Splunk Cluster Administration

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Document Usage Guidelines

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

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Course Prerequisites

- Required:
  - Splunk Enterprise System Administration
  - Splunk Enterprise Data Administration
- Strongly recommended:
  - Troubleshooting Splunk Enterprise
  - Architecting Splunk Enterprise Deployments
  - Working Linux knowledge
  - At least 3 months of hands-on Splunk administration experience

Note

In order to receive credit for this course, you must complete all lab exercises.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Course Goals

- Identify factors affecting large-scale Splunk deployments
- Set up Splunk indexer clusters
- Deploy and configure a Splunk search head cluster
- Add new nodes into an existing cluster
- Decommission nodes from an existing cluster
- Deploy apps and configuration bundles in Splunk clusters
- Manage KV store collections and lookups in Splunk clusters
- Monitor and identify clustering issues with Monitoring Console
- Scale Splunk indexer cluster with SmartStore

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Course Outline

- Module 1: Large-scale Splunk Deployment Overview
- Module 2: Single-site Indexer Cluster
- Module 3: Multisite Indexer Cluster
- Module 4: Indexer Cluster Management and Administration
- Module 5: Forwarder Configuration
- Module 6: Search Head Cluster (SHC)
- Module 7: SHC Management and Administration
- Module 8: KV Store Collection and Lookup Management
- Module 9: SmartStore Implementation

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module 1: Large-scale Splunk Deployment Overview

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module Objectives

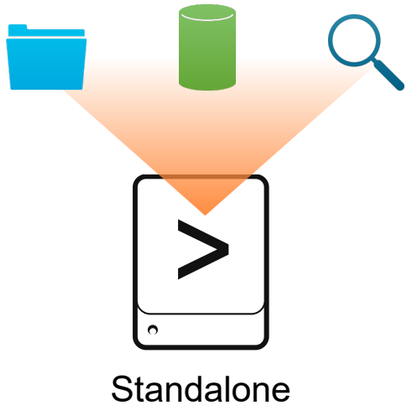
- Review Splunk deployment options
- Identify factors that affect large-scale deployment design
- Describe how Splunk can scale
- Configure a Splunk License Manager

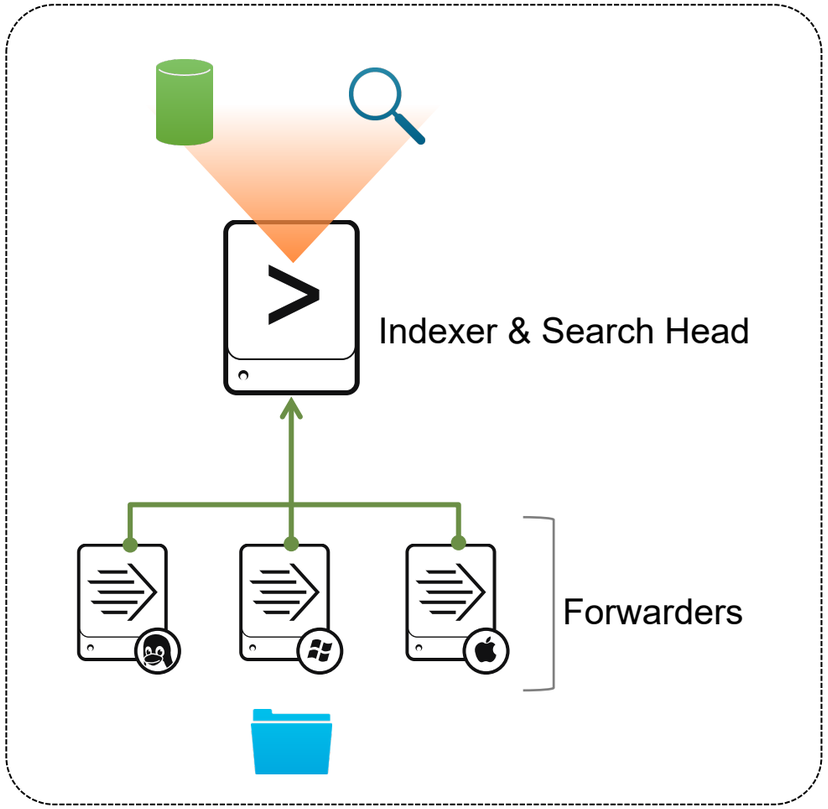
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

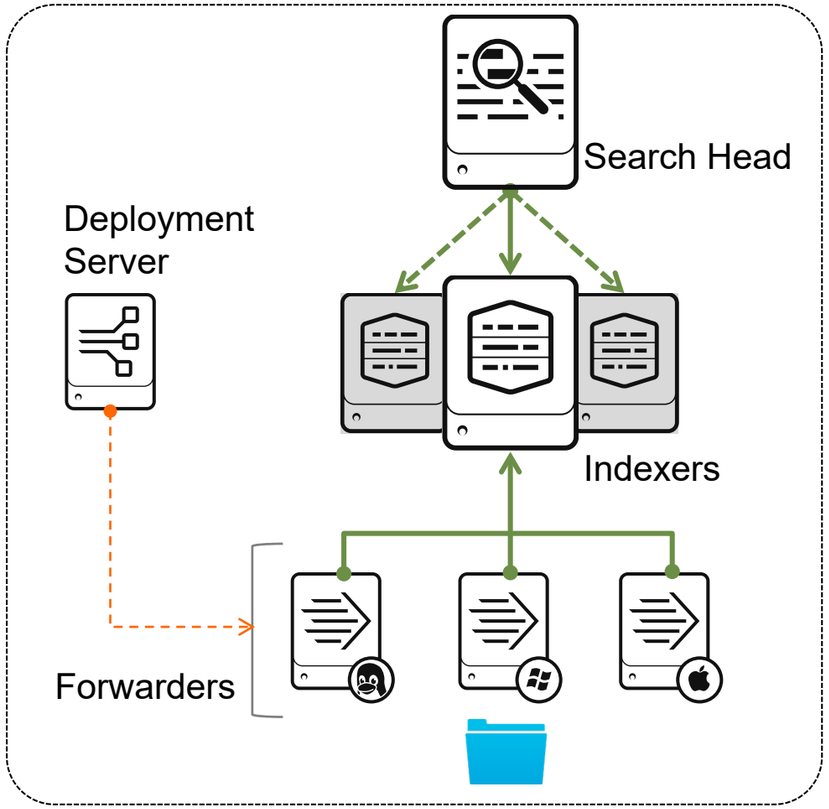
Copyright © 2022 Splunk, Inc. All rights reserved

Review: Splunk Deployment Options

- Key Splunk functions:
  - Consumes data, stores indexed data, and searches indexed data
- Splunk scales by splitting its functionality across multiple dedicated instances







Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Reference Servers for Distributed Deployment

	Indexer	Search Head
OS	Linux or Windows 64-bit distribution	
Network	1Gb Ethernet NIC (optional second NIC for a management network)	
Memory	12 GB RAM	
CPU	Intel 64-bit chip architecture **12 CPU cores** Running at 2+ GHz	Intel 64-bit chip architecture **16 CPU cores** Running at 2+ GHz
Disk	Disk subsystem capable of 800 IOPS	2 x 10K RPM 300GB SAS drives - RAID 1
http://docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware		

- Ratio of indexers to search heads depends on the number of concurrent users and the indexing volume per node

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

Note

Hardware sizing is discussed in detail in Architecting Splunk Course

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Introducing Splunk Clustering

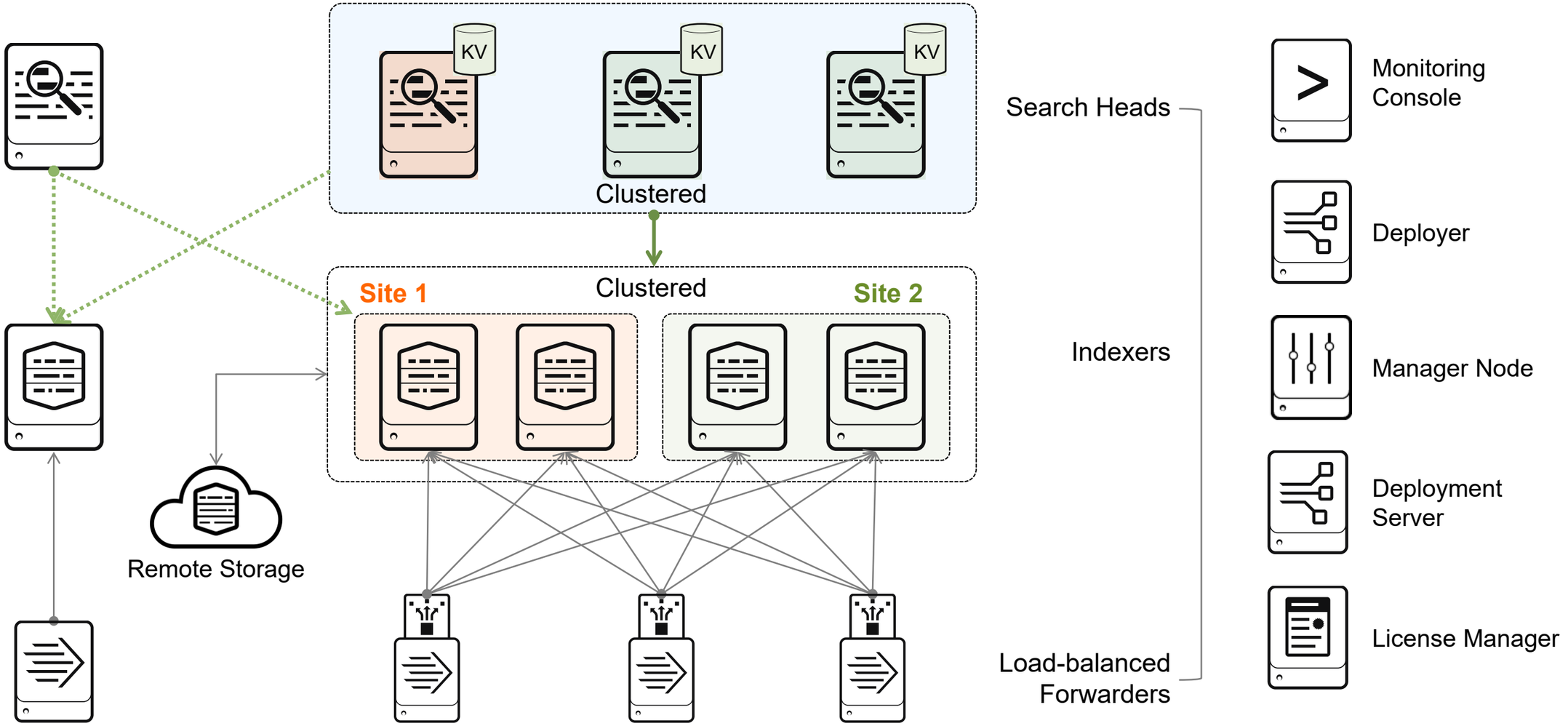
- Using commodity hardware, configure indexers to replicate indexes or group search heads to coordinate their search activities and loads
- Allows you to balance growth, speed of recovery, and overall disk usage

	High Availability (HA)	Disaster Recovery (DR)
Indexing Tier	Single-site cluster • Index replication • Flexible replication policies	Multisite cluster • Can withstand entire site failure • Supports active-passive and active-active configurations
	• SmartStore reduces the storage footprint while maintaining HA/DR	
Search Tier	• Search head or • Search head cluster	Search affinity (site-aware) • Search head or • Search head cluster

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Splunk Server Roles in Splunk Clusters



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Splunk Server Roles in Splunk Clusters (cont.)

License Manager	Allocates license capacity and manages license usage of all cluster members
Manager Node	Regulates the functioning of an indexer cluster
Peer Node	Indexer (search peer) that participates in an indexer cluster
Search Head	Participates in clusters as stand-alone or search head cluster member
Deployment Server	Centralized configuration manager for forwarders
Deployer	Distributes configurations to search head cluster members
Monitoring Console	Allows admins to monitor performance details regarding your Splunk environment

- Splunk recommends that you dedicate a host for each role
  - You can enable multiple Splunk server roles on a server with caveats
    - You will learn more about caveats of each server role throughout this course

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

License Manager Configuration

- By default, every instance is a **License Manager**
- All cluster members must share:
  - The same licensing pool
  - The same licensing configuration
- Only incoming data counts against the license
  - Replicated data does not count
- Cannot use a free license for clustering
- You should forward license manager's internal logs to the indexing layer
  - Do not count against the license
  - Able to run searches against the license logs
  - Any unusual condition can be visible on all search heads

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

License Manager Configuration (cont.)

- To add a license to a License Manager, run:

```
splunk add licenses {path_to_license_file}
```

- To check the list of license peer from the license manager, run:

```
splunk list licenser-slaves
```

- To switch to a License Peer, run this command on each peer:

```
splunk edit licenser-localslave -master_uri https://{LM:Mport}
```

- To check the peer configuration of a particular node, run:

```
splunk list licenser-localslave
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

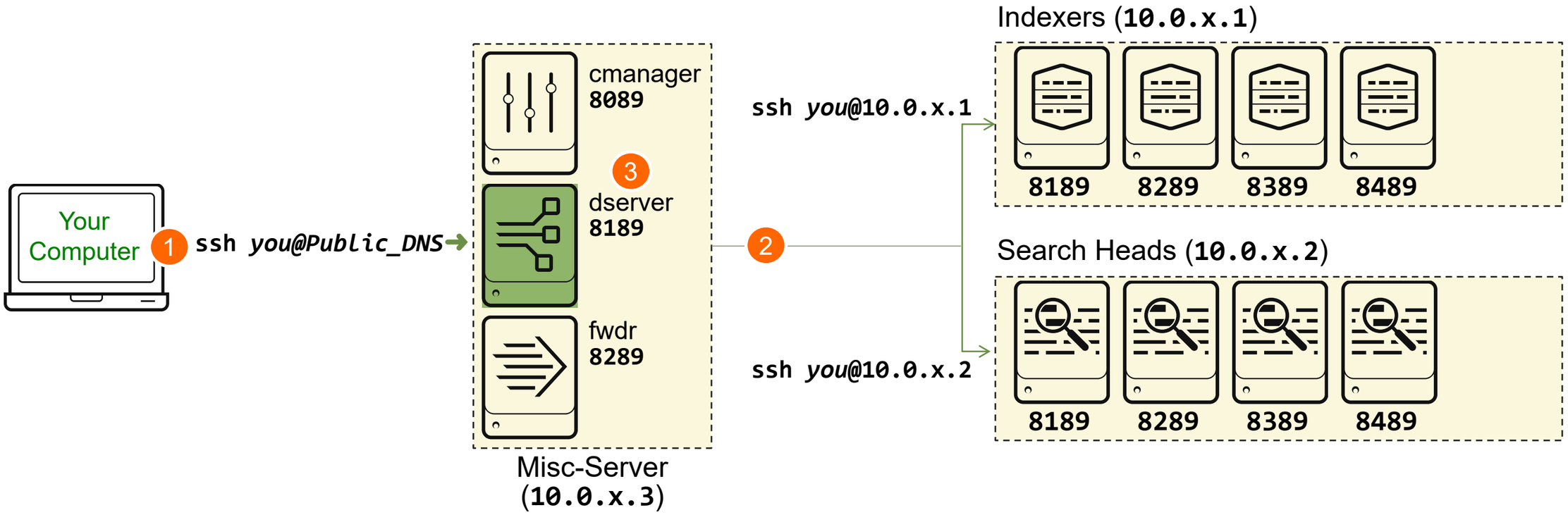
Lab Exercise 1 – Configure Splunk License Manager

- **Time**: 15 - 20 minutes
- **Tasks**:
  - Access your designated Splunk environment
  - Set up password-less SSH connection
  - Configure your License Manager instance
  - Log into Splunk Web and verify the license information

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Lab Exercise 1 – Configure Splunk License Manager (cont.)

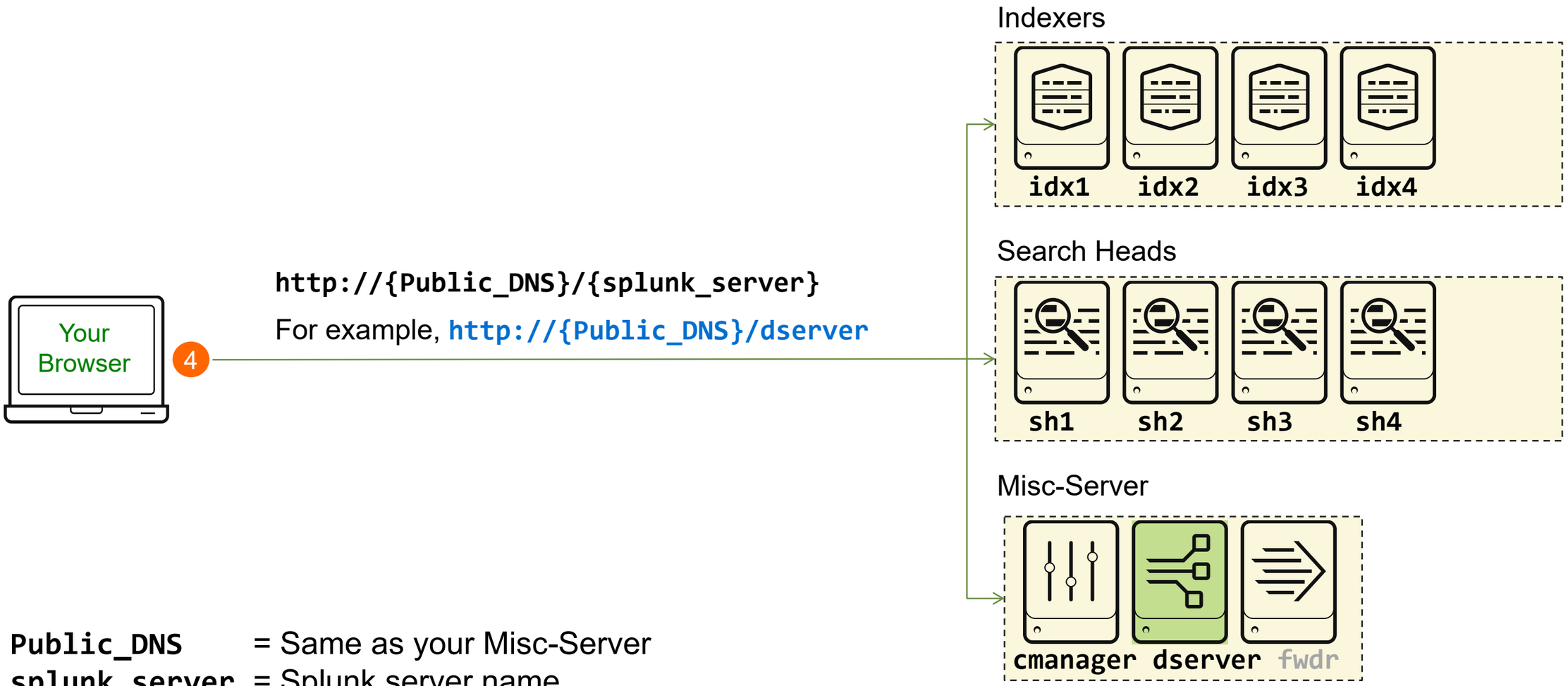


x = Your student ID
8?89 = splunkd-port

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Lab Exercise 1 – Configure Splunk License Manager (cont.)



Public_DNS = Same as your Misc-Server
splunk_server = Splunk server name

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Module 2:
Single-site Indexer Cluster

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module Objectives

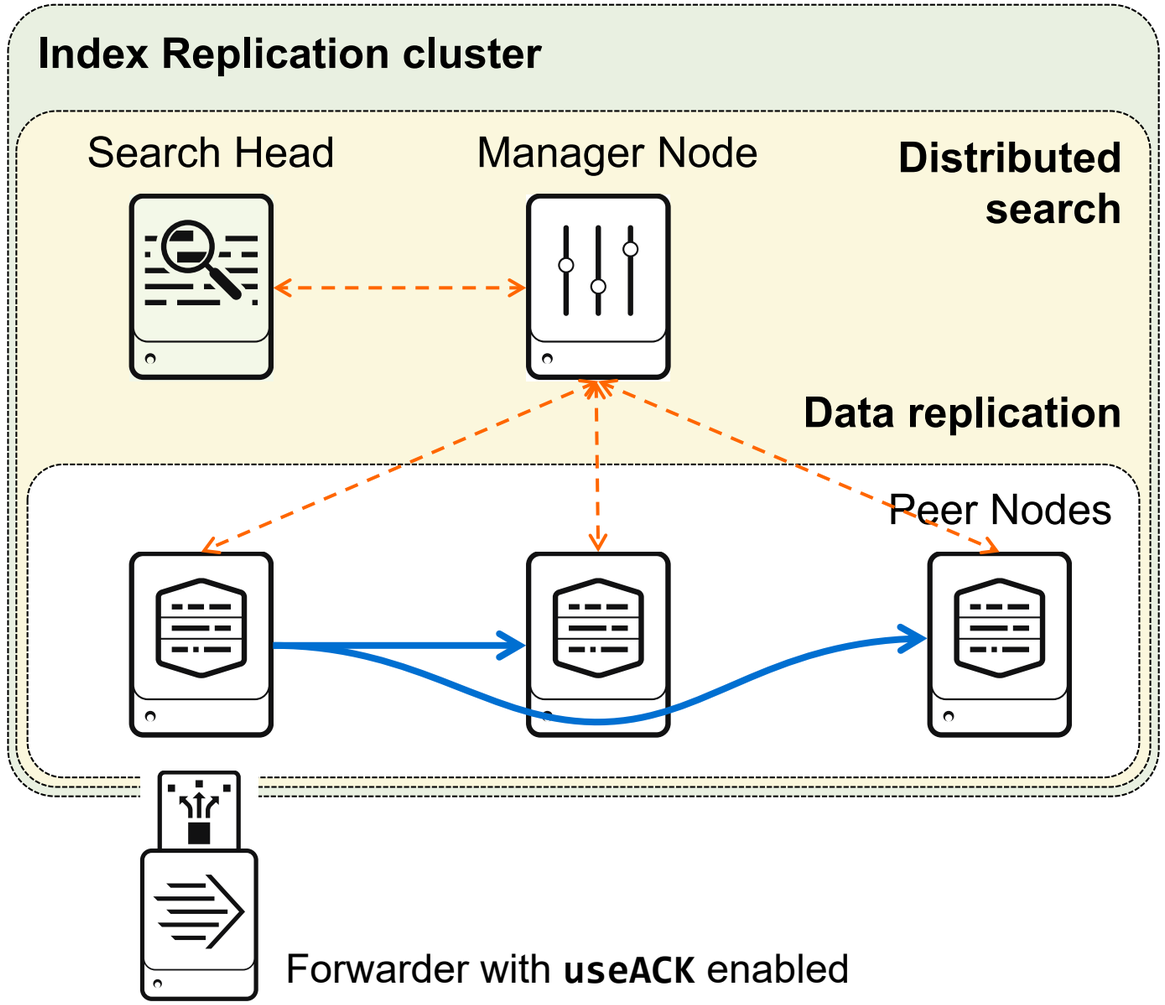
- Describe how Splunk single-site indexer clusters work
- Identify cluster components and terms
- Implement a single-site indexer cluster
- Search and review internal logs related to indexer clustering

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Single-site Indexer Cluster Overview

- Manager node
  - There can only be one cluster manager
  - Controls and manages index replication
  - Distributes app bundles to peer nodes
  - Tells the search head which peers to search
- Peer nodes
  - Index data from inputs/forwarders
  - Replicate data to other peer nodes as instructed by the manager
- Search head
  - Required component of indexer cluster
  - Relies on the manager for its target search peers
  - Works the same as any Splunk search head
- Forwarders
  - Send data to peer nodes



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Indexer Cluster Considerations

Benefits

- Data availability and fast recovery
- Easier overall administration
  - Coordinated indexer configuration management
  - Automatic distributed search setup
  - Elastic indexer discovery
  - Indexer peer node status dashboard on the manager node
- Scale-out indexing capacity
- No additional cost for data replication

Trade Offs

- Increased storage requirements
- Increased processing load
  - Depending on the replication & search factors
- Requires additional Splunk instances
  - Minimum:
    - Replication Factor (RF) + MN + SH
  - Recommended:
    - More than RF + MN + more SHs
- No support for heterogeneous indexers
  - Requires same OS and Splunk versions
- Requires cluster-specific deployment management

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Indexer Cluster System Requirements

- Each node must run on its own host
- The manager node must run the same or a later version than the peer nodes and search heads
  - Can run at most three minor versions later than the peer nodes
    - 8.1 manager node can run against 8.1 and 8.0
- The search heads must run the same or a later version than the peer nodes
- All peer nodes must run EXACTLY the same version
- Peer node storage requirements:
  - Ability to sustain 800 IOPS for each peer node
  - The ratio of disks to disk controllers should mimic a database system requirement
- Cluster recovery depends upon system resources available on manager node

http://docs.splunk.com/Documentation/Splunk/latest/Indexer/Systemrequirements

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Indexer Cluster Deployment Overview

1. Identify your clustering requirements
   - Replication policy, disk space, number of peer nodes, etc.
2. Install Splunk Enterprise and configure cluster instances
   - One manager, at least two indexers, and one search head
   - Synchronize the system clocks on all machines
3. Enable clustering on each cluster instance
   - Use Splunk Web UI, CLI, or manually edit **`server.conf`**
4. Create and distribute configuration bundles to the peer nodes
5. Forward data to the peer nodes

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Best Practices and Guidelines

- Plan, plan, and plan
  - A single cluster or segregated clusters (by sourcetype, department, or use case)
- Cluster instances should not share hardware
  - Dedicate hardware to the manager node, search head, and peer nodes
  - All members share the same license pool
  - Each peer node must have its own storage
- Number of peer nodes is determined by:
  - Expected availability requirements of your organization
  - Level of replication required, daily data rate, retention policy, and concurrent users
    - Index replication does not increase your licensing usage
- Cannot use a deployment server to distribute configuration bundles directly to peer nodes

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Where to Install the Manager Node

- On a dedicated host
  - Cannot be shared with a peer node or search head instance
  - Built-in search head for debugging purposes
- Under certain limited circumstances, it can fulfill additional server roles
  - License manager
  - Monitoring Console
  - Deployer
- DO NOT co-locate a deployment server on the manager node under any circumstances

Note

When hosting additional roles, the cluster node should be under the following limits:

- 30 peer nodes
  - 10 indexes
  - 100,000 buckets
- 10 search heads

Note

Manager node failover is discussed later in this module.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Single-site Cluster: Key Specifications

- Peer nodes copy buckets to other peer nodes (index replication)
  - The copied buckets may be searchable buckets or contain only **rawdata**
- **Replication factor**
  - Specifies how many total copies of **rawdata** the cluster should maintain
  - Sets the total failure tolerance level
- **Search factor**
  - Specifies how many copies are searchable
    - A searchable bucket contains both **rawdata** and index files
    - Its **rawdata** is counted as a part of the replication factor
  - Cannot be larger than the replication factor
  - Determines how quickly you can recover the search capability
    - A trade-off between disk usage and search availability
- **Security key (`pass4SymmKey`)**
  - Authenticates communication between the cluster nodes
  - The key must be the same across all cluster instances

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

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

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

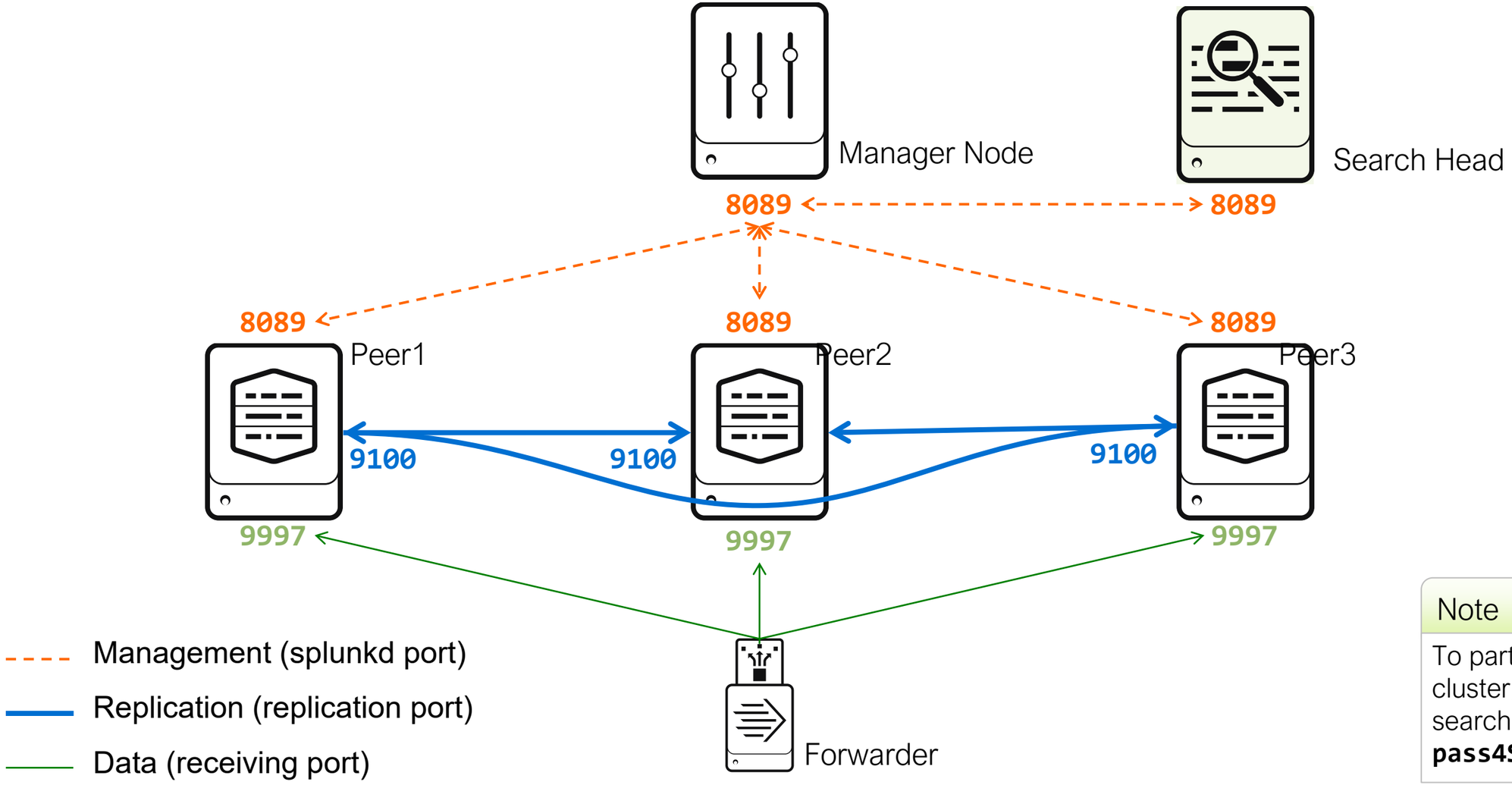
Configuring Splunk Cluster

- There are three ways to configure
  - Splunk Web, CLI, and **`server.conf`**
  - In this course, you will use CLI for configurations and Splunk Web for monitoring
- Enable clustering on the instances in the order of Manager node > Peer nodes > Search heads
- Get help on Splunk cluster commands:
  - **`splunk help cluster`**
  - **`splunk help [list|edit] cluster-config`**

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Ports for Indexer Clustering



Note

To participate in this indexer cluster, all nodes -- including the search head -- must use the same **`pass4SymmKey`**.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Configuring Splunk Manager Node

Enter the single command

```
> splunk edit cluster-config
-mode manager
-replication_factor 2
-search_factor 2
-secret mycluster
```

Results in:

SPLUNK_HOME/etc/system/local/server.conf

```
[clustering]
mode = manager
replication_factor = 2
pass4SymmKey = Hashed_Secret
```

To see the decrypted **pass4SymmKey**, run:

splunk show-decrypted --value '<hashed_secret>'

- Splunk defaults to:
  - **replication_factor = 3**
  - **search_factor = 2**
- The **secret** parameter is encrypted and saved as **pass4SymmKey**
  - Required
  - **mycluster** is the password for this cluster example

Note

Splunk 7.2+ encrypts all new secrets using a new cipher. However, it will not auto-migrate existing hashes.

You can update them by changing the **splunk.secret** file on each instance to use the new cipher.
To change, run: **splunk rotate splunk-secret**

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Configuring the Peer Nodes

```
> splunk enable listen 9997
> splunk edit cluster-config
-mode peer
-master_uri https://10.0.1.3:8089
-secret mycluster
-replication_port 9100
```

SPLUNK_HOME/etc/system/local/server.conf

```
[clustering]
mode = slave
master_uri = https://10.0.1.3:8089
pass4SymmKey = Hashed_Secret

[replication_port://9100]
```

- Ports required on each peer:
  - Receiving port to listen to forwarders
  - Replication port to communicate with other peer nodes
- In this example:
  - **9997** = the forwarder listening port
  - **10.0.1.3** = manager node address
  - **8089** = manager node's splunkd-port
  - **mycluster** = same cluster password
  - **9100** = index replication port

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Configuring the Search Head

```
> splunk edit cluster-config
-mode searchhead
-master_uri https://10.0.1.3:8089
-secret mycluster
```

SPLUNK_HOME/etc/system/local/server.conf

```
[clustering]
mode = searchhead
master_uri = https://10.0.1.3:8089
pass4SymmKey = Hashed_Secret1
```

- To configure as a cluster search head:
  - **`edit cluster-config`**
- Functions as a regular search head
- For more help:

  `splunk help [list|add|edit|remove] cluster-master`

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Adding SH to an Additional Indexer Cluster

```
> splunk add cluster-master
-master_uri https://20.0.2.6:8089
-secret yourCluster
```

- SHs can belong to multiple clusters
- To allow SH to search additional clusters:

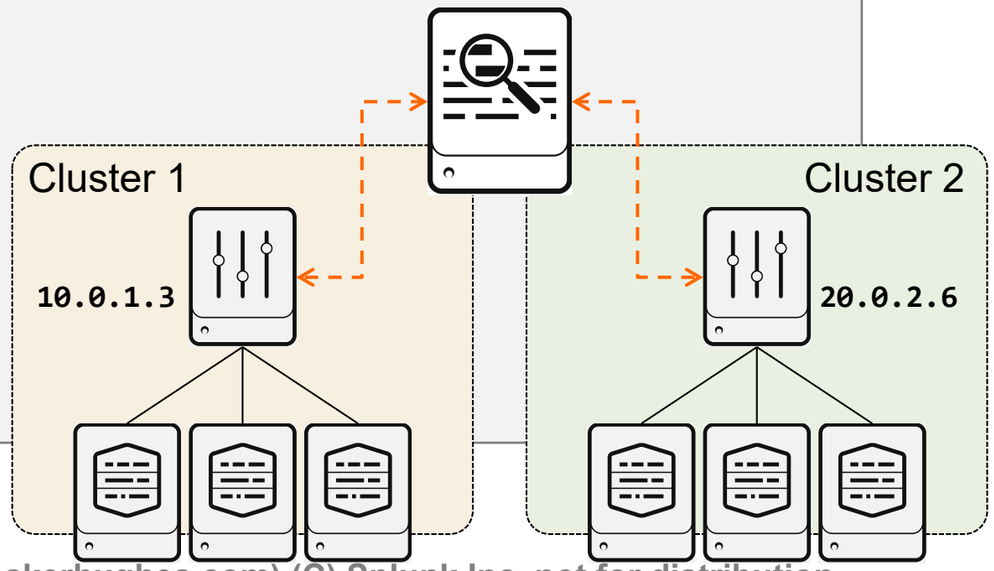
  `splunk add cluster-master`

```
[clustering]
mode = searchhead
master_uri = clustermaster:10.0.1.3:8089, clustermaster:20.0.2.6:8089

[clustermaster:10.0.1.3:8089]
master_uri = https://10.0.1.3:8089
pass4SymmKey = Hashed_Secret1

[clustermaster:20.0.2.6:8089]
master_uri = https://20.0.2.6:8089
pass4SymmKey = Hashed_Secret2
```

`SPLUNK_HOME/etc/system/local/server.conf`



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Generations

- Identifies which copies of a cluster's buckets are primary
  - These buckets will participate in search
  - Non-searchable buckets will lack **`.tsidx`** files, metadata, etc.
- Changes over time, as peers leave and join the cluster
  - Cluster rebalancing
  - Primary reassignment after a peer goes down
- How cluster nodes use the generation
  - **CM** creates each new generation and assigns an ID
  - **Peers** keep track of which bucket copies are primary in the generation

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Clustered Buckets

- Buckets are located in: `$SPLUNK_HOME/var/lib/splunk`
- Naming convention for clustered buckets also distinguishes types of copies: originating vs replicated

Bucket type	Hot bucket	Warm/cold/thawed bucket
Non-clustered	`hot_v1_<localid>`	`db_<newest_time>_<oldest_time>_<localid>`
Clustered originating	`hot_v1_<localid>`	`db_<newest_time>_<oldest_time>_<localid>_<guid>`
Clustered replicated	`<localid>_<guid>`	`rb_<newest_time>_<oldest_time>_<localid>_<guid>`

  - **newest_time & oldest_time** = timestamps indicating the age of data in the bucket
  - **localid** = an ID for the bucket
  - **guid** = the guid of the source indexer

Note

The guid is located in the peer's: `$SPLUNK_HOME/etc/instance.cfg`

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

How the Cluster Manager Sees Buckets

- Buckets are identified using three pieces of information:
- Index name, local ID, GUID of original indexer
- Buckets can appear in two different ways: *name* vs *separate field*

`_audit~3~1318C26A-D9FE-45F0-AF51-7A8038F5419C`

vs

index: `_audit`, ***bucket_id:*** `3_1318C26A-D9FE-45F0-AF51-7A8038F5419C`

- Searchable buckets may be flagged as "primary"
  - REST API: **`/services/cluster/master/buckets`**
  - Returns: 0x000000000 (non-primary) or 0xffffffff (primary)

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Manager Dashboard – Single-site Cluster

Settings > Indexer clustering

Indexer Clustering: Master Node

Edit ▾ | More Info ▾ | Documentation

✓ **All Data is Searchable** ✓ **Search Factor is Met** ✓ **Replication Factor is Met**

3 searchable **0** not searchable
Peers

2 searchable **0** not searchable
Indexes

Peers (3) | Indexes (2) | Search Heads (2)

filter 🔍 10 per page ▾

i	Peer Name ▲	Fully Searchable ⇕	Status ⇕	Buckets ⇕ ?
⌄	idx1	✓ Yes	Up	6
	Location ..... 10.0.1.1:8189 Last Heartbeat ..... 3/5/2018, 5:17:00 PM Replication Port ..... 9100 Base Generation ID 8 GUID DE5BC497-7D49-44A2-9092-0E068697DE70			
>	idx2	✓ Yes	Up	11
>	idx3	✓ Yes	Up	11

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Index Replication Health

Cluster status is	When current operational RF is	When current operational SF is
Complete	Met as specified	Met as specified
Valid		One or greater
Searchable	Have two searchable copies of each bucket (Searchable rolling-restart)	

- With replication factor = 3 and search factor = 2:
  - A **complete** cluster has 3 copies of each bucket, 2 of which are searchable
  - A **valid** cluster has at least one searchable copy of all buckets
- With replication factor = 2, search factor = 2, and 2 peers:
  - A **complete** cluster has 2 searchable buckets, each having its copy of rawdata
  - A **valid** cluster has at least one searchable copy of all buckets

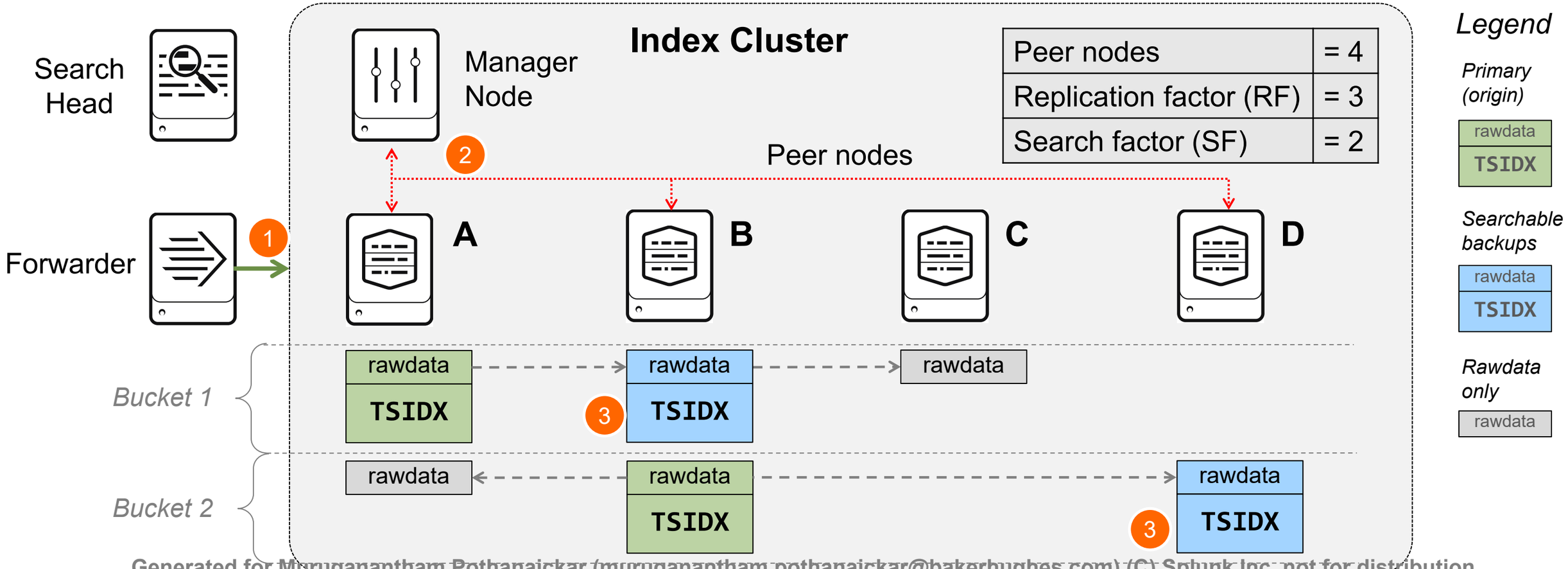
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Factors in Action – Data Replication

Complete & Valid

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



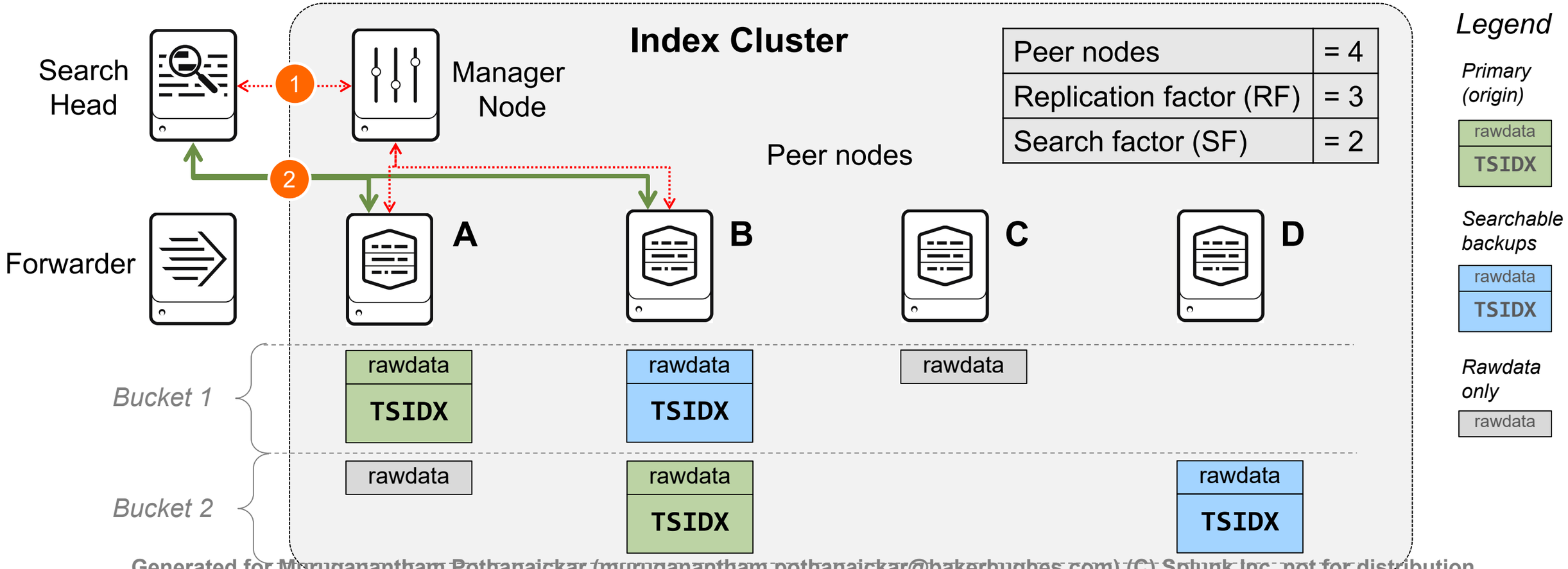
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Factors in Action – Search

Complete & Valid

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



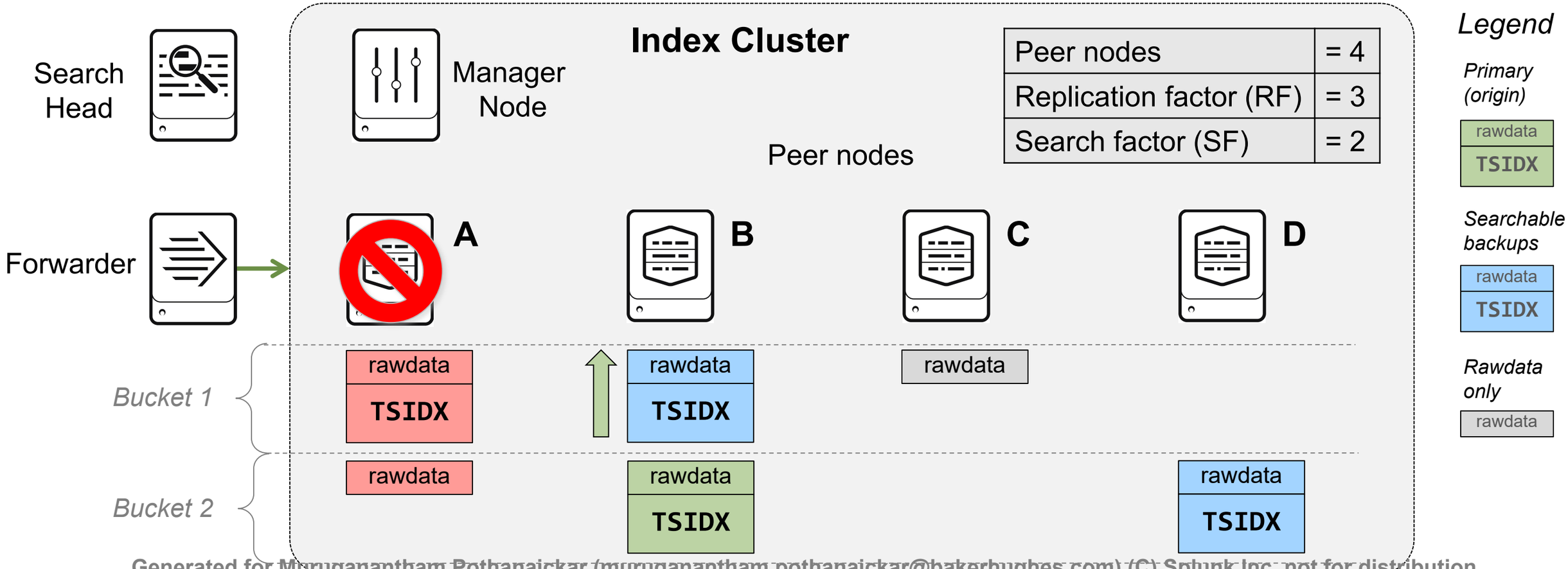
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Factors in Action – Initial Primary Loss

Valid but Not Complete

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



Peer nodes	= 4
Replication factor (RF)	= 3
Search factor (SF)	= 2

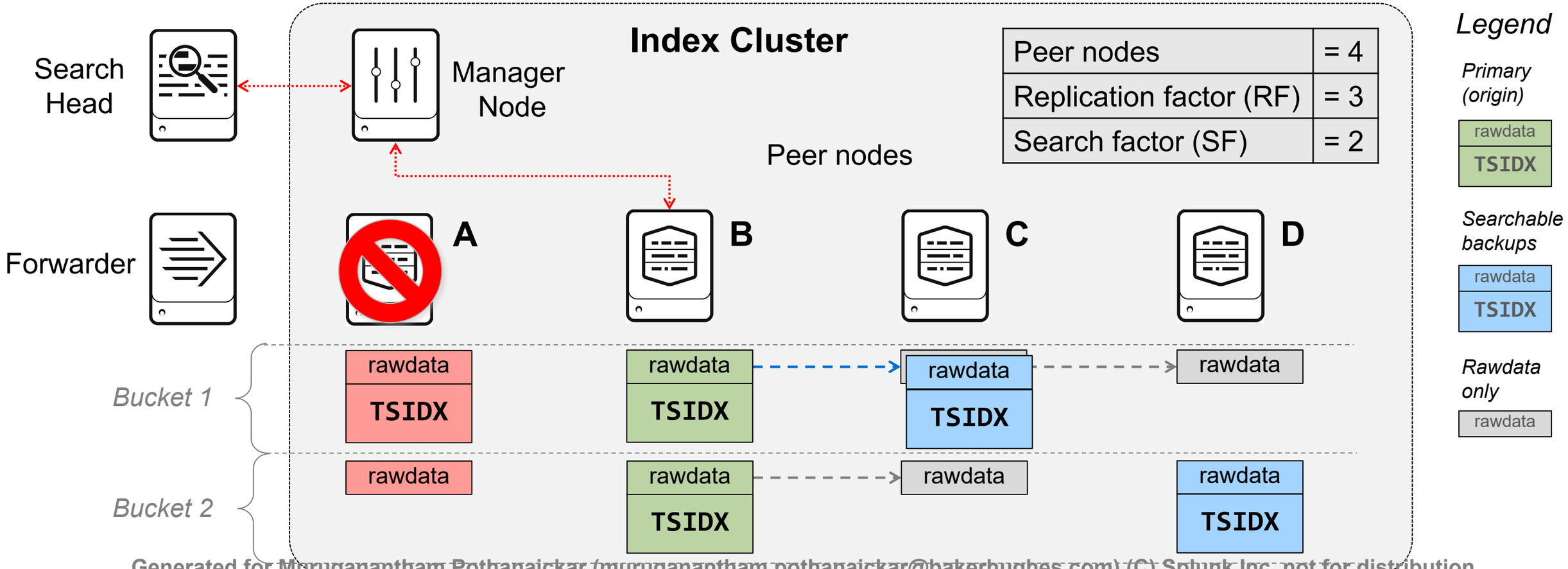
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

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



Peer nodes	= 4
Replication factor (RF)	= 3
Search factor (SF)	= 2

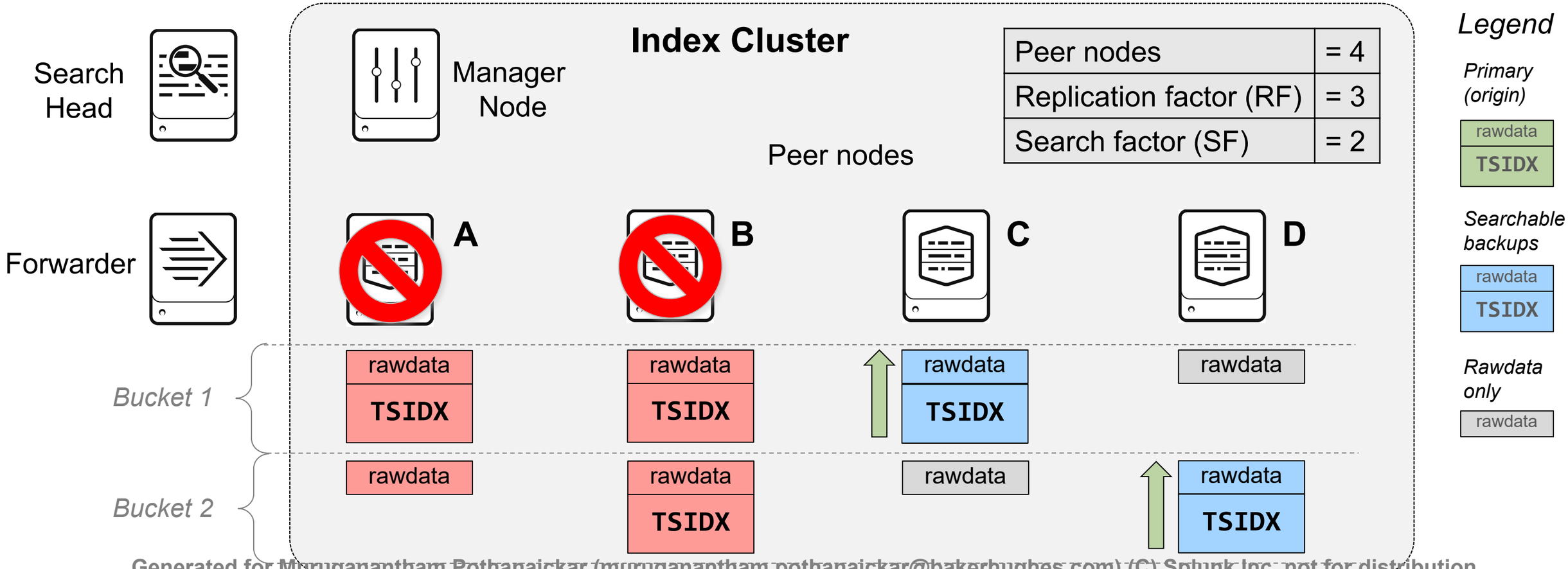
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

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



Peer nodes	= 4
Replication factor (RF)	= 3
Search factor (SF)	= 2

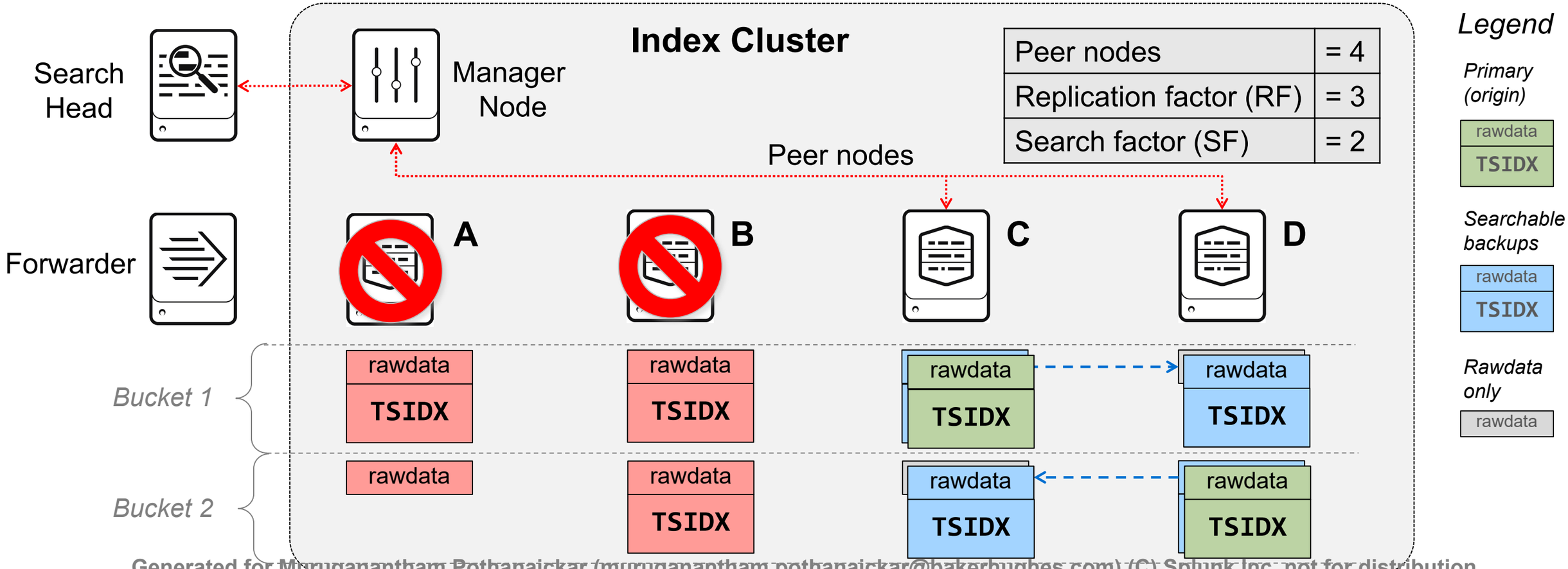
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

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



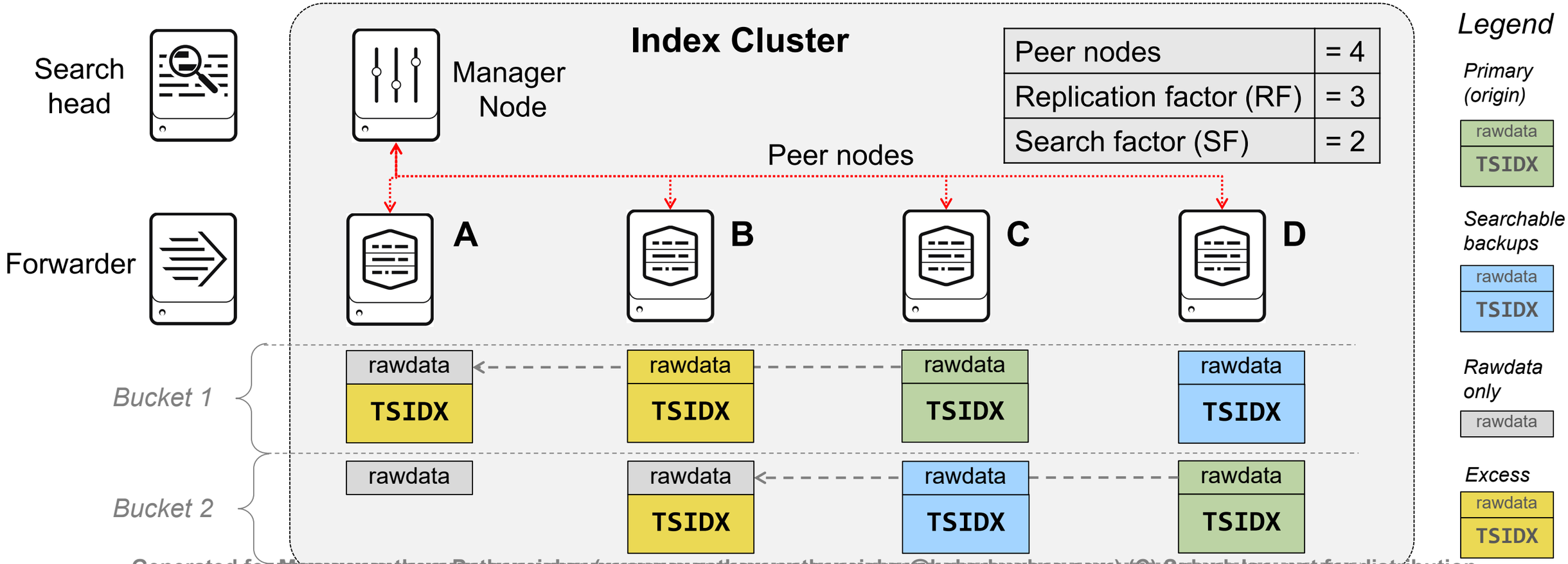
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

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

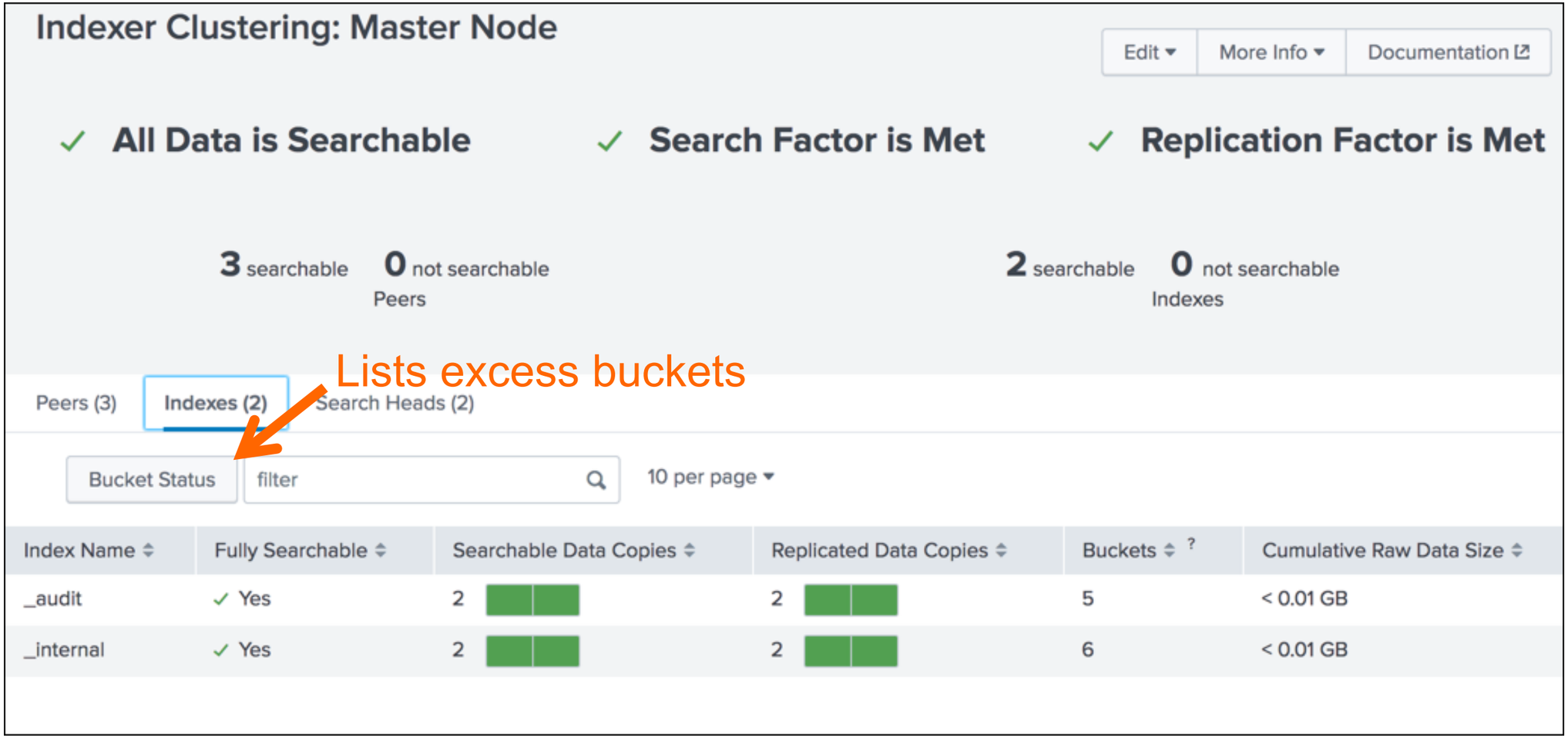


Peer nodes	= 4
Replication factor (RF)	= 3
Search factor (SF)	= 2

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Excess Buckets



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Notable Indexer Cluster Log Channels

- Cluster peers communicate via the **`/services/cluster`** endpoints
  - Peer to manager communication: **`/services/cluster/master`**
  - Manager to peer communication: **`/services/cluster/slave`**
- splunkd_access.log – Indexer cluster communication logs
  - Example:

```
index=_internal sourcetype=splunkd_access
(uri="/services/cluster/slave/buckets*" OR uri="/services/cluster/master/buckets*")
| convert ctime(_time) | table _time uri_path | sort _time
```

  - Higher response time indicates service overloading
  - Response status 200 is good, anything else is not good
- splunkd.log – indexer clustering activity logs
  - **`component=CM* OR component=Cluster*`**
  - Look for **`WARN/ERROR`** on the **`host=<master>`**
- metrics.log
  - **`component=Metrics group=clusterout_connections`**

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Manager Node Failover

- If the manager node is lost, the cluster continues to operate
  - New data arriving at peer nodes is indexed, but might not replicate
  - The search heads continue to send the queries to last known list of peer nodes and peer nodes respond if they can
  - After the manager node comes back online, buckets are re-balanced
- A stand-by manager node can be configured
  - https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Handlemanagernodefailure
- You can employ DNS-based failover, a load balancer, or some other technique to switch the same **`master_uri`** to the stand-by manager
  - Hot-standby is NOT recommended

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Manager Node Failover (cont.)

- A standby manager only needs the primary manager's static state information
  - **`SPLUNK_HOME/etc/system/local/server.conf`**
  - **`SPLUNK_HOME/etc/master-apps`**
- When the standby manager node starts, its services are blocked until it can fulfill the replication factor
  - To have the standby manager unblock immediately, run:
    `splunk set indexing-ready`

Note

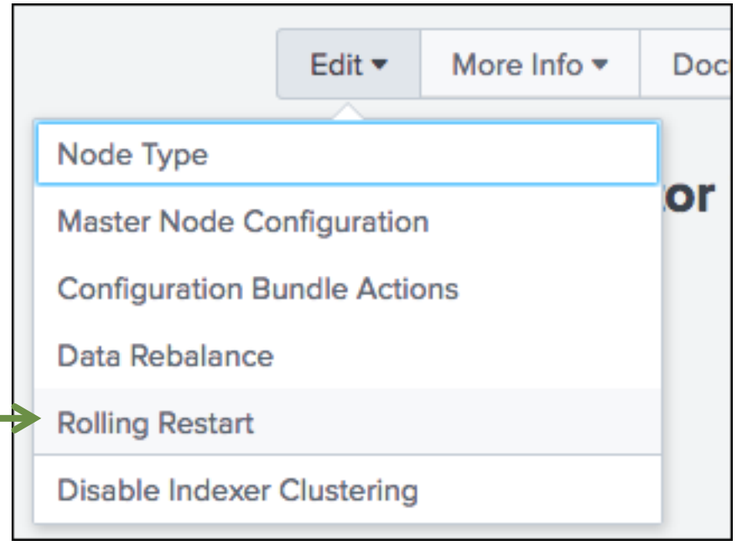
Extra provisioning is required if the Monitoring Console is also enabled on the Manager Node.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Restarting Indexer Cluster

- Ordinarily you do not restart the entire cluster
  - Search heads can be restarted at any time
- If you do need to restart the entire cluster:
  1. Restart the manager node with **`splunk restart`**
  2. Run preliminary health checks
     - Must be in a searchable state
     - Check the manager dashboard for cluster status
     - CLI: **`splunk show cluster-status --verbose`**
  3. Restart peer nodes:
     - Select **Edit > Rolling Restart**
     - CLI: **`splunk rolling-restart cluster-peers`**

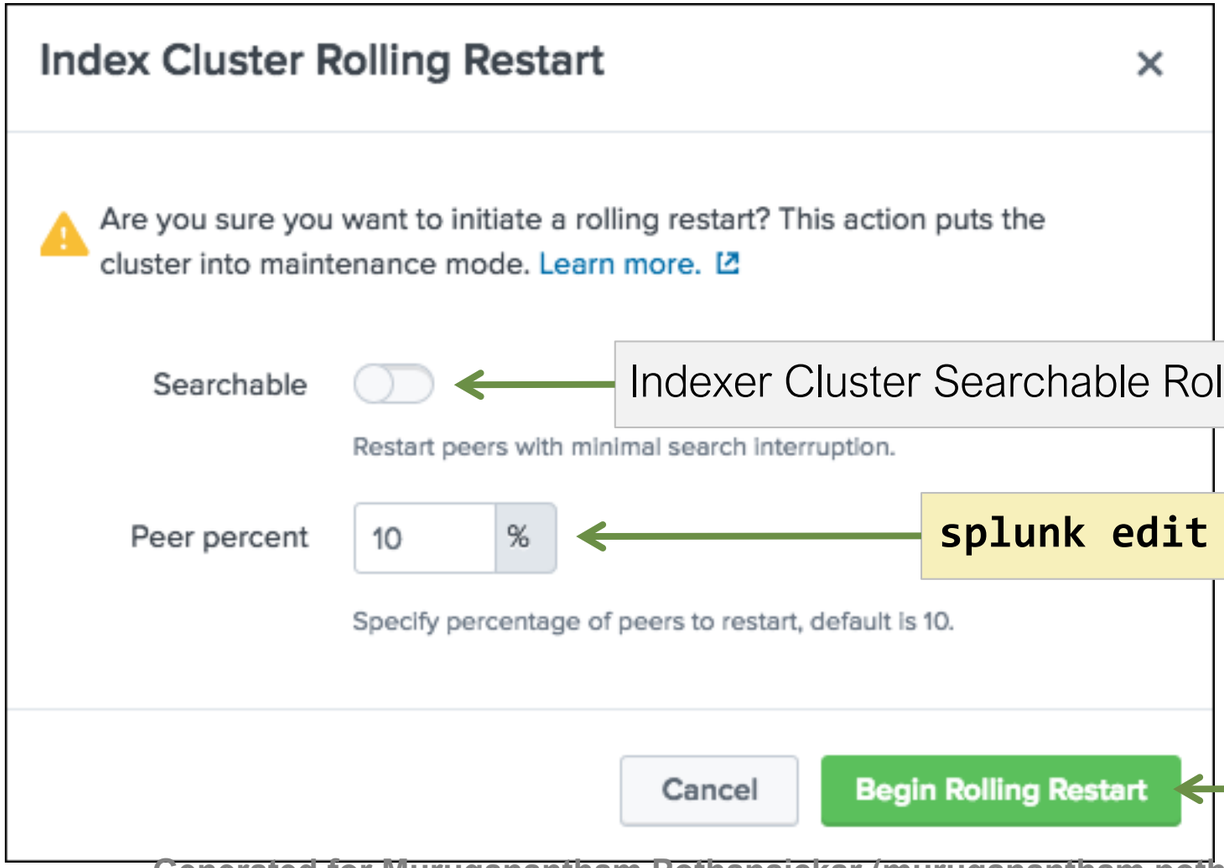


Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Peer Nodes Rolling Restart

- Performs a phased restart of all the peer nodes
  - Restarts 10% of the peers at a time in random order (configurable)



Indexer Cluster Searchable Rolling Restart option (More details in Module 4)

```
splunk edit cluster-config -percent_peers_to_restart 100
```

```
splunk rolling-restart cluster-peers
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Migrating Non-clustered Indexers to a Cluster

- You can add a non-clustered indexer to a cluster as a peer node at any time

```
splunk edit cluster-config -mode peer ...
```

- Apps must be re-distributed via **`master-apps`**
  - You learn about distributing apps in indexer clusters in Module 4
- Only new data coming into this peer is replicated
  - New data follows the cluster's replication factor
- Existing buckets are not replicated
  - Contact Splunk Professional Services if you must replicate legacy buckets

Note

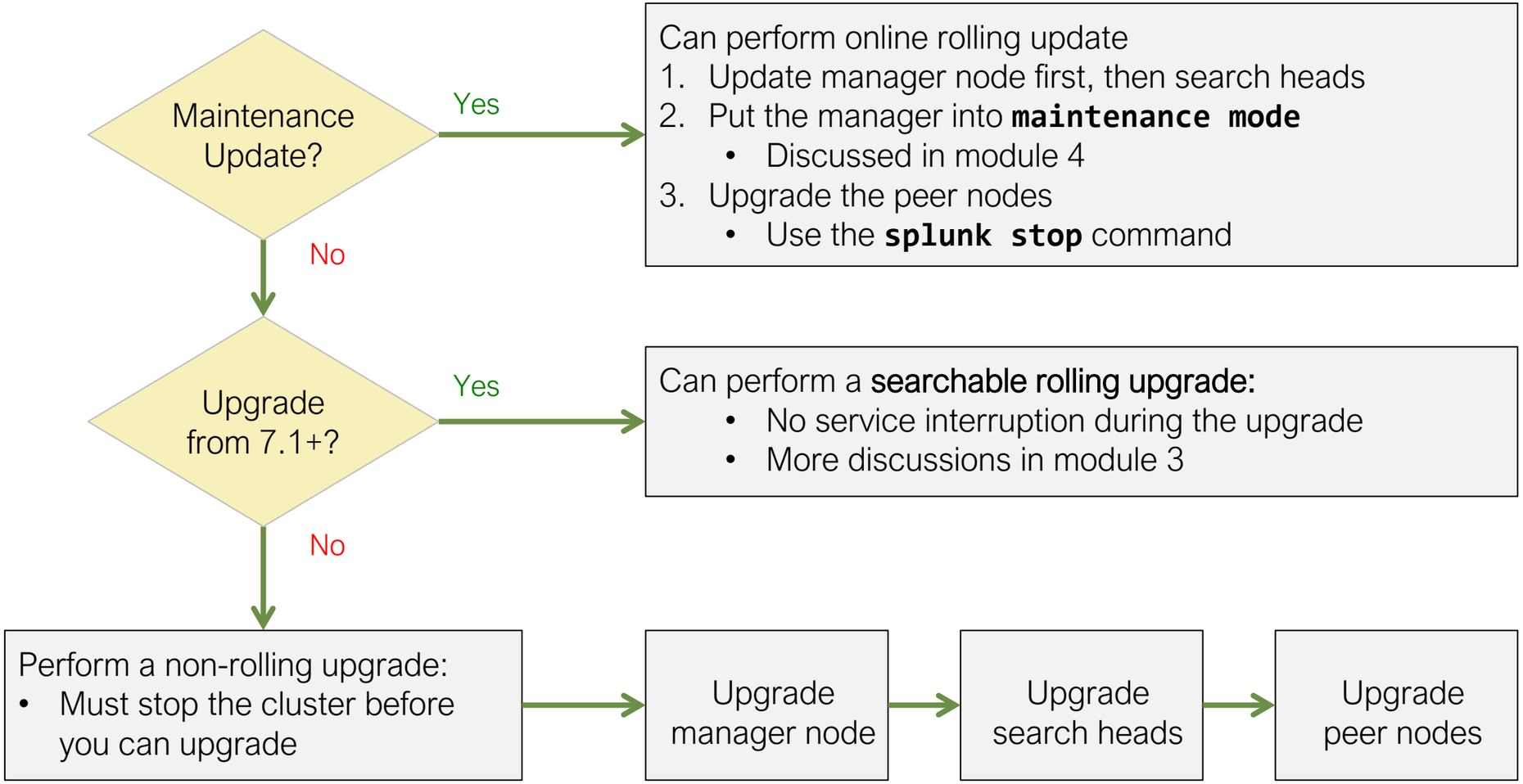
You cannot convert a peer node to a non-clustered indexer.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Upgrading and Applying Maintenance Releases

http://docs.splunk.com/Documentation/Splunk/latest/Indexer/Upgradeacluster



Note

- Manager node must run the highest version
- Search head must run higher version than the peer nodes
- Complete the entire process quickly

Note

- Must upgrade the tiers in the prescribed order
- Within each tier, upgrade all nodes as a single operation

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Lab Exercise 2 – Enable Single-site Cluster

Time: 25 - 30 minutes

Tasks:

- Switch all cluster members to license peers
- Configure the manager node for a single-site indexer cluster
- Configure three indexers to form the replication peers
- Configure a search head to join the cluster
- Monitor the cluster status with Splunk Web

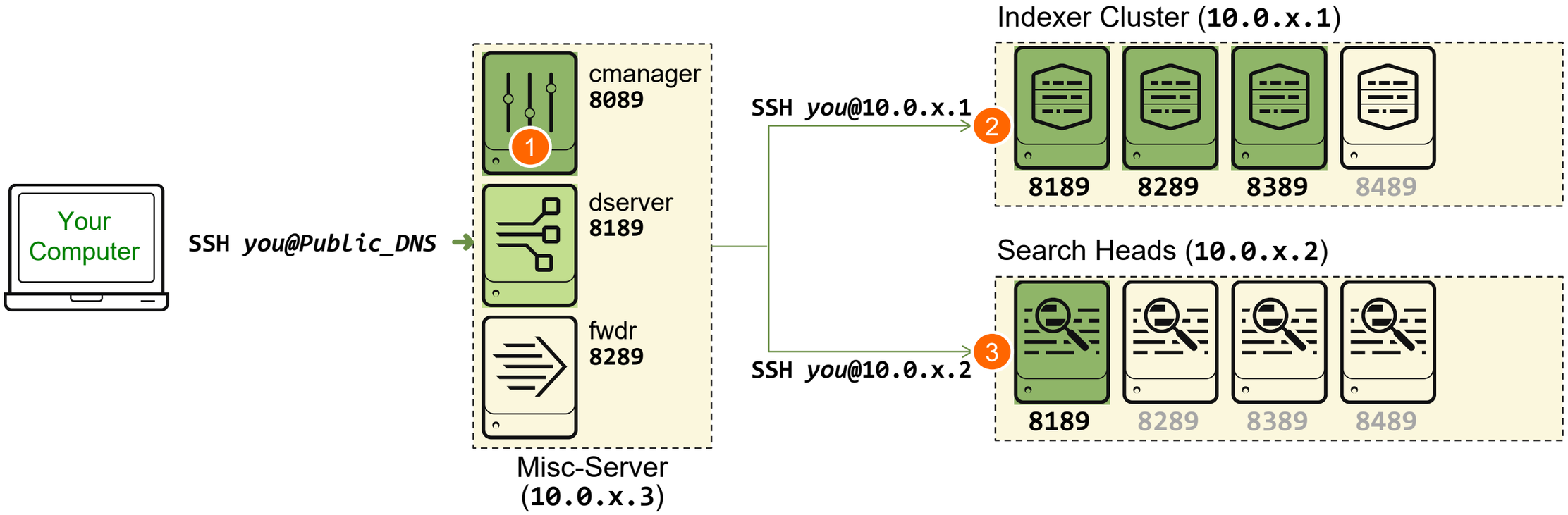
Optional Tasks: (additional 15 minutes)

- Test a peer node failover scenario
- Investigate the peer outage with Splunk internal logs

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Lab Exercise 2 – Enable Single-site Cluster (cont.)



x = Your student ID
8?89 = splunkd-port

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module 3:
Multisite Indexer Cluster

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module Objectives

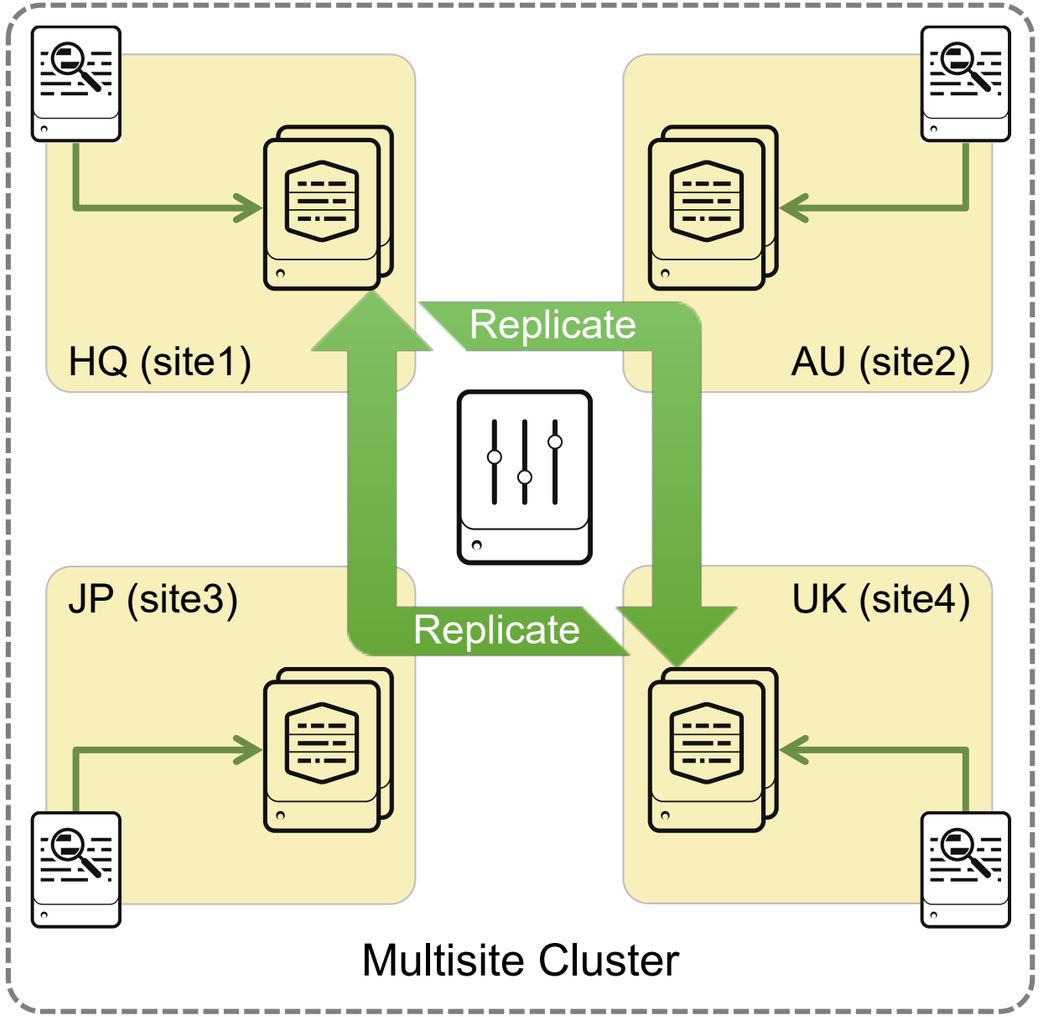
- Describe how Splunk multisite indexer clusters work
- Identify multisite terms
- Implement a multisite indexer cluster
- Describe optional configuration settings

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Key Benefits of Multisite Indexer Cluster

- Allows for an extra layer of data partitioning
  - Indexers are grouped by “sites”
  - A site is logical grouping of Splunk instances
- Multisite clusters offer two key benefits:
  1. Disaster recovery
     - Stores index copies at multiple sites (i.e. geo-location or rack)
     - Provides automatic site-failover capability
     - In case of a disaster, indexing and searching continue on the surviving sites
  2. Search affinity
     - Preferentially searches assigned site
     - Greatly reduces WAN network traffic



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Multisite Cluster Key Attributes

Property Name	Description
`multisite`	Enables multisite clustering
`site`	- A logical group that shares clustering policies - Also the site where the manager node resides
`available_sites`	- Defines the sites in the cluster - Supports up to 63
`site_replication_factor`	Controls how to distribute raw copies of data among the sites
`site_search_factor`	Controls how to distribute searchable copies

- `site_replication_factor origin:2,total:3` ← Replication factor (RF)
- `site_search_factor origin:1,total:2` ← Search factor (SF)

Determines which sites get replicas and how many

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Site Replication Factor Examples

Configuration	Description
`origin:2, total:3`	Default. Put the extra copy on a site that doesn't have a copy
`origin:1, total:4` (where there are 4 sites)	Try to put a copy on any site that doesn't have one
`origin:2, site1:2, total:5`	Both site1 and origin have a minimum of 2 copies
`origin:2, site1:1, total:4`	If origin happens to be site1, then the higher value takes precedence
`origin:2, site1:2, site2:2, total:3`	Invalid

Note

- You must specify the origin
- A factor count must be greater than 0

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

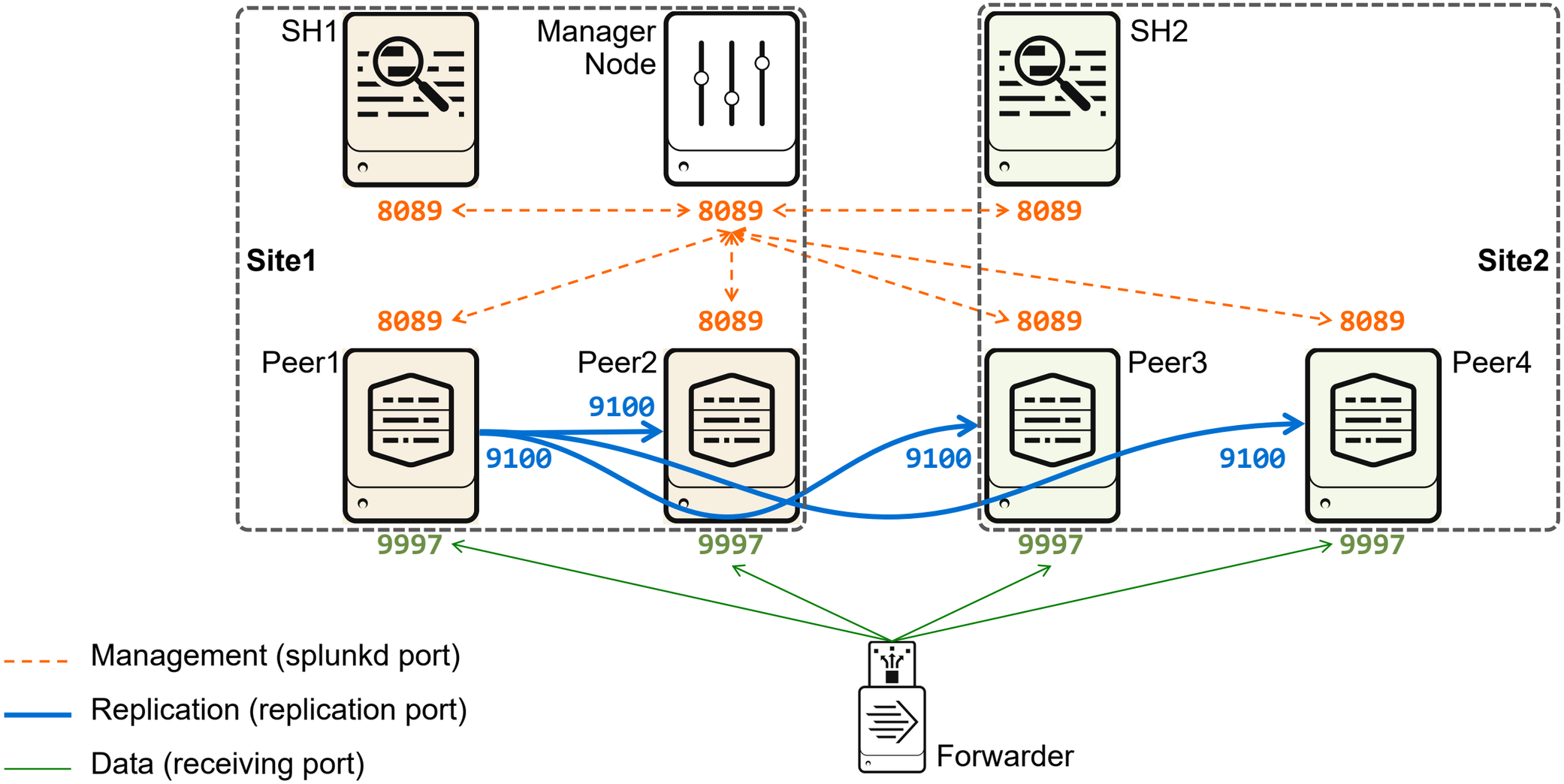
Multisite Indexer Cluster Deployment

1. Determine multisite cluster use cases and requirements
2. Install Splunk Enterprise and configure cluster instances
   - One manager node
   - At least two peer nodes per site
   - One or more search heads per site (recommended)
3. Enable clustering on the instances in the order of **Manager Node > Peer Nodes > Search Heads**
   - Splunk CLI, or manually edit **`server.conf`**
4. Create and distribute the configuration bundle to the peer nodes
5. Configure forwarders to send data to the peer nodes

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Multisite Cluster Topology



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Configuring the Multisite Manager Node

```
splunk edit cluster-config -mode manager -multisite true -site site1
-available_sites site1,site2 -site_replication_factor origin:1,total:2
-site_search_factor origin:1,total:2 -secret mycluster
```

SPLUNK_HOME/etc/system/local/server.conf

```
[general]
site = site1

[clustering]
multisite = true
mode = manager
available_sites = site1,site2
site_replication_factor = origin:1,total:2
site_search_factor = origin:1,total:2
pass4SymmKey = Hashed_Secret
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Configuring Multisite Cluster Peer Nodes

```
splunk edit cluster-config -master_uri https://10.0.1.3:8089
-mode peer -site site1 -replication_port 9100 -secret mycluster
```

Peer1&2

```
splunk edit cluster-config -master_uri https://10.0.1.3:8089
-mode peer -site site2 -replication_port 9100 -secret mycluster
```

Peer3&4

Peer1&2 server.conf

```
[general]
site = site1

[clustering]
mode = slave
master_uri https://10.0.1.3:8089
pass4SymmKey = Hashed_Secret

[replication_port://9100]
```

Peer3&4 server.conf

```
[general]
site = site2

[clustering]
mode = slave
master_uri https://10.0.1.3:8089
pass4SymmKey = Hashed_Secret

[replication_port://9100]
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Configuring Multisite Cluster Search Heads

- Search heads can:
  - Join the indexer cluster at any time
  - Participate in multiple indexer clusters
  - Combine searches across clustered and non-clustered search peers
- Steps to configure a SH to search multiple indexer clusters:
  - If not already a cluster search head, enable it first:

```
splunk edit cluster-config -mode searchhead ...
```

  - To add the search head to another indexer cluster, run:

```
splunk add cluster-master <master_uri:port> ...
```

  - If you need to change the clustering configuration or attributes:

```
splunk edit cluster-master <master_uri:port> ...
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Configuring a New Multisite Search Head

Enable a new instance (SH2) as a cluster search head

```
splunk edit cluster-config -mode searchhead -master_uri https://10.0.1.3:8089 -site site2
-secret mycluster
```

SH2 server.conf

```
[general]
...
site = site2

...

[clustering]
master_uri = https://10.0.1.3:8089
mode = searchhead
multisite = true
pass4SymmKey = Hashed_Secret
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Configuring an Existing SH to Multisite

- Enable the converted SH1 to search an additional single-site cluster

```
splunk add cluster-master https://20.0.2.6:8089 -multisite false -secret 2ndCluster
```

1

- Convert existing single-site cluster search head (SH1) to multisite mode

```
splunk edit cluster-master https://10.0.1.3:8089 -multisite true –site site1 -secret mycluster
```

2

```
1 [clustering]
  master_uri = clustermaster:10.0.1.3:8089,clustermaster:20.0.2.6:8089
  mode = searchhead

2 [clustermaster:10.0.1.3:8089]
  master_uri = https://10.0.1.3:8089
  multisite = true
  pass4SymmKey = Hashed_Secret
  site = site1

1 [clustermaster:20.0.2.6:8089]
  master_uri = https://20.0.2.6:8089
  multisite = false
  pass4SymmKey = Hashed_Secret2
```

SH1 server.conf

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Manager Node View – Multisite Cluster

Indexer Clustering: Master Node

Edit | More Info | Documentation

✓ All Data is Searchable ✓ Search Factor is Met ✓ Replication Factor is Met

4 searchable **0** not searchable
Peers

2 searchable **0** not searchable
Indexes

Peers (4) Indexes (2) Search Heads (3)

filter 10 per page

i	Peer Name	Site	Fully Searchable	Status	Buckets ?
>	idx1	site1	✓ Yes	Up	18
>	idx2	site1	✓ Yes	Up	16
>	idx3	site2	✓ Yes	Up	25
v	idx4	site2	✓ Yes	Up	10

Location 10.0.1.1:8489
Last Heartbeat ..... 3/6/2018, 1:57:52 PM
Replication Port 9400
Base Generation ID 8
GUID DAA8BB0A-8697-4121-A9E7-5E3DC43F160C

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Search Affinity

- In single-site mode, there is only one set of “primary” searchable buckets that respond to searches
- With multisite, each site can have searchable replicas that respond to searches
- Search affinity (enabled by default)
  - Search heads have a site association
  - Searches get as many events as they can from the same site
    - If a searchable bucket exists on the site, it will be the primary bucket for that site
    - Searches will extend across sites only when they are needed
  - Limit the access of each user to only their local search heads

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

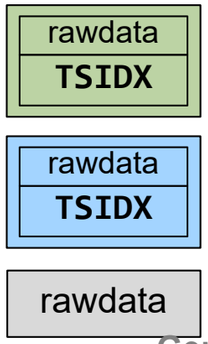
Multisite Factors in Action

Sites: 2
Peer Nodes: 4
Search Heads: 2
Manager Node: 1
Peer Nodes: 4

`site_replication_factor`
`origin: 2`
`total: 3`

`site_search_factor`
`origin: 1`
`total: 2`

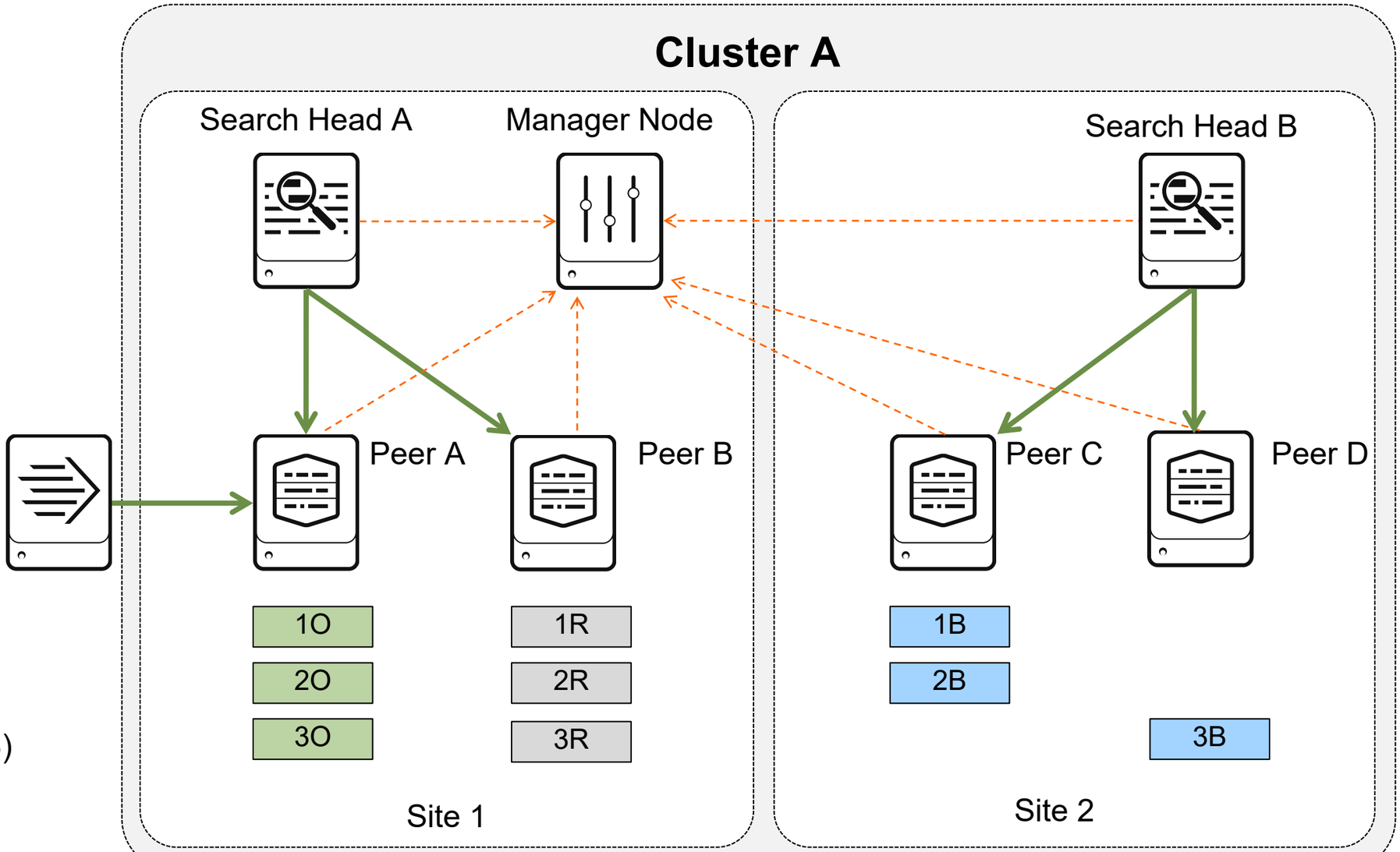
Complete & Valid



Origin (O)

Searchable Backup (B)

Rawdata Only (R)



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Multisite Factors in Action – Primary Loss

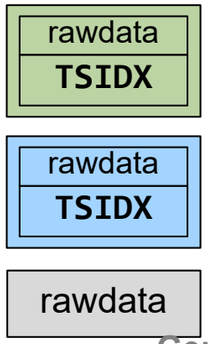
Sites: 2
Peer Nodes: 4
Search Heads: 2
Manager Node: 1
Peer Nodes: 4

`site_replication_factor`
`origin: 2`
`total: 3`

`site_search_factor`
`origin: 1`
`total: 2`

Valid But Not Complete

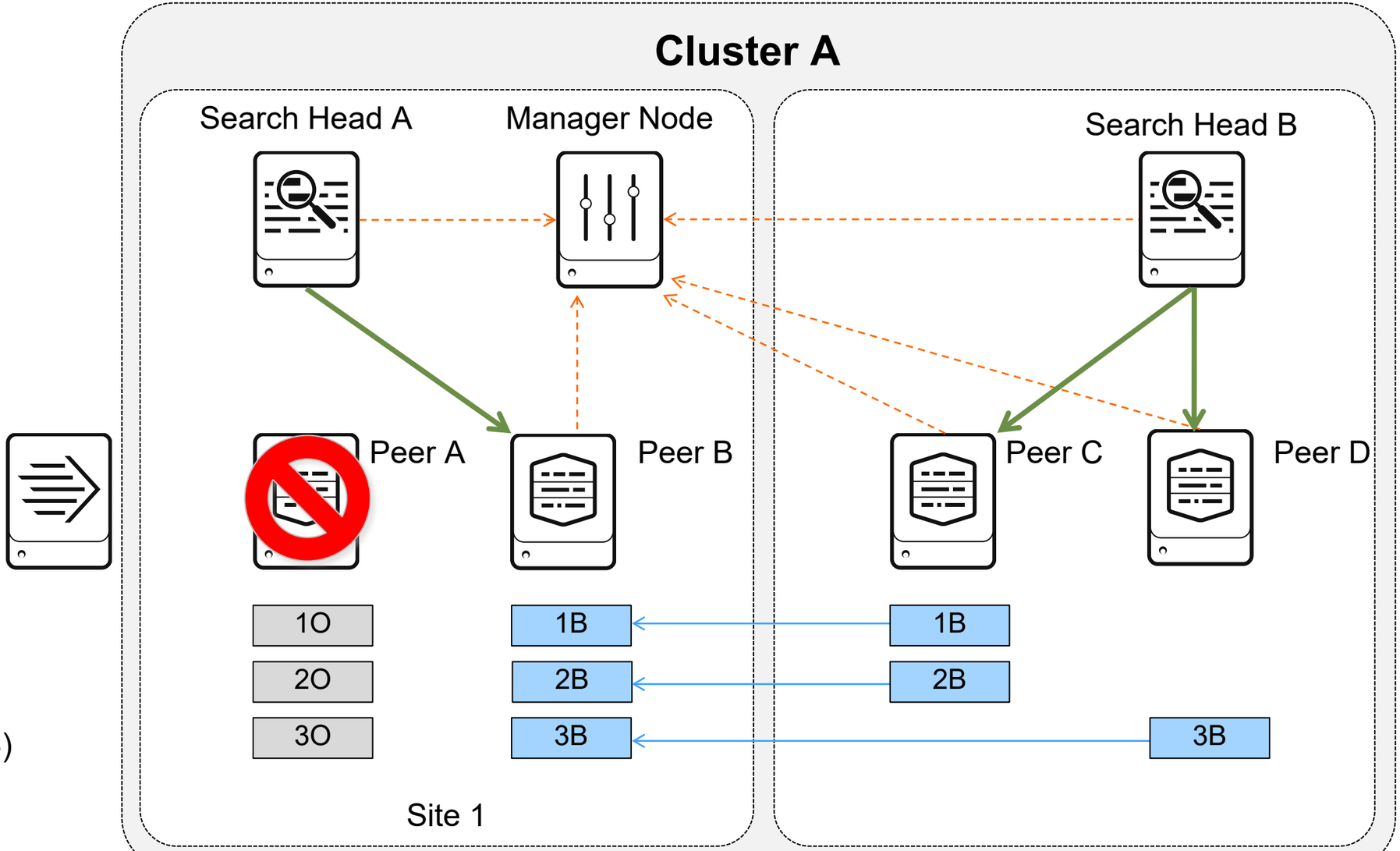
origin:2 is not possible



Origin (O)

Searchable Backup (B)

Rawdata Only (R)



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

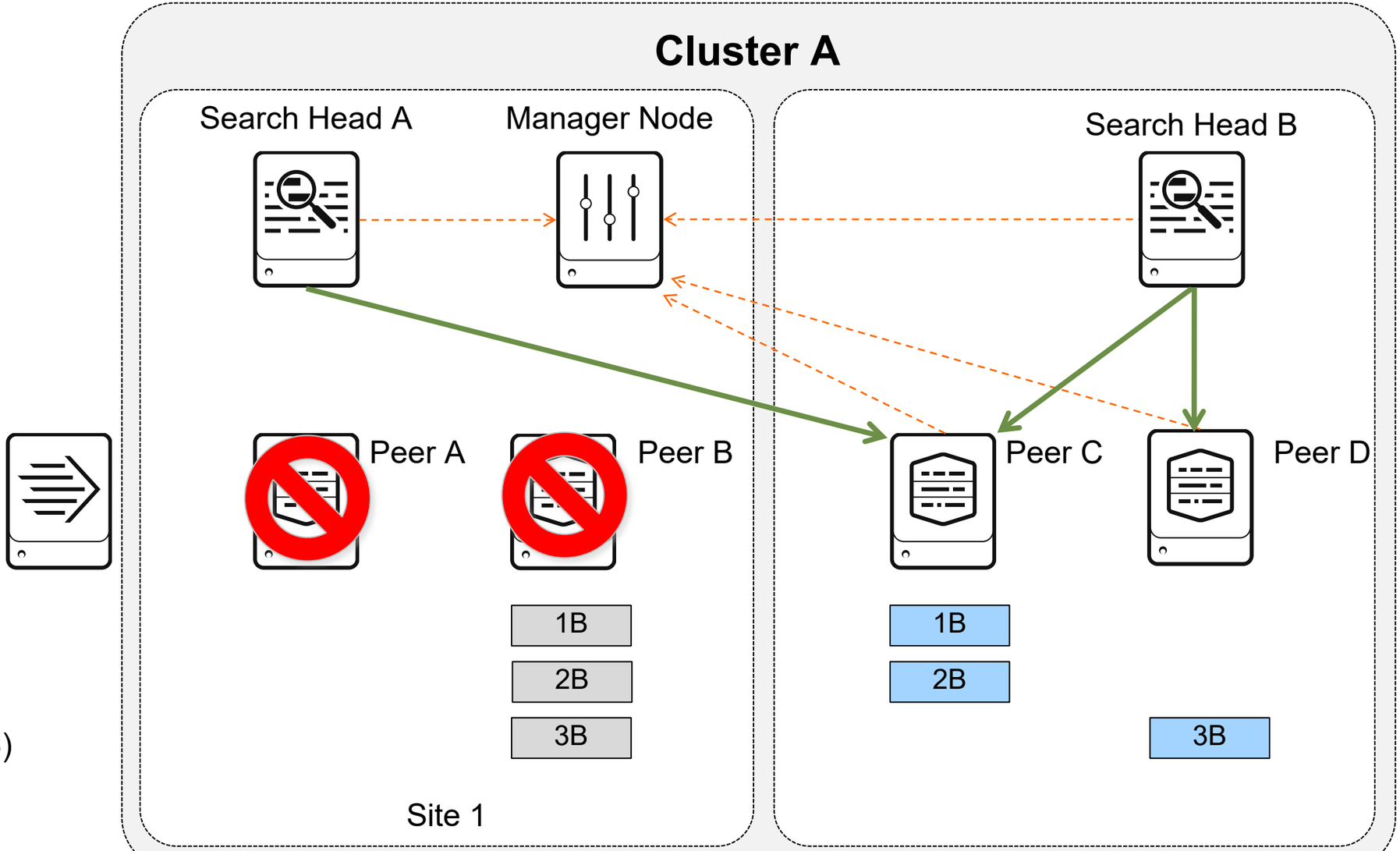
Multisite Factors in Action – Site Loss

Sites: 2
Peer Nodes: 4
Search Heads: 2
Manager Node: 1
Peer Nodes: 4

`site_replication_factor`
`origin: 2`
`total: 3`

`site_search_factor`
`origin: 1`
`total: 2`

Valid But Not Complete



rawdata | TSIDX — Origin (O)

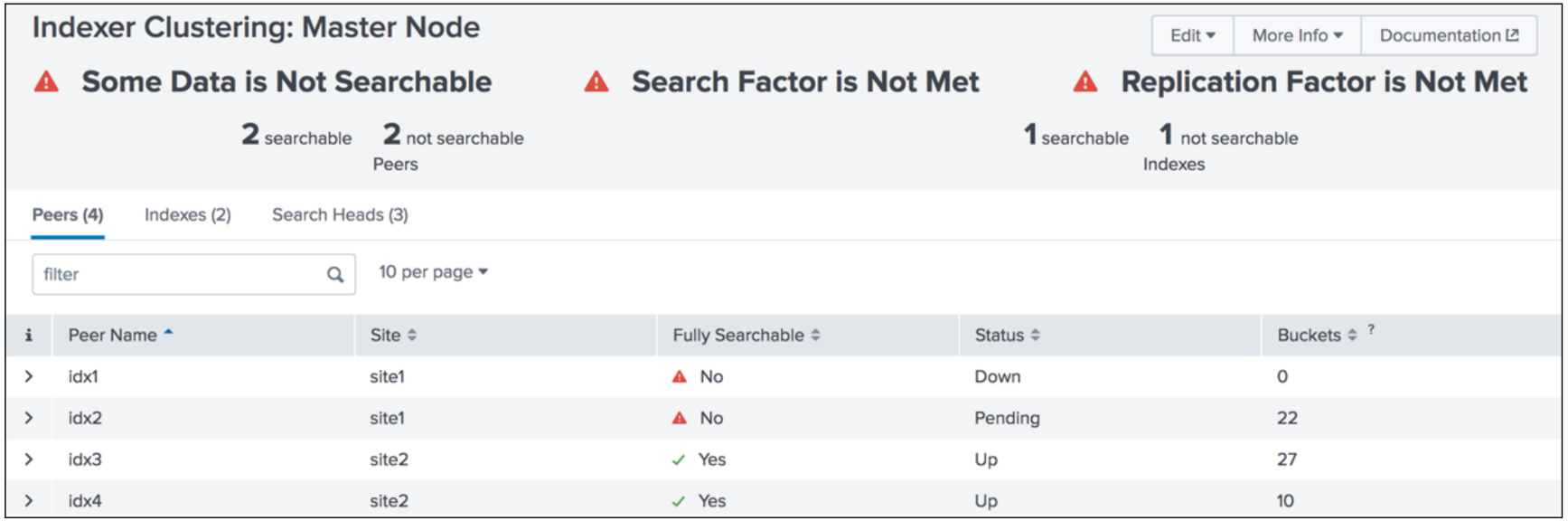
rawdata | TSIDX — Searchable Backup (B)

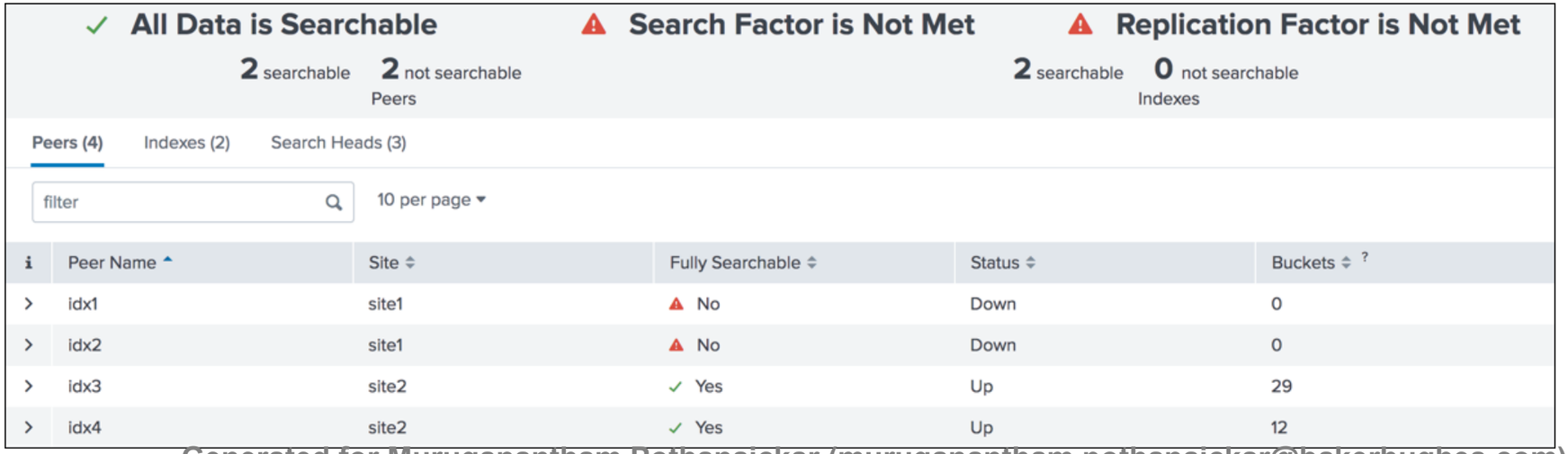
rawdata — Rawdata Only (R)

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Example: **site1** Down





- Pending
  - A replication failed
  - Transitions to the next flag based on the subsequent heartbeat check
- Down
  - The peer went offline for some unknown reason

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Disabling Search Affinity

- You can disable search affinity for overall search performance
  - Spread the search request across indexers on all sites
  - Will increase WAN traffic
- To disable search affinity, edit the search head configuration
  - **IMPORTANT:** all sites must be in close proximity with very low network latency

```
splunk edit cluster-master https://10.0.55.3:8089 -site site0
```

```
[clustermaster:10.0.55.3:8089]
master_uri =
https://10.0.55.3:8089
multisite = true
pass4SymmKey = Hashed_Secret
site = site0
```

SH2 server.conf (Search affinity disabled)

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Manager Node Failover

- Preparing for manager node failover is the same for both single site and multisite clustering
- When a manager restarts, it blocks indexing until enough peers join each site to fulfill the replication factor
- A cluster can be in a state where it CANNOT fulfill the replication factor
  - You need to restart the manager while a site is down

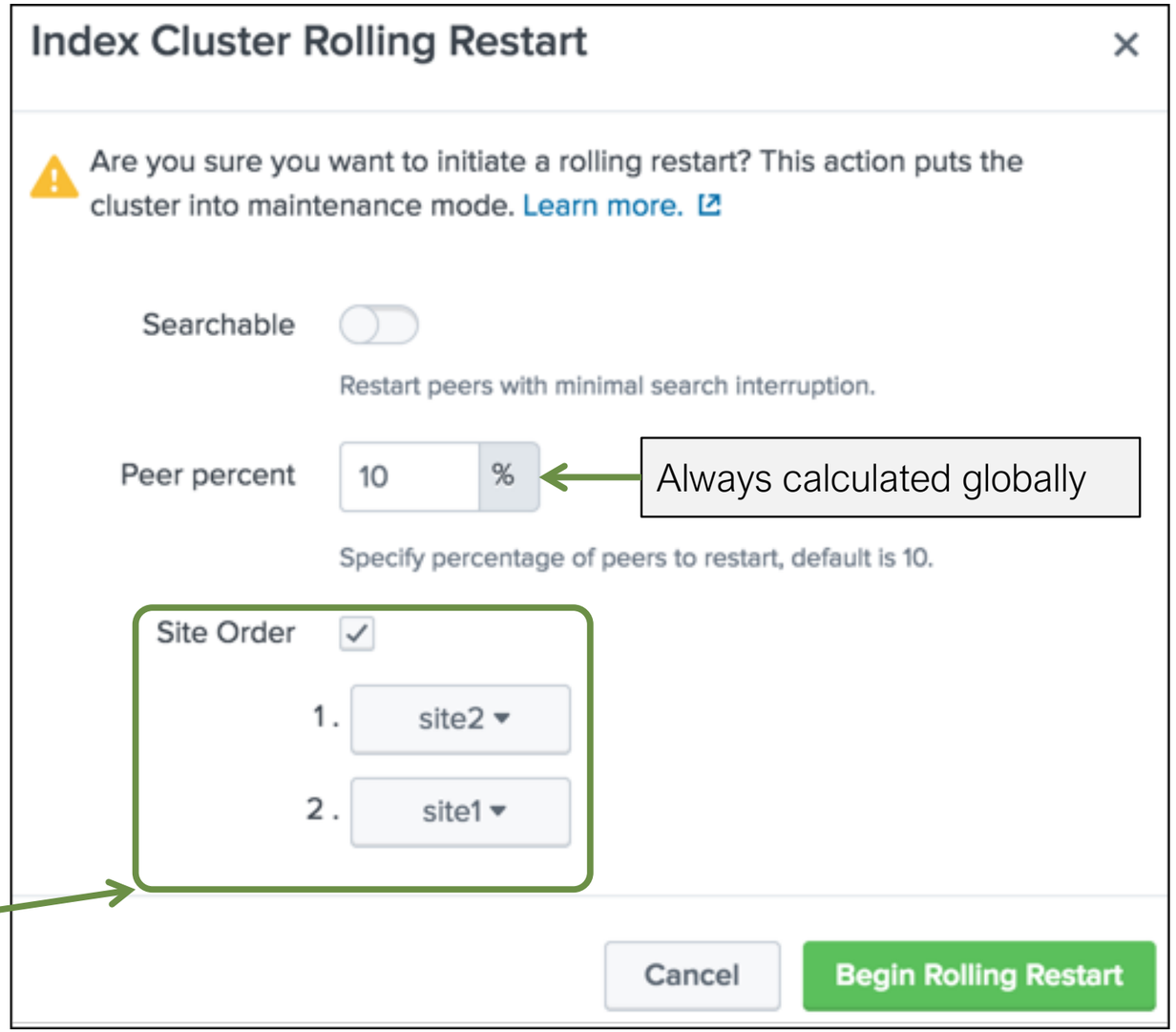
    origin:1, site1:1, ~~site2:1~~, site3:1, total:4
  - The site including the manager goes down and a stand-by manager starts up on another site
- To unblock cluster services, run **`splunk set indexing-ready`** every time you restart the manager node

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Restarting a Multisite Indexer Cluster

- Again, ordinarily you do not restart the entire cluster
  - Search heads can be restarted at any time
- If you must restart the entire cluster:
  1. Restart the manager node
  2. Run preliminary health checks
     - Check the manager dashboard for cluster status
  3. Begin rolling restart
     - The rolling restart in multisite proceeds with site awareness
     - Can set a specific site order




```
splunk rolling-restart cluster-peers
-site-by-site true -site-order site2,site1
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Migrating from Single-site to Multisite

- Make sure all cluster nodes are running the same Splunk Enterprise version

1. Change the manager node to multisite mode and restart
   - DO NOT remove the existing single-site replication factor and search factor
   - New multisite factors must be at least as large as the single-site factors
2. Enable maintenance mode on the manager:

```
splunk enable maintenance-mode
```

3. Change peer nodes to multisite mode with a site association and restart
   - DO NOT restart a peer that hasn't been converted
4. Change search heads to multisite mode and restart

```
splunk edit cluster-master https://CMaster:8089 -multisite true -site
site1 –secret mycluster
```

5. Disable maintenance mode on the manager:

```
splunk disable maintenance-mode
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Indexer Cluster Maintenance Mode

- Invoke **`maintenance-mode`** when performing any work on a peer node that may cause excessive bucket status changes

`> splunk [enable|disable|show] maintenance-mode`

  - Bucket fixup discontinues copying buckets between peers to maintain complete state
  - Only reassigns primaries to maintain a valid state
  - Peer outage while in maintenance mode may return incomplete results
  - Maintenance mode persists across manager restarts
  - No notion of sites; works for both indexer cluster configurations
  - Bucket rolling that would occur due to peer outage is discontinued
  - After disabling maintenance mode, manager node catches up on replication policies

- **`splunk apply cluster-bundle`** and **`splunk rolling-restart`** automatically invoke maintenance mode

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Migration Notes

- Multisite policies apply to new data only
- Existing non-clustered buckets will not replicate; they just age out
- Existing single-site buckets follow the existing policies until they age out by default
  - Do not remove the existing single-site replication attributes
  - Multisite **`total`** values must be larger than the single-site factors
    - Must reduce the single-site factors to match the least number of peers on any site
- Set **`constrain_singlesite_buckets=false`** in manager's **server.conf** to have buckets replicate across sites
  - Follows the specified **`site_replication_factor`** and **`site_search_factor`**

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Indexer Cluster Searchable Rolling Upgrade

- Splunk 7.1+ supports searchable rolling upgrade
  - Minimal service interruption during the upgrade
  - All nodes must be running version 7.1 or later
- For versions prior to 7.1, see: https://docs.splunk.com/Documentation/Splunk/7.0.0/Indexer/Upgradeacluster
- Maintenance releases should be applied in the same order

Note

Health checks are not all inclusive. Checks apply only to the returned criteria.

Manager Node

1. Run preliminary health checks:
   `splunk show cluster-status --verbose`
2. Upgrade the manager node
3. Initialize searchable rolling upgrade
   `splunk upgrade-init cluster-peers`

All Peer Nodes

4. Take the peer offline:
   `splunk offline`
5. Upgrade the peer node
6. Bring the peer online:
   `splunk start`
7. Repeat on all peer nodes

Manager Node

8. Finalize searchable rolling upgrade
   `splunk upgrade-finalize cluster-peers`

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Further Reading: Clustering

- Basic clustering concepts for advanced users
  - http://docs.splunk.com/Documentation/Splunk/latest/Indexer/Basicconcepts
- Manager site failover
  - https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Handlemanagernodefailure
- Configure the search head
  - http://docs.splunk.com/Documentation/Splunk/latest/Indexer/Configurethesearchhead

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

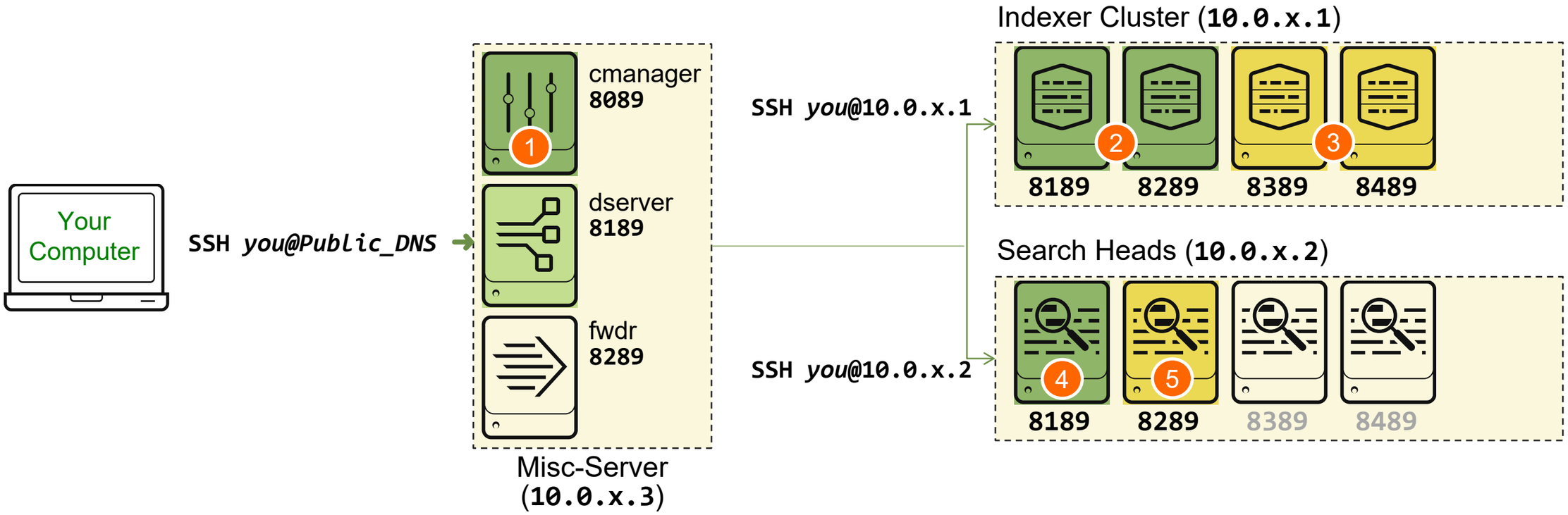
Lab Exercise 3 – Migrate to Multisite Cluster

- **Time**: 20 - 25 minutes
- **Tasks**:
  - Migrate the single-site manager node to the multisite mode
  - Migrate the existing peer nodes and add a new peer
  - To configure **`site2`**, convert **`IDX3`** and add a new peer **`IDX4`**
  - Convert **`SH1`** to **`site1`** search head and add **`SH2`** to **`site2`**
- **Optional Tasks:** (additional 15 minutes)
  - Test the indexer site failover scenario
    - Stop **`site1`** processes
    - Check the cluster status and verify the search affinity

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Lab Exercise 3 – Migrate to Multisite Cluster (cont.)

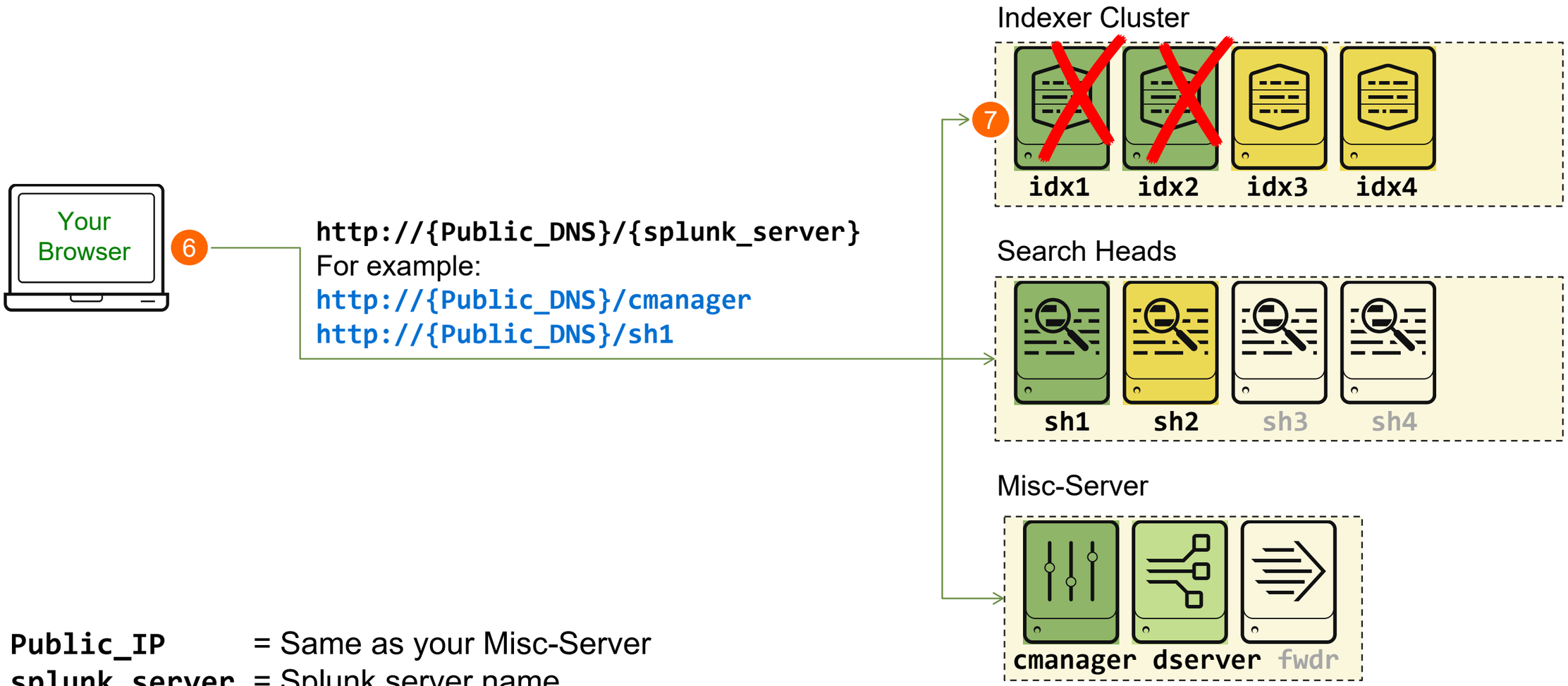


x = Your student ID
8?89 = splunkd-port

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Lab Exercise 3 – Migrate to Multisite Cluster (cont.)



Public_IP = Same as your Misc-Server
splunk_server = Splunk server name

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module 4: Indexer Cluster Management and Administration

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module Objectives

- Enable replication for custom indexes
- Deploy common apps and configurations to peer nodes
- Take a peer offline temporarily
- Decommission a peer permanently
- Clean up excess cluster buckets
- Optimize peer node storage utilization
- Configure Monitoring Console for indexer cluster environment

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Configuring Clustered Indexes: **repFactor**

- The **repFactor** attribute in **indexes.conf** configures the index to participate in the cluster or not
  - **repFactor = auto** (replicate)
  - **repFactor = 0** (do not replicate)
- All peer nodes must use the same set of **indexes.conf** files
  - **DO NOT** use the Splunk UI to configure index settings in a cluster
  - Deploy from the manager node
- Default is **0** (do not replicate), however the internal indexes are set to replicate automatically

master-apps/_cluster/default/indexes.conf

```
[main]
repFactor = auto

[history]
repFactor = auto

[summary]
repFactor = auto

[_internal]
repFactor = auto

[_audit]
repFactor = auto

[_thefishbucket]
repFactor = auto

[_telemetry]
homePath   = $SPLUNK_DB/_telemetry/db
coldPath   = $SPLUNK_DB/_telemetry/colddb
thawedPath = $SPLUNK_DB/_telemetry/thaweddb
repFactor = auto
...
```

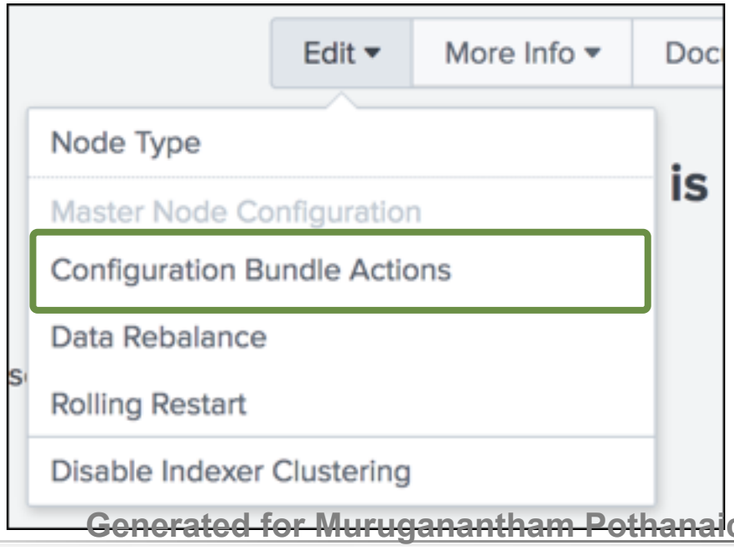
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

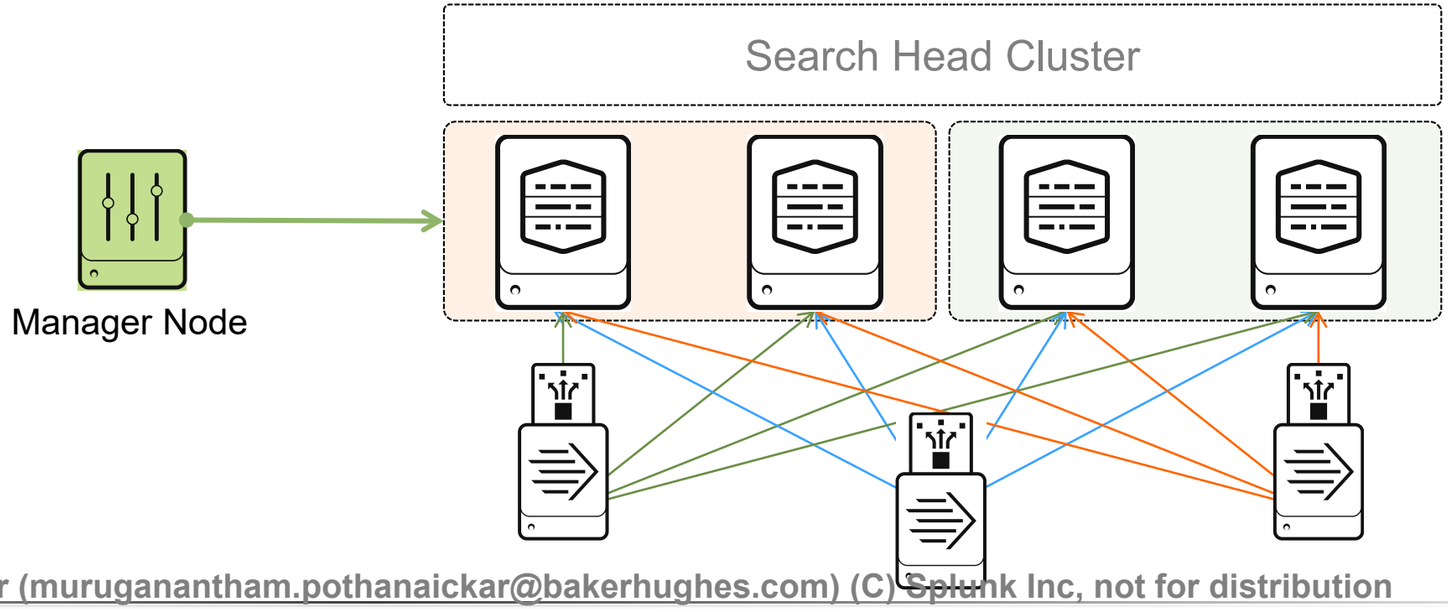
Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Master-apps Deployment Tool

- The manager node distributes configuration bundles (apps) to the peer nodes
  - Supports common configurations for inputs, parsing, and indexing (**`inputs.conf`**, **`props.conf`**, **`transforms.conf`**, **`indexes.conf`**)
- Stage deployment bundles in the manager's **`SPLUNK_HOME/etc/master-apps`** directory
  - For common apps, copy them to the **`<app-name>`** subdirectory
  - For standalone files, copy them to the **`_cluster/local`** subdirectory
- If necessary, manager node initiates an automatic rolling restart of all peers

Manager Node: Settings > Indexer clustering

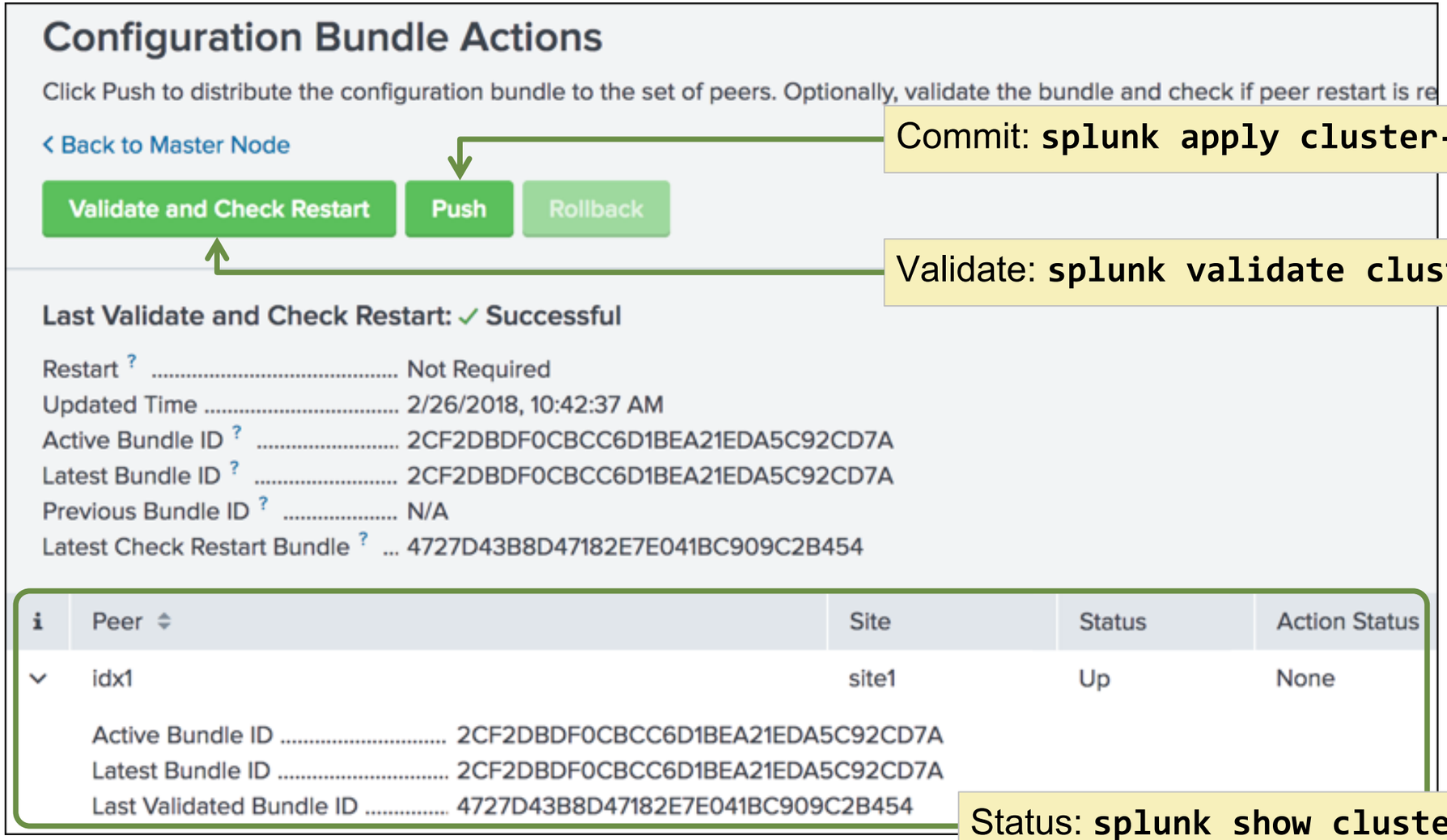




Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Configuration Bundle Status and Actions



Commit: `splunk apply cluster-bundle [--skip-validation]`

Validate: `splunk validate cluster-bundle [--check-restart]`

- DO NOT edit the **`slave-apps`** content directly
  - Read-only
  - Will lose any direct changes

Status: `splunk show cluster-bundle-status [--verbose]`

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Index-time Configuration Precedence Revisited

```
SPLUNK_HOME/etc/master-apps
    /_cluster
        /default
        /local
    /<app_name>
        /default
        /local
```

Manager Node

```
SPLUNK_HOME/etc/slave-apps
    /_cluster
        /default
        /local
    /<app_name>
        /default
        /local
```

Peer Nodes

Precedence order for indexer cluster peers:

1. slave-apps local directories (cluster peers only)
2. System local directory
3. App local directories
4. slave-apps default directories (cluster peers only)
5. App default directories
6. System default directory

Note

Within the **`slave-apps`** directories, the precedence is based on the ASCII sort order.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

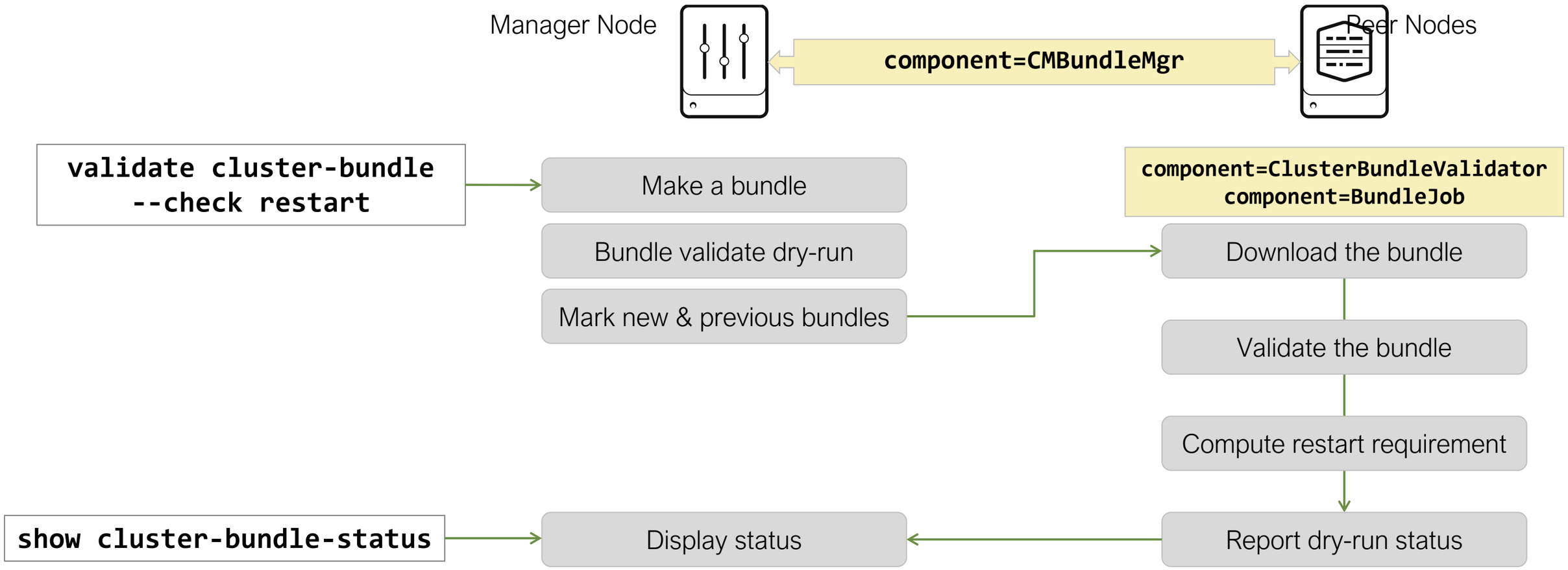
Rollback the Configuration Bundle

- If the **Push** action fails, you can restore to the previously running state
  - **Rollback** command restores the peer nodes to their previous state
  - After the rollback, fix the problem in the **`master-apps`** directory and re-apply
- To restore, click **Rollback** from the manager node
  - Peers can only join the cluster if bundle validation succeeds during restart
  - **Rollback** toggles only between the most recent configuration bundle and the previous bundle
    - This is different than undo
- Also can run: **`splunk rollback cluster-bundle`**

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Log Channels for `master-apps` Activities

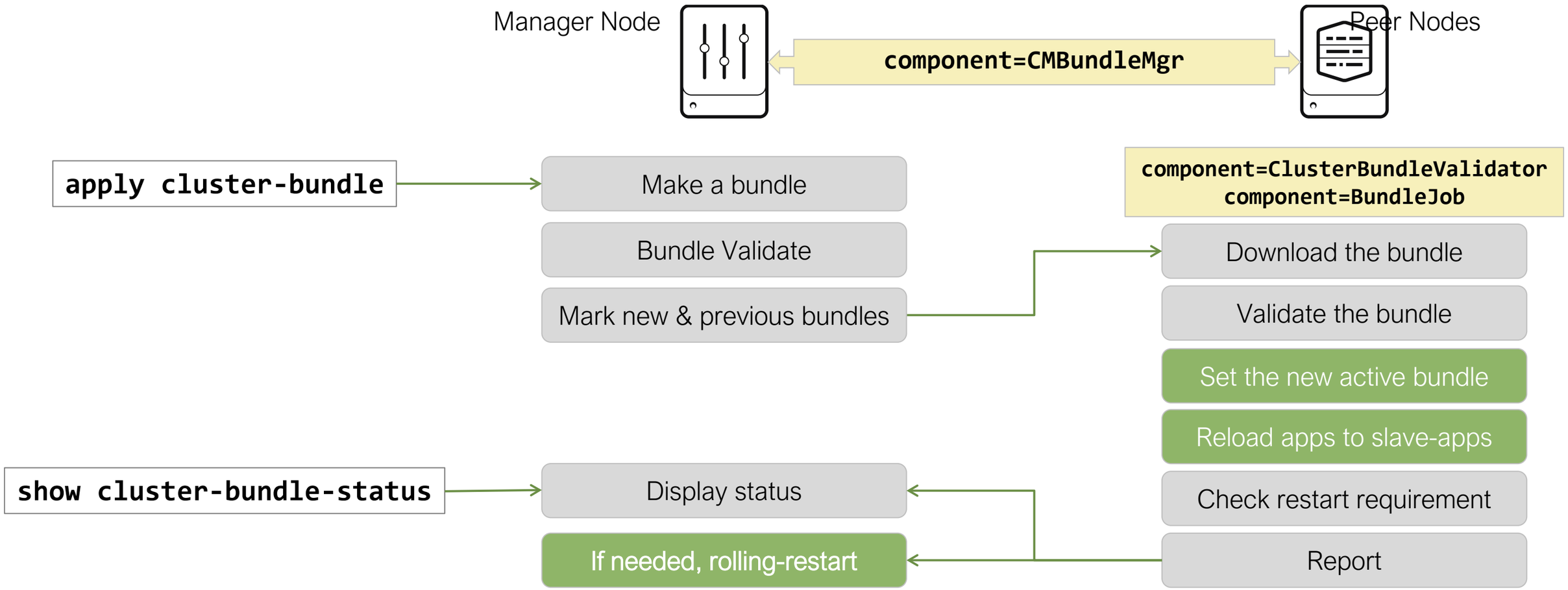



```
index=_internal sourcetype=splunkd component IN (CMBundleMgr, BundleJob, ClusterBundleValidator)
| stats count by _time, host, component, event_message
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Log Channels for `master-apps` Activities (cont.)



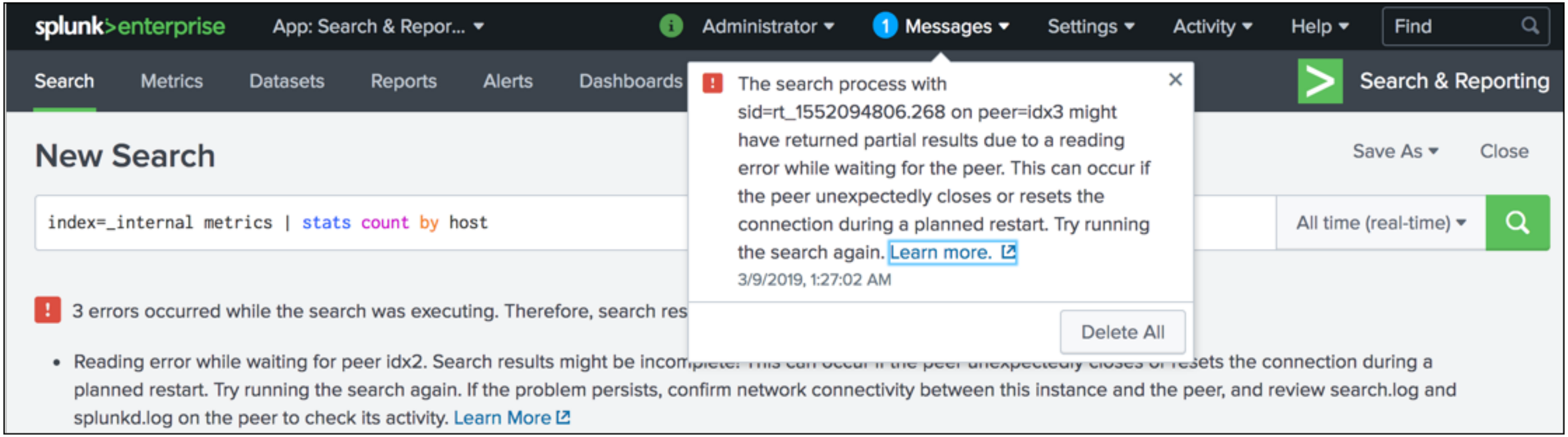

```
index=_internal sourcetype=splunkd component IN (CMBundleMgr, BundleJob, ClusterBundleValidator)
| stats count by _time, host, component, event_message
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Indexer Cluster Searchable Rolling Restart

- Restarts peer nodes while maintaining the search availability
  - Trades search availability with restart completion time
  - Takes considerably longer to complete because it restarts all nodes one at a time
  - Requires all cluster nodes to be on Splunk 7.1 or higher



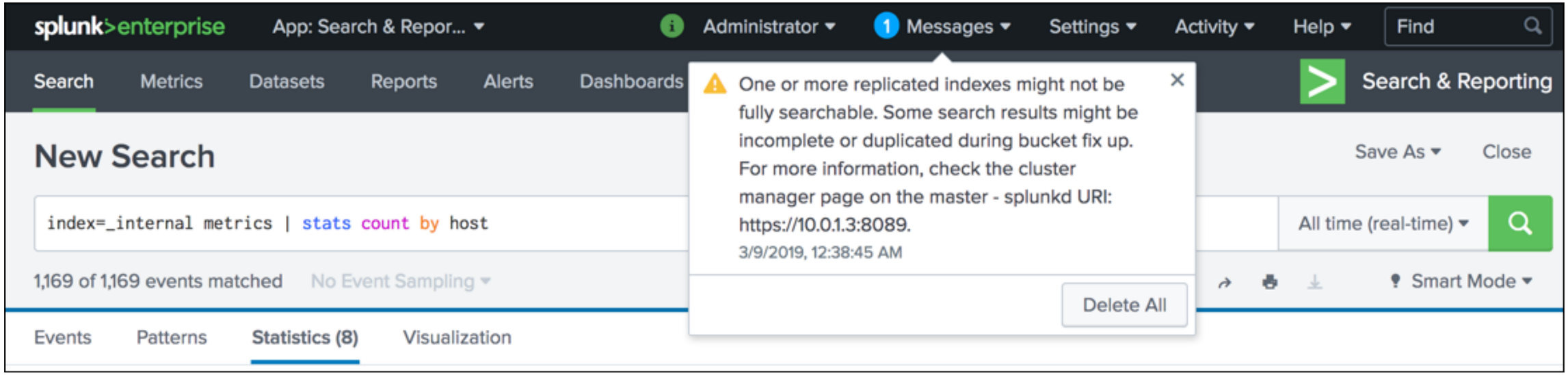
Search head displays error messages when the default rolling-restart is in progress

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Indexer Cluster Searchable Rolling Restart (cont.)

- Best-effort search availability – performs a restart one peer node at a time
  - Completes in-progress searches before peer nodes restart
  - Searches that cannot complete within the timeout (default: 180 sec) are retried, timed-out or optionally deferred
    - In some cases, they may need to be explicitly retried by user
  - Real time and indexed real time searches continue to run with available peer nodes



Search is unaffected and continues when the searchable rolling-restart is in progress

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

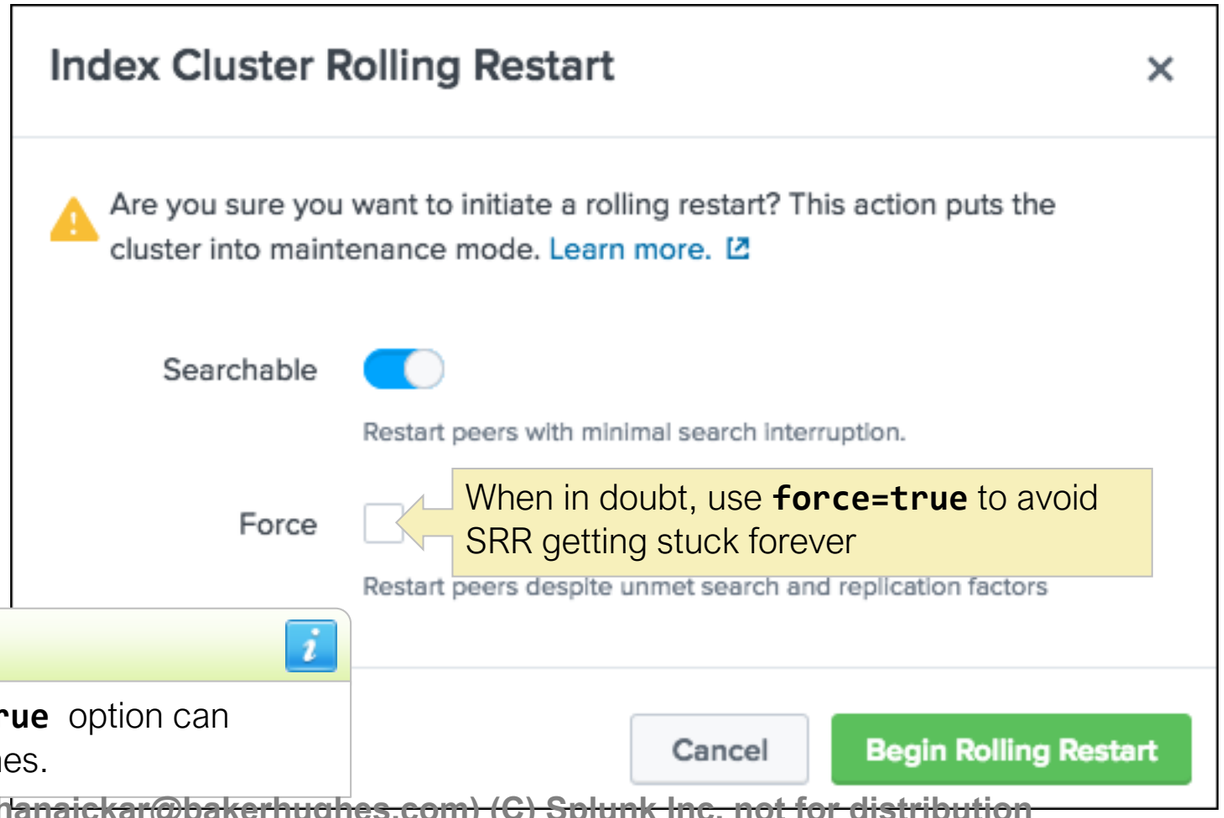
Searchable Rolling Restart (SRR) Options

- **`searchable <true|false>`**
  - **`false`** = ignore all options
- **`force <true|false>`**
  - **`true`** = proceed with the searchable rolling restart despite health check failures
  - Specify these additional parameters
    - **`restart_inactivity_timeout <sec>`**

      Timeout before manager node gives up on the current peer and moves on to the next peer (default: 600 sec = 10 min)
    - **`decommission_force_timeout <sec>`**

      Timeout for a peer to finish and voluntarily restart before it is forced to restart (default: 180 sec = 3 min)

```
splunk rolling-restart cluster-peers
-searchable <true/false>
[-force <true/false>
-restart_inactivity_timeout <sec>
-decommission_force_timeout <sec>]
```



When in doubt, use **`force=true`** to avoid SRR getting stuck forever

Note

The **`force=true`** option can impact searches.

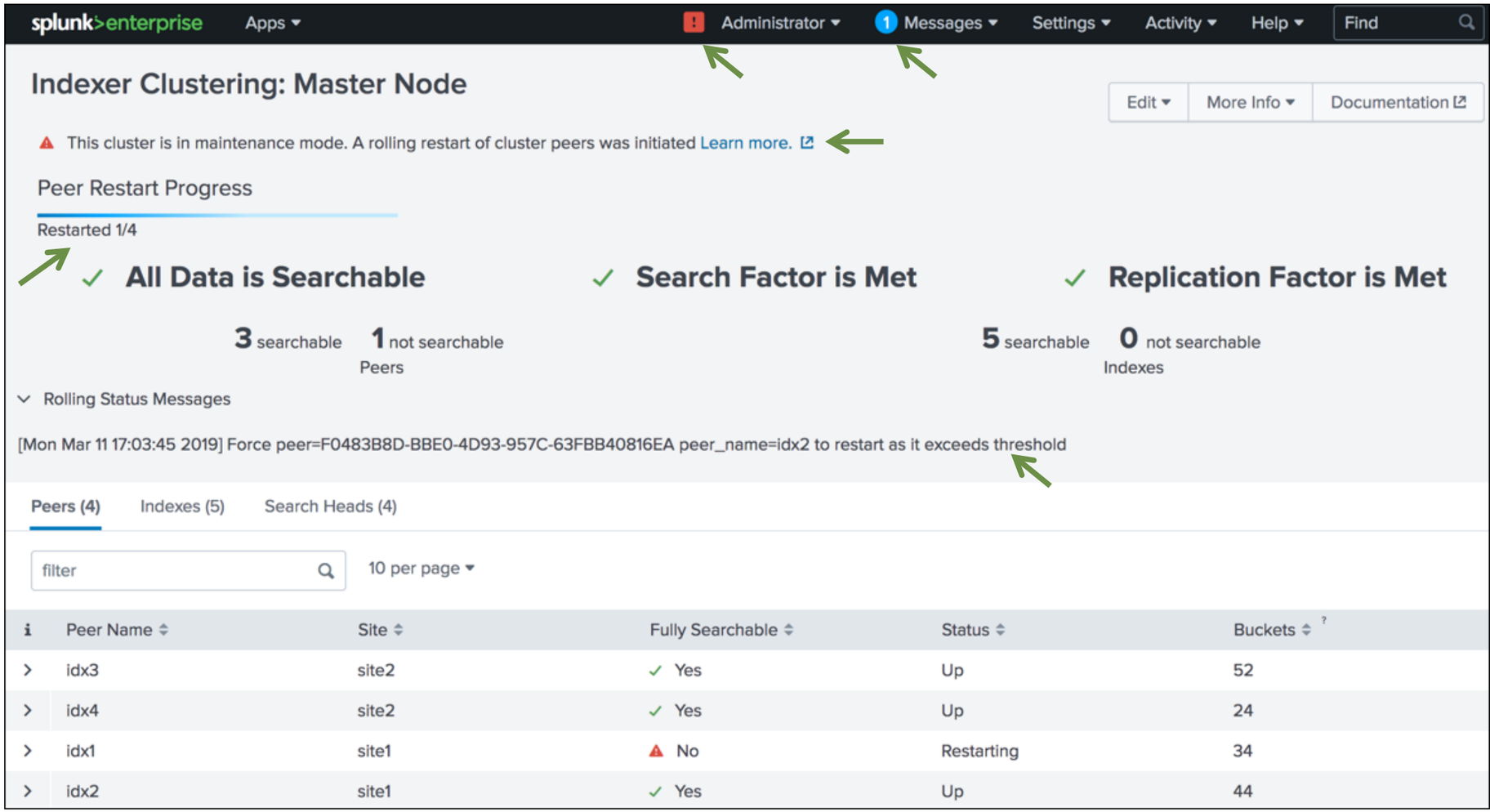
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Tracking Rolling Restart Progress

- Web UI
  - Health status
  - A maintenance message
  - Progress bar
  - Additional messages
- CLI

```
splunk show
cluster-status
--verbose
```



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Temporarily Taking a Peer Offline

- Before taking a peer node offline, make sure the cluster has enough peer nodes to meet the replication policy
  - To minimize bucket fixup activities, take down only one node at a time
- To bring down a peer temporarily, run: **`splunk offline`**
  - The manager node delays bucket-fixing and just maintains a valid state
  - The peer node must be back online within 60 seconds (by default)
    - If the peer node does not return, the manager node initiates bucket fixup activities
  - If you need more time, extend the wait time on the manager node:

```
splunk edit cluster-config -restart_timeout <wait_seconds>
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Permanently Decommissioning a Peer Node

- To decommission a peer node permanently, run:

  `splunk offline --enforce-counts`

  – Does not shut down until all search and remedial activities have completed

  – Can take quite a while because the cluster must come to a complete state

  http://docs.splunk.com/Documentation/Splunk/latest/Indexer/Takeapeeroffline

- The manager keeps the peer node information even when it is decommissioned

  – If you want to remove it from the manager node permanently, run:

  `splunk remove cluster-peers -peers <guid>,<guid>,...`

i	Peer Name	Site	Fully Searchable	Status	Buckets
⌄	idx1	site1	⚠ No	Graceful shutdown	0

Location 10.0.1.1:8189
Last Heartbeat ..... 3/11/2019, 10:22:09 AM
Replication Port 9100
Base Generation ID 18446744073709552000
GUID A0EFDDE0-76B0-4529-AF4C-DDBFC70ED3F2

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Adding or Moving Peer Nodes

- To add a peer node to an existing cluster, use the standard peer node configuration procedures
- To move a peer node to a different site:
  1. Take the node offline with **`splunk offline --enforce-counts`**
  2. Move the server and have it join the new site's network
  3. Delete or uninstall Splunk Enterprise from the peer
     - Remove the index directories, if necessary
  4. Reinstall Splunk Enterprise
  5. Enable it as the peer node to the new site

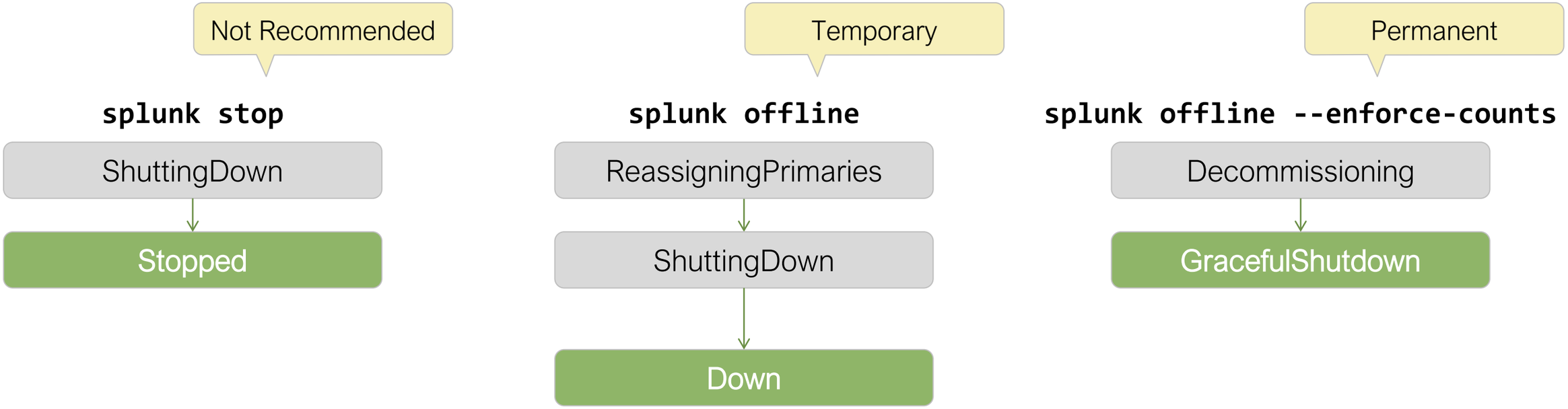
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Indexer Cluster Peer Status

The manager node dashboard reports several possible status conditions for peer nodes

http://docs.splunk.com/Documentation/Splunk/latest/Indexer/Howtomonitoracluster



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Decommissioning a Site

- After a site upgrade/migration, you can decommission a site that is no longer in use
- Prerequisites
  - The cluster must be in a complete state
  - The manager node must not be a part of the decommissioning site
  - There must be at least one searchable copy of each bucket on other remaining sites
- NOTE:
  - Any prior standalone and single-site buckets will be lost
  - Decommissioning starts bucket fixup activities and can take a considerable amount of time

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Steps for Decommissioning a Site

1. Reassign site search head(s) to a remaining site
2. If forwarders are associated with the decommissioned site using indexer discovery, re-assign them to a remaining site
3. Run **`splunk enable maintenance-mode`** on the manager node
4. Update the following attributes in the manager's **server.conf**:
   - `available_sites`
   - `site_replication_factor`
   - `site_search_factor`
   - **`site_mappings`**
5. Restart the manager node
6. Run **`splunk disable maintenance-mode`** on the manager node to start the fixup process
7. Decommission each peer with **`splunk offline --enforce-counts`**

Note

`site_mappings` is a way to handle buckets that are stuck during fixups due to decommissioned origin site.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

site_mappings Example 1

Replace old peers in **site2** with a new site

```
available_sites = site1,site2
site_replication_factor = origin:1, total:2
site_search_factor = origin:1,total:2
```

available_sites = site1,~~site2~~,**site3**
site_replication_factor = origin:1,**site1:1,site3:1**,total:2
site_search_factor = origin:1,**site1:1,site3:1**,total:2
site_mappings = site2:site3

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

site_mappings Example 2

Replace all peers in **site1 & site2**

```
available_sites = site1,site2
site_replication_factor = origin:1, total:2
site_search_factor = origin:1,total:2
```

```
available_sites = site1,site2,site3,site4
site_replication_factor = origin:1,site3:1,site4:1,total:2
site_search_factor = origin:1,site3:1,site4:1,total:2
site_mappings = site1:site3,site2:site4
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

site_mappings Example 3

Migrate from multisites to a single **site4**

```
available_sites = site1,site2,site3
site_replication_factor = origin:1,site1:1,site3:1,total:2
site_search_factor = origin:1,site1:1,site3:1,total:2
site_mappings = site2:site3
```

Note

If a site used in a mapping is later decommissioned, its previous mappings must be remapped to an available site.

```
available_sites = site1,site2,site3,site4
site_replication_factor = origin:2,site4:2,total:2
site_search_factor = origin:2,site4:2,total:2
site_mappings = default_mapping:site4
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

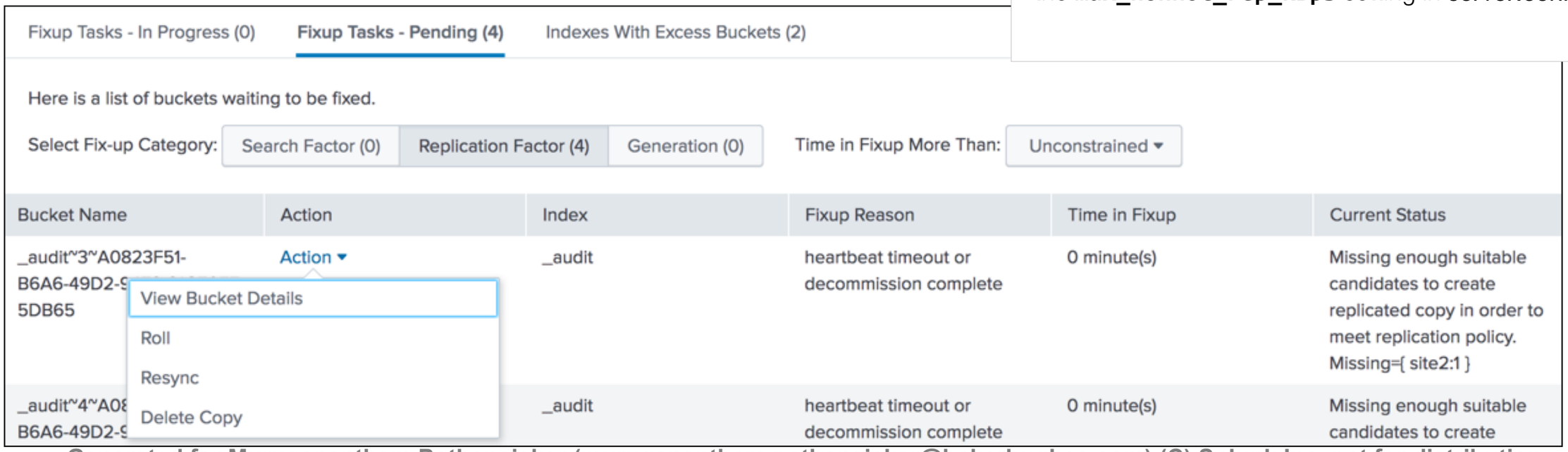
Copyright © 2022 Splunk, Inc. All rights reserved

Bucket Status and Fixup

- Bucket fixup is the process of manager node trying to meet the search and replication policies
  - Copies both rawdata and index data to meet the replication factor and search factor
- The Bucket Status page displays fixup tasks and their states

Note

A massive fixup after the loss of peers can saturate the network and adversely affect indexing tasks. Consider throttling non-hot replication bandwidth with the **`max_nonhot_rep_kBps`** setting in server.conf.

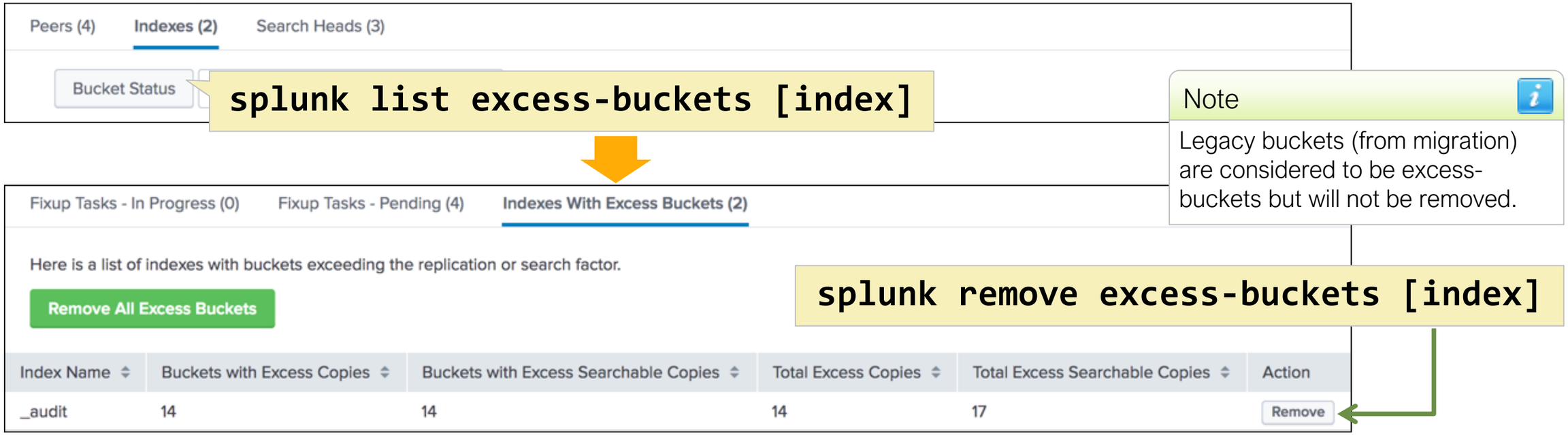


Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Cleaning Up Excess Bucket Replicas

- There might be extra copies of buckets in a cluster when a peer node rejoins a cluster after fixup has occurred
  - This does not affect searching, but consumes storage space
- To determine and manage these excess buckets, use Splunk Web or CLI on the manager node



Note

Legacy buckets (from migration) are considered to be excess-buckets but will not be removed.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Monitoring Indexer Cluster with Metrics

- Internal logs under clustering may get rotated too fast and a **`diag`** may not provide sufficient information
  - For more insight, search:

```
index=_internal sourcetype=splunkd {bucket_id}
```

- **`metrics.log`** can provide service loads and job activities

```
index=_internal sourcetype=splunkd metrics name=cm*
| stats values(group) AS groups by name
```

Cluster service loads based on the number of endpoint accesses and their response times

Scheduled tasks, finished tasks, tasks still pending

Peers have their own corresponding metrics

name	groups
cmmaster	jobs
cmmaster_endpoints	subtask_counts subtask_seconds
cmmaster_executor	executor
cmmaster_service	subtask_counts subtask_seconds
cmslave	jobs
cmslave_endpoints	subtask_counts subtask_seconds
cmslave_executor	executor
cmslave_synchronous	jobs
cmslave_synchronous_executor	executor

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Primary Rebalancing

- Primary rebalancing balances the search load across all peer nodes
  - The manager identifies duplicate searchable buckets and attempts to reassign approximately the same number of primaries on each peer
  - Does not actually move searchable copies to different peer nodes
- Occurs independently for each site in a multisite cluster
  - Does not shift primaries between sites
- Primary rebalancing triggers automatically when:
  - A peer node joins or rejoins the cluster
  - Manager node rejoins the cluster
  - Rolling restart completes
- Can also manually trigger the rebalancing process with the REST endpoint on the manager:

```
services/cluster/master/control/control/rebalance_primaries
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Data Rebalancing

- Uneven bucket distribution doesn't utilize storage optimally and can cause higher load on certain peer nodes
- Uneven bucket distribution can occur:
  - After adding new peer nodes
  - When forwarding data is skewed
  - After frequent bucket fixups due to outages

Duration (seconds)	Component	Invocations	Input count	Output count
8.33	dispatch.stream.remote	51	-	20,767,549
5.72	dispatch.stream.remote.idx1	27		12,316,674
2.61	dispatch.stream.remote.idx2	22	-	8,431,689
0.00	dispatch.stream.remote.idx3	1	-	9,590
0.00	dispatch.stream.remote.idx4	1	-	9,596

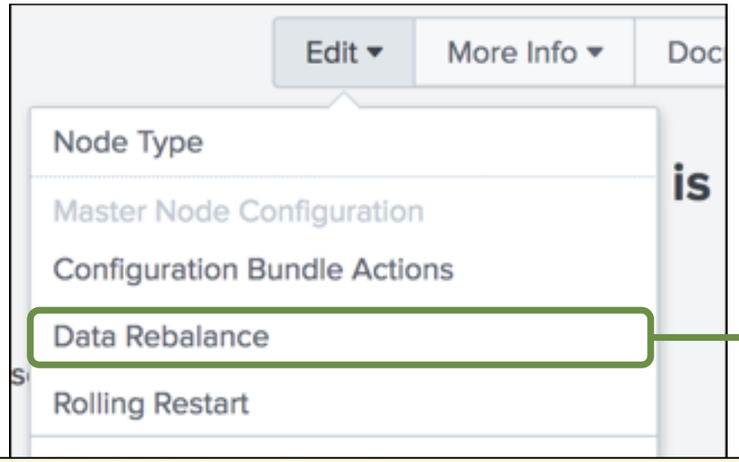
- Data rebalancing redistributes the number of bucket copies per index
  - Balances the storage distribution across the peer nodes
  - Operates on only warm and cold buckets, NOT hot buckets
  - Rebalances all non-searchable, searchable and primary buckets
- In multisite cluster, data is rebalanced within a site as well as across sites

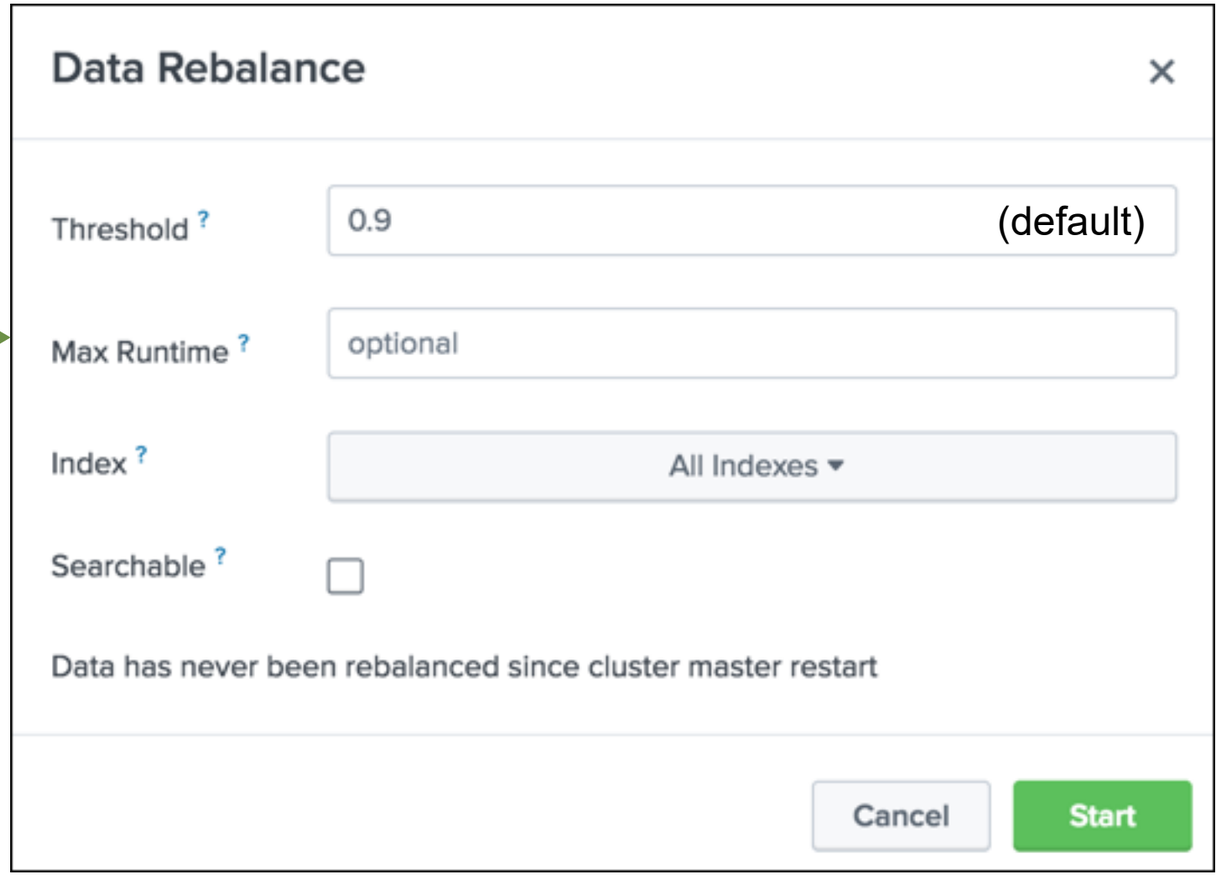
i	Peer Name ^	Site	Fully Searchable	Status	Buckets ?
>	idx1	site1	✓ Yes	Up	68
>	idx2	site1	✓ Yes	Up	14
>	idx3	site2	✓ Yes	Up	40
>	idx4	site2	✓ Yes	Up	40

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Data Rebalancing (cont.)






```
> splunk edit cluster-config -rebalance_threshold 0.90
> splunk rebalance cluster-data -action start
 [-searchable true] [-index <idx>] [-max_runtime <min>]
> splunk rebalance cluster-data -action status
> splunk rebalance cluster-data -action stop
```

- This process impacts search performance
  - Can run it in searchable mode
    - Takes longer to complete and requires more storage space
  - The goal is to achieve a practical balance, not a perfect balance
  - http://docs.splunk.com/Documentation/Splunk/latest/Indexer/rebalancethecluster

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Report and DM Acceleration Replication

- By default, indexer clusters do not replicate report acceleration and data model acceleration summaries
  - Only primary buckets have associated summaries
- To enable summary replication, run this on the manager node:

  `splunk edit cluster-config -summary_replication true`

  Or, set **`summary_replication = true`** in server.conf

```
[clustering]
summary_replication = true
```

- All searchable copies contain all the replicated summaries for that bucket
  - For hot buckets, the cluster creates a summary for each searchable copy
  - For warm/cold buckets, the cluster replicates to fill in any missing or out-of-date summaries

Note

With summary replication enabled, summary-generating searches use more resources across the cluster. The searches may take longer to complete.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Tsidx Reduction in Clustering

- You can trade some search performance for significant index size reduction with the Splunk storage optimization feature
  - Only non-hot buckets old enough qualify
  - Certain metadata files get removed from the optimized buckets
  - Produces minified buckets ending with a **`.mini.tsidx`** extension
- Minified buckets are searchable buckets
  - If the cluster needs a new searchable bucket, it first attempts to replicate from the existing searchable copy
  - If the cluster has no searchable copy, it rebuilds a full bucket and then minifies it during the next minification schedule
  - NOTE:
    - Commands such as **`tstats`** and **`typeahead`** do not work on minified buckets

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Peer Detention – Automatic

- A peer enters the **automatic detention** state when the **`minFreeSpace`** threshold in **`server.conf`** is crossed
- Default value is 5GB
- When a peer is in automatic detention:
  - all indexing is stopped (internal and external)
  - replication is stopped
  - stops participating in searches

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Peer Detention – Manual

- A peer can be put into a detention state manually. When a peer is in manual detention:
  - stops replicating data from other peer nodes
  - optionally disables external data ports, causing it to stop indexing most types of external data
  - continues to index internal data
  - continues to participate in searches
- Use cases for **manual detention**:
  - Before decommissioning a peer, make it available only for searches
  - Preempt automatic detention
  - Diagnose a suspect peer by blocking indexing and replication
  - Force new data to go to other peers
  - Slow the disk writes by only allowing indexing, but not replication

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Enabling Manual Detention

- From the manager node:

```
splunk edit cluster-config -manual_detention [on|on_ports_enabled|off]
-peers <guid1>, <guid2>,...
```

- From the peer:

```
splunk edit cluster-config -manual_detention [on|on_ports_enabled|off]
```

- **on** closes the TCP, UDP, and HEC ports
  - Disables indexing and replication for all network-based or remote (forwarder) data inputs
  - Still indexes local monitor and scripted inputs
- **on_ports_enabled** blocks incoming replication, but continues to index
- **off** disables the manual detention
- Checking the detention status
  - On the manager node: **splunk show cluster-status**
    Settings > Indexer Clustering > Peers
  - On the peer node: **splunk list cluster-config**
  - On monitoring console: Indexing > Indexer Clustering > Indexer Clustering: Status

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Key Indexer Cluster Maintenance Commands

- Helpful CLI commands to run on the Manager Node

```
splunk help clustering

splunk rolling-restart cluster-peers
splunk [enable|disable|show] maintenance-mode
splunk set indexing-ready
splunk validate cluster-bundle
splunk show cluster-bundle-status
splunk apply cluster-bundle
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Indexer Clustering Health Report

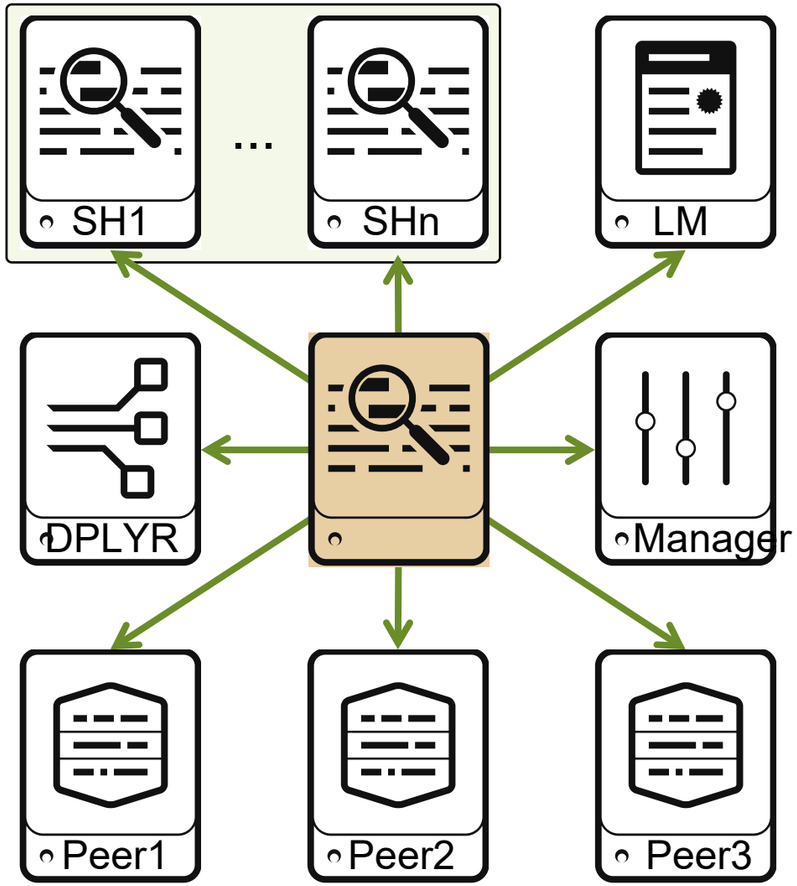
- Reports every 20 seconds by default
- **`feature:cluster_bundles`** reflects whether there are validation errors in the last bundle that were pushed to cluster peers (yellow only)
- **`feature:data_durability`** reflects whether or not:
  - The configured replication factor is met (red only)
  - The configured search factor is met (red only)
- **`feature:data_searchable`** turns red if one or more buckets lack a primary
- **`feature:indexers`** tracks whether any peer nodes are in detention mode
  - Yellow if in manual detention
  - Red if in automatic detention
- **`feature:missing_peers`** tracks any peer nodes that are in transition
  - Yellow if nodes are stopping, stopped, decommissioning, pending or restarting
  - Red if nodes are down
- **`feature:indexing_ready`** stays green when the cluster is functional

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Monitoring Clusters with Monitoring Console

- Enable Monitoring Console (MC) on the system that has the best vantage point of the distributed deployment
  - MC is the search head of all search heads
- Enable only one MC instance in the entire deployment
  - A dedicated search head that only administrators can access within the indexer cluster
  - Deployer or dedicated license manager
  - Manager node
  - DO NOT enable on a search head cluster member or on a peer node



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Monitoring Console Setup Prerequisites

- Users require **`admin_all_objects`** capability to configure the MC
- Each instance must use a unique **`servername`** and **`default-hostname`**
- Platform instrumentation is enabled for every instance (UF optional)
- Optionally on the cmanager: **`splunk edit cluster-config -cluster_label idxc1`**
- Forward all indexes (including internals and summaries) from search heads and
  the cmanager node to the indexing tier

outputs.conf

```
[indexAndForward]
index = false

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

[tcpout:default-autolb-group]
server=idx1:9997,idx2:9997,idx3:9997,idx4:9997
useACK = true
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Post MC Configuration Checklist

- Add all instances, except peer nodes, as search peers to the MC
- After enabling the MC to run in distributed mode, verify that all instances are discovered and the server roles are correct
  - Make sure only peer nodes (indexers) are marked as indexers
  - A search head that is also a license manager should have both roles marked
  - If the correct roles are not selected, click **Edit** and update
- Use custom groups to organize related components
  - The custom groups are used for view selection in the MC dashboards
- For any changes in the environment, return to **Setup**, check the server roles, and update if necessary

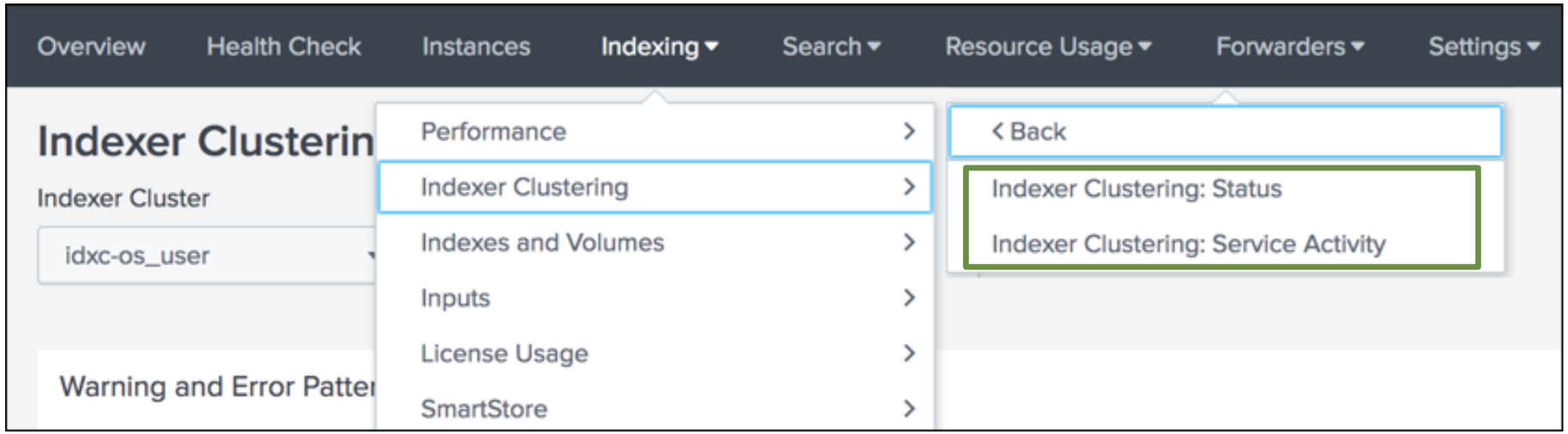
Note

To propagate the changes, always click **Apply Changes** on the MC Setup page.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Indexer Cluster Dashboards in MC



- Indexer Clustering: Status
  - Provides the same information as the manager's indexer clustering page
- Indexer Clustering: Service Activity
  - For an ideal healthy cluster, most of the panels should be blank
  - The trending down of fixup tasks and service jobs count is normal
  - Pay attention to an increasing trend on pending tasks and jobs

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Lab Exercise 4 – Monitor CM Service Activities

- **Time**: 25 - 30 minutes
- **Tasks**:
  - Stage an app and deploy it to the peer nodes
  - Disable indexing on **`cmanager`** and **`dserver`**
  - Enable the Monitoring Console to run in distributed mode on **`dserver`**
  - Monitor the indexer clustering service activities from Monitoring Console

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module 5: Forwarder Configuration

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Module Objectives

- Use indexer discovery to configure forwarders in a clustered environment
- Describe optional indexer discovery settings
  - Polling rate
  - Weighted load balancing
- Optimize indexing loads with volume-based load balancing

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Best Practices for Configuring Forwarders

- Forwarders are not required to be configured for clustering
- Enable load balancing and indexer acknowledgement in **`outputs.conf`**

```
[tcpout:indexers]
server = <peer_node_list>
useACK = true
```

outputs.conf

  - The receiving peer (origin) tracks the write state of indexing data when **`useACK`** is enabled
  - Acknowledges when indexing data is written to a bucket and sent to replicating peers
  - Any node or network failure causes a bucket to roll and triggers a fixup

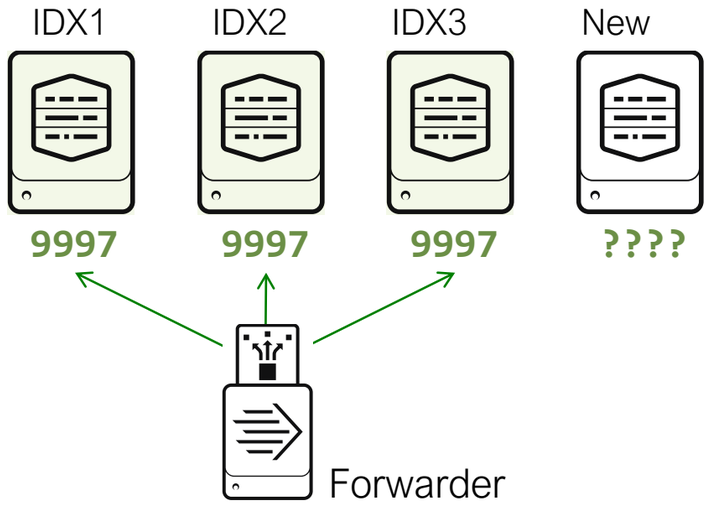
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Forwarder Management Challenges

- In a non-clustered environment, Splunk administrators must track target server changes and update the forwarder **`outputs.conf`** settings manually
  - A static list of indexers has to be deployed to each forwarder
  - Target indexer changes require restarting the forwarders

```
[tcpout:indexers]
server = IDX1:9997,IDX2:9997,IDX3:9997
useACK = true
```



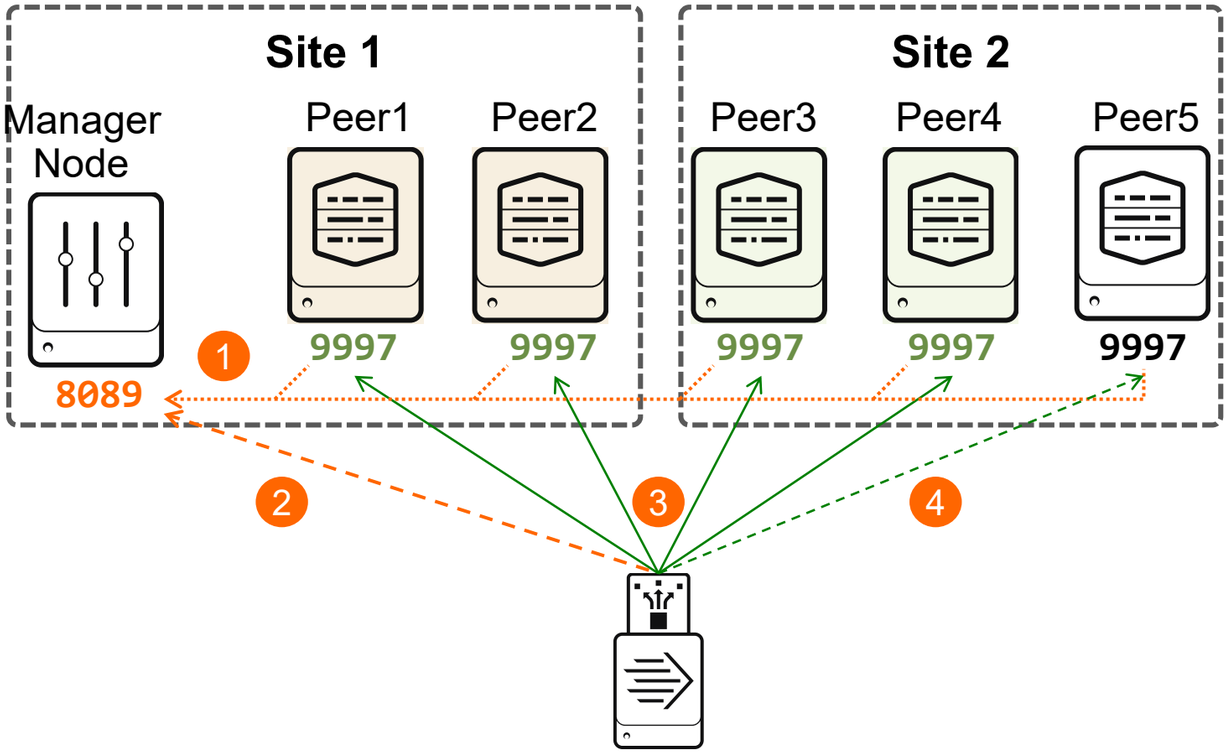
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Using Indexer Discovery

- Designed for dynamic environments where capacity is added and removed on demand
  - Minimizes the forwarder restarts
  - Scales well and easier to manage
  - Reduces the load on DNS servers
  - Can use weighted load balancing
  - Can be site-aware

1. Peers report their receiving ports to manager node
2. Forwarders poll manager node to get the latest list of peer nodes
3. Forwarders send data to the peers in the list
4. A peer can be added or removed without affecting the forwarder configurations



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Configuring Indexer Discovery – Manager Node

- No changes to the peer nodes to receive data from forwarders

```
splunk enable listen 9997
```

- No CLI support for enabling indexer discovery
- Enable indexer discovery on the manager node

```
[indexer_discovery]
pass4SymmKey = AnotherSecret
```

Manager node server.conf

  - The **pass4SymmKey** specifies the security key used to communicate between the master node and the forwarders
    - Must use the same value on all forwarders and the manager node
  - The **pass4SymmKey** here is NOT the same cluster secret
    - For better security, use a different value than the one used between the manager node and the peer nodes

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Configuring Indexer Discovery – Forwarders

Each forwarder's outputs.conf

```
[tcpout:idxc-forwarders]
indexerDiscovery = cluster1
useACK=true

[indexer_discovery:cluster1]
master_uri = https://<master>:8089
pass4SymmKey = AnotherSecret
```

- If both manual and indexer discovery attributes are set, indexer discovery takes precedence
  - Forwarders poll the manager at set intervals to receive the most recent list of peers

- Indexer discovery by default is not site-aware (**`site = site0`**)
  - Forward to peers across all sites
- If you want a forwarder to be site-aware, assign a site-id

```
[general]
site = <site-id>
```

Each forwarder's server.conf

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Indexer Discovery Option – Polling Rate

- The manager determines a polling interval dynamically based on the number of connected forwarders and the **`polling_rate`**
  - poll_interval (seconds) = #_of_forwarders / **`polling_rate + 30`**
  - **`polling_rate`** is a fixed factor that the manager uses to calculate the polling interval
    - Set a factor between 1 and 10 (the default is 10)

# of forwarders	polling_rate	polling_int_sec	polling_interval
100	1	100/1+30=**130**	2 min. 10 sec.
100	10	100/10+30= **40**	40 sec.
1,000	10	1000/10+30=**130**	2 min. 10 sec.

Manager Node server.conf

```
[indexer_discovery]
pass4SymmKey = <string>
polling_rate = <1-10>
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Balancing Indexing Loads

- Evenly distributed index data greatly improves the search performance
- The default load balancing on the forwarder is based on time
  - Time-based forwarding alone cannot distribute data evenly across peers
- Other options:
  - Weighted load balancing
  - Volume-based data forwarding
  - Event breaker
    - Discussed in Splunk Enterprise Data Administration course

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Using Weighted Load Balancing

- With indexer discovery, the manager can adjust the server list based on the peers' relative storage capacities
  - More frequently selects peers with higher advertised capacity

`selection_ratio = peer_capacity / cluster_wide_capacity`

- Peers with more storage capacity, typically new peers, can become preferred search peers because a larger percentage of recent data will be indexed on these peers

Enable it on the manager's server.conf

```
[indexer_discovery]
indexerWeightByDiskCapacity = true
```

Specify the advertised capacity peer nodes (optional)

```
[clustering]
advertised_disk_capacity = <10~100%>
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Using Volume-based Data Forwarding

- Data rebalancing is NOT bucket age aware
  - Recent data can still concentrate on particular peers, while the overall buckets are evenly distributed
  - Therefore, it is preferred to balance the data coming from the forwarders
- With volume-based forwarding, a forwarder can distribute more evenly
  - Sends a predefined amount of data before switching to another peer
- To enable:
  - Set **`autoLBVolume=<size_in_bytes>`** in **`outputs.conf`**
    - Set the **`autoLBVolume`** size in multiples of 64KB (65536)
  - Set **`EVENT_BREAKER_ENABLE=true`** and its associated attributes in **`props.conf`**
- **`autoLBVolume`** and **`autoLBFrequency`** settings work in conjunction
  - Whichever threshold is met first, switch to the next peer node

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Forwarder Site Failover

- You can configure site-awareness for forwarders in a multisite cluster
  - What happens to forwarding in case of a site failure?
- Solution: enable the forwarder site failover
  - Forwarders must use indexer discovery
  - Send data to a secondary site when all nodes on the primary site are down
  - When a node from the primary site is back online, forwarding resumes to the primary site
- To configure, run from the manager node:

```
splunk edit cluster-config -forwarder_site_failover <primary>:<failover>
```

```
[clustering]
mode = master
multisite = true
available_sites = site1,site2, site3
forwarder_site_failover = site1:site3,site2:site3
...
[indexer_discovery]
pass4SymmKey = whatever
```

Manager node's server.conf

```
[general]
site = site1
```

Each forwarder's server.conf

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Indexer Discovery Log Channels

- Search the manager node's indexer discovery log channel for any errors:

```
index=_internal component=CMIndexerDiscovery
```

- Search the forwarder's **splunkd.log** for any indexer discovery events:

```
index=_internal component IN(IndexerDiscoveryHeartbeatThread,
HttpPubSubConnection, TcpOutputProc)
```

- Search the forwarder's **`metrics.log`** for data distribution and failover:

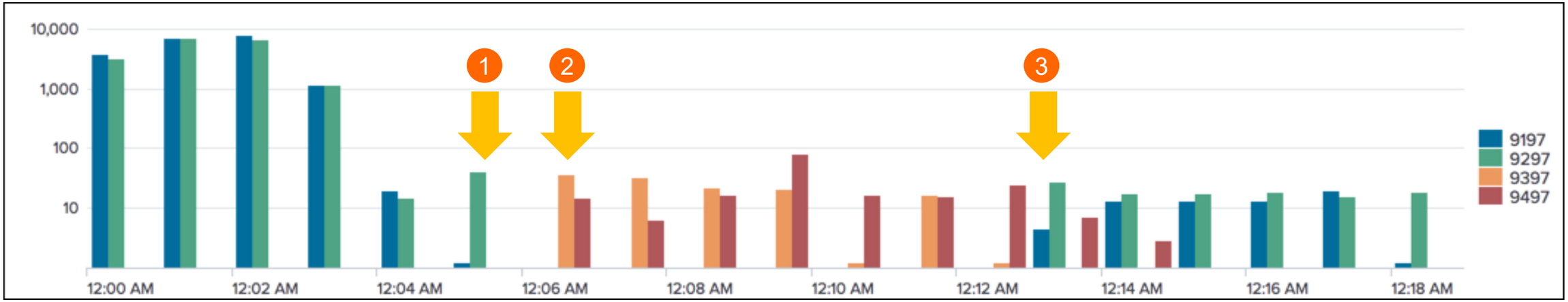
```
index=_internal host=uf component=Metrics
group=tcpout_connections
| timechart span=1h sum(kb) by destIp
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Example: Indexer Discovery Site Failover

```
index=_internal host=uf Metrics group=tcpout_connections | timechart span=1h sum(kb) by destPort
```



1. A volume-based forwarding UF was sending to site1 (9197 & 9297) until this point
2. Detected targets in site1 are no longer available and switched to the failover site (9397 & 9497)
3. The original site has recovered and the forwarding targets gradually transitioned back to the site1 peers

Note

In this example (your lab environment), the search uses **`destPort`**, instead of **`destIp`**.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

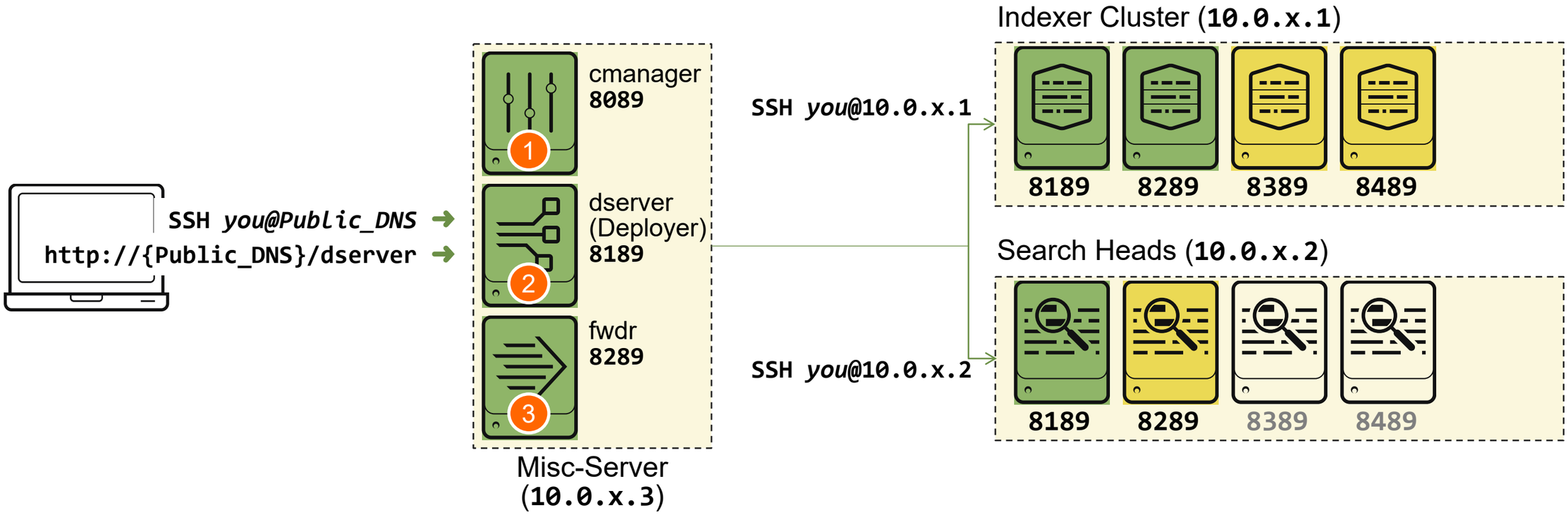
Lab Exercise 5 – Configure a Forwarder

- **Time:** 30 - 35 minutes
- **Tasks:**
  - On the manager node, enable the indexer discovery option with forwarder site failover
  - Configure the deployment server
  - Enable the deployment client setting on the forwarder
  - Update the instance server role in Monitoring Console
  - Verify the forwarder app deployment
  - Test the forwarder site failover scenario

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Lab Exercise 5 – Configure a Forwarder (cont.)

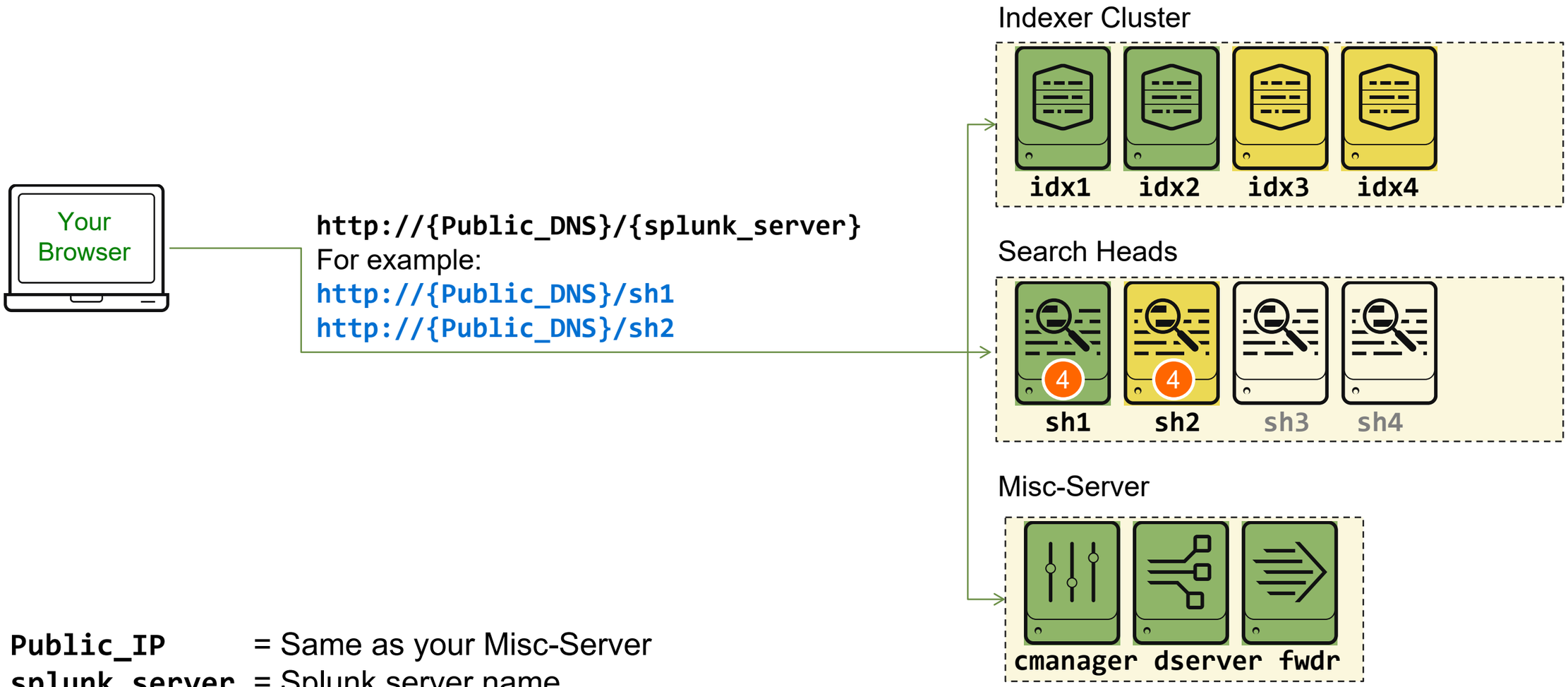


x = Your student ID
8?89 = splunkd-port

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Lab Exercise 5 – Configure a Forwarder (cont.)



Public_IP = Same as your Misc-Server
splunk_server = Splunk server name

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module 6:
Search Head Cluster

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module Objectives

- Describe search head cluster architecture
- Configure a search head cluster
- Identify the captain and monitor cluster status
- Describe optional configuration settings

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Search Head Challenges

- Individual search heads are single points of failure
- Maintaining consistent configurations across multiple search heads
- Increasing concurrent users and searches
- Managing large numbers of scheduled searches and alerts

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Addressing Search Scaling

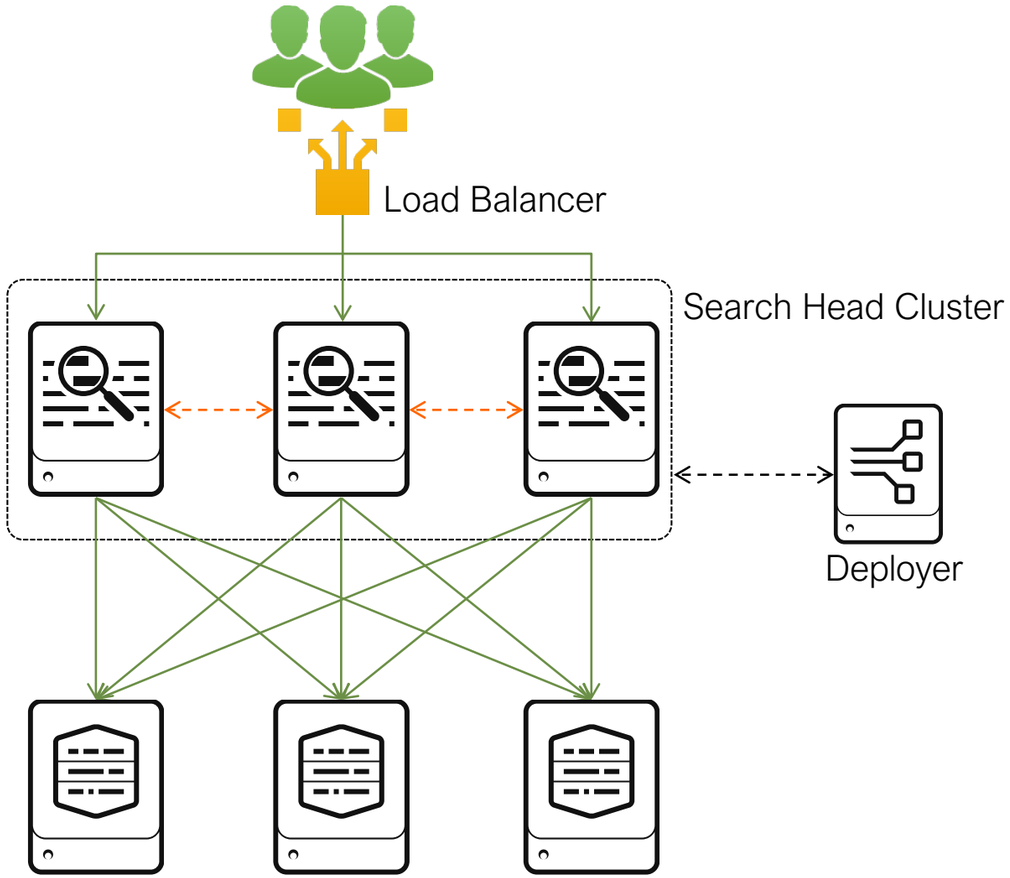
- As the number of simultaneous searches increases, you have several actions to mitigate performance issues
- **Best practices:**
  - Increase the number of search peers (indexers)
  - Optimize scheduled searches to run on non-overlapping time slots
  - Isolate scheduled searches, real-time searches, and ad-hoc searches
  - Limit the time range of end-user searches
  - Add more search heads
  - Configure user roles to limit the number of concurrent real-time searches
  - Implement search head clustering

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Benefits of Search Head Clusters

- Horizontal scaling
  - Members are interchangeable
    - Add more SHC members any time
  - Commodity hardware
  - Seamless user experience
    - Easy to on-board users and apps
- Search high availability
  - Search job failure aware and reschedule
  - Reliable alerts
- No single point of failure
  - Dynamic captaincy
- Dedicated configuration bundle management

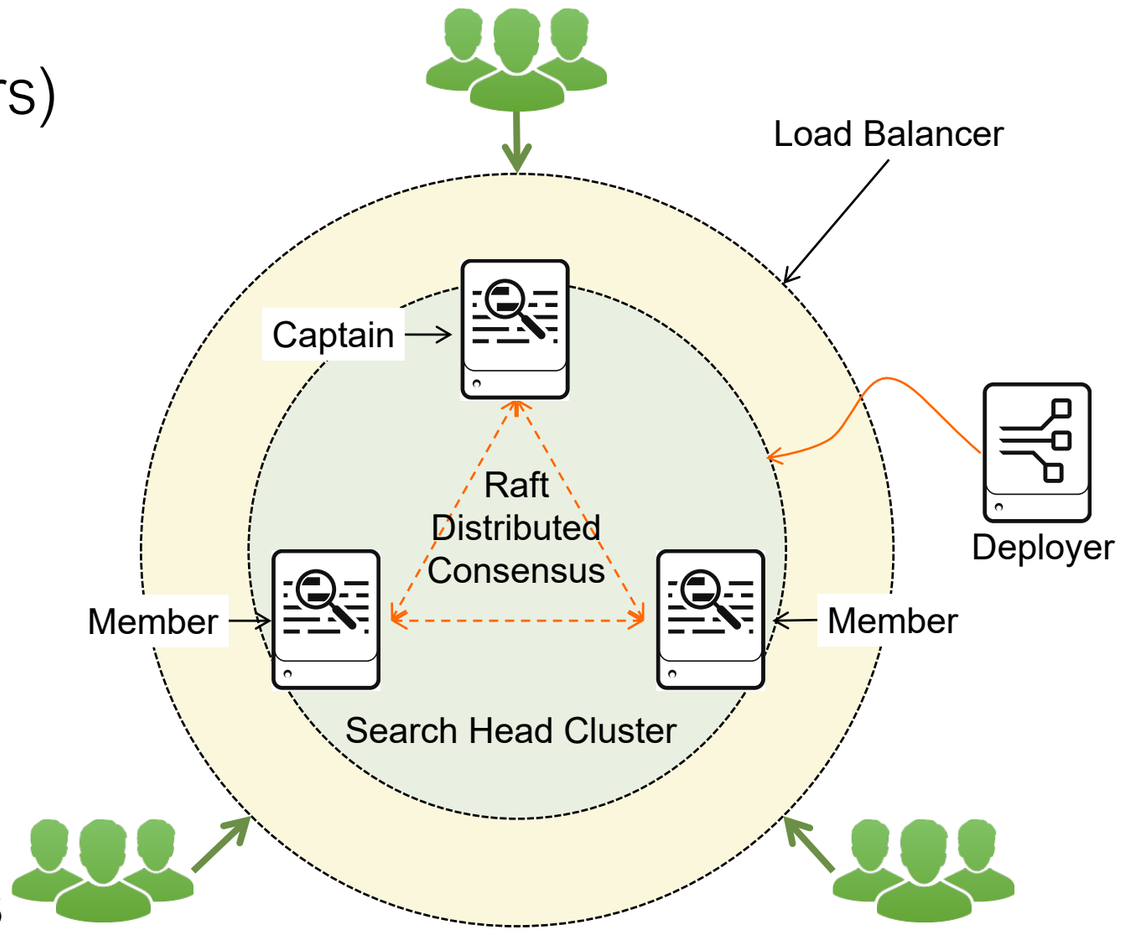


Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Search Head Cluster Terminology

- Raft distributed consensus
  - Captain/Member (instead of manager/peers)
- Replication factor
  - Applies only to search artifacts
- Deployer
  - NOT the same as the deployment server
- How does it work?
  - Members of search head cluster elect the captain dynamically
  - Replicates configuration changes to all cluster members
  - Captain schedules and manages searches



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

How Does SH Cluster Scale Search Capacity?

- Load-based scheduling heuristic
  - Captain is the only job scheduler
    - Captain establishes authority and is also a member
    - The normal scheduler on all members is suppressed
    - Captain schedules and delegates jobs to its members
  - Captain maintains global knowledge of all search jobs
    - Members regularly report their job loads to the captain
    - Ad-hoc and real-time search results (artifacts) are not replicated
    - Saved and scheduled search artifacts are replicated per search head cluster replication factor
  - Captain directs which member to contact to access search results

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Report Scheduler

- Without SHC, a search head can defer and skip search jobs if:
  - Search head restarts (could cause a gap in summary index)
  - Search head encounters resource constraints (max. concurrent search limit)
    - A user performing prolific, ad-hoc searches can overwhelm other searches
    - Infrequent long-running searches can starve out frequent short-running searches
    - A deferred job is implicitly retried (repeated for the duration of its window)
- With SHC, the captain mitigates starvation and recovers missed jobs
  - Implements a heuristic approach based on job load, priority scoring, search history introspection, and schedule window

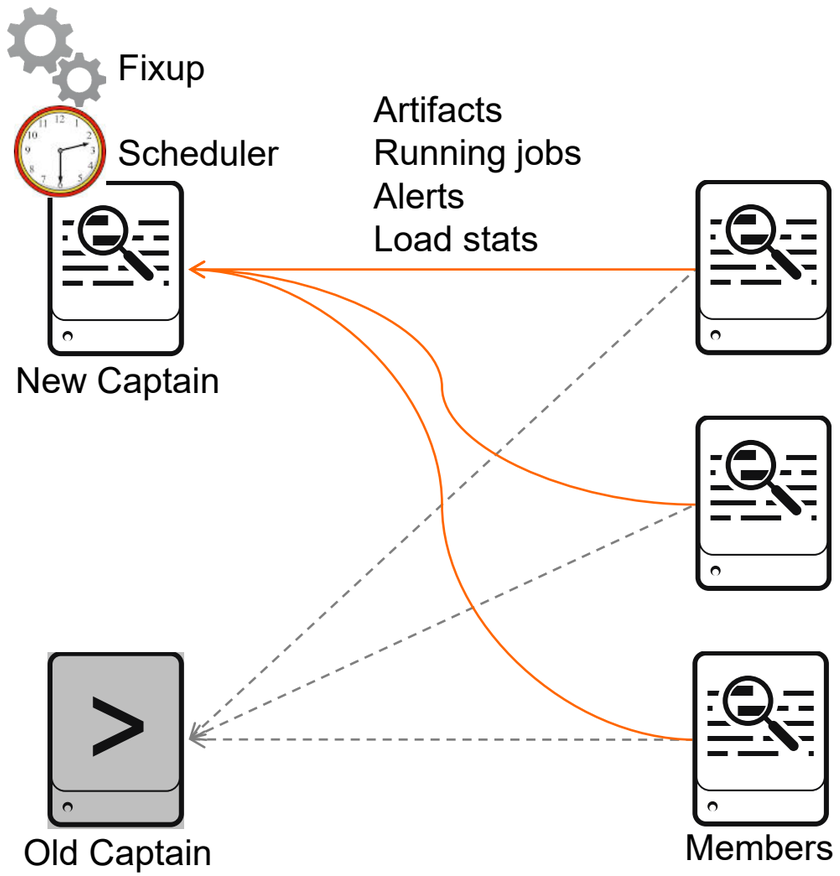
http://docs.splunk.com/Documentation/Splunk/latest/Report/Configurethepriorityofscheduledreports

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

How Does Cluster Provide Always-On Services?

- Auto SH captain failover
  - Elect new captain via Raft
  - Persists its records in **`var/run/splunk/_raft/<server>/log`**
  - Members register their list of artifacts, running jobs, alerts, and search load statistics to a new captain
  - New captain enables its scheduler
  - New captain executes fixups if needed



Note

Use DNS names when initializing members.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Search Head Cluster Key Considerations

- Always use new Splunk instances
  - Must have at least three members
  - You cannot upgrade from an existing SH or a member of SH Pool
    - Migrate the configurations after the SH Cluster is up
- Same hardware requirements as the dedicated search head
  - Use identical specifications for all members (bare metal or VM)
    - Works on all operating systems supported for Splunk Enterprise
    - Same version of Splunk Enterprise
- Synchronize the system clock on all members including the indexing layer

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Sharing Splunk Server Roles

BEST PRACTICE:

- Disable local indexing and forward everything, including all internal indexes, to the peer nodes (discussed later)
- A search head cluster member should not have any other server roles

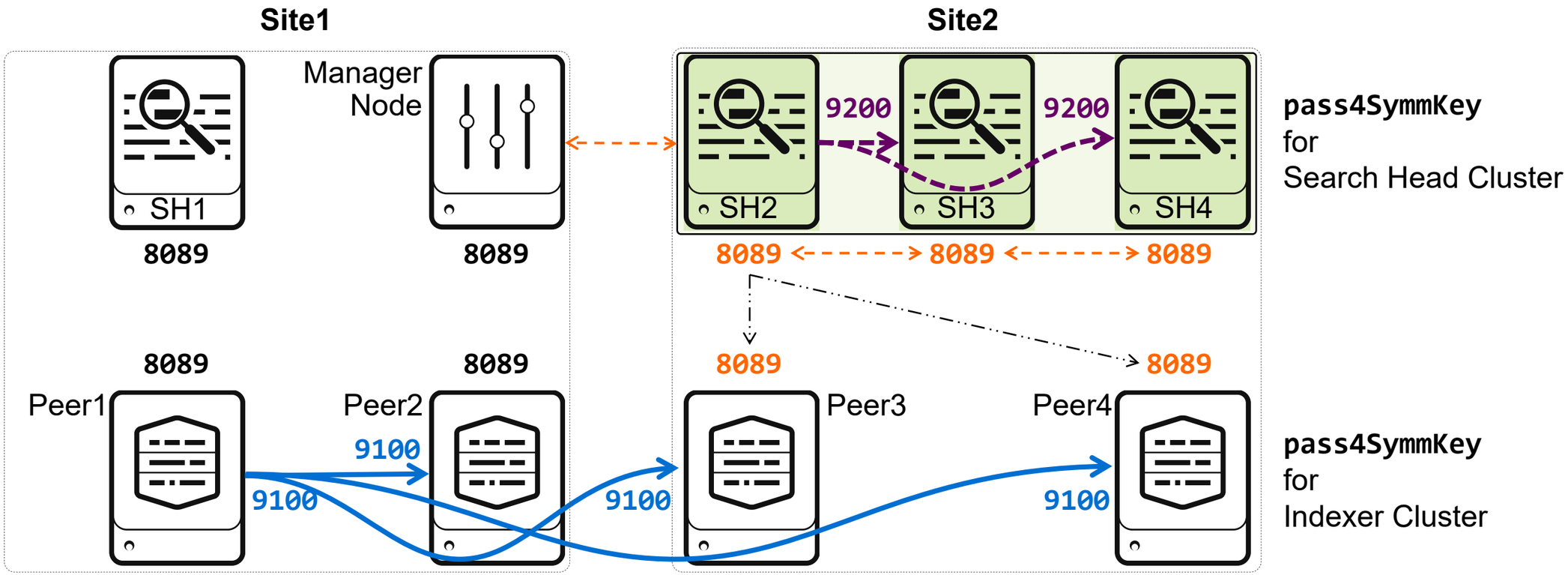
WARNING:

- A member cannot be a search peer to another search head
  - Exception: when it is configured to be a monitored instance of Monitoring Console running on other instance

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Search Head Cluster Ports



Management (splunkd port)

Replication (index replication port)

Replication (search artifact replication port)

Search request/results (distributed search)

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Deploy a Search Head Cluster

1. Install Splunk Enterprise and set admin password
   - Recommend LDAP/SAML
2. Bring up and initialize all SH cluster members:

```
splunk init shcluster-config -mgmt_uri https://SH2:8089
-replication_port 9200 –secret shcluster
```

3. Assign one of the members as the captain and set a member list:

```
splunk bootstrap shcluster-captain –servers_list
https://SH2:8089,https://SH3:8089,https://SH4:8089
```

4. Check search head cluster status:

```
splunk show shcluster-status
splunk list shcluster-members
```

Note

Search head cluster configuration is in **`SPLUNK_HOME/etc/system/local/server.conf`**.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Connecting a SHC to Non-Clustered Indexers

- You have two ways to search non-clustered indexers
  - Individually add the search peers from each SHC member, or
  - Enable search peer replication
    - Add the search peers to one SHC member and let the SHC replicate the peer configurations to all SHC members
    - All SHC members gain access to the same set of search peers

```
[raft_statemachine]
disabled = false
replicate_search_peers = true
```

server.conf of each SHC member

  - Once enabled, you can add new peers with CLI, Web, or REST API

```
splunk add search-server https://<peer>:8089 -remoteUsername <user> -remotePassword <pw>
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Connecting a SHC to Indexer Clusters

- SHC members do not have site awareness
  - No site-by-site artifact replications
  - Using **`site0`** can provide a seamless search experience
- Configure each SHC member as a search head on an indexer cluster
  - The search head members get their list of search peers from the manager node of the indexer cluster
  - Connecting to a single-site indexer cluster:

```
splunk edit cluster-config -mode searchhead -master_uri https://10.0.1.3:8089
-secret idxcluster
```

  - Connecting to a multisite indexer cluster:

```
splunk edit cluster-config -mode searchhead -master_uri https://10.0.1.3:8089 -site site2
-secret idxcluster
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Search Head Cluster Member server.conf

License manager password

Indexer cluster site association

If connected to an indexer cluster

Indexer cluster password

Search head cluster artifact replication port

Member's self identifying address to the SHCluster

Search head cluster password

Generated search head cluster ID

```
[general]
pass4SymmKey = $1$ttbJh5nUk5AM
serverName = sh2
site = site2

[clustering]
master_uri = https://10.0.1.3:8089
mode = searchhead
multisite = true
pass4SymmKey = $7$w7W0kx7n6jztOoNsisPQwfB+

[replication_port://9200]

[shclustering]
disabled = 0
mgmt_uri = https://sh2:8089
pass4SymmKey = $7$yoi+Ts+MTFDA+IlKbDczLeEY
id = 571B9C60-66EA-4B9F-8562-27B62E93E31F
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Checking SH Cluster Status

> **splunk show shcluster-status**

```
Captain:
  dynamic_captain : 1
  elected_captain : Mon Mar 11 21:33:16 2019
               id : 75DBEA2A-0204-4C15-983C-116F1
 initialized_flag : 1
            label : sh2
         mgmt_uri : https://10.0.1.2:8289

min_peers_joined_flag : 1
 rolling_restart_flag : 0
   service_ready_flag : 1

Members:
         sh4    label : sh4
last_conf_replication : Mon Mar 11 21:54:39 2019
             mgmt_uri : https://10.0.1.2:8489
       mgmt_uri_alias : https://10.0.1.2:8489
               status : Up
```

```
     sh2        label : sh2
last_conf_replication : Mon Mar 11 21:54:40 2019
             mgmt_uri : https://10.0.1.2:8289
       mgmt_uri_alias : https://10.0.1.2:8289
               status : Up

     sh3        label : sh3
last_conf_replication : Pending
             mgmt_uri : https://10.0.1.2:8389
       mgmt_uri_alias : https://10.0.1.2:8389
               status : Up
```

Note

A raft metadata corruption can cause the captain election to fail. To confirm, look for **`ERROR SHCRaftConsensus`** in **`splunkd.log`**.

> **splunk clean raft**

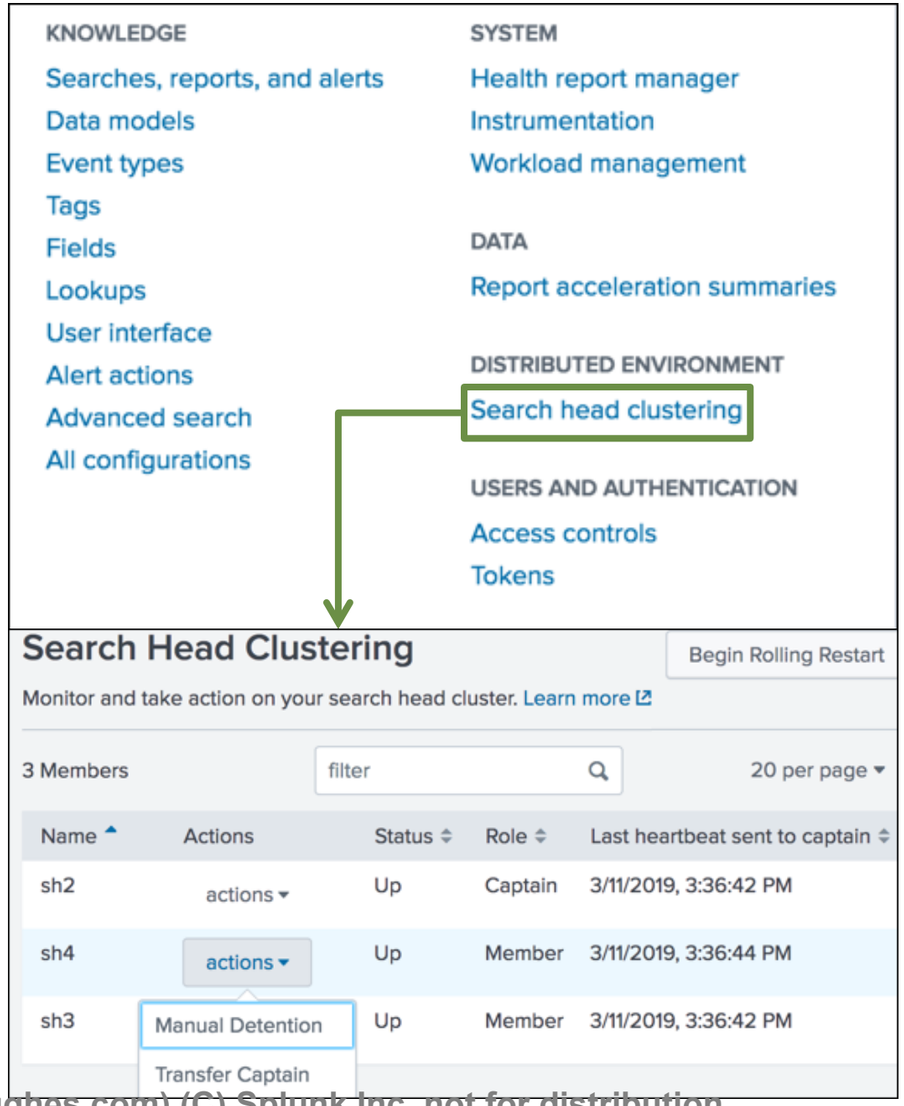
- When SHC can't elect a captain, run on all members before bootstrap
- When SHC has an active captain but a member can't join, run on the failing members

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Splunk Web Settings Menu Changes

- When search heads become members of a search head cluster, the **Settings** menu in Splunk Web changes
  - Hides all non-replicable options
    - You can unhide them, if necessary
  - Enables the search head clustering UI on all SHC members
    - Able to perform rolling restart, manual detention and captaincy transfer
  - If you need to make changes to the settings that are hidden, use the **deployer** to push the underlying changes



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Configuration and Artifact Replication

- Captain orchestrates both configuration and artifact replication
- Knowledge object configurations (replicated to all members):
  - Changes made via Splunk Web, CLI, or API are replicated
  - Direct **`.conf`** file edits must be implemented using the deployer
  - More details are discussed in the next module
- Artifacts (based on the search head cluster replication factor):
  - Only the artifacts resulting from scheduled reports are replicated
  - Real-time and ad-hoc search artifacts are not replicated, instead they are proxied (discussed later)
  - Captain enforces artifact fixups according to its replication policy

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

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Roles and User Account Replication

- Use any of the available authentication methods
  - Splunk native authentication
    - Automatically replicates the underlying **`.conf`** files and **`SPLUNK_HOME/etc/passwd`**
  - SAML authentication
    - Only replicates **`authentication.conf`**
    - Must use the deployer to push the certificates
  - Scripted authentication
    - Must use the deployer to push both the script and **`authentication.conf`**
- User configurations are automatically synchronized across all members

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Ad-hoc Search Management

- Ad-hoc search results are not replicated
  - Artifact proxying is used to access the ad-hoc search results from any member
  - If the search is accessed from a different member, artifact proxying calls the owner member to get the results
- To reduce captain's work load, disable running scheduled searches on the captain
  `captain_is_adhoc_searchhead = true` (on all members)
- To configure a member to run only ad-hoc searches, set
  `adhoc_searchhead = true`

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Alerts

- When results of search meet alerting criteria:
  - The alerts are checked and fired locally on the member that ran the search job
  - The local alert information is reported to the captain
- Captain merges and maintains global view of alerts
  - Centralizes suppression information
    - Remember, captain is the only scheduler and it delegates jobs
  - Merged alerts and suppression information are sent to all members

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Handling Summarization

- The captain coordinates the report and data model acceleration searches
  - The resulting summaries are stored on indexers
- The summary indexes are stored only on the search head that generates them
  - If you want to share them with other members, forward your summary indexes to the indexing layer

BEST PRACTICE:

- To consolidate index data, forward all indexes (including summary and internal indexes) to the indexing layer

```
[indexAndForward]
index = false

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

[tcpout:default-autolb-group]
server=idx1:9997,idx2:9997,idx3:9997,
idx4:9997
useACK = true
```

outputs.conf

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

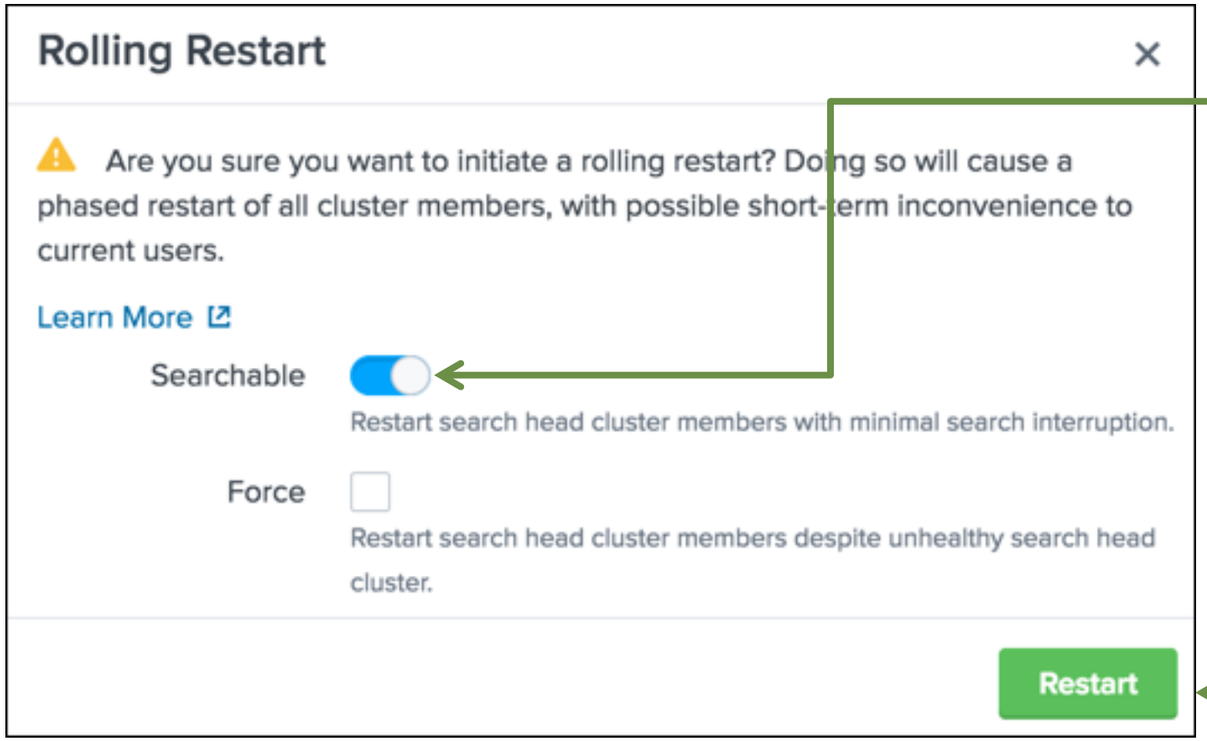
Artifact Reaping

- Reaping (deletion of search results) happens when artifact TTL expires
- Original member reaps its search artifacts and notifies captain
- Captain orchestrates reaping of the replicas
- If the original member is out of commission, captain waits beyond TTL and replicas are reaped thereafter

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Restarting a Search Head Cluster



Puts each SHC member in manual detention to complete in-progress searches before restarting SHC members

```
> splunk rolling-restart shcluster-members

> splunk rolling-restart shcluster-members
  -searchable true
  -decommission_wait_time 180
  -force false

> splunk rolling-restart shcluster-members -status 1
```

- Members restart in phases so the cluster can continue to operate
- The captain is the final member to restart and automatically invokes captaincy transfer, thus preventing captaincy from changing during the restart process
- Deployer automatically initiates a rolling restart, when necessary

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

SHC Manual Detention

- Enable manual detention to:
  - Perform maintenance operations
  - Run diagnostics on a member
  - Do a searchable rolling restart or rolling upgrade
- Gracefully remove a SHC member from services (detention state) with minimal impact on end-user search experience
  - Completes in-progress searches
  - New searches get directed to remaining members
  - Continues to participate in election and conf/bundle replication
  - Does not participate in artifact replication
- How to use:
  - **`splunk edit shcluster-config -manual_detention [on|off]`**
  - **`splunk show shcluster-status`**
  - **`splunk list shcluster-member-info`**

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Search Head Cluster Log Channels

- Heartbeat and election
  - splunkd_access.log: **`uri_path="/services/shcluster/member/consensus*"`**
  - Corresponding events in **`sourcetype=splunkd`**
    - **`component=SHCRaftConsensus OR component=SHClusterMgr`**
    - **`component=Metrics group=captainstability upgrades_to_captain=1`**
- Job scheduling
  - scheduler.log: **`sourcetype=scheduler component=SavedSplunker status=*`**
  - Corresponding events in **`sourcetype=splunkd`**
    - **`component=SHCMaster delegate`**
    - **`component=Metrics group=search_concurrency`**
- Artifact proxy and reaping
  - **`sourcetype=splunkd_access uri_path="/services/search/jobs*"`**
    - **`status!=20*`** indicates an issue
    - **`method=GET isProxyRequest=true`** indicates a proxied request
  - **`sourcetype=splunkd_access uri_path="/services/shcluster/captain/artifacts*"`**

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Useful SHC Debugging Searches

- Election history:
  - `index=_internal host IN (sh2, sh3, sh4) sourcetype=splunkd component=SHCRaftConsensus "All hail leader" | stats values(event_message) by _time host`
- Job scheduling status:
  - `index=_internal host IN (sh2, sh3, sh4) sourcetype=scheduler  status=* | eval status_host=status."-".host | timechart span=5m count by status_host limit=0 usenull=f`
- Skipping jobs:
  - `index=_internal host IN (sh2, sh3, sh4) sourcetype=scheduler status=continued OR status=skipped | eval status_host=status."-".host  | timechart span=5m count by status_host limit=0 usenull=f`
- Artifact proxy:
  - `index=_internal host IN (sh2, sh3, sh4) sourcetype=splunkd_access uri_path="/services/search/jobs*" isProxyRequest=true | stats count by method host file`

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Further Reading: Search Head Cluster

- Basic search head clustering concepts

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

- Migrating a search head pooling environment

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

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

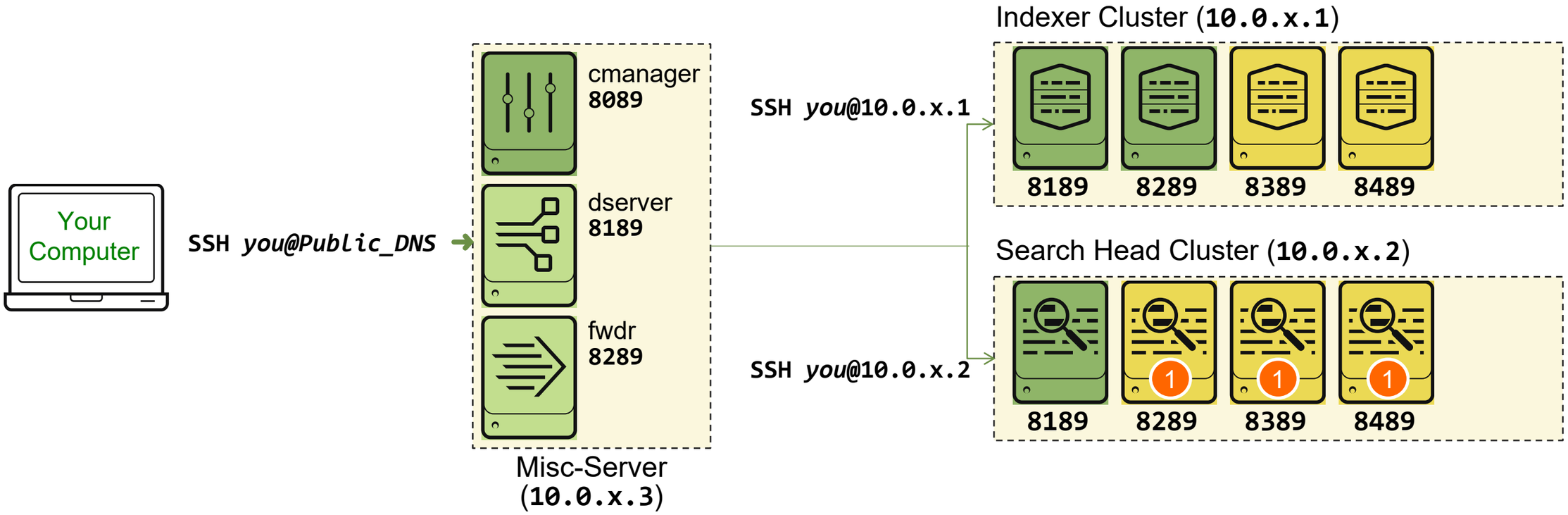
Lab Exercise 6 – Deploy a Search Head Cluster

- **Time:** 30 - 35 minutes
- **Tasks:**
  - Add two more search heads to **`site2`**
  - Enable a search head cluster with **`site2`** search heads
  - Verify that your search head cluster is functioning

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Lab Exercise 6 – Deploy a Search Head Cluster (cont.)

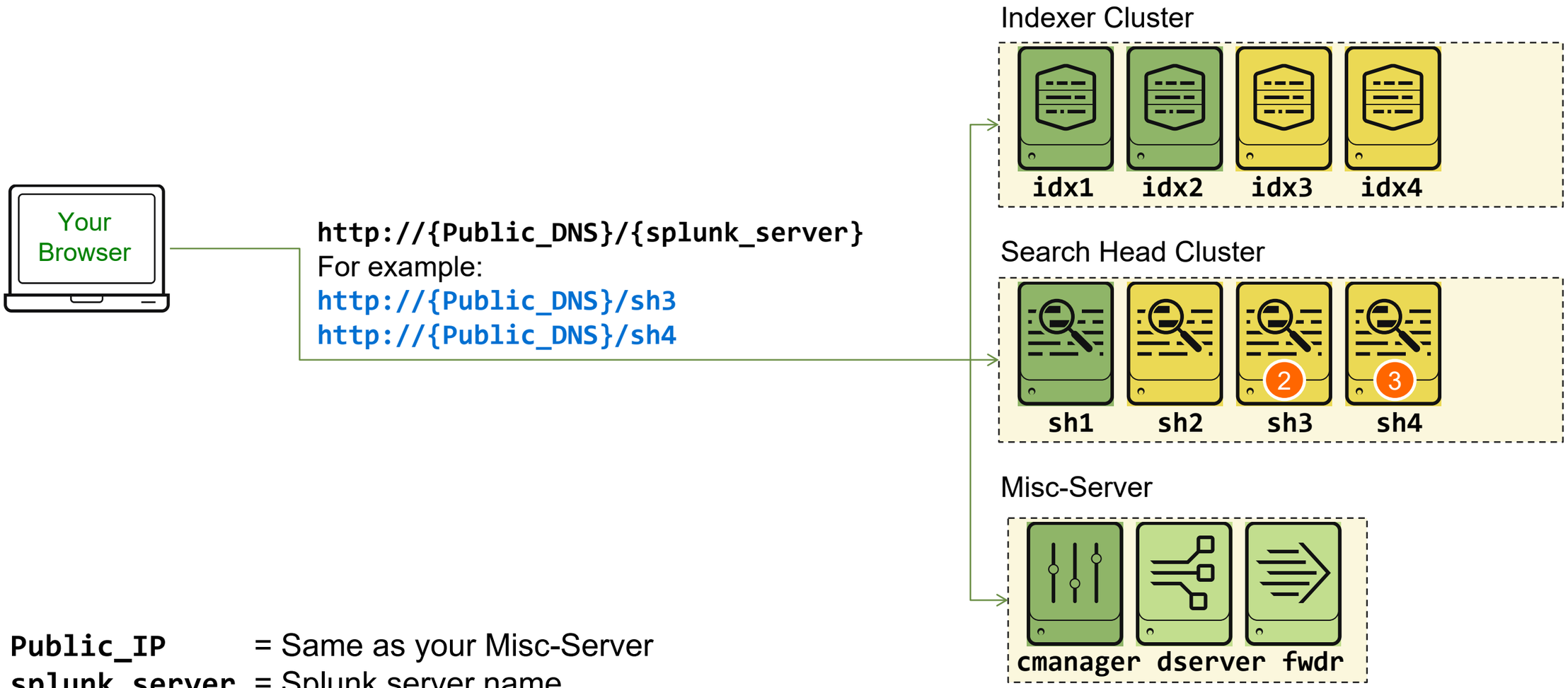


x = Your student ID
8?89 = splunkd-port

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Lab Exercise 6 – Deploy a Search Head Cluster (cont.)



Public_IP = Same as your Misc-Server
splunk_server = Splunk server name

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module 7: SHC Management and Administration

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module Objectives

- Deploy apps to a search head cluster
- Describe when and how to transfer captaincy
- Upgrade and manage search head cluster members
- Monitor SHC health with Monitoring Console

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Configuration Bundle Replication

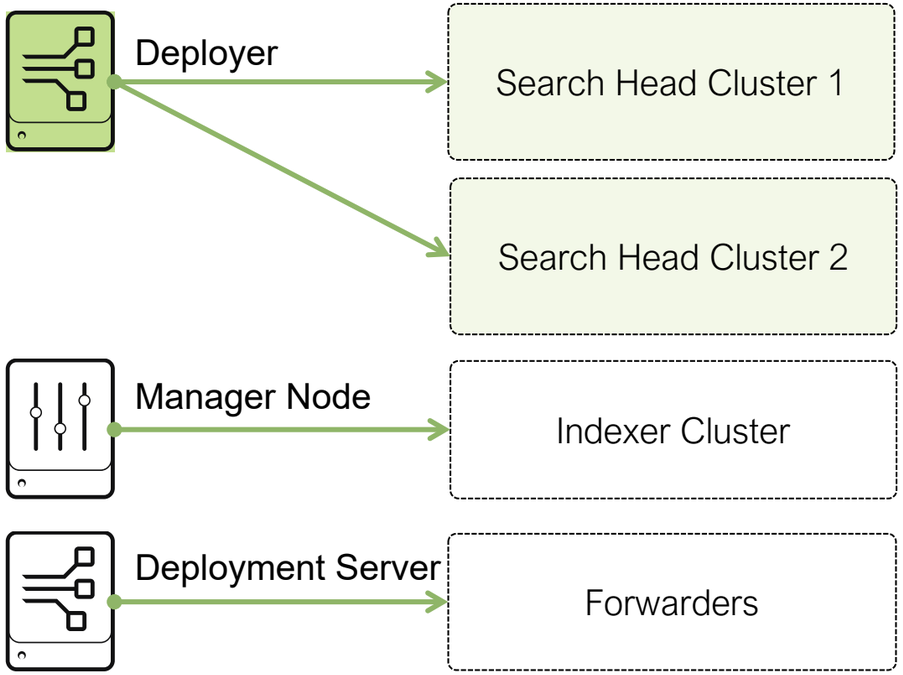
- All SHC members share the same configuration baseline
- Captain functions as a source control server
  - Members replicate changes from/to captain every 5 seconds (replication cycle)
  - Members generate a snapshot every minute and purge old sets every hour
    - **`var/run/splunk/snapshot/*.bundle`**
- All members SHOULD achieve *eventual consistency* at some point
  - In each replication cycle, members first pull (sync) outstanding changes from the captain, then push (submit) local changes to the captain
  - Members resolve conflicts on pull (sync)
  - All members keep a journal of changes in **`etc/system/replication/ops.json`**
    - Members check if the diverging point is at the end of captain's log
    - Pull all changes after the diverging point and then insert the changes

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Splunk Deployer

- Use the deployer to distribute apps and non-replicable files into a SHC
  - Does not represent a "single source of truth"
  - Cannot use it alone to restore members to the latest state
- Must run on a non-search head member
  - Can be enabled on an existing Splunk instance with other responsibilities
- No CLI configuration support
  - Associate the deployer with a SHC by setting the **`pass4SymmKey`** in **`server.conf`**
- Can share a deployer with multiple SHCs if:
  - The clusters have exactly the same apps and configurations and use the same ***`secret`***



Deployer server.conf

```
[shclustering]
pass4SymmKey = <secret>
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Deploying Bundles With Deployer

- Stage apps (configuration bundles) in the deployer's **`etc/shcluster`** folder
  - Optionally, configure the push modes of each app
- Deploying bundles from deployer works in two ways:
  - Push bundles out from deployer to all search head members

    ```
    splunk apply shcluster-bundle –target <member:port>
    ```

    - Can specify any member, but the deployer pushes the bundles to all members
  - Configure search head members to fetch and sync after a restart

    ```
    splunk edit shcluster-config -conf_deploy_fetch_url
    https://<deployer>:8089
    ```

    - Adds the deployer address to the existing search head members

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Deployer Push Modes

- The deployer deploys the app configuration to its members according to the push mode settings of each app
- The push mode can apply at the system level or on a per app basis
  - Configure the settings under the **`[shclustering]`** stanza in **app.conf**
    - **`deployer_push_mode`**
    - **`deployer_lookups_push_mode`**
- The push mode options do not apply to user bundles
  1. Each user bundle is first sent to the captain
  2. The captain commits it to the user's **`local`** directory
     - Treats the commits as member configuration changes
     - Only adopts the new stanzas and ignores the existing stanzas

WARNING

DO NOT change the push mode when a member is down. Doing so can cause members to be in out-of-sync state.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

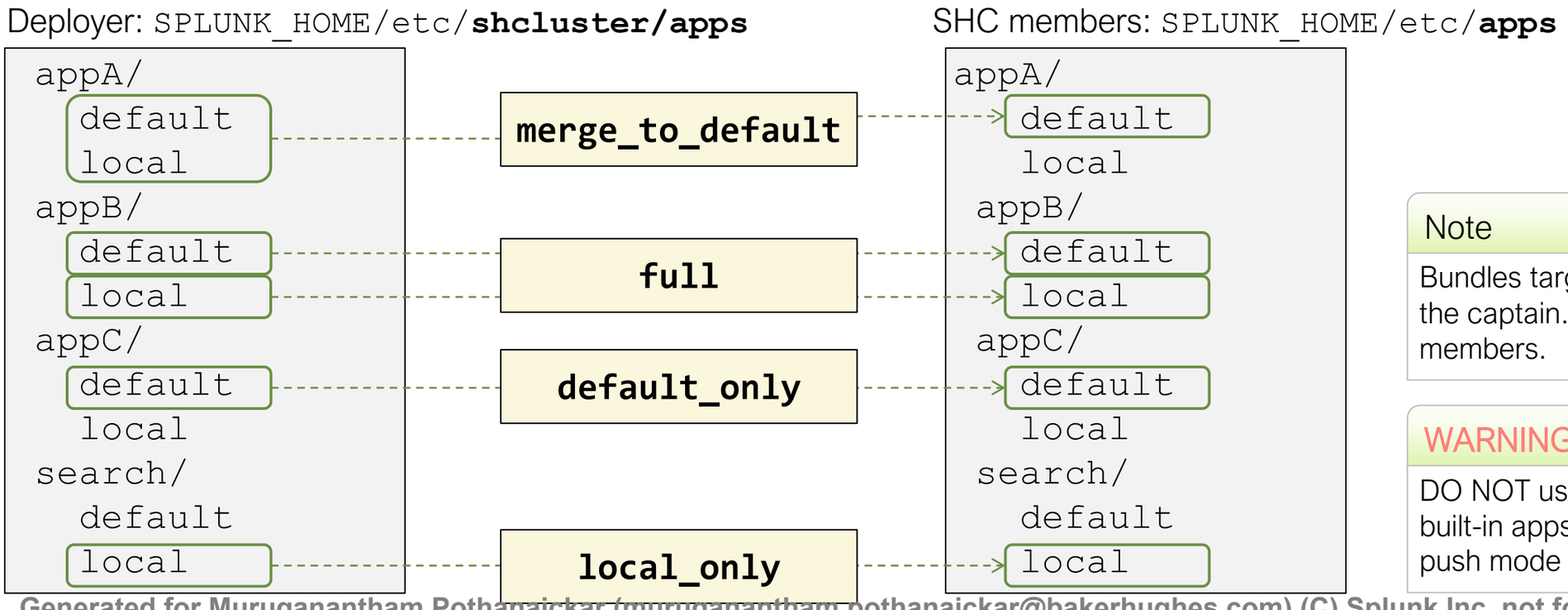
Deployer Push Mode Options

- Provides flexible ways to deploy apps from the deployer

  `deployer_push_mode = merge_to_default | full | default_only | local_only`

  – **`merge_to_default`** is the default if a mode is not specified

    - Is the only behavior for the versions prior to 7.3



Note

Bundles targeting **`local`** is sent to the captain. All others are sent to all members.

WARNING

DO NOT use the deployer to push built-in apps without first setting the push mode to **`local_only`**.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Deployer Lookup Push Mode Options

- Prior to 7.3, the populated lookup tables in SHC get overwritten from the latest bundle update from the deployer by default
  - To preserve the populated lookup tables, you execute:

    `splunk apply shcluster-bundle -target` *`member`* **`-preserve-lookups true`**
    - Can only preserve or overwrite all lookup tables
    - Even experienced admins can make a mistake
- The **`deployer_lookups_push_mode`** setting is introduced in 7.3
  - Provides more granular ways to preserve or overwrite lookups
  - Allows a way to persist the setting per app
  - **`deployer_lookups_push_mode = preserve_lookups`** (default)
    - Follows the **`-preserve-lookups`** flag of the command
  - **`deployer_lookups_push_mode = always_preserve`** | **`always_overwrite`**
    - Ignores the **`-preserve-lookups`** flag
    - Allows the **`deployer_lookups_push_mode`** of the app to decide

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

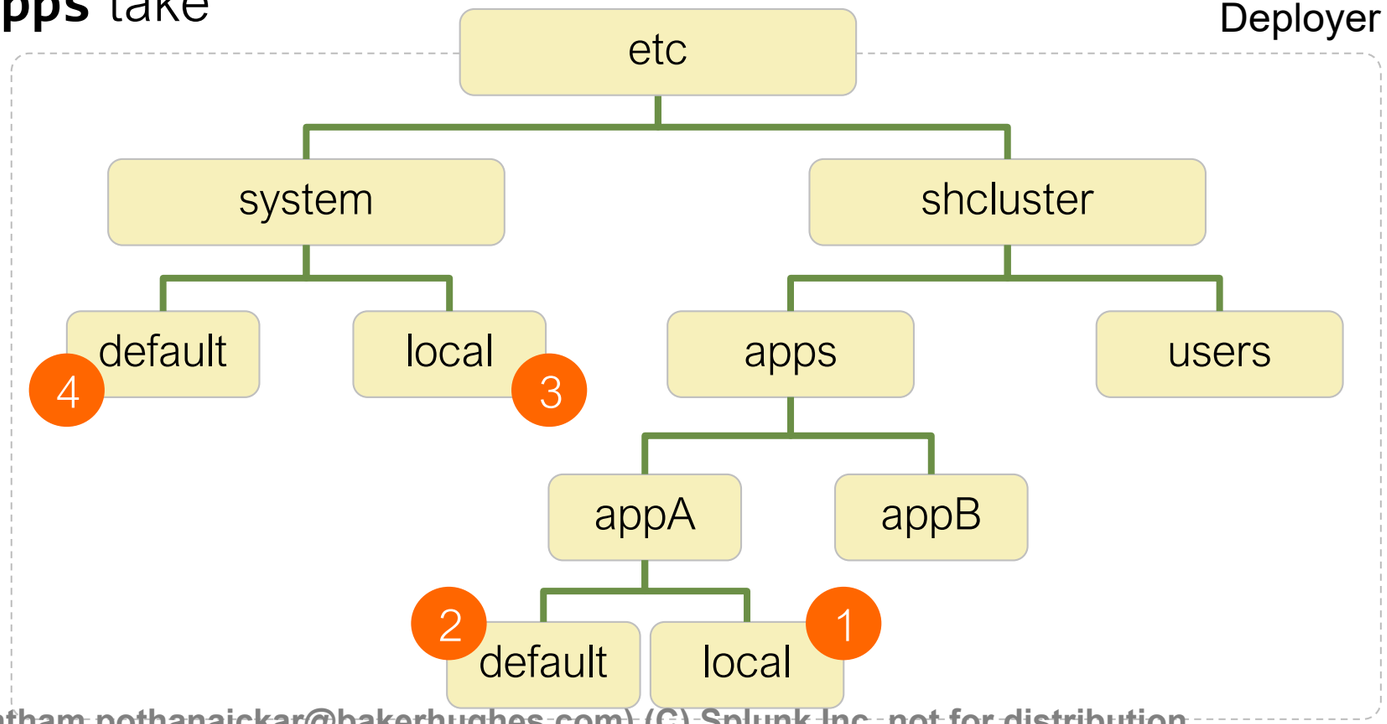
Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Deployer Push Mode Precedence

- The push mode can be set globally or locally for specific apps
  - If the push mode settings are not explicitly set under the specific app, the app follows the global deployer policy
  - The **`local`** takes precedence over any corresponding **`default`** settings
  - The settings under **`etc/shcluster/apps`** take precedence over **`etc/system`**

Note

The SHC members' existing configurations in **`local`** always take precedence over pushed configurations from a deployer.



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Controlling the Deployment Process

- By default, **`splunk apply shcluster-bundle`** automatically triggers a rolling-restart as necessary
- To control the rolling-restart, you can apply in phases

```
splunk apply shcluster-bundle -target <member:port> -action stage
splunk apply shcluster-bundle -target <member:port> -action send
splunk rolling-restart shcluster-members
```

CAUTION: Use the following process with extreme care

- To delete all the apps on SHC members previously distributed by the deployer, you can push an empty bundle
  - The app must be in **`state=enabled`** (check its app.conf)
  - The deployer cannot remove the app if it is in **`state=disabled`**

```
splunk apply shcluster-bundle -target <member:port> -force true
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Multithreaded SHC Deployer Bundle Push

- The **`deployerPushThreads`** allows you to concurrently send a large number of apps to a large number of SHC members
- Splunk checks the setting in the **`shclustering`** stanza of **`server.conf`** on the Deployer and launches the specified number of threads

  `auto` = deployer auto-tunes threads (one per member) depending on the number of members returned by the captain (preferred setting)

  `1` = default setting

  `<positive integer>` = sets thread number

```
[shclustering]
deployerPushThreads = auto
```

server.conf

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

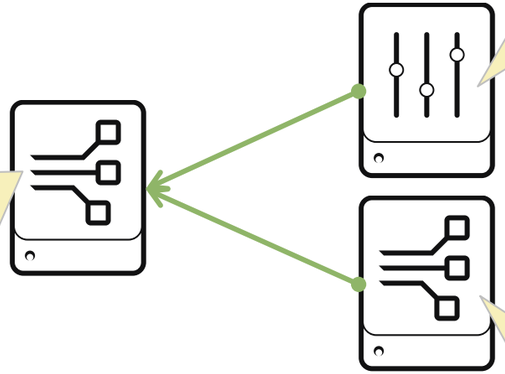
Working with Deployment Server

- You CANNOT use deployment server to directly distribute apps to the peer nodes or SHC members
- You can use it to distribute apps to the **master-apps** and **shcluster** directories

`serverclass.conf`
on **Deployment Server**

```
[serverClass:idxc_x]
stateOnClient = noop
restartSplunkd = false

[serverClass:shc_y]
stateOnClient = noop
restartSplunkd = false
```



`deploymentclient.conf` on **Manager Node**

```
[deployment-client]
serverRepositoryLocationPolicy = rejectAlways
repositoryLocation = SPLUNK_HOME/etc/master-apps
```

`deploymentclient.conf` on **Deployer**

```
[deployment-client]
serverRepositoryLocationPolicy = rejectAlways
repositoryLocation = SPLUNK_HOME/etc/shcluster/apps
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

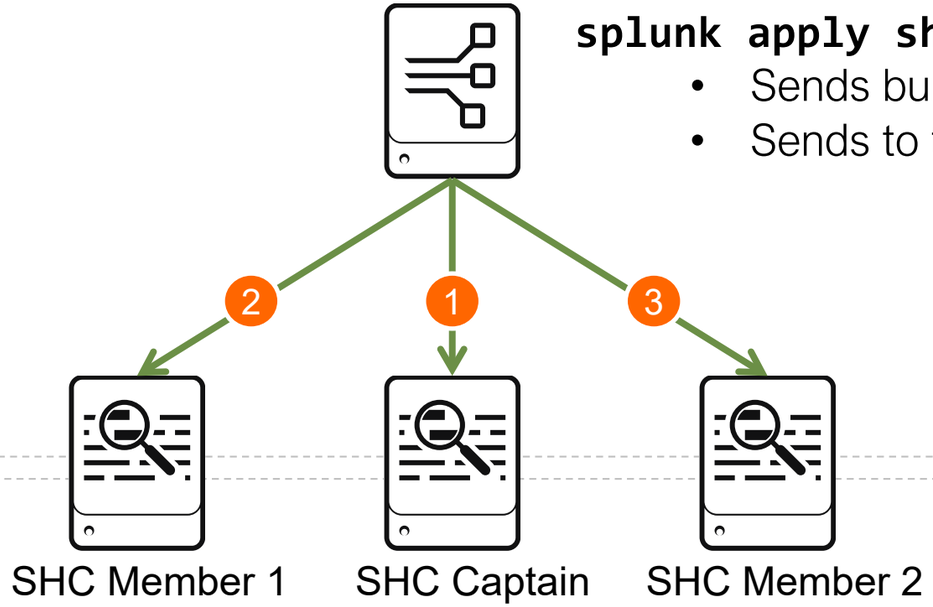
Bundle Deployment Summary

App bundle deployment

Deployer

`splunk apply shcluster-bundle`

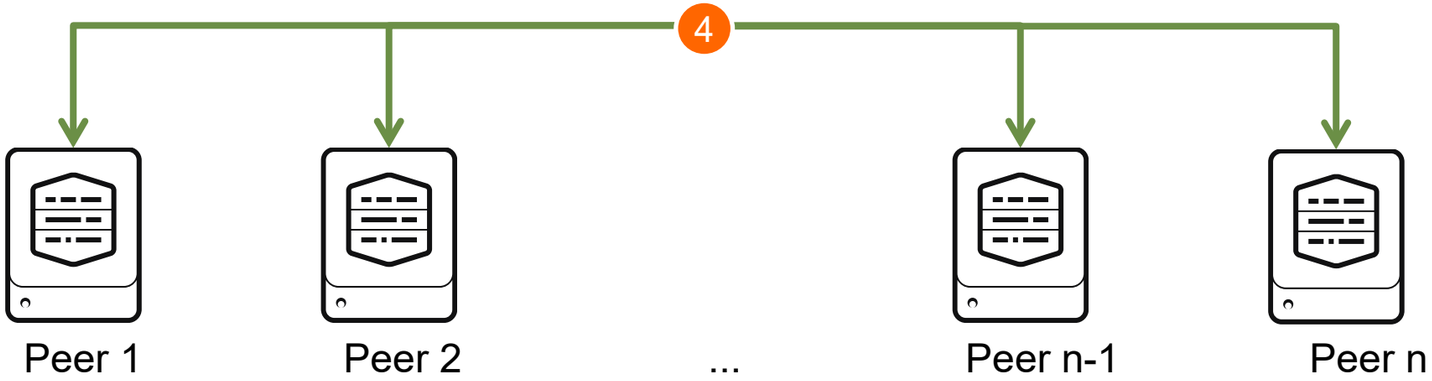
- Sends bundles as defined in **`server.conf`**
- Sends to the captain first



Search bundle deployment

Bundle replication to search peers happens only from the captain

- Sends bundles in parallel per bundle



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

SH Cluster Conf Replication Log Channels

- **`conf.log`** records recent configuration replication activity

  `index=_internal sourcetype=splunkd_conf |timechart list(data.task) by host`

  – Deployer-specific actions:
    - **`createDeployableApps`**: build bundles in **`var/run/splunk/deploy`**
    - **`populateDeployableInfo`**: read bundles from **`var/run/splunk/deploy`**
    - **`sendDeployableApps`**: push baseline apps to a search head cluster member

  – SHC member-specific actions:
    - **`addCommit`**: changes made locally on this member
    - **`pullFrom`**: changes pulled from the captain to this member
    - **`acceptPush`**: changes pushed from a member to this instance
    - **`computeCommon`**: initial negotiation with the captain
    - **`purgeEligible`**: purge in-memory and on-disk data to reduce resource usage
    - **`installSnapshot`**: update to a snapshot of the latest bundle from the captain
    - **`downloadDeployableApps`**: install baseline apps from the deployer on startup

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Checking SHC Bundle Deployment Status

- Search from a search head member:

```
index=_internal component=ConfDeployment data.task=*Apps
| table host data.source data.target_label data.task data.status
```

- Check the Search Head Clustering: App Deployment dashboard
  - MC > Search > Search Head Clustering

Apps Status

2 apps

App	Status
BCG Web	Synchronized
shc_base	Synchronized

This panel shows the status of apps pushed by deployer to search head cluster members.

Synchronized: all members have the latest version of the app.

Out of Synchronization: one or more members does not have the latest version of the app.

Click on a row to see more details.

BCG Web

Checksum on Search Head Cluster Members

Instance	Checksum
sh4	80be99dcced1796a0a01a33e48e00e965ae8e189
sh3	80be99dcced1796a0a01a33e48e00e965ae8e189
sh2	80be99dcced1796a0a01a33e48e00e965ae8e189

Checksum on Search Head Cluster Deployer

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

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Some Useful Debugging Searches

- Find missing baseline:

```
index=_internal sourcetype=splunkd_conf
STOP_ON_MISSING_LOCAL_BASELINE | timechart count by host
```

- Overall configuration replication behavior

```
index=_internal sourcetype=splunkd_conf pullFrom
data.to_repo!=*skipping* | timechart count by data.to_repo
```

- Evidence of captain switching

```
index=_internal sourcetype=splunkd_conf pullFrom
data.from_repo!=*skipping* | timechart count by
data.from_repo
```

- Find the destructive resync events:

```
index=_internal sourcetype=splunkd_conf installSnapshot |
timechart count by host
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

More Useful Conf Replication Log Channels

- **`splunkd.log`** components
  - **`ConfReplication`**
  - **`ConfReplicationThread`**
  - **`ConfReplicationHandler`**
  - **`loader`** – check events during startup
- Replication performance: **`metrics.log group=conf`**
  - **`wallclock_ms_total`** is for an action and **`wallclock_ms_max`** is for a single invocation
- Network activity between the members:
  - **`sourcetype=splunkd_access uri_path="/services/replication/configuration*"`**
- Network activity between the members and the deployer:
  - **`sourcetype=splunkd_access uri_path="/services/apps/local*" OR uri_path="/services/apps/deploy*"`**

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Types of SHC Captaincy

- SHC has two types of captaincy designed to handle specific cases
  - Dynamic captain (default)
    - If you want to reassign captaincy, you can manually transfer captaincy to a preferred member
  - Static captain
    - When members are unable to elect a captain

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Controlling Captaincy

- Why?
  - SHC Captain consumes more CPU and memory resources
  - If a system with less number of cores becomes the captain, the overall scheduling capacity gets lowered
    - SHC search capacity **= *captains_scheduler_count x #_of_members*** with scheduled search enabled (**adhoc_searchhead = false**)
  - Assign captaincy to members based upon geographic preference
- How?
  - Set **preferred_captain=false** in **server.conf** to exclude a member
  - SHC tries to elect a member with **preferred_captain=true** (default), but not always possible
    - For example, if no preferred members are reachable by the majority
  - When a non-preferred captain is chosen, the first available preferred captain member requests a captaincy transfer

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Transferring Captaincy

- To transfer the captaincy to a preferred member, run this command from any member:

```
splunk transfer shcluster-captain -mgmt_uri <new_captain>
```

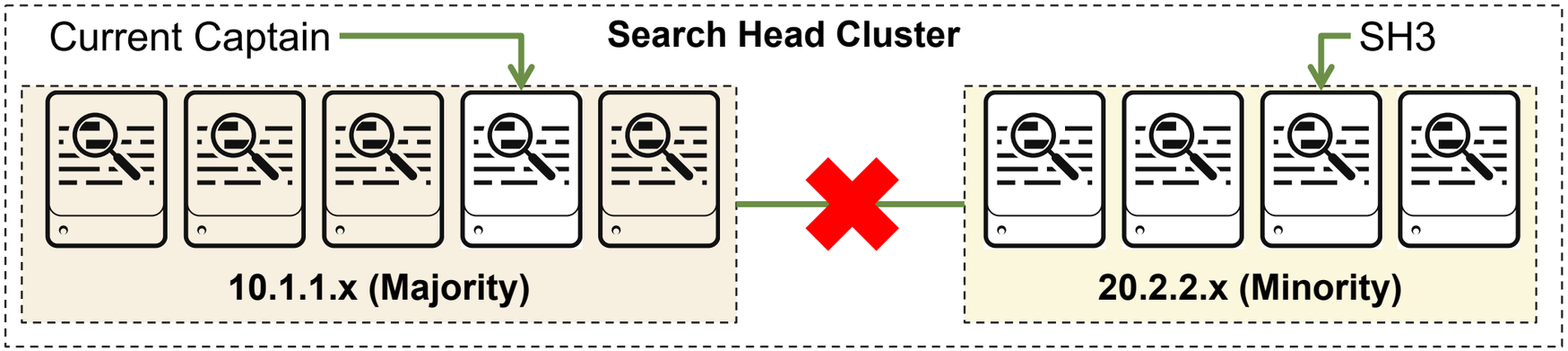
- NOTE:
  - **`splunk rolling-restart shcluster-members`** automatically invokes the captaincy transfer
- To check the transfer status, run this from any member:

```
splunk show shcluster-status
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Designating a Static Captain



- During a network partition failure, minority group members are unable to elect a captain
- Splunk admins can designate a captain for the minority group as a temporary workaround
  - On the new captain node (**SH3**):

```
splunk edit shcluster-config -election false -mode captain -captain_uri https://SH3:8089
```

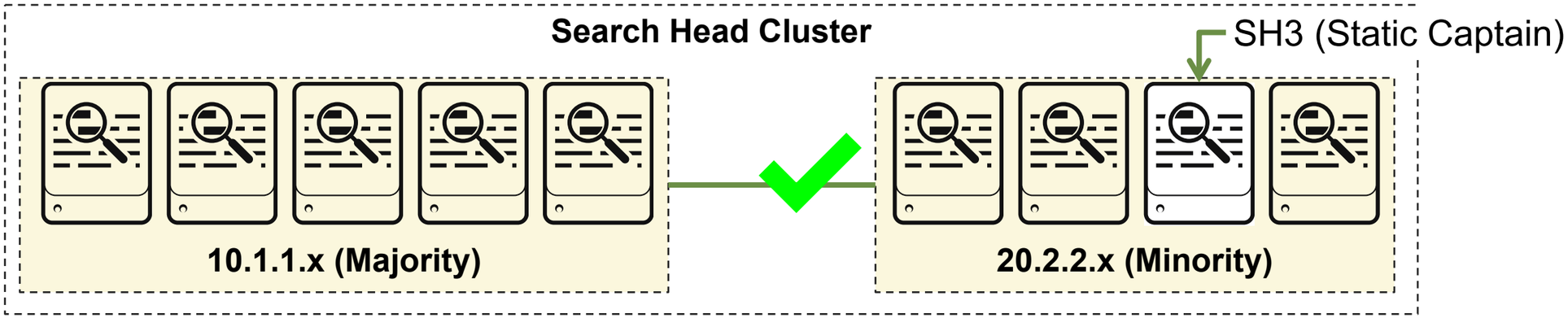
  - On the rest of the minority group members:

```
splunk edit shcluster-config -election false -mode member -captain_uri https://SH3:8089
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Restoring the Cluster to Dynamic Captaincy



Upon resolution of the issue, revert to the dynamic captain mode

1. On all majority members: Disable election and report to the static captain

```
splunk edit shcluster-config -election false -mode member -captain_uri https://SH3:8089
```

2. On all members: Re-enable election; change the static captain last

```
splunk edit shcluster-config -election true -mgmt_uri <THIS_MEMBER>:8089
```

3. On **SH3**: Bootstrap as the new dynamic captain for the entire SHC

```
splunk bootstrap shcluster-captain -servers_list <SEARCH_HEAD_MEMBER_LIST>
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Adding Search Head Members

- Why always use new Splunk instances?
  - SH cluster configuration consistency is derived from the journals
  - The **`ops.json`** file is fixed in size (configurable) and gets rolled
  - Non-members do not have this file
  - Members downed for a long time may not be able to find the diverging point
- Add an offline member to the search head cluster:
  - Restart the offline member
    - Receives the set of intervening changes from the captain and should resync
  - If unable to fully recover, you can force the resync on the re-joining member:

    `splunk resync shcluster-replicated-config`

  http://docs.splunk.com/Documentation/Splunk/latest/DistSearch/Handlememberfailure
- Add a new member or a previously decommissioned member:
  - Details on the next slide

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Adding a New or Decommissioned Member

1. Delete Splunk Enterprise, if exists
2. Install and initialize the instance
3. Join the search head cluster
   - To announce itself to an existing SH cluster, run on the new instance:

     ```
     splunk add shcluster-member -current_member_uri
     https://<any_existing_member>:8089
     ```

   - To introduce a new member to the cluster, run from any existing member:

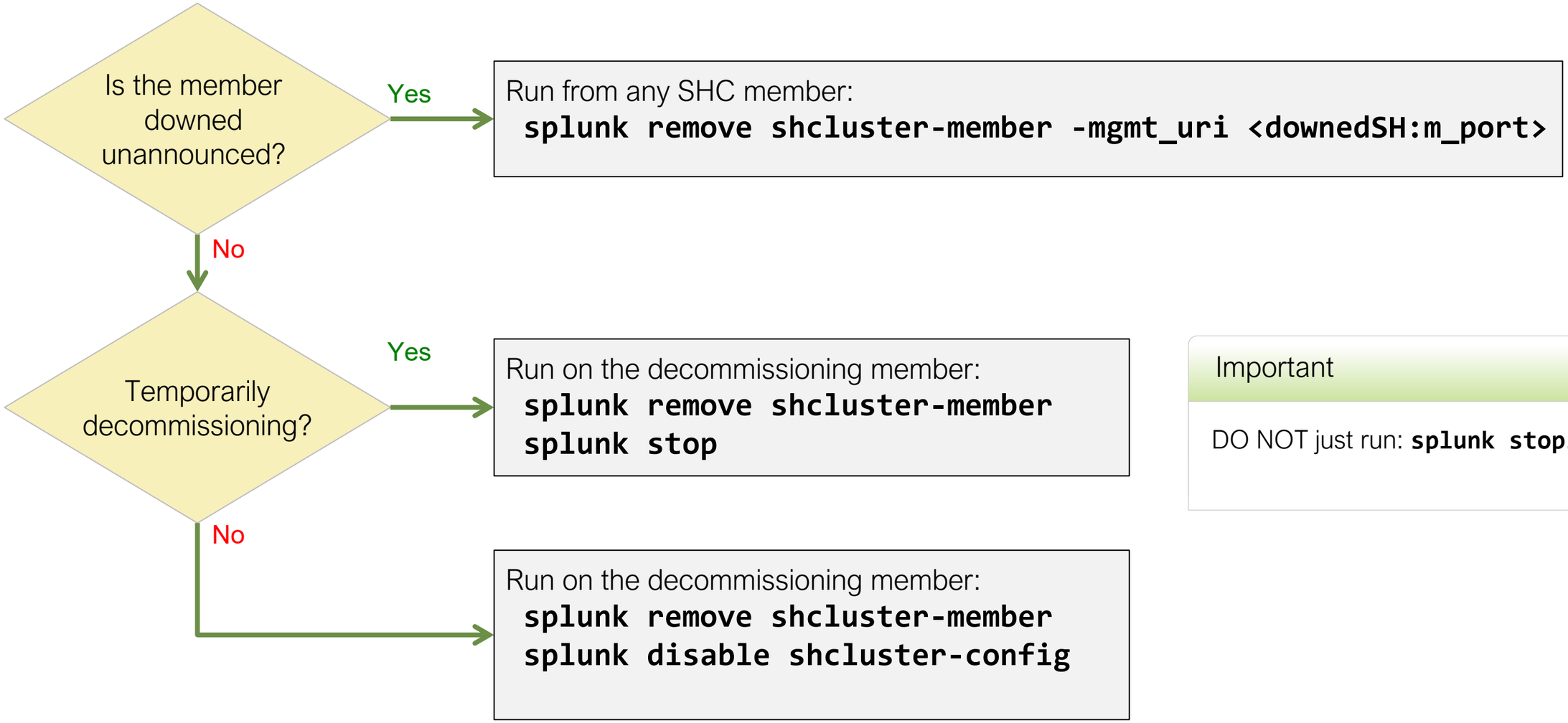
     ```
     splunk add shcluster-member -new_member_uri
     https://<new_member>:8089
     ```

- When a new member joins the cluster, it gets:
  - The deployed bundles from the deployer
  - The replicated configurations and artifacts from the captain

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Decommissioning a SH Cluster Member



Important

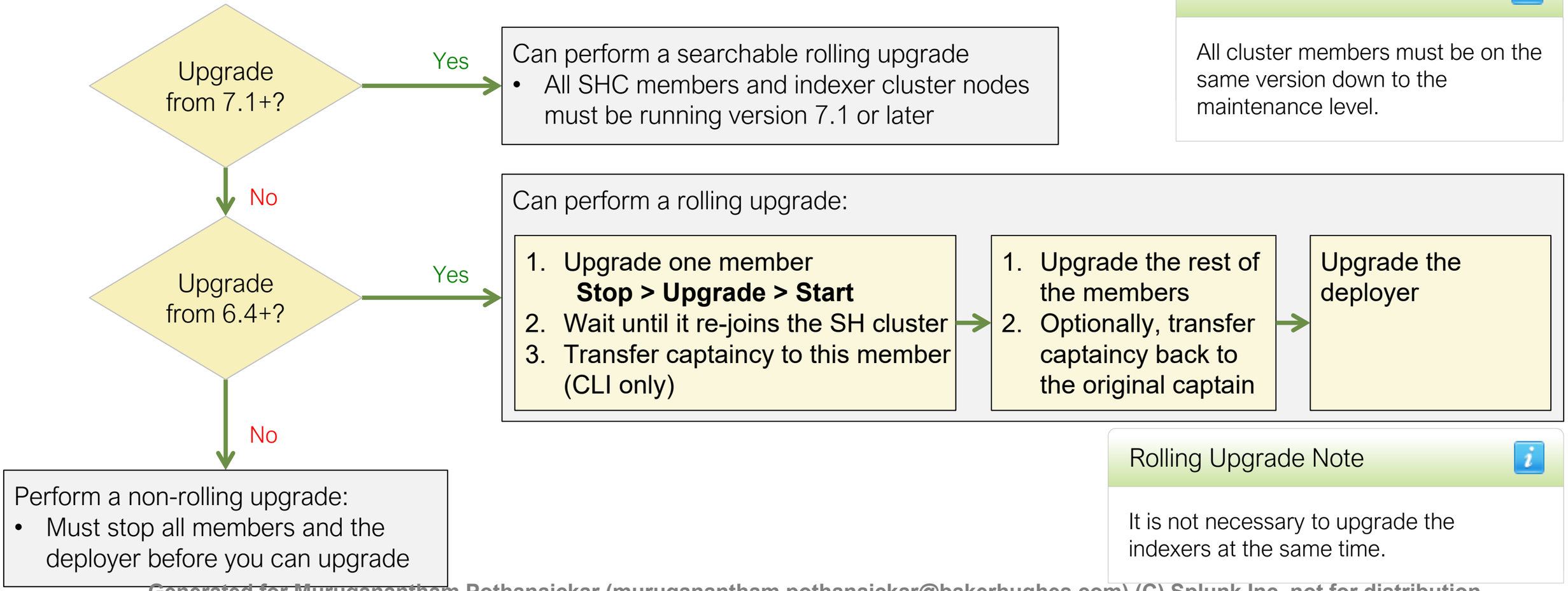
DO NOT just run: **`splunk stop`**.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Upgrading a Search Head Cluster

- The process is the same for maintenance and major release upgrades
  http://docs.splunk.com/Documentation/Splunk/latest/DistSearch/UpgradeaSHC



Note

All cluster members must be on the same version down to the maintenance level.

Rolling Upgrade Note

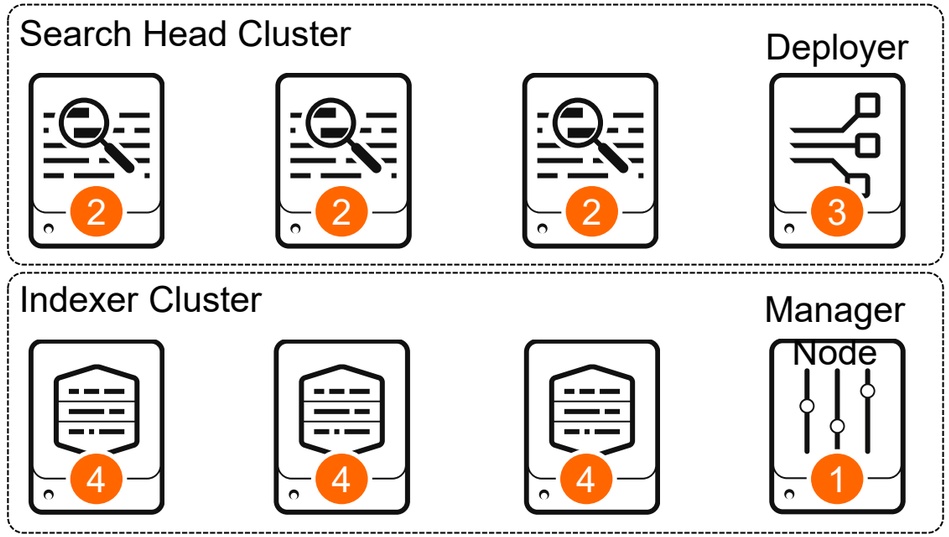
It is not necessary to upgrade the indexers at the same time.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Splunk Cluster Searchable Rolling Upgrade

- Upgrade or patch Splunk clusters with minimal or no downtime
- All SHC members and indexer nodes must be running version 7.1 or later
  - Supports only in dynamic captaincy mode
  - Avoid admin operations while upgrading
    - e.g. bundle push, node addition
- Be prepared to intervene in case a node cannot restart
  1. Upgrade the manager node
  2. Upgrade the SH cluster
  3. Upgrade the deployer
  4. Upgrade indexer cluster peer nodes (site by site)



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

SH Cluster Searchable Rolling Upgrade

```
splunk show shcluster-status --verbose
```

```
splunk [upgrade-init | upgrade-finalize]
 shcluster-members
```

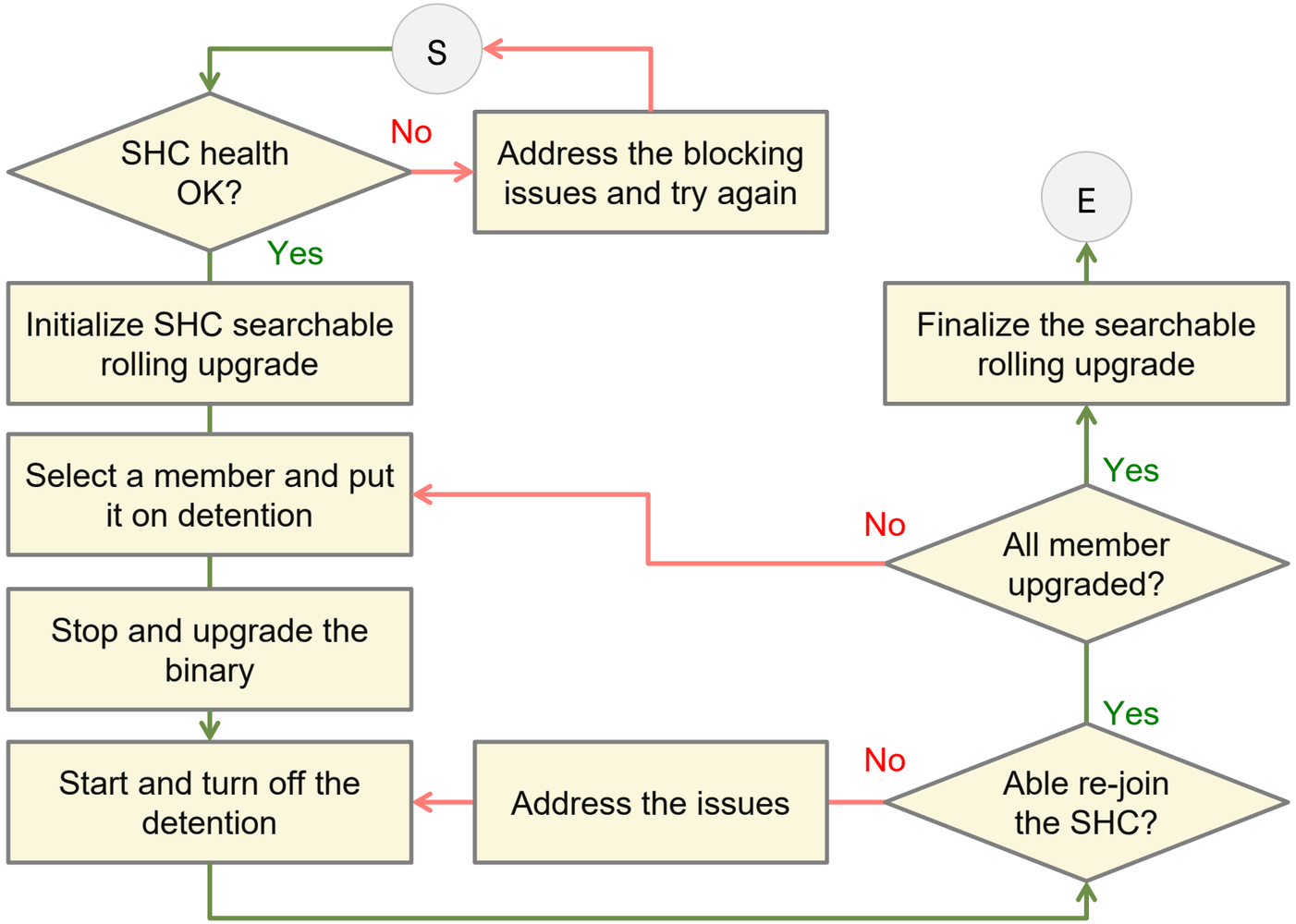
```
splunk list shcluster-member-info
```

Confirm `active_historical_search_count = 0`

```
splunk edit shcluster-config
 -manual_detention [on | off]
```

Note

Splunk provides a template script, **`SPLUNK_HOME/bin/shc_upgrade.py`**, that you can modify and use.



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Key SH Cluster Maintenance Commands

```
> splunk help shclustering
```

- Helpful CLI commands (can be run on Captain or members)

```
splunk rolling-restart shcluster-members
splunk show shcluster-status
```

- Helpful CLI commands to run on the SHC members

```
splunk [edit|list] shcluster-config
splunk add shcluster-member
splunk resync shcluster-replicated-config
splunk clean raft
```

- Helpful CLI commands to run on the SHC deployer

```
splunk apply shcluster-bundle
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

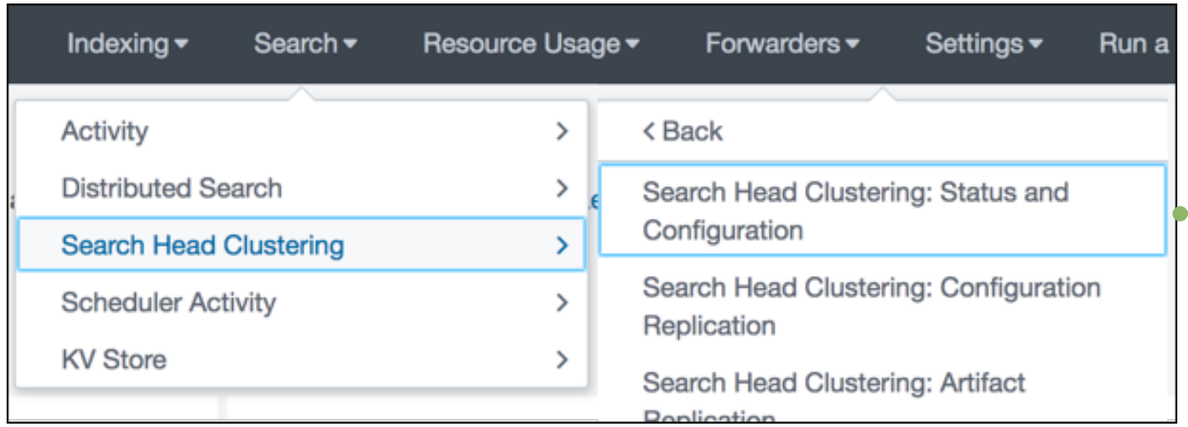
Search Head Cluster Health Report

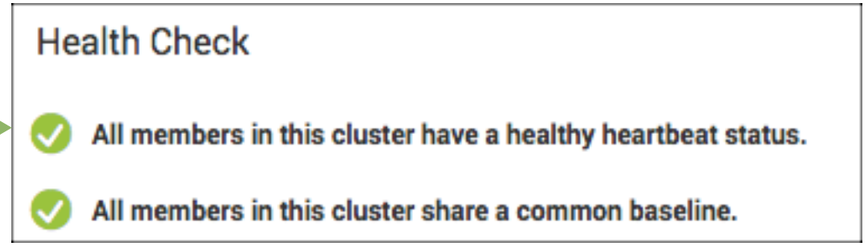
- **`feature:shc_members_overview`** tracks the status of SHC
  - **`status`** turns yellow if members skip a heartbeat and red if they skip more times
  - **`replication_factor`** checks if enough search head cluster members exist to honor the artifact replications (yellow only)
  - **`detention`** turns yellow if a member is in manual detention, red if a member is in automatic detention
- **`feature:shc_captain_election_overview`** tracks the quorum majority required to re-elect a dynamic captain (yellow only)
- **`feature:shc_captain_common_baseline`** reflects if the bundles are synced across members (red only)

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Search Head Cluster Dashboards in MC





- **SHC Status and Configuration** provides high-level SHC health
  - The last heartbeats should be nearly the same
  - A member heartbeat drift and frequent captain election indicate possible problems
- **Configuration Replication** shows how user changes propagate among its members
  - Drill down to see members' common baseline and detect unpublished changes
- Growing backlogs in **Artifact Replication Job Activity** should be investigated
- In **Scheduler Activity**, monitor **Skip Ratio** and **Execution Latency**

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Troubleshooting the SHC with Monitoring Console

Health Check

There are members in this cluster that do not have a healthy heartbeat status. click to see more detail.

There are members in this cluster that do not share a common baseline. Action may be required. click to see more details. Learn More

Status

3 Members

Instance	Role	Status	Last Heartbeat Sent to Captain	Configuration Baseline Consistency	Number of Unpublished Changes	Artifact Count
sh2	Captain (4d)	Up	03/12/2018 21:45:05 +0000	2/3	0	12
sh3	Member	Up	03/12/2018 21:45:03 +0000	2/3	0	12
sh4	Member	Down	03/12/2018 21:43:04 +0000	N/A	N/A	0

By default, members report a heartbeat every five seconds and the captain marks a member as **`Down`** after missing for 60 seconds

Health Check

All members in this cluster have a healthy heartbeat status.

There are members in this cluster that do not share a common baseline. Action may be required. click to see more details. Learn More

Status

3 Members

Instance	Role	Status	Last Heartbeat Sent to Captain	Configuration Baseline Consistency	Number of Unpublished Changes	Artifact Count
sh2	Captain (4d)	Up	03/12/2018 21:45:05 +0000	3/3	0	12
sh3	Member	Up	03/12/2018 21:59:18 +0000	3/3	0	12
sh4	Member	Up	03/12/2018 21:59:19 +0000	1/3	missing common baseline with the captain: https://10.0.1.2:8289	0

If a member was down for a long period of time, it may not be able to find a baseline and a manual resync on the member is required

Health Check

All members in this cluster have a healthy heartbeat status.

All members in this cluster share a common baseline.

Status

3 Members

Instance	Role	Status	Last Heartbeat Sent to Captain	Configuration Baseline Consistency	Number of Unpublished Changes	Artifact Count
sh2	Captain (4d)	Up	03/12/2018 22:01:41 +0000	3/3	0	12
sh3	Member	Up	03/12/2018 22:01:44 +0000	3/3	0	12
sh4	Member	Up	03/12/2018 22:01:44 +0000	3/3	0	12

To restore consistency:

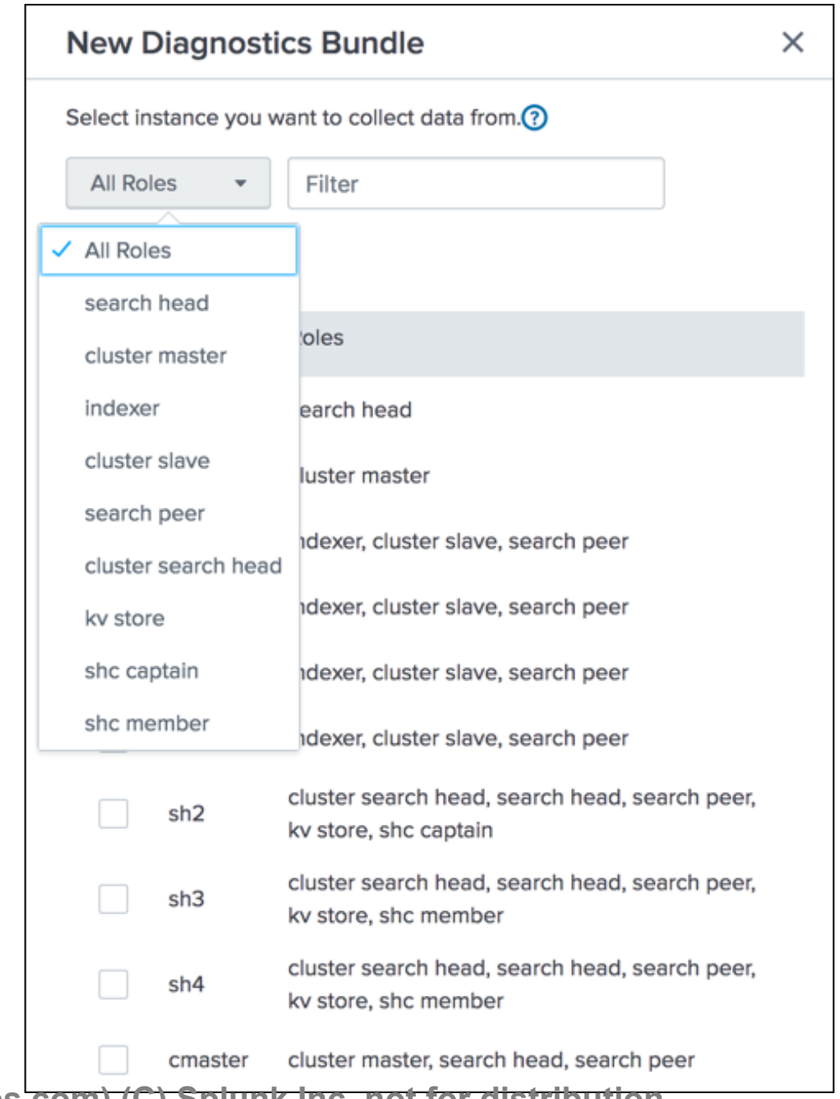
```
splunk resync
shcluster-replicated-config
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Using Diag UI on Monitoring Console

- Fully configured Monitoring Console running Splunk 7.1+ can provide a convenient diag collection service
  - Access **Settings** > **Instrumentation** from a MC node
  - Can collect diags one at a time or multiple instances by role or host name
  - The user requires the **`get_diag`** capability
- MC node authenticates with remote nodes via:
  - Auth token: independent search peers
  - Index cluster secret: manager & peer nodes
  - Search head cluster secret: SHC members



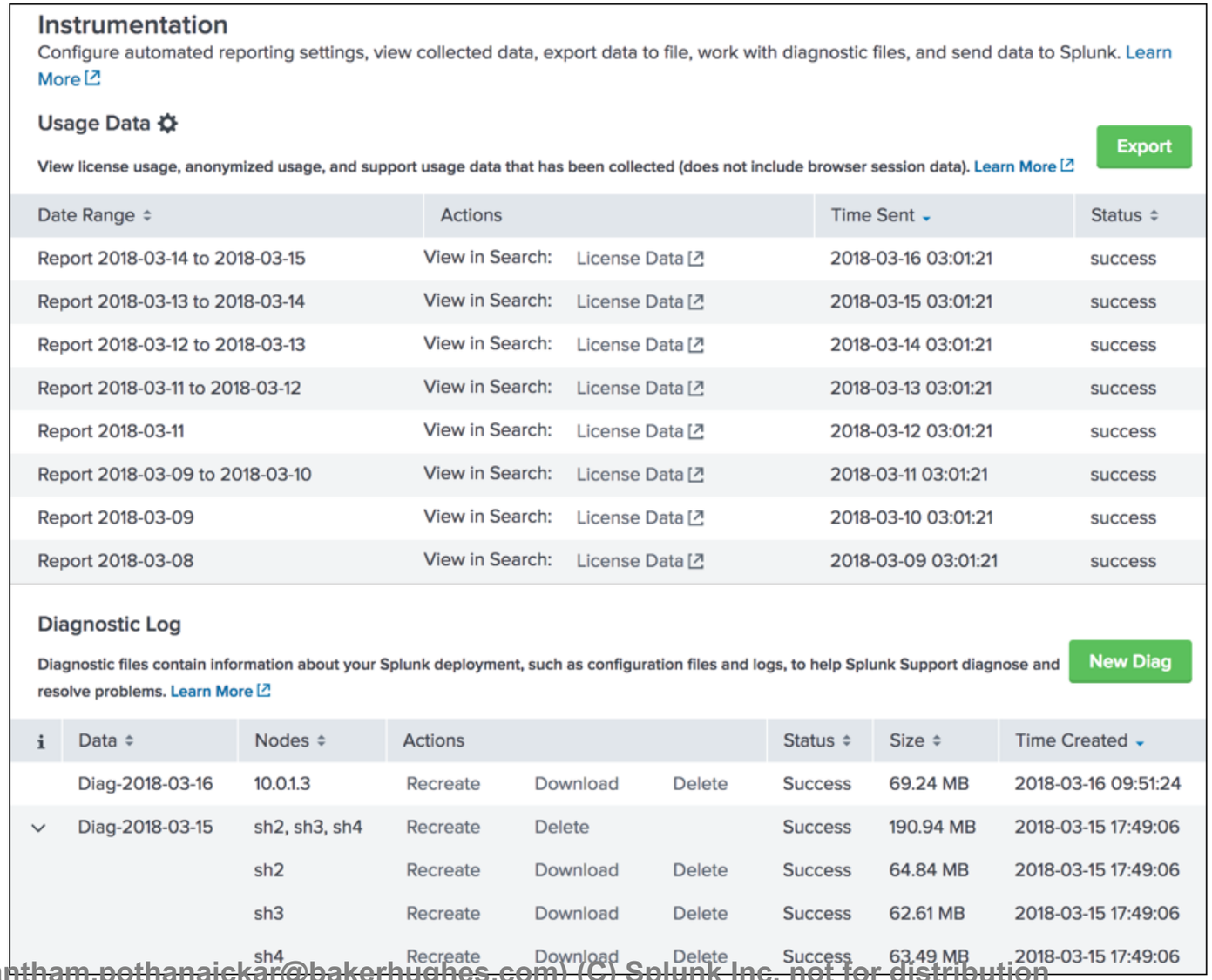
Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Diagnostic Log

- Lists diags previously created
  - Expires after 30 days
- Available actions:
  - Download
  - Delete
  - Recreate
    - Useful to track changes over time

Remote diag Task	Version
Any instance, except a manager node	6.0
Exclude lookups	6.5
View and access a remote diag	6.5
Manager node	7.1
Select component granularity	7.1



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Further Reading:

- Search head forwarding

https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Forwardmanagerdata

- Distribute apps and configuration updates with deployer

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

- Search head cluster status and troubleshoot issues

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

- Use static captain to recover from loss of majority

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

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

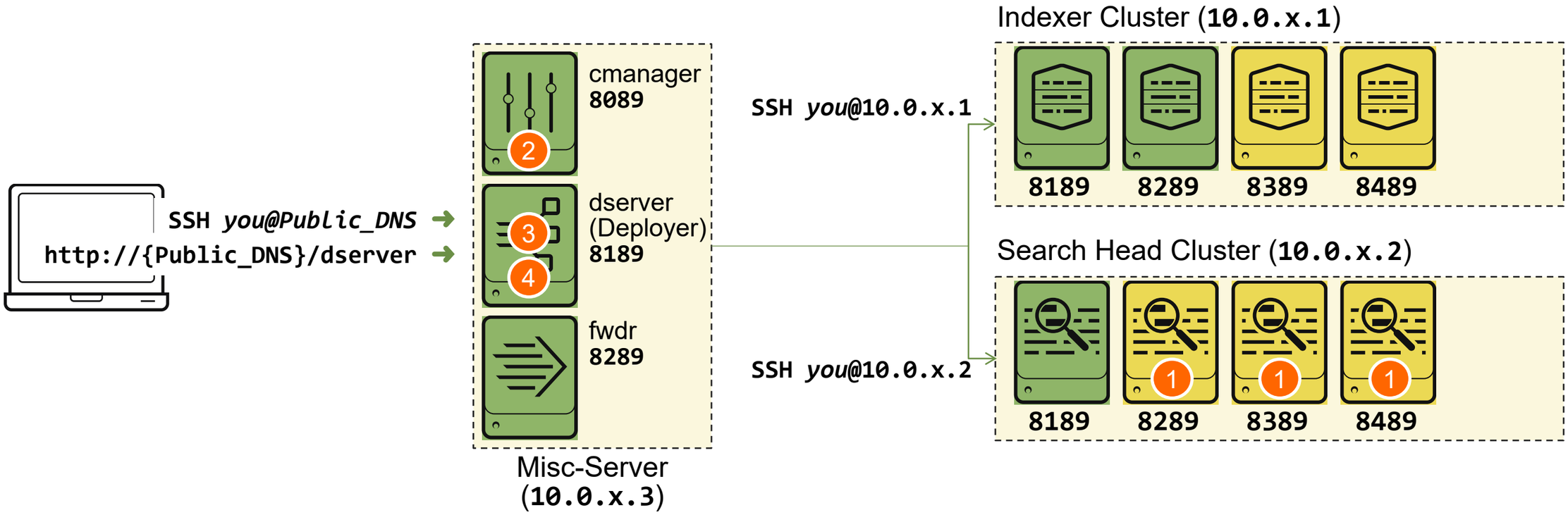
Lab Exercise 7 –Deploy a SHC App

- **Time**: 25 - 30 minutes
- **Tasks**:
  - Configure the SHC members and the deployer
  - Stage and distribute apps to search head cluster members
  - Verify the app deployment
  - Complete the Monitoring Console setup on **`dserver`**
  - Review the search head cluster dashboards

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Lab Exercise 7 – Deploy a SHC App (cont.)



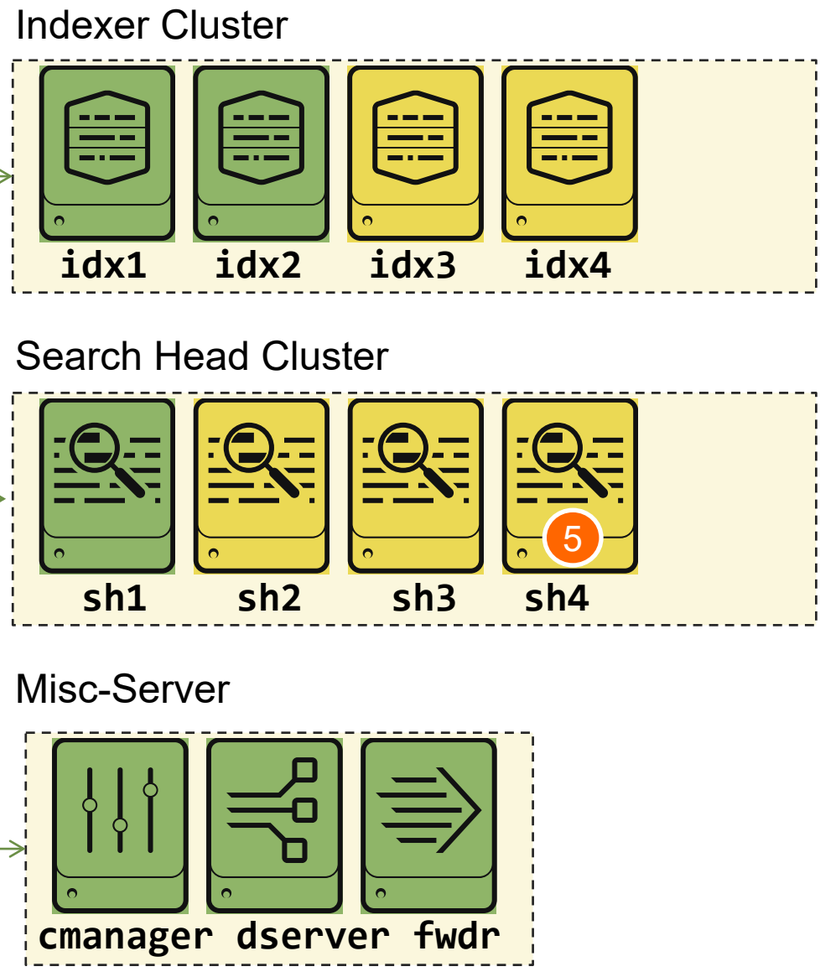
x = Your student ID
8?89 = splunkd-port

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Lab Exercise 7 – Deploy a SHC App (cont.)

http://{Public_DNS}/{splunk_server}
For example:
http://{Public_DNS}/sh2
http://{Public_DNS}/sh3
http://{Public_DNS}/sh4
http://{Public_DNS}/sh5 (Optional)



Public_IP = Same as your Misc-Server
splunk_server = Splunk server name

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Module 8:
KV Store Management in Splunk Clusters

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module Objectives

- Enable a KV store collection under a search head cluster
- Manage KV store collections in a search head cluster
- Monitor and troubleshoot KV store issues in Splunk clusters

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

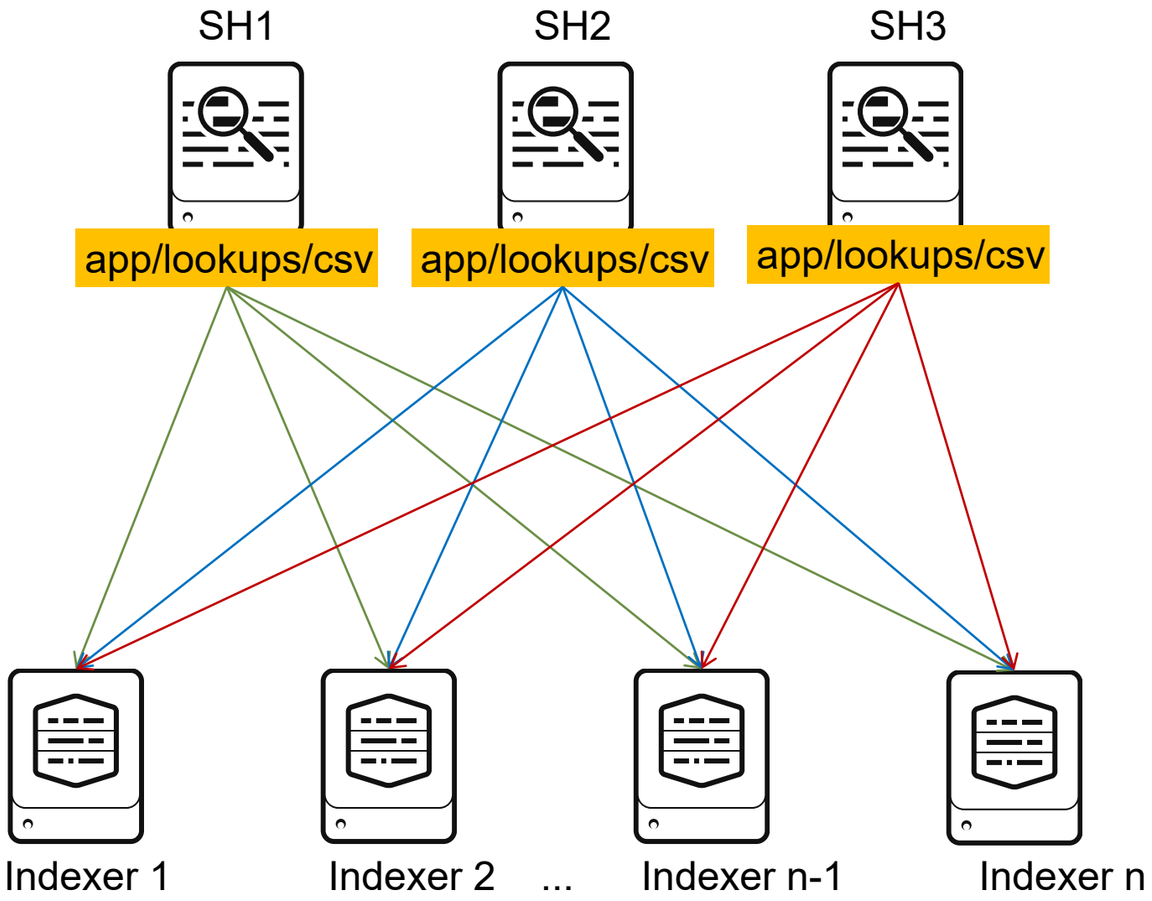
Overview of Splunk Lookups

- A lookup is a Splunk data enrichment knowledge object
  - Splunk lookups are supported during search time and the parsing phase
  - Defined in **`props.conf`** and **`transforms.conf`**
- **File-based lookup** is used for datasets that are small and/or change infrequently
  - Uses CSV files stored in the **`lookups`** directory
  - Gets replicated to search peers
- **KV store lookup** is designed for large key-value collections that frequently change
  - Need to define **`collections.conf`** additionally
    - Can optionally configure data type enforcement and field accelerations
  - Collections live only on the search heads by default

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

CSV Lookup Challenges in Distributed Environment



- Each search head manages and replicates its own CSV lookup files
  - Updates to lookup files propagate to search peers independently
- Searches can fail if a bundle is not replicated to search peers in time
  - By default, a bundle larger than 2GB is not replicated to the search peers
- In Splunk clusters, the timely replication of lookup files is more critical
  - By default, SHC conf replication rejects a bundle size larger than 2GB

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Benefits of KV Store Lookup

- Quick per-record updates
  - Performs Create-Read-Update-Delete (CRUD) operations on individual records using the Splunk REST API and SPL commands
- Standardized interface for app developers
  - REST API and data type validation
- Faster lookup replication from SHC to search peers
  - Enable KV store replication first per collection
    - Distributes a collection in CSV lookup files
    - Can perform automatic lookups on the index tier
- Can facilitate backup and restore of KV store data

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Enabling KV Store Collections

- Before users can use a KV store, an admin must create a collection
- A collection is defined in **`collections.conf`**
  - Must be placed in an app's **`default`** or **`local`** directory
    - Other attempts are ignored
  - Specify the name of the collection (stanza) and optional attributes
    - Matching lookup field, output fields, etc.
  - Enforcing data types is optional
    - If enforced, any input that does not match the type is silently dropped
  - More options discussed later

collections.conf

```
[collection_name]
enforceTypes = [true|false]
field.<name1> = [number|string|bool|time]
field.<name2> = [number|string|bool|time]
accelerated_fields.<xl-name> = <json>
```

Example:

```
[mykv]
enforceTypes = true
field.x = number
field.y = string
accelerated_fields.xl2 = {"x": 1, "y": 1}
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Populating KV Store Lookups

- Create a KV store collection stanza in **`collections.conf`**
  - Enable optional attributes, if needed
- Add lookup definition for KV store
  - Click **Settings** > **Lookups** > **Lookup definitions**
    - The resulting configuration is saved in **`transforms.conf`**
- Write data to the KV store
  - Search: **`... | fields id, location, type | outputlookup <lookup_name>`**
  - Or, use REST APIs

```
curl -k -u <user>:<pw>
https://<url:mport>/servicesNS/<user>/<app>/storage/collections/data/<lookup_name>
-H 'Content-Type: application/json'
-d '{"id": 001, "location": "CA", "type": "basic"}'
```

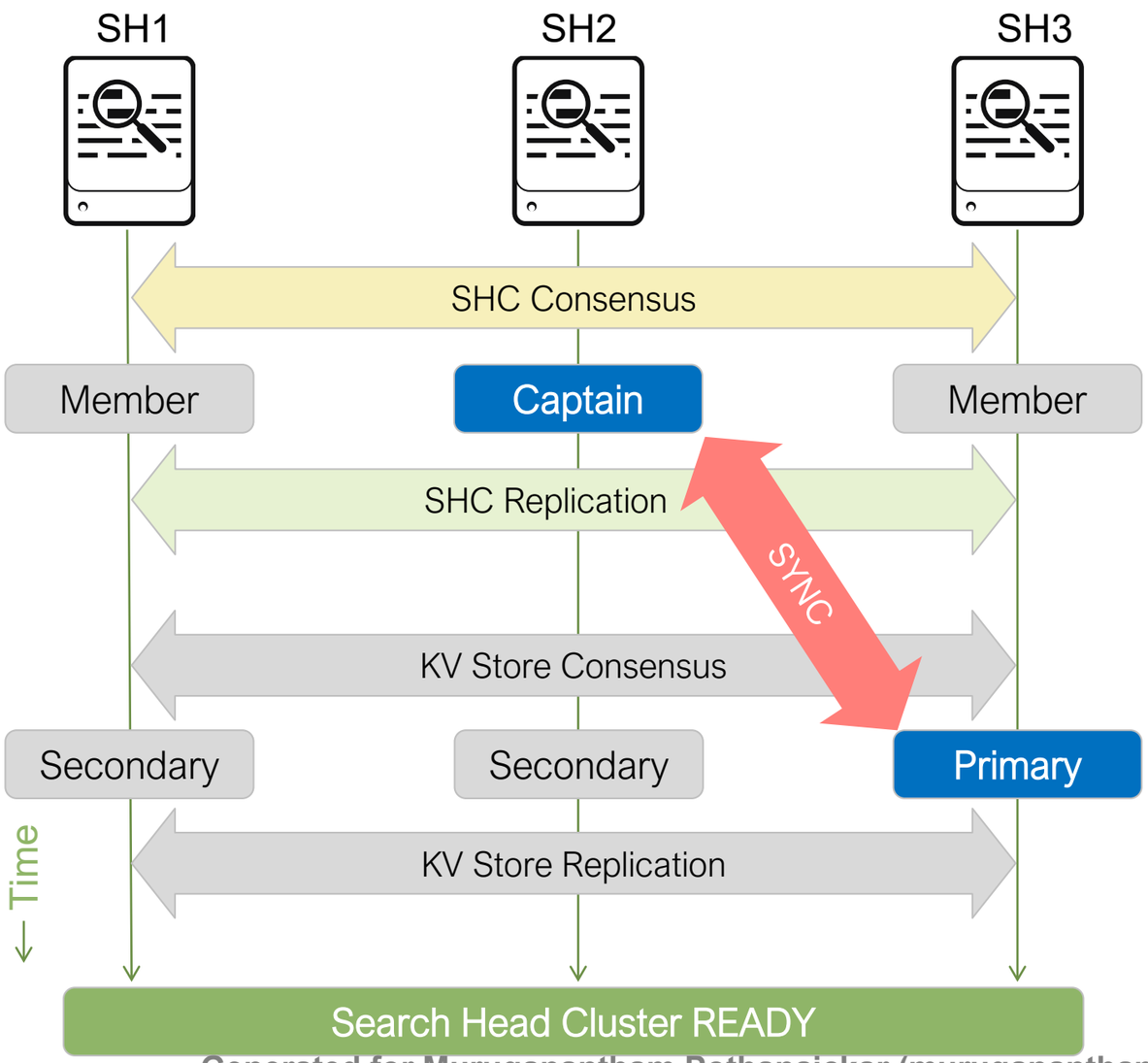
Note

Working with KV store is discussed in detail in Building Splunk Apps course.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

How KV Store Works in SH Cluster

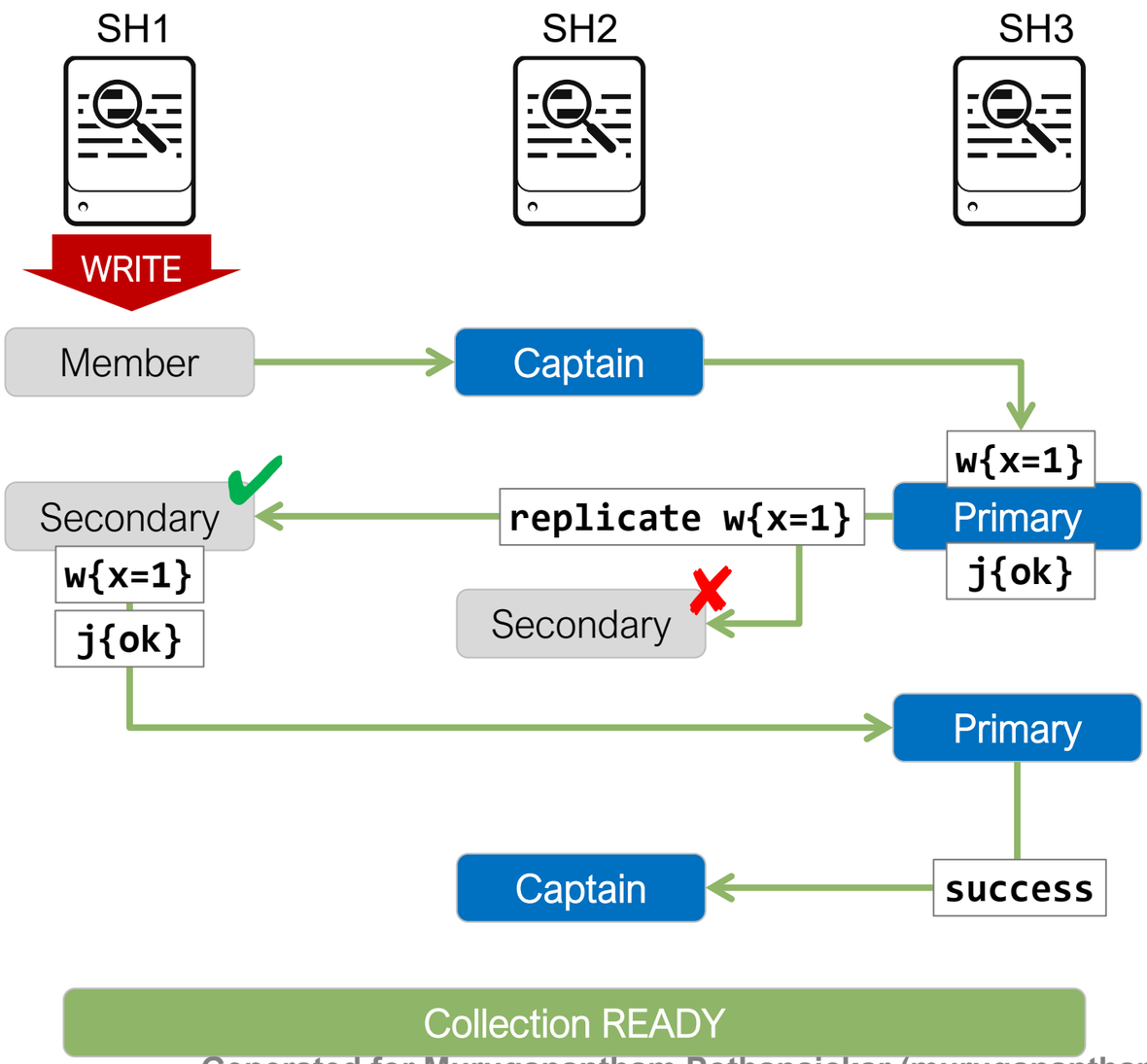


- Within a SHC, the KV store forms its own cluster
  - Can use up to 50 SHC members
- KV store port must be accessible from all SHC members
  - Uses 8191 by default
- SHC captain and KV store primary synchronize their member list every time there is a status change
  - Add, remove, or restart
- By default, the value of **`mgmt_uri`** in **`[shclustering]`** is used for KV store connection and replication

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

KV Store Collection Replication – Write

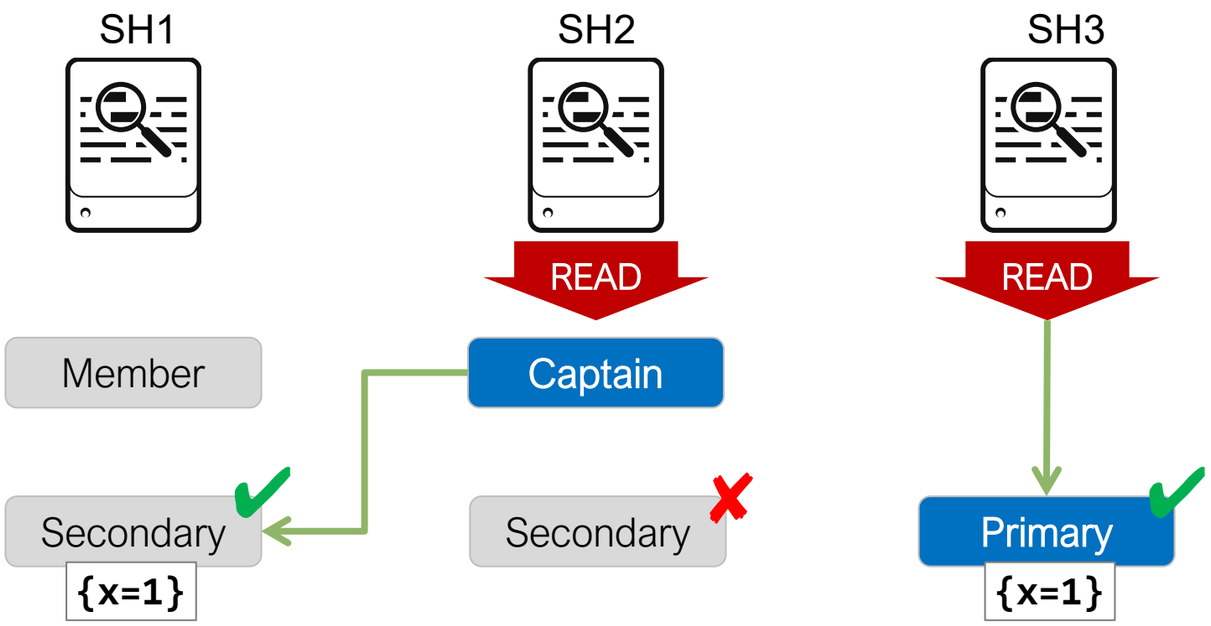


- The primary receives all write operations and records them in its journal
- The secondaries copy and apply these operations asynchronously
- Writes are acknowledged when:
  - The majority of voting KV store nodes have applied the operations
  - The writes have successfully been logged to their respective journals
- Checkpoints in journals provide data consistency
  - Provide recovery information

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

KV Store Collection Replication – Read



- READ operations can be done on any member
- Routed to the *nearest* member
  - Read from the lowest-latency member
  - Most reads are done with local instance preference

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

KV Store CLI Commands

- The similar conditions that cause SHC members to end up in an inconsistent replication state can cause the KV store collections to be out of sync
  - Frequent status changes to the SHC member instances
  - Changing the GUID or hostname of a member
  - Depending on the condition of SHC, KV store cluster can also be in the state where it is impossible to sync
- One workaround is to bootstrap SHC from scratch
  - WARNING: Proceed ONLY when it is absolutely necessary
- Useful commands
  - **`splunk show kvstore-status`**
  - **`splunk [backup | restore]`**
  - **`splunk clean kvstore`**
  - **`splunk resync kvstore -source <GUID>`**

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

splunk show kvstore-status

Example ran on SH2

splunk show shcluster-status

```
Captain:
        dynamic_captain : 1
        elected_captain : Fri Mar  9 00:32:52 2018
                     id : CE1F9057-981B-4419-BBA1-F10A5F3FBC6A
       initialized_flag : 1
                  label : sh2
               mgmt_uri : https://10.0.1.2:8289
  min_peers_joined_flag : 1
   rolling_restart_flag : 0
     service_ready_flag : 1

Members:
 sh2                label : sh2
                 mgmt_uri : https://10.0.1.2:8289
           mgmt_uri_alias : https://10.0.1.2:8289
                   status : Up

 sh3                label : sh3
    last_conf_replication : Wed Mar 14 22:58:43 2018
                 mgmt_uri : https://10.0.1.2:8389
           mgmt_uri_alias : https://10.0.1.2:8389
                   status : Up

 sh4                label : sh4
    last_conf_replication : Wed Mar 14 22:58:43 2018
                 mgmt_uri : https://10.0.1.2:8489
           mgmt_uri_alias : https://10.0.1.2:8489
                   status : Up
```

splunk show kvstore-status

```
This member:                    ...
            replicationStatus : Non-captain KV store member
                   standalone : 0
                       status : ready

Enabled KV store members:
10.0.1.2:8291             guid : 13E6C3B3-293D-468B-A27D-66EC0D1358D8
                   hostAndPort : 10.0.1.2:8291
                                ...
KV store members:
10.0.1.2:8391       configVersion : 3
                     electionDate : Mon Mar 12 21:43:19 2018
                  electionDateSec : 1520890999
                      hostAndPort : 10.0.1.2:8391
                    lastHeartbeat : Wed Mar 14 23:01:54 2018
                lastHeartbeatRecv : Wed Mar 14 23:01:55 2018
                                ...
                       optimeDate : Wed Mar 14 23:01:54 2018
                    optimeDateSec : 1521068514
                           pingMs : 0
                 replicationStatus : KV store captain
                           uptime : 176616
                                ...
10.0.1.2:8291       configVersion : 3
                      hostAndPort : 10.0.1.2:8291
                       optimeDate : Wed Mar 14 23:01:54 2018
                    optimeDateSec : 1521068514
                replicationStatus : Non-captain KV store member
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Monitoring KV Store Status with MC

- MC provides more details on KV store status
  - In the MC General Setup page, add the KV store server role to the instance
  - Go to **MC** > **Search** > **KV Store: Deployment**

KV Store Status

Instance	Physical Memory Usage (MB)	Mapped Memory Usage (MB)	Page Faults per Operation	Total Queued	Active Connections	Lock (%)	Last Flush (ms)	Network Traffic (MB)	Uptime (hours)	Replication Role
sh2	186	2558	0.00	0	19		1	1636.22	142.73	Primary
sh3	176	2558	0.00	0	15		1	1700.68	142.74	Secondary
sh4	169	2558	0.00	0	13		1	561.55	49.30	Secondary

Click instance name for more details. Total queued is operations (readers and writers) waiting for a read or write lock to be cleared.

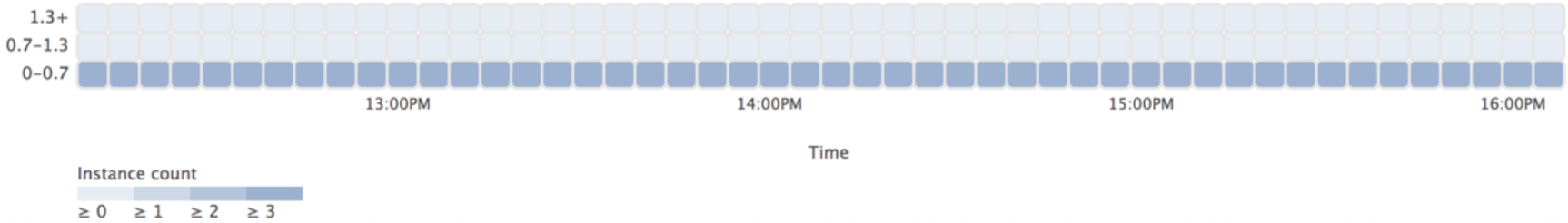
Historical Charts

Instances by Median Page Faults per Operation

Aggregation

Median

Column Chart | Heat Map



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Backing Up and Restoring KV Store

- To back up KV store data in a SHC:
  1. Confirm the KV store status with CLI or MC

     splunk show kvstore-status
  2. From a member with **backupRestoreStatus** and **status** in **ready** state, run:

     splunk backup kvstore [-archiveName <archive>] [-collectionName <collection>] [-appName <app>]
     - Dumps an output to: **SPLUNK_HOME/var/lib/splunk/kvstorebackup/kvdump_<timestamp>.tar.gz**
- To restore when the majority SHC members are stale:
  1. Confirm the KV store status with CLI or MC

     splunk show kvstore-status
  2. Run the restore command:

     splunk restore kvstore -archiveName <archive>.tar.gz

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Fixing Stale KV Store Members

- When KV store members fail on the write operations, they might become stale
  - Run **`splunk show kvstore-status`** to determine the stale members
- If majority members are stale, then the SHC requires a new bootstrap

1. Pick the best member to be the KV store data authority and back up
2. On all SHC members:
   a. Remove the KV store cluster info
   b. Clean KV store local data
   c. Reset SHC raft data
3. Bootstrap a new SHC and add members back
4. Restore the KV store data
5. From the captain, sync KV store (if still see the stale members)

```
splunk backup kvstore
```

```
splunk stop
splunk clean kvstore –cluster
splunk clean kvstore -local
splunk clean raft
```

```
splunk start
splunk bootstrap shcluster-captain -servers_list <sh>
splunk add shcluster-member -current_member_uri <captain>
```

```
splunk show shcluster-status
splunk show kvstore-status
splunk restore kvstore –archiveName <kvdump>
splunk resync kvstore
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Fixing Stale KV Store Members (cont.)

- If only a few members are stale, then resync it from one of the members
  - Stale member:

```
splunk show kvstore-status
splunk stop
splunk clean kvstore -local
splunk start
```

  - SHC captain:

```
splunk resync kvstore [-source <KVstore_source_GUID>]
```

Note

Specify optional **`-source`**, if you want to use a member other than the captain.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

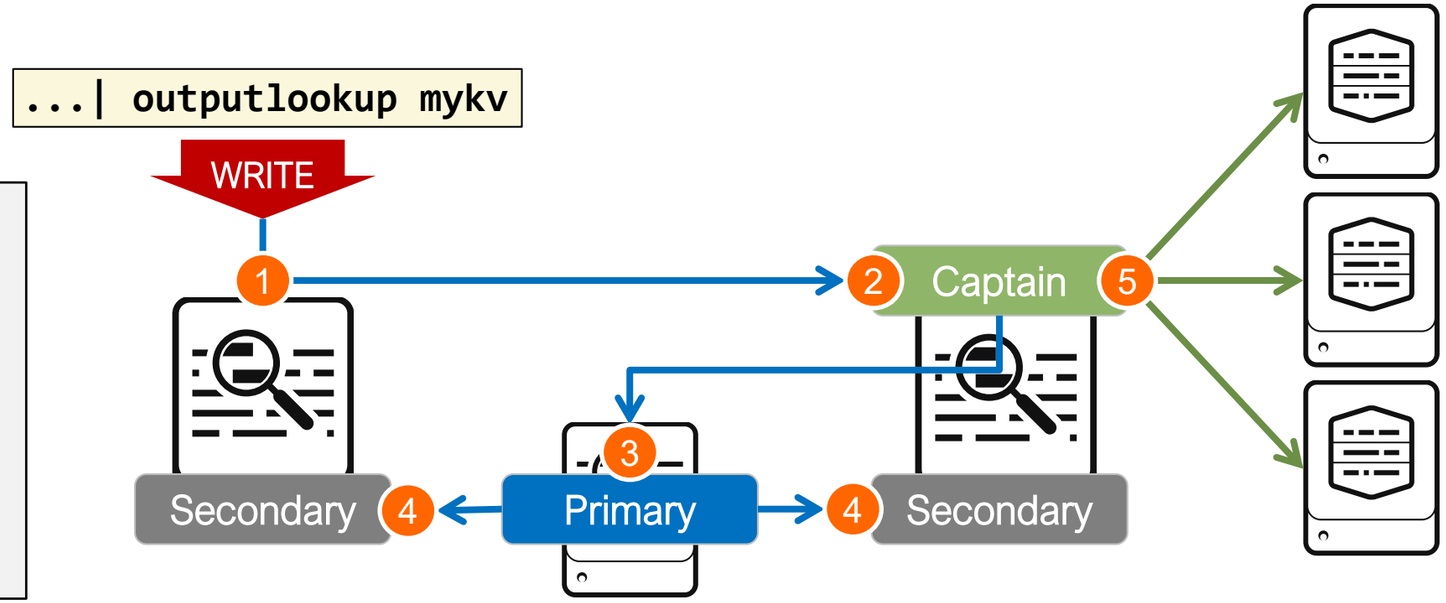
Copyright © 2022 Splunk, Inc. All rights reserved

SHC KV Store Bundle Replication to Indexers

- To enable an automatic lookup with KV store data, you must enable replication in **`collections.conf`**
  - Each automatic lookup configuration is limited to a specific host, source, or source type

collections.conf on all members

```
[mykv]
enforceTypes = true
field.x = number
field.y = string
accelerated_fields.xl2 = {"x": 1, "y": 1}
replicate = true
replication_dump_strategy = one_file|auto
replication_dump_maximum_file_size = <KB>
```



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Notable KV Store Log Channels

- **`Metrics.log`** has two subgroups under **`group=kvstore`** to track different activities
  - **`name=dump OR name=sync`**
  - Example: Show the sync operation duration over time

```
index=_internal metrics group=kvstore | timechart max(msSyncTotal) by name
```

- **`splunkd.log`** contains various components for KV store status, start/stop, sync, and replication activities
  - Logs only **`WARN/ERROR`** events by default
  - Can increase the log verbosity in **`server.conf`**

```
[kvstore]
verbose = true
```

  - For list of KV store components, search:

```
index=_internal sourcetype=splunkd component IN (kvstore*, collection*)
```

- **`kvstore.log`** contains the introspection data feeding the **`_introspection`** index

```
index=_introspection sourcetype=kvstore
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

KV Store Operations Log Size

- The journal keeps record of all operations that modify the collections
- A larger journal can give a KV store cluster a greater tolerance for lag and even make the set more resilient
- The KV store allocates the full log size the first time Splunk is started, regardless of its utilization
  - The operations log is 1 GB by default
  - To adjust, edit **`[kvstore] oplogSize`** in **`server.conf`**
    - Must edit all nodes and run **`splunk clean kvstore –local`**
- *So, what is consuming all that journal space?*
  - A large **`| outputlookup`** operation can generate a lot of records
  - **`outputlookup append=true`** vs **`outputlookup append=false`**

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Monitoring KV Store with Monitoring Console

- **`index=_introspection`** derives the historical KV store performance views in Monitoring Console
- Start with the deployment-wide view and drill down to an instance level
  - **Median Page Faults per Operation** shows the read activity involving disk I/O
  - Excessive hit (1.3+) indicates a need for more RAM
  - **Replication latency** shows the operation lags between the primary and secondary nodes during writes
    - Long lags (30+) can indicate replication (write) issues
    - You may need to increase the operation log size
  - Together with **High lock percentage** (50%+) and **Flushing rate** (50~100%), you can infer that there are heavy write operations or the system is sluggish
  - **Operations Log Window of KV Store Captain** shows the time between the first and last operations in the journal
- **Operations per Minute** in the **KV Store: Instance** dashboard shows the number of calls made to the KV store operations in detail

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Further Reading: KV Store

- About KV Store
  - docs.splunk.com/Documentation/Splunk/latest/Admin/AboutKVstore
- Configure KV Store lookups:
  - docs.splunk.com/Documentation/Splunk/latest/Knowledge/ConfigureKVstorelookups
- KV Store backup and restore
  - docs.splunk.com/Documentation/Splunk/latest/Admin/BackupKVstore

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Lab Exercise 8 – Add a KV Store Collection

- **Time**: 25 - 30 minutes
- **Tasks**:
  - Identify the current SHC captain and KV store captain
  - Verify the state of the KV store service from Monitoring Console
  - Enable the KV store collection replication

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module 9: Introduction to SmartStore

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Module Objectives

- List the use cases for deploying SmartStore
- Provide a SmartStore architecture overview
- Enable SmartStore in indexer cluster
- Monitor SmartStore status and identify potential issues

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

What is SmartStore and Why Use It?

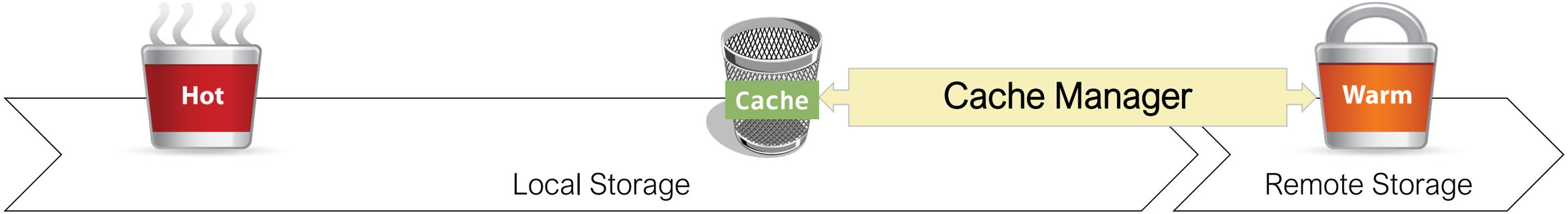
- Scale-out distributed architecture is not a good fit for growing volumes
  - As Splunk deployment and adoption matures, demand for storage outpaces compute resources
  - Adding more peer nodes in response to data growth is expensive
- To scale beyond typical indexer clustering use cases, separating storage from computation resources has benefits
  - Lower cost of data retention
  - Higher reliability
  - Better scalability
- SmartStore is a Splunk indexer capability used to separate the compute resources from storage

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

SmartStore Architecture Overview

- S3-compliant storage
  - https://en.wikipedia.org/wiki/Amazon_S3
  - https://github.com/splunk/s3-tests
- Cache manager
  - **Uploads** warm buckets to a remote storage
  - **Downloads** (fetch) buckets from a remote storage on as needed basis
  - **Evicts** buckets from the local cache based on the bucket's age, search frequency, and other tunable criteria



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Considerations for Moving to SmartStore

- Storage utilization is significantly outpacing other resources
- Considerable amount of admin time is devoted to managing the cluster because the manager node is always busy
  - Bucket fixups, data rebalancing, or software upgrade
- When most searches are over recent data
- NOT beneficial, if you run:
  - Frequent, rare searches with long lookbacks
  - If data is cached, no performance impact
- Latest on restrictions:

  http://docs.splunk.com/Documentation/Splunk/latest/Indexer/AboutSmartStore

NOT SUPPORTED:

- TSIDX reduction
- Data integrity
- Disabling bloom filters
- Custom paths such as **`bloomHomePath`**, **`summaryHomePath`**, **`tstatsHomePath`**, **`coldToFrozenDir`**, etc.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Deploying SmartStore - Requirements

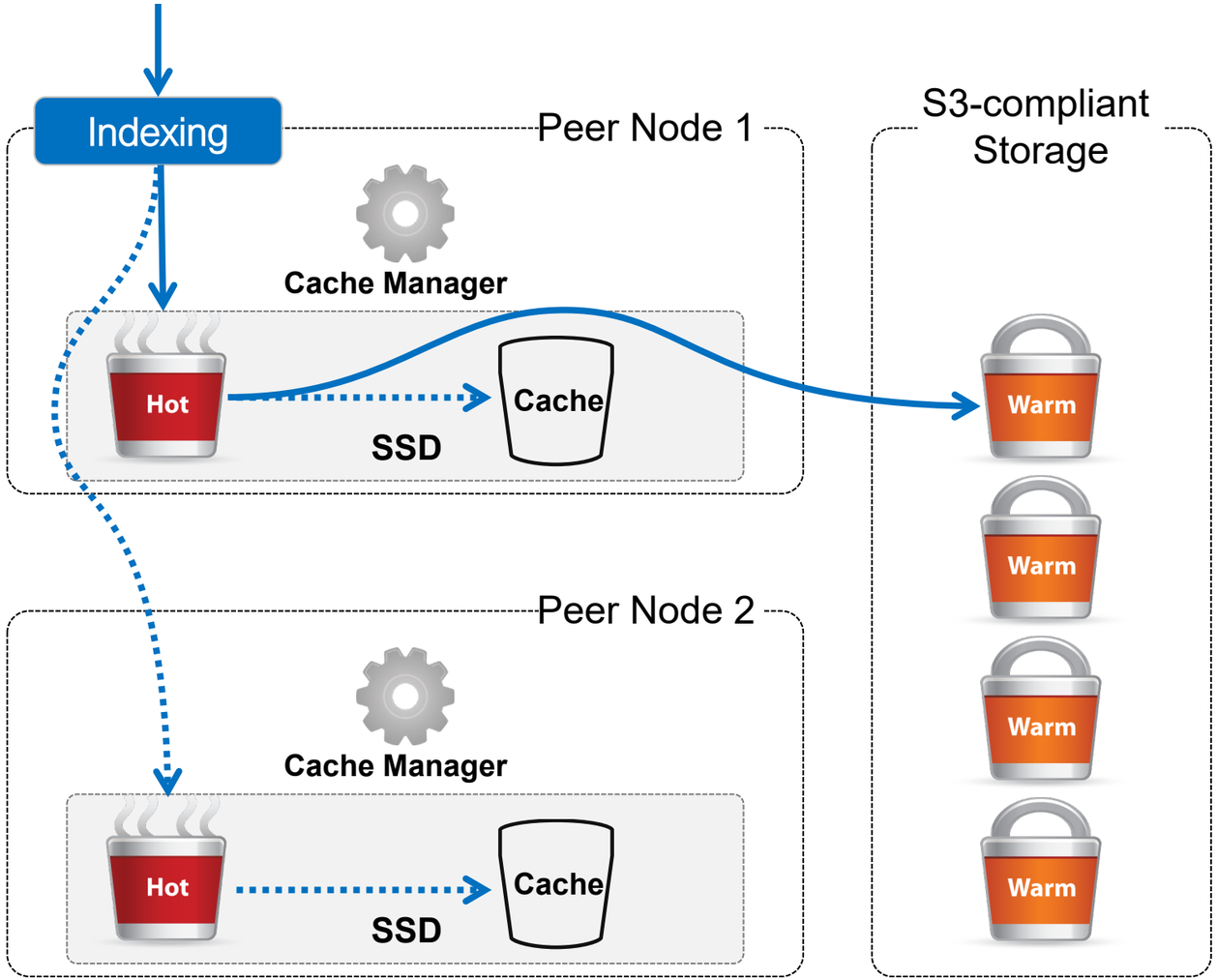
- Same as any Splunk indexer requirements
  - http://docs.splunk.com/Documentation/Splunk/latest/Indexer/Systemrequirements
  - Except, the preferred local storage type is SSD
- Each on-prem machine must run the same Linux 3.x+ 64-bit OS
- For clustering, the peer node configurations must be identical
  - Can configure SmartStore globally or on a per-index basis
  - The local storage on each peer must be in proportion to the eviction policy
    - Recommend to reserve enough storage for a 30-day retention
  - Replication factor and search factor must be equal
    - Only hot buckets follow traditional replication policies
- **`homePath`** and **`coldPath`** must point to the same partition
- Resize **`maxDataSize=auto_high_volume`** to **`auto`**

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

SmartStore Index Time Workflow

1. Data is written to a hot bucket and gets replicated as normal
2. As the bucket rolls into warm (cached), it is uploaded to remote storage
3. Replication of the warm bucket stops
4. After the warm bucket is successfully uploaded to the remote storage, the local bucket is eligible for eviction
5. Buckets freeze directly from warm



Note

When the local warm bucket gets evicted, only the content of the bucket is removed. The bucket directory is empty but not deleted.
The thawed data is stored only locally. The cache manager does not manage it in any way.

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Deploying SmartStore - New

1. Enable a manager for a new indexer cluster
2. Configure the SmartStore settings (no UI)
   - **master-apps/_cluster/local/indexes.conf**
   - Specify the S3 volume and optionally an index
     - An index stanza needs **homePath**, **thawedPath**, and **coldPath** specified
     - The **coldPath** is not used but required
3. Add peer nodes
   - Peers get the master-apps bundles when they join
4. Check the deployment
   - When the cluster is complete, verify the connection from a peer node:

```
splunk cmd splunkd rfs -- ls index:myidx
```

```
[default]
remotePath = volume:s3/$_index_name
repFactor = auto

[volume:s3]
storageType = remote
path = <scheme>://<remote-path>

# S3 example
path = s3://path/to/mysplunk/buckets/
remote.s3.access_key = <S3 access key>
remote.s3.secret_key = <S3 secret key>
remote.s3.endpoint = https://<S3 host>

[myidx]
homePath = $SPLUNK_DB/myidx/db
thawedPath = $SPLUNK_DB/myidx/thaweddb
coldPath = $SPLUNK_DB/myidx/colddb
maxGlobalDataSizeMB =
frozenTimePeriodInSecs =
```

indexes.conf

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

Deploying SmartStore - Migration

- Pre-existing single-site buckets must follow the multisite policy
  - Set **`constrain_singlesite_buckets=false`** in the manager's **server.conf**
- Review the current restrictions and reconfigure all nodes in the cluster to conform to the SmartStore requirements
- Test the SmartStore configurations and remote connectivity
- If the test is successful, apply the bundle from the manager node
  - The manager kicks off the migration but it happens entirely on the peer nodes

  http://docs.splunk.com/Documentation/Splunk/latest/Indexer/MigratetoSmartStore
- SmartStore index conversion can take a long time
  - To monitor the migration process, search on the manager:

```
| rest /services/admin/cacheman/_metrics | fields splunk_server
migration.*
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Deploying SmartStore - Bootstrap

- Bootstrapping fetches buckets present on a remote storage to new node(s)
  - Confirm all buckets are present before bringing down the old node(s)
- To bootstrap, use the same remote storage settings on the new node(s)
- The manager node coordinates a discovery process per index
  1. The manager requests a peer to retrieve a bucket list for a given index
  2. The peer reports back with the bucket list
  3. The manager distributes a set of primaries to fetch across all available peer nodes
  4. Each peer
     - Gets its assigned buckets from the remote storage
     - Recreates bucket's metadata locally and sets it as the primary
     - Replicates only primary's metadata to other peer nodes
  5. Other peers recreate buckets per metadata and report their buckets to the manager as replicated buckets

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Index Retention Policy with SmartStore

- SmartStore indexes do not use the cold buckets
  - Buckets roll to frozen directly from warm
- Data retention is managed cluster-wide
- Attributes affecting the SmartStore data retention:
  - **`maxGlobalDataSizeMB`** (new)
    - Applies to all buckets on a per-index basis and across all peers in the cluster
    - Includes the total size on remote storage plus all warm buckets on all peer nodes to be uploaded to the remote storage
    - Counts only one copy of each bucket
  - **`frozenTimePeriodInSecs`** – behaves same as in non-SmartStore index rolling
  - **`maxGlobalDataSizeMB`** takes precedence over **`frozenTimePeriodInSecs`**
  - The existing **`maxTotalDataSizeMB`** and **`maxWarmDBCount`** settings are ignored
- Freezing removes buckets from both local and remote storages

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved | 25 February 2022

SmartStore Index Freezing Process

- The manager node assigns a freeze job to a peer node that has a local bucket copy
  - Identifies freeze candidates every 15 minutes by default
- The peer node removes the remote bucket first and then the local copy
  - Any buckets participating in a search are forestalled from deletion for up to 5 minutes and then are force-removed
  - Notifies the manager node when the bucket is frozen
- The manager node instructs other peer nodes to delete their local copies
- If you thaw data from an archive, the thawed buckets only exist locally

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

SmartStore Search Considerations

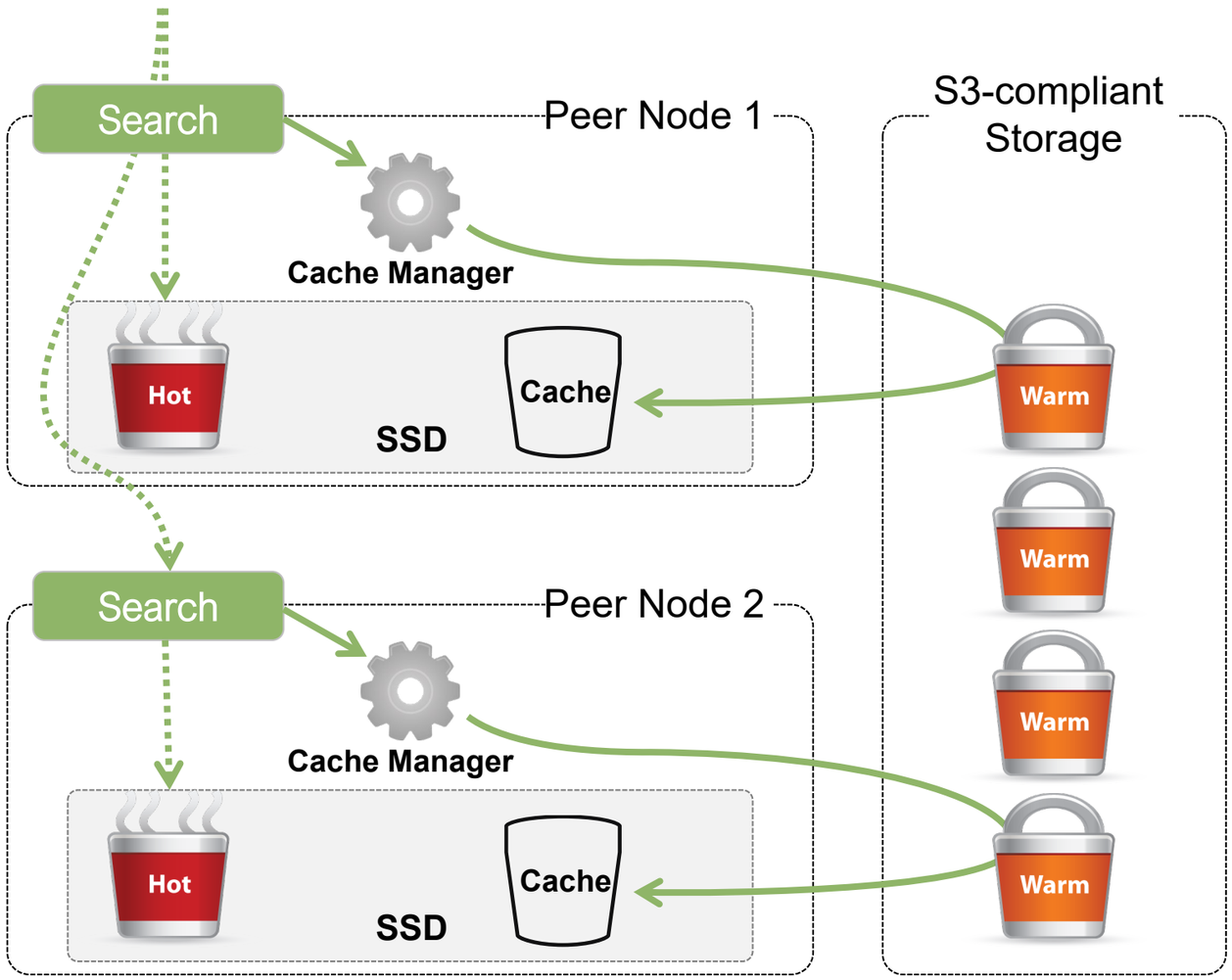
- SmartStore is optimized for certain characteristics of Splunk searches
  - Splunk searches typically occur over near-term data
  - Searches often have spatial and temporal locality
- The searches always occur in local storage
  - The cache manager favors recently created and accessed buckets
  - The cache manager directs fetching and eviction of buckets
  - Cached buckets searched infrequently will likely get evicted
- Only the primary hot buckets participate in a search
- Only the primary buckets from a designated peer node are fetched and accessed locally

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Basic SmartStore Search-Time Workflow

1. SH dispatches a job to search peers
2. Peers spawn search processes and read a bucket list
3. Each search process searches only the "opened" buckets
   - Not all searches require the entire content
   - Fetches bucket files on as needed basis
   - A bucket is "opened" only when it is available locally
   - The cache manager blocks the process until a bucket is "opened"
   - Hot buckets are always "opened"
4. When the search is done, buckets are "closed" and they are eligible for eviction



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

More SmartStore Search-Time Workflow

- Summarization
  - Search head dispatches summary jobs to peer nodes
  - The peer generating the summary uploads its summary buckets
  - When a search needs the summary, the cache manager opens the summarized bucket
  - Ad-hoc summaries are not uploaded to the remote storage
- **`|delete`**
  - The primaries delete the events locally
  - Cache manager syncs the delete journals in the remote storage
- When a peer fails, SmartStore bucket fixup is basically the same as the classic
  - If still in valid state, a fixup replicates only bucket's metadata (faster recovery)
  - If not valid, the manager invalidates the current bucket list and assigns a peer to fetch and re-generates the list

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Cache Size Settings

- Buckets get evicted only when *the cache manager thinks the host is facing space constraints*
  - Hot buckets are always local and do not get evicted
  - The warm buckets continue to reside in remote storage
- The cache size settings apply on the peer (indexer-wide)

server.conf

```
[diskUsage]
minFreeSpace = 5000
[cachemanager]
eviction_policy = lru
eviction_padding = 5120
max_cache_size = 0
```

- The cache manager consumes all free partition space until the free space is less than the total padding size

  Total padding = **`minFreeSpace`** + **`eviction_padding`** (10 GB by default)

- To limit the cache size, additionally set the **`max_cache_size`** setting

http://docs.splunk.com/Documentation/Splunk/latest/Indexer/ConfigureSmartStorecachemanager

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

SmartStore Eviction Policy

- The **`eviction_policy`** setting in **server.conf** and associated parameters determine the eviction priority
  - **`lru`** (default) – evict the least recently used bucket
    - Do not change this default without consulting Splunk Support
  - Rawdata and TSIDX get evicted before metadata
- To protect critical data from eviction, you can enhance the policy:
  - **`hotlist_recency_secs`** – the default keeps the buckets containing events from the last 24 hours
  - **`hotlist_bloom_filter_recency_hours`** – the default keeps the bucket metadata (bloomfilter) for the last 15 days
- Can apply globally (server.conf) or on a per-index level (indexes.conf)

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Notable SmartStore Log Channels

- splunkd.log
  - **`CacheManager`**, **`CacheManagerHandler`** – remote storage activities (INFO)
  - **`S3Client`**, **`CacheManagerEviction`**, **`StorageInterface`** (WARN)
- search.log on peer nodes
  - **`CacheManagerHandler`** – the cache manager bucket operations
  - **`S2BucketCache`** – search-time bucket management (bucket open/close)
- audit.log –bucket upload, download, eviction, and removal events
- metrics.log – metrics for remote storage operations

```
index=_internal metrics group IN(cachemgr*, spacemgr)
```

- splunkd_access.log – records the cache manager calls from searches

```
index=_internal sourcetype=splunkd_access
uri_path="/services/admin/cacheman*"
```

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Monitoring Console – SmartStore

- Per instance and deployment-wide SmartStore activity information
  - Remote storage connectivity
  - Cache hits and misses
  - Bucket upload and download
  - Cache thrashing
  - Migration process
  - Bootstrapping progress

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Further Reading: Splunk SmartStore

- About SmartStore

  http://docs.splunk.com/Documentation/Splunk/latest/Indexer/AboutSmartStore

- How SmartStore works

  http://docs.splunk.com/Documentation/Splunk/latest/Indexer/SmartStoresearching

- Troubleshoot SmartStore

  http://docs.splunk.com/Documentation/Splunk/latest/Indexer/TroubleshootSmartStore

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Lab Exercise 9 – Migrate a Cluster to SmartStore

- **Time**: 25 minutes
- **Tasks**:
  - Verify the SmartStore connectivity from a test instance
  - Test the SmartStore configuration on a test instance
  - Upgrade the indexer cluster to meet the SmartStore prerequisites
  - Configure and deploy the SmartStore bundle to peer nodes
  - Validate the SmartStore-enabled cluster

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

Course Wrap-up

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

What's Next?

- Splunk Certification program
  https://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
  - https://www.splunk.com/pdfs/training/Splunk-Certification-Candidate-Handbook.pdf
- Exam registration
  - https://www.splunk.com/pdfs/training/Exam-Registration-Tutorial.pdf

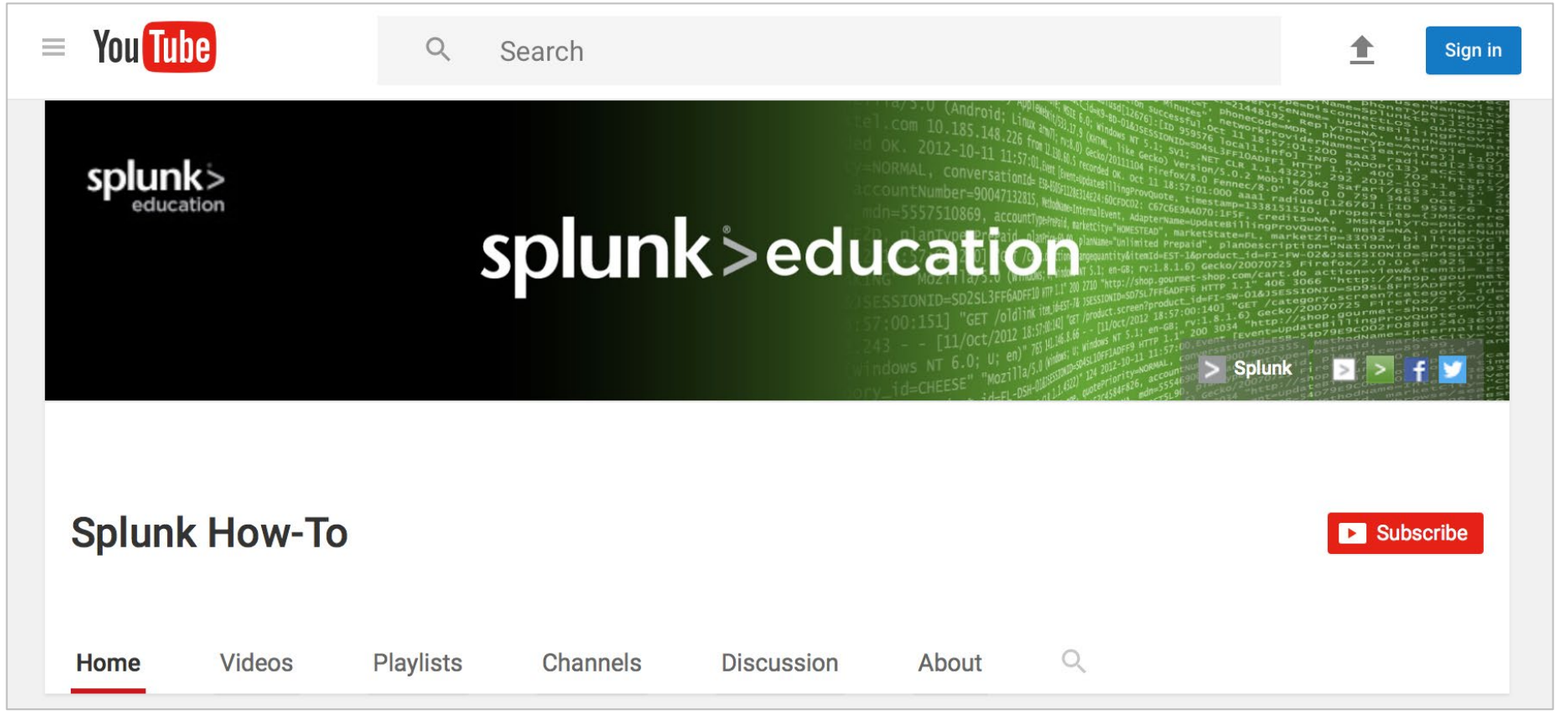
- If you have further questions, send an email to: certification@splunk.com

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

YouTube: The Splunk How-To Channel

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



Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution

Copyright © 2022 Splunk, Inc. All rights reserved

.conf22

splunk>

MGM Grand, Las Vegas, NV | June 13–16
Virtual | June 14–15

Join us for a hybrid experience and learn why data is key to achieving better outcomes.

“ .conf21 gave me the ability to immerse myself in all things Splunk for two full days, I learned so much.”

— John Whitefield
Progressive Insurance, IT DevOps Eng, Senior

Generated for Muruganantham Pothanaickar (muruganantham.pothanaickar@bakerhughes.com) (C) Splunk Inc, not for distribution