splunk> .conf2017

# Introducing Splunk Validated Architectures (SVA)

## Optimizing Your Path To Success With Splunk

Sean Delaney | Principal Architect
Stefan Sievert | Staff Architect

September 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.



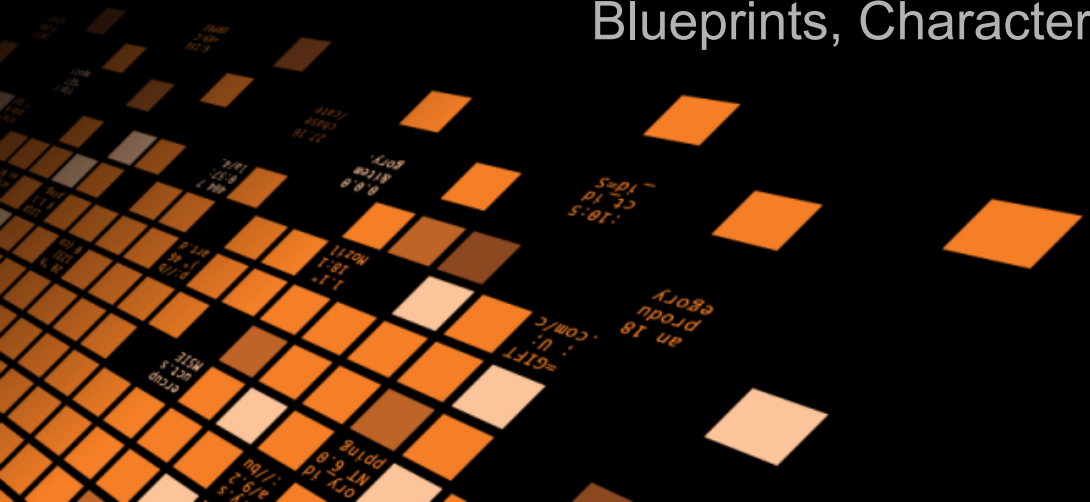
splunk> .conf2017

# What Is This About?

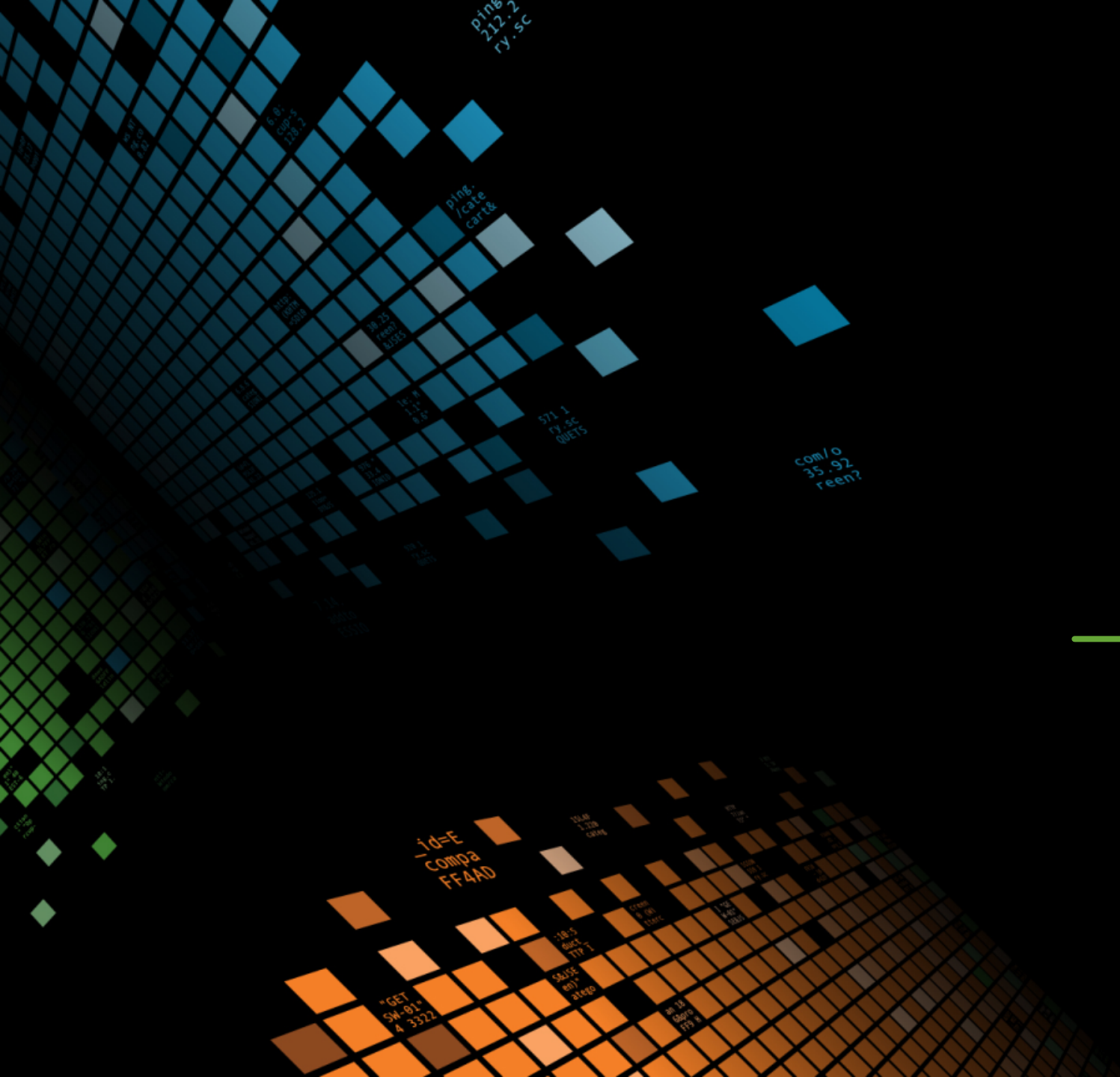
SVA Definition

# Proven reference architectures for stable, efficient and repeatable Splunk deployments

Blueprints, Characteristics And Architecture Best Practices



splunk> .conf2017



# Goal & Scope

Why SVAs?

# Benefits

Why you want to apply SVAs

- Empower customers to design and deploy Splunk more confidently
- Prevent snowflakes that are not scalable, reliable and/or maintainable
- Increase Customer Success
- Accelerate your time to value and agility when growing/scaling
- Minimize TCO for Splunk

# In Scope For Svas

## Components Of A SVA

- **Diagrams**
  Visual representation of the reference architecture

- **Characteristics**
  Written description of fitness-for purpose and limitations

- **Tier-Specific Considerations and Best Practices**
  What to look out for when building out a Splunk deployment

# What Svas Do Not Address

## Out Of Scope Items

- Deployment technologies, like operating systems & server hardware, since they are considered implementation choices

- Deployment sizing involves understanding data ingest and search volumes as well as search use cases and generally does not affect the deployment architecture

# Who Is This For?

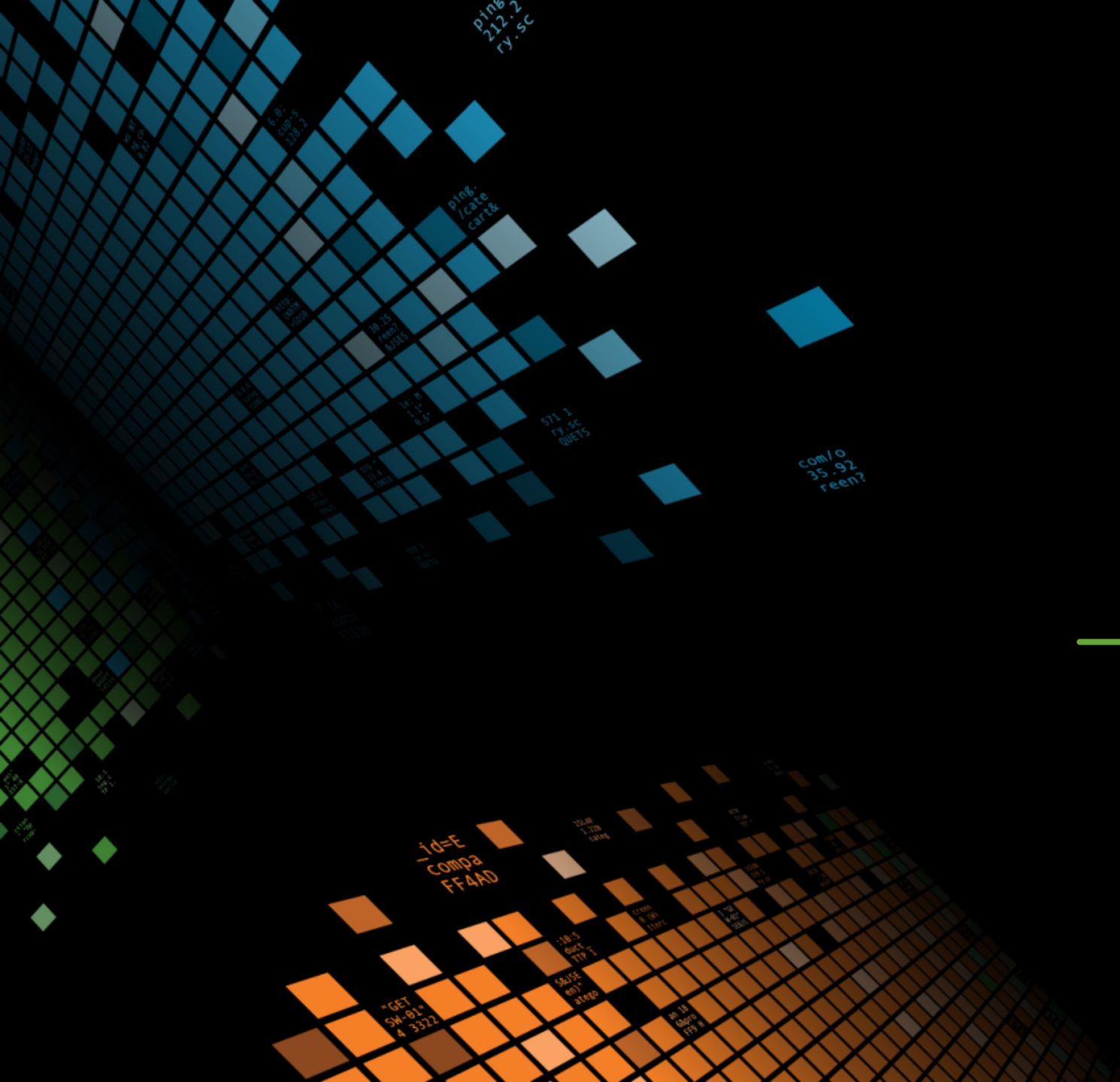
Intended Audience

splunk> .conf2017

# Relevant Personas

## Who Should Care

- **Enterprise Architects**
  Responsible for architecting Splunk deployments to meet enterprise needs
- **Consultants**
  Splunk consultants that provide Splunk architecture, design and implementation services
- **Splunk Administrators**
  Staff that is responsible for managing Splunk lifecycle
- **Managed Service Providers**
  Entities that deploy and run Splunk as a service for customers



# Design Focus

Foundational Pillars

splunk> .conf2017

# Foundational Pillars

Availability

Performance

Scalability

Security

Manageability

splunk> .conf2017

# Design Principles

## Pillar-oriented guidelines

- Design principles are documented and assigned to the appropriate pillar
- Each tier-specific recommendation references the underlying design principle(s)

# Design Principle Examples

## Pillar: Security

- Design for a secure system from the start
- Employ state-of-the art protocols for all communications
- Allow for broad-level and granular access to event data
- Employ centralized authentication
- Implement auditing procedures
- Reduce attack or malicious use surface area

# Tier-Specific Recommendations Example

## Tier: Search

- Minimize network path length between SHs and indexers - PERF
- Avoid using multiple, independent SHs – MGMT, SCAL, AVLB
- Consider LDAP Auth whenever possible – MGMT, SEC
- Ensure sufficient cores for concurrent search needs – PERF, SCAL
- Etc.

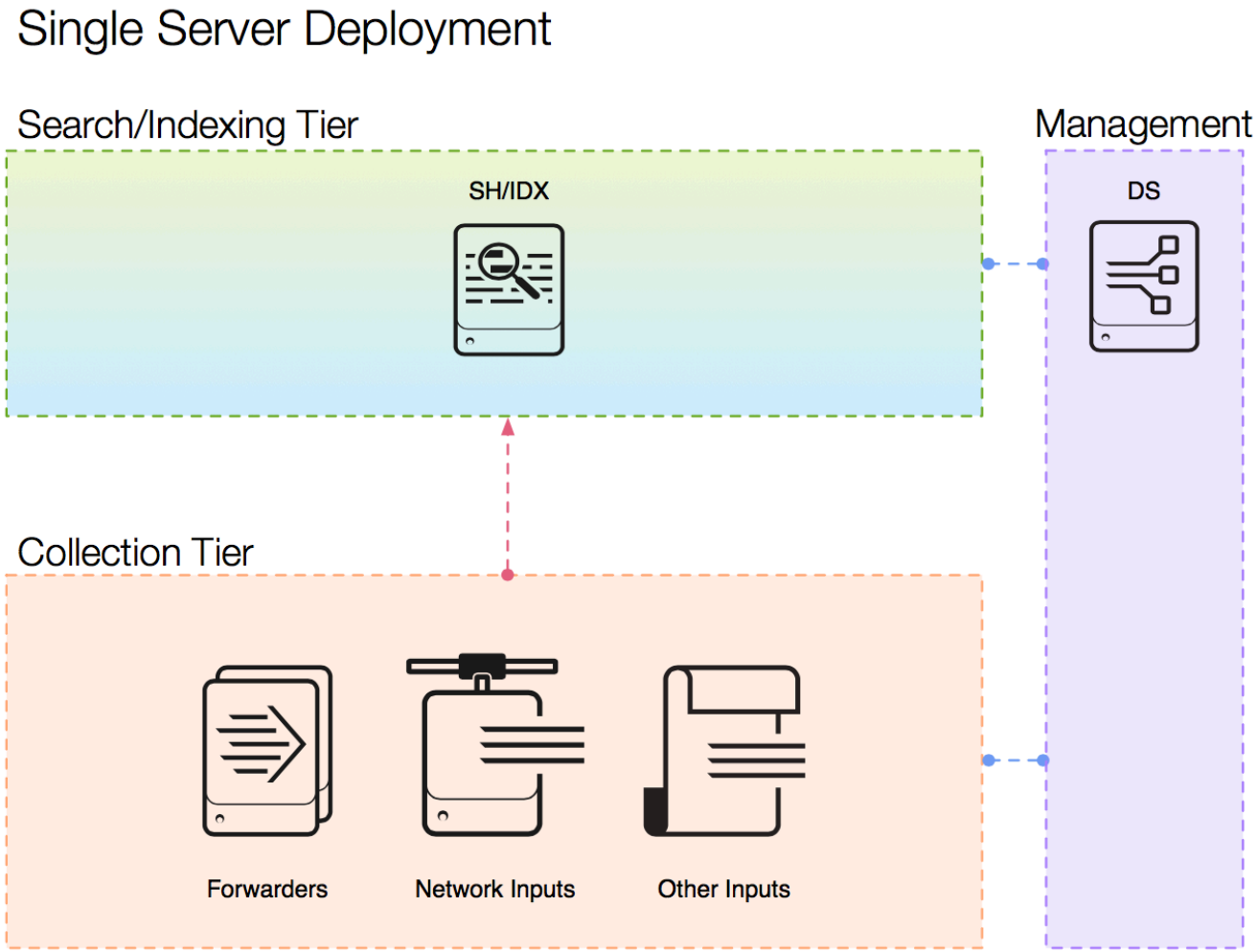
# Topology Examples

A Sneak Peek

splunk> .conf2017

# Example 1: Single Server

## Topology Diagram



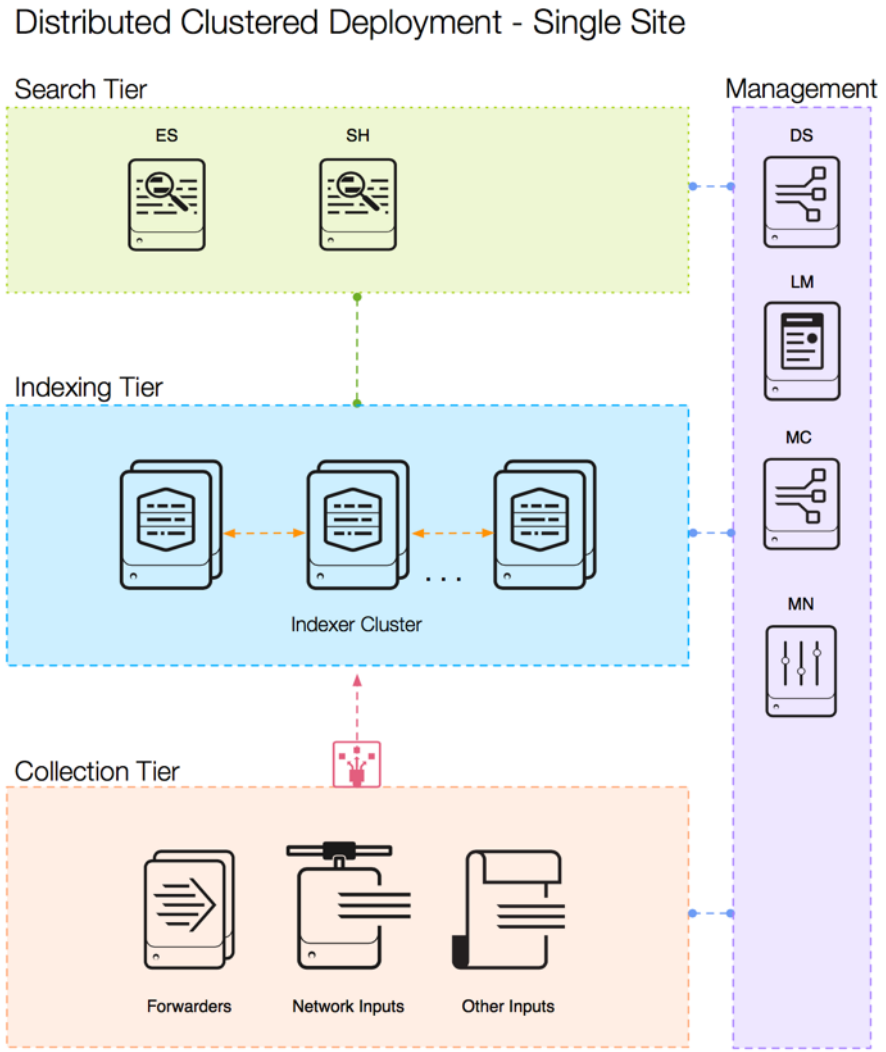
# Example 1: Single Server

## Characteristics

- Departmental, non-critical use cases up to ~300GB/day (Data Onboarding Test environments, small Enterprise log management)
- No High Availability for Search/Indexing
- Scalability limited by hardware capacity, but easy migration path to a distributed deployment exists
- Simple Management

# Example 2: Distributed Single-Site Cluster

## Topology Diagram




splunk> .conf2017

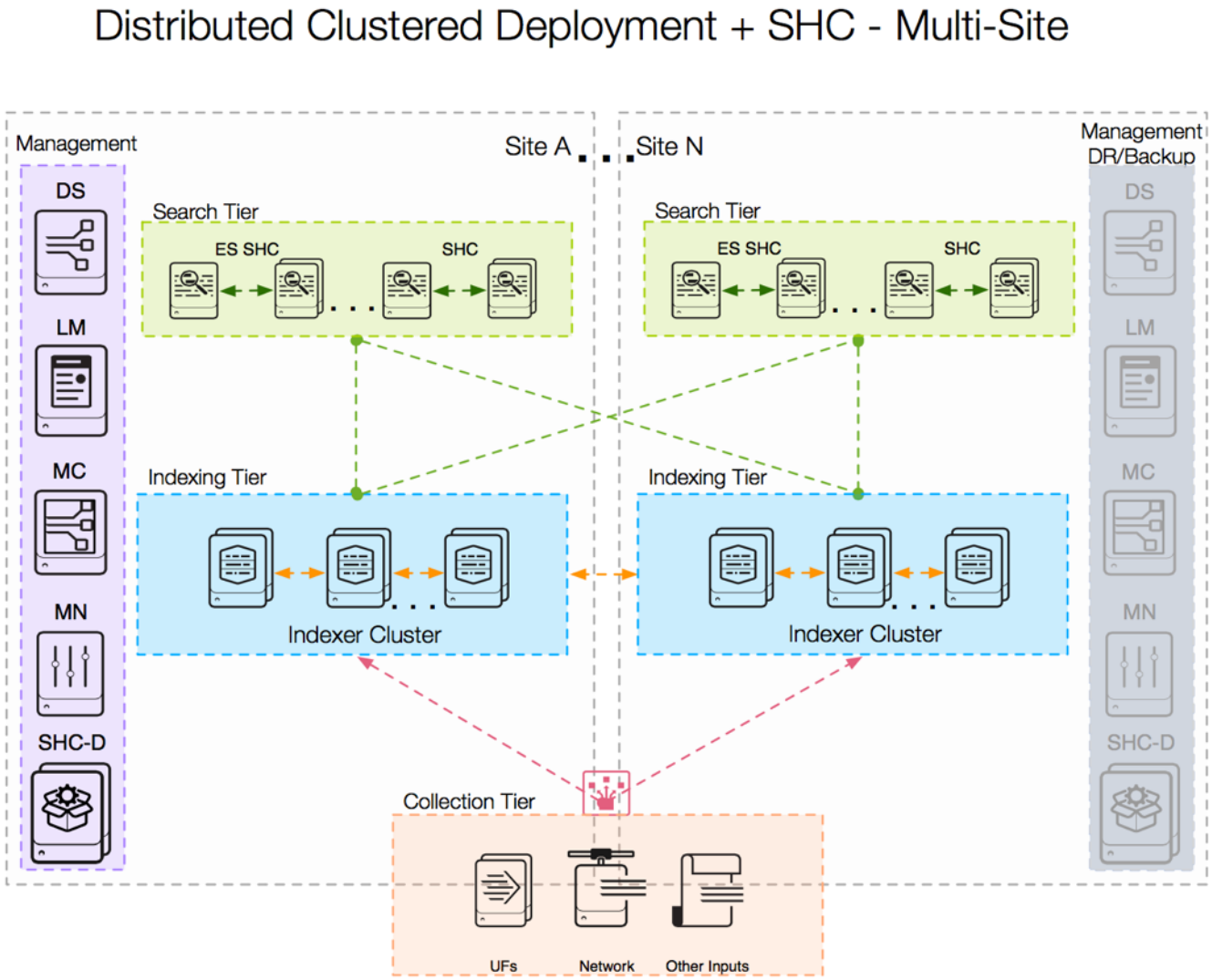
# Example 2: Distributed Single-Site Cluster

## Characteristics

- High Availability for data ingestion and search peers via configurable data replication
- Horizontally scalable indexing to multi-TB/day
- Total number of unique buckets in indexer cluster limited to 5MM as of Kimono (6.6), 15MM total buckets
- No DR capability in case of data center outage
- No HA capability for SH tier
- ES (if used) requires dedicated SH
- Replication is non-deterministic, cluster decides on replication target node

# Example 3: Distributed Multi-Site Cluster

## Topology Diagram



# Example 3: Distributed Multi-Site Cluster

## Characteristics

- Provides protection against site failure
- Adds Search Head Clustering to the search tier.
- Ideally, continuous operation of Search Head tier, when properly configured
- Dedicated ES SHC required
- Search head capacity is shared and (scheduled) search artifacts are replicated in each SHC
- WAN latency must be <100ms

# How To Choose The Right SVA?

You Have To Pay For Getting Bling!

splunk> .conf2017

# Topology Feature Matrix

| | Single Server | Distributed | Single-Site | Multi-Site | +SHC |
|---|---|---|---|---|---|
| Ingest HA (+search peer HA) | | ● | ● | ● | n/a |
| Search Tier HA | | | | | ● |
| Horizontal SH Scaling | | | | | ● |
| Horizontal IDXR Scaling | | ● | ● | | |
| Disaster Recovery/Site failover | | | | ●[1] | ● |
| Simple Management | ● | | ● | ● | |

(1) Management roles (CM, LS, etc.) may need to be failed over manually

splunk> .conf2017

# You Pay For What You Get!

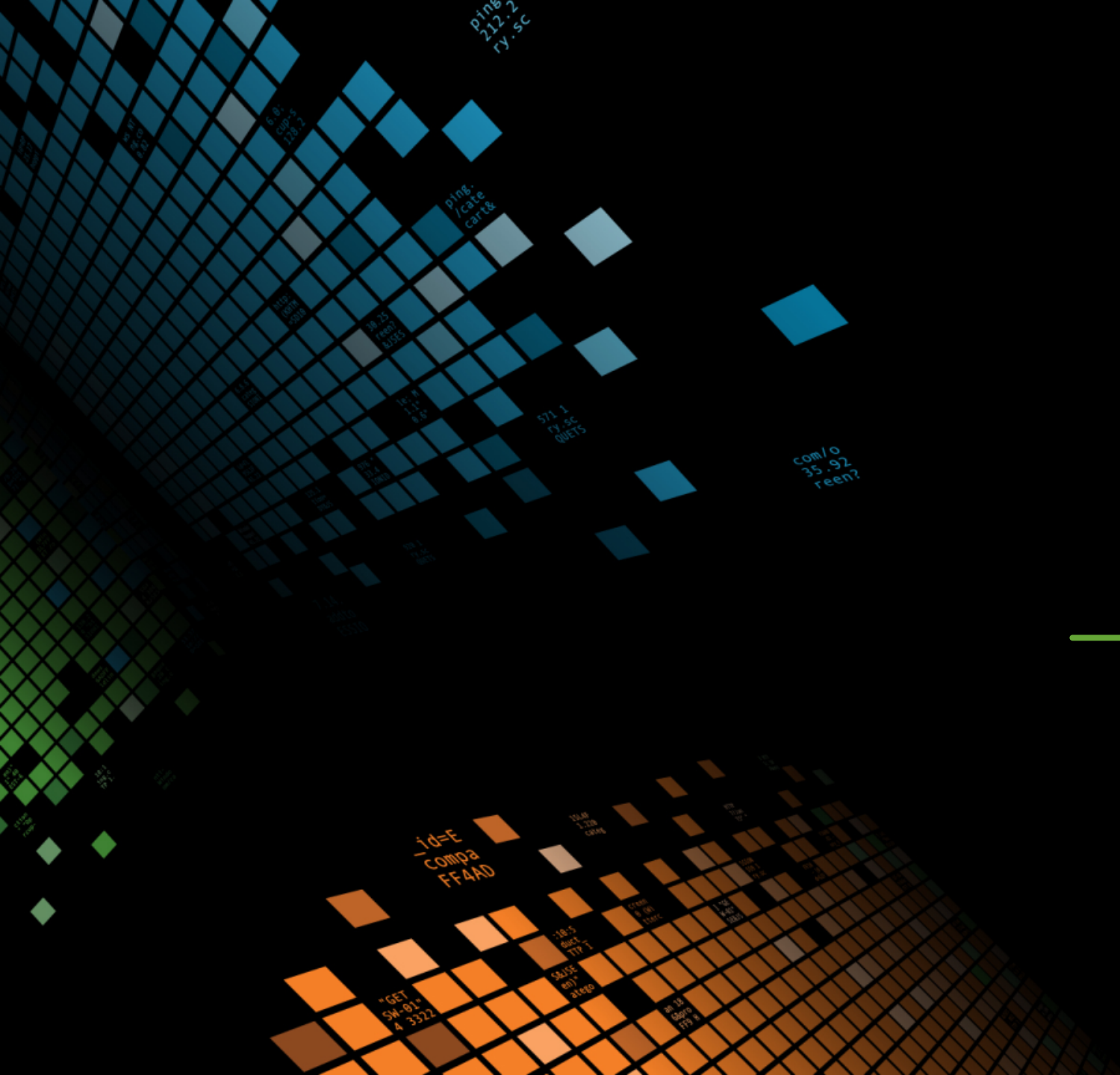
## How architecture choices affect TCO

| | Availability | Scalability | Cost |
|---|---|---|---|
| **Single-Server** | low | limited | fixed |
| **Distributed** | Ingest only | unlimited | Linear increase with node count |
| **Clustered, Single** | Ingest & Search (on indexers) HA | Bucket count limits | More nodes/storage for same ingest (RF) |
| **Clustered, Multi** | Ingest & Search, DR (on indexers) | Bucket count limits, WAN bandwidth | See above + WAN bandwidth cost |
| **Added SHC** | Search tier HA | Max. 50 SHC members | Linear increase with node count, need LB |

# What Are We Saying?

- Overbuilding a Splunk deployment results in
  - A more complex deployment that is…
  - Harder to manage (operate, troubleshoot, etc.) and support and will…
  - Cost you a lot of money for infrastructure and people

- Right-sizing a deployment to meet your requirements will
  - Provide you with the simplest architecture possible that…
  - Allows you to minimize your TCO for Splunk



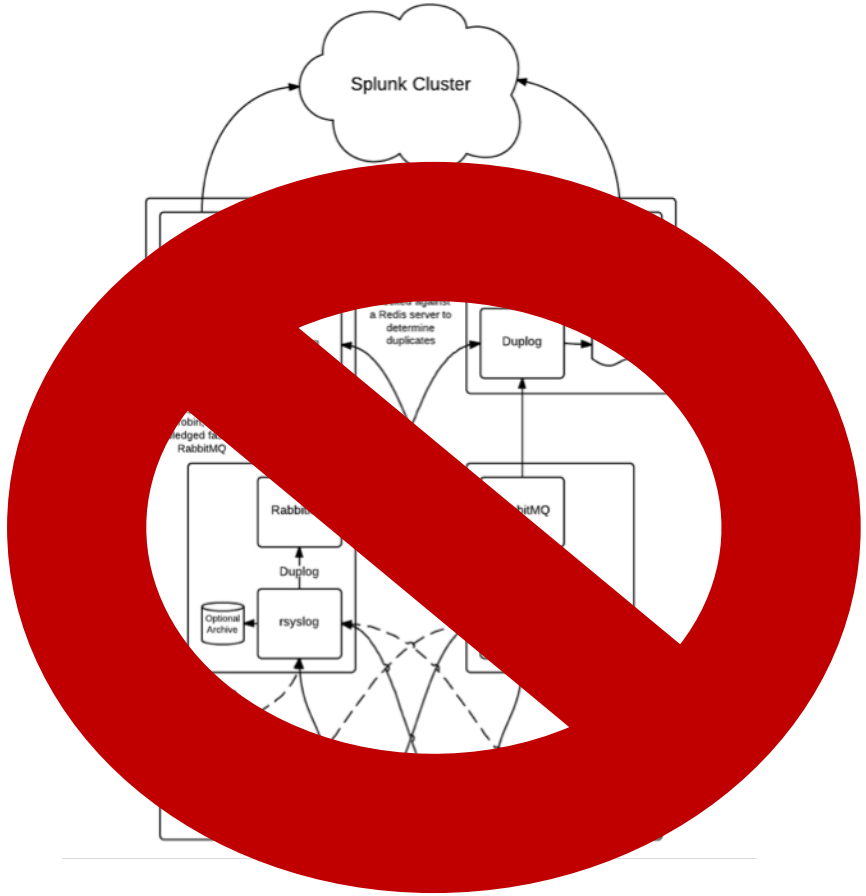
# #FAIL

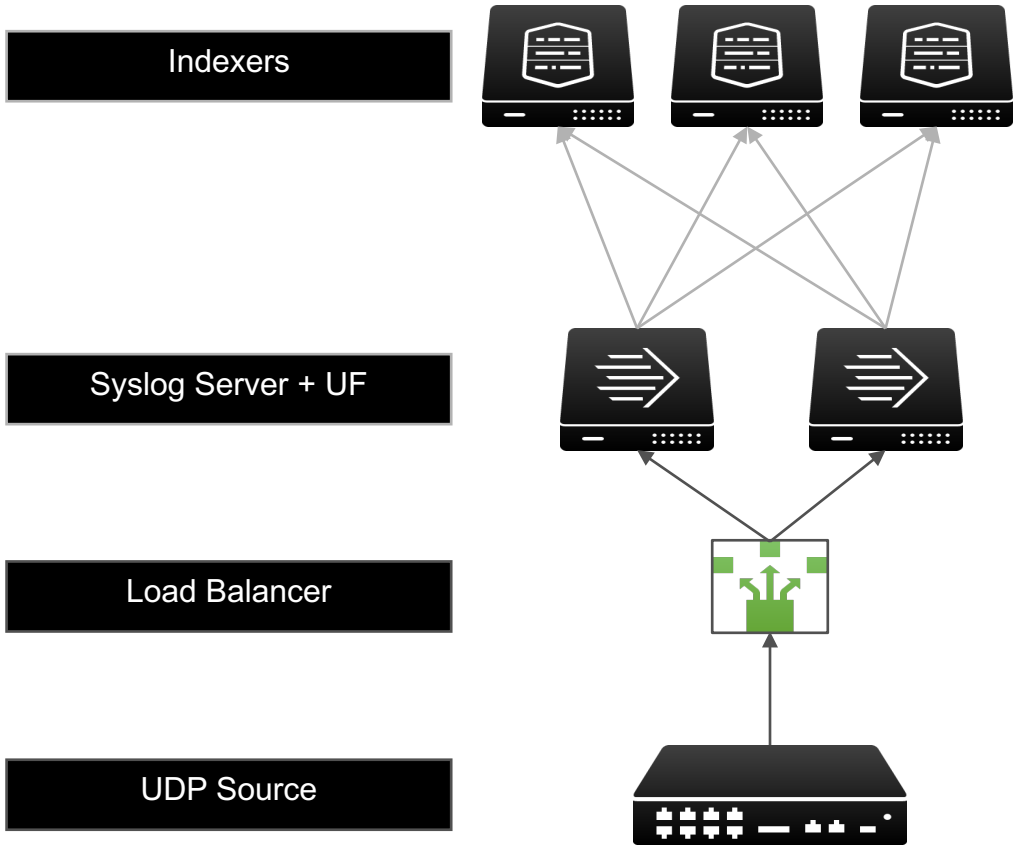
What Svas Are Trying To Prevent

splunk> .conf2017

# #FAIL 1: Syslog Data Collection

## Trying to prevent UDP data loss

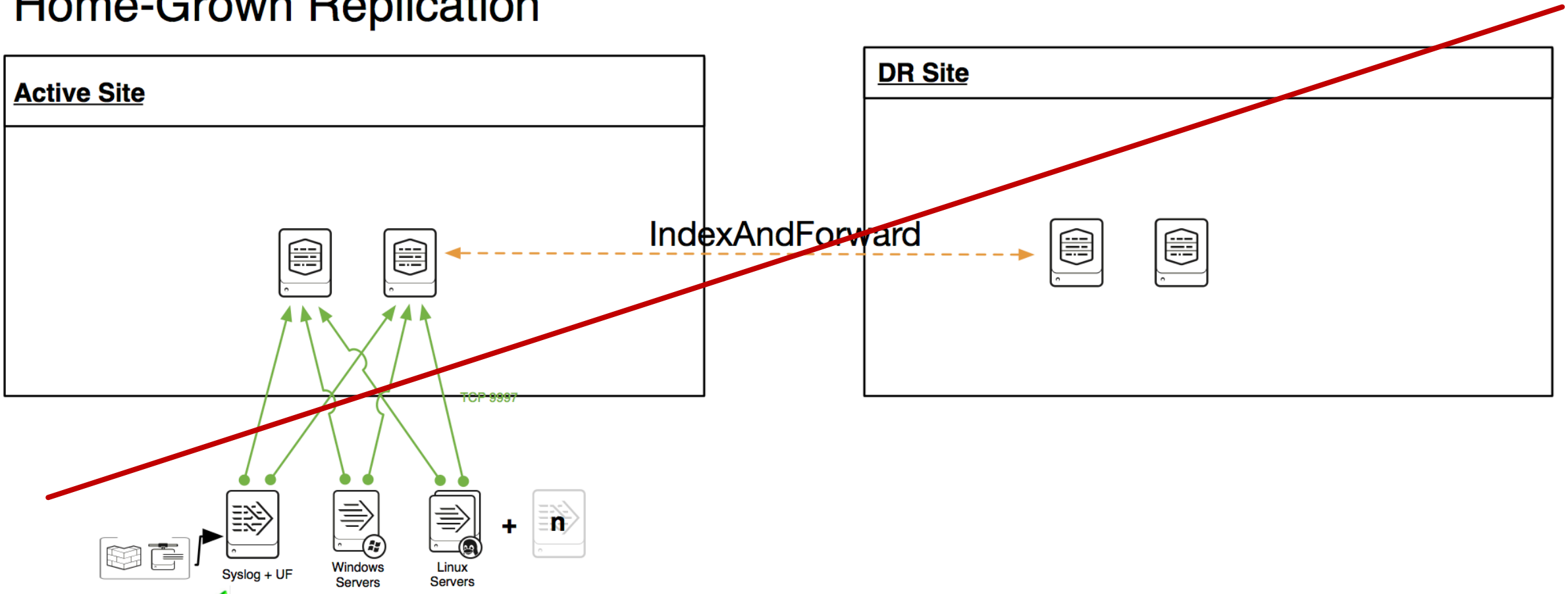


# #FAIL 2: IndexAndForward

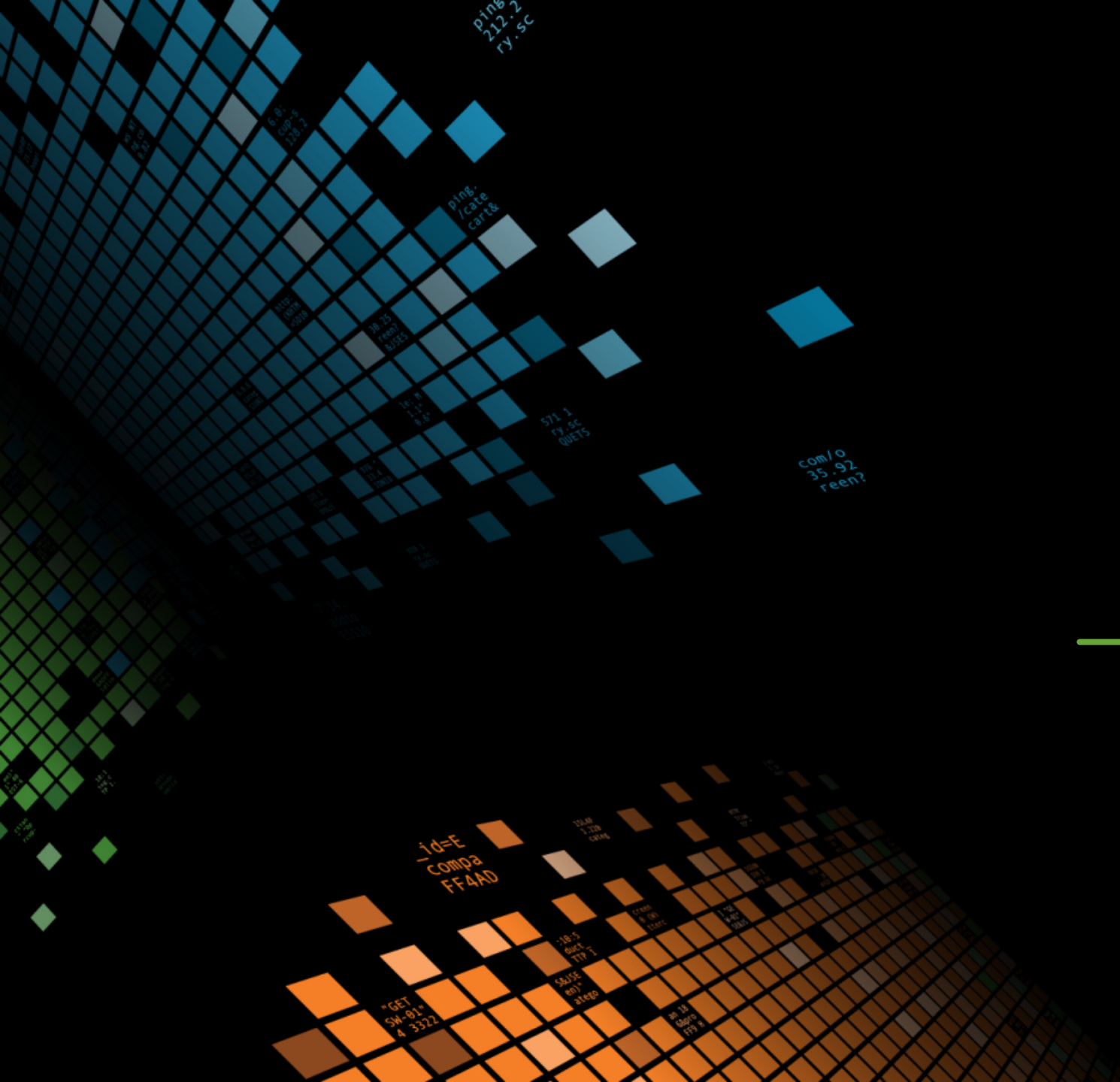
## Covering the DR case

### Home-Grown Replication




**Use Multi-Site Clustering for HA/DR needs**

splunk> .conf2017



# Summary

It's A Wrap!

splunk> .conf2017

# SVAs For The Win!

## A step-by-step guide

**Step 1**

**Identify and define the requirements of your organization/customer**

Don't add 'sexy' things if they are not needed

**Step 2**

**Match requirements to the proper topology using the characteristics**

You will get the required topology to meet your needs

**Step 3**

**Build out the topology using tier-specific recommendations**

You will have a proven architecture

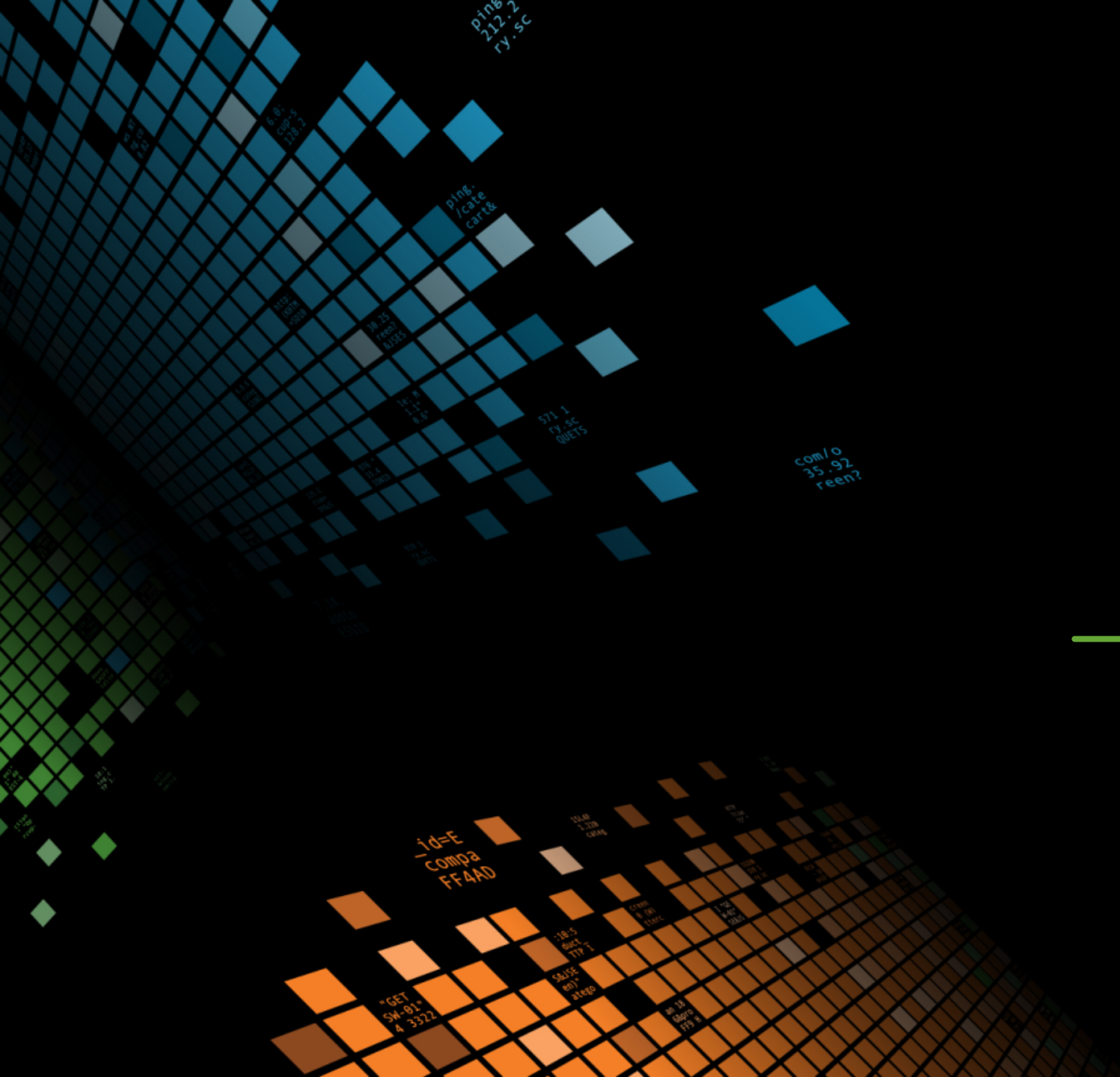
**Step 4**

**Choose implementation details**

OS choices, Capacity planning, Sizing, Staffing

# Where Is It?

- SVAs will be published as a **White Paper** in the splunk.com under the **Resources** section
- We will update the content as the product feature set introduces future changes
- We appreciate your feedback!
  - Do you think this is useful content?
  - What would make it better?
  - **Please let us know via your .conf app feedback. And thank you!**



# Q&A

splunk> .conf2017

# Thank You

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