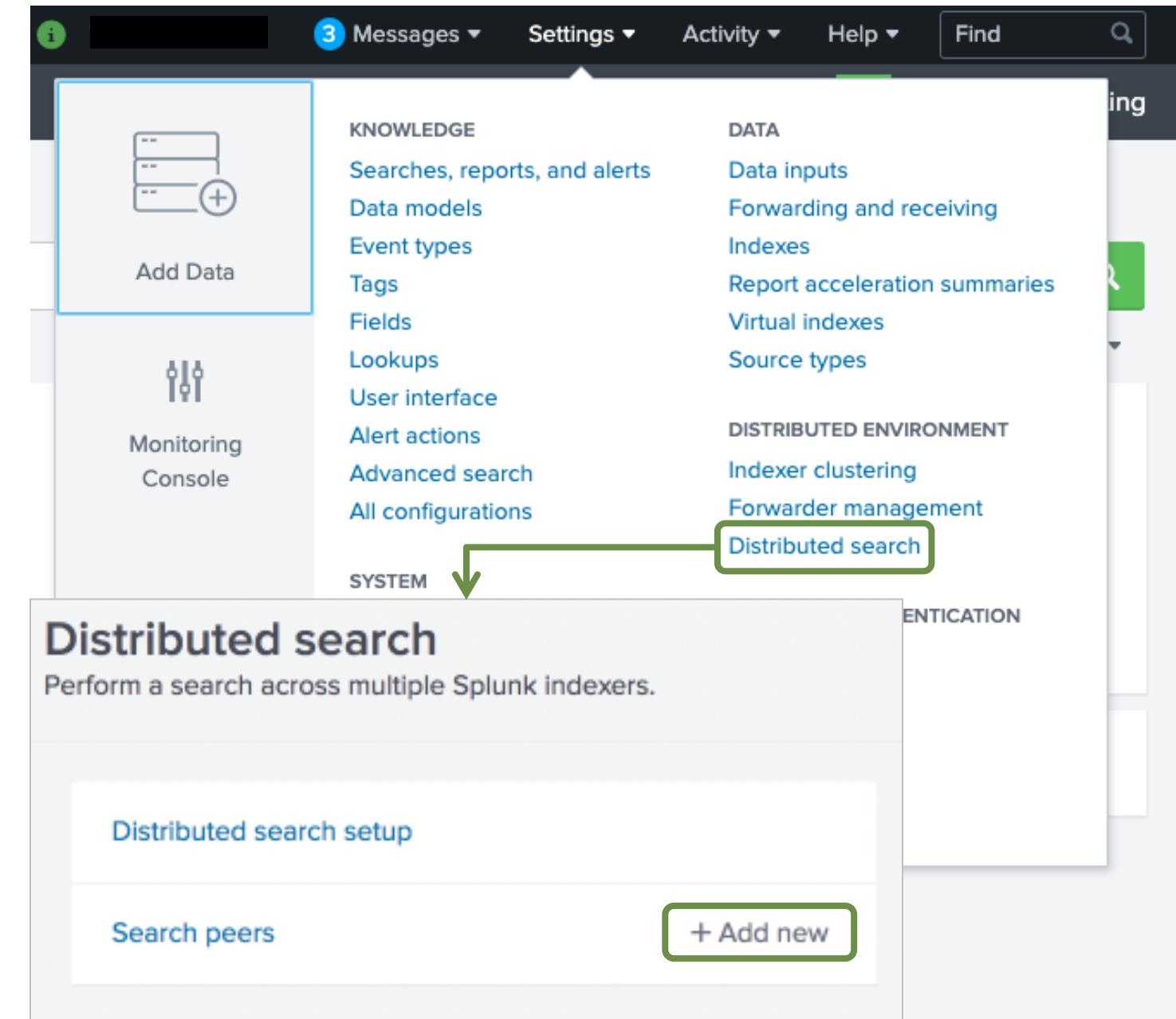
1. Universal forwarders (production servers) send data to indexers
2. Indexers (search peers) store their portion of the data
3. Users log on to the search head and run reports
4. The search head dispatches searches to the indexers
5. Indexers run searches in parallel and return their portion of results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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Setting Up Distributed Search

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Adding Indexers (Search Peers)

Add search peers

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

Peer URI *

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

Distributed search authentication

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

Remote username *

Remote password *

Confirm password

Cancel Save

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

User account with **`edit_user`** capability

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

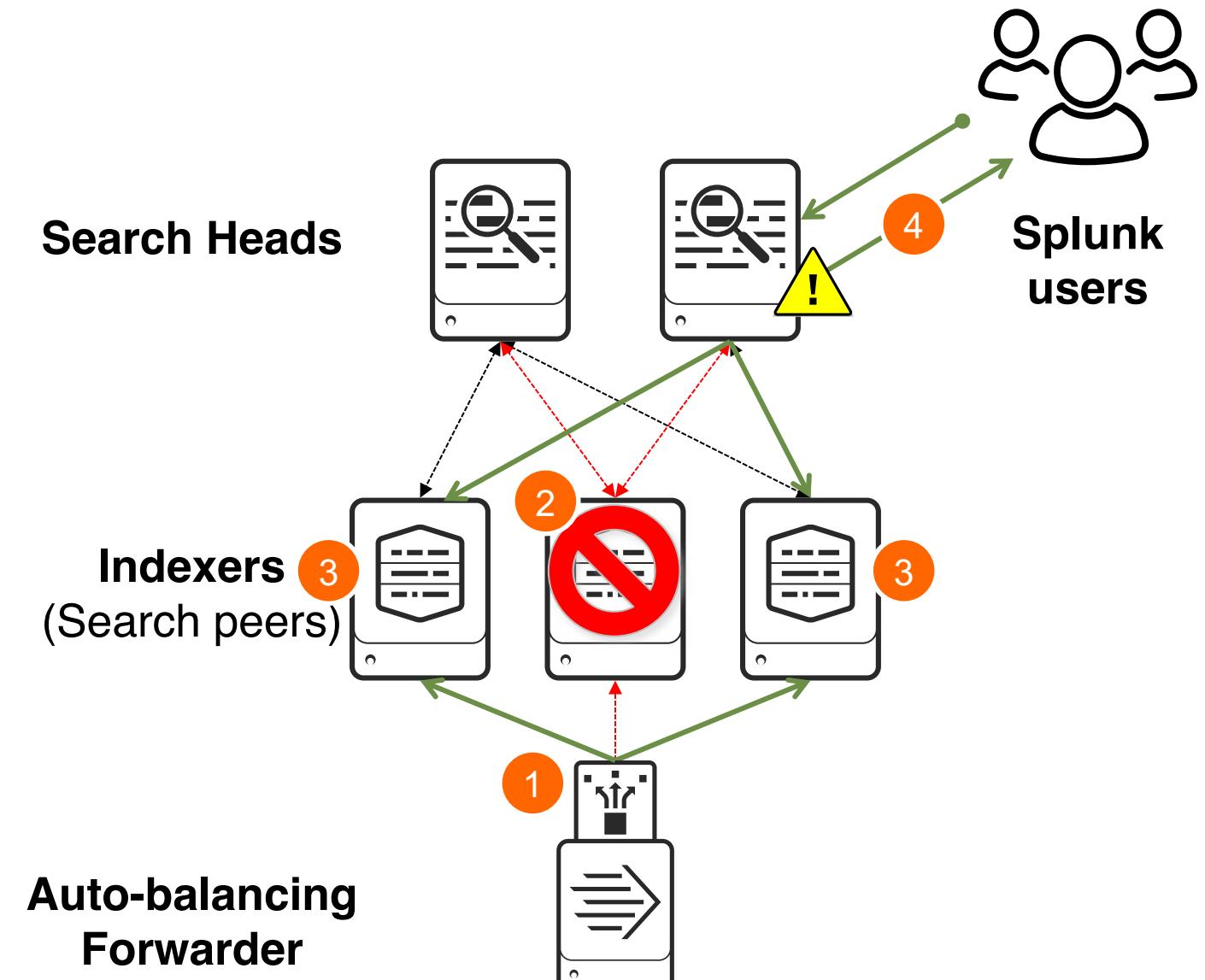
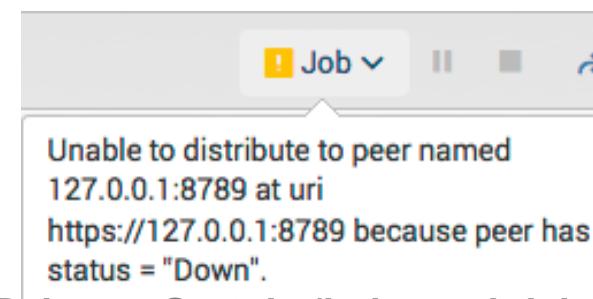
Knowledge Bundles and Replication

- Knowledge bundles
 - Distributed to indexers (search peers) by the search head when a distributed search is initiated
 - Contain the knowledge objects required by indexers for searching
 - Found in:
 - SPLUNK_HOME/var/run** on the search head
 - SPLUNK_HOME/var/run/searchpeers** on the indexer (search peer)
- Replication status of knowledge bundles
 - Splunk Web: Settings > Distributed search > Search peers under the Replication Status column

Indexer (Search Peer) Failure

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

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Viewing Search Peer Status with MC

- Found in the MC: Search > Search Activity: Instance
- Provides a graphical view of the status of indexers (search peers):
 - Median resource usage (Memory, CPU)
 - Top 10 memory-consuming searches
 - Aggregate search runtime

The screenshot shows the Splunk Enterprise interface with the following details:

- Header:** splunk>enterprise, Apps ▾, H Administrator ▾, Messages ▾.
- Navigation Bar:** Overview, Health Check, Indexing ▾, **Search ▾**, Resource Usage ▾, Forwarders ▾, Settings ▾.
- Search Activity Statistics:** A dropdown menu is open under the 'Search' bar, showing options: **Search Activity: Instance** (selected), **✓ Search Usage Statistics: Instance**, KV Store: Instance, and Scheduler Activity: Instance.
- Search Activity: Instance View:** This view is displayed below the dropdown.
 - Role:** Indexers (radio button selected).
 - Group:** All (dropdown).
 - Instance:** tgurantz-mbp-4ce64 (dropdown).
 - Hide Filters:** Link.
 - Select views:** All (selected), Snapshot, Historical.
 - Snapshots:** Search Concurrency (Running/Limit).
 - Ad hoc + Scheduled Searches (0 Running): **0/18** (Historical).
 - Scheduled Searches (0 Running): **0/9** (Historical).
 - Real-time:** **0/18**.
 - Summarization:** **0/4**.

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Search Peer Quarantine

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

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

Use Cases for Multiple Search Heads



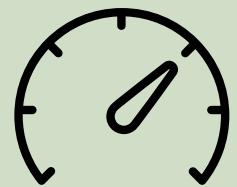
Access control

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



Manage geo-dispersed data

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



Performance enhancement

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

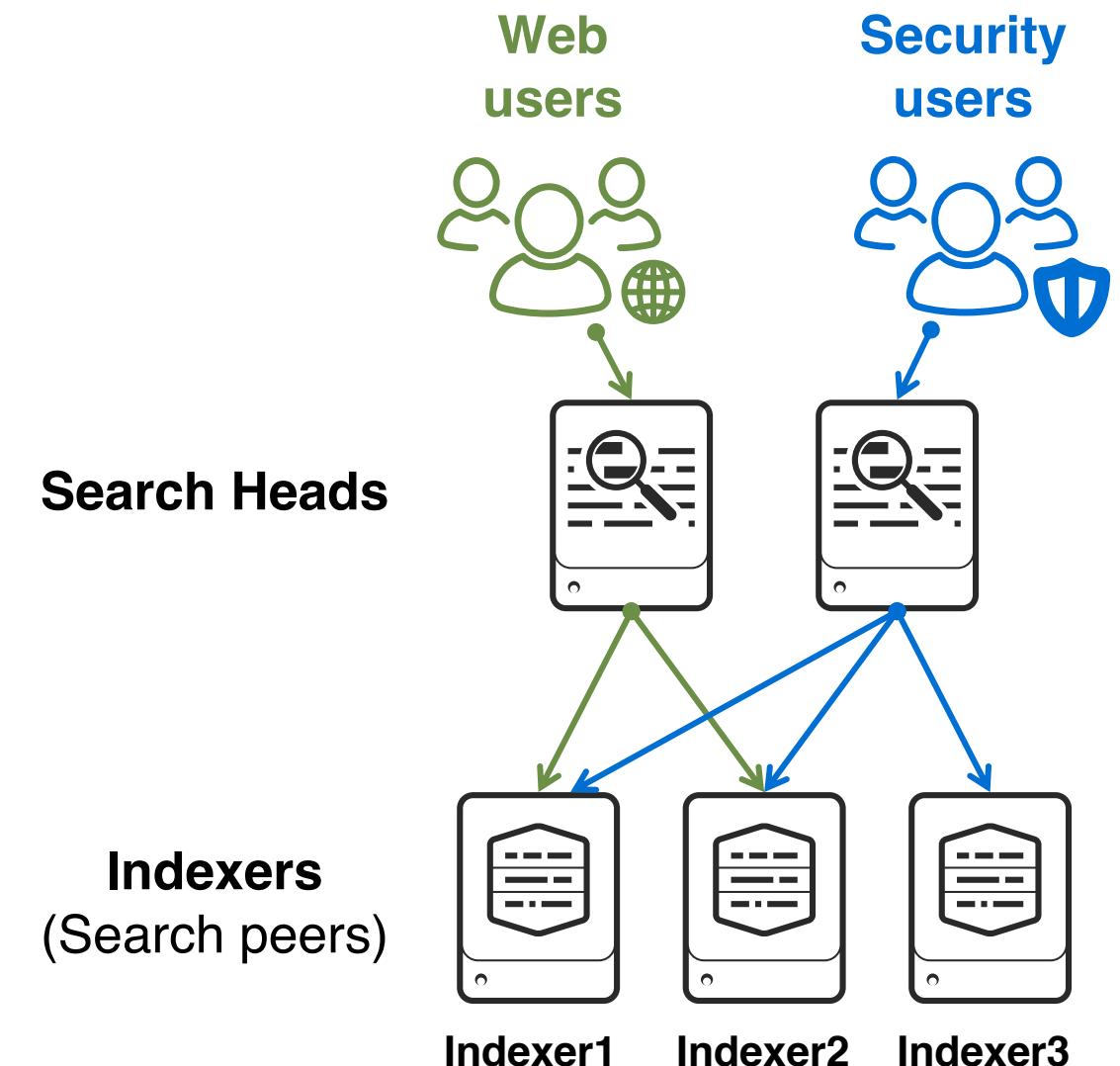
Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Determining the Number of Search Heads

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

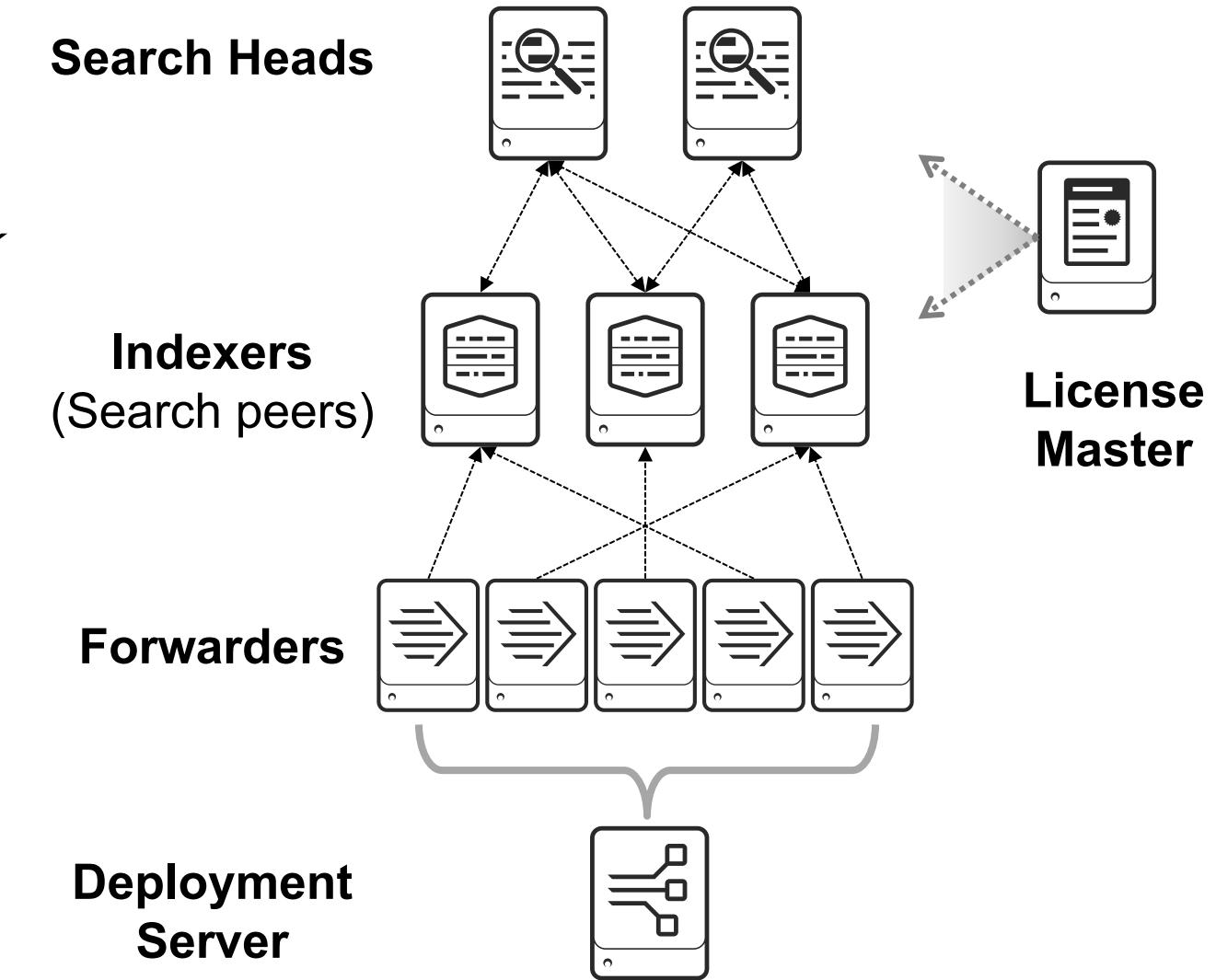
Dedicated Search Heads

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



Distributed Search Best Practices

- Dedicate a host for each role
 - Combine server roles with caveats
 - Discussed in the *Architecting Splunk Deployments* course
- Disable Splunk Web on instances that don't need it
splunk disable webserver
- Use Deployment Server
 - Discussed in the *Splunk Enterprise Data Administration* course



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Distributed Search Best Practices (cont.)

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

Forwarding and receiving

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

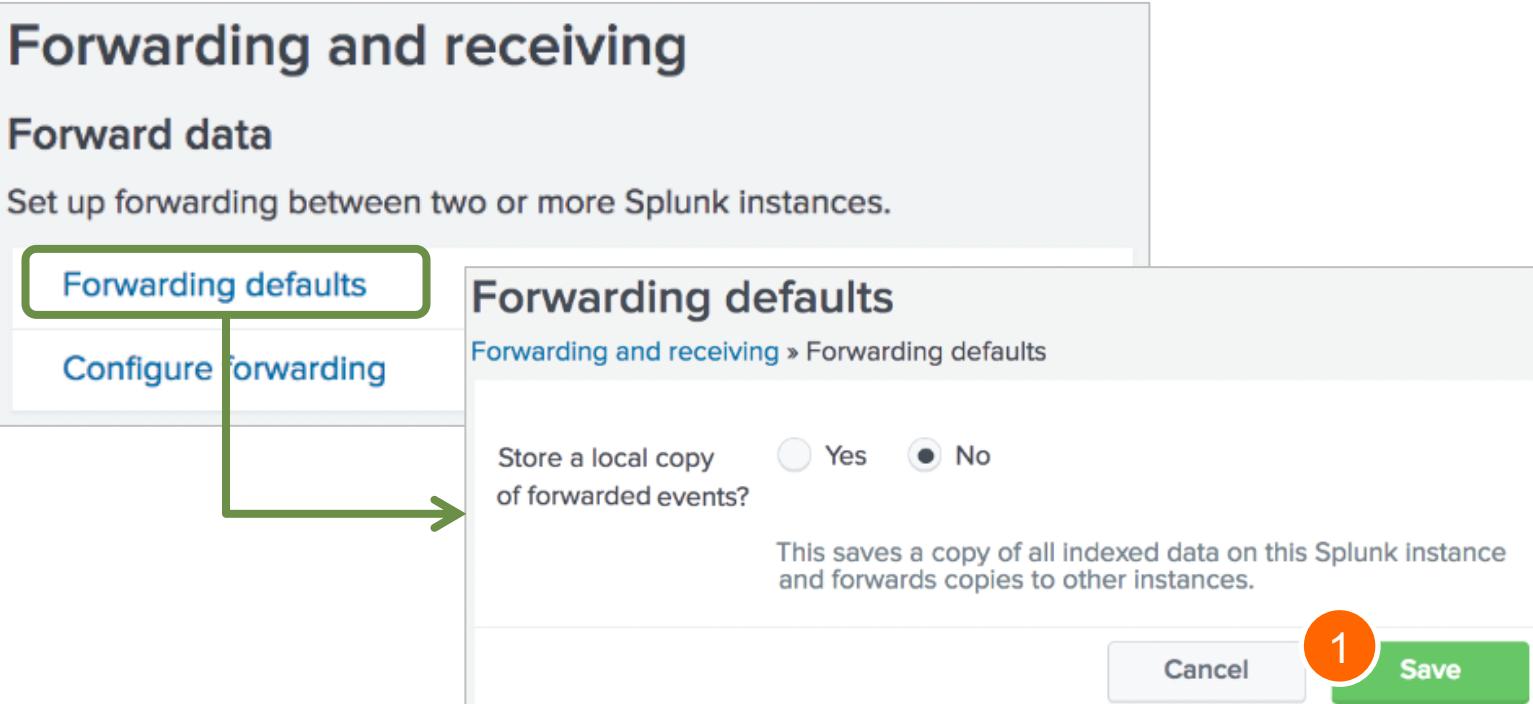
Forwarding defaults

Forwarding and receiving » Forwarding defaults

Store a local copy of forwarded events? Yes No

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

Cancel **1 Save**



outputs.conf

```
[indexAndForward]
index = false

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

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

2 →

What is a Splunk Diag?

- Gathers data and provides insight to your instance

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

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Using the Splunk Diag UI

From Splunk Web, select **Settings > Instrumentation**

Instrumentation

Configure automated reporting settings, view collected data, export data to file, work with diagnostic files, and send data to Splunk. [Learn More](#)

Usage Data

View license usage, anonymized usage, and support usage data that has been collected (does not include browser session data). [Learn More](#)

Date Range: Report 2018-03-06 to 2018-03-07 | Actions: View in Search: License Data | Time Sent: 2018-03-08

Diagnostic Log

Diagnostic files contain information about your Splunk deployment, such as configuration files and logs, to help Splunk Support diagnose and resolve problems. [Learn More](#)

Export

New Diag

New Diagnostics Bundle

Select instance you want to collect data from. [?](#)

All Roles Filter

2 instances

	Name	Roles
<input checked="" type="checkbox"/>	127.0.0.1	search head
<input type="checkbox"/>	bcdgc	license master, search peer

1 selected: 127.0.0.1

Next

Use the dropdown menu or the filter option to list the server roles

Configure the diag bundle settings by selecting the server instances and click **Next**

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Using Splunk Diag UI (cont.)

New Diagnostics Bundle X

Configure bundle settings to be applied to all instances. [Learn more ↗](#)

Include components	<code>index_files, index_listing, dispatch, etc, log, pool, searchpeers, consensus, conf_replication_summary, kvstore, file_validate</code>	Edit
Exclude patterns	<code>None</code>	Edit
Index files	<code>Manifests</code>	▼
Index directory listing level	<code>Light</code>	▼
Exclude etc files larger than	<code>10 MB</code>	▼
Get every crash .dmp file	<code>No</code>	▼

[Revert to default](#) [Cancel](#) [Back](#) [Create](#)

5

Configure the diag bundle settings for each instance by including and/or excluding components and click **Create**

Diag Example

```
[student1@ip-10-0-0-202 bin]$ ./splunk diag
Collecting components: conf_replication_summary, consensus, dispatch, etc,
file_validate, index_files, index_listing, kvstore, log, searchpeers,
suppression_listing
Skipping components: rest
Selected diag name of: diag-ip-10-0-0-202-2019-10-03_21-43-31
Starting splunk diag...
Logged search filtering is enabled.
Skipping REST endpoint gathering...
Determining diag-launching user...
Getting version info...
Getting system version info...
```

Diag reports the components it will collect and components it will skip

```
The following certificates were excluded from the diag output automatically.
/opt/splunk/etc/auth/appsCA.pem
/opt/splunk/etc/auth/cacert.pem
/opt/splunk/etc/auth/appsLicenseCA.pem
/opt/splunk/etc/auth/cloudCA.pem
/opt/splunk/etc/auth/server.pem
```

Diag also reports certificates that were not auto-detected or skipped

```
Copying bucket info files...
Copying Splunk dispatch files...
Copying Splunk consensus files...
Adding manifest files...
Adding cachemanager_upload.json...
Cleaning up...
Splunk diagnosis file created: /opt/splunk/diag-ip-10-0-0-202-2019-10-03_21-43-31.tar.gz
```

When the diag is complete, the output is saved and the file and location are displayed

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Module 9 Knowledge Check

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

Module 9 Knowledge Check – Answers

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

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

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

True.

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

True.

Lab Exercise 9 – Distributed Search / Diag

Time: 15 minutes

Tasks:

- Add a search peer to your search head
- Search for indexes and source types on the search peer
- Create and index a basic diag file

Course Wrap-up

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

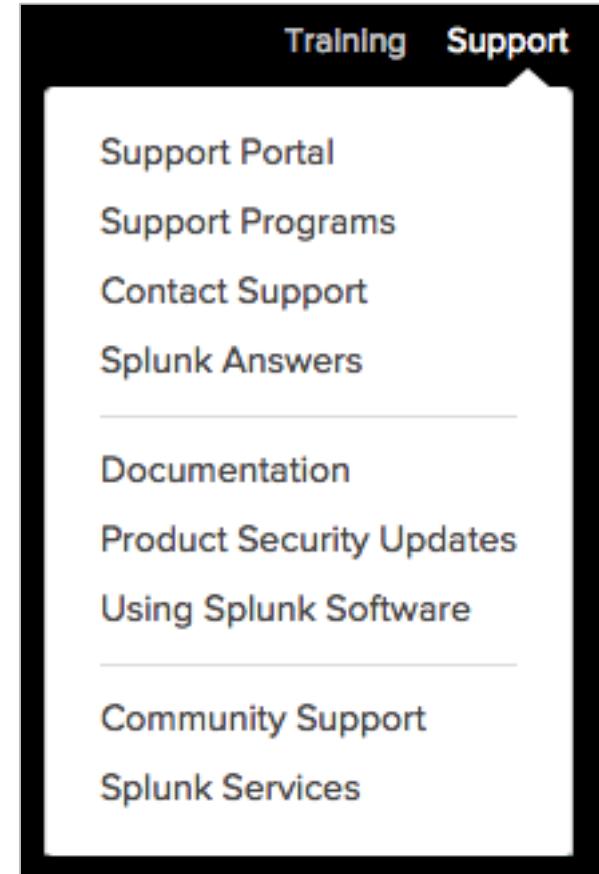
Community

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Support Programs

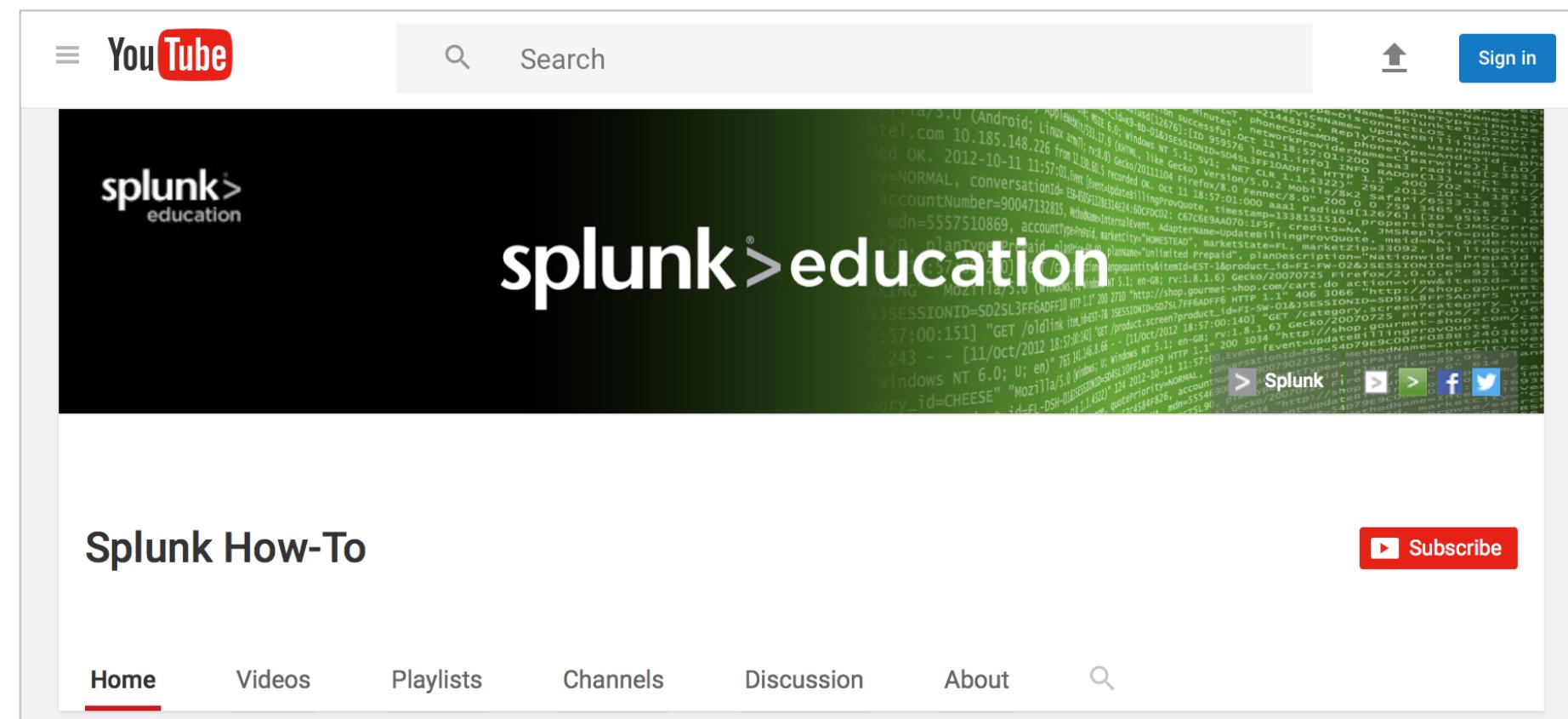
- Web
 - Documentation: docs.splunk.com and dev.splunk.com
 - Wiki: wiki.splunk.com
- Global Support
 - Support for critical issues, a dedicated resource to manage your account – 24 x 7 x 365
 - Web: splunk.com/index.php/submit_issue
 - Phone: (855) SPLUNK-S or (855) 775-8657
- Enterprise Support
 -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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

YouTube: The Splunk How-To Channel

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Splunk Certification

- Splunk Certification program

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



October 20-21, 2020

Join us for two days of innovation featuring dozens of educational sessions and numerous opportunities to do amazing things with data.

“ Splunk makes our imagination the only limit to unlocking and understanding our data. ”

- IT Specialist, US Public Sector

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Learn more at
conf.splunk.com



Thank You



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Appendix A: Splunk Authentication Management

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Module Objectives

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

Splunk Authentication Options

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

Authentication Methods

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

Internal Splunk Authentication (always on)

External None
 LDAP
 SAML

Multifactor Authentication

Not available with external authentication such as SAML.

None
 Duo Security
 RSA Security

Reload authentication configuration

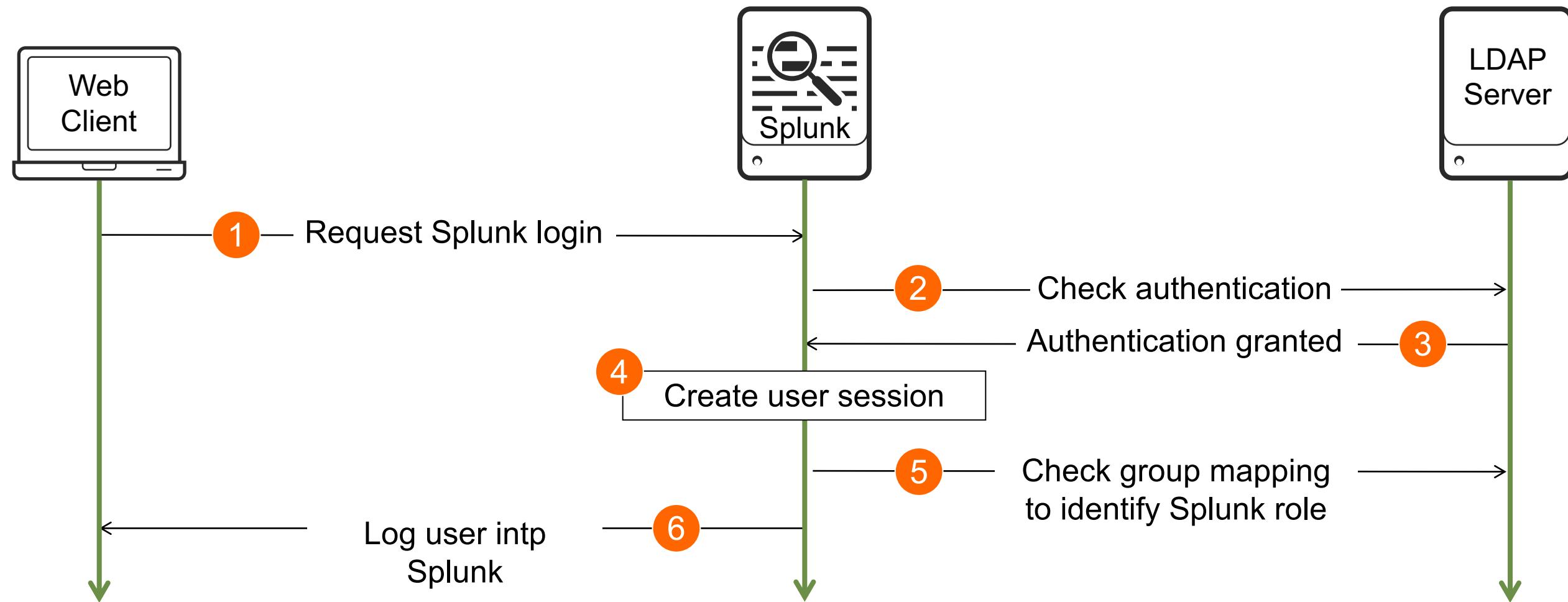
Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Directory Server Integration

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

LDAP Authentication

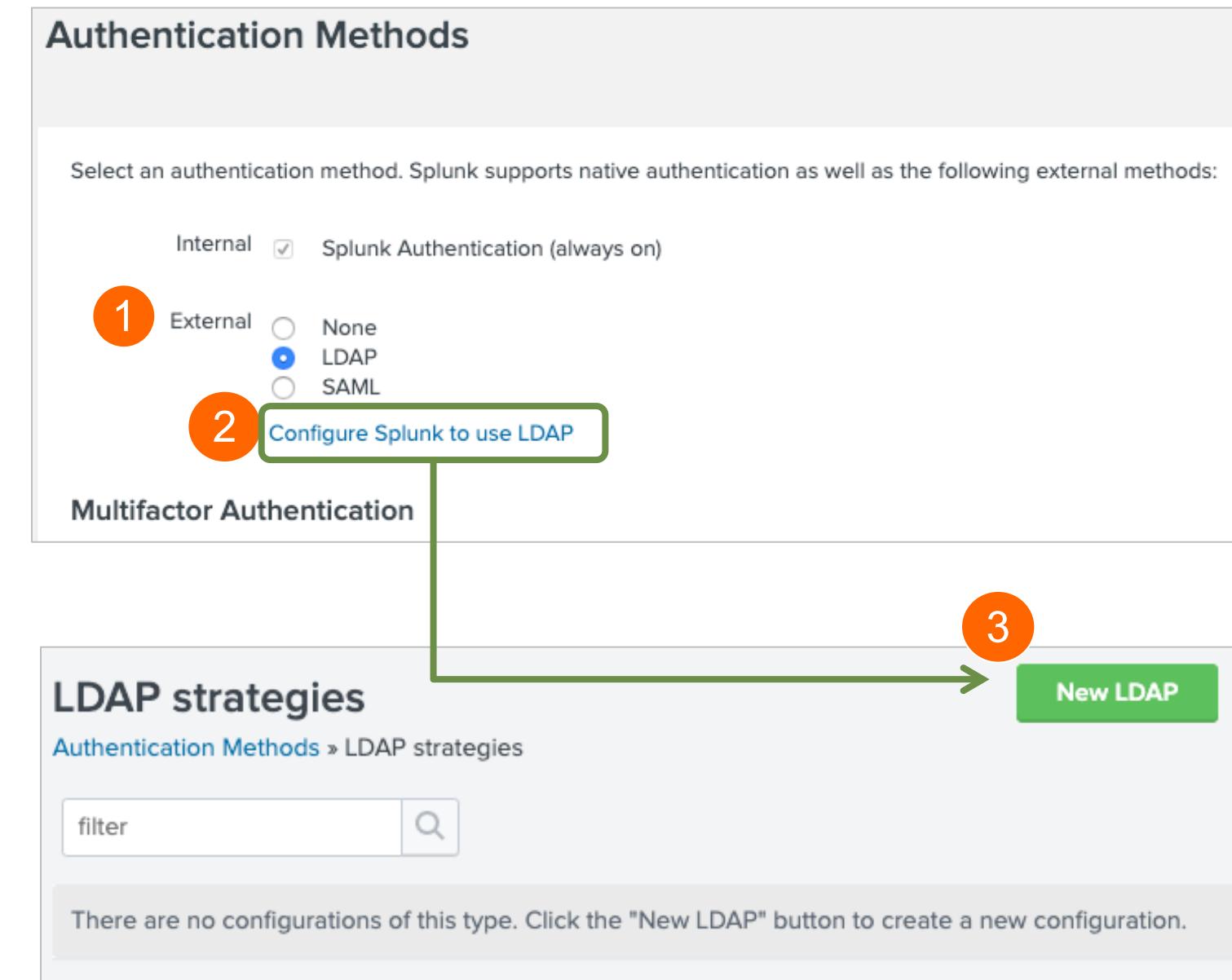
LDAP maintains the user credentials - user ID and password, plus other information - centrally and handles all authentication



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Creating an LDAP Strategy

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

LDAP Strategy Settings

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

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

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

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

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

Mapping LDAP Groups to Roles

LDAP strategies

Authentication Methods » 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	Map groups Clone Delete

| « 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	

New LDAP

Map groups

Select to define relationships between LDAP groups and Splunk roles

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Mapping LDAP Groups to Roles (cont.)

splunkAdmins
Authentication Methods » LDAP strategies » LDAP Groups » splunkAdmins

Available Roles

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

Selected Roles

- admin

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

LDAP Users

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

LDAP Groups
Authentication Methods » LDAP strategies » LDAP Groups

Showing 1-4 of 4 items

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

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

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Managing Users in Splunk

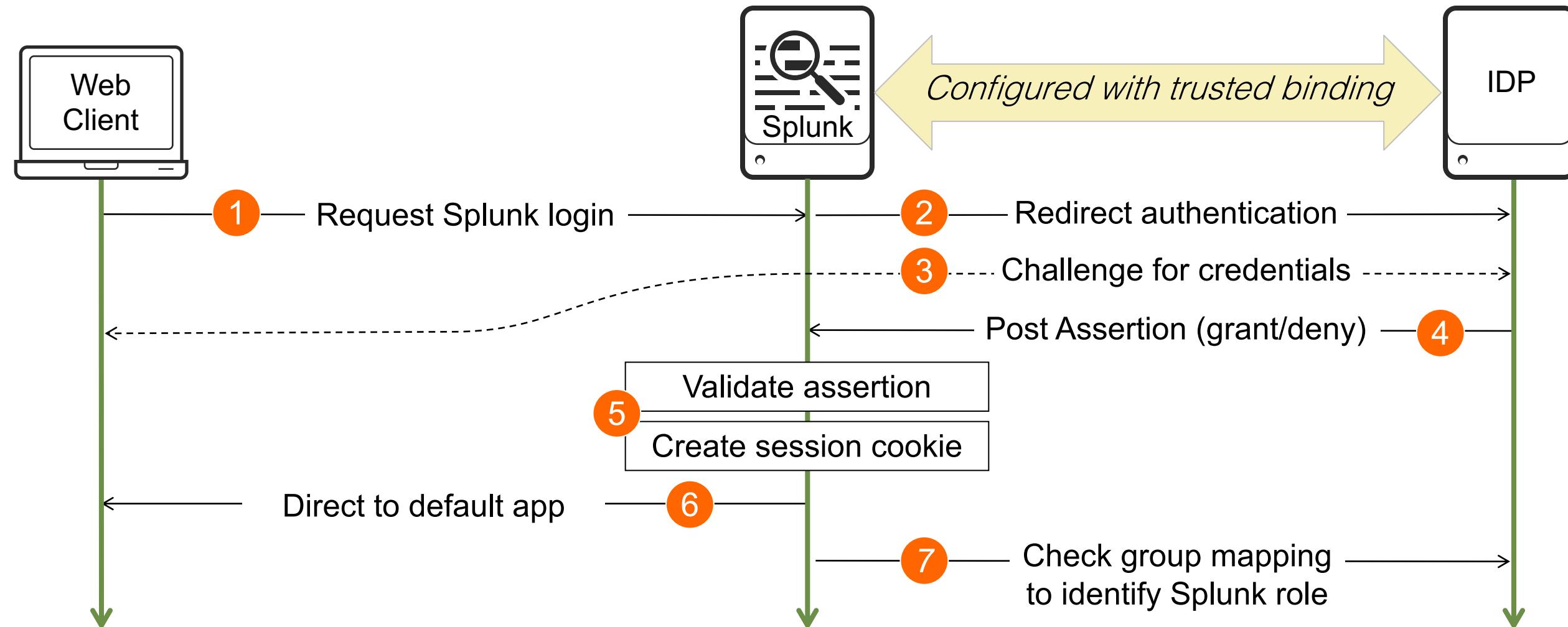
- Splunk native users can be edited or deleted
- Only time zone and default app can be changed on LDAP or other users

Users										
Add new Splunk user → New User										
13 Users filter 10 per page ▾										
Name ▲	Actions	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Status	?
acurry		LDAP	Amanda		launcher	system		soc_analyst	✓ Active	
admin	View Capabilities Edit Clone	Splunk	Administrator	changeme@example.com	launcher	system		admin	✓ Active	
blu	View Capabilities Edit Clone	Splunk	Bao Lu		launcher	system		user	✓ Active	
coryf		LDAP	Cory Flintoff		launcher	system		admin	✓ Active	
dhale		LDAP	Dwight Hale		launcher	system		user	✓ Active	
emaxwell	View Capabilities Edit Clone Delete	Splunk			launcher	system		power	✓ Active	
gvoronoff		LDAP	Gabriel Voronoff		launcher	system		admin	✓ Active	
instructor	View Capabilities Edit Clone Delete	Splunk			launcher	system		admin	✓ Active	

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

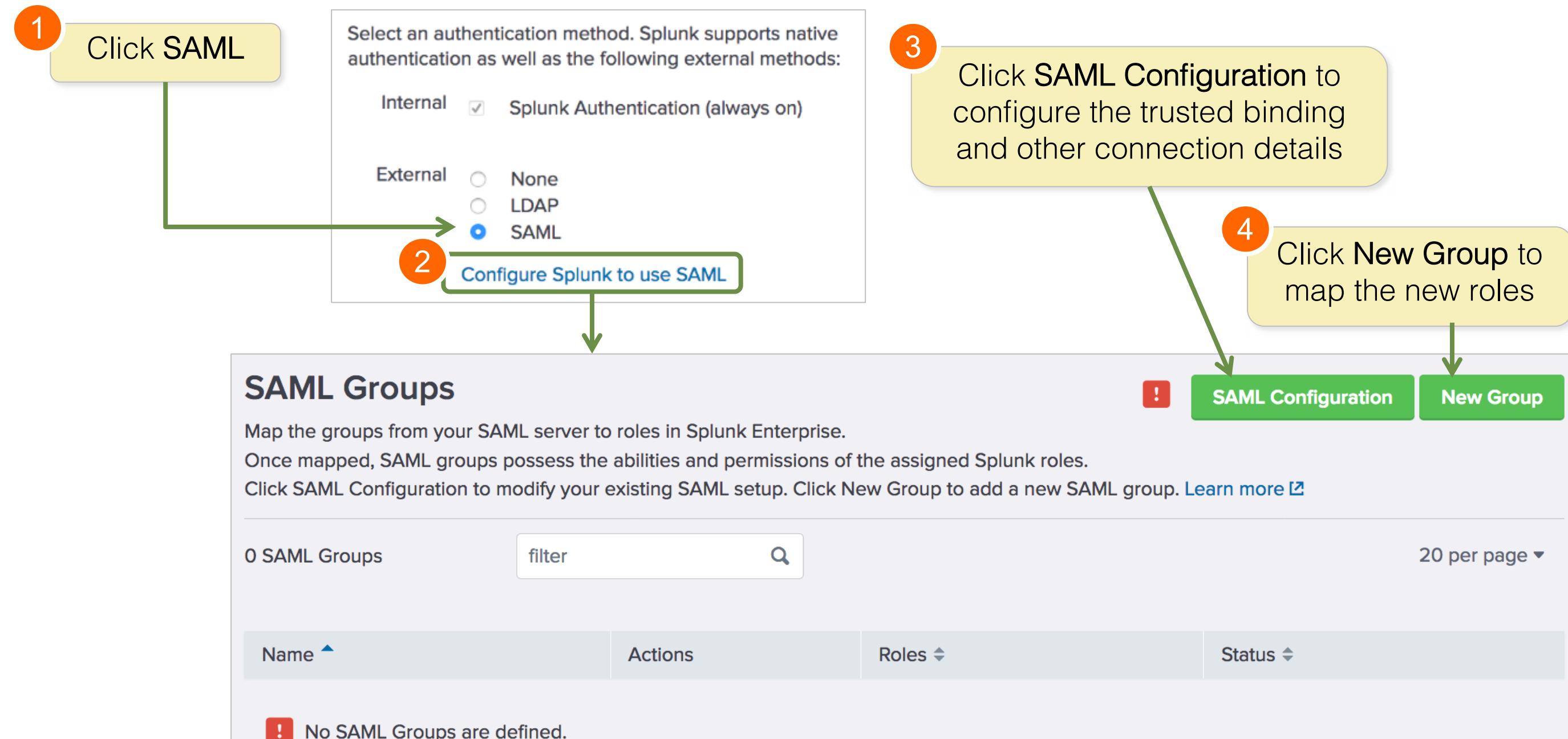
SAML 2.0 Single Sign On

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Configuring SAML



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.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.

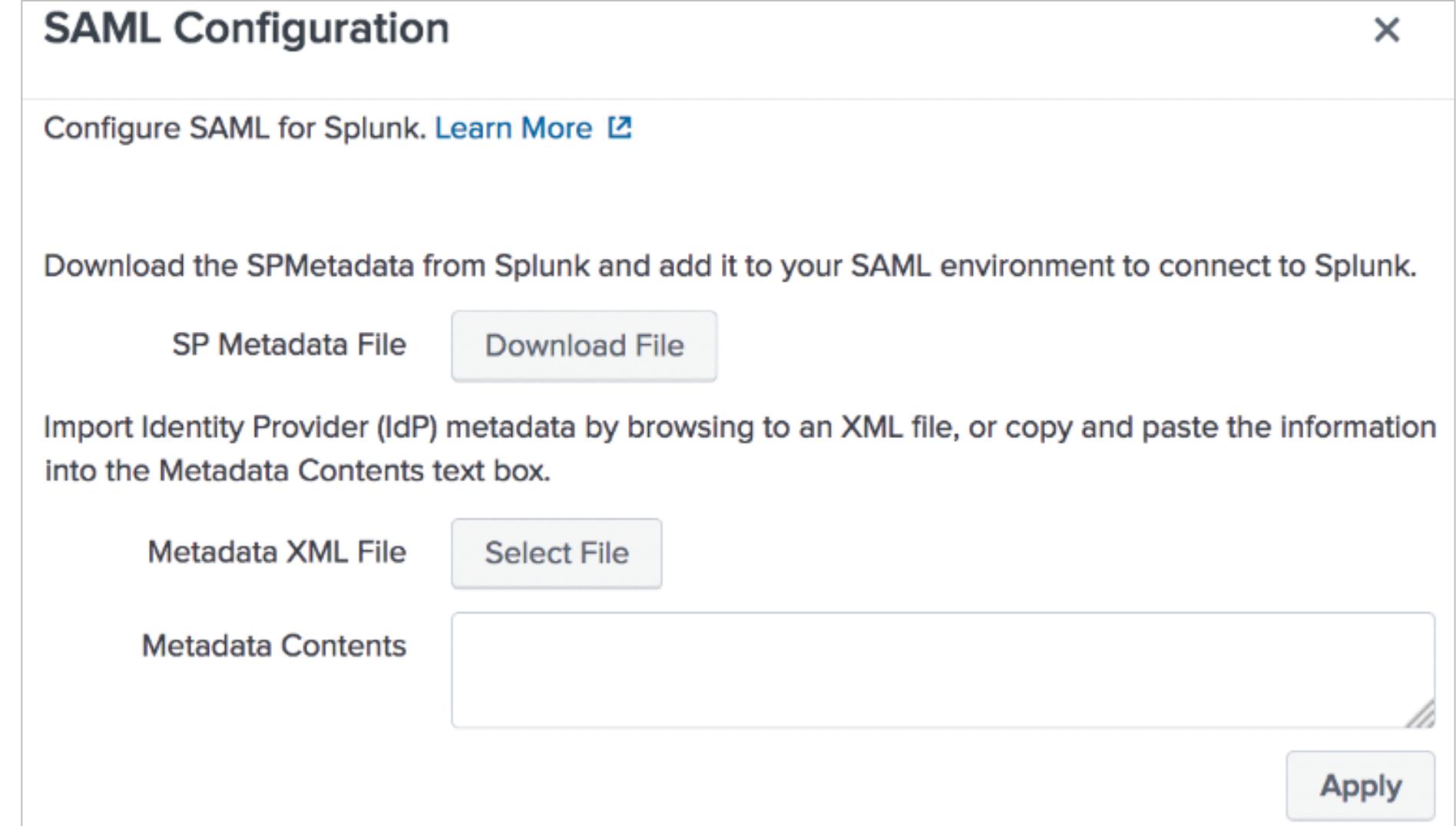
SP Metadata File [Download File](#)

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 Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Configuring SAML – General Settings

- Gather SAML configuration information

Protected endpoints on the IdP which Splunk sends authentication requests to

General Settings

Single Sign On (SSO) URL ?

Single Log Out (SLO) URL ? optional

IdP certificate path ? optional
Leave blank if you store IdP certificates under \$SPLUNK_HOME/etc/auth/idpCerts

IdP certificate chains ?

Replicate Certificates ?

Issuer Id ?

Entity ID ?

Sign AuthnRequest

Verify SAML response ?

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Configuring SAML – Query and Alias Settings

Endpoint on the IdP to which queries over SOAP are sent

▼ Attribute Query Requests

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 Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Configuring SAML – Advanced Settings

Leave this empty or pick the correct format configured on the IdP from the dropdown list

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

Advanced Settings

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

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Creating SAML Groups

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

Create New SAML Group X

Group Name

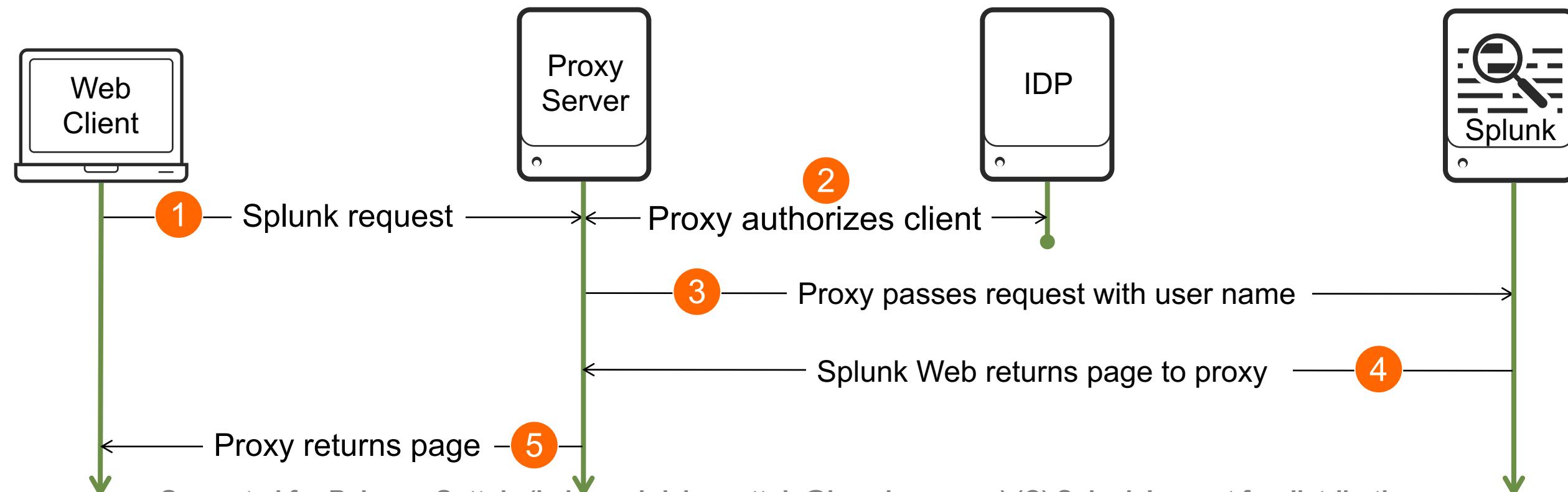
Splunk Roles Available item(s) Selected item(s) « remove all

Splunk Roles	Available item(s)	Selected item(s)
	admin can_delete power securityops <small>splunk-system-role</small>	admin can_delete power securityops

Cancel Save

Single Sign On with Reverse Proxy

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



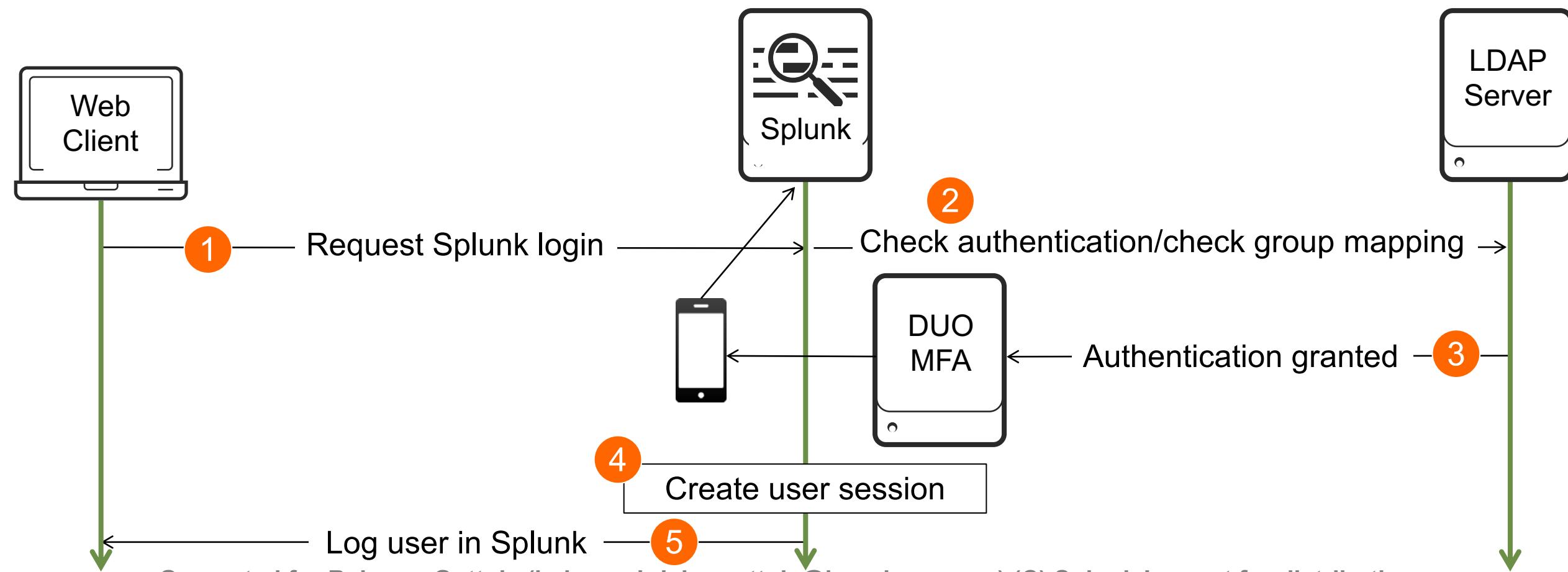
Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Scripted Authentication

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

Duo Multi Factor Authentication

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Configuring Duo MFA

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

The screenshot shows the 'Authentication Methods' section of the Splunk web interface. It includes a note about supporting native authentication and external methods like LDAP and SAML. Under 'External', 'LDAP' is selected. A link to 'LDAP Settings' is present. Below this is the 'Multifactor Authentication' section, which notes it's not available with external authentication like SAML. It shows 'Duo Security' selected from a dropdown menu, with 'Configure Duo Security' highlighted with a green border. A button at the bottom allows reloading the configuration.

Authentication Methods

Select an authentication method. Splunk supports native authentication as well as external authentication methods such as LDAP and SAML.

Internal Splunk Authentication (always on)

External None LDAP SAML

[LDAP Settings](#)

Multifactor Authentication

Not available with external authentication such as SAML.

1 → Duo Security
None
RSA Security

2 [Configure Duo Security](#)

[Reload authentication configuration](#)

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Configuring Duo MFA (cont.)

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

Add new
Authentication Methods » Add new

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

Integration Key *

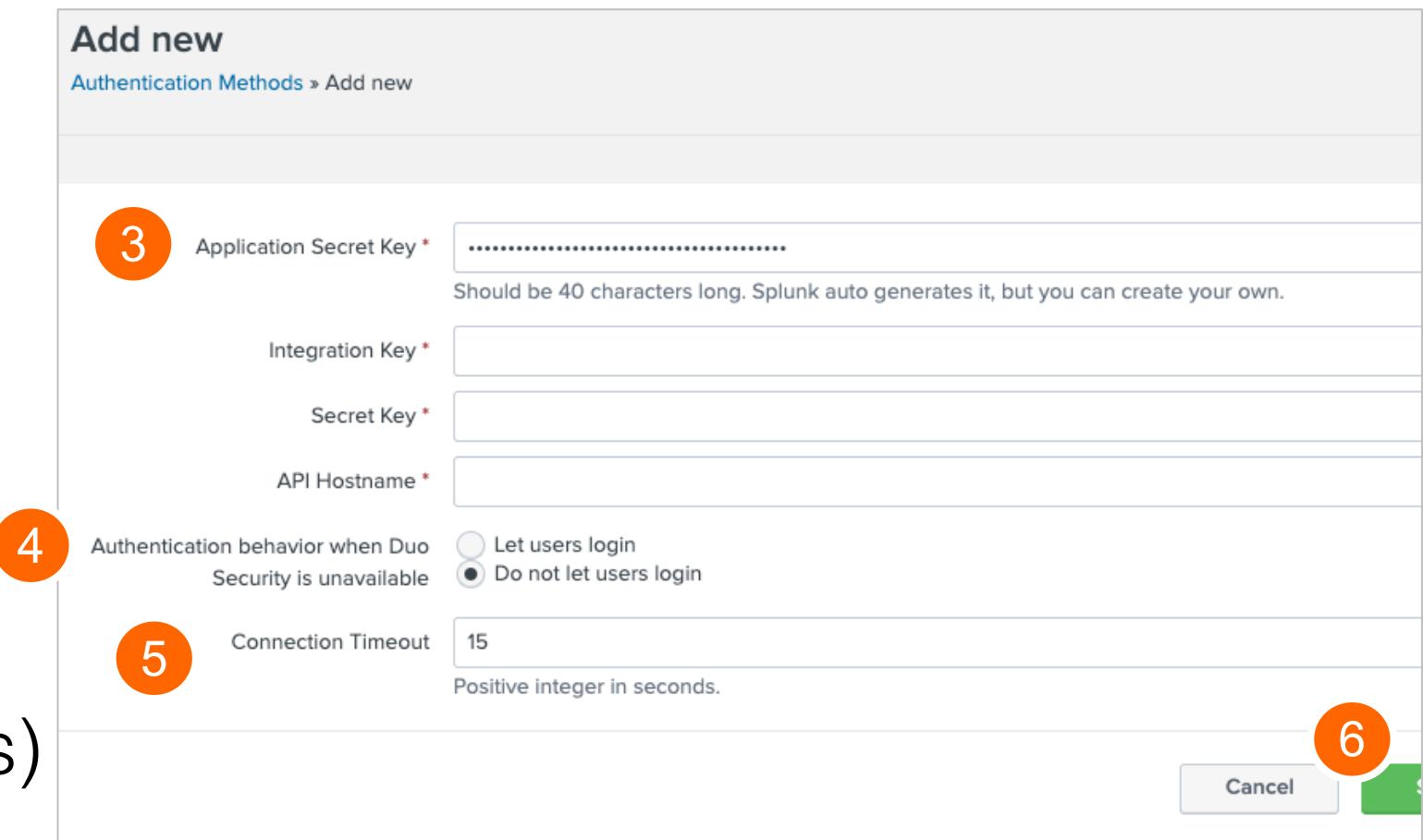
Secret Key *

API Hostname *

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

5 Connection Timeout
15 Positive integer in seconds.

6 Cancel 



Appendix B: Adding Data

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Adding an Input with Splunk Web

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

The screenshot shows the Splunk Web interface. At the top, there is a navigation bar with links for Administrator, Messages, Settings (highlighted with a red circle containing the number 1), Activity, Help, and Find. Below the navigation bar is a sidebar titled "DATA" (also highlighted with a red circle containing the number 2). The sidebar contains links for Data inputs, Forwarding and receiving, Indexes, Report acceleration summaries, Virtual indexes, and Source types. The main content area is titled "Data inputs" and contains instructions for setting up data inputs from files and directories, network ports, and scripted inputs. It also mentions forwarding and receiving between two Splunk instances. Below this, there is a table titled "Local inputs" with columns for Type, Inputs, and Actions. The table has two rows: "Files & Directories" (with 10 inputs) and "HTTP Event Collector" (with 0 inputs). A green box highlights the "+ Add new" button in the Actions column for the "Files & Directories" row (highlighted with a red circle containing the number 3).

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Select Source

Add Data

Select Source Set Source Type Input Settings Review Done

Next >

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

1

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

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

TCP / UDP
Configure the Splunk platform to listen on a network port.

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

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. Then, Splunk monitors all objects within the directory. Then, it indexes data sources in the directory. To a...
Specify the source with absolute path to a file or directory, or use the **Browse** button
2

File or Directory ? /opt/log/www1/access.log
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
3

Whitelist ?
Blacklist ?
For ongoing monitoring
For one-time indexing, or testing; Does not create a stanza in **inputs.conf**

Generated for Balaram Guttula (balaram.krishn.guttula@pmchase.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 ⁴ 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 fix them. You can always create a new one by clicking "Save As".

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

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

View Event Summary

Source type: access_combined_wcookie Save As List ▾ Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

Event Breaker ▾ 5 Data Preview displays how your processed events will be indexed.

	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
2	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 Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Input Settings

Add Data Select Source Set Source Type Input Settings Review Done [Back](#) [Review >](#)

Input Settings

Optional input parameters for this data input:

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: Constant value
 Regular expression on path
 Segment in path
splunk01

Index: [itops](#) [Create a new index](#)

- App Context determines where input configuration is saved
- For Search & Reporting (search): **SPLUNK_HOME/etc/apps/search/local**

- By default, the default host name in General settings is used
- More options are covered in the *Splunk Enterprise Data Administration* class

- Select index where input will be stored
- Alternatively, create a new index

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.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 'Review' is highlighted in green, and buttons for '< Back' and 'Submit >' on the right. The main content area is titled 'Review' and displays the following configuration details:

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 Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

What Happens Next?

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

The screenshot shows the 'Add Data' wizard in Splunk. The progress bar at the top indicates the following steps: 'Select Source' (green dot), 'Set Source Type' (green dot), 'Input Settings' (green dot), 'Review' (green dot with a checkmark), and 'Done' (gray dot). Below the progress bar, a success message says 'File input has been created successfully.' It also provides a link to 'Configure your inputs by going to Settings > Data Inputs'. There are several buttons and links: 'Start Searching' (green button), 'Search your data now or see examples and tutorials.', 'Extract Fields' (button), 'Create search-time field extractions. Learn more about fields.', 'Add More Data' (button), 'Add more data inputs now or see examples and tutorials.', 'Download Apps' (button), 'Apps help you do more with your data. Learn more.', and 'Build Dashboards' (button), 'Visualize your searches. Learn more.'

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

Note



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

Verify your Input

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

The screenshot shows a Splunk search interface with the following elements:

- Search Bar:** Shows the search query: `source="/opt/log/www1/access.log" host="splunk01" index="test" sourcetype="access_combined_wcookie"`. A circled '1' is next to it.
- Timeline:** A horizontal timeline at the bottom of the search results page, spanning from approximately 2/27/18 2:48:45.000 PM to 2/27/18 2:48:45.000 PM. It has a green bar indicating the event range.
- Event List:** The main area displays a list of events. Each event row includes:
 - A timestamp: `2/27/18 2:15:36.000 PM`.
 - An event ID: `i`.
 - A detailed log entry: `27.96.128.0 - [27/Feb/2018:20:15:36] "GET /cart.do?action=addtocart&itemId=EST-16&productId=FS-SG-G03&JSESSIONID=SD10SL2FF4ADFF4963 HTTP 1.1" 200 3651 "http://www.buttercupgames.com/category.screen?categoryId=STRATEGY" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 744`.
 - Auto-extracted field values highlighted in yellow: `host = splunk01 source = /opt/log/www1/access.log sourcetype = access_combined_wcookie`.A circled '2' is next to the timestamp of the first event.
- Selected Fields:** A sidebar on the left lists selected fields: `a host 1`, `a source 1`, and `a sourcetype 1`. A circled '3' is next to the first field.
- Interesting Fields:** A sidebar on the left lists interesting fields: `a action 5`, `# bytes 100+`, `a categoryId 8`, `a clientip 17`, `# date_hour 5`, `# date_mday 1`, `# date_minute 32`, and `a date_month 1`. A circled '4' is next to the first field.

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Appendix C: Introduction to Splunk Clustering

Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Splunk Clustering

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

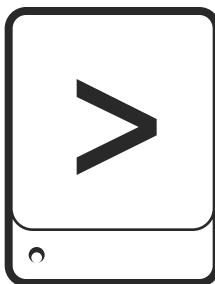
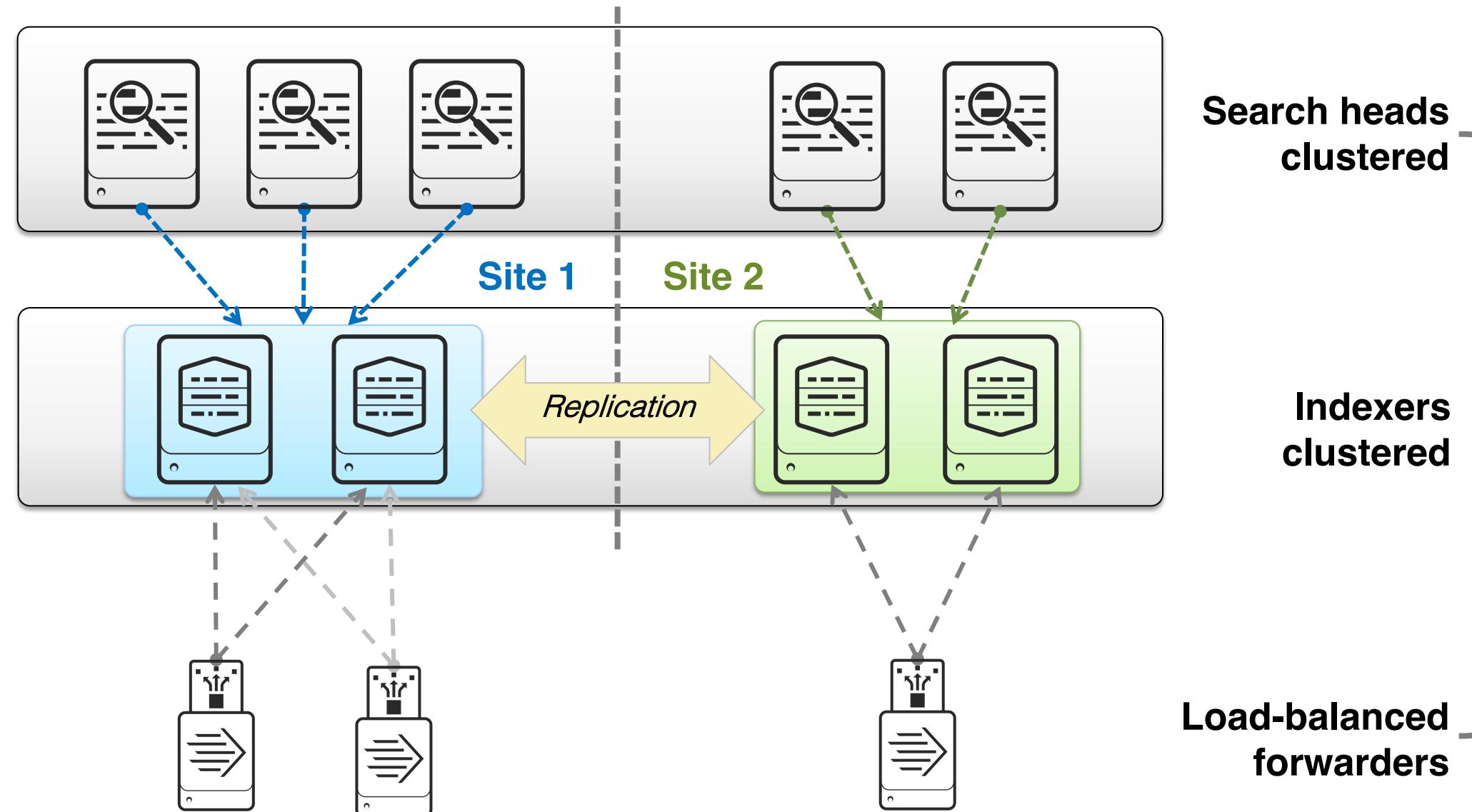
Search head
clustering

- Replicates knowledge objects across search heads

Indexer
clustering

- Replicates buckets (data) across indexers
- Can be configured as single-site or multi-site
- Allows balance of growth, speed of recovery, and overall disk usage

Splunk Cluster Overview

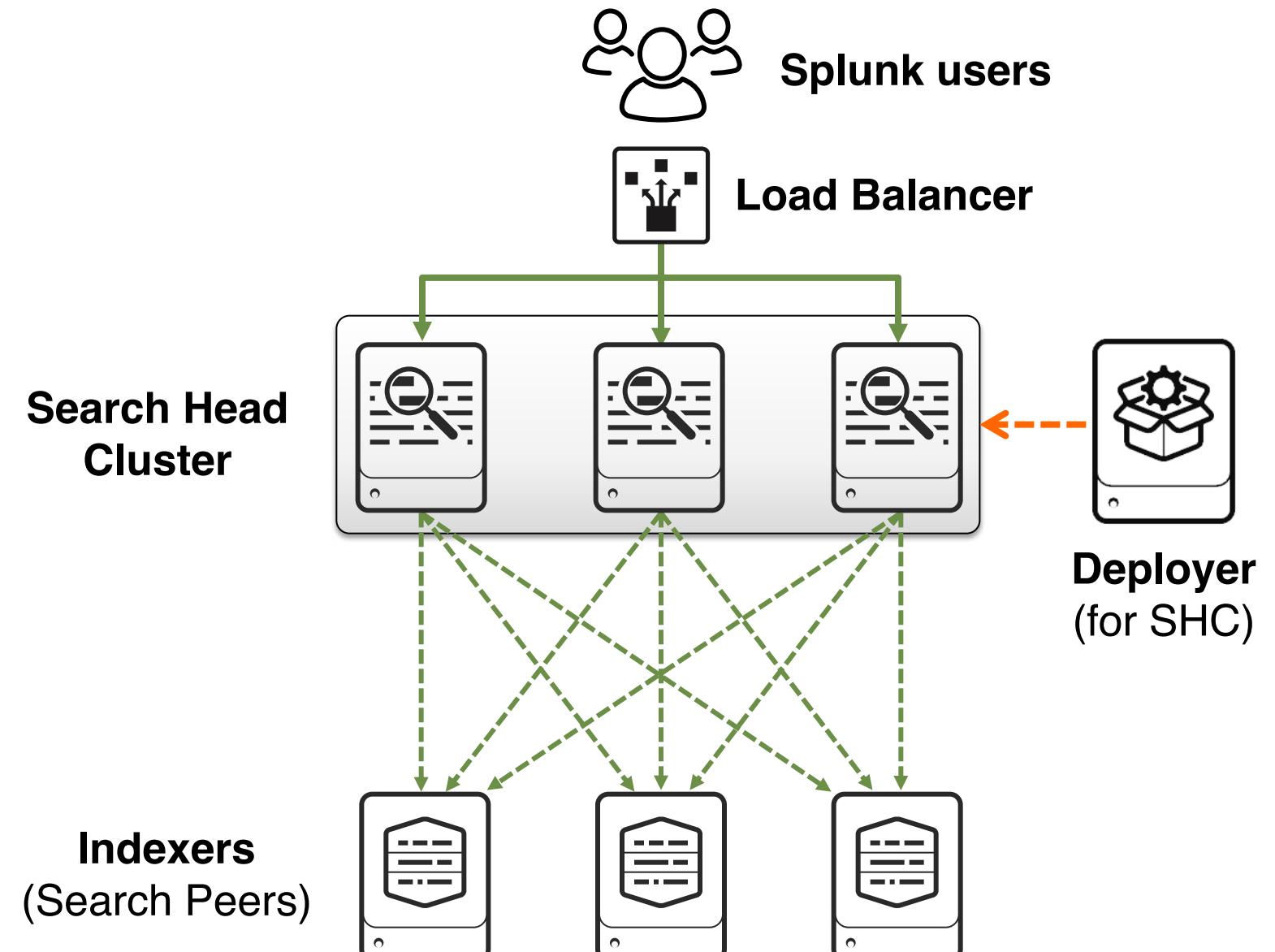


Additional Components:

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

Search Head Cluster

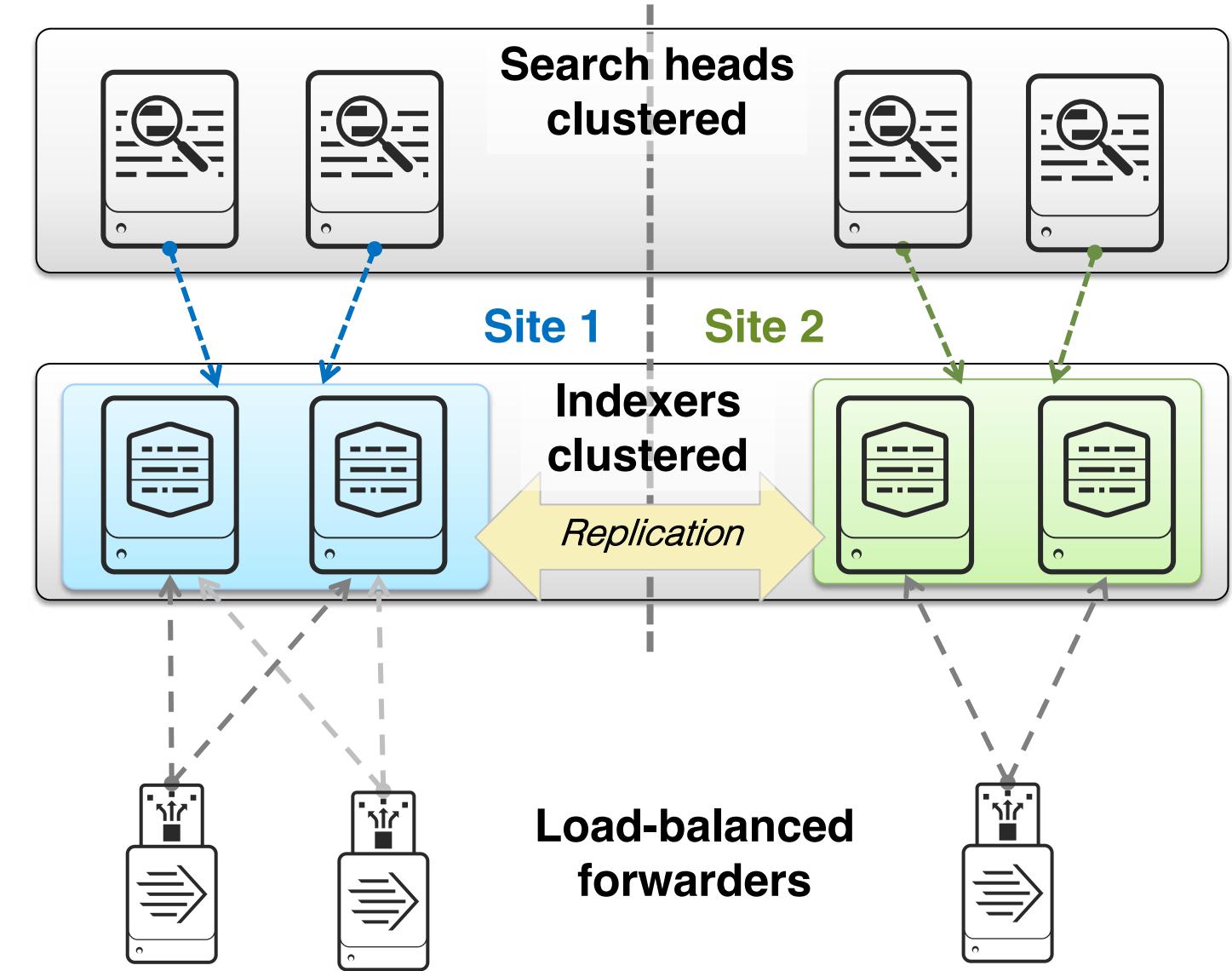
- Accommodates large enterprise use cases
 - Search head high-availability
 - Unified user experience across SHs
 - Search scaling foundation
 - Configuration sharing
 - Artifact replication
 - Job distribution
 - Alert management
 - Load balancing
- Supports external (non-Splunk) load balancers to provide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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Indexer Clustering and Replication

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



Generated for Balaram Guttula (balaram.krishn.guttula@jpmchase.com) (C) Splunk Inc, not for distribution

Further Reading: Clustering

- Basic clustering concepts for advanced users

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

- Configure the search head

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

- Indexer discovery

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