Terminology

edit

@metadata
: A special field for storing content that you don't want to include in output events. For example, the `@metadata` field is useful for creating transient fields for use in conditional statements.

A

edit

action
: 1. The rule-specific response that occurs when an alerting rule fires. A rule can have multiple actions. See Connectors and actions.
2. In Elastic Security, actions send notifications via other systems when a detection alert is created, such as email, Slack, PagerDuty, and Webhook.

administration console
: A component of Elastic Cloud Enterprise that provides the API server for the Cloud UI. Also syncs cluster and allocator data from ZooKeeper to Elasticsearch.

Advanced Settings
: Enables you to control the appearance and behavior of Kibana by setting the date format, default index, and other attributes. Part of Kibana Stack Management. See Advanced Settings.

Agent policy
: A collection of inputs and settings that defines the data to be collected by Elastic Agent. An agent policy can be applied to a single agent or shared by a group of agents; this makes it easier to manage many agents at scale. See Elastic Agent policies.

alias
: Secondary name for a group of data streams or indices. Most Elasticsearch APIs accept an alias in place of a data stream or index. See Aliases.

allocator affinity
: Controls how Elastic Stack deployments are distributed across the available set of allocators in your Elastic Cloud Enterprise installation.

allocator tag
: In Elastic Cloud Enterprise, characterizes hardware resources for Elastic Stack deployments. Used by instance configurations to determine which instances of the

Elastic Stack should be placed on what hardware.

allocator
: Manages hosts that contain Elasticsearch and Kibana nodes. Controls the lifecycle of these nodes by creating new containers and managing the nodes within these containers when requested. Used to scale the capacity of your Elastic Cloud Enterprise installation.

analysis
: Process of converting unstructured text into a format optimized for search. See Text analysis.

annotation
: A way to augment a data display with descriptive domain knowledge.

anomaly detection job
: Anomaly detection jobs contain the configuration information and metadata necessary to perform an analytics task. See Machine learning jobs and the create anomaly detection job API.

API key
: Unique identifier for authentication in Elasticsearch. When transport layer security (TLS) is enabled, all requests must be authenticated using an API key or a username and password. See the Create API key API.

APM agent
: An open-source library, written in the same language as your service, which instruments your code and collects performance data and errors at runtime.

APM Server
: An open-source application that receives data from APM agents and sends it to Elasticsearch.

app
: A top-level Kibana component that is accessed through the side navigation. Apps include core Kibana components such as Discover and Dashboard, solutions like Observability and Security, and special-purpose tools like Maps and Stack Management.

auto-follow pattern
: Index pattern that automatically configures new indices as follower indices for cross-cluster replication. See Manage auto-follow patterns.

availability zone
: Contains resources available to a Elastic Cloud Enterprise installation that are isolated from other availability zones to safeguard against failure. Could be a rack, a server zone or some other logical constraint that creates a failure boundary. In a highly available cluster, the nodes of a cluster are spread across two or three availability zones to ensure that the cluster can survive the failure of an entire availability zone. Also see Fault Tolerance (High Availability).

B

edit

basemap
: The background detail necessary to orient the location of a map.

beats runner
: Used to send Filebeat and Metricbeat information to the logging cluster.

bucket aggregation
: An aggregation that creates buckets of documents. Each bucket is associated with a criterion (depending on the aggregation type), which determines whether or not a document in the current context falls into the bucket.

bucket
: 1. A set of documents in Kibana that have certain characteristics in common. For example, matching documents might be bucketed by color, distance, or date range.
2. The machine learning features also use the concept of a bucket to divide the time series into batches for processing. The *bucket span* is part of the

configuration information for anomaly detection jobs. It defines the time interval that is used to summarize and model the data. This is typically between 5 minutes to 1 hour and it depends on your data characteristics. When you set the bucket span, take into account the granularity at which you want to analyze, the frequency of the input data, the typical duration of the anomalies, and the frequency at which alerting is required.

C

edit

Canvas expression language
: A pipeline-based expression language for manipulating and visualizing data. Includes dozens of functions and other capabilities, such as table transforms, type casting, and sub-expressions. Supports TinyMath functions for complex math calculations. See Canvas function reference.

Canvas
: Enables you to create presentations and infographics that pull live data directly from Elasticsearch. See Canvas.

certainty
: Specifies how many documents must contain a pair of terms before it is considered a useful connection in a graph.

client forwarder
: Used for secure internal communications between various components of Elastic Cloud Enterprise and ZooKeeper.

Cloud UI
: Provides web-based access to manage your Elastic Cloud Enterprise installation, supported by the administration console.

cluster
: 1. A group of one or more connected Elasticsearch nodes. See Clusters, nodes, and shards.
2. A layer type and display option in the **Maps** application. Clusters display a cluster symbol across a grid on the map, one symbol per grid cluster. The cluster location is the weighted centroid for all documents in the grid cell.

codec plugin
: A Logstash plugin that changes the data representation of an event. Codecs are essentially stream filters that can operate as part of an input or output. Codecs enable you to separate the transport of messages from the serialization process. Popular codecs include json, msgpack, and plain (text).

cold phase
: Third possible phase in the index lifecycle. In the cold phase, data is no longer updated and seldom queried. The data still needs to be searchable, but it's okay if those queries are slower. See Index lifecycle.

cold tier
: Data tier that contains nodes that hold time series data that is accessed occasionally and not normally updated. See Data tiers.

component template
: Building block for creating index templates. A component template can specify mappings, index settings, and aliases. See index templates.

condition
: Specifies the circumstances that must be met to trigger an alerting rule.

conditional
: A control flow that executes certain actions based on whether a statement (also called a condition) is true or false. Logstash supports `if`, `else if`, and `else` statements. You can use conditional statements to apply filters and send events to a specific output based on conditions that you specify.

connector

A configuration that enables integration with an external system (the destination for an action). See Connectors and actions.

Console

In Kibana, a tool for interacting with the Elasticsearch REST API. You can send requests to Elasticsearch, view responses, view API documentation, and get your request history. See Console.

In Elasticsearch Service, provides web-based access to manage your Elastic Cloud deployments.

constructor

Directs allocators to manage containers of Elasticsearch and Kibana nodes and maximizes the utilization of allocators. Monitors plan change requests from the Cloud UI and determines how to transform the existing cluster. In a highly available installation, places cluster nodes within different availability zones to ensure that the cluster can survive the failure of an entire availability zone.

container

Includes an instance of Elastic Cloud Enterprise software and its dependencies. Used to provision similar environments, to assign a guaranteed share of host resources to nodes, and to simplify operational effort in Elastic Cloud Enterprise.

content tier

Data tier that contains nodes that handle the indexing and query load for content, such as a product catalog. See Data tiers.

coordinator

Consists of a logical grouping of some Elastic Cloud Enterprise services and acts as a distributed coordination system and resource scheduler.

cross-cluster replication (CCR)

Replicates data streams and indices from remote clusters in a local cluster. See Cross-cluster replication.

cross-cluster search (CCS)

Searches data streams and indices on remote clusters from a local cluster. See Search across clusters.

custom rule

A set of conditions and actions that change the behavior of anomaly detection jobs. You can also use filters to further limit the scope of the rules. See Custom rules. Kibana refers to custom rules as job rules.

D

edit

dashboard

A collection of visualizations, saved searches, and maps that provide insights into your data from multiple perspectives.

data center

Check availability zone.

data frame analytics job

Data frame analytics jobs contain the configuration information and metadata necessary to perform machine learning analytics tasks on a source index and store the outcome in a destination index. See Data frame analytics overview and the create data frame analytics job API.

data source

A file, database, or service that provides the underlying data for a map, Canvas element, or visualization.

data stream

A named resource used to manage time series data. A data stream stores data across multiple backing indices. See Data streams.

data tier

Collection of nodes with the same data role that typically share the same hardware profile. Data tiers include the content tier, hot tier, warm tier, cold tier, and frozen

tier. See Data tiers.

data view
: An object that enables you to select the data that you want to use in Kibana and define the properties of the fields. A data view can point to one or more data streams, indices, or aliases. For example, a data view can point to your log data from yesterday, or all indices that contain your data.

datafeed
: Anomaly detection jobs can analyze either a one-off batch of data or continuously in real time. Datafeeds retrieve data from Elasticsearch for analysis.

dataset
: A collection of data that has the same structure. The name of a dataset typically signifies its source. See data stream naming scheme.

delete phase
: Last possible phase in the index lifecycle. In the delete phase, an index is no longer needed and can safely be deleted. See Index lifecycle.

deployment template
: A reusable configuration of Elastic products and solutions used to create an Elastic Cloud deployment.

deployment
: One or more products from the Elastic Stack configured to work together and run on Elastic Cloud.

detection alert
: Elastic Security produced alerts. Detection alerts are never received from external systems. When a rule's conditions are met, Elastic Security writes a detection alert to an Elasticsearch alerts index.

detection rule
: Background tasks in Elastic Security that run periodically and produce alerts when suspicious activity is detected.

detector
: As part of the configuration information that is associated with anomaly detection jobs, detectors define the type of analysis that needs to be done. They also specify which fields to analyze. You can have more than one detector in a job, which is more efficient than running multiple jobs against the same data.

director
: Manages the ZooKeeper datastore. This role is often shared with the coordinator, though in production deployments it can be separated.

Discover
: Enables you to search and filter your data to zoom in on the information that you are interested in.

distributed tracing
: The end-to-end collection of performance data throughout your microservices architecture.

document
: JSON object containing data stored in Elasticsearch. See Documents and indices.

drilldown
: A navigation path that retains context (time range and filters) from the source to the destination, so you can view the data from a new perspective. A dashboard that shows the overall status of multiple data centers might have a drilldown to a dashboard for a single data center. See Drilldowns.

E

edit

Elastic Cloud Enterprise (ECE)
: The official enterprise offering to host and manage the Elastic Stack yourself at scale. Can be installed on a public cloud platform, such as AWS, GCP or Microsoft Azure, on your own private cloud, or on bare metal.

Elastic Cloud on Kubernetes (ECK)

Built on the Kubernetes Operator pattern, ECK extends the basic Kubernetes orchestration capabilities to support the setup and management of Elastic products and solutions on Kubernetes

edge

A connection between nodes in a graph that shows that they are related. The line weight indicates the strength of the relationship. See Graph.

Elastic Agent

A single, unified way to add monitoring for logs, metrics, and other types of data to a host. It can also protect hosts from security threats, query data from operating systems, forward data from remote services or hardware, and more. See Elastic Agent overview.

Elastic Common Schema (ECS)

A document schema for Elasticsearch, for use cases such as logging and metrics. ECS defines a common set of fields, their datatype, and gives guidance on their correct usage. ECS is used to improve uniformity of event data coming from different sources.

Elastic Maps Service (EMS)

A service that provides basemap tiles, shape files, and other key features that are essential for visualizing geospatial data.

Elastic Package Registry (EPR)

A service hosted by Elastic that stores Elastic package definitions in a central location. See the EPR GitHub repository.

Elastic Security indices

Indices containing host and network source events (such as `packetbeat-*`, `log-*`, and `winlogbeat-*`). When you create a new rule in Elastic Security, the default index pattern corresponds to the values defined in the `securitySolution:defaultIndex` advanced setting.

Elastic Stack

Also known as the *ELK Stack*, the Elastic Stack is the combination of various Elastic products that integrate for a scalable and flexible way to manage your data.

Elasticsearch Service

The official hosted Elastic Stack offering, from the makers of Elasticsearch. Available as a software-as-a-service (SaaS) offering on different cloud platforms, such as AWS, GCP, and Microsoft Azure.

element

A Canvas workpad object that displays an image, text, or visualization.

endpoint exception

Exceptions added to both rules and Endpoint agents on hosts. Endpoint exceptions can only be added when:

- Endpoint agents are installed on the hosts.
- The Elastic Endpoint Security rule is activated.

Event Query Language (EQL)

Query language for event-based time series data, such as logs, metrics, and traces. EQL supports matching for event sequences. See EQL.

event

A single unit of information, containing a timestamp plus additional data. An event arrives via an input, and is subsequently parsed, timestamped, and passed through the Logstash pipeline.

exception

In Elastic Security, exceptions are added to rules to prevent specific source event field values from generating alerts.

external alert

Alerts Elastic Security receives from external systems, such as Suricata.

F

edit

Feature Controls
: Enables administrators to customize which features are available in each space. See Feature Controls.

feature importance
: In supervised machine learning methods such as regression and classification, feature importance indicates the degree to which a specific feature affects a prediction. See Regression feature importance and Classification feature importance.

feature influence
: In outlier detection, feature influence scores indicate which features of a data point contribute to its outlier behavior. See Feature influence.

feature state
: The indices and data streams used to store configurations, history, and other data for an Elastic feature, such as Elasticsearch security or Kibana. A feature state typically includes one or more system indices or data streams. It may also include regular indices and data streams used by the feature. You can use snapshots to back up and restore feature states. See feature states.

field reference
: A reference to an event field. This reference may appear in an output block or filter block in the Logstash config file. Field references are typically wrapped in square (`[]`) brackets, for example `[fieldname]`. If you are referring to a top-level field, you can omit the `[]` and simply use the field name. To refer to a nested field, you specify the full path to that field: `[top-level field][nested field]`.

field
: 1. Key-value pair in a document. See Mapping.
2. In Logstash, this term refers to an event property. For example, each event in an apache access log has properties, such as a status code (200, 404), request path ("/", "index.html"), HTTP verb (GET, POST), client IP address, and so on. Logstash uses the term "fields" to refer to these properties.

filter plugin
: A Logstash plugin that performs intermediary processing on an event. Typically, filters act upon event data after it has been ingested via inputs, by mutating, enriching, and/or modifying the data according to configuration rules. Filters are often applied conditionally depending on the characteristics of the event. Popular filter plugins include grok, mutate, drop, clone, and geoip. Filter stages are optional.

filter
: Query that does not score matching documents. See filter context.

Fleet Server
: Fleet Server is a component used to centrally manage Elastic Agents. It serves as a control plane for updating agent policies, collecting status information, and coordinating actions across agents.

Fleet
: Fleet provides a way to centrally manage Elastic Agents at scale. There are two parts: The Fleet app in Kibana provides a web-based UI to add and remotely manage agents, while the Fleet Server provides the backend service that manages agents. See Elastic Agent overview.

flush
: Writes data from the transaction log to disk for permanent storage. See the flush API.

follower index
: Target index for cross-cluster replication. A follower index exists in a local cluster and replicates a leader index. See Cross-cluster replication.

force merge
: Manually triggers a merge to reduce the number of segments in an index's shards. See the force merge API.

frozen phase
: Fourth possible phase in the index lifecycle. In the frozen phase, an index is no longer updated and queried rarely. The information still needs to be searchable, but it's okay if those queries are extremely slow. See Index lifecycle.

frozen tier
: Data tier that contains nodes that hold time series data that is accessed rarely and not normally updated. See Data tiers.

G

edit

gem
: A self-contained package of code that's hosted on RubyGems.org. Logstash plugins are packaged as Ruby Gems. You can use the Logstash plugin manager to manage Logstash gems.

geo-point
: A field type in Elasticsearch. A geo-point field accepts latitude-longitude pairs for storing point locations. The latitude-longitude format can be from a string, geohash, array, well-known text, or object. See geo-point.

geo-shape
: A field type in Elasticsearch. A geo-shape field accepts arbitrary geographic primitives, like polygons, lines, or rectangles (and more). You can populate a geo-shape field from GeoJSON or well-known text. See geo-shape.

GeoJSON
: A format for representing geospatial data. GeoJSON is also a file-type, commonly used in the **Maps** application to upload a file of geospatial data. See GeoJSON data.

graph
: A data structure and visualization that shows interconnections between a set of entities. Each entity is represented by a node. Connections between nodes are represented by edges. See Graph.

Grok Debugger
: A tool for building and debugging grok patterns. Grok is good for parsing syslog, Apache, and other webserver logs. See Debugging grok expressions.

H

edit

hardware profile
: In Elastic Cloud, a built-in deployment template that supports a specific use case for the Elastic Stack, such as a compute optimized deployment that provides high vCPU for search-heavy use cases.

heat map
: A layer type in the **Maps** application. Heat maps cluster locations to show higher (or lower) densities. Heat maps describe a visualization with color-coded cells or regions to analyze patterns across multiple dimensions. See Heat map layer.

hidden data stream or index
: Data stream or index excluded from most index patterns by default. See Hidden data streams and indices.

host runner (runner)
: In Elastic Cloud Enterprise, a local control agent that runs on all hosts, used to deploy local containers based on role definitions. Ensures that containers assigned to the host exist and are able to run, and creates or recreates the containers if necessary.

hot phase
: First possible phase in the index lifecycle. In the hot phase, an index is actively updated and queried. See Index lifecycle.

hot thread
: A Java thread that has high CPU usage and executes for a longer than normal period of time.

hot tier
: Data tier that contains nodes that handle the indexing load for time series data, such as logs or metrics. This tier holds your most recent, most frequently accessed data. See Data tiers.

I

edit

ID
: Identifier for a document. Document IDs must be unique within an index. See the `_id` field.

index lifecycle policy
: Specifies how an index moves between phases in the index lifecycle and what actions to perform during each phase. See Index lifecycle.

index lifecycle
: Five phases an index can transition through: hot, warm, cold, frozen, and delete. See Index lifecycle.

index pattern
: In Elasticsearch, a string containing a wildcard (`*`) pattern that can match multiple data streams, indices, or aliases. See Multi-target syntax.

index template
: Automatically configures the mappings, index settings, and aliases of new indices that match its index pattern. You can also use index templates to create data streams. See Index templates.

index
: 1. Collection of JSON documents. See Documents and indices.
2. To add one or more JSON documents to Elasticsearch. This process is called indexing.

indexer
: A Logstash instance that is tasked with interfacing with an Elasticsearch cluster in order to index event data.

indicator index
: Indices containing suspect field values in Elastic Security. Indicator match rules use these indices to compare their field values with source event values contained in Elastic Security indices.

inference aggregation
: A pipeline aggregation that references a trained model in an aggregation to infer on the results field of the parent bucket aggregation. It enables you to use supervised machine learning at search time.

inference processor
: A processor specified in an ingest pipeline that uses a trained model to infer against the data that is being ingested in the pipeline.

inference
: A machine learning feature that enables you to use supervised learning processes – like classification, regression, or natural language processing – in a continuous fashion by using trained models against incoming data.

influencer
: Influencers are entities that might have contributed to an anomaly in a specific bucket in an anomaly detection job. For more information, see Influencers.

ingestion
: The process of collecting and sending data from various data sources to Elasticsearch.

input plugin
: A Logstash plugin that reads event data from a specific source. Input plugins are the first stage in the Logstash event processing pipeline. Popular input plugins include file, syslog, redis, and beats.

instance configuration

In Elastic Cloud, enables the instances of the Elastic Stack to run on suitable hardware resources by filtering on allocator tags. Used as building blocks for deployment templates.

instance type
In Elastic Cloud, categories for instances representing an Elastic feature or cluster node types, such as `master`, `ml` or `data`.

instance
A product from the Elastic Stack that is running in an Elastic Cloud deployment, such as an Elasticsearch node or a Kibana instance. When you choose more availability zones, the system automatically creates more instances for you.

instrumentation
Extending application code to track where your application is spending time. Code is considered instrumented when it collects and reports this performance data to APM.

integration policy
An instance of an integration that is configured for a specific use case, such as collecting logs from a specific file.

integration
An easy way for external systems to connect to the Elastic Stack. Whether it's collecting data or protecting systems from security threats, integrations provide out-of-the-box assets to make setup easy—many with just a single click.

J

edit

job
Machine learning jobs contain the configuration information and metadata necessary to perform an analytics task. There are two types: anomaly detection jobs and data frame analytics jobs. See also rollup job.

K

edit

Kibana privilege
Enable administrators to grant users read-only, read-write, or no access to individual features within spaces in Kibana. See Kibana privileges.

Kibana Query Language (KQL)
The default language for querying in Kibana. KQL provides support for scripted fields. See Kibana Query Language.

Kibana
A user interface that lets you visualize your Elasticsearch data and navigate the Elastic Stack.

L

edit

labs
An in-progress or experimental feature in **Canvas** or **Dashboard** that you can try out and provide feedback. When enabled, you'll see **Labs** in the toolbar.

leader index
Source index for cross-cluster replication. A leader index exists on a remote cluster and is replicated to follower indices. See Cross-cluster replication.

Lens
Enables you to build visualizations by dragging and dropping data fields. Lens makes makes smart visualization suggestions for your data, allowing you to switch between visualization types. See Lens.

local cluster
Cluster that pulls data from a remote cluster in cross-cluster search or cross-cluster replication. See Remote clusters.

Lucene query syntax
: The query syntax for Kibana's legacy query language. The Lucene query syntax is available under the options menu in the query bar and from Advanced Settings.

M

edit

machine learning node
: A machine learning node is a node that has `xpack.ml.enabled` set to `true` and `ml` in `node.roles`. If you want to use machine learning features, there must be at least one machine learning node in your cluster. See Machine learning nodes.

map
: A representation of geographic data using symbols and labels. See Maps.

mapping
: Defines how a document, its fields, and its metadata are stored in Elasticsearch. Similar to a schema definition. See Mapping.

master node
: Handles write requests for the cluster and publishes changes to other nodes in an ordered fashion. Each cluster has a single master node which is chosen automatically by the cluster and is replaced if the current master node fails. Also see node.

merge
: Process of combining a shard's smaller Lucene segments into a larger one. Elasticsearch manages merges automatically.

message broker
: Also referred to as a *message buffer* or *message queue*, a message broker is external software (such as Redis, Kafka, or RabbitMQ) that stores messages from the Logstash shipper instance as an intermediate store, waiting to be processed by the Logstash indexer instance.

metric aggregation
: An aggregation that calculates and tracks metrics for a set of documents.

module
: Out-of-the-box configurations for common data sources to simplify the collection, parsing, and visualization of logs and metrics.

monitor
: A network endpoint which is monitored to track the performance and availability of applications and services.

multi-field
: A field that's mapped in multiple ways. See the `fields` mapping parameter.

N

edit

namespace
: A user-configurable arbitrary data grouping, such as an environment (`dev`, `prod`, or `qa`), a team, or a strategic business unit.

natural language processing (NLP)
: A machine learning feature that enables you to perform operations such as language identification, named entity recognition (NER), text classification, or text embedding. See NLP overview.

no-op
: In Elastic Cloud, the application of a rolling update on your deployment without actually applying any configuration changes. This type of update can be useful to resolve certain health warnings.

node
: A single Elasticsearch server. One or more nodes can form a cluster. See Clusters, nodes, and shards.

O

edit

Observability
: Unifying your logs, metrics, uptime data, and application traces to provide granular insights and context into the behavior of services running in your environments.

output plugin
: A Logstash plugin that writes event data to a specific destination. Outputs are the final stage in the event pipeline. Popular output plugins include elasticsearch, file, graphite, and statsd.

P

edit

Painless Lab
: An interactive code editor that lets you test and debug Painless scripts in real-time. See Painless Lab.

panel
: A dashboard component that contains a query element or visualization, such as a chart, table, or list.

pipeline
: A term used to describe the flow of events through the Logstash workflow. A pipeline typically consists of a series of input, filter, and output stages. Input stages get data from a source and generate events, filter stages, which are optional, modify the event data, and output stages write the data to a destination. Inputs and outputs support codecs that enable you to encode or decode the data as it enters or exits the pipeline without having to use a separate filter.

plan
: Specifies the configuration and topology of an Elasticsearch or Kibana cluster, such as capacity, availability, and Elasticsearch version, for example. When changing a plan, the constructor determines how to transform the existing cluster into the pending plan.

plugin manager
: Accessed via the `bin/logstash-plugin` script, the plugin manager enables you to manage the lifecycle of plugins in your Logstash deployment. You can install, remove, and upgrade plugins by using the plugin manager Command Line Interface (CLI).

plugin
: A self-contained software package that implements one of the stages in the Logstash event processing pipeline. The list of available plugins includes input plugins, output plugins, codec plugins, and filter plugins. The plugins are implemented as Ruby gems and hosted on RubyGems.org. You define the stages of an event processing pipeline by configuring plugins.

primary shard
: Lucene instance containing some or all data for an index. When you index a document, Elasticsearch adds the document to primary shards before replica shards. See Clusters, nodes, and shards.

proxy
: A highly available, TLS-enabled proxy layer that routes user requests, mapping cluster IDs that are passed in request URLs for the container to the cluster nodes handling the user requests.

Q

edit

Query Profiler
: A tool that enables you to inspect and analyze search queries to diagnose and debug poorly performing queries. See Query Profiler.

query
: Request for information about your data. You can think of a query as a question, written in a way Elasticsearch understands. See Search your data.

R

edit

Real user monitoring (RUM)
: Performance monitoring, metrics, and error tracking of web applications.

recovery
: Process of syncing a replica shard from a primary shard. Upon completion, the replica shard is available for searches. See the index recovery API.

reindex
: Copies documents from a source to a destination. The source and destination can be a data stream, index, or alias. See the Reindex API.

remote cluster
: A separate cluster, often in a different data center or locale, that contains indices that can be replicated or searched by the local cluster. The connection to a remote cluster is unidirectional. See Remote clusters.

replica shard
: Copy of a primary shard. Replica shards can improve search performance and resiliency by distributing data across multiple nodes. See Clusters, nodes, and shards.

roles token
: Enables a host to join an existing Elastic Cloud Enterprise installation and grants permission to hosts to hold certain roles, such as the allocator role. Used when installing Elastic Cloud Enterprise on additional hosts, a roles token helps secure Elastic Cloud Enterprise by making sure that only authorized hosts become part of the installation.

rollover
: Creates a new write index when the current one reaches a certain size, number of docs, or age. A rollover can target a data stream or an alias with a write index.

rollup index
: Special type of index for storing historical data at reduced granularity. Documents are summarized and indexed into a rollup index by a rollup job. See Rolling up historical data.

rollup job
: Background task that runs continuously to summarize documents in an index and index the summaries into a separate rollup index. The job configuration controls what data is rolled up and how often. See Rolling up historical data.

rollup
: Summarizes high-granularity data into a more compressed format to maintain access to historical data in a cost-effective way. See Roll up your data.

routing
: Process of sending and retrieving data from a specific primary shard. Elasticsearch uses a hashed routing value to choose this shard. You can provide a routing value in indexing and search requests to take advantage of caching. See the `_routing` field.

rule
: A set of conditions, schedules, and actions that enable notifications. See Rules.

Rules
: A comprehensive view of all your alerting rules. Enables you to access and manage rules for all Kibana apps from one place. See Rules.

runner
: A local control agent that runs on all hosts, used to deploy local containers based on role definitions. Ensures that containers assigned to it exist and are able to run, and creates or recreates the containers if necessary.

runtime field
: Field that is evaluated at query time. You access runtime fields from the search API like any other field, and Elasticsearch sees runtime fields no differently. See Runtime fields.

S

edit

saved object
: A representation of a dashboard, visualization, map, data view, or Canvas workpad that can be stored and reloaded.

saved search
: The query text, filters, and time filter that make up a search, saved for later retrieval and reuse.

scripted field
: A field that computes data on the fly from the data in Elasticsearch indices. Scripted field data is shown in Discover and used in visualizations.

search session
: A group of one or more queries that are executed asynchronously. The results of the session are stored for a period of time, so you can recall the query. Search sessions are user specific.

search template
: A stored search you can run with different variables. See Search templates.

searchable snapshot index
: Index whose data is stored in a snapshot. Searchable snapshot indices do not need replica shards for resilience, since their data is reliably stored outside the cluster. See searchable snapshots.

searchable snapshot
: Snapshot of an index mounted as a searchable snapshot index. You can search this index like a regular index. See searchable snapshots.

segment
: Data file in a shard's Lucene instance. Elasticsearch manages Lucene segments automatically.

services forwarder
: Routes data internally in an Elastic Cloud Enterprise installation.

shard
: Lucene instance containing some or all data for an index. Elasticsearch automatically creates and manages these Lucene instances. There are two types of shards: primary and replica. See Clusters, nodes, and shards.

shareable
: A Canvas workpad that can be embedded on any webpage. Shareables enable you to display Canvas visualizations on internal wiki pages or public websites.

shipper
: An instance of Logstash that send events to another instance of Logstash, or some other application.

shrink
: Reduces the number of primary shards in an index. See the shrink index API.

snapshot lifecycle policy
: Specifies how frequently to perform automatic backups of a cluster and how long to retain the resulting snapshots. See Automate snapshots with SLM.

snapshot repository
: Location where snapshots are stored. A snapshot repository can be a shared filesystem or a remote repository, such as Azure or Google Cloud Storage. See Snapshot and restore.

snapshot
: Backup taken of a running cluster. You can take snapshots of the entire cluster or only specific data streams and indices. See Snapshot and restore.

solution
: In Elastic Cloud, deployments with specialized templates that are pre-configured with sensible defaults and settings for common use cases.

source field
: Original JSON object provided during indexing. See the `_source` field.

space

A place for organizing dashboards, visualizations, and other saved objects by category. For example, you might have different spaces for each team, use case, or individual. See Spaces.

span

Information about the execution of a specific code path. Spans measure from the start to the end of an activity and can have a parent/child relationship with other spans.

split

Adds more primary shards to an index. See the split index API.

stack rule

The general purpose rule types Kibana provides out of the box. Refer to Stack rules.

standalone

This mode allows manual configuration and management of Elastic Agents locally on the systems where they are installed. See Install standalone Elastic Agents.

stunnel

Securely tunnels all traffic in an Elastic Cloud Enterprise installation.

system index

Index containing configurations and other data used internally by the Elastic Stack. System index names start with a dot (`.`), such as `.security`. Do not directly access or change system indices.

T

edit

tag

A keyword or label that you assign to Kibana saved objects, such as dashboards and visualizations, so you can classify them in a way that is meaningful to you. Tags makes it easier for you to manage your content. See Tags.

term join

A shared key that combines vector features with the results of an Elasticsearch terms aggregation. Term joins augment vector features with properties for data-driven styling and rich tooltip content in maps.

term

See token.

text

Unstructured content, such as a product description or log message. You typically analyze text for better search. See Text analysis.

time filter

A Kibana control that constrains the search results to a particular time period.

time series data stream

A type of data stream optimized for indexing metrics time series data. A TSDS allows for reduced storage size and for a sequence of metrics data points to be considered efficiently as a whole. See Time series data stream.

time series data

A series of data points, such as logs, metrics and events, that is indexed in time order. Time series data can be indexed in a data stream, where it can be accessed as a single named resource with the data stored across multiple backing indices. A time series data stream is optimized for indexing metrics data.

Timelion

A tool for building a time series visualization that analyzes data in time order. See Timelion.

token

A chunk of unstructured text that's been optimized for search. In most cases, tokens are individual words. Tokens are also called terms. See Text analysis.

tokenization

Process of breaking unstructured text down into smaller, searchable chunks called tokens. See Tokenization.

trace
: Defines the amount of time an application spends on a request. Traces are made up of a collection of transactions and spans that have a common root.

tracks
: A layer type in the **Maps** application. This layer converts a series of point locations into a line, often representing a path or route.

trained model
: A machine learning model that is trained and tested against a labeled data set and can be referenced in an ingest pipeline or in a pipeline aggregation to perform classification or regression analysis or natural language processing on new data.

transaction
: A special kind of span that has additional attributes associated with it. Transactions describe an event captured by an Elastic APM agent instrumenting a service.

TSVB
: A time series data visualizer that allows you to combine an infinite number of aggregations to display complex data. See TSVB.

U

edit

Upgrade Assistant
: A tool that helps you prepare for an upgrade to the next major version of Elasticsearch. The assistant identifies the deprecated settings in your cluster and indices and guides you through resolving issues, including reindexing. See Upgrade Assistant.

Uptime
: A metric of system reliability used to monitor the status of network endpoints via HTTP/S, TCP, and ICMP.

V

edit

vCPU
: vCPU stands for virtual central processing unit. In Elastic Cloud, vCPUs are virtual compute units assigned to your nodes. The value is dependent on the size and hardware profile of the instance. The instance may be eligible for vCPU boosting depending on the size.

vector data
: Points, lines, and polygons used to represent a map.

Vega
: A declarative language used to create interactive visualizations. See Vega.

visualization
: A graphical representation of query results in Kibana (e.g., a histogram, line graph, pie chart, or heat map).

W

edit

warm phase
: Second possible phase in the index lifecycle. In the warm phase, an index is generally optimized for search and no longer updated. See Index lifecycle.

warm tier
: Data tier that contains nodes that hold time series data that is accessed less frequently and rarely needs to be updated. See Data tiers.

Watcher
: The original suite of alerting features. See Watcher.

Web Map Service (WMS)
: A layer type in the **Maps** application. Add a WMS source to provide authoritative geographic context to your map. See the OpenGIS Web Map Service.

worker

The filter thread model used by Logstash, where each worker receives an event and applies all filters, in order, before emitting the event to the output queue. This allows scalability across CPUs because many filters are CPU intensive.

workpad

A workspace where you build presentations of your live data in Canvas. See Create a workpad.

X

edit

Y

edit

Z

edit

ZooKeeper

A coordination service for distributed systems used by Elastic Cloud Enterprise to store the state of the installation. Responsible for discovery of hosts, resource allocation, leader election after failure and high priority notifications.

On this page

Subscribe to our newsletter

Email address

Sign up

Follow us




PRODUCTS & SOLUTIONS

- Enterprise Search
- Observability
- Security
- Elastic Stack
- Elasticsearch
- Kibana
- Integrations
- Subscriptions
- Pricing

COMPANY

- Careers
- Board of Directors
- Contact

RESOURCES

- Documentation
- What is the ELK Stack?
- What is Elasticsearch?
- Migrating from Splunk
- OpenSearch vs. Elasticsearch
- Public Sector