Glossary

 docs.datadoghq.com/glossary

Welcome to our Glossary! This is a work in progress and we are actively building up a complete term list, which will take time. If you have feedback about how this glossary works, or terms you'd like to see defined, please click **Feedback** and let us know.

A

action

In Datadog RUM, an action is a type of event. Action events track user interactions during a user journey.

administrative status

Synonyms: admin status

The administrative status of a port (up/down) refers to whether the port is disabled.

Agent

Synonyms: Datadog Agent

The Datadog Agent is an open source software that runs on a host. It collects metrics and events from the host and sends them to Datadog. It can run on your local hosts (Windows, macOS), containerized environments (Docker, Kubernetes), and in on-premises data centers. For more information, see the documentation.

alert

Datadog monitors generate alerts, indicating that a set condition has been reached.

Amazon Elastic Container Service (ECS)

ECS is a container orchestration service.

Amazon Elastic Kubernetes Service (EKS)

EKS is a managed Kubernetes service.

Amazon Resource Name (ARN)

An ARN is a string that uniquely identifies an AWS resource. See the AWS documentation for more information.

analytics

Log analytics is the process of querying, grouping, and visualizing logs for investigation and exploration.

Annotation

In Kubernetes, annotations are key/value maps that can be used to attach metadata to Kubernetes objects.

API key

An API key is a token used to authenticate a user or an application. The Datadog Agent requires an API key to submit metrics and events to Datadog.

api test

Related terms: multistep api test
In Datadog Synthetic Monitoring, an API test allows you to launch requests through individual network protocols. For more information, see the documentation.

APM

Synonyms: Tracing, Distributed Tracing

Application Performance Monitoring (APM) monitors requests, errors, and latency in your application. Add distributed traces throughout your application to correlate to browser sessions, logs, profiles, synthetic checks, network, processes, and infrastructure metrics across your hosts, containers, proxies, and server less functions.

For more information about APM, see the APM documentation.

archive

An archive is a long-term cloud storage solution to store logs, whether they are indexed or not, for longer periods.

attribute

An attribute is a piece of information about a log.

Autodiscovery

In Datadog, Autodiscovery is a feature that automatically identifies the services running on containers. This enables you to define configuration templates for Agent checks and specify which containers each check should apply.

AWS Fargate

Synonyms: Fargate

AWS Fargate is a serverless compute engine.

Azure Kubernetes Service (AKS)

AKS is a managed Kubernetes service.

B

browser test

Related terms: mobile app test
In Datadog Synthetic Monitoring, a browser test monitors web business transactions or web user journeys. A single test may involve several actions and pages to verify that users can successfully complete processes such as signing up for an account and checking out. For more information, see the documentation.

C

cardinality

In Datadog, cardinality is the number of tag values associated with a tag key for a metric.

Center for Internet Security (CIS)

The CIS is an organization that maintains CIS Controls and CIS Benchmarks, which are recommendations and guidelines for best security practices.

Check

Checks are small Python programs run periodically by the Agent. A Check performs an action and then gathers the result, which the Agent then stores and reports to the Datadog platform. These programs are freeform and are generally used to collect metrics from custom environments or applications. Note that the word “check” - when not capitalized - refers to the generic act of taking a measurement.

child org

A child org belongs to a parent org and maintains its own data separate from the parent org and other child orgs.

Cluster Agent

The Cluster Agent is a version of the Datadog Agent that provides a streamlined, centralized approach to collecting cluster-level monitoring data.

cold start

In computing, a cold start refers to when a system or component was recently created or restarted. In serverless computing, a cold start refers specifically to the problems (such as increased latency) that may arise when a function is invoked for the first time or after an idle period.

collector

The collector is the Agent process that runs checks on the machine and collects metrics. For more information, see the documentation.

ConfigMap

A ConfigMap is an API object that stores data in key-value pairs. ConfigMaps can be supplied to Pods as environment variables, command-line arguments, or configuration files in a volume.

Container Agent

The Container Agent is the version of the Datadog Agent that runs on a containerized environment.

container runtime

A container runtime is the part of a container engine that mounts the container and stops/starts containerization.

Container Runtime Interface (CRI)

The CRI interface allows a kubelet to use different container runtimes.

containerd

Containerd is a container runtime.

control

A specific recommendation for how technology, people, and processes should be managed. A control is typically based on a regulation or industry standard.

Core Web Vitals

Core Web Vitals are a set of metrics that Google has identified as meaningful signals for UX testing. These metrics concern how long it takes for a page to load, how long it takes for a user to interact, how stable a page is as it loads, and more. For more information, see the documentation.

count

“Count” is a metric type that adds up all the submitted values in a time interval. For more information, see the documentation.

crawler delay

A crawler delay is a delay in metrics for Datadog cloud integrations due to constraints with the cloud provider API. For more information, see the documentation.

cross-site request forgery (CSRF)

Synonyms: XSRF

CSRF is a type of exploit where an attacker uses a web client, such as a browser, to access or manipulate information.

D

DaemonSet

In Kubernetes, a DaemonSet is a controller that manages groups of Pods. You can describe a DaemonSet in a YAML file.

datadog.yaml

The `datadog.yaml` is the main Agent configuration file for enabling and disabling different features. For more information, see the documentation.

delay

An evaluation delay tells the monitor to wait a specified number of seconds before it begins evaluation. For more information, see the Advanced alert conditions.

distributed tracing

Distributed tracing is a method of tracking application requests as they flow from frontend devices to backend services and databases. Developers can use distributed tracing to troubleshoot requests that exhibit high latency or errors.

distribution

A distribution is a metric type that aggregates values sent from multiple hosts during a flush interval. For more information, see the documentation.

Docker

Docker is a framework for managing containers.

DogStatsD

DogStatsD refers to two related things: a protocol based on StatsD, and an application for reporting metrics which implements that protocol. The DogStatsD protocol is an extension of the StatsD protocol, with some modifications that are specific to the Datadog platform. The DogStatsD application is a service that is bundled with the Agent, and is used as a lightweight mechanism for reporting metrics.

See the DogStatsD documentation for more information.

downtime

Downtimes are scheduled periods during which monitors' alerts and notifications are silenced. For more information, see the documentation.

dynamic application security testing (DAST)

DAST is a security testing methodology that analyzes a running application without looking at its source code.

E

eBPF

eBPF is a Linux kernel technology that allows users to run bytecode without changing the kernel or adding kernel modules.

enhanced metric

Synonyms: enhanced Lambda metric

Datadog generates a set of enhanced Lambda metrics from your Lambda runtime. These are in addition to the default Lambda metrics provided by the AWS Lambda integration. Enhanced Lambda metrics are prepended with `aws.lambda.enhanced.*`.

error

In Datadog RUM, an error is a type of event. An error event is generated when the browser emits a frontend error.

evaluation window

The evaluation window is the look back timeframe of the data that the monitor aggregates and uses to compare against the defined thresholds. For more information, see the documentation.

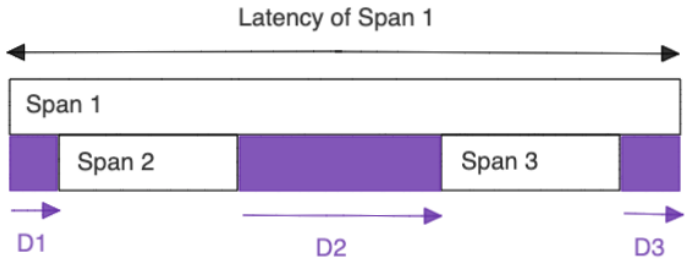
exclusion filter

An exclusion filter determines which logs should not be indexed. These logs still show in Live Tail.

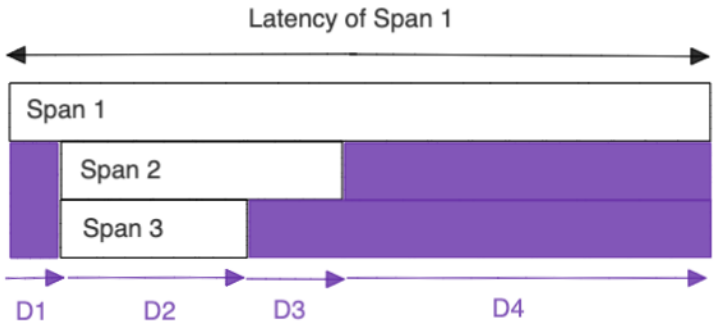
execution time

In APM, execution time is the total time that a span is considered active, or not waiting for a child span to complete.

Execution time is calculated by adding up the time that a span is active, meaning it has no child spans. For non-concurrent work, this is straightforward. In the following image, the execution time for Span 1 is D1+D2+D3. The execution time for Spans 2 and 3 are their respective widths.



When child spans are concurrent, execution time is calculated by dividing the overlapping time by the number of concurrently active spans. In the following image, Spans 2 and 3 are concurrent (both are children of Span 1), overlapping for the duration of Span 3, so the execution time of Span 2 is D2÷2+D3, and the execution time of Span 3 is D2÷2.



explorer

Events Explorer is a page in Datadog where you can view and aggregate events. Events Explorer displays the most recent events generated by the user's infrastructure and services, such as code deployments, service health, configuration changes, or monitoring alerts. For more information, see the Events Explorer documentation.

Trace Explorer is a page in Datadog where you can view and create analytics on 100% of ingested traces for 15 minutes, and all indexed spans for 15 days.

F

facet

A facet is a user-defined tag or attribute of indexed logs. It can be quantitative or qualitative and is used in Log Explorer to search logs, define log patterns, and perform log analytics.

faceted search

A faceted search uses filters to narrow down search results.

finding

A finding is the primary primitive for a rule evaluation against a resource. Every time a resource is evaluated against a rule, a finding is generated with a **pass** or **fail** status.

flaky test

A flaky test is a test that exhibits both a passing and failing status across multiple test runs for the same commit. If you commit some code and run it through CI, and a test fails, and you run it through CI again and the test passes, that test is unreliable as proof of quality code. For more information, see the documentation.

flame graph

A flame graph is a visualization of a trace, where bars represent spans and show the span's execution time as well as what called it and what calls it made. Flame graphs are also used to represent profiles.

flare

The `flare` command is a quick way to send troubleshooting information to the Datadog support team. `flare` gathers all of the Agent's configuration files and logs into an archive file, removes sensitive information like passwords, and then sends the archive file to Datadog support.

flow

In computer networks, a flow is the path taken when one endpoint communicates with another. Datadog's network map provides a visualization for network data flow. For more information, see the documentation.

forecast

Forecasts use algorithms to predict the future behavior and values of a metric.

forwarder (Agent)

The forwarder is the Agent process that sends metrics over HTTPS to Dataodog. For more information, see the documentation.

framework

Synonyms: compliance framework, compliance standard, compliance benchmark

A collection of requirements that map to an industry benchmark or regulatory standard.

function

In serverless computing, a function is a programmatic function hosted on managed infrastructure.

funnel analysis

Funnel analysis analyzes a user's journey towards a defined outcome, such as signup or purchase. Funnel analysis looks at the sequence of events along this journey.

G

gauge

Gauge is a metric type that takes the last value reported during the interval. For more information, see the documentation.

global variable

In Datadog Synthetic Monitoring, a global variable is a variable that is accessible from all of a user's Synthetic tests. For more information, see the documentation.

Google Kubernetes Engine (GKE)

GKE is a managed Kubernetes service.

granularity

Granularity is the frequency at which data is collected or displayed on graphs. For more information, see the documentation.

grok

Grok is a method for parsing and extracting attributes from semi-structured log messages.

H

Helm

Helm is a tool for managing pre-configured Kubernetes resources.

histogram

A histogram reports five different values that summarize the submitted values: the average, count, median, 95th percentile, and max. For more information, see the documentation.

HorizontalPodAutoscaler (HPA)

In Kubernetes, an HPA automatically deploys more Pods to meet demand.

host

A host is a computer or a virtual machine.

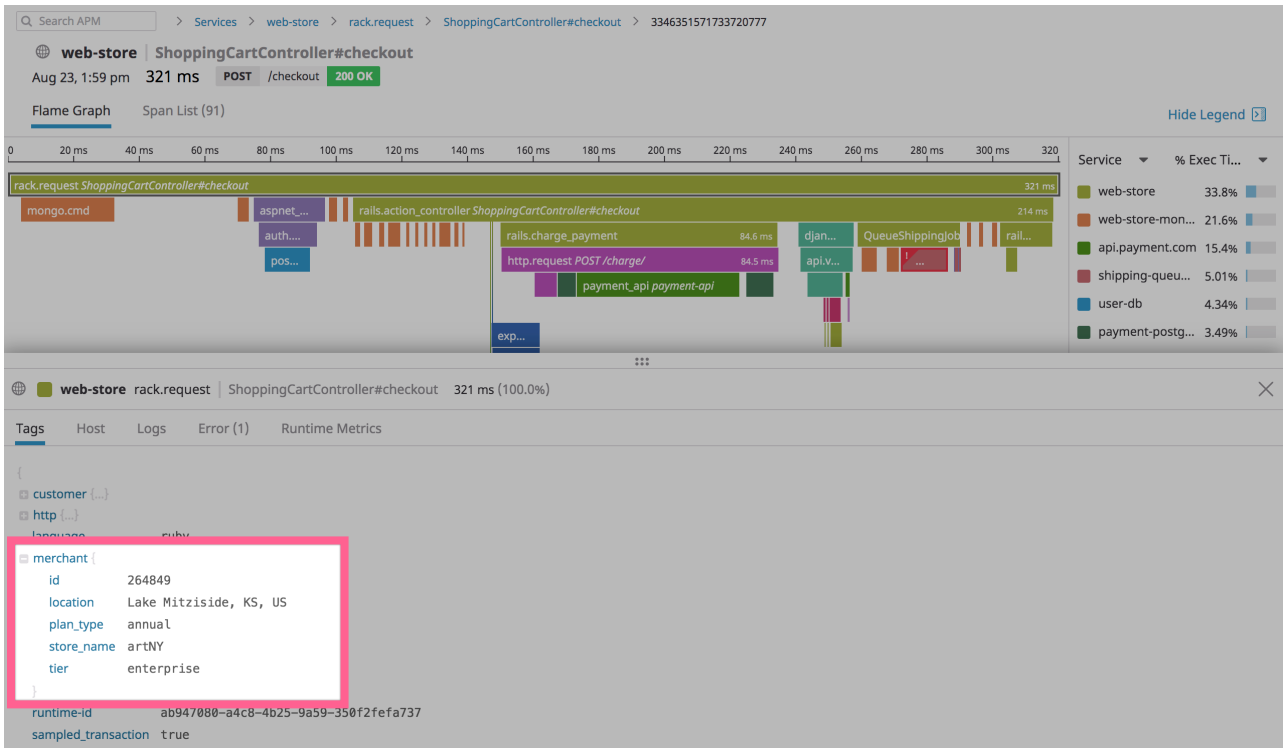
I

indexed

Indexed logs are logs that have been collected, processed, and retained for analysis, alerting, and troubleshooting.

Indexed spans represent spans indexed by a retention filter stored in Datadog for 15 days that can be used to search, query, and monitor in Search Spans by the tags included on the span.

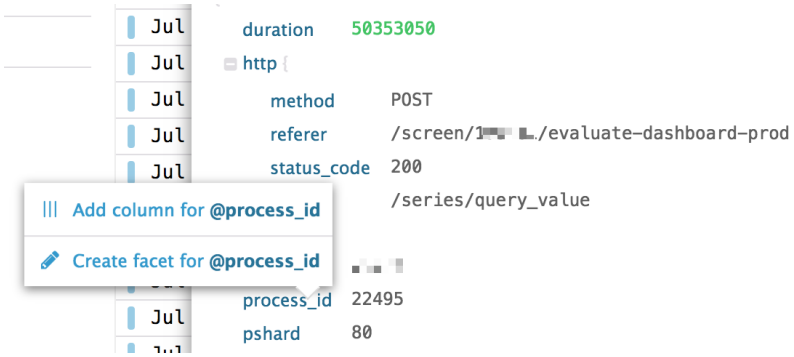
Creating tag-based retention filters after ingestion allows you to control and visualize exactly how many spans are being indexed per service.



In this example, the requests (`merchant.store_name` and `merchant.tier`) have been added as tags to the span.

To get started with tagging spans in your application, see the Adding span tags guide.

After a tag has been added to a span, search and query on the tag in Analytics by clicking on the tag to add it as a facet. Once this is done, the value of this tag is stored for all new traces and can be used in the search bar, facet panel, and trace graph query.



ingested

Ingested logs and spans are all logs and spans collected throughout your environment.

ingestion control

Ingestion control refers to the mechanisms and rules in the Agent and in tracing libraries for determining what traces are sent from an application to Datadog.

Intelligent Retention Filter

A Datadog default retention filter that is always active, keeping a representative proportion of traces, true high latency, and diverse error traces to help you monitor the health of your applications. It is not random, and so traces only retained by Intelligent Retention are not included in trace metrics.

interactive application security testing (IAST)

IAST is a security testing methodology that combines static and dynamic testing.

invocation

In serverless computing, an invocation is when a deployed function is called.

K

Kubernetes

Kubernetes is a platform for managing containers.

L

layer 2

Synonyms: data link layer

In the OSI model of computer networking, layer 2 defines the network data format. Layer 2 concerns frames and physical addressing.

layer 3

Synonyms: network layer

In the OSI model of computer networking, layer 3 determines how data is physically routed from source to destination. Layer 3 concerns packets and logical addressing.

Live Tail

Live Tail is all logs ingested by Datadog after processing but before indexing or archiving.

log indexing

Log indexing filters logs into value groups for different retention periods, quotas, usage monitoring, and billing.

M

manifest (Kubernetes)

In Kubernetes, a manifest is a file that describes the creation and management of resources in a cluster.

measure

A measure is a quantitative facet that can be used to aggregate values from multiple logs, filter logs using a range, or sort logs against a value.

minified code

Minified code is code (often JavaScript) stripped of comments, extra whitespace, unused code, and anything else that does not affect functionality. Minified code is less human-readable, but its smaller size improves website performance.

MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)

MITRE ATT&CK is a knowledge base of cyber adversary tactics and techniques.

mobile app test

Related terms: browser test
In Datadog Synthetic Monitoring, a mobile app test monitors key business flows that may involve several actions and pages to verify that users can successfully complete processes such as signing up for an account and checking out. For more information, see the documentation.

multi alert

A multi alert applies the alert to each source according to the monitor's group parameter. An alert notification is sent for each group that meets the set conditions. For more information, see the documentation.

multi-org

Multi-org is an account feature to manage multiple child organizations from one parent organization account. Users can be added to the parent-org and multiple child-orgs.

multistep API test

Related terms: api test
In Datadog Synthetic Monitoring, a multistep API test has several HTTP requests chained together to monitor user journeys on your services. For more information, see the documentation.

mute

Mute a monitor to silence a monitor's alerts and notifications.

N

NetFlow

NetFlow is a network protocol system that collects IP network traffic as it enters or exits an interface. It was introduced by Cisco in 1996.

Network Device Monitoring (NDM)

Datadog's Network Device Monitoring (NDM) provides visibility into on-premise and virtual network devices, such as routers, switches, and firewalls. For more information, see the documentation.

Network Performance Monitoring (NPM)

Datadog's Network Performance Monitoring (NPM) provides visibility into network traffic between services, containers, availability zones, etc. For more information, see the documentation.

network profile

A network profile is set of attributes that describe how a network is configured.

No Data

No Data is when an integration or application is no longer submitting metrics to Datadog.

Node Agent

The Node Agent is the version of the Datadog Agent that runs on a host.

O

object identifier (OID)

An OID is a standardized name used to identify an object.

Open Web Application Security Project (OWASP)

OWASP is an organization that provides web application security resources.

operational status

The operational status of a port (up/down) refers to whether the port is up or down.

orchestrator

In a containerized infrastructure, an orchestrator automates the management of containers. This includes the provisioning, deploying, scaling, and networking of containers.

P

parent org

A parent org can manage and view the usage of multiple child organizations.

pattern

A pattern is when log messages have a similar structure. Pattern aggregation groups these logs together and displays them in the patterns view.

pipeline

A pipeline is an ordered set of processers applied to a filtered subset of logs, which happens after the collection of logs but before indexing.

Pod

In Kubernetes, a Pod is the smallest deployable unit of computing.

policy-based routing (PBR)

In computer networks, PBR is a technique for routing data according to policies and filters.

private location

In Datadog Synthetic Monitoring, a private location is a Docker container that a user can install inside a private network. This enables users to monitor internal-facing applications or private URLs that are not accessible from the public internet. For more information, see the documentation.

processing pipeline

Related terms: processor , pipeline
For Datadog Events, a processing pipeline is a set sequence of data-structuring actions on event attributes when they are ingested. Users can configure processing pipelines to normalize and enrich events. For more information, see the documentation.

processor

A processor is a set of instructions executed in a log pipeline to restructure log data and generate attributes to enrich logs.

profile

A profile is snapshot in time of how much work (CPU usage, memory usage) is being done by code.

Q

query

A query is composed of the metric name, the time aggregator, the space aggregator, and the scope. For more information, see the documentation.

R

rate

Rate is a metric type that takes the count and divides it by the length of the time interval. For more information, see the documentation.

real user monitoring (RUM)

RUM is a UX monitoring technology that records user interactions with a website or application.

RED metrics

RED stands for “Rate, errors, and duration,” three key metrics for evaluating the performance of some code.

reference table

A reference table lists entities in Datadog like customer details, service names, and information, or IP addresses. The information is represented by a primary key and the associated metadata. For more information, see the documentation.

Rehydration

Rehydration is when archived logs are recalled back into Datadog.

requirement

A group of controls representing a single technical or operational topic, such as access management or networking. The regulatory framework PCI DSS, for example, has 12 requirements.

resource

1. In APM, a resource is a particular domain of an application, typically an instrumented web endpoint, database query, or background job.

2. In RUM, a resource is a type of event. A resource event is generated for images, XHR, Fetch, CSS, or JS libraries loaded on a page.
3. In Cloud Security Management Misconfigurations, a resource is a configurable entity that needs to be continuously scanned for adherence with one or more controls. Examples of AWS instance resources include hosts, containers, security groups, users, and customer-managed IAM policies.

retention filter

Synonyms: indexing

Mechanisms and rules for determining what traces are retained for 15 day storage. Datadog retains a certain amount (Intelligent Retention) and users can create custom filters.

role

A role defines the account permissions for users. In Datadog, there are three default roles: Admin, Standard, and Read-only. For more information, see the documentation.

Role-Based Access Control (RBAC)

RBAC is a method to control read and write access to account assets based on roles that are granted permissions and assigned to users. For more information, see the documentation.

rule

Synonyms: detection rule, compliance rule

A security rule evaluates the configuration of a resource to validate an element related to one or more controls. Rules may map to multiple controls, requirements, and frameworks.

runtime application self-protection (RASP)

RASP is a security technology that detects and prevents attacks in real time.

S

Saved Views

In an Explorer view, saved views keep track of different search queries, customized default visualizations, and a selected subset of facets. Saved views are shared across your organization.

scope

The scope uses tag(s) to filter the query. For more information, see the documentation.

Secrets (Kubernetes)

In Kubernetes, a Secret is an object that can be used to store sensitive data, such as passwords, tokens, and keys.

security information and event management (SIEM)

SIEM is a field in computer security that uses data from security events to support threat detection, security incident management, and compliance.

security posture score

Synonyms: posture score, compliance score

For Cloud Security Management Misconfigurations, the security posture score represents the percentage of your environment that satisfies all of your active Datadog out-of-the-box Cloud and Infrastructure compliance rules.

Formula:

$$(\text{PcricticalPcritical} + \text{Fcritical2})*8+(\text{PhighPhigh} + \text{Fhigh})*6+(\text{PmediumPmedium} + \text{Fmedium})*3+(\text{PlowPlow} + \text{Flow})*2+(\text{PinfoPinfo} + \text{Finfo})*1$$

- P is the number of misconfigurations that evaluate to pass.
- F is the number of misconfigurations that evaluate to fail.

The formula uses a weighted ratio that considers the severity of the misconfiguration and the number of pass/fail misconfigurations for each severity. Only rules and misconfigurations that have the tag `scored:true` are included in the calculation.

You can improve your score by remediating misconfigurations, either by fixing the underlying issues or by muting the misconfiguration for the impacted resource. The posture score is updated every hour.

Sensitive Data Scanner

The Sensitive Data Scanner is a stream-based, pattern matching service to identify, tag, and optionally redact or hash sensitive data.

server-side request forgery (SSRF)

SSRF is a type of exploit where an attacker uses a server to access or manipulate information.

serverless

Serverless is a cloud development and execution model in which a cloud service provider handles server infrastructure.

Serverless Insights

Serverless insights are automatically-generated indicators (such as *high memory usage*, *cold start*, *out of memory*, etc.) that Datadog uses to identify and flag Lambda functions that are failing or performing poorly.

service

1. In APM, a service is a group of related endpoints, queries, or jobs that perform a piece of work for your application. A microservices-based architecture is built from multiple services, each performing part of the operation of the application.
2. In serverless computing, a service is an independently-deployed piece of functionality in your architecture. Serverless applications are powered by managed services.

service account

A service account is a non-human user that can be assigned a role and own application keys. For more information, see the documentation.

service check

A service check monitors whether the status of a specific service is up or down. For more information, see the documentation.

service entry span

A span is a service entry span when it is the entrypoint method for a request to a service. You can visualize this in APM when the color of the immediate parent on a flame graph is a different color.

Service Level Agreement (SLA)

An SLA is an explicit or implicit agreement between a client and service provider stipulating the client's reliability expectations and the service provider's consequences for not meeting them.

Service Level Objective (SLO)

An SLO is a target percentage for application performance over a specific period of time. For more information, see the documentation.

Service Map

In APM, the Service Map visualization provides an overview of your services and their health. It decomposes your application into its component services and draws observed dependencies between them.

session

In Datadog RUM, a session is a type of event. A user session begins when a user starts browsing the web application. It contains high-level information about the user, including their browser and device.

Session Replay

Session replay is a technique in UX testing that replays a user's journey on a website or application.

Simple Network Management Protocol (SNMP)

SNMP is a protocol for collecting, organizing, and modifying information about managed devices on IP networks.

SNMP Management Information Base (MIB)

An SNMP MIB is a collection of definitions for a managed object's properties (such as data types, access permissions, etc.) For more information, see the documentation.

SNMP trap

SNMP Traps are notifications sent from an SNMP-enabled device to an SNMP manager. When a network device encounters unusual activity, such as a sudden state change on a piece of equipment, the device triggers an SNMP Trap event. For more information, see the documentation.

software development kit (SDK)

An SDK is a set of tools that enable developers to create applications for a specific technology, such as an operating system or a programming language.

source

A log source is where logs are collected and ingested into Datadog.

source map

A source map is a file that maps minified JavaScript code to the original source.

space aggregation

Space aggregation splits a single metric into multiple timeseries by tags such as host, container, and region. There are four aggregation options: `sum`, `min`, `max`, and `avg`. For more information, see the documentation.

span

A span is a logical unit of work in a distributed system for a given period. Multiple spans construct a trace.

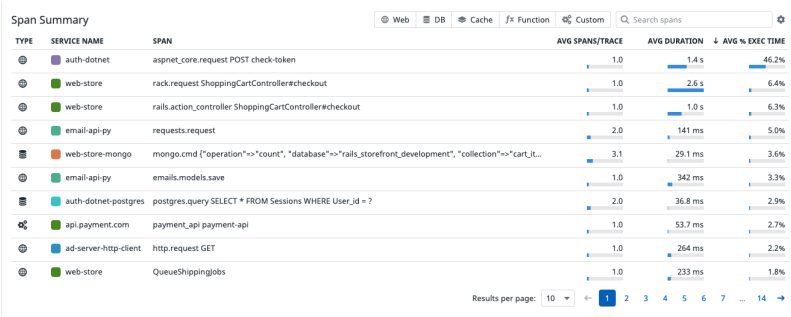
span ID

A span ID is a numerical identifier generated by the tracing library for a span. Together with trace IDs, they are used to correlate traces and logs in Datadog.

span tag

A span tag is a tag that is applied to a span, in the form of a key-value pair, to correlate a request with other telemetry (or to filter it in searches). Tags can be added to a single span or globally to all spans.

The span summary table in APM shows metrics for spans aggregated across all traces, including how often the span shows up among all traces, what percent of traces contain the span, the average duration for the span, and its typical share of total execution time of the requests. This helps you detect N+1 problems in your code so you can improve your application performance.



The span summary table is only available for resources containing service entry spans, and contains the following information:

Average spans per trace
Average number of occurrences of the span for traces, including the current resource, where the span is present at least once.

Percentage of traces
Percentage of traces, including the current resource, where the span is present at least once.

Average duration
Average duration of the span for traces, including the current resource, where the span is present at least once.

Average percentage of execution time
Average ratio of execution time for which the span was active for traces, including the current resource, where the span is present at least once.

span tag

A span tag is a tag that is applied to a span, in the form of a key-value pair, to correlate a request with other telemetry (or to filter it in searches). Tags can be added to a single span or globally to all spans.

standard attribute

A standard attribute is from a default set of attributes. These default attributes can be customized to create a naming convention for your organization.

static application security testing (SAST)

Synonyms: static analysis

SAST is a security testing methodology that analyzes a program's source code or binaries.

sublayer metric

A sublayer metric is the execution duration of a given type or service within a trace.

Some Tracing Application Metrics are tagged with `sublayer_service` and `sublayer_type` so that you can see the execution time for individual services within a trace.

Sublayer metrics are only available if a service has downstream dependencies.

T

tail

The term *tail* is derived from the `tail` command in Unix and Linux operating systems. Tailing is an alternative to printing the entire contents of a file. When you tail a file, you print the last few lines of the file to the terminal. Tailing is commonly used with log files to find the most recently logged events for a process or service. You can set the Datadog Agent up to tail a log file. For more information see Custom log collection.

template variable

A template variable is an attribute used to customize and route monitor notifications based on the alert details, or to provide multiple views a single dashboard. For more information, see the documentation.

test regression

A test run is marked as a regression when its duration is both five times the mean and greater than the max duration for the same test in the default branch. A benchmark test run is marked as a regression when its duration is five times the standard deviation above the

mean for the same test in the default branch.

A benchmark test has `@test.type:benchmark`. The mean and the max of the default branch is calculated over the last week of test runs. For more information, see the documentation.

test service

A test service is a group of tests associated with, for example, a project or repo. It contains all the individual tests for your code, optionally organized into test suites, which are like folders for your tests. For more information, see the documentation.

time aggregation

Synonyms: rollup

Time aggregation is how Datadog combines data points into time buckets. There are five aggregation options: sum, min, max, avg, and count. For more information, see the documentation.

trace

A trace tracks the time spent processing a request, and the status of this request. Each trace consists of one or more spans.

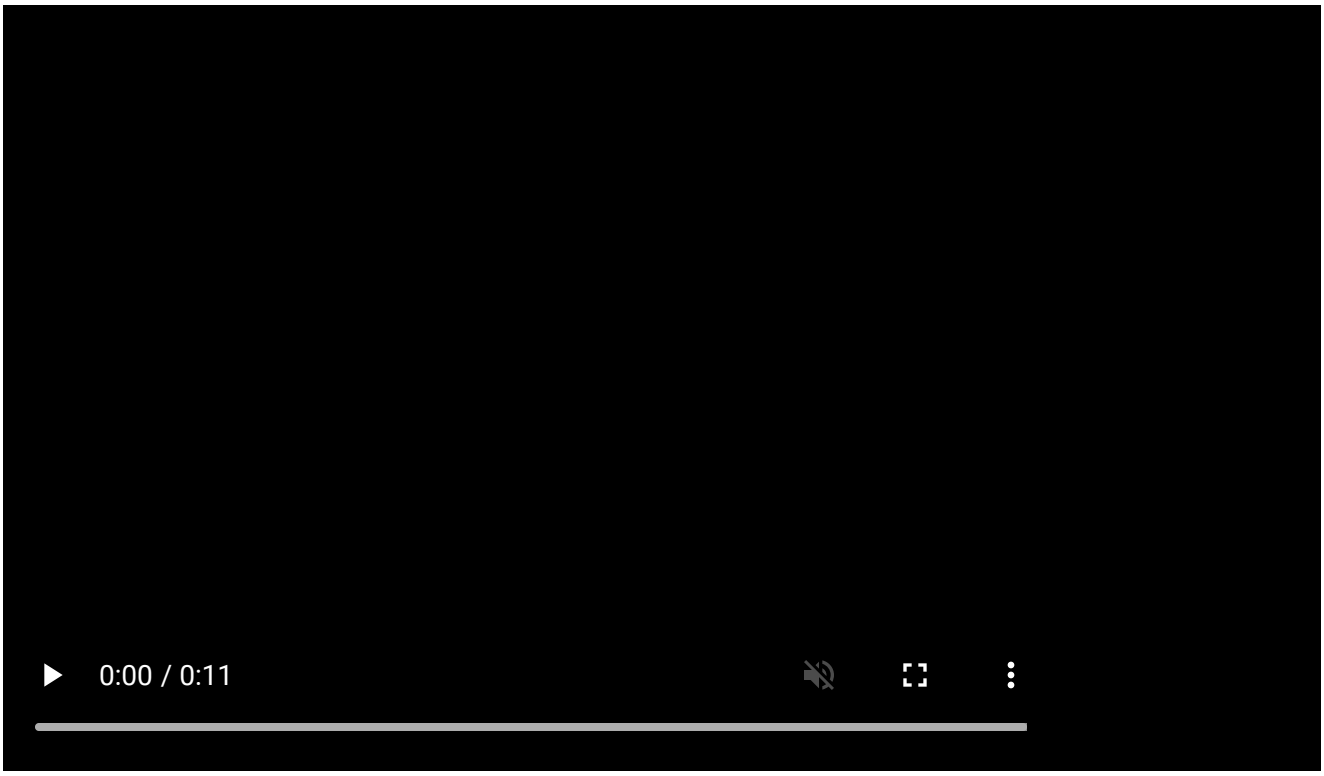
trace ID

The trace ID is a numerical identifier generated by the tracing library for a trace. Together with span IDs, they are used to correlate traces and logs in Datadog.

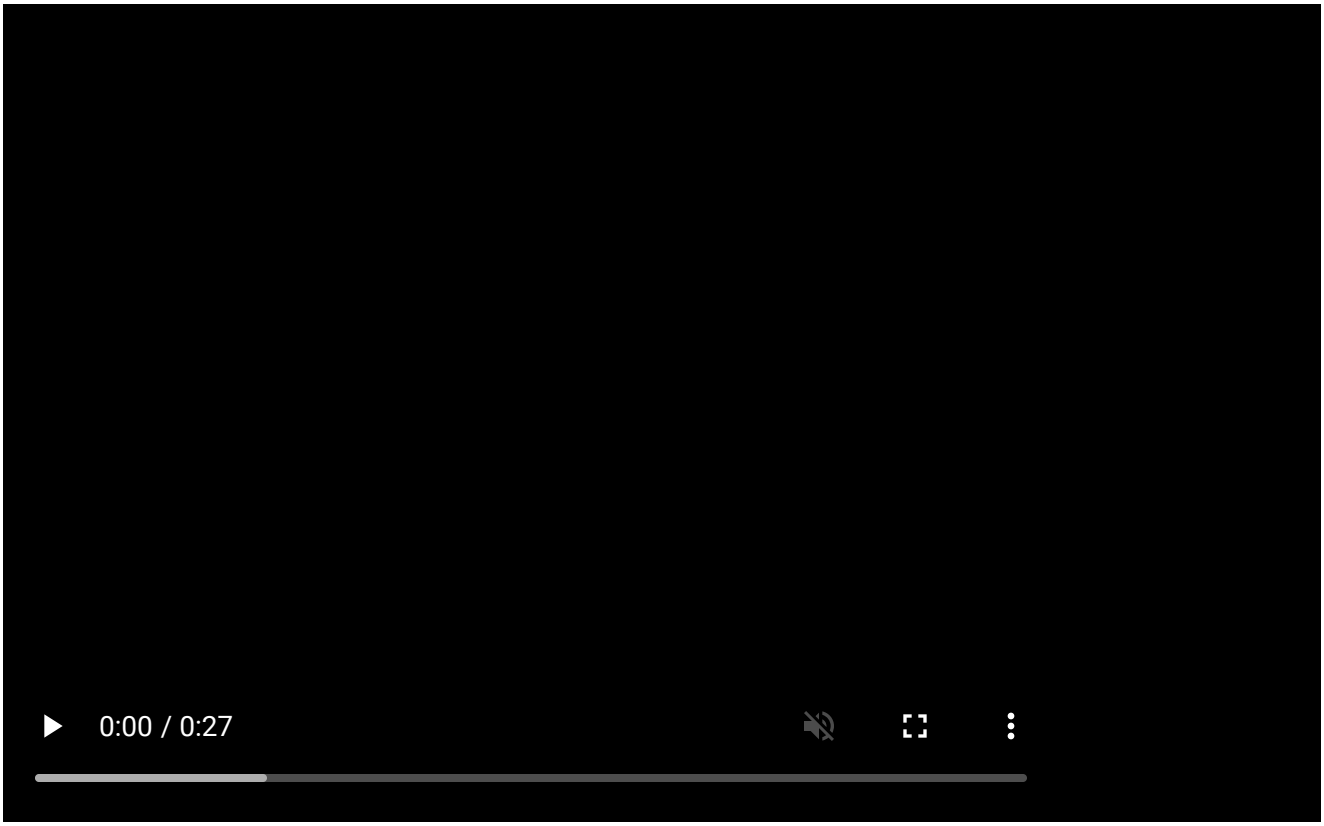
trace metric

Trace metrics are automatically collected and kept with a 15-month retention policy similar to any other Datadog metric. They can be used to identify and alert on hits, errors, or latency. Statistics and metrics are always calculated based on all traces, and are not impacted by ingestion controls.

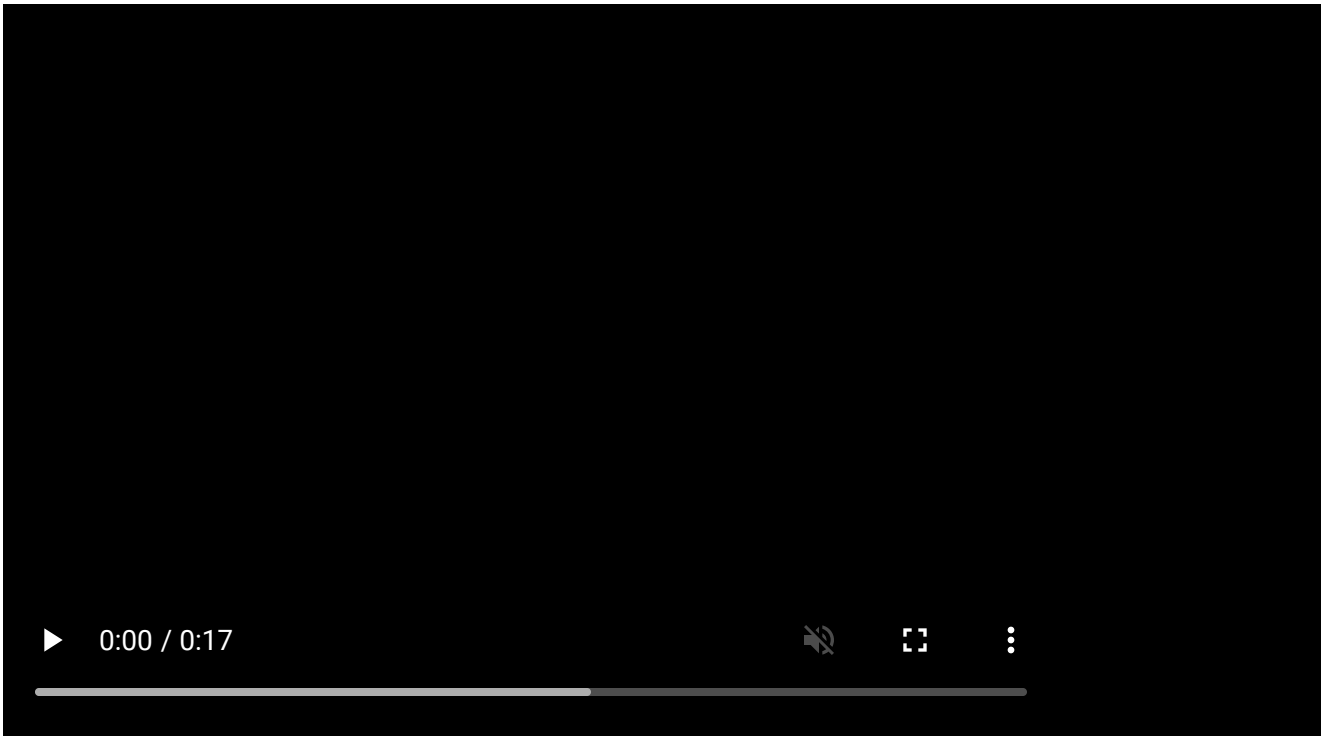
Trace metrics are tagged by the host receiving traces along with the service or resource. For example, after instrumenting a web service trace metrics are collected for the entry-point span `web.request` in **Metrics > Summary**.



Trace metrics can be exported to a dashboard from the **Service** or **Resource** page. Additionally, trace metrics can be queried from an existing dashboard.

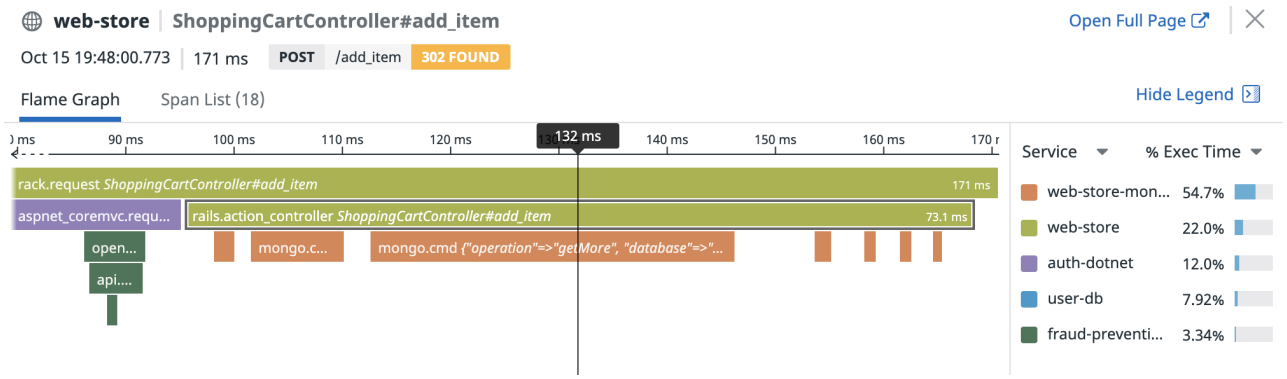


Trace metrics are useful for monitoring. APM monitors can be set up on the New Monitors, Service, or Resource page. A set of suggested monitors is available on the Service or Resource page.



trace root span

A span is a trace root span when it is the first span of a trace. The root span is the entry-point method of the traced request. Its start marks the beginning of the trace.



In this example, the **service entry spans** are:

- `rack.request` (which is also the *root span*)
- `aspnet_coremvc.request`
- The topmost green span below `aspnet_coremvc.request`
- Every orange `mongodb` span

transaction

A transaction aggregates indexed logs based on an instance of a sequence of events, such as a user session or a request processed across multiple micro-services.

U

user

A user is someone who has access to data in Datadog based on their assigned role.

V

view

In Datadog RUM, a view is a type of event. A view event is generated each time a user visits a web application page.

W

wall time

Wall time is the real time elapsed while the test suite runs, which is less than the sum of all test times when tests are run concurrently. For more information, see the documentation.

warning

A warning is an optional monitor threshold setting for sending a warning notification, where the priority level is lower than an alert.

web application firewall (WAF)

A WAF is a security tool that monitors and filters HTTP traffic from a web application.

webhook

A webhook uses a URL to connect your services, and alerts your services when a metric alert is triggered. For more information, see the documentation.