Architecting and Sizing your Splunk Deployment

Simeon Yep
Sr. Manager BD Tech Serv, Splunk
Karandeep Bains
Sr. Sales Engineer, Splunk

splunk>

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.

Objective

Show you how to build a robust and scalable Splunk deployment

Introduction

About Simeon

- 6+ years @ Splunk
- Experience:
  - Supporting, administering, and architecting large scale deployments
  - OEM, technical sales
  - Strategic Accounts, technical sales
- Based in HQ (San Francisco office)
- Currently:
  - Business Development, Technical Synergies

About Deep

- 7+ years @ Splunk
- Experience:
  - Supporting, administering, and architecting large scale deployments
  - OEM, technical sales
  - Strategic Accounts, technical sales
- Based in HQ (San Francisco office)
- Currently
  - Business Development, OEM

Agenda

- Sizing fundamentals
- Architecting fundamentals
- Deployment topologies

Sizing Fundamentals

splunk>

Sizing Fundamentals

- Understand the sizing factors
- Data volume
- Search volume

Sizing Factors

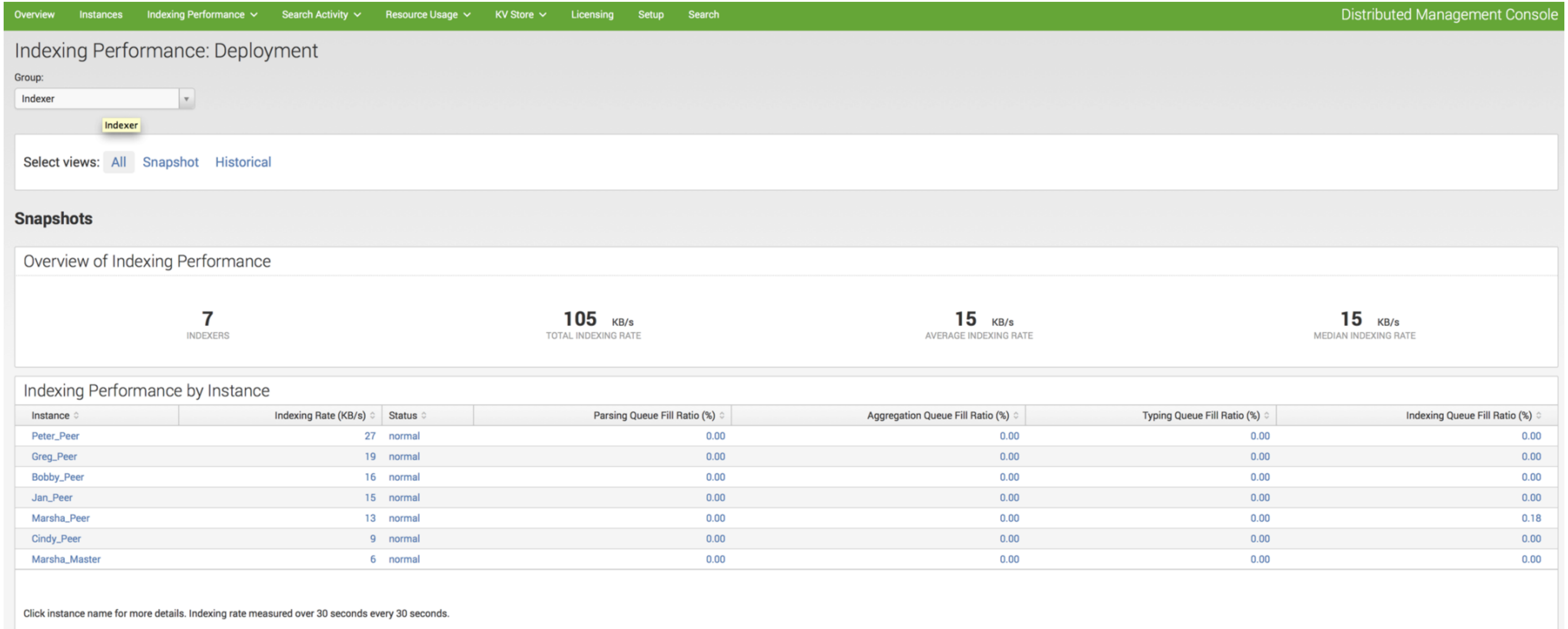
- How much data (raw sizes)?
  - Daily volume
  - Peak volume
  - Retained volume (archive size)
  - Future volume?
- How much searching?
  - Use cases
  - How many people? How often?
  - Apps
- Jobs
  - Summarization, alerting, reporting

Data Volumes

- Estimate input volume
  - Verify raw log sizes
  - Leverage _internal metrics to get actual input volumes
- Confirm estimates with actual data
  - Create a baseline with real or simulated data
  - Find compression rates (range from 30%-120%, typically 50%)
  - Determine retention needs
  - Clustering needs
- Document use cases
  - Use case determines search needs
  - Plan for expansion as adoption grows (search and volume)

Data Sizing Exercise

- Via filesystem
- Use the Splunk log files: metrics.log or license_usage.log
- Recommended:
  - Introspection data and dashboards in 6.2



Indexing Performance: Deployment

Group: Indexer

Select views: All Snapshot Historical

Snapshots

Overview of Indexing Performance

7	105 KB/s	15 KB/s	15 KB/s
INDEXERS	TOTAL INDEXING RATE	AVERAGE INDEXING RATE	MEDIAN INDEXING RATE

Indexing Performance by Instance

Instance	Indexing Rate (KB/s)	Status	Parsing Queue Fill Ratio (%)	Aggregation Queue Fill Ratio (%)	Typing Queue Fill Ratio (%)	Indexing Queue Fill Ratio (%)
Peter_Peer	27	normal	0.00	0.00	0.00	0.00
Greg_Peer	19	normal	0.00	0.00	0.00	0.00
Bobby_Peer	16	normal	0.00	0.00	0.00	0.00
Jan_Peer	15	normal	0.00	0.00	0.00	0.00
Marsha_Peer	13	normal	0.00	0.00	0.00	0.18
Cindy_Peer	9	normal	0.00	0.00	0.00	0.00
Marsha_Master	6	normal	0.00	0.00	0.00	0.00

Click instance name for more details. Indexing rate measured over 30 seconds every 30 seconds.

Search Volumes

- Gather use case information
  - How much ad-hoc searching?
  - How much background searching?
- Ad-hoc searching
  - Evaluate the data being searched
  - Evaluate the time duration (real-time vs historic)
  - Real-time searches are typically less overhead
- Background searching
  - Alerting and monitoring
  - General reports
  - Summary indexing

Search Volume Exercise

- Use the Splunk log files: audit.log
- Recommended:
  - Introspection data and dashboards in 6.2

Sizing Fundamentals

- Data capacity
  - Daily and peak
- User capacity
  - Concurrent and total
- Search capacity
  - Concurrent and total

*Document the use cases!!

Architecture Fundamentals

Architecture Fundamentals

- Splunk server roles: distributed/clustered deployments
- Reference server
- Rules of thumb
- Hardware factors

Splunk Distributed Roles

Search Head

(Search Head Captain)

LM

License Master

DS

Deployment Server

Indexer

CM

Cluster Master

Forwarders

Recommended Configurations

	Standalone	Indexer (Distributed)	Search Head (Distributed)	Indexer (Clustered)	Search Head (Clustered)	Cluster Master (Clustered)
Forwarder	*	*	*	*		
Searching	√		√	*	√	
Indexing	√	√	*	√		
Deployment Server		*	*			
License Master		*	√			*
Cluster Master						√
Search Head Captain			√		√	

√ common   * uncommon

What's a "Search Head Reference" Server?

- Sizing based on commodity x86 servers – 64bit
- 4 x quad-core CPUs at 2.0 GHz
- 12 GB of RAM – (16 GB is common)
- 64-bit OS
- 2x10k RPM local SAS drives in RAID 1
- Variations cause corresponding changes in performance/ requirements

What's an "Indexer Reference" Server?

- Sizing based on commodity x86 servers – 64bit
- 2 x six-core CPUs at 2.0 GHz
- 12 GB of RAM – (16 GB is common)
- 64-bit OS
- Local or attached storage (1200+ IOPs)
- Variations cause corresponding changes in performance/ requirements

Rules of Thumb

- These all have exceptions and qualifications
- 1 Reference indexer per 250 GB/day
- 1 Reference search head per 20-40 jobs
- 1 Deployment server per 3,000 polls/min
- Replication later….

How Many Indexers?

- Rule of thumb says: 1 per 250 GB/day
- Leaves room for:
  - Daily peaks
  - Light searching and reporting for about 5 concurrent users
- Need more indexers for:
  - Heavy reporting
  - More users
  - Slower disks, slower CPUs, fewer CPUs

How Many Search Heads?

- Rule of thumb says: 1 per 20 – 40 concurrent jobs
- Limit is concurrent queries
- Search Query may utilize up to 1 CPU core
- Only add first search head if ≥3 indexers
- Don't add search heads - add indexers. Indexers do most work
- But you need more if:
  - Running a lot of scheduled jobs on the search head

How Many Deployment Servers?

- Rule of thumb says: 1 per 3000 polls/minute
- Just use one deployment server, and adjust the polling period
- Small deployments can share the same Splunkd
- Low requirement for disk performance (good candidate for virtualization)
- Windows OS – 1 per 500 polls/minute
- Or use something other than deployment server

More is Better?

- CPUs
  - Search process utilizes up to 1 CPU core
  - Indexers still need to do the heavy lifting (search exists on indexer AND search head)
  - Limited benefit for indexing (up to 4 CPU cores for indexing)
- Memory
  - Good for search heads and indexers (16+ GB)
- Disks
  - Faster is better (15k rpm) or SSD
  - More disks in RAID 1+0 = Faster
  - SSDs can provide benefit for rare term searches and many concurrent jobs

Performance and Sizing Tips

System Change	Search Speed	Indexing Speed
Faster disks	++	++
Add an indexer	++	++
Add a search head	+	
Report acceleration/summaries	++	

Performance and Sizing Tips

System change	Search Speed	Indexing Speed
Optimize searches	+++	
Optimize field extraction	+	
Optimize input parsing		+
Faster CPU	+	+

Capacity → Architecture

- Sizing recipe
  - Capacity
  - Rules of thumb determines number of servers
- Building blocks for architecture

Architecture Factors

- What are my sizing requirements?
- Where is the data?
- Where are the users?
- What is the security policy?
- What are the retention and compliance policies?
- What is the availability requirement?
- What about the cloud?

Architecture Factors

- What are my sizing requirements?
  - Data capacity
  - Search capacity
  - User capacity
- Obtained from the sizing process

Architecture Factors

- Where is the data?
  - Local or remote to the indexing machine
  - If remote – use forwarders when possible
  - Index in local data center (zone) or index centrally
  - Persist network data to disk as a best practice
  - Use intermediate forwarders to distribute data
- Where are the users?
  - User experience affected by search head location
    - Time zone tuning
    - Distributed search over LAN vs WAN

Architecture Factors

- What is the security policy?
  - Apply user security policies
    - Auth method
    - Roles
    - Filters
  - Apply physical security policies
    - Index location

Architecture Factors

- Retention, compliance, governance
  - Where is the data allowed to be?
  - Where is the data not allowed to go?
  - Where must the data go?
- Availability
  - Local failover, fault-tolerance, clustering
  - Geographic disaster recovery/fault-tolerance
  - Index replication!

Architecture Factors

- Cloud Considerations
  - Authentication restrictions
  - Data transfer costs
  - Security – SSL Tunnel
  - Zones

Architecture → Topologies

- What are my sizing requirements?
- Where is the data?
- Where are the users?
- What is the security policy?
- What are the retention and compliance policies?
- What is the availability requirement?
- What about the cloud?

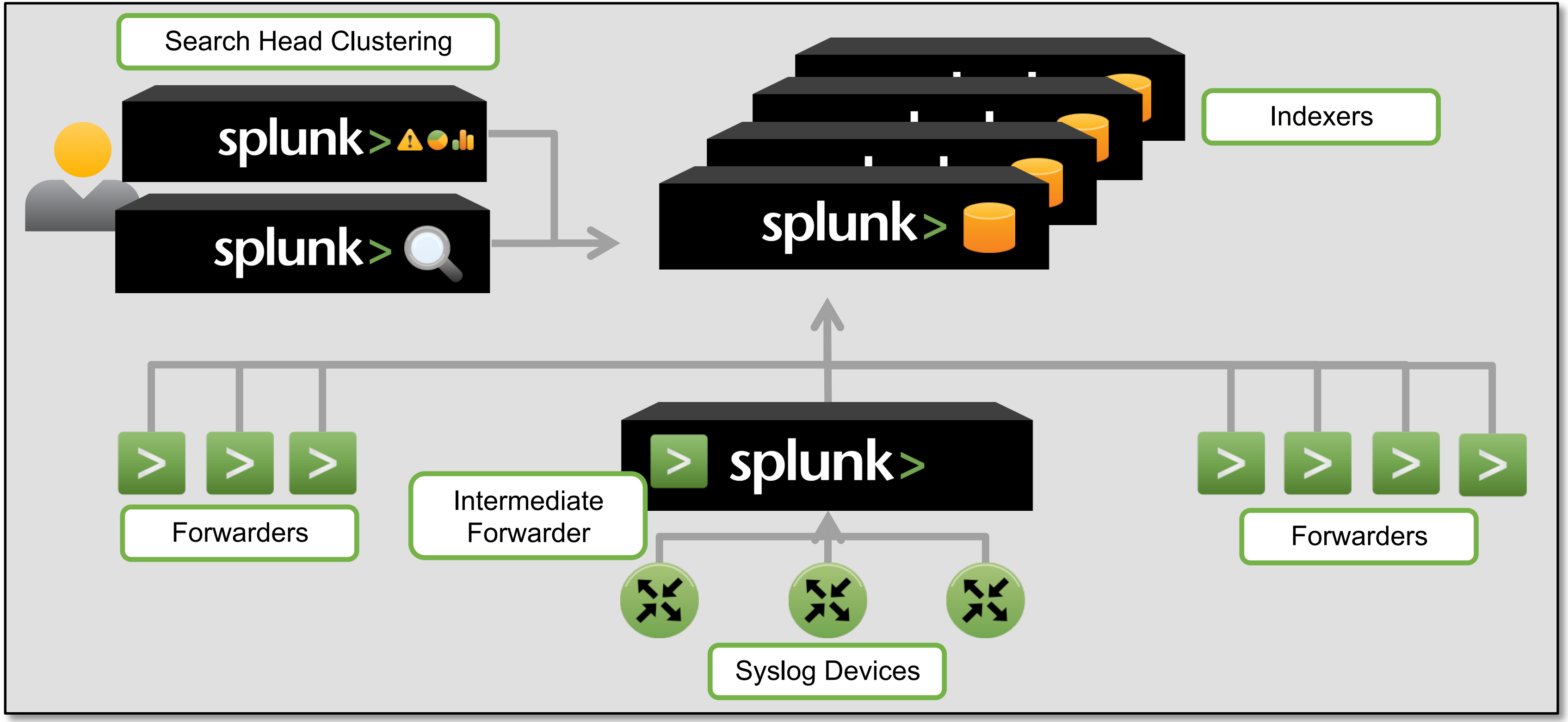
Topologies

splunk>

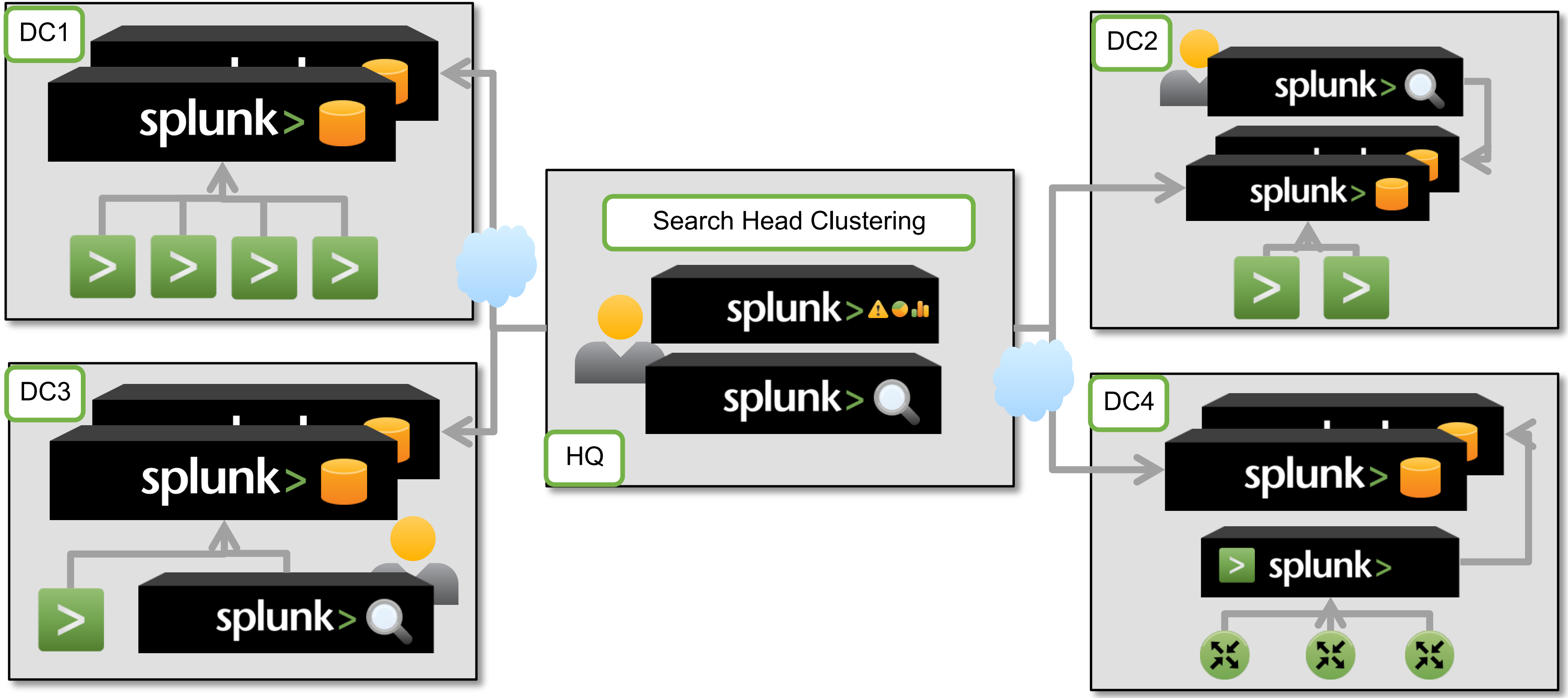
Architecture Factors → Topology

- Topology Examples
  - Centralized
  - Decentralized
  - Hybrid
  - Index replication
  - Search head clustering

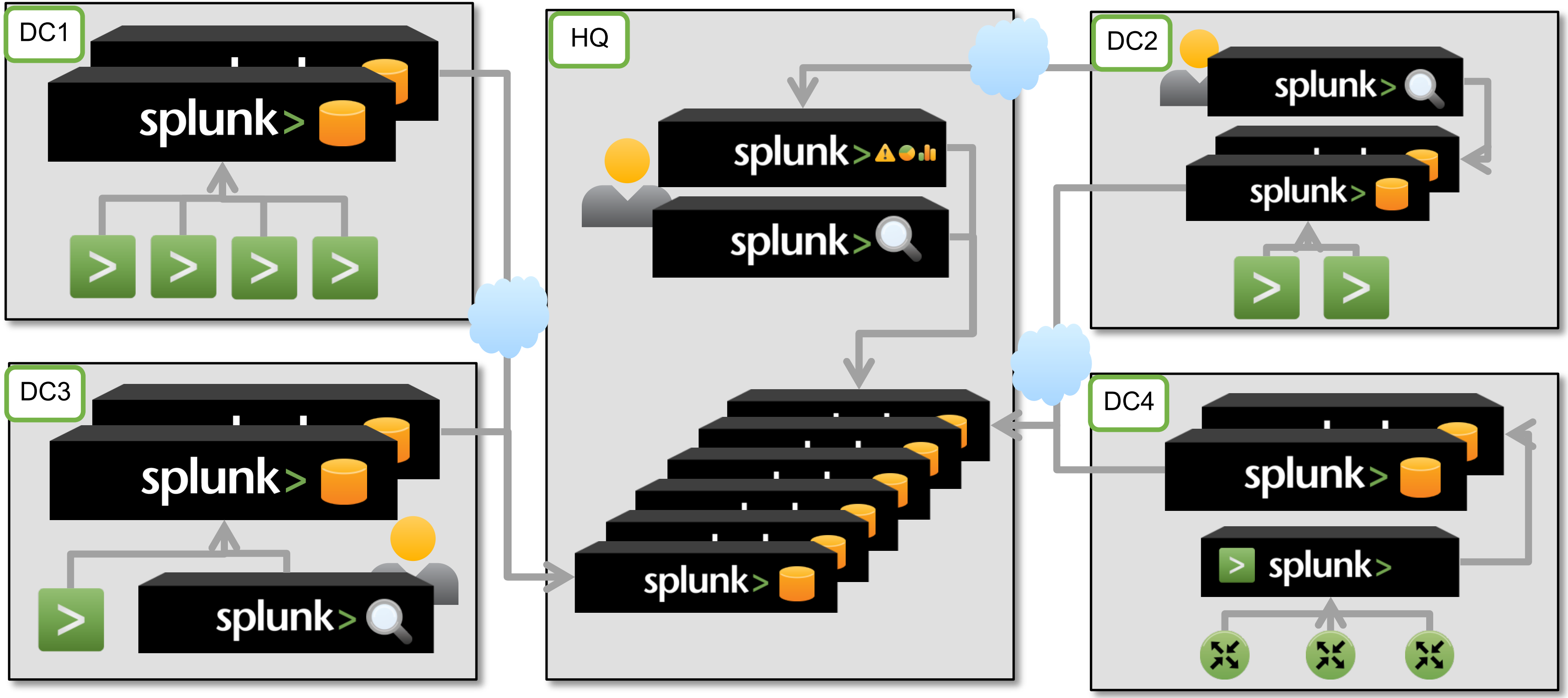
Centralized Topology



Decentralized Topology



Hybrid Topology



Index Replication (aka Clustering)

- What is it?
  - Indexes are replicated to 1 or more indexers (tunable)
  - Splunk cluster master controlled
- Basics
  - Master node (manages indexing and searching location)
  - Distributed deployment
  - NOT = “Index and Forward “
- HA vs DR
  - HA - Data is made available on 1 or more indexers in one location
  - DR - All data exists in multiple locations

Clustering

- Replication factor
  - Determine the number of copies of data to maintains
- Search factor
  - Determine the number of searchable copies of the data
- Data retention equation
  - General rule of thumb:
    - 15% for each RF; 35% for each SF
  - Example:
    - 100 GB of raw = 50 GB on disk.
    - RF – 2; SH – 2;
      - ((.15 * 2 RF * 100GB) + (.35 * 2 SH * 100GB)) = 100 GB

Index Replication Reminders

- Logically, multiple copies of the data
  - Increase in I/O, CPU, and disk requirement
  - Need more Indexers
- Increase in search factor vs replication factor
  - (rawdata + tsidx) vs. (only rawdata)
- Multi-site replication
  - WAN Load
  - Search head affinity

Search Head Clustering (aka NOT SHP)

- What is it?
  - Uses Raft protocol
  - Splunk head captain controlled
- Basics
  - Ability to group search heads into a cluster in order to provide highly available search services
  - NOT NFS based
  - Replication using local storage
- How does it work?
  - Group search heads into a cluster
  - A captain gets elected dynamically
  - User created reports/dashboards automatically replicated to other search heads

Scaling and Expansion

- Add to your indexer pool for more performance or capacity
  - Mixed platform and hardware is not recommended
- Use search head clustering for more UI capacity
  - Does not requires NFS
- Create new indexes for new data types
  - Follows best practices

Final Thoughts

- Sizing is more than data volume—it's also search load
- Centralized architecture is the baseline
- Variations on architecture are driven by
  - Sizing
  - Data location
  - User location
  - Retention/Access/Governance
  - Availability requirements

More Information

- Contact:
  - syep@splunk.com
  - deep@splunk.com
- Documentation: http://docs.splunk.com
- Answers: http://answers.splunk.com
- Other presentations
  - Multisite Indexer Clustering with Search Affinity – 10/9/2014 @ 9:00 am
  - Splunk Search Acceleration Technologies – 10/9/2014 @ 10:30 am

THANK YOU

splunk>