



Logs Workshop

Log Management & Analytics at scale!

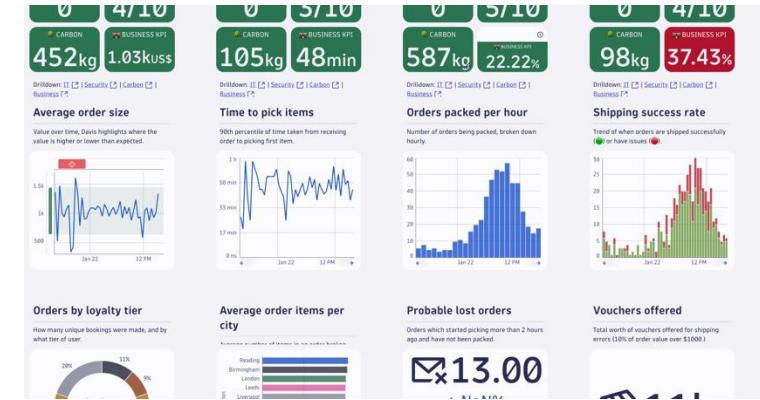
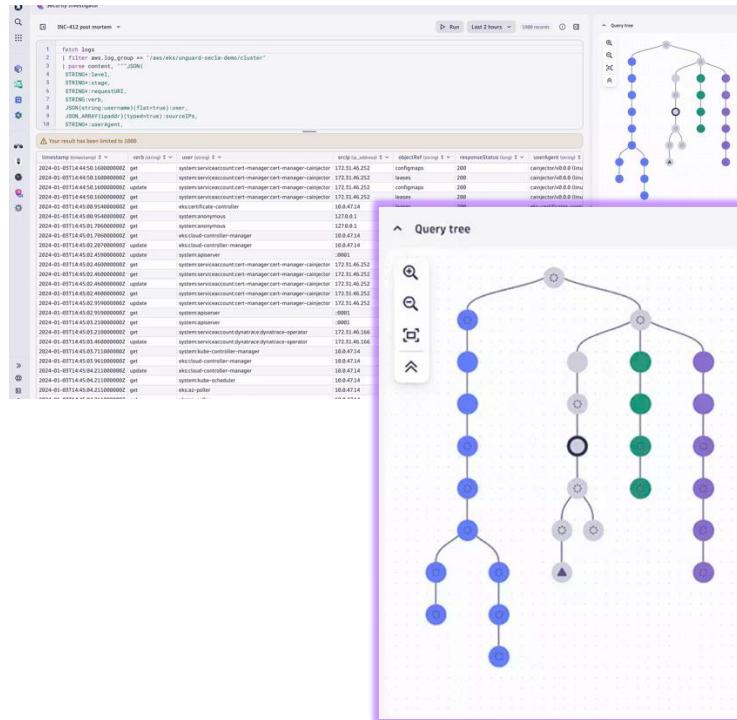
Agenda

- Log Management and Analytics in Dynatrace provides instant answers to critical questions across:
 - Business
 - DevOps
 - SRE
 - Operations
 - Security
- This technical session will cover best practices and strategies for Log Management and Analytics in Dynatrace, including scalable implementation.
- Attendees will gain knowledge on managing enterprise logging in Dynatrace and leave with actionable insights for their own implementations.

Agenda Items:

- Log Management and Analytics
- OpenPipeline
- Understanding Query behavior
- Buckets and Segments
- Permissions
- Logs to Metrics / Events
- Dashboarding
- Anomaly Detection
- Live Demo
- Hands-on Training

Logs are a key data source for Observability, Security and Business Goals



Analytics, AI, and Automation for Unified Observability and Security



dynatrace

AutomationEngine

AppEngine

Smartscape®

Davis® AI

Grail™

Hub

OpenPipeline™

PurePath®

OneAgent®



Topology



Traces



Metrics



Logs



Behavior



Code



Metadata



Network



Security Events



Threats

Discussion Question

What are necessary capabilities for a Log Management and Analytics Solution?

Ingest logs from many sources

Retain logs for selected timeframe

Permissions and Access Controls

Scalability

Filtering

Alerts from log data

Automatic parsing for standard logs

Deep dive analytics

Data security

Discussion Question

What are necessary capabilities for a Log Management and Analytics Solution?

Easily get answers from Logs!

Logs in context reduces MTTR and provides instant answers

The figure consists of three side-by-side screenshots of a cloud-based monitoring and logging interface. All three screenshots share a common header: "Failure rate increase" (Closed P-2502156), "Error Started at Feb 3, 2025, 7:06 PM for 28 min", and four summary metrics: Events (4), SLOs (3), Affected users (93), and Affected entities (3).

1. **Affected infrastructure (Left):** This section lists the "TradeManagement" service as the root cause. It shows a tree view of the infrastructure: "eks" (Kubernetes cluster) which contains "i-061c82f7d0e098b13" (Host) and multiple instances of ".NET BrokerService.dll easytrade production" (broker-service Process). A chart below shows the "Failure rate increase" over time from 07:05 PM to 07:25 PM, with values ranging from 0.002 to 0.022.

2. **Logs (Middle):** This section shows the "Logs" tab with a bar chart titled "10733 records". The x-axis represents time from 07:10 PM to 07:30 PM. The bars are colored blue for "INFO" and red for "ERROR". Below the chart is a "Recommended queries" section with two buttons: "Show the last 100 error logs" and "Show logs in current context".

3. **Requests (Right):** This section shows the "Requests" tab for the "/cart/checkout" endpoint. It displays a table of 10 records with columns: Start time, Endpoint, Service, Response time, Request type, and Span source. The table includes rows for various API calls like "Charge", "Convert", "GetQuote", and "POST". A specific trace ID "962fd7e6f1a402794d28824f24589718" is highlighted. Below the table is a detailed view of the trace, showing a duration of 5.11 s and a response time of 5.11 s.

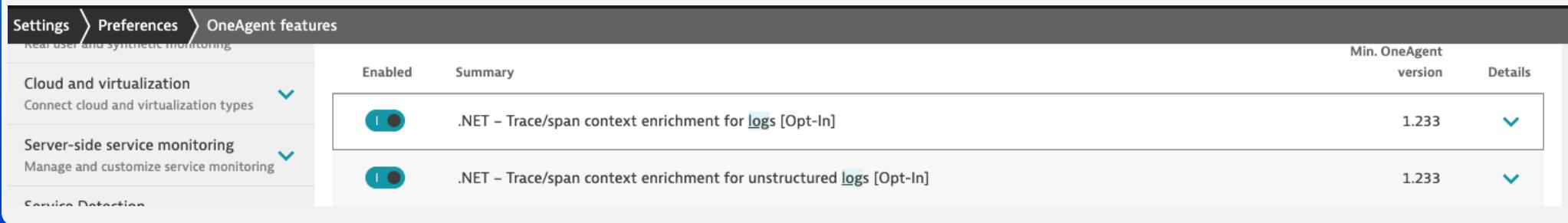
We used to spend hours manually searching through metrics, logs, and traces to piece together insights about user experience. Now, this takes minutes or seconds.

Discussion Question

How does Dynatrace enrich logs with trace context?

Discussion Question

How does Dynatrace enrich logs with trace context?



The screenshot shows the Dynatrace interface under 'Settings > Preferences > OneAgent features'. On the left, there's a sidebar with 'Cloud and virtualization' and 'Server-side service monitoring' sections. The main area is titled 'Summary' and contains two entries:

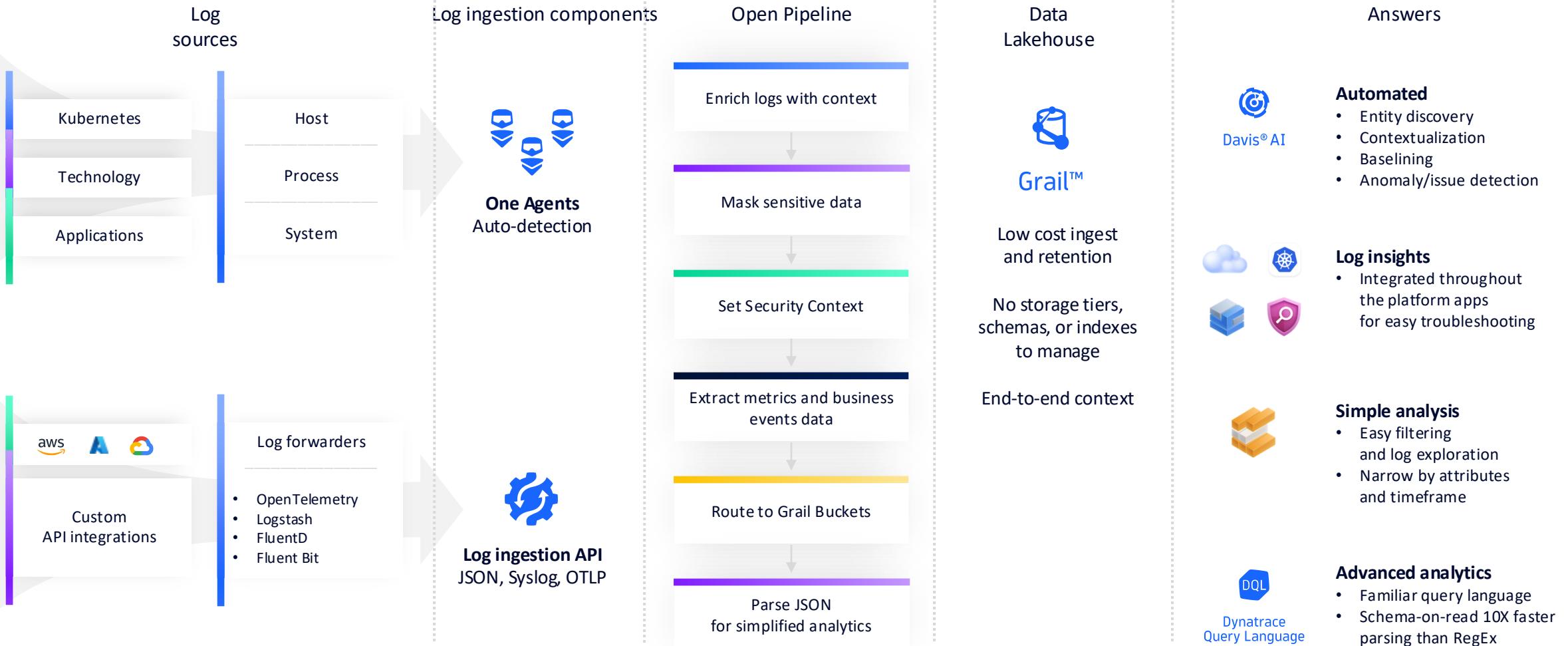
Enabled	Description	Min. OneAgent version	Details
<input checked="" type="checkbox"/>	.NET – Trace/span context enrichment for logs [Opt-In]	1.233	
<input checked="" type="checkbox"/>	.NET – Trace/span context enrichment for unstructured logs [Opt-In]	1.233	

Automatically for popular logging frameworks!
Just toggle it on in OneAgent Features

Dynatrace also provides guides for enrichment for other logging methods or for use with OpenTelemetry

Log Management & Analytics workflow

Fast insights without the painful data management



Discussion Question

What is OpenPipeline?

OpenPipeline is the data handling solution (pipeline) for Dynatrace to seamlessly ingest and process data.

Used for configuring processing, transforming, metric or data extraction, permissions and storage.

Discussion Question

What is OpenPipeline?

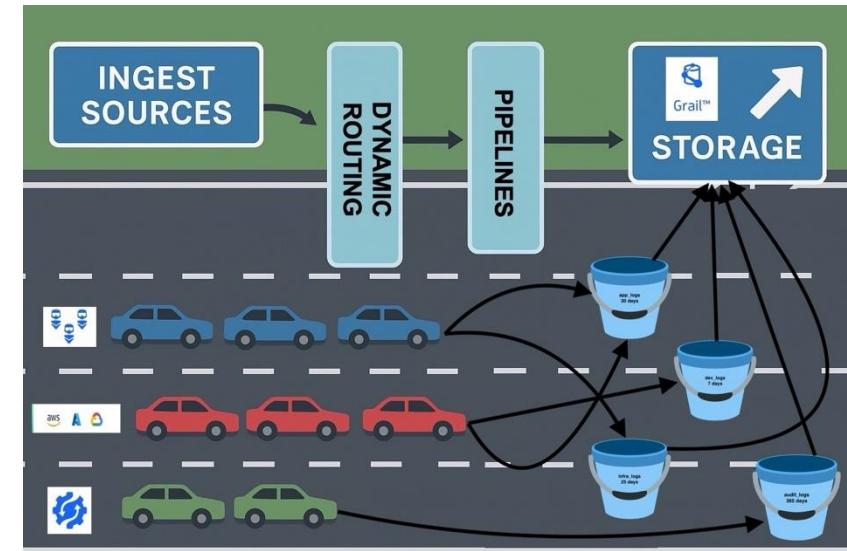
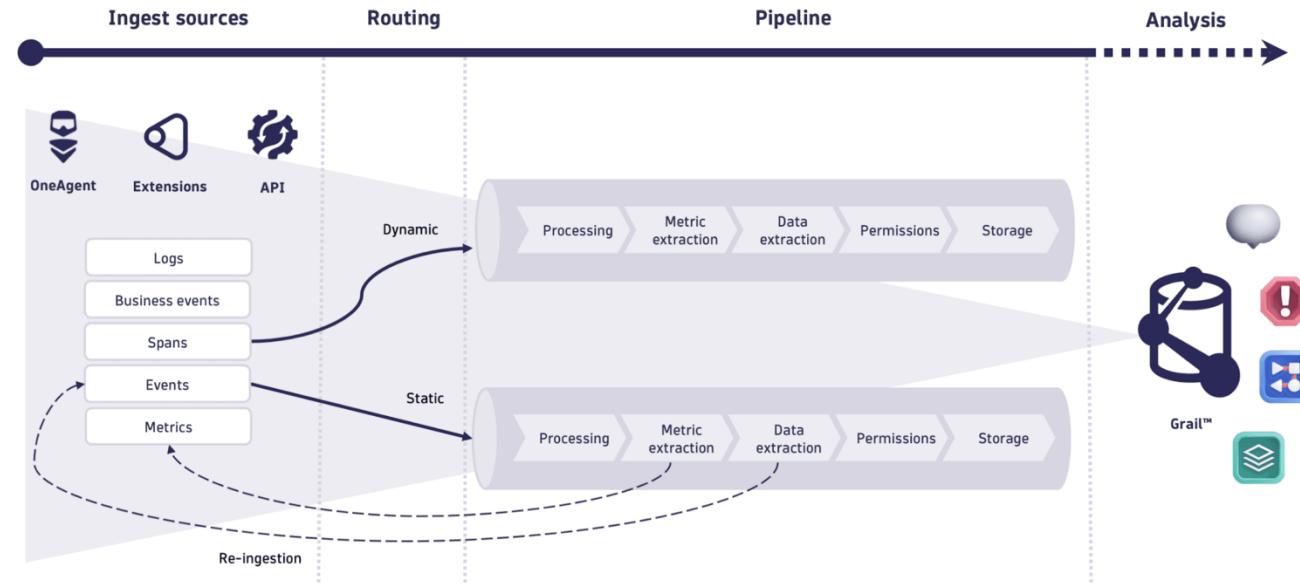
Unified solution for ingestion and processing of different data types, not just logs.



OpenPipeline

- OpenPipeline is used to normalize log records with processing rules, create metrics, create events, assign security context, and define storage to buckets
- Mapping incoming log records to specific buckets is done via OpenPipeline.
- OpenPipeline should be strategized in a similar manner to buckets.
 - 1:1 pipeline to bucket
 - 1:many pipeline to buckets

OpenPipeline How does OpenPipeline work?





OpenPipeline

Open Pipeline for Data Processing

K8s Logs
ID: pipeline_K8s_Logs_1199

Processing Metric Extraction Data extraction Permission Storage

Processing

Remove or mask sensitive data, reshape format, parse values.

+ Processor

shipping service
DQL ID: processor_payment_service_8218

Name*
shipping service

Matching condition*
1 matchesPhrase(k8s.deployment.name, "shippingservice-*")

DQL processor definition*

```
1 parse content,"JSON:Data"
2 | fieldsAdd Message=Data[message],Sev=Data[severity]
3 | fieldsAdd slatotal = if(contains(Message,"received request"), "Received"
4 )
```

Sample data

```
1 {
2   "timestamp": "2025-01-16T00:49:23.647434000-06:00",
3   "content": "{\"message\":\"[GetQuote] received request\",
4   \"Message\": \"[GetQuote] received request\",
5   \"dt.openpipeline.pipelines\": [
6     \"logs:pipeline_K8s_Logs_1199\"
7   ],
8   \"k8s.deployment.name\": \"shippingservice-*\""
9 }
```

You can test the selected processor on sample data. Fetch sample data from Notebooks [Notebooks](#)

> Run sample data

A red arrow points from the 'Processing' tab in the top navigation bar to the 'Processor' section on the left. Another red arrow points from the 'DQL processor definition*' section to the sample data preview on the right.

- OpenPipeline works in sequential mode, first vertical and then horizontal for each pipeline.
- Processing allows you to parse, add/remove/rename fields and drop record.
- Metric extraction allows you to create counter or value metric.



Scaling Log Analytics

Understanding Query Behavior

- DQL and in app queries will scan all buckets a user has permission to read by default.
- Dynatrace automatically optimizes queries based on filters
- To realize performance and cost optimizations from a bucket strategy, queries must be filtered to relevant buckets.
 - This can be accomplished in three ways:
 - Only give users access to relevant buckets*
 - Apply dt.system.bucket filter into DQL query
 - Utilize segments for targeting appropriate buckets*

Policy name*
Digital Log Access

Policy description
Description

Policy statement*

```
1 // Logs read for digital business unit
2 ALLOW storage:buckets:read WHERE storage:bucket-name
3 = "aws_digital_35d";
4 ALLOW storage:logs:read;
5
6 // can also use matcher functions such as matches phrase:
7 // | filter matchesPhrase(dt.system.bucket, "k8s")
```

```
fetch logs
| filter
// permission-based filters
... AND
// Segment-based filters
(
    (condition_a1 OR condition_a2 OR ...) AND
    (condition_b1 OR condition_b2 OR ...)
)
// consumer query continues
| summarize ...
```

All segments

Business Unit

+ Description

Variables

Create variables to apply in your Segment data filters

\$bu \$bucket

Digital aws_digital_35d

Segment data

Include all data that should be accessible when applying the Segment

Logs

dt.system.bucket = "\$bucket"

Business Unit: Digital

```
1 fetch logs
2 | filter matchesPhrase(content, "error")
```



Discussion Question

What is a bucket in Dynatrace?

Buckets are a way to organize data in Dynatrace.

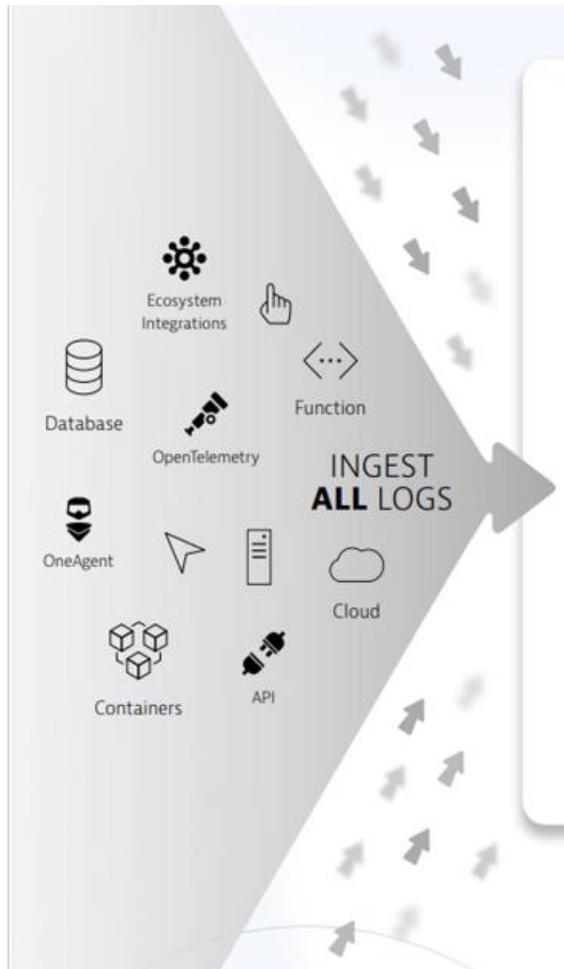
Buckets can be used for data retention, separating use cases, and access permissions.

Discussion Question

What is a bucket in Dynatrace?

Buckets can be used to improve query performance by reducing query execution time and the scope of data read.

Scaling Log Analytics



default_logs
retention: 35d
Size: 10tb/day

A screenshot of a log analytics interface. At the top, a code snippet shows a search query:

```
1 fetch logs
2 | filter isnotnull(k8s.deployment.name)
3 | summarize Count = count(), _ : {k8s.deployment.name}
4 | sort Count desc
5 | limit 10
6
```

The results table below shows 10 records. A blue arrow points from the 'Count' column to a circled sad face icon. The table includes columns for deployment name and count, with a total scanned bytes value of 500 GB.

k8s.deployment.name	Count
unguard-malicious-load-generator-*	39,054,339
unguard-user-simulator-*	31,541,074
offerservice-*	14,599,336
calculationservice-*	13,817,824
ingress-nginx-controller-*	13,233,959
pvc-out-of-space-kaniko-big-image-push-*	10,944,380
currencyserviceproxy-*	9,513,482
frontendreverseproxy-*	5,521,804
astroshop-imageprovider-*	5,030,592
aggregator-service-*	4,461,697

Scaling Log Analytics



default_logs
retention: 35d
Size: 10tb/day

Partition log data
by scaling buckets



aws_digital_35d



aws_cloudtrail_90d



aws_audit_3yr



myorg_finance_35d



myorg_security_1yr



myorg_restricted_35d



azure_digital_35d



k8s_area1_35d

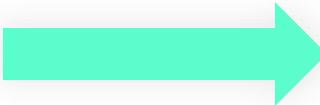


k8s_area2_35d



Define your bucket scaling strategy

- Developing a tailored data partitioning (bucket) strategy should gather the following information:
 - Ingest sources
 - Estimated Ingest volume
 - Retention desires
 - Compliance Requirements (audit)
 - Sensitive data & masking
 - Permission requirements



Bucket strategy best practice:

- Define a strict naming standard such as <provider>_<type>_<retention> or <provider>_<bu>_retention.
- Consider Business units or App Groupings
- Dedicate buckets to your largest ingest sources.
- Ingest of 1tb per day is ideal.
- Additional permissions such as restricted access can be built on top of the standard:
`aws_hr_restricted_35d` &
`aws_hr_nonrestricted_35d`

Additional bucket considerations

- 80 bucket limit per tenant by default
- Can be significantly increased based on ingest volume – contact support
- Buckets exist for all data types in Grail
 - Logs, events, BizEvents, spans, RUM, Metrics etc..
- Strategy can be replicated for other high volume data types such as BizEvents or spans.
- More buckets = more setup / admin management – strike a balance
- Ensure bucket design aligns with available attributes on log records (host group, account / Sub-IDs, log source)
- Entity properties are not available for lookups to map records to buckets.

How to create buckets

- Storage Management App or Platform API (/platform/storage/management/v1)

The screenshot shows a dark-themed web interface for managing buckets. At the top, there's a header with a back arrow, the title 'Buckets', a search bar, and a button to 'Create Bucket'. Below the header, a message says 'You can create, update, or delete buckets here. Explore our documentation for [Assigning Access Rights](#) or [Data Removal Procedures](#)'. There are filter options for 'Filter' and 'Select bucket type' (set to 'logs'). A table lists ten buckets with columns for Bucket name, Display name, Retention period (days), Table, Status, and Actions. Most buckets have a retention period of 35 days, except for 'aws_audit_3yr' (1,095 days) and 'myorg_security_1yr' (365 days). All buckets are currently active.

Bucket name	Display name	Retention period (days)	Table	Status	Actions
aws_audit_3yr	AWS Audit 3yr	1,095	logs	Active	:
aws_cloudtrail_90d	AWS CloudTrail 90d	90	logs	Active	:
aws_digital_35d	AWS Digital 35d	35	logs	Active	:
azure_digital_35d	Azure Digital BU 35d	35	logs	Active	:
default_logs	Logs	35	logs	Active	:
k8s_area1_35d	K8s Area 1 35d	35	logs	Active	:
k8s_area2_35d	K8s Area 2 35d	35	logs	Active	:
myorg_finance_35d	Finance logs 35d	35	logs	Active	:
myorg_restricted_35d	Restricted access logs 35d	35	logs	Active	:
myorg_security_1yr	Security Logs 1yr	365	logs	Active	:



Segments

Filter

Select management zone

All

FinOps - Host aks-default-77091117-vmss00001...

mz-az-af

mz-az-af-abssahara

mz-az-agcs

mz-az-agcs-cl

mz-az-agcs-fa

mz-az-agcs-ipp

mz-az-agcs-middleware

mz-az-agcs-ms

mz-az-agcs-pa

mz-az-agcs-ra

mz-az-agcs-sd

mz-az-agcs-uw

mz-az-agcs-wp

mz-az-at

mz-az-at-appdev

mz-az-at-appdev_playground

mz-az-at-bmpproduct

mz-az-au

mz-az-au-aaldevops

mz-az-au-prod

mz-az-ay

mz-az-ay-digitalplatform

mz-az-azp

mz-az-azp-AZGACanadaIT

mz-az-azp-development

mz-az-bcm_de

mz-az-bcm_de-dbitkvi5co

mz-az-bcm_de-global

mz-az-bg

mz-az-bg-AZBG_DynaTrace

Why Segments?

Settings > Preferences > Management zones

Settings

Monitoring

Setup and overview

Cloud Automation

Setup and configuration

Processes and containers

Monitoring, detection and naming

Web and mobile monitoring

Real user and synthetic monitoring

Cloud and virtualization

Connect cloud and virtualization types

Server-side service monitoring

Manage and customize service monitoring

Service Detection

Define rules for services and spans

Log Monitoring

Set up management of logs

Anomaly detection

Configure detection sensitivity

Alerting

Configure alerting settings

Dashboards

Configure dashboard settings

Metrics

Management zones settings

Management zones enable defining fine grained access rights to parts of an environment. A

Management zone consists of a set of entities like applications, hosts, process groups, or services.

[More...](#)

 Your user does not have the necessary write permissions.

Filter items...

Summary

FinOps - Host aks-default-77091117-vmss00001Y TEST

Page Unresponsive

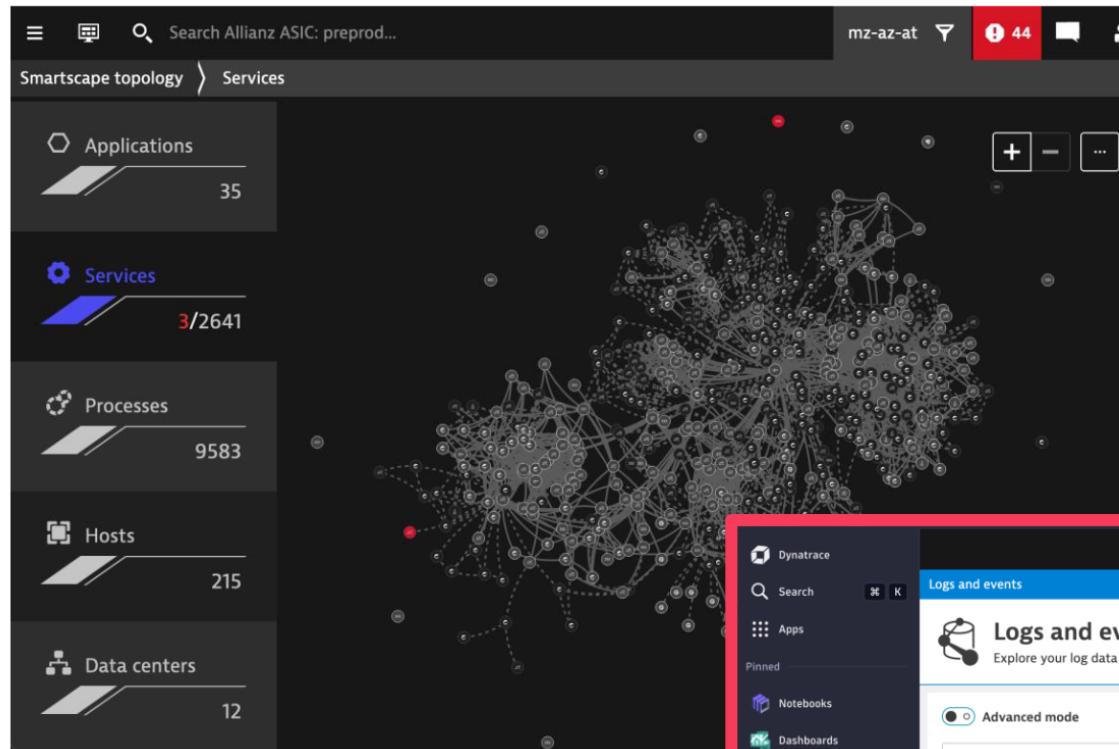
You can wait for it to become responsive or exit the page.

 Management zones settings - Environment - Settings - Allianz ASI...

Wait

Exit page

Why Segments?



Experience the
full power of
 Grail and the
Dynatrace Query
Language

 Where MZ?

A screenshot of the Dynatrace Logs and events interface. The top navigation bar shows "Logs and events" and "Last 2 hours". The main area displays a table of log results. The table has columns for "timestamp", "status", and "content". The first two rows of the table are as follows:

timestamp	status	content
2023-11-16 13:21:50.401	NONE	SNMP trap (CISCO-SMI::ciscoMgmt.41.2.0.1) reported from 10.69.0.18
2023-11-16 13:21:50.401	NONE	SNMP trap (CISCO-SMI::ciscoMgmt.41.2.0.1) reported from 10.69.0.19
{ "timestamp": "2023-11-16T12:21:45.191917656Z", "message": "Update loop too		

Segments: Preconfigured Dynamic Filtering

The screenshot shows a dark-themed Kubernetes monitoring interface. At the top left, there's a navigation bar with icons for Kubernetes, Explorer, and Anomaly detectors. Below it is a dropdown menu showing "Cluster: CL-Prod20" with a green border around it. To the right of the dropdown is a search bar labeled "Filter by:" and a "+ Add filter" button. A large green banner with the text "1 click to block out all the noise" is positioned on the right side of the header.

The main area displays a table titled "Clusters" with 12 records. The table includes columns for Cluster, Problems, Nodes, Namespaces, Workloads, Pods, CPU Usage, CPU Requests, and CPU. Each row contains a cluster name, its status (e.g., 2 problems), and numerical values for each metric, followed by horizontal bar charts representing the usage and requests. A summary bar at the top of the table provides a quick overview of the total count for each category: Clusters (16), Nodes (456), Namespaces (137), and Workloads (149).

Cluster	Problems	Nodes	Namespaces	Workloads	Pods	CPU Usage	CPU Requests	CPU
code-matrix-cluster	2	12	8	789	1.2k	<div style="width: 120px;"></div>	<div style="width: 100px;"></div>	<div style="width: 100px;"></div>
quantum-compute-pod	1	1 / 2	5	12	78	<div style="width: 12px;"></div>	<div style="width: 10px;"></div>	<div style="width: 10px;"></div>
binary-nexus	-	30	12	◆ 13 / 568	234	<div style="width: 234px;"></div>	<div style="width: 100px;"></div>	<div style="width: 100px;"></div>
devops-grid	-	1	5	456	48	<div style="width: 48px;"></div>	<div style="width: 10px;"></div>	<div style="width: 10px;"></div>
cyberspace-core	-	◆ 2 / 500	23	1.3k	89	<div style="width: 89px;"></div>	<div style="width: 10px;"></div>	<div style="width: 10px;"></div>
robo-mesh-cluster	-	4	3	◆ 8 / 90	5	<div style="width: 5px;"></div>	<div style="width: 10px;"></div>	<div style="width: 10px;"></div>
nano-dene-forge	-	12	1	◆ 4 / 45	67	<div style="width: 67px;"></div>	<div style="width: 10px;"></div>	<div style="width: 10px;"></div>
crypto-mesh-hub	-	◆ 1 / 45	24	456	124	<div style="width: 124px;"></div>	<div style="width: 10px;"></div>	<div style="width: 10px;"></div>
data-pipeline-grid	-	5	4	545	78	<div style="width: 78px;"></div>	<div style="width: 10px;"></div>	<div style="width: 10px;"></div>
quantum-logic-nest	-	1	3	3	3	<div style="width: 3px;"></div>	<div style="width: 10px;"></div>	<div style="width: 10px;"></div>

Simple Segment



Show me entities, logs, events, etc. of my application

- Equivalent to single MZ

Multiple Segments

2 segments ^

Segments

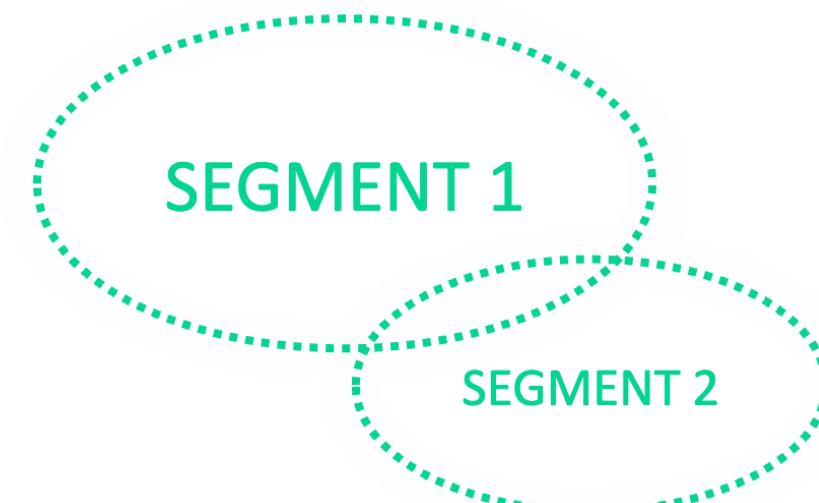
Region	▼	eu-ireland, eu-austria	▼	X
App-env	▼	production	▼	X

+ Segment Clear all

[Manage segments](#) [Learn more ↗](#)

Show me data of my application from a specific infrastructure

- Intersection of multiple segments
(eu-ireland OR eu-austria) AND production



How it all works

2 segments ^

Segments

Region	eu-ireland, eu-austria	X
App-env	production	X

+ Segment Clear all

[Manage segments](#) [Learn more](#)

Region:
eu-ireland,
eu-austria

App-env:
production

- 1) Segment IDs and values are passed to query API
FiRmGMvWzPY([eu-ireland, eu-austria](#)), HCKccp8aAIU([production](#))
- 2) Grail filters consumer queries with conditions defined in segments

```
fetch logs
| filter
  // permission-based filters
  ... AND
  // Segment-based filters
  (
    (condition_a1 OR condition_a2 OR ...) AND
    (condition_b1 OR condition_b2 OR ...)
  )
  // consumer query continues
  | summarize ...
```

Transparent
filter conditions

Segments and in-app filters

2 Additional filter for further problem analysis

Region (2) Type to filter

Filter by segments

Region eu-ireland, eu-austria

+ Segment

1 Segments selector to set context

Manage segments Learn more

24 Nodes 3 / 3 Namespaces 12 Workloads 3.5k / 12.7k

Probabilities Topology

12 columns hidden

Node	Problems	Pods	Workloads	Services	Usage	Requests	alertmanager	apiserver	key	key
full-observability...	-	123	3	45	main	main	main	main	✓	-
full-observability...	-	12	3	345	-	longvaluetextexample...	✓	longvaluetextexample...	-	-
GKE CP KLU	-	3	12	3	-	main	main	main	✓	-
OCP 3.11	-	12	456	1	-	-	longvaluetextexample...	longvaluetextexample...	✓	-
ocp4-12	-	467	24	12	-	-	-	longvaluetextexample...	-	-
ocp4-9-in-cluster	-	4	89	3	longvaluetext	longvaluetextexample...	longvaluetextexample...	longvaluetextexample...	-	-
ocp4-9-kuberne...	-	4	45	54	main	longvaluetext	longvaluetext	longvaluetext	-	-
rauter-cri-test	-	45	456	34	-	✓	✓	longvaluetextexample...	main	-
trauter-e2e	-	5	545	1,234	-	-	-	✓	longvaluetextexample...	longvaluetext
full-observability...	-	123	3	45	main	main	main	main	✓	-
full-observability...	-	12	3	345	-	longvaluetextexample...	✓	longvaluetextexample...	-	-
GKE CP KLU	-	3	12	3	-	main	main	main	✓	-
OCP 3.11	-	12	456	1	-	-	longvaluetextexample...	longvaluetextexample...	✓	-
ocp4-12	-	467	24	12	-	-	-	longvaluetextexample...	-	-
ocp4-9-in-cluster	-	4	89	3	longvaluetext	longvaluetextexample...	longvaluetextexample...	longvaluetextexample...	-	-
ocp4-9-kuberne...	-	4	45	54	main	longvaluetext	longvaluetext	longvaluetext	-	-
rauter-cri-test	-	45	456	34	-	✓	✓	longvaluetextexample...	main	-
trauter-e2e	-	5	545	1,234	-	-	-	✓	longvaluetextexample...	longvaluetext
ocp4-12	-	467	24	12	-	-	-	longvaluetextexample...	-	-
trauter-e2e	-	1	3	3	-	-	✓	longvaluetextexample...	-	-

20 rows per page

Page 1 of 2



Problems

2 Additional filter for further problem analysis

Region (2) Type to filter Last 24 hours Update

Filter by segments Region eu-ireland, eu-austria **1 Segments selector to set context**

+ Segment Manage segments Learn more

2

Category All Slowdown Error Monitoring unavailable Custom Available Resources shortage Root cause paymentService easyService easyTravel Windows

1 / 12.2k

0 5:40 5:50 6:00 6:10 6:20 6:30 6:40 6:50 7:00 7:10 7:20 7:30 7:40 7:50 8:00 8:10 8:20 8:30 8:40 8:50 9:00 9:10 9:20 9:30 9:40

2 selected Open **2 columns hidden**

ID	Name	Status	Labels	Category	Affected	Root cause	Started	Duration
P-230980	Service slowdown	Active	Ack Warning service09 Show more	Slowdown	150	loginService	21/09/2023, 6:10	30 min
P-230981	SLO Burnrate	Active	Ack	Availability	23	easyService	21/09/2023, 5:42	2 min
P-230982	Failure rate increase	Active	Warning	Monitoring unavailable	4	SSO-Service	21/09/2023, 6:22	42 min
P-230983	Support sliding window size	Active	Warning	Custom	12	loginService	21/09/2023, 6:36	56 min
P-230984	Security - Critical vulnerability detected	Closed	Ack	Warning	7	loginService	21/09/2023, 7:33	1 hr 23 min
P-230985	Error rate increment	Closed	Ack	Error	1	easyService	21/09/2023, 6:34	min
P-230986	CPU saturation	Closed	Ack	Resources shortage	4	paymentService	21/09/2023, 6:32	1 hr
P-230987	Multiple infrastructure problems	Closed	Ack	Custom	2	loginService	21/09/2023, 6:32	1 hr
P-230988	State Service is in undesirable state	Closed	Ack	Availability	1	paymentService	21/09/2023, 6:32	1 hr
P-230989	Windows Search is in undesirable	Closed	Ack	Availability	1	easyService	21/09/2023, 6:32	1 hr
P-230990	zyrdy	Closed	Ack	Custom	1	easyService	21/09/2023, 6:32	1 hr
P-230991	!ChPe_test_2	Closed	Ack	Slowdown	1	easyService	21/09/2023, 6:32	1 hr
P-230992	Embedded Mode is in undesirable state	Closed	Ack	Availability	1	easyService	21/09/2023, 6:32	1 hr
P-230993	Security - Critical vulnerability detected	Closed	Ack	Error	1	paymentService	21/09/2023, 6:32	1 hr
P-230994	Simple default transformation	Closed	Ack	Resources shortage	1	easyService	21/09/2023, 6:32	1 hr
P-230995	Browser monitor global outage	Closed	Ack	Availability	1	paymentService	21/09/2023, 6:32	1 hr



Building a Segment

< All segments

This segment has unsaved changes.

[Discard changes](#) [Save](#)



ACE DT

(Full-stack) Observability data for ACE DT team.



Variables ⓘ

Create variables to apply in your Segment data filters

2 Variables for dynamic segments

\$namespace.name \$namespace.id

dynatrace

CLOUD_APPLICATION_NAM...



Owner

R Roman Windischhofer

Visibility

任何人都可以在环境中查看

1 Visible to anyone or unlisted

3 Include data directly

Logs k8s.namespace.name = \$namespace.name

Logs, Delete, Up, Down, More

Preview



Metrics k8s.namespace.name = \$namespace.name

Metrics, Delete, Up, Down, More

Preview



4 Include data of entities

Tags = team:ACE

Hosts, Delete, Up, Down, More

Preview

Include

Problems, Vulnerabilities, Metrics, Logs, Events, BizEvents, Spans

5 Include data of related entities

Runs on = \$this.hosts

Services, Delete, Up, Down, More

Preview

Include

Problems, Vulnerabilities, Metrics, Logs, Events, BizEvents, Spans

20 include blocks per segment

1 filter for data of entities (logs, events, spans)

No limit for problems, vulnerabilities, metrics

1 topology traversal step only

+ All types + Metrics + Logs + Events + BizEvents + Spans + Entities



12

Permissions

Permissions

- Controlling access to logs can be accomplished via IAM policies and defining bucket level and/or record level access.
- Bucket level control is done via bucket names.
- Record level control is done via fields or `dt.security.context` which must be set on the records themselves and defined within the policy.

All bucket access with deny

Policy name*

Generic Log Viewer

Policy description

Description

Policy statement*

1	<pre>// Logs read all except restricted</pre>
2	<pre>ALLOW storage:buckets:read WHERE storage:table-name</pre>
= "logs";	
3	<pre>DENY storage:buckets:read WHERE storage:bucket-name</pre>
= "myorg_restricted_35d";	
4	<pre>ALLOW storage:logs:read;</pre>

Digital bucket read & security context = hipstershop

Policy name*

Hipster App Team Logs

Policy description

Description

Policy statement*

1	<pre>// Allow digital bucket read but restrict to</pre>
2	<pre>specific records</pre>
3	<pre>ALLOW storage:buckets:read WHERE storage:bucket-name</pre>
= "aws_digital_35d";	
4	<pre>ALLOW storage:logs:read WHERE</pre>
	<pre>storage:dt.security_context = "hipstershop";</pre>



Permissions: Supported Fields

Field name	IAM condition	Supported IAM tables
<code>event.kind</code>	<code>storage:event.kind</code>	<code>events</code> , <code>bizevents</code> , <code>system</code>
<code>event.type</code>	<code>storage:event.type</code>	<code>events</code> , <code>bizevents</code> , <code>system</code>
<code>event.provider</code>	<code>storage:event.provider</code>	<code>events</code> , <code>bizevents</code> , <code>system</code>
<code>k8s.namespace.name</code>	<code>storage:k8s.namespace.name</code>	<code>events</code> , <code>bizevents</code> , <code>logs</code> , <code>metrics</code> , <code>spans</code>
<code>k8s.cluster.name</code>	<code>storage:k8s.cluster.name</code>	<code>events</code> , <code>bizevents</code> , <code>logs</code> , <code>metrics</code> , <code>spans</code>
<code>host.name</code>	<code>storage:host.name</code>	<code>events</code> , <code>bizevents</code> , <code>logs</code> , <code>metrics</code> , <code>spans</code>
<code>dt.host_group.id</code>	<code>storage:dt.host_group.id</code>	<code>events</code> , <code>bizevents</code> , <code>logs</code> , <code>metrics</code> , <code>spans</code>
<code>metric.key</code>	<code>storage:metric.key</code>	<code>metrics</code>
<code>log.source</code>	<code>storage:log.source</code>	<code>logs</code>
<code>dt.security_context</code>	<code>storage:dt.security_context</code>	<code>events</code> , <code>bizevents</code> , <code>system</code> , <code>logs</code> , <code>metrics</code> , <code>spans</code> , <code>entities</code>
<code>gcp.project.id</code>	<code>storage:gcp.project.id</code>	<code>events</code> , <code>bizevents</code> , <code>logs</code> , <code>metrics</code>
<code>aws.account.id</code>	<code>storage:aws.account.id</code>	<code>events</code> , <code>bizevents</code> , <code>logs</code> , <code>metrics</code>
<code>azure.subscription</code>	<code>storage:azure.subscription</code>	<code>events</code> , <code>bizevents</code> , <code>logs</code> , <code>metrics</code>
<code>azure.resource.group</code>	<code>storage:azure.resource.group</code>	<code>events</code> , <code>bizevents</code> , <code>logs</code> , <code>metrics</code>



Discussion Question

Why would you want to create a metric from a log?

Query Performance

Cost efficient storage and query

Discussion Question

Why would you want to create a metric from a log?

Simplified alert creation



Why Logs to Metrics?



• Enhanced Performance:

- Efficient storage
- Faster query performance
- Better scalability for handling of large volumes of data

• Simplified Alerting:

- Easier to setup and manage Metrics-based alerts
- Easier to generate dynamic thresholds
- Easy to aggregate and summarize data

- A metric can be either a Counter or Value type.
- Counter metric - # of HTTP requests
- Value metric - Product quantity, Revenue

The screenshot shows a 'Metric Extraction' configuration interface. On the left, a sidebar lists various metrics categorized by processor:

- Processor
- getCart (Counter metric)
- Slow cart (Counter metric)
- failPayments (Counter metric)
- order Checkout (Counter metric)
- successful payments (Counter metric)
- Procesed orders (Counter metric)
- Received Requests (Counter metric)
- Shipped Requests (Counter metric)
- Revenue (Value metric)
- shipping (Counter metric)

On the right, two specific metrics are detailed:

getCart
Counter metric ID: processor_getCart_3570
Name*: getCart
Matching condition*: 1 matchesPhrase(content, "GetCartAsync")
Metric key*: log. getCart ←

Revenue
Value metric ID: processor_Revenue_6652
Name*: Revenue
Matching condition*: 1 matchesPhrase(k8s.deployment.name, "paymentservice-*") and matchesPhrase(Message, "Transaction processed:")
Field extraction*: Amount
Metric key*: log. revenue ←
Dimensions Pre-defined Custom
Select an option





Log to Events

Log to Events is a system for capturing and analyzing events from various sources.

An event can be either Davis or Business event:



Davis Event

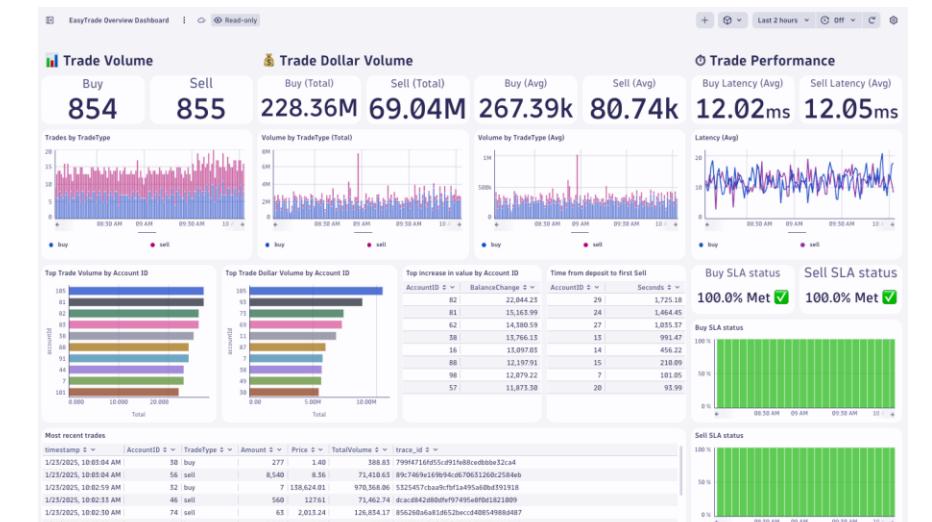
- Does this anomaly need to be reported?
- Is it an INFO Event that needs to be generated?



Business Event

- Is this data for reporting business data?
- Is this data for analytics for your Ops team?

Problem Analysis - Last 24 Hours						
Status	Problem	Affected	StartTime	EndTime	Duration	event.id
OPEN	P-25013783 - High CPU throttling	unguard-user-simulator	1/17/2025, 5:59:00 PM	In Progress	5.67 d	-102163872572261559_1737154740000V2
OPEN	P-25015137 - Job failure event	pvc-out-of-space-kaniko-big-image-push	1/23/2025, 1:01:00 AM	In Progress	9.06 h	2902693588201881192_1737612060000V2
CLOSED	P-25015026 - Job failure event	pvc-out-of-space-kaniko-big-image-push	1/22/2025, 5:01:00 PM	1/22/2025, 8:16:00 PM	3.25 h	650715238141236067_1737583260000V2
CLOSED	P-25014994 - Job failure event	pvc-out-of-space-kaniko-big-image-push	1/22/2025, 12:46:00 PM	1/22/2025, 5:01:00 PM	4.25 h	5751904292146087284_1737567960000V2
CLOSED	P-25014950 - Job failure event	pvc-out-of-space-kaniko-big-image-push	1/22/2025, 7:01:00 AM	1/22/2025, 12:46:00 PM	5.75 h	-5931107189908644196_1737547260000V2
CLOSED	P-25015181 - Out-of-memory kills	paymentservice	1/22/2025, 10:22:00 PM	1/22/2025, 10:37:00 PM	15.00 min	3345252567425892024_1737602520000V2
CLOSED	P-25015021 - Memory usage close to limits	paymentservice	1/22/2025, 4:52:00 PM	1/22/2025, 10:36:00 PM	5.75 h	-6865210290140368054_1737527200000V2
OPEN	P-25014976 - Memory usage close to limits	manager	1/22/2025, 9:45:00 AM	1/22/2025, 10:47:00 AM	1.03 h	-1425355036653467008_1737571000000V2
OPEN	P-25015212 - Not all pods ready	mail-service	1/23/2025, 9:30:00 AM	In Progress	34.58 min	-1194887507921015297_1737642600000V2
CLOSED	P-25015211 - Pods stuck in pending	mail-service	1/23/2025, 9:18:00 AM	1/23/2025, 9:55:00 AM	45.00 min	453651796561041882_1737641400000V2
CLOSED	P-25014971 - Not all pods ready	mail-service	1/22/2025, 9:30:00 AM	1/22/2025, 10:20:00 AM	50.00 min	-2528180704712407912_1737562600000V2
CLOSED	P-25015173 - Container restarts	ingress-dev-controller	1/23/2025, 5:04:00 AM	1/23/2025, 5:20:00 AM	16.00 min	-5925771486552286267_1737626640000V2





Dashboarding

Dashboarding is a process of visualizing data.

- Spot the differences between these two dashboards?



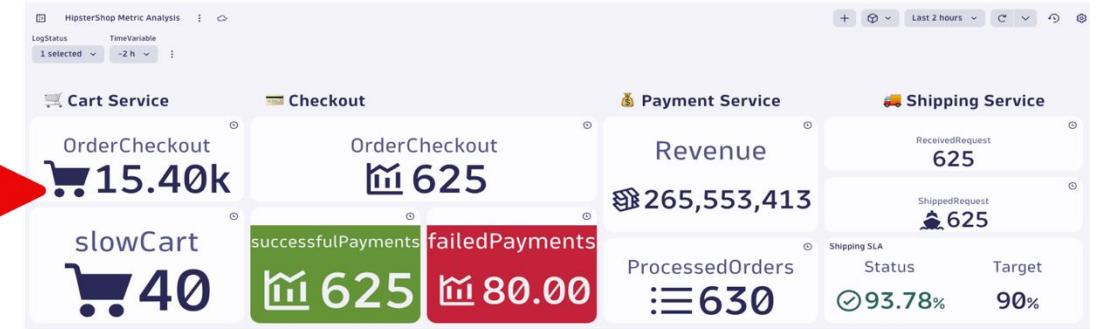
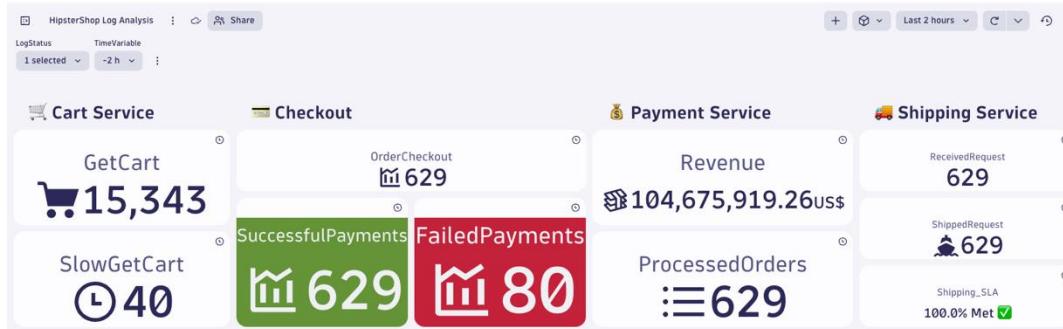
Use logs when:

- Low frequency refresh
- Involve a complex DQL
- Joining different types of data
- Analyzing short timeframes



Use metrics when:

- High frequency refresh
- Trending over long timeframes (timeseries)
- Optimize query cost
- To create SLOs alerts





Alerting



- **Use logs when:**

- Infrequent ingest of log records
- Complex query
- Detailed investigations



- **Use metrics when:**

- Frequent data points
- Dynamic thresholds
- Performance tracking

The screenshot displays the Grafana interface for creating and editing anomaly detectors. It shows two separate configuration panels side-by-side.

Left Panel (Edit anomaly detector):

- Get started:** Add a title and description.
- Configure your query:** Define your time series data. A code editor shows the following query:

```
1 fetch logs
2 | filter contains(k8s.deployment.name, "shippingservice-*")
3 | makeTimeseries shipping=count(), interval:1m
```
- Show advanced options:** A radio button is selected.
- Actor:** Rohan Shah (selected)
- Customize parameters:** Set thresholds and alerts.
- Create an event template:** Set event description and properties.
 - Event name:** Auto adaptative log threshold
 - Event description:** Type { for placeholder hints.
 - Event properties:**
 - dt.source_entity: {dims:dt.source_entity}
 - event.type: CUSTOM_ALERT
 - event.name: Auto adaptative log threshold
 - Enter a key: Enter a value

Right Panel (Edit anomaly detector):

- Get started:** Add a title and description.
- Configure your query:** Define your time series data.
- Customize parameters:** Set thresholds and alerts.
- Analyzers:** Auto adaptive threshold anomaly detection (selected).
 - Anomaly detection:** Auto adaptive threshold anomaly detection (highlighted with a red box).
 - Seasonal baseline anomaly detection
 - Static threshold anomaly detection
- Create an event template:** Set event description and properties.

At the bottom right of the interface, there are buttons for 427 GB, Discard, Save, and a small logo.

Training Environment

1. Log out of any existing Dynatrace environments.

2. Login to the following tenant:

<https://XXXXX.sprint.apps.dynatracelabs.com/>

ID: XXXXX@protonmail.com
Password: Dynatrace123*

Live Demo & Hands-on Training

Questions?