

# Log Management & Analytics at scale!

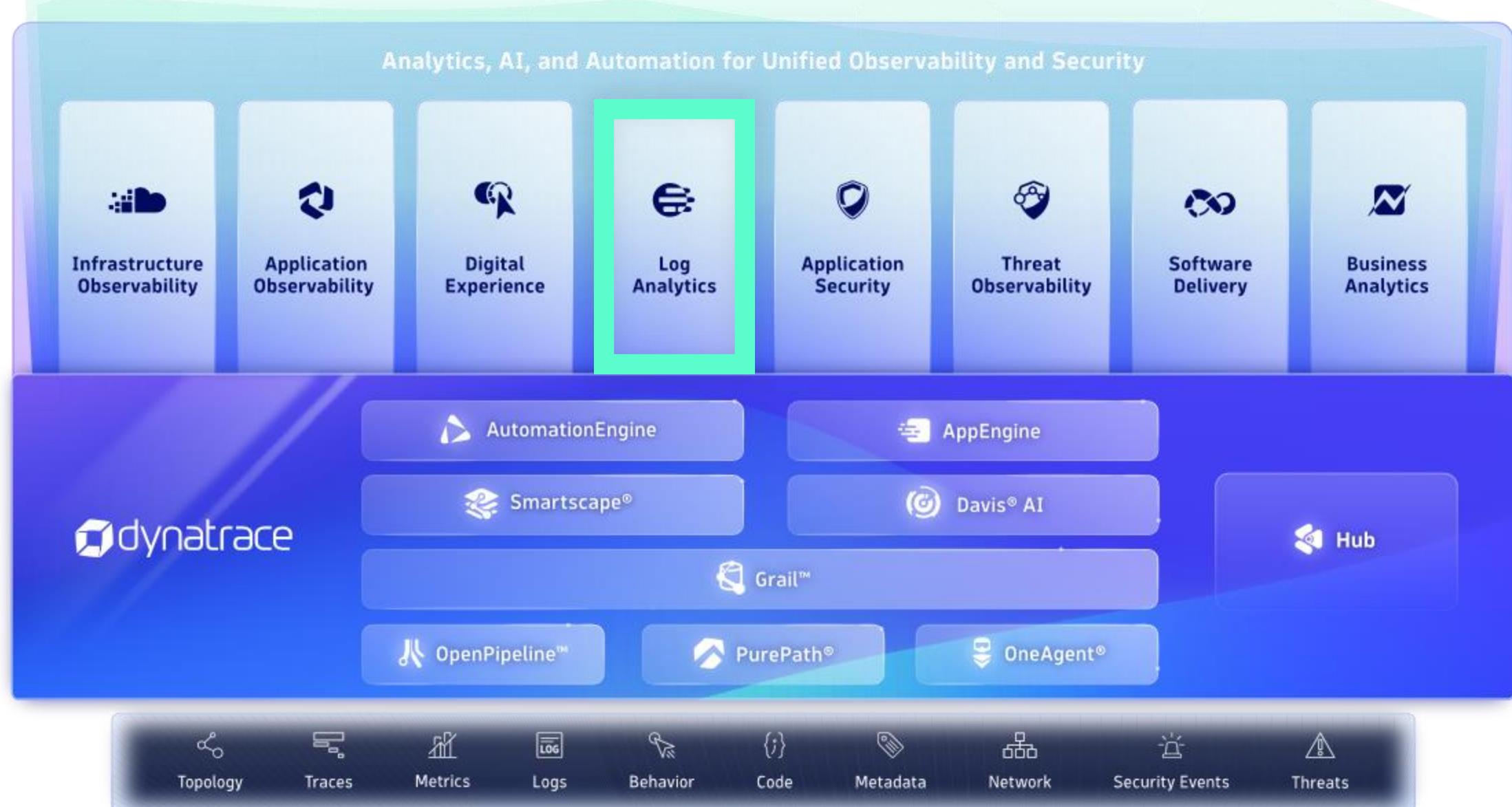


# Agenda

- 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



# 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

# Discussion Question

Scalability

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

Filtering

Alerts from log data

Automatic parsing for standard logs

Deep dive analytics

Data security

# Logs in context reduces MTTR and provides instant answers

**Failure rate increase**  
Closed: P-2502156 Error Started at Feb 3, 2025, 7:06 PM for 28 min

Events 4 SLOs 3 Affected users 93 Affected entities 3

Deployment Events Logs

**Affected infrastructure**

**TradeManagement** Service Root cause Open entity

Events 2 found

Failure rate increase  
Feb 3, 2025, 7:01 PM  
The error rate increased to 22.56 %. Service TradeManagement has a failure rate increase.

Chart Properties

Client-side service error rate increase  
Feb 3, 2025, 6:47 PM

**Failure rate increase**  
Closed: P-2502156 Error Started at Feb 3, 2025, 7:06 PM for 28 min

Events 4 SLOs 3 Affected users 93 Affected entities 3

Deployment Events Logs

**Logs**  
10733 records

● ERROR ● INFO

**Recommended queries**

Show the last 100 error logs Run query  
Show logs in current context Run query

Trace id: 962fd7e6f1a402794d28824f24589718 | Feb 4, 2025, 7:04 PM → 7:10 PM

**Requests**  
10 records Search Open with

Start time	Endpoint	Service	Response time	Request type	HTTP status	Span source	Process	Kubernetes	Kubernetes
Feb 4, 19:09:35.864	Charge	[eks]prod	5.43 ms	Failure	OneAgent	index.js... payment...	prod	...	...
Feb 4, 19:09:35.834	Convert	[eks]prod	1.99 ms	Success	OneAgent	server.js... currency...	prod	...	...
Feb 4, 19:09:35.815	GetQuote	[eks]prod	318.00 µs	Success	OneAgent	shipping...	prod	...	...
Feb 4, 19:09:35.805	Convert	[eks]prod	1.26 ms	Success	OneAgent	server.js... currency...	prod	...	...

**checkout**  
Open with Close details Maximize

January 4, 2025 at 19:09:30.766 Duration: 5.11 s Response time: 5.11 s Errors: 7

962fd7e6f1a402794d28824f24589718

20 spans Search name, endpoint, service, or attributes

Name	Duration	2.0 s	4.0 s
/cart/checkout [eks]prod:9090	5.11 s		
POST	5.11 s		

Attributes Logs

Core Start time 2025-02-04T19:09:30.766000000Z



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?

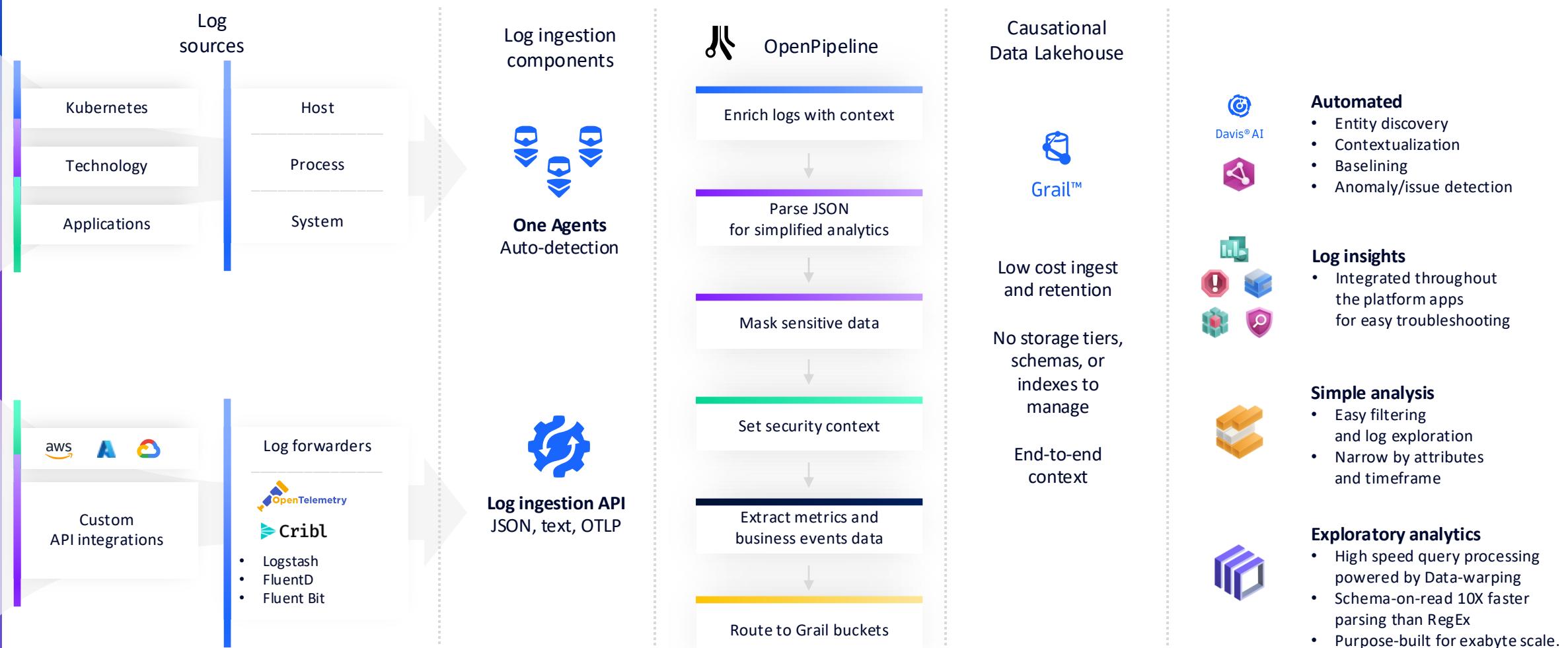
# Discussion Question

How does Dynatrace enrich logs with trace context?

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

# The all-in-one unified platform advantage



# Discussion Question

What is OpenPipeline?

# Discussion Question

## What is OpenPipeline?

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

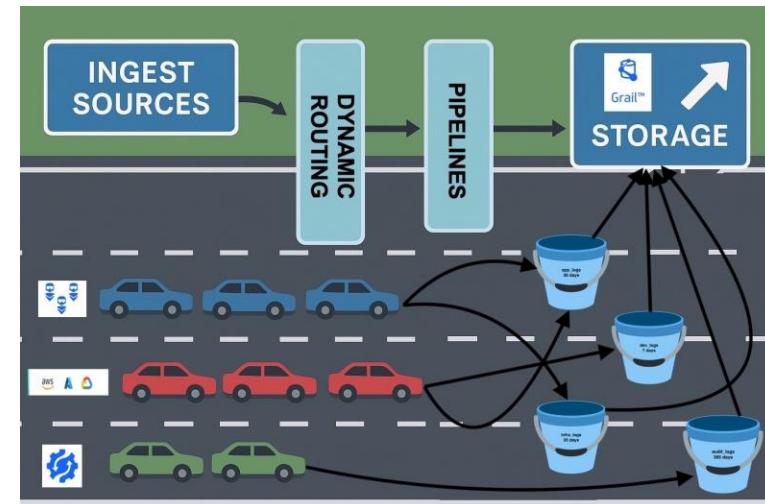
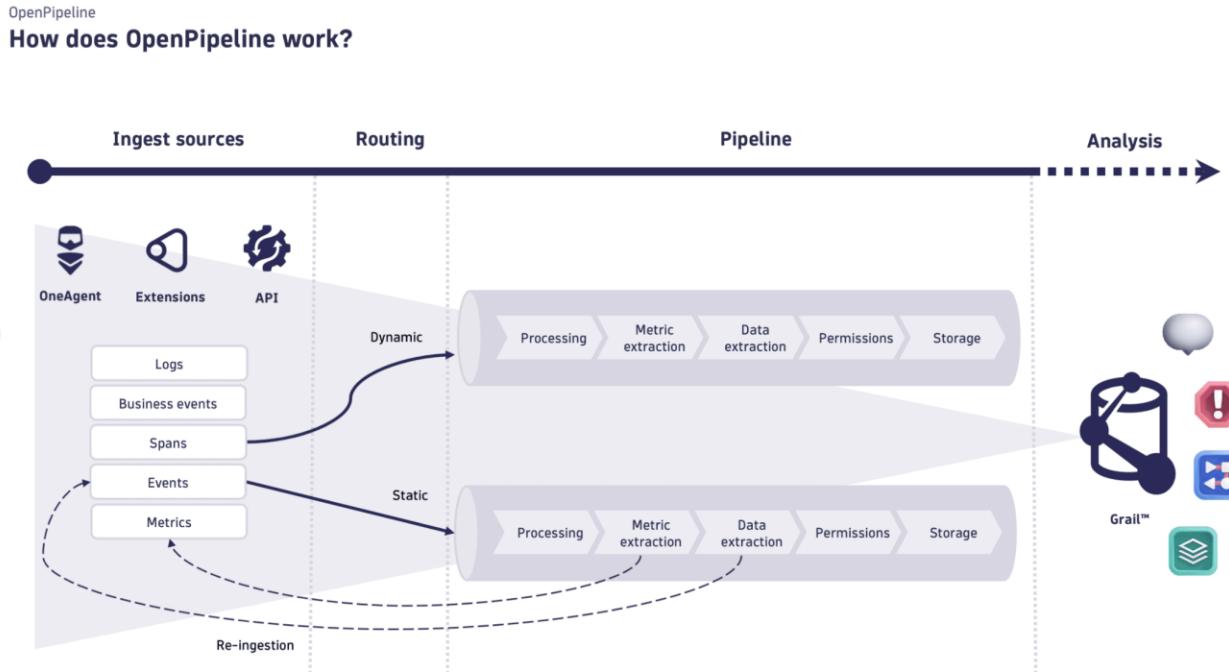
Used for configuring processing, transforming, metric or data extraction, permissions and storage.

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

< Logs

**Parse payload**  
ID: pipeline\_prio1\_parse\_json\_payload\_6715

Processing Data extraction Davis Metric Extraction Permission Cost allocation Product allocation Storage

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

+ Processor JFrog Artifactory Technology bundle

Drop DEBUG Drop record  
parse json payload DQL  
JFrog Artifactory Technology bundle

**JFrog Artifactory Technology bundle**

Details  
JFrog Artifactory technology parsers  
Matching condition Pre-defined Custom

1 matchesValue(log.source, "jfrog\_artifactory")

Processors

JFrog Generic processor  
JFrog Artifactory Request processor  
JFrog Artifactory Access processor  
JFrog Artifactory Access Audit processor  
JFrog Artifactory Access Security Audit processor  
Loglevel from HTTP status code  
Validate timestamp parsing  
Populate status value based on loglevel  
Cleanup temporary fields  
Cleanup log.source  
Cleanup host.name  
Cleanup service.name  
Cleanup container.image.name

**Preview**  
Sample Data

```
1  {
2    "log_source": "jfrog_artifactory",
3    "service.name": "jfrog.saas.rt.artifactory.access",
4    "content": [
5      {
6        "log_source": "jfrog_artifactory",
7        "service.name": "jfrog.saas.rt.artifactory.access",
8        "host.id": "abde12345",
9        "host.hostname": "dtta",
10       "component.name": "Dynatrace",
11       "timestamp": "2025-07-07T13:54:27.747Z",
12       "content": {
13         "action": "LOGIN",
14         "action_response": "ACCEPTED LOGIN",
15         "ip.address": "127.0.0.1",
16         "log.timestamp": "2025-07-07T13:54:27.747Z",
17         "repository.path": null,
18         "response": "ACCEPTED",
19         "trace_id": "12345abc-67de-8901-f234-gh567ijk18901",
20         "type": "token",
21         "user.name": "john@0112345abc-67de-8901"
22       }
23     },
24   ],
25   "log_source": "jfrog_artifactory",
26   "service.name": "jfrog.saas.rt.artifactory.request",
27   "content": [
28     {
29       "log_source": "jfrog_artifactory"
30     }
31   ]
32 }
```

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

Run sample data

A red arrow points from the 'Processing' tab in the top navigation bar to the 'JFrog Artifactory Technology bundle' section. Another red arrow points from the 'JFrog Artifactory Technology bundle' section down to the 'Processors' list.

- 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 or log records\*
    - 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
   = "aws_digital_35d";
3 ALLOW storage:logs:read;
```

```
1 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 ...
```

```
1 fetch logs
  // only return logs that are stored in the following bucket
  | filter dt.system.bucket == "k8s_area1_35d"
2
3
4
5 // can also use matcher functions such as matches phrase:
6 // | 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	Digital	\$bucket	aws_digital_35d
------	---------	----------	-----------------

Segment data

Include all data that should be accessible when applying the Segment

Logs

| dt.system.bucket == "\$bucket"

Business Unit: Digital

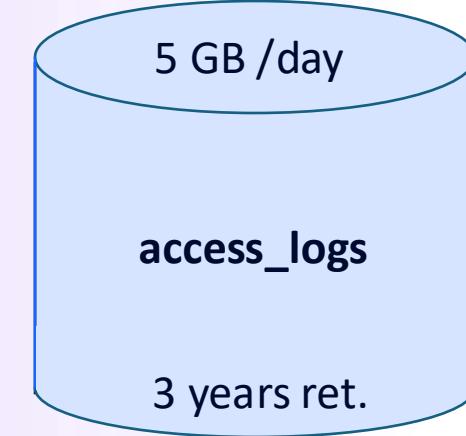
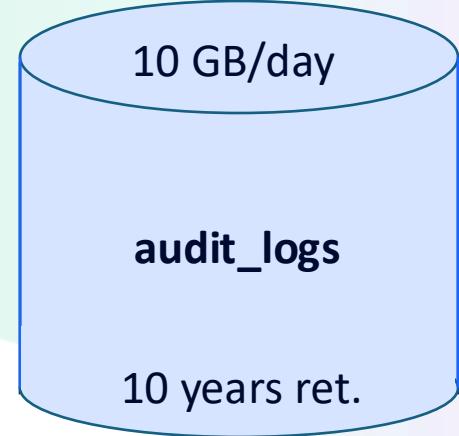
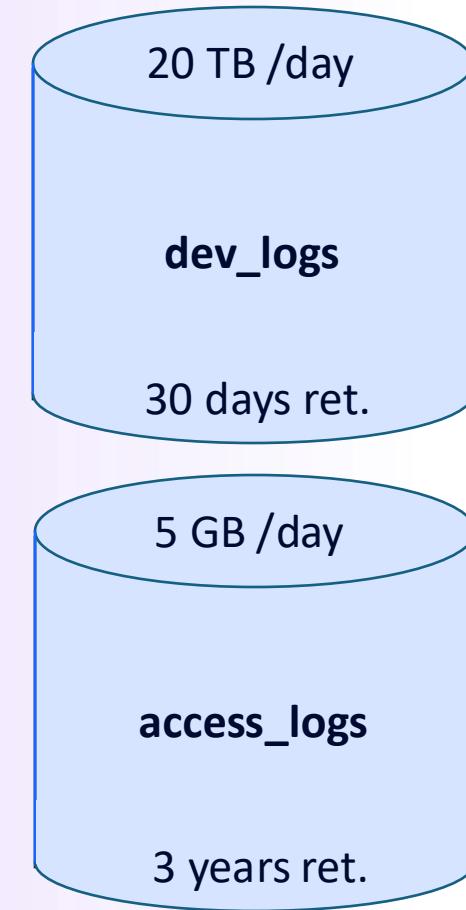
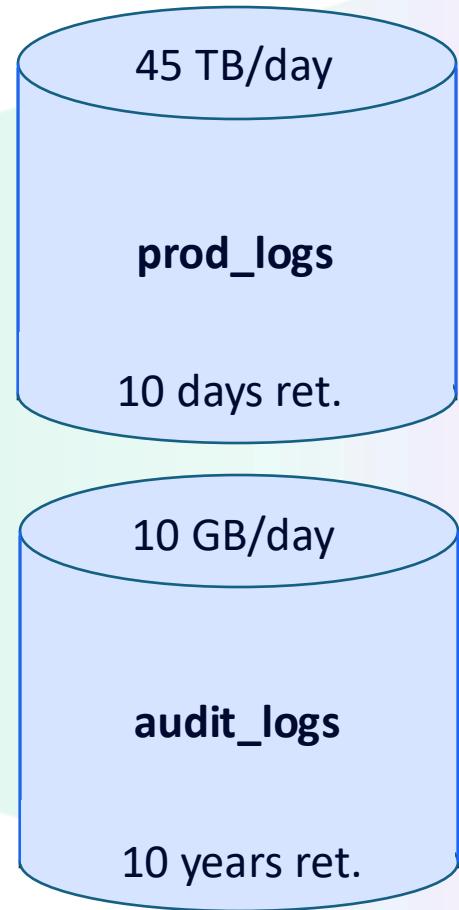
```
1 fetch logs
2 | filter matchesPhrase(content, "error")
```

# Bucket Query Strategy - Unoptimized

**DQL Query:**  
fetch logs

**IAM Policy:**  
ALLOW storage:logs:read

**Default Scan Limit:**  
500 GB

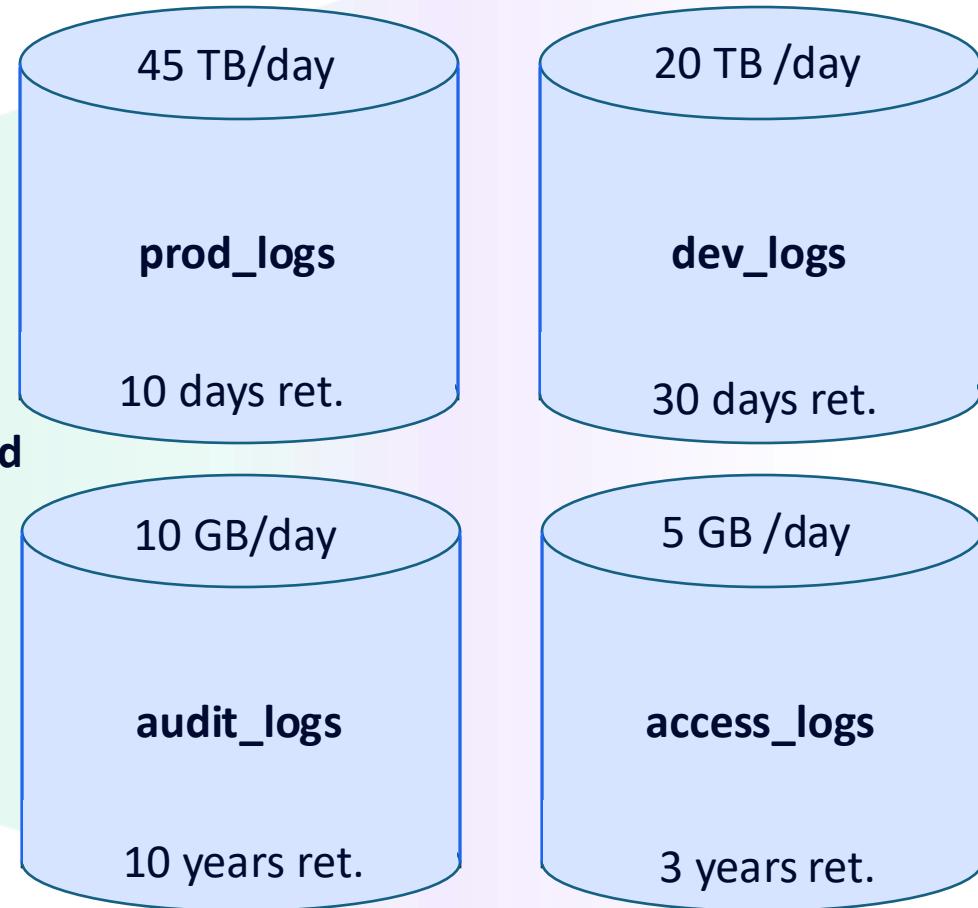


# Bucket Query Strategy - Unoptimized

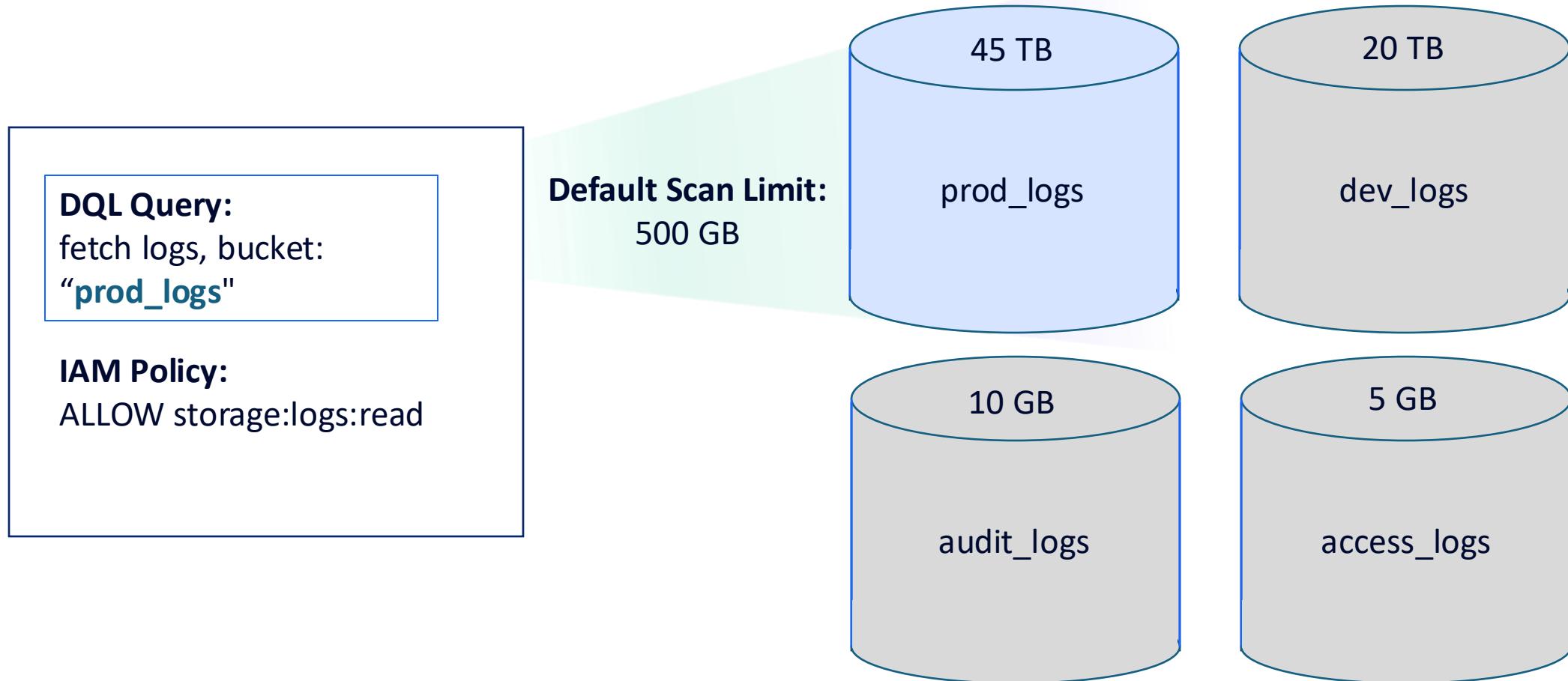
**DQL Query:**  
fetch logs,  
**scanlimitGBytes=-1**

**IAM Policy:**  
ALLOW storage:logs:read

Scan Limit uncapped  
result:  
**~80 TB**

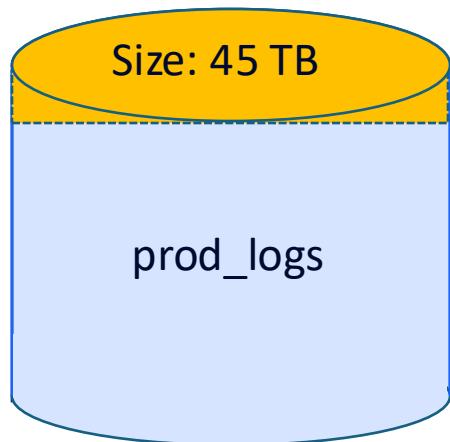


# Bucket Query Strategy – Filtered, but Unoptimized Bucket



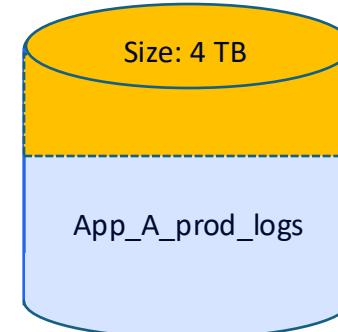
# Bucket Strategy – Why you should have one?

**Default Scan Limit:** 500 GB (0.5 TB)  
1.11% of 45 TB per Day = 0.5 TB

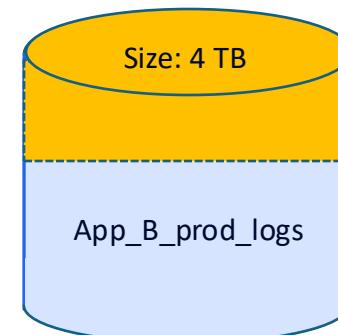
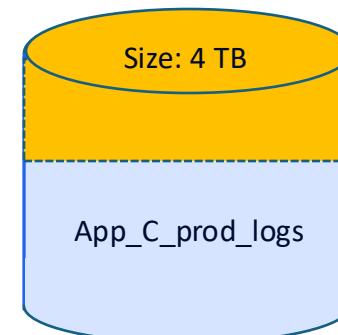


24h of retained logs

**0.5 TB scanned logs  
16 minutes (1.11%)**

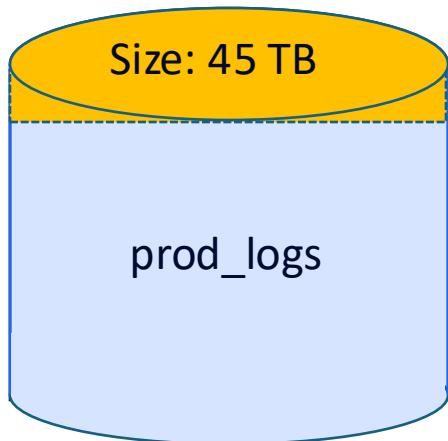


24h of retained logs  
**0.5 TB scanned logs  
3 hours (12.5%)**



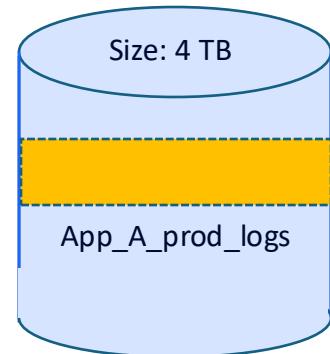
# Bucket Query Strategy – Optimize Your Query Window

**Default Scan Limit:** 500 GB (0.5 TB)  
fetch logs, bucket: “App\_x\_prod\_logs”,  
from: -6h, to:-4h



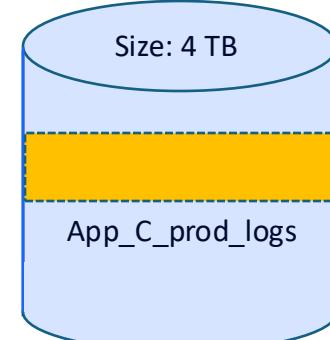
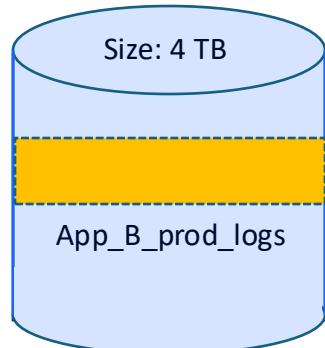
24h of retained logs

**0.5 TB scanned logs  
16 minutes (1.11%)**

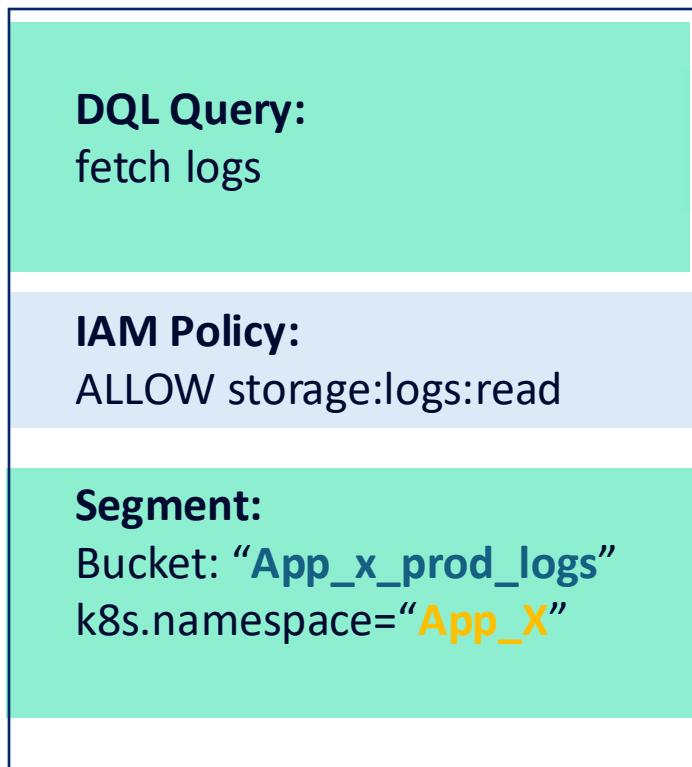


24h of retained logs

**0.33 TB scanned logs  
2 hours (8.3%)**



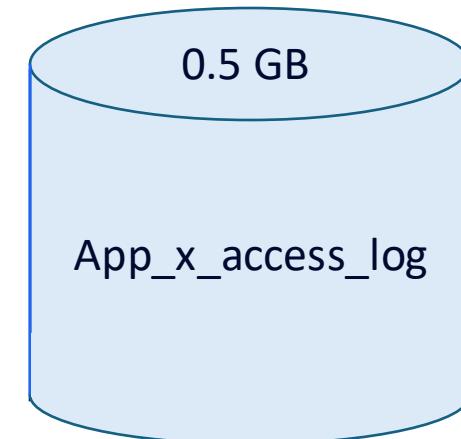
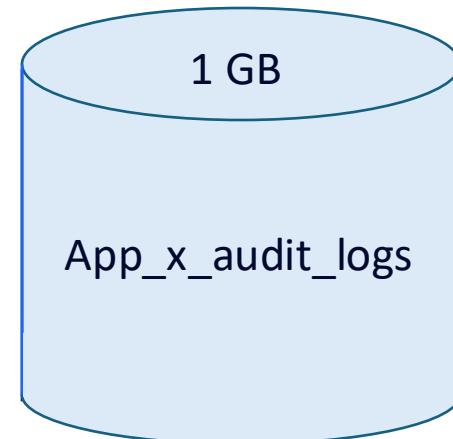
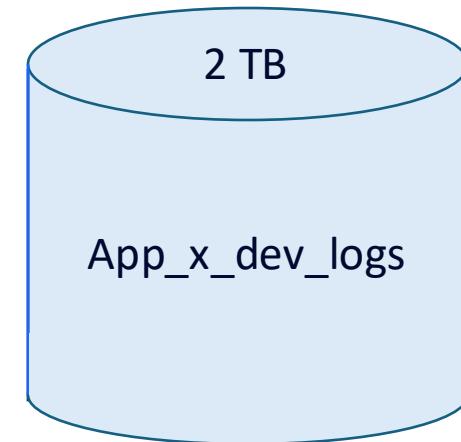
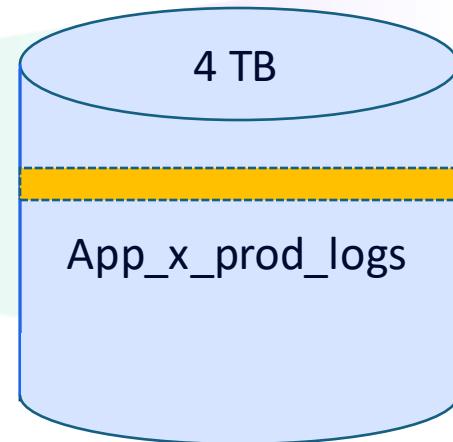
# Bucket Query Strategy – Filter using Segments



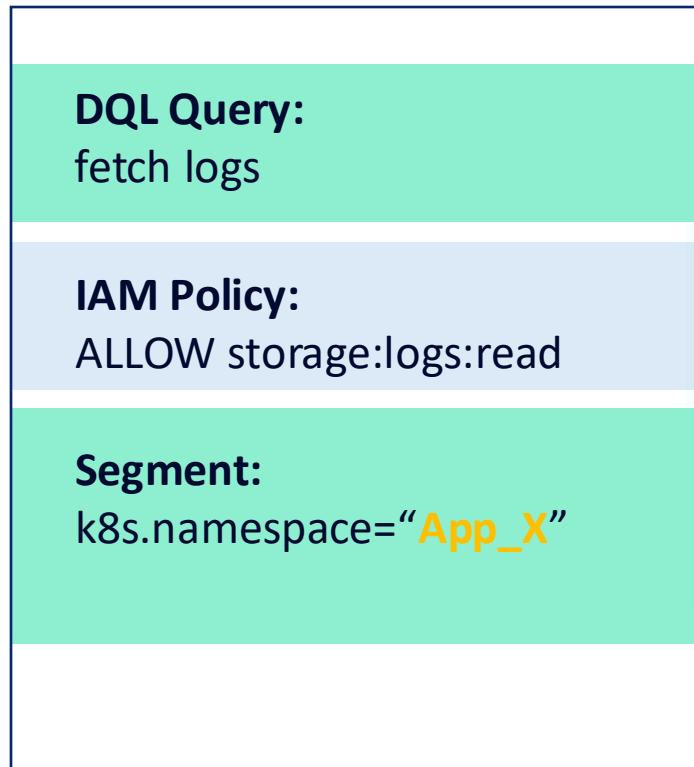
Filter: K8s App\_X

\* User or admin defined

Filtered  
on-demand  
by segment

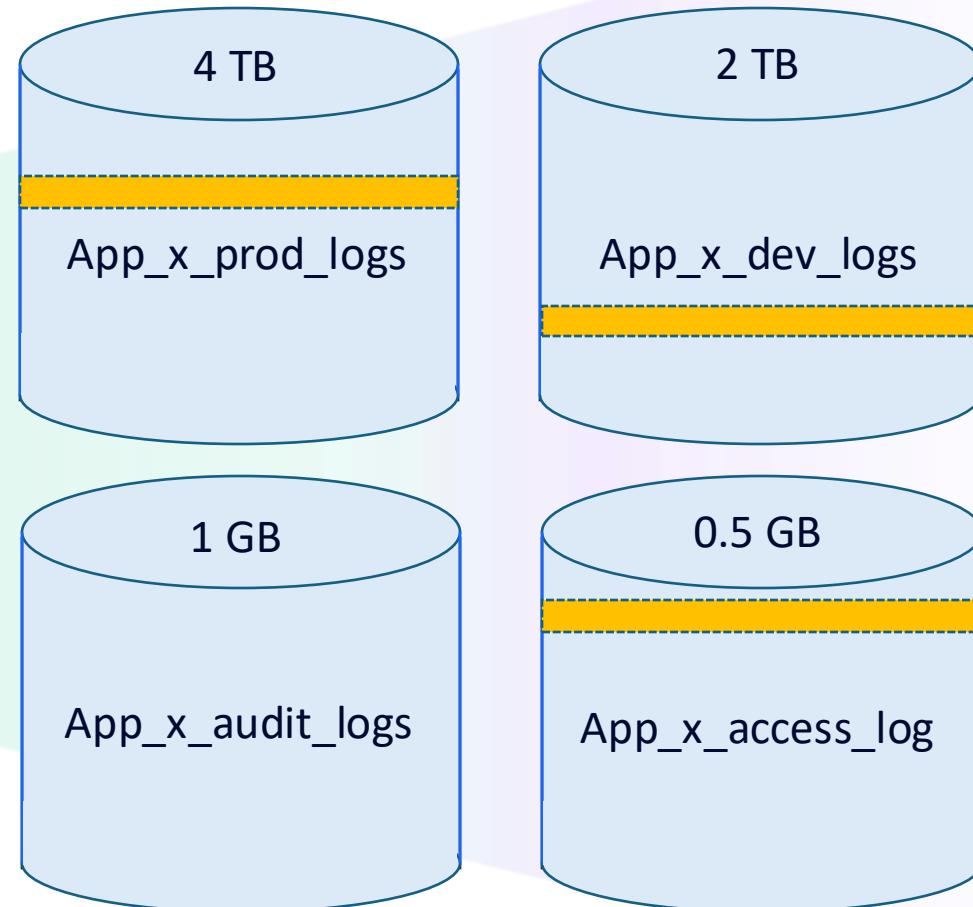


# Bucket Query Strategy – Filter using Segments

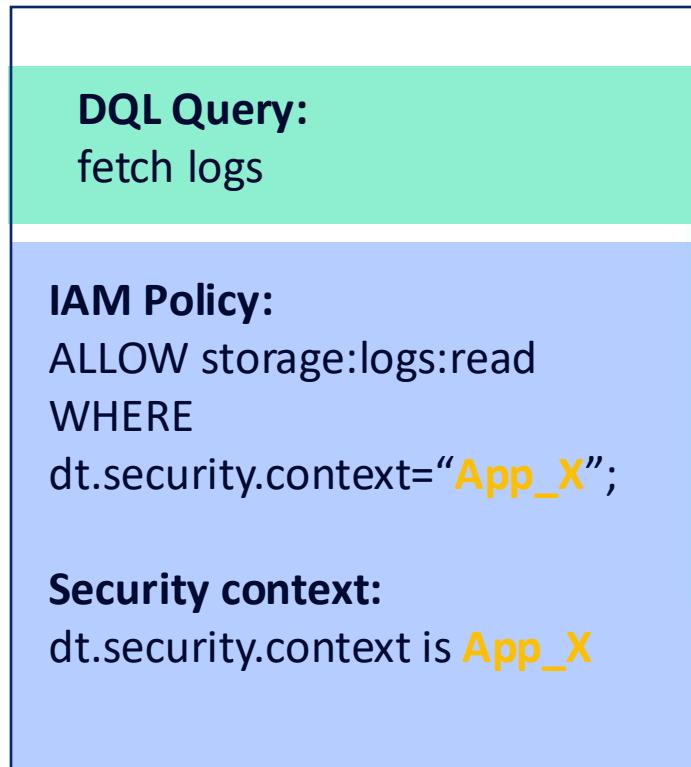


\* User or admin defined

Filtered  
on-demand  
by segment



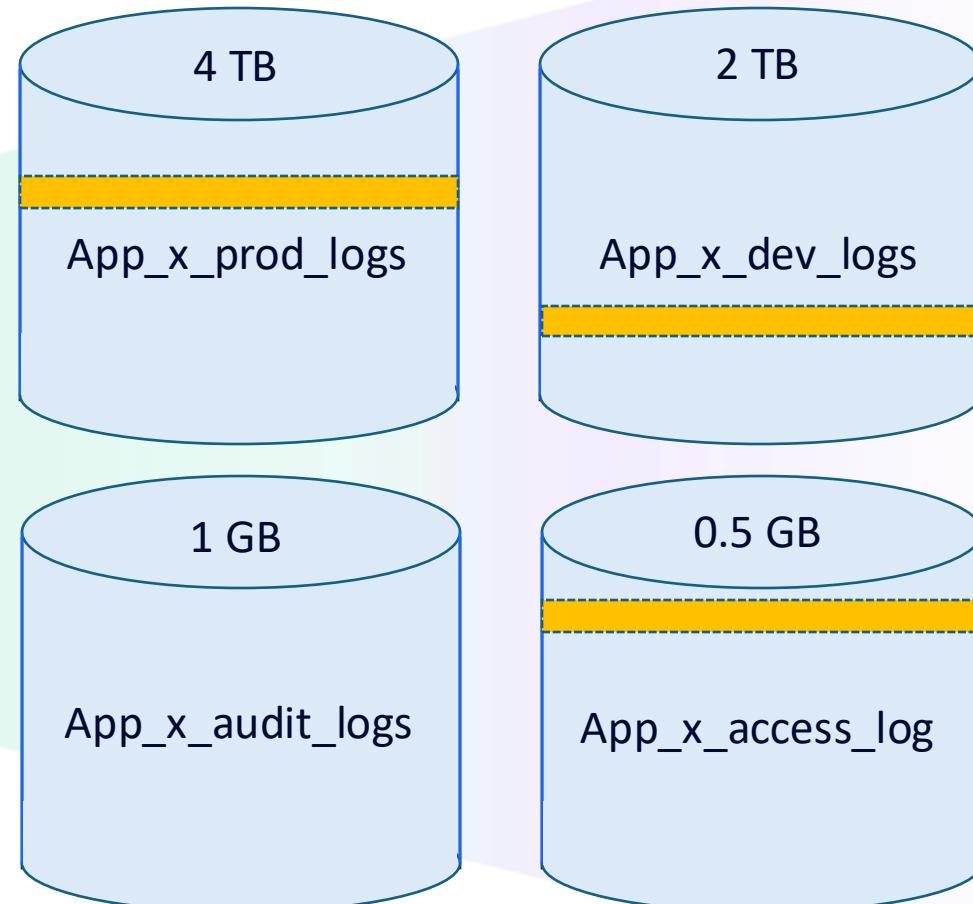
# Bucket Query Strategy – Limit using Security context



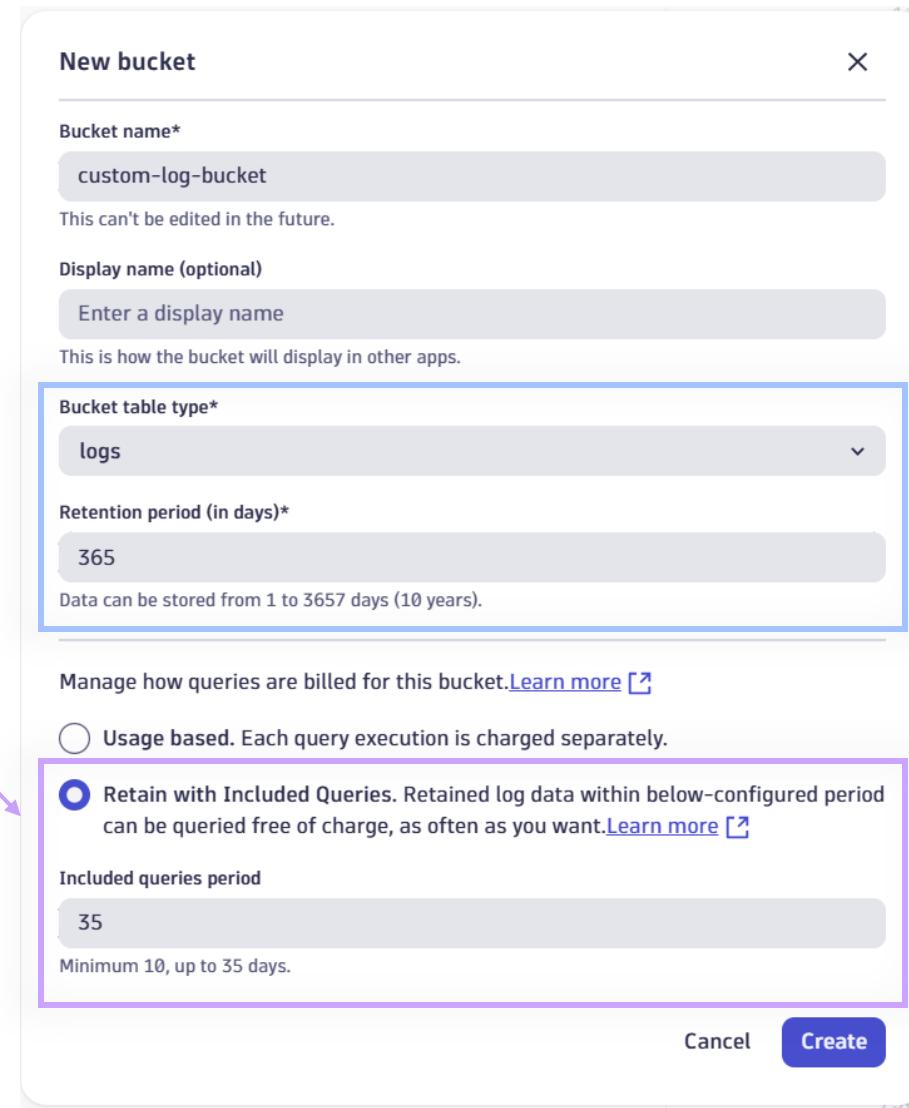
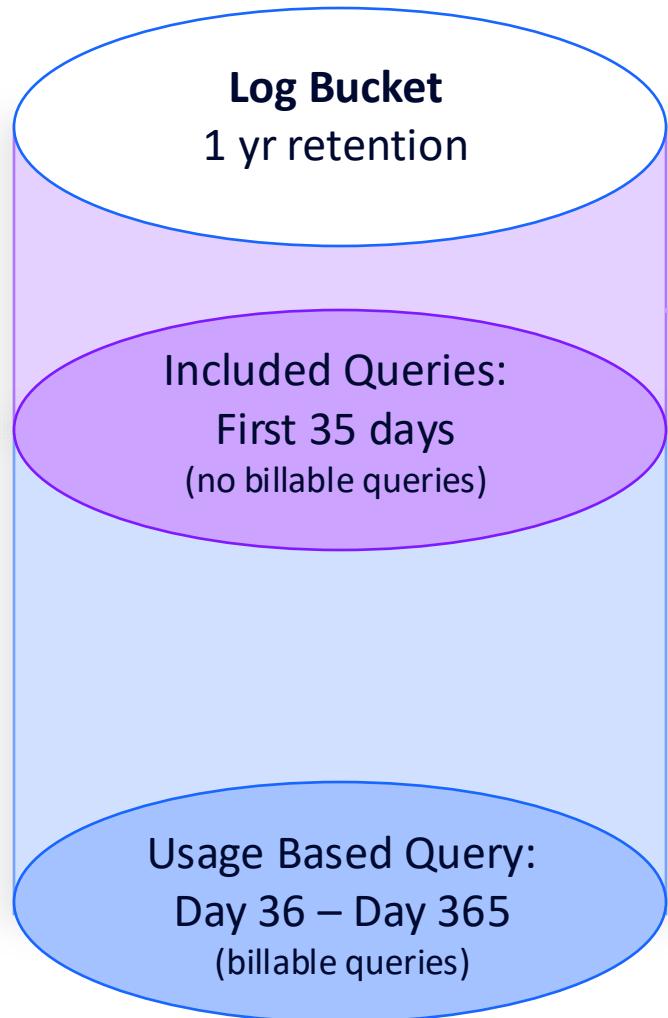
Filter: K8s App\_X

\* Admin defined

Limit access  
based on  
Security  
context



# Retain with Included Queries – Configuration Details



# 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
  - <provider>\_<type>\_<retention>
  - <provider>\_<bu>\_retention.
- Consider Business units or App Groupings
- Ingest of 1-2 TB per day is ideal.
- 80 bucket limit per tenant by default
  - Can be significantly increased based on ingest volume – contact support
  - More buckets = more setup / admin management – strike a balance
- Strategy can be replicated for other high volume data types such as BizEvents or spans.

# 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

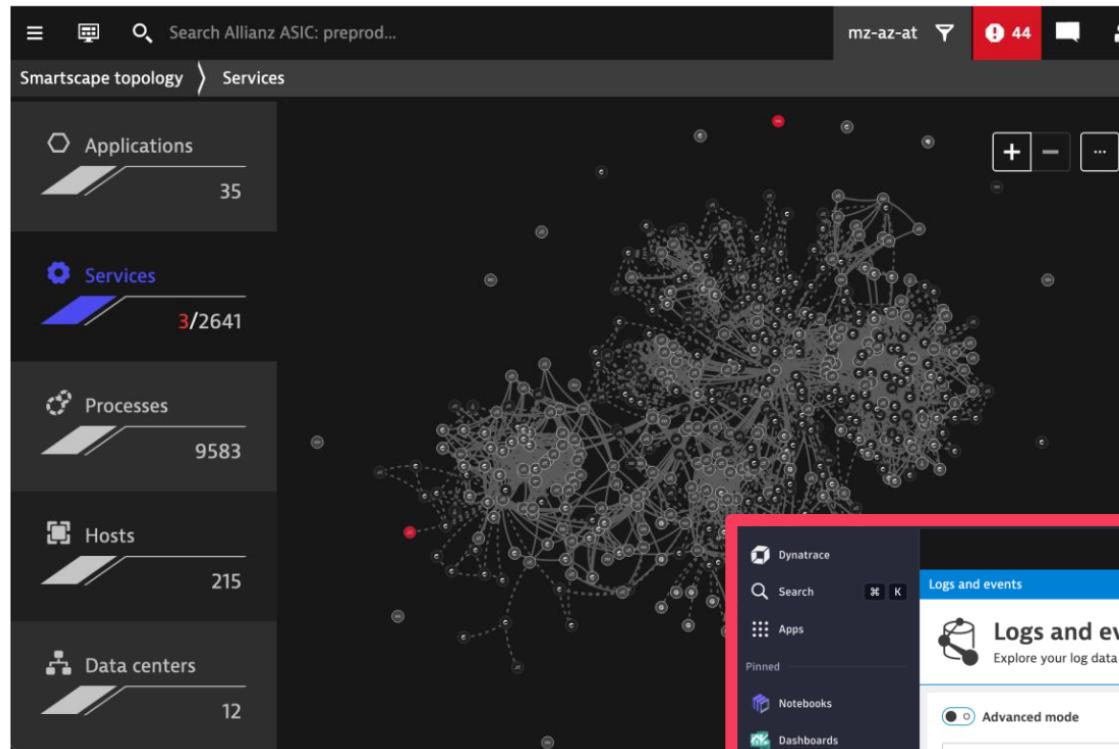
You can wait for it to become responsive or exit the page.

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

[Wait](#) [Exit page](#)

- 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

# 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 log search results table with the following columns: timestamp, status, and content. The table contains two rows of data:

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
2023-11-16 13:21:50.401	NONE	{"timestamp":"2023-11-16T12:21:45.191917656Z","message":"Update loop too

The left sidebar includes links to "Logs and events" (which is highlighted with a red border), "Search", "Apps", "Notebooks", "Dashboards", "Workflows", "Hub", "Dashboards classic", "Problems", "AWS", "Hosts", and "Logs and events".

# 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 set to "Cluster: CL-Prod20". To the right of the dropdown is a search bar labeled "Filter by:" and a "+ Add filter" button. A large green callout box with the text "1 click to block out all the noise" is positioned in the upper right area.

The main content area is titled "Clusters" and displays 12 records. It includes a summary bar at the top with metrics for Davis® AI Health status, Clusters (1 / 16), Nodes (4 / 456), Namespaces (137), Workloads (149 / 5.9k), and CPU usage. Below this is a table with columns: Cluster, Problems, Nodes, Namespaces, Workloads, Pods, CPU Usage, CPU Requests, and CPU. Each row shows data for a specific cluster, including numerical values and small bar charts for CPU usage and requests.

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

# Simple Segment

---



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

- Equivalent to single MZ

# Multiple Segments

2 segments ^

Segments

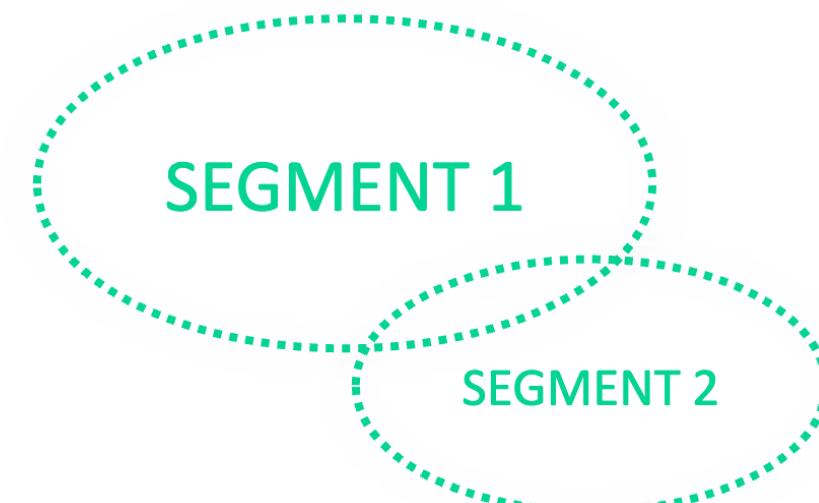
Region	▼	eu-ireland, eu-austria	▼	X
App-env	▼	production	▼	X

+ 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

# 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

Anyone in the environment

1 Visible to anyone or unlisted

### 3 Include data directly

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

### Metrics

k8s.namespace.name = \$namespace.name	Preview
---------------------------------------	---------

### 4 Include data of entities

Hosts	tags = team:ACE	Preview
-------	-----------------	---------

Include  Problems  Vulnerabilities  Metrics  Logs  Events  BizEvents  Spans

### 5 Include data of related entities

Services	runs_on = \$this.hosts	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

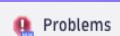
## 2 Additional filter for further problem analysis

K8s namespace (2) ▾ Type to filter Last 30 minutes ▾ < > Now Summary Refresh

Filter by segments K8s namespace astroshop, dynatrace X + Segment Clear all Apply

Recently used 1 Segments selector to set context K8s namespace: astroshop, dynatrace Learn more about segments

	State	Condition	Age	Pod warning signals	Containers	Container restarts	OOM events	Workload	Namespace
oneagent-4v...	Running	Ready	2 w 2 d	-	1/1	-	-	demo-aks-ger-westcentral-asc-o...	dynatrace
nlmmt	Running	Ready	1 w 3 d	-	4/4	-	-	dynatrace-oneagent-csi-driver	dynatrace
	Running	Ready	21 h 44 min	-	1/1	-	-	otel-collector	astroshop
	Running	Ready	2 w 2 d	-	1/1	-	-	eks-live-oneagent	dynatrace
StatefulSets	eks-live-oneagent-8kxlv	Running	Ready	2 w 2 d	1/1	-	-	eks-live-oneagent	dynatrace
ReplicaSets	dynatrace-webhook-959468759-c7wwg	Running	Ready	42 w 2 d	1/1	-	-	dynatrace-webhook	dynatrace
ReplicationControllers	dynatrace-webhook-687fffb45-65qpg	Running	Ready	45 w 1 d	1/1	-	-	dynatrace-webhook	dynatrace
Jobs	cart-5dc697bf66-qcwkg	Succeeded	Complet...	14 min 32 s	-	-	-	cart	astroshop
CronJobs	flagd-57475dc5fb-45ftn	Failed	Initialized	4 h 3 min	-	-	-	flagd	astroshop
Other workloads	product-catalog-f6fbcb555-hbvq8	Running	Ready	21 h 35 min	1/1	-	-	product-catalog	astroshop
Pods	load-generator-798cd5c5ff-jwmwl	Running	Ready	21 h 44 min	1/1	-	-	load-generator	astroshop
Services	dynatrace-webhook-645b69ff4f-gd5l4	Running	Ready	21 h 35 min	1/1	-	-	dynatrace-webhook	dynatrace
Containers	dynatrace-operator-845598f6dd-f5465	Running	Ready	1 w 3 d	1/1	-	-	dynatrace-operator	dynatrace
	ad-796688b769-5j5pq	Running	Ready	21 h 35 min	1/1	-	-	ad	astroshop
	extensions-live-oneagent-vp7zg	Running	Ready	2 w 2 d	1/1	-	-	extensions-live-oneagent	dynatrace
	dynatrace-oneagent-csi-driver-qv6mk	Running	Ready	42 w 2 d	4/4	-	-	dynatrace-oneagent-csi-driver	dynatrace
	dynatrace-oneagent-csi-driver-nddt4	Running	Ready	45 w 1 d	4/4	-	-	dynatrace-oneagent-csi-driver	dynatrace
	payment-5589f9659f-2v8vv	Running	Ready	21 h 35 min	1/1	-	-	payment	astroshop
	currency-78c89b7596-tv5sn	Running	Ready	21 h 35 min	1/1	-	-	currency	astroshop
	flagd-57475dc5fb-hqlcw	Failed	Initialized	29 min 58 s	-	-	-	flagd	astroshop
	dynatrace-webhook-5c69565bd9-6fkvk	Running	Ready	34 w	1/1	-	-	dynatrace-webhook	dynatrace
	dynatrace-oneagent-csi-driver-v7fqx	Running	Ready	1 w 3 d	4/4	-	-	dynatrace-oneagent-csi-driver	dynatrace
	ocp-demo1-oneagent-54rj5	Running	Ready	2 w 2 d	1/1	-	-	ocp-demo1-oneagent	dynatrace
	extensions-live-oneagent-pldc7	Running	Ready	2 w 2 d	1/1	-	-	extensions-live-oneagent	dynatrace
	quote-857f7bf674-6llsh	Running	Ready	21 h 44 min	1/1	-	-	quote	astroshop
	fraud-detection-66dbd5b789-ljbmr	Running	Ready	21 h 44 min	1/1	-	-	fraud-detection	astroshop
	gke-live-oneagent-cmxc8	Failed	Initialized	3 min 44 s	-	-	-	gke-live-oneagent	dynatrace
	extensions-live-oneagent-26wc4	Running	Ready	2 w 2 d	1/1	-	-	extensions-live-oneagent	dynatrace
	extensions-live-oneagent-7pq9c	Running	Ready	2 w 2 d	1/1	-	-	extensions-live-oneagent	dynatrace



Problems

?

Default filter



Problems ◇ 1 active / 3

## 3 Additional filter for further problem analysis

Last 24 hours



refreshed 1 min. ago

Status



All



Active



Closed

2

Category



Availability



Error



Slowdown



Resource contention



Custom alert



Monitoring unavailable

Filter by segments

K8s namespace

easytrade-live-debugger



+ Segment

Clear all

Apply

Recently used

K8s namespace: astroshop, dynatrace



Learn more about segments

## 1 Segments selector to set context

09 PM

Sep 26

03 AM

06 AM

09 AM

12 PM

26 columns hidden



ID	Name	Status	Category	Affected	Root cause	Started	Duration
P-25095682	Failure rate increase	Active	Error	2	[eks-live][easytra...	Sep 26, 2025, 8:43 AM	4 h 53 min
P-25095586	Failure rate increase	Closed	Error	2	[eks-live][easytra...	Sep 26, 2025, 12:32 AM	7 h 46 min
P-25095362	Failure rate increase	Closed	Error	3	[eks-live][easytra...	Sep 25, 2025, 12:32 AM	23 h 34 min

# Permissions

# Permissions



## 1. Bucket and table access

### Basic functionality

- Organize records in buckets and table
- Control access per table and per bucket
- Optimized for query performance



## 2. Record-level security

### Record filtering

- Filter out records based on known fields
- Optimized for query performance



## 3. Field-level security

### Data masking

- Filter out fields that contain sensitive data by default
- Admin can access sensitive fields
- Optimized for query performance

Policy name\*

Generic Log Viewer

Policy description

Description

Policy statement\*

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

Policy name\*

Hipster App Team Logs

Policy description

Description

Policy statement\*

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

Policy name\*

Logs Sensitive FieldSet Viewer

Policy description

Allows user groups with this policy to view sensitive fieldsets. Specifically the fieldset 'sensitive-fields-logs'

Policy statement\*

```
1 ALLOW storage:fieldsets:read WHERE storage:fieldset-
   name="sensitive-fields-logs";
```

# Record/Field-level security brings fine-grained access controls

- Allows customer to create access policies on record or field level in Grail

## Bucket: audit

Retention: 7y

*"All audit logs"*



I needs access to my business unit's infra logs, security events and debug data

## Bucket: infra

Retention: 3mo

*"Business unit X infra logs"*

timestamp

content

...

timestamp

content

...

timestamp

content

...



Makes sure the Dynatrace monitoring components are deployed, updated and working fine.

## Bucket: debug

Retention: 10d

*"All debug logs"*



When developing or troubleshooting services, I need to monitor performance and regression

# How do we set record-level permissions?

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

## storage:logs:read

Grants permission to read records from the logs-table

### conditions:

- storage:bucket-name - This condition reduces the effect of the record-level permission to a defined list of buckets.  
operators: =, !=, IN, NOT IN, startsWith, NOT startsWith
- storage:k8s.namespace.name - The name of the namespace that the pod is running in.  
operators: =, IN, startsWith
- storage:k8s.cluster.name - The name of the cluster that the pod is running in.  
operators: =, IN, startsWith
- storage:host.name - Name of the host.  
operators: =, IN, startsWith
- storage:dt.host\_group.id - Id of the host group.  
operators: =, IN, startsWith
- storage:log.source - The location where the log comes from.  
operators: =, IN, startsWith
- storage:dt.security\_context - Custom field for security context.  
operators: =, IN, startsWith
- storage:gcp.project.id - Google Cloud Platform Project ID.  
operators: =, IN, startsWith
- storage:aws.account.id - Amazon Web Services Account ID.  
operators: =, IN, startsWith
- storage:azure.subscription - Azure subscription.  
operators: =, IN, startsWith
- storage:azure.resource.group - Azure resource group.  
operators: =, IN, startsWith

# How do we set field-level permissions?

## Field permissions

1 Request URL

```
1 POST https://myapps.mydomain.com/platform/storage/fieldsets/v1/fieldsets
```

2 Request body

```
1 {
2   "name": "sensitive-fields-retail",
3   "description": "Sensitive fields retail",
4   "enabled": true,
5   "scope": "BUCKET",
6   "fields": [
7     "credit_card",
8     "DOB"
9   ],
10  "buckets": [
11    "logs_retail"
12  ]
13 }
```

To unmask the `credit_card` and `DOB` fields, you need the following permission:

```
1 ALLOW storage:fieldsets:read WHERE storage:fieldset-name="sensitive-fields-retail"
```

# Discussion Question

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

# Discussion Question

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

Query Performance

Cost efficient storage and query

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 the Metric Extraction interface with two defined metrics:

- getCart**: Counter metric ID: processor\_getCart\_3570. It has a matching condition of "1 matchesPhrase(content, "GetCartAsync")". The Metric key is set to "log.getCart". A red arrow points to this field.
- Revenue**: Value metric ID: processor\_Revenue\_6652. It has a matching condition of "1 matchesPhrase(k8s.deployment.name, "paymentservice-\*") and matchesPhrase(Message, "Transaction processed:")". The Field extraction is "Amount", and the Metric key is "log.revenue". A red arrow points to this field.



# Log to Events

An event can be either Davis or Business event:



## Davis Event

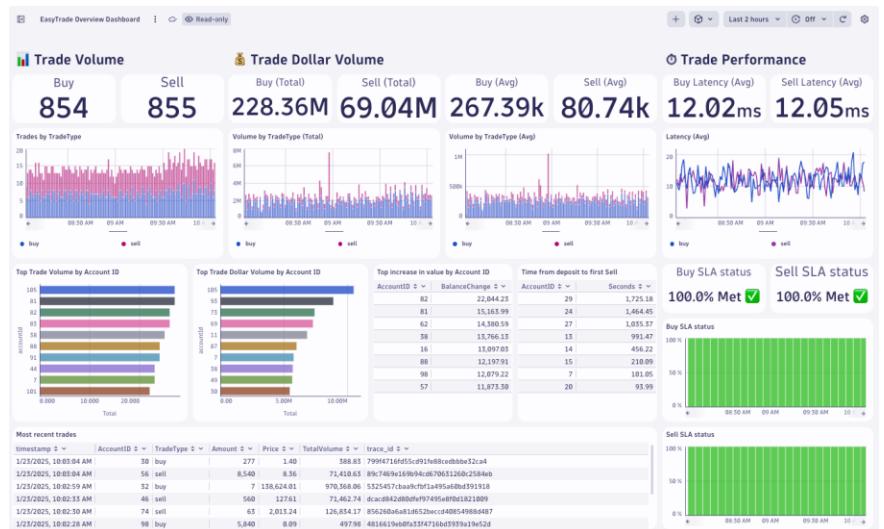
- Does this anomaly need to be reported?
- Is it an INFO Event that needs to be generated?



## 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-25013785 - High CPU throttling	unguard-user-simulator	1/27/2025, 5:59:00 PM	In Progress	5.67 d
OPEN	P-25015157 - Job failure event	pvc-out-of-space-kaniko-big-image-push	1/22/2025, 5:01:00 PM	1/27/2025, 8:16:00 PM	9.06 h
CLOSED	P-25015026 - Job failure event	pvc-out-of-space-kaniko-big-image-push	1/22/2025, 5:01:00 PM	1/27/2025, 8:16:00 PM	3.25 h
CLOSED	P-25014994 - Job failure event	pvc-out-of-space-kaniko-big-image-push	1/22/2025, 12:46:00 PM	1/27/2025, 5:01:00 PM	4.25 h
CLOSED	P-25014950 - Job failure event	pvc-out-of-space-kaniko-big-image-push	1/22/2025, 7:01:00 AM	1/27/2025, 12:46:00 PM	5.75 h
CLOSED	P-25015101 - Out-of-memory kills	paymentservice	1/22/2025, 10:22:00 PM	1/27/2025, 10:37:00 PM	15.00 min
CLOSED	P-25015021 - Memory usage close to limits	paymentservice	1/22/2025, 4:52:00 PM	1/27/2025, 10:36:00 PM	5.73 h
CLOSED	P-25014976 - Memory usage close to limits	manager	1/22/2025, 9:45:00 AM	1/27/2025, 10:47:00 AM	1.03 h
OPEN	P-25015212 - Not all pods ready	mail-service	1/23/2025, 9:30:00 AM	In Progress	34.58 min
CLOSED	P-25015211 - Pods stuck in pending	mail-service	1/23/2025, 9:10:00 AM	1/23/2025, 9:55:00 AM	45.00 min
CLOSED	P-25014971 - Not all pods ready	mail-service	1/22/2025, 9:30:00 AM	1/27/2025, 10:20:00 AM	50.00 min
CLOSED	P-25015175 - Container restarts	ingress-dev-controller	1/23/2025, 5:04:00 AM	1/23/2025, 5:20:00 AM	16.00 min





# Dashboarding

- Spot the differences between these two dashboards?



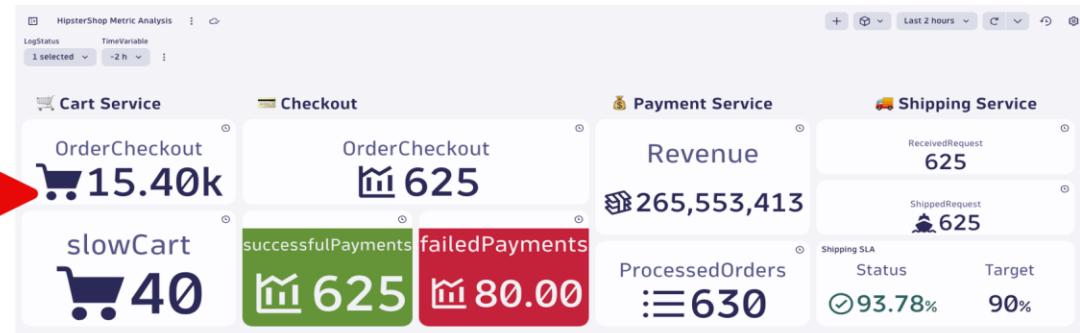
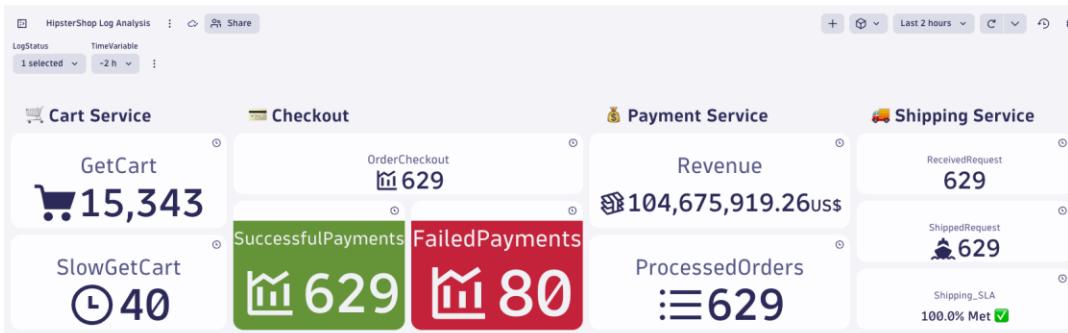
## Use logs when:

- 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 shows the Grafana interface for creating an alert. On the left, there's a sidebar with navigation links like 'Metrics', 'Logs', 'Dashboards', etc. The main area is titled 'Edit anomaly detector'.

**Anomaly Detector Configuration:**

- 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
```
- Actor:** Rohan Shah (selected)
- Customize parameters:** Set thresholds and alerts.
- Create an event template:** Set event description and properties.

**Event Template Configuration:**

- 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

**Anomaly detection:** A dropdown menu is open, showing three options: 'Auto adaptive threshold anomaly detection' (selected), 'Seasonal baseline anomaly detection', and 'Static threshold anomaly detection'. This menu is highlighted with a red box.

**Bottom Navigation:** Buttons for 'Create an event template', 'Learn more', 'Save', and 'Discard'.

**Thank you!**