splunk> .conf2017

Splunk Data Lifecycle

Determining When And Where To Roll Data

Jeff Champagne | Splunk Staff Architect

September 27, 2017 | Washington, DC

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.

splunk> .conf2017

Who's This Dude?

Jeff Champagne

jchampagne@splunk.com
Staff Architect

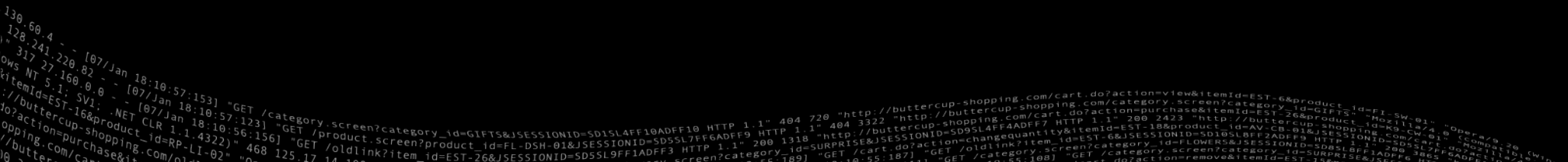
- Started with Splunk in the fall of 2014
- Former Splunk customer in the Financial Services Industry
- Lived previous lives as a Systems Administrator, Engineer, and Architect
- Loves Skiing, traveling, photography, and a good Sazerac

Am I In The Right Place?

You'll find this session helpful if…

Target Audience: Splunk Admins

- You should have *some* experience administering Splunk
  - It's okay if you're a n00b
- Questions you might have…
  - How should I setup my storage strategy?
  - How can I keep my data longer without using as much disk space?
  - Are there ways to archive my data?
  - Can I do things to improve search performance?

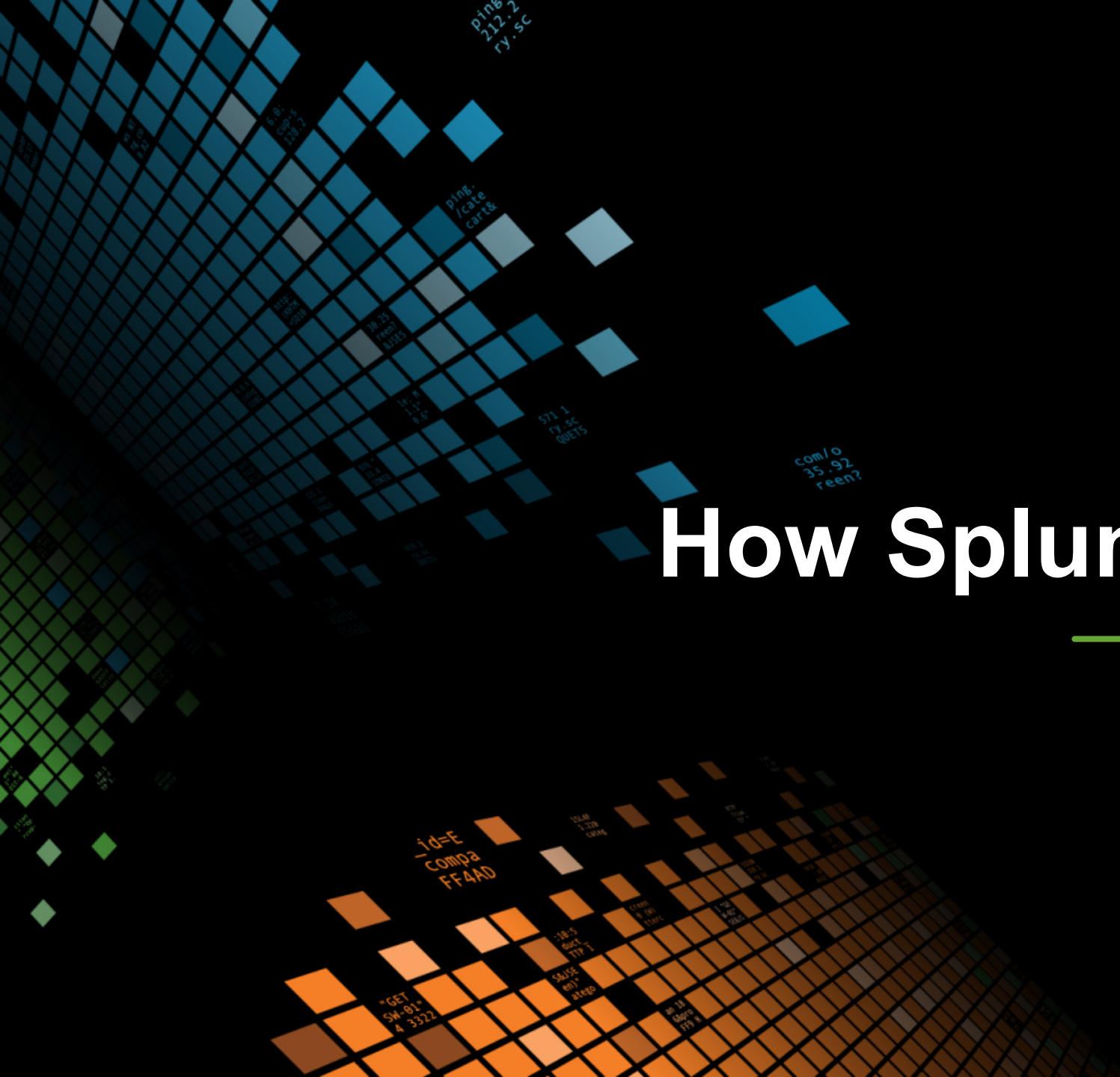


What Will I Learn?

Agenda

- Brief Explanation: How Splunk stores data
- Bucket Rolling
  - Hot/Warm
  - Cold
  - Frozen / Delete / Thawing
- Archiving: Data Roll
- Storage Savings: TSIDX Reduce
- Managing Retention
- Impact of Index Clustering
- Data Model Accelerations

splunk> .conf2017



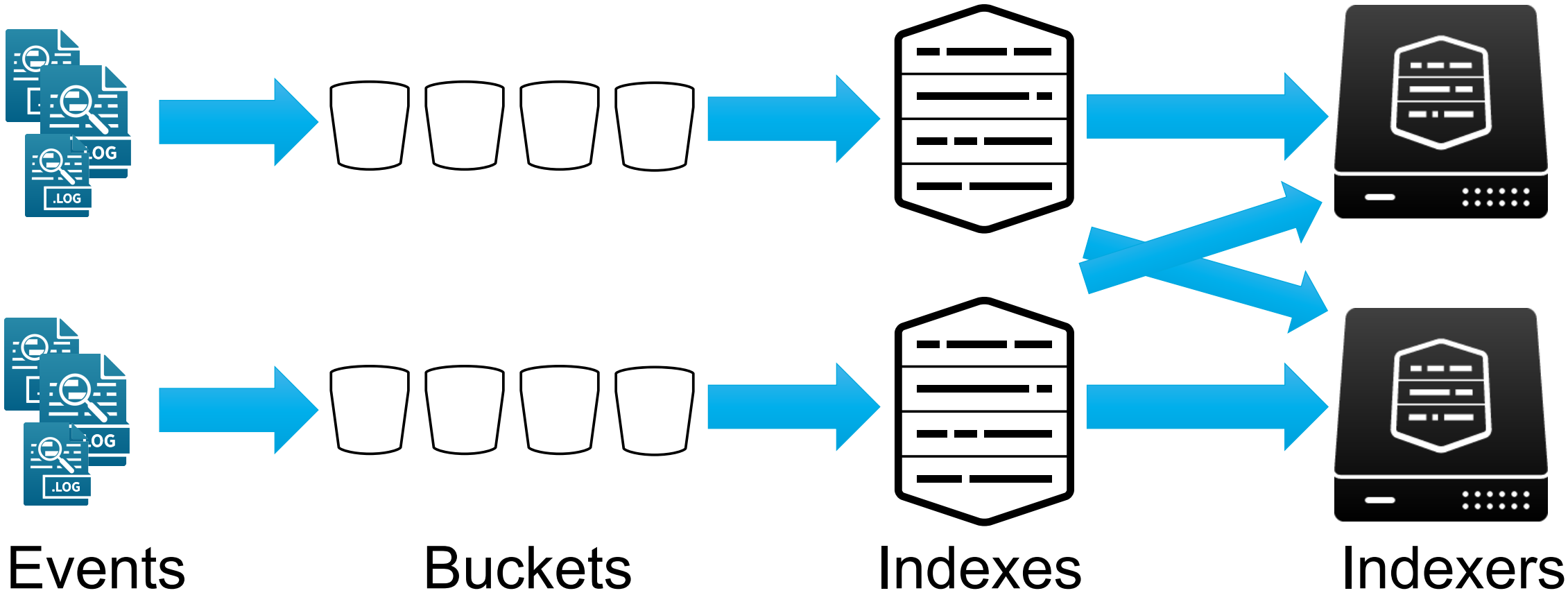
How Splunk Stores Data

A Primer…

splunk> .conf2017

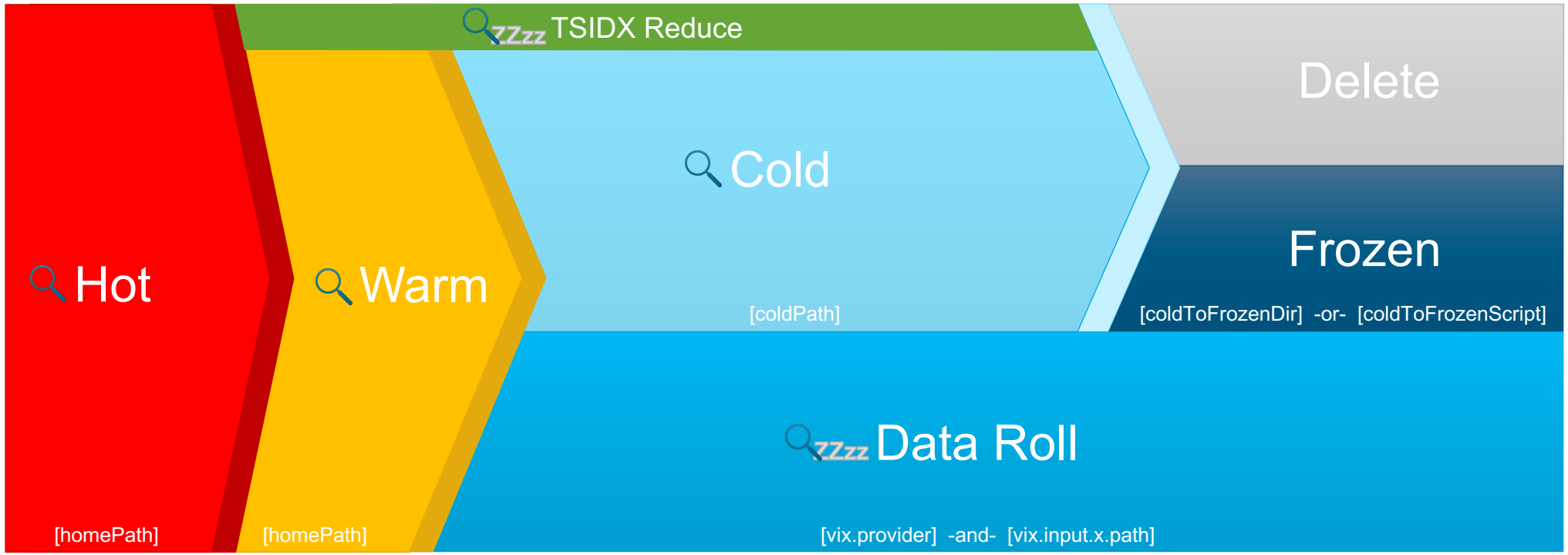
How Are Events Stored?

Buckets, Indexes, and Indexers



How Are Events Stored?

We've got options…

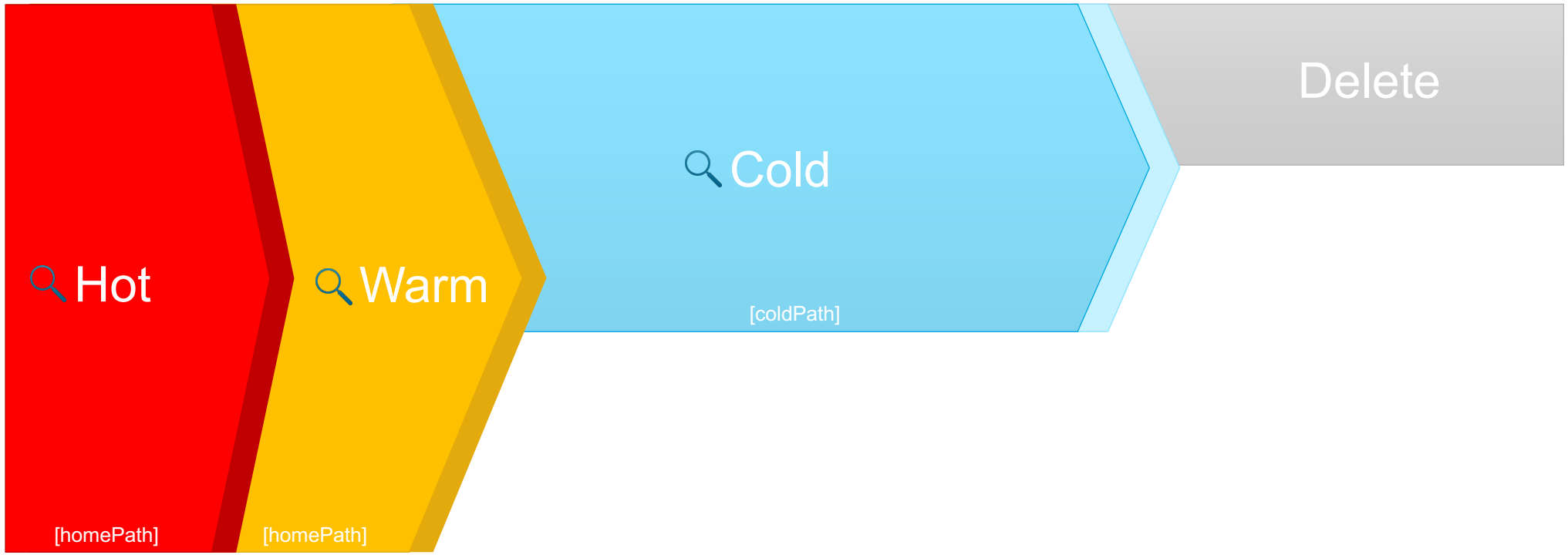


Searchable

Searchable
(but slower)

How Are Events Stored?

What's enabled out of the box?



Searchable

Hot/Warm Storage

I'm too hot (hot damn)

Make a dragon wanna retire man

splunk> .conf2017

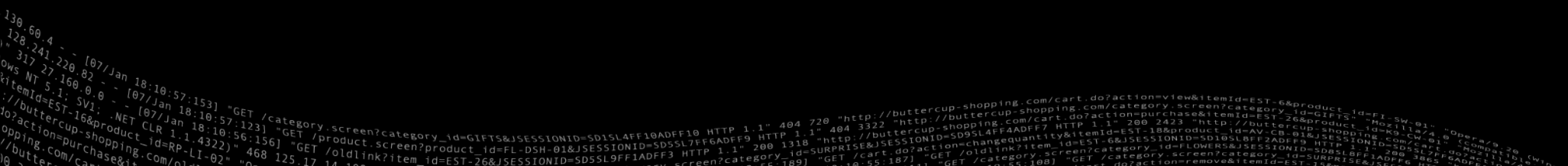
Hot/Warm Storage

How is it used?

- New data lives here
  - Hot & Warm buckets

Conf File	indexes.conf
Parameter	[<index name>] homePath = $SPLUNK_DB/$_index_name/db

- At least 1 hot bucket per index, per indexer
  - Additional hot buckets will be created…
    - For each parallel ingestion pipeline
    - When quarantine buckets are needed



splunk> .conf2017

Hot/Warm Storage

How is it used?

- Buckets roll from Hot to Warm when…
  - We get too many hot buckets [maxHotBuckets]

You don't typically need to edit the following ones…

  - DON'T UNLESS YOU'RE TOLD TO
  - The timespan of a bucket gets too large
  - A hot bucket hasn't received data in a while
  - Bucket metadata files have grown too large
  - There is an index clustering replication error

Conf File	indexes.conf
Parameter	[<index name>] maxHotBuckets = 3 maxHotSpanSecs = 7776000 (90 days) maxHotIdleSecs = 0 (disabled) maxMetaEntries = 1000000 (1M lines)

splunk> .conf2017

Hot/Warm Storage

Requirements

800+

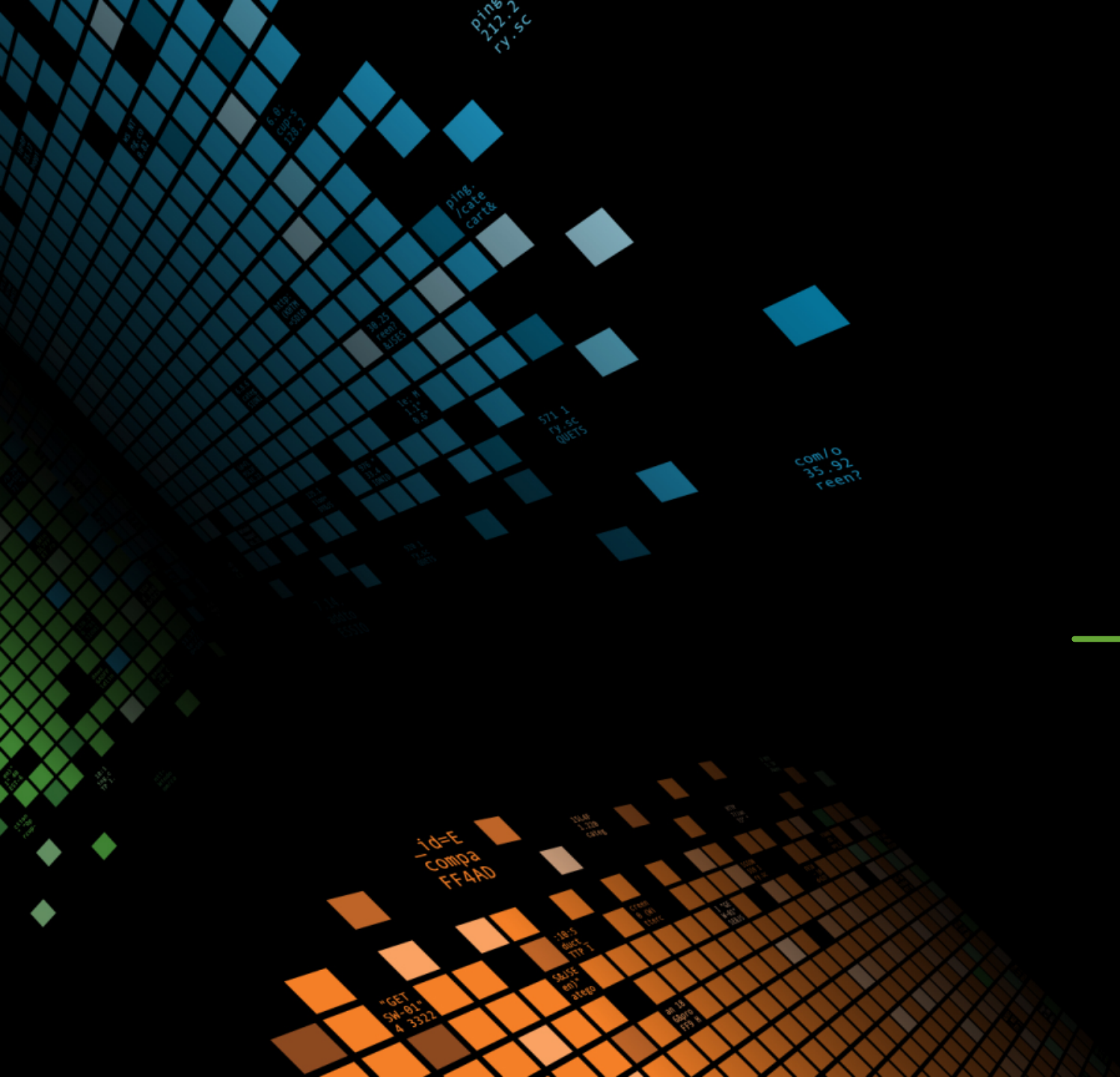
IOPS

splunk> .conf2017

Hot/Warm Storage

I/O Requirements

- IOPS
  - 800+ IOPS for Standard Workloads
  - 1200+ IOPS for Heavy Workloads
    - Enterprise Security
    - High search concurrency
  - Do yourself a favor and use SSD
- Sustained I/O per indexer simultaneously
  - All indexers search at the same time
  - Important if you're using a SAN
- Measured using Bonnie++
  - IOPS = Random Seeks
  - *nix only (sorry Windows)
  - New test suite is coming
  - There's an app for that: https://splunkbase.splunk.com/app/3002/
- Block Storage
  - We DO NOT support NFS/NAS for Hot/Warm volumes
    - Common filesystems: EXT4 or XFS



Cold Storage

Champagne on Ice

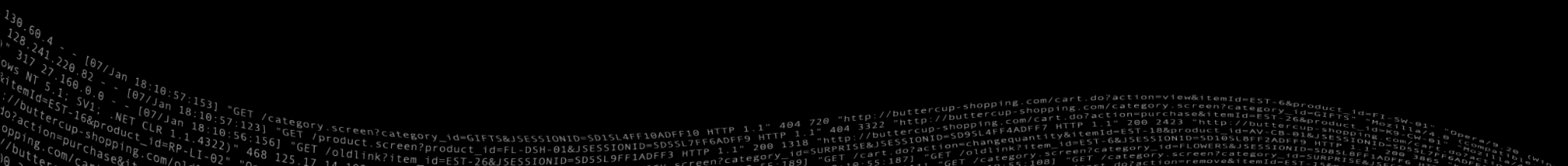
splunk> .conf2017

Cold Storage

How is it used?

- Historical data goes here
  - Cold buckets
- Allows older data to be kept on slower (cheaper) storage
  - Older events are typically searched less often
  - Slower performance may be more acceptable
- Buckets roll from Warm to Cold when…
  - We have too many Warm buckets

Conf File	indexes.conf
Parameter	[<index name>] coldPath = $SPLUNK_DB/$_index_name/colddb maxWarmDBCount = 300



Cold Storage

Requirements

- IO Performance
  - Lower IOPS can be tolerated with the expectation of slower search

Don’t go below 350 IOPS

  - Remember: Sustained IO across all indexers
- Additional storage platforms are supported
  - NAS/NFS

Frozen Storage

Let it go, let it go…

splunk> .conf2017

Frozen Storage

Ice Ice, Baby

- No longer searchable
  - Keep data in Cold as long as you can
- Data rolls from Cold to Frozen when…
  - The total size of the index (Hot+Warm+Cold) grows too large
  - The oldest event in a bucket exceeds a specific age
- Default freezing process
  - TSIDX file is removed
  - Bucket is copied to a destination you specify
  - Splunk no longer manages the data – You're in charge!
- Custom freezing process
  - You provide a custom script

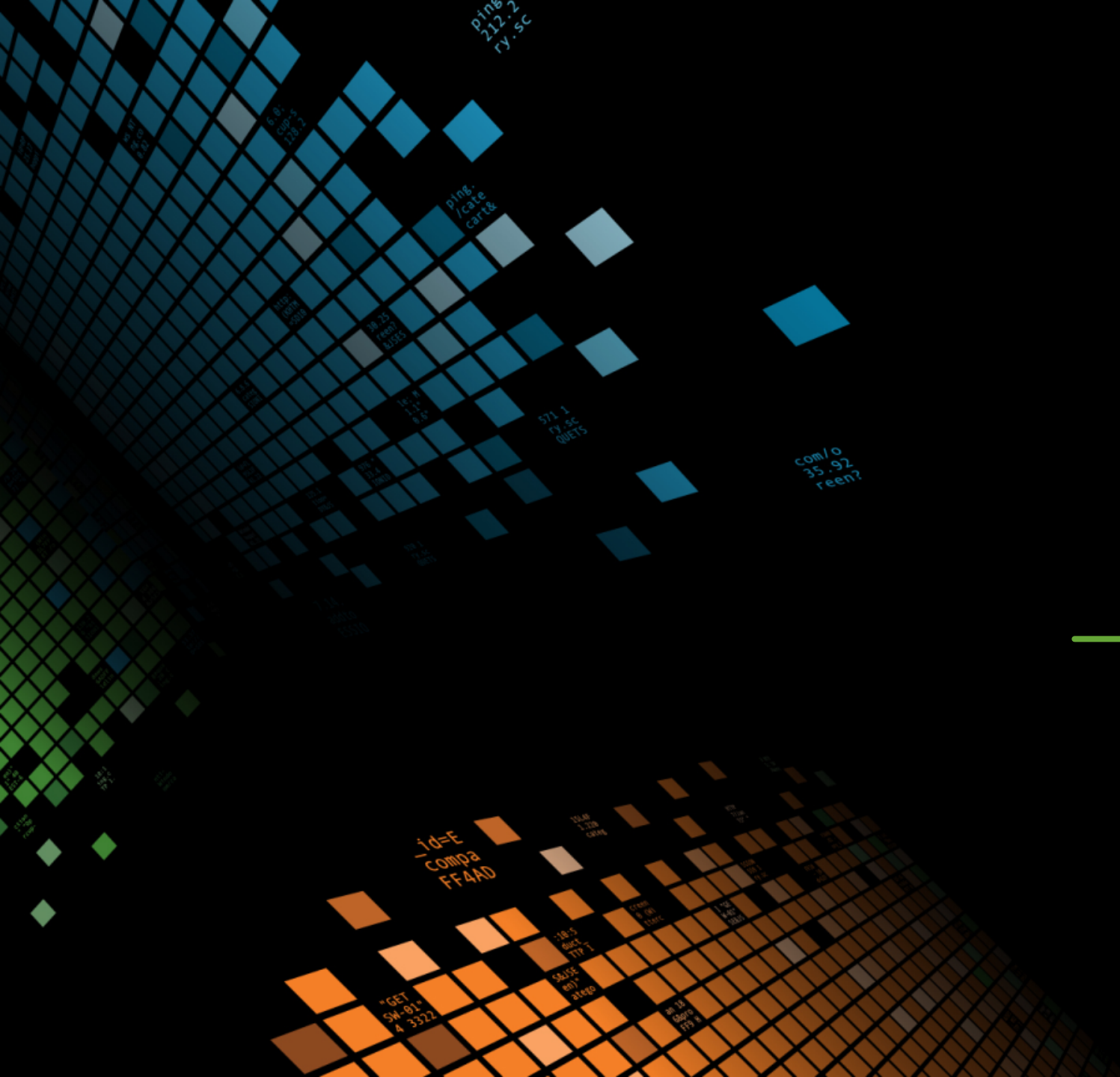
Conf File	indexes.conf
Parameter	[<index name>] maxTotalDataSizeMB = frozenTimePeriodInSecs = coldToFrozenDir = coldToFrozenScript = thawedPath =

splunk> .conf2017

Thawing Data

Bringing data back from the deep freeze

- Manual Process
  - Copy frozen buckets to thawed path [thawedPath]
  - Use the rebuild command to re-index the data
    - CLI command
  - http://docs.splunk.com/Documentation/Splunk/latest/Indexer/Restorearchiveddata
- Re-Indexing
  - Does not count against your license
  - Takes time
    - Use the same estimates for indexing new data
    - Example: A reference indexer can index 300GB/day



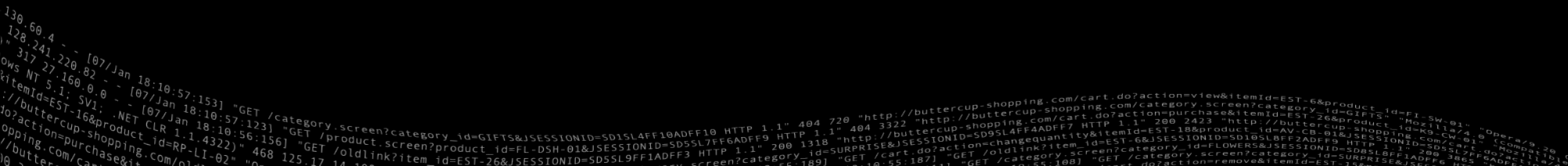
Delete

Lets just dump it all…

Delete

When do we delete?

- If don't setup freezing, we will delete
  - [coldToFrozenDir]
  - [coldToFrozenScript]
- Data is deleted when…
  - The total size of the index (Hot+Warm+Cold) grows too large [maxTotalDataSizeMB]
  - The oldest event in a bucket exceeds a specific age [frozenTimePeriodInSecs]



splunk> .conf2017

Splunk Data Roll

Rollin' Rollin' Rollin'

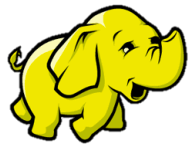
Keep Those Buckets Rollin'

splunk> .conf2017

Splunk Data Roll

How does this work?

- Enabled per index
  - Doesn't have to be all or nothing
- Buckets are archived to HDFS once the oldest event reaches a specific age
  - vix.output.buckets.older.than = <*seconds*>
  - Hadoop and AWS EMR+S3 are supported
- Virtual indexes are created to reference the archived data
  - Unified search can seamlessly search across native and virtual indexes
    - vix.unified.search.cutoff_sec = <*seconds*>
  - Some overlap between what is stored in Splunk & HDFS
    - Data is still searchable while archiving
    - Unified search ensures no duplicate results



HDFS

EMR + S3

splunk> .conf2017

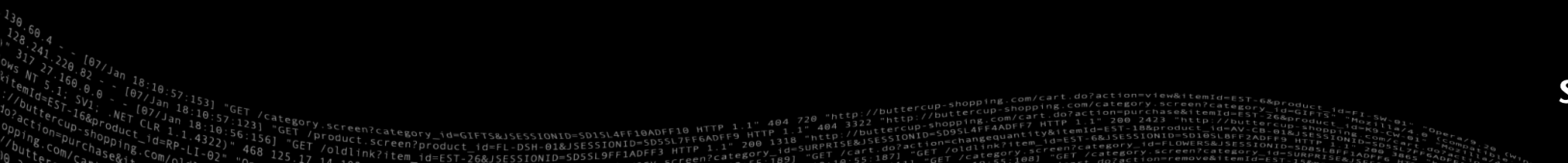
Splunk Data Roll

When would I use this?

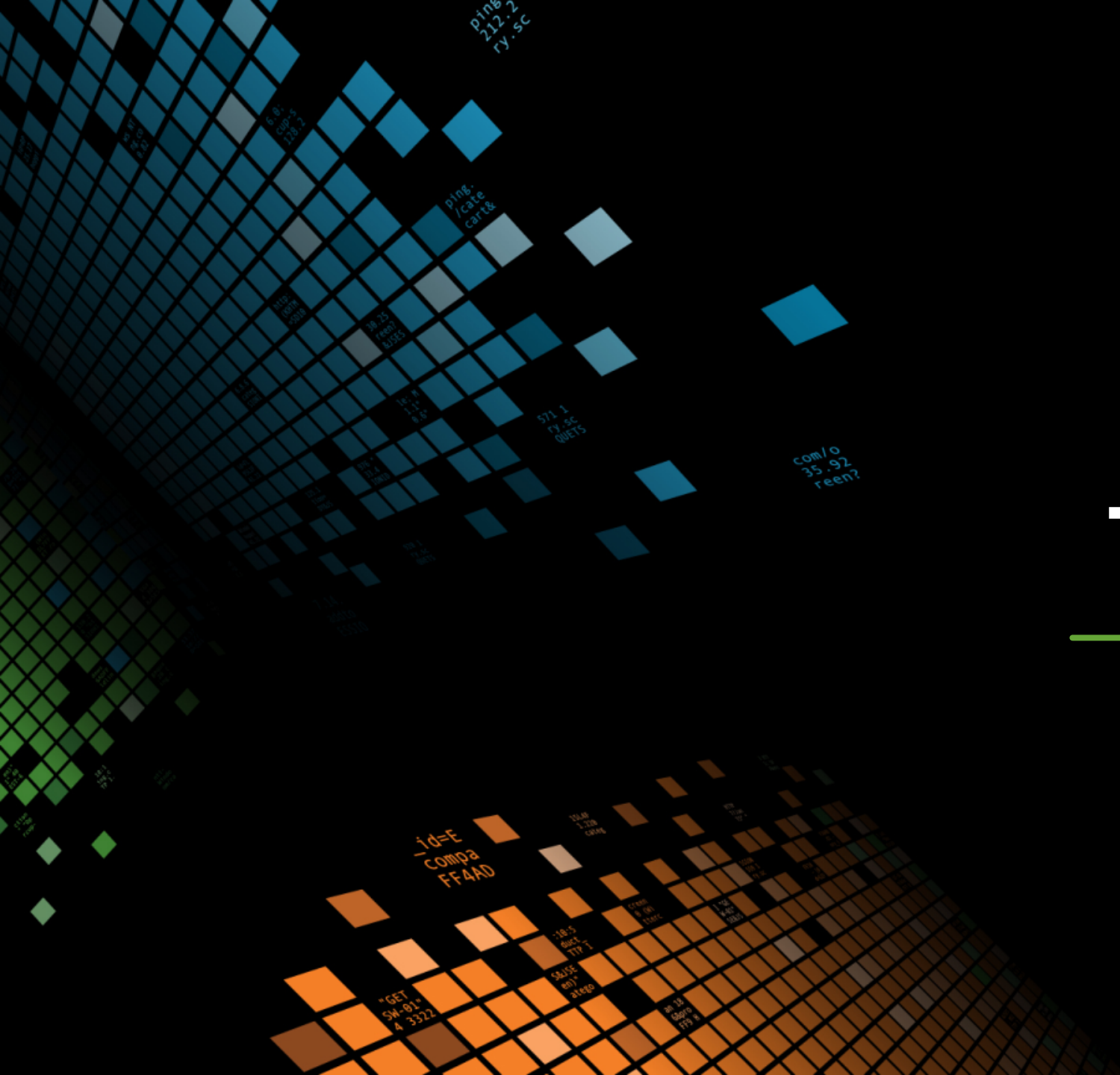
- If you already have HDFS deployed and are experienced with Hadoop
  - Data roll can help reduce Splunk storage costs
  - Use Splunk Bucket Reader to search archived data without Splunk
- Don’t use Data Roll if you don’t already use HDFS
  - You can deploy Splunk in a similar manner to achieve cost savings

Searching data natively in Splunk will be faster

- Dense searches on HDFS will have the best performance
  - Data in HDFS is indexed on-the-fly
    - Sparse searches will be slower



splunk> .conf2017



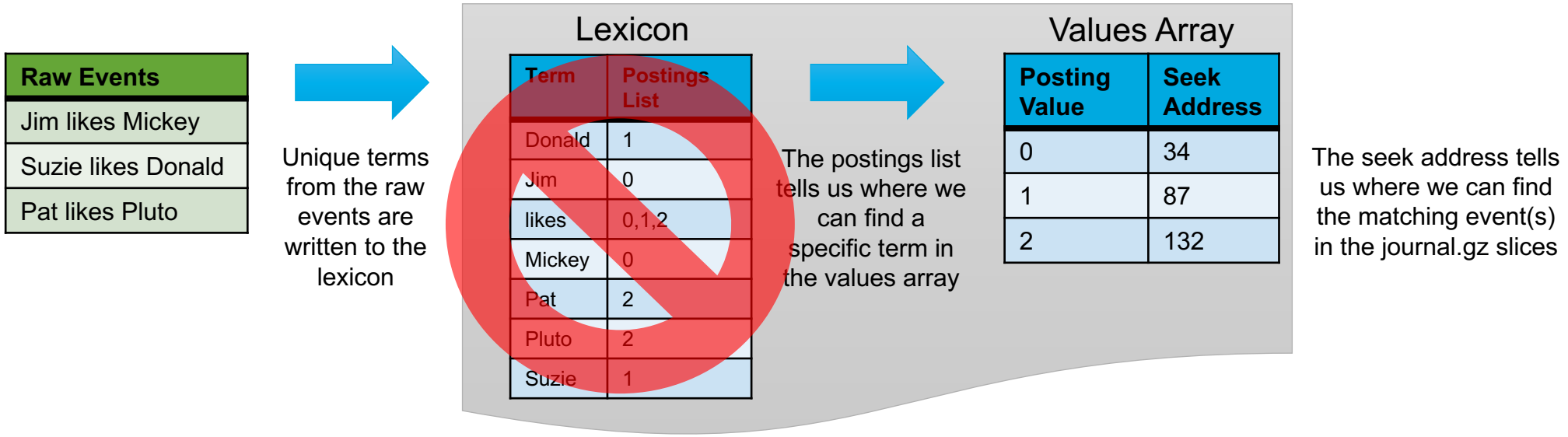
TSIDX Reduce

Put your buckets on a diet

splunk> .conf2017

TSIDX Reduce

How does it work?



- Lexicon is removed from the TSIDX file
- All searches become brute-force searches
  - Every event in a bucket is read from disk and filtered in memory

*The overall structure of a TSIDX file has been simplified for illustrative purposes

splunk> .conf2017

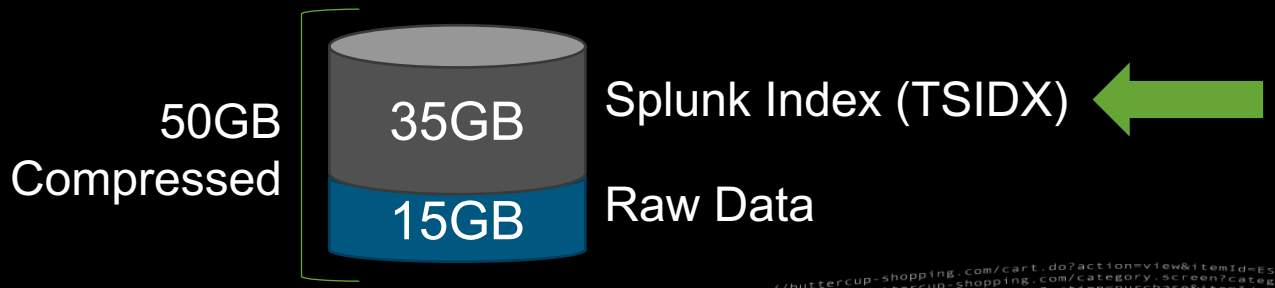
TSIDX Reduce

How much storage do I save?

- Anywhere between 30% - 70% smaller buckets
  - Example: 1GB bucket would decrease in size between 350MB – 700MB

Typical savings is 60% - 70%

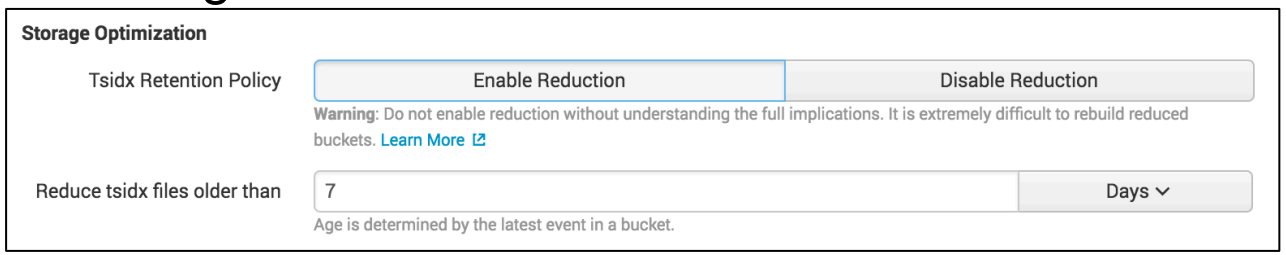
- Size reduction depends on data cardinality
  - More unique values = better disk savings
    - Numerical data
    - Large lexicons
  - merged_lexicon.lex gives an idea of potential reduction



TSIDX Reduce

How do I enable it?

- Can be enabled per-Index
- Warm and Cold buckets can be reduced
- Splunk UI
  - Settings > Indexes > Select an Index



- Conf File

Conf File	indexes.conf
Parameter	[<index name>] enableTsidxReduction = true timePeriodInSecBeforeTsidxReduction = <seconds>

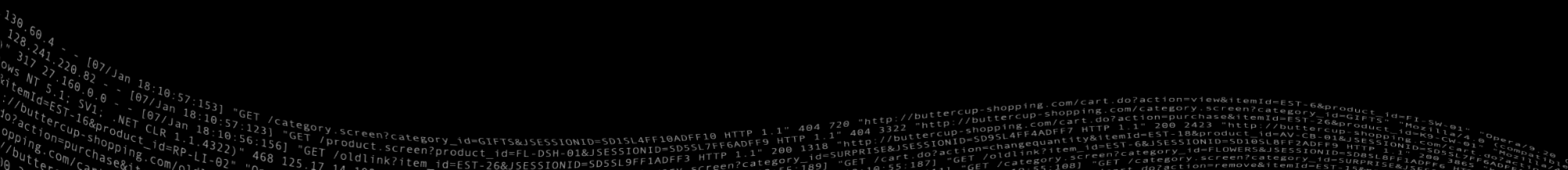
TSIDX Reduce

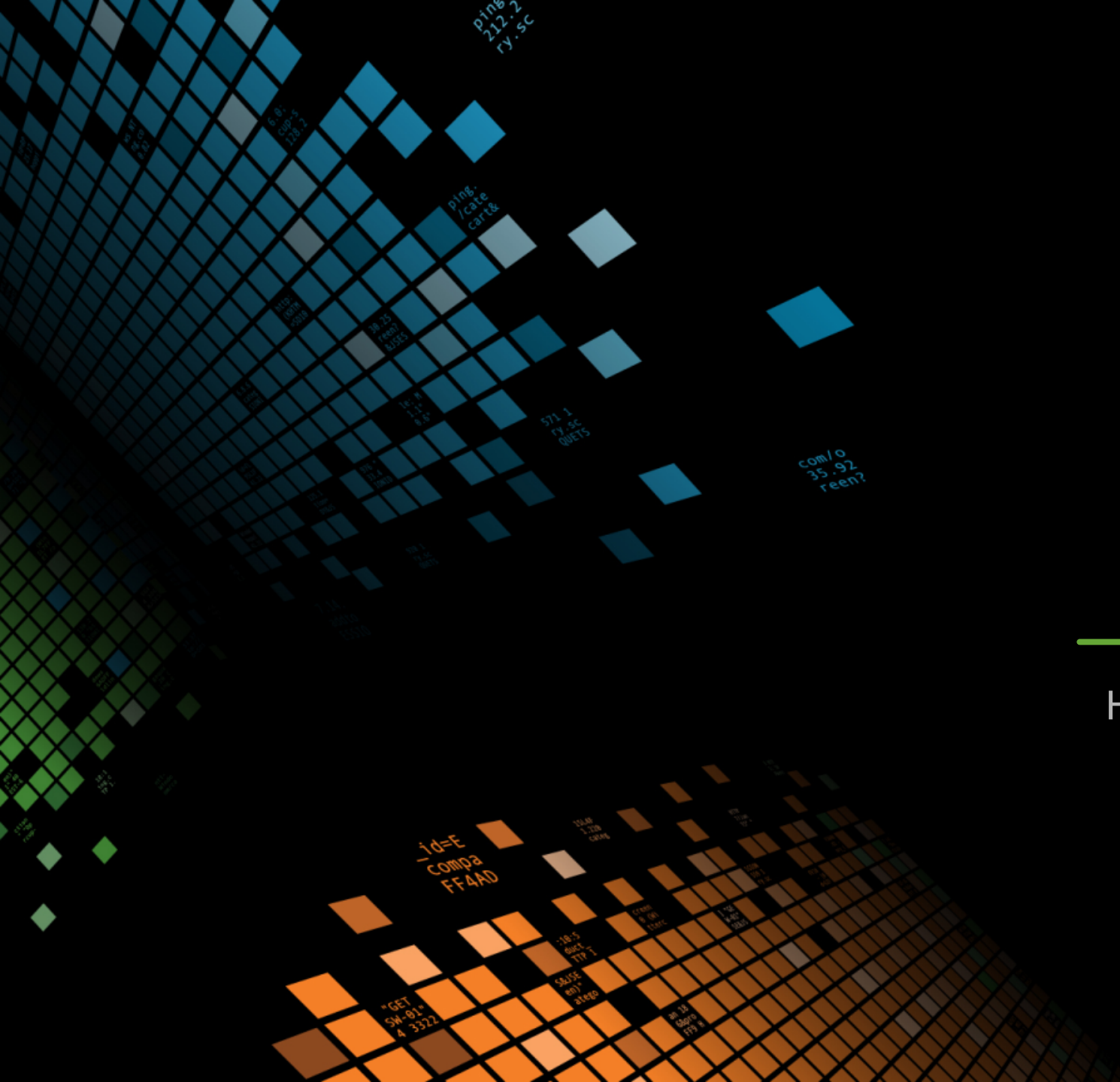
When would I use this?

- Historical/Archive data

Do NOT use TSIDX reduce on frequently searched data

- Dense searches
  - Return a large percentage (10% or more) of matching events from a bucket
  - Largely unaffected by TSIDX reduce
- Sparse searches
  - Needle in the haystack style searches
  - Significantly affected by TSIDX reduce
    - 3-10X slower
    - Depends on the volume of data searches





Retention

How long does this stuff stay around?

Retention

General Guidelines

- Retention **IS NOT** managed across indexers

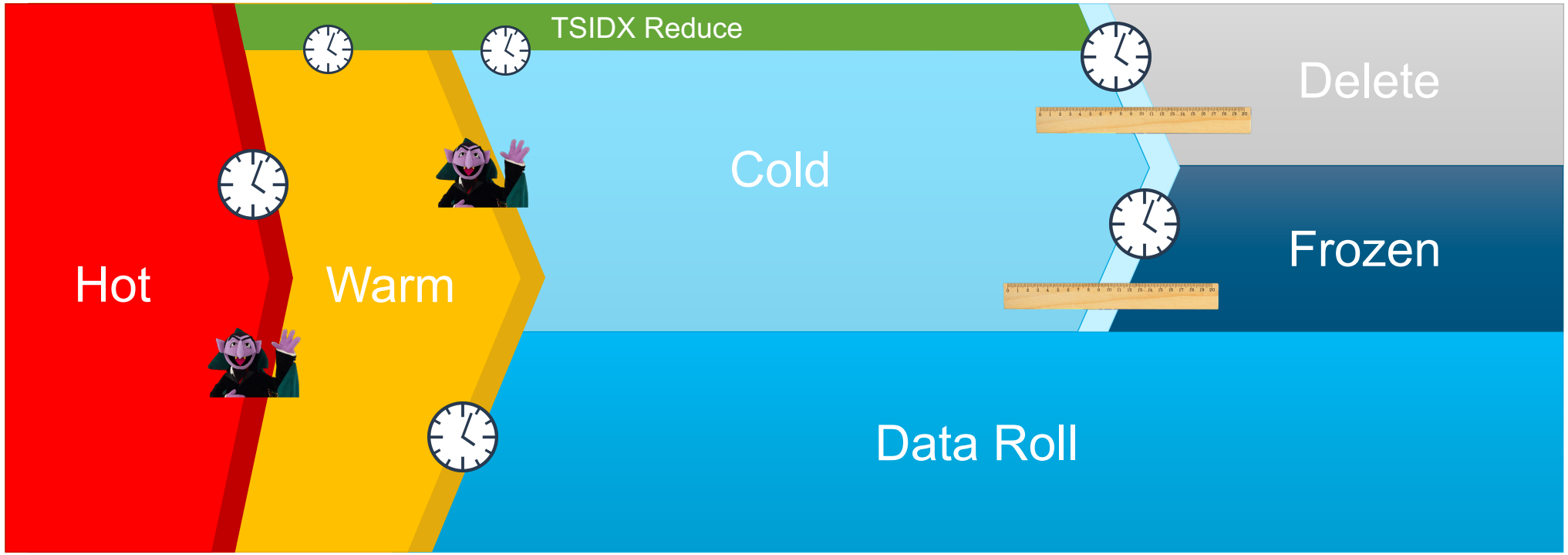
Each indexer will manage data retention independently

  - Data may age faster on one indexer than another
    - Data imbalance
    - Uneven disk utilization

- Avoid forcing bucket rolling
  - Creates small buckets
  - Impacts search performance
  - Can impact index clustering

Retention

When do we roll data?



# of Buckets

Age

Size on disk

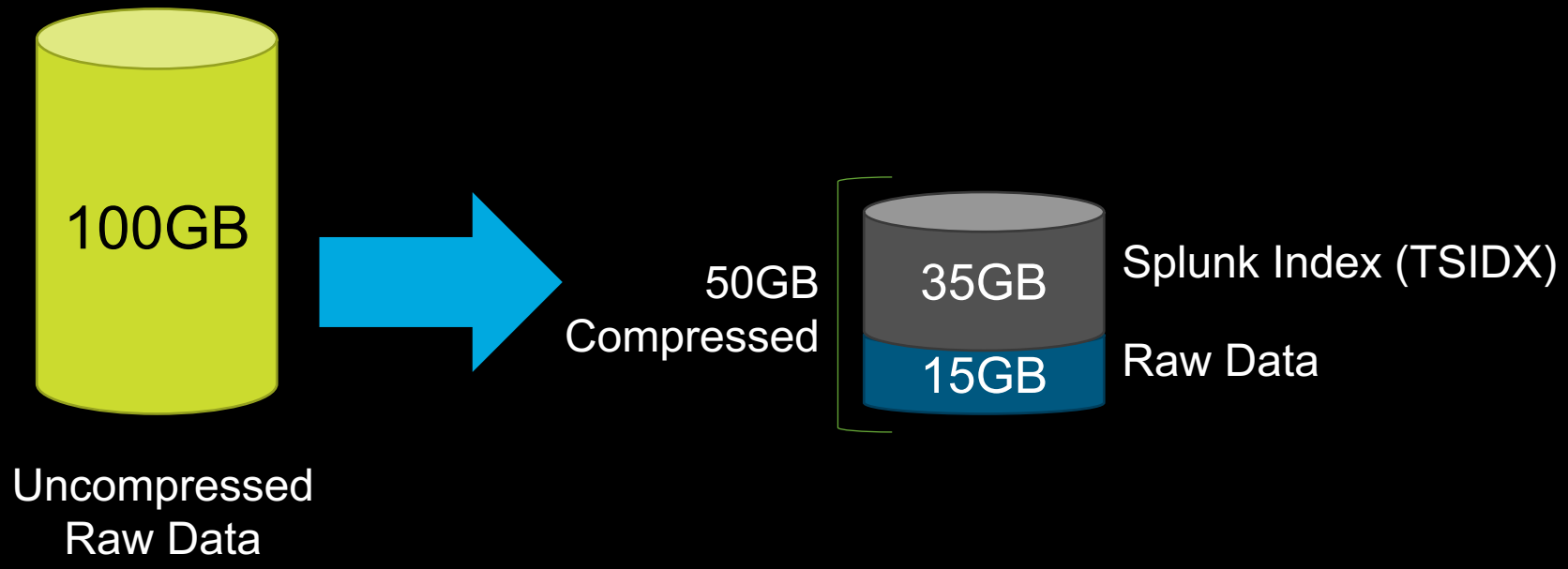
Calculating Retention

How much storage do you need?

- In general, Splunk will compress raw data by 50%

<Daily Ingest> * .5 = Daily size on disk * <days of retention> = Total storage needed

  - We have an app for that: http://splunk-sizing.appspot.com/



Calculating Retention

Splunk Volumes

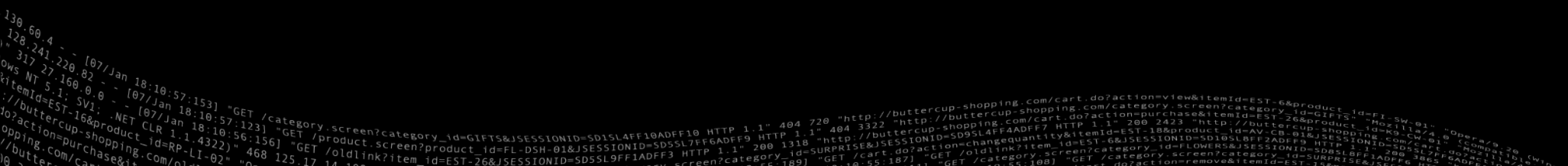
- Hot/Warm Volume
  - Frequently searched data should be here
  - Most customer searches are over the last 48hrs of data

Rarely will you need >14 days of hot/warm

  - Find your “typical” search range

```
index=_audit action=search info=completed is_realtime=0
```

- Cold Volume
  - All data that isn’t in Hot/Warm
  - Consider keeping data in Cold vs. rolling to frozen
    - Much easier to manage
  - Consider using TSIDX reduce to conserve more disk space
    - Factor reduced buckets into storage planning



splunk> .conf2017

Retention

Volume Definitions

- Control retention for all indexes that reference the volume
  - Allows you to consume a defined storage amount across multiple indexes

Conf File	indexes.conf
Parameter	[volume:<volume name>] path = maxVolumeDataSizeMB = [<index name>] homePath = volume:<volume name>/$_index_name/db coldPath = volume:<volume name>/$_index_name/colddb

- Oldest bucket in the volume is deleted/frozen when defined size is exceeded
  - Take care when placing indexes in the same volume
  - “Noisy” indexes can cause older data to be deleted

splunk> .conf2017

Index Clustering

Index Clustering

How does it affect my data strategy?

- Retention is **not** managed cluster-wide

Each indexer handles retention independently

- Pay attention to disk utilization
  - Monitoring Console > Indexing > Indexes and Volumes > Indexes and Volumes: Deployment
  - Buckets may be deleted/archived from an indexer faster than others
- Use cluster rebalance when necessary
  - http://docs.splunk.com/Documentation/Splunk/6.6.2/Indexer/Rebalancethecluster#Rebalance_indexer_cluster_data

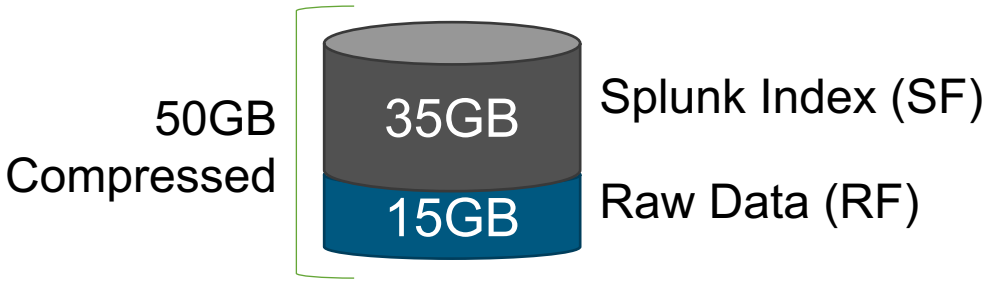
- Freezing Data
  - Frozen buckets are not fixed-up
    - http://docs.splunk.com/Documentation/Splunk/latest/Indexer/Bucketsandclusters#How_the_cluster_handles_frozen_buckets
  - Splunk does **not** de-duplicate data when freezing/thawing
    - You must de-dupe buckets using the <localid> in the folder path
      - http://docs.splunk.com/Documentation/Splunk/latest/Indexer/HowSplunkstoresindexes#Bucket_naming_conventions

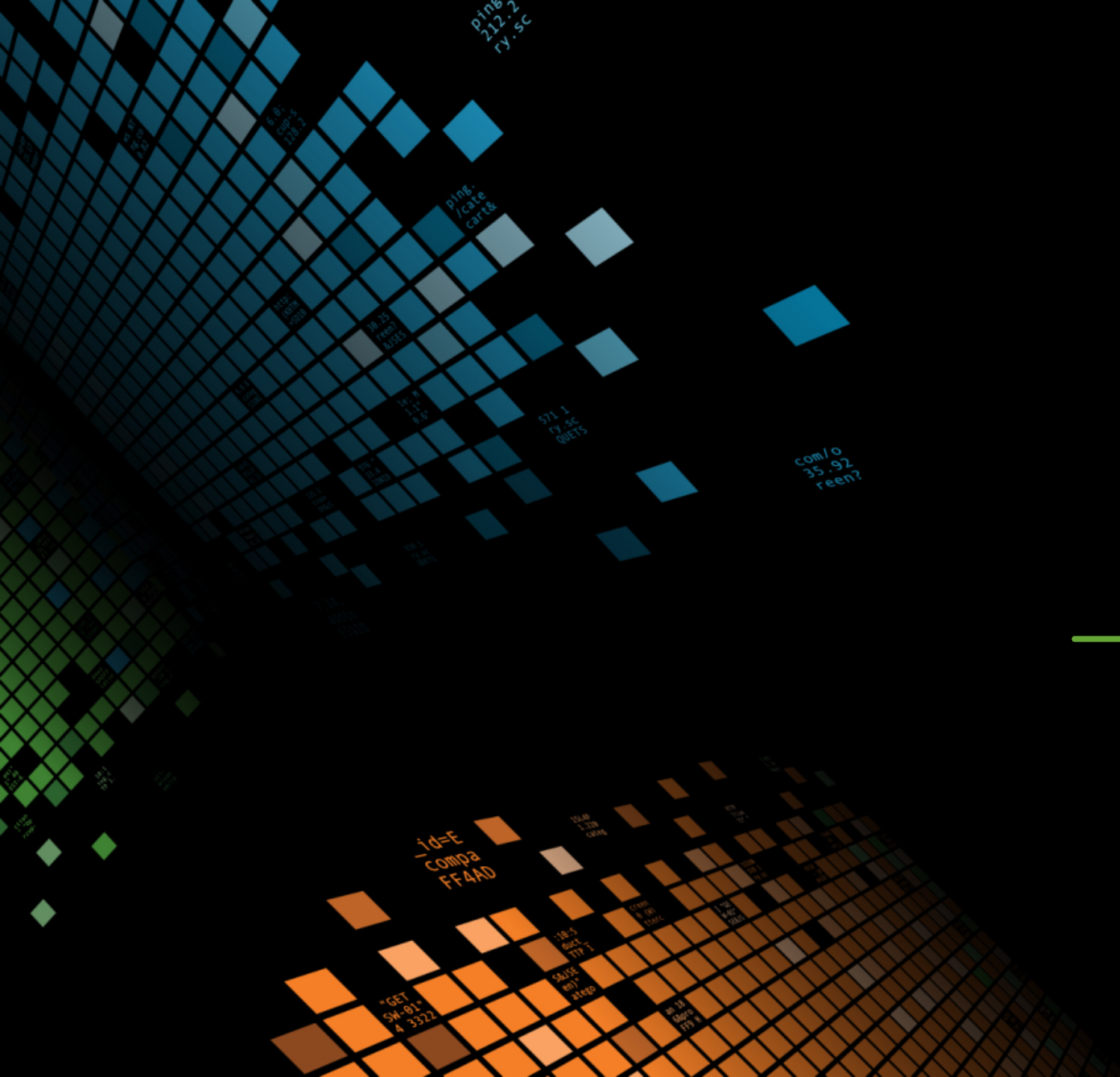
splunk> .conf2017

Index Clustering

How does it affect my data strategy?

- Capacity Planning
  - Replication policy will affect disk utilization
    - Search Factor = Splunk Index (TSIDX File)
    - Replication Factor = Raw Data
  - Use the sizing app: http://splunk-sizing.appspot.com/





Data Model Accelerations

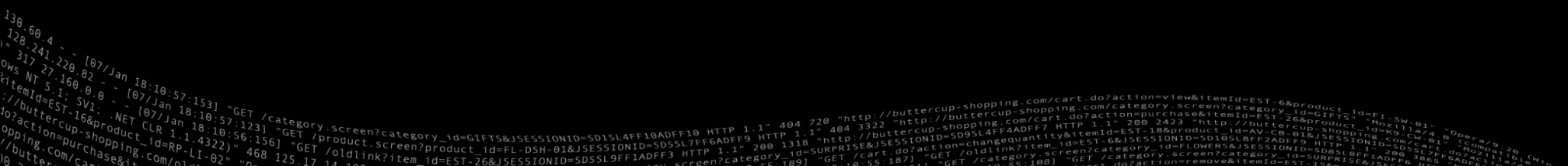
splunk> .conf2017

Data Model Accelerations

Planning for performance

- A pre-summarized set of fields defined by a Data Model
  - Typically much smaller than the source index
  - Only accelerate the data you will search often (Summary Range)
    - http://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Aboutsummaryindexing#Data_model_acceleration
- Storage
  - Keep your summaries in the Hot/Warm volume for best performance
    - Be aware of storage impact

Conf File	indexes.conf
Parameter	[<index name>] tstatsHomePath =



splunk> .conf2017

Data Model Accelerations

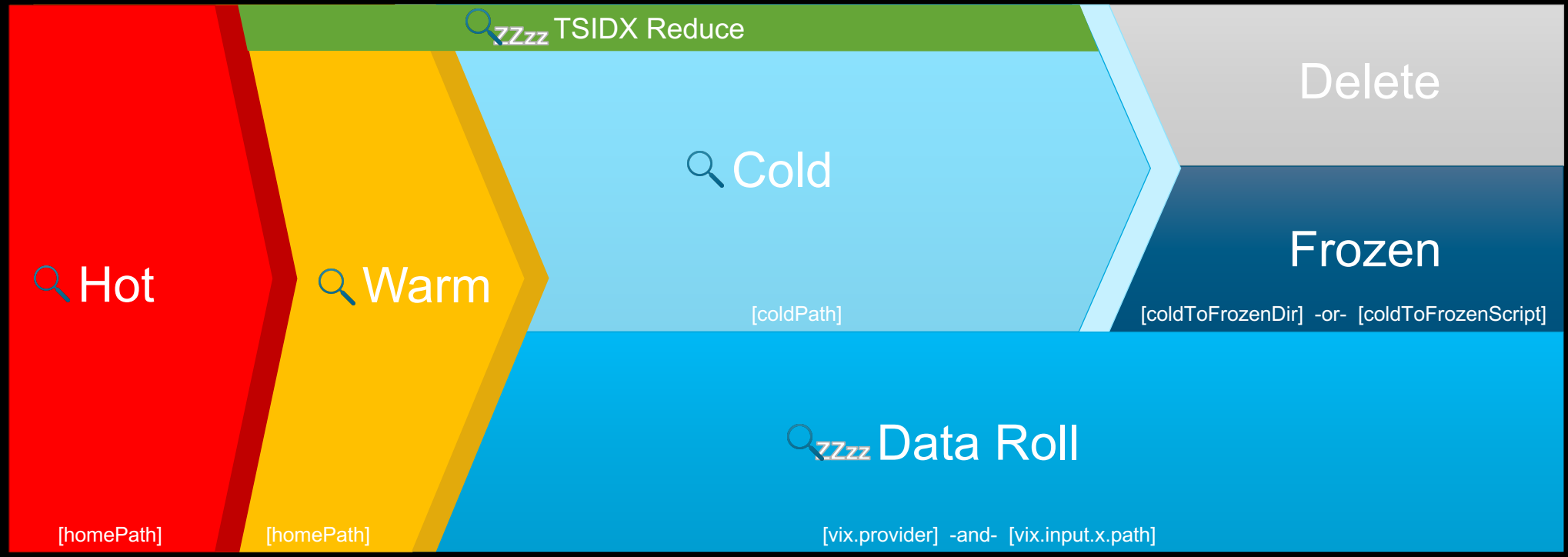
Capacity Planning

- Retention
  - Summary is deleted when the oldest event exceeds the summary range
  - Summaries cannot be kept longer than the raw data
- Sizing
  - Depends on your data model definition
    - # of fields
    - Cardinality of data (# of unique values)
  - Run your own tests to get size estimates
    - Settings > Data Models
  - Enterprise Security
    - Daily Ingest * 3.4 = 1 year of accelerations
      - http://docs.splunk.com/Documentation/ES/latest/Install/Datamodels#Data_model_acceleration_storage_and_retention

splunk> .conf2017

Data Lifecycle

Recap



splunk> .conf2017

Questions?

Help me help you

splunk> .conf2017

Thank You

Don't forget to rate this session in the .conf2017 mobile app