

『振興五倍』 的 K8S 監控 可觀察性分析

Daniel Yeung

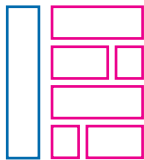
Splunk Taiwan 資深技術顧問



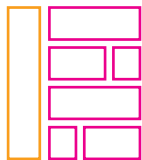
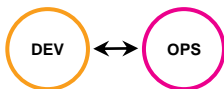
每個企業，正在經歷『雲和容器』演進歷程

To increase velocity, agility and responsiveness

Retain & Optimize



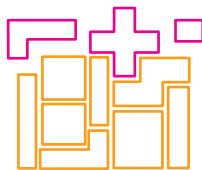
Lift & Shift



Re-Factor



Cloud Managed e.g. RDS, DynamoDB, SaaS

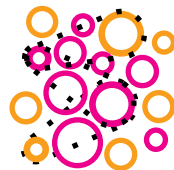


More Modular, but

Re-Architect / Cloud-Native



Cloud First Architecture



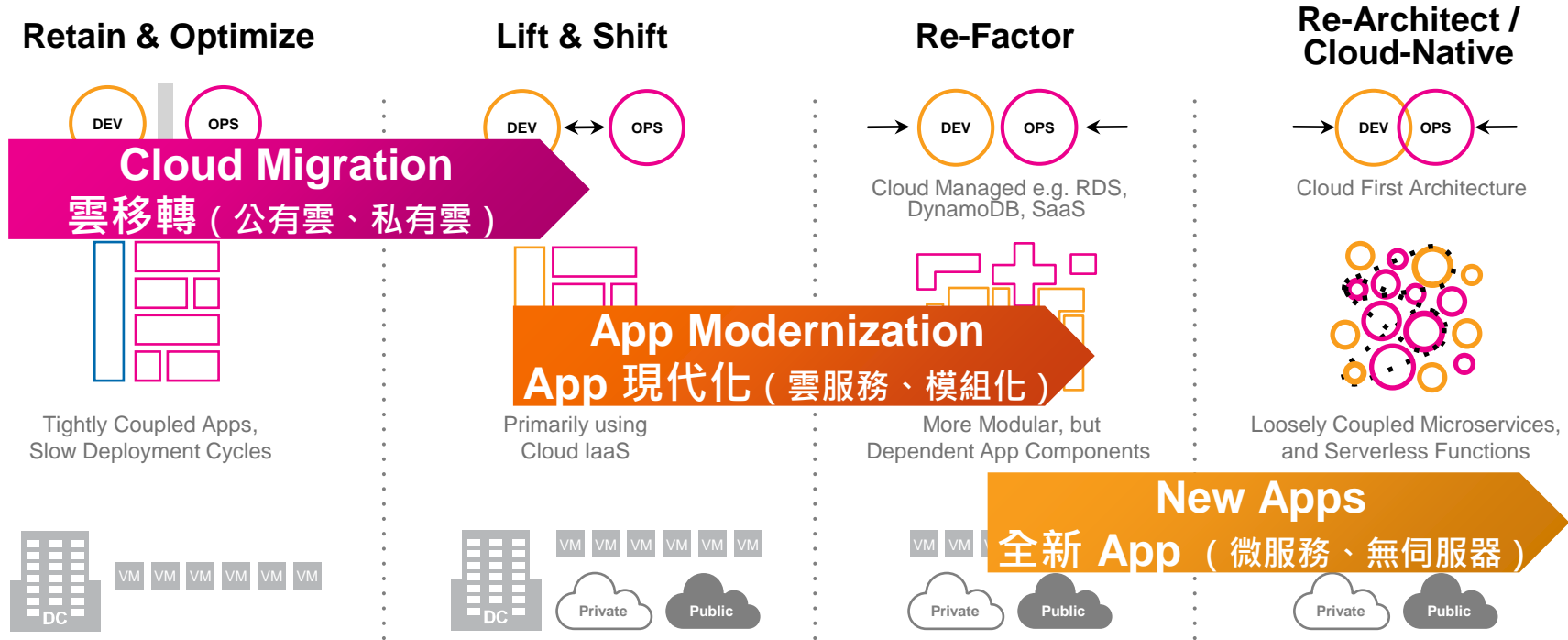
Loosely Coupled Microservices, Serverless Functions

“By 2025, 85% of organizations will run containers in production, up from less than 30% in 2020”. 2025 年會有 85 % 移到容器執行。

– Gartner, Dec 14, 2020

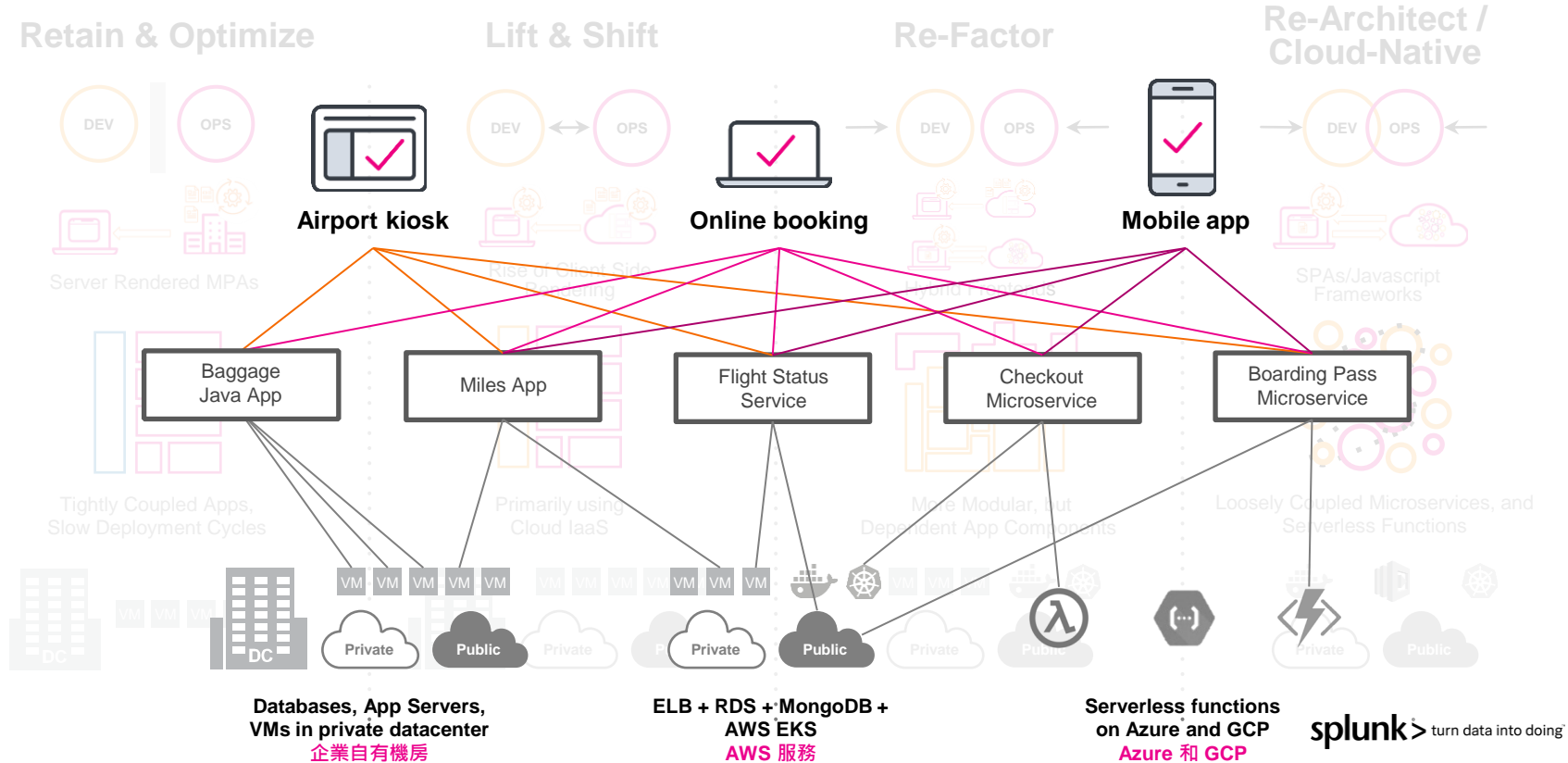
進行中 雲移轉、App現代化、新架構App上線

To increase reliability, velocity and agility



Your World has Never Been More Complex

App現代化、容器架構、雲服務，帶來更多複雜度



Observability Is the Future

傳統監控做不到，需透過『可觀察性』監控

Traditional monitoring doesn't work anymore

Monitoring 監控

Point Tools (單點工具)

Data on Screen (資料顯示)

Ad Hoc and Siloed
(隨機查詢、分開)

Observability 可觀察性

Integrated (整合)

Answers (答案)

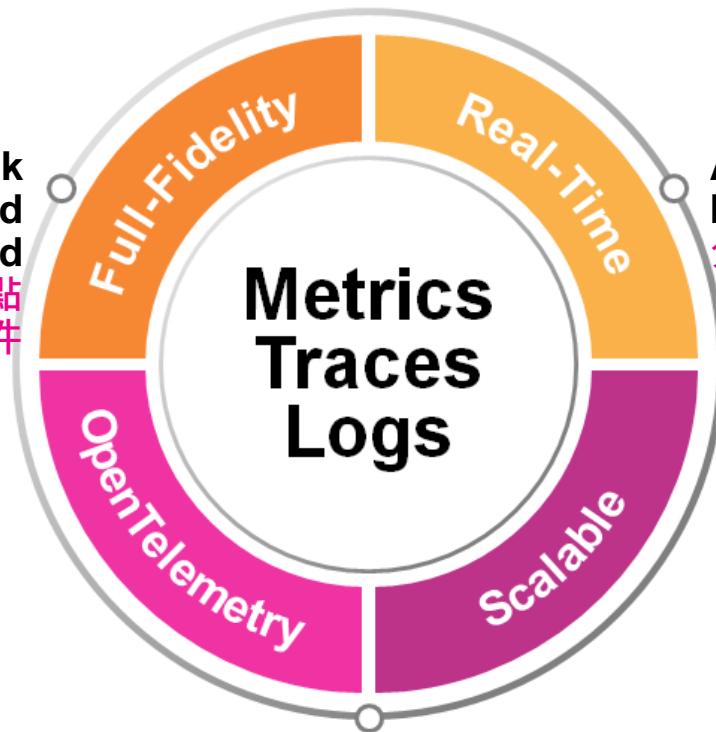
Centralized and Scalable
(集中、可擴充)

What's Required for Observability

『可觀察性』
必要需求

(效能、追蹤、日誌)

Full-Stack
and
End-to-End
點對點
完整套件



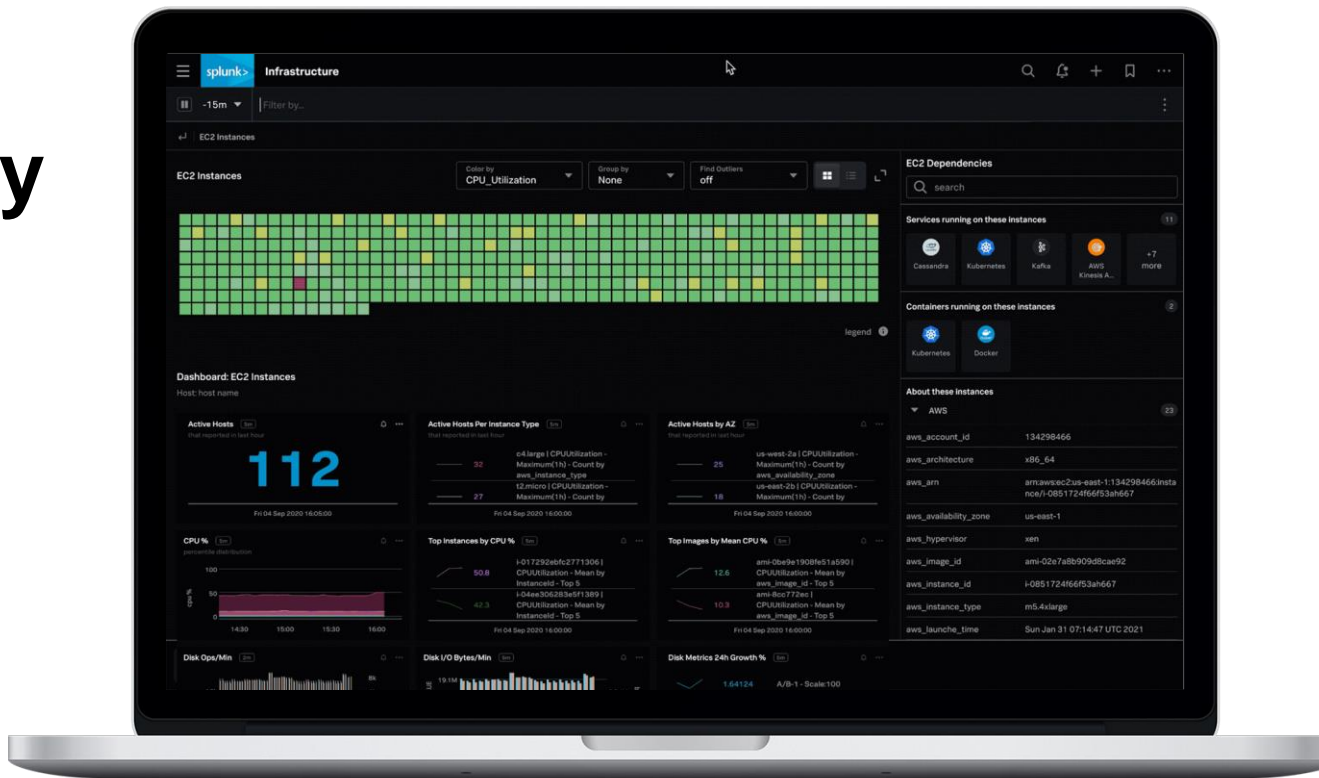
Analytics-
Powered
分析驅動

Enterprise-Grade
企業等規模產品

Splunk 推出 Observability Cloud

可觀察性 雲服務

- Full-Stack, End-to-End
- Analytics-Powered
- Enterprise-Grade
- OpenTelemetry-Native

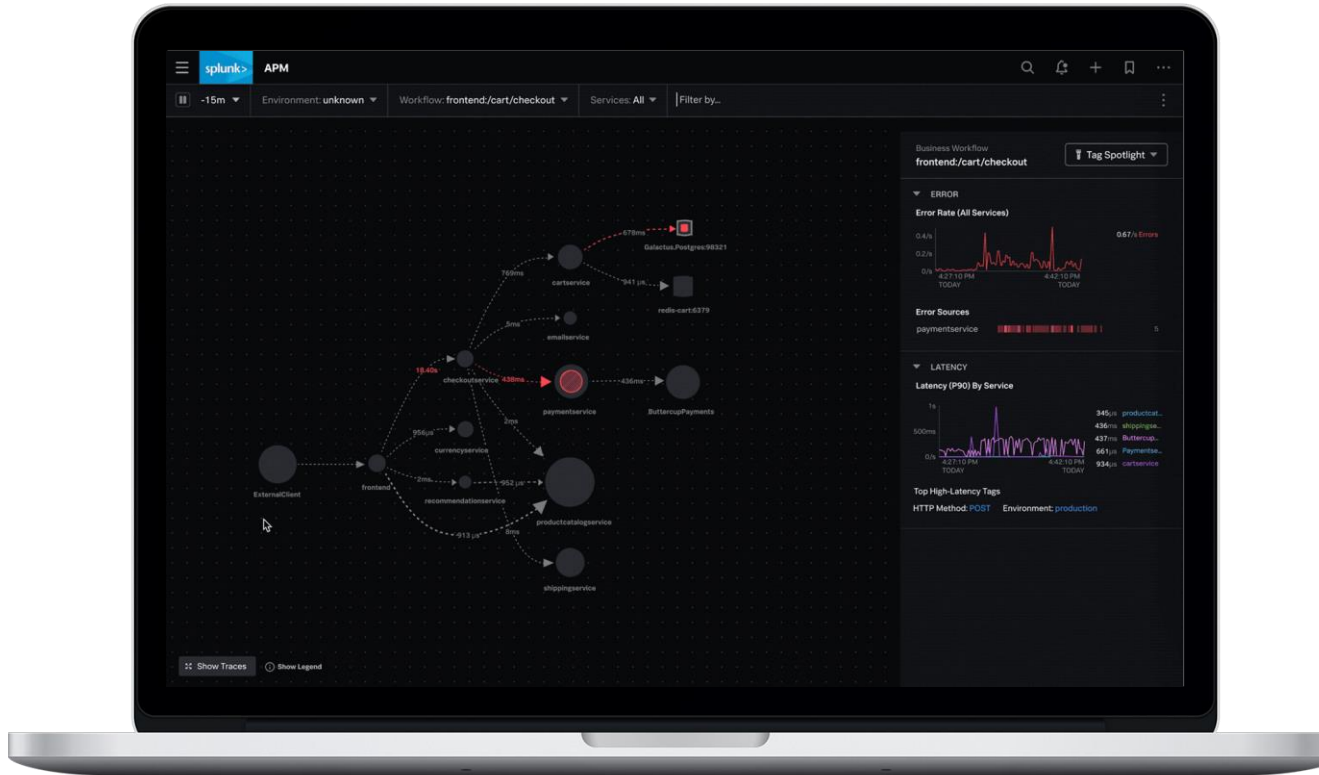


Analytics-Powered

分析驅動

No more dead-end investigations

- Connected and contextualized data
- Pattern detection for more accurate alerting
- Directed troubleshooting



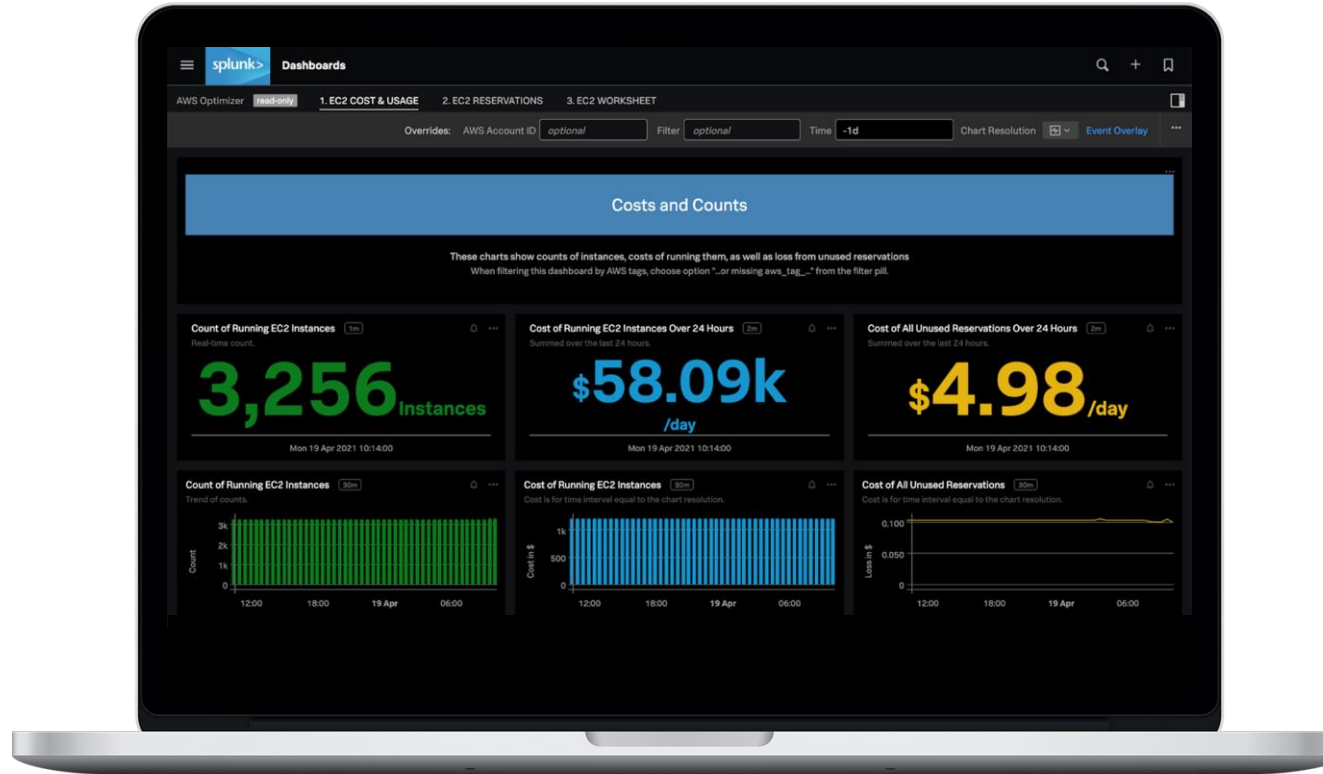
Enterprise Grade

企業等級



Scale confidently with predictable costs and enterprise controls

- Observability as a Service
- Best-in-class performance and scale
- Trusted by 91 of the Fortune 100



Open Telemetry-Native

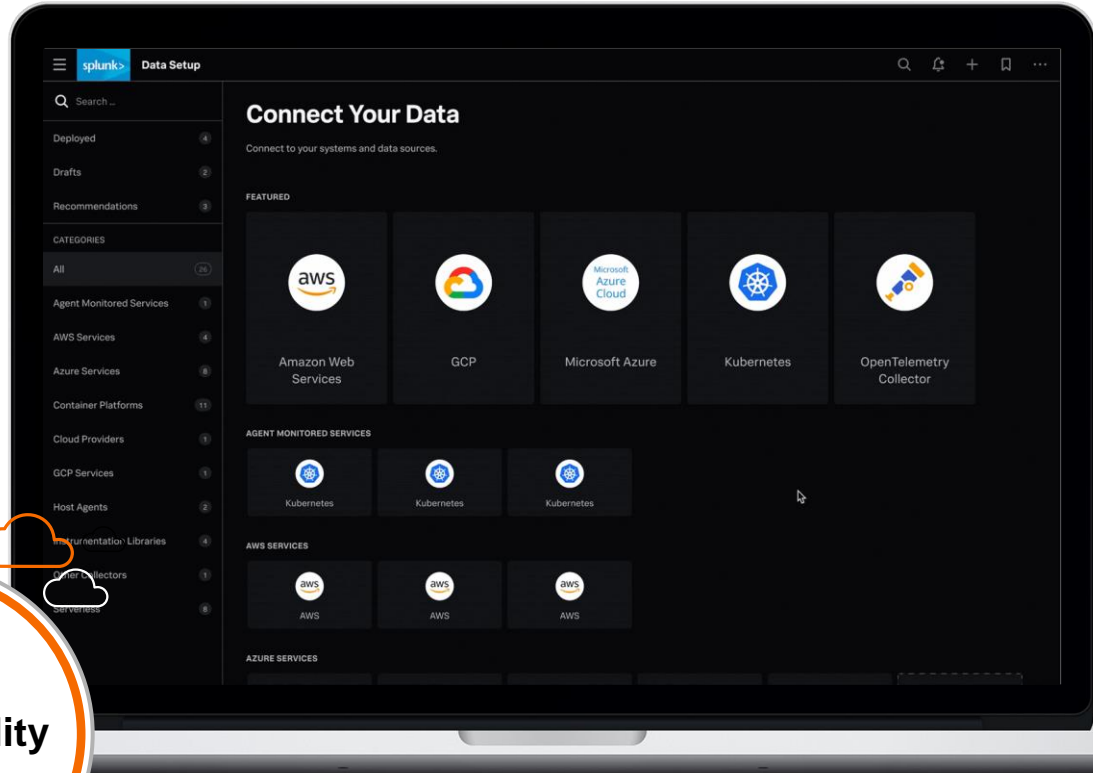
開源 Agent

Single, open standards-based agent for metrics, traces, logs and more for more control and greater ROI



Open Standards
Data Collection

Splunk
Observability
Cloud



Splunk Observability Cloud 提供上百種整合

Hundreds of out-of-the-box integrations with tech that customers use every day

Client Libraries

Function Wrappers Lambda Extension

OTel Collector

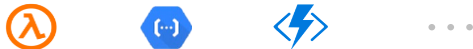
- for Linux
- for Windows
- for Kubernetes

Cloud Integrations

Custom apps and services 客製化程式開發



Serverless 無伺服器的服務



Service mesh 服務網格



Open source 開源平台



Database 資料庫



K8s / containers 容器



Hosts 主機

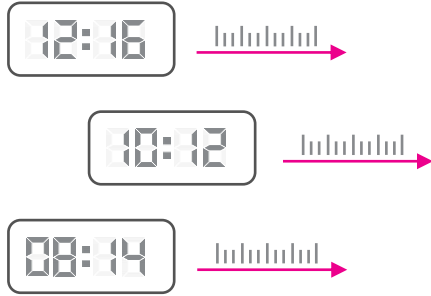


Public and private cloud 公有雲 / 私有雲

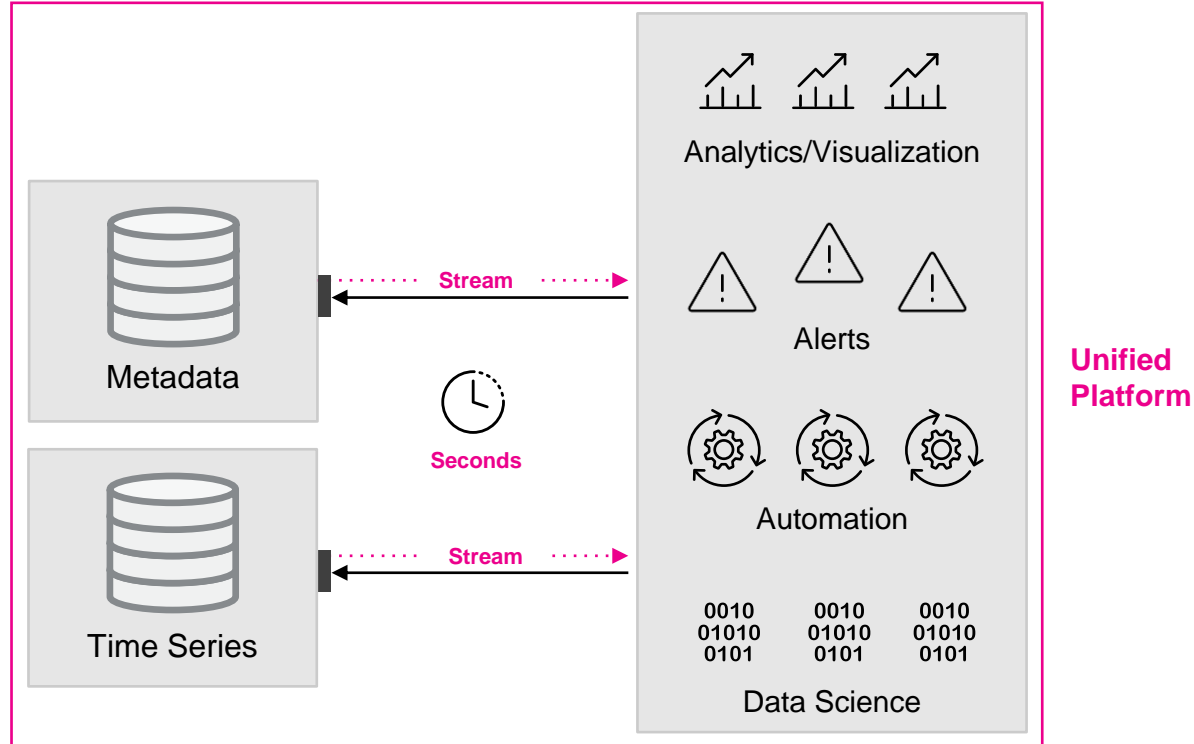


Observability Cloud 即時收集資料架構 : Streaming Metrics Architecture Provides Insights in Seconds

Metrics



- Two separate DBs for high scalability
- Streaming system for instant visibility
- Unified platform for a single source of truth



Splunk 提供 Full-Stack End-to-End 完整套件

Seamlessly integrated
UX, context and
workflows

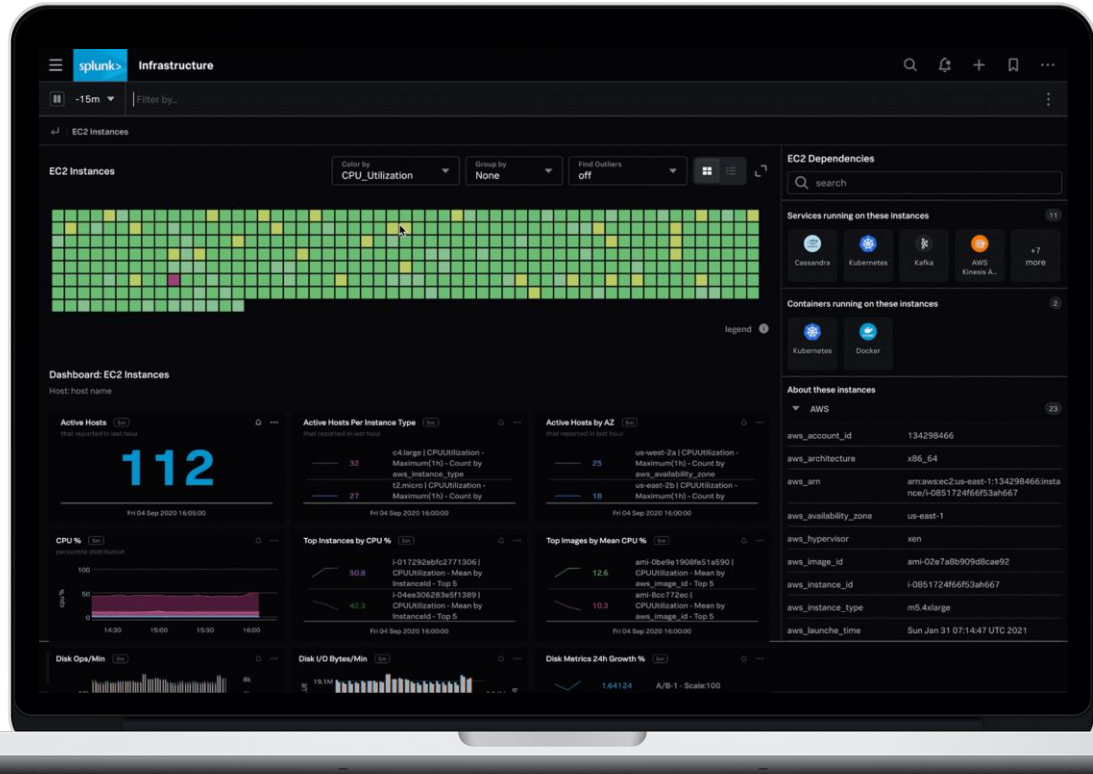


Splunk Infrastructure Monitoring

基礎建設監控

Real-time streaming metrics platform

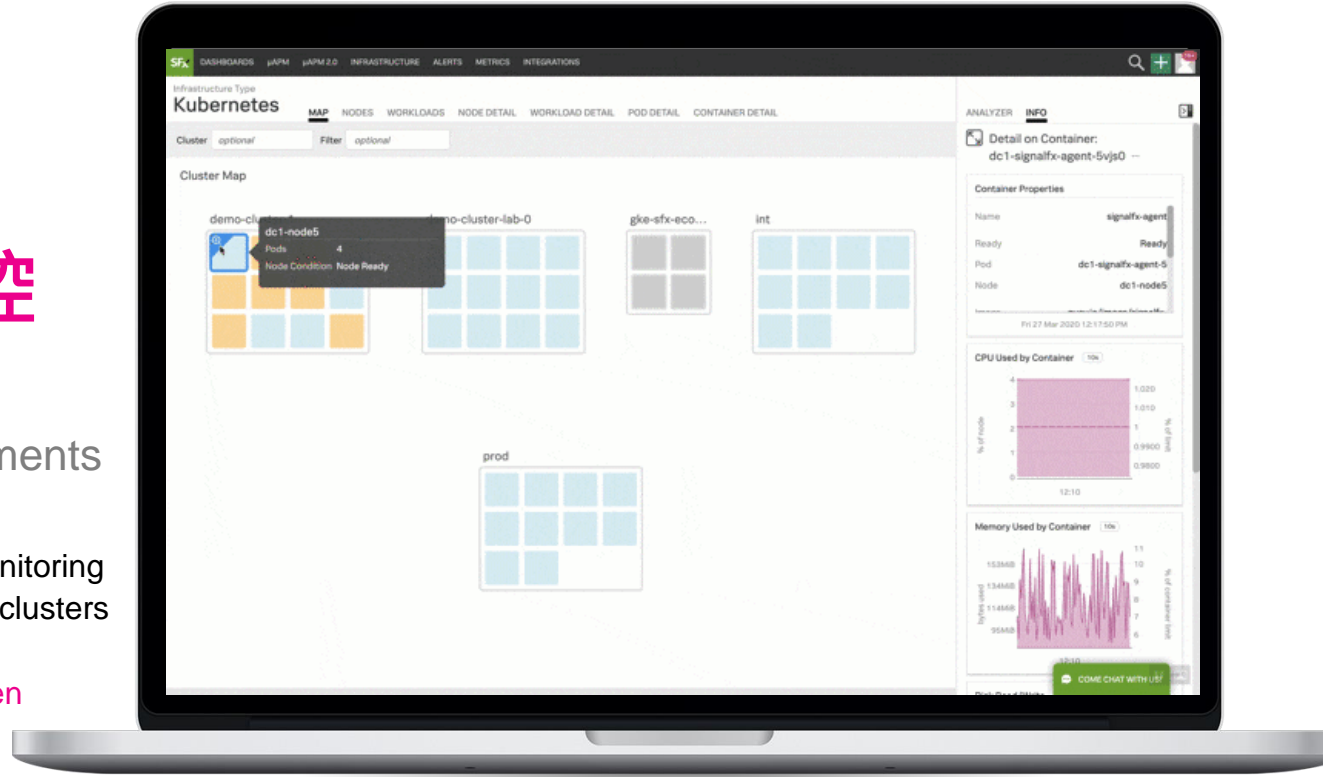
- On-prem, hybrid/ multicloud monitoring
 - Linux
 - Windows
 - VMware
 - Public clouds: AWS, Google Cloud, Azure
- Kubernetes and containers monitoring
- Serverless Monitoring
- Automatic service discovery
- Analytics-driven accurate alerting
- Over 200+ pre-built integrations for immediate visibility & monitoring



Splunk Kubernetes Navigator K8S 即時監控

Real-time observability
for containerized deployments

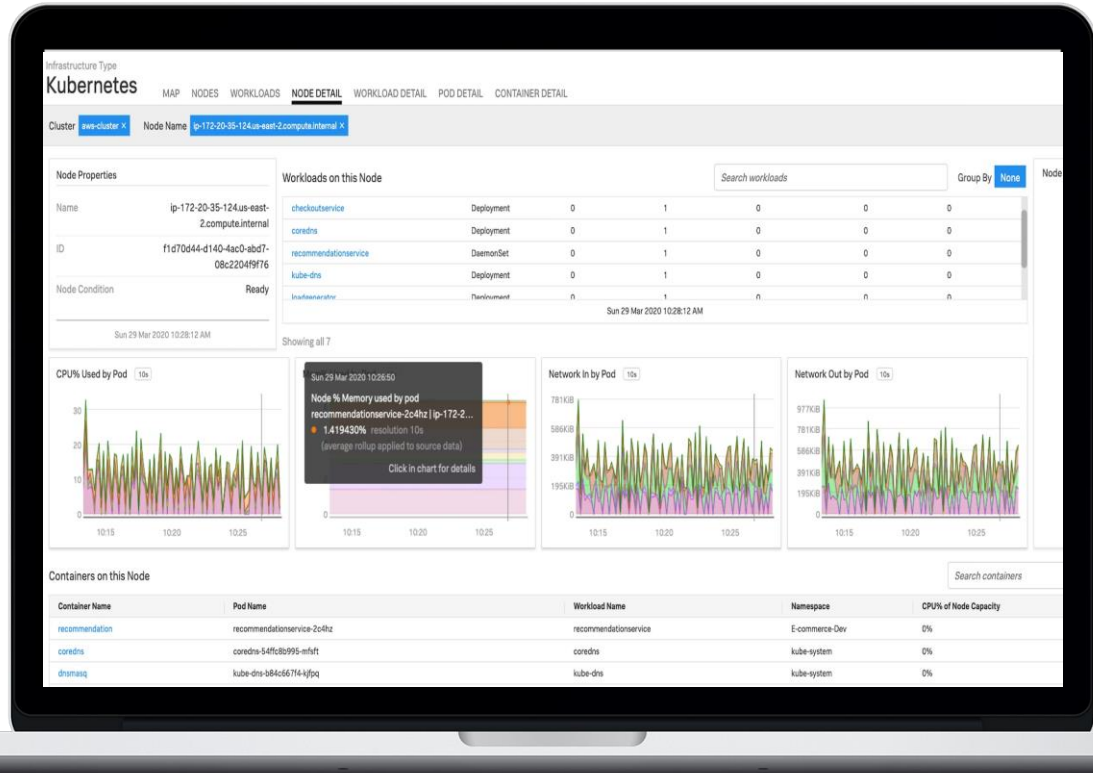
- Fully Automated Kubernetes Monitoring
- At-a-glance visibility into all K8s clusters
- Drill Downs within seconds
- Kubernetes Analyzer for AI-driven troubleshooting
- Splunk Cloud logs in context



Splunk Kubernetes Navigator K8S 即時監控

Real-time observability
for containerized deployments

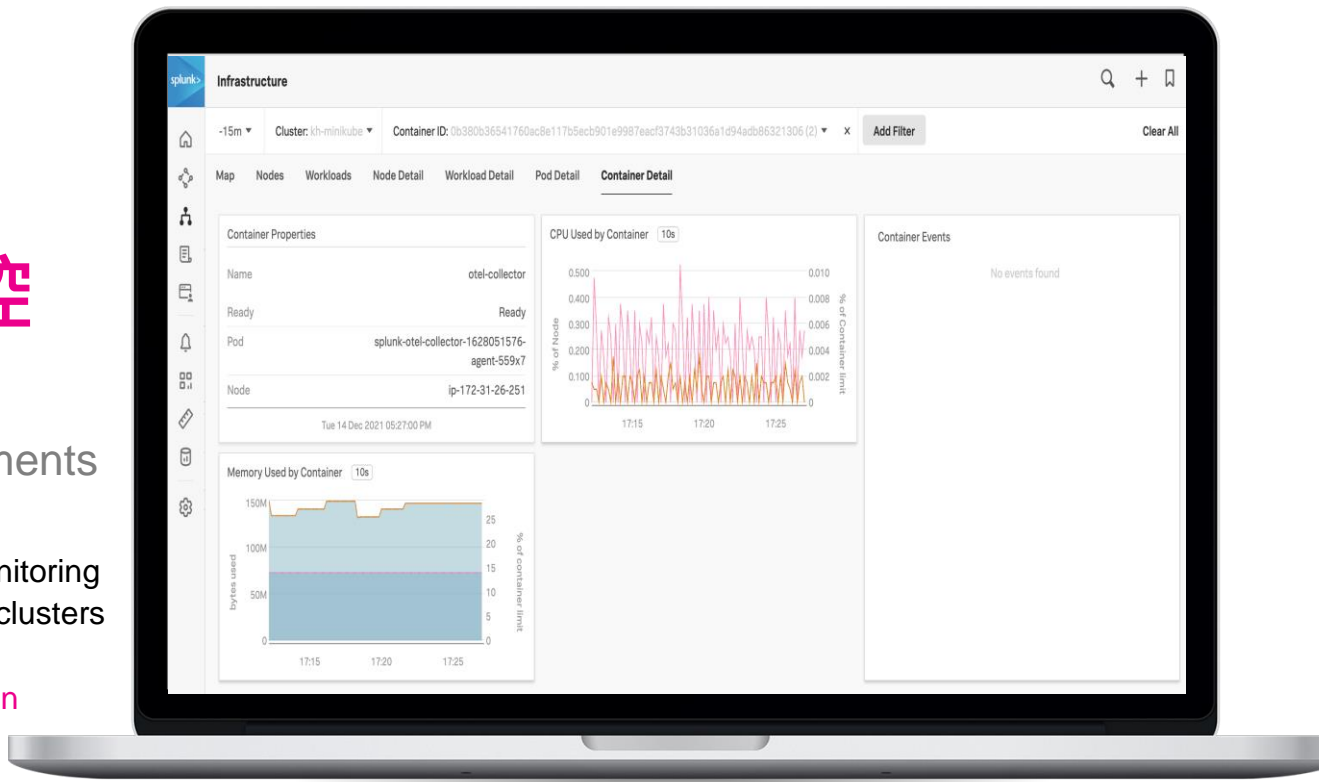
- Fully Automated Kubernetes Monitoring
- At-a-glance visibility into all K8s clusters
- Drill Downs within seconds
- Kubernetes Analyzer for AI-driven troubleshooting
- Splunk Cloud logs in context



Splunk Kubernetes Navigator K8S 即時監控

Real-time observability
for containerized deployments

- Fully Automated Kubernetes Monitoring
- At-a-glance visibility into all K8s clusters
- Drill Downs within seconds
- Kubernetes Analyzer for AI-driven troubleshooting
- Splunk Cloud logs in context

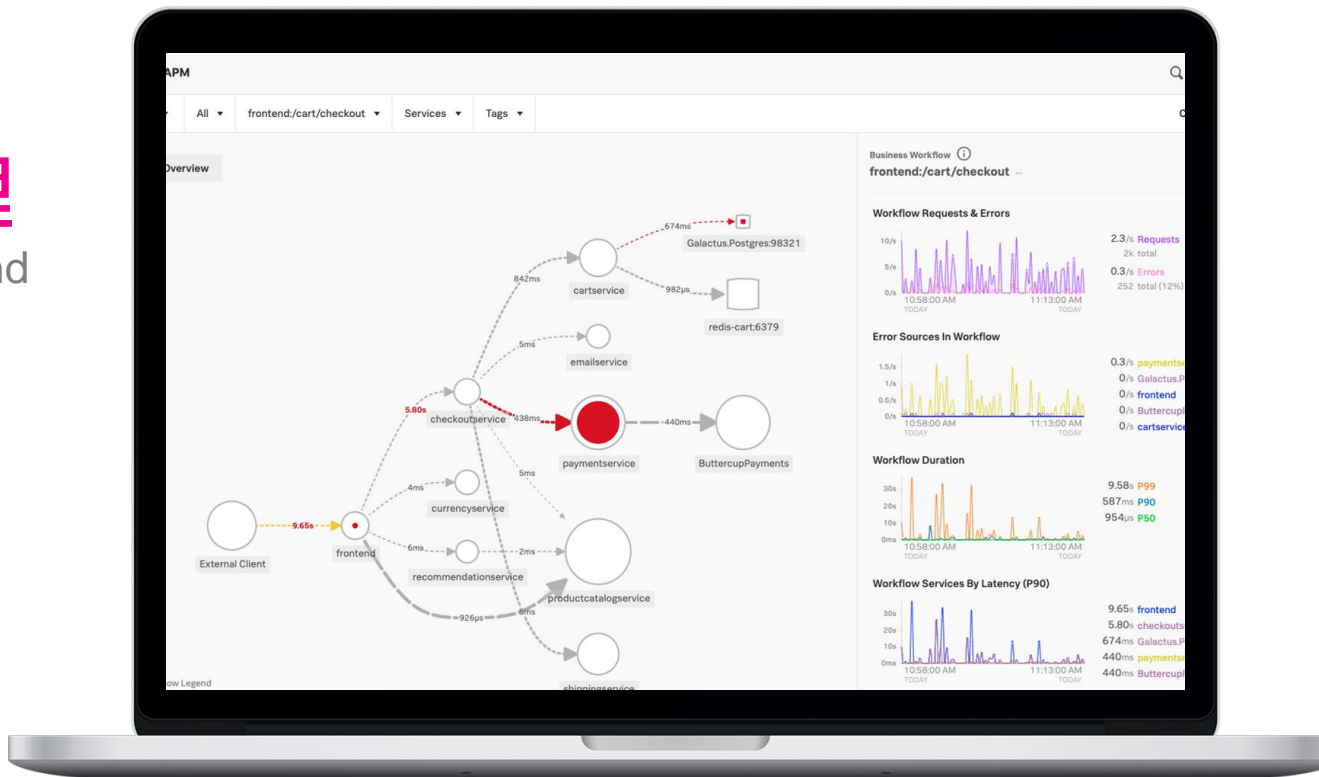


應用程式管理

Application Monitoring and Troubleshooting



- Lightweight, open instrumentation
- Rich, dynamic service map
- Full-stack correlation
- NoSample™ full-fidelity ingestion
- Unlimited cardinality exploration-search across any tag or dimension (UserName, TransactionID, Geography, etc.)
- Speedy UI, analytics & drilldowns
- AI-driven alerting and directed troubleshooting

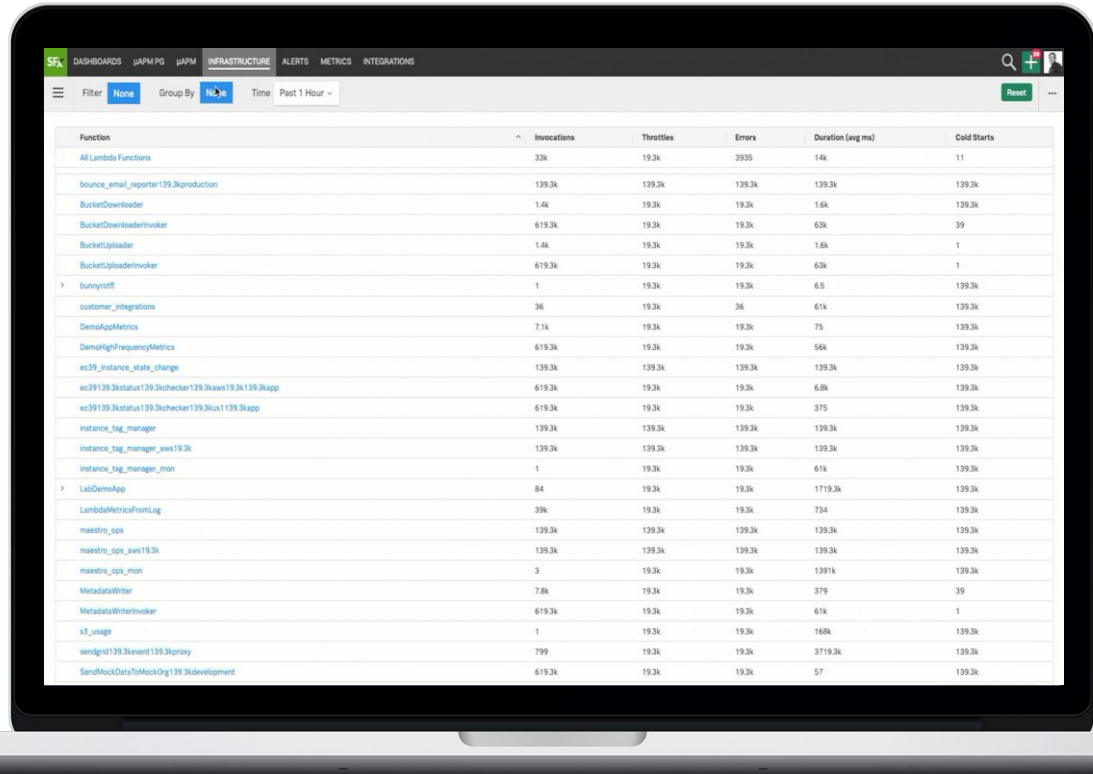


Serverless Monitoring

無伺服器服務 監控

AWS Lambda, Google Cloud Functions, and Azure Functions

- Any Language, Any Runtime for AWS Lambda using Splunk Extension without the need for instrumentation
- Deep insights into performance and cost
- Key business performance metrics in real-time with function wrappers

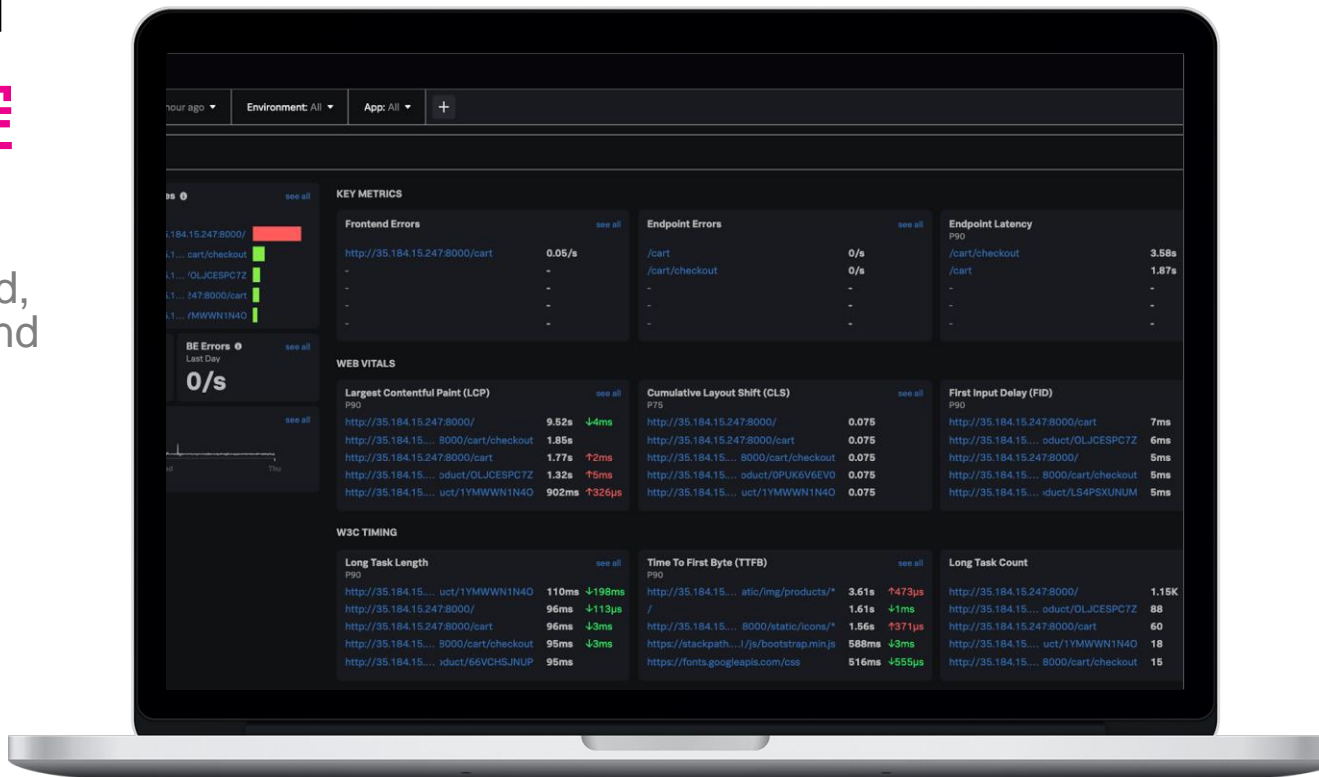


Splunk RUM

真實用戶監控

Industry's only end-to-end, full-fidelity visibility into end user experiences

- Track and monitor continuously for performance
- Elevate quality end-user experiences in real time
- Simplify troubleshooting for faster resolution
- Unlock user data through open standards
- Built for Observability, with flexibility and choice
- v1 Browser-only. Native-mobile support on roadmap

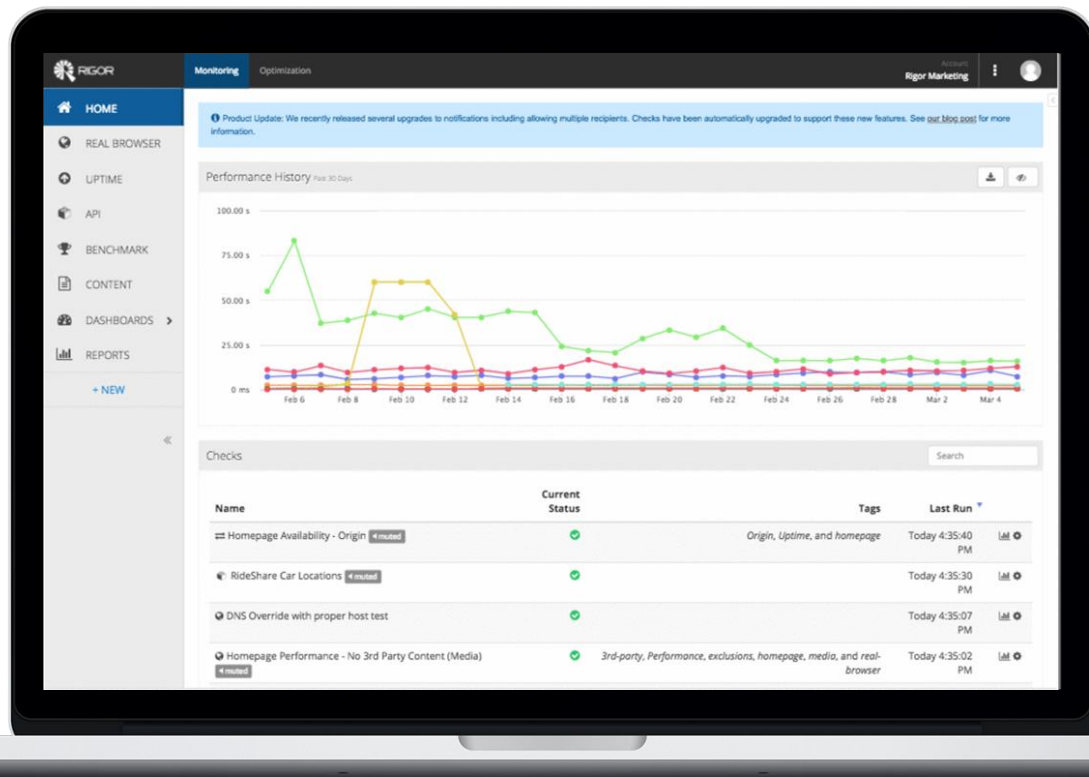


Splunk Synthetic Monitoring

網站綜合壓測

The leading fully featured synthetic monitoring solution for application transactions

- Record and test user journeys in minutes
- Proactively reduce performance regression
- Emulate real-world service dependencies
- Robust, tightly integrated real-time notification
- Low touch performance baselining

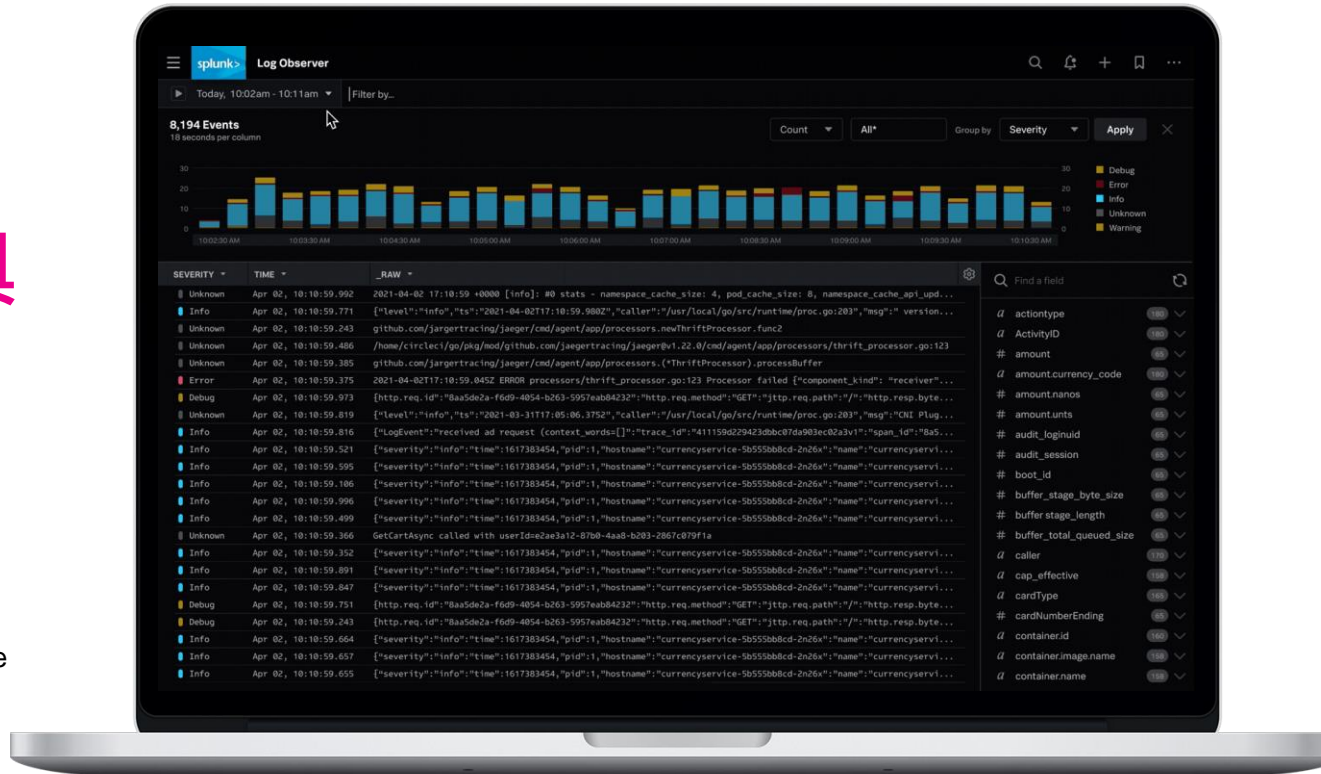


Splunk Log Observer

日誌調査工具

Log Investigation for DevOps & Security

- Fast start + fast troubleshooting
- Graphical Log Exploration without the need for a query language
- “Live Tail” - Real time log insights optimized for debugging
- Infinite Logging - Ingest all the data, index the most valuable data
- Security & Audit Use cases

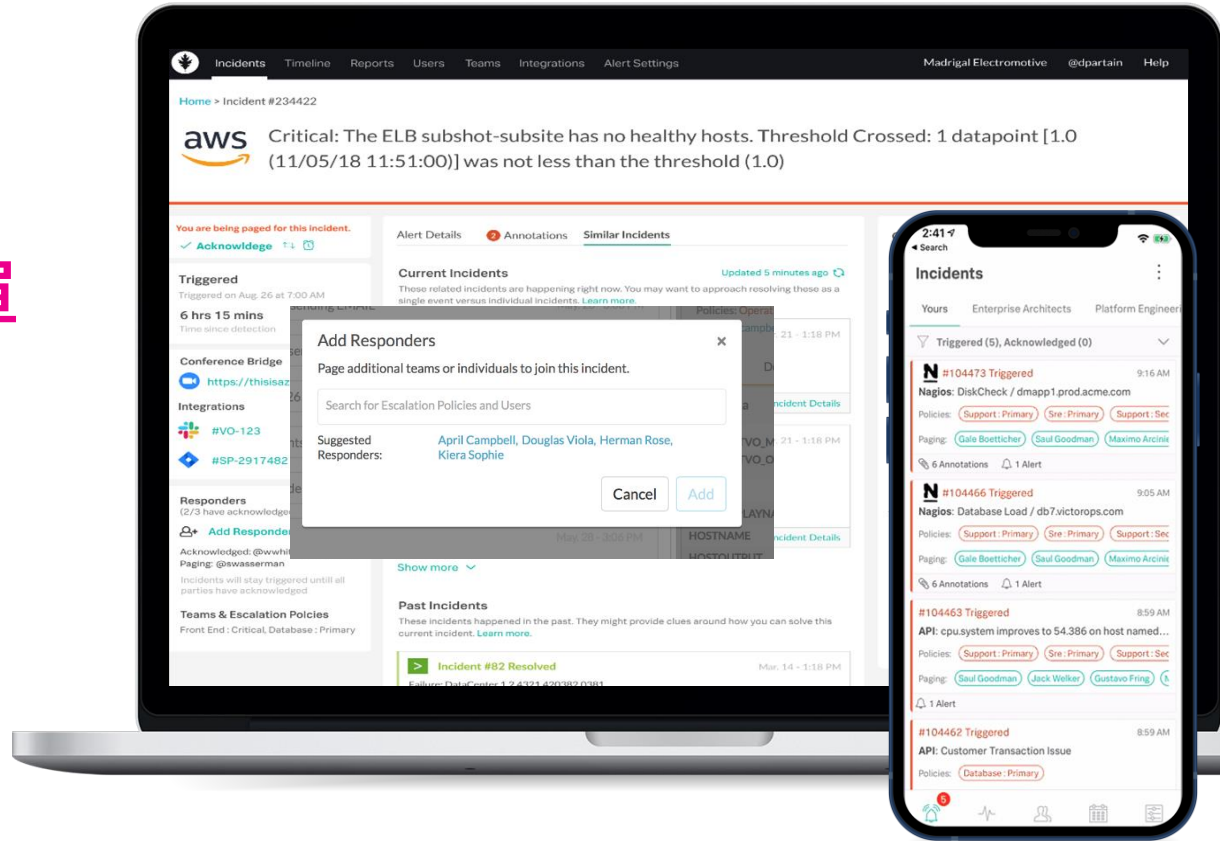


Splunk On-Call

事件協同接單

Collaborative Incident Response

- Intelligent on-call
- Post-incident analysis and reporting
- Mobile-first



實機展示

splunk> turn data into doing™

實機展示：以 K8S 基礎、微服務 開發的購物網站





Welcome to Splunk Observability Cloud

APM

Discover application dependencies, isolate issues and optimize performance with automatically generated service maps, multi-dimensional tag analysis, and full-fidelity trace search.

RUM

Analyze front end performance, javascript errors and user behavior. Isolate problems with end-to-end views that connect front end traces with corresponding back end traces from APM.

Infrastructure

See patterns, trends and anomalies for your infrastructure in aggregate views, or drill into the health, performance and capacity of individual hosts, containers, databases and more in real-time.

Alerts

Set up alerts to detect outliers or anomalies in seconds, and get notified through your favorite incident response or chat tools.

Log Observer

Investigate issues with point-and-click querying. Correlate logs with infrastructure and application metrics and traces for fast, in-context troubleshooting.

Dashboards

Dashboards provide useful insights into your systems and services. Enrich and customize them to better suit your environment.

About this Suite

Splunk Observability Cloud brings together our best-in-class solutions: Splunk Infrastructure Monitoring, Splunk APM, Splunk RUM, Splunk Log Observer into a single, tightly integrated suite of products.

It delivers a consistent user experience that combines metrics, traces, and logs giving IT and development teams a simple and seamless workflow across monitoring, troubleshooting, investigation, and response. It's the industry's only suite that offers full-stack, end-to-end observability across any environment and the entire spectrum of application architectures.

Support

Documentation

Learn more about the Observability Cloud with step by step tutorials on how to get the most out of your account. [View Documentation](#)

Support

Need additional help? Reach out to our support team with any questions. Reach out to support at: observability-support@splunk.com.

-3h

Public Clouds

 Amazon Web Services Google Cloud Platform Microsoft Azure

Containers

 Kubernetes

My Data Center

 My Data Center

Amazon Web Services (11 services)

(Data resolution is 5 minutes.)

CloudFront Distributions

13

Active Distributions

DynamoDB

No Data Found

This can occur if an integration
has been recently disabled.

[Go to Data Setup](#)

EBS

8,960

Running Volumes

EC2

4,669

Running Instances

ECS

1

Running Clusters

Elastic Load Balancers

23

Active Load Balancers

ElastiCache

157

Running Nodes

Lambda Functions

46

Active Functions

RDS

28

Running Databases

SNS Topics

1

Active Topics

SQS Queues

47

Active Queues

Google Cloud Platform (8 services)

(Data resolution is 1 minute.)

App Engine

Cloud Bigtable

Cloud Functions

Cloud Spanner

-15m ▾

Cluster: - ▾ ×

Add Filter

Clear All

Map

Nodes

Workloads

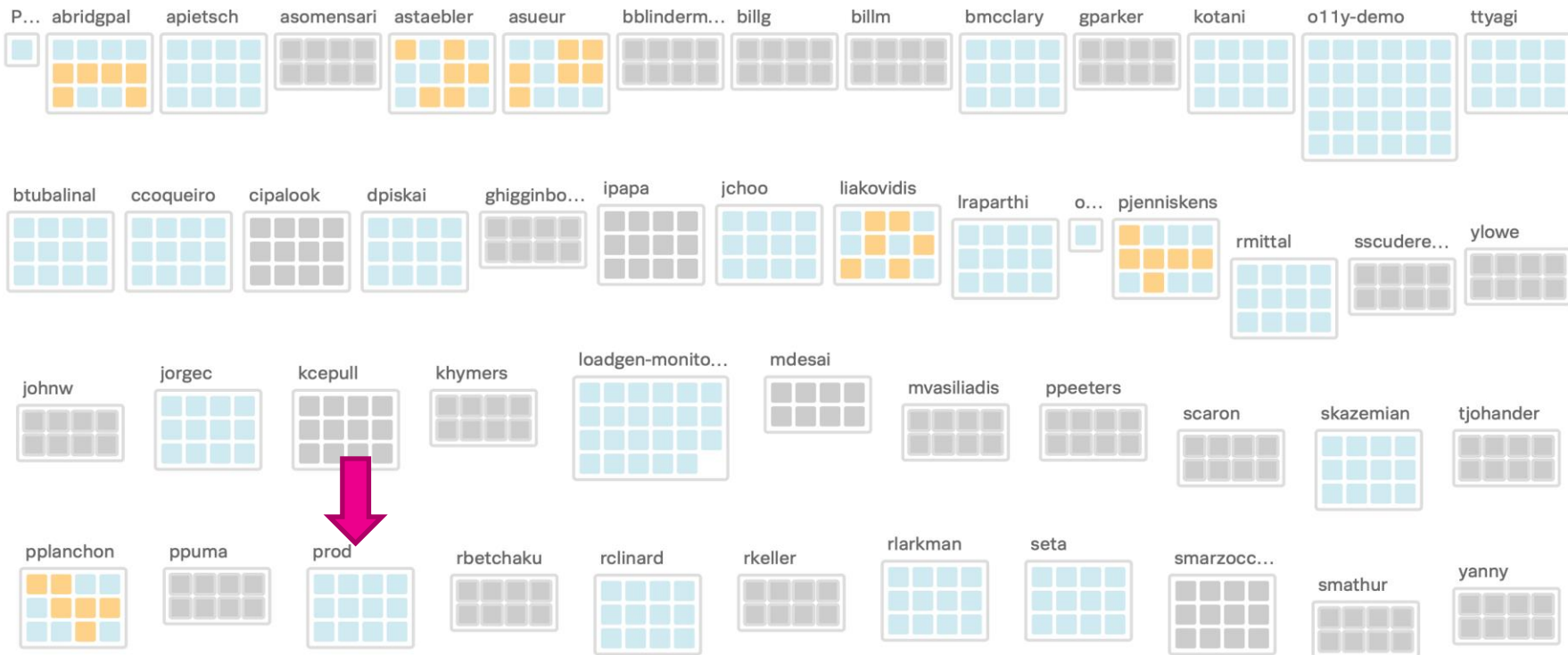
Node Detail

Workload Detail

Pod Detail

Container Detail

Cluster Map





-15m ▾

Cluster: **prod** ▾Node Name: **prodnode1** ▾ ×Pod Name: **prodcatalog-1 (4)** ▾ ×

Add Filter

Clear All

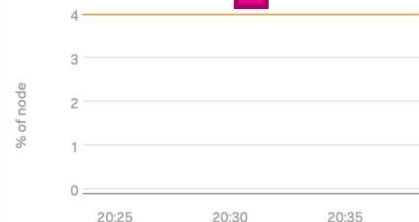
Map Nodes Workloads Node Detail Workload Detail **Pod Detail** Container Detail

Pod Properties

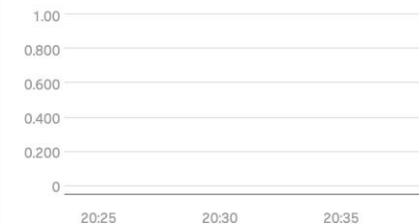
Name	prodsignalfx-agent-1
Pod ID	prodsignalfx-agent-1
Pod age	Unknown
Pod phase	Running
Node	prodnode1
Workload Type	DaemonSet
Workload	-
Namespace	sfxagent

Sun 19 Dec 2021 08:38:30 PM

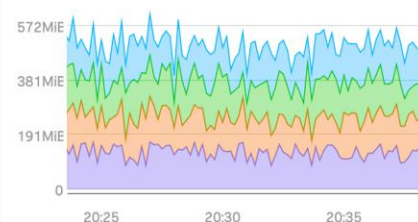
CPU% of Node Used/Container



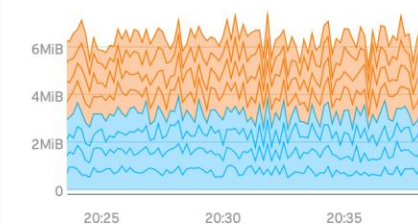
Pod Network Errors



Memory Used by Container



Pod Network Throughput



Pod Events

No events found

Containers in this Pod

Search containers

Group By **None**

Container	Pod Name	CPU % of Limit	CPU % of Node	Memory % of Limit	Memory Used (Bytes)
catalog	prodcatalog-1	10%	4%	10%	108MiB
checkout	prodcheckout-1	10%	4%	5.4%	112MiB
signalfx-agent	prodsignalfx-agent-1	10%	4%	8.9%	136MiB
tiller-deploy	prodtiller-deploy-1	10%	4%	9.8%	102MiB

Sun 19 Dec 2021 08:38:30 PM

-15m ▾

Cluster: **prod** ▾

Container ID: **prodpayment-71r23g (2)** ▾ ×

Add Filter

Clear All

Map Nodes Workloads Node Detail Workload Detail Pod Detail **Container Detail**

Container Properties

Name	payment
Ready	Ready
Pod	prodpayment-7
Node	prodnod7

Sun 19 Dec 2021 08:40:30 PM

CPU Used by Container

10s

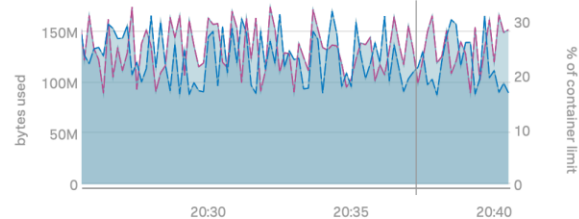


Container Events

No events found

Memory Used by Container

10s



-3h

Public Clouds

 Amazon Web Services Google Cloud Platform Microsoft Azure

Containers

 Kubernetes

My Data Center

 My Data Center

Amazon Web Services (11 services)

(Data resolution is 5 minutes.)

CloudFront Distributions

13

Active Distributions

DynamoDB

No Data Found

This can occur if an integration
has been recently disabled.

[Go to Data Setup](#)

EBS

8,960

Running Volumes

EC2

4,669

Running Instances

ECS

1

Running Clusters

Elastic Load Balancers

23

Active Load Balancers

ElastiCache

157

Running Nodes

Lambda Functions

46

Active Functions

RDS

28

Running Databases

SNS Topics

1

Active Topics

SQS Queues

47

Active Queues

Google Cloud Platform (8 services)

(Data resolution is 1 minute.)

App Engine

Cloud Bigtable

Cloud Functions

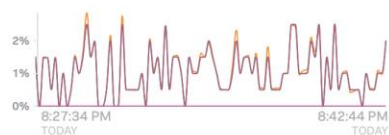
Cloud Spanner



-15m ▾ prod (1) ▾

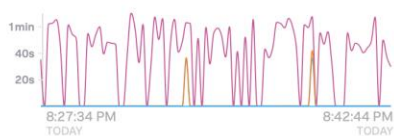
APM Overview

Top Services by Error Rate



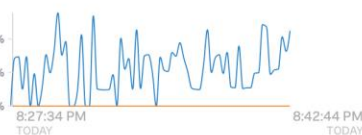
1.08% checkout
1.05% api
1.05% authorization
1.05% idp
0% order-proce...

Top Services by Latency (P90)



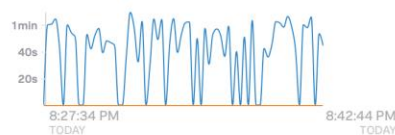
47.56s order-proce...
468ms api
295ms checkout
70ms catalog
60ms payment

Top Business Workflows by Error Rate



2.24% api/checkout
0% api/catalog

Top Business Workflows by Duration (P90)



50.05s api/checkout
122ms api/catalog

Services

Business Workflows

Sort Active alerts, then name ▾

Q Search

NAME ▾

LATENCY ▾

REQUESTS & ERRORS ▾

api/catalog



123ms p99
122ms p90
117ms p50



10.2/s Requests
9.1k total
0/s Errors

api/checkout



1.4min p99
49.65s p90
361ms p50



9.83/s Requests
8.8k total
0.22/s Errors
198 total (2%)

Explore

Explore services visually on a dependency map

Tag Spotlight

Find connections between tag values and service behaviors

Traces

View and search for traces

View Trace ID

Go

Database Query Performance

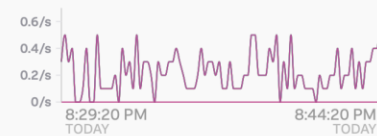
View Database Query Performance

AlwaysOn Profiling

View potential root causes

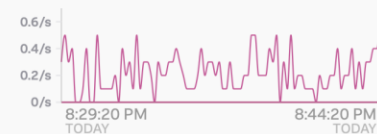


Services by Error Rate



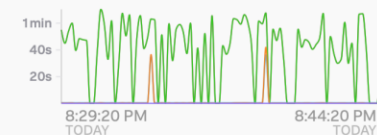
0.23/s ■ checkout
0.23/s ■ authorization
0.23/s ■ api
0.23/s ■ ldp
0/s ■ Catalog-0002

Top Error Sources



0.23/s ■ Idp
0/s ■ PwnyPostalSe...
0/s ■ PeachPay
0/s ■ ColtEmailService
0/s ■ Catalog-0002

Services By Latency (P90)



47.97s ■ order-processor
47.97s ■ mysql:mysql-p...
472ms ■ api
293ms ■ checkout
71ms ■ Catalog-0001

Traces

View Trace ID

Go

Tag Spotlight

-15m ▾

prod

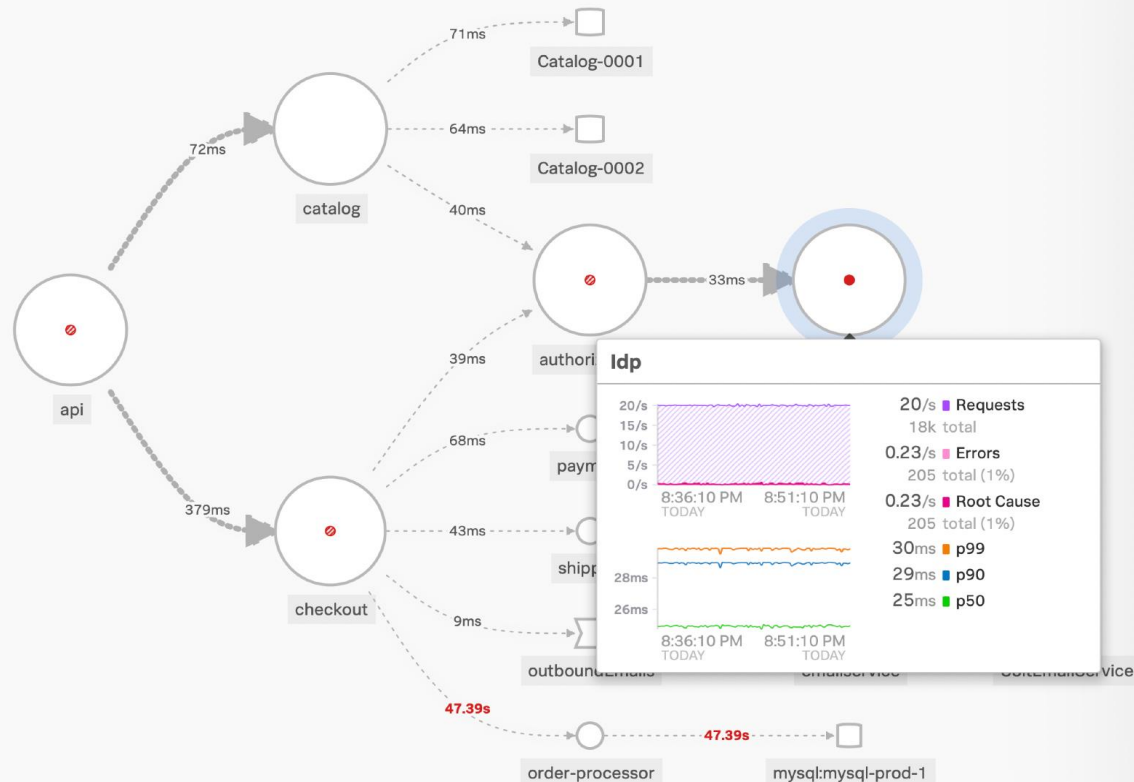
(1) ▾

All Workflows ▾

Services ▾

Tags ▾

< Overview



ldp ...

✕

Breakdown ▾

[Add to Filter](#)[View Dashboard](#)

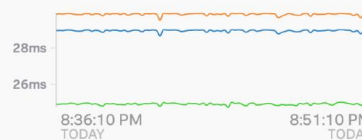
Service Requests & Errors



20/s **Requests**
18k total

0.23/s **Errors**
205 total (1%)

Service Latency



30ms **P99**
29ms **P90**
25ms **P50**

Dependencies

① → ○ ➤

Traces[Go](#)**Tag Spotlight**

Loading...

-15m prod (1) All Workflows Services Tags

Clear All

Traces

Duration (ms)

Min

Max

Errors Only

View Trace ID

Go

X

Trace ID	Start Time	Initiating Operation	Services	Duration
107b9abf84f70369	Dec 19 2021 20:38:27	frontend: GET /_healthz	frontend	36µs
10dc55423ea714fb	Dec 19 2021 20:38:53	frontend: POST /setCurrency	frontend	138µs
10e046ac759d617f	Dec 19 2021 20:38:11	frontend: GET /cart	frontend (21) productcatalogservice (10) currencyservice (5) cartservice (3) recommendationservice (2) shippingservice redis-cart:6379 Galactus.Postgres:98321	698ms
113c04d64257ce8f	Dec 19 2021 20:38:15	checkoutservice: grpc.client	checkoutservice currencyservice	4ms
115771eb624b6a199618a9caba00f69c	Dec 19 2021 20:38:09	currencyservice: grpc.hipstershop.Currency Service/Convert	currencyservice	151µs
11cc852affbd4478	Dec 19 2021 20:38:52	checkoutservice: /grpc.health.v1.Health/Check	checkoutservice	112µs
12b293240bc88c50	Dec 19 2021 20:38:42	frontend: GET /_healthz	frontend	48µs
12b444b43a2aa4cb	Dec 19 2021 20:38:05	checkoutservice: /grpc.health.v1.Health/Check	checkoutservice	109µs
12c7b3f7f00b924a	Dec 19 2021 20:38:47	shippingservice: /grpc.health.v1.Health/Check	shippingservice	98µs
12fe359a50faff3d20e934c5d369cb46	Dec 19 2021 20:38:43	currencyservice: grpc.hipstershop.Currency Service/Convert	currencyservice	195µs
0139490c22d1101c7e5190bbb63c17d5	Dec 19 2021 20:38:37	currencyservice: grpc.hipstershop.Currency Service/Convert	currencyservice	178µs
14044fd7500e04b3	Dec 19 2021 20:38:39	checkoutservice: grpc.client	checkoutservice currencyservice	2ms
158a12c4cc04fe11	Dec 19 2021 20:38:14	shippingservice: /grpc.health.v1.Health/Check	shippingservice	108µs
1608e3b03bc363c52a75468a3eb7b8fa	Dec 19 2021 20:38:11	recommendationservice: /grpc.health.v1.Health/Check	recommendationservice	132µs
1716495877c9d727	Dec 19 2021 20:38:56	shippingservice: /grpc.health.v1.Health/Check	shippingservice	158µs



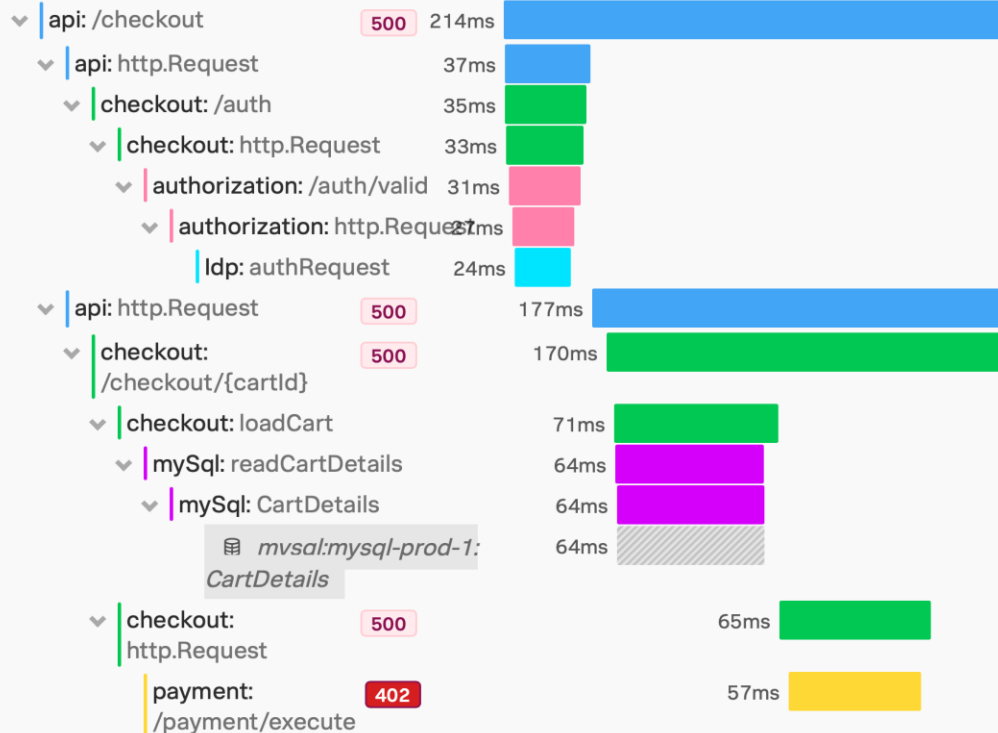
Waterfall

Span Performance



Service: Operation

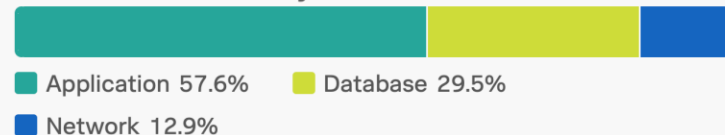
0ms 54ms 107ms 161ms 215ms

api
/checkoutToday at 8:38:08 PM
19 minutes ago

Trace ID 1bf3f7b7864bc893 ...

Download Trace

Performance Summary



Global Tags

Workflow Name
api:/checkout ...



Waterfall

Span Performance

Service	Operation	Workload % ▾
mySql	CartDetails ■	29.5% <div></div>
payment	/payment/execute ■	26.5% <div></div>
checkout	/checkout/{cartId} ■	15.9% <div></div>
Idp	authRequest ■	11.3% <div></div>
checkout	http.Request ■	5.0% <div></div>
api	http.Request ■	3.7% <div></div>
checkout	loadCart ■	3.2% <div></div>
authorization	/auth/valid ■	2.0% <div></div>
authorization	http.Request ■	1.1% <div></div>
checkout	/auth ■	0.9% <div></div>
api	/checkout ■	0.6% <div></div>
mySql	readCartDetails ■	0.3% <div></div>

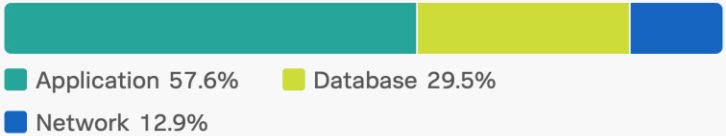
api
/checkout

Today at 8:38:08 PM
19 minutes ago

Trace ID 1bf3f7b7864bc893 ...

⌚ Download Trace

Performance Summary



Global Tags

Workflow Name
api:/checkout ...

-15m ▾

prod

(1) ▾

All Workflows ▾

Services ▾

Tags ▾

Clear All



Database Query Performance

Database:

mysql:mysql-prod-1 ▾



Top Queries

Compare to:

-1h ▾

Sort:

Total Time ▾

QUERY	TOTAL TIME	P90	TOTAL REQ	REQ/S
<code>select "business_profiles"."id", "business_profiles"."business_id", "business_profiles"."created_at",</code>	16.67min 8.33min 	20.2h ■ Total Time +1.66% 19.9h ■ History	1.4min 1.1k	1.23/s
<code>select ? as one from "fields" where "fields"."business_profile_id" = ? and "fields"."name" = ? and "fields"."value"</code>	1s 500ms 	1.2min ■ Total Time -0.36% 1.2min ■ History	85ms 1.1k	1.26/s
<code>insert into views (cta_id, user_agent) values (?)</code>	1.5s 1s 500ms 	1.2min ■ Total Time -0.75% 1.2min ■ History	85ms 1.1k	1.25/s
<code>insert into "fields" ("name", "value", "source", "reported_at", "business_profile_id", "value_json")</code>	1s 500ms 	1.2min ■ Total Time -2.22% 1.2min ■ History	85ms 1.1k	1.24/s
<code>select "people".* from "people" where "people"."id" = ? limit ?</code>	1s 500ms 	1.2min ■ Total Time -2.52% 1.2min ■ History	85ms 1k	1.21/s
<code>select "business_aliases".* from "business_aliases" where "business_aliases"."business_profile_id"</code>	1.5s 1s 500ms 	1.2min ■ Total Time -2.01% 1.2min ■ History	85ms 1k	1.2/s

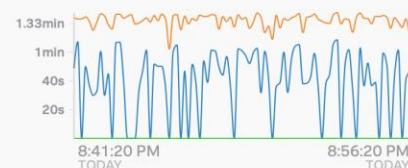
Database Overview

mysql:mysql-prod-1

Database Requests & Errors



Database Latency



Tag Spotlight: Request Latency

Endpoint

db.system

↓ P90

CartDetails

46.23s

mysql

46.23s

↓ P90

Workflow

db.name

↓ P90

api/checkout

46.23s

mysql-prod-1

46.23s

↓ P90



-15m ▾

Saved Queries ▾

Add Filter



No active search-time rules



835,287 Events

30 seconds per column

COUNT ▾

All (*)

Group by

severity

(1) ▾

Apply

Reset

50K

25K

2021 8:48 PM 8:49 PM 8:50 PM 8:51 PM 8:52 PM 8:53 PM 8:54 PM 8:55 PM 8:56 PM 8:57 PM 8:58 PM 8:59 PM 9:00 PM 9:01 PM

DEBUG
ERROR
INFO
UNKNOWN
WARNING

Logs table



Severity ▾

Time ▾

_raw ▾

13.3K new events

INFO	Dec 19 21:01:14.491	{"severity":"info","time":1639918866,"pid":1,"hostname":"currencyservice-688c9ffcdd-qq9l8","name":"currencyservice-ser
DEBUG	Dec 19 21:01:14.336	{"http.req.id":"eb2135c6-30b6-40b5-b3e7-72bc07995862","http.req.method":"GET","http.req.path":"/","http.resp.bytes":16
INFO	Dec 19 21:01:14.328	{"instant":{"epochSecond":1639918865,"nanoOfSecond":932000000},"thread":"grpc-default-executor-1488","level":"INFO","l
INFO	Dec 19 21:01:14.311	{"severity":"info","time":1639918866,"pid":1,"hostname":"currencyservice-688c9ffcdd-25dfl","name":"currencyservice-ser
INFO	Dec 19 21:01:14.311	{"severity":"info","time":1639918866,"pid":1,"hostname":"currencyservice-688c9ffcdd-25dfl","name":"currencyservice-ser
INFO	Dec 19 21:01:14.304	{"severity":"info","time":1639918866,"pid":1,"hostname":"currencyservice-688c9ffcdd-25dfl","name":"currencyservice-ser
INFO	Dec 19 21:01:14.303	{"severity":"info","time":1639918866,"pid":1,"hostname":"currencyservice-688c9ffcdd-25dfl","name":"currencyservice-ser
INFO	Dec 19 21:01:14.297	{"severity":"info","time":1639918866,"pid":1,"hostname":"currencyservice-688c9ffcdd-25dfl","name":"currencyservice-ser
INFO	Dec 19 21:01:14.296	{"severity":"info","time":1639918866,"pid":1,"hostname":"currencyservice-688c9ffcdd-25dfl","name":"currencyservice-ser
INFO	Dec 19 21:01:14.289	{"severity":"info","time":1639918866,"pid":1,"hostname":"currencyservice-688c9ffcdd-25dfl","name":"currencyservice-ser
INFO	Dec 19 21:01:14.288	{"severity":"info","time":1639918866,"pid":1,"hostname":"currencyservice-688c9ffcdd-25dfl","name":"currencyservice-ser
INFO	Dec 19 21:01:14.281	{"severity":"info","time":1639918866,"pid":1,"hostname":"currencyservice-688c9ffcdd-25dfl","name":"currencyservice-ser
INFO	Dec 19 21:01:14.281	{"severity":"info","time":1639918866,"pid":1,"hostname":"currencyservice-688c9ffcdd-25dfl","name":"currencyservice-ser
INFO	Dec 19 21:01:14.273	{"severity":"info","time":1639918866,"pid":1,"hostname":"currencyservice-688c9ffcdd-25dfl","name":"currencyservice-ser

Fields



🔍 Find field

a	ad_context_words_all	2.92K	▾
a	amount.currency_code	584	▾
#	amount.nanos	584	▾
#	amount.units	584	▾
a	api_token	1.38K	▾
a	app	5	▾
#	audit_loginuid	2	▾
#	audit_session	2	▾
a	boot_id	3	▾
#	buffer_available_buffer_sp...	82	▾
#	buffer_queue_byte_size	82	▾
#	buffer_queue_length	82	▾
#	buffer_stage_byte_size	82	▾
#	buffer_stage_length	82	▾
#	buffer_total_queued_size	82	▾
a	cap_effective	2	▾



-15m ▾

SL - Payment errors ▾

Add Filter

severity = ERROR x

service.name = paymentservice x

deployment.environment = yli2-shop x

No active search-time rules

65 Events

30 seconds per cc

10

5

2021

Enter names and tags to filter for a saved query.

CrashLoopBackoff

kubernetes

Apply

Crash loop backoff errors

Reason = CrashLoopBackOff

keyword = *containerStatuses*

ImagePullErrors

kubernetes

Apply

Filter for image pulls

Reason = ErrImagePull

Reason = ImagePullBackOff

Get Pod events

kubernetes

Apply

Kind = Pod

Get Deployment events

kubernetes

Apply

Kind = Deployment

Pod Errors

kubernetes

Apply

Kind = Pod

severity = ERROR

severity = OOMKILLED

Errors

Apply

severity = ERROR

service.name = paymentservice

deployment.environment = mgrover-shop

Logs table

Severity ▾

Time

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

ERROR Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec

Dec



Q Search...



CATEGORIES

All 161

AWS Services 25

GCP Services 12

Azure Services 13

Platforms 6

Applications 49

Metric Instrumentation 5

APM Instrumentation 7

RUM Instrumentation 1

Notification Services 11

Login Services 8

Data Link Destinations 4

Community Integrations 11

Other Integrations 4

Deprecated Components 5

AWS SERVICES



Amazon Web Services



AWS ALB



Amazon API Gateway



AWS Auto Scaling



Amazon CloudFront



Amazon CloudWatch Events

[View More](#)

GCP SERVICES



Google Cloud Platform



Google App Engine



Google Cloud BigQuery



Google Cloud BigTable



Google Compute Engine



Google Cloud Datastore

[View More](#)

AZURE SERVICES



Microsoft Azure



Azure App Service



Azure Batch



Azure Cache for Redis



Azure Event Hubs



Azure Functions

[View More](#)

PLATFORMS



Amazon ECS EC2



Amazon Fargate



Kubernetes



Linux



Windows

Splunk OpenTelemetry
Connector

APPLICATIONS



ActiveMQ



Apache



Apache Solr



Apache Spark

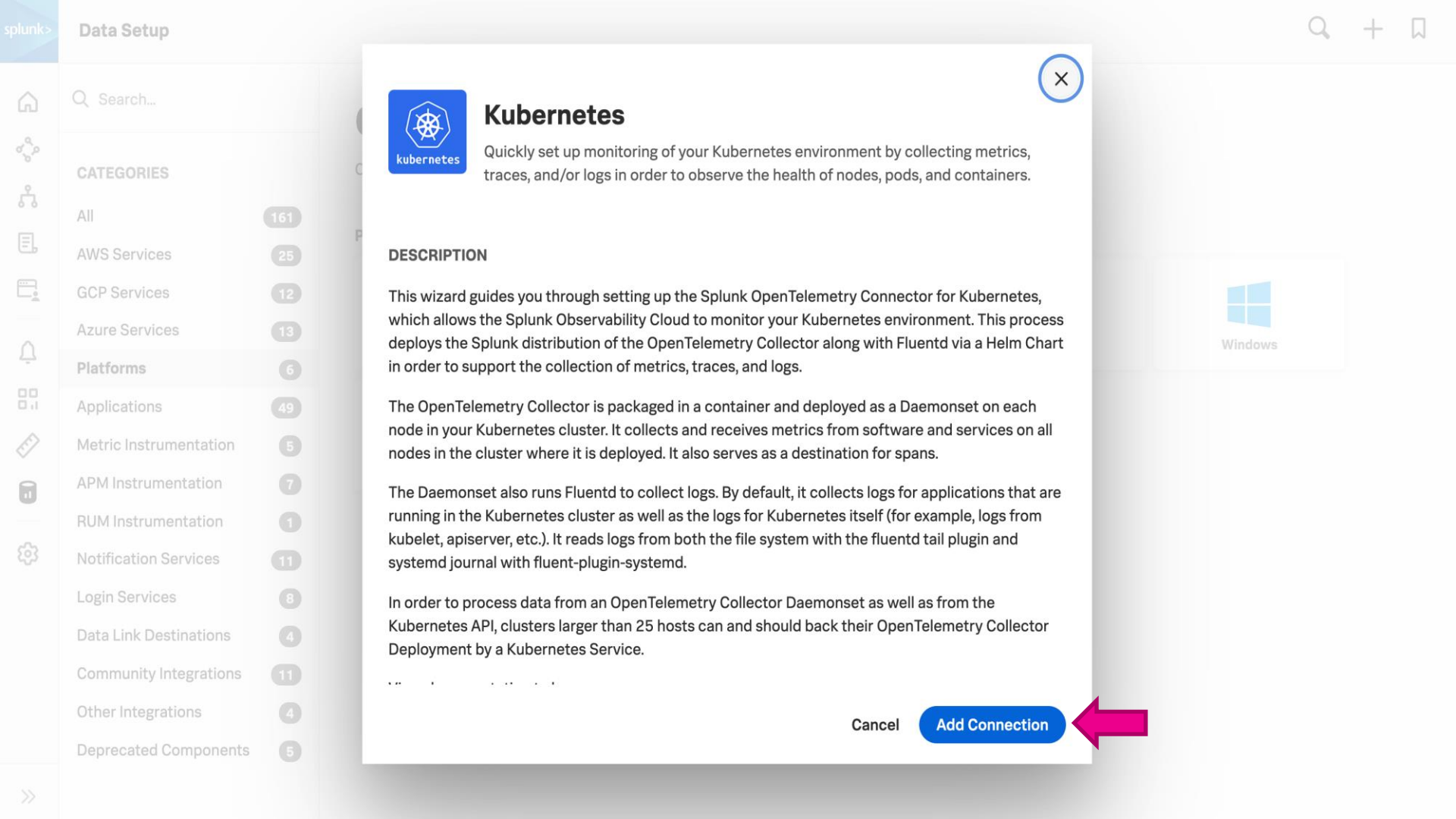


Cassandra



chrony

[View More](#)



Search...



CATEGORIES

All

161

AWS Services

25

GCP Services

12

Azure Services

13

Platforms

6

Applications

49

Metric Instrumentation

5

APM Instrumentation

7

RUM Instrumentation

1

Notification Services

11

Login Services

8

Data Link Destinations

4

Community Integrations

11

Other Integrations

4

Deprecated Components

5



Kubernetes

Quickly set up monitoring of your Kubernetes environment by collecting metrics, traces, and/or logs in order to observe the health of nodes, pods, and containers.

DESCRIPTION

This wizard guides you through setting up the Splunk OpenTelemetry Connector for Kubernetes, which allows the Splunk Observability Cloud to monitor your Kubernetes environment. This process deploys the Splunk distribution of the OpenTelemetry Collector along with Fluentd via a Helm Chart in order to support the collection of metrics, traces, and logs.

The OpenTelemetry Collector is packaged in a container and deployed as a Daemonset on each node in your Kubernetes cluster. It collects and receives metrics from software and services on all nodes in the cluster where it is deployed. It also serves as a destination for spans.

The Daemonset also runs Fluentd to collect logs. By default, it collects logs for applications that are running in the Kubernetes cluster as well as the logs for Kubernetes itself (for example, logs from kubelet, apiserver, etc.). It reads logs from both the file system with the fluentd tail plugin and systemd journal with fluent-plugin-systemd.

In order to process data from an OpenTelemetry Collector Daemonset as well as from the Kubernetes API, clusters larger than 25 hosts can and should back their OpenTelemetry Collector Deployment by a Kubernetes Service.

... ..

Cancel

Add Connection



PROGRESS

- 1 **Configure Integration**
- 2 Install Integration
- 3 Review Inventory


Configure Integration

Provide the following details.

Splunk Access Token ⓘ	<input type="text" value="profiling-demo"/>
Cluster Name ⓘ	<input type="text" value="test-GKE"/>
Provider ⓘ	<input type="text" value="Google Cloud Platform"/>
Distribution ⓘ	<input type="text" value="Google GKE / Standard mode"/>
Add Gateway ⓘ	<input type="text" value="Yes"/>
Log Collection ⓘ	<input type="text" value="True"/>

[Back](#)[Next](#)

PROGRESS

 Configure Integration 2 Install Integration 3 Review Inventory

Install Integration

Complete the following steps to deploy the tracing instrumentation to your application.

HELM (Recommended)

A Ensure that you have installed and configured the Helm 3.0 client.



B Add the Splunk OpenTelemetry Connector for Kubernetes' Helm chart repository

```
helm repo add splunk-otel-collector-chart https://signalfx.github.io/splunk-otel-collector-chart
```



C Ensure the latest state of the repository

```
helm repo update
```



D Install the Splunk OpenTelemetry Connector for Kubernetes with the desired configuration values

```
helm install --set cloudProvider='gcp' --set distribution='gke' --set splunkObservability.accessToken='2-bqpllnPEdhzW9SaJJtJA' --set clusterName='test-GKE' --set splunkObservability.realm=
```

[Back](#)[Next](#)

🔍 Search...

CATEGORIES

All 161

AWS Services 25

GCP Services 12

Azure Services 13

Platforms 6

Applications 49

Metric Instrumentation 5

APM Instrumentation 7

RUM Instrumentation 1

Notification Services 11

Login Services 8

Data Link Destinations 4

Community Integrations 11


























Other Integrations 4

Deprecated Components 5

Connect Your Data

Connect to your systems and data sources.

AWS SERVICES

 Amazon Web Services	 AWS ALB	 Amazon API Gateway	 AWS Auto Scaling	 Amazon CloudFront
 Amazon CloudWatch Events	 Amazon Dynamo DB	 Amazon EBS	 Amazon EC2	 Amazon ECS
 Amazon EKS	 Amazon ElastiCache	 AWS ELB	 Amazon Kinesis Analytics	 Amazon Kinesis Streams
 AWS Lambda	 AWS OpsWorks	 Amazon RDS	 Amazon Redshift	 Amazon Route 53
 Amazon SNS	 Amazon SQS	 AWS Optimizer	 Amazon ECS EC2	 Amazon Fargate

🔍 Search...

CATEGORIES

All 161

AWS Services 25

GCP Services 12

Azure Services 13

Platforms 6

Applications 49

Metric Instrumentation 5

APM Instrumentation 7

RUM Instrumentation 1

Notification Services 11

Login Services 8

Data Link Destinations 4

Community Integrations 11

Other Integrations 4

Deprecated Components 5

Connect Your Data

Connect to your systems and data sources.

GCP SERVICES



Google Cloud Platform



Google App Engine



Google Cloud BigQuery



Google Cloud BigTable



Google Compute Engine



Google Cloud Datastore



Google Cloud Functions



Google Kubernetes Engine



Google Cloud Pub/Sub



Google Cloud Router



Google Cloud Spanner



Google Cloud Storage



CATEGORIES

All 161

AWS Services 25

GCP Services 12

Azure Services 13

Platforms 6

Applications 49

Metric Instrumentation 5

APM Instrumentation 7

RUM Instrumentation 1

Notification Services 11

Login Services 8

Data Link Destinations 4

Community Integrations 11

Other Integrations 4

Deprecated Components 5

Connect Your Data

Connect to your systems and data sources.

AZURE SERVICES



Microsoft Azure



Azure App Service



Azure Batch



Azure Cache for Redis



Azure Event Hubs



Azure Functions



Azure Kubernetes Service



Azure Logic Apps



Azure SQL Database



Azure SQL Elastic Pools



Azure Storage



Azure VM



Azure VM Scale Sets

客戶案例分享

splunk> turn data into doing™

Splunk Observability Cloud 對客戶帶來的好處

More productive developers and happier customers

Release Quality
and Velocity
版本發佈品質、速度

8X

Higher quality and
faster code releases
for new launches and
updates

Customer
Experience
客戶滿意度

100X

Fewer missed
anomalies and end
user-impacting
incidents as well as
ability to effectively
optimize experience

System
Availability
系統可用度

80%

Faster identification,
acknowledgement
and resolution of
defects

Developer
Efficiency
開發者工作效率

70%

Reduction in
developer disruptions
from fewer incidents
and less time spent
troubleshooting
defects

Lenovo

Lenovo Offers Frictionless E-Commerce Experience With Splunk Observability



https://www.splunk.com/en_us/customers/success-stories/lenovo-with-splunk-observability.html

Key Challenges

Operating an e-commerce site often means getting unexpected web traffic and data usage spikes, so performance, stability and flexibility are top priorities, especially when cloud migration is also underway.

Key Results

With Splunk Observability Cloud, Lenovo cut troubleshooting time in half, reduced total cost of ownership and maintained 100% uptime despite a 300% increase in web traffic.

Splunk Observability Cloud 可觀察性雲服務

Seamlessly integrated
UX, context and
workflows



SYNTHETICS

INFRASTRUCTURE
MONITORING

APM

ON-CALL

LOG
OBSERVER

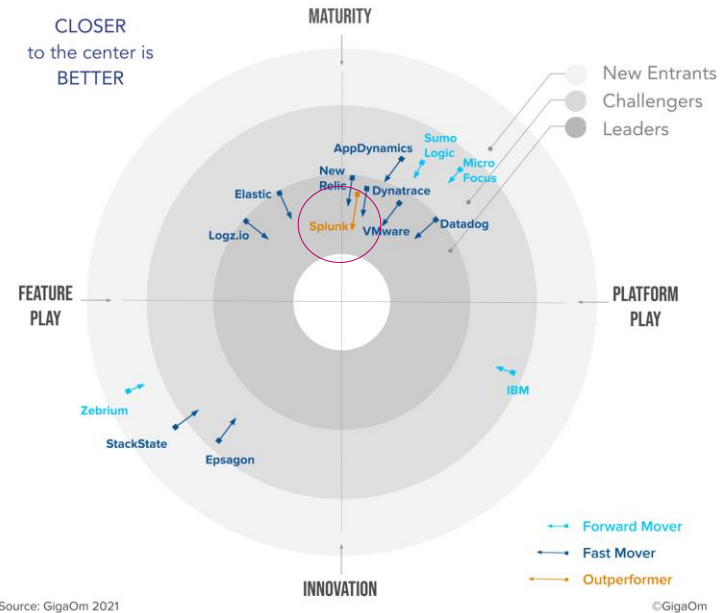
RUM

Splunk Recognized as the 研究報告分析 Market Leader in Observability 市場領導者

Top-ranked vendor and only Outperformer in GigaOm Radar for Cloud Observability

- Splunk earns **highest ranking of all vendors**, beating Datadog, New Relic & Dynatrace
- GigaOm praises Splunk Observability's **"massive scalability, sophisticated in-stream analytics and native OpenTelemetry support."**
- "Splunk, with its multiple recent acquisitions to bolster the Observability stack, is an outperformer in this space."

– Andy Thurai, Senior Analyst, GigaOm

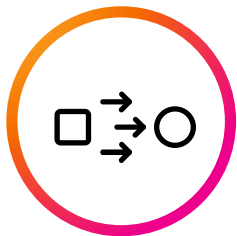


GIGAOM

Splunk Observability Cloud 五倍振興的優勢

Five attributes of an effective Observability Environment

Real-Time
即時收集



Instant analysis and insight to drive down time to respond and resolve

End-to-End Full Stack
完整套件



Unified interface and integrated workflow for monitoring, troubleshooting, investigation

Analytics Powered
分析驅動



Full-fidelity data analysis and correlating data. For fast alerts and investigations with no dead-ends

Enterprise Grade Scale
企業等級



Scale, pricing, role-based capabilities that make Splunk easy for enterprises to adopt and scale

Open Standards
開放標準



Lower cost to maintain and prevent vendor lock-in

試用 Splunk Observability Cloud 免費 **FREE** for 14 days

https://www.splunk.com/en_us/observability/o11y-cloud-free-trial.html



待會，歡迎 大家 參加：

604會議室

15:30 – 17:00

可觀察性 Observability 實戰工作坊：獲取 DevOps 實踐的基本原則

蘇禮順 | Splunk 台灣區資深售前工程師

完成的，會有『小米 洗手機』小禮物～

完成的，會有『小米 洗手機』小禮物～



splunk > turn data into doing

Thank You!

