

In this video...

- Use whatever you have
- Data pipeline
- Splunk components
- Distributed / Non-distributed / Clustered

CYB7A7Y

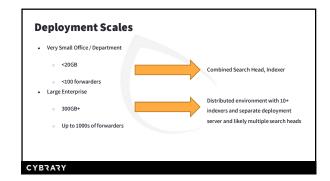
Data Pipeline Input Parsing Indexing Searching

| Scheduled searches, alerts, dashboards Distributes searches to indexers Watchboard Watch | Search Heads | | | |
|--|--|--|---|--|
| Double late southers to indexes ANATY Indexers Receive, index, store data South data based on search head Service data based on search requests from search head Service data based on search re | Search management | | | |
| Table 2 A Service of the service of | Scheduled searches, alerts, dashboards Distributes searches to indexers | | | |
| Indexers Breche, Index, store data Secret data based on search requests from search head Secret data based on search re | arko estarorlas — Age Seico Likovoria e von Didelek Mojelik Jainik Geldekelik | ■ Annicolor * ■ Missippi * Selling * Acting * Map * [First G] ■ Selling & Papenting ■ Selling & Papenting | | |
| Acceptance of the state of the | arch ter stands here | unt Stroom * Q | | |
| Idexers Receive, index, store data Search data based on search neglests from search head STARY Index - noun data repository | Cores Servis : fave to Servis 'you are not senter the seast features, or wast to leave notes, see one of the Soboring resources. | What is Sewith 1,353 Events a reanth ago a month ago | | |
| Idexers Biscole, Index, store data Search data based on search neguests from search head Idex? Index - noun, data repository | documentation IZ Tatavia IZ | | | |
| Receive, Index, store data Search data based on search requests from search head STARY Index nounc data repository | Search History | | | |
| Receive, index, store data Search data based on search requests from search head | BRARY | | | |
| Receive, index, store data Search data based on search requests from search head | | | | |
| Receive, index, store data Search data based on search requests from search head | | | | |
| Receive, index, store data Search data based on search requests from search head | | | | |
| Receive, index, store data Search data based on search requests from search head | | | | |
| Receive, index, store data Search data based on search requests from search head | | | | |
| Receive, index, store data Search data based on search requests from search head | | | | |
| Receive, index, store data Search data based on search requests from search head | | | | |
| Receive, index, store data Search data based on search requests from search head | | | | |
| Receive, index, store data Search data based on search requests from search head | | |] | |
| Search data based on search requests from search head | ndexers | | | |
| Search data based on search requests from search head | | | | |
| ACCENT. Index - noun-data repository | | | | |
| ndex? | TO COMPANY MATCHING THE TAY OF THE THE THE TAY OF THE T | "Tipestane" (1983-13-2019) (8-19-240902", "Count" (3, 1997-140) (8-19) (1993-140) (1997-140) | | |
| ndex? | 6. 1. SECTIONE S. V. NORMON, CO., 2011. 10 - MISSELVENT ADMINISTRAÇÃO DE PROPRIO DE P | hallocy; Die de Baddy macein Certificatio Antonity; Gr. "81], cert_800: "Freedom "Redepopilications (Interpretation Computation Computati | | |
| andex? | | | | |
| ACTARY Index - noun: data repository | enemenenene-na-jasoryosakero-hanearokene en ana yisenearokene-sesakina hanearokene-nasakina nasakina nasakina nasakina nasakina nasakina nasakina nasak | Tringersen Character State Care and address recovered their factors of the response | | |
| ndex? Index - noun: data repository | The state of the s | Land Lange - TML 12-2109-Line 4 MONIZET - count 1-1, feet July - 17-22-21-22 - (Life - Life - | | |
| ndex? Index - noun: data repository | The state of the s | | | |
| ndex? | content of the Conten | ************************************** | | |
| Index - noun: data repository | busy star conserve utbal-values softist specific in the | THE PART WAS UNION TO THE PART OF THE PART | | |
| Index - noun: data repository | BRARY | | | |
| Index - noun: data repository | | | | |
| Index - noun: data repository | | | | |
| Index - noun: data repository | | | | |
| Index - noun: data repository | | | | |
| Index - noun: data repository | | | | |
| Index - noun: data repository | | | | |
| Index - noun: data repository | | | | |
| Index - noun: data repository | | | | |
| Index - noun: data repository | | | , | |
| Index - noun: data repository | | | | |
| | ndex? | | | |
| | Index – noun: data repository | | | |
| | | | 1 | |

Indexer: Splunk instance that indexes data
 An indexer indexes data and puts it into an index.

CYBRARY

| Forwarders | | |
|---|---------------------|--------|
| | | |
| Sends data onward Hair word for word and an armonic for the send of t | | |
| Universal forwarder Light forwarder (deprecated) | | |
| Heavy forwarder | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| CVPZAZV | | |
| CYBRARY | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | \neg |
| Other communication | | |
| Other server roles | Edit Server Roles × | |
| | | |
| | Search Head | - |
| | Cluster Master | |
| | License Master 🗹 | - |
| | Indexer 🗸 | |
| | Deployment Server | |
| | KV Store 🗹 | |
| | SHC Deployer | |
| | | |
| | Cancel | |
| | | |
| CYBRARY | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | _ |
| | | |
| Distributed environments | | |
| | | |
| "Horizontal scaling" Separate out the pieces | | |
| - Scharace out the bieces | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | l . |



Clustering - Data replication - Availability - Fidelity - Recovery



| Review | - |
|--|---|
| Forwarders send data, indexers turn data into events and place them in indexes, search heads send search | |
| requests, display data | |
| A large company will likely need a distributed environment Clustering provides redundancy | |
| · clastering provides redundancy | · |
| | |
| | |
| | |
| | |
| | |
| CYBRARY | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| Next up: Installation! | |
| | |
| | |
| | |
| | |
| | |
| CYBRARY | |
| | |