



# Logger Troubleshooting for Power Users

Damian Pfister

Backline Logger Support

April 2014

# Agenda

- Logger Architecture
- Common Logger Problems
- Support Tickets
- Disaster Recovery and Backups
- Customer Resources
- Example Cases



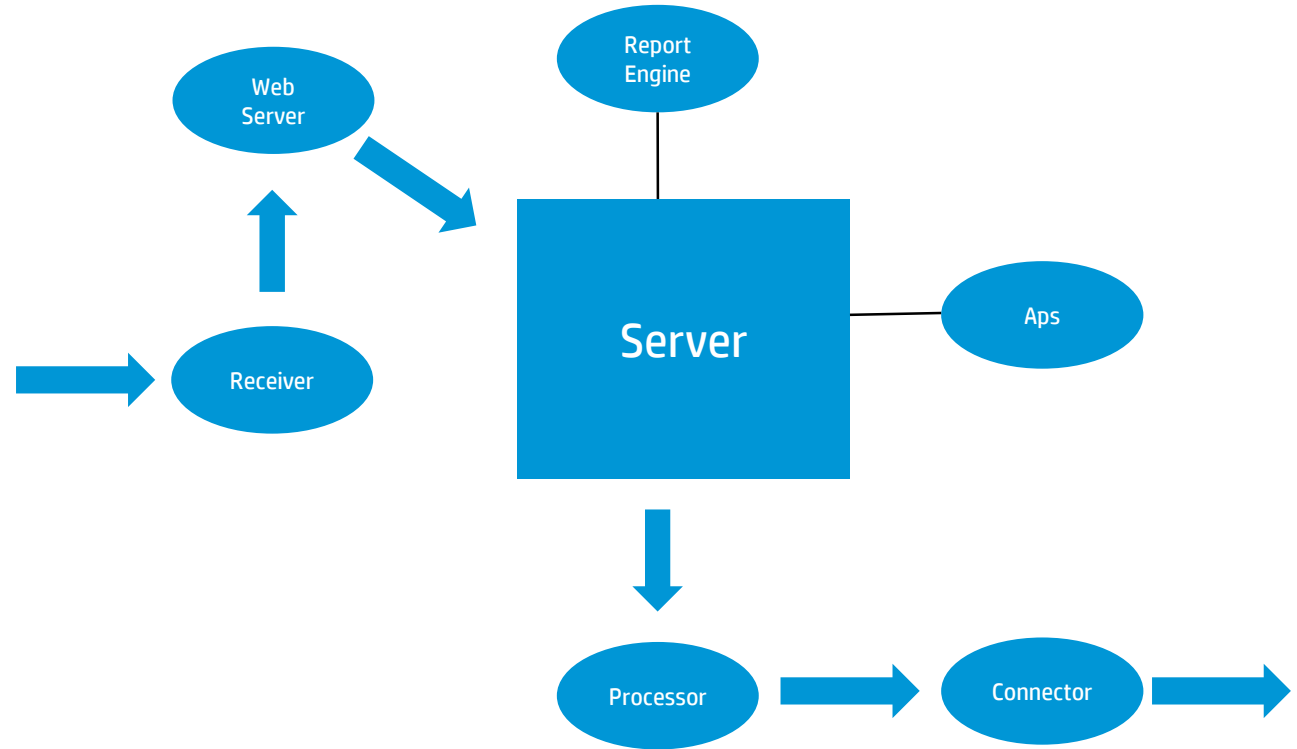
# Understanding Logger Architecture



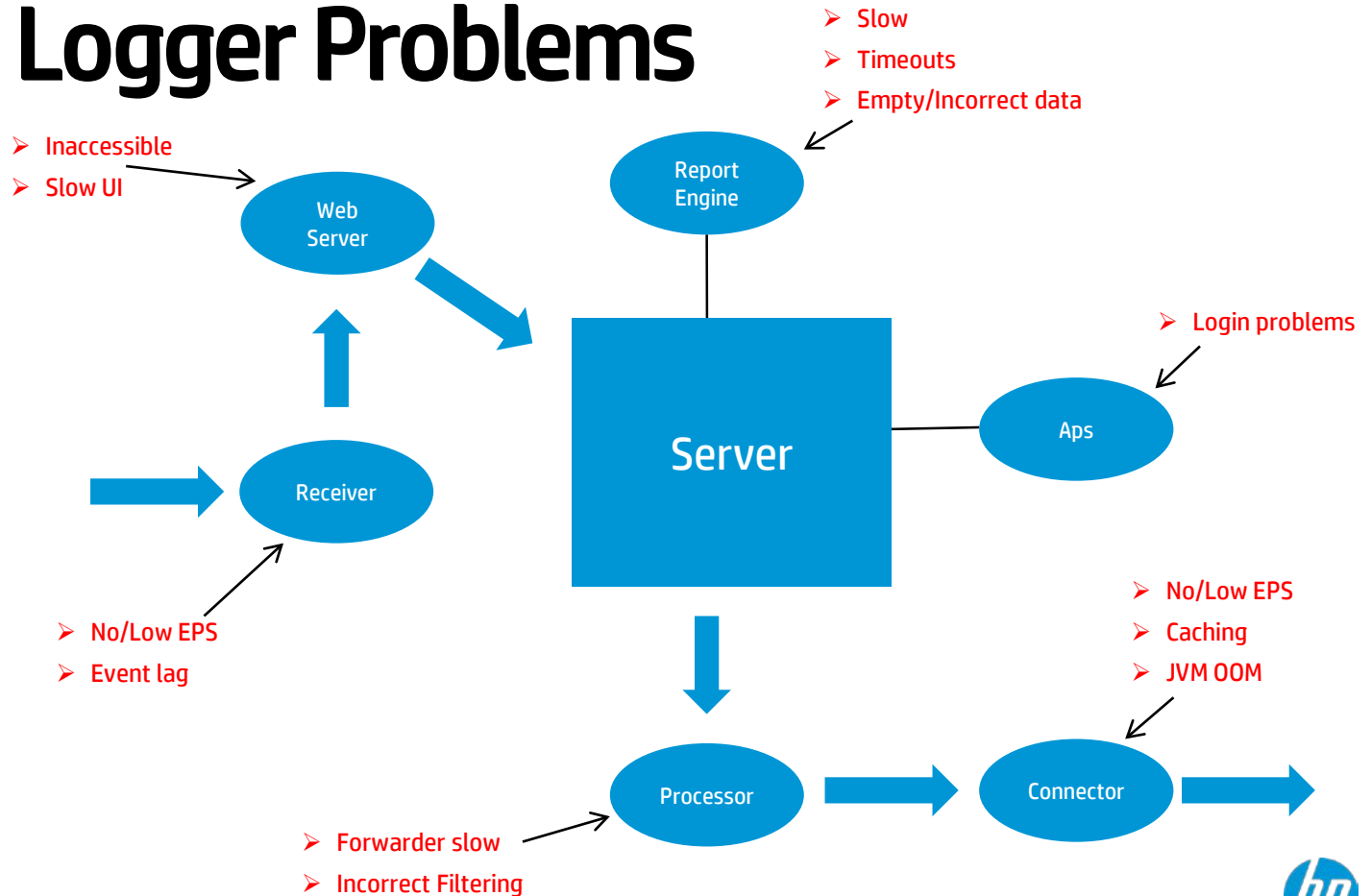
# Logger Architecture

## How it fits together

- Server
- Receiver
- Connector
- Processor
- Report Engine
- Web Server
- Aps



# Common Logger Problems



# Troubleshooting 101



## 1. Problem definition

What is the expected behaviour vs actual behaviour?

## 2. Circumstances

Did it ever work as expected or is it first usage of this feature? Any changes in environment/system?

## 3. Scope

Does it happen to all users/all reports/all Loggers? Random or predictable? Schedule or ad hoc?

## 4. Problem description

What are the steps/scenario when this issue happens? Timing?

## 5. Environment

What is the setup/architecture? Software/appliance/SAN? CIF/NFS?

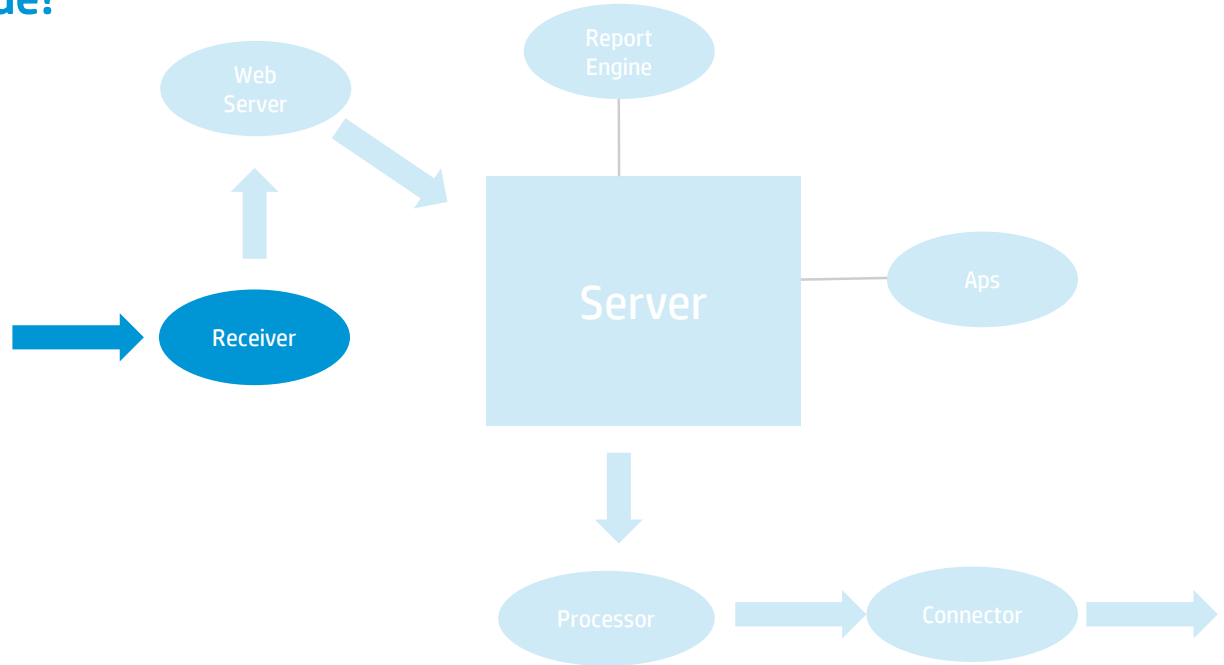


# Receiving

## Where are you seeing the issue?

### Receivers

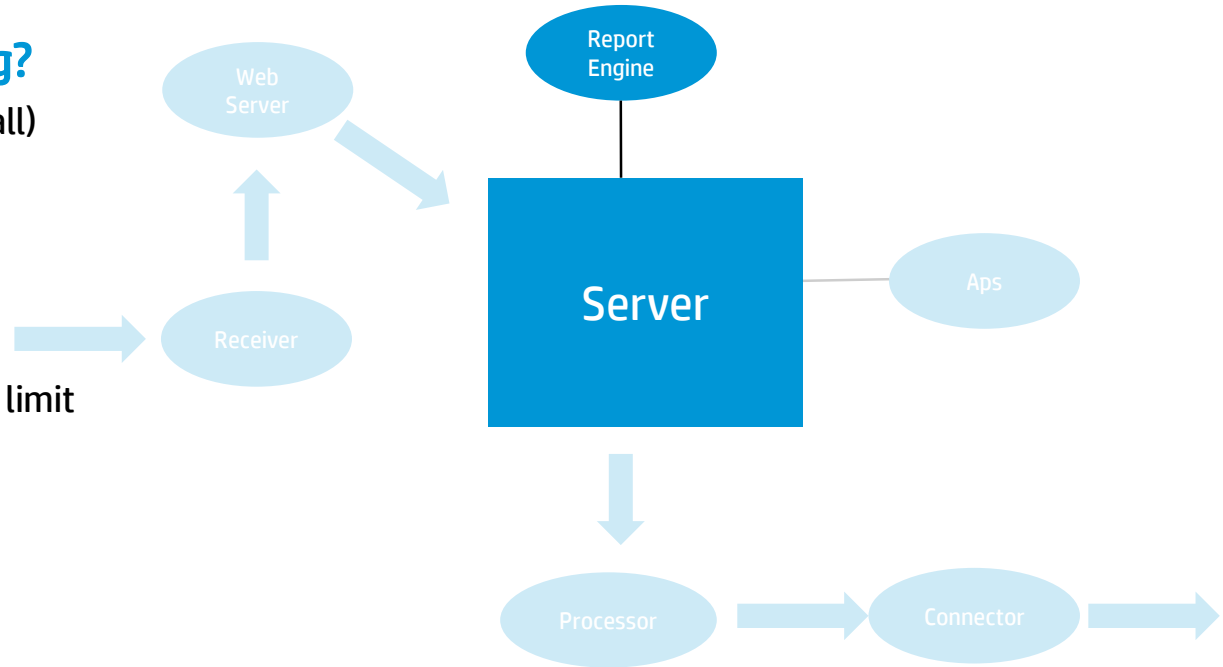
- EPS in for receiver is zero
- EPS in is not as expected
- Lagging in event time
- Passively Listens on port 443



# Reporting Issues

## Reports failing or not arriving?

- Empty reports (single, multiple or all)
  - Queries not matching data
  - Scan limit
  - Expensive queries / time out
- Not published or emailed
  - Queries not matching data / Scan limit
  - SMTP configuration
- Schedules
  - 5 concurrent
  - Conflicts





# Search

## Unexpected results

- Queries not matching data
  - Full text or regex works but not field-based
  - Is the field in the Logger Schema?
  - Time range correct?
- Time out
  - Only some results
- Exporting events
  - Limitations

The screenshot displays a search interface with the following details:

- Navigation tabs: Summary, Analyze, Dashboards, Reports, Configuration, System Admin
- User: admin
- Search filters: Local Only (checked), Field Summary (unchecked), Custom time range
- Time range: Start 2/27/2014 22:00:58, End 2/27/2014 22:05:00
- Search query: Blue |regex = "^.\*TCP\_NC\_MISS"
- Advanced Search button
- Fields: All Fields
- Auto Update: 5 min
- Results: 477,537 records, 751,207 bytes, 00:47.968 duration
- Export Results... button

The Events table below shows the following data:

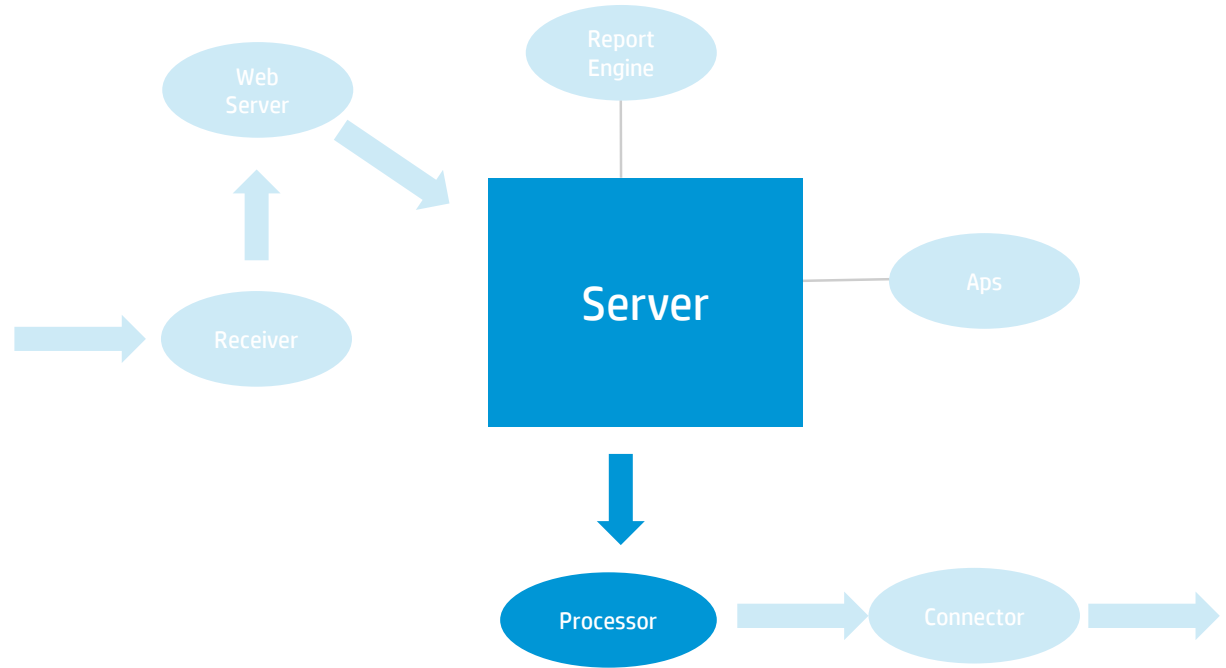
	Time (Event Time)	Device	Logger	deviceVendor	deviceProduct	deviceVersion	deviceEventClassId
1	2014/02/27 22:00:58 PST	15.214.156.161 [foobar]	Local	BlueCoat			TCP_NC_MISS



# Forwarding

## Forwarding is search

- Filters – Test!
  - Time based
  - Unified query
    - Indexing
  - Regular expression
- Caching
- Networking



# Configuration Issues

## Who configured your system?

- Authentication
- Remote file systems
- SAN configuration

The screenshot shows a window titled "Configure Remote File System" with a sub-header "Add Remote Mount Point". The form contains the following fields:

Select File System Type	S *
Name	NFS *
Hostname/IP Address	192.168.1.200 *
Remote Path	/home/archives/storage *
Mount Options	rw *
Description (optional)	

At the bottom of the dialog are two buttons: "Add" and "Cancel".

# Upgrades

## Follow the path

- Read the release notes thoroughly
- Validate the upgrade file
- Config backups & Archives
- iLo

Upgrade Paths to 5.3 SP1	
Logger Appliance	
Most common upgrade paths	3.0 GA (L3308) -> 3.0 SP1 (L3393) -> 4.0 SP1 Patch 1 (L_2c-4265) -> 4.5 GA (L4892) -> 5.0 Patch 2 (L5355) -> 5.1 GA (L5887) -> 5.2 Patch 1(L6307) -> 5.3 GA (L6684) -> 5.3 SP1 (L6836)

The screenshot shows the ArcSight Logger web interface. At the top, there are three gauges: EPS In (0/150K), EPS Out (0/150K), and CPU (10%/100%). The navigation bar includes Summary, Analyze, Dashboards, Reports, Configuration (selected), System Admin, and a user profile for 'admin'. A sidebar on the left lists various configuration options, with 'Configuration Backup' selected. The main content area is titled 'Edit Configuration Backup' and contains the following fields:

- Protocol: SCP (dropdown)
- Port: 22 (text input)
- Ip/Host: (text input)
- User: (text input)
- Password: (text input)
- Remote directory: (text input)
- Backup content: All (dropdown)
- Schedule:  One time only

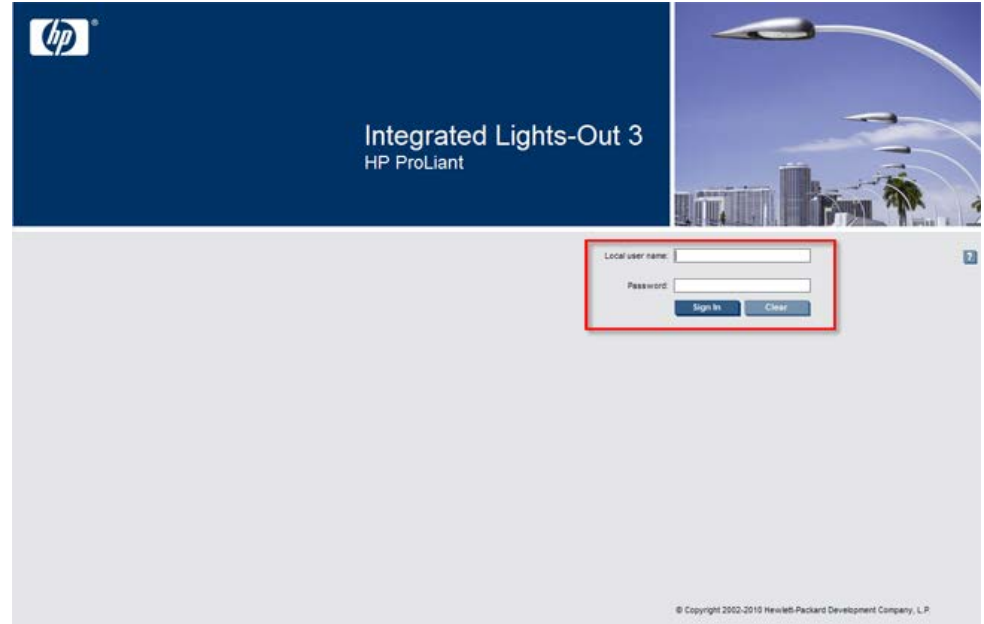
Buttons for 'Save' and 'Cancel' are located at the bottom right of the form.



# Hardware Issues

## Is it broke or not?

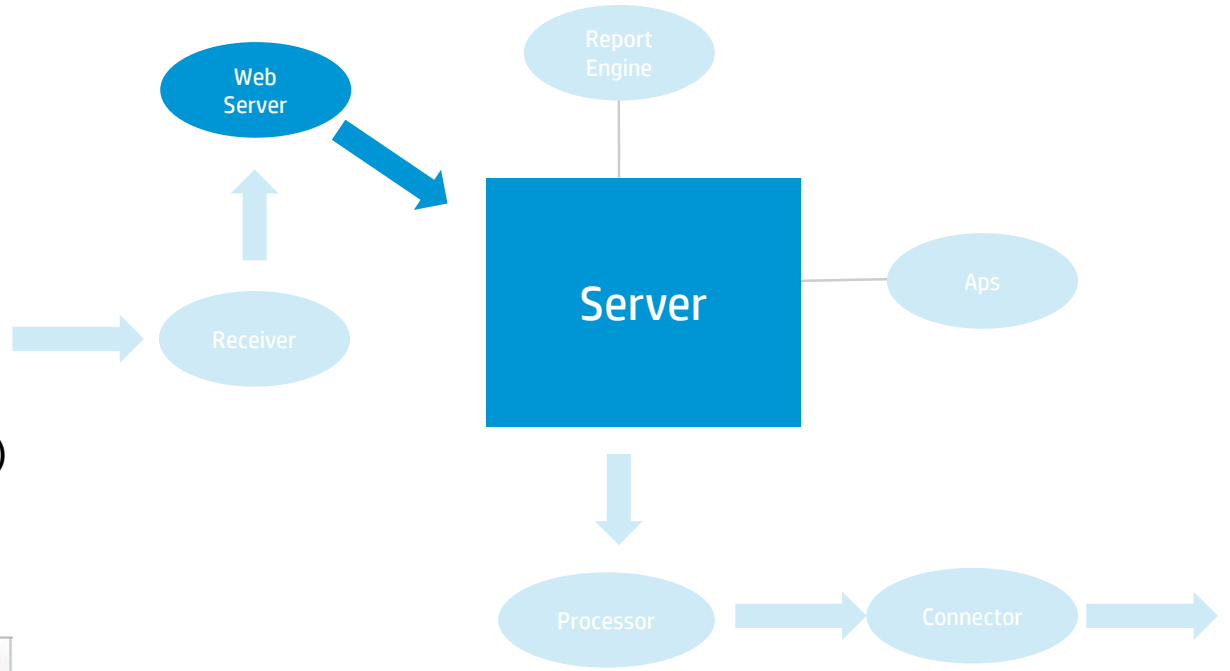
- RAID
  - Status
- Screenshot – Picture is worth a thousand words
- iLo – Integrated Lights Out
- Boot issues



# Performance Issues

## S-l-o-w

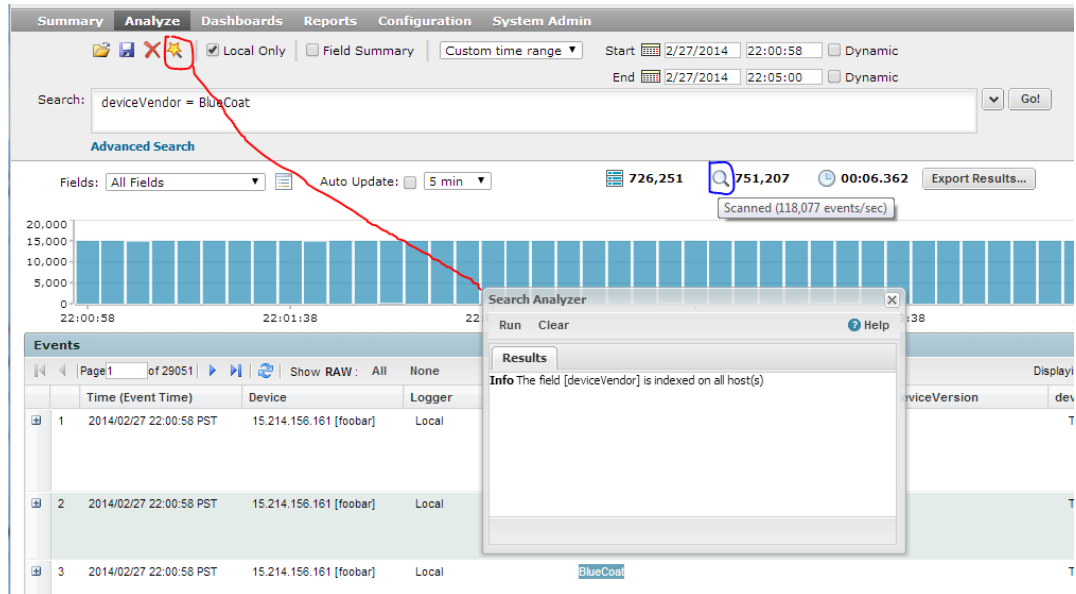
- Quantify
  - UI Performance Speed
  - Search scan rates
  - CPU Load
  - EPS in
    - Index lag (over 5k EPS average)
  - Storage Group Size



# Determine Baseline Scan Rate

## What is my Logger capable of?

- Performance speeds
  - Are they archived events?
  - What is the scan rate?
  - How many events are being scanned?
  - What is the time cost?
- Determine Baseline Scan Rate
  - Run a keyword search for a known search term (e.g.. “Blue”)
  - Run an indexed field search (1) over a short (1 min) time span
  - Disable field summary
  - Check scan rate



# Contact Logger Support





# HP-ArcSight Support

## Taking the information from your own troubleshooting

- Screen capture
- Logs
- Symptoms and their frequency
- Quantify slowness
- Overview of your environment
- Software version
- Platform
- Software or Appliance?
- Is this enough? Is a remote session necessary?
  - WebEx will be suggested by the engineer

### Troubleshooting 101

1. Problem definition - What is the expected behaviour vs actual behaviour?
2. Circumstances - Did it ever work as expected or is it first usage of this feature? Any changes in environment/system?
3. Scope - Does it happen to all users/all reports/all Loggers, random or predictable, schedule/ad hoc?
4. Problem description - What are the steps/scenario when this issue happens? timing?
5. Environment - What is the setup/architecture? Software/appliance/SAN? CIF/NFS?



# Recovery and Backup

## There to Help when disaster strikes

- Configuration backup – these are your configuration settings
- Event Archives – this is your data
- iPackager for reports



# Customer Resources



## Where to go for help

- Protect 7/24 – <https://protect724.arcsight.com/>
  - User forums
  - Product announcements & Alerts
- Logger Admin Guide
- Release Notes
- Logger Best Practices Guide



# Example Cases



# A Few Examples From the Field

## Global Summary Persistence

### Steps

- ilo
- Capture what you see on the screen?
- Gather the logs (there is a KB)
- Support provides solution

## Server JVM Out of Memory

### Steps

- Screen capture UI messages
- Check processes
- Which component is not running?
- Restart process
- Restart Logger
- Provide logs & screenshots to Support

## Stopped Receiving Events

### Steps

- Stop/start receiver process
- Is it enabled
- Is it completely stopped?
- Some sources and not others?
- What is the overall system load?



# Questions



# Thank you

