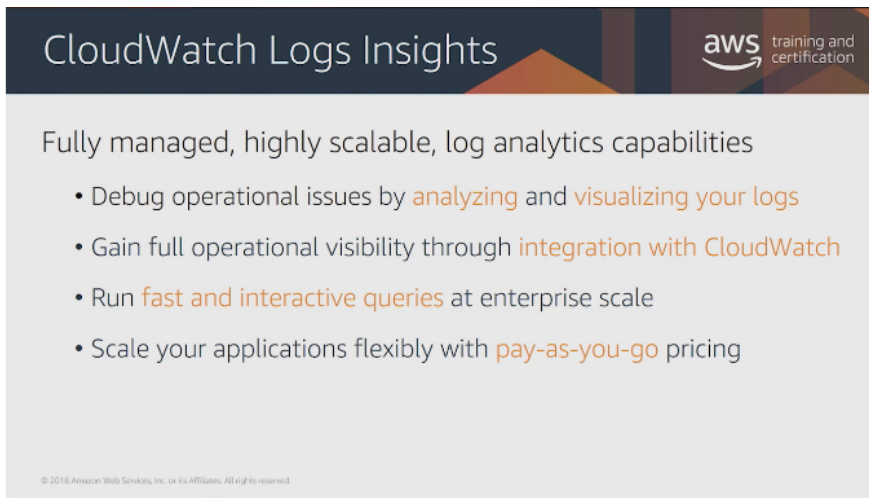


CloudWatch Logs Insights - features / review (PUBLIC)

- Slides and descriptions from AWS Digital Training : CloudWatch Insights by Manbeen Kohli
 - Fully managed, highly scalable, log analytics capabilities
 - Features : Works with any log sent to CloudWatch
 - AWS or on-premises applications
 - Any being sent to CloudWatch
 - Simple Powerful Querying
 - Writing Queries - Simple Query Language
 - sample queries, common descriptions
 - Stats : aggregation , Sort, Limit
 - Parse : ephemeral field creation can be used later on in the query.... in this case "@severity" field
 - Programmatic access : to Logs Insights : automated solutions
 - Example Insights Demonstration :
- Cost : \$0.005 per GB in US East (N. Virginia)
- Custom Metrics to set alarms to accelerate troubleshooting
- Reference Links :
 - Announcement overview : <https://aws.amazon.com/blogs/aws/new-amazon-cloudwatch-logs-insights-fast-interactive-log-analytics/>
 - AWS Training Digital : <https://www.aws.training/learningobject/video?id=27171>

Slides and descriptions from AWS Digital Training : CloudWatch Insights by Manbeen Kohli

Fully managed, highly scalable, log analytics capabilities

A presentation slide for AWS CloudWatch Logs Insights. The header features the title "CloudWatch Logs Insights" in white text on a dark blue background, with the AWS logo and "training and certification" text to the right. The main content area has a light gray background and lists four bullet points: "Debug operational issues by analyzing and visualizing your logs", "Gain full operational visibility through integration with CloudWatch", "Run fast and interactive queries at enterprise scale", and "Scale your applications flexibly with pay-as-you-go pricing". The words "analyzing", "visualizing", "integration", "fast and interactive", and "pay-as-you-go" are highlighted in orange. At the bottom left, there is a small copyright notice: "© 2018 Amazon Web Services, Inc. or its Affiliates. All rights reserved."

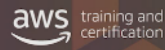
Alarms Operational Visability in seconds ...

Features : Works with any log sent to CloudWatch

AWS or on-premises applications

Any being sent to CloudWatch

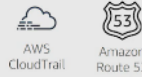
Works with Any Log Type



- Use logs from **AWS services** or **on-premises applications**
- Instantly query **any log** being sent to CloudWatch
- No setup required
- Automatic **Log Field Discovery**
 - Creates system fields for all logs **@timestamp**, **@message**, and **@logStream**
 - Automatically **discovers fields** for **AWS logs** and **any JSON-based application log**



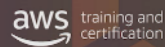
{json}



© 2018 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Simple Powerful Querying

Simple but Powerful Querying



- Write queries with **aggregations**, **filters**, and **regular expressions**
- **Visualize query results** and **time series data**
- Add results to **CloudWatch Dashboards**

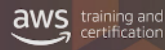
© 2018 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Writing Queries - Simple Query Language

sample queries, common descriptions

Fields, Filter, Java regex

Writing Queries



- Easy-to-learn **query language** with simple query commands
- In-product help via **sample queries**, **command descriptions**, and **query autocompletion**

© 2018 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Query Commands



FIELDS: retrieve a list of fields

```
fields srcAddr, dstAddr bytes, @timestamp
```

FILTER: retrieve log events that match search criteria

```
fields srcAddr, bytes |filter srcAddr = "10.0.183.98"
```

Filter using a regular expression

```
fields @message | filter like /Exception/
```

© 2018 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

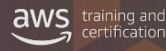
one or more log fields

numeric, string, datatype manipulation , conditional and mathematical operations

Filter : 1 or more log events java style regex

Stats : aggregation , Sort, Limit

Query Commands



STATS: calculate aggregate statistics

```
stats sum(bytes) by srcAddr |filter srcAddr = "10.0.183.98"
```

SORT: sort results based on a field in ascending or descending order

```
stats sum(bytes) as @mbytes by srcAddr |sort by @mbytes desc
```

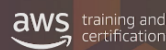
LIMIT: retrieve a limited number of log events

```
fields srcAddr, bytes |sort by @timestamp desc |limit 25
```

© 2018 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Parse : ephemeral field creation can be used later on in the query.... in this case "@severity" field

Query Commands



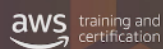
PARSE: Extract data from a log field, creating an ephemeral field

```
Log:
[INFO] 5 requests received ...
[INFO] 5 requests processed ...
[ERROR] java.lang.NullPointerException ...
parse @message "[*]" as @severity |stats count(*) by
@severity
```

© 2018 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Programmatic access : to Logs Insights : automated solutions

Programmatic Access



Available through:

- AWS Management Console
- AWS CLI
- Amazon CloudWatch Logs Insights APIs
- AWS SDK

© 2018 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Example Insights Demonstration :

- Open CloudWatch Console and then click "insights"

The screenshot shows the AWS CloudWatch Insights console. At the top, there's a navigation bar with 'Services', 'Resource Groups', and 'IAM | N. Virginia'. Below this, a dropdown menu shows 'VPC-VPCStack-1ACRQV385DTQA-FlowLogsGroup-199AHXMTPTNA2'. A query input field is present with a placeholder 'Start typing your query here...'. Below the input field are buttons for 'Run query', 'Sample queries', and 'Have feedback? Email us.'. The 'Logs' tab is selected, showing a 'Distribution of log events over time' chart. The chart shows a distribution of log events over time, with a peak around 12:30. The 'Visualization' tab is also visible.

- Select log you wish to query
- Specify timeframe
- enter a query / or use a sample query
- "Busiest" . IP address that has transferred the most/maximum amount of data over the last hour :
 - fields bytes, srcAddr, dstAddr, @timestamp

The screenshot shows the AWS CloudWatch Insights console with a query entered: 'fields bytes, srcAddr, dstAddr, @timestamp'. The 'Logs' tab is selected, showing a 'Distribution of log events over time' chart. Below the chart, a table of log results is displayed. The table has columns for '#', 'bytes', 'srcAddr', 'dstAddr', and '@timestamp'. The results show a distribution of log events over time, with a peak around 12:30. The table lists 11 records, with the first record being the most frequent.

#	bytes	srcAddr	dstAddr	@timestamp
1	3193	10.1.32.118	52.94.238.183	2018-11-12 21:14:43.000
2	40	52.216.131.179	10.1.32.118	2018-11-12 21:14:43.000
3	722	52.46.128.96	10.1.32.118	2018-11-12 21:14:43.000
4	40	52.216.131.179	10.1.32.118	2018-11-12 21:14:43.000
5	40	52.216.131.179	10.1.32.118	2018-11-12 21:14:43.000
6	6372	52.94.238.183	10.1.32.118	2018-11-12 21:14:43.000
7	40	52.216.131.179	10.1.32.118	2018-11-12 21:14:43.000
8	2055	10.1.32.118	52.46.128.96	2018-11-12 21:14:43.000
9	452	10.1.32.118	10.8.173.197	2018-11-12 21:14:43.000
10	40	52.216.131.179	10.1.32.118	2018-11-12 21:14:43.000
11	11821	10.1.32.118	52.94.238.183	2018-11-12 21:14:43.000

- automatically discovers "fields" from AWS services such as (Route53, Lambda, CloudTrail, VPC flowlogs , any json format) list fields under Discovered fields .
- calculate over next 5 min and sort by desc ,

aws Services Resource Groups

IAD | N. Virginia | Support

Add to dashboard Actions

VPC-VPCStack-1ACRQV385DTGA-FlowLogsGroup-198AH0MTPFN2 15m 30m 1h 6h 12h 1d custom

stats sum(bytes) as mbytes by srcAddr, dstAddr, bin(5m) | sort mbytes desc

Cancel Sample queries Have feedback? Email us.

Logs Visualization

Distribution of log events over time

3,525,408 records matched | 4,650,061 records (837.0 MB) scanned in 16.5s @ 282,193 records/s (36.7 MB/s)

#	srcAddr	dstAddr	bin(5m)	mbytes
1	18.214.68.60	10.0.149.85	2018-11-12 20:50:00.000	951628989
2	18.214.68.60	10.0.24.63	2018-11-12 20:45:00.000	66402637
3	18.214.68.60	10.0.77.225	2018-11-12 20:35:00.000	602091200
4	18.214.68.60	10.0.149.85	2018-11-12 20:35:00.000	563457512
5	18.214.68.60	10.0.77.225	2018-11-12 20:30:00.000	418653384
6	18.214.68.60	10.0.149.85	2018-11-12 20:55:00.000	33969729
7	10.0.24.63	10.1.161.24	2018-11-12 20:30:00.000	161466571
8	10.0.149.85	10.1.49.282	2018-11-12 20:55:00.000	14940898
9	10.0.24.63	10.1.49.282	2018-11-12 20:55:00.000	144039641
10	10.0.24.63	10.1.54.33	2018-11-12 20:45:00.000	135642586
11	10.0.24.63	10.1.176.138	2018-11-12 20:30:00.000	129908791

Feedback English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

- then filter by that IP address

stats sum(bytes) as mbytes by srcAddr, dstAddr, bin(5m) | sort mbytes desc | filter srcAddr='18.214.60.60'

aws Services Resource Groups

IAD | N. Virginia | Support

Add to dashboard Actions

VPC-VPCStack-1ACRQV385DTGA-FlowLogsGroup-198AH0MTPFN2 15m 30m 1h 6h 12h 1d custom

stats sum(bytes) as mbytes by srcAddr, dstAddr, bin(5m) | sort mbytes desc | filter srcAddr='18.214.60.60'

Run query Sample queries Have feedback? Email us.

Logs Visualization

Distribution of log events over time

7,596 records matched | 9,454,813 records (1.3 GB) scanned in 6.5s @ 1,457,726 records/s (196.7 MB/s)

#	srcAddr	dstAddr	bin(5m)	mbytes
1	18.214.68.60	10.0.149.85	2018-11-12 20:50:00.000	998019158
2	18.214.68.60	10.0.149.85	2018-11-12 20:40:00.000	912137952
3	18.214.68.60	10.0.24.63	2018-11-12 20:55:00.000	895334586
4	18.214.68.60	10.0.77.225	2018-11-12 20:20:00.000	819296560
5	18.214.68.60	10.0.77.225	2018-11-12 21:05:00.000	755199858
6	18.214.68.60	10.0.149.85	2018-11-12 20:30:00.000	75060948
7	18.214.68.60	10.0.24.63	2018-11-12 20:50:00.000	667881134
8	18.214.68.60	10.0.24.63	2018-11-12 20:45:00.000	66402637
9	18.214.68.60	10.0.24.63	2018-11-12 21:05:00.000	663189280
10	18.214.68.60	10.0.24.63	2018-11-12 20:30:00.000	627888882
11	18.214.68.60	10.0.149.85	2018-11-12 20:35:00.000	606852755

Feedback English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

- Now max min and avg byte transfer for all IP over 5 min intervals

stats avg(bytes), min(bytes), max(bytes) by bin(5m)

aws Services Resource Groups

IAD | N. Virginia | Support

Add to dashboard Actions

VPC-VPCStack-1ACRQV385DTGA-FlowLogsGroup-198AH0MTPFN2 15m 30m 1h 6h 12h 1d custom

stats avg(bytes), min(bytes), max(bytes) by bin(5m)

Cancel Sample queries Have feedback? Email us.

Logs Visualization

Distribution of log events over time

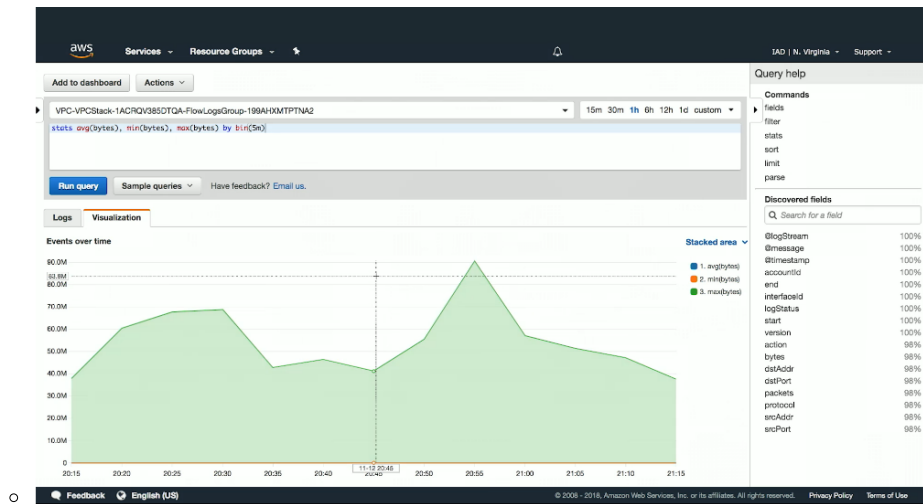
2,366,712 records matched | 4,626,905 records (633.7 MB) scanned in 3.0s @ 1,537,688 records/s (210.6 MB/s)

#	bin(5m)	avg(bytes)	min(bytes)	max(bytes)
1	2018-11-12 21:15:00.000	48671.2829	40	3792699
2	2018-11-12 21:10:00.000	3146.1879	30	3796496
3	2018-11-12 21:05:00.000	38258.482	40	37854270
4	2018-11-12 21:00:00.000	38036.4506	32	43245982
5	2018-11-12 20:55:00.000	44464.1469	37	96528426
6	2018-11-12 20:50:00.000	45194.6299	32	55516312
7	2018-11-12 20:45:00.000	49999.1983	40	37559597
8	2018-11-12 20:40:00.000	36352.7241	32	37929455
9	2018-11-12 20:35:00.000	46449.8931	32	42974665
10	2018-11-12 20:30:00.000	43021.7797	40	68720856
11	2018-11-12 20:25:00.000	45991.6556	40	67783271

Feedback English (US)

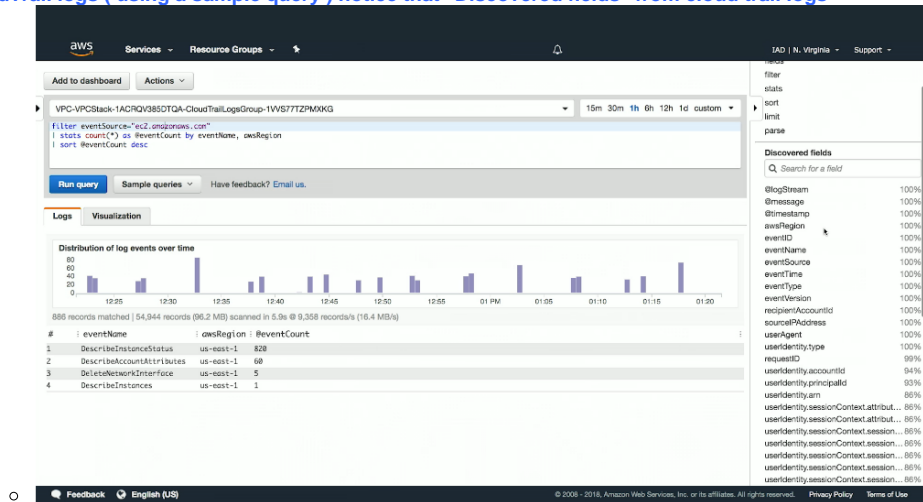
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Or use Visualization to see graph of results .



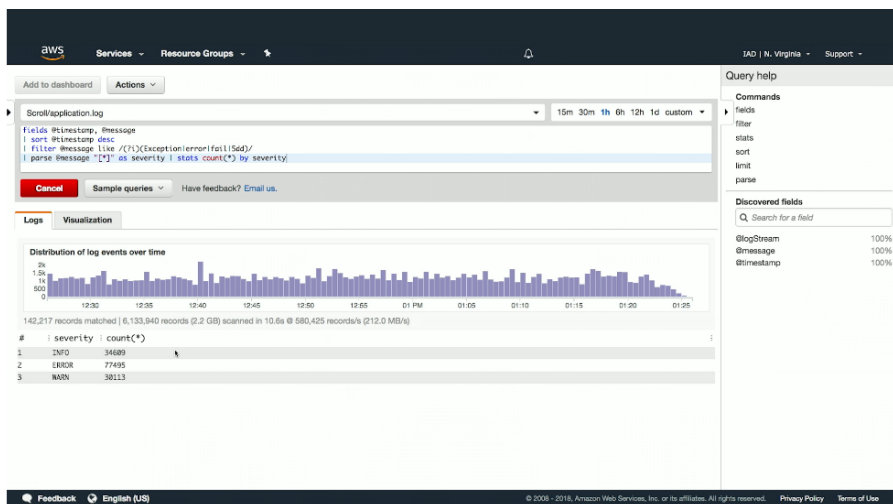
- History of queries
- Export to dashboard so you can see

- CloudTrail logs (using a sample query) notice that "Discovered fields" from cloud trail logs



Application logs : autodiscovered the fields that were defined by system logs int his case sent to cloudwatch . looking for error, exception or failed

- And using parse command to create a field called "severity" and then use the count(*)



Cost : \$0.005 per GB in US East (N. Virginia)

- Pricing is based on the amount of ingested log data scanned for each query; you pay **\$0.005 per GB in US East (N. Virginia)**, with similar prices in the other regions.

Custom Metrics to set alarms to accelerate troubleshooting

Reference Links :

- Announcement overview : <https://aws.amazon.com/blogs/aws/new-amazon-cloudwatch-logs-insights-fast-interactive-log-analytics/>
- AWS Training Digital : <https://www.aws.training/learningobject/video?id=27171>
- When logged into your AWS Console access using this url : <https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:logs-insights>