Architecting Splunk Enterprise Deployments

Document Usage Guidelines

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

Course Prerequisites

- Required
  - Splunk Fundamentals 1 and Splunk Fundamentals 2
  - Splunk Enterprise System Administration
  - Splunk Enterprise Data Administration
  - Splunk Enterprise Cluster Administration
- Strongly Recommended
  - Advanced Searching and Reporting with Splunk
  - Creating Dashboards
  - Troubleshooting Splunk Enterprise

Note

In order to receive credit for this course, each student is expected to complete their own lab exercises.

Course Goals

- Apply best practices for architecting and documenting Splunk Enterprise distributed deployments
- Provide a framework and methodology for Splunk deployments

Course Outline

Module 1: Introduction

Module 2: Project Requirements

Module 3: Infrastructure Planning: Index Design

Module 4: Infrastructure Planning: Resource Planning

Module 5: Clustering Overview

Module 6: Forwarder and Deployment Best Practices

Module 7: Integration

Module 8: Performance Monitoring and Tuning

Module 9: Use Cases

Module 1: Introduction

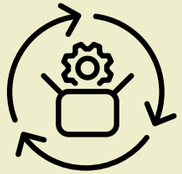
Module Objectives

- Define the responsibilities of a Splunk Architect
- Introduce the Splunk deployment planning process and tools
- Review the network topology for Buttercup Games

Splunk Architect Tasks

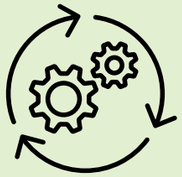
Capacity planning

Current need and future growth

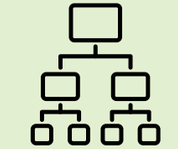


Create a deployment strategy

Hardware needs, number of search heads and indexers, clustering, Splunk Cloud, number of sites



Define backup strategies



Implement High Availability and Disaster Recovery strategy

Create test environments

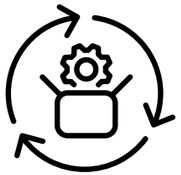
Document Splunk deployment architecture

Evangelize Splunk within your organization

Architect and Administrator Responsibilities

Capacity Planning

Splunk Deployment Installation



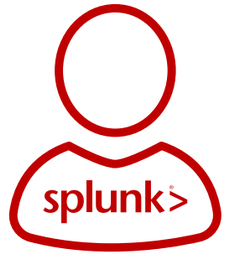
Splunk Deployment Management

Software Upgrades

Splunk Deployment Problem Management

Evangelizing Splunk

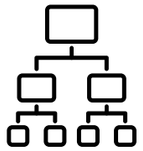
Architect



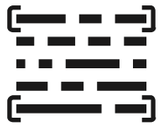
Admin

User Enablement / Onboarding

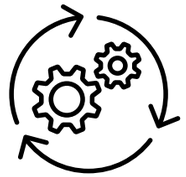
System Documentation



High Availability / Disaster Recovery



Data Onboarding Management

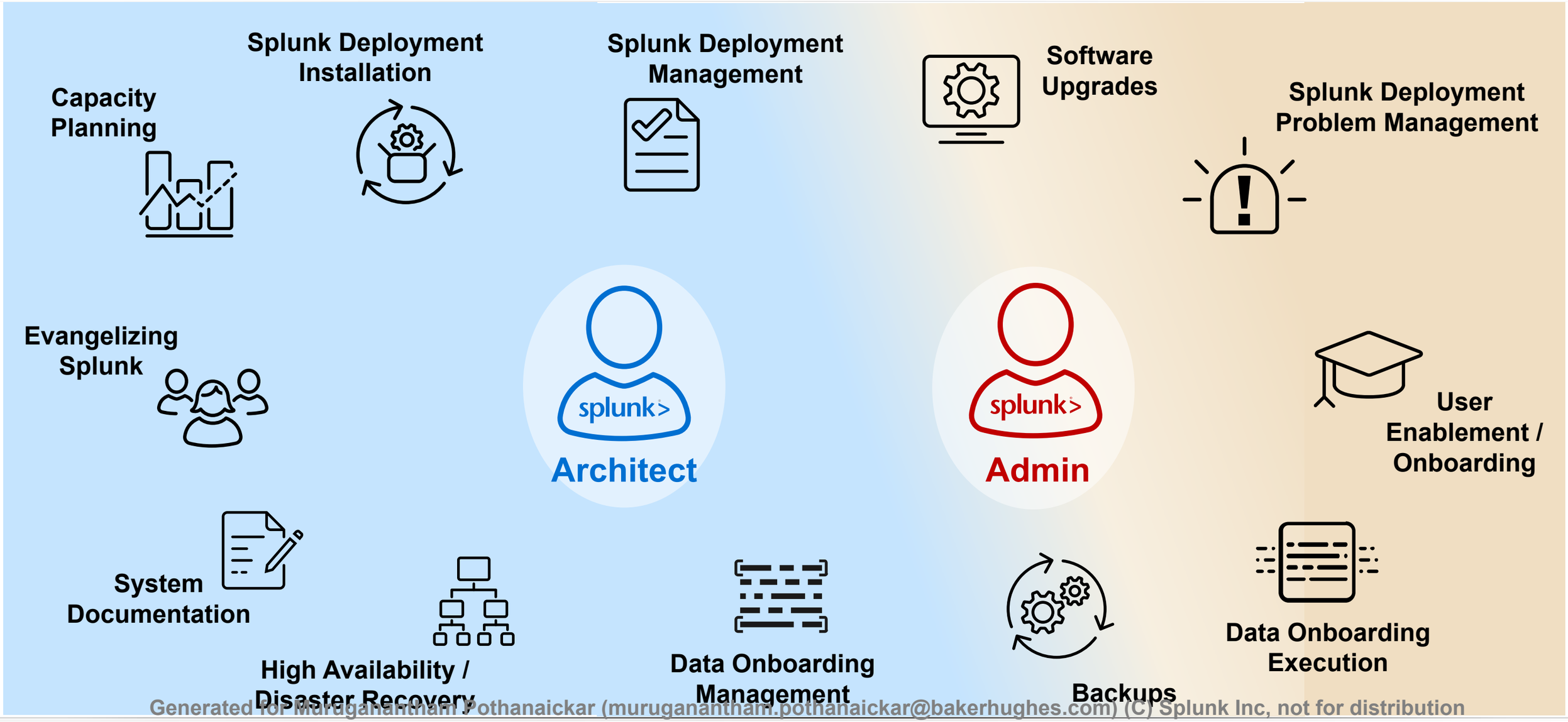


Backups

Data Onboarding Execution

 | 12 February 2021

Architect and Administrator Responsibilities



Architect and Administrator Responsibilities (1/3)

Responsibility	Who?	Description
Budget Management	Program Manager	• Facilitate executive and procurement discussions/documentation • Obtain funding for additional license and infrastructure growth
Capacity Planning	Architect	• Monitor environments in conjunction with projected future growth • Identify future capacity needs • Recommend any horizontal or vertical scaling
Splunk Deployment Installation	Architect	• Deploy Splunk to new environments • Create new non-production environments for testing/development
Splunk Deployment Management	Architect + Admin Architect Admin	• Scale existing environments to meet capacity needs • Alter the state of existing environments (non-clustered to clustered, single site to multi-site, shared roles to dedicated roles, and so on) • Manage configurations effectively including version control to ensure bad configurations can be reverted
Splunk Deployment Problem Management	Admin	• Proactively monitor and respond to issues with the system including regular monitoring of the MC. • Respond to system alerts generated by Splunk • Respond to and investigate issues reported by end users • Manage support tickets with Splunk support

Architect and Administrator Responsibilities (2/3)

Responsibility	Who?	Description
Software Upgrades	Admin Architect	• Routine software upgrades to Splunk and underlying layered technologies • Define and execute testing procedures to ensure successful upgrades
Data Onboarding Management	Architect Admin Admin	• Define and manage strategies and processes to ingest new data sources • Work with users to request new data sources to be onboarded • Prioritize new requests
Data Onboarding Execution	Admin	• Document existing and newly ingested data sources • Design and deploy inputs to UFs/HFs to capture new data • Manage parsing, event breaking, timestamping, etc. • Move configuration through non-production testing, as required • Deploy changes to production • Repeat above for dashboards, reports, alerts, etc.
User Enablement / Onboarding	Admin	• Define and manage strategies and processes for new users • Manage access controls to the system • Provide education and training resources • Define and provide support for end user issues

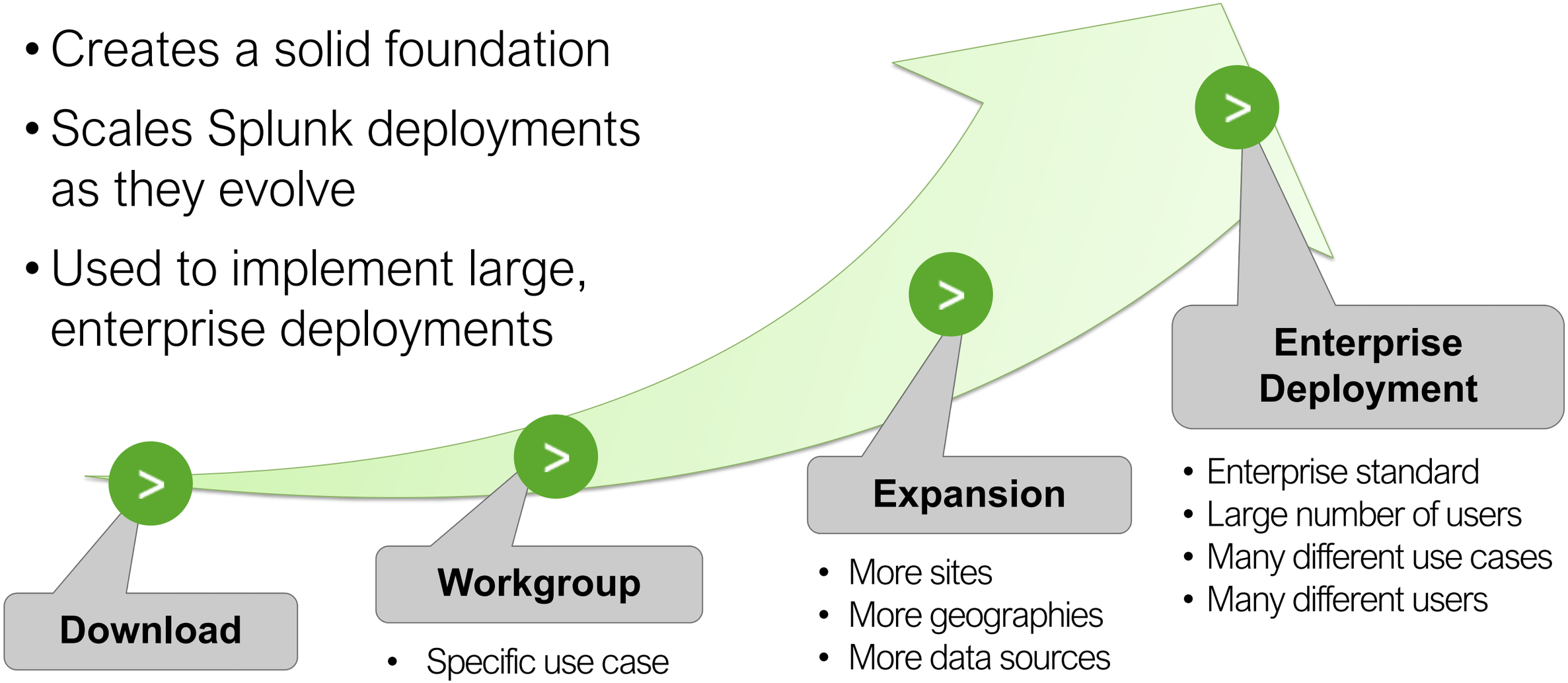
Architect and Administrator Responsibilities (3/3)

Responsibility	Who?	Description
Backups	Architect + Admin	Define, implement, and test backup strategies for Splunk, including configurations and Index data
High Availability / Disaster Recovery	Architect	Define, implement, and test disaster recovery and high availability for Splunk
System Documentation	Architect	Document installation steps, support procedures, backup and recovery, troubleshooting, and so on
Evangelizing Splunk	Architect	Ability to work with prospective Splunk teams or users to: • Discuss the problems and business domains of prospective users • Identify opportunities for Splunk to solve challenges / pain points • Foster a culture and environment where Splunk can spread/thrive including leading internal collaboration / technology sharing events

For details about upgrading Splunk, please review the following document:
https://docs.splunk.com/images/d/d3/Splunk_upgrade_order_of_ops.pdf

Deployment Scaling Plan

- Creates a solid foundation
- Scales Splunk deployments as they evolve
- Used to implement large, enterprise deployments

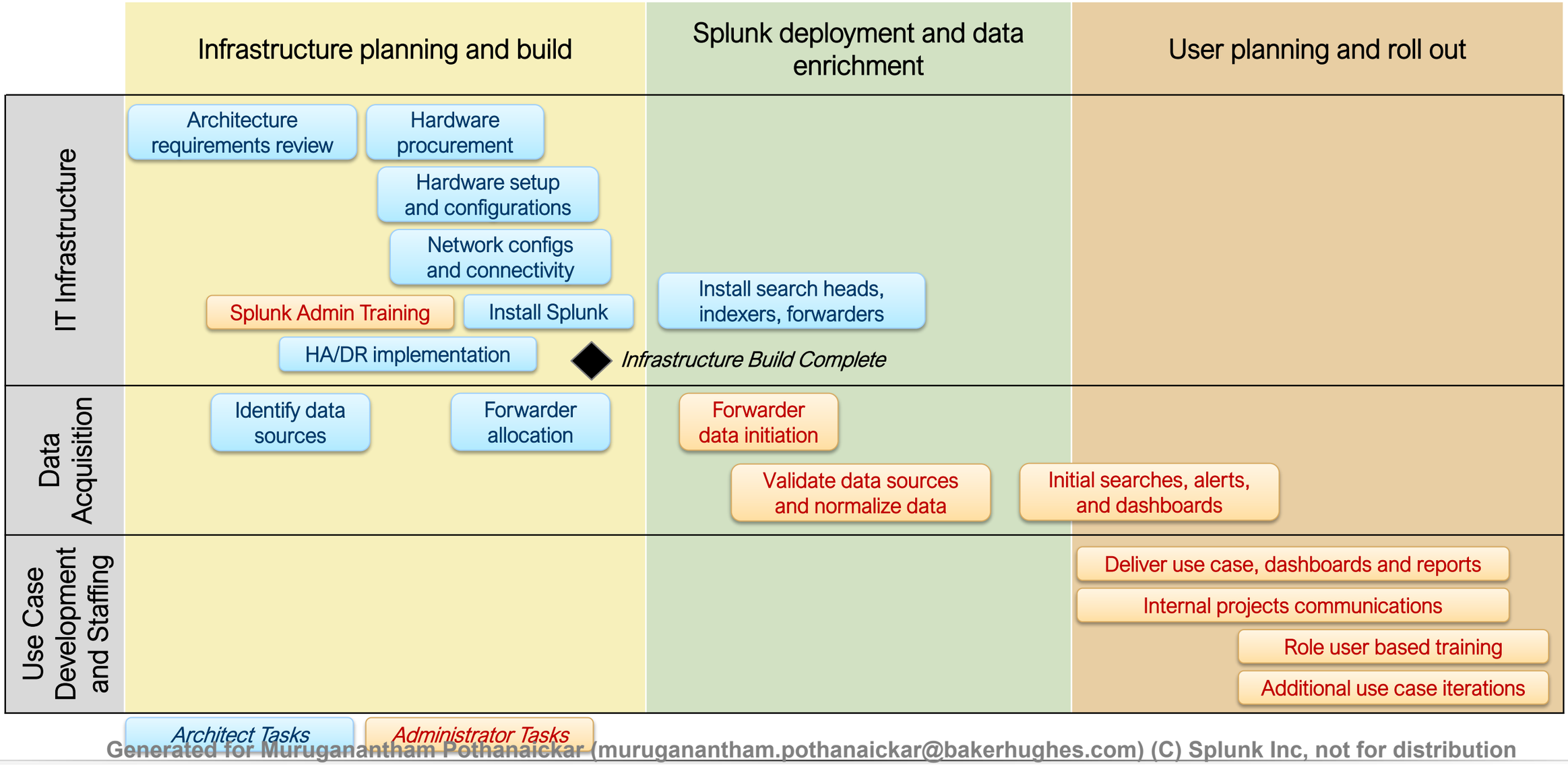


- Initial User
- Specific use case
- Specific users
- More sites
- More geographies
- More data sources
- More data volume
- Enterprise standard
- Large number of users
- Many different use cases
- Many different users

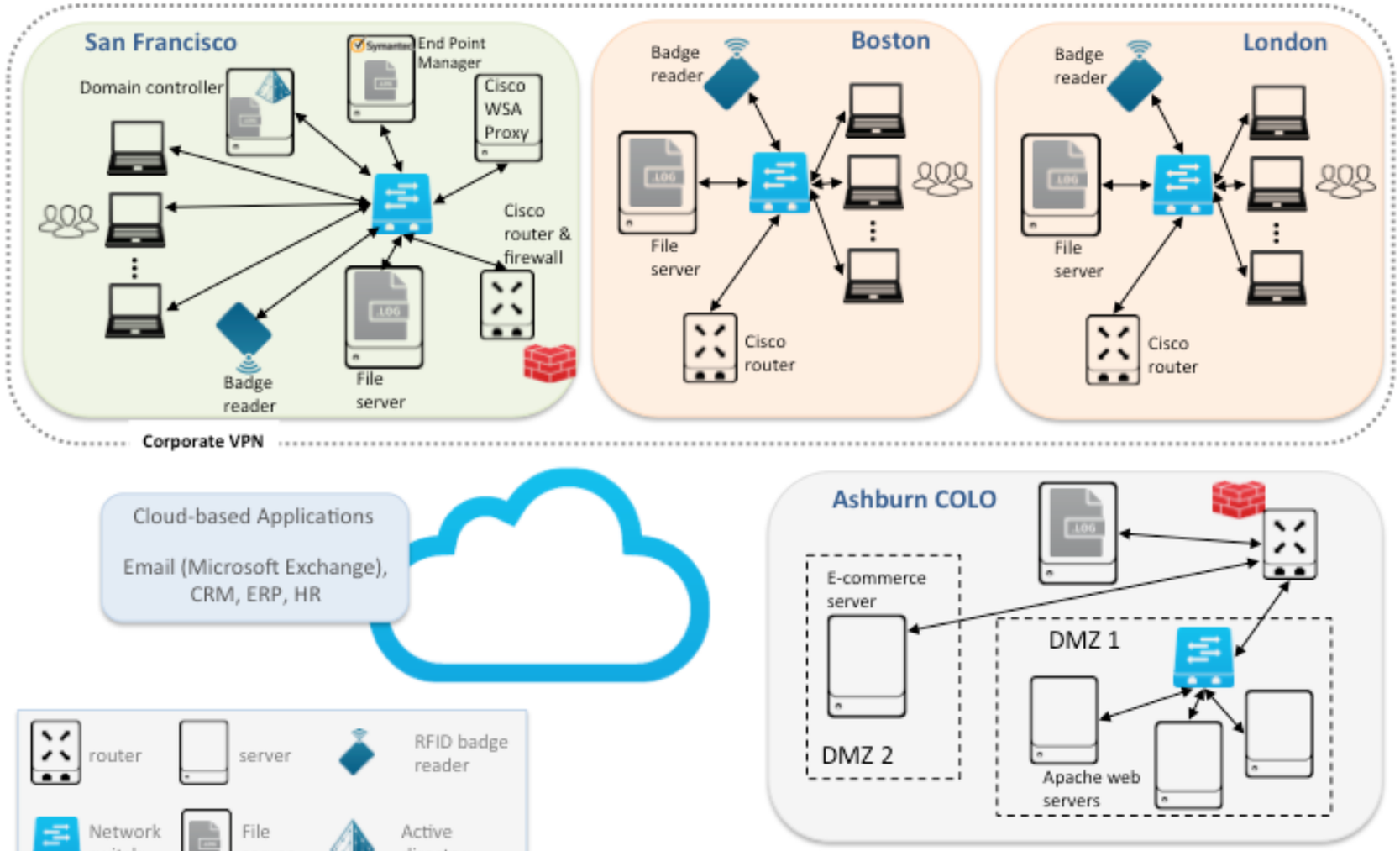
What should a Deployment Plan include?

- Deployment goals
- Data source inventory
- User roles / staffing list
- Data policy definition
- Physical topology diagrams
- Suggested Splunk apps
- Logging topology diagrams
- Education / training plan
- Splunk deployment topology
- Deployment schedule

Splunk Deployment Process

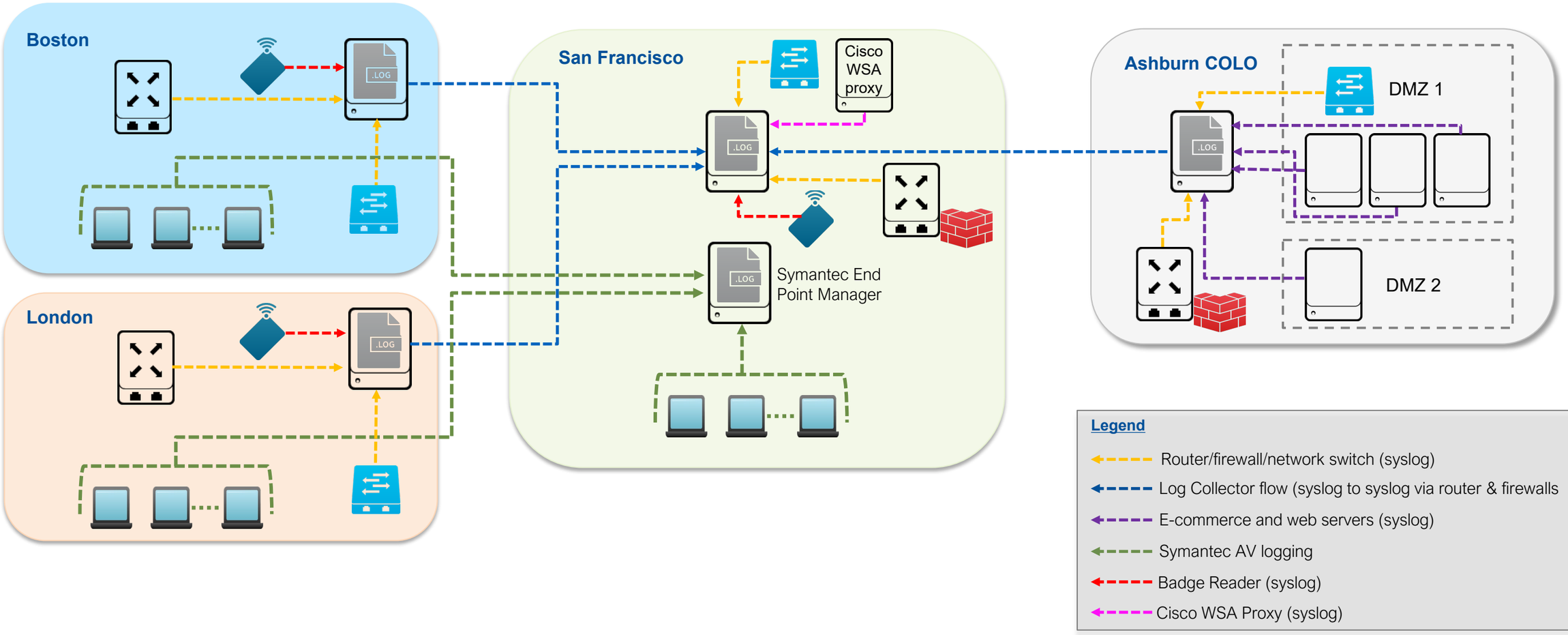


Buttercup Games (BCG) - IT Environment



 | 12 February 2021

BCG Logging Environment - Corporate



Module 1 Lab Exercise

Time: 10 minutes

Tasks:

- Read the lab document for Module 1 (pages 1- 4)
  - **`ArchSplunk_801_labs.pdf`**
  - If you have difficulty seeing the graphics in the lab document, they also appear on the previous pages
- Download planning tools
  - Data Source inventory (**`data_inventory.docx`**)
  - Index planning and sizing (**`data_sizing.xlsx`**)
  - Splunk icon library (**`SplunkIconLibrary.ppt`**)
  - Use case checklist (**`use_case.pdf`**)

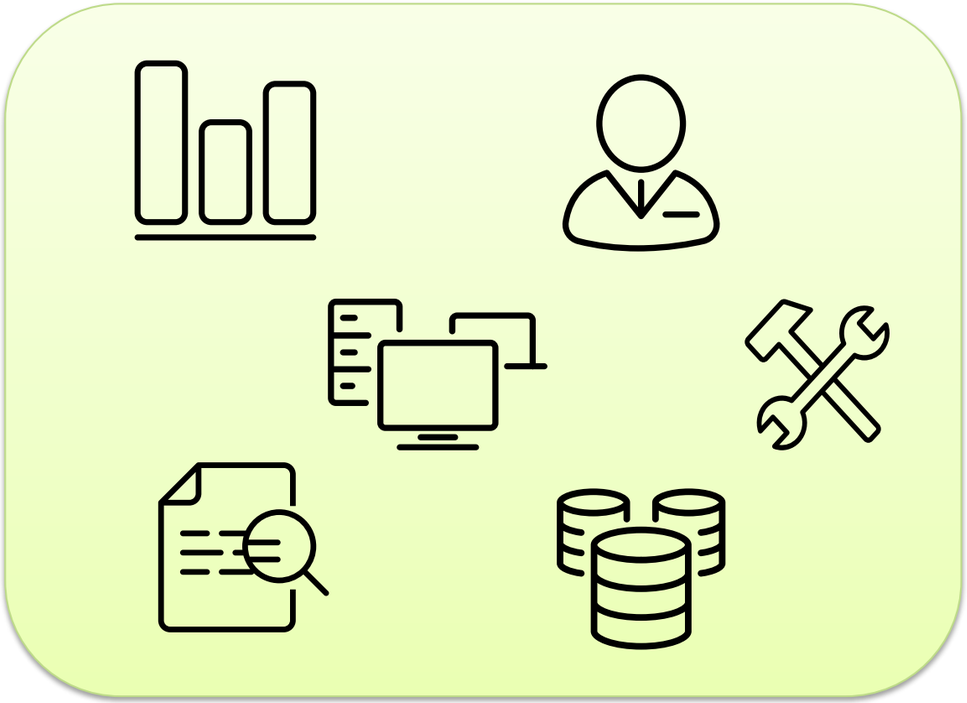
Module 2:
Project Requirements

Module Objectives

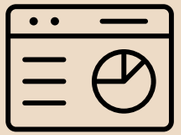
- Identify the information that is needed for deployment decisions
- Identify use cases
- Provide lists and resources to aid in collecting requirements

Key Planning Information

- Identify requirements
  - More information is uncovered throughout the phases of deployment
- Gather raw material for the deployment plan
  - Overall deployment goals
  - Key users, including their goals and use cases
  - Environment specifications
  - Monitoring tools in use
  - Expected daily data ingestion
  - Data sources



Use Cases



What will the users do with Splunk?

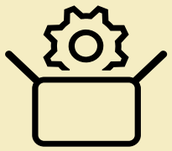
- Tasks performed? Reports generated? Other use cases?

Customer success stories:

- https://www.splunk.com/en_us/customers.html

Use Case Checklist handout

- View **`use_case.pdf`** (course material)

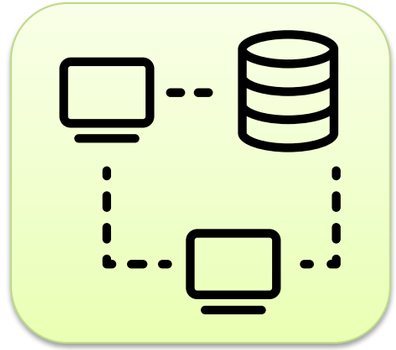


Splunk apps

- http://splunkbase.splunk.com

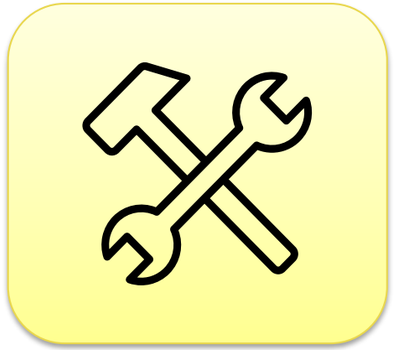
Current IT Environment

- **Overall IT topology?**
  - Data centers
  - Network zones
  - Number and type of servers
  - Location of users
- **Network diagram?**
  - Security restrictions
  - Bandwidth
- **Authentication systems?**
  - LDAP, RSA, etc.



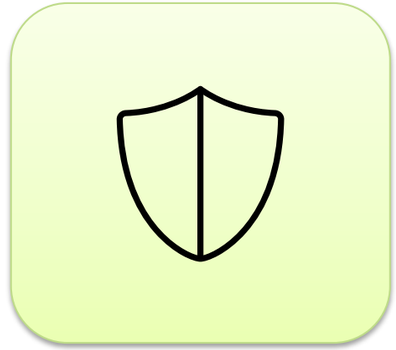
Current Logging Environment

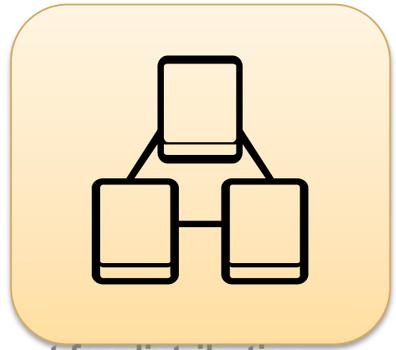
- **Collection and centralization?**
  - Logged to network devices
  - Centralized via syslog (or similar) tools
  - Parsed and stored in a SQL database
- **Tools in use?**
  - Log parsing / scraping tools or scripts
  - Query tools
  - Monitoring and ticketing systems
- **Splunk expectations?**
  - Integrating with existing tools
  - Replacing existing tools



General Requirements

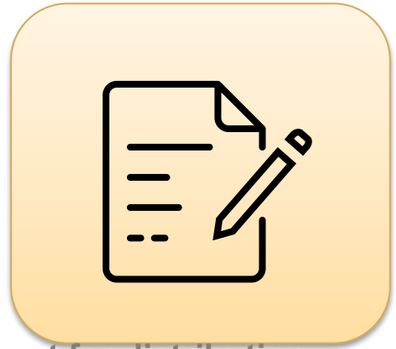
- **Security?**
  - Security policies that may affect collection, retention, and reporting of data
  - What approvals are needed? By whom?
- **Regulatory?**
  - Laws, regulations, or policies affecting data collection, reporting, and more
- **High Availability or Disaster Recovery?**
  - Data availability needs
  - Data replication requirements





Data Sources

- **Data source inventory?**
  - What is the superset of data sources needed by all users?
  - How much data is generated per day?
- **Data policy?**
  - How long should each data source be retained?
  - Who can see particular data elements?
  - What data needs protection against tampering?
  - What proof of integrity needs to be provided?
  - Will Splunk be the primary repository for data?
- **Handout:**
  - **`data_inventory.docx`**



Example Data Source Inventory

Data source:	Cisco ASA Firewall log
Data volume (Average):	500 MB / day
Data volume (Peak):	6000 EPS (events/sec) at ~100 bytes/event
Retention:	6 months
Visibility (Ownership and Access):	• Network team owns • Security has access
Collection method (*file, network, …*):	**`UDP:514`**
Location:	San Francisco office
Format / source type:	syslog?

Module 2 Lab Exercise

Time: 15 minutes

Task:

Complete the abbreviated data source inventory

- You may not know enough to supply answers for all data sources
- Part of the inventory has been completed for you
  - Do you agree with the completed portion?
  - Do you have questions for the sponsor?

Module 3: Index Design

Module Objectives

- Define index implementation
- Design indexes
- Estimate storage requirements for indexes
- Identify relevant apps and document impact on inputs and indexes

Indexing Review: Overview

- Optimized for quickly indexing and persisting unstructured data
- Parsed for line-breaking, timestamps and other metadata fields
- Persisted in its raw form, with minimal schema
- Provided as two types of indexes:

Index Type	Consists of	Ingest-based licensing
Events 	**rawdata** (raw text), **timestamp**, **source**, **source type** and **host**	Measured as data (full size) that flows through parsing pipeline
Metrics 	**timestamp**, **metric name** (e.g. “os.cpu.user”), **value**, **dimensions** (for grouping, e.g. “region”)	Measurement capped at 150 bytes per metric event

For more on Metrics, refer to: docs.splunk.com/Documentation/Splunk/latest/Metrics/Overview

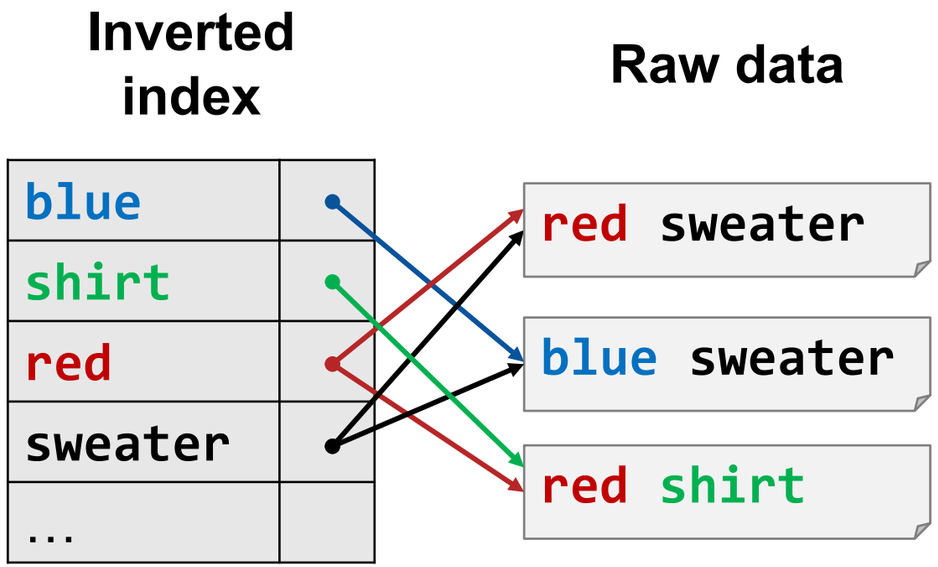
Indexing Review: Index Time Processing

- Defer additional processing on raw events until search time
  - Increases indexing speed
  - Requires less effort
  - Maintains original data
  - Resilient to change

Inverted Index

- A type of index data structure
- Allows fast full text searches
- Maps from content (such as words or numbers) to their locations

  en.wikipedia.org/wiki/Inverted_index
- Used to map keywords to location in the raw data by Splunk **`.tsidx`** files



Source: Wikipedia

Event Index Review: File Types

rawdata

Index files (`.tsidx`)

Metadata (`.data`)

Bloom filters

Example files in a Splunk index warm bucket:

```
$ ls -l SPLUNKDB/<index_name>/db/<bucket_name>
drwx--x---  3 root root 4.0K Sep 11 22:10 .
drwx------ 31 root root 4.0K Sep 14 23:15 ..
-rw-------  1 root root  30K Sep 11 22:06 1505167548-1505166495-2478884372982387461.tsidx
-rw-------  1 root root 1.5K Sep 11 22:06 bloomfilter
-rw-------  1 root root   75 Sep 11 22:10 bucket_info.csv
-rw-------  1 root root  249 Sep 11 22:05 Hosts.data
drwx------  2 root root 4.0K Sep 11 22:05 rawdata
-rw-------  1 root root    6 Sep 11 22:05 .rawSize
-rw-------  1 root root  483 Sep 11 22:05 Sources.data
-rw-------  1 root root  175 Sep 11 22:05 SourceTypes.data
-rw-------  1 root root  305 Sep 11 22:05 Strings.data
```


Event Index Review: Rawdata

rawdata

Index files (`.tsidx`)

Metadata (`.data`)

Bloom filters

- Contains original data in compressed form
- Size is dependent on how well data compresses
- For "syslog-like" data, size is ~10-15% of pre-indexed data
- Exists for all replicated buckets

Event Index Review: Index Files (`.tsidx`)

rawdata

Index files (`.tsidx`)

Metadata (`.data`)

Bloom filters

- Required for searchable buckets
- Points to unique terms in raw data
- Size is ~10-110% of raw data (affected by number of unique terms)
- Uses *inverted index* format for fast full text searches

Note

Adding indexed field extractions increases size of `.tsidx` files

Event Index Review: Metadata (`.data`)

rawdata

Index files (`.tsidx`)

Metadata (`.data`)

Bloom filters

- Information about sources, source types and hosts of the events contained in each bucket

Event Index Review: Bloom filters

rawdata

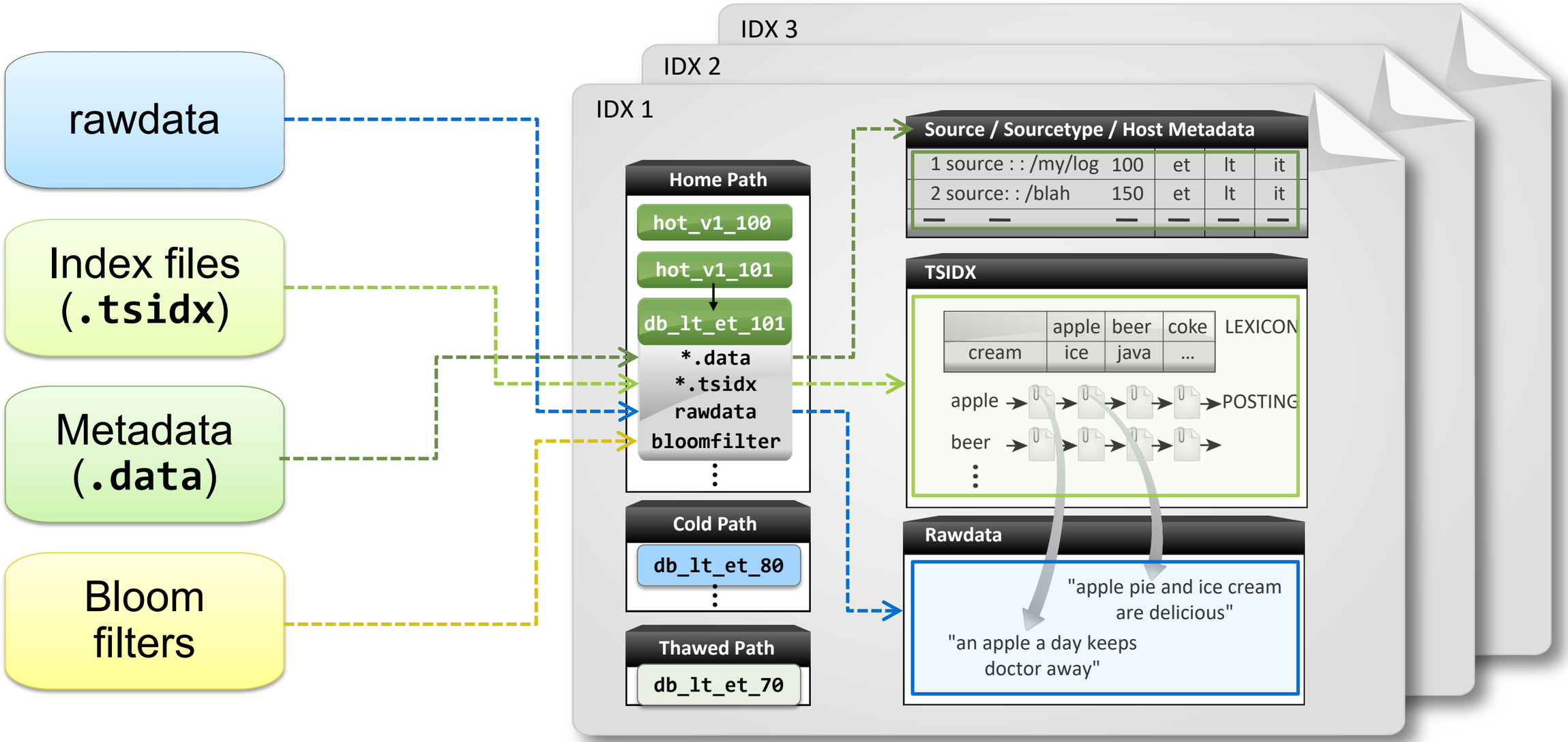
Index files (`.tsidx`)

Metadata (`.data`)

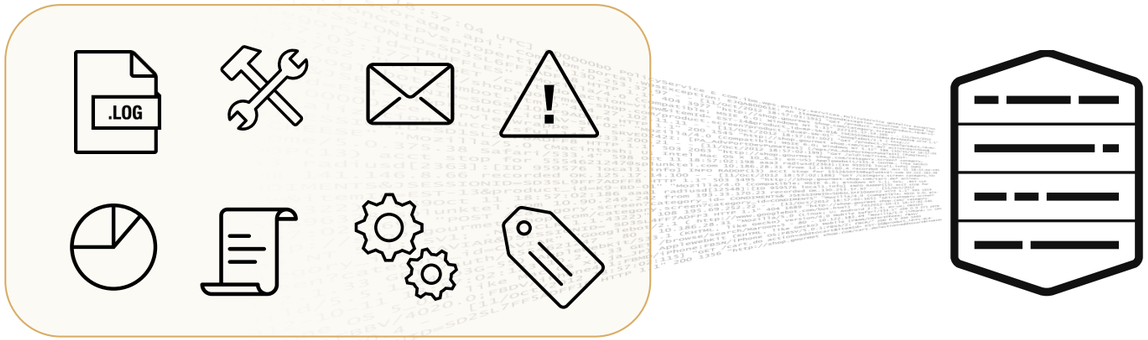
Bloom filters

- Efficient data structure that provides 100% certainty that a search term is ***not*** present in a bucket
- Consulted by every search
- Very fast (1-2 I/O)
  - Refer to https://en.wikipedia.org/wiki/Bloom_filter
- Created as a bucket rolls from hot to warm

Splunk Index Files



Estimating Indexing Volume



Estimate input volume

- Verify raw log sizes
- Daily, peak, retained, future volume
- Total number of data sources and hosts
- Add volume estimates to data source inventory / spreadsheet

Estimate index volume size

- For “syslog”-type data, index occupies ~50% of original size
- 15% for rawdata (compression)
- 35% for associated index files

Testing Indexing Compression

- Confirm estimates with actual data
  - Create a baseline with simulated or (preferably) real data
  - Find compression rates
  - Leverage **`_internal`** index metrics to determine actual input volumes
- To test specific data types:
  1. Index a sample of data (at least two buckets)
  2. Check the sizes of the resulting directories in **`defaultdb`**
- Get baseline compression rates in the Monitoring Console:

For step-by-step space estimation method:
docs.splunk.com/Documentation/Splunk/latest/Capacity/Estimateyourstoragerequirements

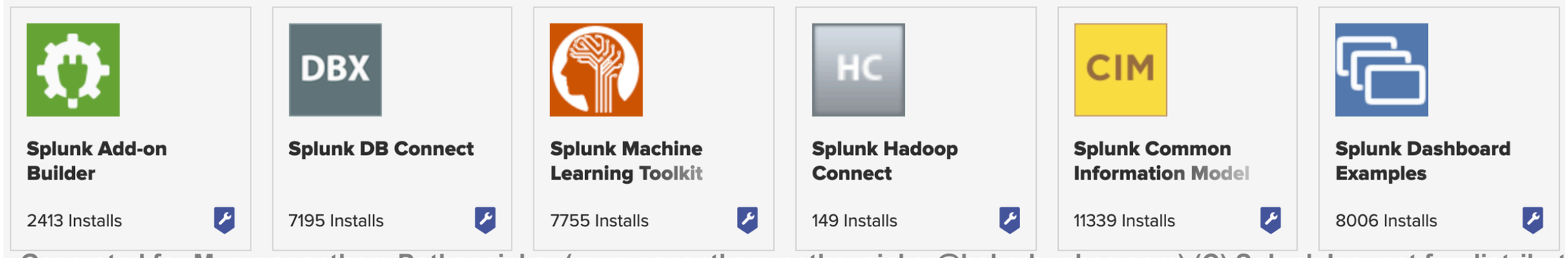
Apps and Indexes

- Apps may define inputs and indexes
- Understand the effect of the app on the environment
  1. Identify new inputs and indexes
     - Acquire any new data sources required to support the app
  2. Determine inputs-to-index mappings
     - Avoid overlaps and conflicts
     - Generally, a data source goes to a single index
     - Identify new sourcetype defined by the app
  3. Update index design and data source inventory
     - Integrate apps with overall design

Splunk Apps

- Often chosen based on devices, technologies, use cases, or inputs
- May have infrastructure requirements
- Most are free
- Can be added dynamically, but plan up front when possible

http://www.splunkbase.com



Key Criteria for Using Separate Indexes

Index Data Type

- What type of data is being ingested?
- Events versus Metrics

Retention

- How long the data is kept? Online / Offline?
- All retention settings apply per-index to all data sources

Access

- Who can search against the data?
- All index data has the same visibility (determined by Splunk role)

Additional Design Criteria

- Search Performance
  - Less common to differentiate here, but *may* be important
  - Mixed data = mixed lexicon, larger number of keywords, therefore larger index
  - Things searched together can be indexed together
  - Example:
    - Both a high-volume / high-noise data source and a low-volume data source feed into the same index
    - If you search mostly for events from the low-volume data source, the search speed will be slower than necessary
    - To improve performance, create a separate index for the high-volume data source

Module 3 Lab Exercise

Time: 15 minutes

Tasks:

- Estimate the disk space required
- Index design
  - Identify the indexes
  - Estimate the Splunk license required for indexing

Challenge:

- Identify potential apps
  - Identify apps for the environment
  - Add any index and input information from the apps to your solution

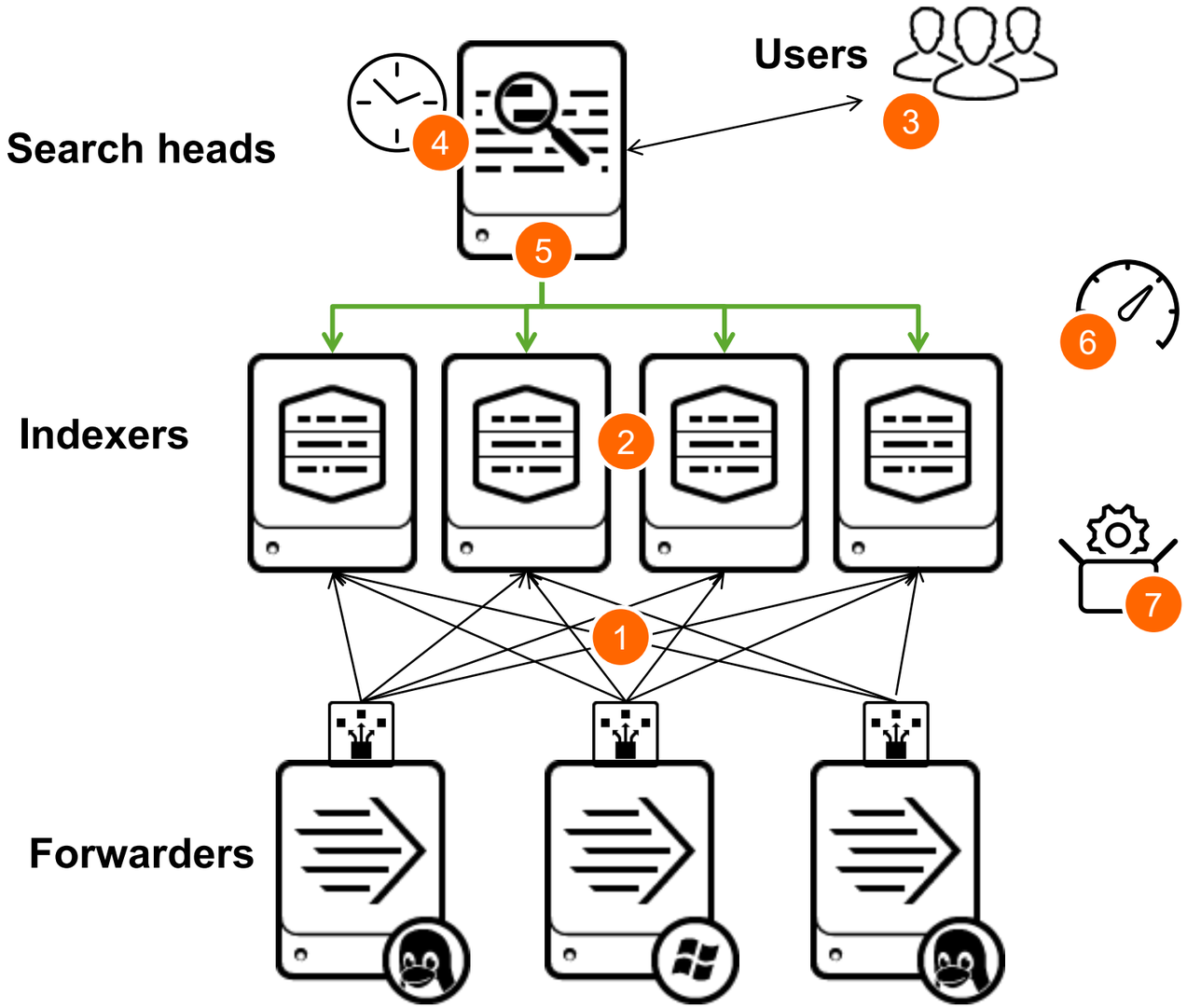
Module 4: Resource Planning

Module Objectives

- Determine sizing based on Splunk usage
- Define reference server requirements for:
  - Indexers
  - Search heads
  - Other Splunk components
- Describe deployment options such as virtualization and cloud
- Describe the impact of acceleration and apps on resource sizing

Basic Sizing Considerations

1. Amount of incoming data
2. Amount of indexed (stored) data
3. Number of concurrent users
4. Number of scheduled searches
5. Types of searches
6. Acceleration
7. Specific Splunk apps

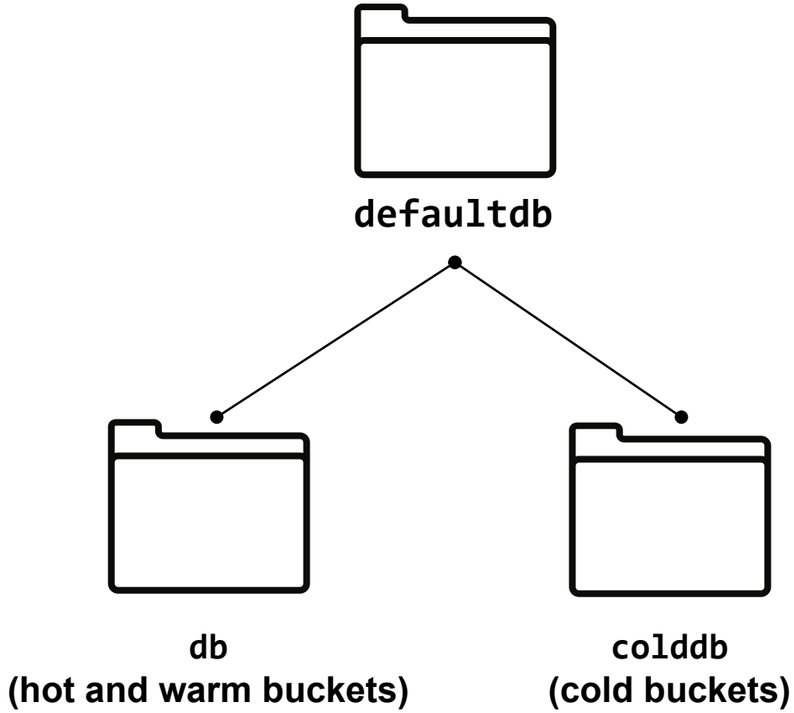


Disk Storage Details – About IOPS

- Input/Output Operations Per Second (IOPS)
  - Measures disk throughput
  - A blend of read and write speed
  - Should be prioritized for hot and warm buckets
- Splunkbase app to analyze disk performance: Bonnie++
  - https://splunkbase.splunk.com/app/3002/
- Links to additional information on determining IOPS
  - www.symantec.com/connect/articles/getting-hang-iops-v13
  - www.cmdln.org/2010/04/22/analyzing-io-performance-in-linux

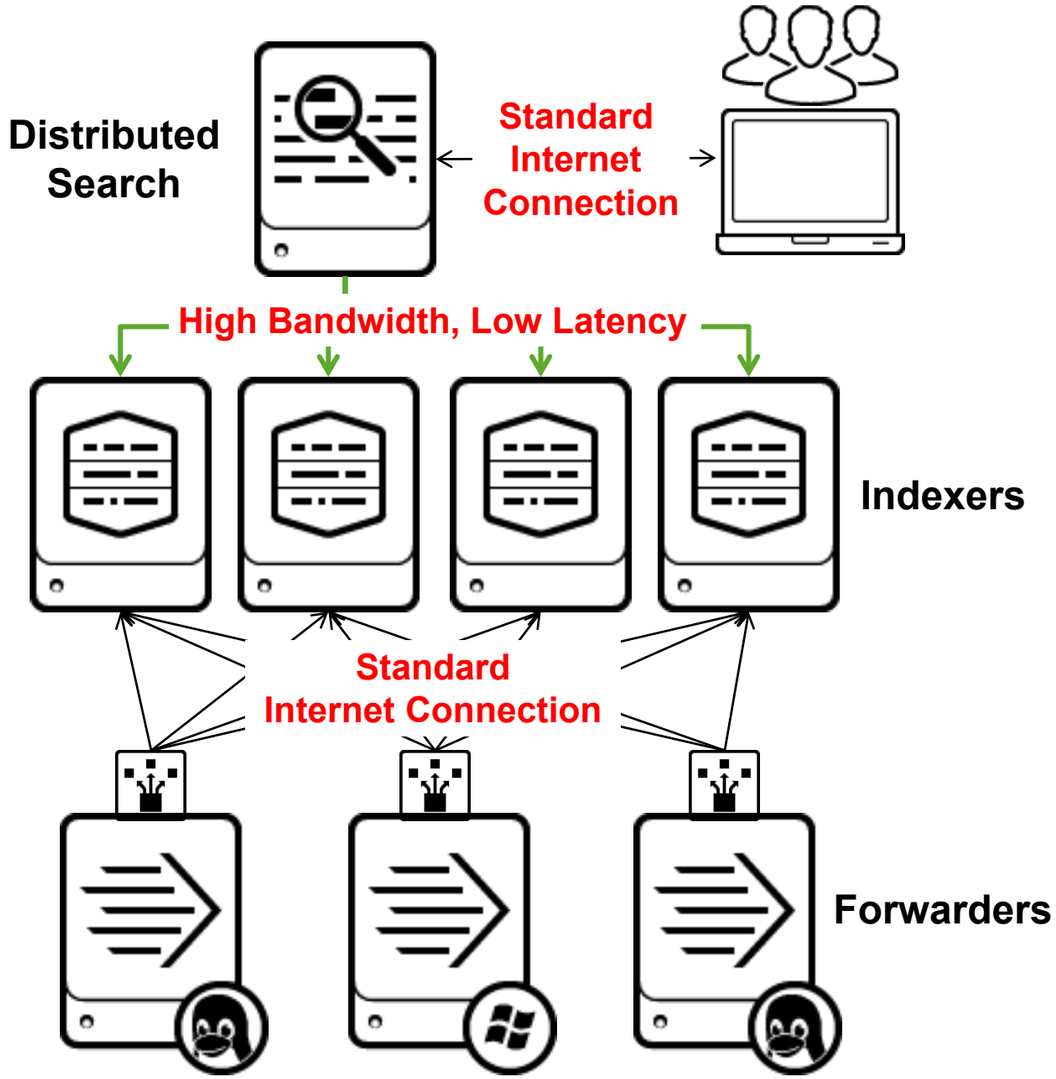
Disk Storage Details – SAN and NAS

- Storage Area Networks (SAN) and Network-attached Storage (NAS)
  - Avoid for hot and warm buckets (**db**)
  - Suitable for cold buckets (**colddb**), but may cause slower searches for older data
- High performance SAN can be used
  - High speed networking and low latency
  - **IOPS** and **reliability** are the definitive factors



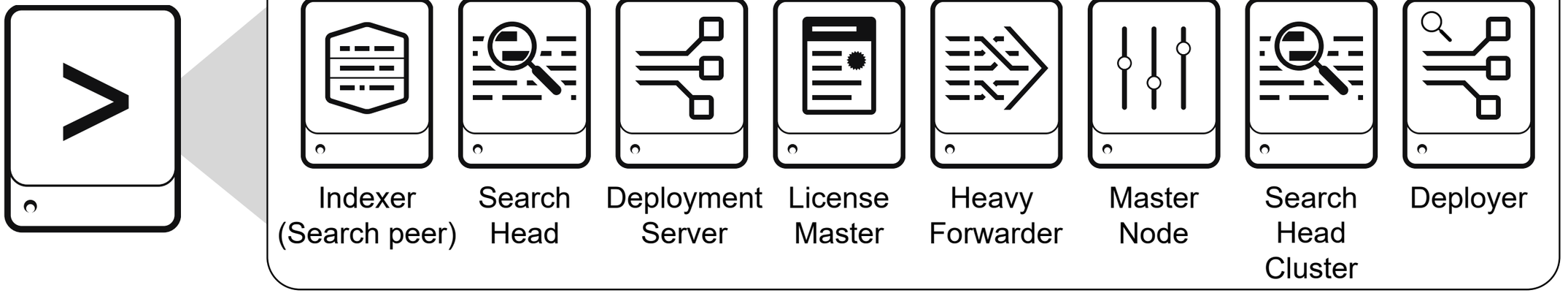
Foundation for Splunk Deployment

- Low latency network
  - Minimum bandwidth: 1 Gbps
  - Search head cluster, SH to SH: < 200ms
  - Indexer to indexer: < 100ms
- Enterprise-wide time sync (NTP)
- Domain Name Service (DNS)
- On Linux:
  - Turn off Transparent Huge Pages (THP)
  - Increased **`ulimit`** settings

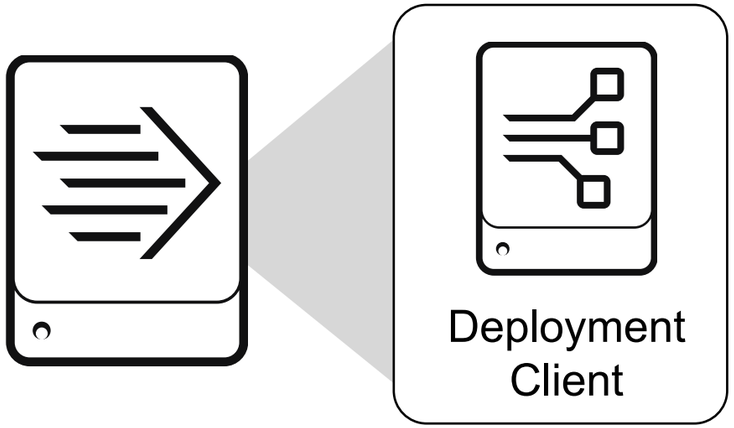


Splunk Components

Splunk Enterprise package



Universal Forwarder package



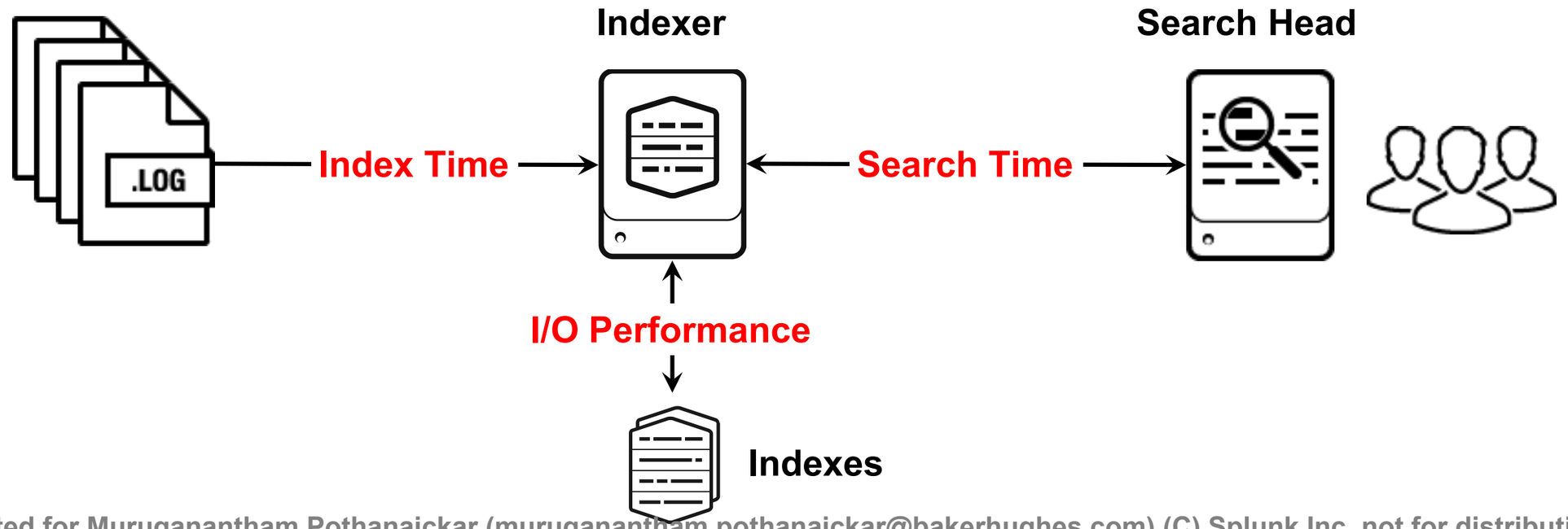
Note

The heavy forwarder and universal forwarder are discussed in Module 6.

 | 12 February 2021

Component Types – Indexer

- Indexes data, transforming raw data into **events** and placing the results into an **index**
- Searches the indexed data in response to search requests



Indexer – (Single Instance) Reference Server

- Based on reference hardware:
  - Ingest up to 300GB/day
  - Simultaneously supports a standard search load
- Indexing
  - Can use **4** full cores at full load
- Searching
  - Uses **1** core per concurrent search
- Additional servers can:
  - Reduce search duration
  - Increase search throughput
  - Increase user capacity

Component	Reference hardware
Hardware	Intel 64-bit chip architecture
CPU	12 cores (2+ GHz/core)
Memory	12 GB RAM
Disk	**800+ IOPS** SAS drives in RAID 1+0
Network	1Gb Ethernet NIC (optional 2nd NIC - management network)
OS	Linux or Windows 64-bit distribution

Indexer – (Single Instance) Max Performance

- Indexing performance
  - Up to 20MB per second (1700GB/day) of raw indexing performance
    - Does not include search or other index related activity
- Search performance
  - Up to 50,000 events/second for dense searches
  - Up to 5,000 events/second for sparse searches
  - Up to 2 seconds/index bucket for super-sparse searches
  - From 10 – 50 buckets/second for rare searches with bloom filters

> **Note**
>
> This information is based on the reference server specifications on the previous page.

For more information about how searches impact performance, read:
docs.splunk.com/Documentation/Splunk/latest/Capacity/HowsearchtypesaffectSplunkEnterpriseperformance

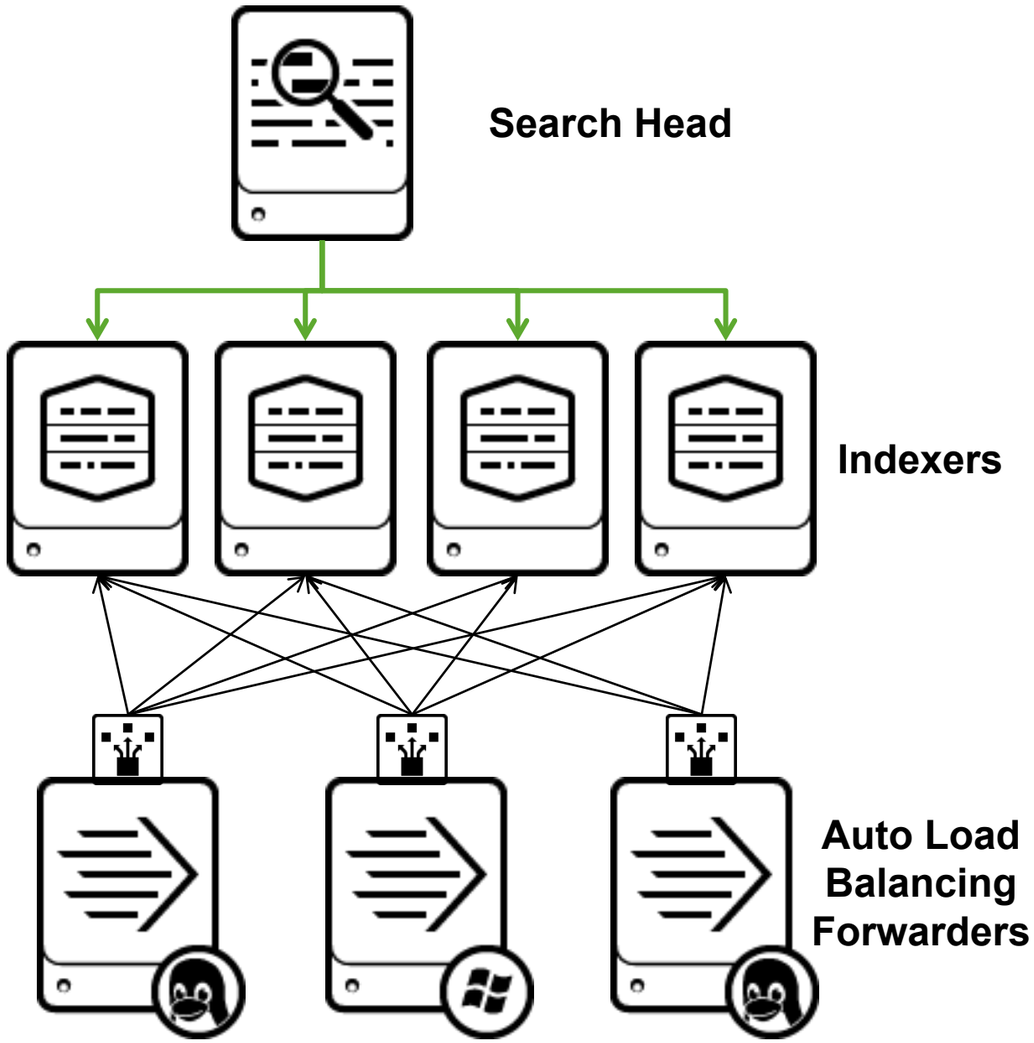
Indexer – Reference Server Specifications

Component	Reference	Mid-range	High-performance
Hardware	Intel 64-bit chip architecture		
CPU	**12** cores (2+ GHz/core)	**24** cores (2+ GHz/core)	**48** cores (2+ GHz/core)
Memory	**12** GB RAM	**64** GB RAM	**128** GB RAM
Disk	**800+** IOPS SAS drives in RAID 1+0	**800+** IOPS SAS drives in RAID 1+0	**1200+** IOPS Solid State Drives (SSDs)
Network	1Gb Ethernet NIC (optional 2nd NIC for a management network)		
OS	Linux or Windows 64-bit distribution		

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

Horizontal Scaling

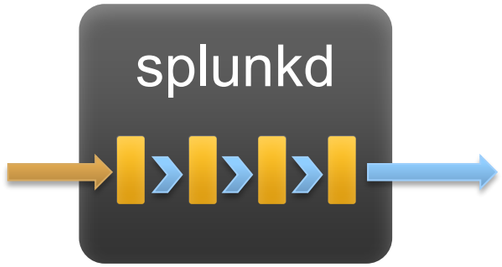
- Adding indexers scales capacity
  - Allows greater daily indexing volume
  - Speeds searches
- When using multiple indexers
  - Use Splunk's built-in forwarder load balancing
  - Use distributed search
- When scaling, first step is to look at adding another commodity indexer



Increasing Index Parallelization

Single pipeline

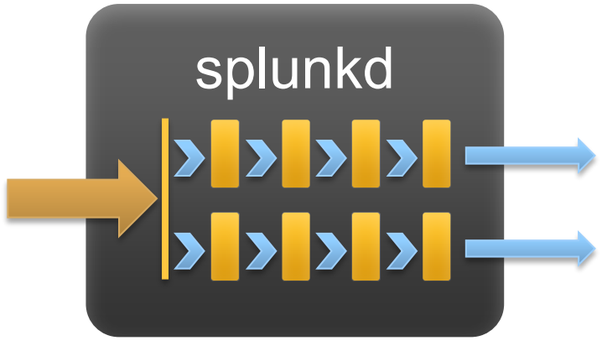
- Default behavior
- Uses approximately 4-6 cores for indexing



Single pipeline set

Multiple pipelines

- Increases hardware utilization (and system resources)
- Uses additional 4-6 cores for indexing
- Use on CPU and I/O-underutilized indexers and intermediate forwarders
- Eventually moves bottleneck from cores (pipeline) to disk



Multiple pipeline set

Storage Requirements

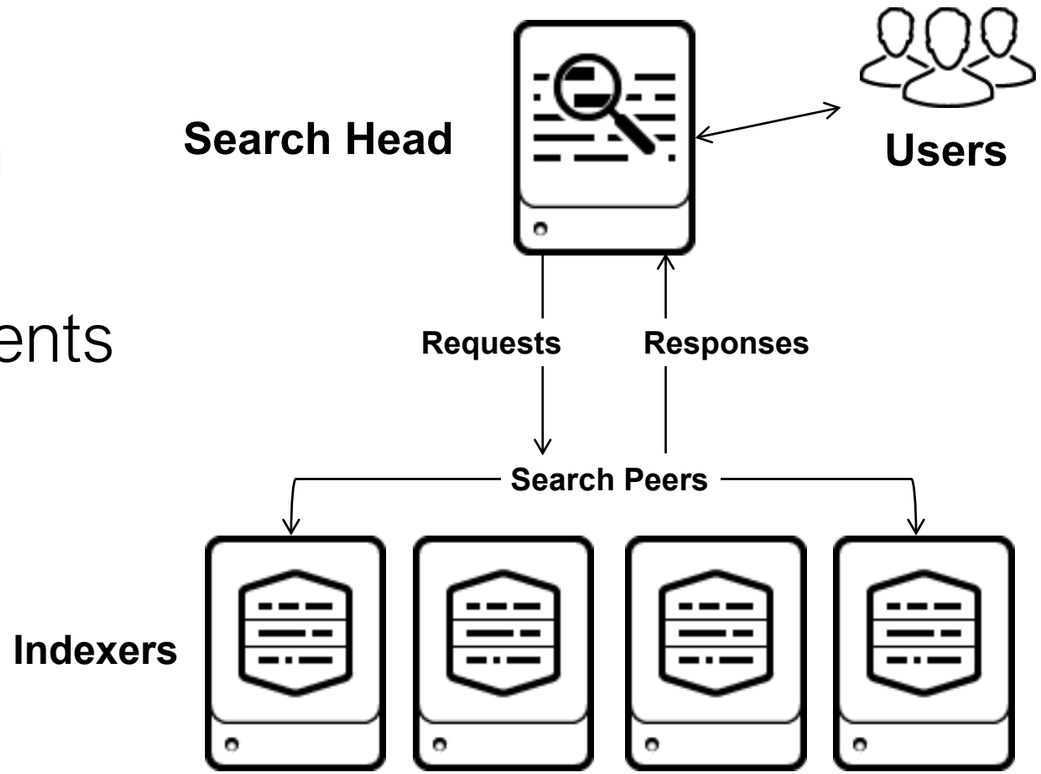
- Disk storage for indexer is primarily determined by:

  (size of all indexes) + (base storage for OS) + (configuration files)

- Additional disk storage is needed for
  - Indexer Clustering's
    - Data replication
    - Discussed in a later module
  - Summarization and Acceleration
    - Data models
    - Report acceleration
    - Summary indexing
    - Refer to appendix B for more information

Component Types – Search Head

- Handles search management functions
  - Directs search requests to a set of search peers (indexers)
  - Federates or merges the results and presents them to the user



Search Head – Reference Server

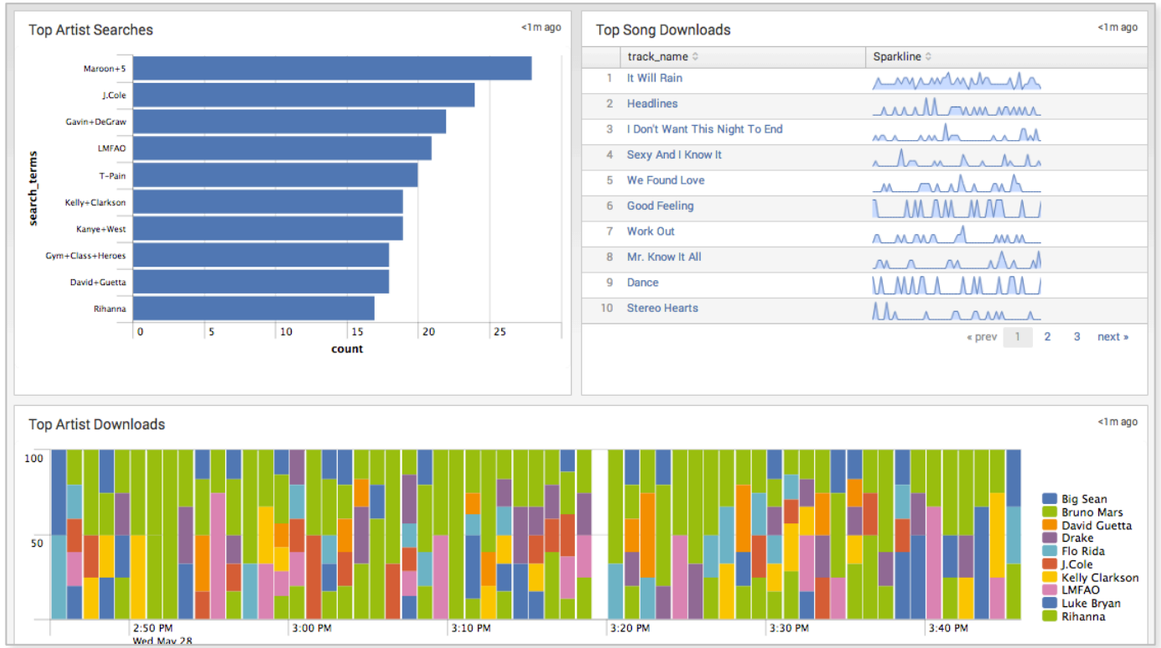
- Requires more CPU than an indexer
- Uses 1 CPU core while the search is active for each search request
  - More users / concurrent searches require additional CPU cores
- Search heads mostly aggregate results
  - Some types of searches may create bottlenecks
- Account for scheduled searches in addition to ad-hoc searches

Search Head

Component	Reference hardware
Hardware	Intel 64-bit chip architecture
CPU	16 cores (2+ GHz/core)
Memory	12 GB RAM
Disk	**2 x 300GB**, **10,000 RPM** SAS hard disks, configured in RAID 1
Network	1Gb Ethernet NIC (optional 2nd NIC - management network)
OS	Linux or Windows 64-bit distribution

Sizing Factors for Searching

- Number of searches
  - Concurrent & total
- Number of users
  - Concurrent
- Types of searches
  - Reporting, dashboard, ad-hoc
- Jobs
  - Summarization, Alerting, Reporting
- Acceleration
  - Report, Summary Indexing, Data Model
- Apps may increase the search load
  - Real time and/or scheduled searches may be features of apps
- Plan for expansion as adoption grows



Daily Indexing Volume Guidelines

Total Users	Daily rate →	< 2GB	2 - 300 GB	300 - 600 GB	600 GB - 1 TB	1 - 2 TB	2 - 3 TB
	< 4	1 combined instance	1 combined instance	1 Search head 2 Indexers	1 Search head 3 Indexers	1 Search head 7 Indexers	1 Search head 10 Indexers
	Up to 8	1 combined instance	1 Search head 1 Indexers	1 Search head 2 Indexers	1 Search head 3 Indexers	1 Search head 8 Indexers	1 Search head 12 Indexers
	Up to 16	1 Search head 1 Indexers	1 Search head 1 Indexers	1 Search head 3 Indexers	2 Search head 4 Indexers	2 Search head 10 Indexers	2 Search head 15 Indexers
	Up to 24	1 Search head 1 Indexers	1 Search head 2 Indexers	1 Search head 3 Indexers	2 Search head 6 Indexers	2 Search head 12 Indexers	3 Search head 18 Indexers
	Up to 48	1 Search head 2 Indexers	1 Search head 2 Indexers	2 Search head 4 Indexers	2 Search head 7 Indexers	3 Search head 14 Indexers	3 Search head 21 Indexers

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

Additional Component Types

Component	Description
License Master	• Allocates licensing capacity / manages licensing usage for all instances • Contacted over network frequently by license slaves (which should be all indexers, search heads, Master Nodes, deployers and deployment servers)
Deployment Server	• Manages Splunk configuration files for deployment clients • Operates on a "pull" model – clients "phone home" at intervals over network
Master Node	Regulates the functioning of an indexer cluster
Deployer	Distributes configurations to search head cluster members

Additional Components: Sizing

Component	CPU	Memory	Disk	Network	Factors
License Master	Low	Low	Low	1 Gb	# of slaves
Deployment Server	Med*	Med*	Low	1 Gb	# of clients # of apps + config files * CPU+Mem can spike during downloads
Master Node	Med	Med	Low	1 Gb	required for indexer cluster
Deployer	Low	Low	Low	1 Gb	number of SHC members

- Splunk recommends that you dedicate a host for each role
  - Enable multiple Splunk server roles on a server with caveats
- Master Node and Deployer are discussed in more detail in the Clustering section

Virtualizing Splunk

- Any Splunk instance can be virtualized
- Tips for virtualization
  - Ensure minimum resource requirements are met and reserved
    - Do not overcommit CPU or memory
  - Use locally attached volumes; direct access to a dedicated volume is best
  - Separate search head VMs from indexer VMs
    - Together they can cause CPU activity bursts
  - Plan for performance reduction by 10-15%
- Refer to the virtualization tech brief:
  - splunk.com/pdfs/technical-briefs/splunk-deploying-vmware-tech-brief.pdf

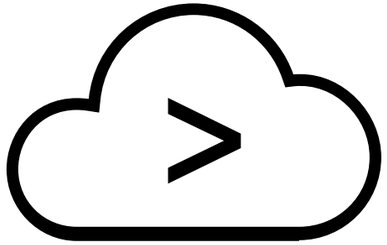
Splunk Enterprise in the Cloud (Self-managed)

- Offers similar performance to bare-metal hardware, but dependent on vendor provisioning the instance

  - On AWS:
    - Measures CPU on Elastic Compute Cloud (EC2) instances in virtual CPUs (vCPUs)
    - Generally, each vCPU is a hyper thread of an Intel Xeon core
  - Indexing and data storage considerations
    - Elastic Block Storage (EBS) volume determines performance
    - Not all EBS volume types provide necessary IOPS
    - Provisioned IOPS and Magnetic EBS volume types are recommended
    - Verify EC2 instance type offers needed network throughput

Splunk Cloud

- Subscription service to store, index and search data
- Cloud resources are managed and maintained by Splunk
  - Contact Splunk Cloud Support to scale your deployment
- Data is sent to Splunk Cloud via Forwarders and HTTP Event Collector (HEC)

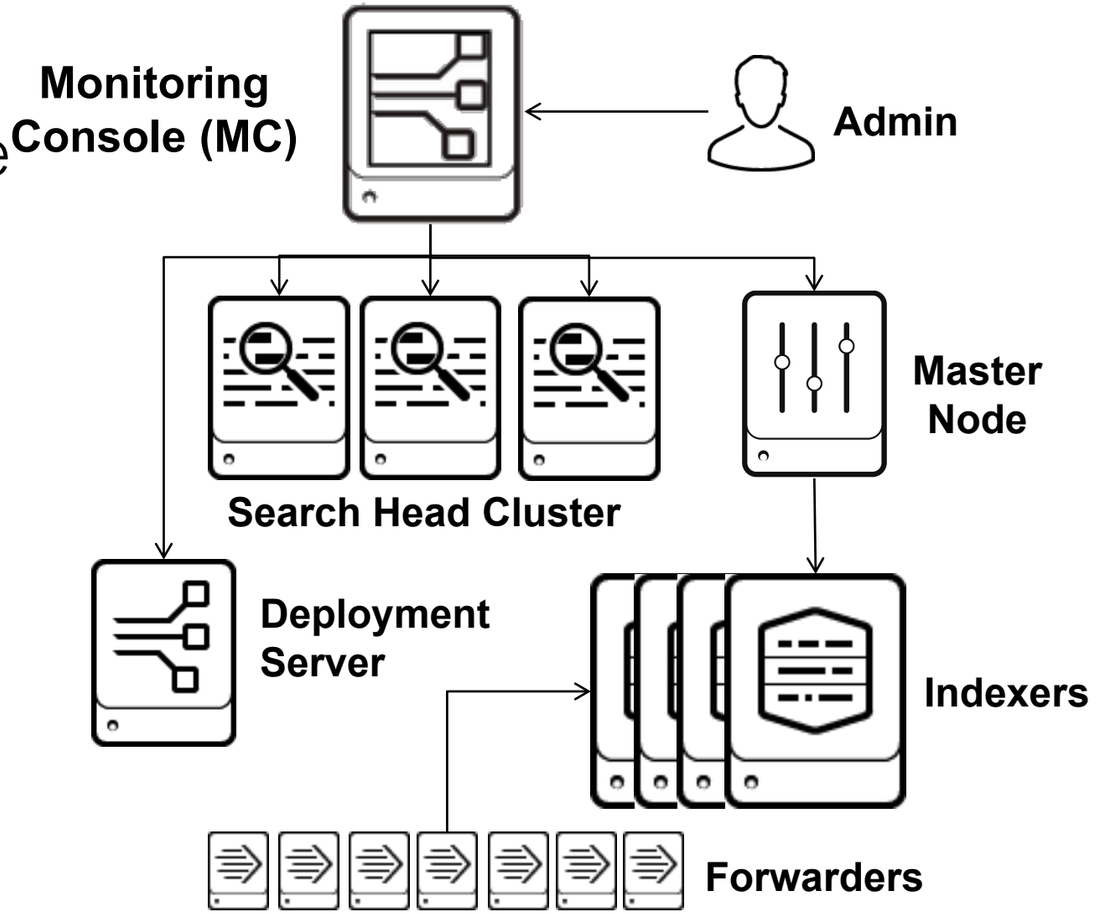


Note

If you are using Splunk Cloud in your environment, attending the *Splunk Cloud Administration* course is recommended.

Monitoring Console (MC) App

- Monitoring tool for Splunk Enterprise
- Provides detailed topology and performance information
- Should run on a dedicated search head
  - Follow the SH reference server guidelines
  - Should not run on a production SH
  - Can run on a shared instance with caveats
- Only admins should access
- Forward all internal indexes (internals and summaries) to the indexing tier



docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview

Acceleration Review

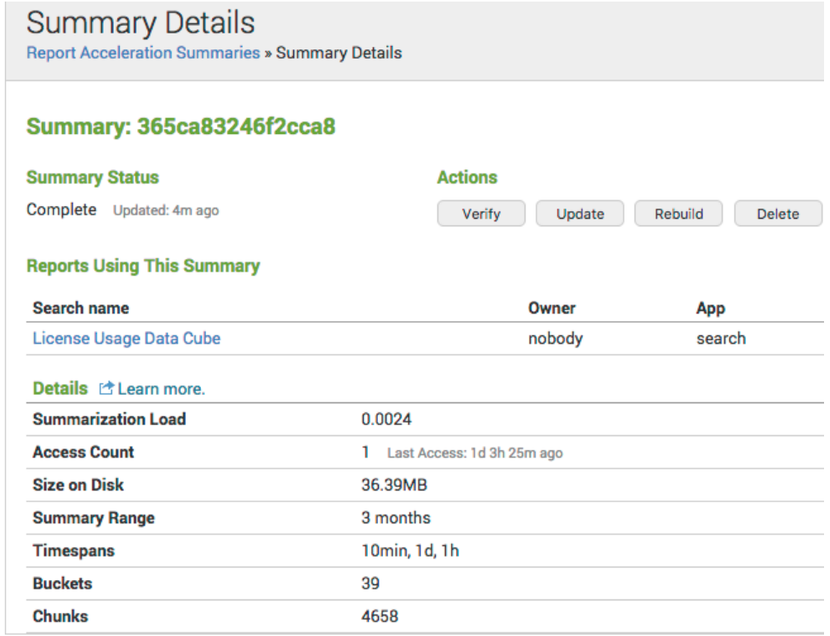
Report Acceleration	• **Accelerates individual reports** • Easier to create than summary indexes and backfills automatically • Always ages out when corresponding data ages out • Runs every 10 minutes
Summary Indexing	• **Accelerates reports that don't qualify for report acceleration** • Uses manually created summary indexes that exist separate from main indexes • Backfill is a manual (scripted) process • Runs when configured to
Data Model Acceleration	• **Accelerates all of the fields defined in a data model** • Backfills automatically • Always ages out when corresponding data ages out • Runs every 5 minutes

Report Acceleration and Disk Sizing

- Exists on the indexer tier, in parallel with the buckets that contain the events
- Uses unlimited disk space, by default
  - Location and maximum size is set in **`indexes.conf`**
  - Location specified with **`summaryHomePath`**
  - Default location:

    `SPLUNK_HOME/var/lib/splunk/`*`indexName`*`/summary`
- Managed from Splunk Web in **Settings > Report Acceleration Summaries**

> **Note**
>
> By default, the user and power user roles have the *accelerate_search* capability to accelerate reports.



docs.splunk.com/Documentation/Splunk/latest/Knowledge/Manageacceleratedsearchsummaries

Summary Indexing Review

What is summary indexing?

- Efficiently report on large volumes of data
- Spread the cost of a computationally expensive report over time
  - Run reports over long time ranges for large datasets more efficiently
- Retain summarized data after original data sources have been frozen
- Defined at docs.splunk.com/Documentation/Splunk/latest/Knowledge/Usesummaryindexing

How does it work?

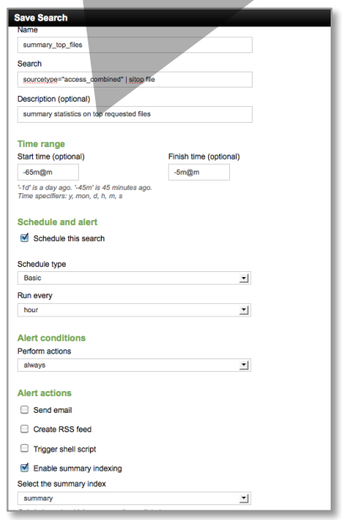
- Data is collected and summarized
  - A populating search is scheduled to run periodically
  - The populating search stores its results in a summary index
- Reports are run against the summary index
  - Searches run faster over the smaller summary index
  - The summary index may be used to report when data ages out of the original index

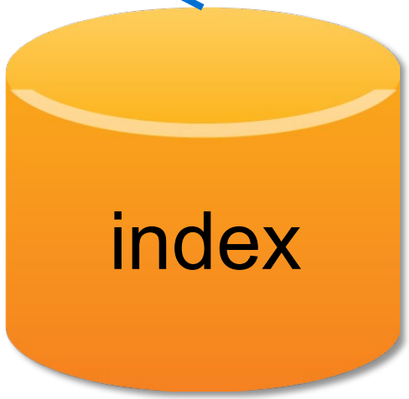
Summary Indexing Flow

purchasedProducts search Populating Search

```
sourcetype=access_combined | sistats count by product_name
```

Run every hour, time range 1 hour





Populating search results are formatted and stored as statistics

	product_name	psrsvd_gc	psrsvd_v
1	Birthday Bouquet	2139	1
2	Cake Serving Set	2185	1
3	Chocolate Dreams Confections	2174	1
4	Day Spa Certificate	2210	1
5	Dozen Red Roses	2096	1
6	Greetings Fruit Basket	2087	1
7	Mixed Rose Bouquet	2196	1
8	Sweet Dreams Bouquet	2117	1
9	Sweet Splendor Bouquet	2143	1
10	Tulip Bouquet	2173	1

Search

```
index=summary search_name=purchasedProducts | stats count by product_name
```

Last 30 days

 | 12 February 2021

Forwarding Summary Indexes

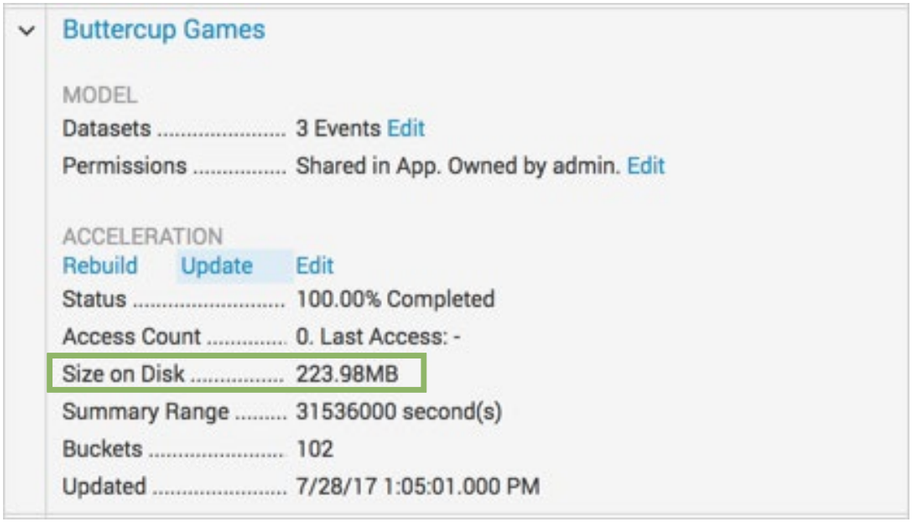
- Summary indexes are created on the search head by default
- If you use summary indexes, forward your summary indexes to the indexing layer
  - Configure **`outputs.conf`** on the search head to forward to indexers
  - This allows all members to access them
    - Otherwise, they're only available on the search head that generates them
  - This is *required* for search head clustering
- Configure the search head as a forwarder

splunk> Best Practice

http://docs.splunk.com/Documentation/Splunk/latest/DistSearch/Forwardsearchheaddata

Disk Usage: Data Model Acceleration

- Data model acceleration summaries are stored on the indexer in buckets next to raw data
- By default, accelerations can use an unlimited amount of disk space
  - Set up size-based retention for data model acceleration summaries in `indexes.conf`:
    - `maxVolumeDataSizeMB = volume size`



- To see the size on disk of a particular data model acceleration, go to **Data Models** > *[data model name]*

docs.splunk.com/Documentation/Splunk/latest/Knowledge/Acceleratedatamodels

How Apps Affect Infrastructure Sizing

- Review the documentation for each app
  - Identify any impact on the Splunk deployment
- For example
  - Splunk App for Enterprise Security places a heavy load on search heads
  - Splunk IT Service Intelligence requires a dedicated search head or search head cluster

Note

Refer to Appendix B for detailed information about Premium App resource requirements

Staging & Testing Environments

- Part of your Splunk deployment should include a separate "sandbox" or testing / staging environment
  - Same version of Splunk in production is preferred
- Sizing the testing environment depends on types of tests

splunk> Best Practice

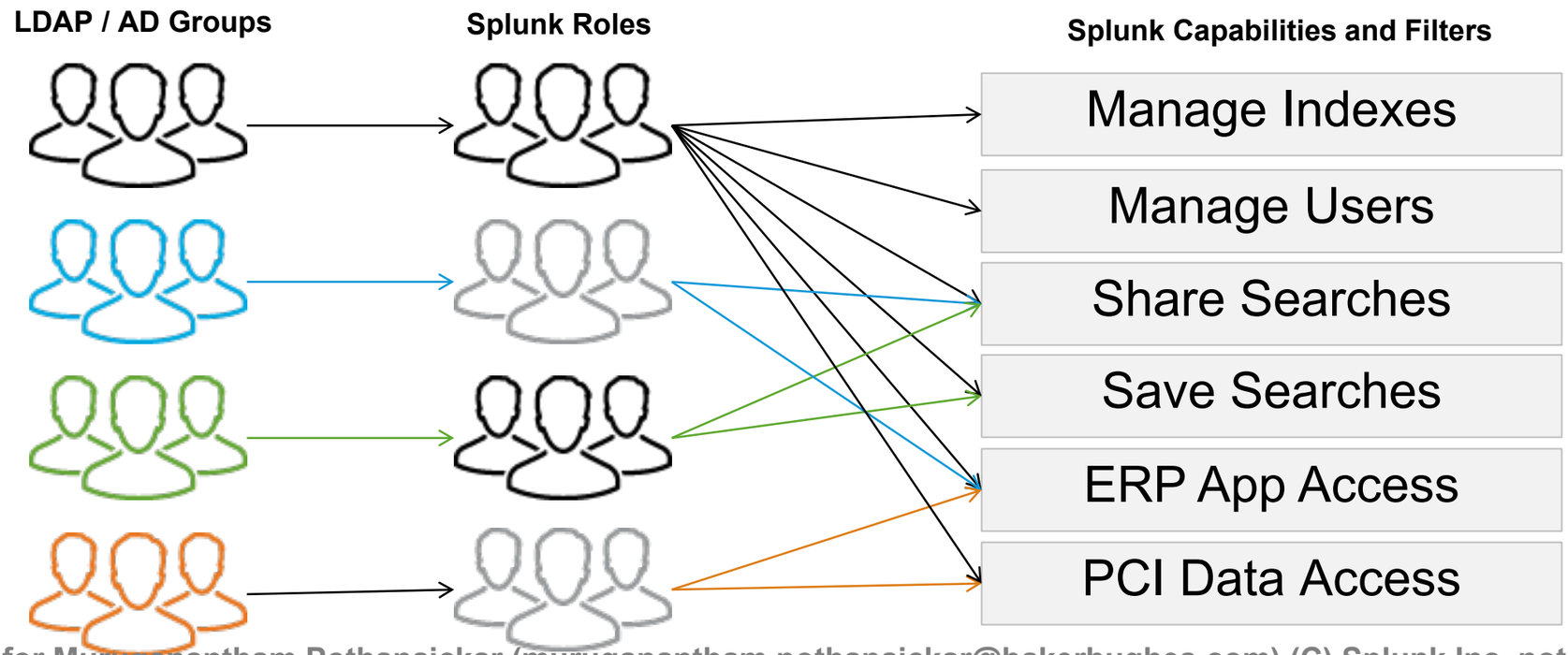
Test Inputs	A standalone indexer with minimal performance and capacity
Test Configurations	A minimum set of components (one Search Head, one Indexer, one Deployment Server, …)
Test Performance	An accurate duplication of the production environment

Authentication / Authorization

- **LDAP / AD** for authentication and group management
  docs.splunk.com/Documentation/Splunk/latest/Security/SetupuserauthenticationwithLDAP
- **SSO** authentication can be leveraged by Splunk:
  - SAML
    docs.splunk.com/Documentation/Splunk/latest/Security/HowSAMLSSOworks
  - ProxySSO
    docs.splunk.com/Documentation/Splunk/latest/Security/AboutProxySSO
  - Reverse proxy
    docs.splunk.com/Documentation/Splunk/latest/Security/HowSplunkSSOworks
- Scripted authentication
  - A user-generated Python script serves as the middleman between the Splunk server and an external authentication system
  - Supported systems include PAM and RADIUS
    docs.splunk.com/Documentation/Splunk/latest/Security/ConfigureSplunkToUsePAMOrRADIUSAuthentication

Access Control

- Integrate authentication / access control with LDAP and Active Directory
- Map LDAP and AD groups to flexible Splunk capability or data-access roles
  - Define any search as a filter



Security, Privacy, Integrity Measures

- HTTPS transport is available end-to-end
  - Create your own certificates or acquire from a valid 3rd party
  - Distributed search (enabled by default between search head and indexer)
  - Forwarder to indexer over TCP
  - Web browser access to Splunk Web
- Indexer Acknowledgement
- Index Splunk's configurations and logs to track changes
- For more information about using SSL:

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

- For more information about event auditing:

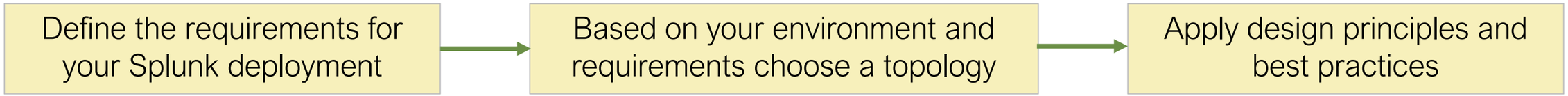
docs.splunk.com/Documentation/Splunk/latest/Security/Audityoursystemactivity

Security, Privacy, Integrity Measures (cont.)

- Disable Splunk Web when it is not required
  - For example, indexers in a distributed deployment do not require Splunk Web
- Harden your Splunk servers
  - Follow best practices: docs.splunk.com/Documentation/Splunk/latest/Security/Hardenyourserversandsecureyouroperatingsystem

Splunk Validated Architectures (SVAs)

- Proven reference architectures
- Designed by Splunk Architects based on best practices
- Repeatable deployments
- Offer topology options for your environment and requirements



Note

Refer to Appendix A for more information about Splunk Validated Architectures.

Module 4 Lab Exercise

Time: 10 minutes

Task:

- Size the infrastructure
  - How many indexers, search heads and other components?

Module 5: Clustering Overview

Module Objectives

- Review indexer clustering, including single-site and multi-site clusters
- Define clustering requirements, best practice, and SmartStore
- Review search head clustering
- Defined search head clustering requirements and best practices

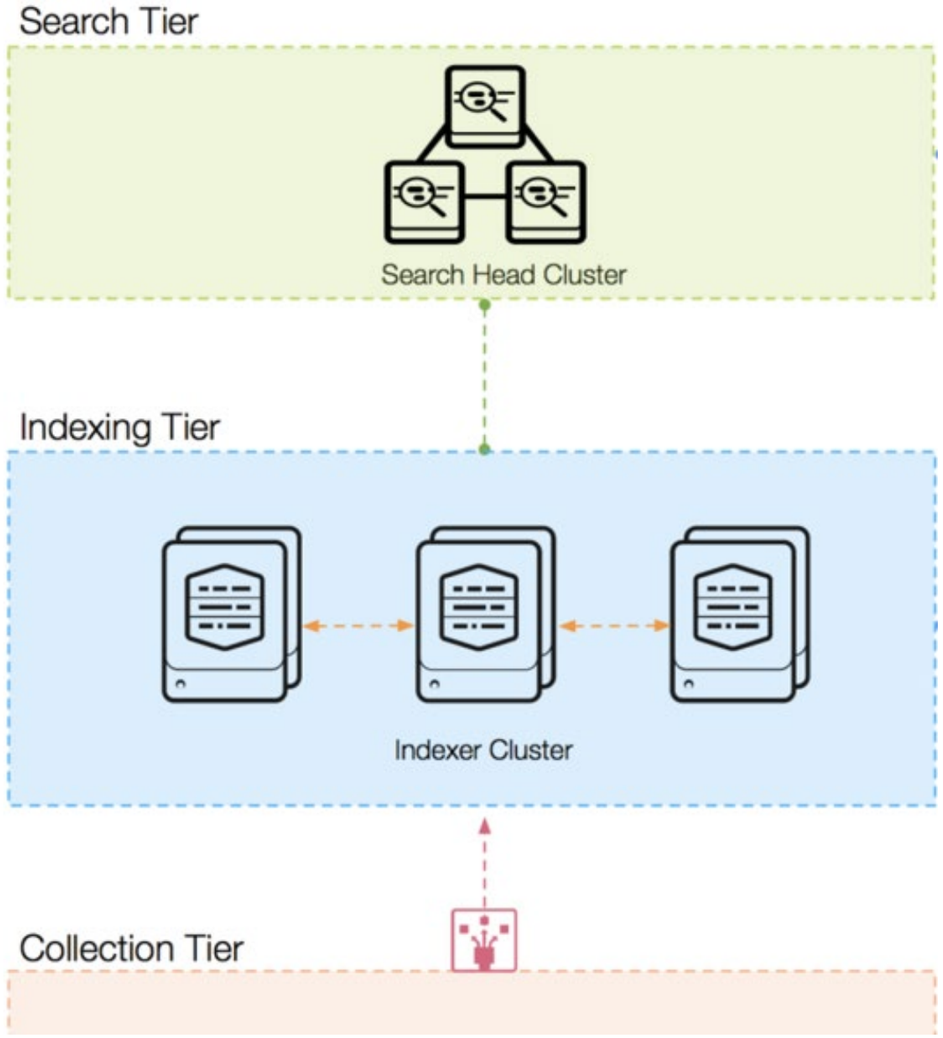
Splunk's Cluster Capabilities

Search head clustering

- Provides improved resource scheduling and increased search accessibility
- Replicates knowledge objects and search artifacts across a set of search heads

Indexer clustering

- Provides availability and recovery
- Replicates data (buckets) based on configured policies

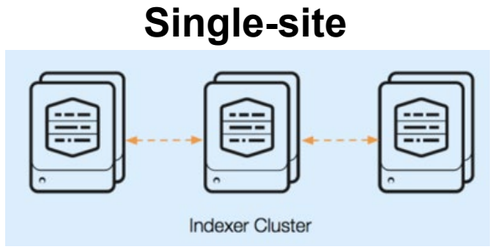


Note

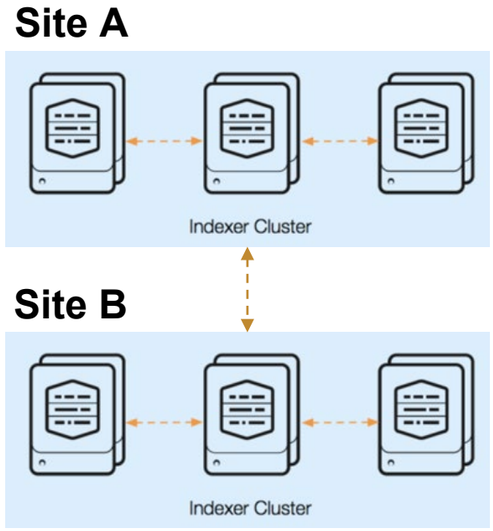
These topics are discussed in detail in the Splunk Enterprise Cluster Administration course.

About Indexer Clusters

- **Single-site indexer clusters**
  - Splunk Enterprise nodes working together to provide redundant indexing and searching capability
  - docs.splunk.com/Documentation/Splunk/latest/Indexer/Aboutclusters

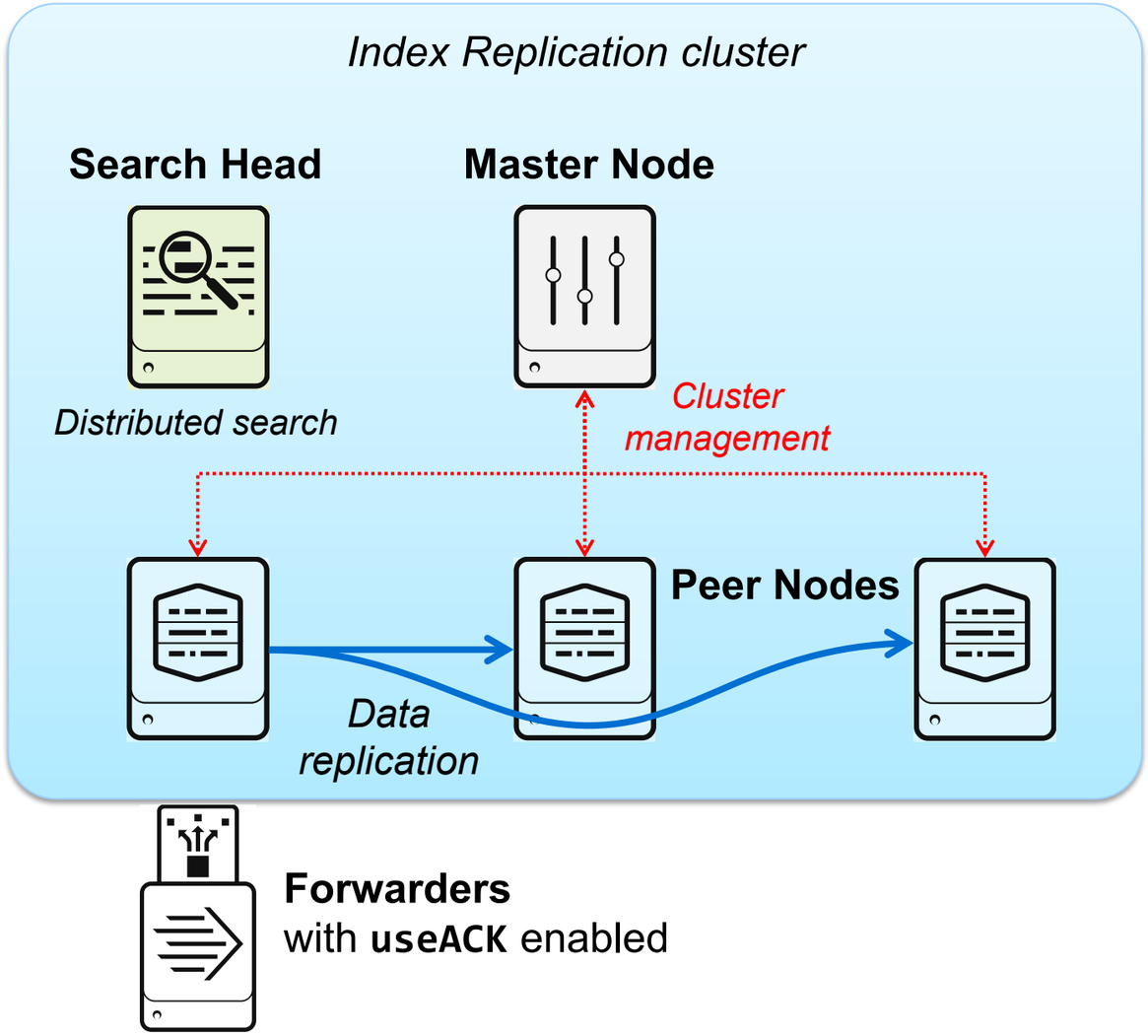


- **Multisite indexer cluster**
  - Indexer cluster spanning multiple sites
  - Each site:
    - Has its own set of peer nodes and search heads
    - Obeys site-specific replication and search factor rules
    - Defined by the cluster administrator
    - Can represent a location or something else
  - docs.splunk.com/Documentation/Splunk/latest/Indexer/Multisiteclusters



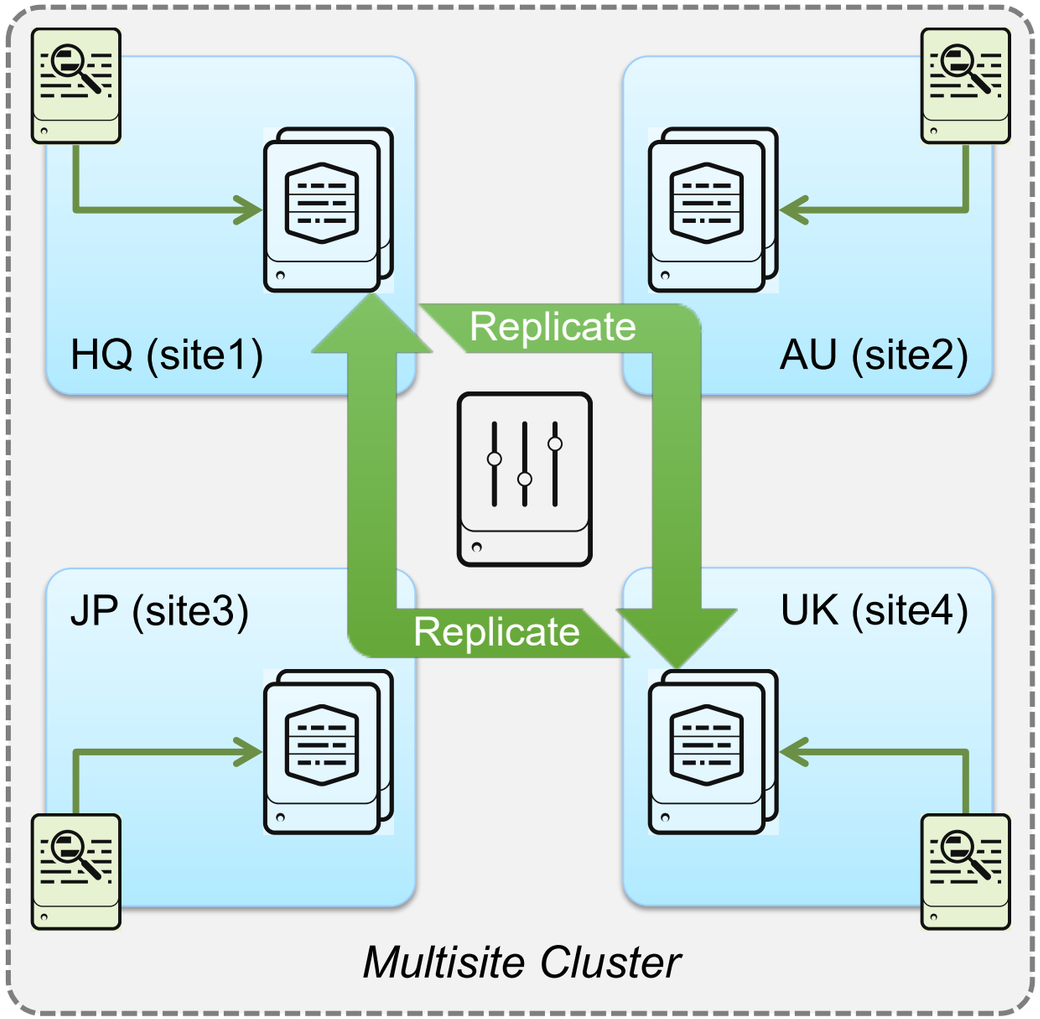
Single-site Indexer Cluster Review

- Master node
  - There can only be one master
  - Controls and manages index replication
  - Distributes apps and configurations to peer nodes
- Peer nodes
  - Indexes data from inputs/forwarders
  - Replicates data to other peer nodes as instructed by the master node
- Search head
  - Required component of indexer cluster
- Forwarders
  - Send data to peer nodes

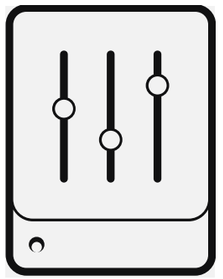


Multisite Indexer Cluster Overview

- Allows for extra layer of data partitioning
  - Indexers are grouped by “sites”
- Offers two key benefits:
  1. **Disaster recovery**
     - Stores index copies at multiple sites (i.e. geo-location or rack)
     - Automatic site-failover capability
     - Provides indexing and search in case of a site-specific disaster
  2. **Search affinity**
     - Preferentially searches assigned site
     - Greatly reduces WAN network traffic



Master Node



- Manages an indexer cluster
  - Coordinates the replicating activities of the peer nodes
  - Tells search heads where to find data
  - Manages the configuration of peer nodes
  - Orchestrates remedial activities if a peer becomes unavailable
- There can be *only one* Master Node, even in a multisite cluster
  - A stand-by Master Node should exist offline for manual Master Node failover
  - Cluster will continue to operate while the Master Node is offline

Replication and Search Factors

- Peer nodes replicate data: copy buckets to each other
  - Copied buckets may be complete buckets or contain only rawdata
  - Replication factors apply to the entire cluster
  - Replication must be enabled for each index (default: disabled)
- **Replication factor (RF)**
  - Specifies how many total copies of **rawdata** the cluster should maintain
  - Sets the total failure tolerance level
- **Search factor (SF)**
  - Specifies how many copies will be ***searchable***
    - Searchable buckets have both rawdata and index files
  - Determines how quickly you can recover the search capability

Note

Refer to *Appendix B: Indexer Cluster Action Review* for *Factors in Action* review slides

Indexer Clustering Requirements

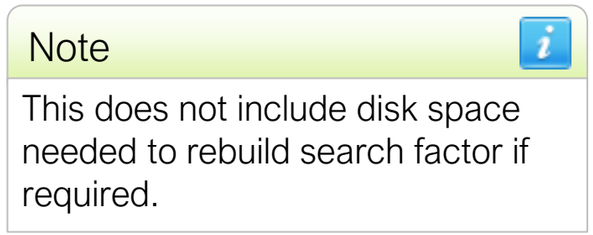
- One Master Node
- Additional "stand-by" Master Node
- For single-site mode:
  - Minimum number of peer nodes equal to replication factor (RF)
    - Example: RF = 3 requires a minimum of three peer nodes
  - **Best Practice**: Minimum of (RF + 1) peer nodes
- For multisite mode:
  - Minimum 2 peer nodes per site in multisite mode

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

Local Storage Requirements for Clustering

- Replication factor (RF) and search factor (SF) affect storage requirements
  - Total rawdata disk usage = rawdata total * RF
  - Total index disk usage = index data total * SF

For more information about storage requirements, go to:
docs.splunk.com/Documentation/Splunk/latest/Indexer/Systemrequirements#Storage_considerations



Estimating Disk Usage

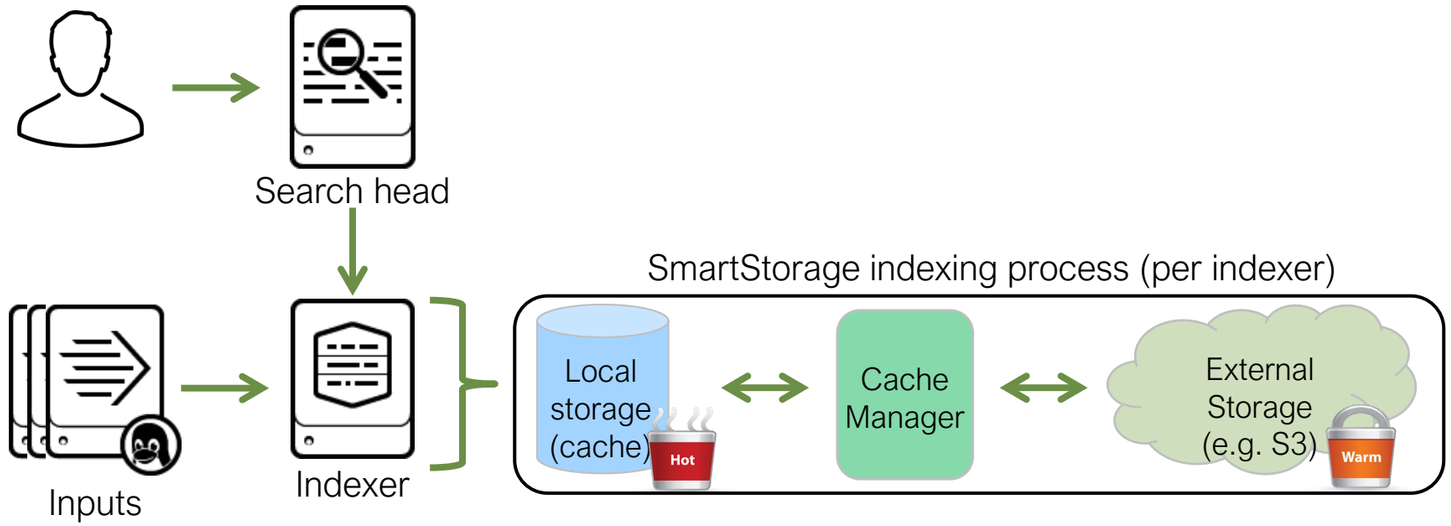
- For this example, assume:
  - Daily index data = ~100GB
  - rawdata on disk = ~15% of daily index data
  - index files on disk = ~35% of daily index data

> **Note**
> Per day storage must still be multiplied by the # days retention!

Daily Index data = ~100GB	RF=3 & SF=2 on 3 peer nodes	RF=3 & SF=2 on 6 peer nodes	RF=3 & SF=3 on 6 peer nodes
rawdata (~15GB/day)	15 * 3 = 45 GB	15 * 3 = 45 GB	15 * 3 = 45 GB
index files (~35GB/day)	35 * 2 = 70 GB	35 * 2 = 70 GB	35 * 3 = 105 GB
Total size across cluster	115 GB	115 GB	150 GB
Per Peer storage / day	115 / 3 = 38.3 GB	115 / 6 = 19 GB	150 / 6 = 25 GB

Remote Storage – SmartStore Overview

- Reduces local storage requirements for index clusters
- A cost-effective way to store your indexed data
- Hot buckets are still stored in local storage, but warm buckets are stored remotely and retrieved using the cache manager



SmartStore and Index Clustering

- Indexer clusters maintain replication and search factor copies of hot buckets only
- During SmartStore replication, target peer nodes also create an empty directory for each warm bucket that has metadata in their `.bucketManifest` files
  - The file contains metadata for each bucket copy that the peer node maintains
- The indexer cluster can recover all of its warm bucket data even when the number of failed nodes equals or exceeds the replication factor

For detailed information about Index clustering with SmartStore, please refer to:
docs.splunk.com/Documentation/Splunk/latest/Indexer/IndexerclusteroperationsandSmartStore

SmartStore Use Cases

- The cost of storing replicated copies in local storage is costly
- Leverages data fidelity guarantees provided by storage or cloud vendors
  - Eliminates the need to store local copies of warm or cold buckets
- Upgrade/bring down clusters by temporarily moving data to remote storage
- Not suitable if you are executing long lookback searches regularly

SmartStore Unsupported Features

- TSIDX reduction
  - Do not set **`enableTsidxReduction = true`**
- Data integrity
- Disabling bloom filters
  - Do not set **`createBloomFilter = false`**
- Changing the location of bloom filters
  - Do not change **`bloomHomePath`**
- Summary replication

For more information about SmartStore:
docs.splunk.com/Documentation/Splunk/latest/Indexer/AboutSmartStore

Search Head Clusters

- A group of Splunk Enterprise search heads that serves as a resource for searching
- Must have matching hardware specs
- Allow for running the same searches, viewing the same dashboards, and accessing the same search results from any search head member
- To achieve this, the search heads in the cluster share
  - Configurations and apps
  - Search artifacts
  - Job scheduling

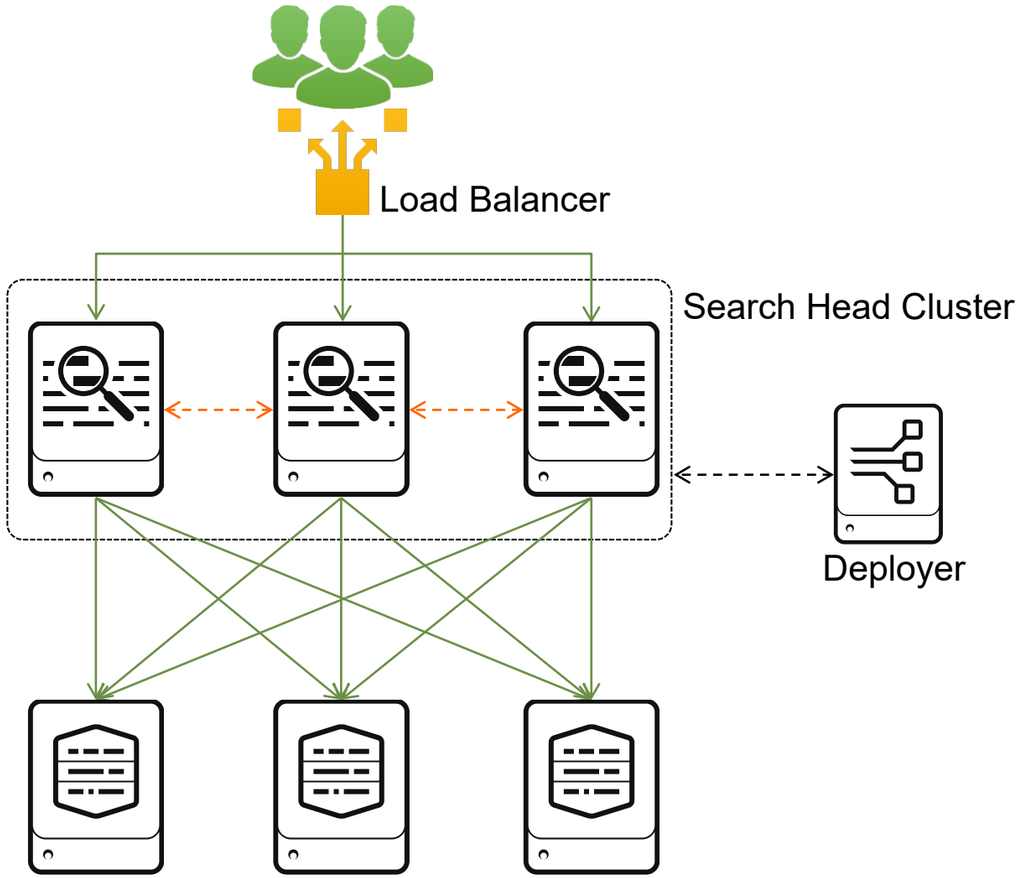
For more information about search head clustering, go to:
docs.splunk.com/Documentation/Splunk/latest/DistSearch/AboutSHC

Search Scaling: Do you Need a Cluster?

- To mitigate performance issues as the search load increases
  - Distribute search load
    - Optimize scheduled searches to run on non-overlapping time slots
  - Limit resource usage
    - Limit the time range of end-user searches
    - Configure user roles to limit the number of concurrent real-time searches
  - Increase the number of peer nodes (indexers)
  - Add more search heads
  - **Use a search head cluster**

Search Head Cluster Review

- Highly available and scalable search service that groups search heads into a cluster
  - Always-on search services
  - Simple horizontal scaling
    - Add more members any time
    - Commodity hardware
    - No need for NFS
- Seamless user experience
  - Easy to on-board users and apps
- Reliable alerts
  - Search job failure aware and reschedule
- Dedicated configuration bundle management



Search Head Clustering Requirements

- Requirements
  - At least 3 search heads
  - A deployer
- Sizing guidelines – Search Heads
  - Search heads should meet the minimum reference server requirements
- Sizing guidelines – Deployer
  - No published minimums
  - Must have sufficient CPU and network resources to service requests and to push configurations

Notes for Search Head Clustering

- Summary indexes must be forwarded to the indexer tier
  - This is a general best practice, but required for search head clustering
  - This may increase the disk space required on the indexers
- In search head cluster, add more search heads to horizontally scale the capacity
  - Assumes that the indexer layer has sufficient search capacity
  - If capacity is insufficient, a bottleneck is created at the indexers/peer nodes
  - Remember that the rule of thumb for scaling is "add another indexer"

Final Notes on Clustering

- Planning is essential
  - What are the requirements for high availability and disaster recovery?
  - How quickly must recovery occur?
  - How many servers can be lost before service degrades or data is lost?
- You can mix clustered and non-clustered servers
  - You can have a mix of clustered and standalone indexers
  - You can have a mix of clustered and standalone search heads
    - This may be the best solution for some special-purpose or single app search heads

Module 5 Lab Exercise

Time: 10 minutes

Task:

Using the infrastructure from the previous module, update your data sizing table to use indexer clustering for data replication

Module 6: Forwarder and Deployment Best Practices

Module Objectives

- Review forwarder types
- Manage forwarder installation in an enterprise environment using:
  - Deployment Server
  - Master Node
  - Deployer

Types of Forwarders

Universal forwarder (UF)

- Streamlined binary package containing only components needed to forward data
- Network bandwidth defaults to 256 KBps (configurable)
- Use whenever possible

Heavy forwarder (HF)

- Uses the Splunk Enterprise binary with all capabilities
- Parses data before forwarding
- Use when you require:
  - The Splunk Web UI
  - Advanced event level routing
  - Filtering > 80% of incoming events
  - Anonymizing or masking data before forwarding to indexer
  - Predictable version of Python
  - App/Modular Input that needs HF (HEC, DBX, Checkpoint OPSEC LEA, etc.)

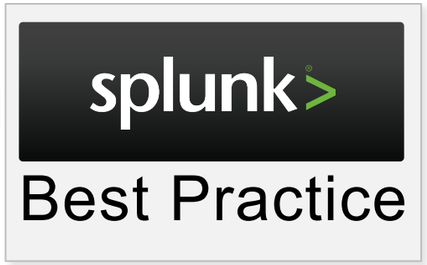
Note

Parsing on a HF can consume more resources than parsing on the indexer.

www.splunk.com/blog/2016/12/12/universal-or-heavy-that-is-the-question.html

Forwarding Tier Design

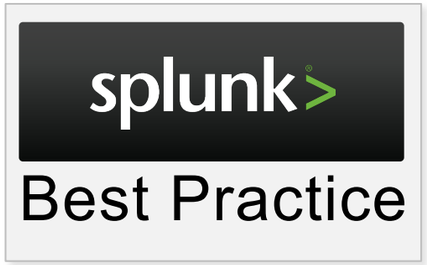
- Use the UF unless there are specific requirements that necessitate an HF
  - Sending cooked data through a HF to indexers impacts overall throughput performance
- Use a syslog server for syslog data
- Avoid intermediate forwarders when possible:
  - Bottlenecks can occur
  - Reduces the distribution of events across indexers
- If intermediate forwarders are required, ensure there are enou them



Forwarding Tier Design (cont.)

- Forwarders automatically load balance over available indexers
  - **AutoLB** is enabled by default
  - May need to increase UF **thruput** setting in **limits.conf** (default: 256KBps) for high velocity sources
    - This value should be based on the ratio of forwarders to indexers

```
[thruput]
maxKBps = 0
#zero is unlimited
#default was 256
```

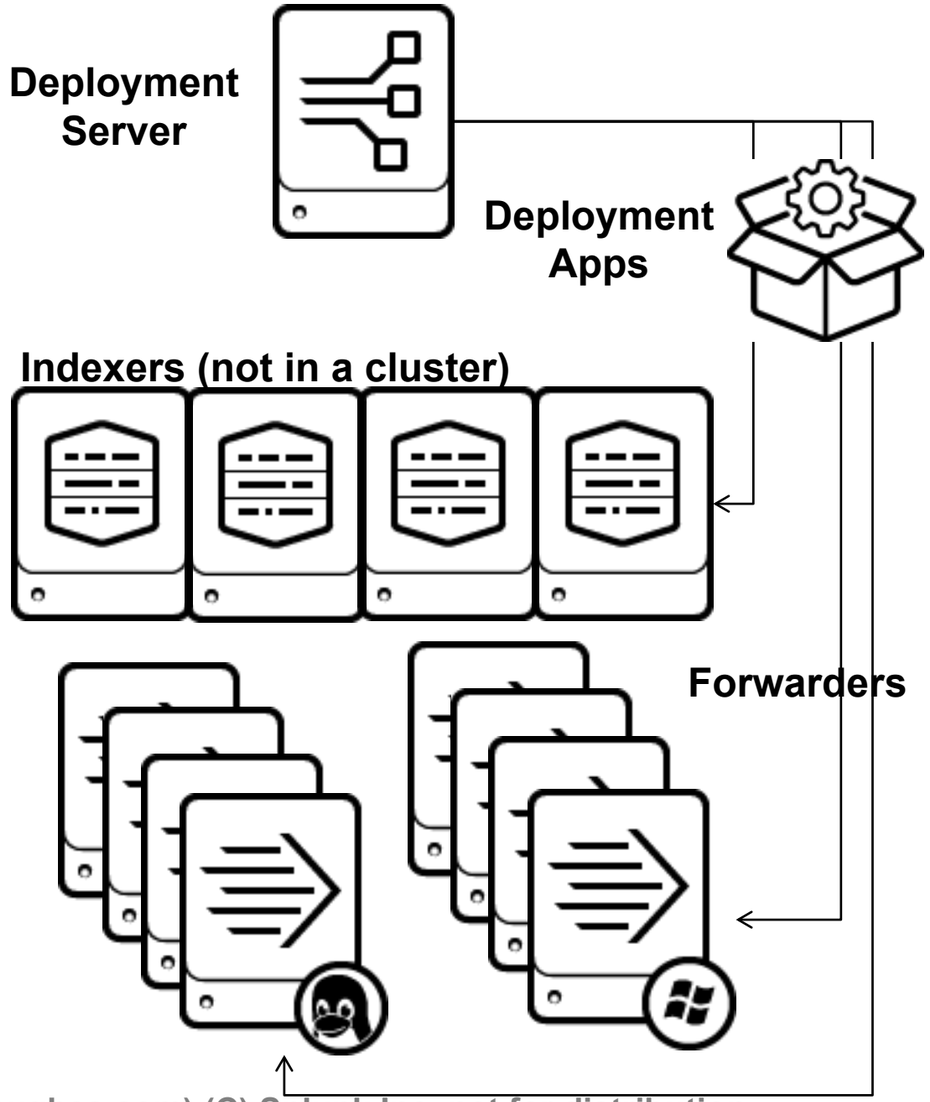


Deployment Management

Type of Instance	Manage Configurations with…
Forwarder Search Head (stand-alone) Indexer (stand-alone)	Deployment Server or other configuration management tool
Search Head Cluster Member	Deployer only
Peer Node in Indexer Cluster	Master Node only

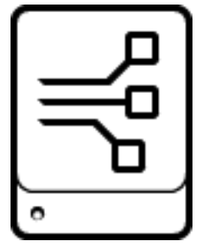
Deployment Server

- A centralized configuration manager that delivers updated content to deployment clients
  - Units of content are known as deployment apps
  - Do **NOT** store configuration in **`SPLUNK_HOME/etc/system/local`** on clients
    - System-level configurations on clients cannot be over-ridden with Deployment Server



Deployment Server (cont.)

- One reference server safely handles approximately 5000 clients
- Be sensitive to the **`phoneHomeIntervalInSecs`** attribute in **`deploymentclient.conf`**
  - Default client poll is 60 seconds
  - Prioritize servers that need more frequent updates
  - In general, adjust client polling interval to scale
- For small environments:
  - Deployment server can share with other components
- For more than 50 deployment clients:
  - Deployment server should be on a dedicated server



Deployment Server

splunk> Best Practice

docs.splunk.com/Documentation/Splunk/latest/Updating/Calculatedeploymentserverperformance

Config Management – Deployment Server

- When using Forwarder Management or the Deployment Server (DS)
  - Build an install script/package for clients with only the files needed to contact the DS (basic installation + **`deploymentclient.conf`**)
    - Clients will get the rest of the configuration information from the DS
- Use in combination with another configuration management (CM) tool for:
  - Authentication certificates, passwords, **`log-local.cfg`**, **`deploymentclient.conf`**, upgrades of forwarder software, remote boot-start of production system
  - Use other CM tools for rare tasks, deployment server for routine tasks

 | 12 February 2021

Deploy Apps to Search Head Cluster

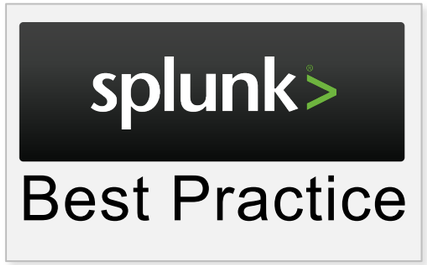
- Use the Deployer to distribute apps to SHC members
  - DO NOT stage any out-of-the-box apps in deployer (search, launcher, etc.)
  - All members of the cluster will receive the same apps
- Deployer supports both push and pull mechanisms
  - Push apps to search head cluster members
  - Polled by new or restarted search head cluster members for updates
- Knowledge objects that are created by users in Splunk Web
  - Are automatically replicated
  - Are not sent to the Deployer

Deploy Apps to Indexer Cluster

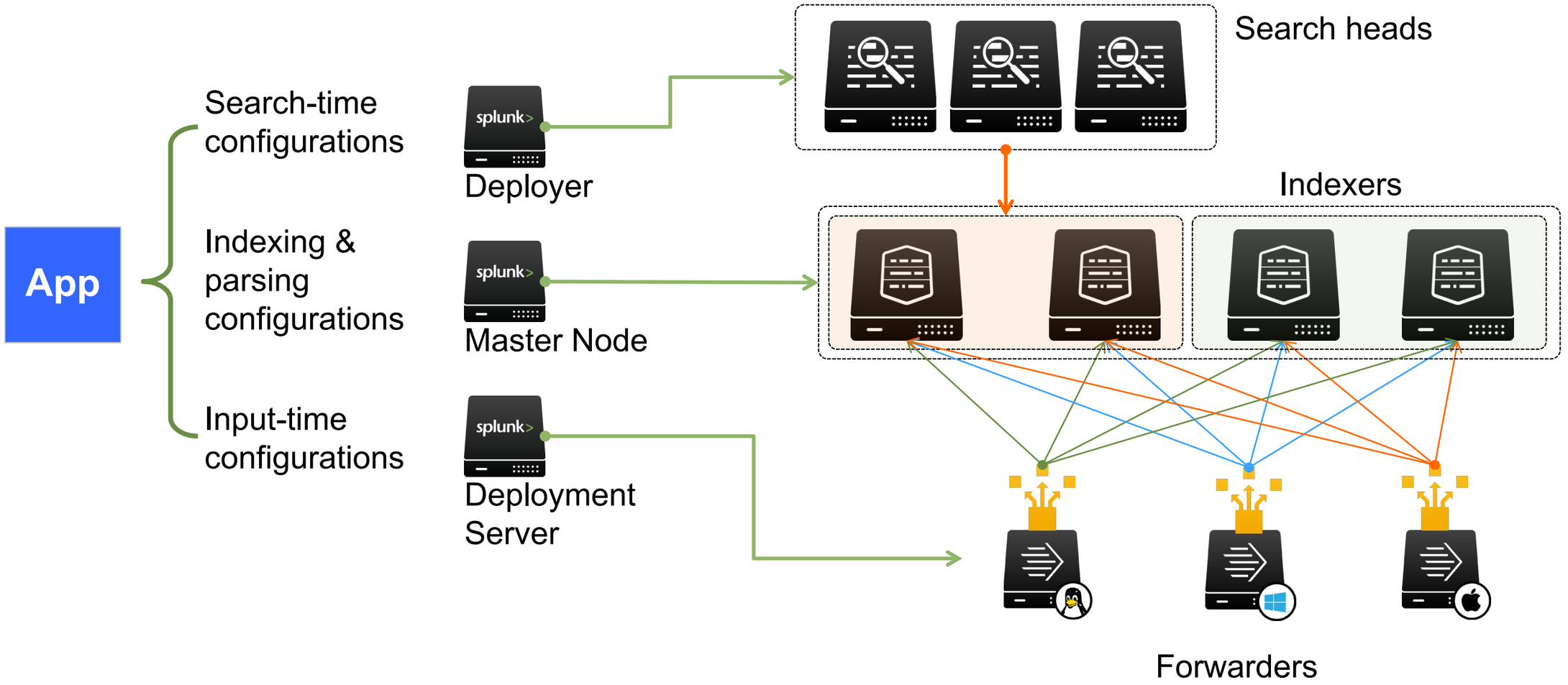
- Use the Master Node to distribute apps to the peer nodes
  - DO NOT stage any out-of-the-box apps in Master Node (search, launcher, etc.)
  - All members of the cluster will receive the same apps
  - Master Node pushes apps and rolling-restarts peer nodes if needed
  - Master Node repository: **`/etc/master-apps`**
  - Destination directory on indexers: **`/etc/slave-apps`**
- You cannot use the Deployment Server to distribute apps to the peer nodes

Deployment Apps

- Design your deployment app
  - An app is a set of deployment content (a configuration bundle)
  - An app is deployed as a unit and should be small
  - Take advantage of Splunk's configuration layering
  - Use a naming convention for the apps
  - Create classes of apps, for example
    - Input apps
    - Index apps
    - Web control apps
- Carefully design apps regardless of your configuration management tool (DS, Master Node, Puppet, etc.)



Splunk Deployment Tools



Module 6 Lab Exercise

Time: 15 minutes

Tasks:

- Create a Phase 1 topology diagram
- Analyze apps and understand deployment issues
  - Remember that some Splunkbase apps may need to be repackaged into deployment apps for your environment
- Design a test environment
  - How many servers are needed for testing?
  - How will you test the deployment, including the apps?

Module 7: Integration

Module Objectives

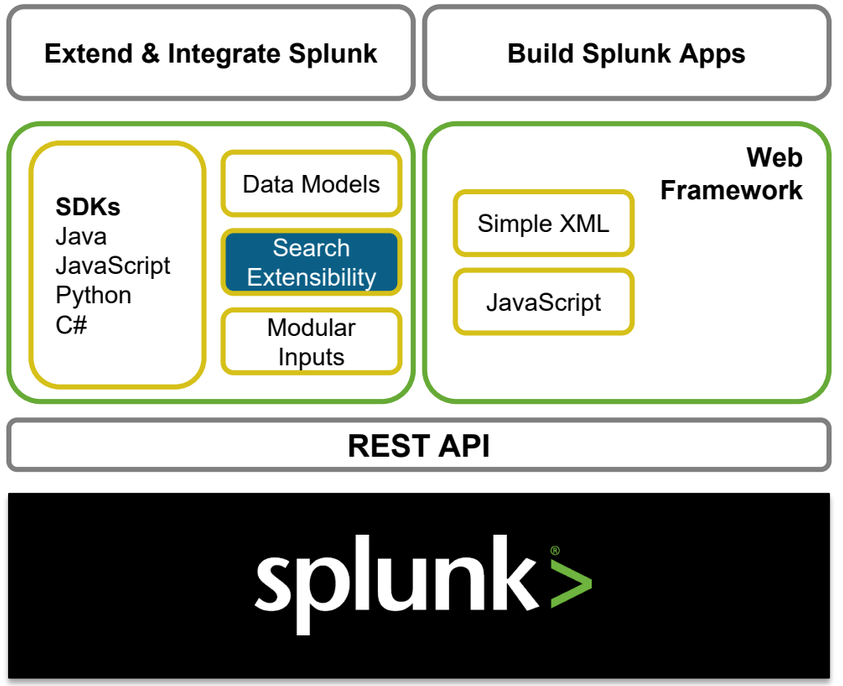
- Describe and identify common integration methods

Types of Integration

- Accessing other data or applications from within Splunk
- Accessing Splunk from another application
- Re-forwarding data to other applications after it is indexed in Splunk
- Integration with the Hadoop File System (HDFS)
- Apps may also provide convenient integration points

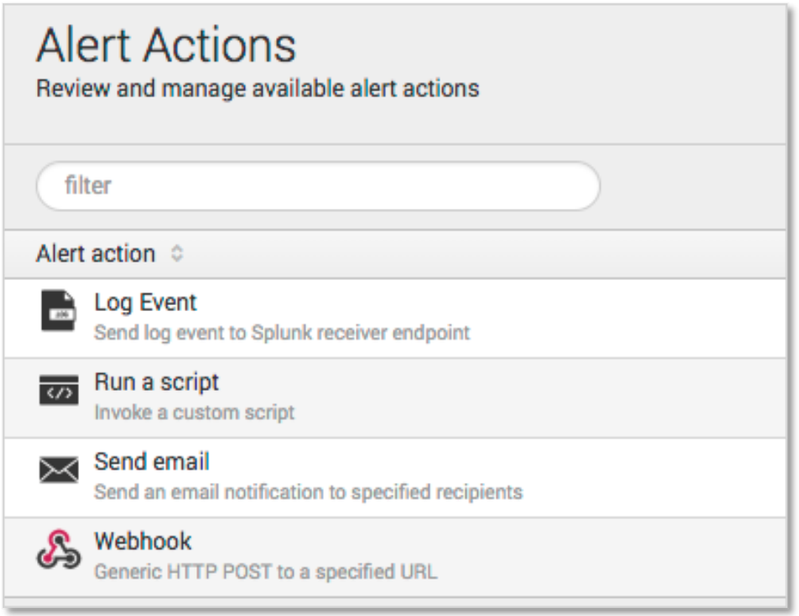
Search Extensibility Review

- Custom search commands
  - Write a new search command in Python
  - dev.splunk.com/view/python-sdk/SP-CAAAEU2
- Scripted lookups
  - Programmatically script lookups in Python
- Workflow actions and custom navigation
  - Access additional resources outside Splunk with a single click



Integration Using Alert Actions

- Allows developers to extend Splunk to build, package and publish new alert actions for Splunk
- Can be used by any scheduled search
- Several modular alerts are available on Splunkbase



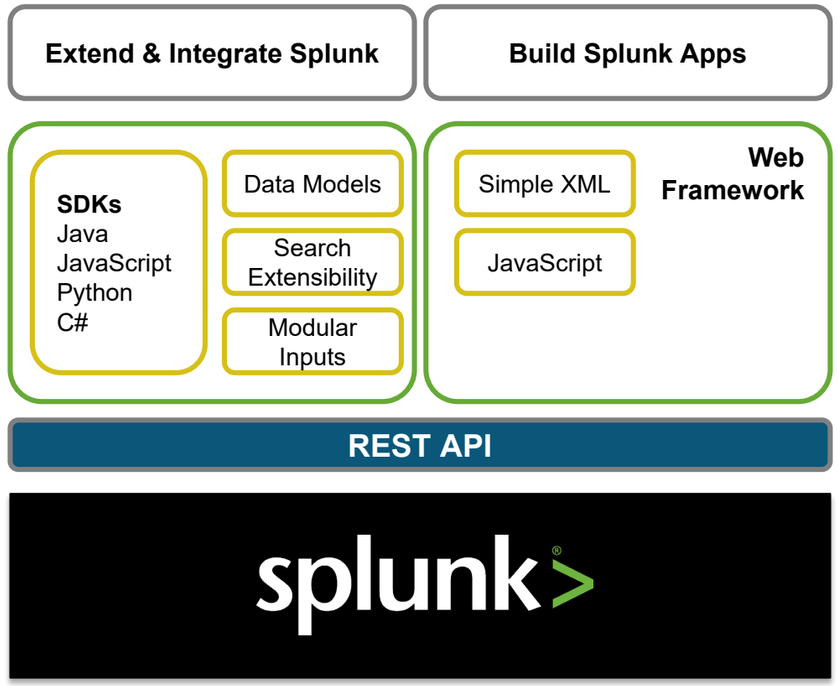
splunkbase.splunk.com/apps/#/search/alert/

docs.splunk.com/Documentation/Splunk/latest/Alert/CreateCustomAlerts

docs.splunk.com/Documentation/Splunk/latest/AdvancedDev/ModAlertsIntro

Splunk REST API

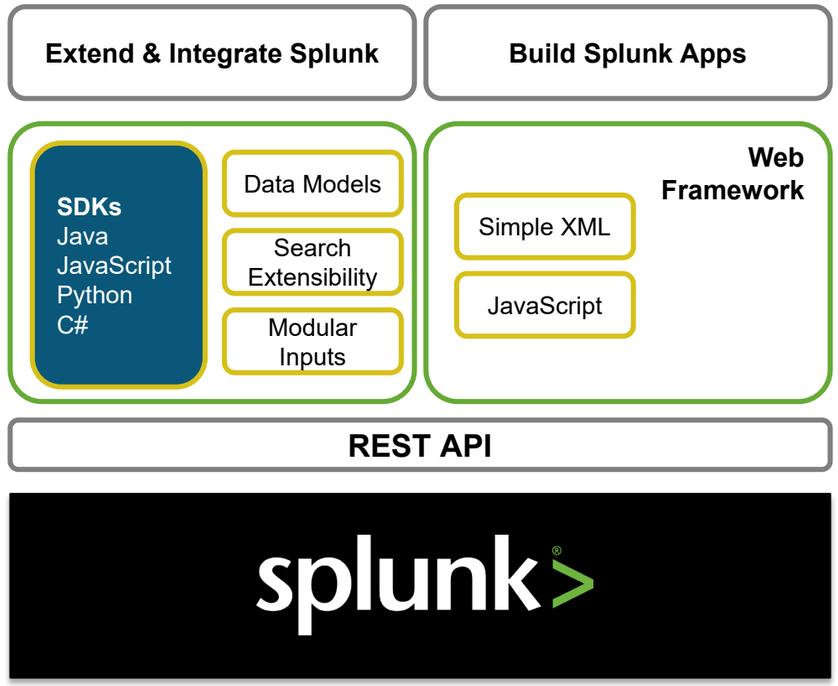
- **RE**presentational **S**tate **T**ransfer
- The most basic way to programmatically access Splunk is to use the REST API via HTTP requests
- With over 200 endpoints, the REST API allows you to interact directly with a Splunk instance
- For more information: dev.splunk.com/restapi



Software Development Kits (SDKs)

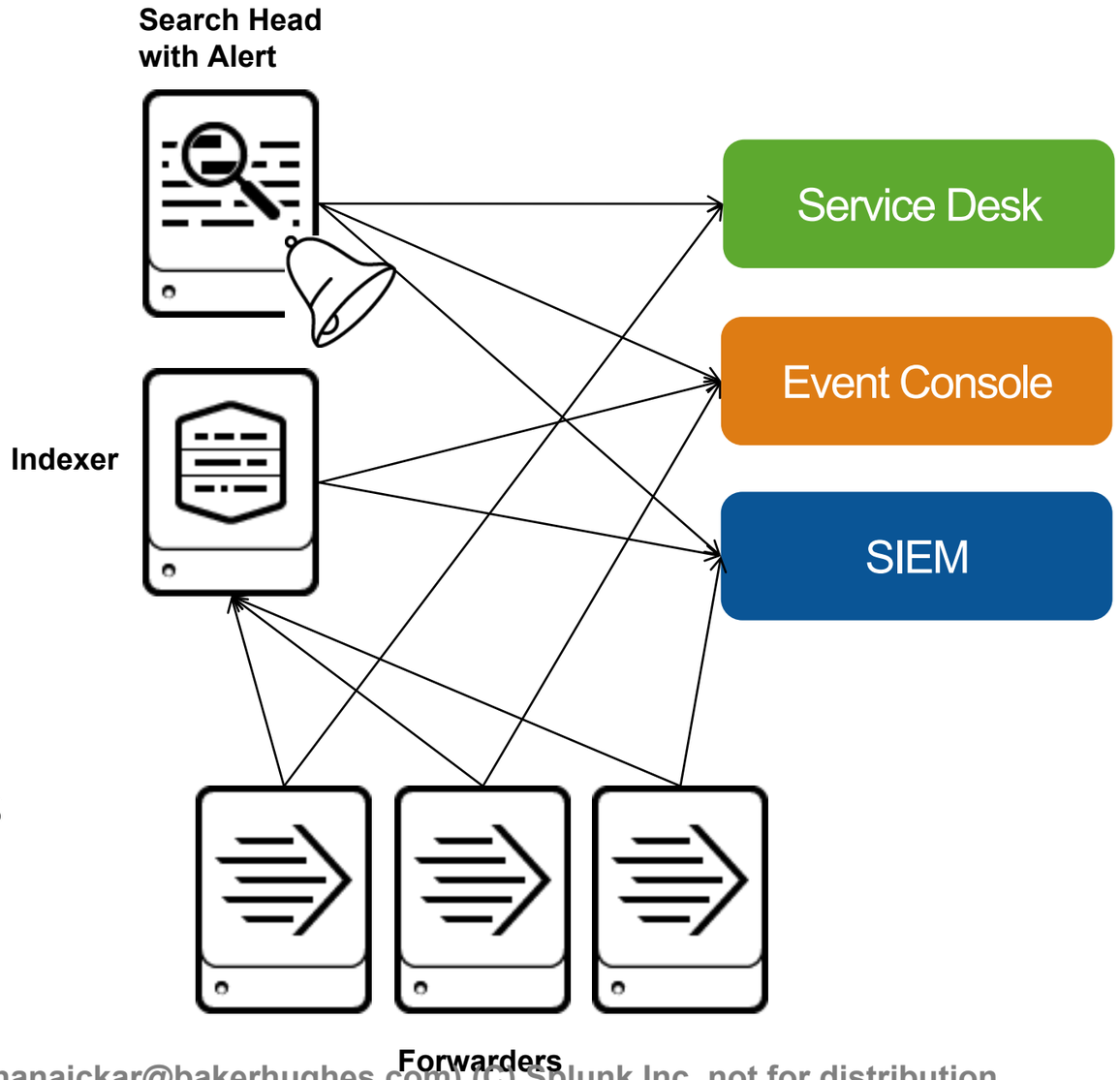
- SDKs provide language-specific libraries for accessing the Splunk REST API
  - Includes documentation, code samples, resources, and tools
  - Simplifies code development for
    - Python
    - JavaScript
    - Java
    - C#

dev.splunk.com/sdks



Sending Data to Other Systems

- Forward all or a subset of data via TCP to other systems
  - Forward either raw text or syslog
  - Can be done centrally via the indexer
  - Does not increase license
- Use scheduled searches to insert events into other systems
  - Leverages alert functionality
  - For example, use correlation searches and configure the alerts to open tickets or insert events into a SIEM



Splunk Analytics for Hadoop

- Add a Splunk Analytics for Hadoop license to Splunk Enterprise
  - Add-on can be downloaded from Splunkbase splunkbase.splunk.com/app/3311/
- Uses the MapReduce framework to HDFS when performing searches
  - Hadoop searches only work in Linux installs
- Accesses both Splunk indexes and HDFS from a single Splunk search head
- License is based on Hadoop Nodes

For more information, go to:

www.splunk.com/en_us/products/apps-and-add-ons/splunk-analytics-for-hadoop.html

docs.splunk.com/Documentation/Splunk/latest/HadoopAnalytics/MeetSplunkAnalyticsforHadoop

docs.splunk.com/Documentation/Splunk/latest/HadoopAnalytics/Importantinformationaboutinstallationanduser

Module 7 Lab Exercise

Time: 10 minutes

Task:

- Using the topology from Lab 6, review the forwarder configuration and create a Phase 2 topology diagram

Module 8: Performance Monitoring and Tuning

Module Objectives

- Use the Monitoring Console (MC) to track performance of your test environment before going into production
- Identify options to optimize the production environment
- Overview of Workload Management

Monitoring your Test Environment

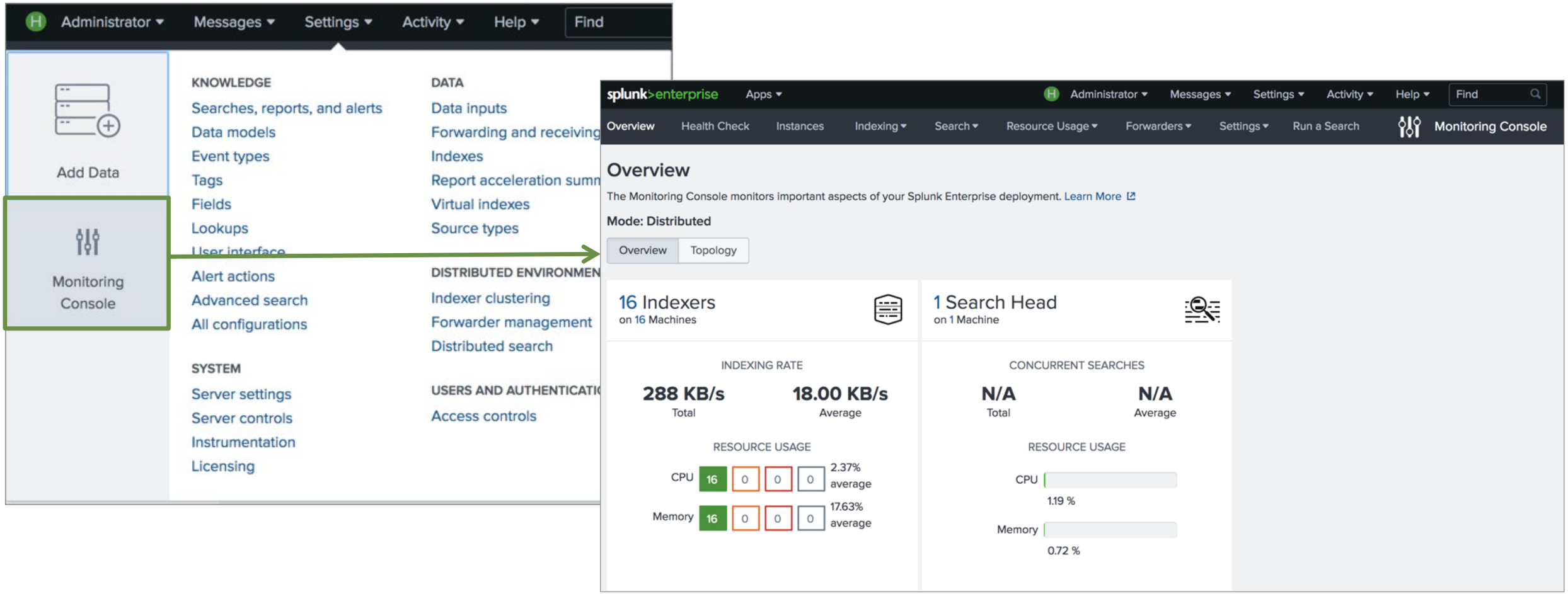
- Perform searches expected in production environment
  - Are specific searches taking a long time?
  - Are specific searches resource heavy?
- Run reports expected in production environment
  - Ad-hoc searches
  - Scheduled searches
- Test load and performance on system with max concurrent users
  - Should user roles be modified based on searches?
    - Restrict access to certain indexes

Note

Work with the Splunk Administrator to monitor your test environment.

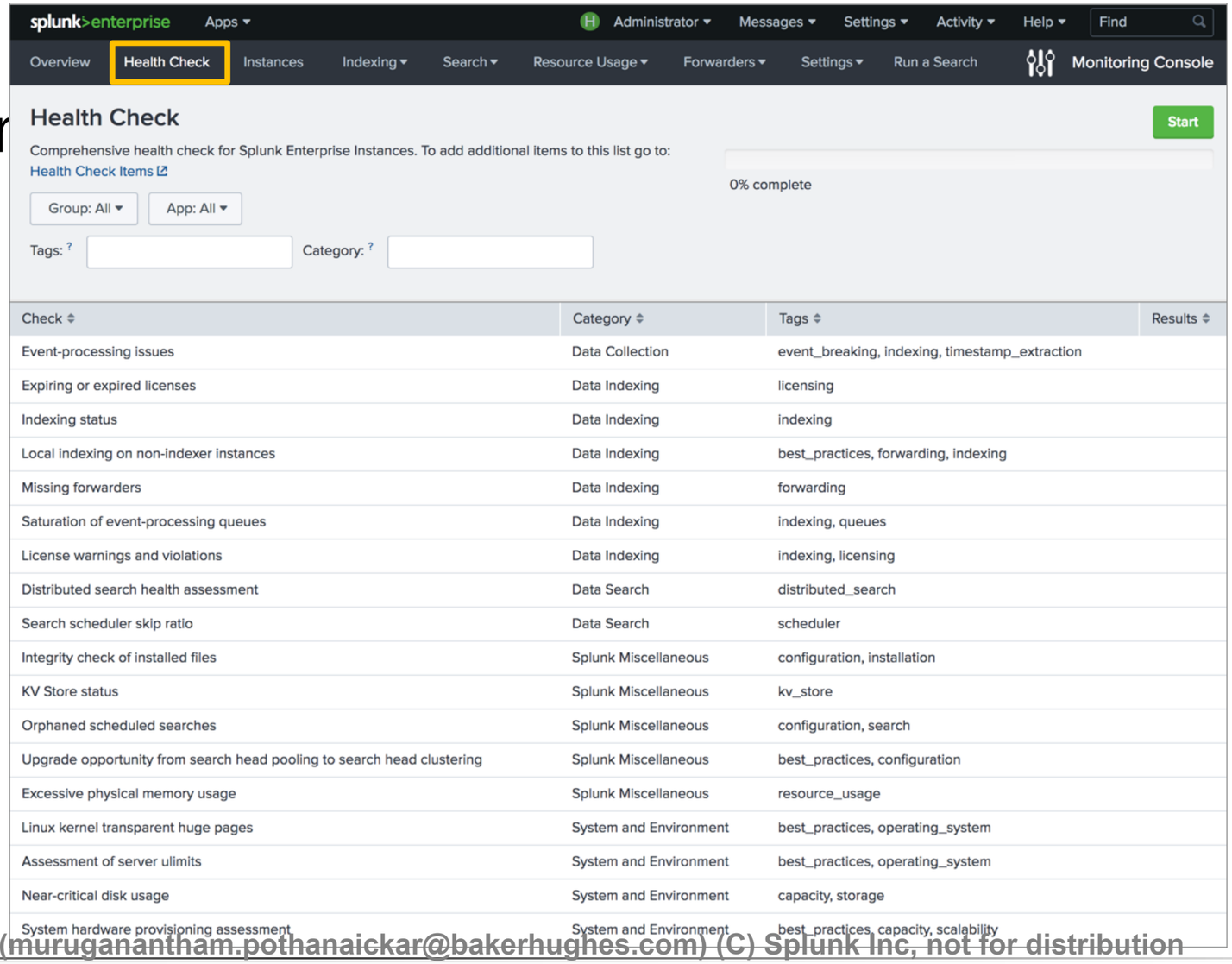
Using the Monitoring Console

Create a base line for performance



Perform Health Checks

Use **Health Check** for a high-level summary of your system's performance

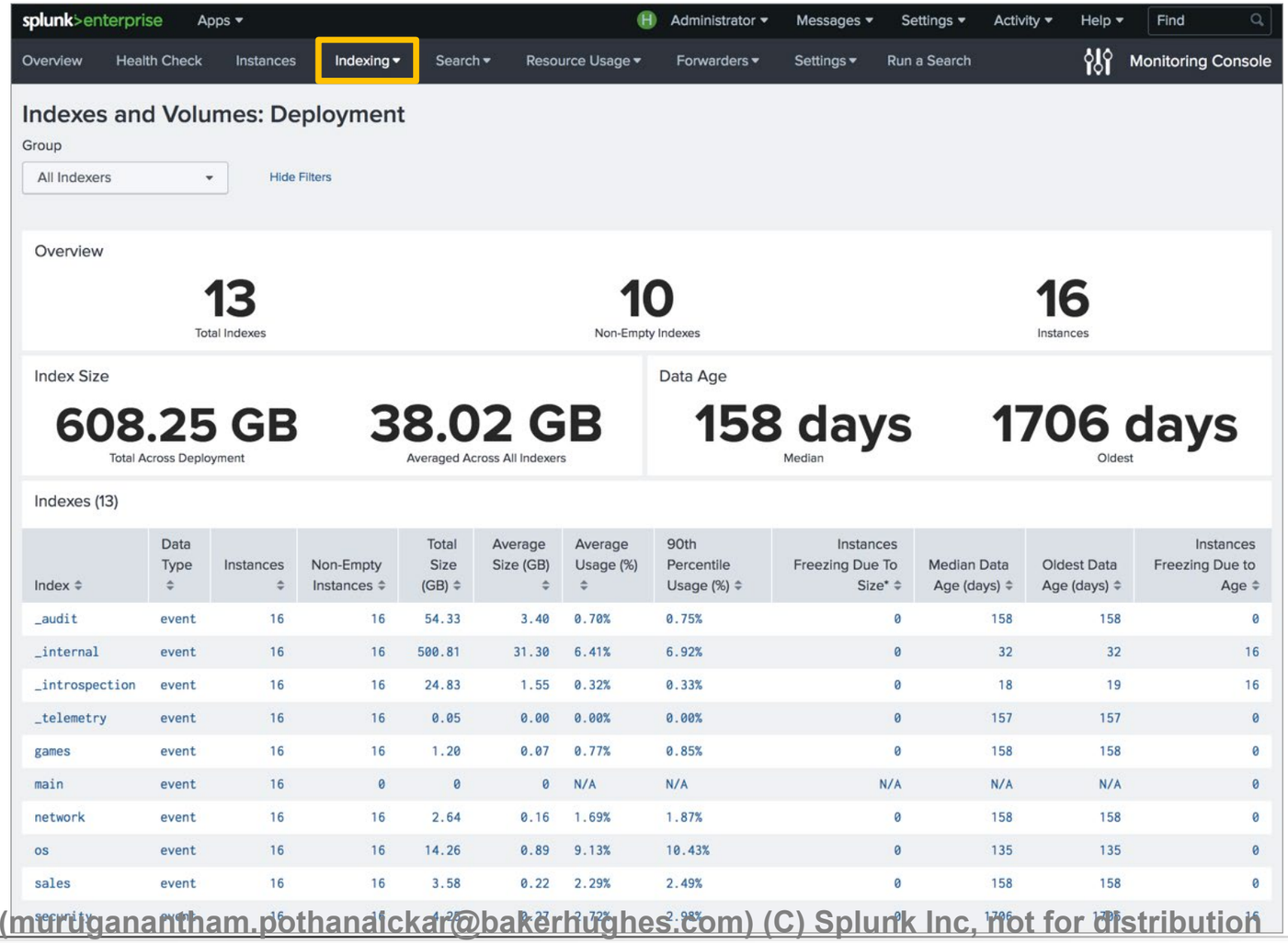


Check	Category	Tags	Results
Event-processing issues	Data Collection	event_breaking, indexing, timestamp_extraction	
Expiring or expired licenses	Data Indexing	licensing	
Indexing status	Data Indexing	indexing	
Local indexing on non-indexer instances	Data Indexing	best_practices, forwarding, indexing	
Missing forwarders	Data Indexing	forwarding	
Saturation of event-processing queues	Data Indexing	indexing, queues	
License warnings and violations	Data Indexing	indexing, licensing	
Distributed search health assessment	Data Search	distributed_search	
Search scheduler skip ratio	Data Search	scheduler	
Integrity check of installed files	Splunk Miscellaneous	configuration, installation	
KV Store status	Splunk Miscellaneous	kv_store	
Orphaned scheduled searches	Splunk Miscellaneous	configuration, search	
Upgrade opportunity from search head pooling to search head clustering	Splunk Miscellaneous	best_practices, configuration	
Excessive physical memory usage	Splunk Miscellaneous	resource_usage	
Linux kernel transparent huge pages	System and Environment	best_practices, operating_system	
Assessment of server ulimits	System and Environment	best_practices, operating_system	
Near-critical disk usage	System and Environment	capacity, storage	
System hardware provisioning assessment	System and Environment	best_practices, capacity, scalability	

Indexing Activity

Indexing provides detailed information about:

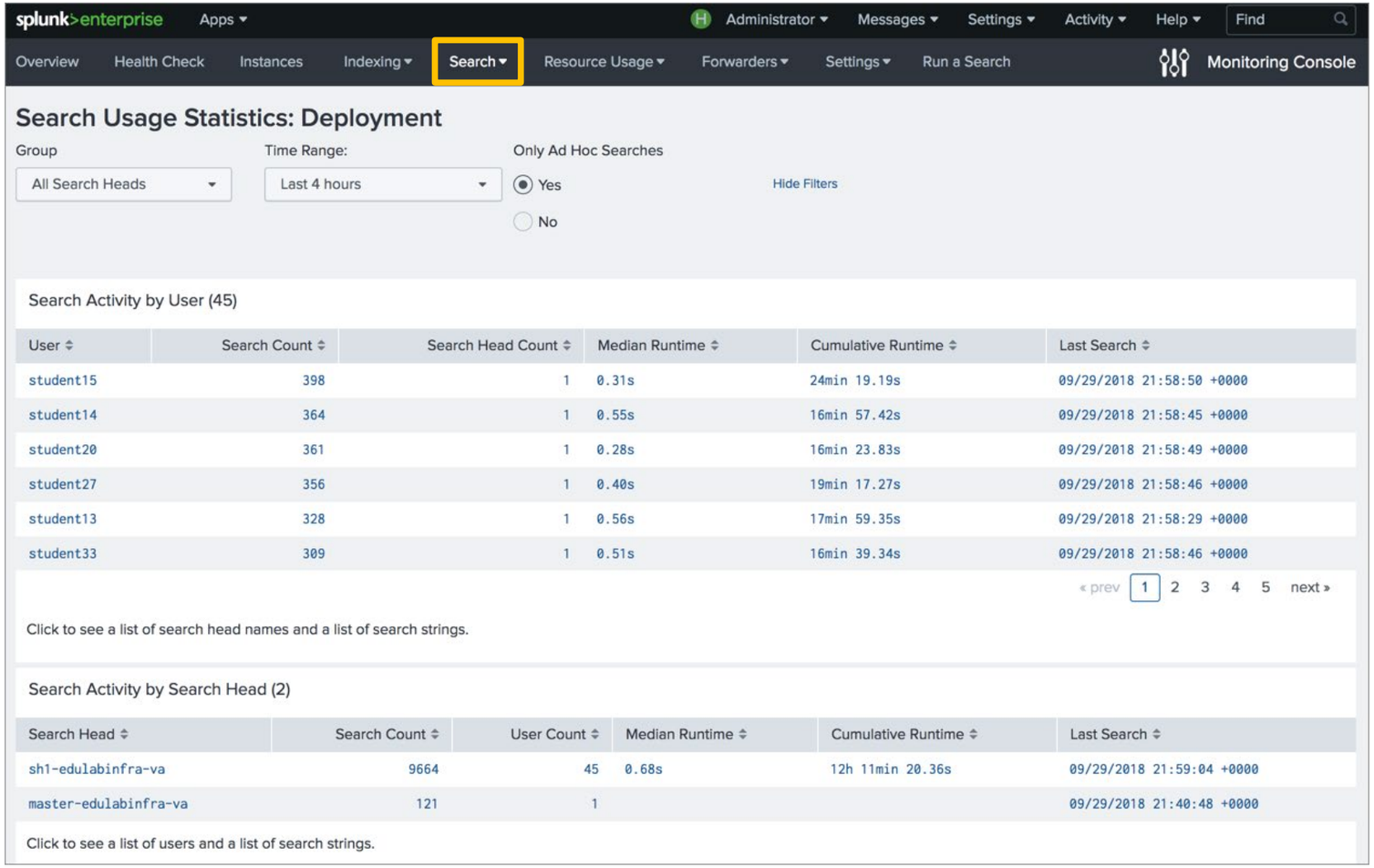
- Performance
- Indexer Clustering
- Indexes and volumes
- Inputs
- License usage



Search Statistics

Search provides stats for search activity such as:

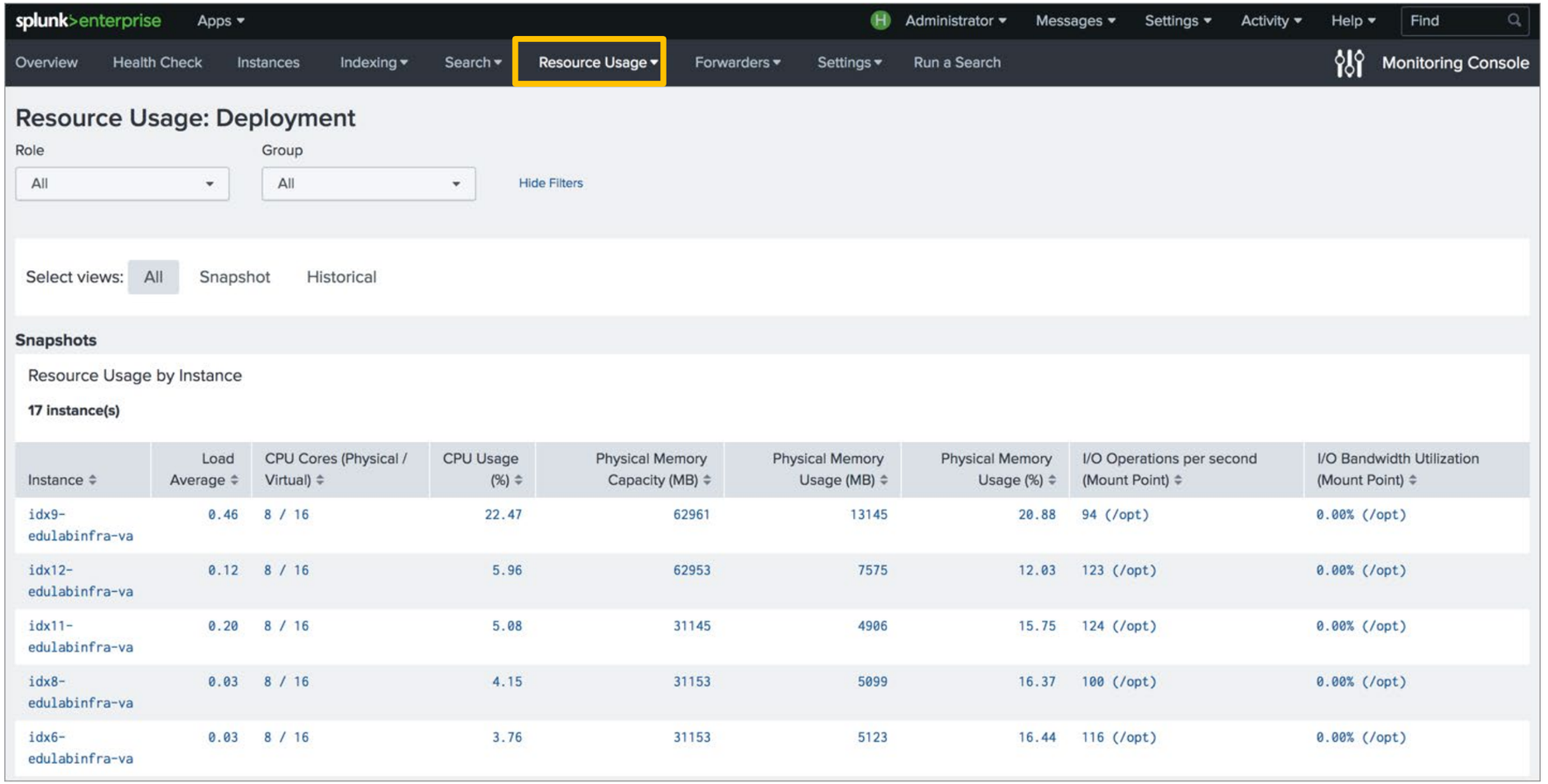
- Searches run by user
- Search duration
- Most run searches



Resource Usage

Resource Usage provides snapshots and detailed information about:

- Memory
- CPU
- Disk usage (by deployment or machine)



Improve Performance with `limits.conf`

- If you have unused CPU/memory resources, you can set multiple search pipelines
- Indexing real-time significantly improves performance if there are many real-time searches
  - Normally, real-time searches read the indexing queue
  - Indexing real-time causes the indexer to read the indexes on disk and collect events as they arrive in the hot buckets

`limits.conf` (Indexer)

```
[search]
batch_search_max_pipeline = 2

[realtime]
indexed_realtime_use_by_default = true
indexed_realtime_disk_sync_delay = 60
indexed_realtime_default_span = 1
indexed_realtime_maximum_span = 0
```


Tune **props.conf**

- Indexing time improves significantly by including the following parameters in all **props.conf** files at the indexer-level
- These parameters can also be included in **props.conf** files on search heads, however they apply at index-time and will have no effect if they are only on the search heads

$SPLUNK_HOME/etc/system/local/props.conf

```
    line_breaker =
(LM) should_linemerge = false
(TP) time_prefix =
(MLA)max_timestamp_lookahead =
(TF) time_format =
     truncate =
(AP) annotate_punct = false
     tz=
```

Note

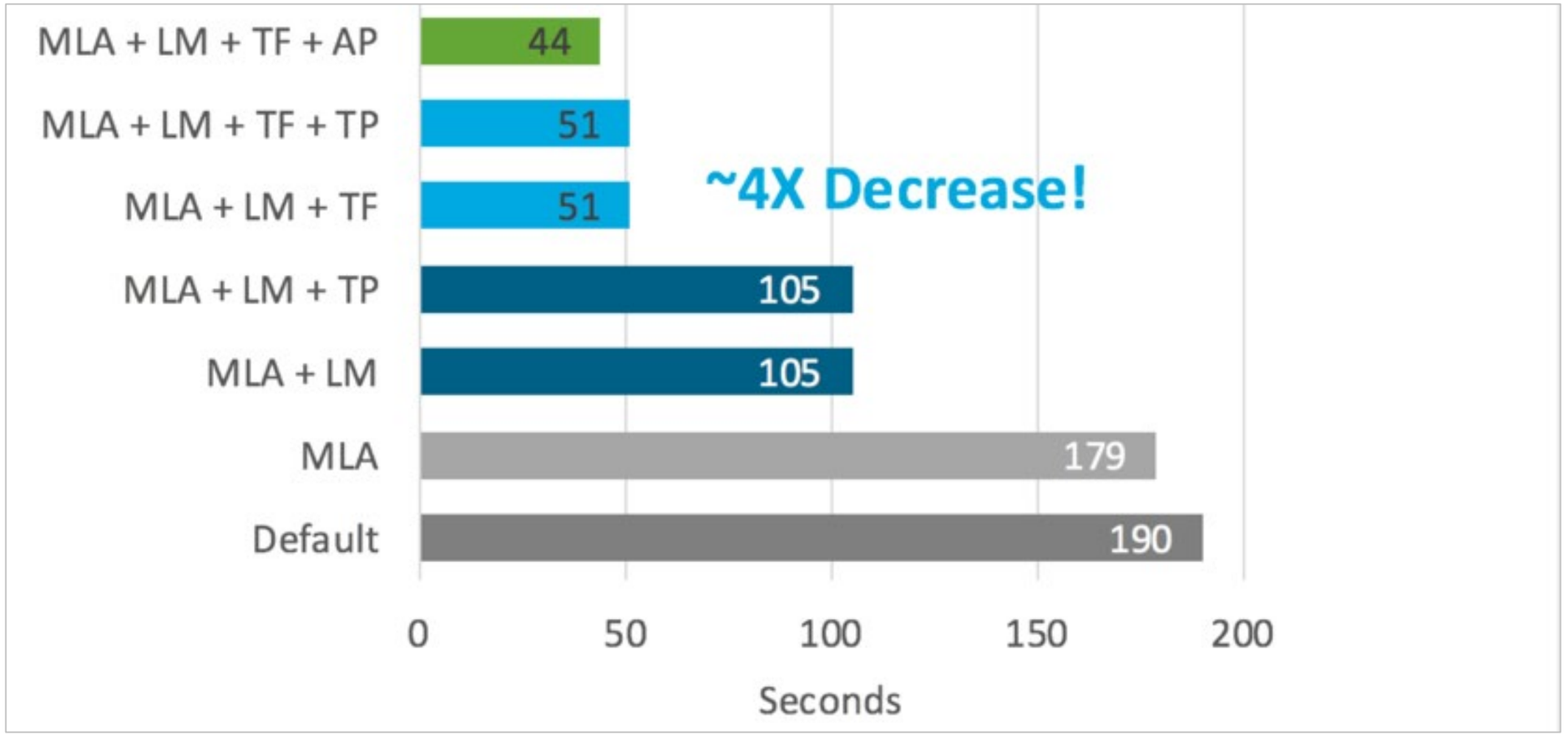
If the **punct** field is being used, DO NOT set **annotate_punct = false**

Tune **props.conf** (cont.)

- **line_breaker=** goes hand-in-hand with **should_linemerge=**
- Understand use cases before turning off **annotate_punct=**
- If this is disabled, the **punct** field will no longer be available
- **tz=** The Universal Forwarder will automatically include the time zone for source system
- If you are not using the Universal Forwarder, it is important to include **TZ** in your configs so that time is displayed properly

Tune **`props.conf`** (cont.)

Indexing Pipeline Test Results



conf.splunk.com/session/2015/conf2015_DBitincka_Splunk_Deploying_NotesonOptimizingSplunk.pdf

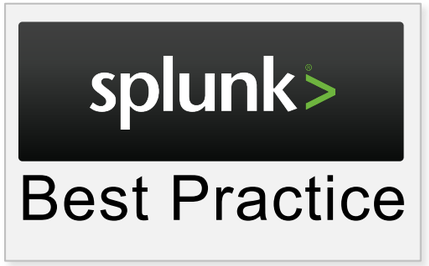
Search Performance – Types of Searches

Type of search	Description	Indexer throughput	Impact
Dense	A large percentage of the data matches the search	Up to 50K matching events per second	CPU bound
Sparse	A small percentage of data matches the search	Up to 5K matching events per second	CPU bound
Super-sparse	A "needle in a haystack" search Indexer must check all buckets to find results Time consuming for large numbers of buckets	Up to 2 seconds per bucket	Primarily I/O bound
Rare	Similar to super-sparse searches, but bloom filters are able to eliminate buckets that don't include search results	10 – 15 buckets per second	Primarily I/O bound

docs.splunk.com/Documentation/Splunk/latest/Search/Aboutsearch

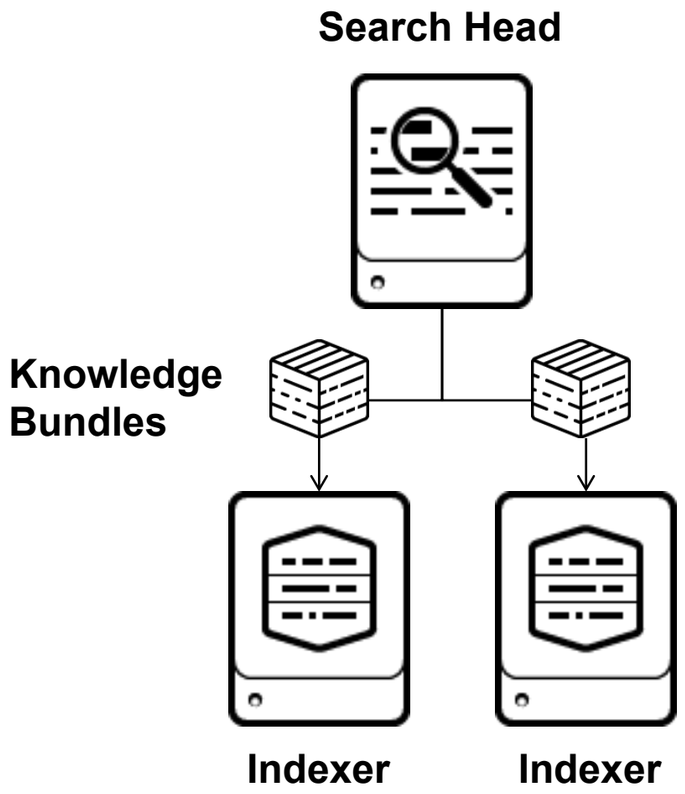
Improving Search Performance

- Make sure disk I/O is as good as you can get
  - Increase CPU hardware only if needed
- Most search performance issues can be addressed by adding additional search peers (indexers)
- Look at resource consumption on both the indexer tier and search head tier to diagnose slow searches
- Rebalance buckets (only available in indexer clustering)



Knowledge Bundles

- When initiating a distributed search, the search head replicates its knowledge objects (KOs) in the form of a knowledge bundle to its search peers
  - Therefore, indexers may receive nearly the entire contents of all the search head's apps
- If an app contains large files that do not need to be shared with the indexers, blacklist large lookup files
- Be careful not to eliminate needed KOs



http://docs.splunk.com/Documentation/Splunk/latest/DistSearch/Limittheknowledgebundlesize

Splunk Workload Management

A mechanism in Splunk that allows you to:

- Reserve system resources for search and indexing processes
- Prioritize critical search workloads
- Prevent over-usage of system resources
- Avoid data ingestion latency due to heavy search load
- Create rules to reserve and assign system resources based on apps and roles

Workload Management – Use Cases

- Workaround solutions to managing search loads are ineffective when there is excessive usage by a single incoming ingest data stream or by a single end user
- Critical searches may be skipped or queued and indexing is slow resulting in data lag
- Onboarding new users/data disrupts existing ingestion and search performance

For detailed information on the configuration of Workload management:
docs.splunk.com/Documentation/Splunk/latest/Workloads/PrerequisiteLinuxconfiguration
docs.splunk.com/Documentation/Splunk/latest/Workloads/Configureworkloadmanagement

Module 8 Lab Exercise

Time: 15 minutes

Task:

- Use the MC to determine the following:
  - The resource usage for the test environment
  - The index performance for the test environment
  - The search performance for the test environment
  - Based on your findings, what changes should be made to maximize performance?

Module 9:
Use Cases

Module Objectives

- Review different use cases
- Answer questions and discuss final architecture solution

Energy Service Provider

Use Case

Energy Service provider needs to detect potential breaches and increase the scalability of their infrastructure. The Ops and SCO teams need access to the data.

Assets

- Cisco Routers
- Cisco Firewalls
- IBM iSeries
- Windows Server Logs
- Cisco Switches
- MSSQL/Oracle Servers
- F5 Load Balancers
- App Servers
- Syslog Forwarders

Energy Service Provider (cont.)

Data Centers

1

Data Indexed Daily

- 100GB

Data Retention Period

- Hot/Warm 30 – 90 Days
- Cold - 12 months

Data Inventory

The customer decided on ES and wants a single site index cluster with a RF=2 and a SF=2

Data Source	Max Daily Usage	Retention	Days in Hot/Warm	Access	Collection Method
Cisco general logs	15	60	30	IT Ops / Sec	UF on Syslog server
Cisco SEC logs	2	60	30	Sec	UF on Syslog server
IBM iSeries	20	365	30	IT Ops / Sec	
Windows server logs	6	60	30	Sec	UF on Windows servers
MSSQL /Oracle servers	15	365	60	IT Ops / Sec	UF on server
F5 load balancers	1	365	30	IT Ops / Sec	UF on Syslog server
Windows app servers	30	60	30	IT Ops / Sec	UF on Windows servers
Syslog server	1	90	30	IT Ops / Sec	UF on Syslog server
total	90				

Energy Service Provider - Discussion

- What is the minimum number of indexes required?
- How many indexers do you recommend?
- Would you have the master node and license master on the same Splunk instance?
- In the long term, would you look to replace the syslog servers and just listen on TCP ports for the data?
- How would data get from iSeries into Splunk?

Financial Service Provider

Use Case

This company needs to monitor the health of its servers on a global deployment level. They also need to monitor the SAP, Informix and dev-ops environment for an app development project. The customer is also interested in ES and ITSI.

Assets

- Solaris Servers (10,000)
- Windows Servers (25,000)
- Linux Servers (15,000)
- Cisco Switches and Routers (2,000)
- IBM Mainframe (1)
- Legacy Gateways (8)

Data Indexed Daily

3TB – 4TB

Financial Service Provider (cont.)

Data Centers

2 (New York, Zurich)

Data Indexed Daily

3TB – 4TB

Financial Service Provider - Discussion

- Would you treat this as one Splunk deployment or two?
- How would you look to collect data from the IBM mainframe?
- The customer ends up using 50 indexers and 5 search heads. Assuming an equal split of users/data at each site, what does your network topology look like?

Retail Company

Use Case

This department store needs to monitor its rewards program cash flow and the amount of time a credit card takes to process a sale from the bluebird banking servers. There are two dual-homed data centers connected via WAN and all 1000 stores are connected via corporate VPN.

They want to roll out their deployment in two phases:

- Start with four users to monitor the rewards program
- Add 10 more users over the next 6 months

Retail Company (cont.)

Assets

- RF Scanners
- Bluebird Banking Servers
- HP Printers
- Windows Desktop Servers
- Windows Store Domain Servers (two at each store to collect data from devices)

Data Centers

2

Data Indexed Daily

2.4TB

Data Retention Period

- Hot/Warm - 3 months (186 days)
- Cold - 12 months

Retail - Discussion

- How many indexers and search heads do you suggest for this customer?
- Would you use index or search head clustering for this deployment?
- Is a two stage or one stage approach recommended to the customer?
- The customer is on a virtualization campaign. Which Splunk instances do you recommend for virtualization?

Wrap-up Slides

Resources and Additional Study

- Splunk documentation for architects
  - Installation Manual (for hardware and capacity planning information)
  - Distributed Deployment Manual
  - Capacity Planning Manual
  - Other manuals for specific topics
- Splunk Answers

  answers.splunk.com
- Splunk's public wiki (watch dates for outdated topics)

  www.splunk.com/wiki/Deploy:Deployment_topics

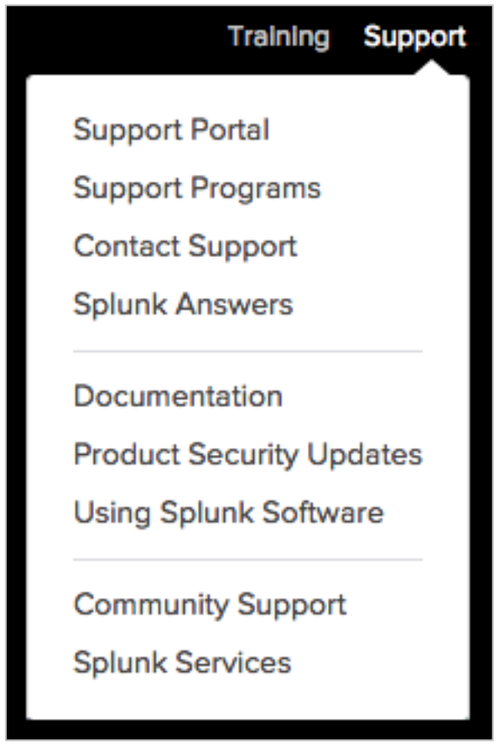
  Deployment scenarios, performance info and other useful topics

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

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)



What's Next?

- Splunk Certification program
  www.splunk.com/en_us/training/faq-training.html
  - Splunk Core Certified User
  - Splunk Core Certified Power User
  - Splunk Enterprise Certified Admin
  - Splunk Enterprise Certified Architect
  - Splunk Certified Developer
- Program information
  - www.splunk.com/pdfs/training/Splunk-Certification-Handbook-v.8.31.2018.pdf
- Exam registration
  - www.splunk.com/pdfs/training/Exam-Registration-Tutorial.pdf

- If you have further questions, send an email to: certification@splunk.com

SAVE THE DATE!

Splunk .conf21

October 18-21, 2021

Las Vegas, Nevada

splunk> .conf20

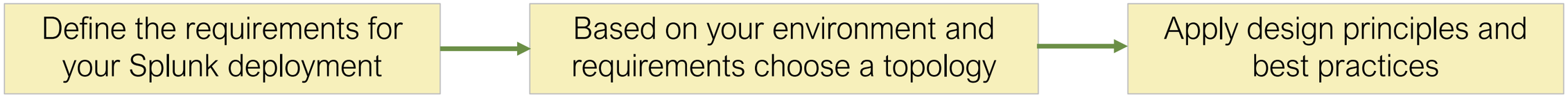
Thank You

Appendix

Appendix A: Splunk Validated Architectures

Splunk Validated Architectures (SVAs)

- Proven reference architectures
- Designed by Splunk Architects based on best practices
- Repeatable deployments
- Offer topology options for your environment and requirements

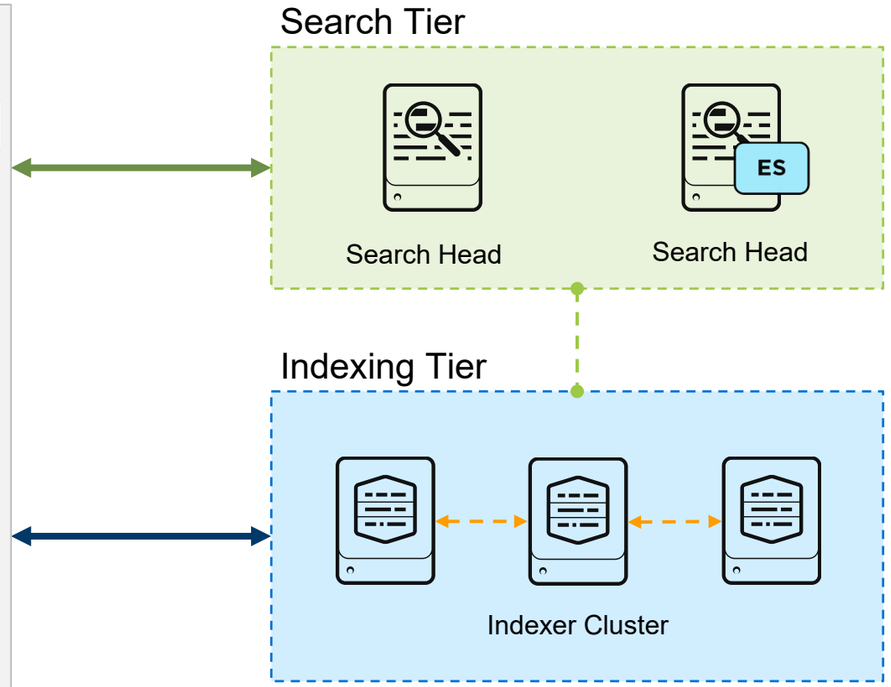


For detailed information about SVAs read the following white paper:
www.splunk.com/pdfs/white-papers/splunk-validated-architectures.pdf

Understanding Topology Categories

Code	Search Tier Categories
1	Single search head
2	Multiple search heads are required
3	Search head cluster is required
4	Search head cluster that spans multiple sites
+10	Dedicated search head is required for ES. Add 10 to the search tier and read specific requirements for ES

Code	Indexing Tier Categories
S	Indexer of a single-server Splunk deployment
D	Distributed indexer tier with at least 2 indexers
C	Cluster indexer tier (data replication required)
M	Cluster indexer tier with multiple sites



= Code: C11

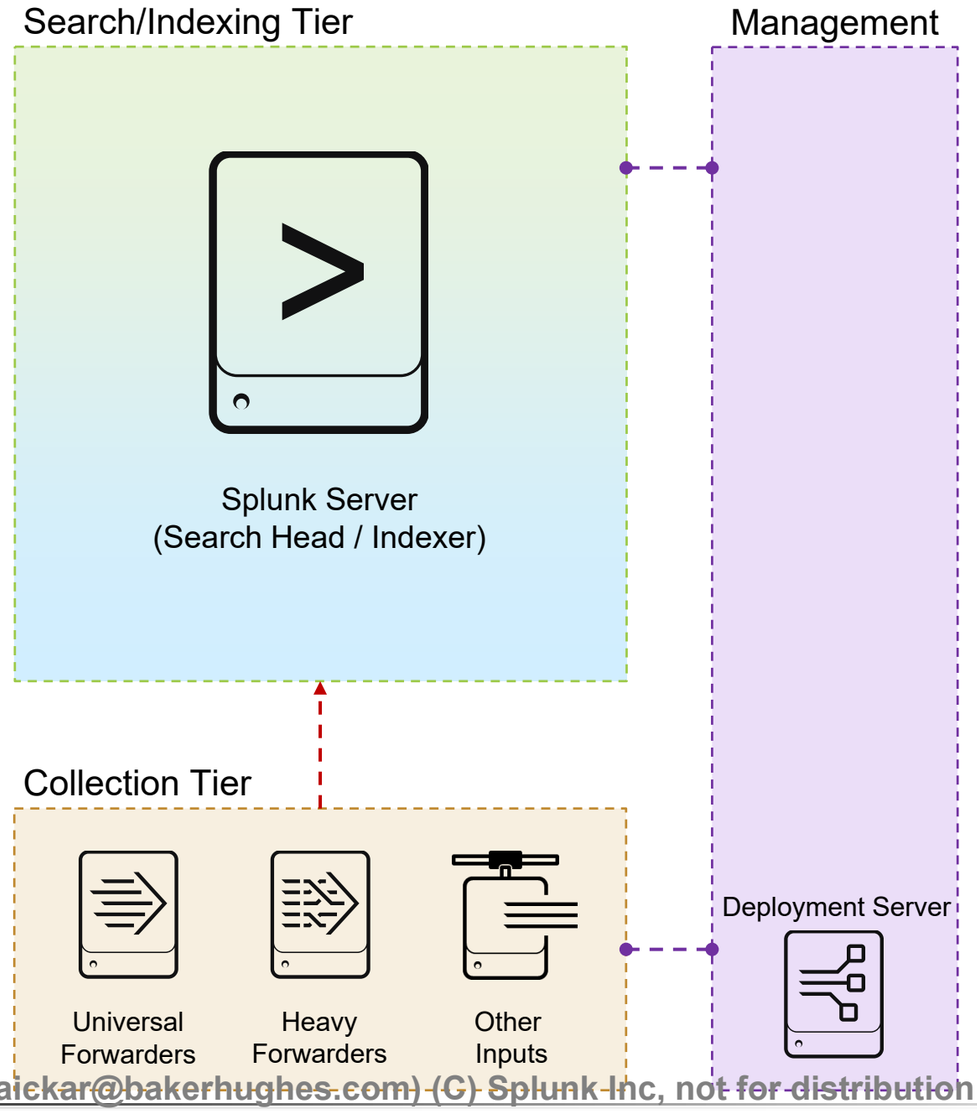
S1 - Single Server

Code	Search Tier Categories
1	Single search head
2	Multiple search heads are required
3	Search head cluster is required
4	Search head cluster that spans multiple sites
+10	Dedicated search head is required for ES. Add 10 to the search tier and read specific requirements for ES

Code	Indexing Tier Categories
S	Indexer of a single-server Splunk deployment
D	Distributed indexer tier with at least 2 indexers
C	Cluster indexer tier (data replication required)
M	Cluster indexer tier with multiple sites

Code:

S1



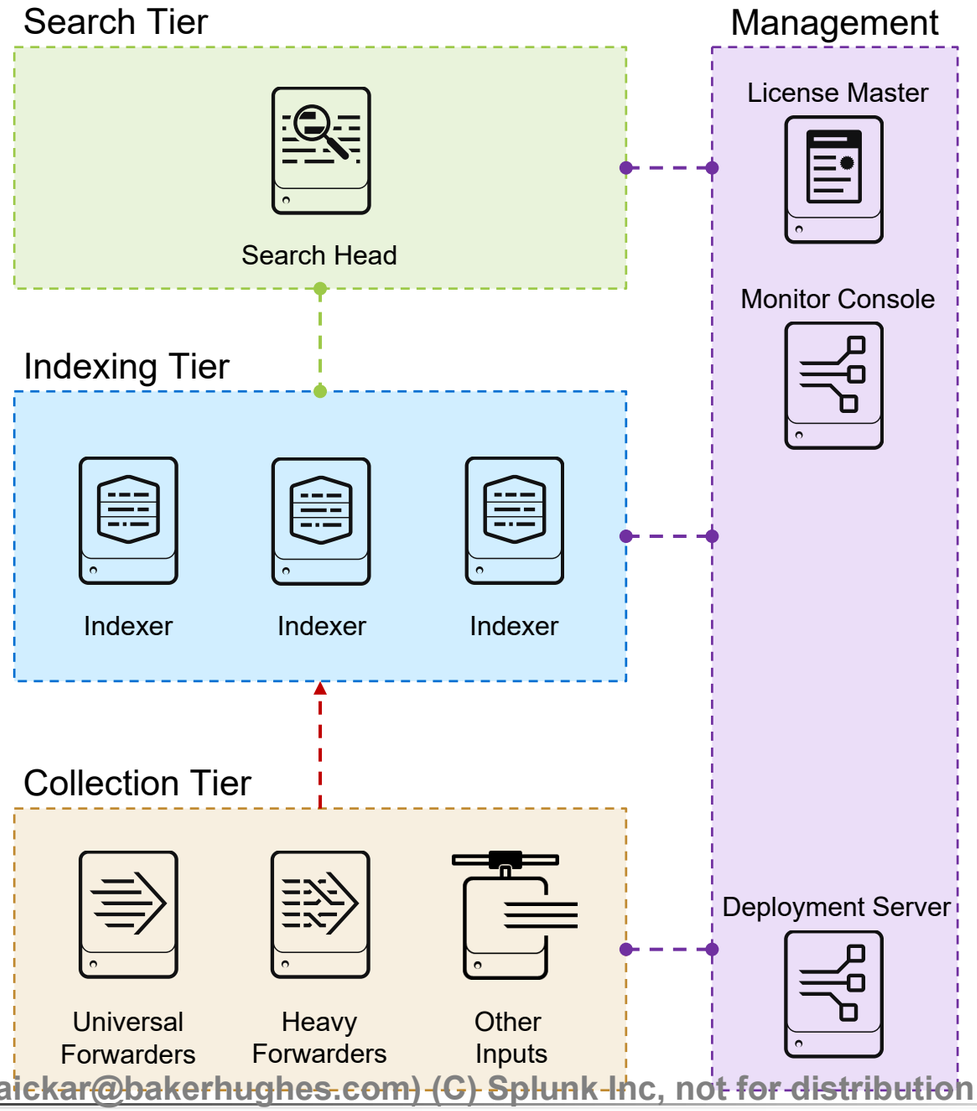
 | 12 February 2021

D1 - Distributed Non-Cluster (Single Site)

Code	Search Tier Categories
1	Single search head
2	Multiple search heads are required
3	Search head cluster is required
4	Search head cluster that spans multiple sites
+10	Dedicated search head is required for ES. Add 10 to the search tier and read specific requirements for ES

Code	Indexing Tier Categories
S	Indexer of a single-server Splunk deployment
D	Distributed indexer tier with at least 2 indexers
C	Cluster indexer tier (data replication required)
M	Cluster indexer tier with multiple sites

Code:
D1/D11

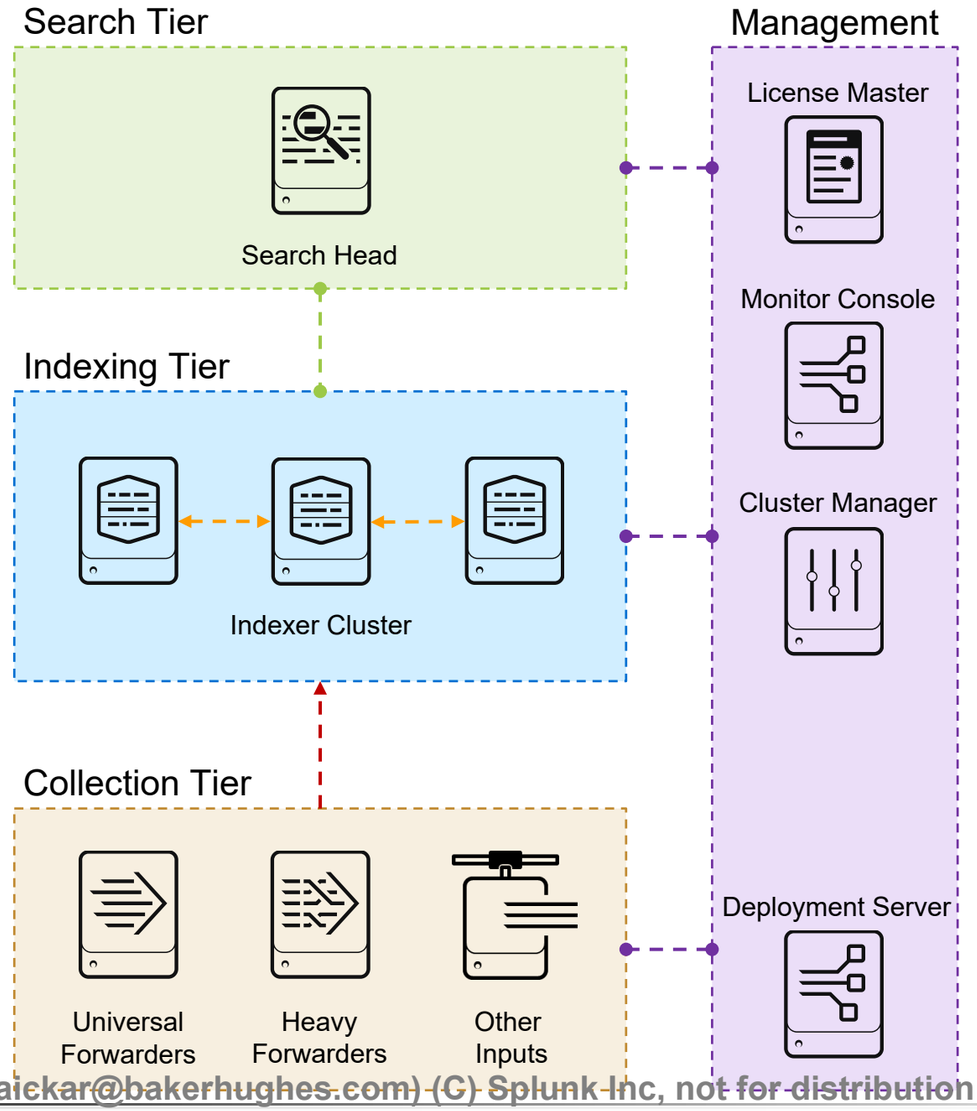


C1 - Distributed Cluster (Single Site)

Code	Search Tier Categories
1	Single search head
2	Multiple search heads are required
3	Search head cluster is required
4	Search head cluster that spans multiple sites
+10	Dedicated search head is required for ES. Add 10 to the search tier and read specific requirements for ES

Code	Indexing Tier Categories
S	Indexer of a single-server Splunk deployment
D	Distributed indexer tier with at least 2 indexers
C	Cluster indexer tier (data replication required)
M	Cluster indexer tier with multiple sites

Code:
C1/C11

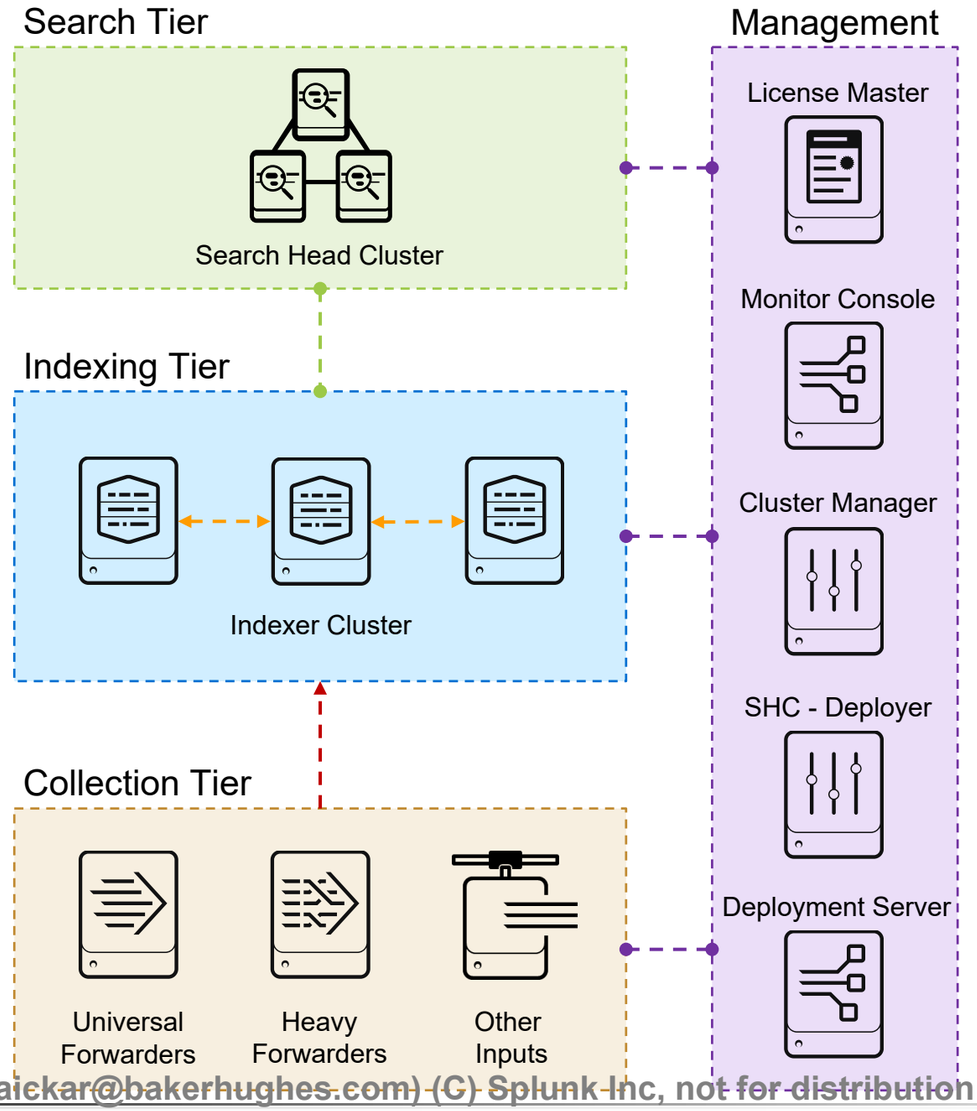


C3 - Distributed Cluster + SHC (Single Site)

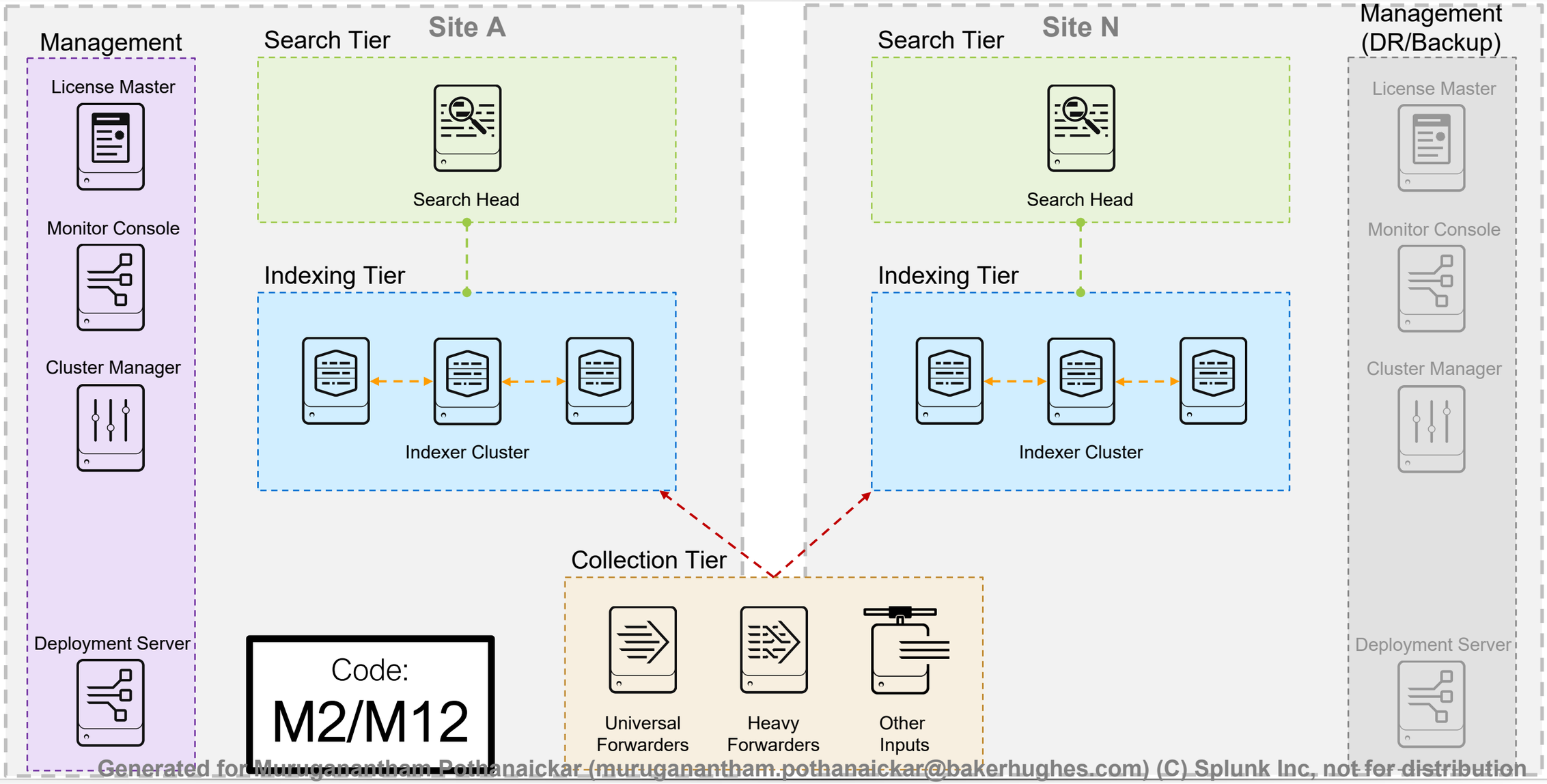
Code	Search Tier Categories
1	Single search head
2	Multiple search heads are required
3	Search head cluster is required
4	Search head cluster that spans multiple sites
+10	Dedicated search head is required for ES. Add 10 to the search tier and read specific requirements for ES

Code	Indexing Tier Categories
S	Indexer of a single-server Splunk deployment
D	Distributed indexer tier with at least 2 indexers
C	Cluster indexer tier (data replication required)
M	Cluster indexer tier with multiple sites

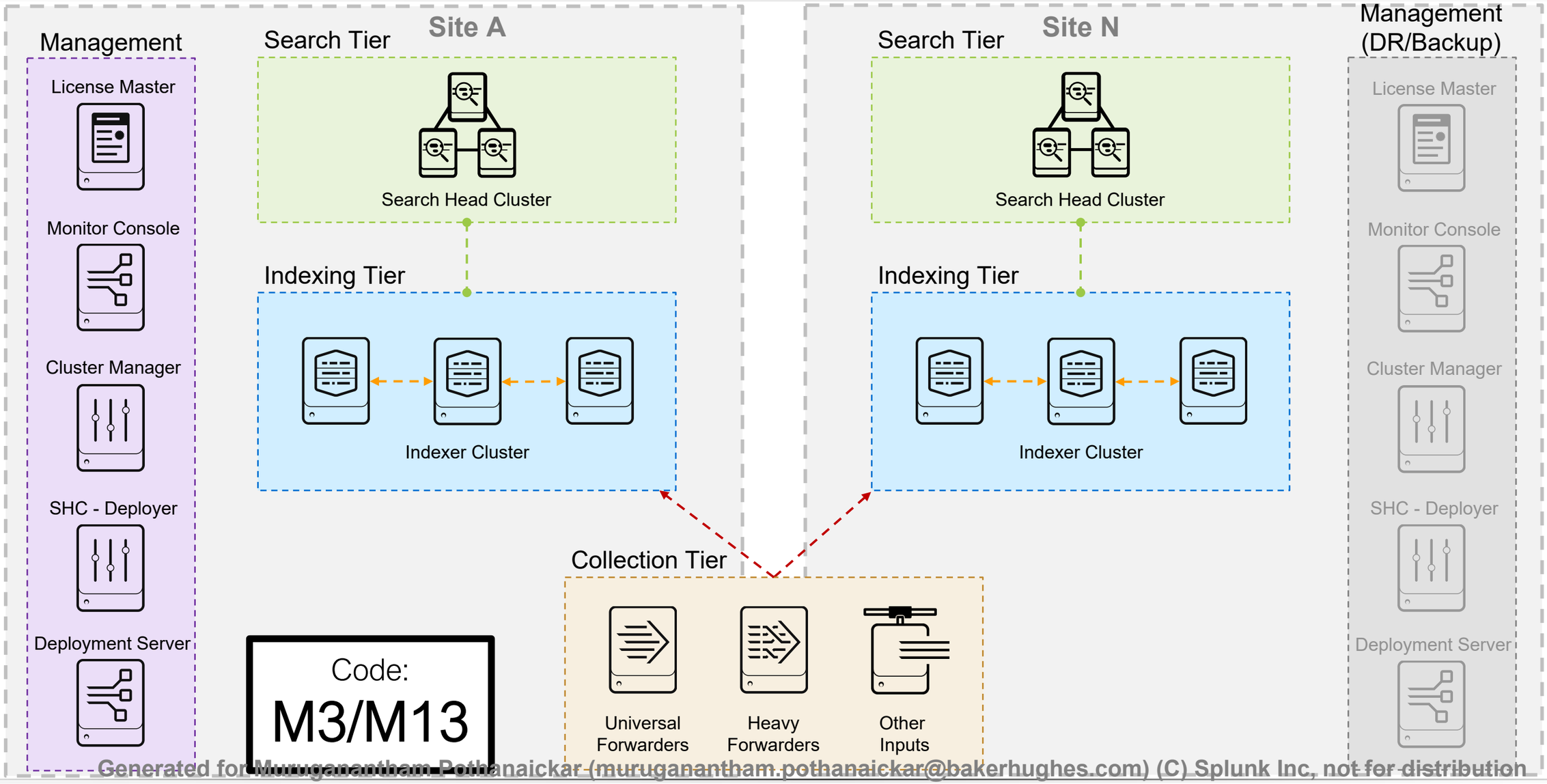
Code:
C3/C13



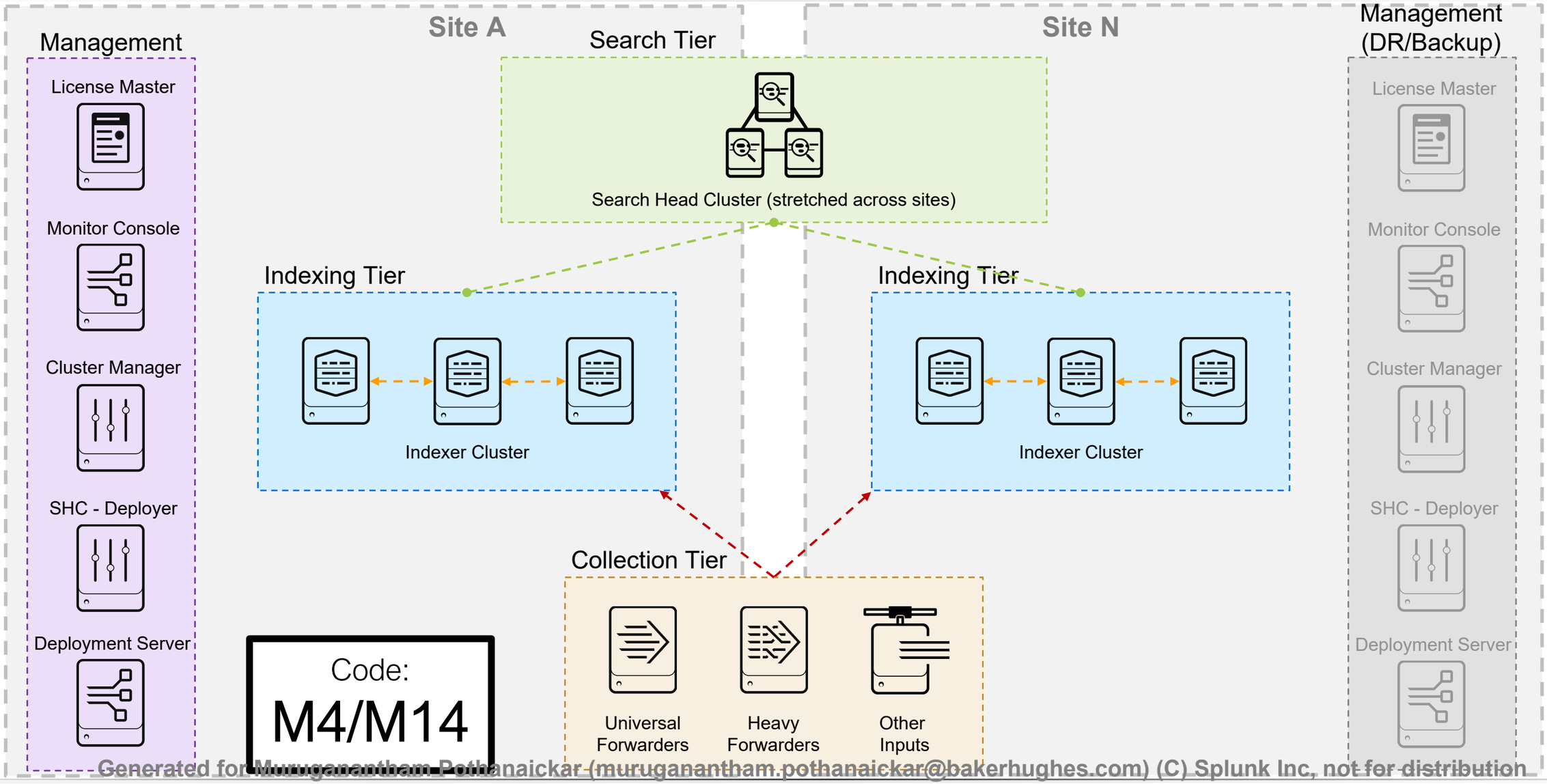
M2 - Distributed Cluster (Multi-Site)



M3 - Multi-Site With Search Head Clusters



M4 - Multi-Site With a Spanning SHC

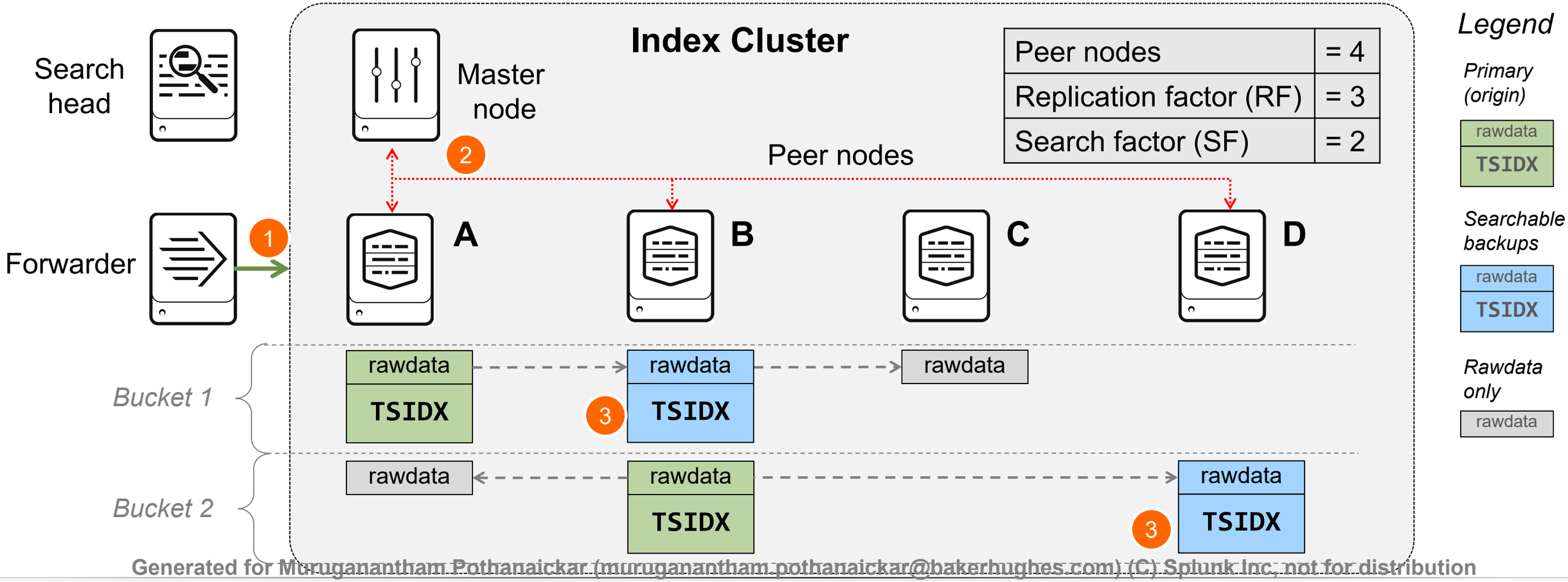


Appendix B: Indexer Cluster Action Review

Factors in Action – Data Replication

Complete & Valid

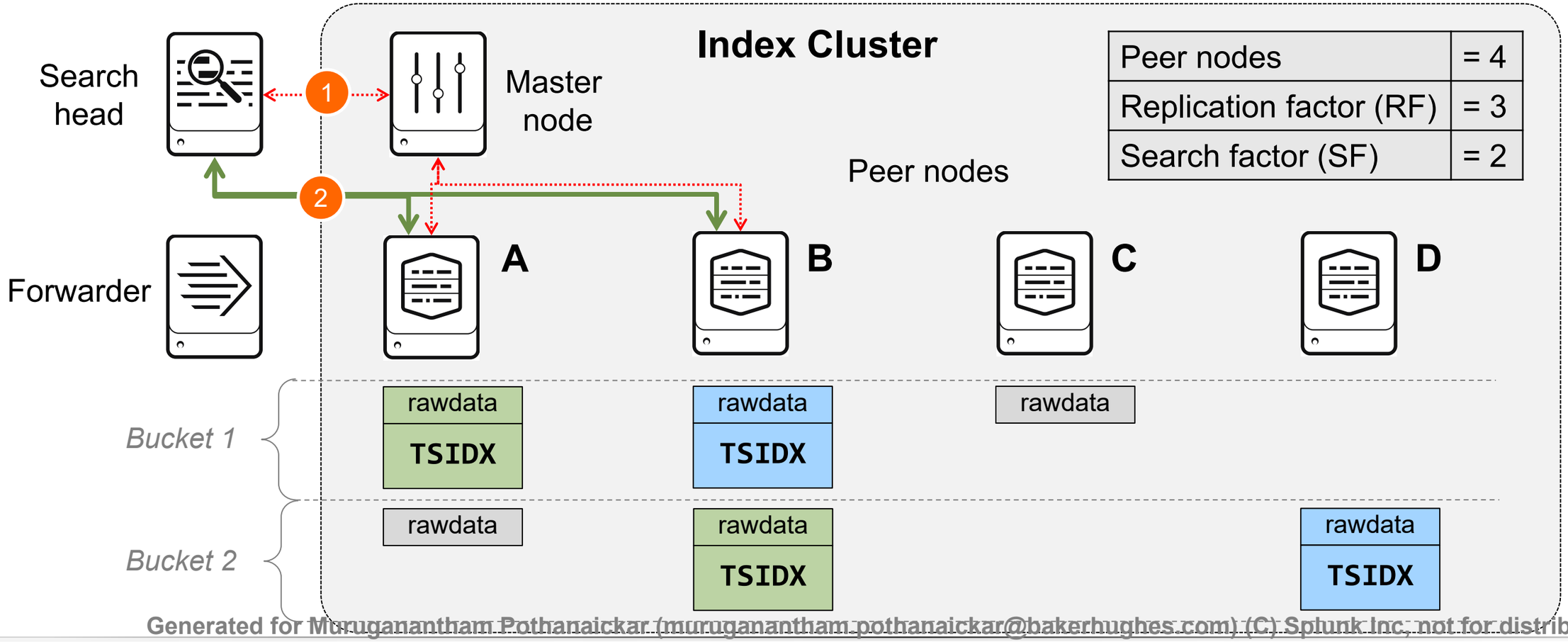
1. The peer receiving the data has the original bucket (Primary)
2. The Master Node allocates replication jobs to the original peer to copy rawdata to randomly selected peers to meet RF
3. The Master Node allocates jobs to random peers with a rawdata copy to build the `tsidx` file locally



Factors in Action – Search

Complete & Valid

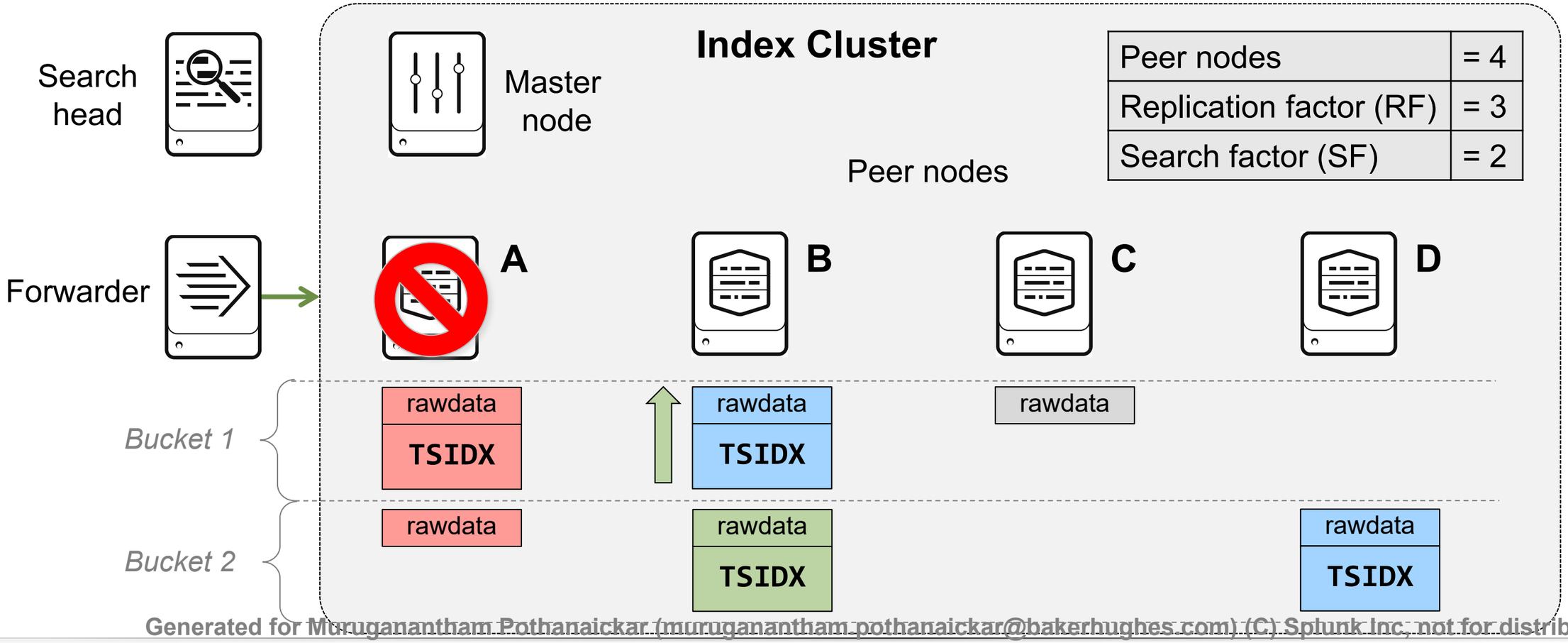
When a user initiates a search:
1. Master Node responds with a manifest of current primary peers
2. Search head dispatches search job to the peers with primary buckets



Factors in Action – Initial Primary Loss

Valid but Not Complete

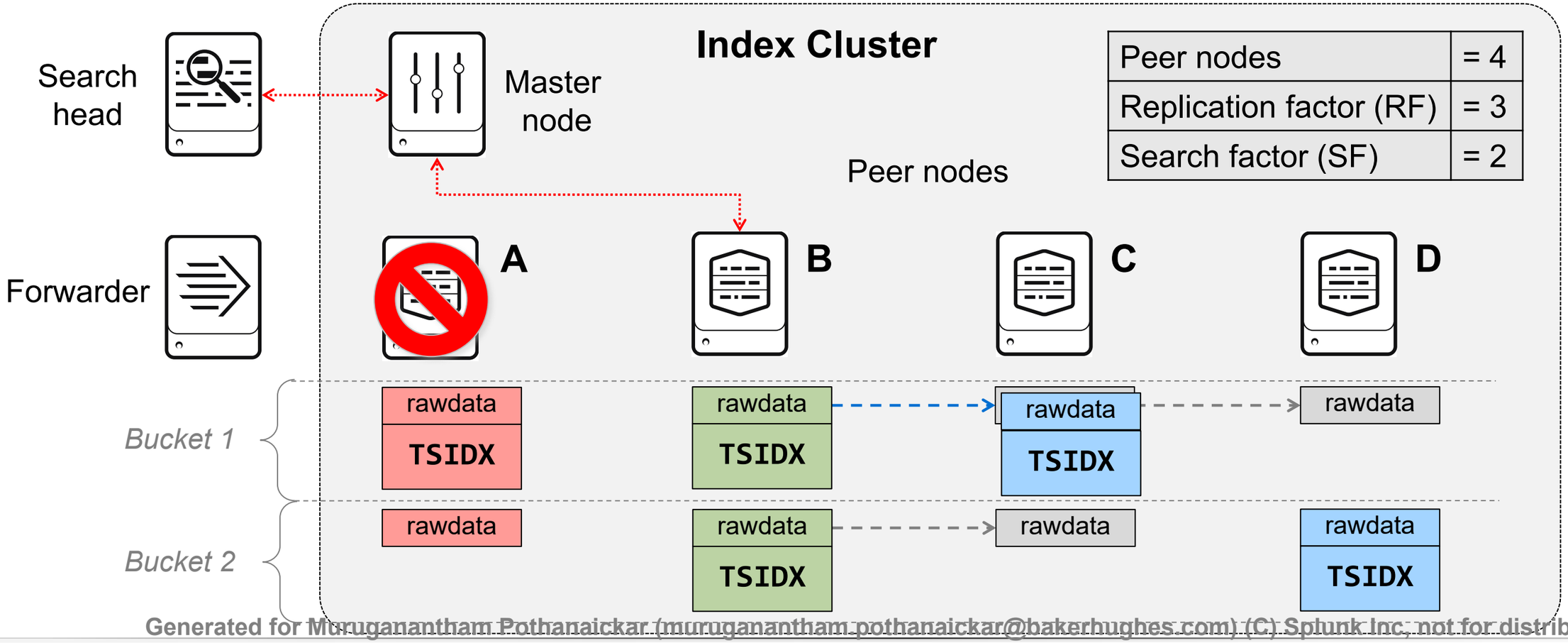
In the scenario of losing Peer A, the Master Node randomly instructs the peers with Searchable Backups to promote them to Primary



Factors in Action – Initial Primary Loss (cont.)

Complete & Valid

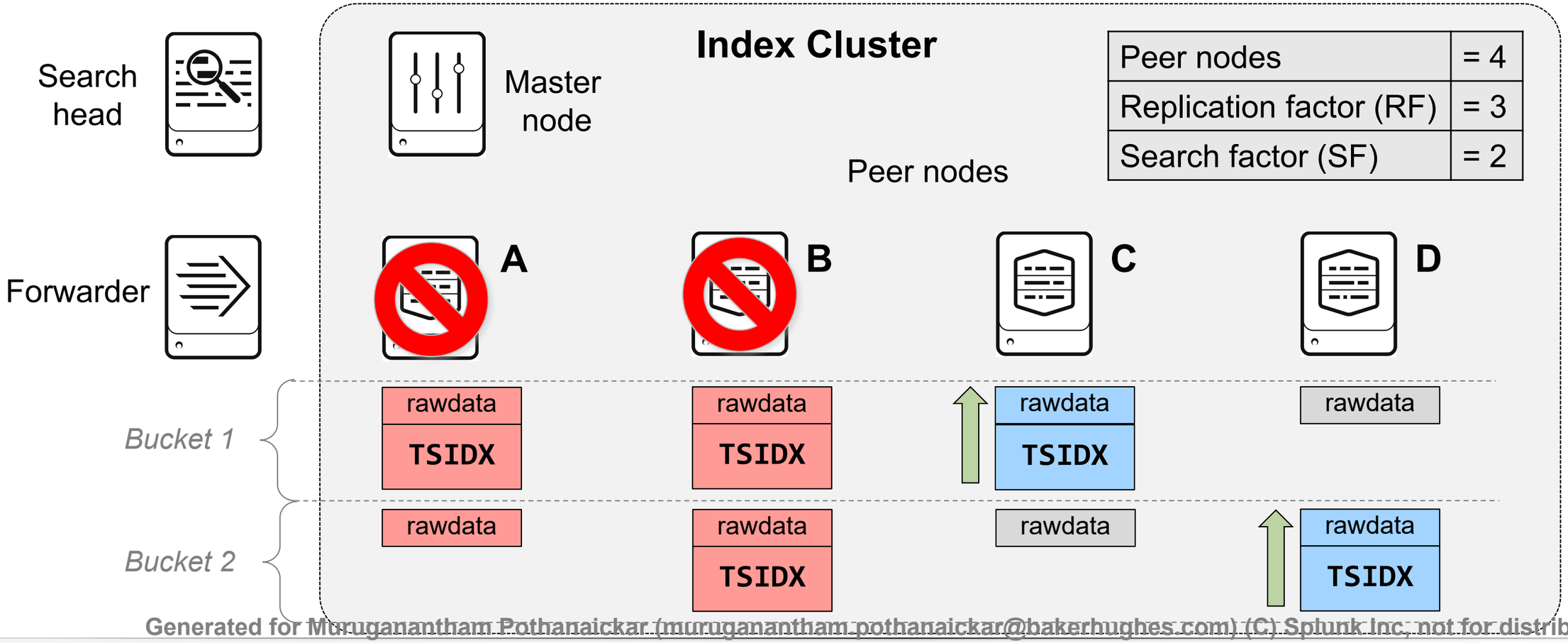
The cluster will attempt to establish the RF/SF by copying the **`.tsidx`** files to the **Rawdata Only** buckets (promote them to **Searchable Backups**) and copying rawdata to the remaining peers



Factors in Action – Second Peer Loss

Valid but Not Complete

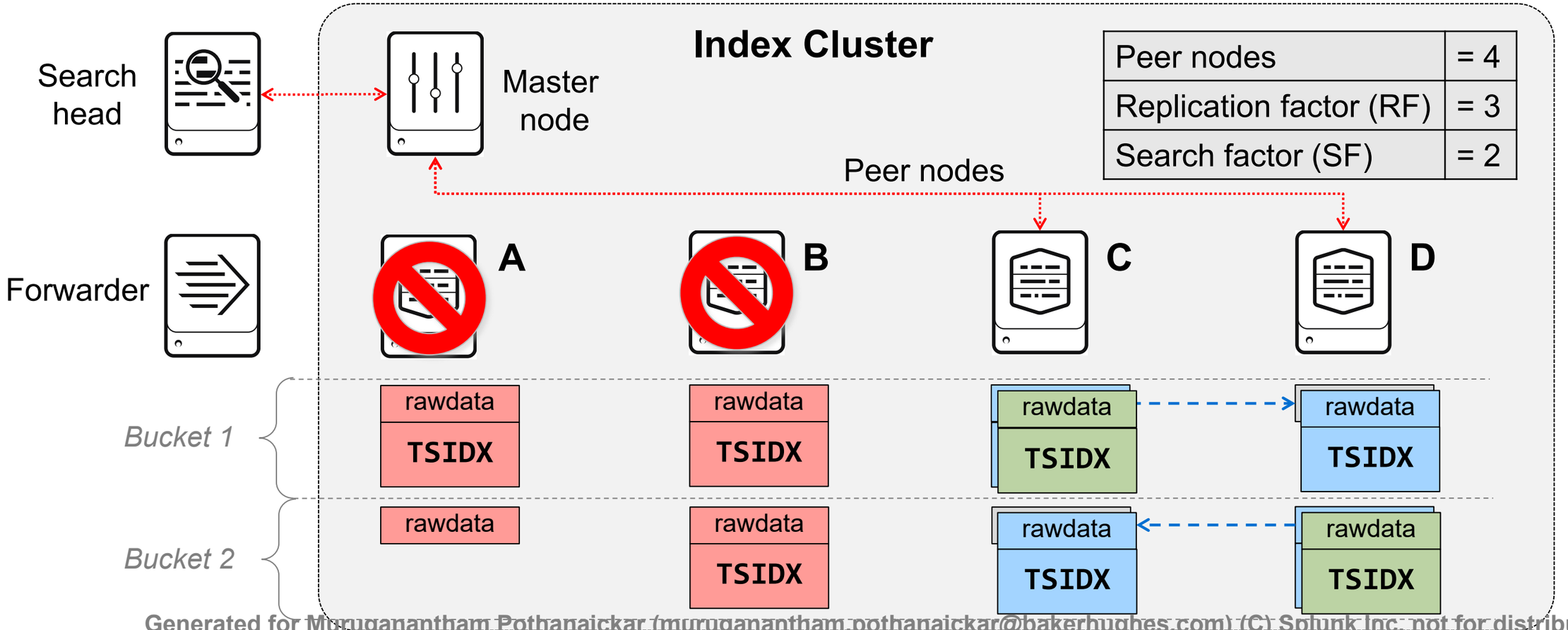
In the scenario of losing two peers, searchable backups are promoted to a primary copies



Factors in Action – Second Peer Loss (cont.)

Valid but Not Complete

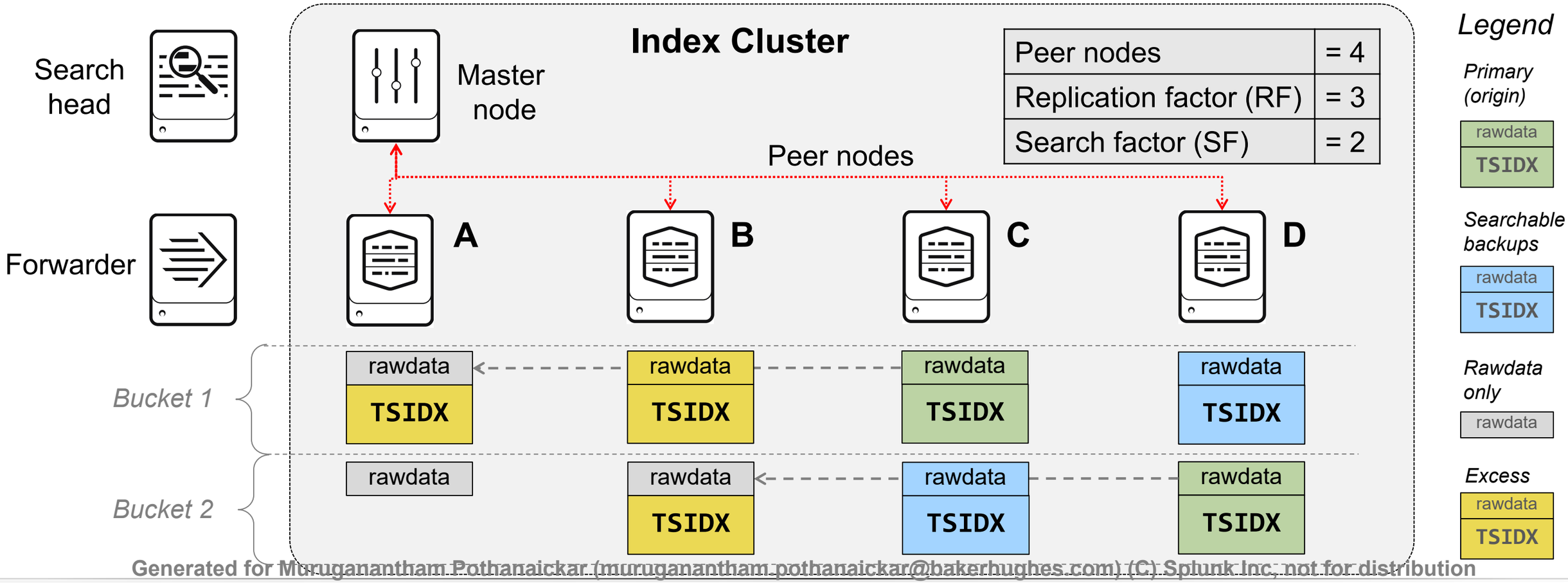
Rawdata copy promoted to searchable backup to meet SF, but RF cannot be met because the extra storage to maintain the copies does not exist



Factors in Action – Rebalancing

Complete & Valid After Rebalancing

- If the peers come back online, Splunk will automatically perform primary rebalancing and reassign primary buckets
- There will only be one primary at a time which will result in excess copies



Appendix C: Premium App Requirements

Splunk App for Enterprise Security (ES)

- Infrastructure impacts
  - A dedicated search head or search head cluster
  - 16 CPU / 32 GB RAM (Indexers and SH) ***minimum***
  - Requires extensive amount of data onboarding and configuration to work *properly*
  - One indexer per 100GB data indexed per day maximum
    - Assumes 15 correlation searches running
    - For more information about ES, read the following documentation

http://docs.splunk.com/Documentation/ES/latest/Install/Overview

Proper ES Sizing

- Sizing for ES is based on:
  - Data mix
  - Concurrent searches and users
  - Data Model acceleration
  - Assets & Identities (lookups)
- Example: 330GB Authentication Data + 70GB Network Traffic + 20GB Web + 130GB Other Data == 550GB/day total @ 20 concurrent searches
  - Sizing == 8 indexers with 24 cores

For more information about ES requirements, refer to:
docs.splunk.com/Documentation/ES/latest/Install/DeploymentPlanning

Note

Detailed information about ES deployments is discussed in the *Administering Splunk Enterprise Security* course.

Splunk App for IT Service Intelligence (ITSI)

- Infrastructure Impacts
  - Additional infrastructure may be needed, depending on the number of Key Performance Indicators (KPIs) that are tracked
    - The documentation has recommendations

For more information about ITSI, go to:

docs.splunk.com/Documentation/ITSI/latest/Configure/DeploymentPlanning

Splunk User Behavior Analytics (UBA)

- Hardware requirements
  - 50GB disk space for Splunk UBA installation
  - 500GB additional disk space for metadata
  - 16 CPU cores
  - 64 GB RAM
  - 800 IOPS
- Network Requirements
  - Static IP addresses for UBA servers
  - Firewalls and proxies must support inbound and outbound ports

Note

Contact Splunk Professional Services for installation assistance.

For more information go to:
docs.splunk.com/Documentation/UBA/latest/Install/Requirements

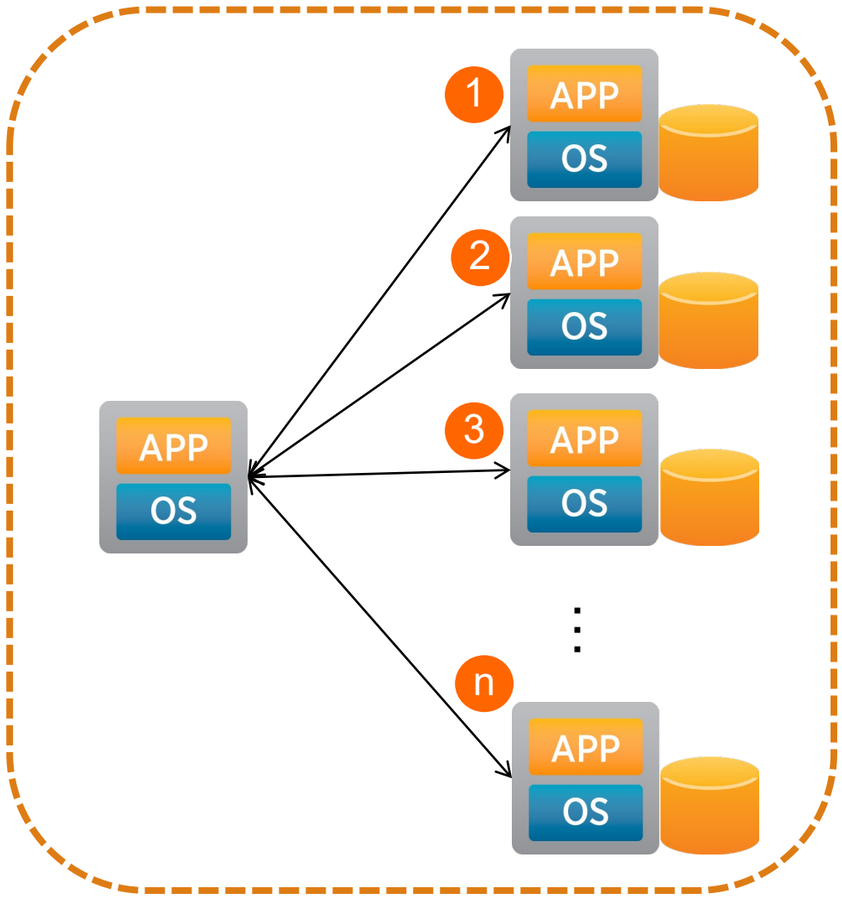
Appendix D: Search Considerations

Module Objectives

- Define MapReduce
- Discuss search performance
- Review how scheduled reports are dispatched
- Discuss differences between data summary methods

MapReduce Introduction

- A framework for processing parallelizable problems across huge datasets using a large number of computers (nodes) in a cluster
  en.wikipedia.org/wiki/MapReduce
- Splunk search uses this technology

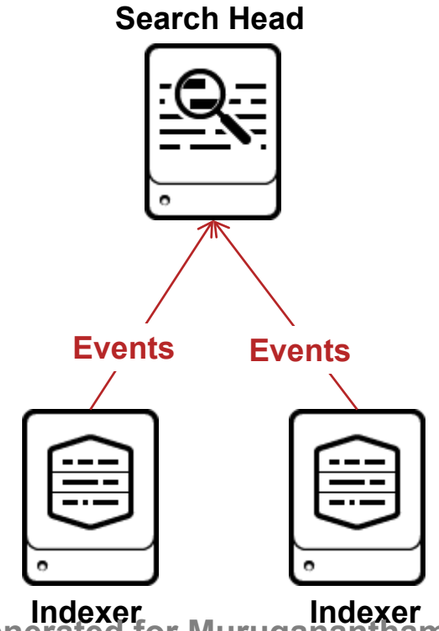


Source: Wikipedia

Performance Considerations for MapReduce

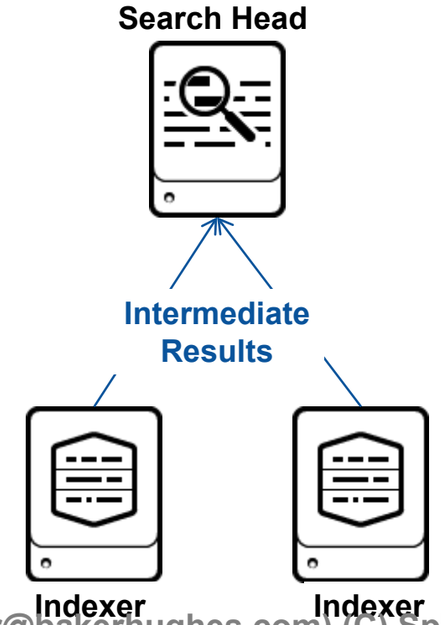
- Which searches MapReduce well? Which do not?
  - This is determined by how much of the work can be done on the indexers vs. how much manipulation of the search results must be done by the search head

Event searches and non-distributable commands



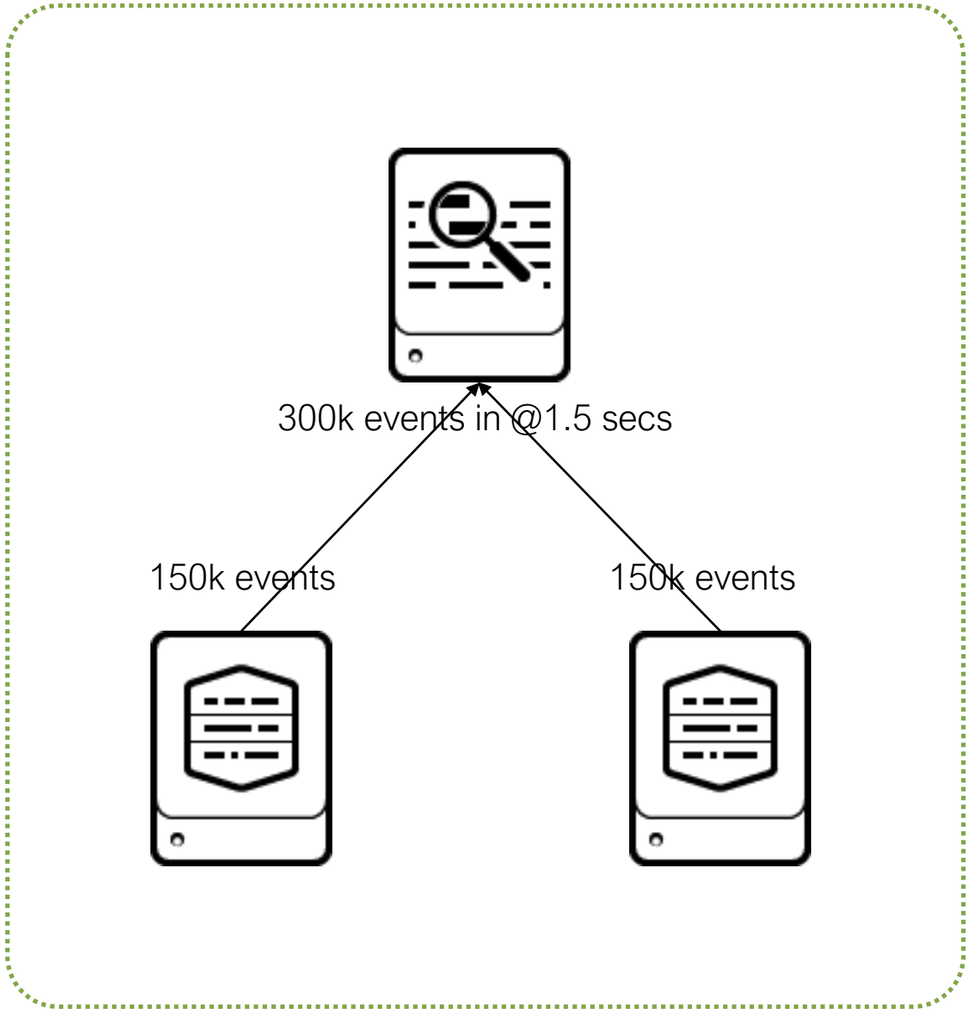
- Indexers retrieve events in parallel
- Efficient for event searches
- For other searches
  - Additional steps, if needed, must be done on the search head
  - CPU & memory bottlenecks can occur on the search head

Reporting searches



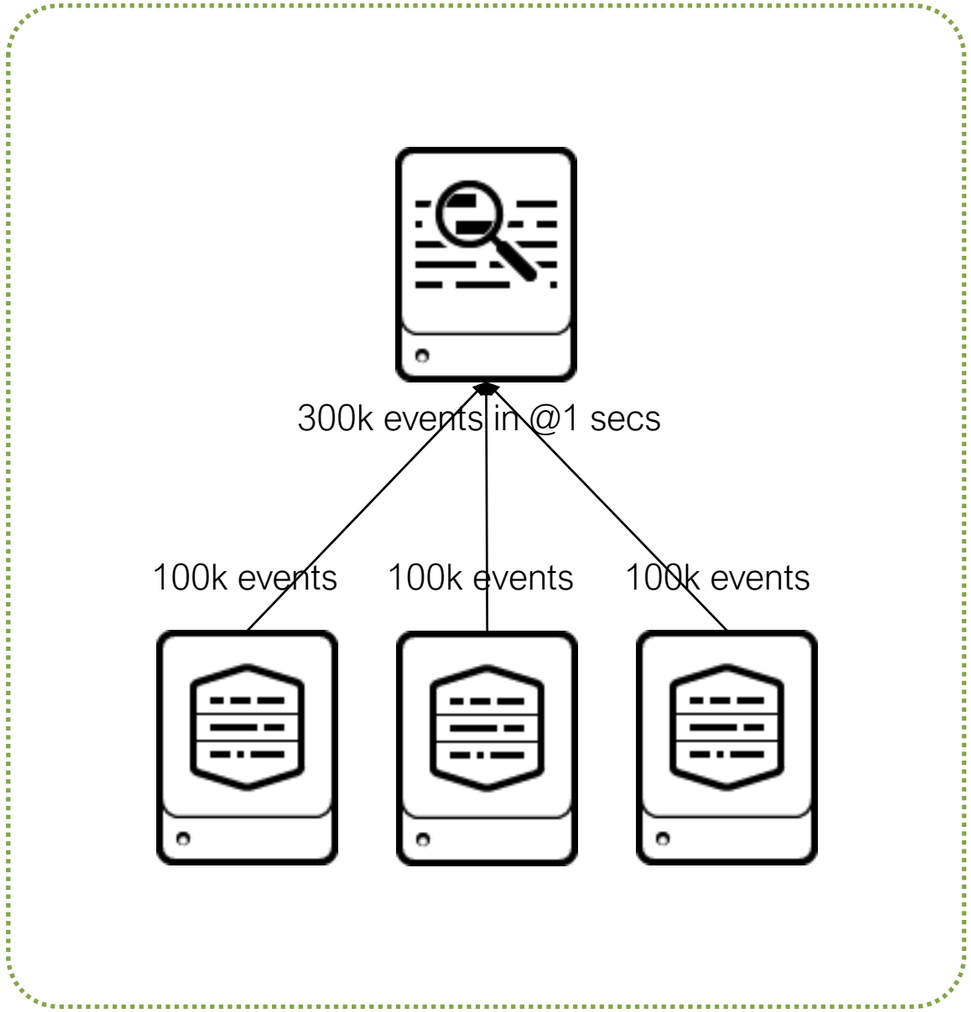
- Indexers can perform event retrieval and additional steps in parallel
- Intermediate results are returned
- The search head combines and presents the results

MapReduce – Why Add More Indexers?



vs

.

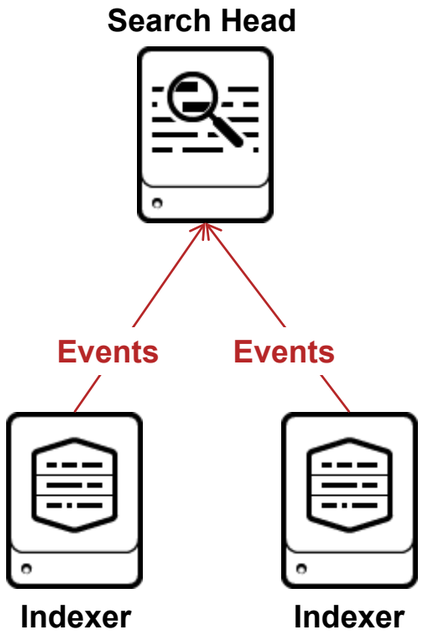


Questions for Search Types and Volume

What types of searches do you expect?	• Free-text search • Search by fields • Complex correlations and transactional searches
What types of alerts do you expect?	• Alerts and notifications of specific events • Alerts and notifications of thresholds reached or changed • Alerts and notifications of complex thresholds
Reporting	• How frequently will the reports run? • How current must the report data be? Near real time, to an hour, to the previous day? • Will historical or retroactive reports be required, or only current reports? • How will the reports be delivered to users? Via email, web interface, or other method? • Are there users who do not have access to the raw data who must see the reports?

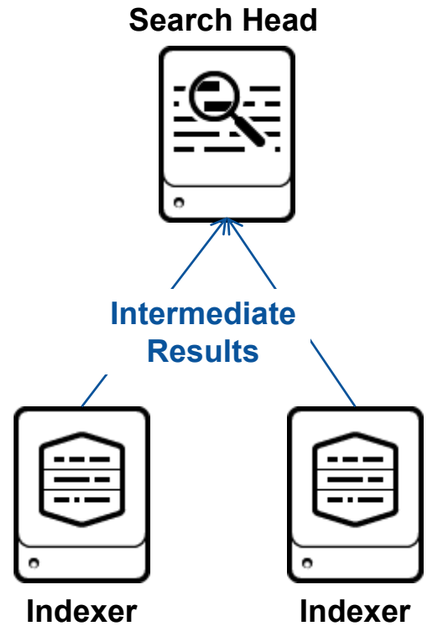
Raw Event Searches

- These search queries contain only the search command
  - The results are usually a list of raw events
  - Usually categorized as *super-sparse* or *rare* type searches
- A typical use case would be the deep analysis of a specific problem or incident
- Examples include:
  - Checking error codes
  - Correlating events
  - Investigating security issues
  - Analyzing failures



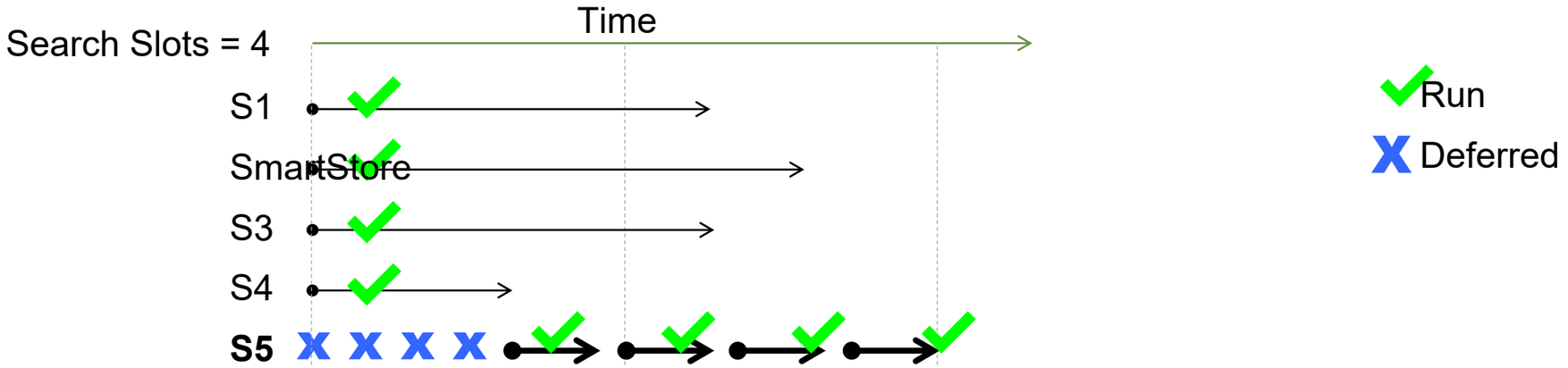
Report Generating Searches

- These search queries consist of initial search followed by some statistical calculation
  - The result is usually a table, graph or a single value
  - Often categorized as *dense* or *sparse* type searches
- They always require fields and at least one statistical command
- Examples include:
  - Compiling a daily count of error events
  - Counting the number of times a specific user has logged in
  - Calculating the 95th percentile of field values

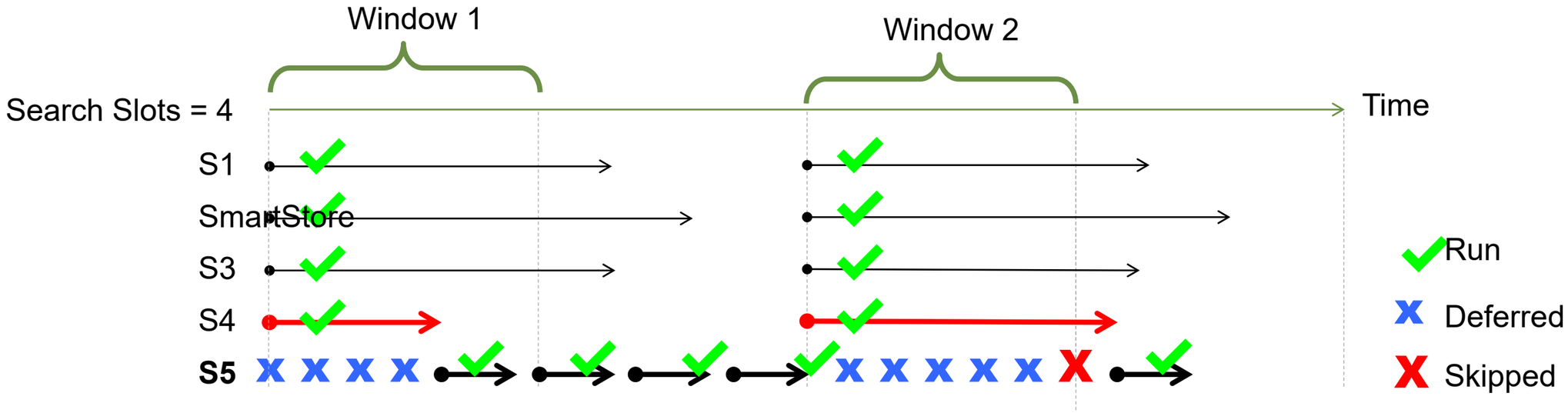


Splunk Report Scheduler Behavior

- Splunk runs as many concurrent jobs as it can, based on `limits.conf`
  - On a 16 CPU search head, the default is 11 concurrent scheduled searches
- In the example, 4 concurrent scheduled searches are used
  - Jobs S1, SmartStore, S3, and S4 take the first 4 slots
  - Job S5 must wait until another job finishes (S4)



Skipped Scheduled Jobs



- Every scheduled job has a **window** – a time period when it *should* run
- A job is deferred if it can't start when scheduled
  - A deferred job is retried (repeatedly for the duration of its window)
  - Example: Job S5 is deferred 4 times, but then runs during Window 1
- A job is skipped if it cannot start in its window
  - Example: Job S5 never runs during Window 2, and so is skipped

Report Scheduler Priorities

- The scheduler calculates priorities so that a skipped job has a higher priority in its next scheduled window
- To identify if Splunk has skipped searches, run the following

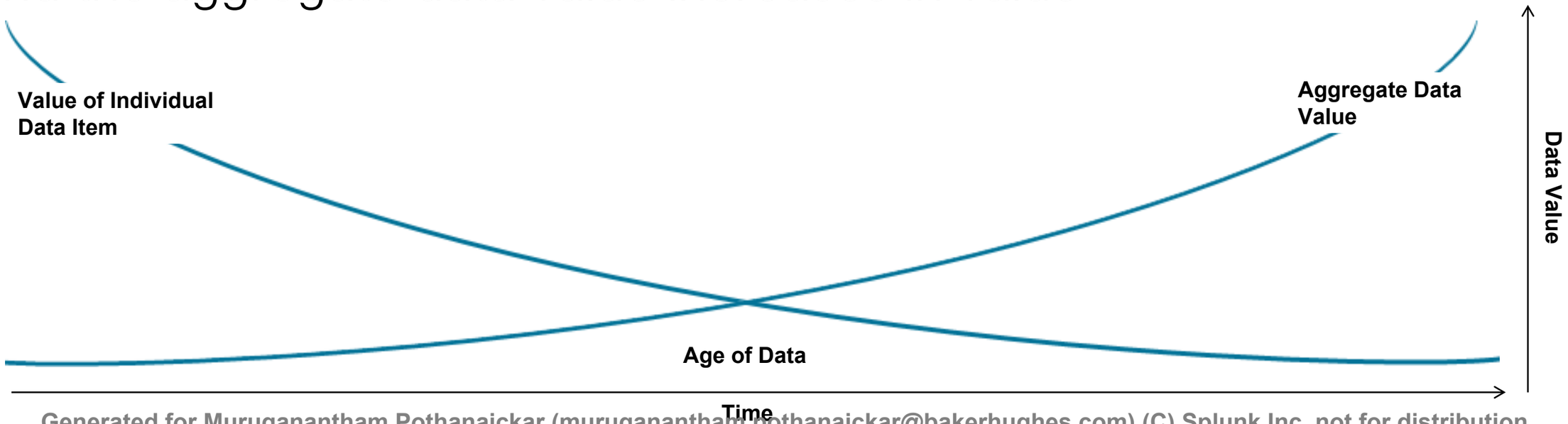
```
index=_internal source=*scheduler.log status!=success
| stats count by user app savedsearch_name status
```

```
Priority  = Next_runtime
          + Avg_runtime x priority_runtime_factor
          - skipped_count x period x priority_skipped_factor
          + window_adjustment
```

wiki.splunk.com/Community:TroubleshootingSearchQuotas

Summarization and Time Value of Data

- The value of data can be broken into two curves
  - Value of an individual data item
  - Aggregate data value
- In most cases, the value of an individual data item declines over time and the aggregate data value increases in value



How Acceleration Works

- Report acceleration and summary indexing speed up individual searches on a report-by-report basis
  - This is accomplished by building collections of pre-computed search result aggregates
- Data model acceleration speeds up reporting for the specific set of attributes (fields) that you define in a data model
  - Creates summaries for the specific set of fields, accelerating the dataset represented by that collection of fields rather than a particular search

Data Model Acceleration

- Used to speed up retrieval of the events that underlie a data model
- Speeds up reporting for the *entire set* of attributes (fields)
- Updated every five minutes
- Affects only *event* object hierarchies
  - Hierarchies based on search or transaction objects *cannot* be accelerated
- Most efficient if the root event objects include the index(es) in their initial constraint search

Data Model Acceleration (cont.)

- The High Performance Analytics Store
  - Consists of time-series index files with the **`.tsidx`** file extension
  - Exists on the indexer tier, parallel to the buckets that contain the events referenced in the **`.tsidx`** files
  - Spans a "summary range," which is the time range selected for acceleration
- Location and size can be set in **`indexes.conf`**
  - Default location is

    `$SPLUNK_HOME/var/lib/splunk/`*`indexName`*`/data_model_summary`

Report Acceleration

- Report Acceleration
  - Report results are "pre-computed" at regular intervals and stored on the indexer tier
  - All reports that use a similar set of data and computations automatically use the same report acceleration summaries if they can
- Report Acceleration Summaries
  - Span a time range selected for acceleration
  - Update every 10 minutes by default
  - Are automatically rebuilt if the data in the underlying bucket changes

docs.splunk.com/Documentation/Splunk/latest/Knowledge/Manageacceleratedsearchsummaries

Report Acceleration (cont.)

- Requirements for acceleration
  - The report was not created using Pivot
  - The underlying search qualifies for acceleration
- Splunk typically won't generate a summary if:
  - There are fewer than 100K events in the summary range
    - Faster to execute the search without a summary
  - Summary size is projected to be too large
    - Faster to execute the search using the normal index because it is smaller
- If a summary is defined but not created for the above reasons
  - Splunk continues to check periodically
  - Automatically creates a summary when/if the search meets the requirements

Thank You