Copyright © 2015 Splunk Inc.

.conf2015

Using Splunk Internal Logs For System Health Diagnosis And Troubleshoot

Xiaoyuan Li

Victor Ebken

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.

About Contributors

Xiaoyuan Li

- Developer, Release System Infrastructure
- Formerly in Server Sustaining
- xli@splunk.com

Victor Ebken

- Developer, Server Sustaining
- vebken@splunk.com

Tianyi Gou

- Developer, Server Sustaining
- tgou@splunk.com

Mathew Elting

- Developer, UI System
- melting@splunk.com

What Splunk Logs Provide

- System operation information: data input/output, indexing, searching and analysis
- Application deployment messages
- Performance information
- Resource utilizations
- User activities
- License usages

Why Do We Care?

Splunk Logs are Useful

Troubleshooting

Tuning system

Expanding knowledge

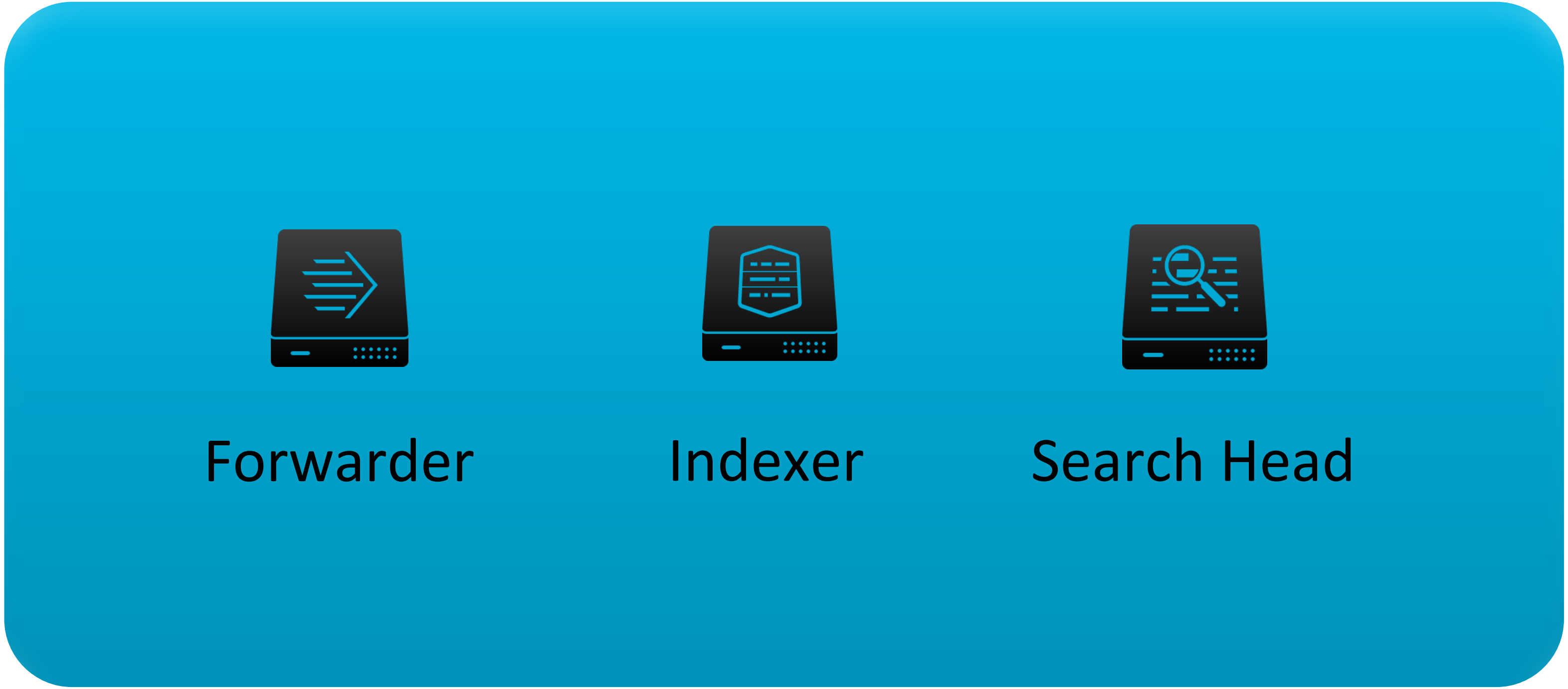
Agenda

- What Splunk Logs
  - Understanding the messages
- How to Use Splunk Logs
  - Tuning logger settings
- Q & A

Splunk Internal Logs

audit.log	license_usage.log	splunkd.log
btool.log	metrics.log	splunkd_access.log
conf.log	migration.log	splunkd_stderr.log
crash.log	MSI.log	splunkd_stdout.log
disk_objects.log	resource_usage.log	splunkd_ui_access.log
kvstore.log	scheduler.log	splunkd_utility.log
license_audit.log	search.log	

splunkd.log



Forwarder

Indexer

Search Head

splunkd.log

- The primary log written to by the Splunk server.
- Contains general server operation information, including errors and warnings as well as debugging messages.
- Also contains log messages generated by modular/scripted inputs.
- Default location:

  {SPLUNK_HOME} / var / log / splunk

Example of splunkd.log

```
11-05-2014 10:47:26.873 -0500 INFO  loader - Splunkd starting (build 207789).
11-05-2014 10:47:26.873 -0500 INFO  loader - Maximum number of threads (approximate): 16383
11-05-2014 10:47:26.873 -0500 INFO  loader - Arguments are: "-p" "8089”
11-05-2014 10:47:28.043 -0500 INFO  DC:DeploymentClient - Starting phonehome thread.
11-05-2014 10:47:28.043 -0500 INFO  ServerRoles - Declared role=deployment_client.
11-05-2014 10:47:28.043 -0500 INFO  loader - win-service: Windows service is now in running state.
11-05-2014 10:47:38.205 -0500 INFO  TcpOutputProc - Connected to idx=10.10.25.11:9997
11-05-2014 10:48:04.298 -0500 INFO  DC:HandshakeReplyHandler - Handshake done.
11-05-2014 10:48:04.423 -0500 INFO  DeployedApplication - Checksum mismatch 0 <> 14104735397260466464 for app=Windows
Server. Will reload from=’PP01.splunk.com:8089/services/streams/deployment?name=Windows%20Servers:Windows%20Server'
11-05-2014 10:48:04.438 -0500 INFO  DeployedApplication - Downloaded url=PP01.splunk.com:8089/services/streams/deployment?
name=Windows%20Servers:Windows%20Server to file='C:\Program Files\SplunkUniversalForwarder\var\run\Windows Servers
\Windows Server-1415135580.bundle' sizeKB=10
11-05-2014 10:48:04.438 -0500 INFO  DeployedApplication - Installing app=Windows Server to='C:\Program Files
\SplunkUniversalForwarder\etc\apps\Windows Server'
11-05-2014 10:48:04.469 -0500 WARN  DC:DeploymentClient - Restarting Splunkd…
```

View splunkd.log from Splunk UI

- splunkd.log Will be rotate to a new file when it reaches 25MB
- Only recent 5 splunkd.log files are kept in the local file system
- splunkd.log Messages are indexed by the Splunk server
- Searchable from UI via index = _internal
- Using UI, splunkd.log messages of remote forwarders and indexers can be viewed at a Search Head
- Search example:

```
index=_internal  host=forwarder01.splunk.com  source=*splunkd.log*  “ERROR”
```

Tuning splunkd.log

- Edit log.cfg or log-local.cfg in $SPLUNK_HOME/etc directory
  - a) Set appender attributes
  - b) Set individual logging levels for any Splunk modules.
  - c) Log levels: DEBUG, INFO, WARN, CRIT, ERROR
- Example log.cfg file

```
rootCategory=WARN,A1
appender.A1=RollingFileAppender
appender.A1.fileName=${SPLUNK_HOME}\var\log\splunk\splunkd.log
appender.A1.maxFileSize=25000000     # default: 25MB
appender.A1.maxBackupIndex=5
category.TailingProcessor=INFO
category.ArchiveProcessor=DEBUG
```

Tuning splunkd.log for Modular Inputs

- Edit $SPLUNK_HOME/etc/log-local.cfg

  to set category.ExecProcessor:

  ```
  category.ExecProcessor=DEBUG        // set to INFO level by default
  ```

- Edit $SPLUNK_HOME/etc/log-cmdline.cfg

  reset the specific modular input category

  ```
  rootCategory=WARN,rootAppender
  category.splunk-admon=ERROR
  category.splunk-hostmon=ERROR
  category.splunk-monitornohandle=ERROR
  category.splunk-netmon=ERROR
  category.splunk-printmon=ERROR
  category.splunk-winevtlog=DEBUG
  ```

Tuning splunkd.log from Splunk UI

- Temporary and will reset at next startup

Tuning splunkd.log from CLI

- Temporary and will reset at next startup

- At start time, provide --debug flag in CLI:

```
bin/splunk start --debug
```

- At run time, enter CLI set command as:

```
bin/splunk set log-level <category> -level <level>
```

  E.g.

```
bin/splunk set log-level TailingProcessor -level DEBUG
```

Splunkd Logging Categories
Data Input Modules

TailingProcessor

WatchedFile

BatchReader

ExecProcessor

TcpInputProc

UDPInputProcessor

FSChangeManagerProcessor

ArchiveProcessor

CsvLineBreaker

TcpInputConfig

VerboseCrc

Splunk Logging Categories
Data Output Modules

TcpOutputProc

TcpOutputQ

IndexAndForwardProc

SyslogOutputProc

TcpOutputFd

ThruputProcessor

SyslogOutputConfig

Splunkd Logging Categories
Data Processing Modules

UTF8Processor

HeaderProcessor

regexExtractionProcessor

LineBreakingProcessor

AggregatorMiningProcessor

Splunkd Logging Categories
Indexing Modules

IndexProcessor

IndexAdminHandler

HotDBManager

ClusterBundleValidator

CMConfig

IndexConfig

VolumeManager

DatabaseDirectoryManager

MetaData

SiteFactor

Splunkd Logging Categories
Deployment Server/Client Modules

DeploymentServer

Serverclass

ClientSessionsManager

ServerclassAdminHandler

PackageDownloadRestHandler

DeploymentServerAdminHandler

DSClientFilter

DeployedApplication

DeploymentClientAdminHandler

Splunkd Logging Categories
Authentication System

AuthenticationManagerLDAP

AuthenticationManagerSplunk

AuthorizationManager

ScopedLDAPConnection

UserManager

search.log

Indexer

Search Head

search.log

- Location: {SPLUNK_HOME}/var/run/splunk/dispatch/{search_id}.

- Generated by Splunk search process. (each search will generate own search.log)

- Contains operation information for the corresponding search command running in the process, including errors and warnings

- For ad hoc searches, search.log can be accessed from Splunk UI

Tuning search.log

- Edit $SPLUNK_HOME/etc/log-searchprocess.cfg

```
rootCategory=INFO,searchprocessAppender
appender.searchprocessAppender=RollingFileAppender
appender.searchprocessAppender.fileName=${SPLUNK_DISPATCH_DIR}\search.log
appender.searchprocessAppender.maxFileSize=10000000     # default: 10MB
appender.searchprocessAppender.maxBackupIndex=3
category.BatchSearch=WARN
```

search.log example

- Demo troubleshooting

Example Search Logging Categories

TsidxStats

PivotUtil

PreviewGenerator

DispatchProcess

MultiValueProcessor

DispatchSearch

SearchProcessRunner

SummaryIndexProcessor

SearchOperator:Typeahead

StatsProcessor

DispatchManager

SearchOperator:rex

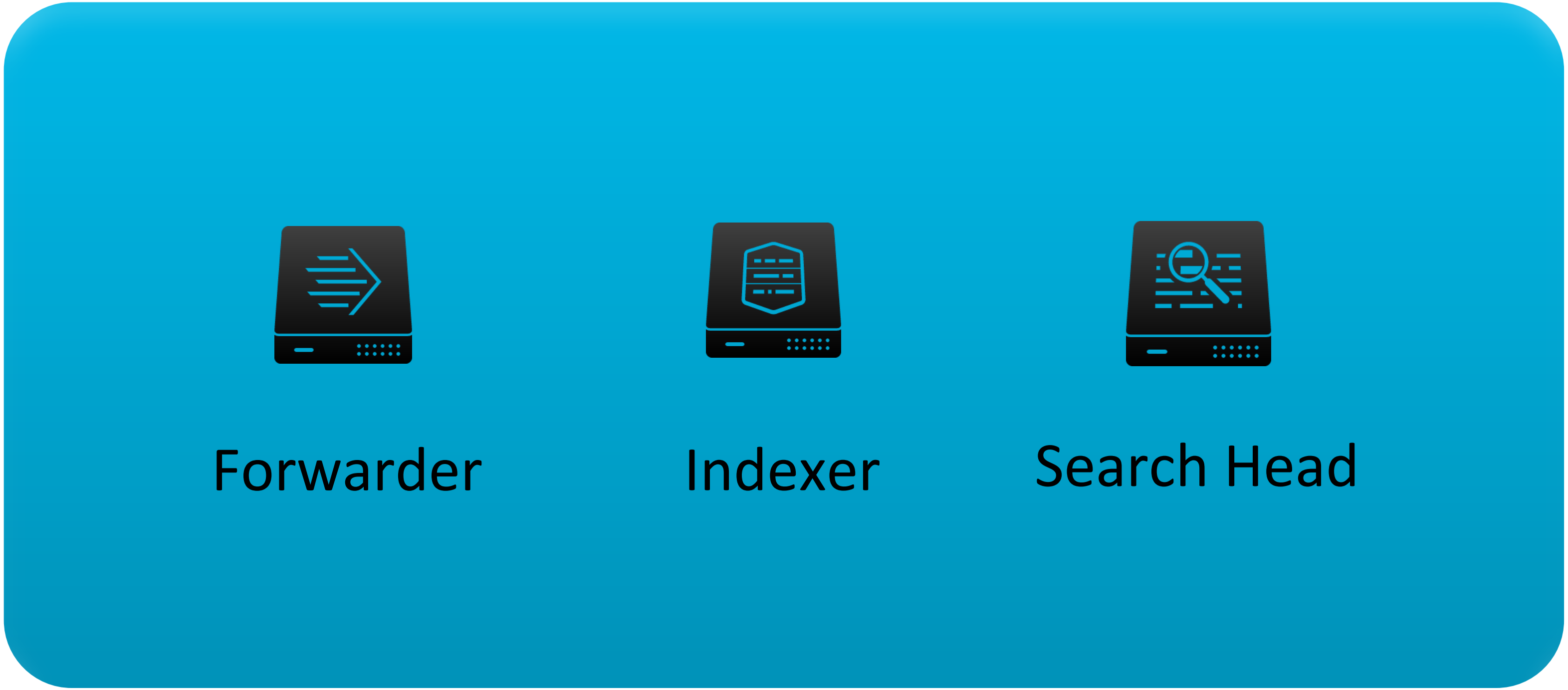
EvalCommand

SearchOperator:fields

SearchResultCollator

ExportProcessor

metrics.log



Forwarder

Indexer

Search Head

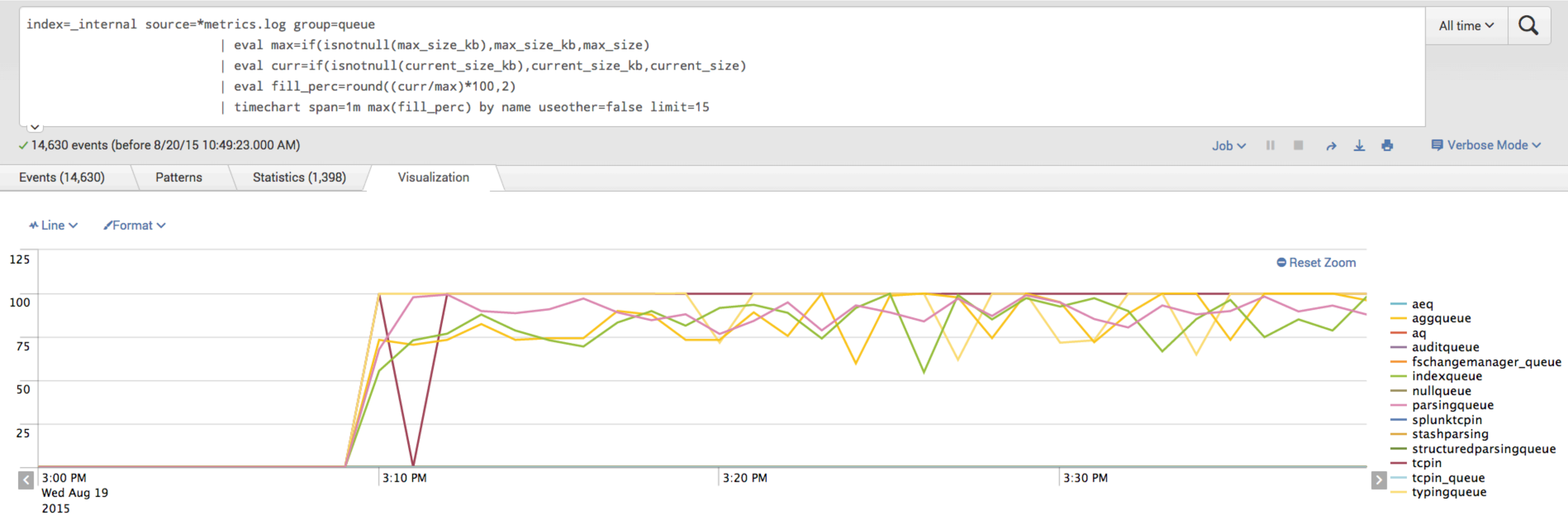
metrics.log

- Location: {SPLUNK_HOME}/var/log/splunk.

- Contains periodic snapshots of Splunk performance and system data, including information about CPU usage by internal processors and queue usage in Splunk's data processing.

- metrics.log is a sampling of the top ten items in each category in 30 second intervals, based on the size of _raw. It can be used for analysis of volume trends for data inputs, indexing and outputs.

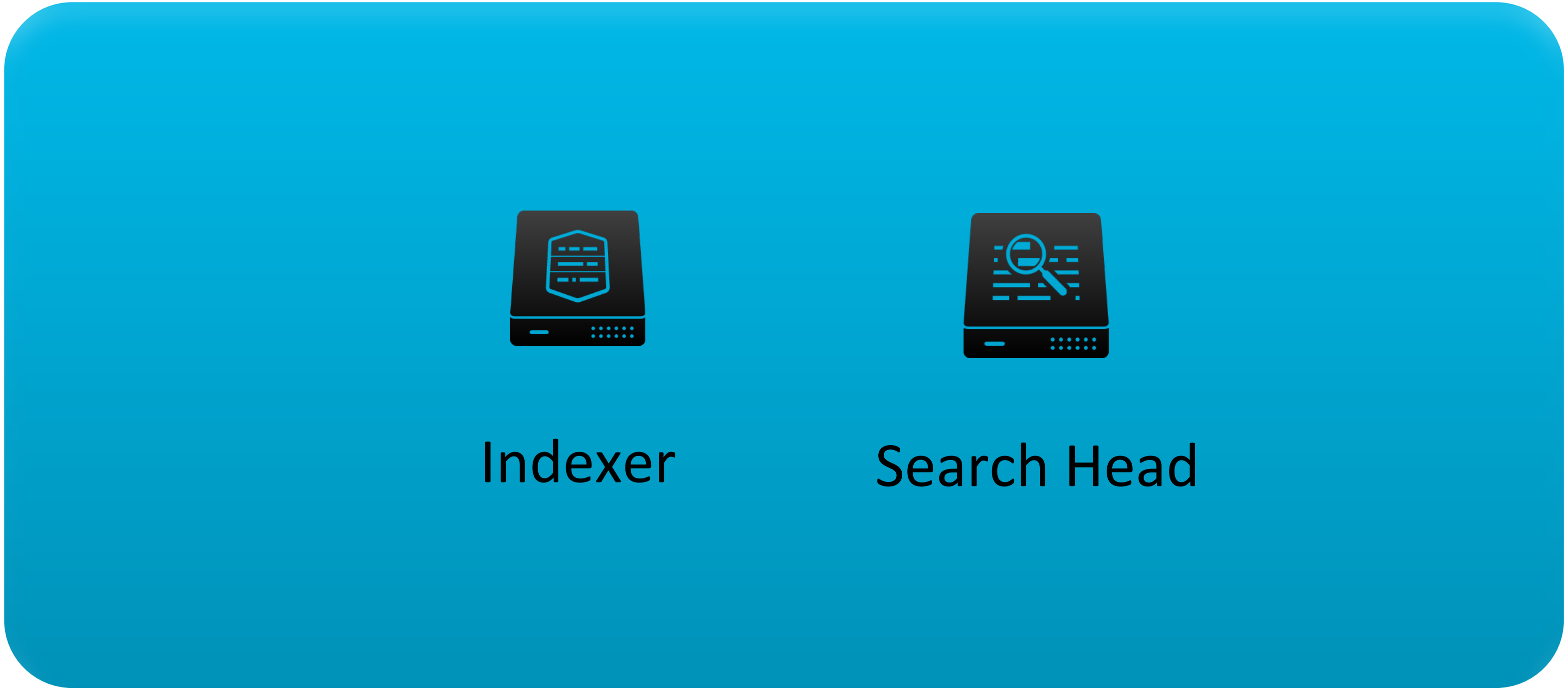
metrics.log Example



```
index=_internal source=*metrics.log group=queue
                            | eval max=if(isnotnull(max_size_kb),max_size_kb,max_size)
                            | eval curr=if(isnotnull(current_size_kb),current_size_kb,current_size)
                            | eval fill_perc=round((curr/max)*100,2)
                            | timechart span=1m max(fill_perc) by name useother=false limit=15
```

✓ 14,630 events (before 8/20/15 10:49:23.000 AM)

splunkd_ui_access.log



Indexer

Search Head

splunkd_ui_access.log

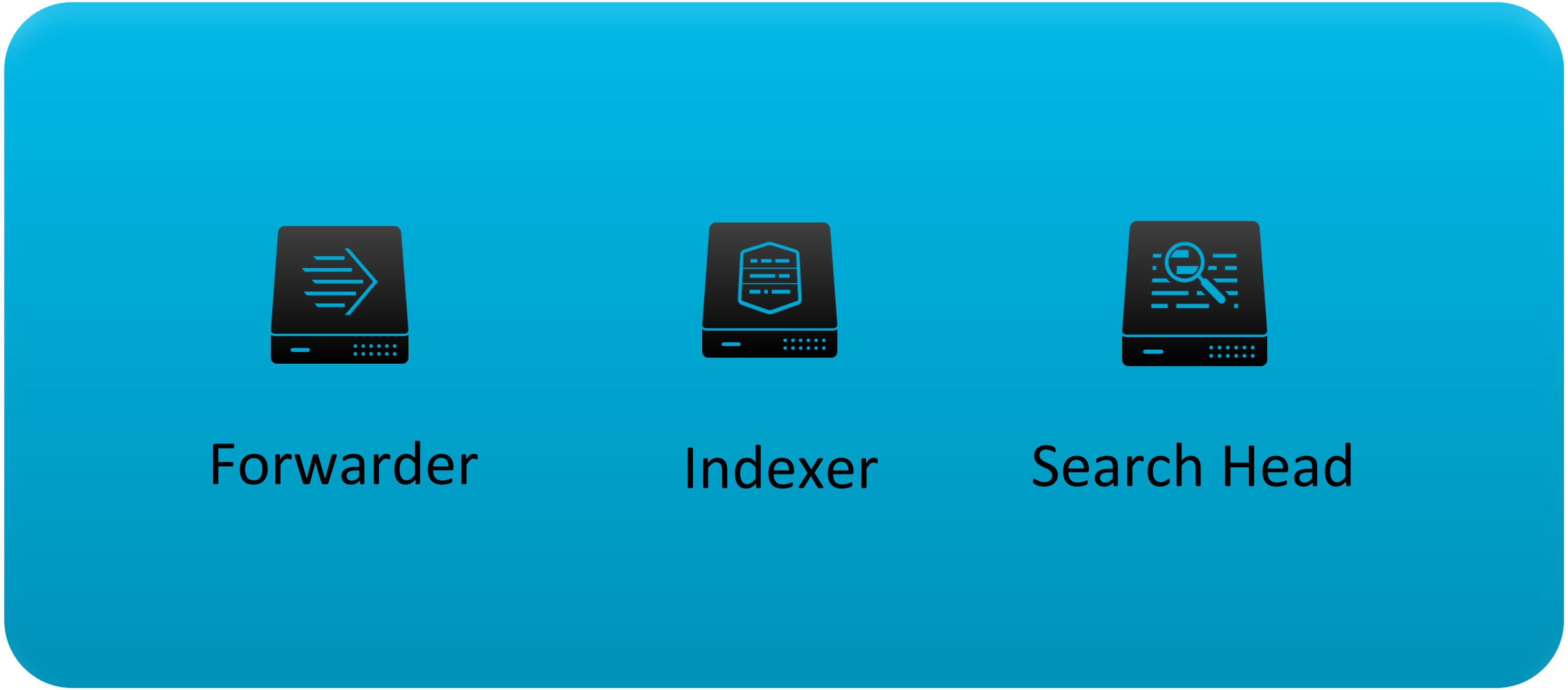
- Location: {SPLUNK_HOME}/var/log/splunk.
- Generated by splunkd process
- Containing HTTP requests from Splunk UI such as a web browser or curl command line
- In Apache access log format

splunkd_ui_access.log example

```
10.54.84.5 - admin [29/Jun/2015:19:35:04.949 +0200] "GET /en-US/splunkd/__raw/
servicesNS/admin/LOSecurity/search/jobs/
admin__admin__LOSecurity__search22_1435578694.1958?
output_mode=json&_=1435578697325 HTTP/1.1" 200 1932 "https://re.splunk.com/en-US/
app/Security/suspicious_activity?form.field1.earliest=-7d
%40h&form.field1.latest=now&earliest=0&latest=" "Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/38.0.2125.104 Safari/537.36" -
35d130dedb12777cb3cc0712e0a70de7 3ms
```

- <address> - <user> [<timestamp>] “<request>” <status> <response_size> - - - <duration>
- Helps to understand: Is IU slowing down? Who is accessing dashboards? Is my request successful?

splunkd_access.log



Forwarder

Indexer

Search Head

splunkd_access.log

- Location: {SPLUNK_HOME}/var/log/splunk.
- Generated by splunkd process
- Any action done by splunkd through the UI is logged here, including splunkweb, the CLI, all POST GET actions, deleted saved searches, and other programs accessing the REST endpoints
- Logs the time taken to respond to the requests. Search job artifacts logged here include size of data returned with search
- In Apache access log format

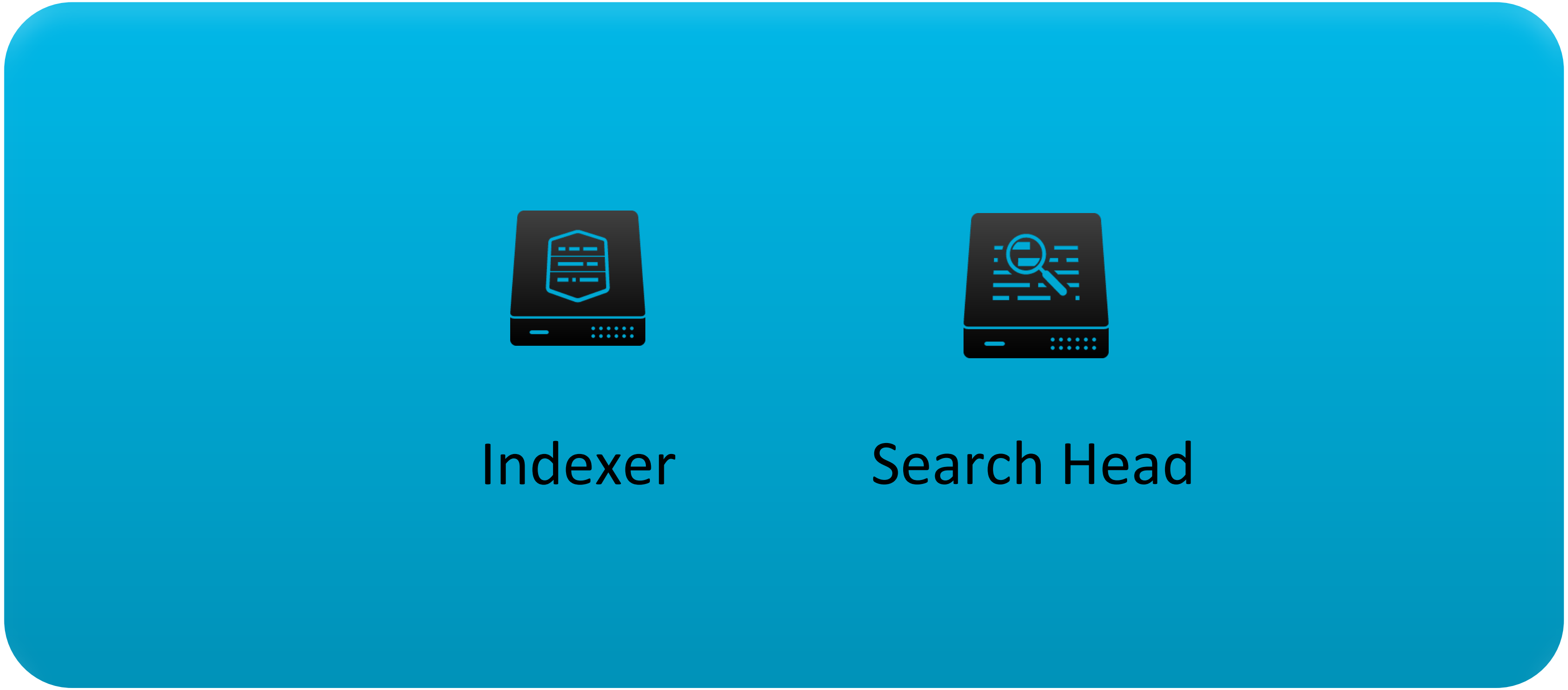
splunkd_access.log example

```
127.0.0.1 - admin [20/Aug/2015:10:33:40.004 -0700] "GET /servicesNS/admin/search/data/inputs/monitor HTTP/1.0" 200 60071 - - - 13ms
```

```
127.0.0.1 - - [04/Aug/2015:15:08:48.145 -0700] "GET /services/server/info HTTP/1.0" 200 4789 - - - 7ms
```

- <address> - <user> [<timestamp>] “<request>” <status> <response_size> - - - <duration>
- Troubleshoot slow endpoints

scheduler.log



scheduler.log

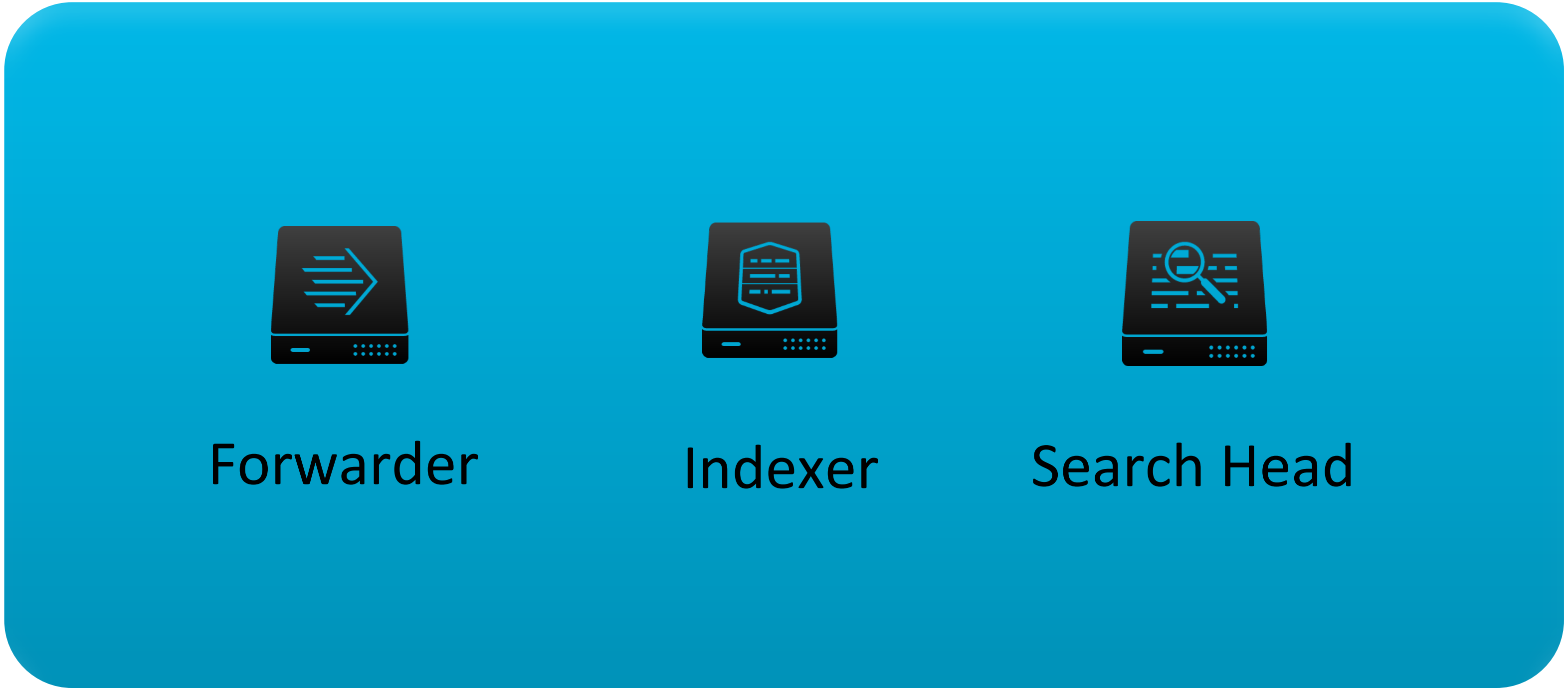
- Generated by splunkd process
- Contains messages about all successful and unsuccessful actions performed by the search/alert scheduler
- Provides general information about activities of scheduled searches
- Default location: {SPLUNK_HOME}/var/log/splunk.

scheduler.log example

Did my scheduled search “Conf_Scheduler_Log” run?

```
07-29-2015 23:25:01.331 -0700 INFO  SavedSplunker - Historical:
savedsearch_id="admin;search;Conf_Scheduler_Log", user="admin", app="search",
savedsearch_name="Conf_Scheduler_Log", status=success, digest_mode=1,
scheduled_time=1438237500, dispatch_time=1438237501, run_time=0.154,
result_count=10, alert_actions="",
sid="scheduler__admin__search__RMD5580e3246_at_1438237500_184",
suppressed=0, thread_id="AlertNotifierWorker-0"
```

splunkd-utility.log



Forwarder

Indexer

Search Head

splunkd-utility.log

- Generated by the checking utilities of splunkd:

  splunkd validatedb

  splunkd check-license
- The checking utilities log Splunk version, some basic configurations, and current OS limits like max number of threads
- Consult this log file when splunkd doesn't start
- Location: {SPLUNK_HOME}/var/log/splunk.

splunkd-utility.log example

```
07-28-2014 16:06:27.782 +1000 INFO  loader - Running utility: "validatedb"
07-28-2014 16:06:27.782 +1000 INFO  loader - Getting configuration data from: C:\Program Files
\Splunk\etc\myinstall\splunkd.xml
07-28-2014 16:06:27.798 +1000 INFO  loader - Writing out composite configuration file: C:
\Program Files\Splunk\var\run\splunk\composite.xml
07-28-2014 16:06:27.860 +1000 INFO  loader - Validated 34 indexes in 62.50 milliseconds
07-28-2014 16:06:28.360 +1000 INFO  ServerConfig - My hostname is ”SPLUNK0386".
07-28-2014 16:06:28.376 +1000 INFO  ServerConfig - Setting HTTP server compression state=on
07-28-2014 16:06:28.376 +1000 INFO  ServerConfig - Setting HTTP client compression state=0
(false)
07-28-2014 16:06:28.376 +1000 INFO  ServerConfig - Default output queue for file-based input:
parsingQueue.
07-28-2014 16:06:33.329 +1000 INFO  loader - Running utility: "check-transforms-keys”
```

Introspection logs

Forwarder

Indexer

Search Head

Introspection logs

- Provide Splunk platform instrumentation data
- Introspection logs include:
  - disk_objects.log: about disk usages
  - resource_usage.log: about system resources (memory/cpu) usages
  - kvstore.log: about embedded MongoDB system information
- Log file location:

  {SPLUNK_HOME}/var/log/introspection
- Configuration file location:

  {SPLUNK_HOME}/etc/apps/introspection_generator_addon.
- Splunk server index: _introspection

Introspection Logs: Troubleshooting Issues Related to System Resources

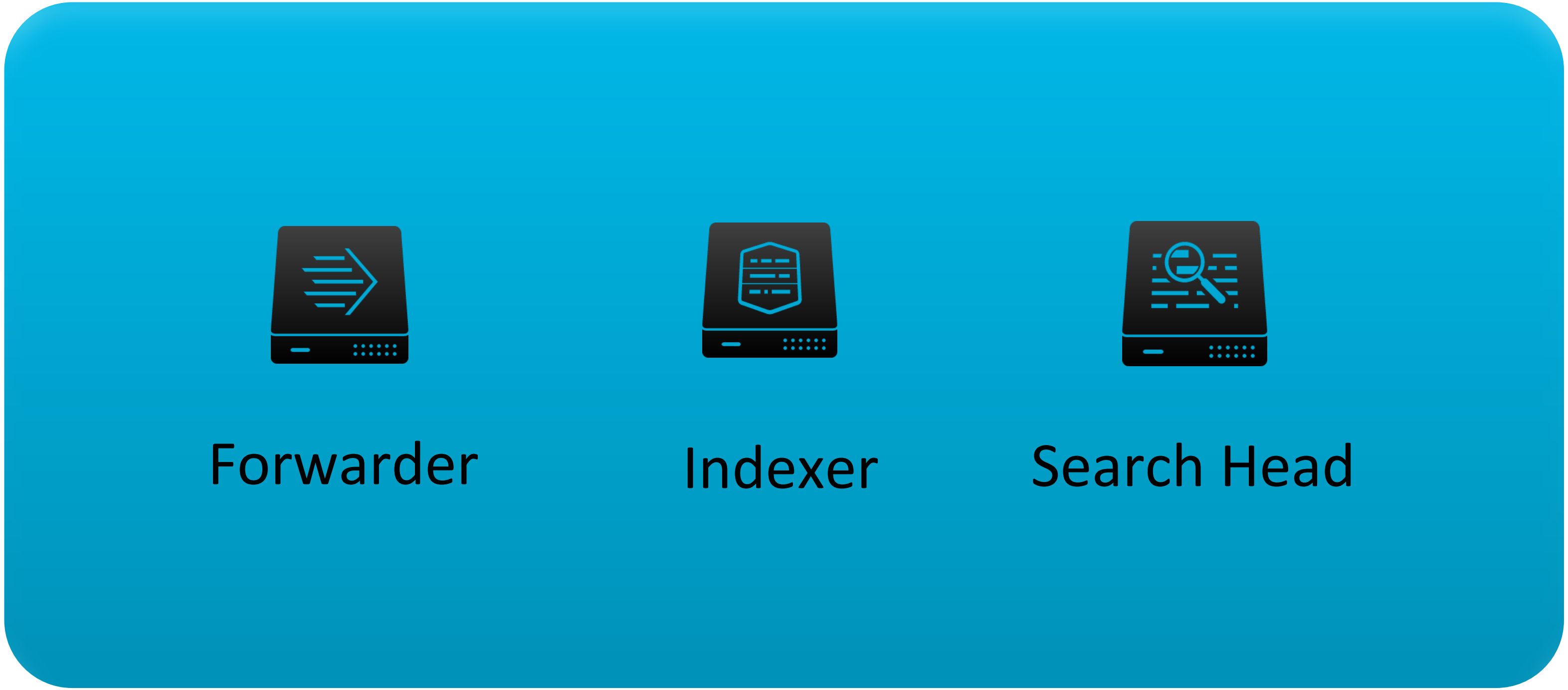
- Operating system resource usages for Splunk applications, broken down by process
- Operating system resource usages for the entire host, by all applications and system processes
- Disk object data
- KV store performance data

Introspection log example

```
{"datetime":"06-30-2015 10:12:15.980 +0200","log_level":"INFO","component":"PerProcess","data":{"pid":"6876","ppid":"1952","t_count":"16","mem_used":"240.277","pct_memory":"0.49","page_faults":"120214","pct_cpu":"0.00","normalized_pct_cpu":"0.00","elapsed":"252.0001","process":"splunkd","search_props":{"sid":"scheduler_U3BsdW5rX1NBX0N_at_1435651680_7214","user":"splunk-user","app":"Splunk_SA","role":"head","mode":"historical","type":"report acceleration"}}}

{"datetime":"06-30-2015 10:12:15.980 +0200","log_level":"INFO","component":"Hostwide","data":{"mem":"49117.277","mem_used":"8293.867","swap":"77131.461","swap_used":"8179.578","pg_paged_out":"0","pg_swapped_out":"0","forks":"0","runnable_process_count":"1","cpu_user_pct":"0.16","cpu_system_pct":"0.00","cpu_idle_pct":"99.81"}}
```

migration.log



Forwarder

Indexer

Search Head

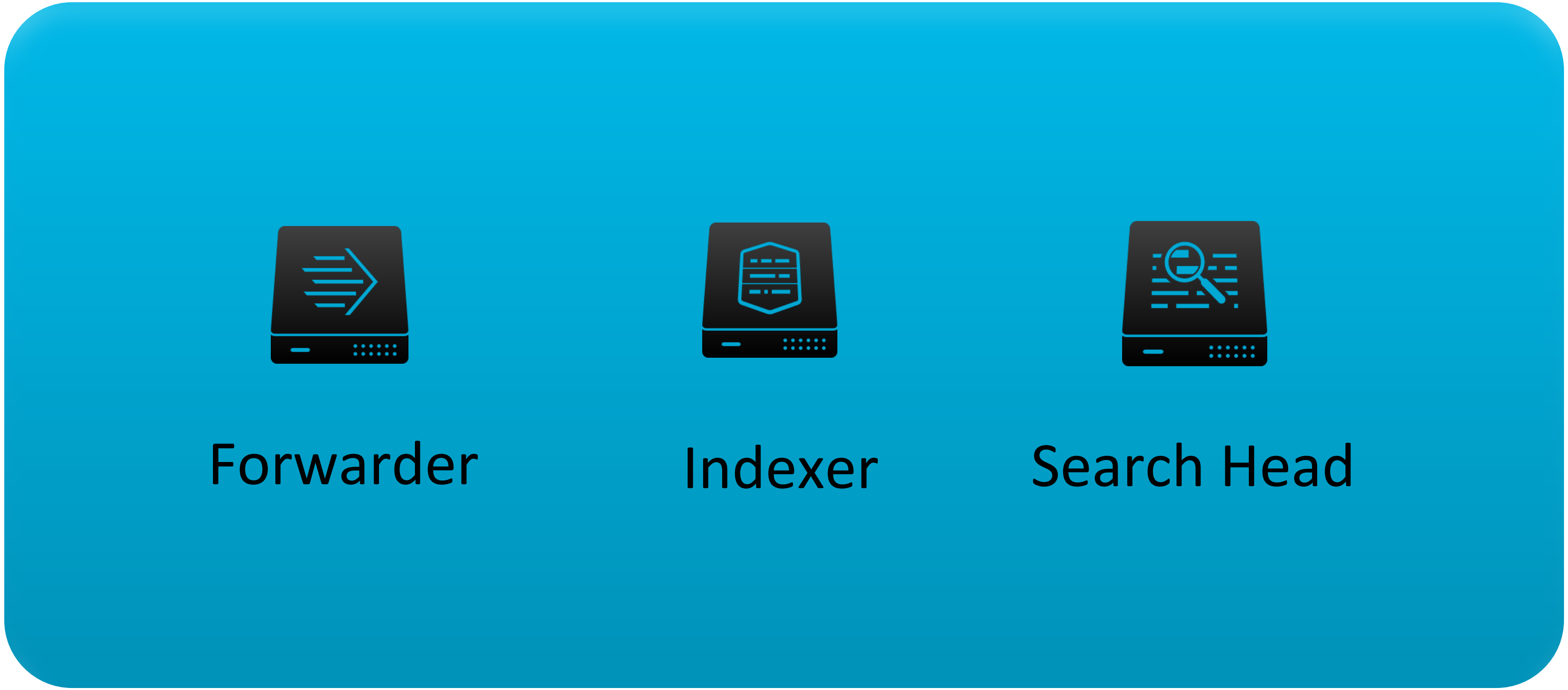
migration.log

- A log generated during installation of upgraded version
- Specifies which files were altered during upgrading
- Containing the activities that the installer performed, including whether the installation is successful and why failed if unsuccessful
- Location: {SPLUNK_HOME}/var/log/splunk.

migration.log Example

```
Migrating to:
VERSION=6.0.3
BUILD=204106
PRODUCT=splunk
PLATFORM=Linux-x86_64
Copying '/opt/splunk/etc/myinstall/splunkd.xml' to '/opt/splunk/etc/myinstall/splunkd.xml-migrate.bak’.
Checking saved search compatibility…
Checking for possible timezone configuration errors…
Checking script configuration…
Copying '/opt/splunk/etc/myinstall/splunkd.xml.cfg-default' to '/opt/splunk/etc/myinstall/splunkd.xml'.
Deleting '/opt/splunk/etc/system/local/field_actions.conf'.
Moving '/opt/splunk/share/splunk/search_mrsparkle/modules' to '/opt/splunk/share/splunk/search_mrsparkle/
modules.old.20140503-211251'.
Moving '/opt/splunk/share/splunk/search_mrsparkle/modules.new' to '/opt/splunk/share/splunk/
search_mrsparkle/modules'.
```

MSI Logs (Windows Platform)



Forwarder

Indexer

Search Head

MSI Log on Windows

- Generated by MSI during installation of Splunk on Windows
- Contains the activities that MSI performed, including whether the installation is successful and why failed if unsuccessful
- Location: %TEMP%.

MSI Log Example: Why Did my Installation Fail?

```
•  MSI (c) (70:F8) [15:30:53:521]: Doing action: FindRelatedProducts
•  Action start 15:30:53: FindRelatedProducts.
•  FindRelatedProducts: Found application: {5F8EDC0C-403A-41EC-B458-B02254CE5550}
•  MSI (c) (70:F8) [15:30:53:521]: PROPERTY CHANGE: Adding ISFOUNDNEWERPRODUCTVERSION
   property. Its value is '{5F8EDC0C-403A-41EC-B458-B02254CE5550}'.
•  Action ended 15:30:53: FindRelatedProducts. Return value 1.
•  MSI (c) (70:F8) [15:30:53:521]: Doing action: ISFoundNewerVersion
•  Action 15:30:53: ISFoundNewerVersion.
•  MSI (c) (70:F8) [15:31:09:480]: Product: Splunk -- A newer version of Splunk is already installed
   in your computer
•  Action ended 15:31:09: ISFoundNewerVersion. Return value 3.
•  Action 15:31:09: SetupCompleteError.
```

Summary

- Splunk logs provide information about operation and performance
- Splunk log messages are useful for troubleshooting
- Splunk log settings are tunable
- Recent Splunk log files are accessible via local file system
- Current and historical Splunk logs can be viewed via UI at Search Heads

Questions?

.conf2015

THANK YOU

splunk>