Making sure your clustered environment is NOT a total mess

Michael Gilliam
Rana Nujaidi

Saudi Aramco

October 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Our Speakers

MICHAEL GILLIAM

Saudi Aramco, Security Specialist

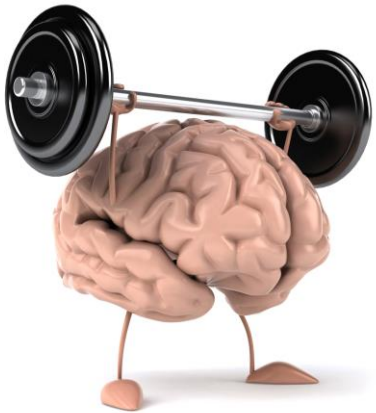
RANA NUJAIDI

Saudi Aramco, Security Specialist

What you will learn

After This Session

- What are the different types of clusters
- Purpose and advantages of each
- Best practices to ensure availability and accuracy
- Reasons for mistakes and how to avoid them



Quick Overview

Michael Gilliam

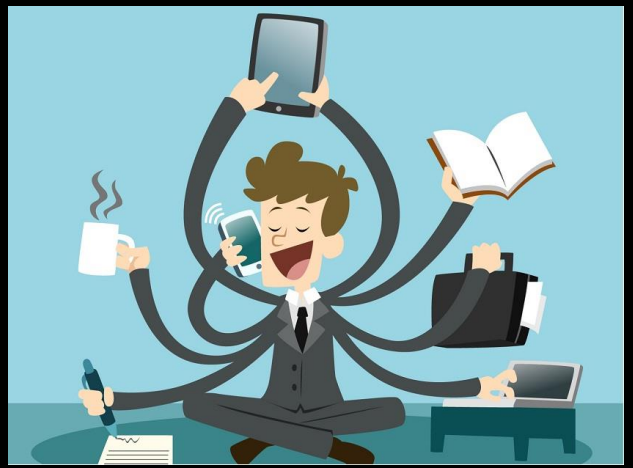
splunk> .conf18

Types of Management Components

- The license master handles Splunk Enterprise licensing.
- The monitoring console performs centralized monitoring of the entire deployment.
- The deployment server updates configurations and distributes apps to processing components, primarily forwarders.
- The indexer cluster master node, sometimes referred to as the "cluster master", coordinates the activities of an indexer cluster. It also handles updates for indexer clusters.
- The search head cluster deployer handles updates for search head clusters.

Job(s) of Splunk Software

- The same software can be search head, indexer, deployer, license manager,
  - The stanza configuration determines the functions and capabilities



Distributed Deployment Components

Component	LM	MC	DS	CM	Deployer	Indexer	Search head
License master	-	Y	Y	Y	Y	Y	Y
Monitoring Console	Y	-	Y	Y	Y	N	Y
Deployment Server	Y	Y	-	N	Y	Y	Y
Indexer Cluster Master Node	Y	Y	N	-	Y	N	N
Search Cluster Deployer	Y	Y	Y	Y	-	N	N

Key: "LM" = license master "MC" = monitoring console
"DS" = deployment server "CM" = cluster master

Cluster Master

Rana Nujaidi

splunk> .conf18

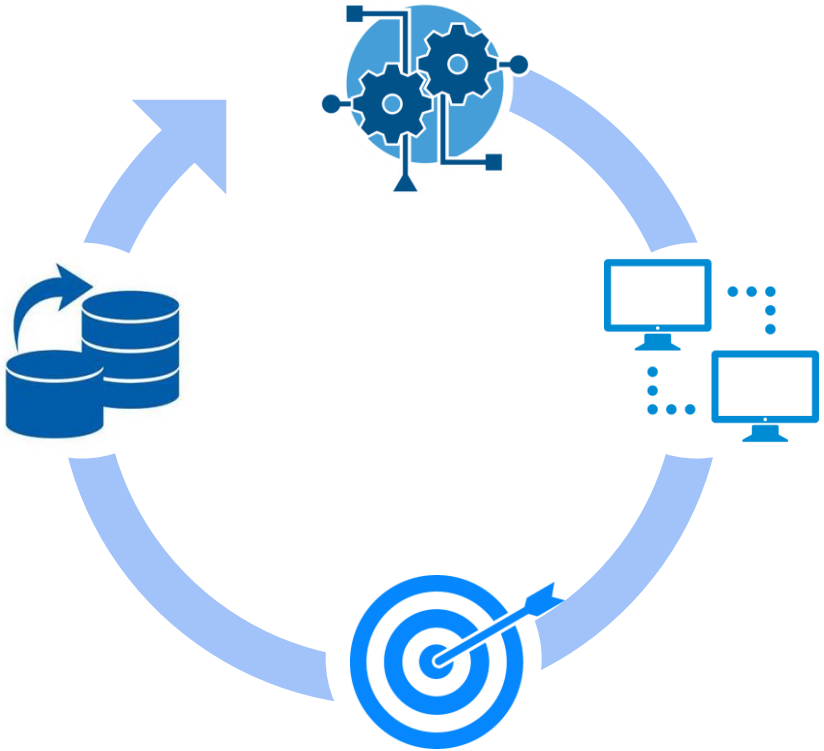
What is Cluster Master?

- A Cluster Master manages a cluster of indexers which can indexes multiple copies of the data

Explaining What It Does

- The Cluster Master coordinates the activities of the peer nodes.a
  - Peer nodes' configuration
  - Replication Activity
  - Search head direction to peer nodes
  - Peer nodes status Monitoring

Bundle Replication



Bundle Importance

What can go wrong

1. Broken Buckets
2. Cluster Master Failure
3. Misconfigured Bundles

Broken Buckets

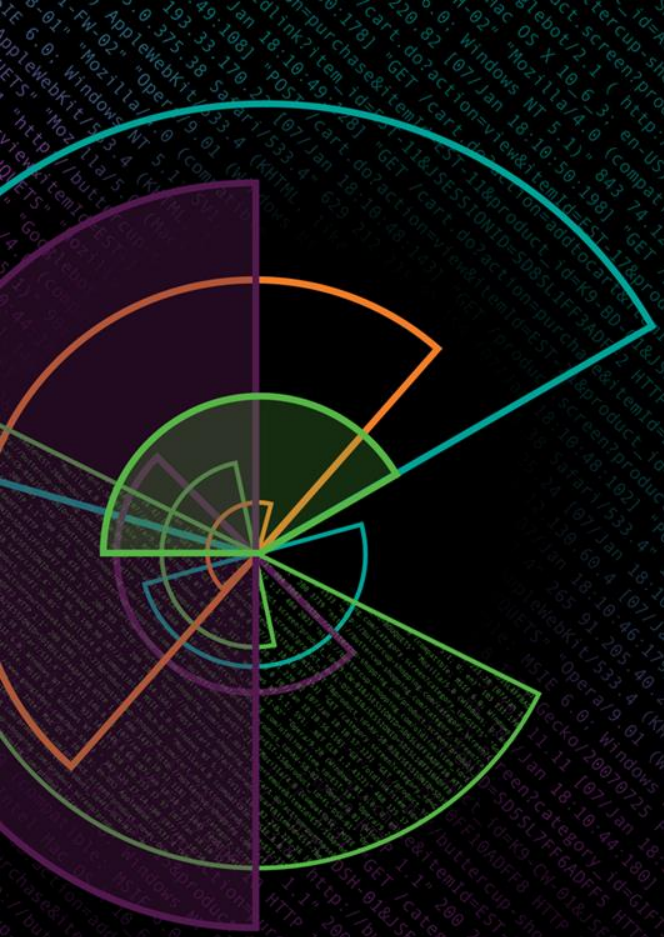
- Storage disconnection
- Indexer failure
- Network interruption

Cluster Master Fail

- Server error
- Network interruption
- Server Failure

Misconfigured Bundles

- Misconfiguration
- Bundle Push



Deployer

Michael Gilliam

splunk> .conf18

The purpose

Why is it necessary?

- Distribute apps to cluster members
  - It handles migration of app and user configurations into the search head cluster from non-cluster instances and search head pools.
  - It deploys baseline app configurations to search head cluster members.
  - It provides the means to distribute non-replicated, non-runtime configuration updates to all search head cluster members.

The deployer is not a search head cluster member

What Can It Do?

- New or upgraded apps.
- Configuration files that you edit directly.
- All non-search-related updates, even those that can be configured through the CLI or Splunk Web, such as updates to indexes.conf or inputs.conf.
- Settings that need to be migrated from a standalone search head. These can be app or user settings.

So What Could Possibly Go Wrong?

- Updates from the GUI are stored in local, so always will take precedence
- Unique names are necessary
- The bundle must contain **ALL** the apps to be deployed
  - If the state must be enabled in app.conf for the app to be removed
- User attributes cannot overwrite already existing system settings
- When the election process fails
  - (talking about Splunk here, not presidential elections)
- Trouble shooting heart beat failures
  - How to detect them.
  - Why they may happen
  - How to fix them.

Key requirements

- Each member must run on it’s own machine, or virtual machine
- All machines must run the same operating system
- All members must run the same version of Splunk
- All members must be connected to a network
- The deployment must be the replication factor or three, whichever is greater

Deployer should never be used to perform production searches

Deployment Server

Rana Nujaidi

splunk> .conf18

Who & what does it control?

- A deployment server distributes configuration to deployment clients, who can be universal/heavy forwarders, indexers, or search heads
- It controls the configuration for deployment clients through server classes

What should be done?

- Change the phonehome default settings
  - You don’t need to communicate with your forwarders all the time
- CAREFUL with the number of connected deployment clients
- Don’t take advantage of “reload” command
- Ship your logs directly to Indexers (why bother the heavy forwarders)

Upgrading Process

Michael Gilliam

splunk> .conf18

The situation

Don’t make assumptions

1. Operating system *nix
2. Do not have root access
   - So cannot just install binary
3. Window manager such as GNU Screen
4. All devices have the same install script
5. Splunk install file saved same location

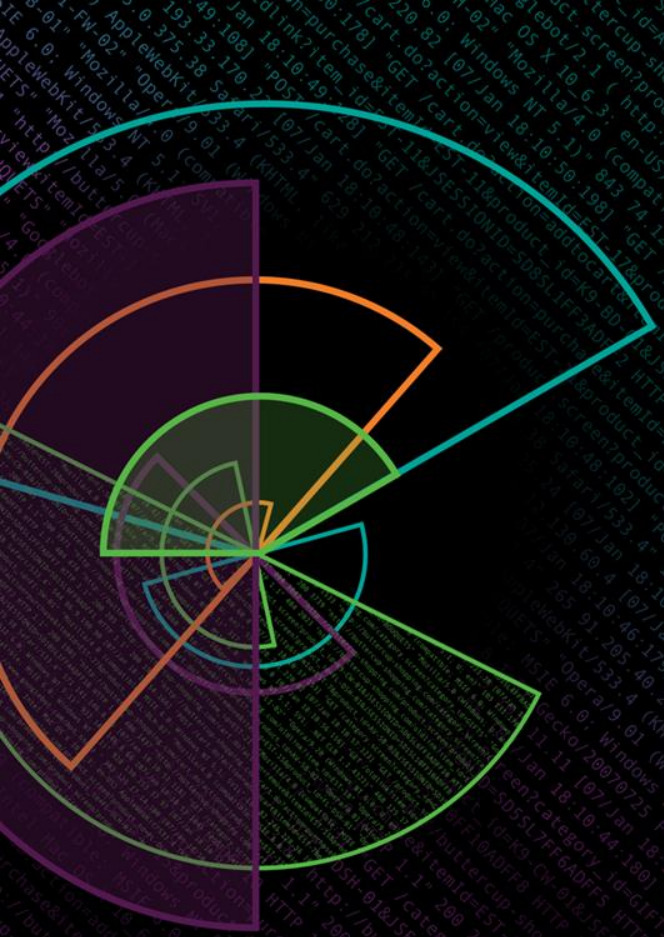
One method for getting the file distributed

- Upload info
- Retrieve instructions
- Download Splunk
- Save locally

Now all at once

Proper preparation, reduce execution

- Login to half the servers
  - Indexers need maintenance mode
- Shutdown Splunk
- Run install script
  - Verifies Splunk down
    - Stop the Splunk if necessary
    - Verify $SPLUNK_HOME
    - Extract the files
    - Start Splunk, accept license
    - Report Splunk status



Security & Performance

Rana Nujaidi

splunk> .conf18

Being secure without impacting operations

- Importance of setting different password
- Changing port number for additional security
- Consider configuring using SSL
  - The configuration and possible complications
  - Troubleshooting SSL problems

Finding what's bad

- Identify the corrupted bucket,
  - If it's a main buckets, GOOD LUCK with repair
  - If it's a backup buckets, a simple delete command

Fixing corrupt buckets

- Be lazy
  - wait for an error to occur
- Be Proactive
  - Run a monthly search to verify the health of the buckets

Commands to locate

1. From the clustermaster interface:

| dbinspect index=<index> index=<index> host=* corruptonly=true
| streamstats count BY bucketId

2. Identify the corrupted buckets

Syntax to fix the problem(s)

3. switch the cluster master to maintenance mode
4. offline the peer with corrupted bucket
    a. if corrupted bucket is backup copy: simply delete
    b. if corrupted bucket is main copy:

```
$SPLUNK_HOME/bin/splunk fsck \
repair --all-buckets-one-index \
--index-name=<index>
```

Parallelization

- Batch mode search parallelization
  - Additional search pipelines
- Parallelization summarization for data models
  - Concurrent data model acceleration searches
- Parallel summarization for report acceleration
  - Concurrent report acceleration searches
- Index parallelization
  - Concurrent data processing pipelines on indexers and forwarders

Batch Mode Search Parrelization

- Return event data by bucket
- By increasing batch search pipelines,
- → speeding the return of search results

Data Model accelerations

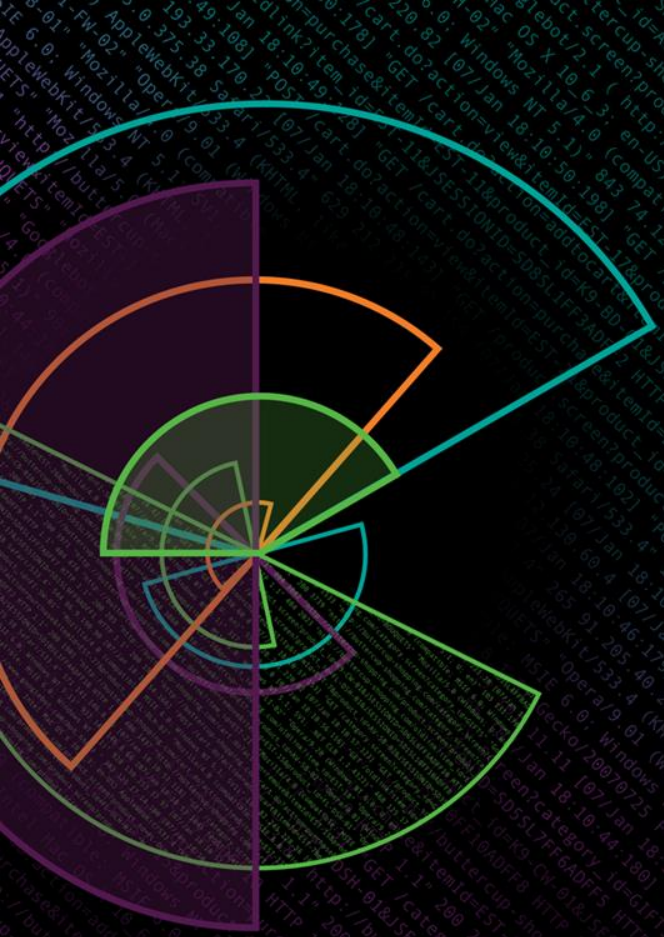
- By increasing the number of scheduled acceleration searches per datamodel → increase of IO, processing, and memory used on every indexer.

Report accelerations

- By increasing the number of scheduled acceleration searches per report
  → increase of IO, processing, and memory used on every indexer.

Index Parallelization

- By increasing the parallelization to 2 → use additional 4-6 CPU cores, and requires 300-400 IOPS to maintain indexing throughput on every indexer → fewer CPU cores available for search processing



Putting it all together

Michael Gilliam

splunk> .conf18

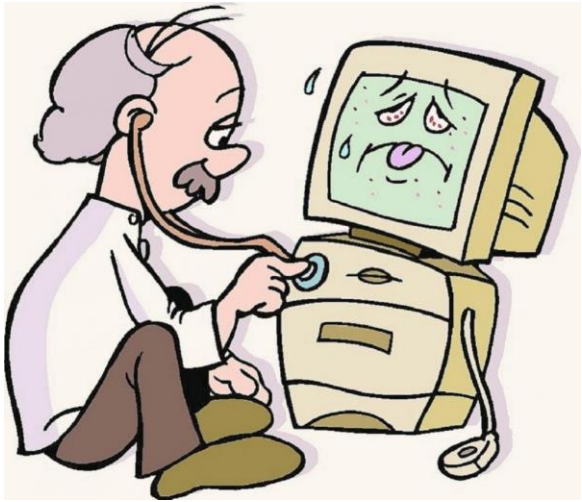
Be prepared

Standby

- Cluster master
- Deployer
- License master
- Deployment server (good luck with redirecting all forwarders to the new server)

Cold Standby

- Wait till you get an issue
- Requires additional server
- Restore the files from backup
- Takes the most time to implement
  - No external modifications



Warm Standby

Exact Copy

- Have a duplicate server
- Monitor the files on the master
- Copy the updated files from Active
- Failover → assign master's ip
  - Faster than cold

Warm Standby

Impersonating the original

- Control access with either DNS or load-balancer
- Copy the files across both servers
- Assign a server as master
- Failover → Activate standby server

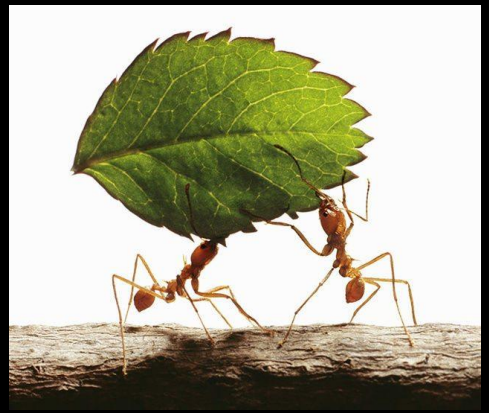
Warm Standby

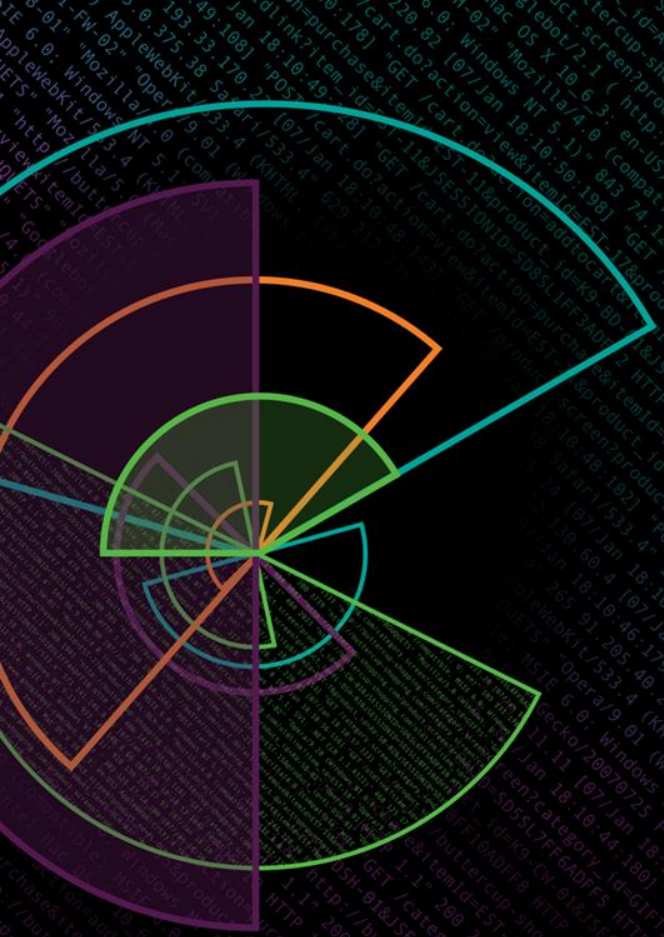
Reconfiguring everyone else

- Have a duplicate server
- Copy the updated files from master
- Monitor files on the master
  - Make the necessary changes
- Failover →configure infrastructure to new master

Things to keep in mind

- Multiple clusters does not have to be tedious
- Proper planning + Successful implementation = FUN
- It’s possible to increase assets without adding manpower, when done correctly





Q&A

Rana Nujaidi

Michael Gilliam

Thank You

Don't forget to rate this session in the .conf18 mobile app