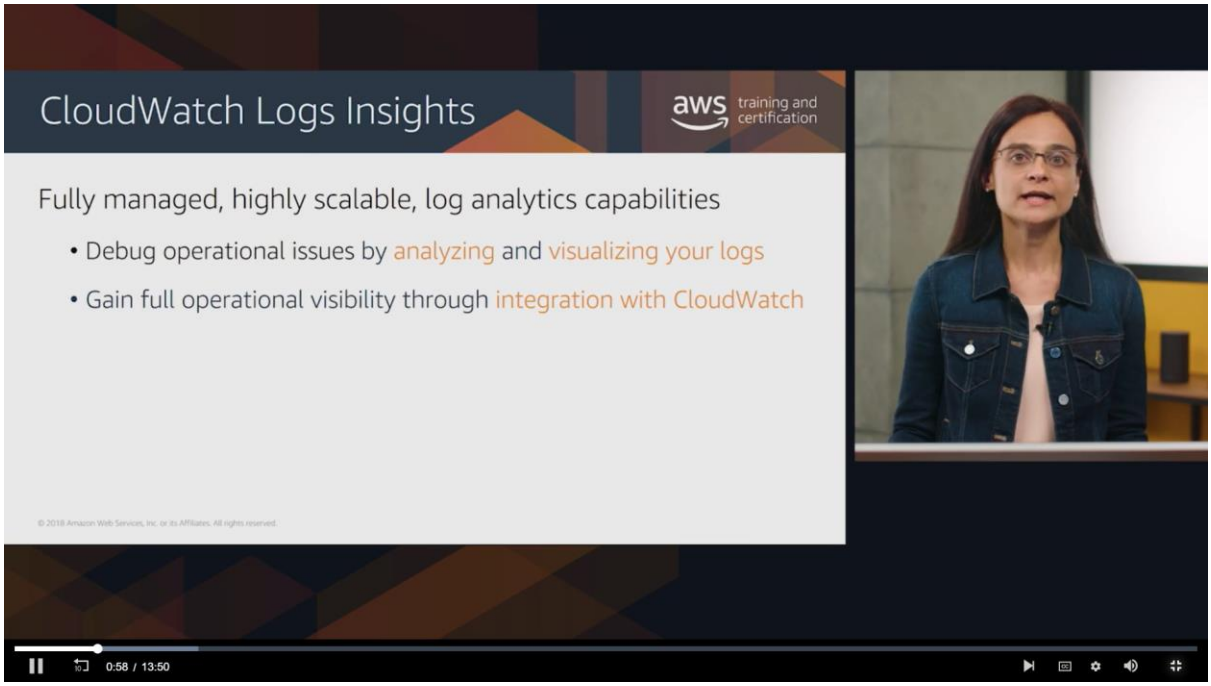

CloudWatch Logs Insights
aws training and certification
Fully managed, highly scalable, log analytics capabilities
• Debug operational issues by analyzing and visualizing your logs
• Gain full operational visibility through integration with CloudWatch
© 2018 Amazon Web Services, Inc. or its Affiliates. All rights reserved.
0:58 / 13:50

Works with Any Log Type

aws training and certification

- 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

AWS Lambda

VPC flow logs

AWS CloudTrail

Amazon Route 53

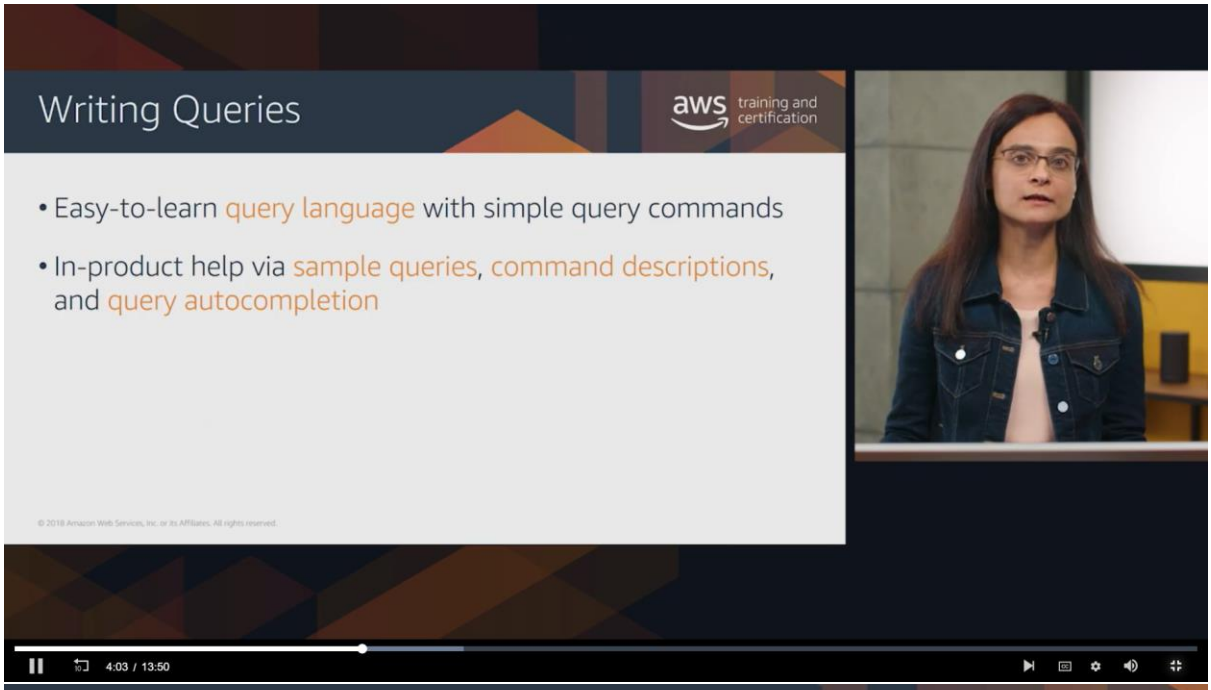
© 2018 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Simple but Powerful Querying

aws training and certification

- Write queries with aggregations, filters, and regular expressions
- Visualize query results and time series data

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



Query Commands

aws training and certification

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.

Query Commands

aws training and certification

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
```

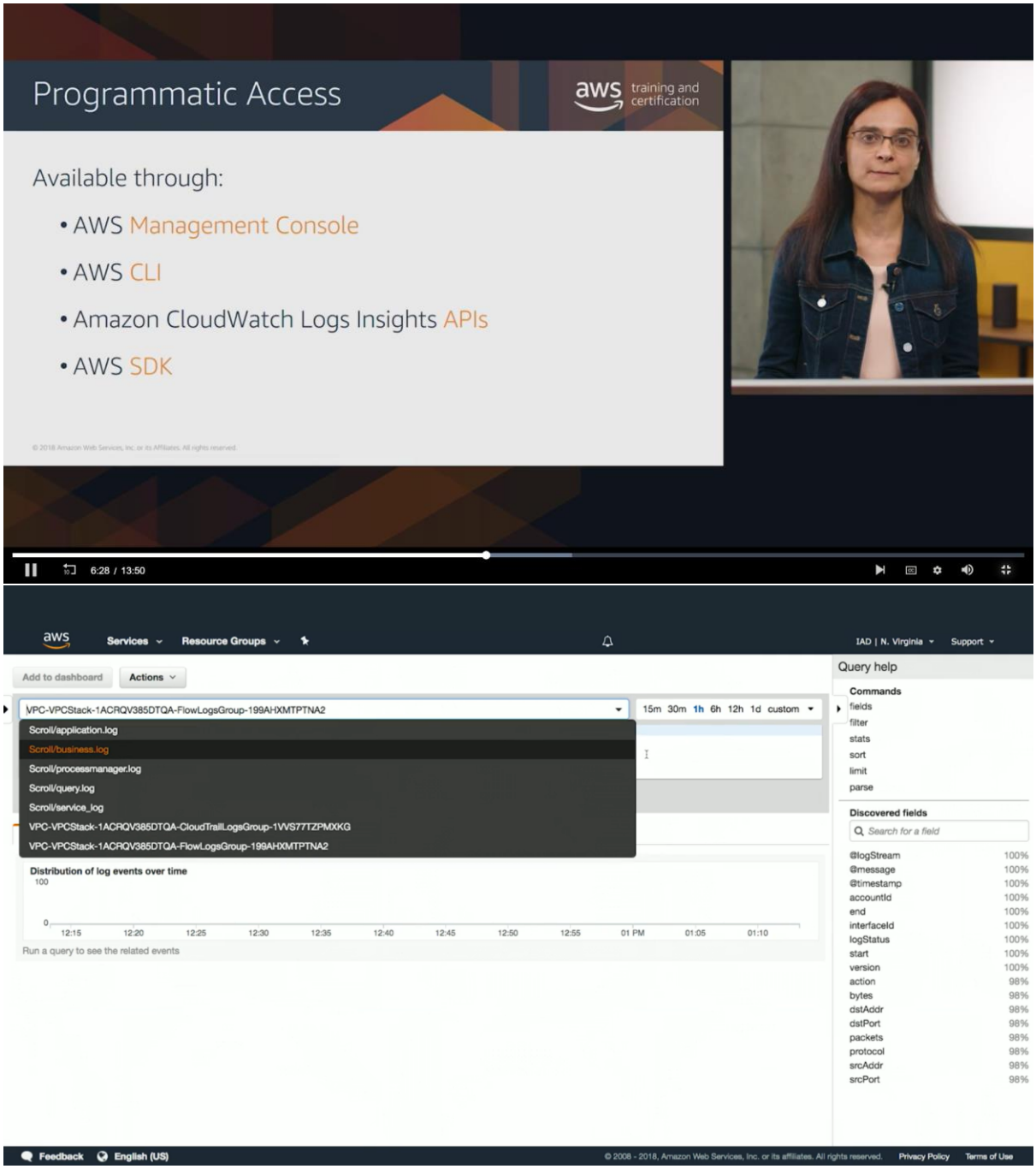
© 2018 Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Query Commands

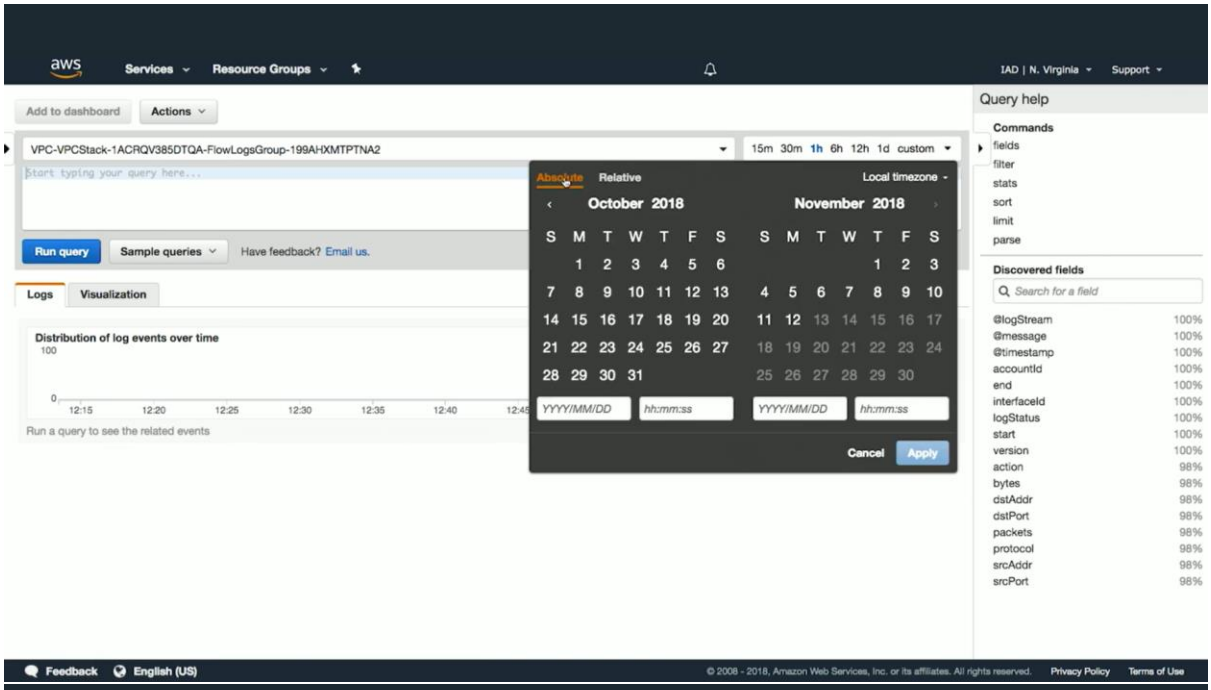
aws training and certification

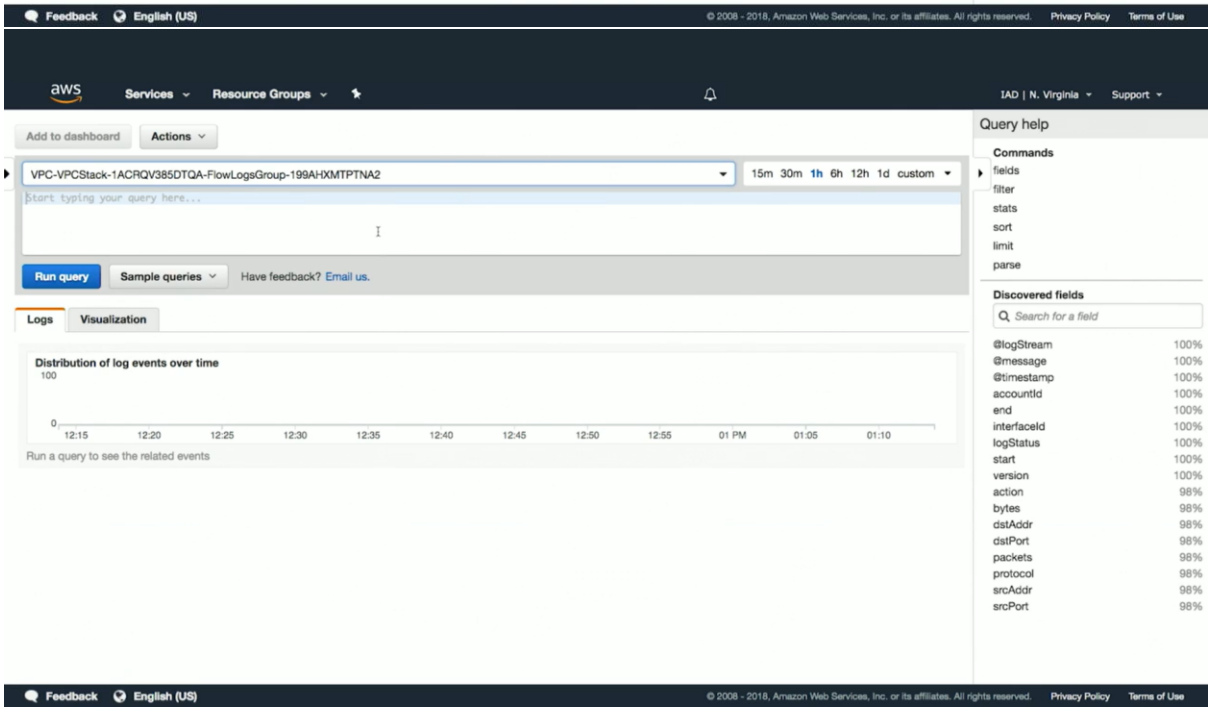
PARSE: Extract data from a log field, creating an ephemeral field

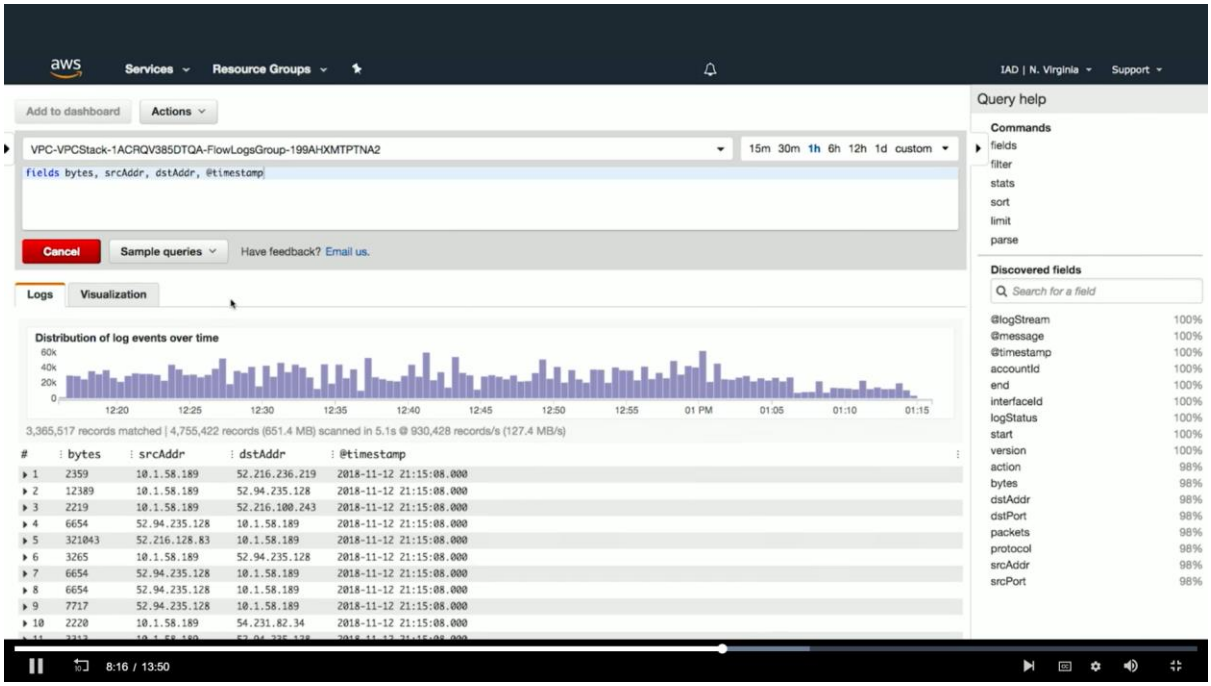
```
Log:
[INFO] 5 requests received …
[INFO] 5 requests processed …
[ERROR] java.lang.NullPointerException …
parse @message "[*]" as @severity |stats count(*) by
@severity
```

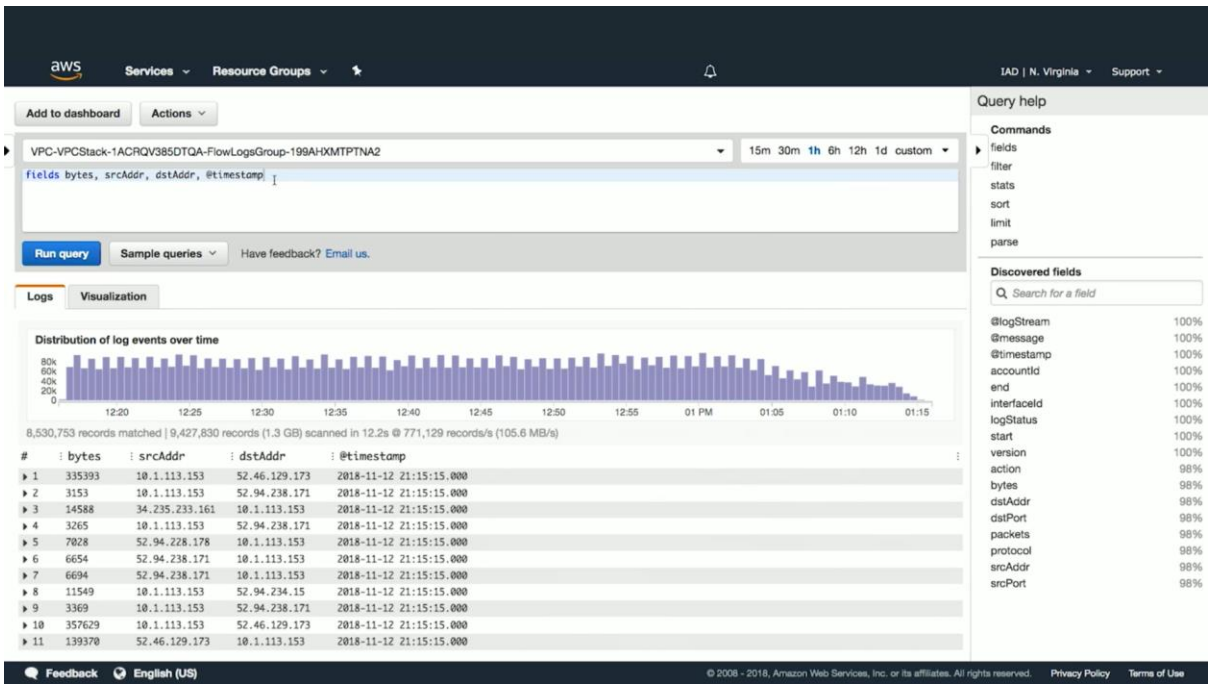

Programmatic Access
aws training and certification
Available through:
• AWS Management Console
• AWS CLI
• Amazon CloudWatch Logs Insights APIs
• AWS SDK
© 2018 Amazon Web Services, Inc. or its Affiliates. All rights reserved.
6:28 / 13:50

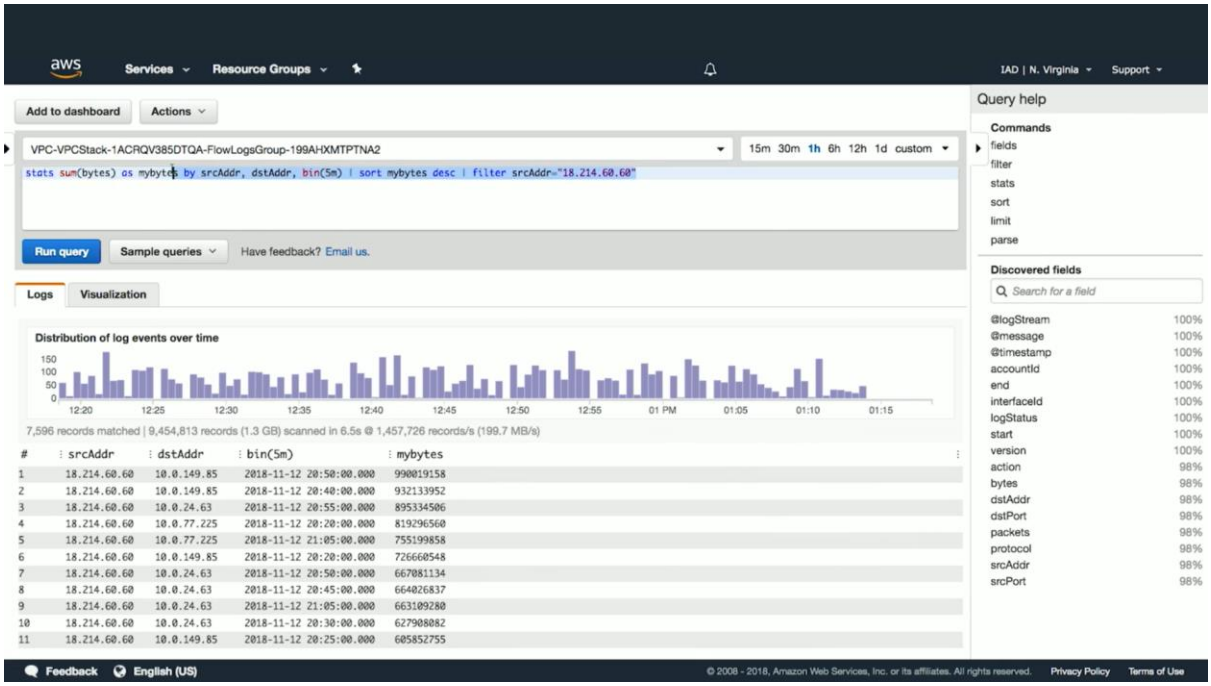
aws
Services
Resource Groups
IAD | N. Virginia
Support
Add to dashboard
Actions
VPC-VPCStack-1ACRQV385DTQA-FlowLogsGroup-199AHXMTPTNA2
15m 30m 1h 6h 12h 1d custom
Scroll/application.log
Scroll/business.log
Scroll/processmanager.log
Scroll/query.log
Scroll/service_log
VPC-VPCStack-1ACRQV385DTQA-CloudTrailLogsGroup-1VVS77TZPMXKG
VPC-VPCStack-1ACRQV385DTQA-FlowLogsGroup-199AHXMTPTNA2
Distribution of log events over time
100
0
12:15
12:20
12:25
12:30
12:35
12:40
12:45
12:50
12:55
01 PM
01:05
01:10
Run a query to see the related events
Query help
Commands
fields
filter
stats
sort
limit
parse
Discovered fields
Search for a field
@logStream 100%
@message 100%
@timestamp 100%
accountId 100%
end 100%
interfaceId 100%
logStatus 100%
start 100%
version 100%
action 98%
bytes 98%
dstAddr 98%
dstPort 98%
packets 98%
protocol 98%
srcAddr 98%
srcPort 98%
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

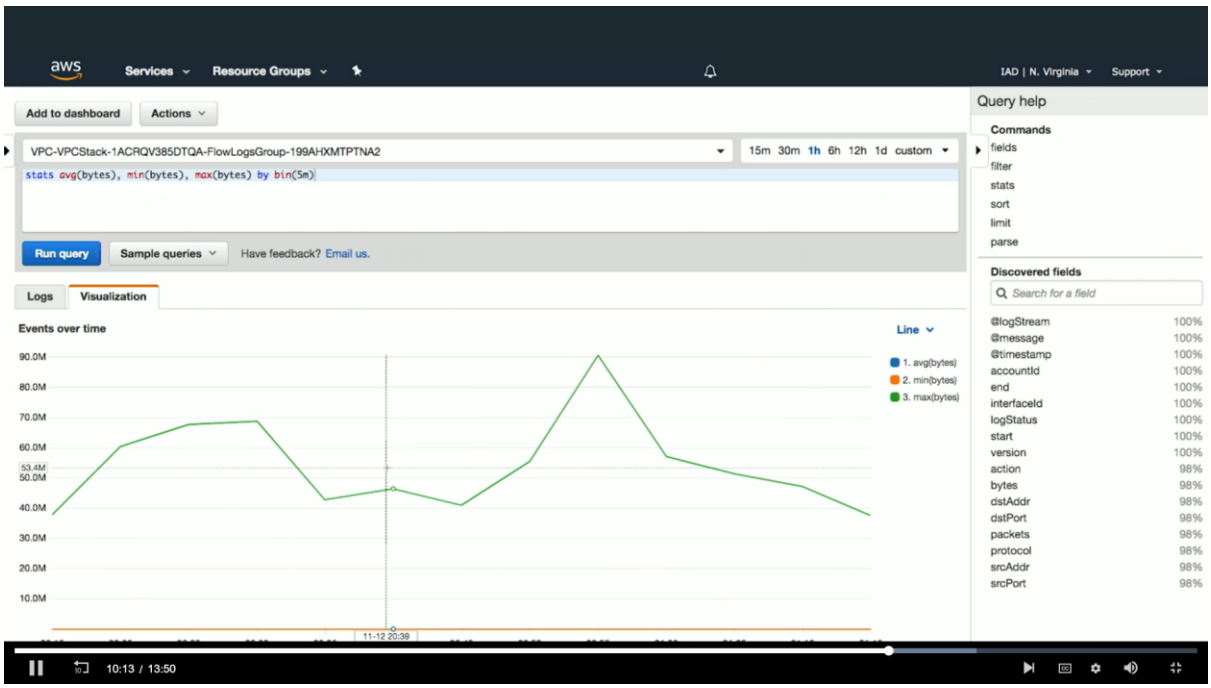

aws
Services
Resource Groups
IAD | N. Virginia
Support
Add to dashboard
Actions
VPC-VPCStack-1ACRQV385DTQA-FlowLogsGroup-199AHXMTPTNA2
15m 30m 1h 6h 12h 1d custom
Start typing your query here...
Run query
Sample queries
Have feedback? Email us.
Logs
Visualization
Distribution of log events over time
100
0
12:15 12:20 12:25 12:30 12:35 12:40 12:45
Run a query to see the related events
Absolute
Relative
Local timezone
October 2018
November 2018
S M T W T F S
YYYY/MM/DD
hh:mm:ss
Cancel
Apply
Query help
Commands
fields
filter
stats
sort
limit
parse
Discovered fields
Search for a field
@logStream 100%
@message 100%
@timestamp 100%
accountId 100%
end 100%
interfaceId 100%
logStatus 100%
start 100%
version 100%
action 98%
bytes 98%
dstAddr 98%
dstPort 98%
packets 98%
protocol 98%
srcAddr 98%
srcPort 98%
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

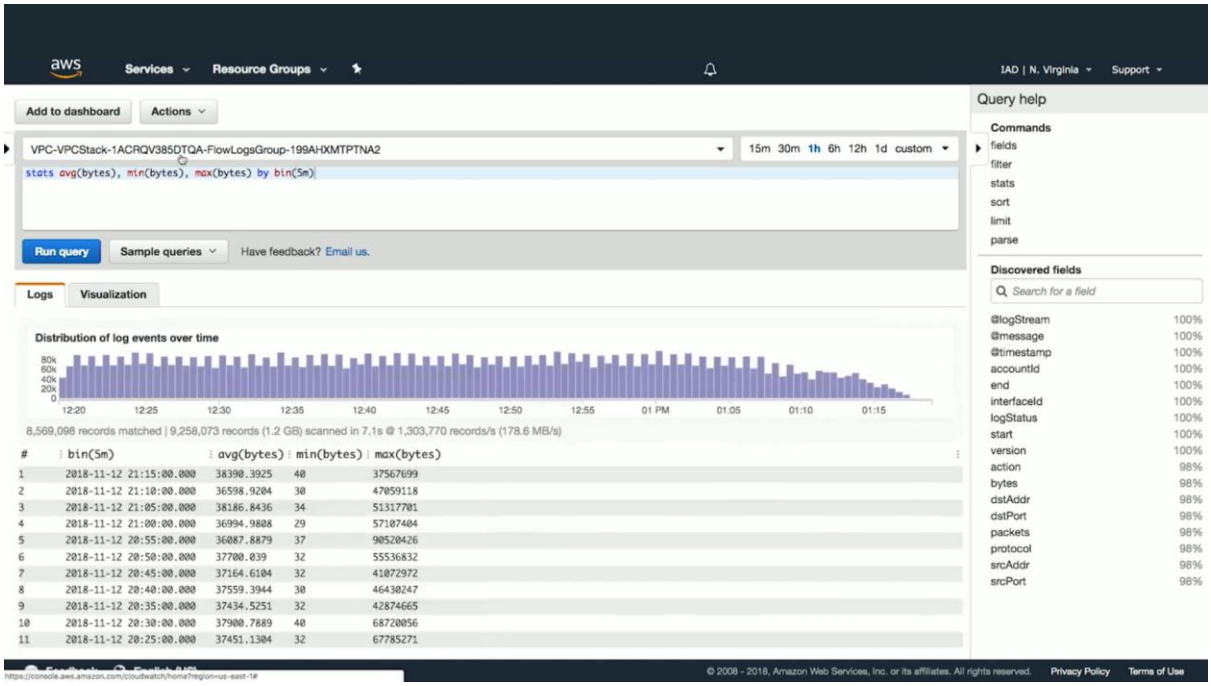

aws
Services
Resource Groups
IAD | N. Virginia
Support
Add to dashboard
Actions
VPC-VPCStack-1ACRQV385DTQA-FlowLogsGroup-199AHXMTPTNA2
15m 30m 1h 6h 12h 1d custom
Start typing your query here...
Run query
Sample queries
Have feedback? Email us.
Logs
Visualization
Distribution of log events over time
100
0
12:15 12:20 12:25 12:30 12:35 12:40 12:45 12:50 12:55 01 PM 01:05 01:10
Run a query to see the related events
Query help
Commands
fields
filter
stats
sort
limit
parse
Discovered fields
Search for a field
@logStream 100%
@message 100%
@timestamp 100%
accountId 100%
end 100%
interfaceId 100%
logStatus 100%
start 100%
version 100%
action 98%
bytes 98%
dstAddr 98%
dstPort 98%
packets 98%
protocol 98%
srcAddr 98%
srcPort 98%
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

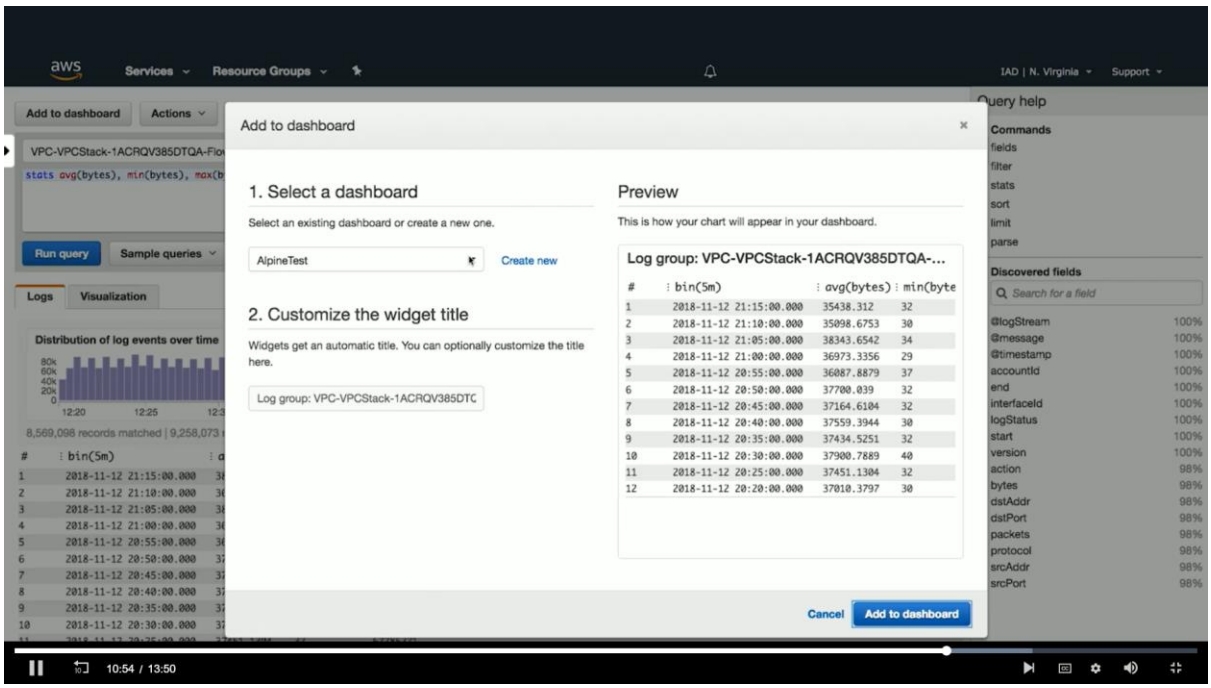

aws
Services
Resource Groups
IAD | N. Virginia
Support
Add to dashboard
Actions
VPC-VPCStack-1ACRQV385DTQA-FlowLogsGroup-199AHXMTPTNA2
15m 30m 1h 6h 12h 1d custom
fields bytes, srcAddr, dstAddr, @timestamp
Cancel
Sample queries
Have feedback? Email us.
Logs
Visualization
Distribution of log events over time
60k
40k
20k
0
12:20 12:25 12:30 12:35 12:40 12:45 12:50 12:55 01 PM 01:05 01:10 01:15
3,365,517 records matched | 4,755,422 records (651.4 MB) scanned in 5.1s @ 930,428 records/s (127.4 MB/s)
bytes srcAddr dstAddr @timestamp
1 2359 10.1.58.189 52.216.236.219 2018-11-12 21:15:08.000
2 12389 10.1.58.189 52.94.235.128 2018-11-12 21:15:08.000
3 2219 10.1.58.189 52.216.100.243 2018-11-12 21:15:08.000
4 6654 52.94.235.128 10.1.58.189 2018-11-12 21:15:08.000
5 321043 52.216.128.83 10.1.58.189 2018-11-12 21:15:08.000
6 3265 10.1.58.189 52.94.235.128 2018-11-12 21:15:08.000
7 6654 52.94.235.128 10.1.58.189 2018-11-12 21:15:08.000
8 6654 52.94.235.128 10.1.58.189 2018-11-12 21:15:08.000
9 7717 52.94.235.128 10.1.58.189 2018-11-12 21:15:08.000
10 2220 10.1.58.189 54.231.82.34 2018-11-12 21:15:08.000
Query help
Commands
fields
filter
stats
sort
limit
parse
Discovered fields
Search for a field
@logStream 100%
@message 100%
@timestamp 100%
accountId 100%
end 100%
interfaceId 100%
logStatus 100%
start 100%
version 100%
action 98%
bytes 98%
dstAddr 98%
dstPort 98%
packets 98%
protocol 98%
srcAddr 98%
srcPort 98%
8:16 / 13:50

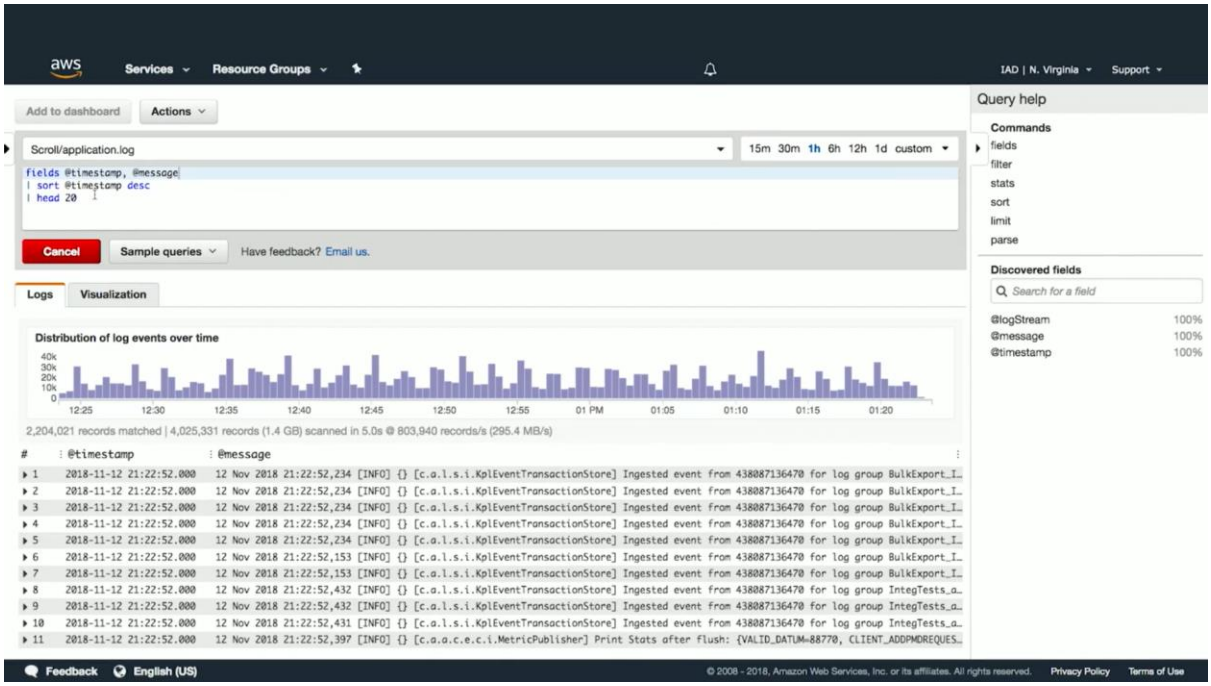

aws
Services
Resource Groups
IAD | N. Virginia
Support
Add to dashboard
Actions
VPC-VPCStack-1ACRQV385DTQA-FlowLogsGroup-199AHXMTPTNA2
15m 30m 1h 6h 12h 1d custom
fields bytes, srcAddr, dstAddr, @timestamp
Run query
Sample queries
Have feedback? Email us.
Logs
Visualization
Distribution of log events over time
80k
60k
40k
20k
0
12:20 12:25 12:30 12:35 12:40 12:45 12:50 12:55 01 PM 01:05 01:10 01:15
8,530,753 records matched | 9,427,830 records (1.3 GB) scanned in 12.2s @ 771,129 records/s (105.6 MB/s)
bytes srcAddr dstAddr @timestamp
1 335393 10.1.113.153 52.46.129.173 2018-11-12 21:15:15.000
2 3153 10.1.113.153 52.94.238.171 2018-11-12 21:15:15.000
3 14588 34.235.233.161 10.1.113.153 2018-11-12 21:15:15.000
4 3265 10.1.113.153 52.94.238.171 2018-11-12 21:15:15.000
5 7028 52.94.228.178 10.1.113.153 2018-11-12 21:15:15.000
6 6654 52.94.238.171 10.1.113.153 2018-11-12 21:15:15.000
7 6694 52.94.238.171 10.1.113.153 2018-11-12 21:15:15.000
8 11549 10.1.113.153 52.94.234.15 2018-11-12 21:15:15.000
9 3369 10.1.113.153 52.94.238.171 2018-11-12 21:15:15.000
10 357629 10.1.113.153 52.46.129.173 2018-11-12 21:15:15.000
11 139370 52.46.129.173 10.1.113.153 2018-11-12 21:15:15.000
Query help
Commands
fields
filter
stats
sort
limit
parse
Discovered fields
Search for a field
@logStream 100%
@message 100%
@timestamp 100%
accountId 100%
end 100%
interfaceId 100%
logStatus 100%
start 100%
version 100%
action 98%
bytes 98%
dstAddr 98%
dstPort 98%
packets 98%
protocol 98%
srcAddr 98%
srcPort 98%
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use


aws
Services
Resource Groups
IAD | N. Virginia
Support
Add to dashboard
Actions
VPC-VPCStack-1ACRQV385DTQA-FlowLogsGroup-199AHXMTPTNA2
15m 30m 1h 6h 12h 1d custom
stats sum(bytes) as mybytes by srcAddr, dstAddr, bin(5m) | sort mybytes 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 (199.7 MB/s)
srcAddr dstAddr bin(5m) mybytes
1 18.214.60.60 10.0.149.85 2018-11-12 20:50:00.000 990019158
2 18.214.60.60 10.0.149.85 2018-11-12 20:40:00.000 932133952
3 18.214.60.60 10.0.24.63 2018-11-12 20:55:00.000 895334506
4 18.214.60.60 10.0.77.225 2018-11-12 20:20:00.000 819296560
5 18.214.60.60 10.0.77.225 2018-11-12 21:05:00.000 755199858
6 18.214.60.60 10.0.149.85 2018-11-12 20:20:00.000 726660548
7 18.214.60.60 10.0.24.63 2018-11-12 20:50:00.000 667081134
8 18.214.60.60 10.0.24.63 2018-11-12 20:45:00.000 664026837
9 18.214.60.60 10.0.24.63 2018-11-12 21:05:00.000 663109280
10 18.214.60.60 10.0.24.63 2018-11-12 20:30:00.000 627908082
11 18.214.60.60 10.0.149.85 2018-11-12 20:25:00.000 605852755
Query help
Commands
fields
filter
stats
sort
limit
parse
Discovered fields
Search for a field
@logStream 100%
@message 100%
@timestamp 100%
accountId 100%
end 100%
interfaceId 100%
logStatus 100%
start 100%
version 100%
action 98%
bytes 98%
dstAddr 98%
dstPort 98%
packets 98%
protocol 98%
srcAddr 98%
srcPort 98%
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

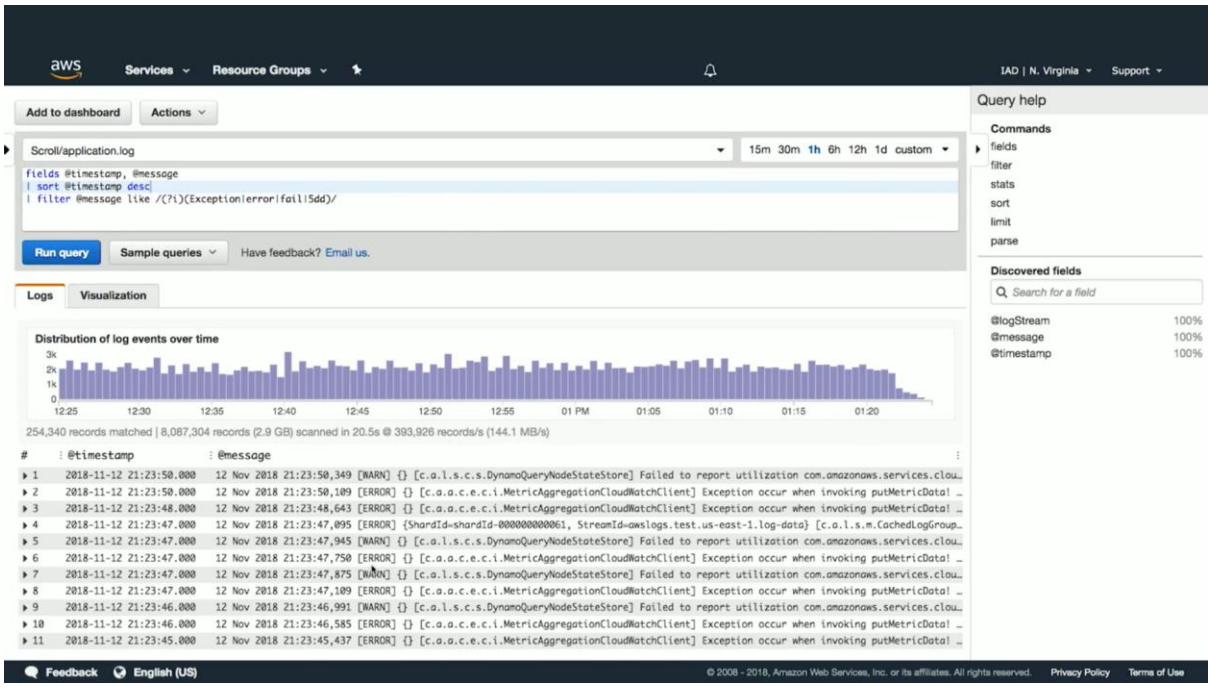

aws
Services
Resource Groups
IAD | N. Virginia
Support
Add to dashboard
Actions
VPC-VPCStack-1ACRQV385DTQA-FlowLogsGroup-199AHXMTPTNA2
15m 30m 1h 6h 12h 1d custom
stats avg(bytes), min(bytes), max(bytes) by bin(5m)
Run query
Sample queries
Have feedback? Email us.
Logs
Visualization
Events over time
Line
1. avg(bytes)
2. min(bytes)
3. max(bytes)
90.0M
80.0M
70.0M
60.0M
53.4M
50.0M
40.0M
30.0M
20.0M
10.0M
11-12 20:39
Query help
Commands
fields
filter
stats
sort
limit
parse
Discovered fields
Search for a field
@logStream 100%
@message 100%
@timestamp 100%
accountId 100%
end 100%
interfaceId 100%
logStatus 100%
start 100%
version 100%
action 98%
bytes 98%
dstAddr 98%
dstPort 98%
packets 98%
protocol 98%
srcAddr 98%
srcPort 98%
10:13 / 13:50

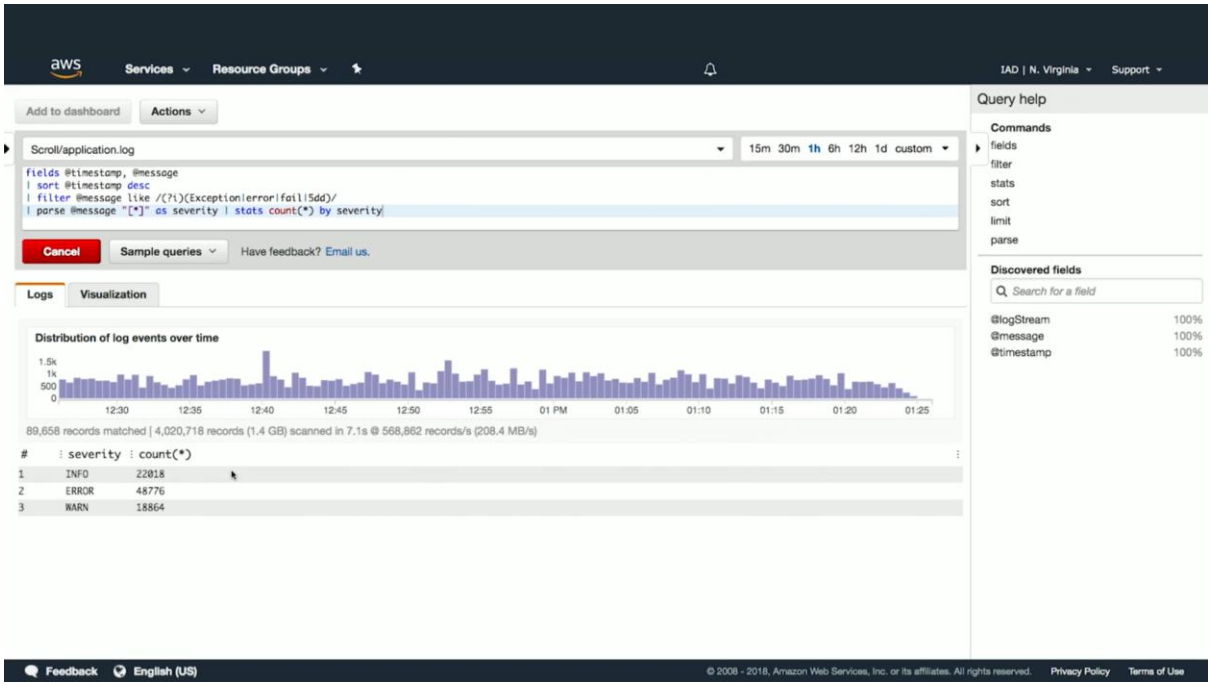

aws
Services
Resource Groups
IAD | N. Virginia
Support
Add to dashboard
Actions
VPC-VPCStack-1ACRQV385DTQA-FlowLogsGroup-199AHXMTPTNA2
15m 30m 1h 6h 12h 1d custom
stats avg(bytes), min(bytes), max(bytes) by bin(5m)
Run query
Sample queries
Have feedback? Email us.
Logs
Visualization
Distribution of log events over time
80k
60k
40k
20k
0
12:20 12:25 12:30 12:35 12:40 12:45 12:50 12:55 01 PM 01:05 01:10 01:15
8,569,098 records matched | 9,258,073 records (1.2 GB) scanned in 7.1s @ 1,303,770 records/s (178.6 MB/s)
bin(5m) avg(bytes) min(bytes) max(bytes)
1 2018-11-12 21:15:00.000 38390.3925 40 37567699
2 2018-11-12 21:10:00.000 36598.9204 30 47059118
3 2018-11-12 21:05:00.000 38186.8436 34 51317701
4 2018-11-12 21:00:00.000 36994.9808 29 57107404
5 2018-11-12 20:55:00.000 36087.8879 37 90520426
6 2018-11-12 20:50:00.000 37700.039 32 55536832
7 2018-11-12 20:45:00.000 37164.6104 32 41072972
8 2018-11-12 20:40:00.000 37559.3944 30 46430247
9 2018-11-12 20:35:00.000 37434.5251 32 42874665
10 2018-11-12 20:30:00.000 37900.7889 40 68720056
11 2018-11-12 20:25:00.000 37451.1304 32 67785271
Query help
Commands
fields
filter
stats
sort
limit
parse
Discovered fields
Search for a field
@logStream 100%
@message 100%
@timestamp 100%
accountId 100%
end 100%
interfaceId 100%
logStatus 100%
start 100%
version 100%
action 98%
bytes 98%
dstAddr 98%
dstPort 98%
packets 98%
protocol 98%
srcAddr 98%
srcPort 98%
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use


aws
Services
Resource Groups
IAD | N. Virginia
Support
Add to dashboard
Actions
Add to dashboard
1. Select a dashboard
Select an existing dashboard or create a new one.
AlpineTest
Create new
2. Customize the widget title
Widgets get an automatic title. You can optionally customize the title here.
Log group: VPC-VPCStack-1ACRQV385DTC
Preview
This is how your chart will appear in your dashboard.
Log group: VPC-VPCStack-1ACRQV385DTQA-...
bin(5m) avg(bytes) min(byte
1 2018-11-12 21:15:00.000 35438.312 32
2 2018-11-12 21:10:00.000 35098.6753 30
3 2018-11-12 21:05:00.000 38343.6542 34
4 2018-11-12 21:00:00.000 36973.3356 29
5 2018-11-12 20:55:00.000 36087.8879 37
6 2018-11-12 20:50:00.000 37700.039 32
7 2018-11-12 20:45:00.000 37164.6104 32
8 2018-11-12 20:40:00.000 37559.3944 30
9 2018-11-12 20:35:00.000 37434.5251 32
10 2018-11-12 20:30:00.000 37900.7889 40
11 2018-11-12 20:25:00.000 37451.1304 32
12 2018-11-12 20:20:00.000 37010.3797 30
Cancel
Add to dashboard
Query help
Commands
fields
filter
stats
sort
limit
parse
Discovered fields
Search for a field
@logStream 100%
@message 100%
@timestamp 100%
accountId 100%
end 100%
interfaceId 100%
logStatus 100%
start 100%
version 100%
action 98%
bytes 98%
dstAddr 98%
dstPort 98%
packets 98%
protocol 98%
srcAddr 98%
srcPort 98%
10:54 / 13:50



For warning error alert exception




aws
Services
Resource Groups
IAD | N. Virginia
Support
Add to dashboard
Actions
Scroll/application.log
15m 30m 1h 6h 12h 1d custom
fields @timestamp, @message
| sort @timestamp desc
| filter @message like /(?i)(Exception|error|fail|5dd)/
| parse @message "[*]" as severity | stats count(*) by severity
Cancel
Sample queries
Have feedback? Email us.
Logs
Visualization
Distribution of log events over time
1.5k
1k
500
0
12:30
12:35
12:40
12:45
12:50
12:55
01 PM
01:05
01:10
01:15
01:20
01:25
89,658 records matched | 4,020,718 records (1.4 GB) scanned in 7.1s @ 568,862 records/s (208.4 MB/s)
severity count(*)
1 INFO 22018
2 ERROR 48776
3 WARN 18864
Query help
Commands
fields
filter
stats
sort
limit
parse
Discovered fields
Search for a field
@logStream 100%
@message 100%
@timestamp 100%
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use