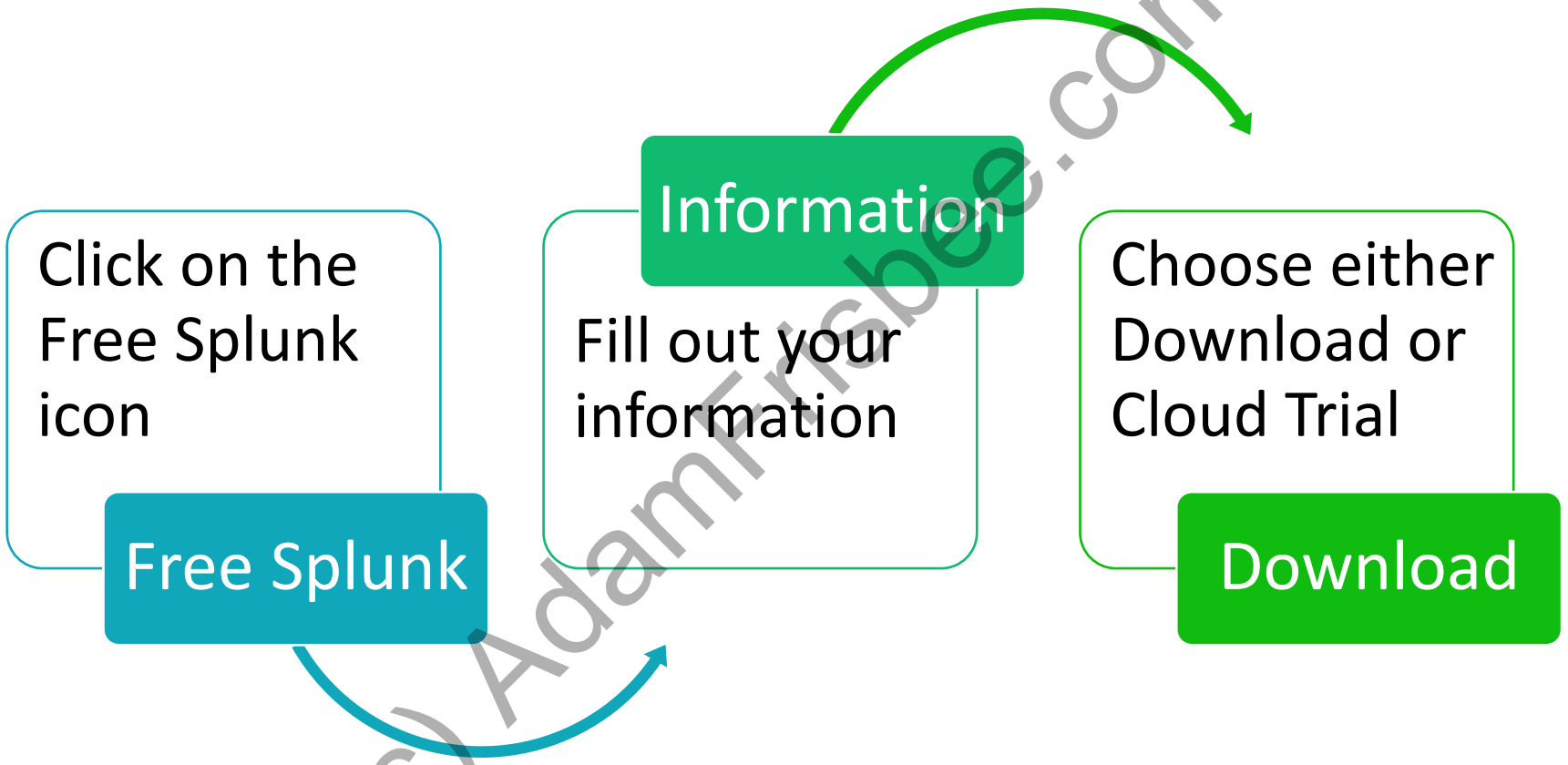
Splunk Admin Basics

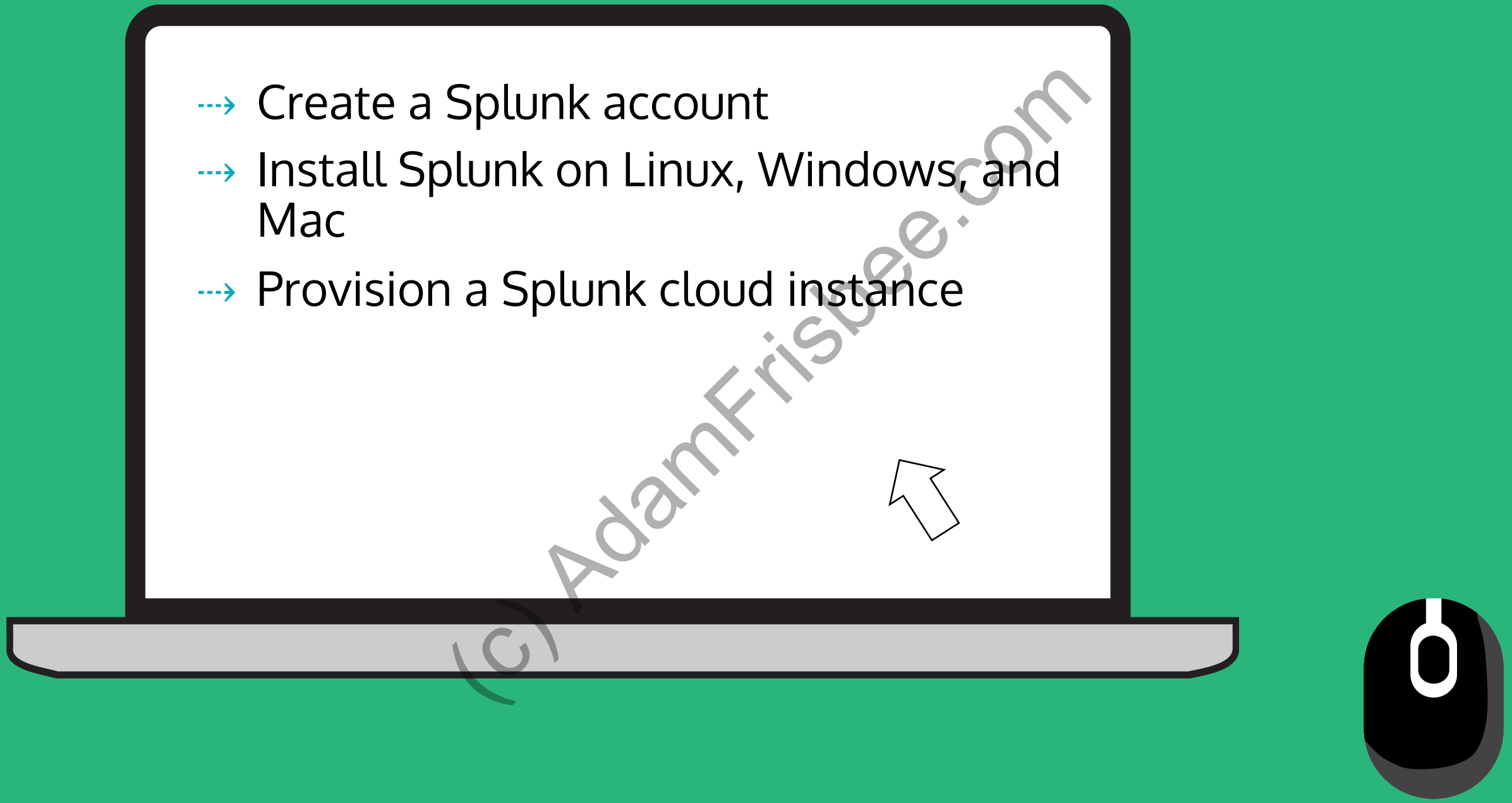
- Creating a Splunk account
- Installing Splunk
- Identifying Splunk components

Creating a Splunk Account and Installing Splunk



Installation Options

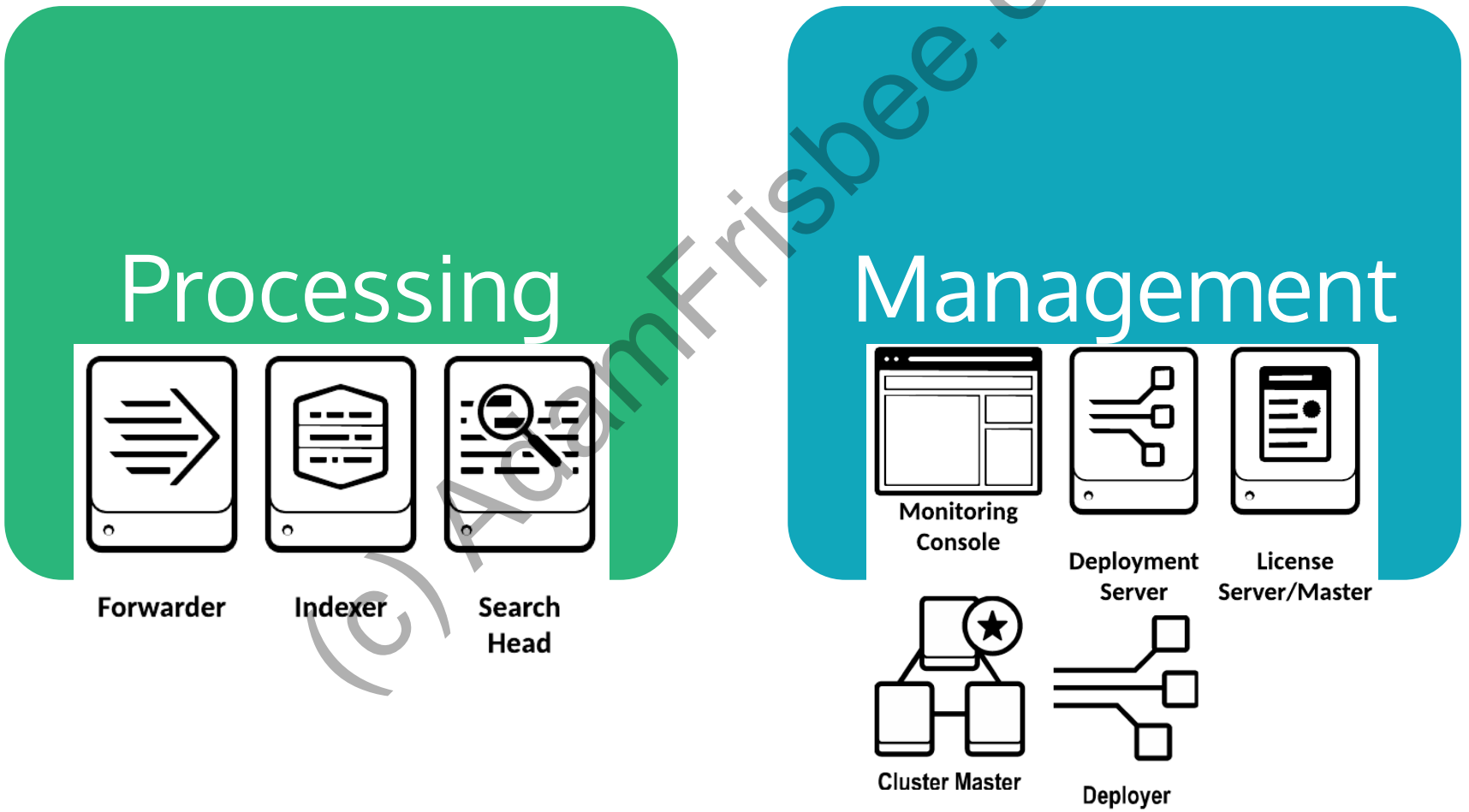
- Download
  - Windows, Linux, or Mac
- Cloud
  - Self service
  - Managed



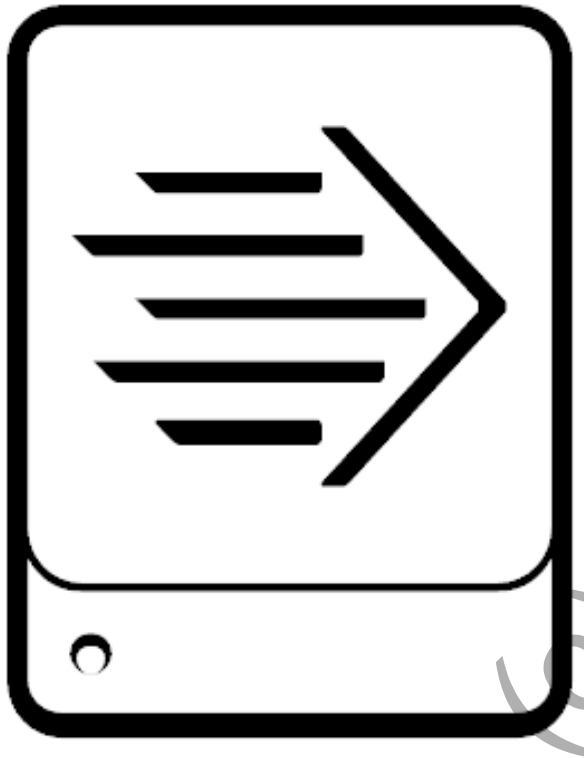
Identifying Splunk Components

Identifying Splunk Components

- Splunk only does three things
  1. Ingests data
  2. Parses, indexes, and stores data
  3. Runs searches on indexed data

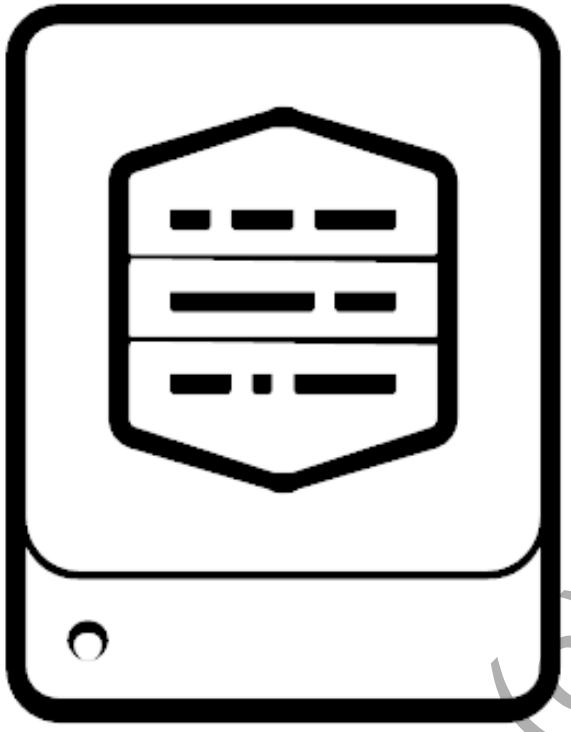


Forwarder



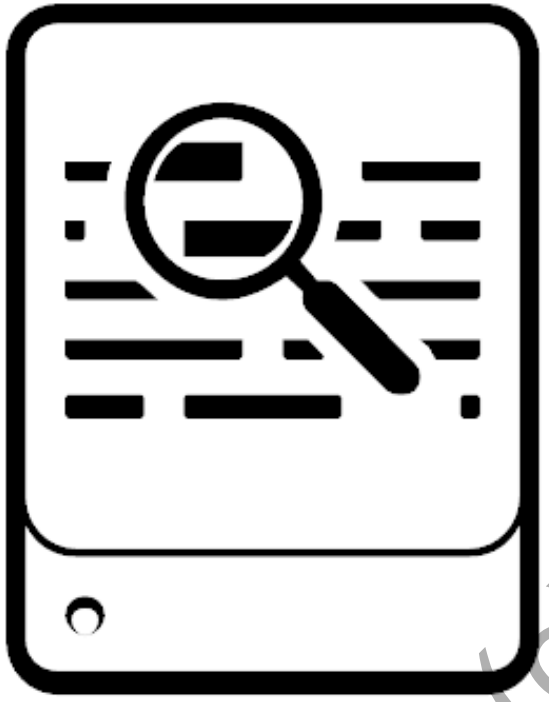
- Forwarders forward data from one Splunk component to another
  - From a source system to an indexer or indexer cluster
  - From a source system directly to a search head

Indexer



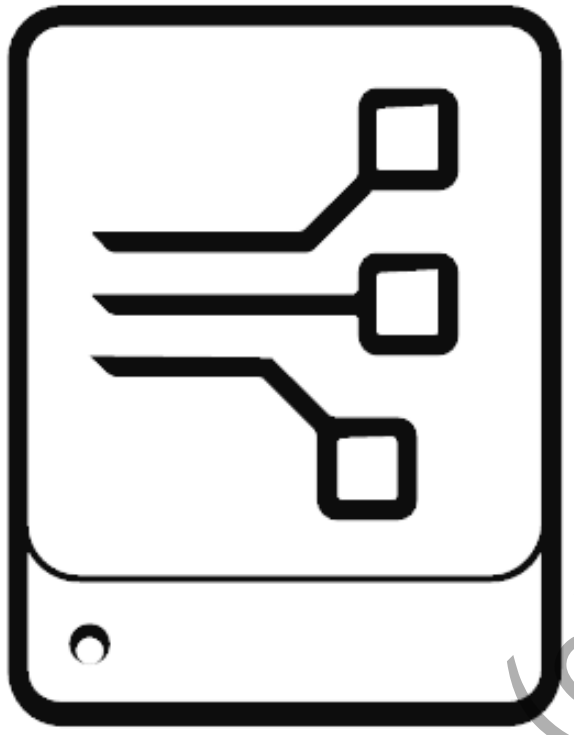
- Indexers index and store data
- In a distributed environment
  - Reside on dedicated machines
  - Can be clustered or independent
  - Clustered indexers are known as peer nodes

Search Head



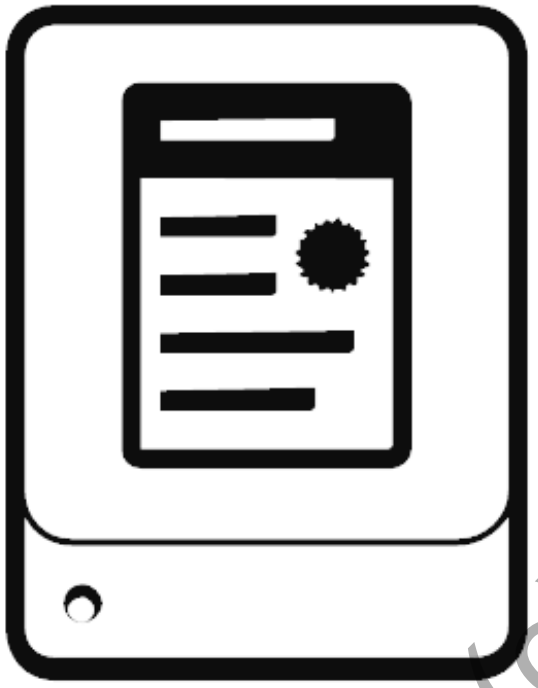
- Search heads manage search requests from users
  - Distributes searches across indexers
  - Consolidates the results from the indexers

Deployment Server



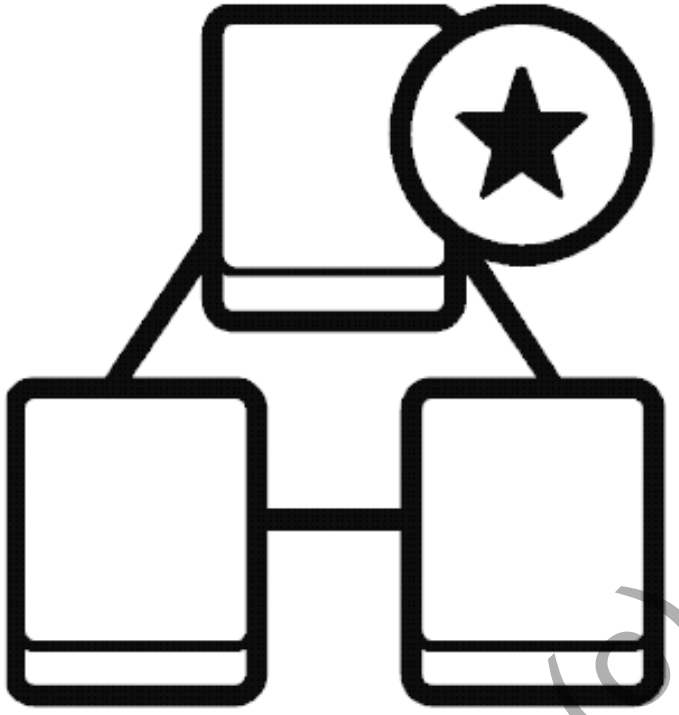
- Centralized configuration manager
- Manages deployment apps for clients
- Configured through the forwarder management interface

License Master



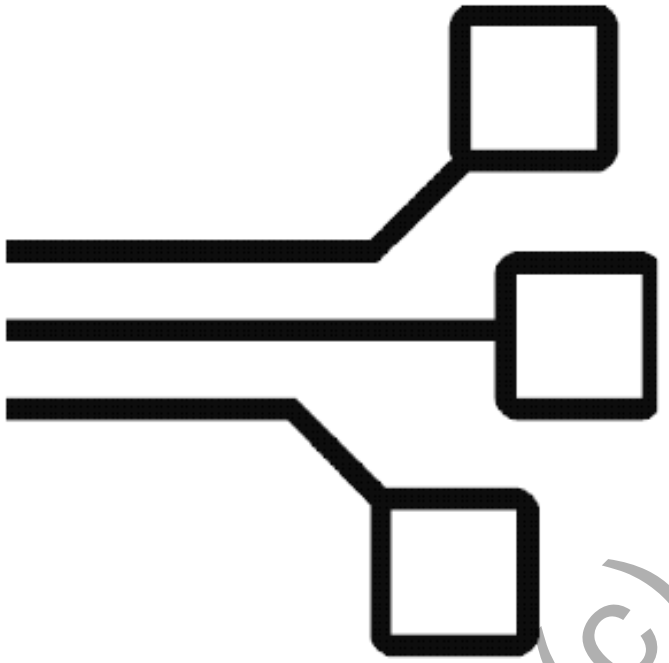
- Centralized license manager
- Clients are called license slaves
- Manages license pools and stacks

Indexer Cluster Master



- Manages indexer clusters
  - Coordinates the activities within the cluster
  - Manages data replication
  - Manages buckets (storage) for the cluster
  - Handles updates for the indexer cluster

Search Head Cluster Deployer



- Manages baselines and apps for search head cluster members
  - This is how Splunk scales
  - Not a member of the cluster

Every Splunk component is built using Splunk Enterprise. It's only a matter of configuration!

Except the Universal Forwarder, which is a specialized "light" Splunk Enterprise installation

Summary

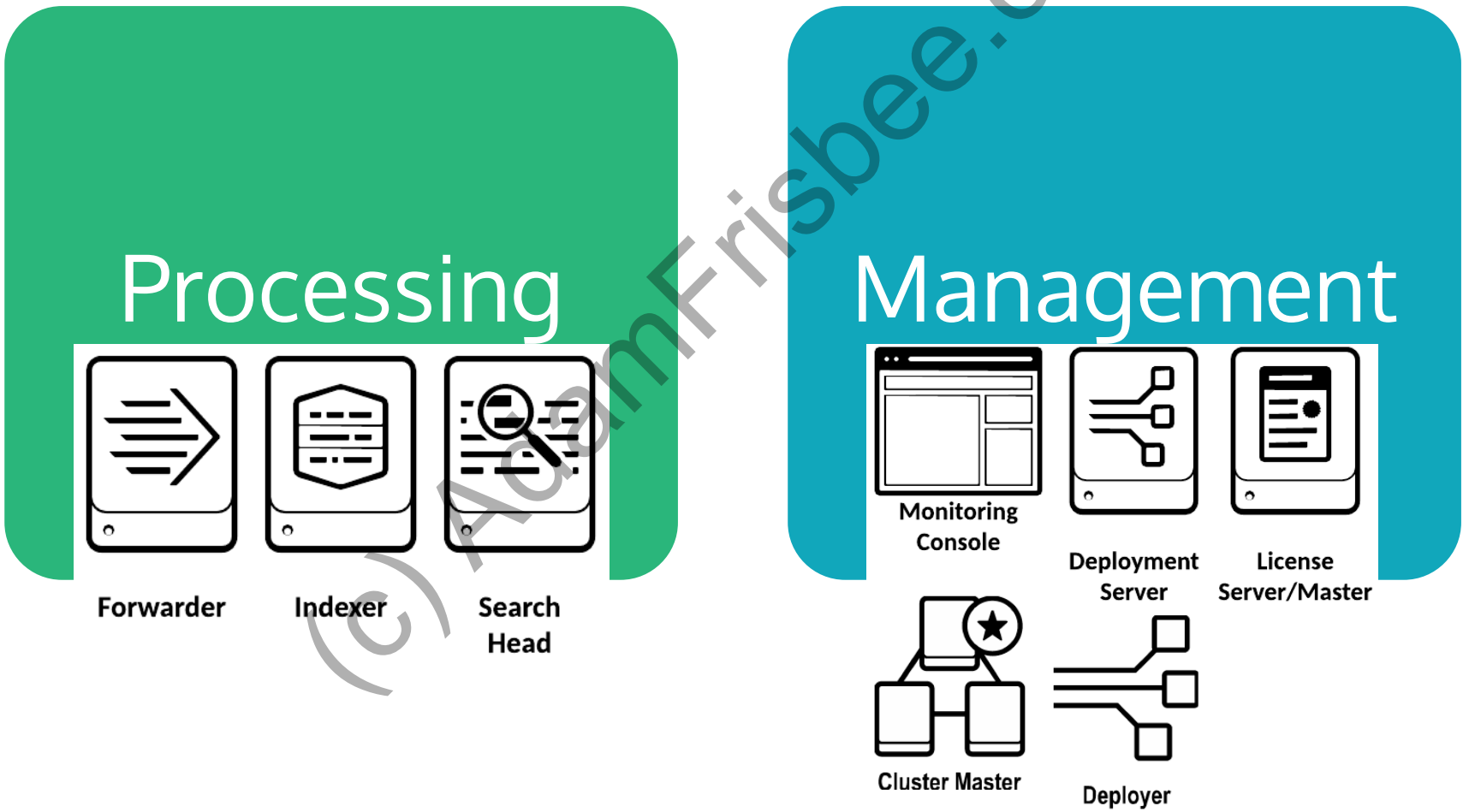
- Identified Splunk components
- Remember: every Splunk component is just an installation of Splunk Enterprise

Identifying Splunk Components

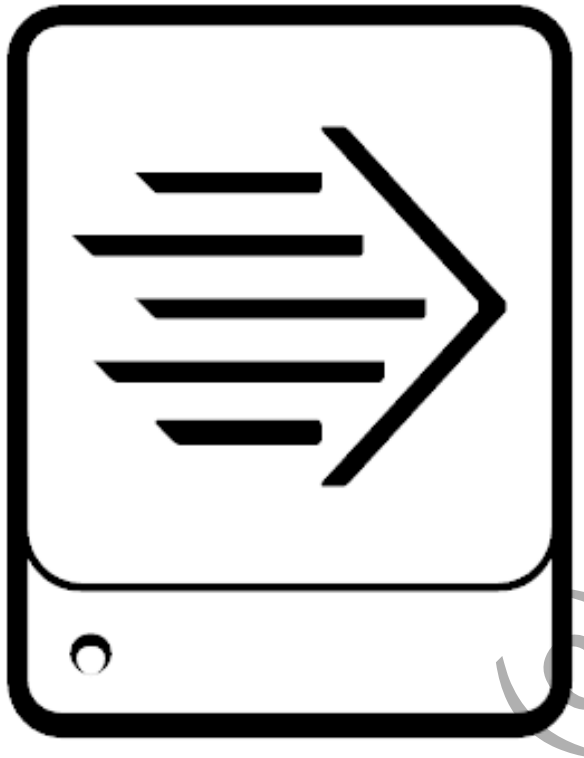
- 1.1 Identifying Splunk components

Identifying Splunk Components

- Splunk only does three things
  1. Ingests data
  2. Parses, indexes, and stores data
  3. Runs searches on indexed data

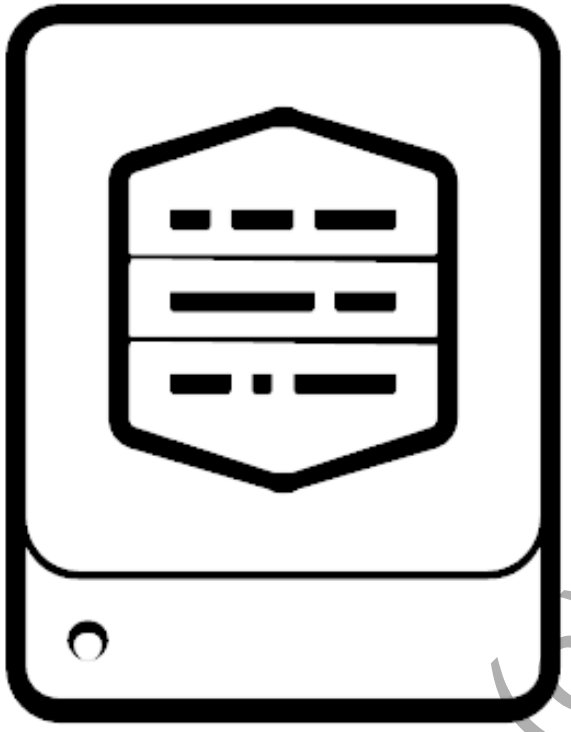


Forwarder



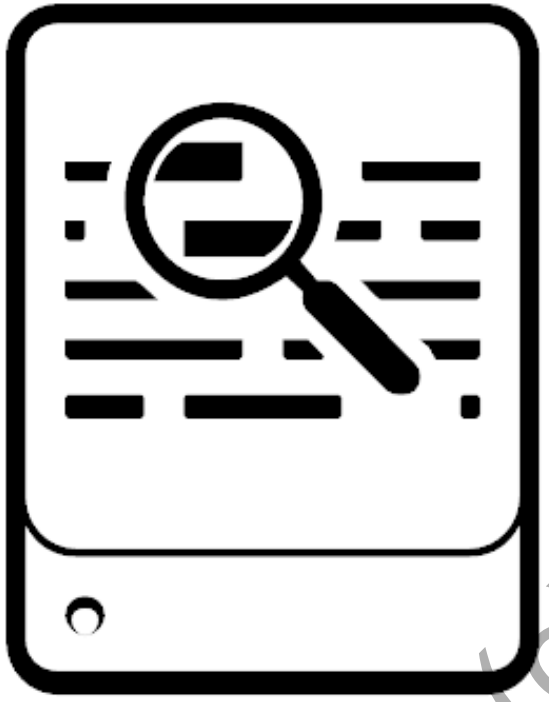
- Forwarders forward data from one Splunk component to another
  - From a source system to an indexer or indexer cluster
  - From a source system directly to a search head

Indexer



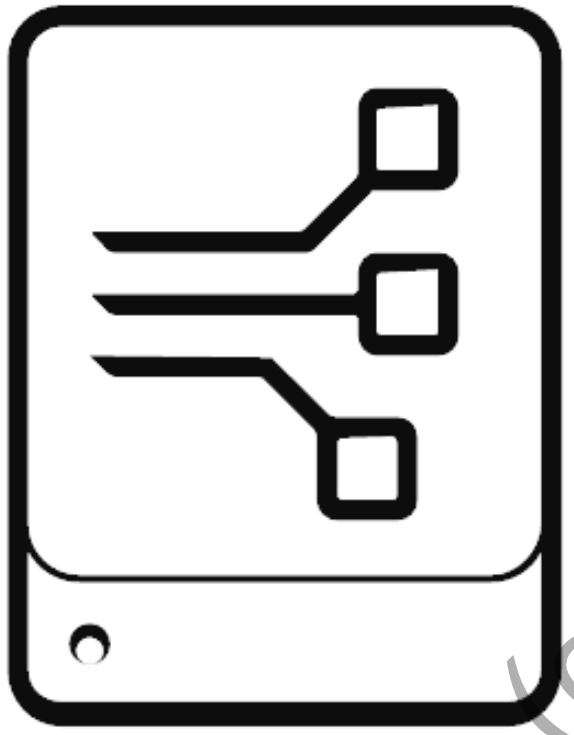
- Indexers index and store data
- In a distributed environment
  - Reside on dedicated machines
  - Can be clustered or independent
  - Clustered indexers are known as peer nodes

Search Head



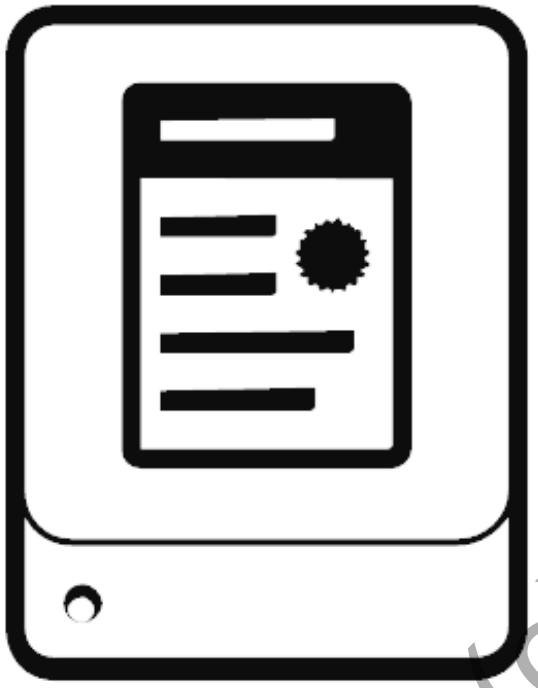
- Search heads manage search requests from users
  - Distributes searches across indexers
  - Consolidates the results from the indexers

Deployment Server



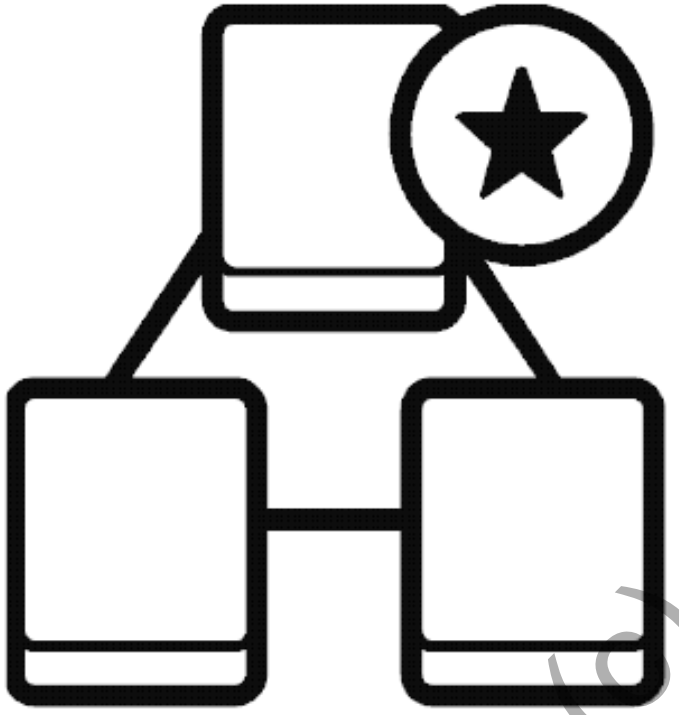
- Centralized configuration manager
- Manages deployment apps for clients
- Configured through the forwarder management interface

License Master



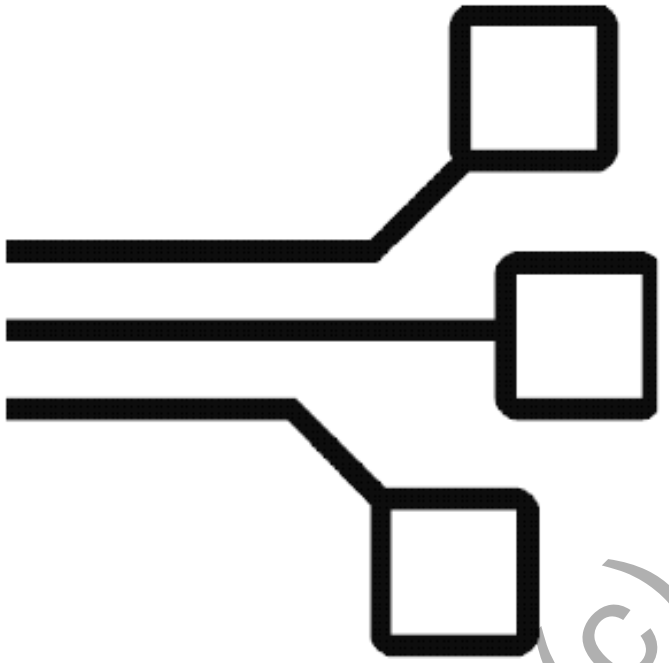
- Centralized license manager
- Clients are called license slaves
- Manages license pools and stacks

Indexer Cluster Master



- Manages indexer clusters
  - Coordinates the activities within the cluster
  - Manages data replication
  - Manages buckets (storage) for the cluster
  - Handles updates for the indexer cluster

Search Head Cluster Deployer



- Manages baselines and apps for search head cluster members
  - This is how Splunk scales
  - Not a member of the cluster

Every Splunk component is built using Splunk Enterprise. It's only a matter of configuration!

Except the Universal Forwarder, which is a specialized "light" Splunk Enterprise installation

Summary

- Identified Splunk components
- Remember: every Splunk component is just an installation of Splunk Enterprise

License Management

- Identifying license types
- Understanding license violations
- Distributed licensing

License Types

Splunk Licensing

- You license data ingested per day, not data stored
- Daily indexing volume is measured from midnight to midnight by the clock on the license master

License Types

Standard

Enterprise Trial

Sales Trial

Dev/Test

Free

Industrial IoT

Forwarder

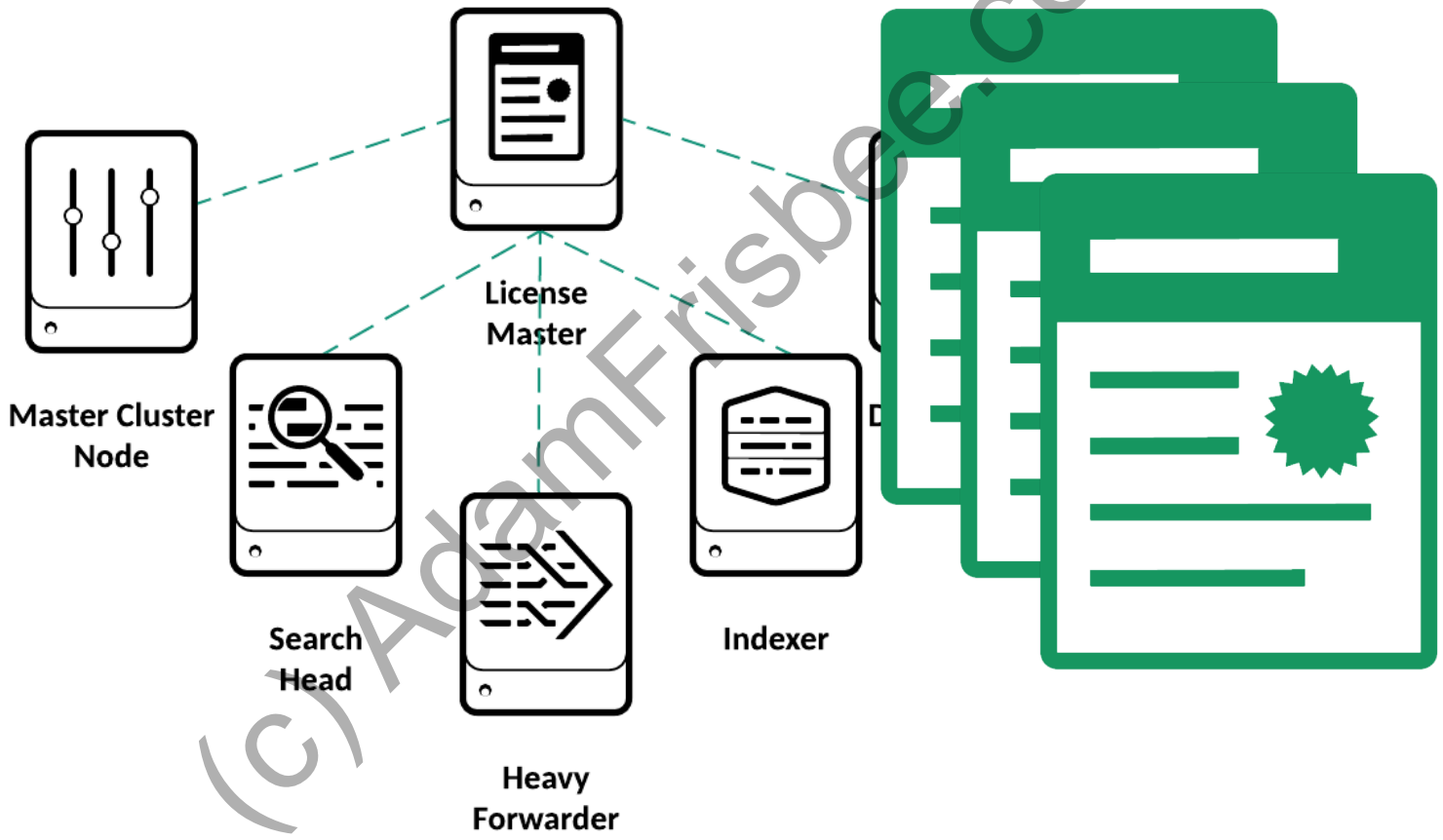
License Violations

License Violations

Starting with version 6.5, Splunk Enterprise no longer disables search when you exceed your licenses data ingestion quota.

Distributed Licensing

Distributed Licensing

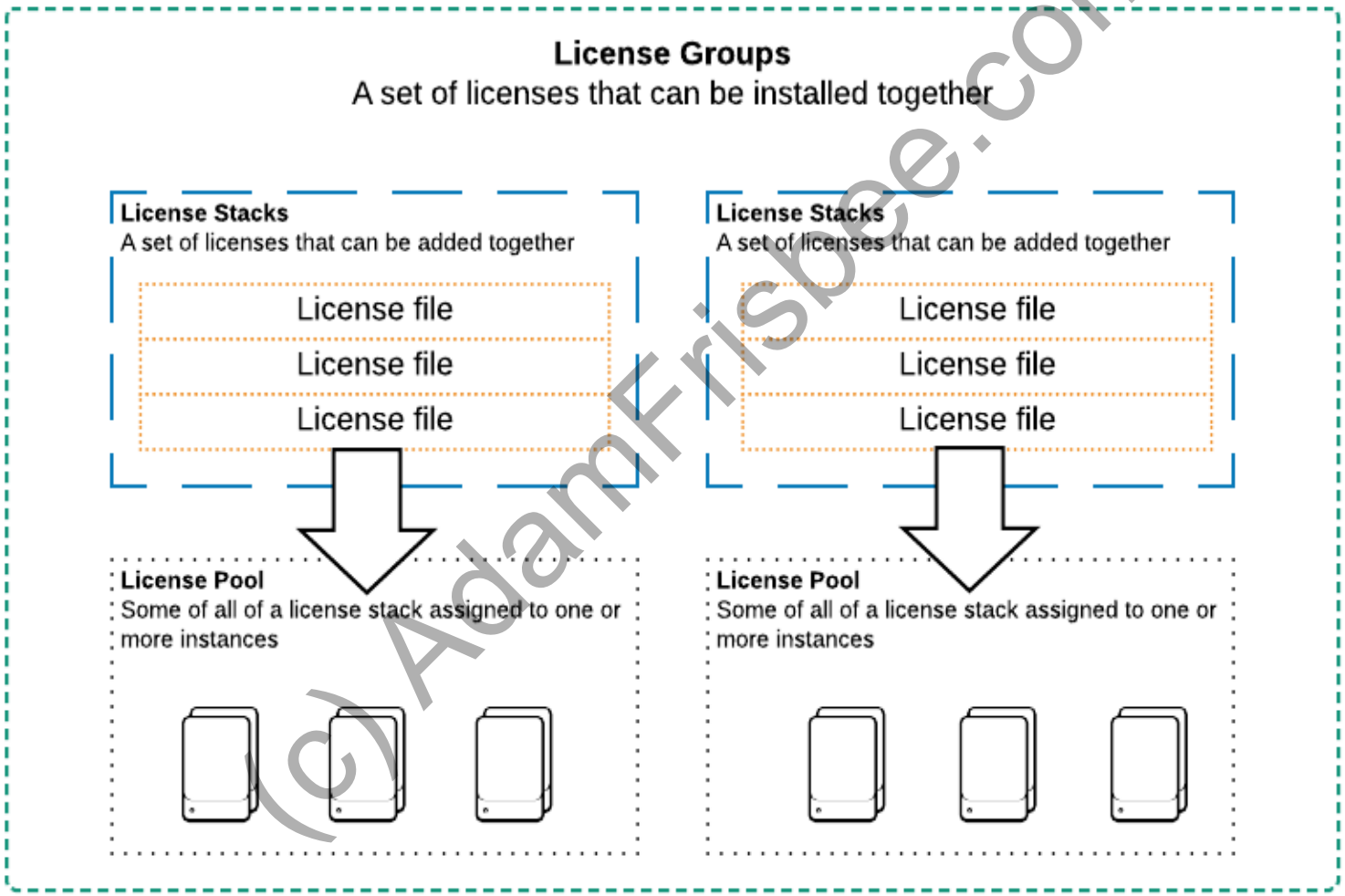


Distributed Licensing

- License pools are created from license stacks
- Pools are sized for specific purposes
- Managed by the license master
- Indexers and other Splunk Enterprise instances are assigned to a pool

Pool

Distributed Licensing



- Explore the licensing console
  - License groups
    - Forwarder license
  - Adding a license
  - Creating a license master or slave

Summary

- Learned how Splunk licensing works
  - License types
  - Violations and warnings
  - Distributed licensing
  - Pools, stacks, and groups

Configuration Files

- Describe Splunk configuration directory structure
- Understand configuration layering
- Understand configuration precedence
- Use `btool` to examine configuration settings

Splunk Configuration Directory Structure

Configuration Files

- Splunk runs on configuration (.conf) files
  - Every behavior and function within Splunk is defined in a .conf file
- Multiple copies of the same configuration file
  - Evaluated by Splunk based on precedence

Common Configuration Files

`inputs.conf`

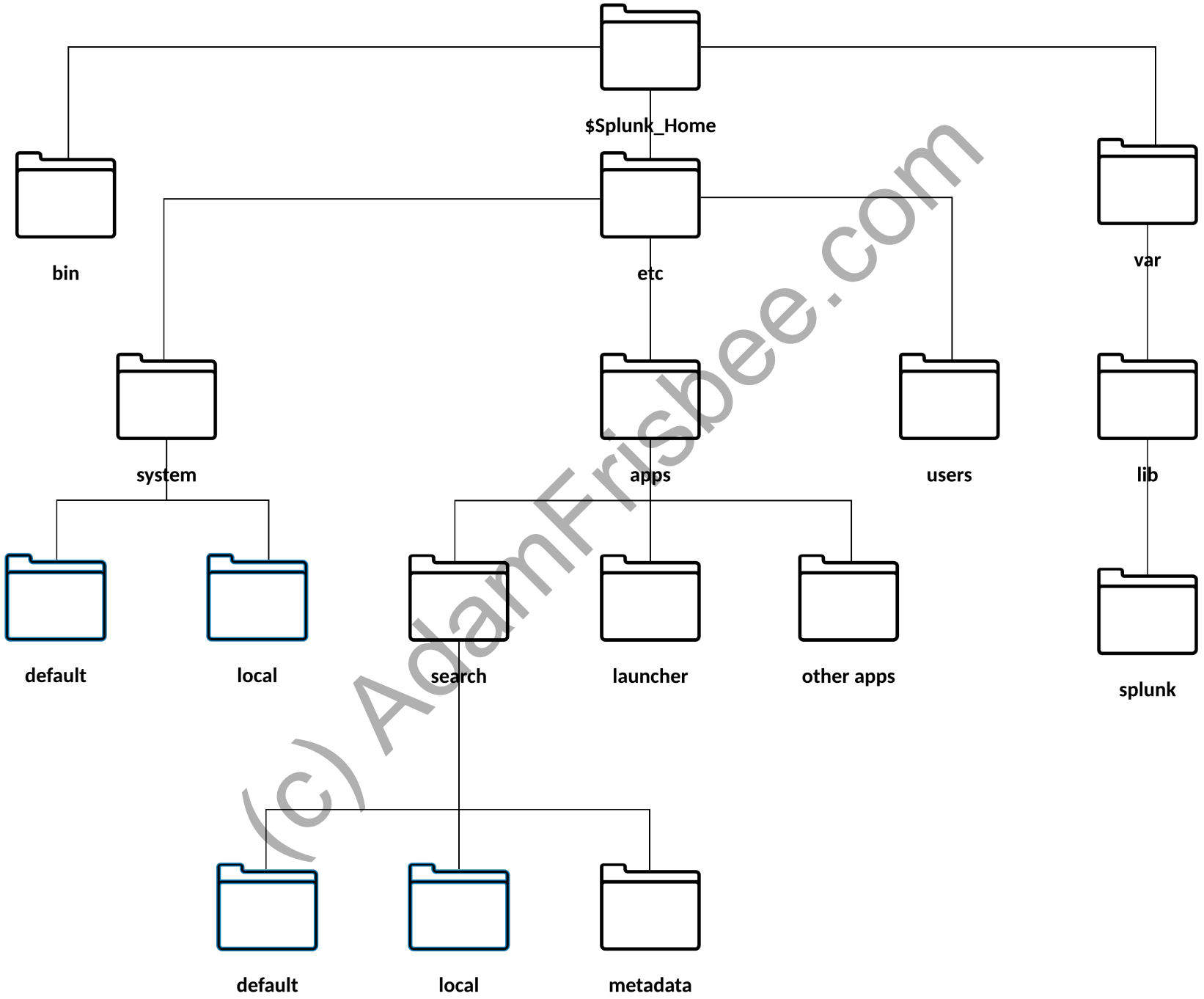
- Governs data inputs such as forwarders and file system monitoring

`props.conf`

- Governs indexing property behavior

`transforms.conf`

- Settings and values that govern data transformation



Configuration Layering and Precedence

Configuration file context

Global

App or user specific

Global context

System **local** directory

⇢App **local** directories

⇢App **default** directories

⇢System **default** directory

App or User Context

User directories for **current user**

- App directories for **currently running app** (local, followed by default)
  - App directories for **all other apps** (local, followed by default)
    - **System** directories (local, followed by default)

What's Inside?

- Stanzas
- Attribute = value pairs

app.conf

```
[id]
group = <group-name>
name = <app-name>
version = <version-number>
```

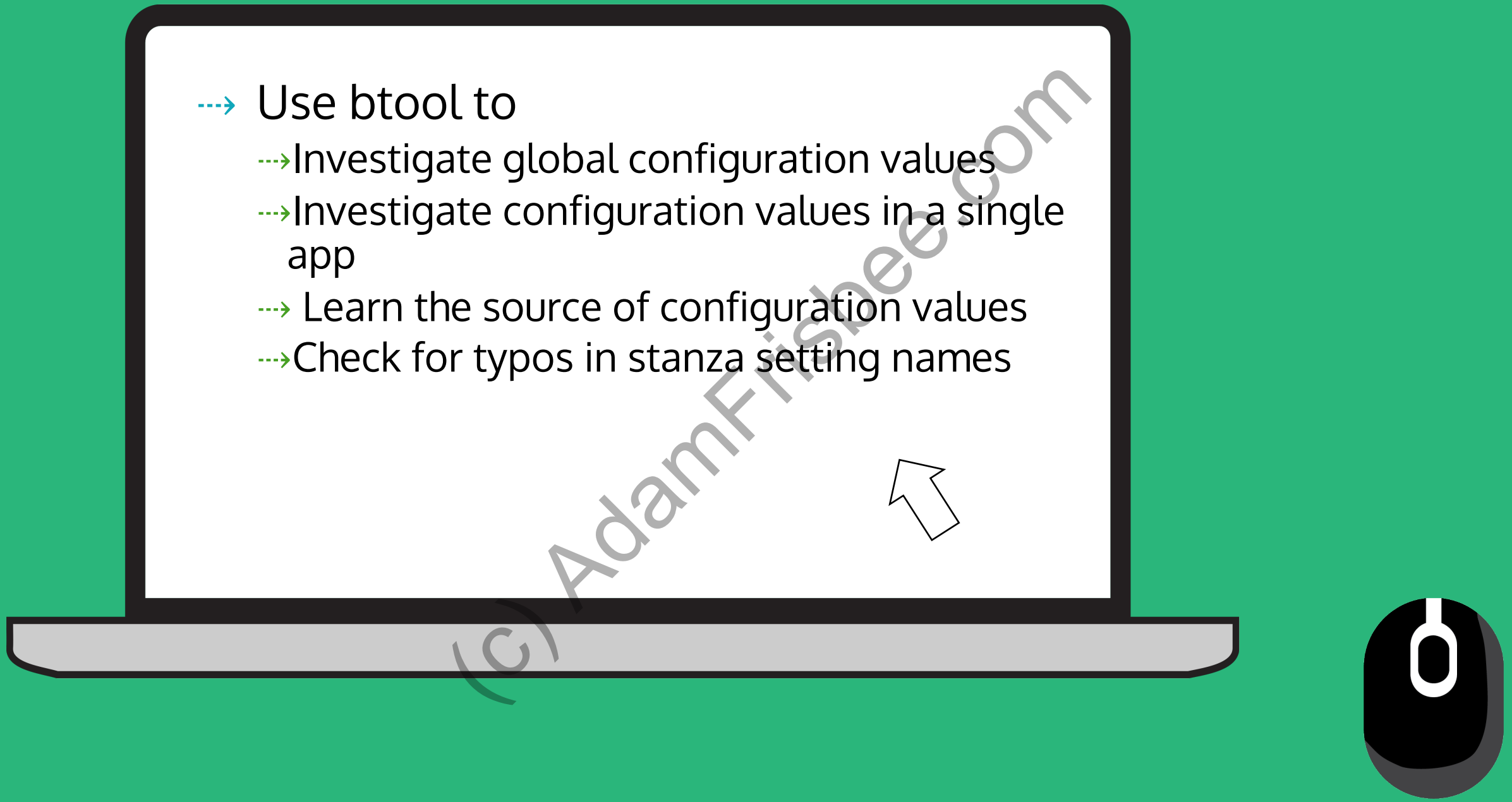
Use `btool` to Examine Configuration Settings

Btool

Troubleshoot

```
$Splunk_Home/bin
./splunk cmd btool <configuration file prefix> list
```

Merged configurations


Use btool to
Investigate global configuration values
Investigate configuration values in a single app
Learn the source of configuration values
Check for typos in stanza setting names
(c) AdamFrisbee.com

Summary

- Learned about configuration files
  - Govern almost every aspect in Splunk
  - What you do in the GUI edits the .conf files
- Discussed conf file precedence
  - Remember, don't touch the default folder no matter what context
- Use btool to verify conf file stanza values that are being used

Indexes

- Describing index structure
- Listing types of index buckets
- Checking data integrity
- Describing `indexes.conf` options
- Describing the fishbucket
- Applying data retention policy

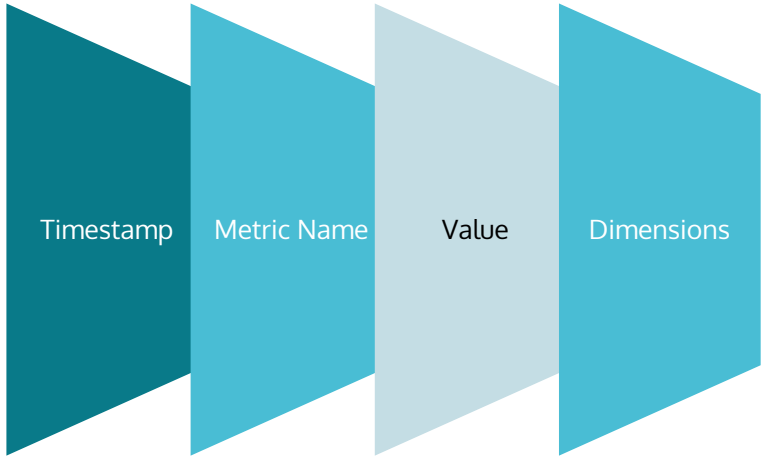
Describe Index Structure

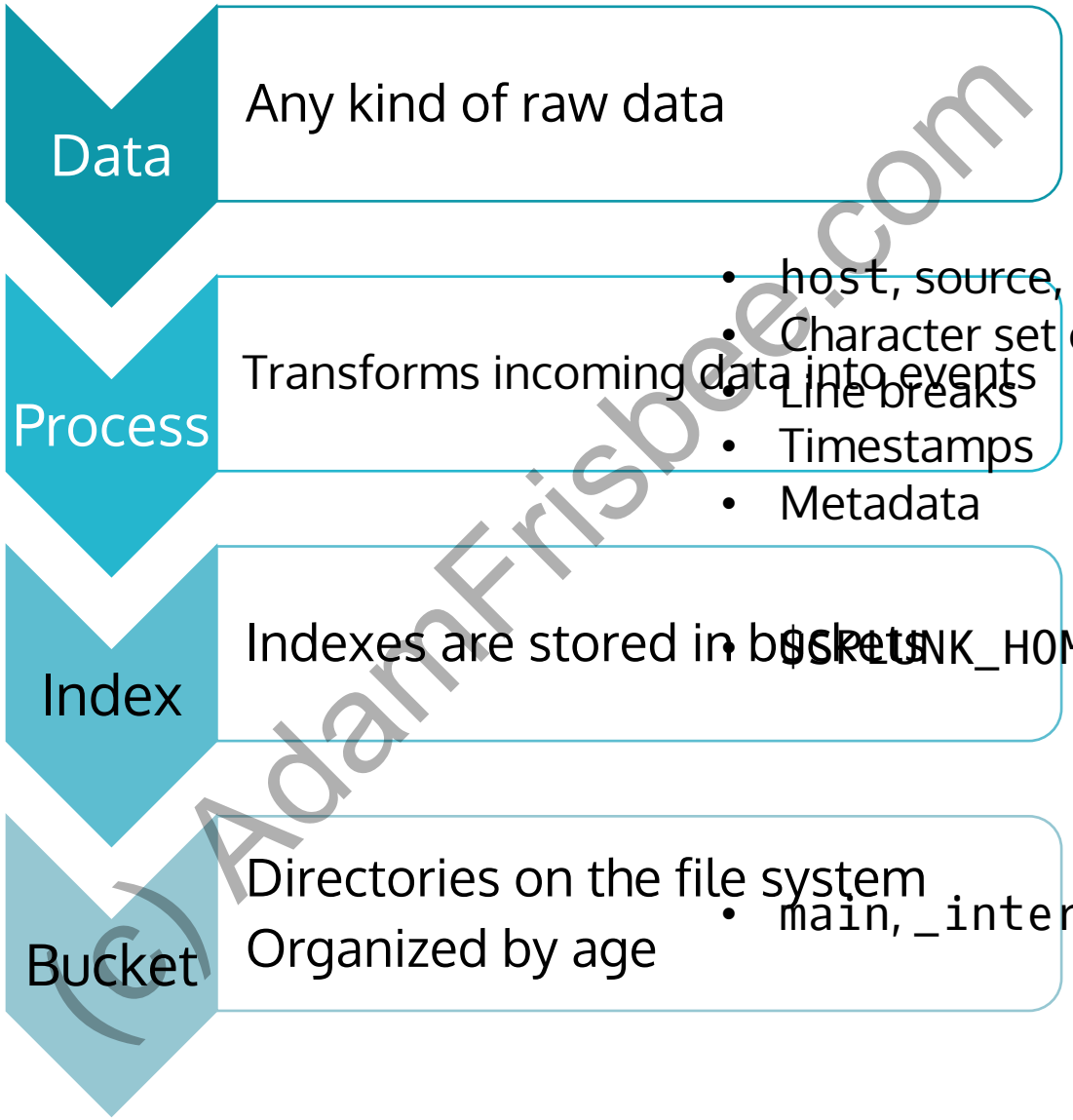
Indexes

- Repository of Splunk events
- Built-in or custom
- Indexes contain three types of data
  1. Raw data in compressed form
  2. Indexes that point to the raw data
  3. Metadata

Index Types

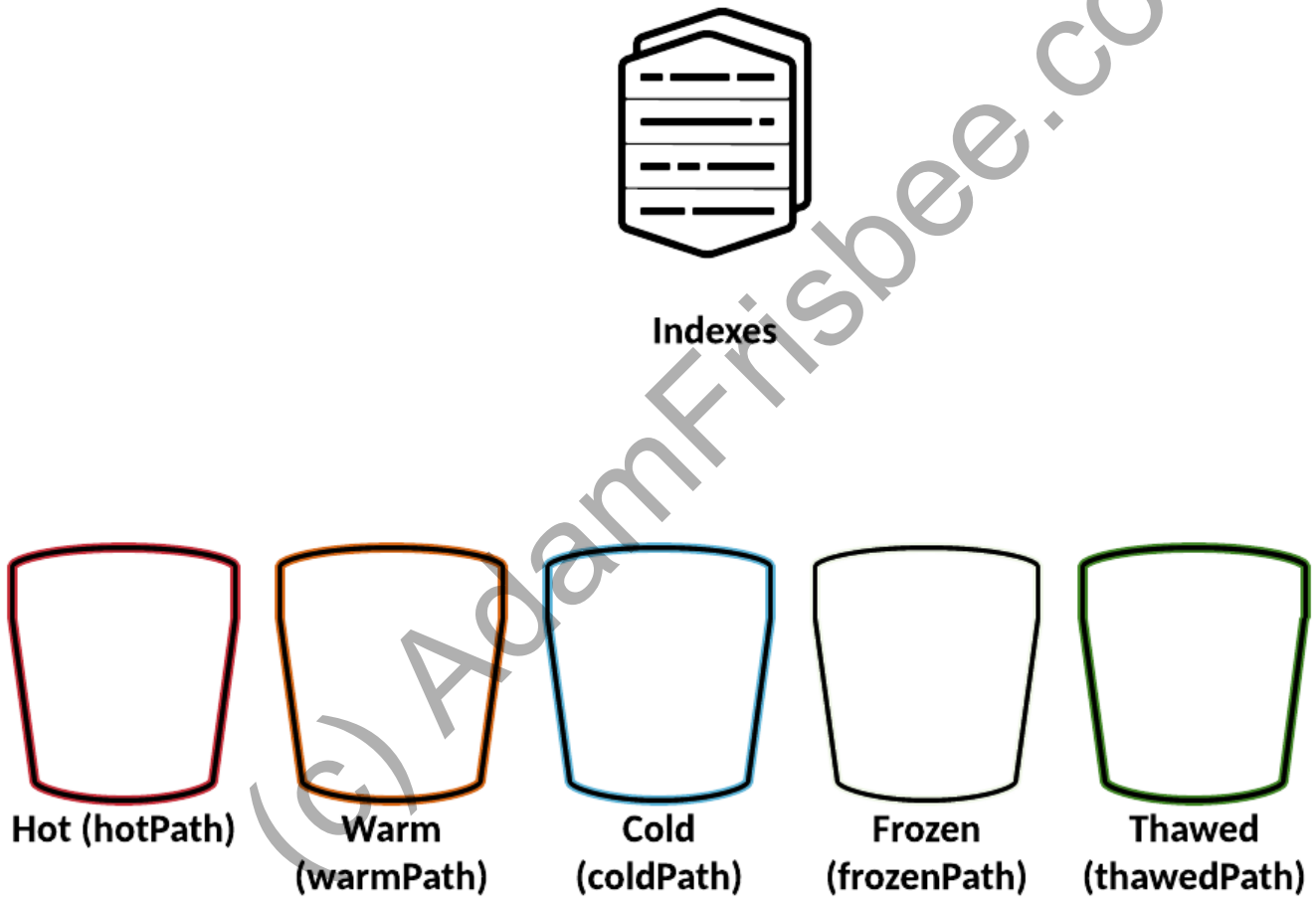
- Event
  - The default type
  - Can handle any type of data
- Metrics
  - Optimized to store and retrieve *metrics data*





Types of Index Buckets

Buckets

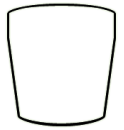


Buckets

`$SPLUNK_HOME/var/lib/splunk/defaultdb/db/*`

`$SPLUNK_HOME/var/lib/splunk/defaultdb/db/*`

`$SPLUNK_HOME/var/lib/splunk/defaultdb/colddb/*`

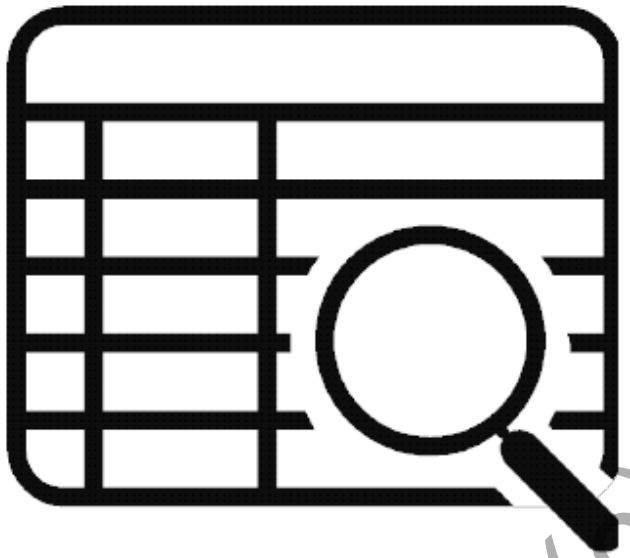


Location that you specify

`$SPLUNK_HOME/var/lib/splunk/defaultdb/thaweddb/*`

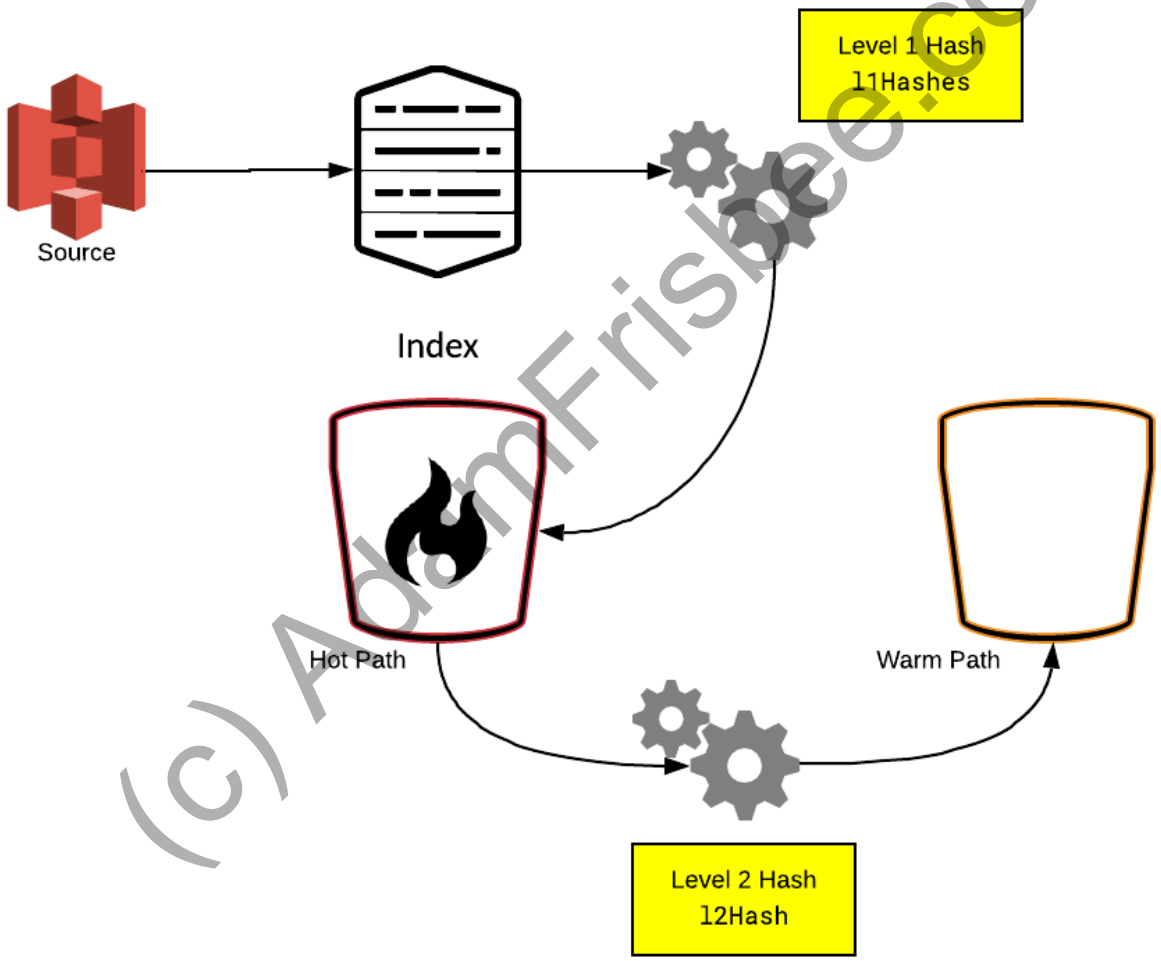
Check Data Integrity

How Data Integrity Works



- Splunk's double hash
  - Computes a hash on newly indexed data
  - Computes another hash on the same data when it moves buckets
  - Stores both hash files in the /rawdata directory

How Data Integrity Works



Command Line Options

- Check hashes to validate data

```
./splunk check-integrity -bucketPath [ bucket path ] [ -verbose ]
```

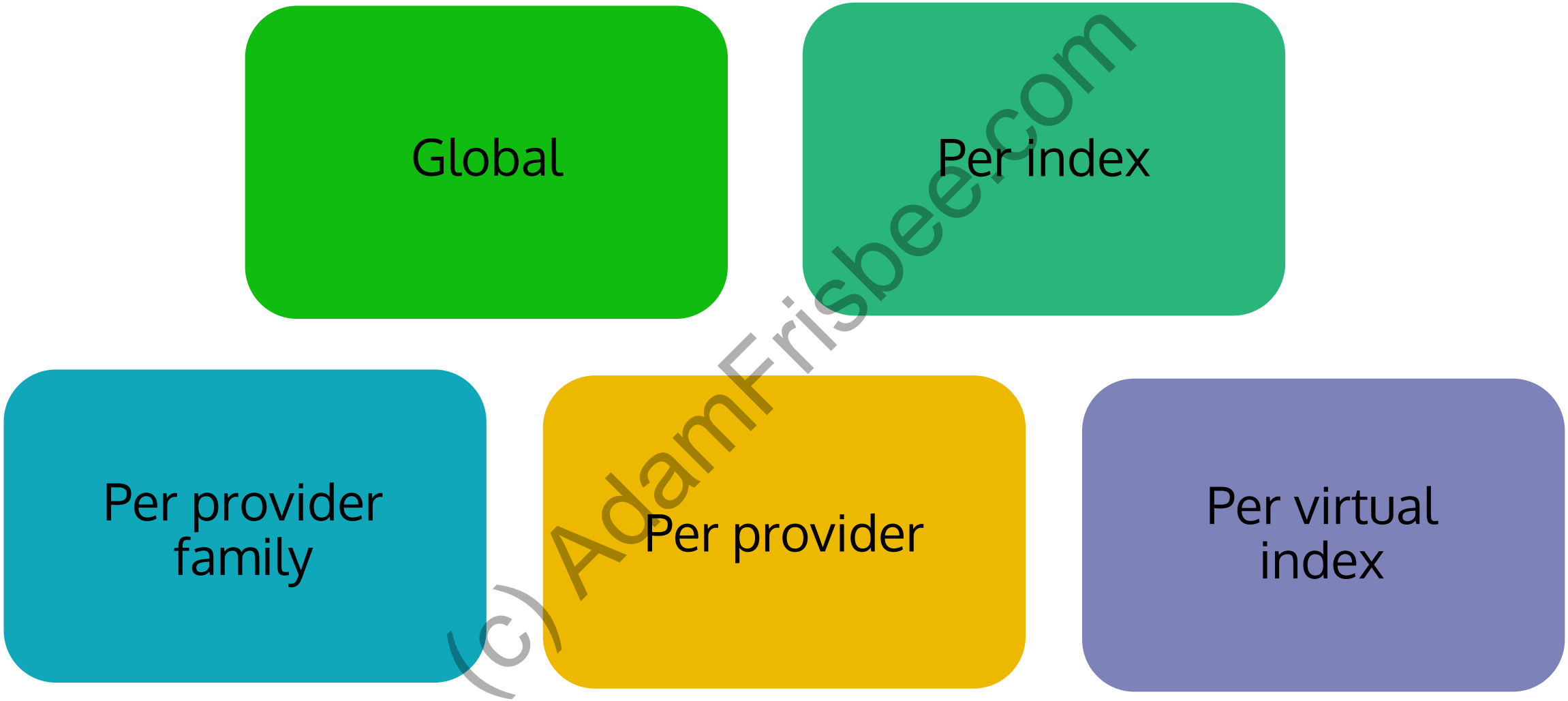
- Configure data integrity control

```
enableDataIntegrityControl=true
```

- Regenerate hashes

```
./splunk generate-hash-files -bucketPath [ bucket path ] [ verbose ]
```

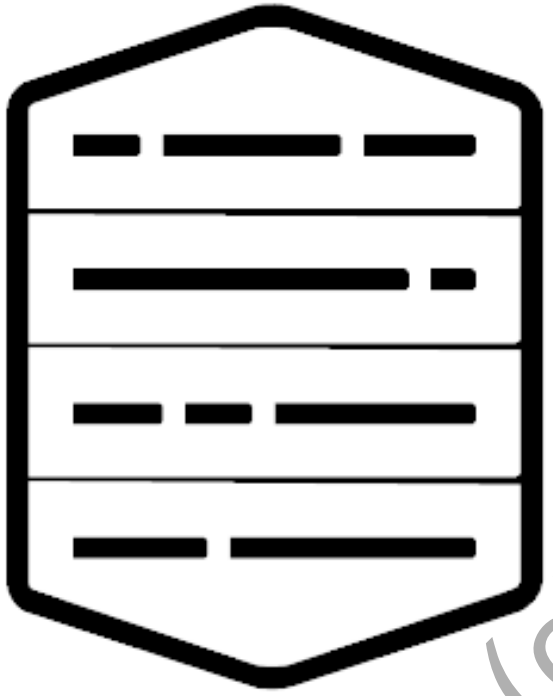
Indexes.conf Options



Global Settings

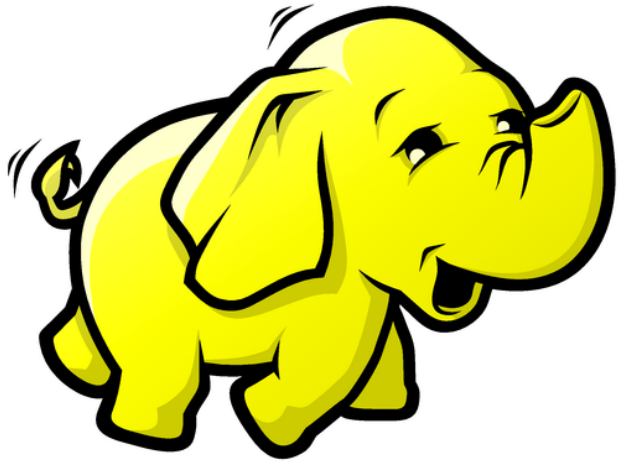
- Defined either at the beginning of the file or in the `[default]` stanza
- Each index.conf file has only one `[default]` stanza

Per Index Options



- Options under an `[<index>]` stanza
- A few of the many options
  - Set bucket paths
  - Set database sizes
  - Specify event or metric data types

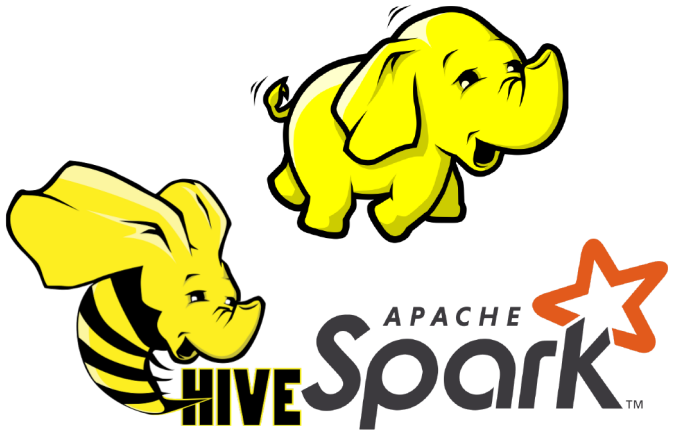
Per Provider Options



- Options for External Resource Providers (ERPs)
- All provider stanzas begin with

```
[provider: ]
```

Per Provider Family Options



- Properties that are common to multiple providers
- All properties that can be used in a family can be used in a provider
- Stanzas for provider families begin with `[provider-family:  ]`