Splunk Cloud
Under The Hood

Disclaimer

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 the 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.

Rajiv Battula
Software Engineer

Nikhil Mungel
Sr. Software Engineer

splunk>cloud

Site Reliability Engineering
San Francisco

What is splunk>cloud™?

Agenda

- Overview
- Design Principles
- Data Ingestion
- Reliability & Availability
- Security from the Ground Up
- Hybrid
- Operational Excellence

Design Principles

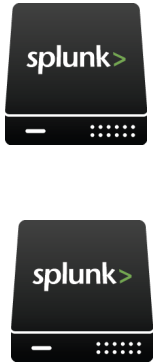
Design Principles

Secure

Instant

Reliable

Hybrid



Clustering &
License Managers

Indexers

Search Heads

Single Tenant

Clustering &
License Managers

Indexers

Search Heads

EC2 Instance


splunk>
cloud

Secure By Default

Network Isolation

System Isolation

Encryption

Non-repudiable Logging

Secure coding practices


splunk>
cloud


splunk>
cloud

Reliable

Replicated Data

Replicated Configs

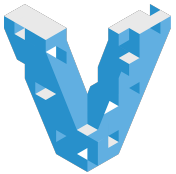
Disaster Recovery

Redundant infrastructure

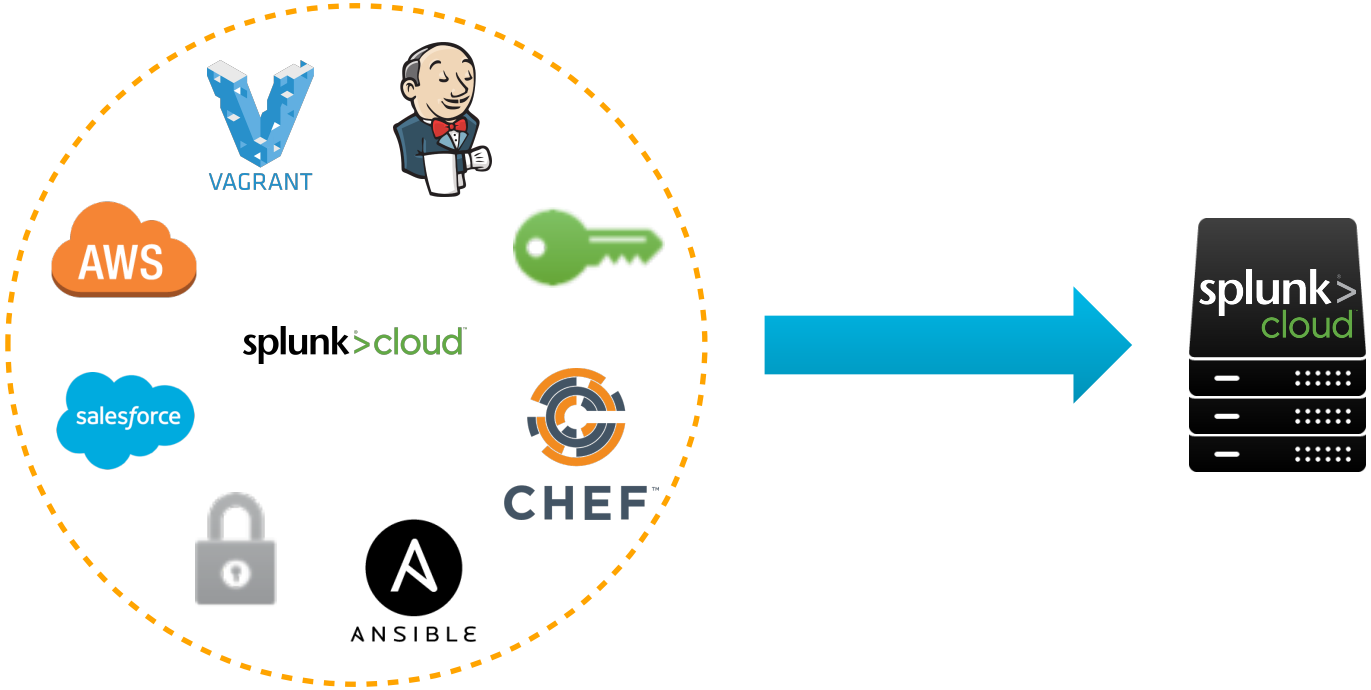
Licenser Service

splunk>cloud™

Cert Generation



Instant

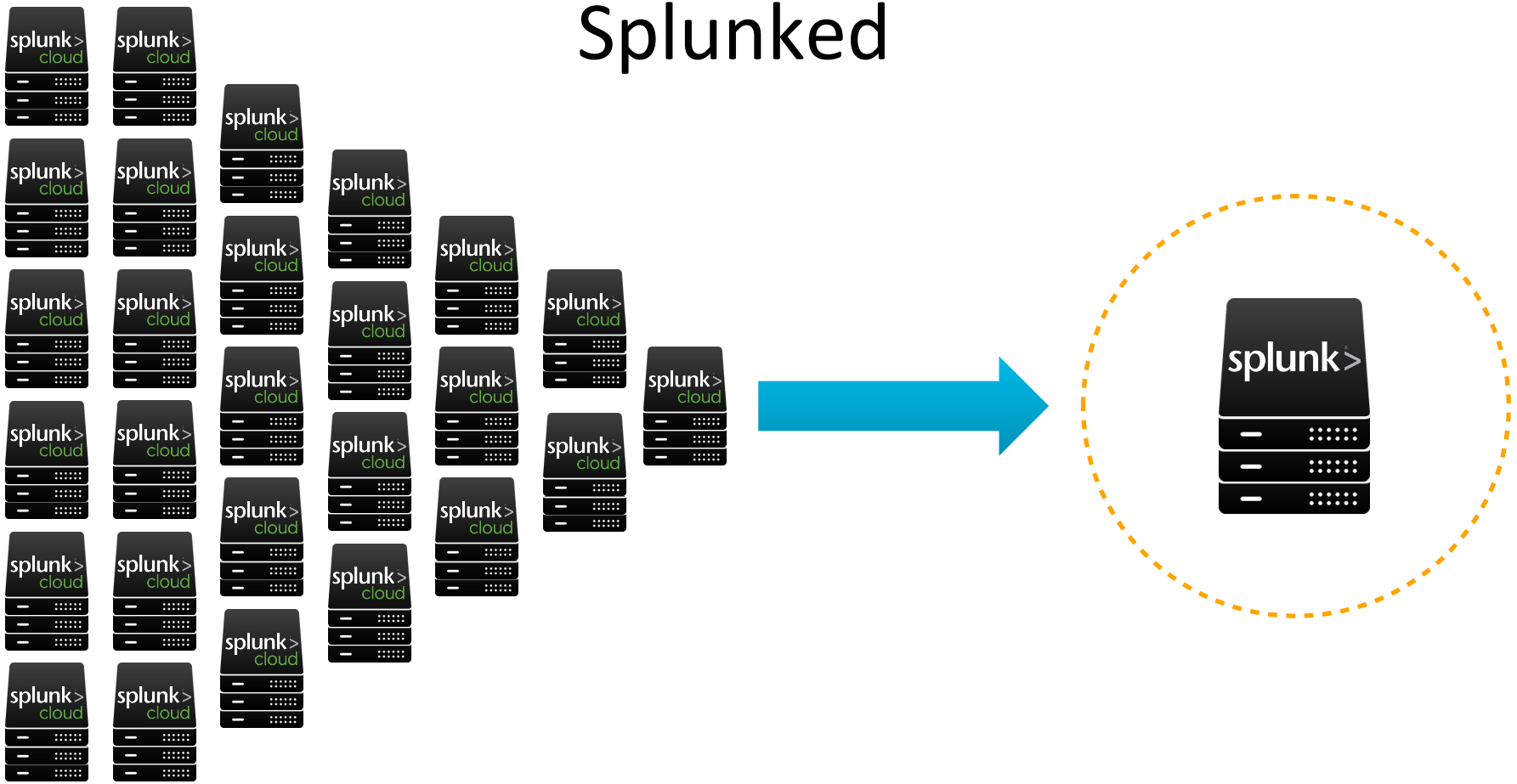

VAGRANT
AWS
splunk>cloud
salesforce
CHEF
ANSIBLE
splunk>
cloud

Scalable


VAGRANT
AWS
splunk>cloud
salesforce
CHEF
ANSIBLE

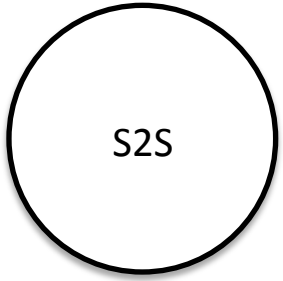

splunk> cloud

Splunked



Data Ingestion

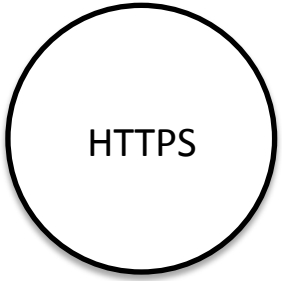
Two Methods Of Ingesting Data



Splunk-to-Splunk with SSL

Universal & Heavy Forwarders

High performance



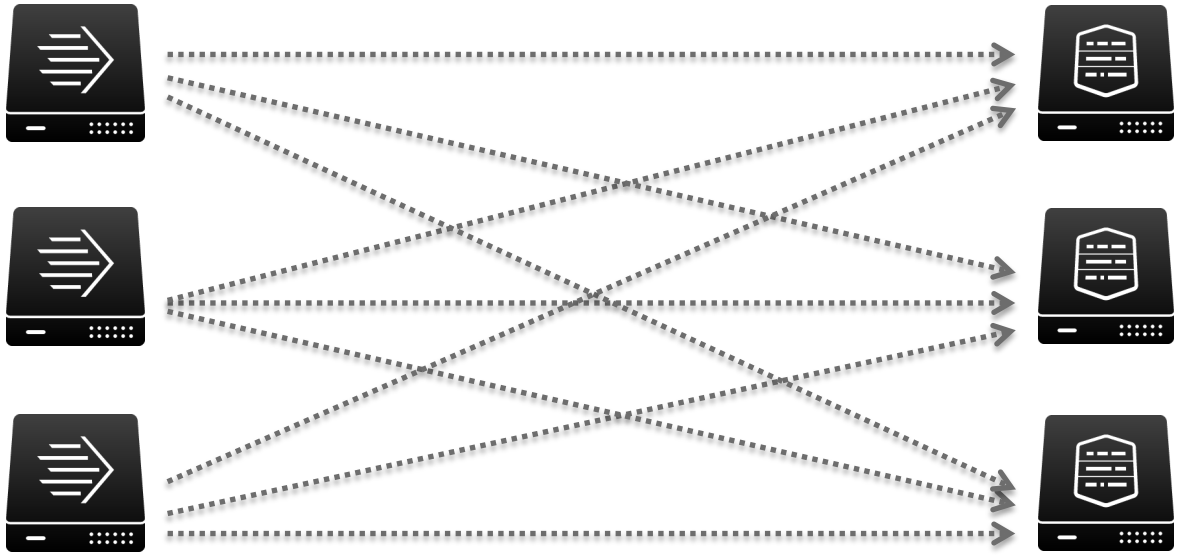
Forward JSON events over HTTPS

No Splunk forwarders necessary

SDKs allow for application integration

High performance & scalable

S2S Ingestion



ACME CORPORATION

splunk>cloud

S2S Ingestion

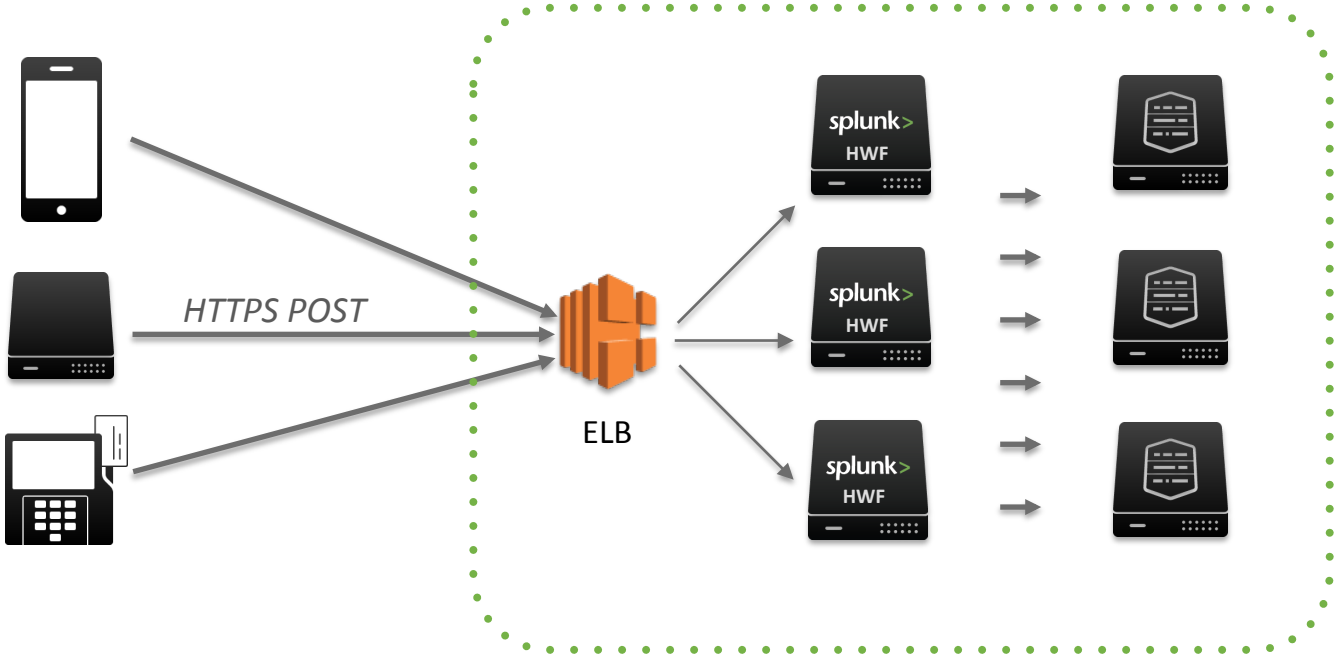
Forwarders

Round Robin DNS
+
Elastic IP Addresses

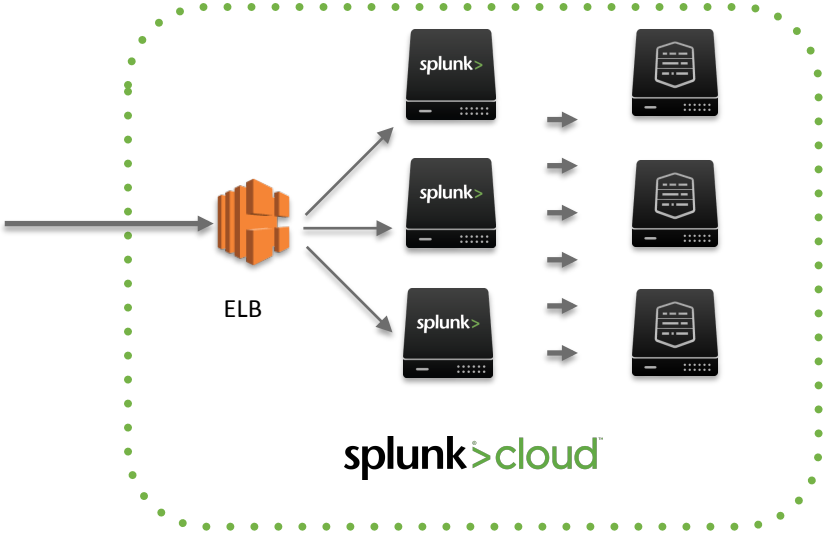
```
[default outputs.conf]
autoLBFrequency=30
dnsResolutionInterval=300
```

Indexers

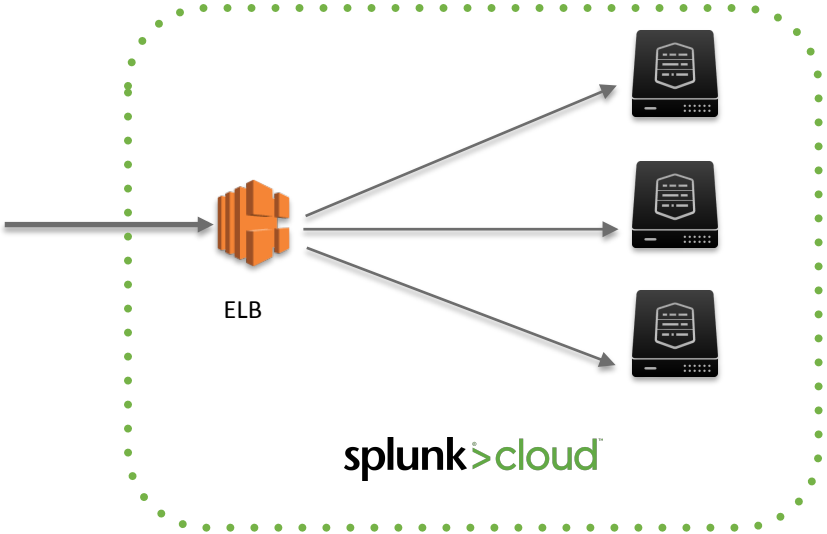
HTTP Event Collector



Large number of HTTP clients
Small bursts of data, **millions of times**



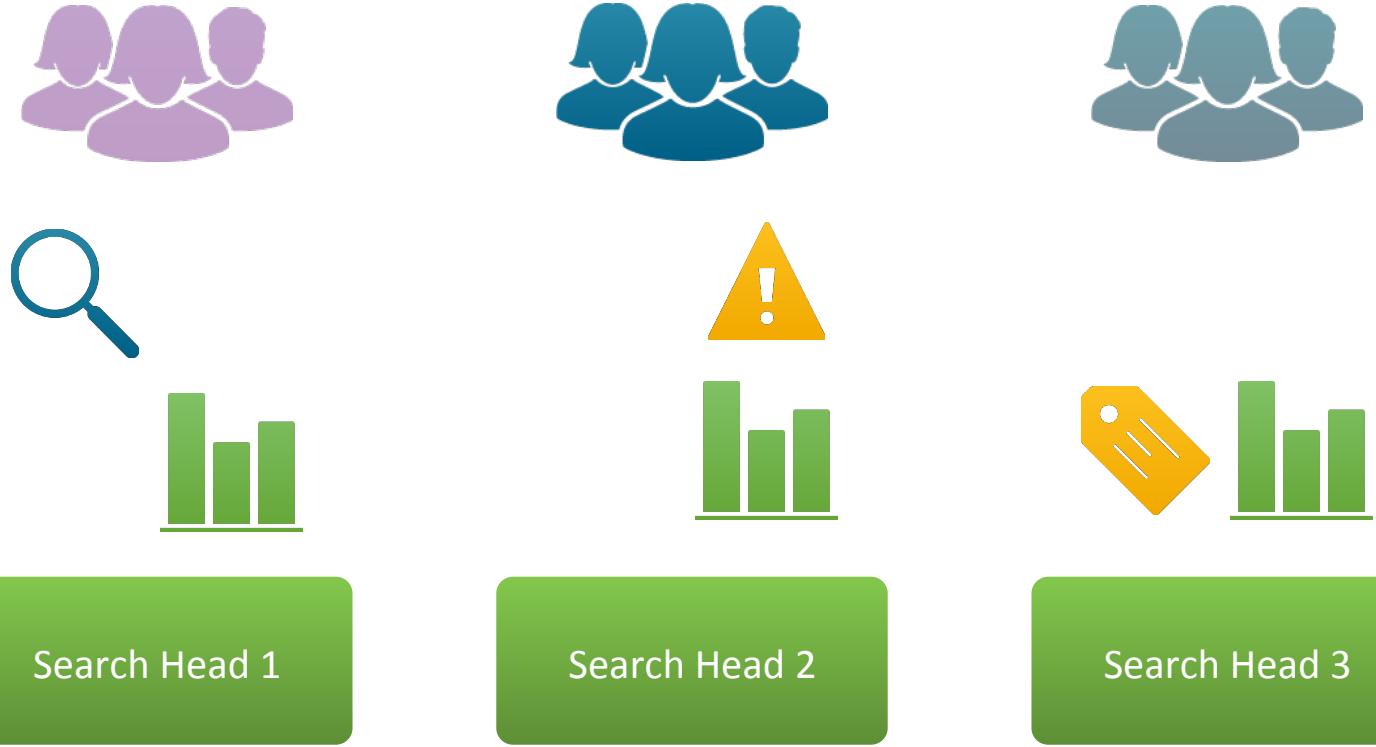
Small number of HTTP clients
Continuous **streams of data**



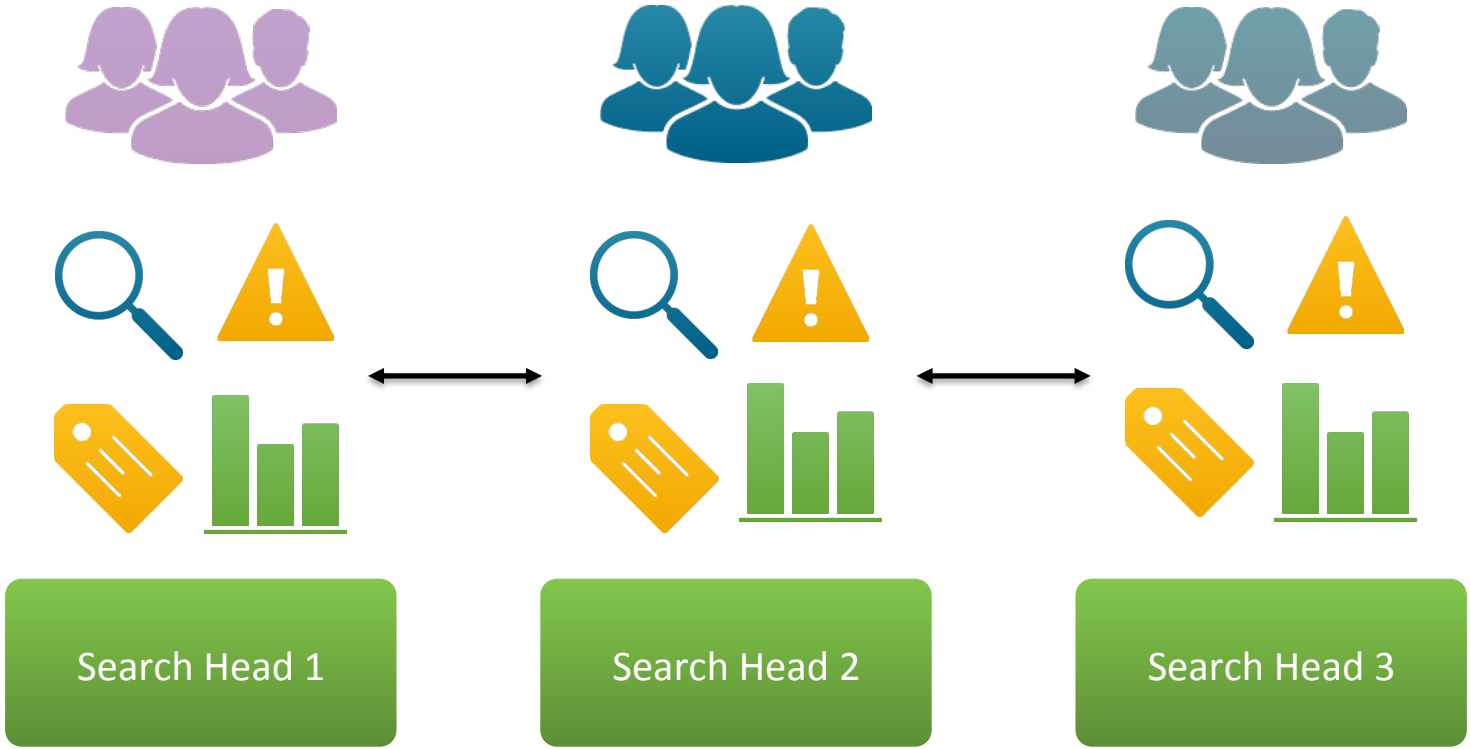
Reliable & Available

High Availability

High Availability



High Availability



High Availability

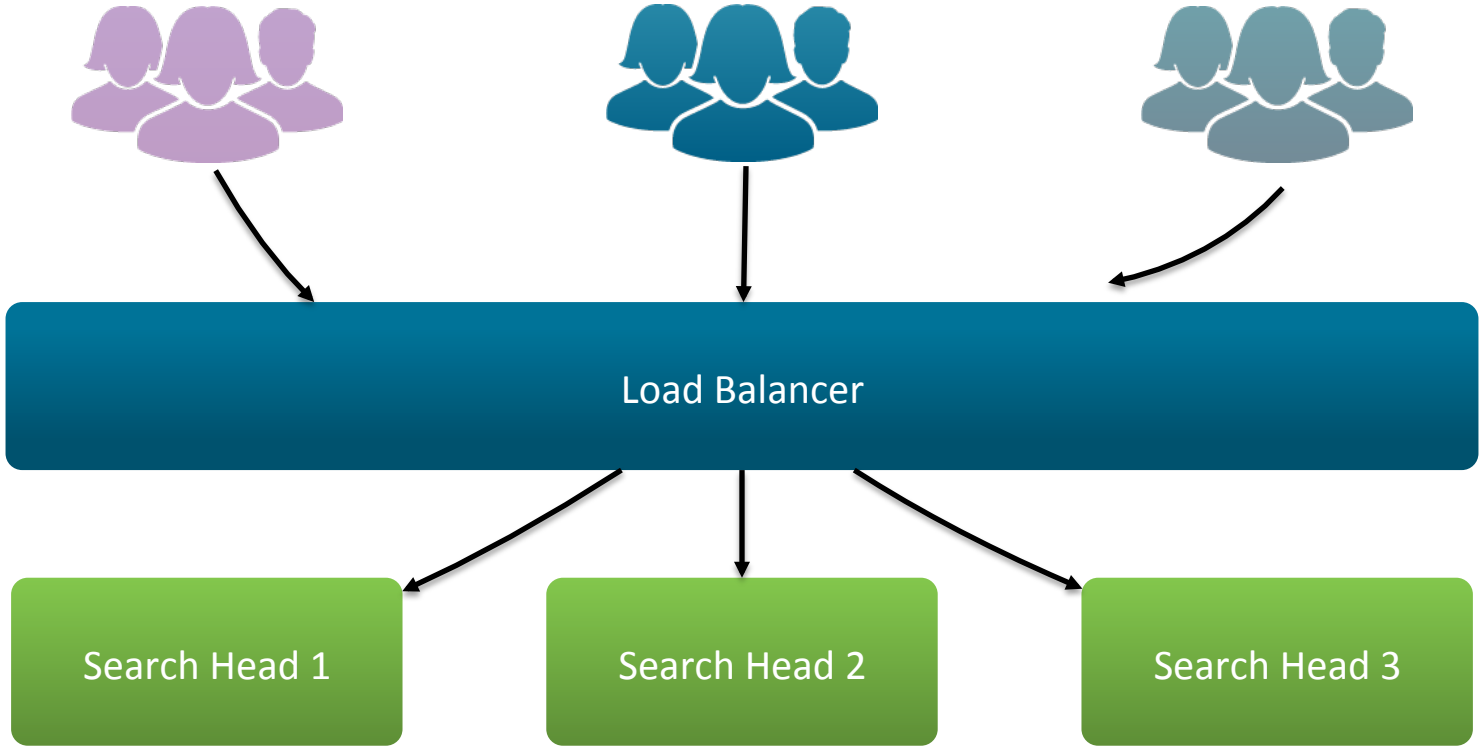
Load Balancer

Search Head 1

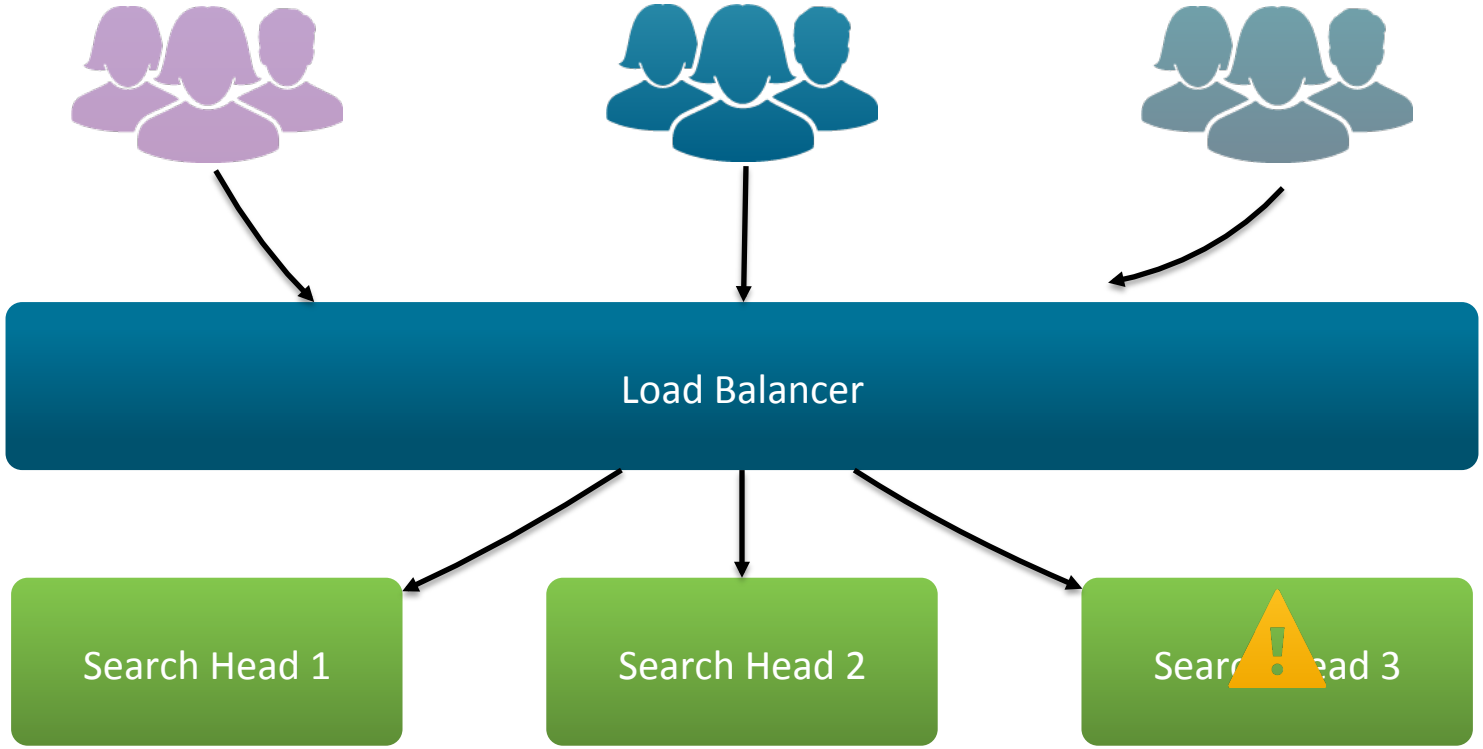
Search Head 2

Search Head 3

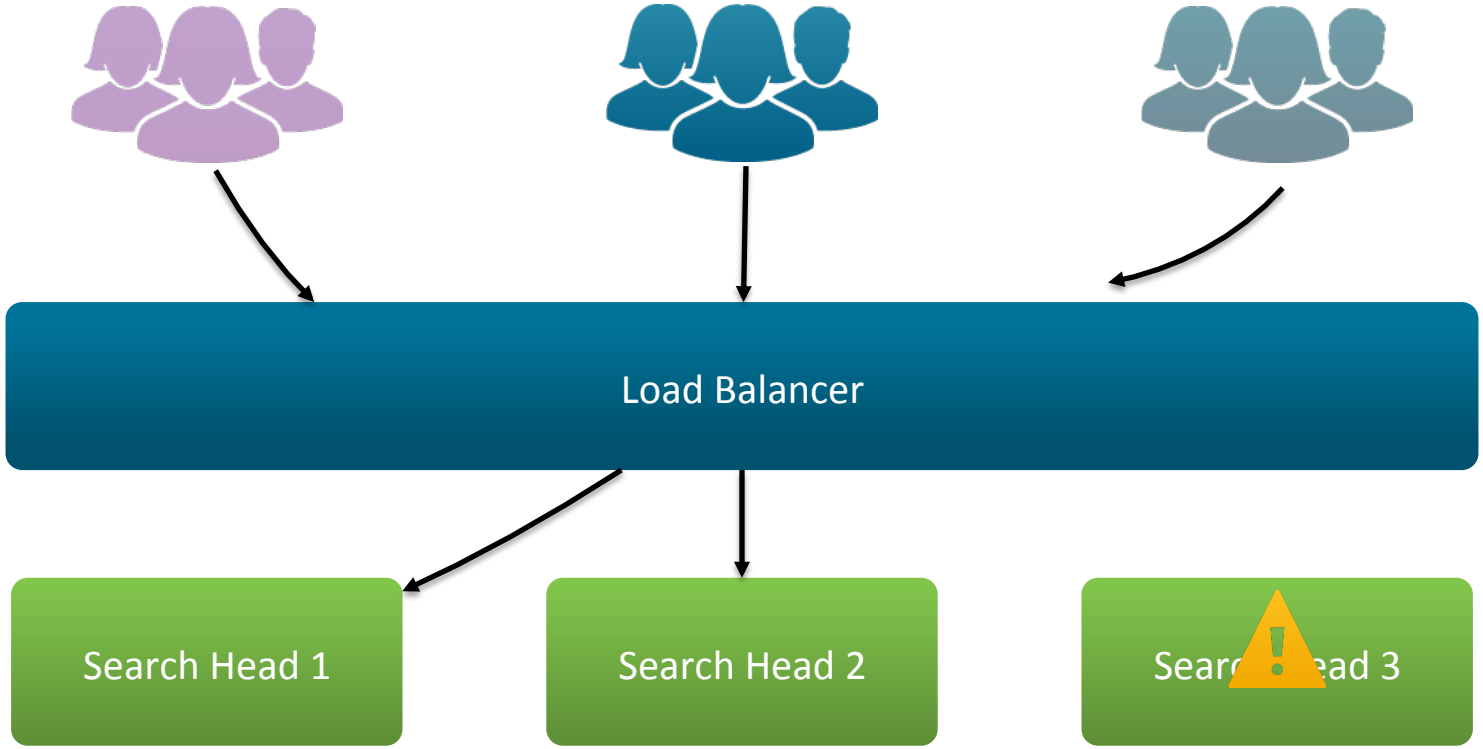
High Availability



High Availability



High Availability



Reliability

3 Indexers

Splunk Buckets

Searchable Bucket
Contains raw data & Splunk metadata

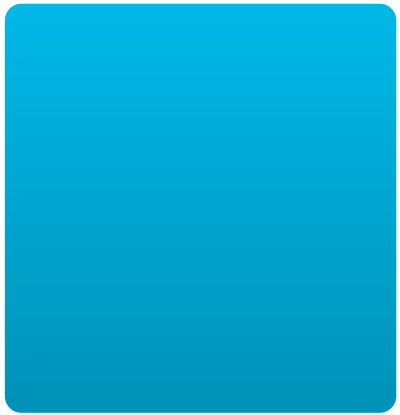
Splunk Buckets

Searchable Bucket
Contains raw data & Splunk metadata

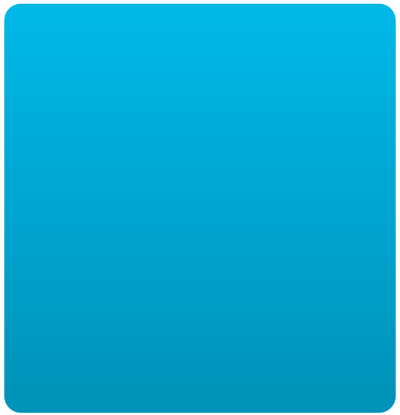
Replicated Bucket
Contains only raw data

Reliability

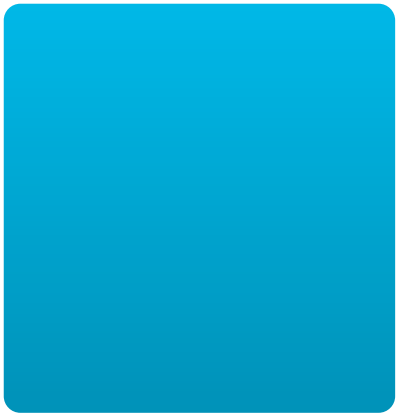
Indexer 1



Indexer 2



Indexer 3

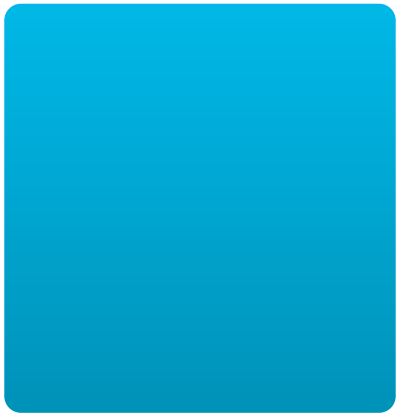


Reliability

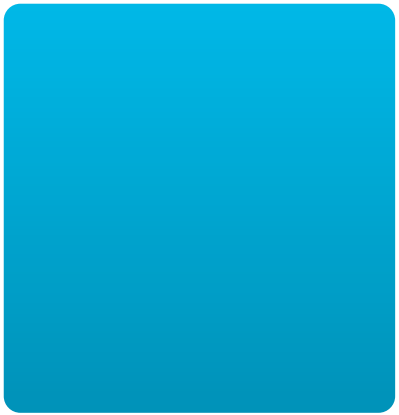
Indexer 1

Searchable Bucket

Indexer 2



Indexer 3



Reliability

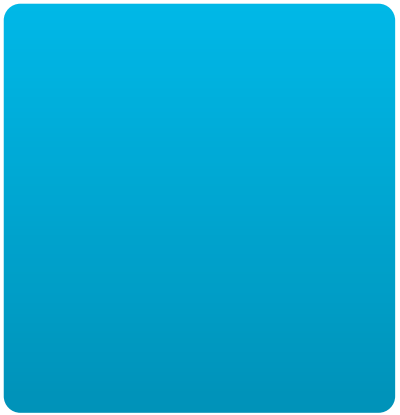
Indexer 1

Searchable Bucket

Indexer 2

Searchable Bucket

Indexer 3



Reliability

Indexer 1

Searchable Bucket

Indexer 2

Searchable Bucket

Indexer 3

Replicated Bucket

Reliability

Indexer 1

Searchable Bucket

Indexer 2

Searchable Bucket

Indexer 3

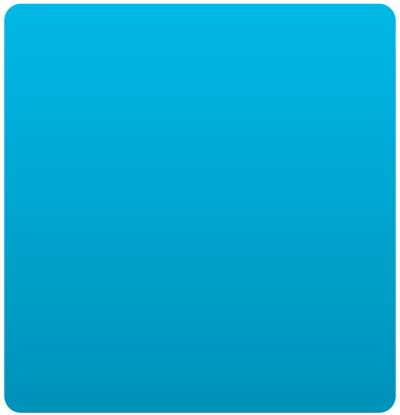
Replicated Bucket

Reliability

Indexer 1

Searchable Bucket

Indexer 2



Indexer 3

Replicated Bucket

Reliability

Indexer 1

Searchable Bucket

Indexer 2

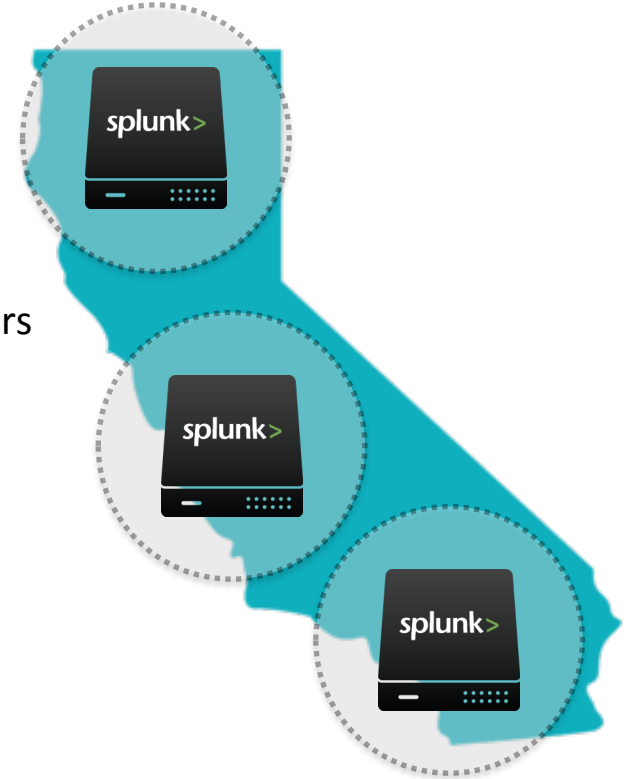
Searchable Bucket

Indexer 3

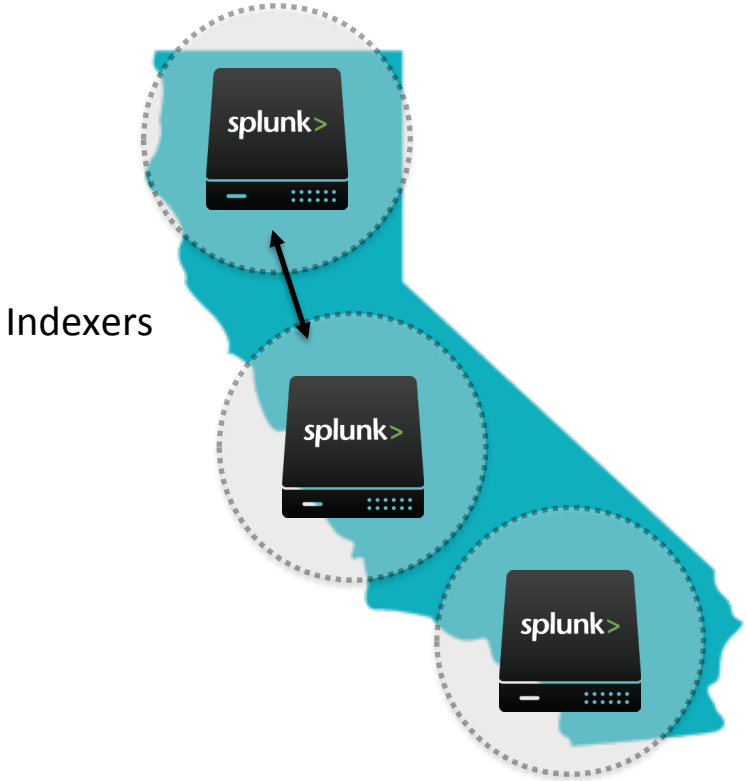
Replicated Bucket

High Availability

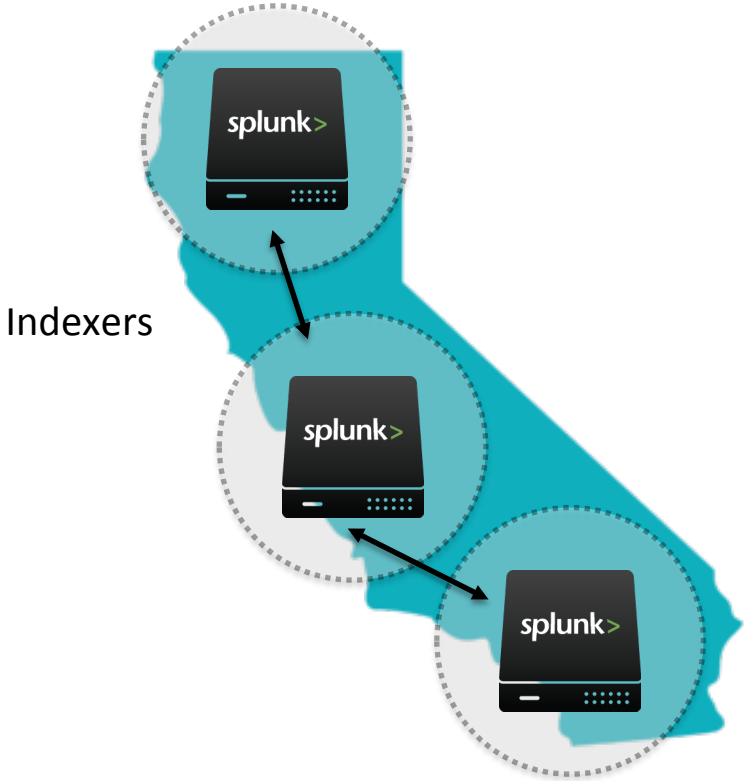
Indexers



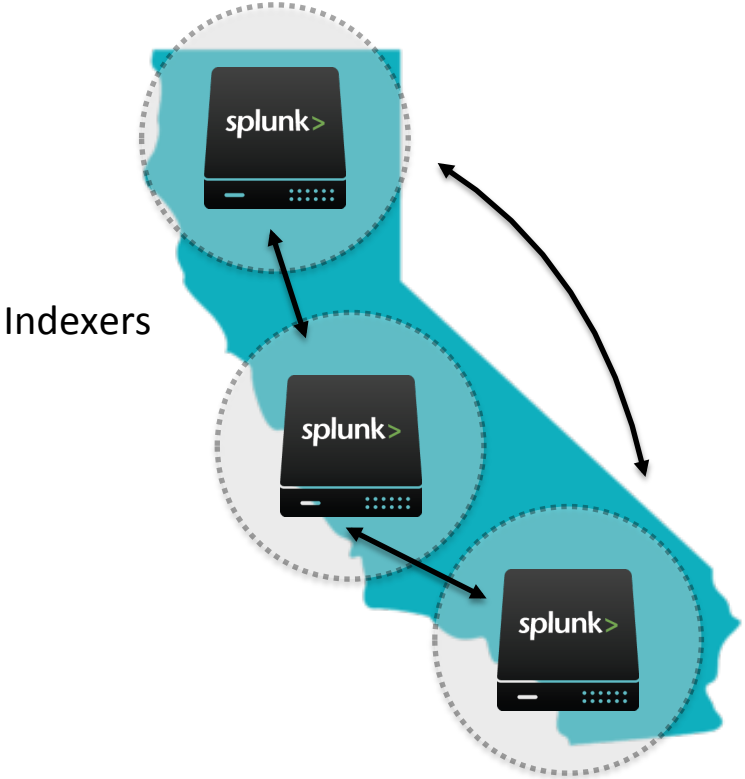
High Availability



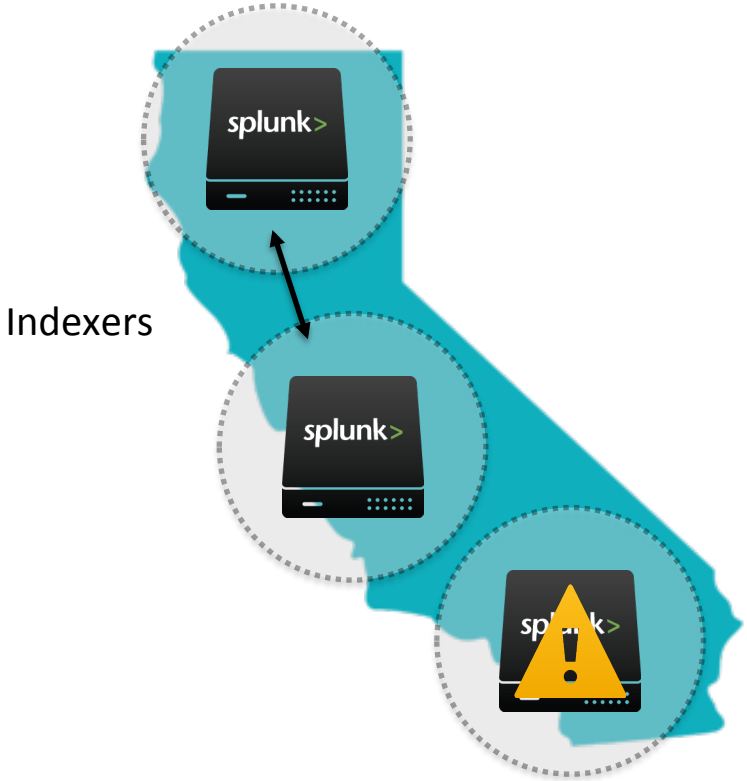
High Availability



High Availability

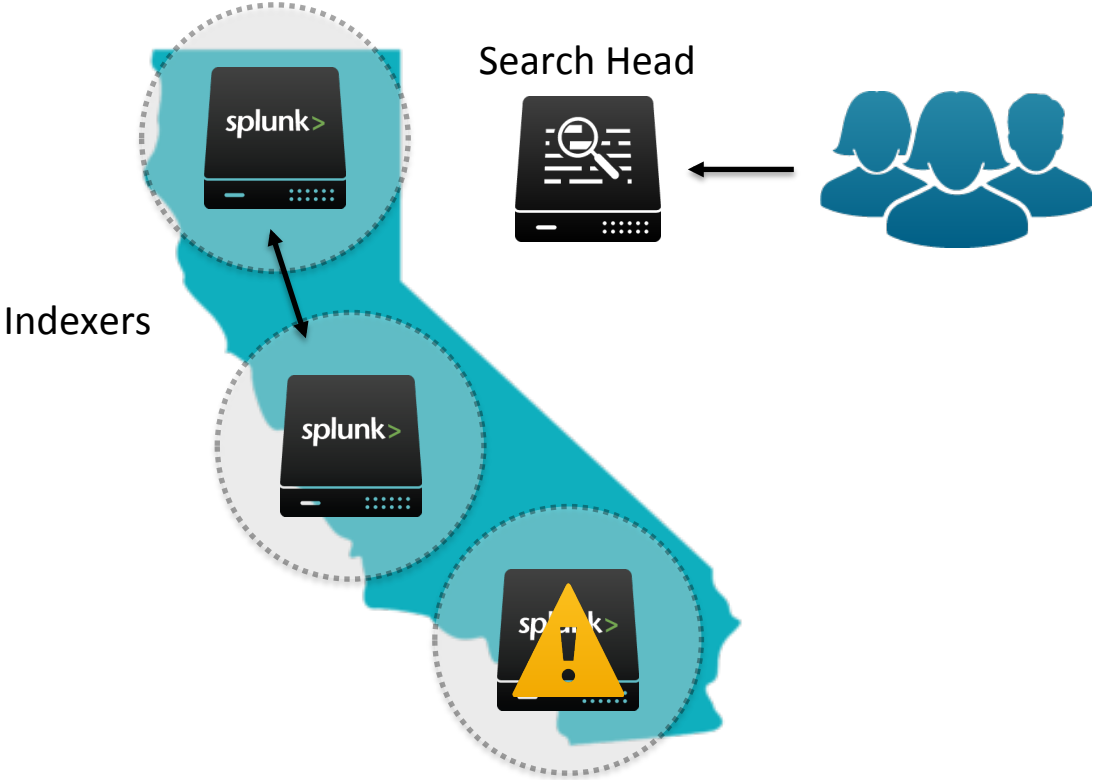


High Availability

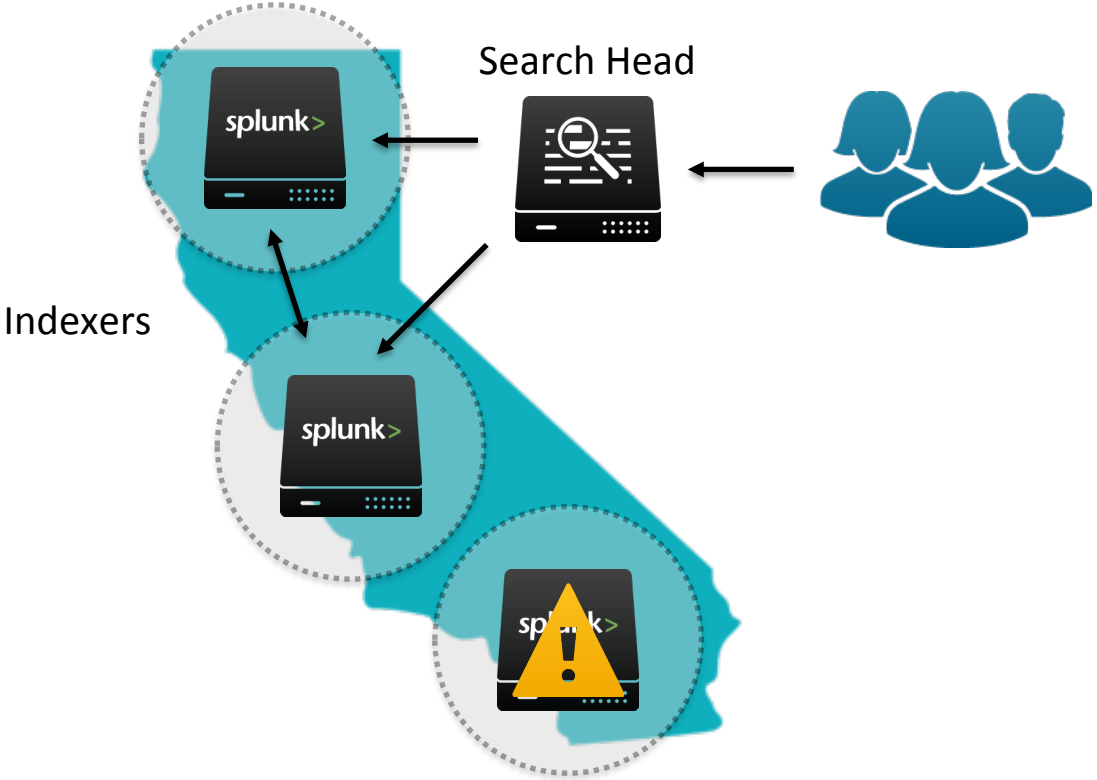


High Availability

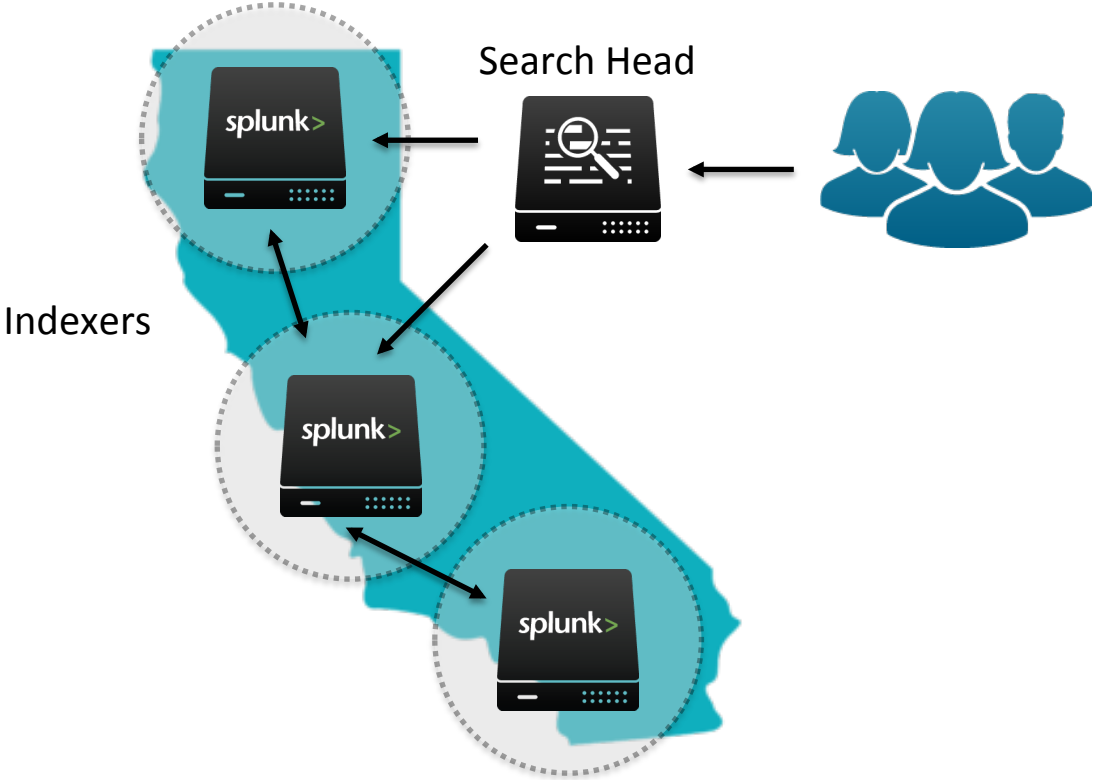
High Availability



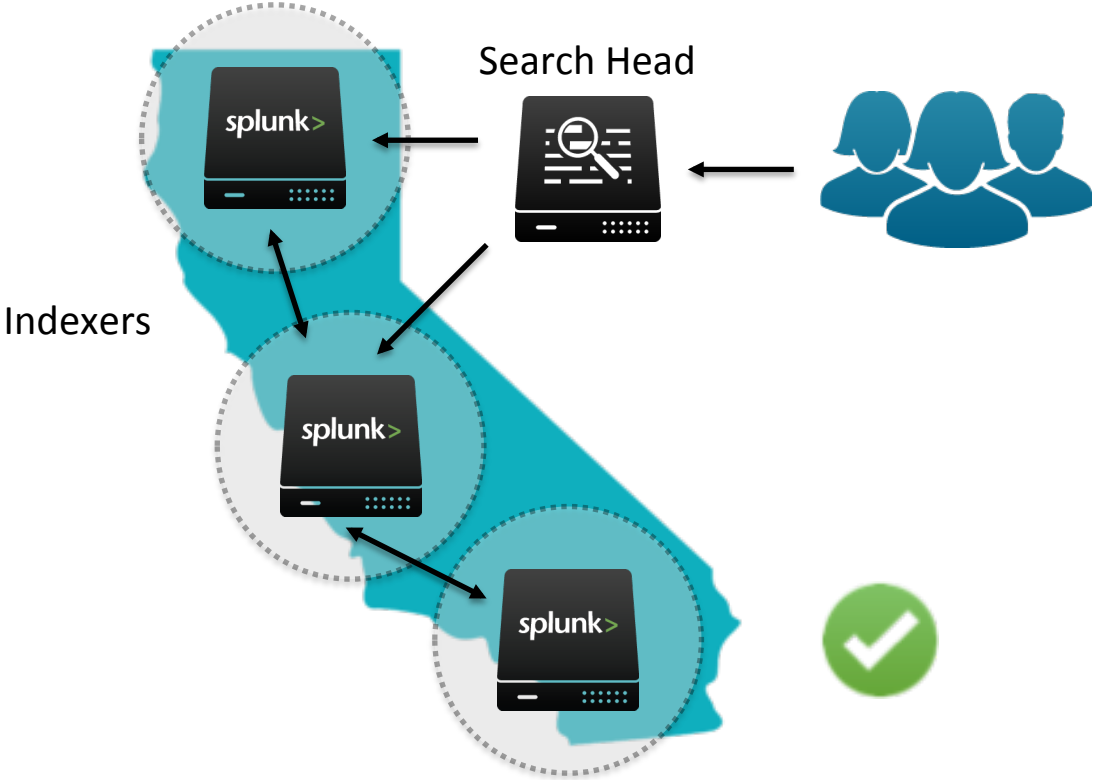
High Availability



High Availability



High Availability

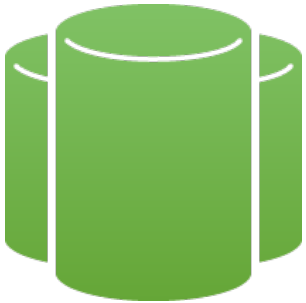


Disaster Recovery

Splunk Buckets &
Configuration

Disaster Recovery

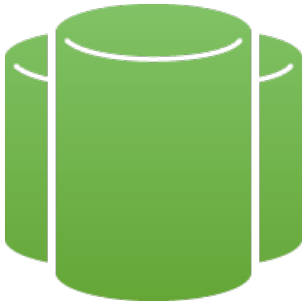
Splunk Buckets & Configuration



Amazon S3

Disaster Recovery

Splunk Buckets & Configuration

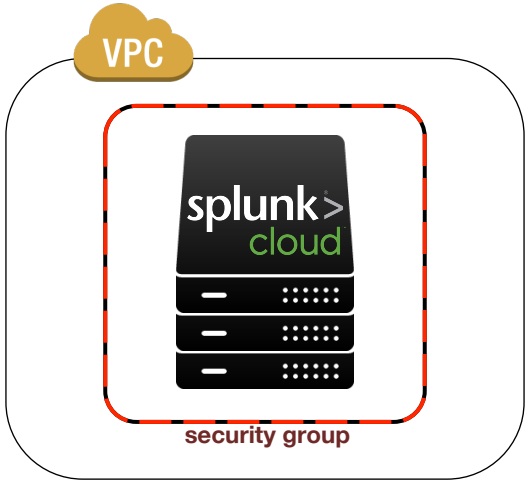


Amazon S3

Security

Customer Stack

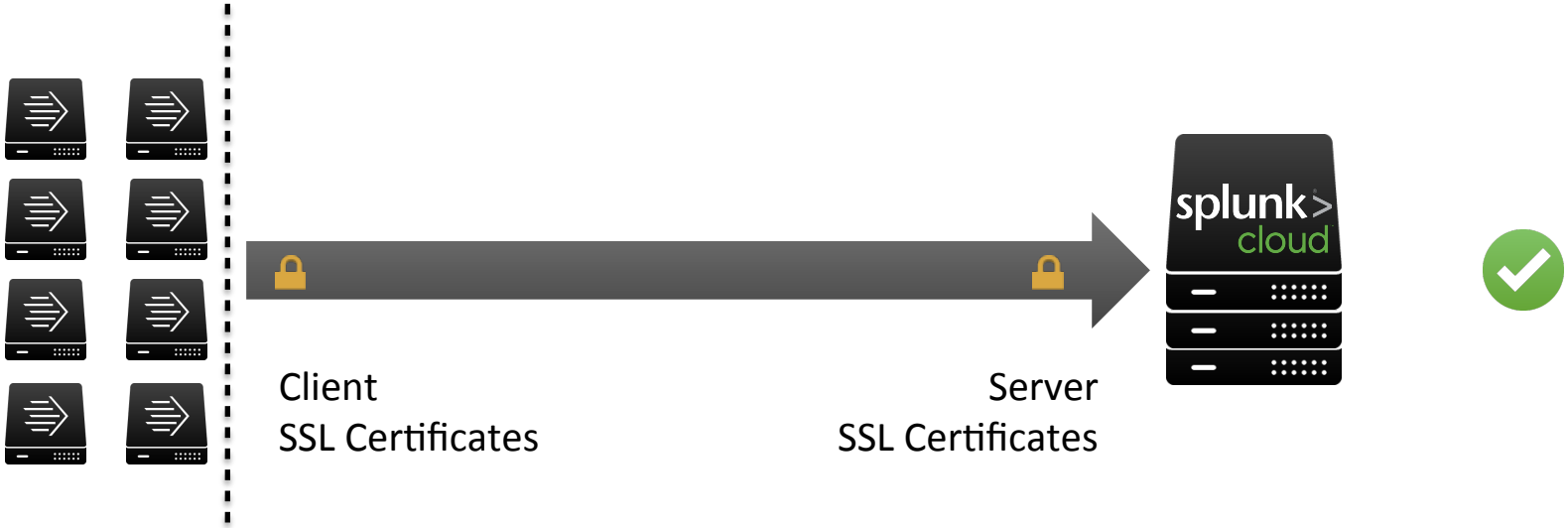
Isolated by Security Groups



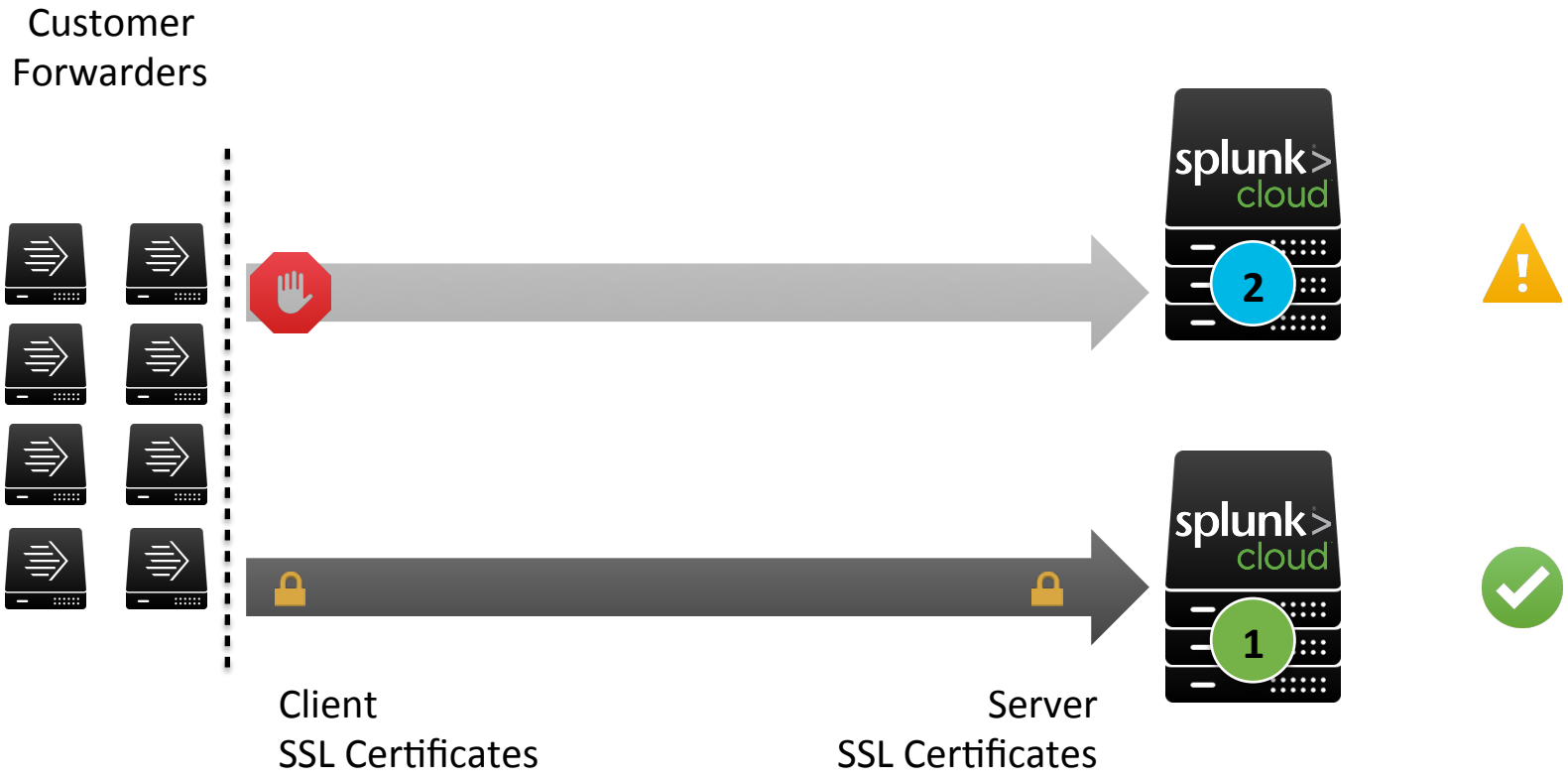
Further Isolated by a Splunk VPC

Authentication

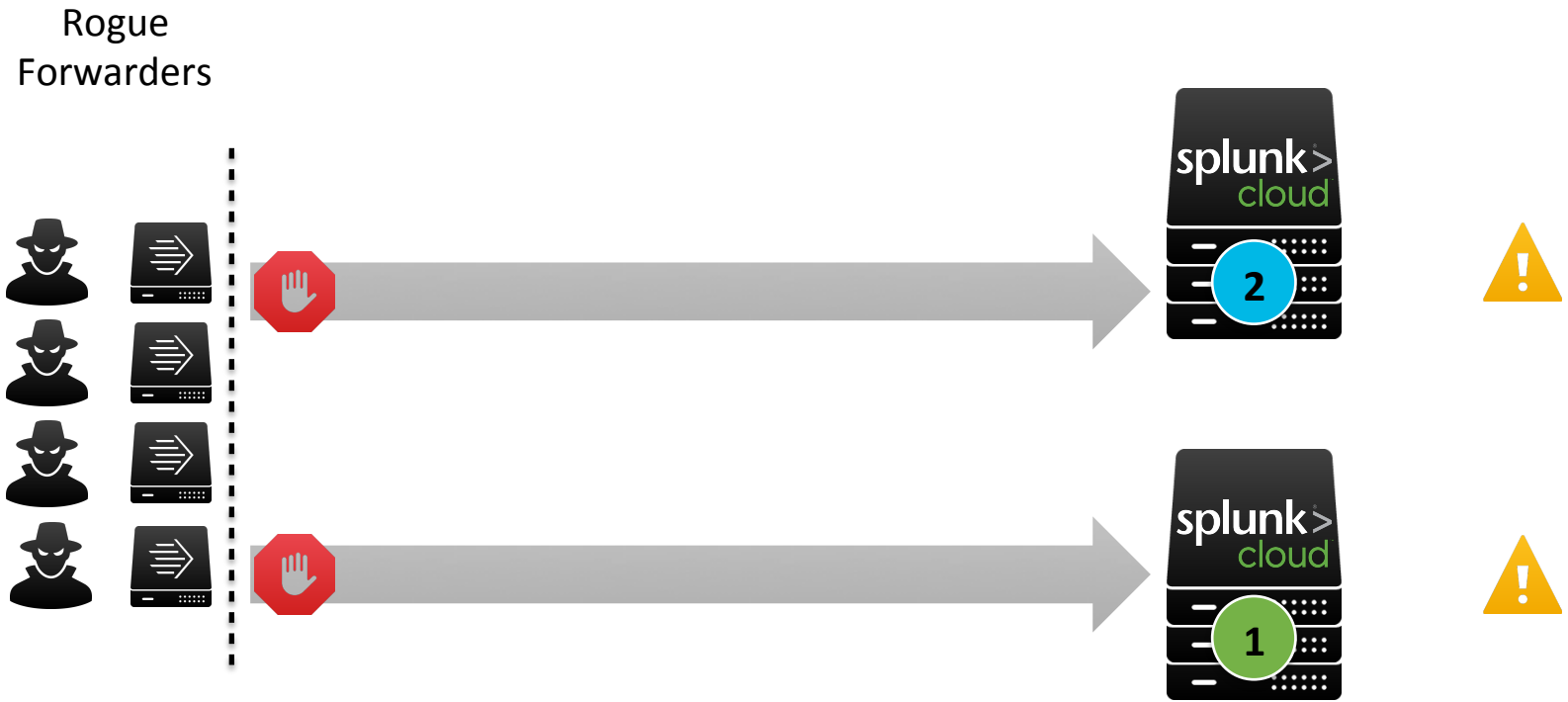
Customer
Forwarders



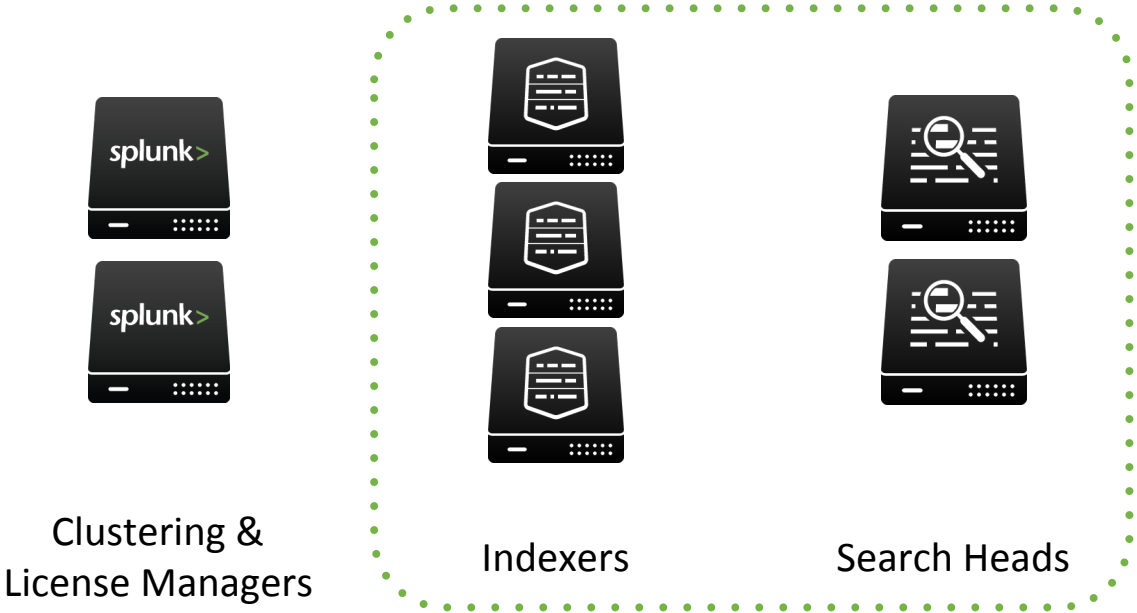
Authentication

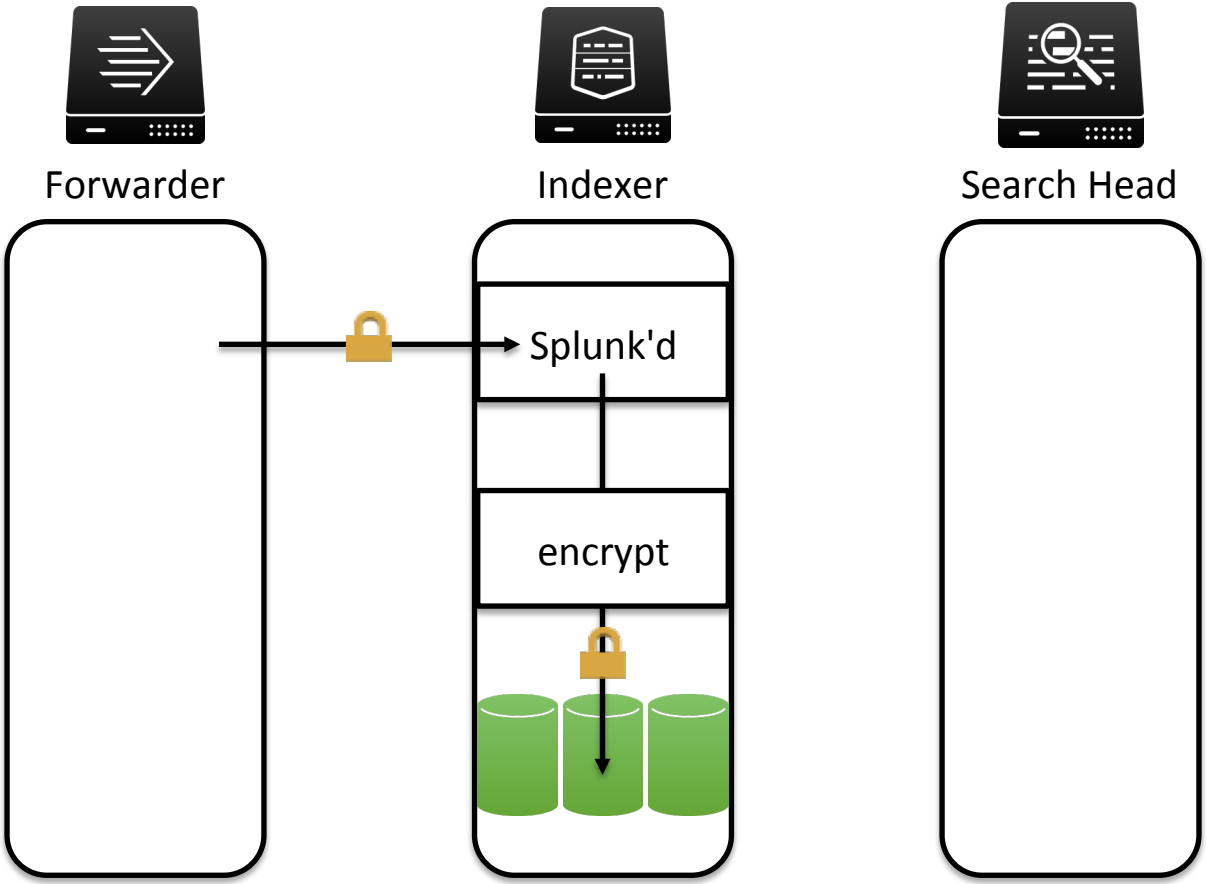


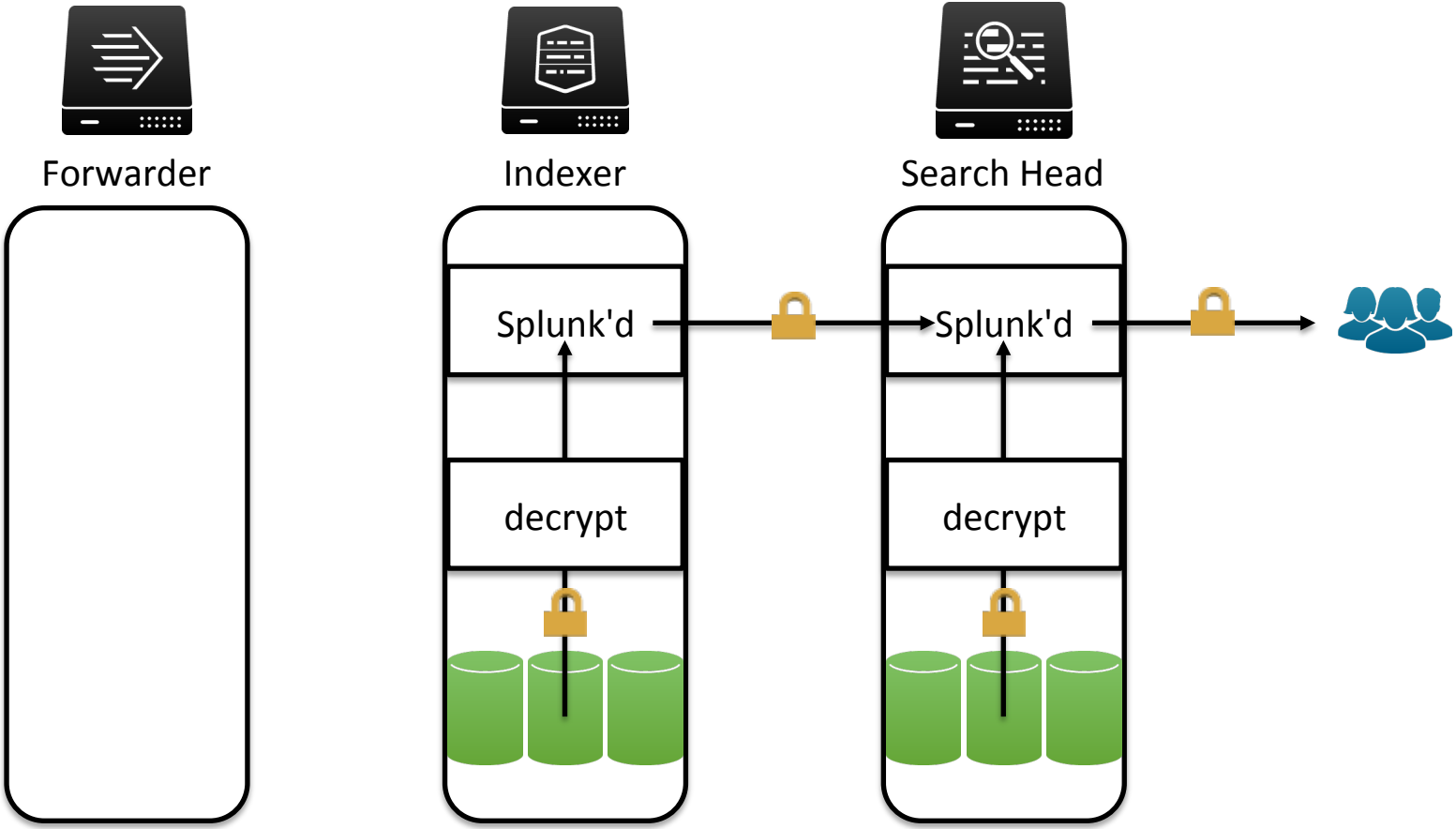
Authentication



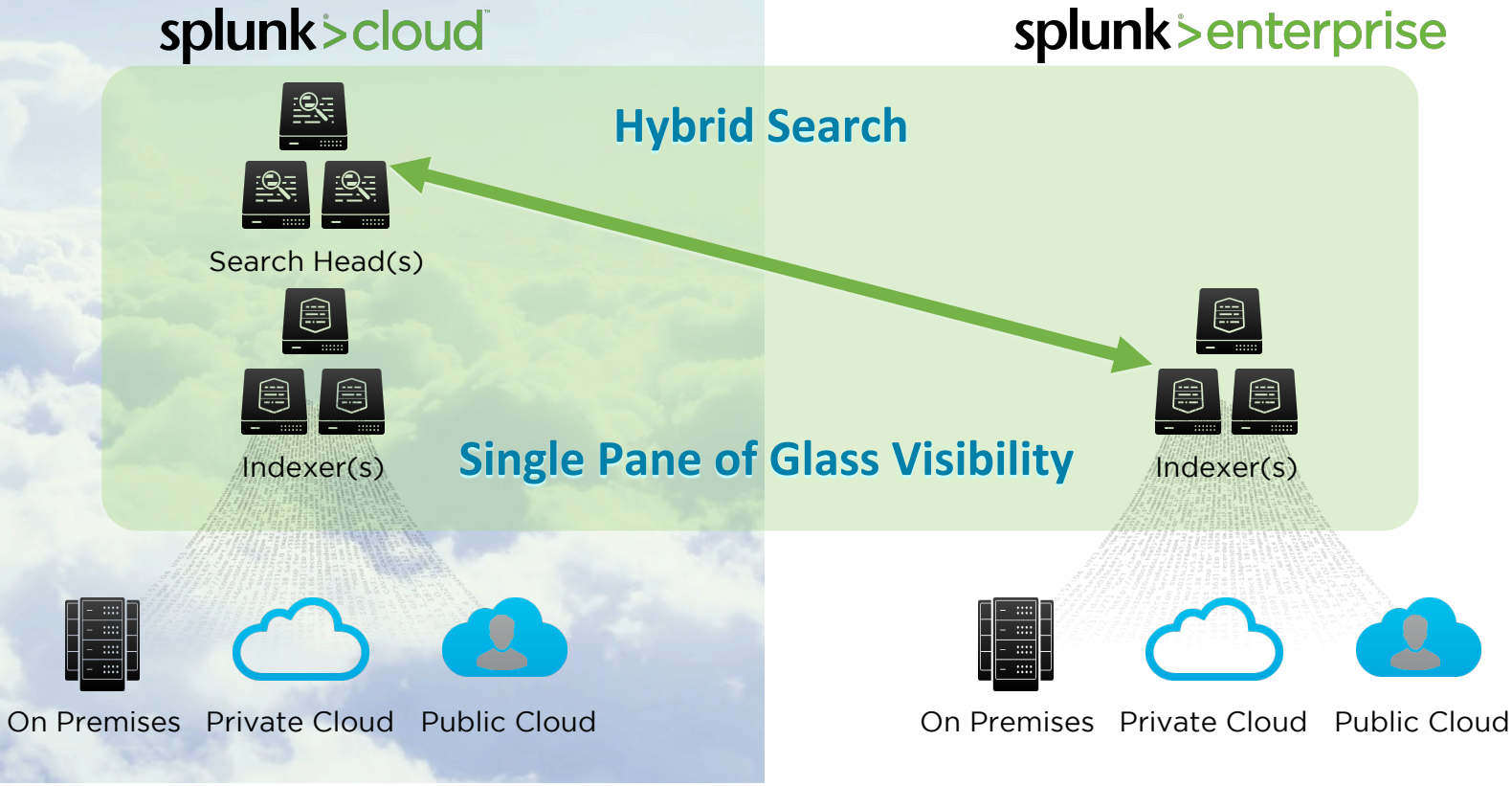
Encryption At Rest







Hybrid


splunk>cloud
splunk>enterprise
Hybrid Search
Search Head(s)
Indexer(s)
Single Pane of Glass Visibility
Indexer(s)
On Premises
Private Cloud
Public Cloud
On Premises
Private Cloud
Public Cloud

Wrapping Up

- Highly performant
- Highly available
- Built with security from the ground up
- Operationally automated
- A single pane of glass visibility with hybrid search

Thank You!

Questions?

Rajiv Battula
Software Engineer
rajiv@splunk.com

Nikhil Mungel
Sr. Software Engineer
nikhil@splunk.com