Guance Full Stack Observability and Monitoring in One Platform

www.guance.one

# Guance
# Product White Paper

# Preface

Observability is an emerging concept in the era of cloud computing. Although not a new concept, it was previously used to ensure system stability through monitoring before entering the field of computer software. Few people mentioned observability in computer science until recently.

To effectively monitor a computer system, the monitored object must generate observable metrics and other data. Monitoring the data generated by the computer is the premise for monitoring. The value and significance of monitoring will decrease if there are few observable metrics or data. For example, if we can only monitor the status of a server, we cannot observe the state of the operating system above it. If we want to monitor the application, each application must be observable.

Monitoring is an action whose prerequisite is observability. More observable data means better control of the entire system. With the development of the Internet, we are about to face more Internet device access, such as the Internet of Things and the Industrial Internet under IoT technology. As a result, more new cloud technologies and data technologies will appear, and these devices and new technologies also need to be observable and have monitoring products to manage them. Monitoring and observability will continue to evolve to ensure the success of these complex systems.

Guance is an observability platform in the cloud era launched by cloud-based technology. It was created to meet the needs of users and keep up with the historical trend.

# Contents

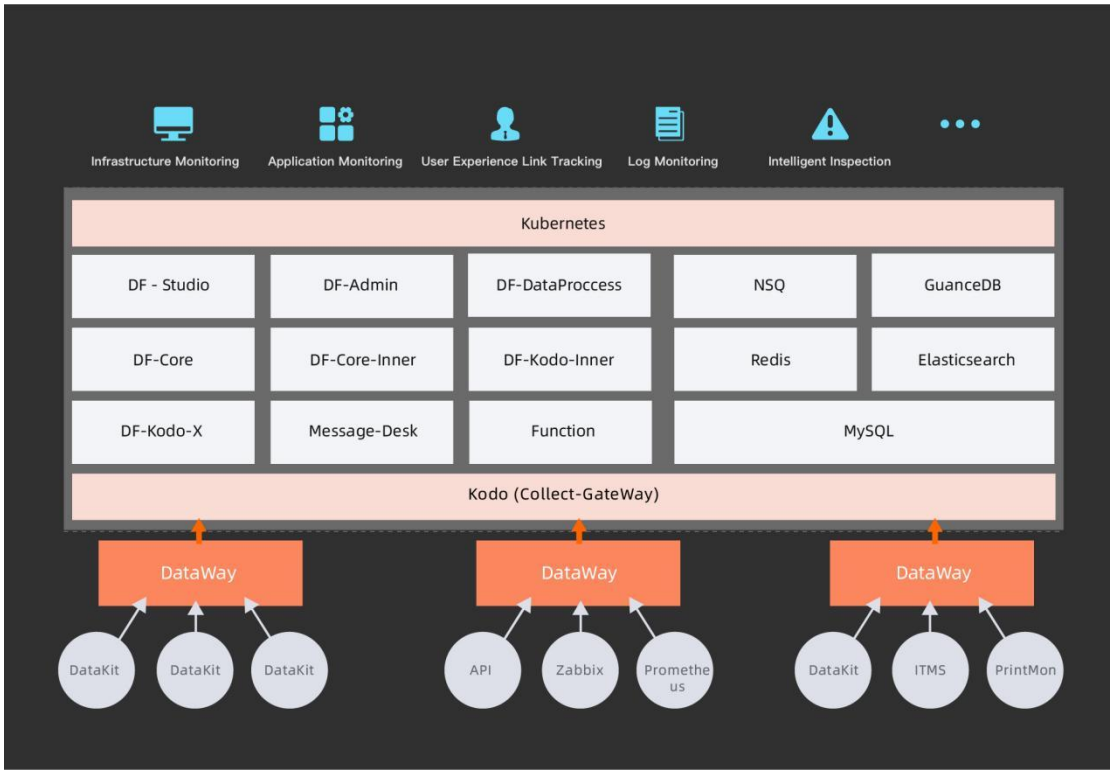
# Overview

Guance is a cloud service platform designed to solve the problem of cloud computing and build **full-link observability** for every complete application in the cloud native era system. Shanghai Guance Information Technology Co., Limited has been developing the product since 2018 to provide services for the vast number of **cloud-based development project teams** in China.

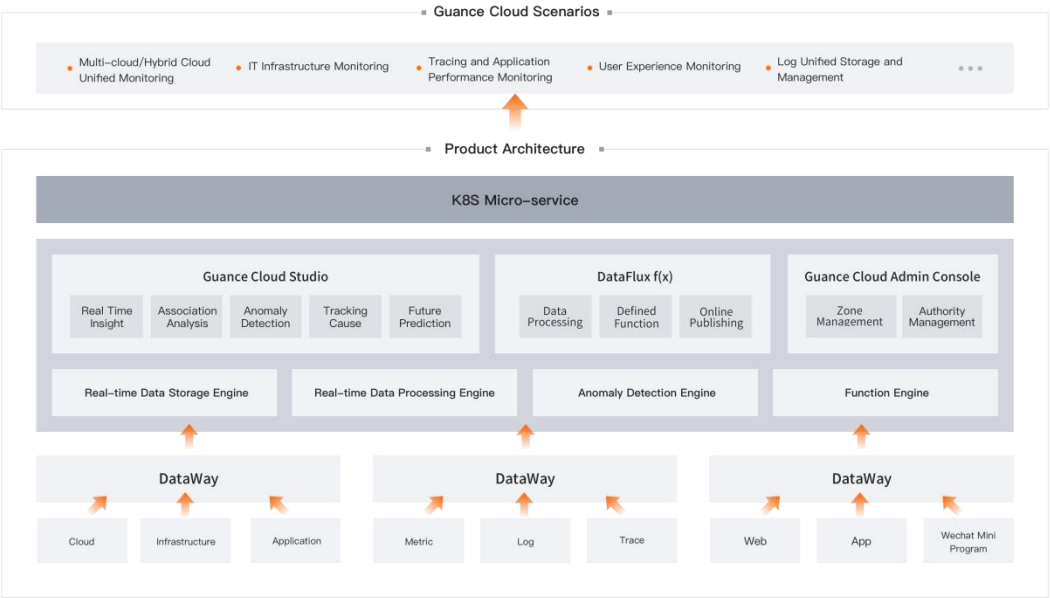
Compared to complex and changeable open source products such as ELK, Prometheus, Grafana, and Skywalking, Guance not only provides a monitoring product, but also offers overall observability services. This includes **integration of the underlying storage and system architecture**, as well as complete analysis and deconstruction of all the technology stacks related to cloud computing and cloud nativity. Any project team can easily use our products without investing too much energy to study or transform immature open source products.

Guance collects fees in the form of service, according to demand and quantity, and completely according to the amount of data generated by users, without hardware investment. For paying customers, we also establish a professional service team to help build **a core guarantee system based on data**.

# System Architecture




# Product Architecture



Guance platform architecture is generally divided into four layers:

- **Data collection layer:** Guance's data collection supports various data collectors, including the official DataKit, open-source Telegraf and Prometheus, etc. Users can also develop custom collectors through WDF and DataWay API. Guance data collector can collect various data types such as cloud, infrastructure, applications, me09o-ilitrics, logs, links, Web, App, and applets, meeting the requirements of real-time and high-frequency data collection.
- **Data gateway layer:** Guance's data gateway layer is based on the self-developed DataWay gateway, which can realize the functions of data proxy reporting and data cleaning.
- **Data analysis and processing layer:** Guance's data analysis and processing layer is divided into three modules: Guance data analysis and insight platform, Guance data processing development platform, and Guance management background. Guance realizes real-time insight, association analysis, anomaly detection, and cause tracking of data based on a time-series data storage engine and an anomaly detection engine. Guance data processing development platform realizes the development and online publishing of data processing functions based on a real-time data processing engine and a function calculation engine.
- **API Gateway layer:** Guance is based on K8S micro-service architecture, which meets the needs of enterprises to develop custom data applications through the scalability provided by Inner API.

# Product Advantages

## Unified Storage

Guance adopts a unified storage scheme, and the bottom layer adopts a multi-mode data lake form. We store data structures such as time series, logs, objects, links, and events in a unified way, realizing consistent, efficient, and low-latency writing through a unified Dataway interface through the Line Protocol. The self-developed query language DataFlux Query Language (DQL) carries out unified query and analysis.

## Powerful and Secure Data Collection Scheme

We provide a powerful data collection terminal DataKit independently developed, which integrates comprehensive data collection capabilities, including hosts (cloud hosts), containers, processes, middleware, databases, message queues, applications developed in various languages, network access performance, black box dialing tests, security inspections, etc. We are also compatible with open-source mainstream data collection schemes, such as Prometheus, Telegraf, etc. Compared with these schemes, besides collecting the corresponding index data and log data of the corresponding technical stack, the most powerful part is that it can effectively build a unified relationship between all the data, which is convenient for users to quickly find the relationship between metrics.

## Full-link Observability

Based on powerful data collection capabilities, Guance is built for infrastructure, container, middleware, database, message queuing, application link, front-end access, system security, network access performance, providing full-link observability. Based on our standard products, when users correctly configure DataKit, they can quickly realize the complete observability construction of their own projects. At the same time, based on the Line Protocol and our scene construction ability, users can also customize the metrics they need to observe and integrate them conveniently to achieve further observability.

## User-friendly Interface

As a complete technical product oriented to observability, Guance has many technical thresholds. Compared with various open-source schemes, we strive to reduce the learning cost of using our products and improve the ease of use for users from the beginning. We reduce the configuration difficulty of users, conforming to the habits of most programmers and operation and maintenance engineers, and improve the ease

of use and professionalism of the UI. This way, users can quickly understand the users of products and the value they bring.

### Powerful Technology

Throughout the entire product construction process of Guance, we have accumulated a robust technical system and strength. In addition to Datakit, which has high performance and can be completely cross-platform, DataWay data gateway has powerful data processing capabilities, an independent query language DQL, a self-developed log text data batch script pipeline, a script model Scheck that can perform complete security inspections, and a powerful algorithm development platform Function.

### Service-Based

Guance, as a DevOps-oriented platform, helps project teams build complete and observable products. In addition to providing product abilities, we also provide all-around services for our commercial customers, including a technical service team for each customer. During the usage process, we assist every user in commercial customers, whether programmers, test engineers, or operation and maintenance engineers, in effectively obtaining real benefits from the use of Guance.

# Key Technology

As a system observability platform in the cloud era, Guance includes five key technologies:

1. **Data storage technology based on time series and column data**

Time series and column databases have a high compression ratio and superior writing and query performance, which can meet massive and high-frequency data writing

requests at the data writing end and realize flexible multi-dimensional query and association analysis at the data reading end.

**2. Compatible with multiple text analysis engines**

Support text analysis engine databases such as OpenSearch and Elasticsearch, realize the unified storage of log, object, link, event, and other data structures. Through the unified Dataway interface, it realizes the consistent, efficient, and low-delay writing through the Line Protocol. The self-developed query language Debug Query Language (DQL) carries out unified query and analysis.

**3. Low-intrusive bypass data collection technology**

Data collection is the initial link of data analysis on the big data platform. Most data collectors of Guance realize the function of data collection based on bypass technology, which can complete the task of data collection without affecting the business system as much as possible.

**4. Data consistency assurance and high system reliability**

On the whole link from data collection to data cleaning to data processing, Guance ensures the consistency of data based on message queue technology and multi-attempt mechanism, and makes up for the weakness of time series and column number databases. At the same time, based on k8s and Alibaba Cloud's highly available time series database products, we ensure the reliability of the entire system.

**5. Cloud native**

The entire platform is based on cloud-native products in the selection of underlying technical modules and the overall architecture, which achieves high cost performance on the premise of ensuring the integrity of functions and the reliability of technical architecture.

# Function Introduction

## Data Collection

Guance has the ability of global data collection and supports the collection of various data sources, such as machine data, log data, link tracking data, business data, cloud platform data, and industry public data. The data collection of Guance has the characteristics of real-time. Besides the standard data collector DataKit developed by the government, we also support third-party data collectors such as Telegraf and Prometheus Exporter.

## DataWay

DataWay is a data gateway deployed in the user environment, which has two main functions:

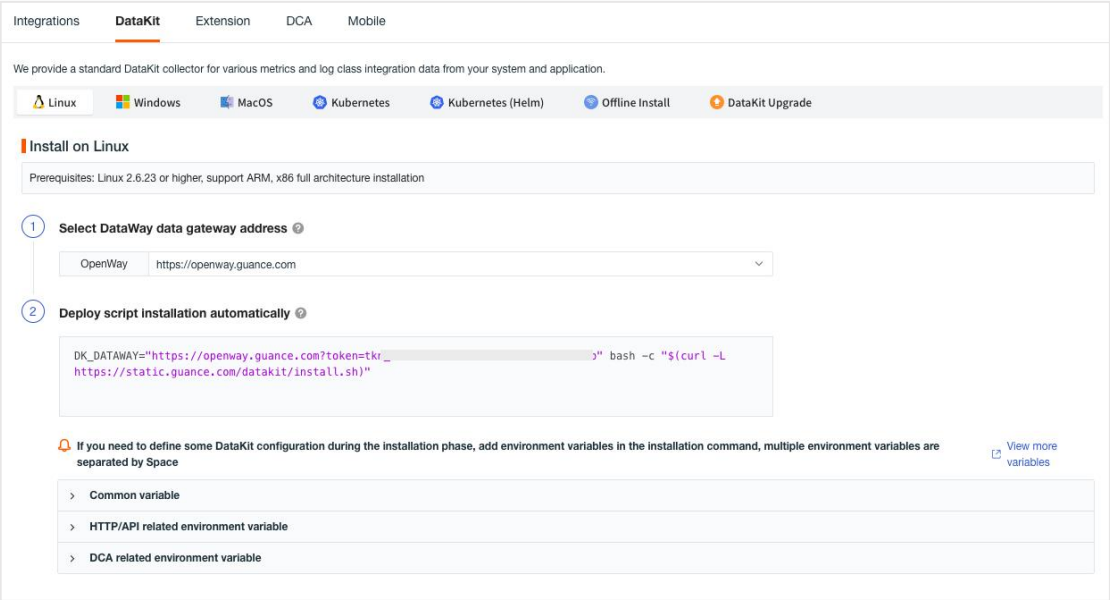
- Receiving the data sent by the collector, and then reporting the data to the Guance center for storage.
- Processing the collected data and then sending it to the Guance center for storage.

## DataKit Collector

DataKit is a real-time data collector developed by the government, which supports the collection of hundreds of kinds of data, covering most data types. Configuration tutorials and instructions for all data sources can be found in the **Integration** of the Guance studio.

After collecting data, DataKit needs to send it to DataWay data gateway, and DataWay gateway will finally report the data to the Guance center for storage. DataKit needs to be deployed into the user's own IT environment and supports multiple operating systems.

Users can log in to the **Integration > DataKit** page of the Guance studio to view and use the DataKit installation instructions.




DataKit supports remote administration through DCA (DataKit Control APP). DCA facilitates the management of installed and configured collectors, and supports functions such as viewing collector operation, collector configuration management, Pipeline management, blacklist management and collector document help.

To view the installation steps of DCA in the Guance workspace, click **Integration > DCA**.

Integrations DataKit Extension **DCA** Mobile

DCA is the DataKit online management platform that supports viewing DataKit operation and unified management of configuring collectors, blacklists, and pipelines.

**Offline Installation**

Only Docker image installation is currently supported

1 **Download mirror**

Download the DCA image via docker pull

```
docker pull pubrepo.guance.com/tools/dca
```

2 **Run containers**

Create and start the DCA container with the command docker run，The container default exposed access port is 80.

```
docker run -d --name dca -p 8000:80 pubrepo.guance.com/tools/dca
```

- -d # Means running in the background
- --name # Name of the created container
- -p 8000:80 # Port mapping, i.e. mapping local port 8000 to port 80 inside the container

After execution, you can use your browser to access to initialize the operation interface

**Additional supported installation variables are as follows, and can be custom configured, separate multiple environment variables with spaces**

- DCA_INNER_HOST：The auth API address of the Guance, the default value is https://auth-api.guance.com
- DCA_FRONT_HOST：The console API address of the Guance, the default value is https://console-api.guance.com
- DCA_LOG_LEVEL：Log level, take the value of NONE | DEBUG | INFO | WARN | ERROR, if you do not need to record logs, you can set to NONE
- DCA_LOG_ENABLE_STDOUT：default is false, logs will be output to a file, located under /usr/src/dca/logs. If you need to write logs to stdout, you can set it to true

Example：

```
docker run -d --name dca -p 8000:80 -e DCA_LOG_ENABLE_STDOUT=true -e DCA_LOG_LEVEL=WARN pubrepo.guance.com/tools/dca
```

# Scenes

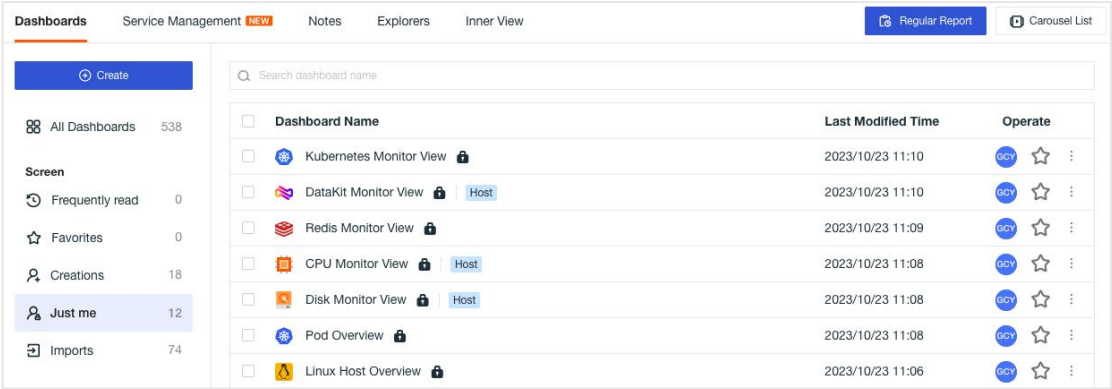
In Guance, users can build different insight scene instrument versions, take notes, and customize explorers according to different perspectives to meet the scene requirements and data analysis of different businesses.

# Dashboards

In **Scenes**, users can create multiple dashboards to build data insight scenarios. Users can build different dashboards according to different business requirements, such as infrastructure and application monitoring, Nginx, JVM, Docker monitoring, etc.

- Support exporting dashboards as reports and sending them to relevant personnel via email on a scheduled basis based on different time dimensions.
- Support modifying, exporting, and deleting existing dashboards.
- Support filtering dashboards through Favorites, Import Projects, Creations, and Frequently Read.
- Support grouping and filtering dashboards using tags.

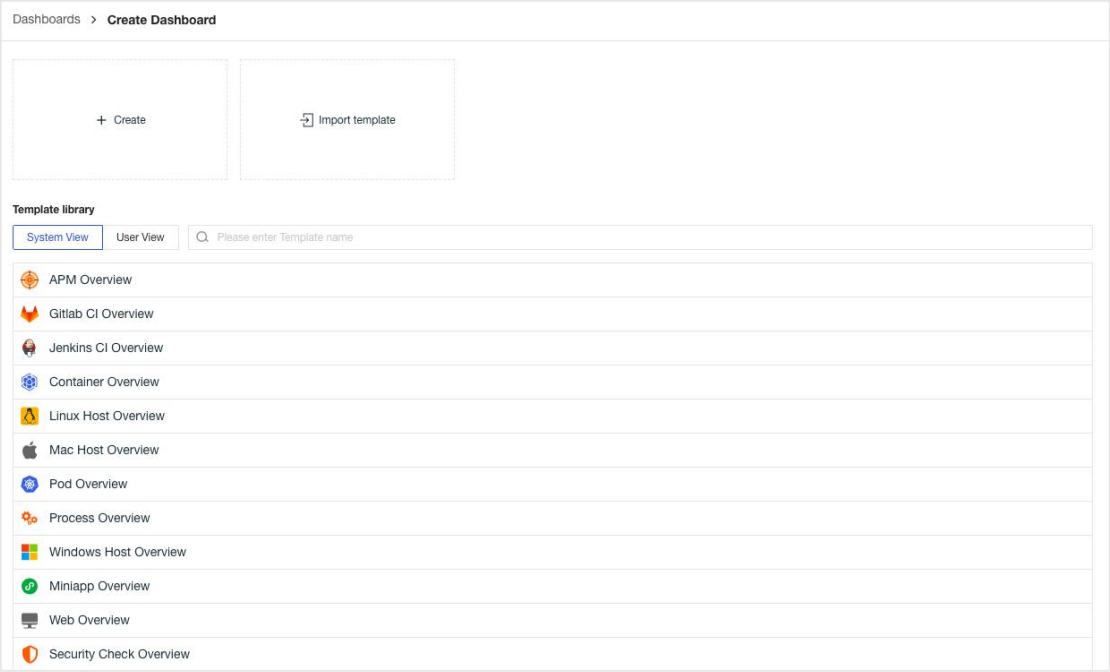
- Support setting viewing permissions for dashboards as public or private (only visible to oneself).
- Support carousel display of multiple related business dashboards.
- Support creating Issues, saving snapshots, and saving inner views for the current dashboard.
- Support switching to view chart information for authorized workspaces.
- Support for setting workspace level home Dashboard




## Create Dashboards

After entering **Scenes**, click **Create** in **Dashboards** to select the dashboard template you want to create. You can create a blank dashboard and customize the charts in the dashboard, import custom view templates, or select a inner template from the template library.

- Blank Dashboard: Create a blank dashboard and subsequently customize the charts in the dashboard.
- Custom Templates: Import custom view templates.
- Inner template library: Include system provided view templates and user-defined created view templates, no configuration required, ready to use.




# Regular Report

Regular report supports exporting dashboards as reports in different forms, and sending them to relevant personnel on a regular basis according to different time dimensions such as daily, weekly, and monthly.

To create a scheduled report, follow these steps:

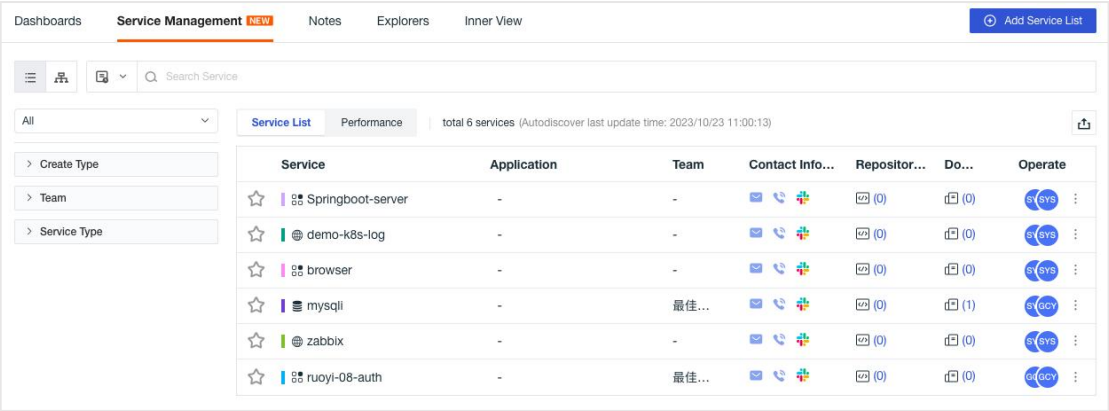
- Go to the Scenes section.
- Click on Dashboards.
- Select the desired dashboard.
- Click on Regular report.

# Service Management

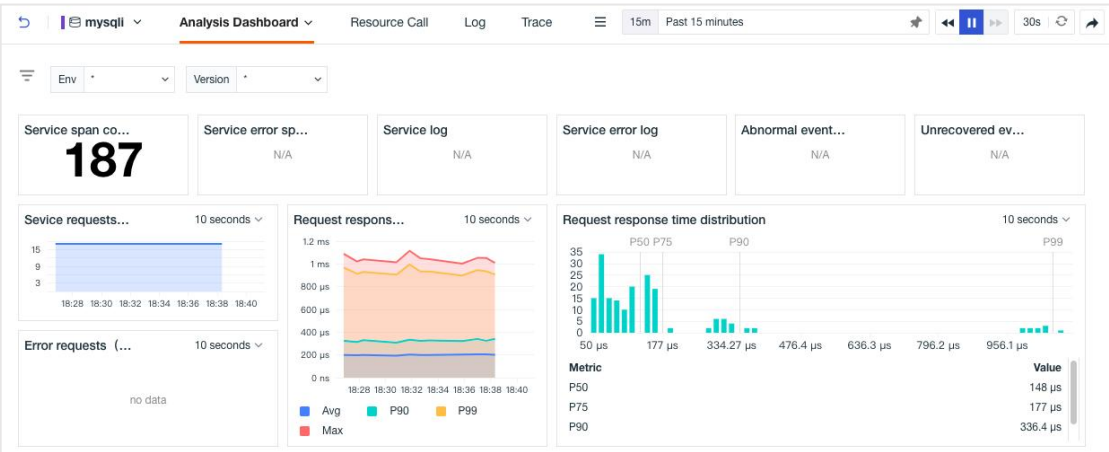
Service Management supports accessing and viewing key information from all services within the current workspace from a global perspective. By linking with repositories and documents, it allows for quickly identifying the code location and problem-solving solutions for urgent issues.

After entering **Scenes**, click on **Service Management > Add Service List** to create a new service. Once created, it can be viewed from three perspectives: service inventory list, performance list, and service topology diagram.

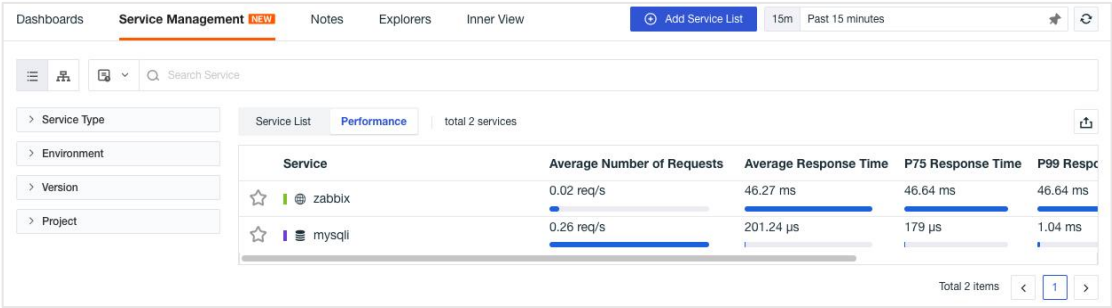
## 1. Service Inventory



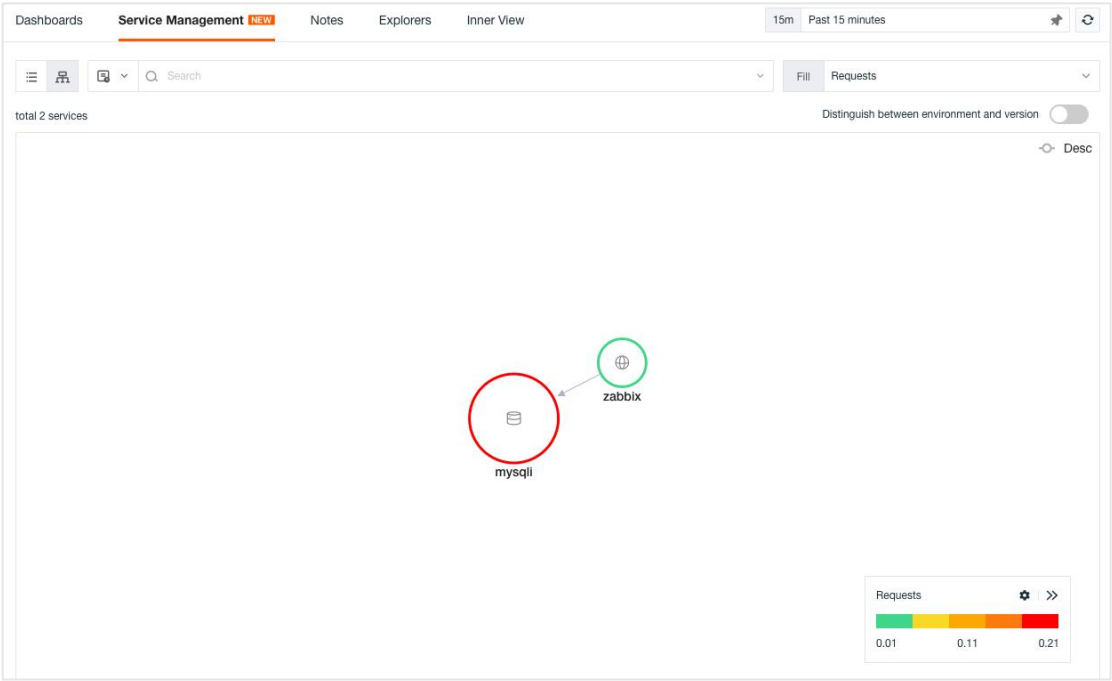

Click on any service to view its related information.



### 2. Performance




### 3. Service Map

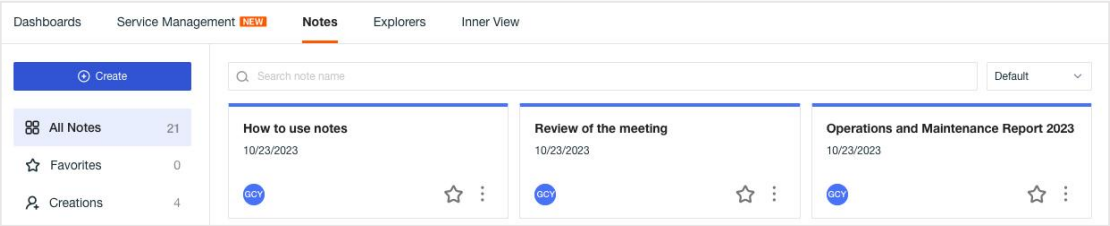



# Notes

In **Scenes**, you can create multiple notes for summarizing reports, storing abnormal data analysis, and helping with problem tracing, locating, and solving.

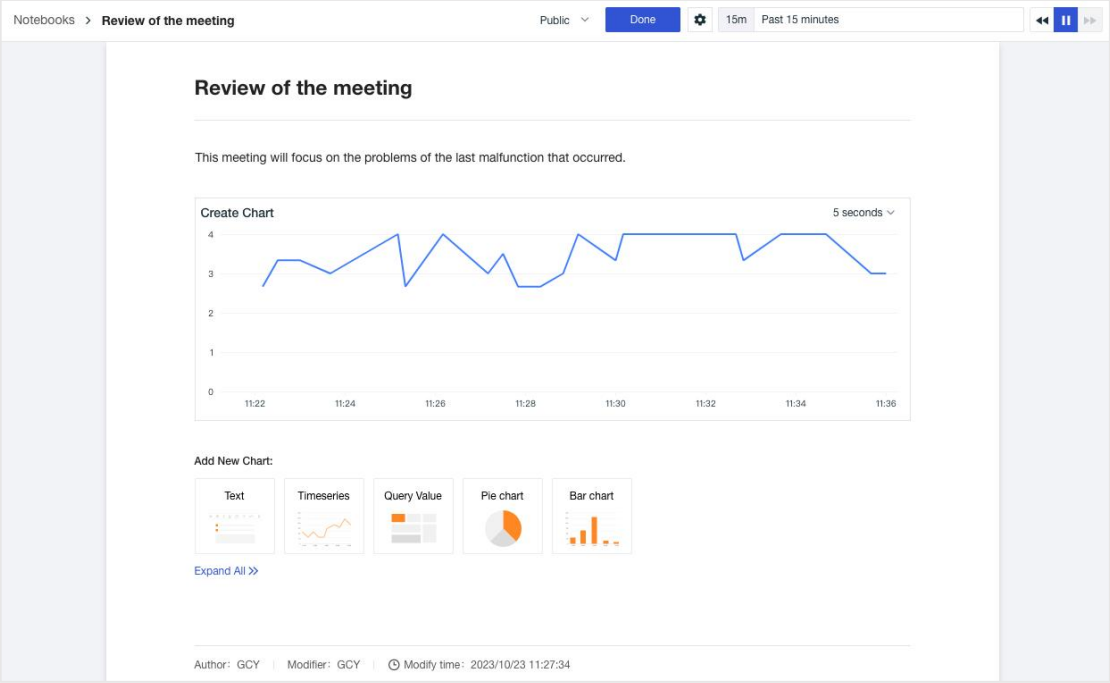
- Supports inserting real-time visual charts for data analysis, and inserting text documents for explanations, combining charts and documents for data analysis and summary reports.
- Supports setting viewing permissions for notes as public or private, by setting public notes to be shared with all members in the workspace.

- Supports modifying and deleting existing notes.
- Supports filtering notes through "My Favorites" and "My Creations".




## Create Notes

After entering the **Scenes**, click **Create** in **Notes** to add notes for editing.

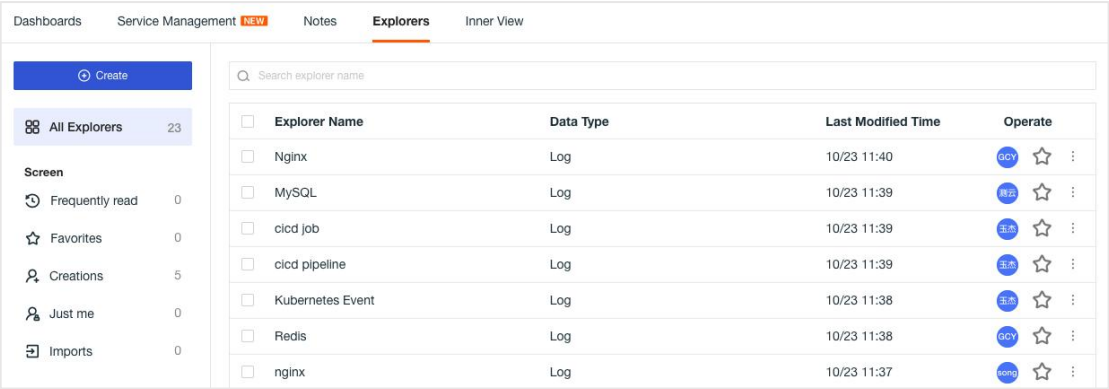



# Explorers

In **Scenes**, you can quickly build multiple custom explorers in collaboration with space members to meet specific viewing needs.

- Supports modifying, exporting, and deleting existing dashboards.
- Supports adding the current explorer to infrastructure, metrics, logs, application performance monitoring, real user monitoring, synthetic tests, security check, and CI visibility navigation menus.

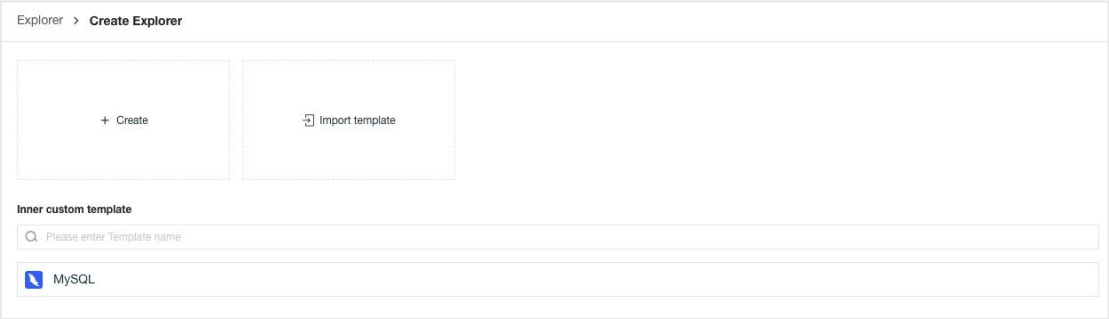
- Supports dashboard filtering through "My Favorites," "Imported Projects," "My Creations," and "Frequently Read."
- Supports setting viewing permissions for explorers as public or private.
- Supports grouping and filtering explorers using tags.
- Supports creating Issues and saving snapshots for the current explorer.
- Supports switching explorer information for authorized workspaces.




## Create Explorers

After entering **Scenes**, click **Create** in **Explorers** and complete the custom explorer name and label to create a new explorer.

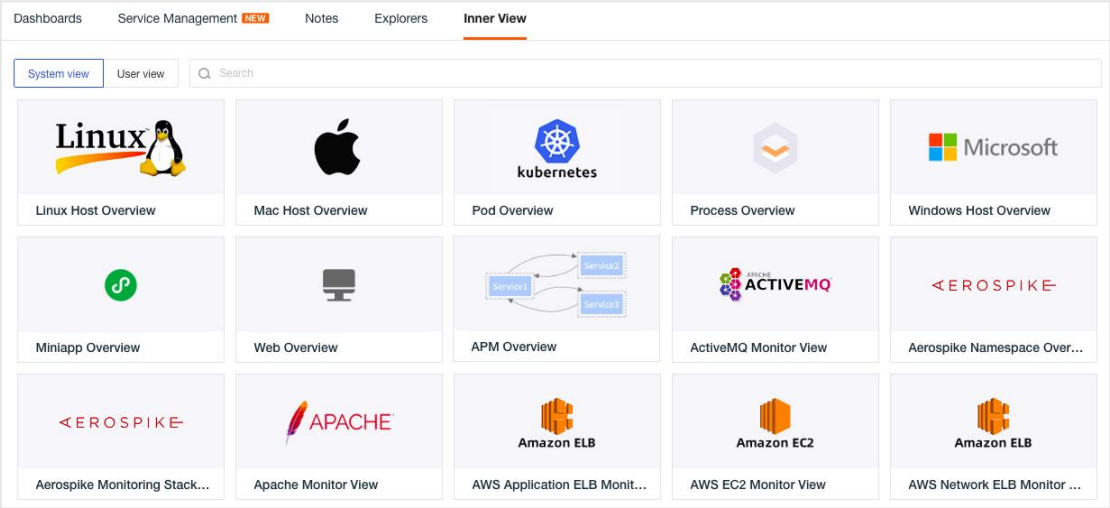
- Blank Explorer: Create a blank explorer that can be customized later.
- Custom Template: Import a custom explorer template for use.
- Inner Explorer Templates: explorer templates provided by the system, ready to use without any configuration.



# Inner View

Inner view displays all view templates of the current workspace, including system view and user view. You can view and edit it in the workspace **Scenes > Inner View**.

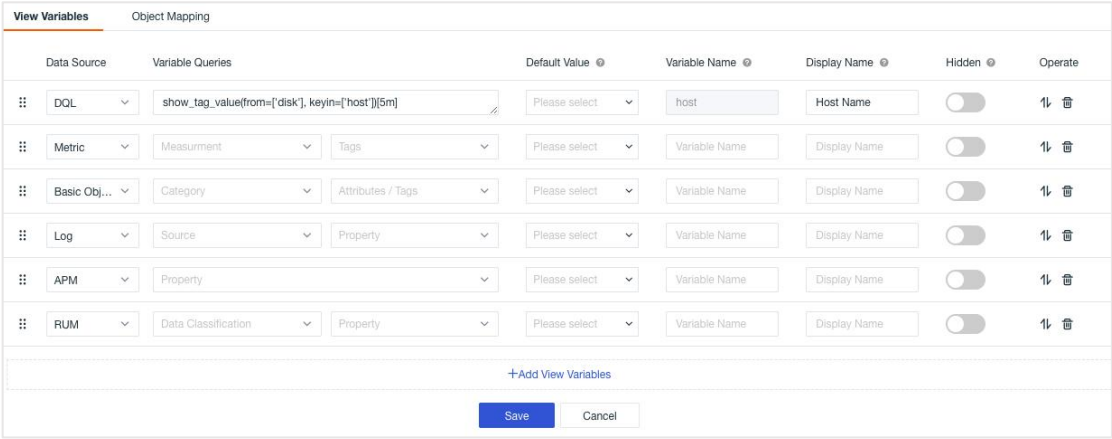
- Support creating dashboards in the scene selection with inner view template library
- Support exporting to dashboard from inner views
- Support manually binding inner views in the explorer




# View Variable

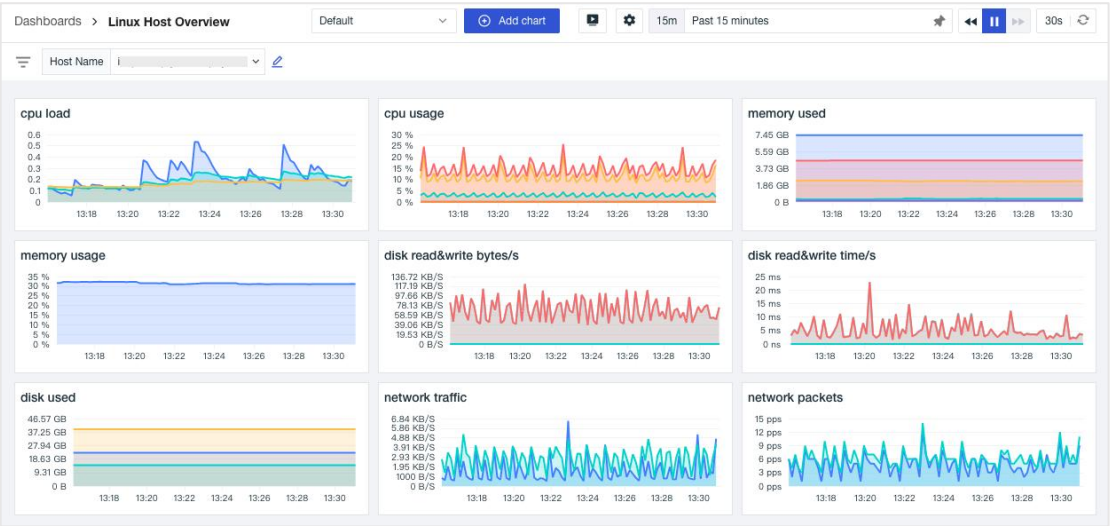
Add view variables in the dashboard and enter the view variable configuration page. After the view variable configuration is completed, use view variables in the chart to complete the dynamic screening of the chart.

- View variables support multiple selections, and multiple default values are supported during configuration;
- The data sources supported by view variables include **DQL**, **PromQL, Metrics**, **Basic Object**, **Custom Object**, **Log**, **Application Performance**, **User Access**, **Security Check**, and **Custom**.




Object view variables support attribute mapping function. After setting according to the following steps, you can view the set variable names in the view and display them in the chart with the display format of **Mapped Field (Original Field)**.

- First define a view variable based on the object class fields
- Select the fields to be mapped for the object category in **Object Mapping**
- Group the mapped labels in the **Chart Query**
- Enable **Field Mapping** in **Settings**




# Visual Chart

On the chart adding page, you can choose chart type, query method and chart setting.

- Chart query methods include simple query, expression query, PromQL query and DQL query.

- Chart types include time sequence chart, overview chart, pie chart, histogram, SLO, ranking list, dashboard, scatter chart, bubble chart, table chart, rectangular tree chart, funnel chart, China map, world map, honeycomb chart, log flow chart, object list chart, alarm statistical chart, text, video, picture, command panel and IFrame. Users can select the corresponding chart presentation mode according to the content they need to query and support grouping and combination chart presentation.

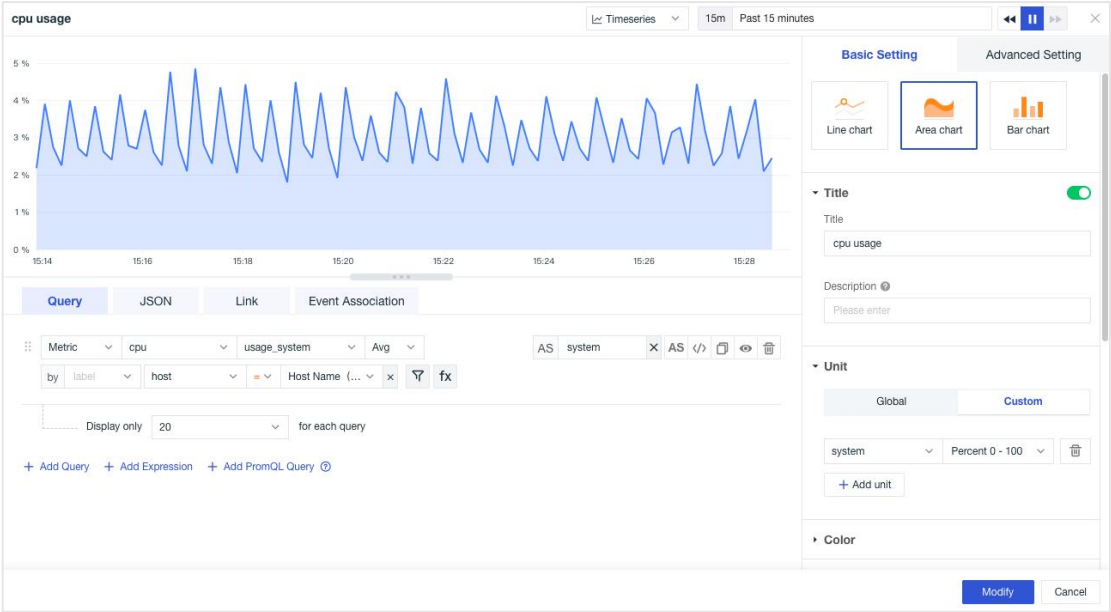
## Chart Query

Visual charts in the dashboard support three types of queries: simple queries, expression queries and DQL queries. A chart supports multiple queries at the same time. Chart query supports selecting different labels for grouping display, selecting multiple labels for data filtering at the same time, adding functions for data collection, and modifying aliases for queries.

**1. Simple query**

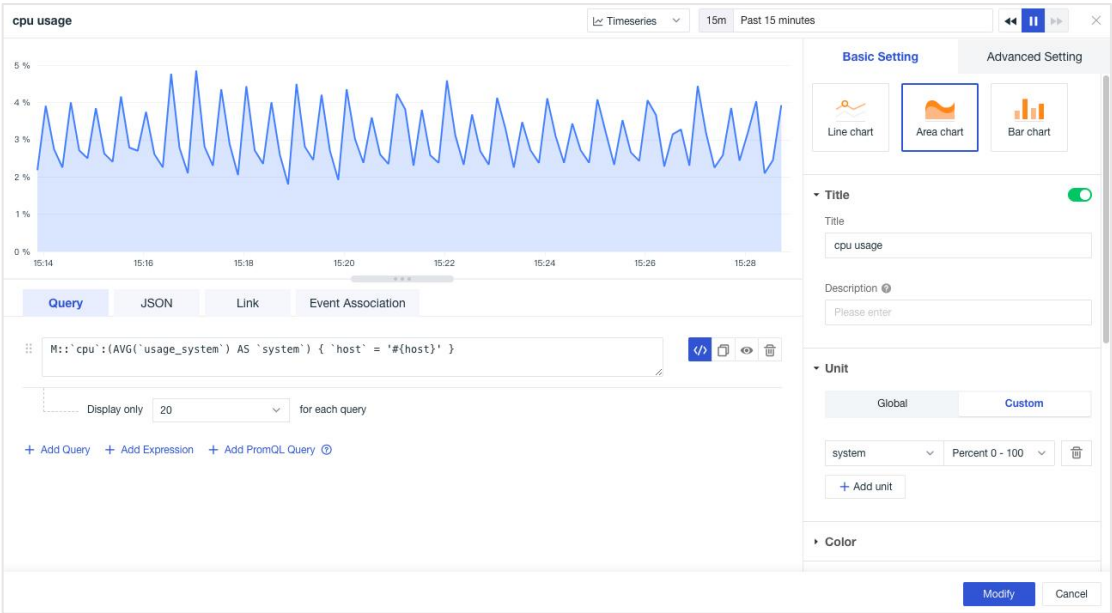
Different data sources can be selected for query, and chart display can be adjusted through functions, grouping, labels, etc. Data sources include metrics, logs, basic objects, custom objects, events, application performance, user access, security check, network, Profile, etc.

- A chart supports multiple query statements at the same time.
- Support grouping queries by selecting multiple tags.
- Support adding functions to query for data calculation.
- Support modifying aliases for queries.
- Support hiding a query result on the chart.
- Support presetting query field values for queries.



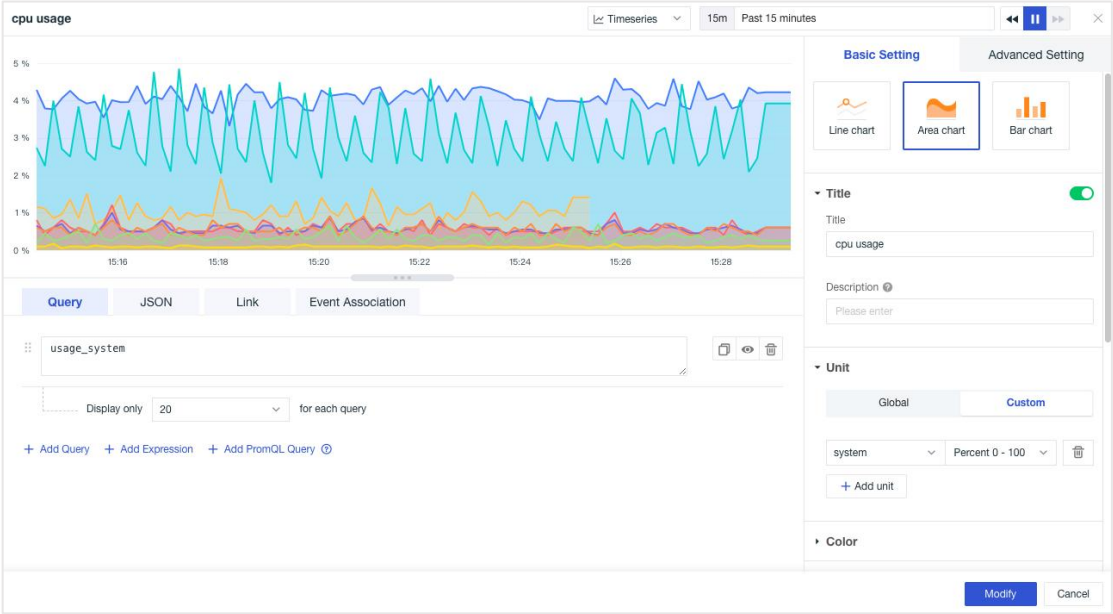

## 2. DQL query

DQL is a language specially used for Guance data query. You can manually enter DQL for query according to DQL syntax and click < > between simple query and DQL query.



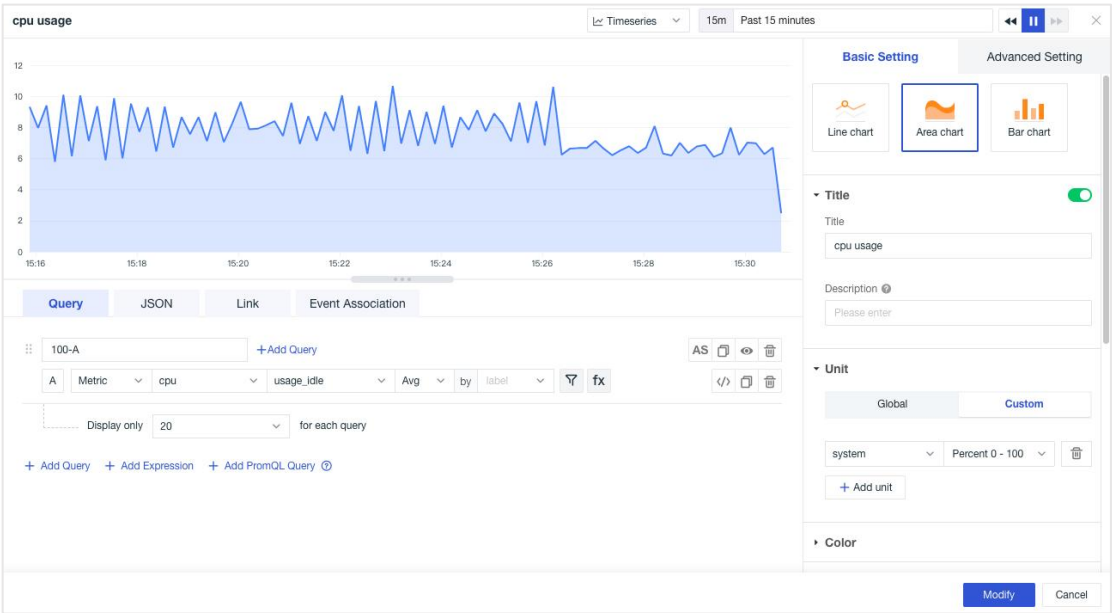

## 3. PromQL query

PromQL is a kind of query language used in Prometheus to query its time series data



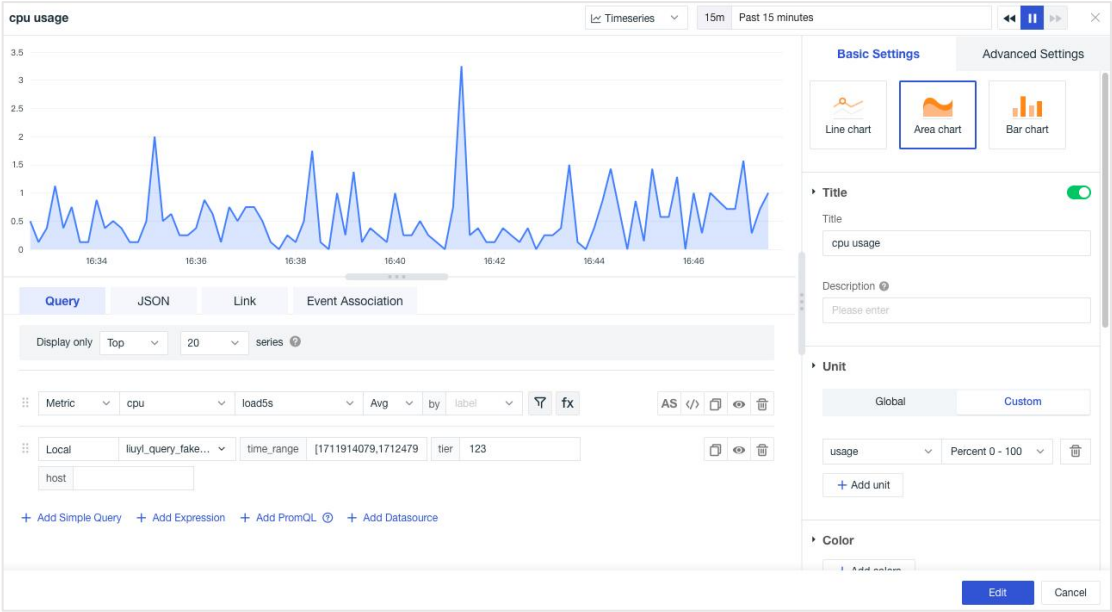

## 4. Expression

Add expression evaluation on the basis of simple query and DQL query.



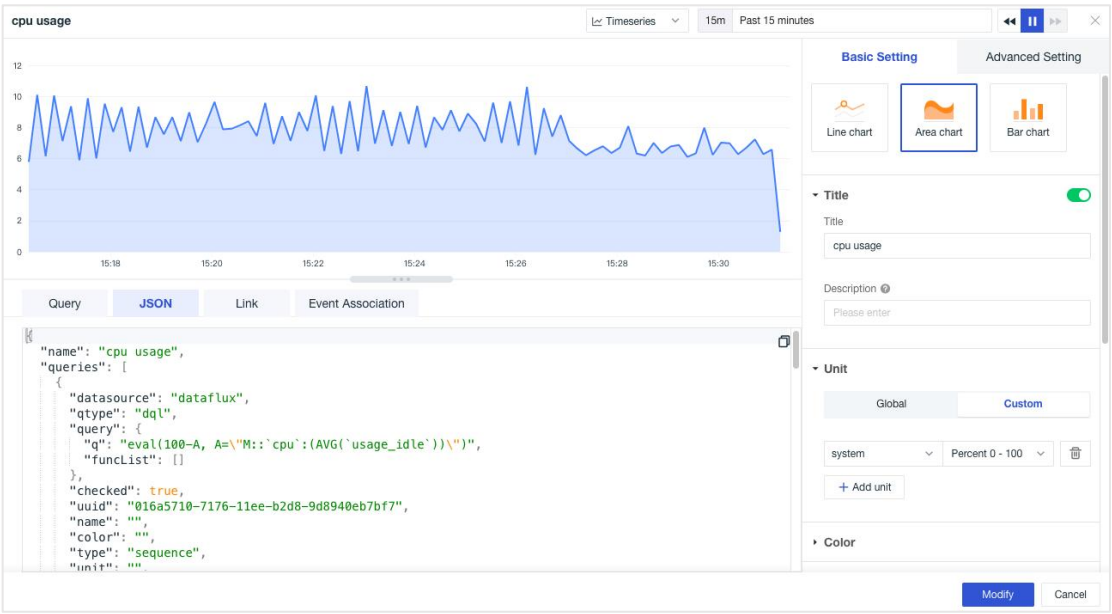

## 5. Datasource

Filtering, searching, aggregating and analyzing data attributes stored in the database.




# JSON

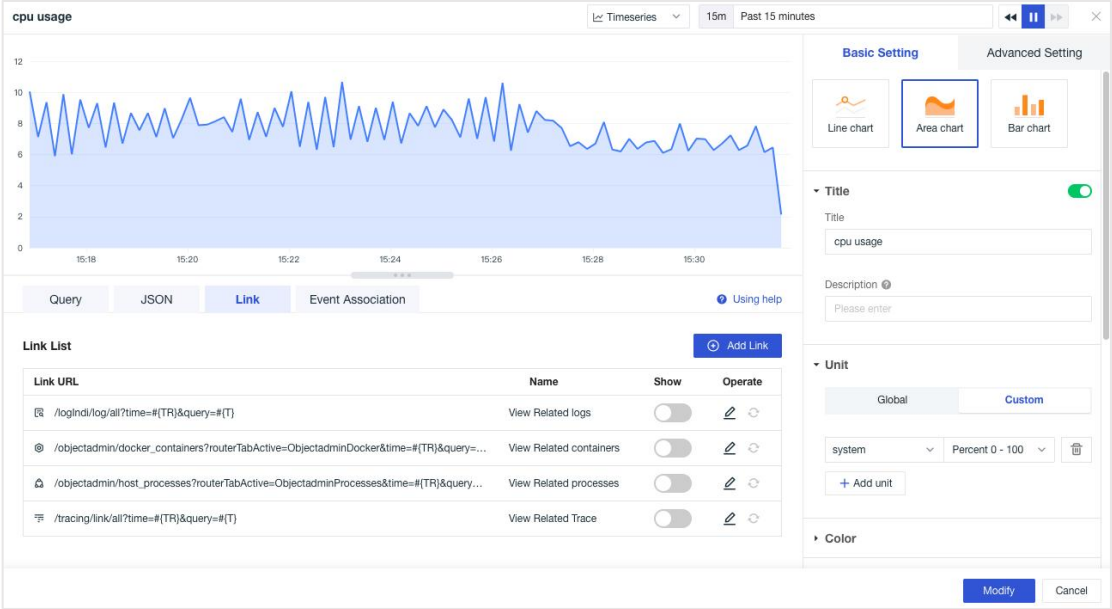
When editing charts, each correct query corresponds to a JSON text, support copy and paste. It supports editing JSON and linking with query/setting, checking the input JSON and displaying error message if there is any error.




# Links

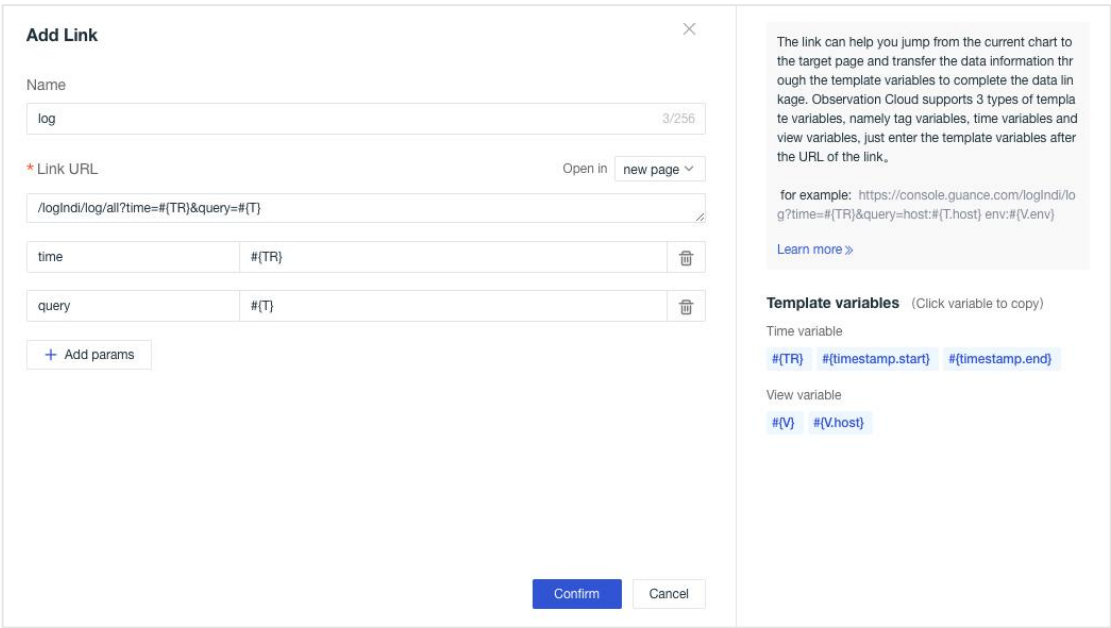
Links can realize jumping from the current chart to the target page. It supports adding internal links and external links of the platform and modifying the corresponding

variable values in the links through template variables to transfer data information to complete data linkage.



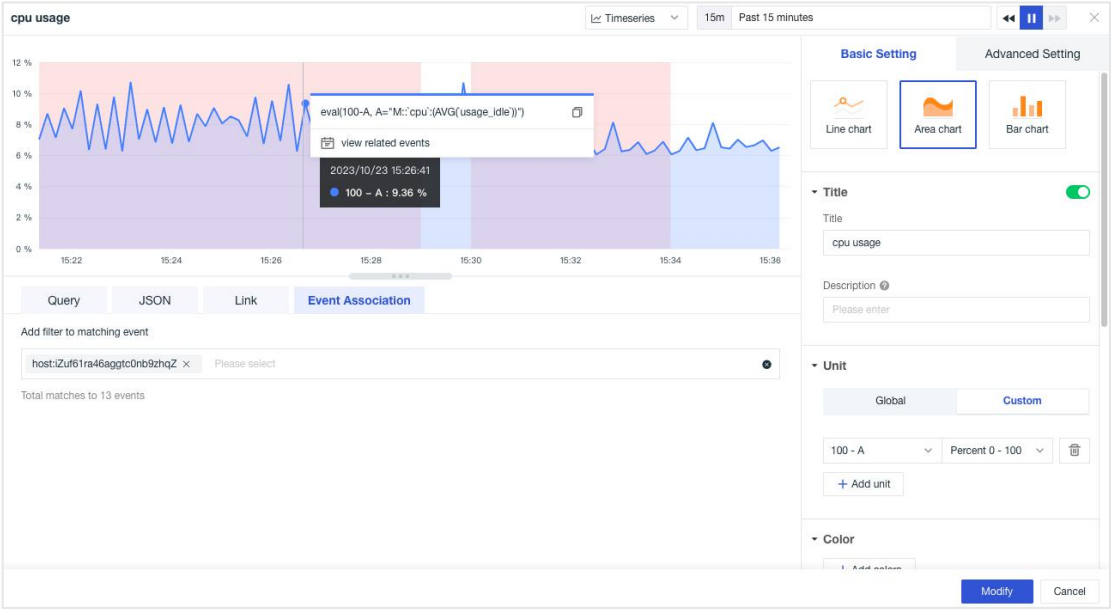

## Custom Link

Guance supports adding custom links to charts. On the basis of text box input, the final chart association link address is generated through free combination of parameter configuration to view relevant data. After adding custom links, it will be displayed by default, and relevant links can be displayed directly in chart preview.



# Event Association

Event association can detect whether there are related events during data fluctuation while viewing trends, which helps to locate problems. In the sequence chart event association, the abnormal events related to the selected fields are matched by adding filter fields. After the addition is completed, if there are event records, shadow highlights will be marked on the sequence chart; Click to view the exception events related to the selected field.




# Chart Analysis

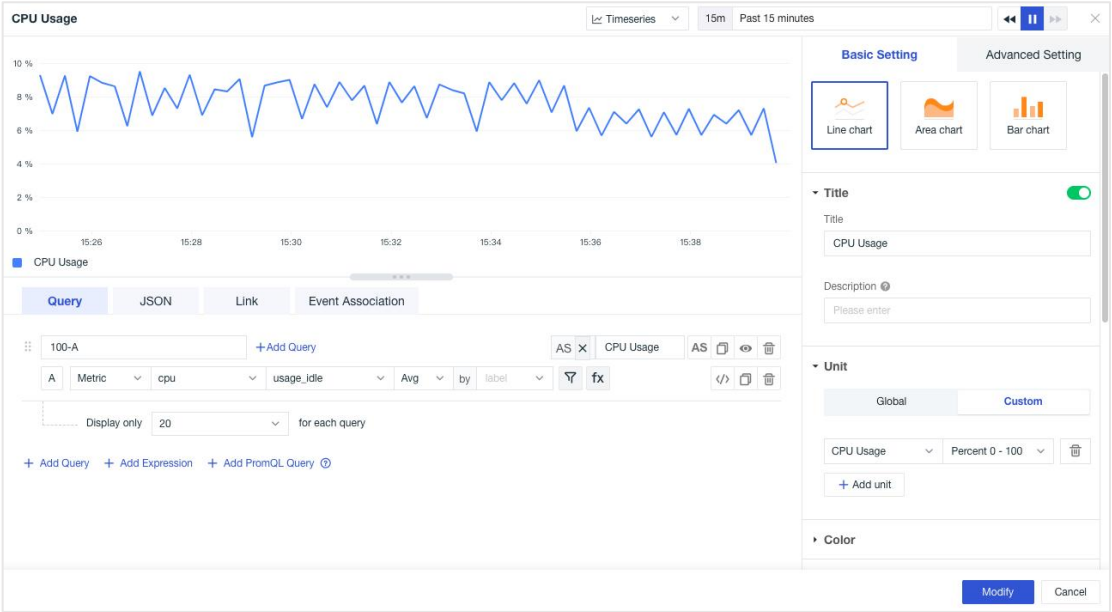
Guance suppors in the analysis mode of time series charts, through similar trend analysis, root cause analysis, drill-down analysis, further analyze and troubleshoot indicator data, quickly discover problems.

Note: Currently, root cause analysis supports two metrics, disk usage and memory usage.

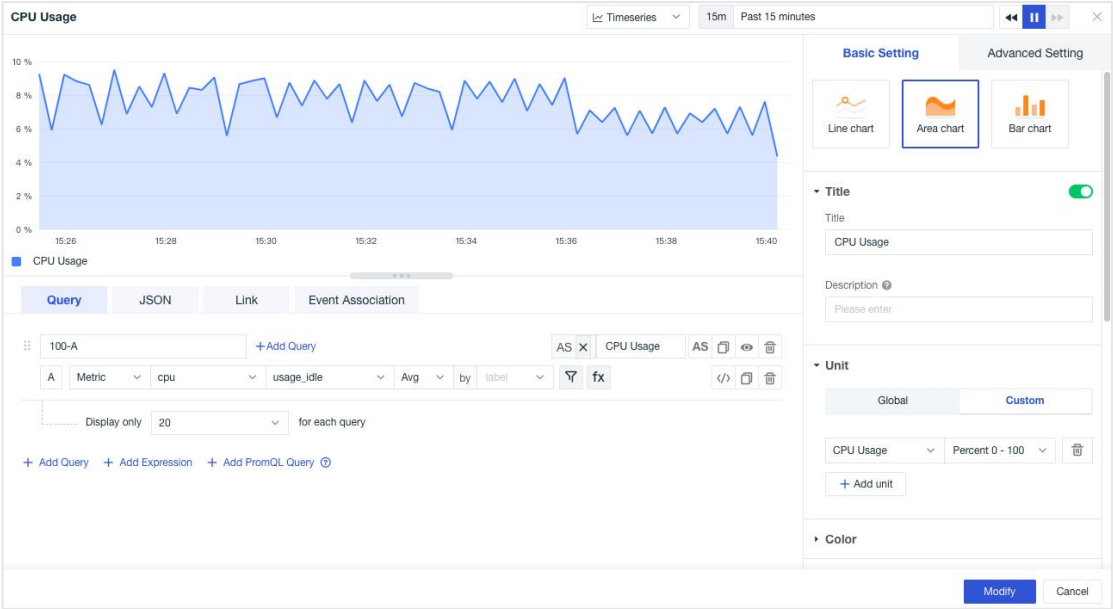

# Timeseries

Timeseries are commonly used to show changes in data over equal time intervals, and can also be used to analyze the effects and interactions among multiple groups of metric data. Chart types supported include line charts, bar charts, and area charts.

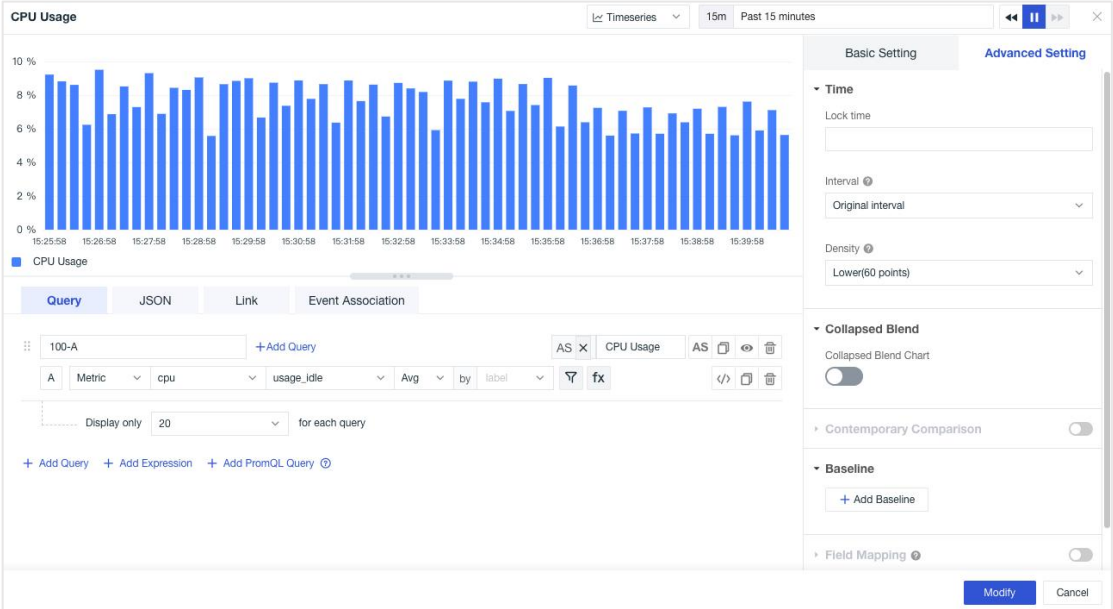
1. Line chart




2. Area chart

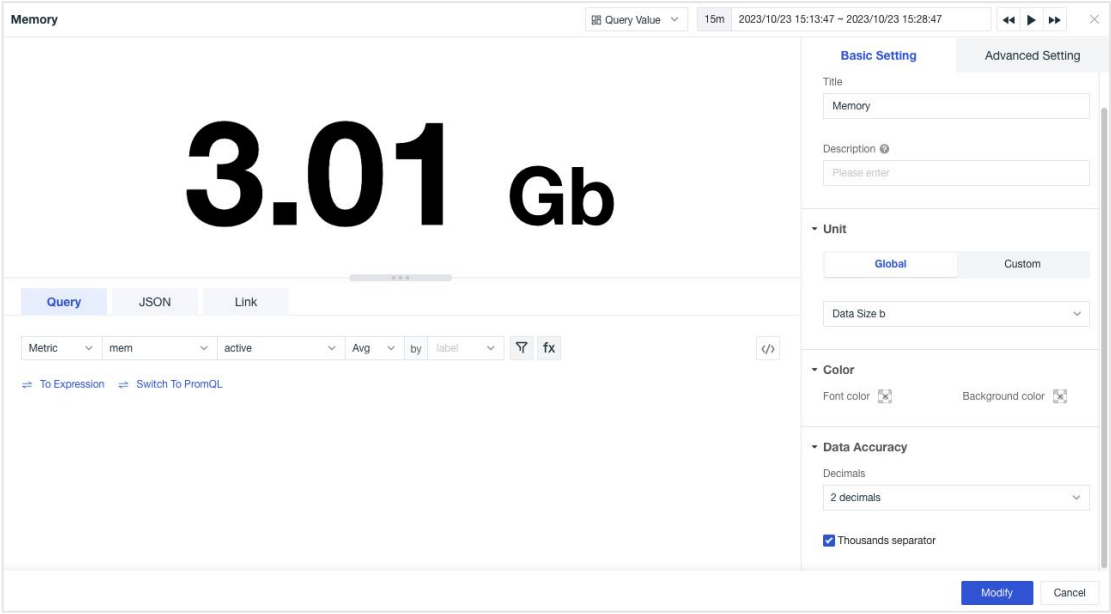



3. Bar chart




# Query Value

The query value can clearly show the result value of a metric. Users can set thresholds, colors and mapping values. At the same time, it supports mixed display with line charts, which helps users know the metric trend while querying the current metric value.

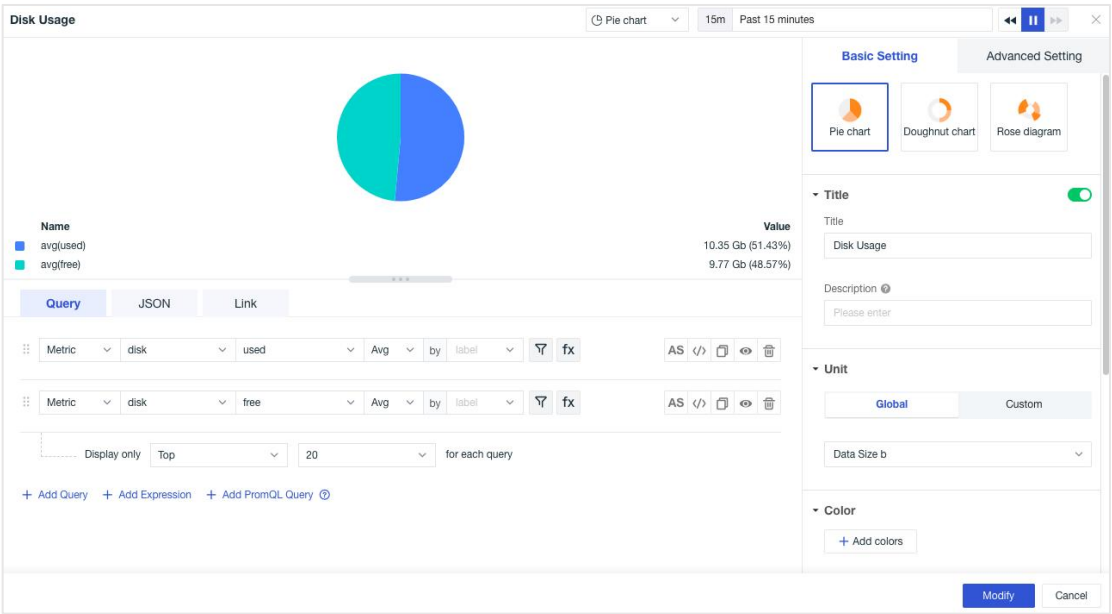



# Pie Chart

Pie charts are generally suitable for showing the comparison of data groups. Guance supports three pie chart style settings:

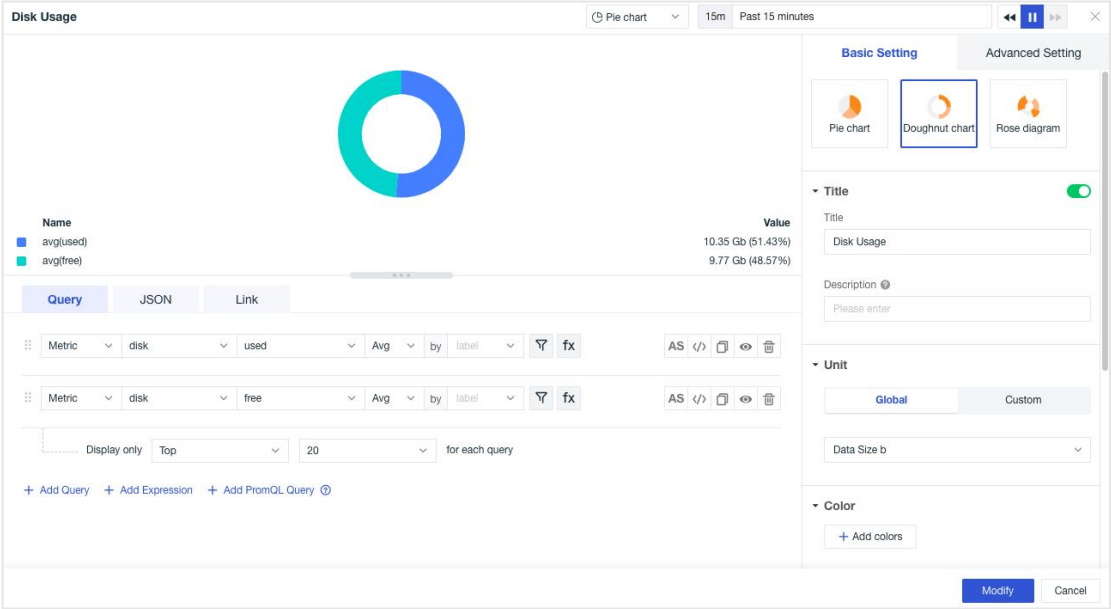
1. Pie chart

Show the comparison of data groupings and is more commonly used in sceces with fewer sample metrics.



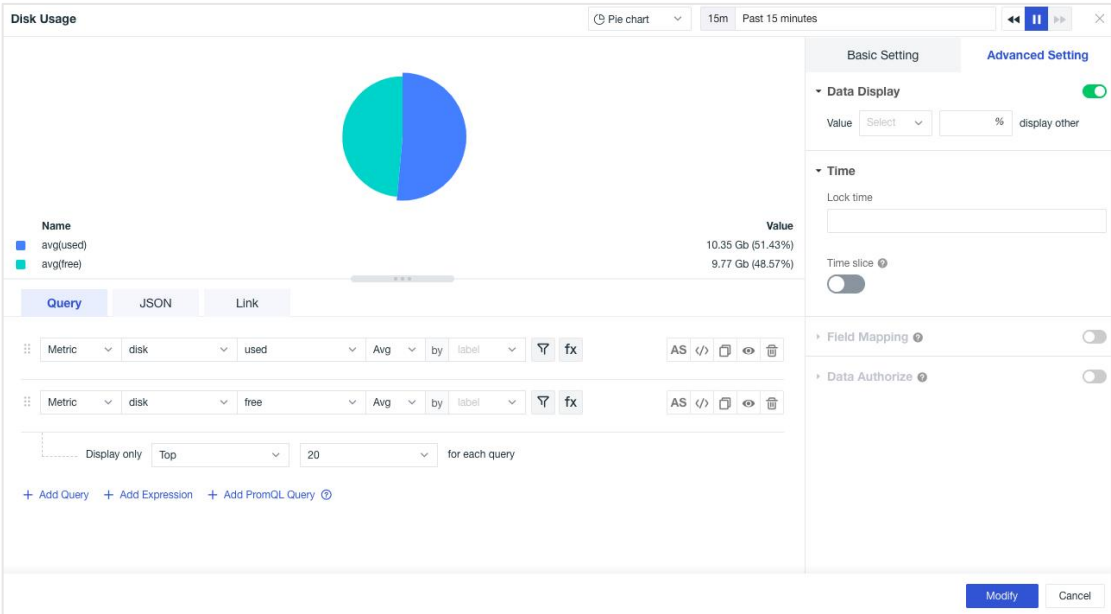

2. Doughnut chart

It is more suitable to reflect the proportion of each part of multiple sample metrics.




3. Rose chart

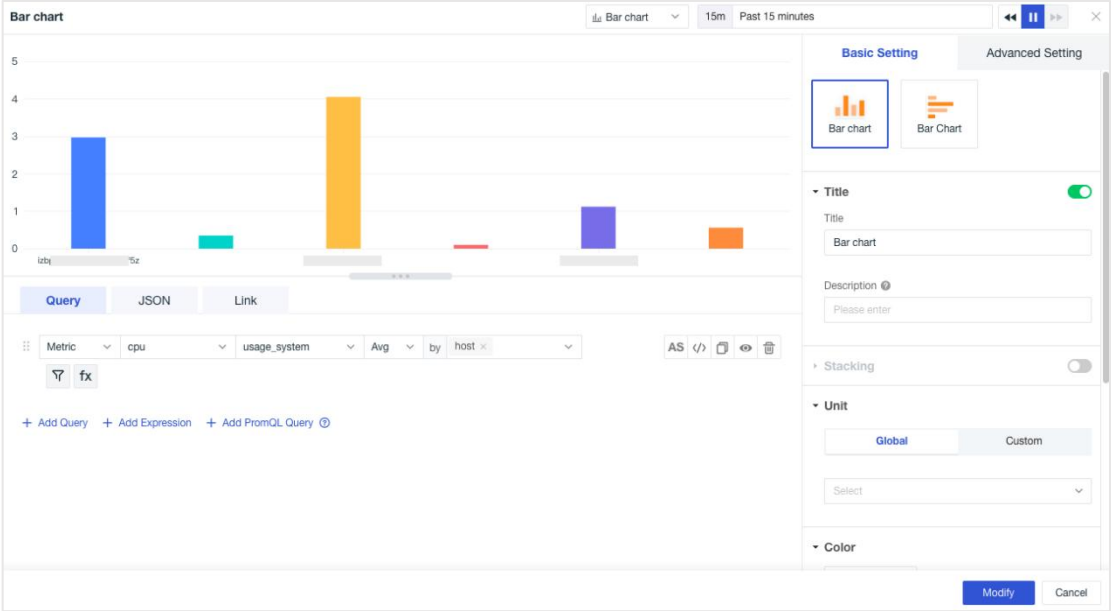
The size of the arc radius indicates the size of the data, which is suitable for reflecting scenes with too many classifications and scenes with similar numerical values.



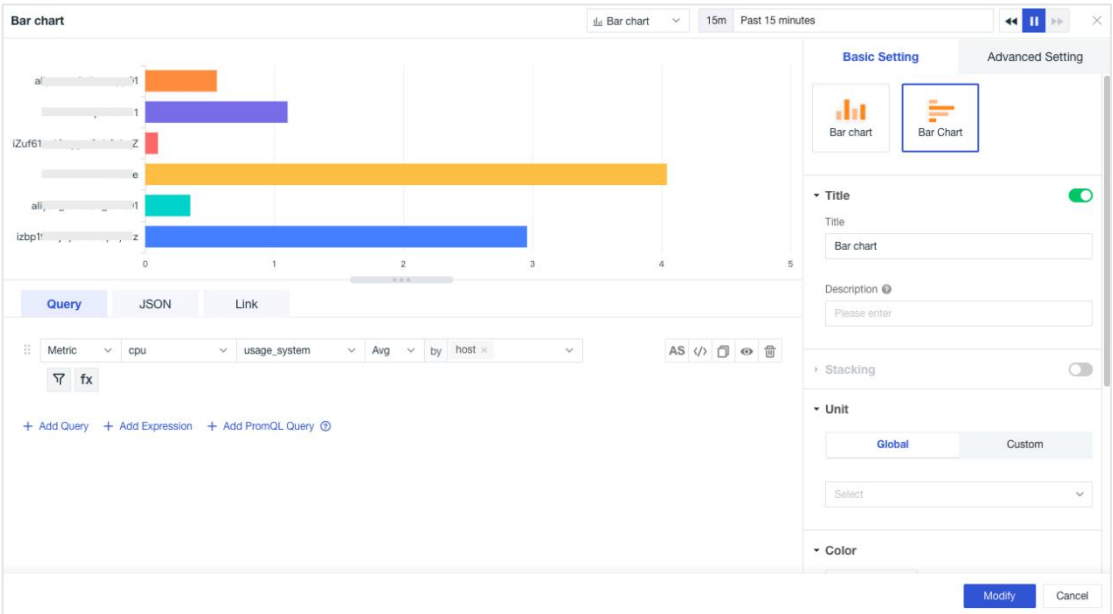

# Bar Chart

Bar chart is generally applicable to realizing the changes in data over a period of time and the comparison between variables, supporting two chart styles.

1. Bar Chart



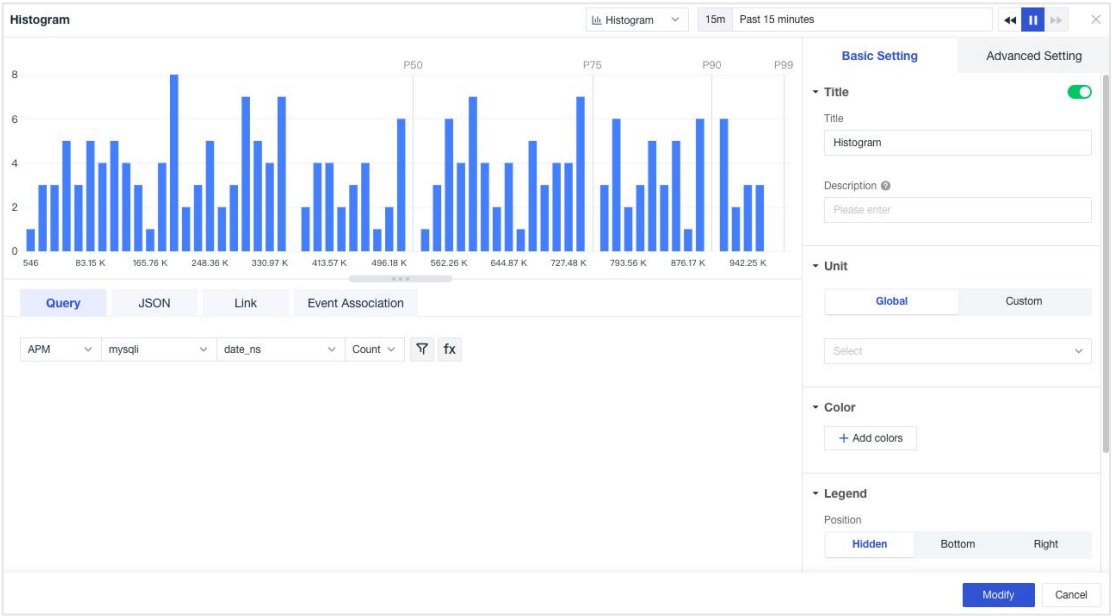

2. Bar Chart




# Histogram

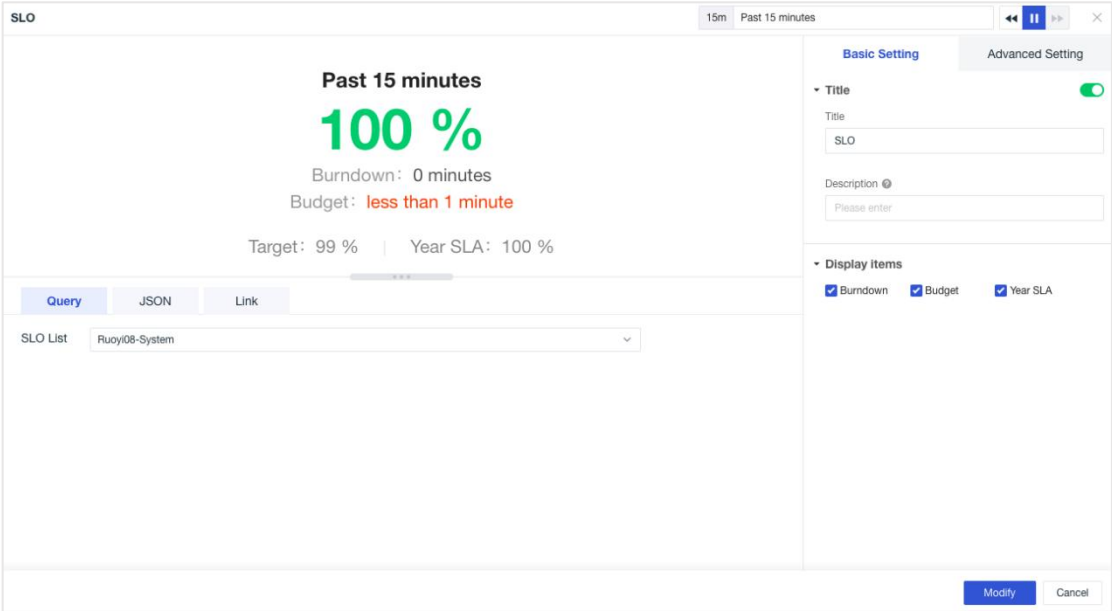
Histogram, also known as quality distribution chart, is a common statistical chart. Generally, the horizontal axis represents the data interval and the vertical axis

represents the distribution. The shape of the chart is similar to that of a histogram. The higher the column, the greater the number of columns falling in the interval.



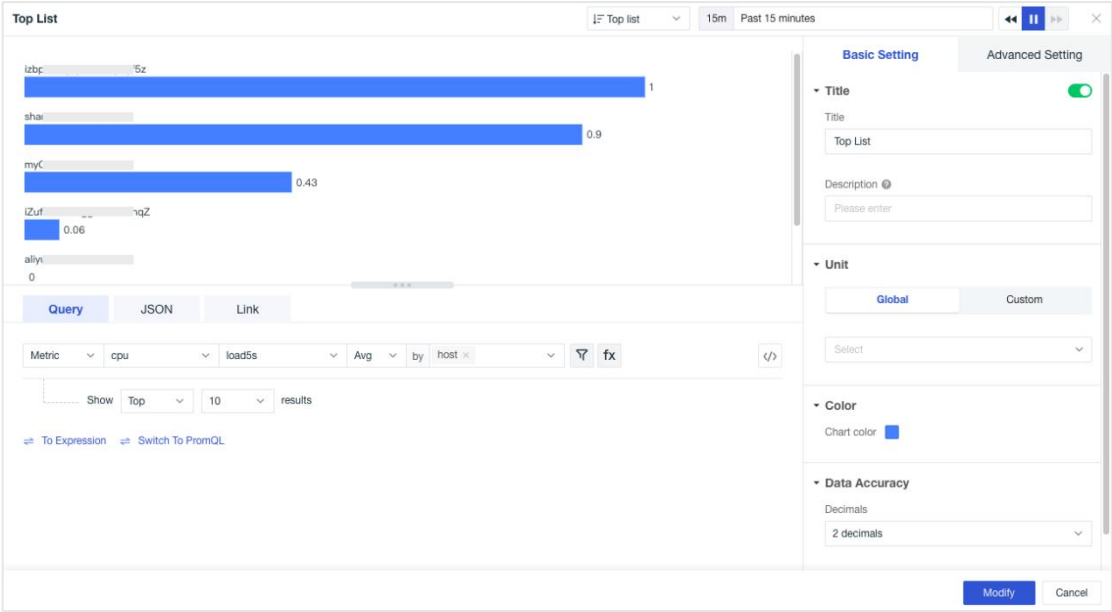

# SLO

SLO can directly select the set monitoring SLO for SLO data display.




# Top List

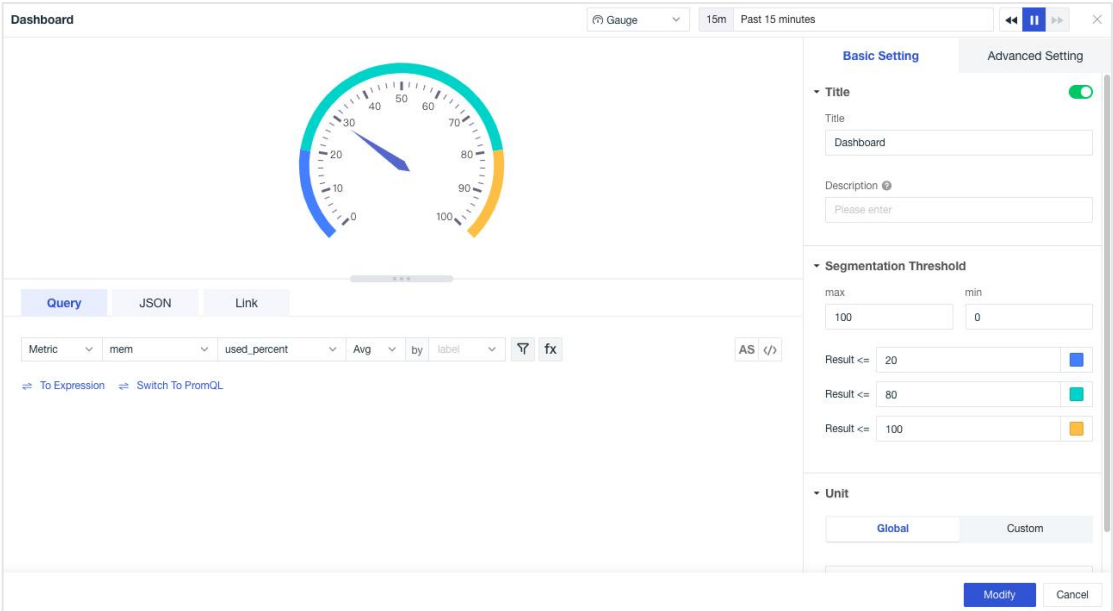
The Top List is a reflection of the objective strength of a related similar thing, which simply shows the ascending and descending order of Top N or Bottom N.




# Gauge

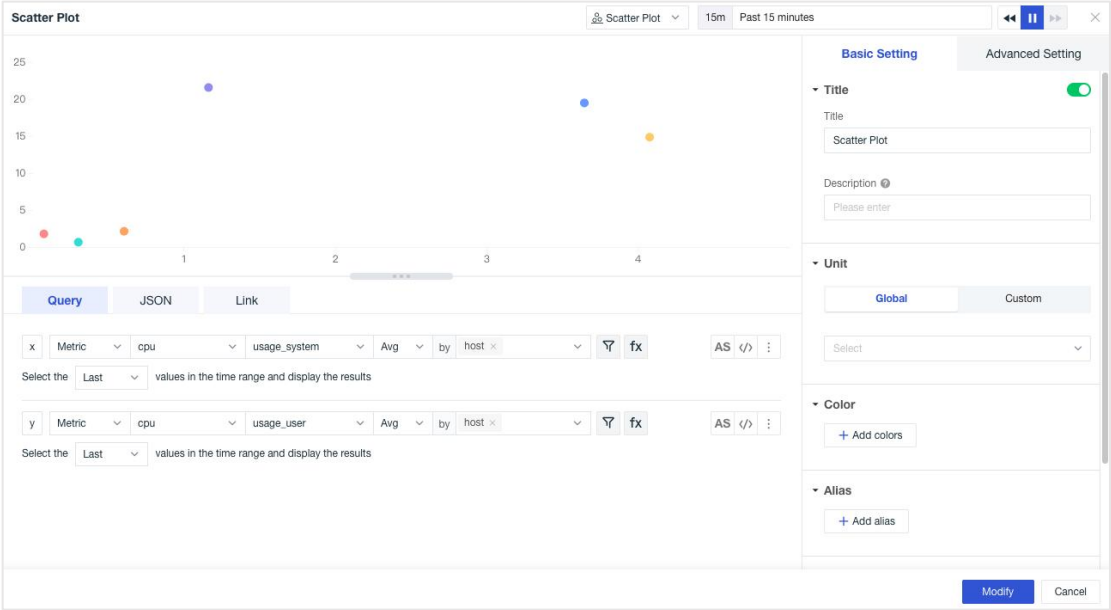
Gauge can clearly show the range of metric data values.

1. Minimum value: Set the minimum value of the instrument panel, i.e., the leftmost value in the chart;
2. Maximum value: Set the maximum value of the instrument panel, i.e., the sum of the leftmost and rightmost values in the chart;
3. egmentation threshold: Set the segmentation threshold value and dial color for numerical value. Click + and - to increase and delete corresponding thresholds;



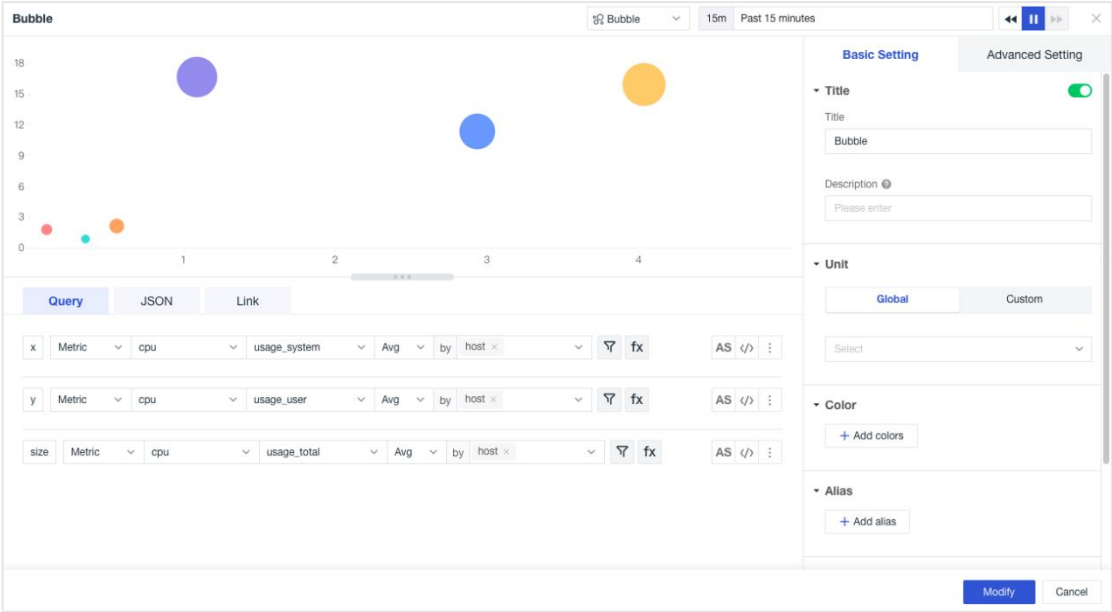
## Scatter Plot

Scatter plot shows the general trend of dependent variable changing with independent variable, from which the trend can be fitted with an appropriate function for empirical distribution, and then the functional relationship between variables can be found. It can be used to observe the distribution and aggregation of data.



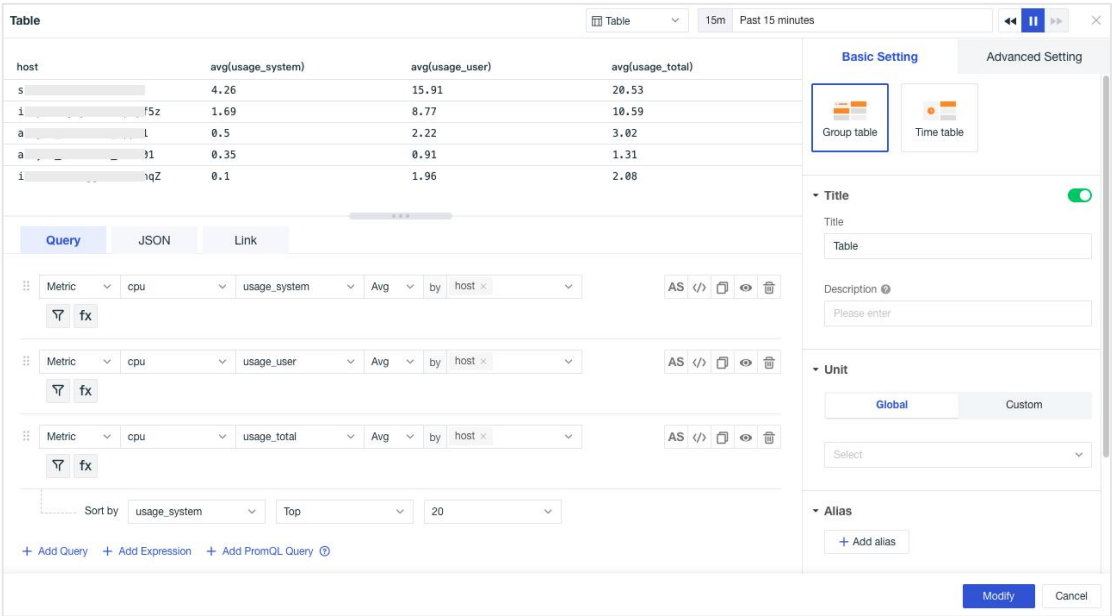

## Bubble

Bubble can be used to show the relationship between three variables. Similar to the scatter chart, it is divided into horizontal and vertical axes, and variables representing size are added for comparison. It represents the general trend of dependent variables changing with independent variables, from which the appropriate function can be selected to fit the empirical distribution, and then the functional relationship between variables can be found. It can be used to observe the distribution and aggregation of data.



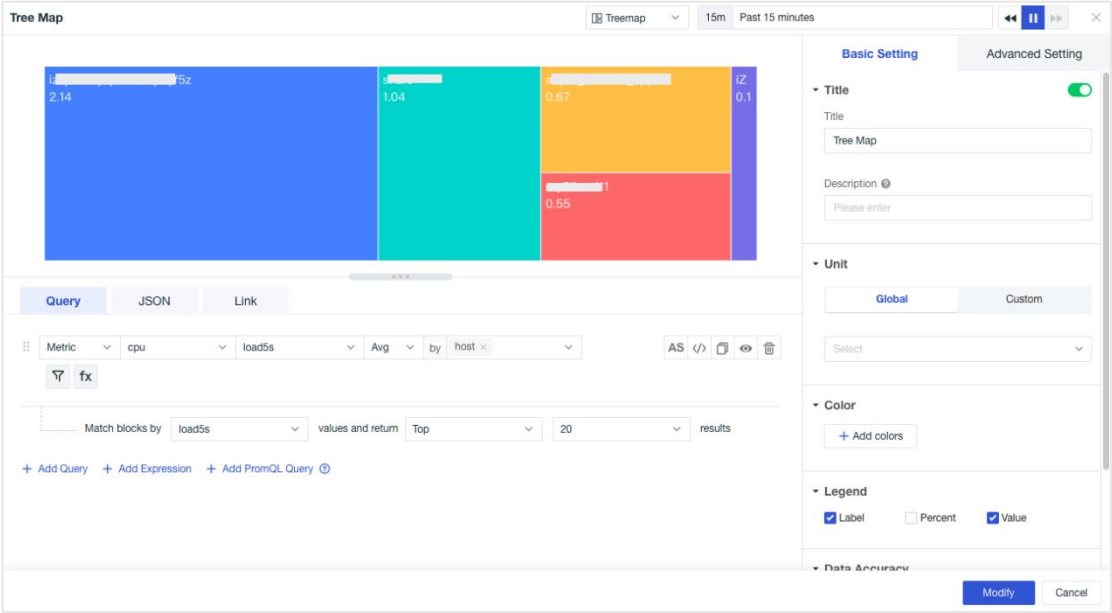

# Table

Table has the characteristics of visually displaying the attributes of statistical information and reflecting the relationship between data. Users can set the jump target page of the current chart through links and transmit data information through template variables to complete data linkage.图表类型支持分组和时序两种类型。



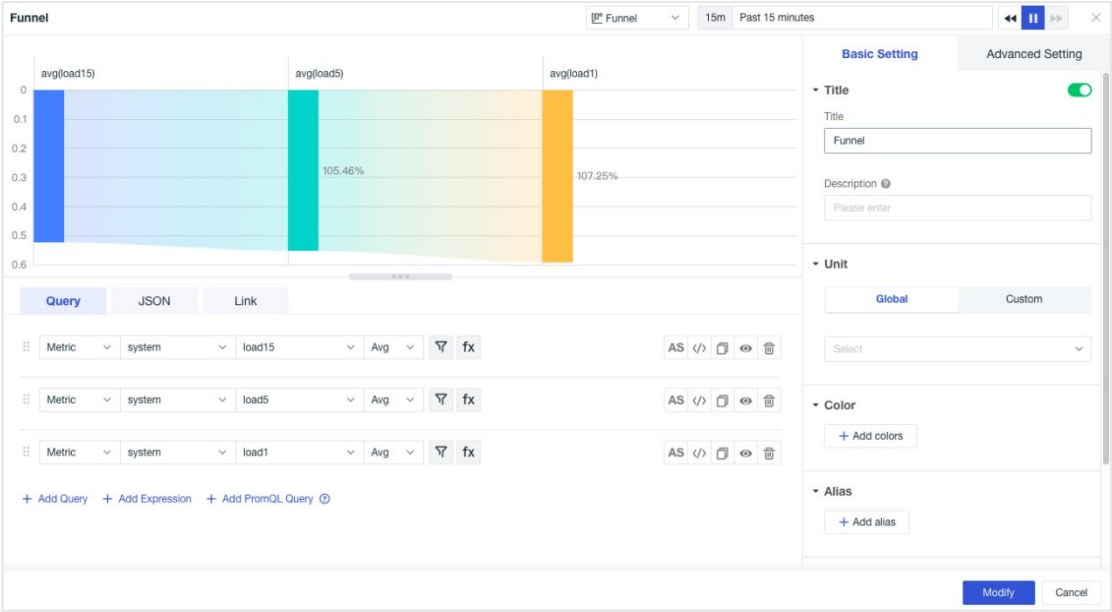
## Tree Map

Tree map is used to show the visualization of the proportion distribution of metric data under different groups.



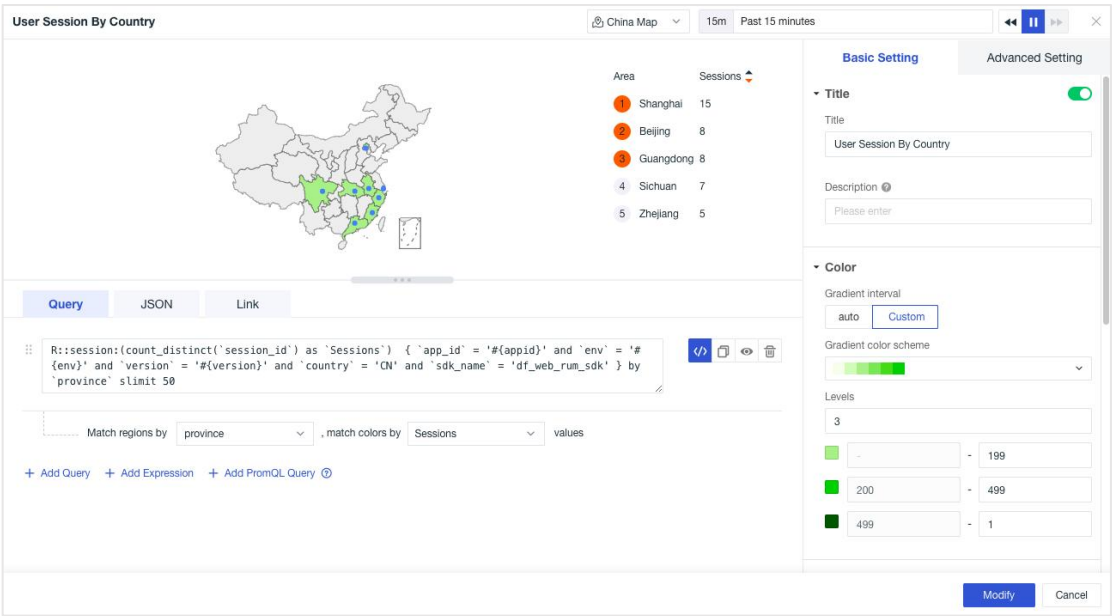

## Funnel

Funnel is generally applicable to process analysis with standardization, long cycle and many links. By comparing the data of each link with the funnel, problems can be compared intuitively. In addition, the funnel chart is also suitable for website business process analysis, showing the final conversion rate of users from entering the website to realizing purchase and the conversion rate of each step.



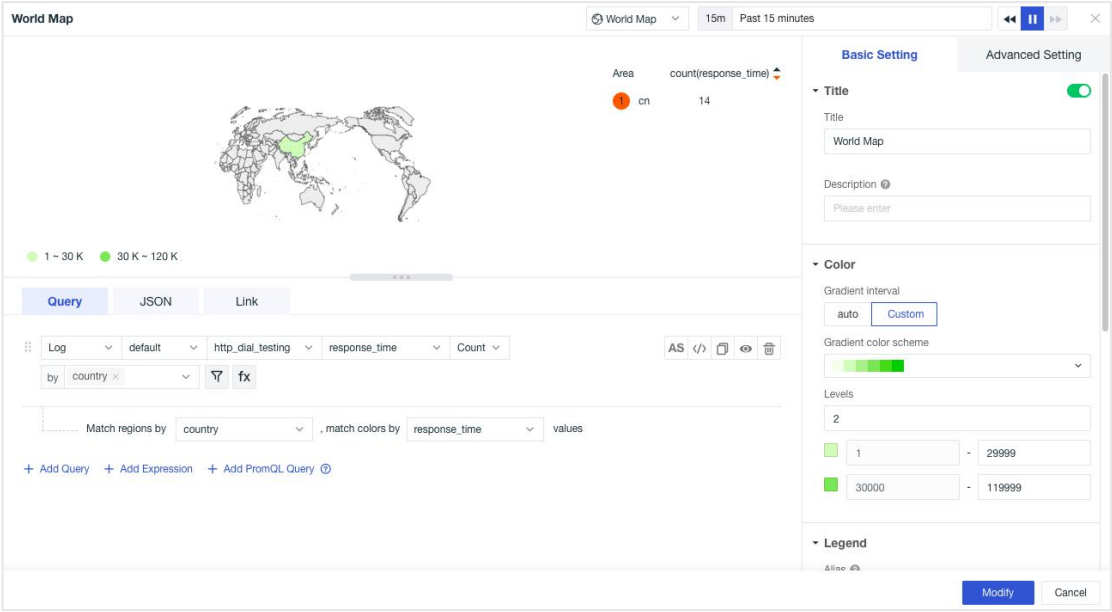

## China Map

Guance supports the display in the chart form of the China map. Users can customize the color block level, range, and color displayed.



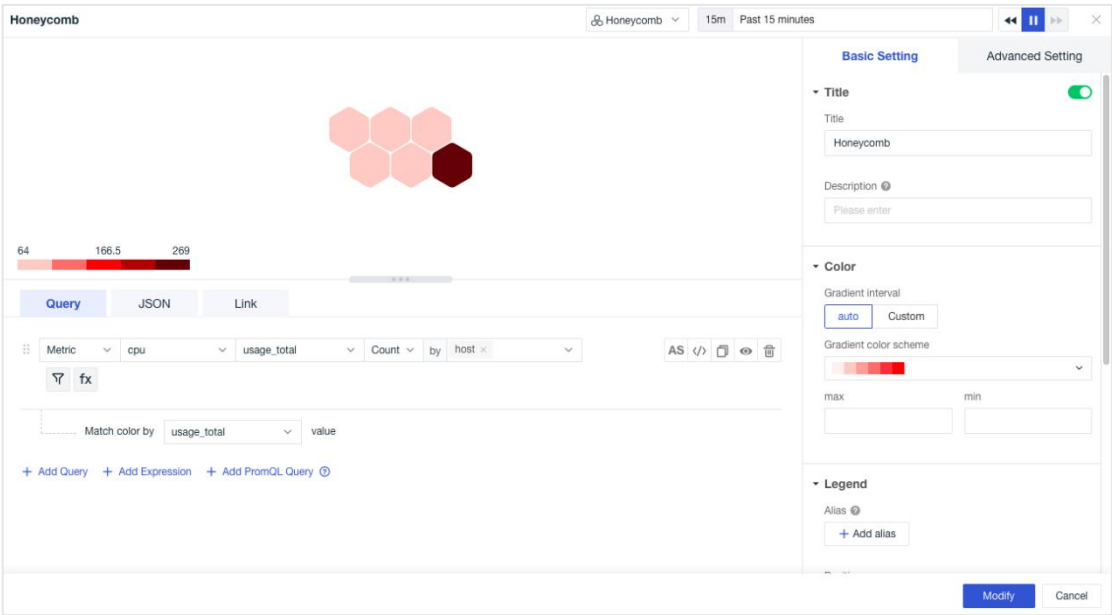

## World Map

Guance supports the display in the form of a chart of the world map. Users can customize the color block level, range and color displayed.




## Honeycomb

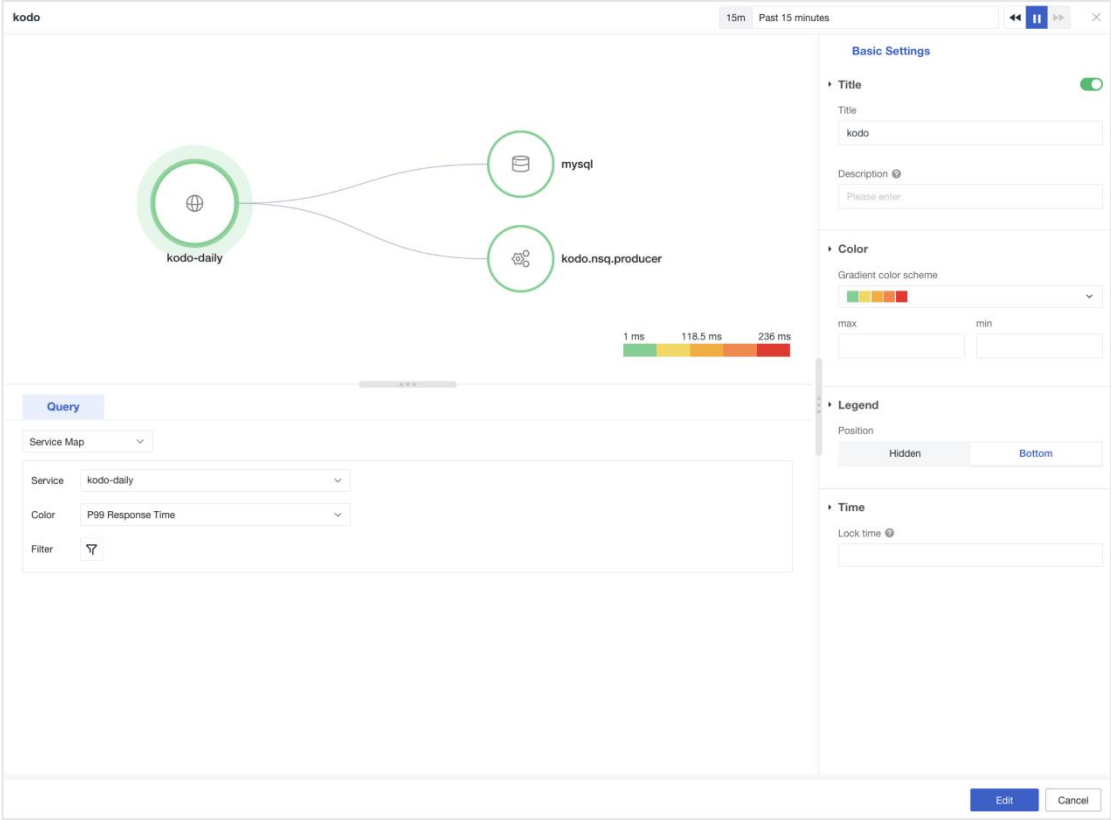
Honeycomb shows the data under different groups, which can be used to monitor assets and infrastructure.



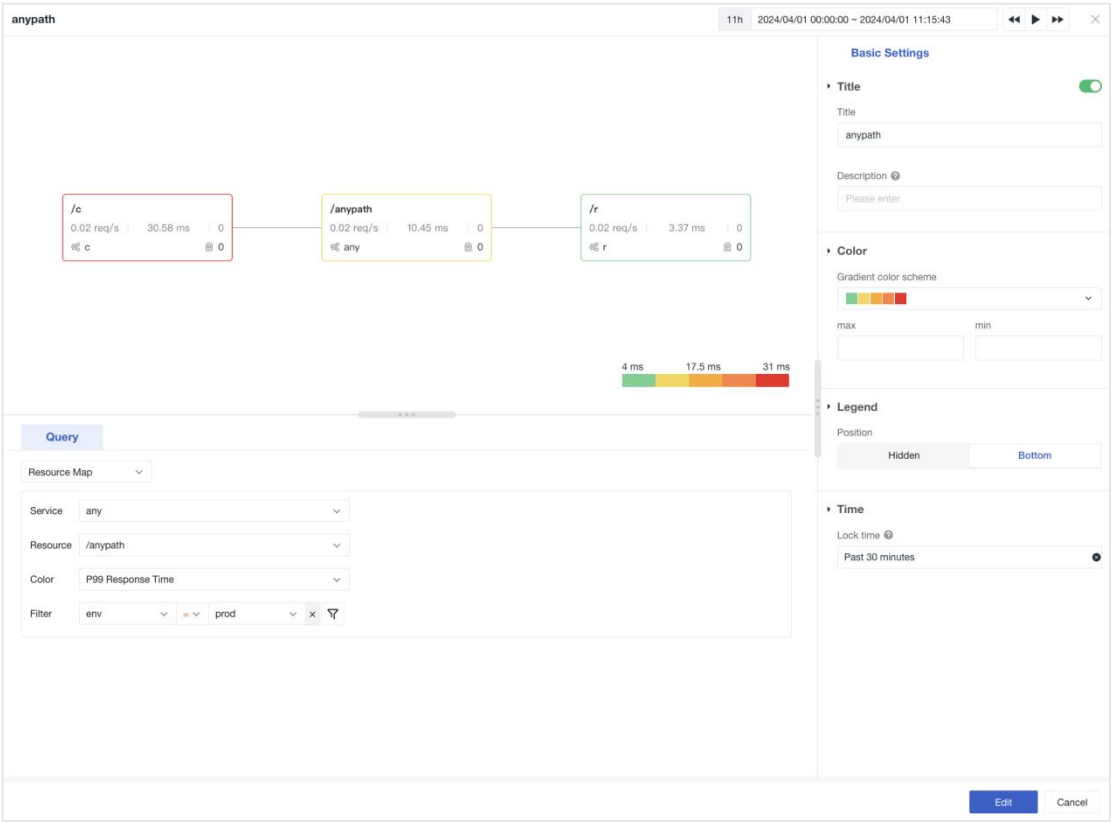

## Topology Chart

In order to enhance the visualization of the dashboard, Guance is componentized according to the existing service topology and resource call graph.

1. Service Map

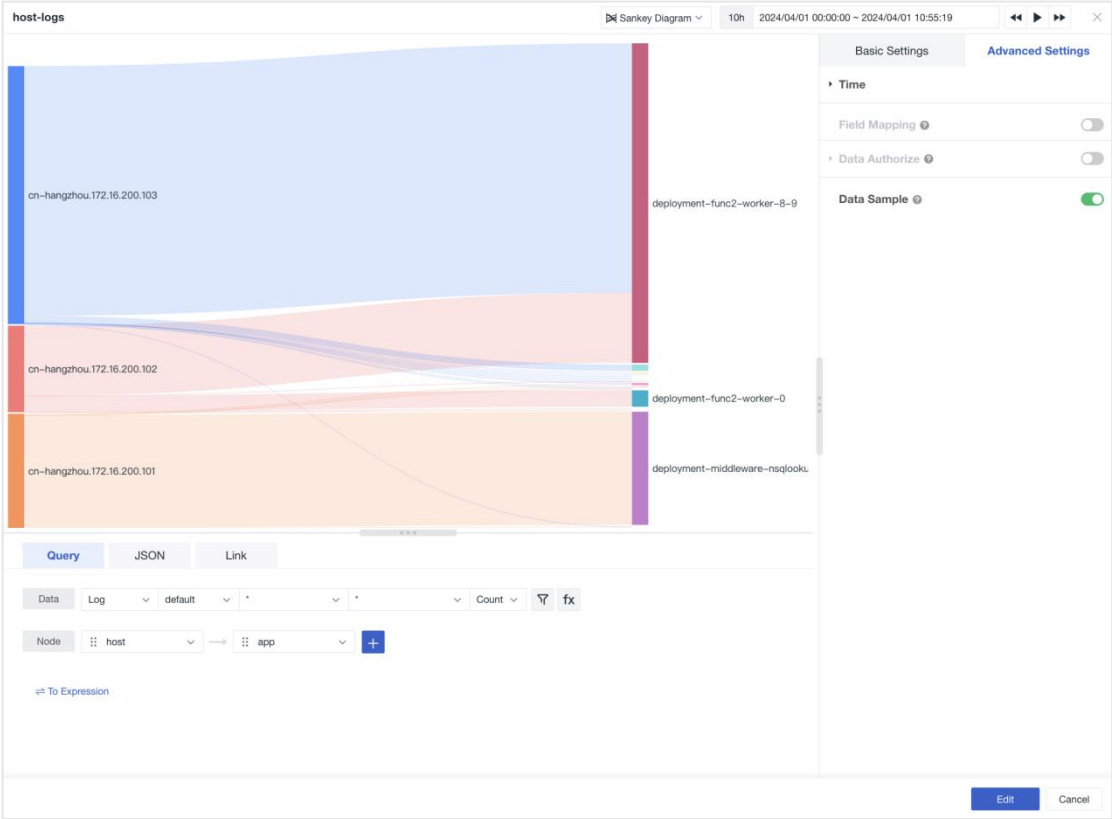



2. Resource Map



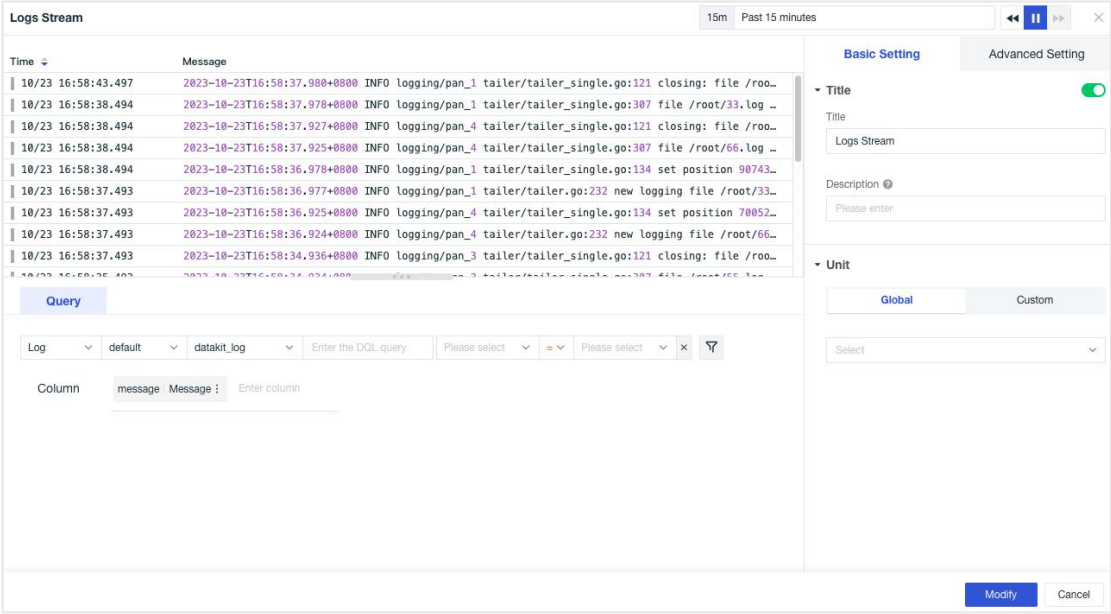
## Sankey Diagram

A Sankey diagram is a special type of flow diagram used to display the flow of data or energy. For example, it can show the flow of users from one page to another, or the energy transfer between different parts of a system. With a Sankey diagram, you can quickly understand the flow and distribution of data.



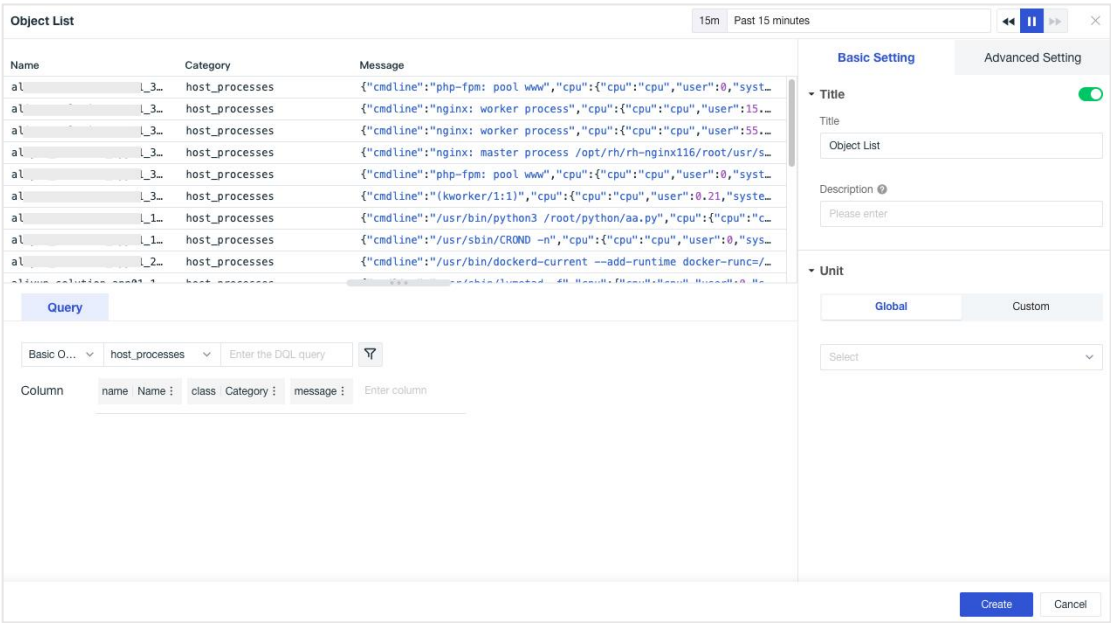

## Logs Stream

Guance supports adding log streams to the view, which can display the collected log data and can filter the data through tag filtering and keyword search before displaying it.




# Object List

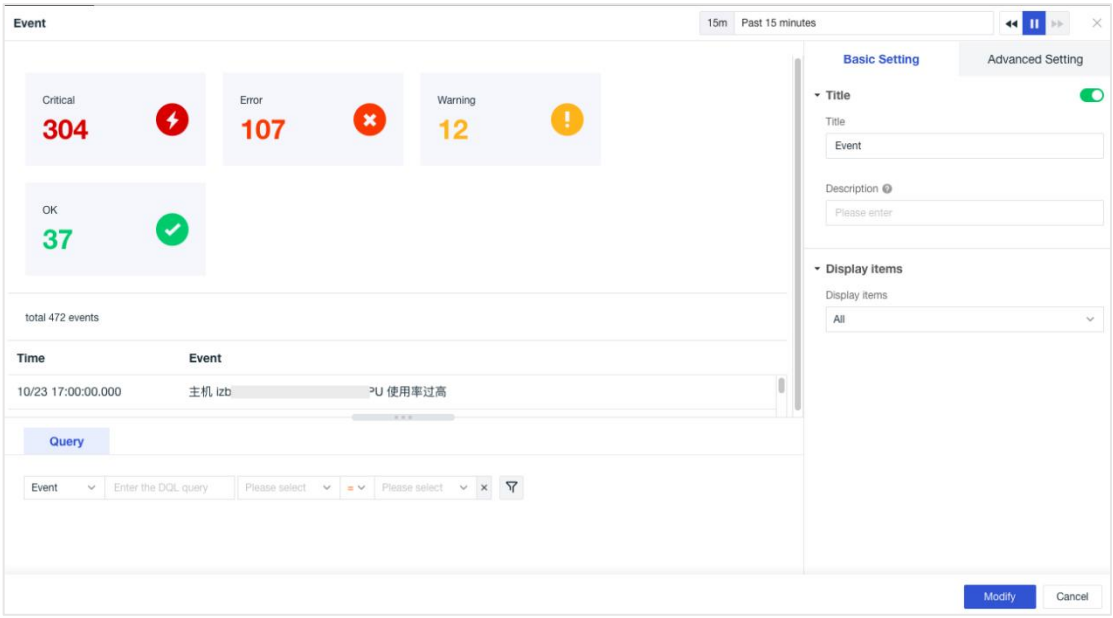
Guance supports adding object lists to the view and can filter the data to view the data under the corresponding object classification.




# Event

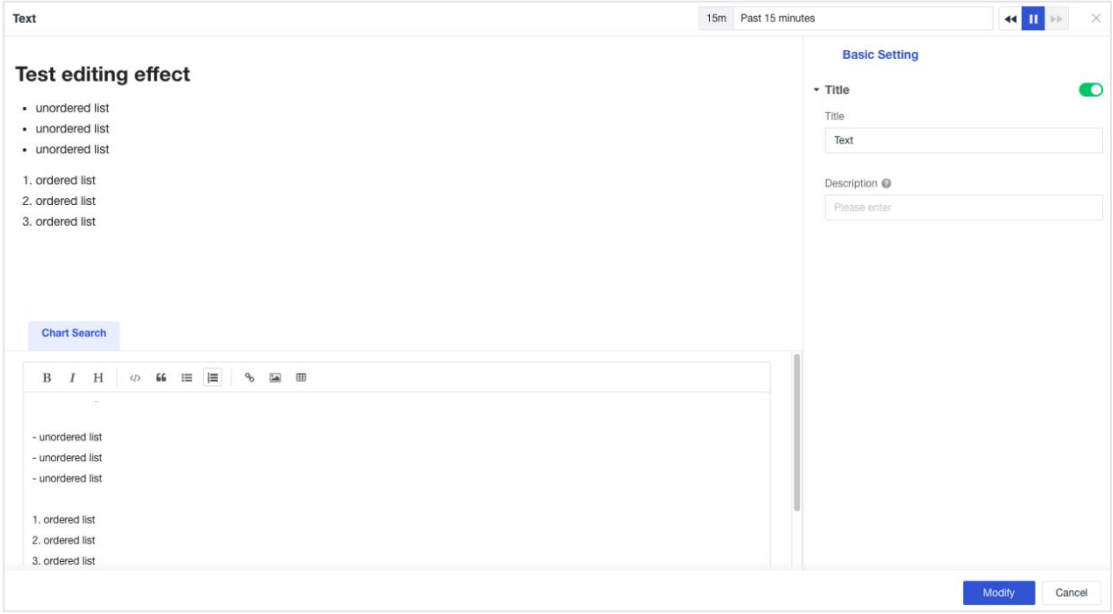
Event supports to add anomaly detection alarm events to the view and filter data through label filtering and keyword search. The alarm statistical chart is divided into two parts, namely statistical chart and alarm list.

1. Statistical chart: Group events according to levels and count the number of events in each level and support clicking the statistical chart to jump to query the details of events;
2. Alarm list: Display unrecovered alarm events within the selected time range.



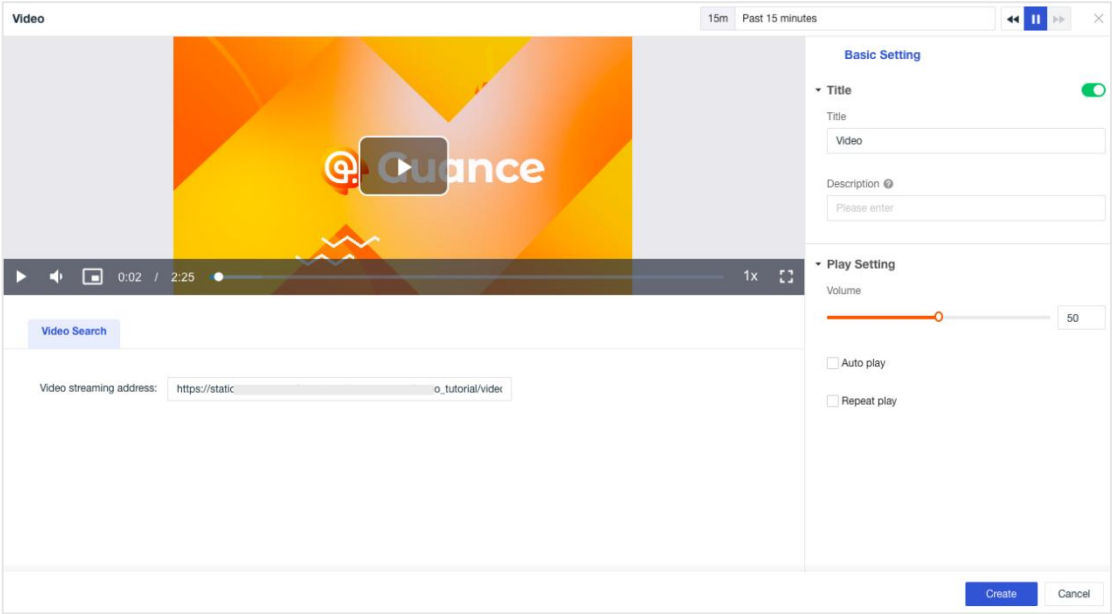

# Text

Text is typically used for providing hints and explanations. You can add text, images, hyperlinks to the text. The text here is in Markdown format.



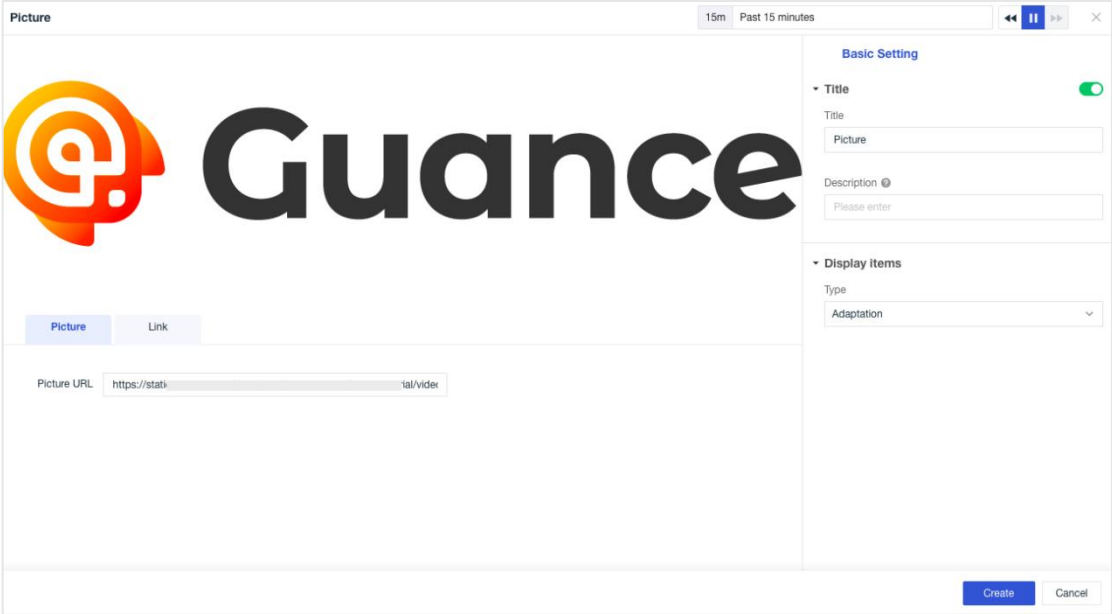
# Video

Videos can generally be used for tutorials, instructions, and other purposes. They are easy to embed - simply fill in the video address.



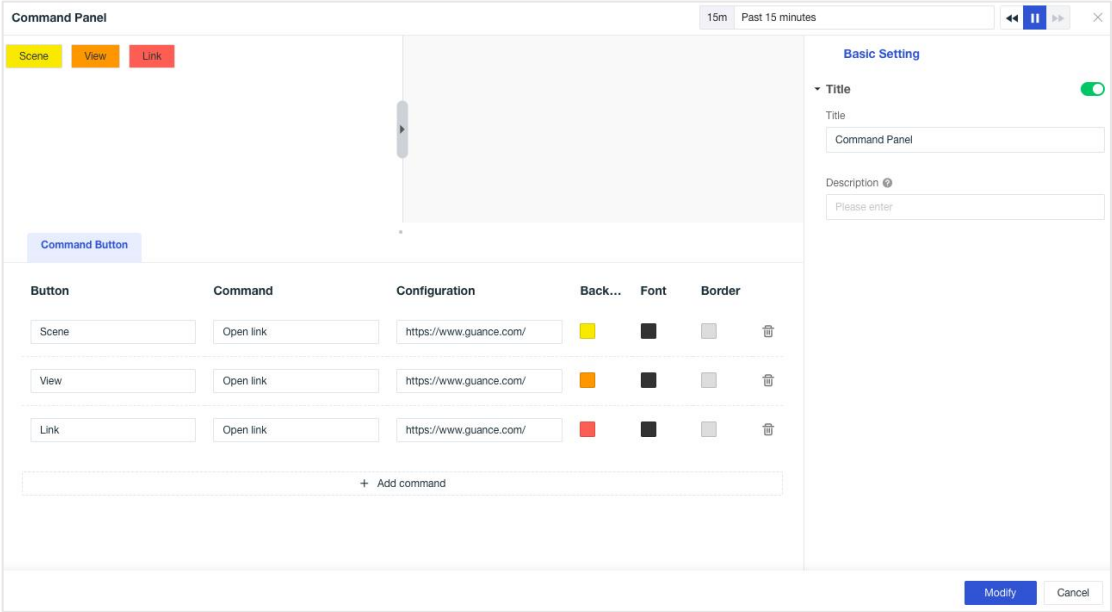

# Picture

Pictures are generally used to display images, and you can add picture addresses to display the corresponding pictures.



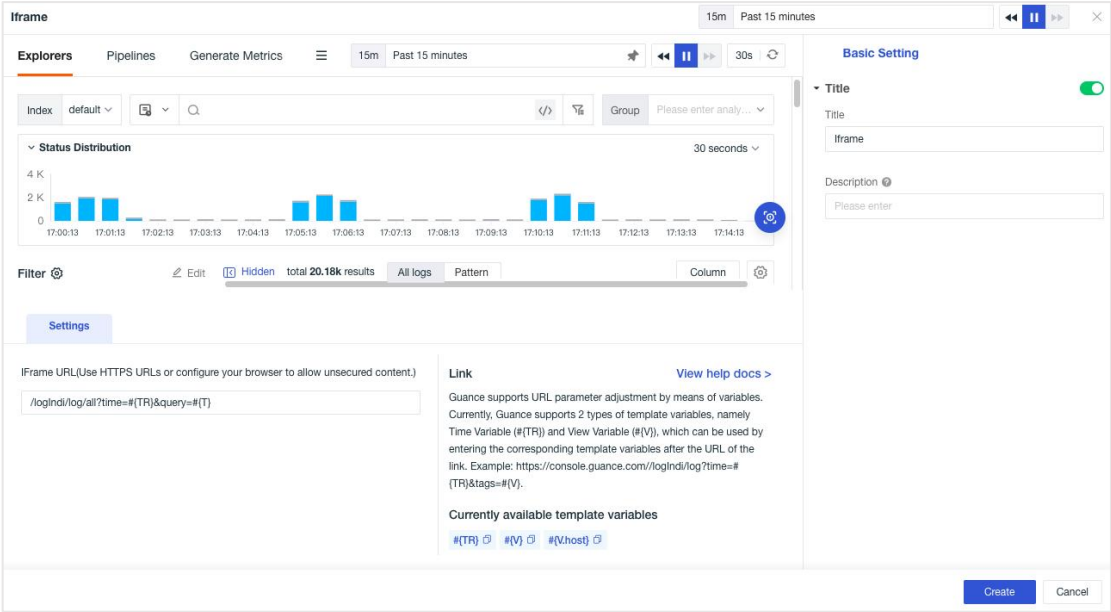
# Command Panel

The command panel is composed of command buttons, which allow you to click and jump to specified scenes and views, open specified links, execute specified commands, and perform interactive actions in views. You can adjust the position for typesetting by dragging and dropping buttons.




# IFrame

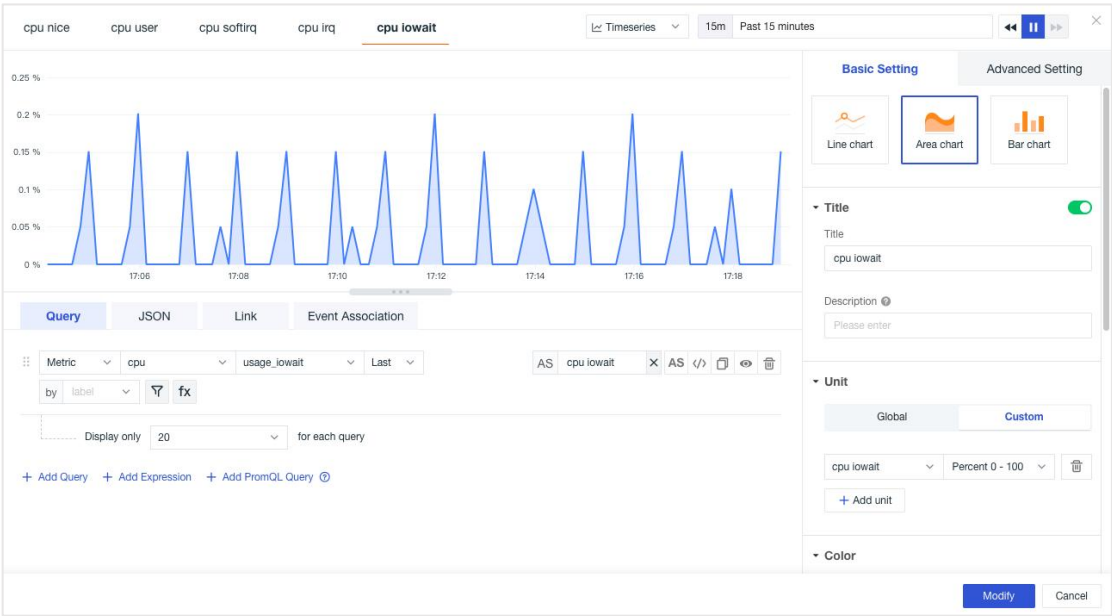
IFrame supports the configuration of https or http link address and supports the adjustment of URL address parameters through a variable form.




# Combination Graph

Combination charts are generally used to combine multiple charts with different result values of a metric to help users understand the comparison results of metrics.

Different types of charts can be combined at will.

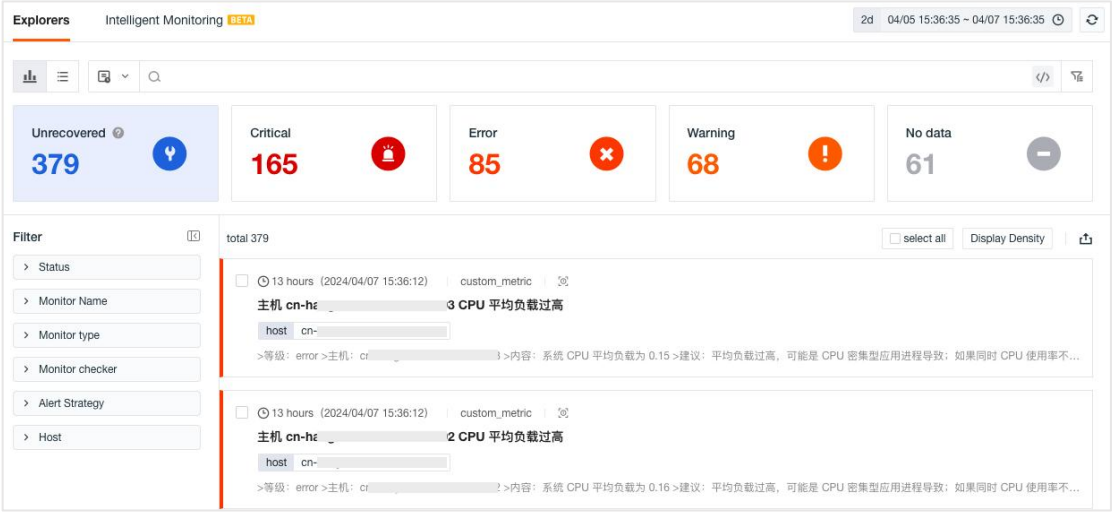


# Events

Guance supports one-stop viewing and auditing of all event data, including alarm events triggered by monitors, alarm events triggered by intelligent inspection, SLO events, system audit events, and user-defined reporting events.

## Unrecovered Event

In the list of unrecovered events, you can see all the unrecovered events continuously triggered in the space, and the data volume statistics and alarm information details of unrecovered events under different alarm levels. It supports querying event data by searching keywords and filtering, saving and viewing historical snapshots, and viewing metric data trends in the last 6 hours through window functions.




## All Events

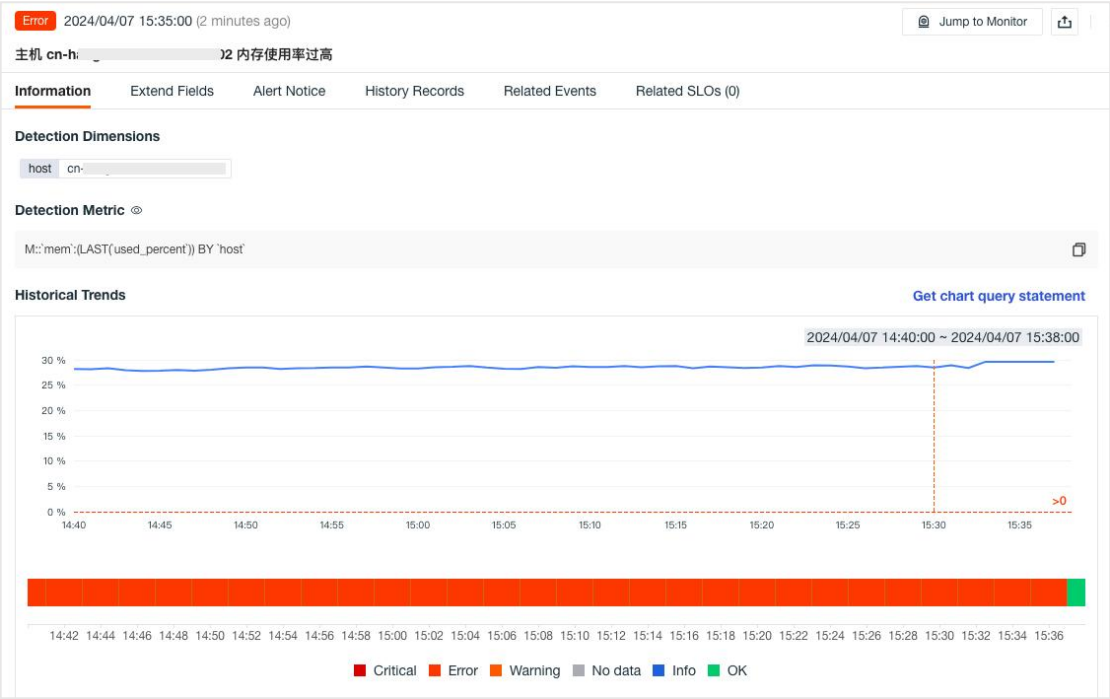
In all event lists, users can search, multi-label filter, aggregate statistics by monitor group and quick filter. It supports data export, and supports saving and viewing historical snapshots.


# Event Aggregation

In all event list analysis columns, multi-dimensional analysis based on label field is supported to reflect aggregated event statistics under different analysis dimensions.


# Event Details

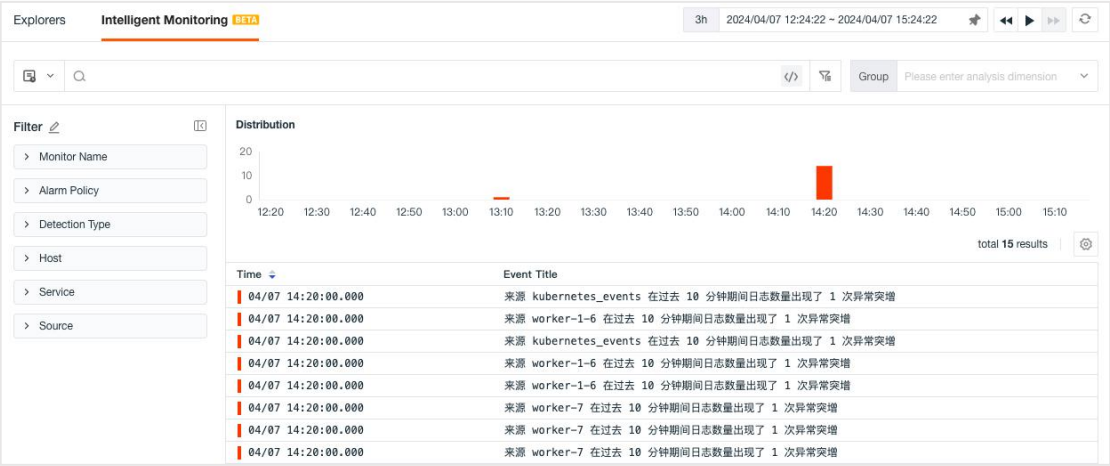
Click **Event** or **Aggregate Event** to view the basic information, status & trend, alarm notification, history and related events of the corresponding event in the Event Details page. You can export and jump to monitor configuration.




# Intelligent Monitoring

In the **Events > Intelligent Monitoring** explorer, you can view a complete list of events generated by intelligent monitoring in the current workspace.

- Use a stacked bar chart to count the number of events that occurred at different times and under different rules in the current event explorer.
- Search for events based on tags, fields, and text using keywords, tag filtering, field filtering, and related searches.
- Perform aggregated event analysis by grouping events based on selected fields.



**Intelligent Monitoring Details**

In the Intelligent Monitoring event explorer, click on any event to open the event details, including analysis reports, extend fields, alert notice and related events. On the event details page, you can also jump to the monitors associated with the current event and export key event information to PDF or JSON files.


# Incidents

Guance supports any member in the workspace to define observed anomalies as Issues and manages all Issues generated within the current workspace through the "Channels" of anomaly tracking. By manually creating and collaborating with members, timely identification and effective resolution of ongoing abnormal issues can be achieved.

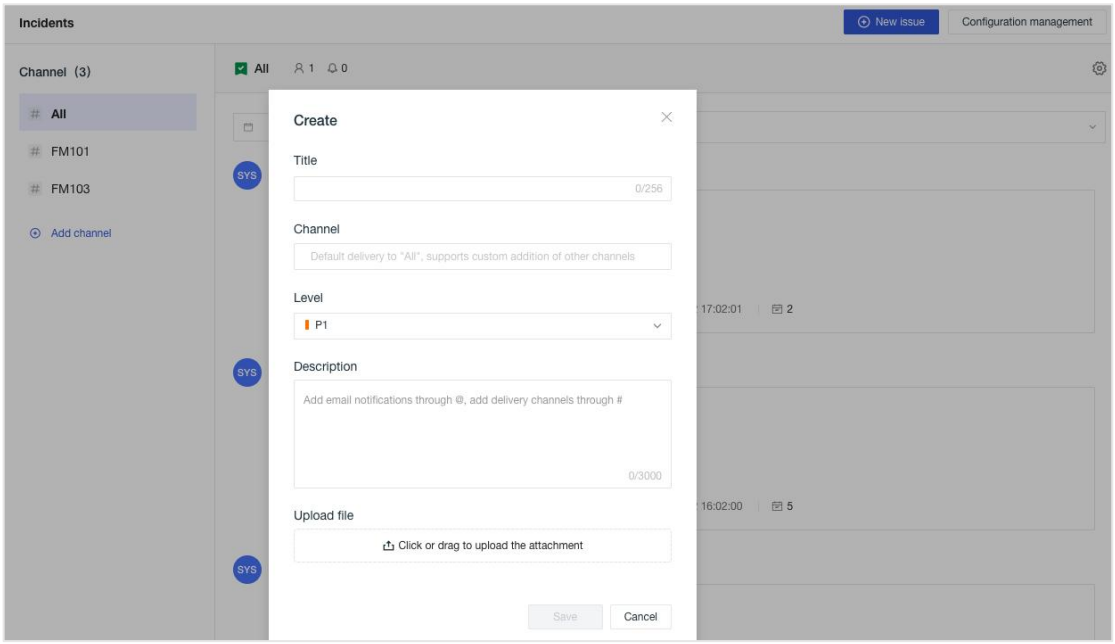
# Create Issue

An Issue includes information such as title, anomaly source, severity, description, and attachments. Any member of the Guance workspace can create an Issue based on observed anomalies and notify relevant members to track and address them.

There are two ways to create an Issue: manual creation and automatic creation.

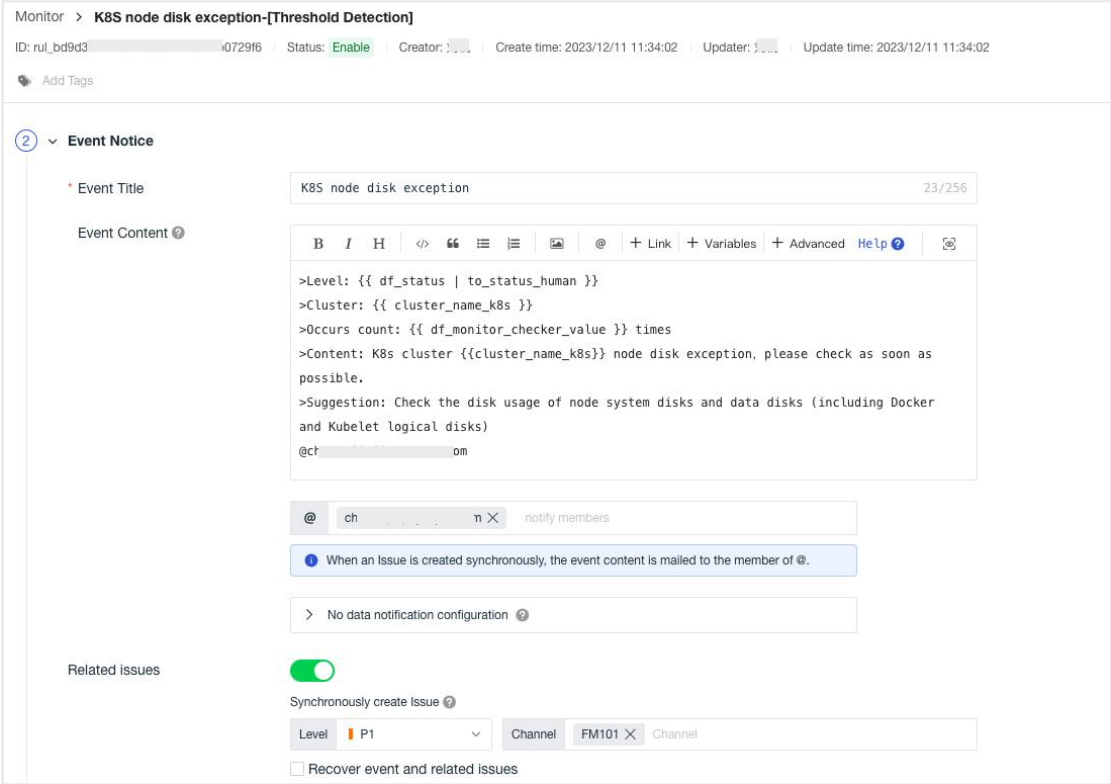
**1. Manual creation**

In Incidents, select a Channel and click New Issue to create one. Additionally, Guance supports manual Issue creation in modules such as the dashboard, viewer, and events.




## 2. Automatic creation

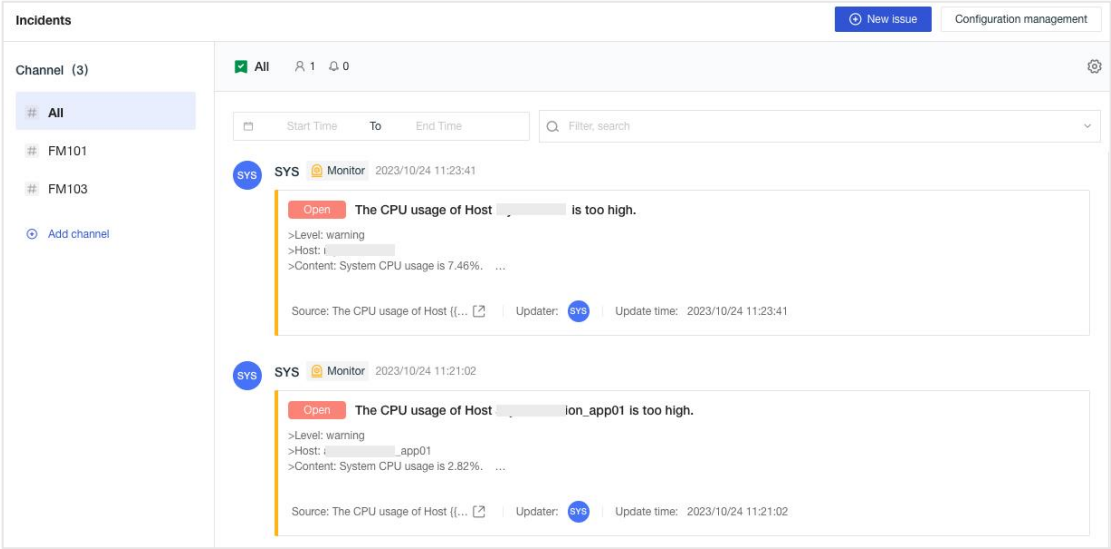
In Monitoring, select the configuration of Monitors and configure notification members in the event content of event notification. Turn on “Related issues”, so that an issue will be created automatically when the monitor generates an alert for an abnormal event. Check "Recover event and related issues", so that the exception tracking issue will be resumed synchronously when the abnormal event is resumed.




# Manage Issue

Guance manages all the issues generated within the current workspace through the Channels of anomaly tracking. Based on channels, you can customize the scope of issues to subscribe to, view subscribed members or notification recipients, use time controls, or reply to issues to achieve member collaboration.

In Incidents, on the left side of the current page, below the channel list, click on Add Channel to enter the channel name and create a new channel.

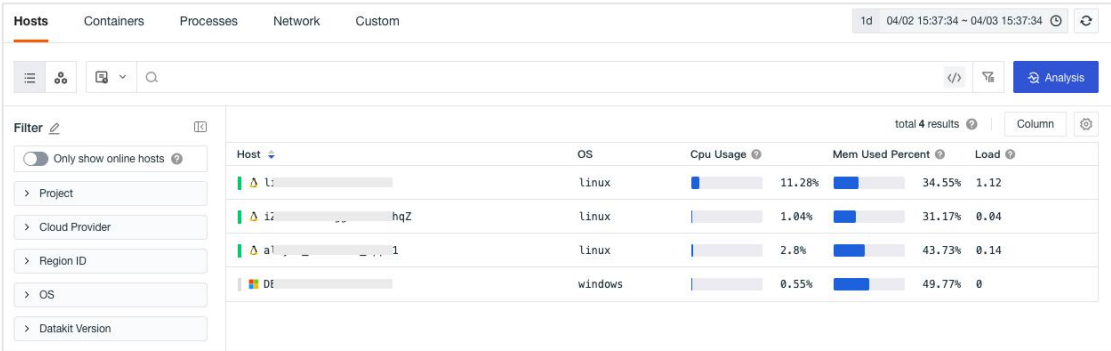



# Infrastructure

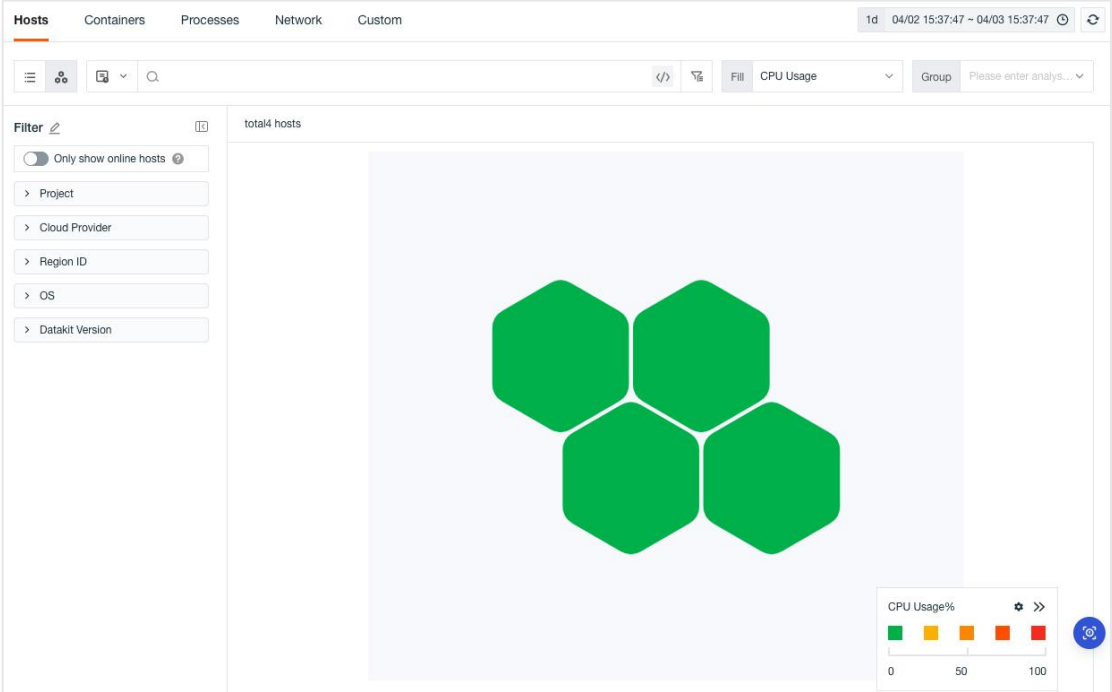
Guance supports viewing all infrastructure data collected in the workspace, including hosts, containers, processes, networks and custom objects

# Host

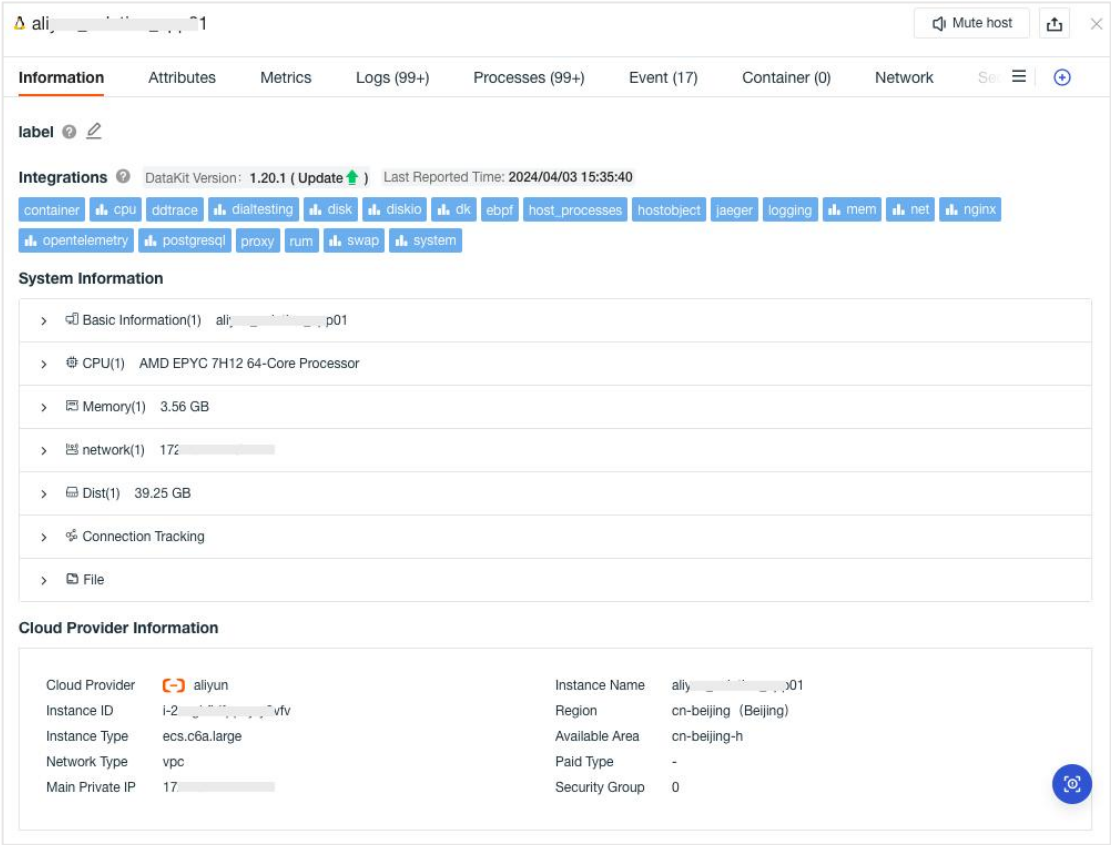
Guance supports collecting host data, searching hosts, multi-label screening, multi-dimensional analysis statistics, and quick screening in the host list of Infrastructure, data export, adding display columns, saving and viewing historical snapshots and only show online hosts.



You can switch to the host topology chart to visually display the host list.



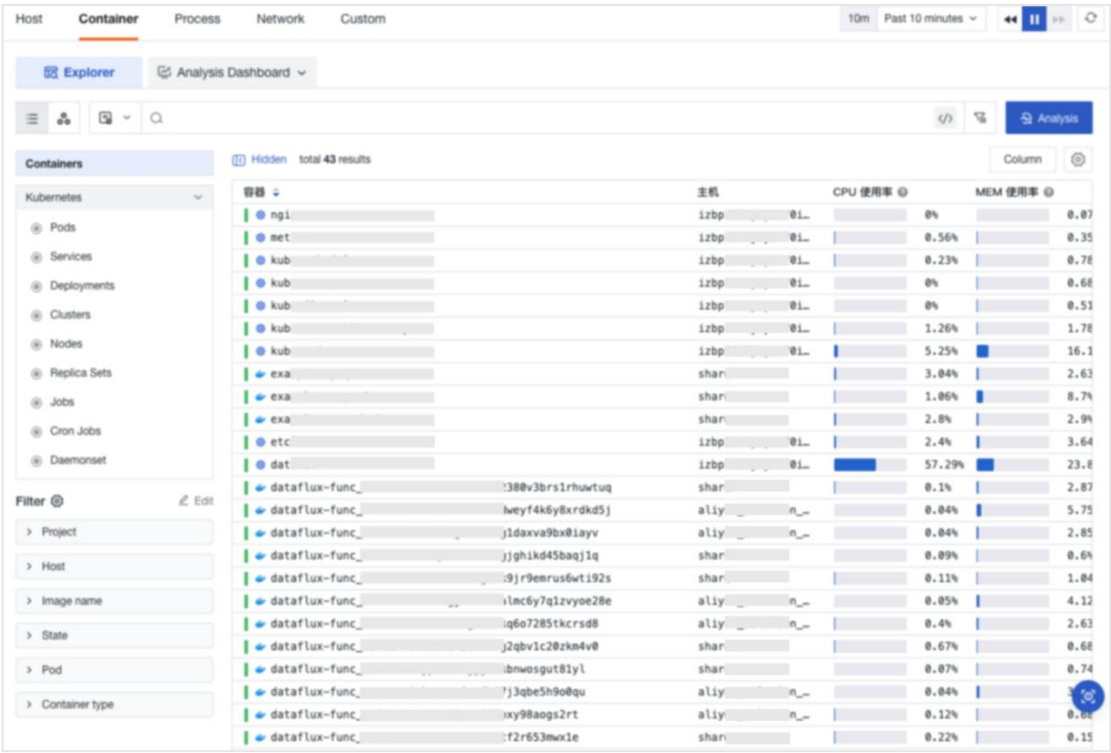

Click on the host to view the details of the host, including host status, host name, basic attributes, associated logs, processes, events, containers, networks, security inspections, metrics, and bound inner views. The basic attributes include label attributes, integrated operation, system information, cloud vendor information, and more. By clicking on the collector under integrated operation, you can view the corresponding view and error reporting information.



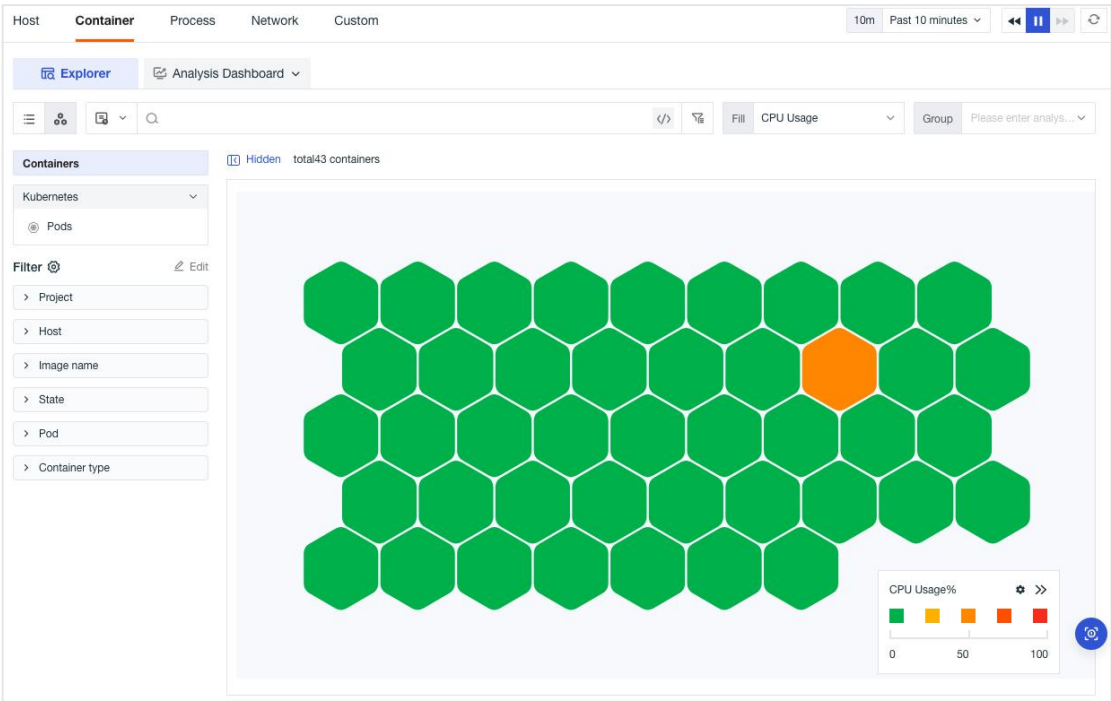

# Container

## Explorer

Guance supports the collection of container data. On **Infrastructure > Container > Explorer**, it is supported to view the data of Containers, Pods, Services, Deployments, Clusters, Nodes, Replica Sets, Jobs, and Cron Jobs collected in the current workspace in the last ten minutes in the form of a list. You can search, multi-label screen, multi-dimensional analysis statistics, and quick screen the data in the list. It is supported to save and view historical snapshots. Click on the container to skid to view container details.

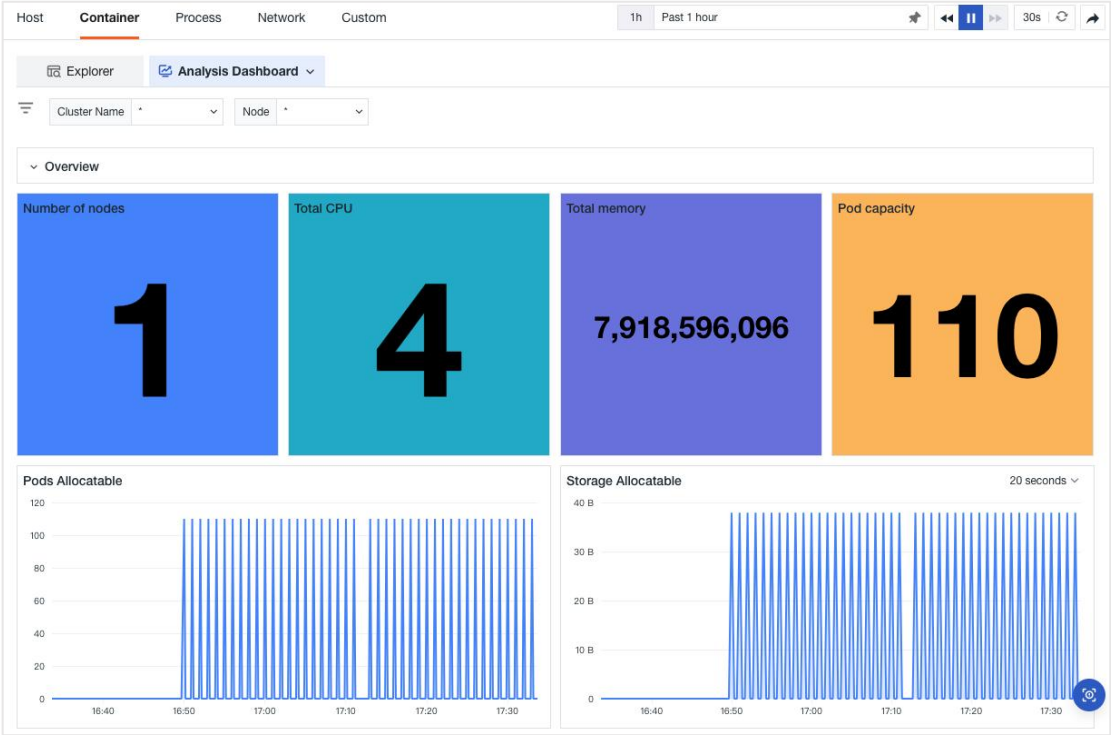



On the **Containers > Pods List** page, you can switch to the Container topology, view the Containers and Pods data of the workspace in the form of a distribution diagram, and quickly identify the performance status of Containers / pods based on the size of the populated data.



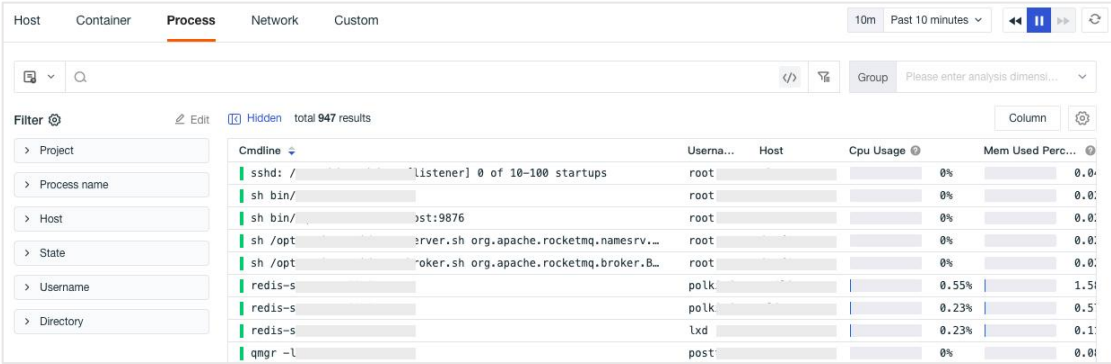
## Analysis Dashboard

On **Infrastructure > Container > Analysis Dashboard**, it is supported to comprehensively monitor Kubernetes' data metrics by building a multi-dimensional data insight scenario.



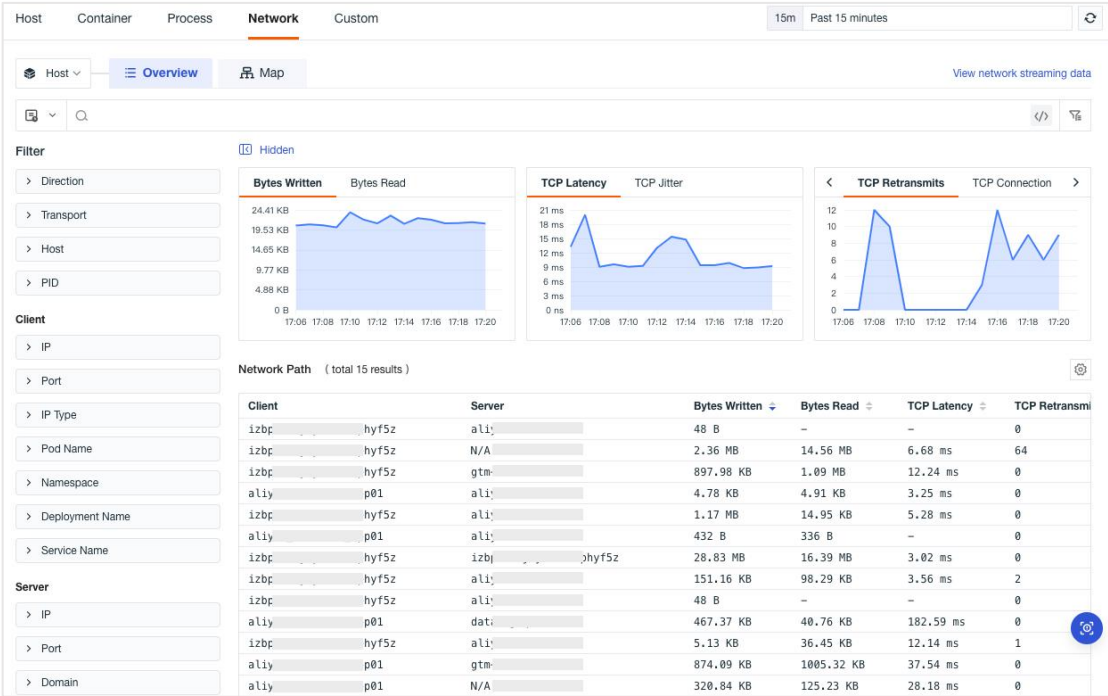

## Process

Guance supports collecting object process data. In the process list of **Infrastructure**, it supports searching for processes, multi-label filtering, multi-dimensional analysis statistics and quick filtering, data export, adding display columns, saving and viewing historical snapshots, and clicking on processes can sideslip to view process details.

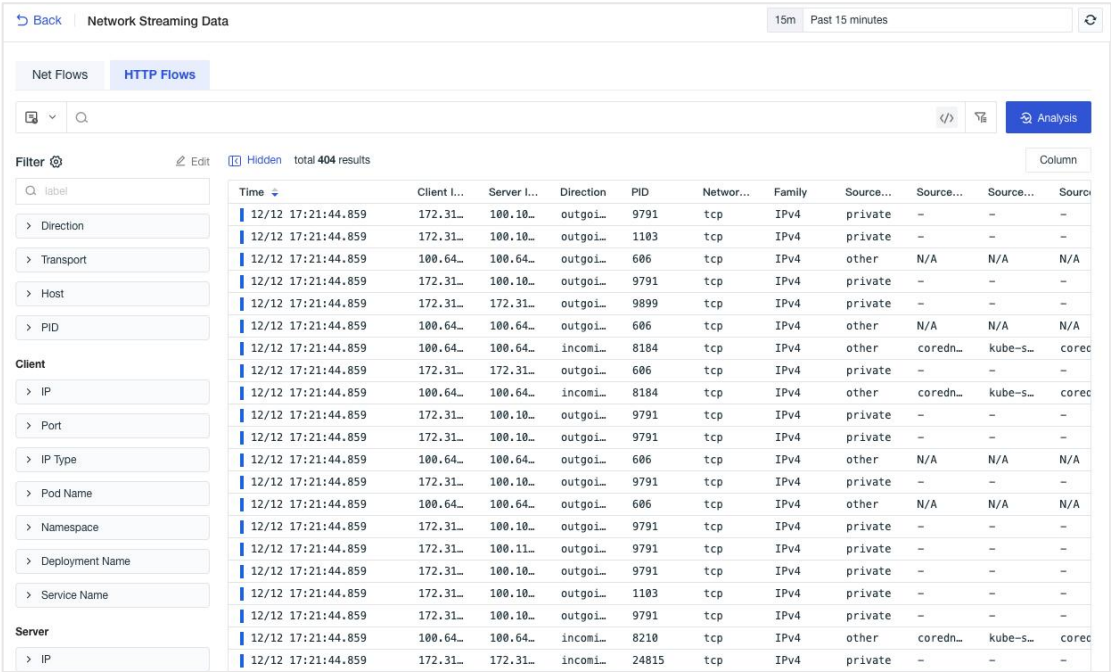


# Network

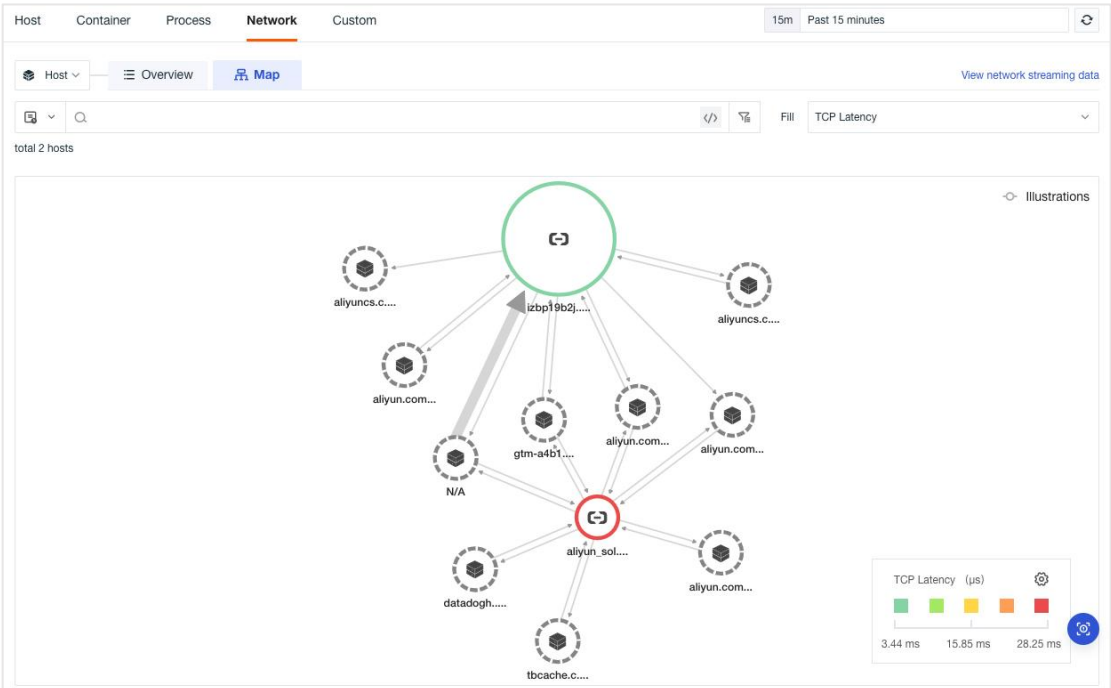
Network supports views network traffic between the host, Pod, Deployment, and Service. Support to view network traffic and data connection between source IP and target IP based on IP/port, and support to click nodes to view upstream and downstream data connection. Through visual real-time display, it helps enterprises know the network running status of business systems in real time, quickly analyze, track and locate problems and faults, and prevent or avoid business problems caused by network performance degradation or interruption.



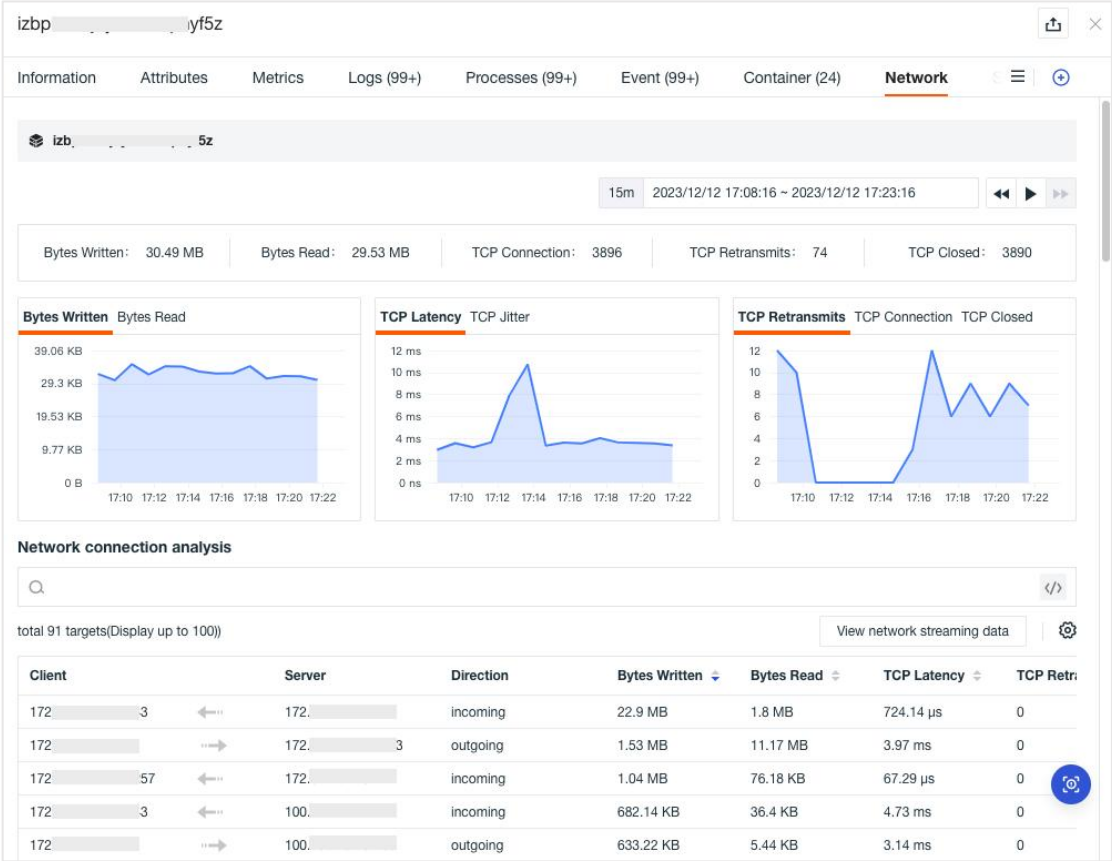

It supports switching to the network list to view network traffic and data connections for hosts, Pods, Deployment and Services.




It supports switching to topology to view the upstream and downstream distribution of the network.

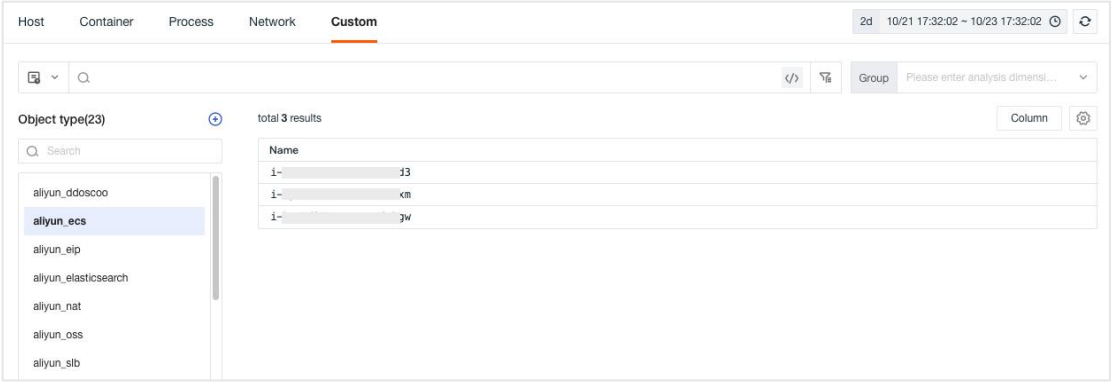



Click on the host, Pod, Deployment and Service to view the network details.




# Customize

Guance supports custom collection of object data other than hosts, containers, and processes, such as Alibaba Cloud ECS. In the Custom list of Infrastructure, you can create new object classes and customize object class names and object fields by adding object classes. After adding custom object classification, you can report custom data through API. Support to search the reported data, multi-label screening and multi-dimensional analysis and statistics, support data export, support to add display columns, and click to view details by sideslip.

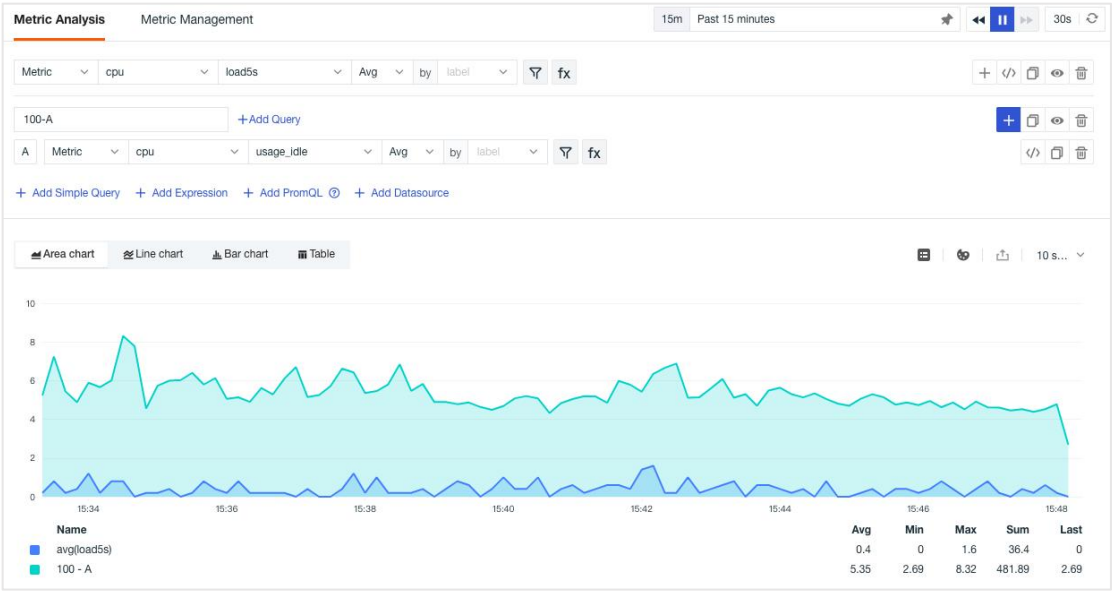



# Metrics

Guance supports viewing all data metric sets, metrics, and labels collected in the current workspace in metrics. You can query and analyze data such as metrics, logs, basic objects, custom objects, events, application performance, user access, security check, network, and Profile.

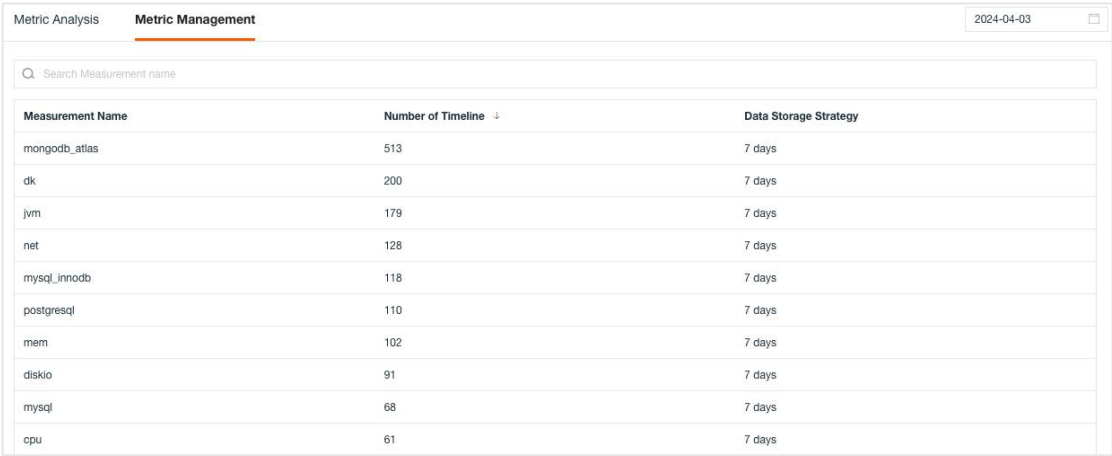
# Metric Analysis

Enter the **Metrics > Metric Analysis** page and support users to visually query different data based on Simple Query, Expression Query, PromQL Query, DQL Query and Datasource Query. It supports switching various viewing modes of line chart, area chart, bar chart, and table chart, supports adding query results as key metrics of warroom, supports exporting data in table chart view mode, and table chart supports querying and analyzing in time mode, group mode and query tool.

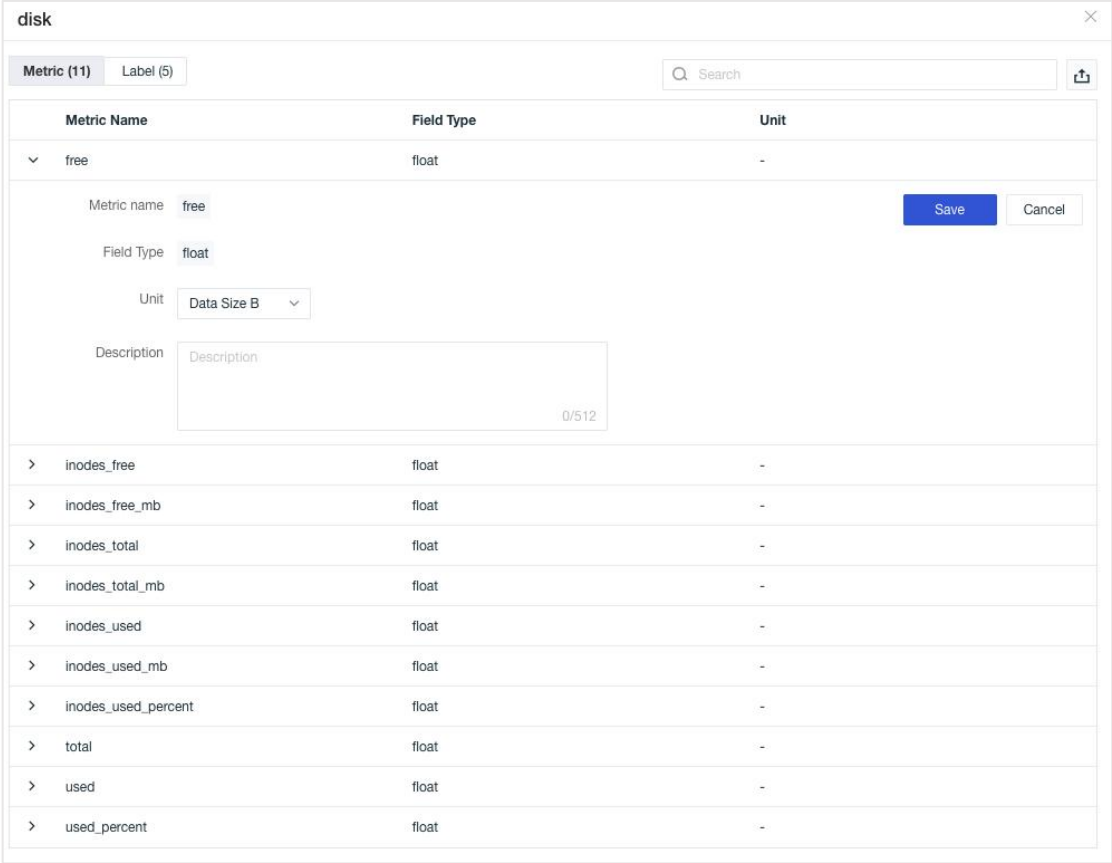



# Metric Management

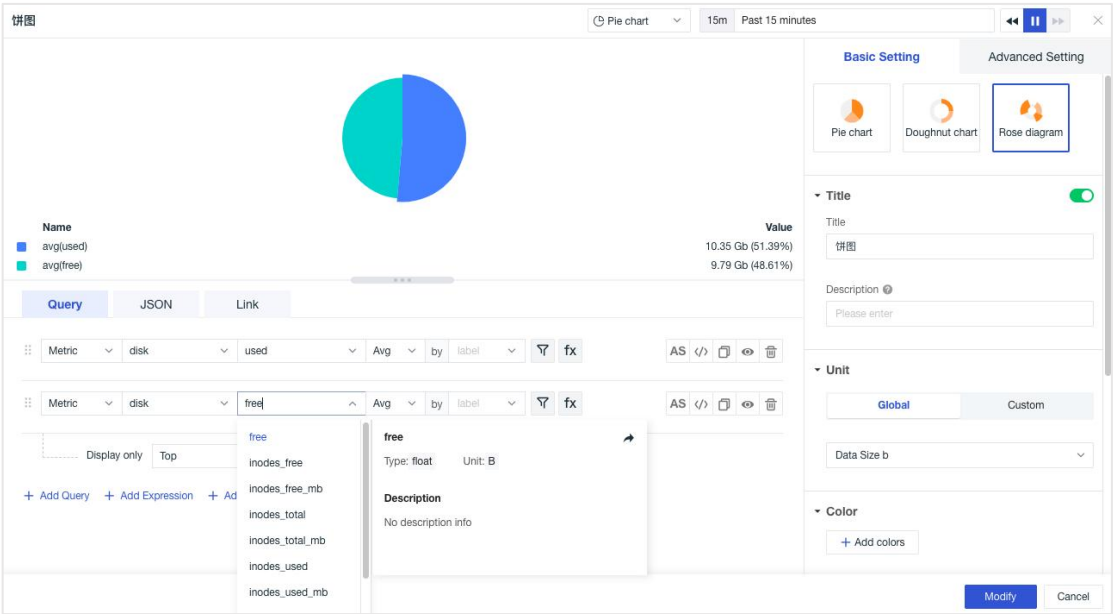
After the metric data is collected, you can view all the collected measurements, their metrics and labels, timeline number, data storage policy, and support the workspace owner to set the metric data storage policy in the **Metric Management** of the Guance workspace.




It supports to view all available metrics and labels under the measurement on the details page, support fuzzy search, customize metric units and descriptions on the metric page and view label descriptions on the Tag page.




Metric units and descriptions and label descriptions can be viewed and applied in simple modes of scene chart query, monitor metric detection and DQL query.




# Logs

Log data plays an important role in various aspects, including:

- Data search: Retrieving log information to locate corresponding problems and find solutions.
- Service diagnosis: Analyzing log information statistics to understand server load and service running status.
- Data analysis: Supporting further data analysis.

Guance provides comprehensive log collection capabilities. By configuring log collection, log data can be uniformly reported to the Guance workspace, where it can be stored, audited, monitored, alarmed, analyzed and exported.

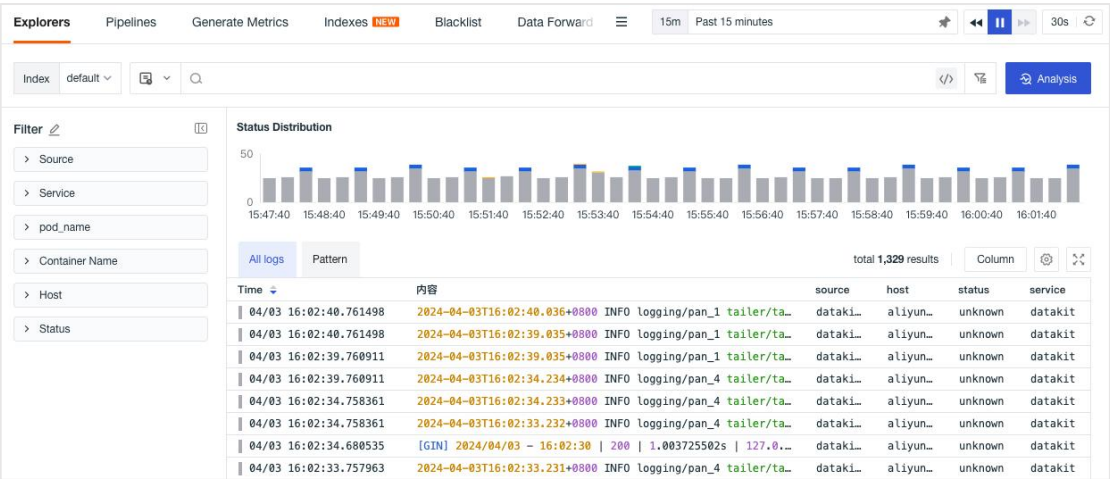
## Log Explorer

In the **Log Explorer**, you can search logs, apply multi-label filtering, perform multi-dimensional analysis statistics and quick filtering and view filtering history. It also supports data export, adding display columns, hiding sensitive log data contents or highlighting log data contents that need to be viewed through formatting configuration, saving current display contents, time range and filter conditions to snapshots and view historical snapshots.

Log Explorer supports three viewing modes: All Logs, Clustering, and Multidimensional Chart Analysis.

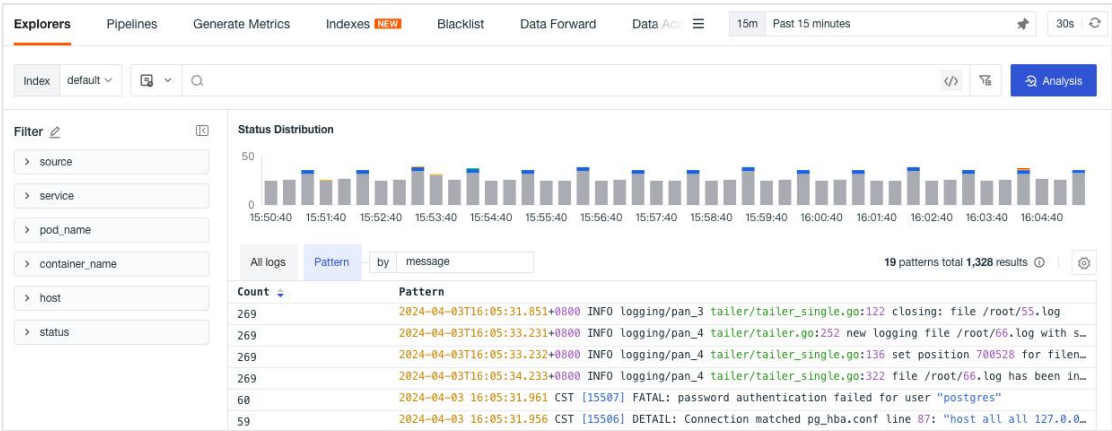
1. All Logs

View and analyze collected raw log data.



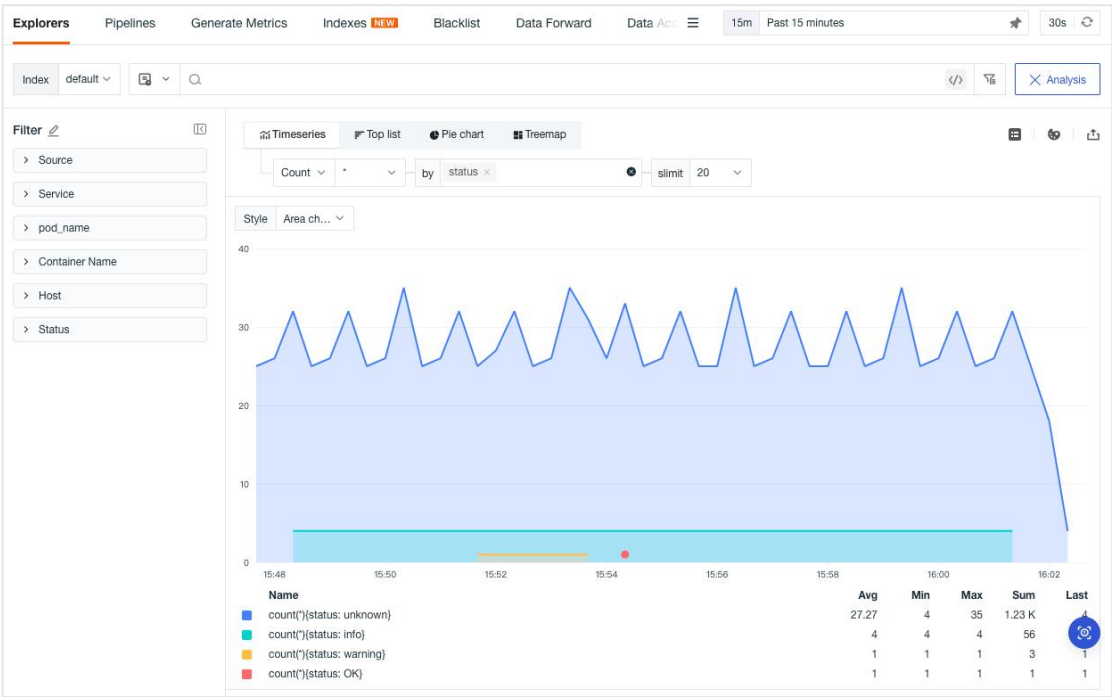
2. Clustering

Fix the current time period according to the time range selected at the top right, obtain 10,000 pieces of data in this time period for cluster analysis, aggregate logs with high approximation, and extract common pattern clustering, which is beneficial to finding abnormal logs and quickly locating problems.




3. Multidimensional Chart Analysis

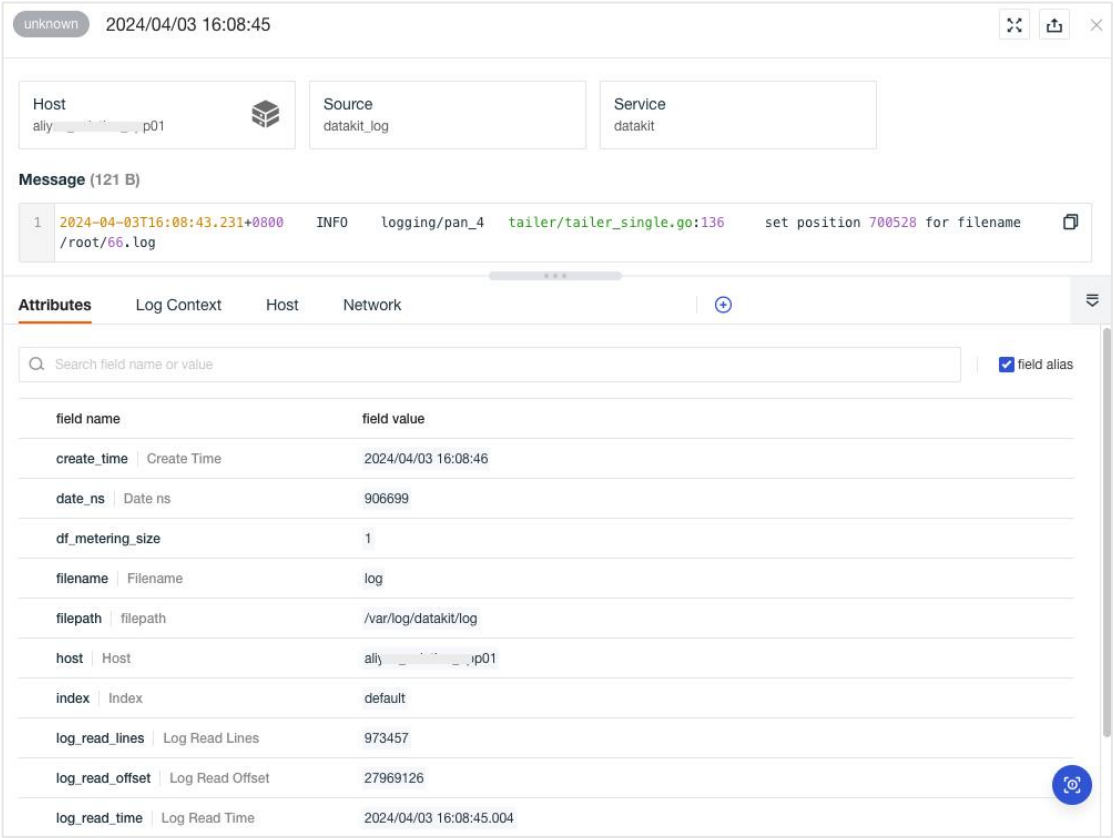
Group statistics of original log data based on 1-3 labels, to reflect the distribution characteristics and trends of log data in different groups and at different times.



## Log Details

Click on a log to view its corresponding details, including all attributes, log contents, extended fields associated with the log. It also supports viewing associated hosts, containers, Pod, links, metrics, etc.

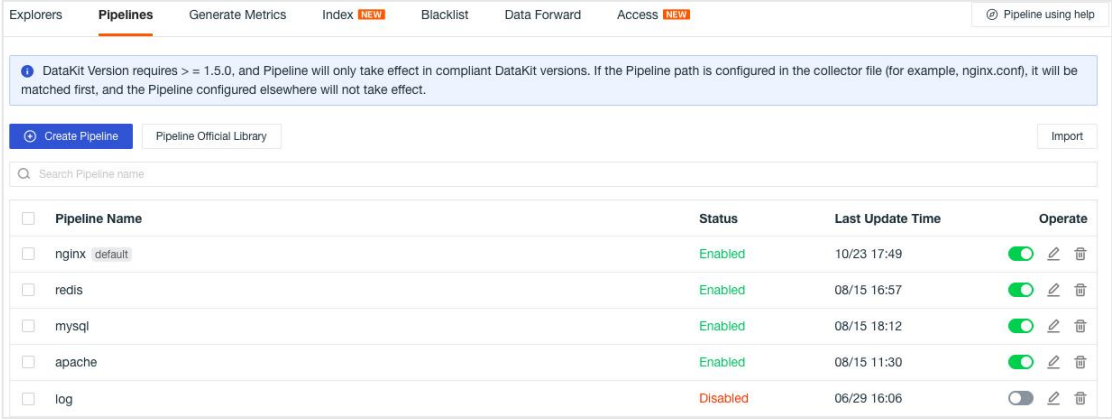
Note: To view the associated host, container, Pod, link and metric in the log details page, you need to match the relevant fields "host", "container_name", "pod_name", "trace_id", "service", "project" and "source", otherwise you cannot view the relevant pages in the log details.




## Pipelines

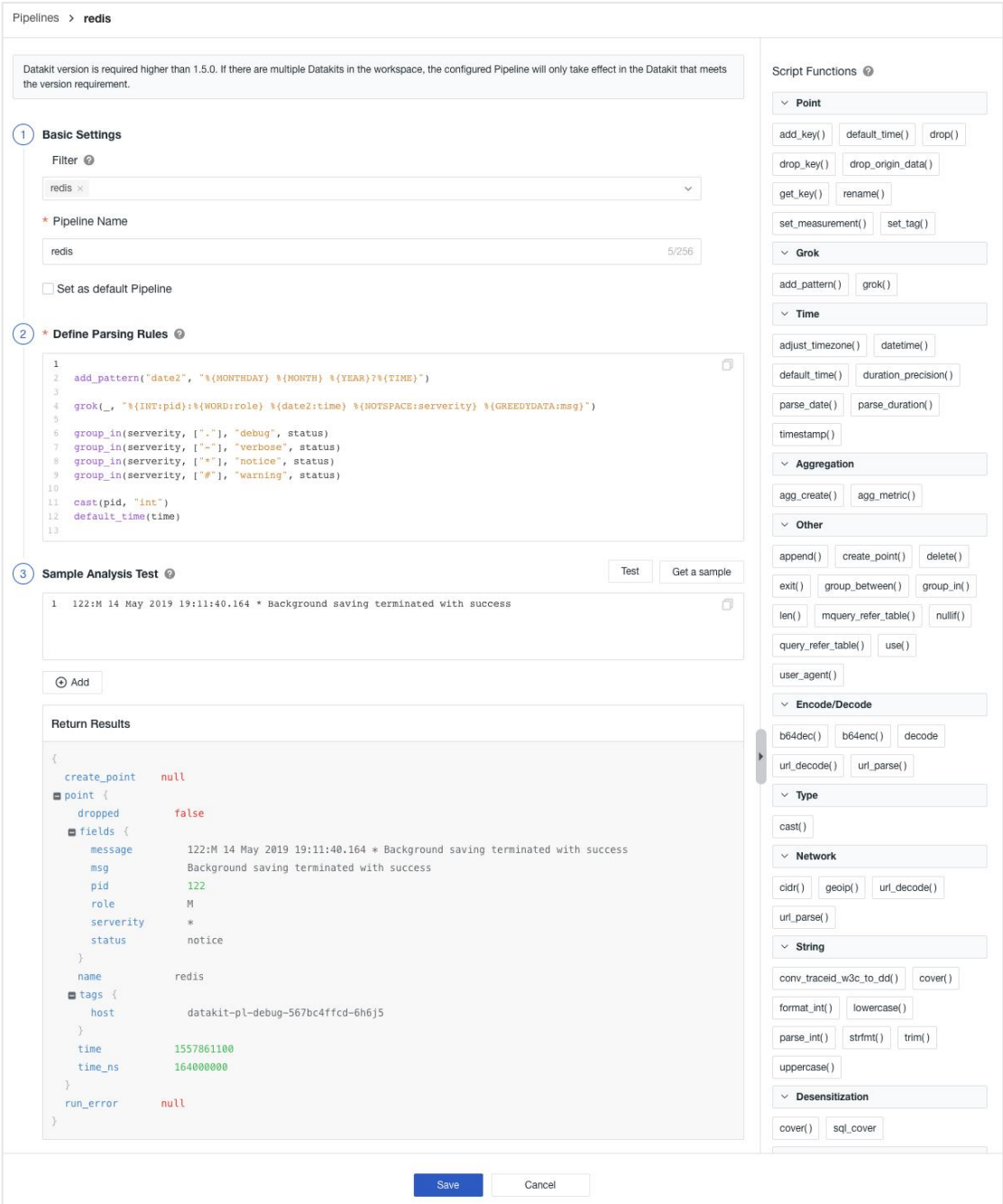
Pipeline supports text parsing of log data in different formats. By writing Pipeline scripts, you can customize and cut structured logs that meet the requirements, and use

the cut fields as attributes. Through the attribute field, we can quickly filter related logs, conduct data association analysis and help quickly locate and solve problems.




## Custom Pipeline Management

Guance supports users to create custom Pipeline scripts. In the Guance workspace **Log > Pipelines**, click **Create** to create a new Pipeline file. It supports a variety of script functions, and it can directly view their syntax format through the list of script functions provided by Guance, and supports one-click collection of samples for analysis rule testing, adding multiple sample analysis tests and setting default Pipeline scripts.




## Pipeline Official Library

Guance provides Pipeline official script library with inner log parsing Pipeline. In the Guance workspace **Log > Pipelines**, click **Pipelines Official Library** to view the inner standard pipeline official website file library, including nginx, apache, redis, elasticsearch, mysql and so on. You can choose to open any pipeline file, and create a

new pipeline file by cloning, which supports testing parsing rules through sample examples provided by Guance.

Note: The official pipeline library file does not support modification.

jenkins

Clone

1 Basic Settings

Filter

jenkins ×

* Pipeline Name

jenkins 7/256

2 * Define Parsing Rules

```
1
2  grok(_, "%{TIMESTAMP_ISO8601:time} \\[id=%{GREEDYDATA:id}\\]\t%{GREEDYDATA:status}\t")
3  default_time(time)
4  group_in(status, ["WARNING", "NOTICE"], "warning")
5  group_in(status, ["SEVERE", "ERROR"], "error")
6  group_in(status, ["INFO"], "info")
7
8
```

3 Sample Analysis Test

Test Sample Examples Jenkins log

```
1  2021-05-18 03:08:58.053+0000 [id=32]    INFO    jenkins.InitReactorRunner$1#onAttained: Started al
   l plugins
```

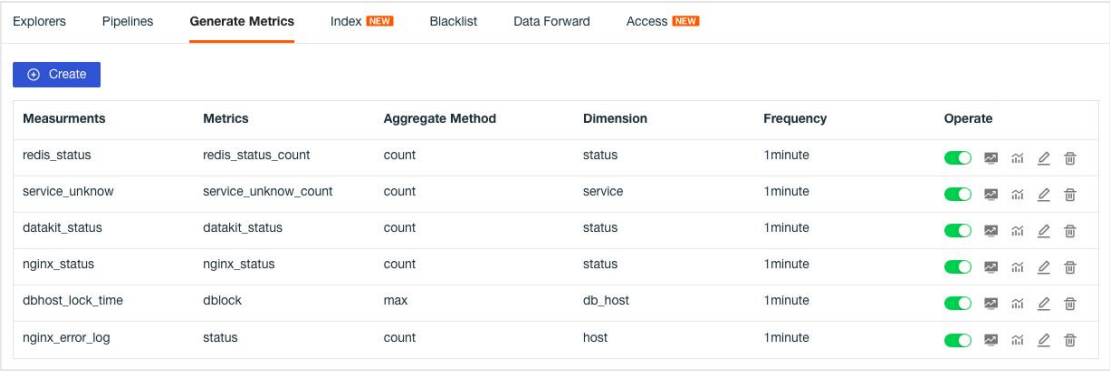
Return Results

```
{
  create_point    null
  point {
    dropped         false
    fields {
      id              32
      message         2021-05-18 03:08:58.053+0000 [id=32]   INFO
                     jenkins.InitReactorRunner$1#onAttained: Started all plugins
      status          info
    }
    name            jenkins
    tags {
      host            datakit-pl-debug-567bc4ffcd-6h6j5
    }
    time            1621307338
    time_ns         53000000
  }
  run_error       null
}
```

Cancel

## Generate Metrics

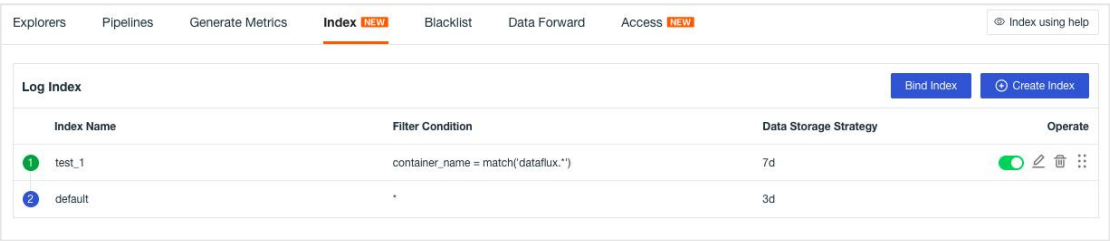
Guance supports configuring aggregation rules based on log data to generate new metric data, which is convenient for deeper data analysis.




## Index

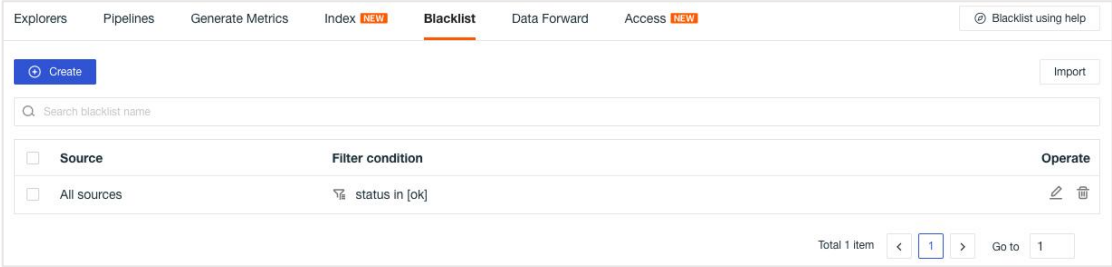
Guance supports setting multiple log indexes, filtering qualified logs, and saving them in different log indexes. This helps users save log data storage costs by selecting different data storage policies for log indexes.

Guance supports binding external index data, including the index data of SLS Logstore, Elasticsearch and OpenSearch. After successful binding, you can query and analyze the external index data in the Guance workspace.




## Blacklist

Guance supports blacklist function, and reduces unnecessary log data reporting by adding log filtering rules.



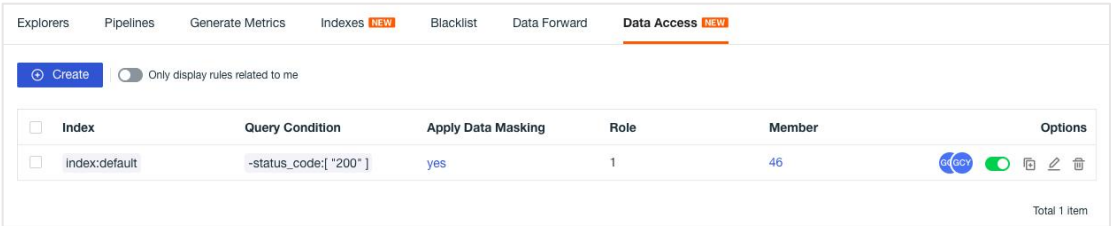

# Data Forward

Guance supports forwarding logs, links, and user access data that meets certain criteria to Guance's object storage and external storage, including Alibaba Cloud OSS, AWS S3, Huawei Cloud OBS, Kafka message queues, etc.


# Data Access

Guance supports configuring corresponding log data access query scopes for different member roles within the current workspace. In Logs > Data Access, click Create Rule. In the pop-up new page, select the index, set the filtering criteria, desensitization field, regex and authorize the role object.

Note: If "Show rules impact me" is enabled, only data access rules associated with the current account role will be shown and the log content queried in the log explorer will be synchronized to be affected by it.



# Application Performance Monitoring

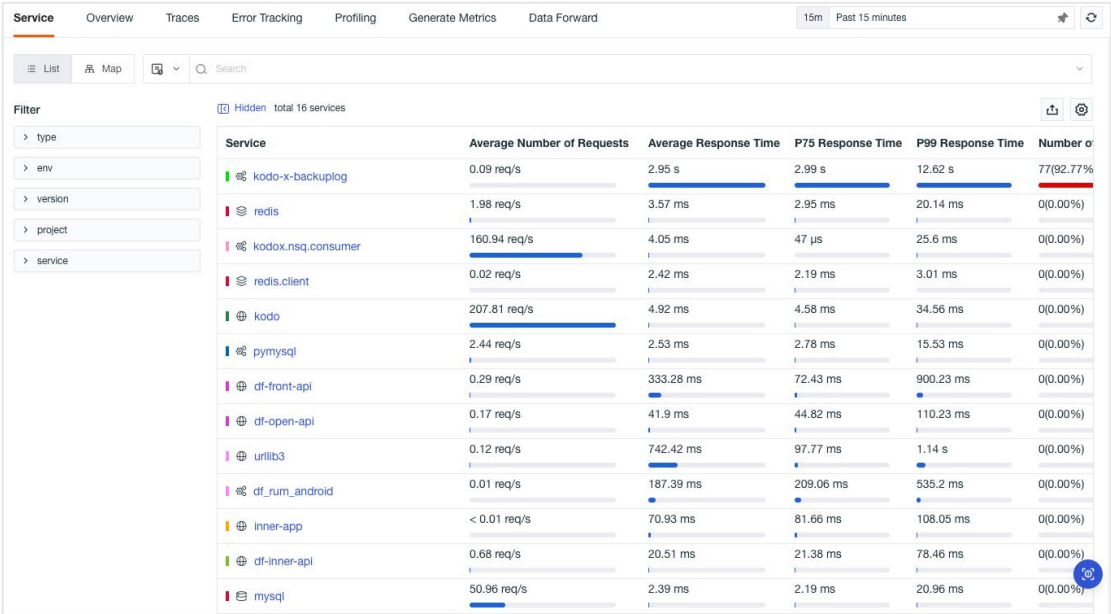
Guance supports the analysis and management of link data, tracks the time taken by all services to process requests and the status of requests, and can be used to monitor the performance of applications.

- Support reducing application performance data collection through sampling to save storage space.
- Support viewing key performance indicators of services, service call relationship topology, and ownership of different services' teams. Real-time monitoring of service performance indicators, their dependencies, and associated data to quickly identify and resolve service bottlenecks.
- Support querying and analyzing all collected and reported link data. Through flame graphs, intuitively view the context and execution efficiency of each span in the link. Support correlation analysis with user access monitoring and log monitoring to help quickly locate performance issues.
- Support viewing the historical trend and distribution of similar errors in the link to quickly identify error problems.
- Support obtaining associated code execution fragments of link-related spans through collecting profile data, visually displaying performance bottlenecks, and helping developers discover code optimization directions.
- Support generating new metric data based on existing data within the current space, facilitating the design and implementation of new technical indicators according to requirements.

# Services

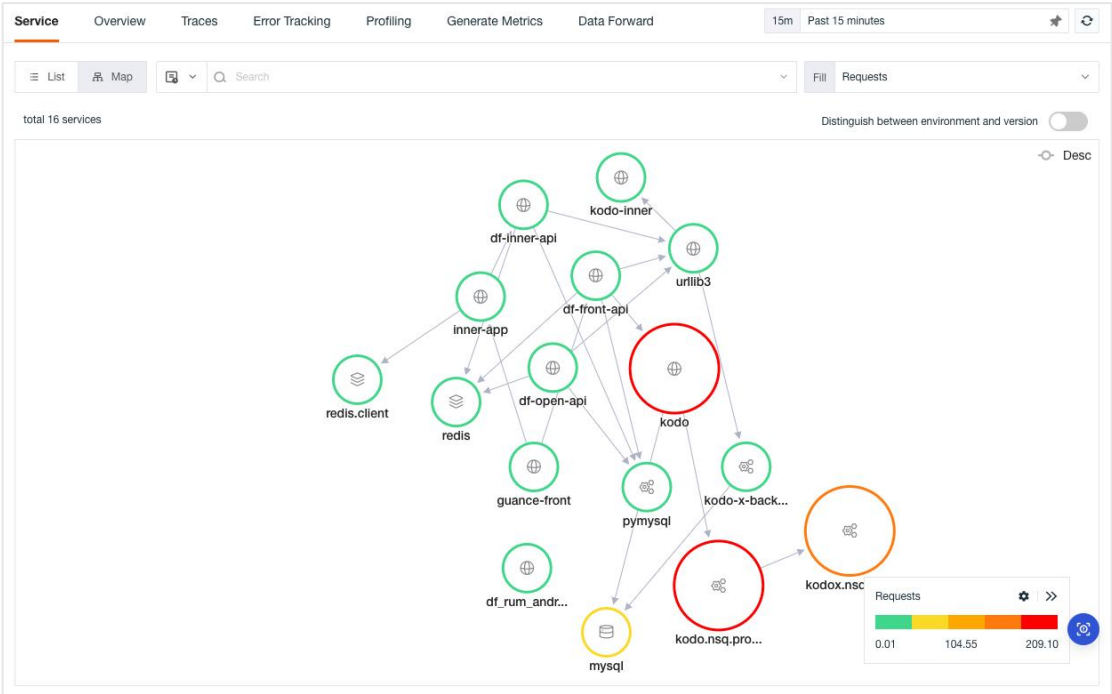
The **Service** in **APM** displays the list of all link services in the workspace, and can view the tracking metrics of all services: "average number of requests per second", "average response time", "P75 response time", "P95 response time" and "number of errors", which are sorted in descending order according to "number of errors" by

default. It supports clicking the name of key performance metrics to adjust the sorting display and searching, multi-label filtering and quick filtering, and binding performance view dashboards to display current service performance metrics.



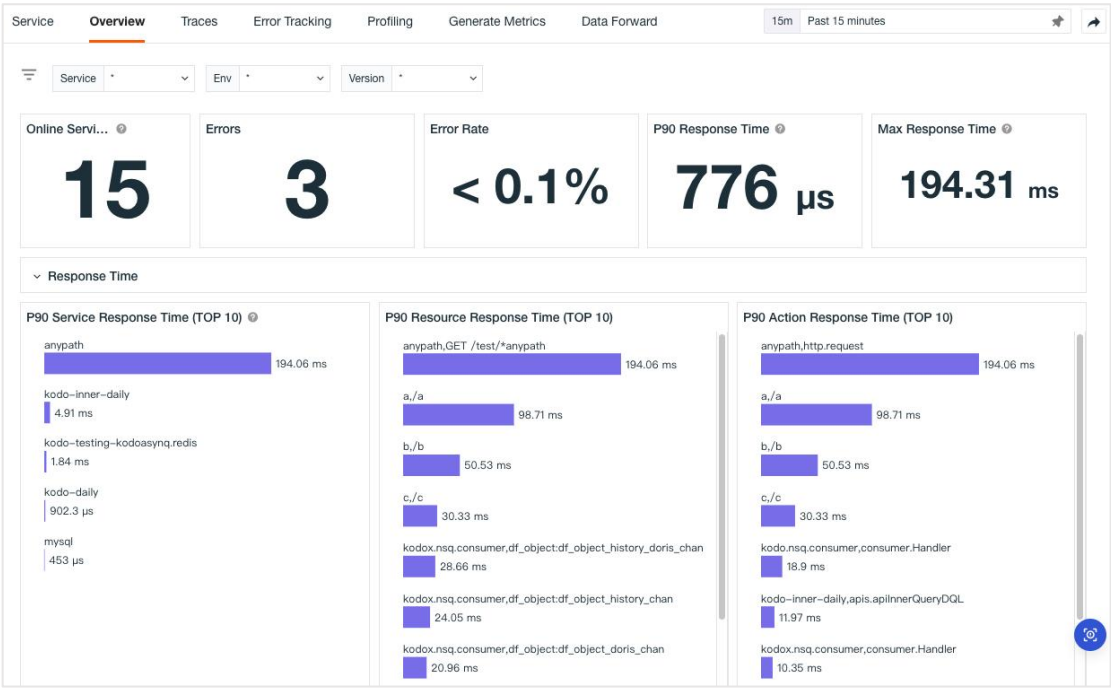

## Service Map

Link service supports switching list to topology diagram mode to view the call relationship between various services. When you hover the mouse over the service node, you can view the "number of requests", "P50 response time", "P75 response time", "P99 response time" and "number of errors" of the service. It supports screening and displaying through different performance metrics, and customizing the color interval of link service performance metrics. It also supports adjusting the distribution map by highlighting, node size, filling items, thumbnails, etc.



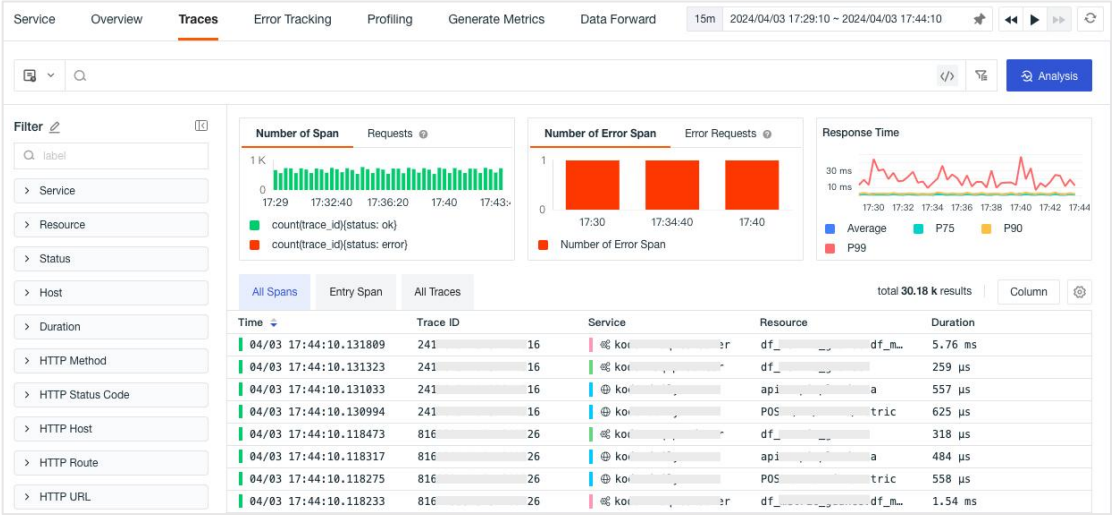

# Overview

In the **Overview** of application performance monitoring, it is supported to view the statistics of online service quantity, P90 service response time, service maximum impact time, service error number and service error rate. At the same time, it is also possible to view the Top10 ranking of P90 service, resource and operation response time, as well as the Top10 ranking of service error rate, resource 5xx error rate and resource 4xx error rate.




## Traces

In the Traces for which performance monitoring is applied, it is supported to count the "Span number", "Request number", "Error Span number", "Error request number" and "Response time" of links within the selected time range, and display a list of all traces served. Guance provides three traces filtering viewing lists, namely "All Spans", "Service Top Spans" and "All Traces". It supports trace data search, multi-label filtering, quick filtering, data export, adding display columns and other operations, and also supports saving the current display content, time range and filtering conditions to snapshots and viewing historical snapshots.




## Trace Details

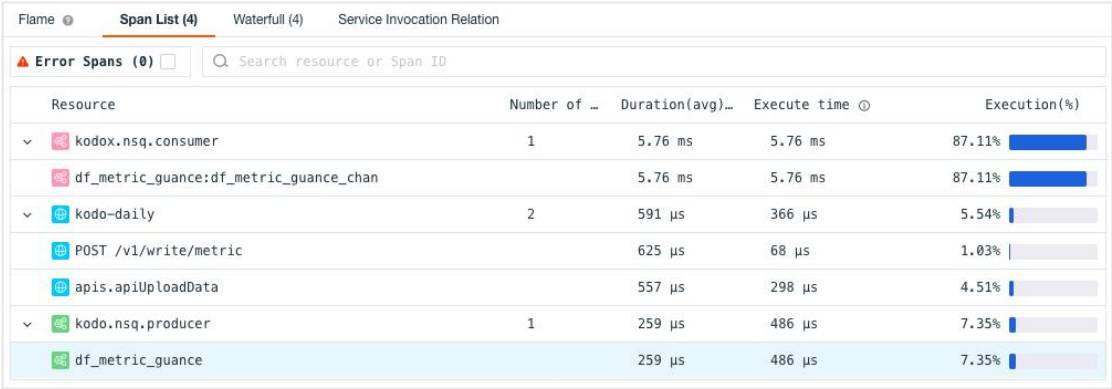
Click on the Trace list to view the details of the trace, including all relevant "attribute labels", "flame", "span list", "waterfall", "service invocation relation" and data such as hosts, logs, networks and code hotspots associated with the trace. It supports filtering Error Spans, searching for resource names or Span IDs, keyword searching and multi-label filtering in associated logs. Click log content to jump directly to log details page, which can combine log details to analyze trace performance, and support binding inner views for association analysis.

### 1. Flame

Used to clearly show the flow and execution time of each span in the whole trace. At the same time, the corresponding service list and response time are displayed.

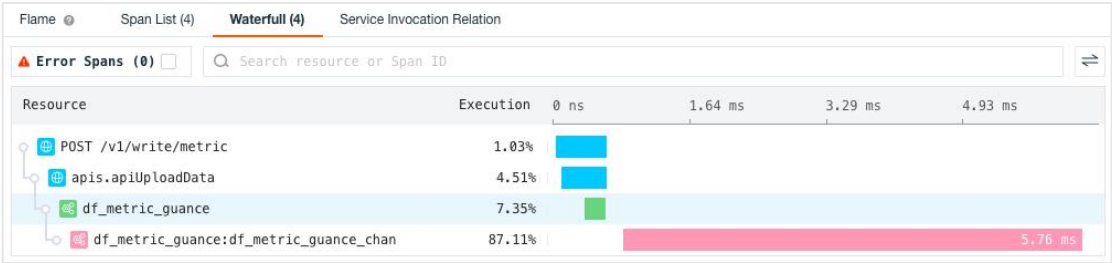

### 2. Span List

Show a list of all the spans in the link, including "resource", "span number", "duration", "execution time" and "execution time percentage". Click **Span Name** to view the corresponding span details.



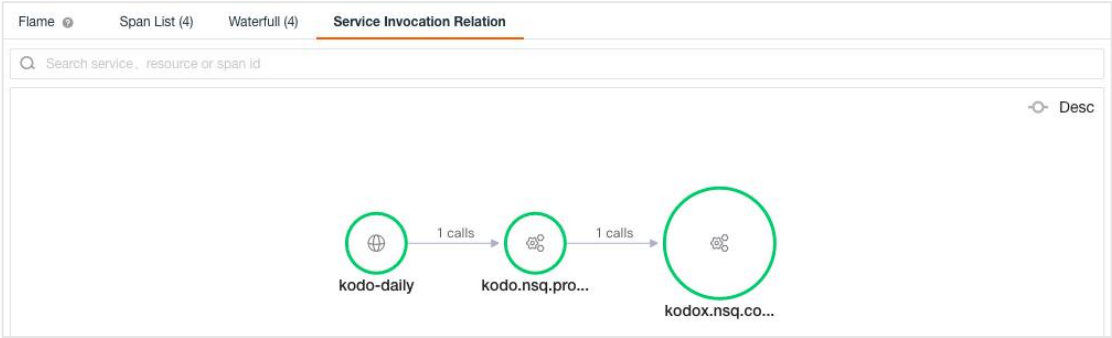

### 3. waterfall

Switch to the waterfall chart to view the parent-child relationships between various resources. The waterfall chart displays Span data in chronological order based on the start time.




### 4. Service Invocation Relation

Used to view the invocation relationship between various services.

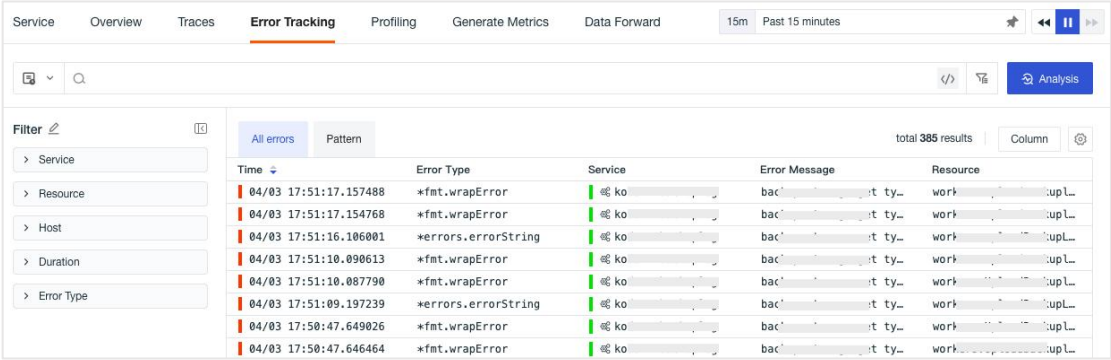



## Error Tracking

In the application of Error Tracking of performance monitoring, it supports a quick view of the historical trend and distribution of similar errors in the link, and helps to

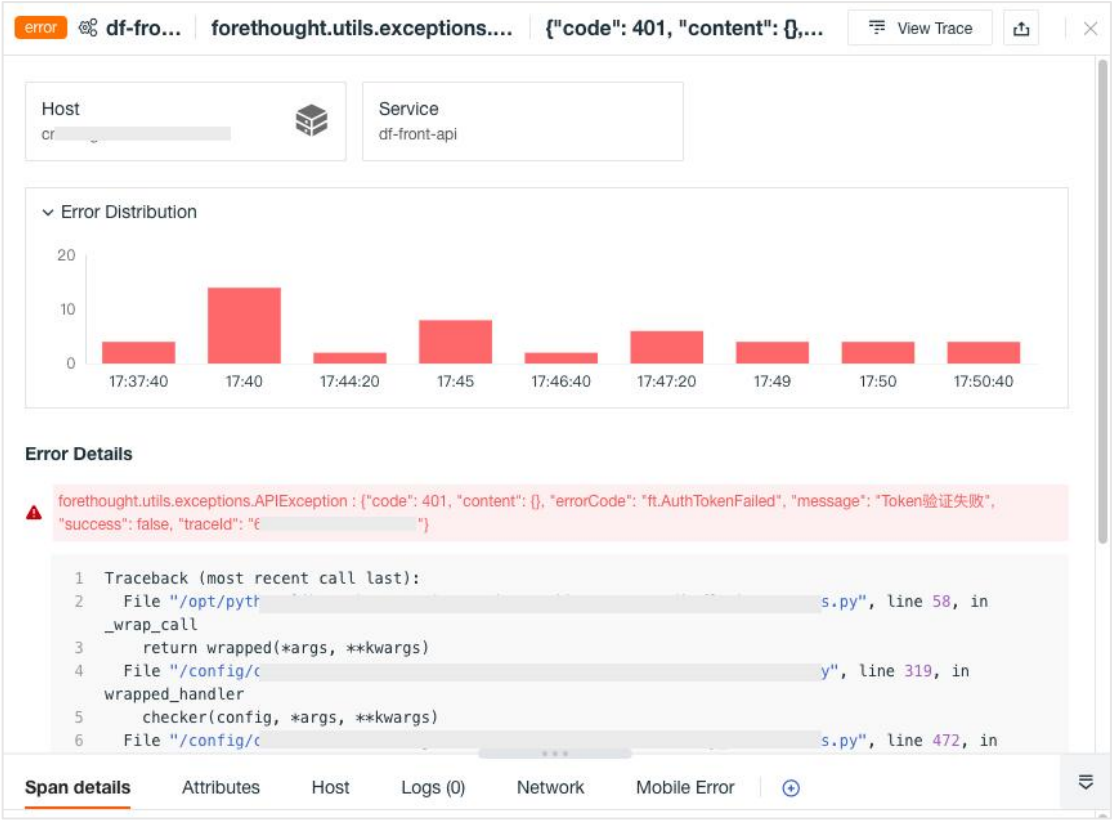
quickly locate performance problems. The error tracking explorer includes two lists: All Errors and Clustering Analysis:

- All Errors: Used to view all link errors that occur in the project application as a whole.
- Clustering analysis: Used to quickly view the most frequent link errors that need to be resolved.



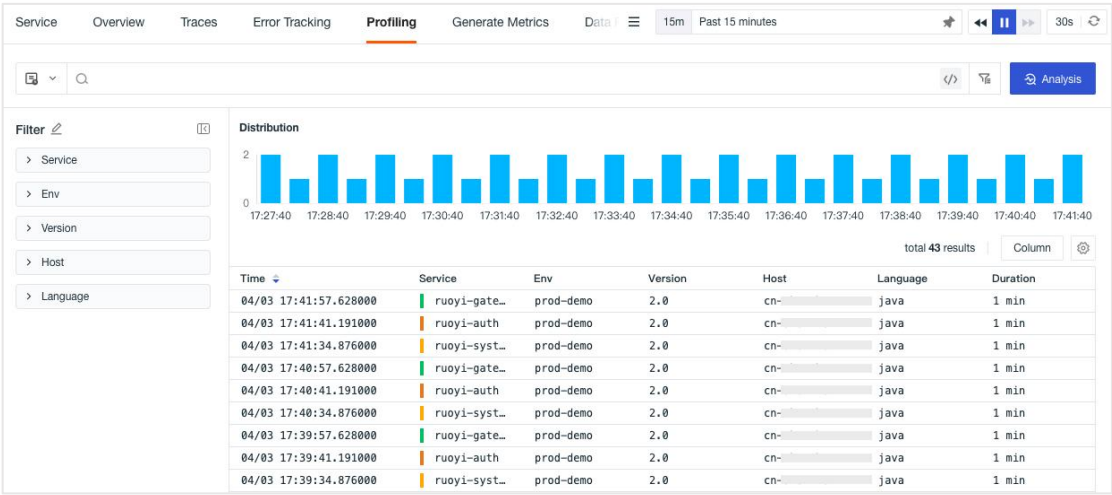

Click on any error link to view error details.

- Error profile: Based on error information error_message and error type error_type, the error links with high approximation are aggregated and counted, and according to the time range selected by the error explorer, the corresponding time interval is automatically selected to show the distribution trend of errors, which helps you intuitively view the time points or time ranges where frequent errors occur and quickly locate link problems.
- View Link: You can locate link problems by looking at the upstream and downstream Spans of the flame diagram of the wrong link.




# Profile

Profile supports collecting dynamic performance data of applications running in different language environments such as Java/Python, and helps users to view performance problems of CPU, memory and IO. In the Profile explorer, it supports operations such as searching Profile data, multi-label filtering, quick filtering, data export, adding display columns, etc. It supports saving the current display content, time range and filter conditions to snapshots and viewing historical snapshots.

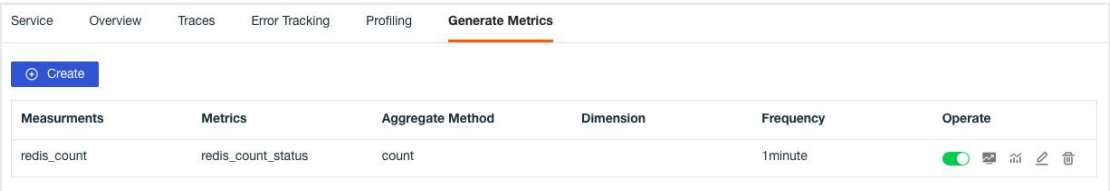


## Profile Details

Click on the Profile list to view the corresponding performance details, including property tags, performance flames, and operational information. Through the performance flame diagram, we can analyze the usage of CPU, memory or IO at the level of different types of code methods, and intuitively understand the execution performance and call of methods. At the same time, Profile provides analysis and view of execution data based on methods, libraries, threads and other dimensions, which shows some methods with large execution more intuitively and locates performance problems faster.


## Generate Metrcis

Guance supports generating new metric data based on link data configuration aggregation rules, which is convenient for deeper data analysis.



# Data Forward

Guance supports forwarding logs, links, and user access data that meets certain criteria to Guance's object storage and external storage, including Alibaba Cloud OSS, AWS S3, Huawei Cloud OBS, Kafka message queues, etc.


# Real User Monitoring

Guance supports the collection of user access data for web, Android/iOS apps, and applets. It provides scenario analysis such as explorer, overview, performance analysis, resource analysis, and error analysis to help you quickly monitor user behavior and identify problems.

- Sampling is supported to reduce data collection for user access and save storage space. The generation of new metric data based on existing data in the current space is convenient for designing and implementing new technical metrics according to requirements.
- When creating applications, custom application IDs can be used as the unique identification of the current workspace, and different workspaces can use the same application ID for uploading and matching SDK collection data.
- Support "local deployment" and "public DataWay deployment" to receive RUM data.
- Access session playback is supported, which generates video records by capturing clicks, mouse movements, and page scrolling. This helps to deeply understand the user's operation experience and locate errors, reproduce, and solve problems in combination with user access performance data.
- Implementation of "browser plug-in" is also supported, using a browser to record user access behavior and create codeless end-to-end tests.

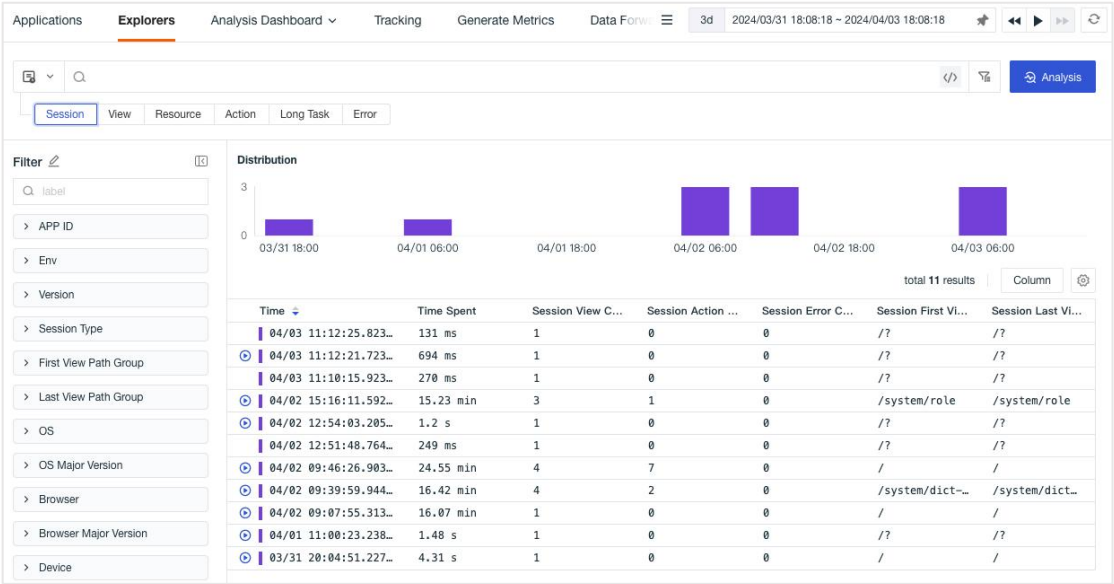
# Explorer

Guance user access explorer supports searching, multi-label filtering, quick filtering, and export viewing analysis of user access data in applications. Custom addition/deletion of display columns is supported. Clicking on session or page data will display details. Snapshotting is supported to save current display content, time range, and filter criteria to view historical snapshots.

Guance user access monitoring explorer includes session, view, resource, action, long_task and error.

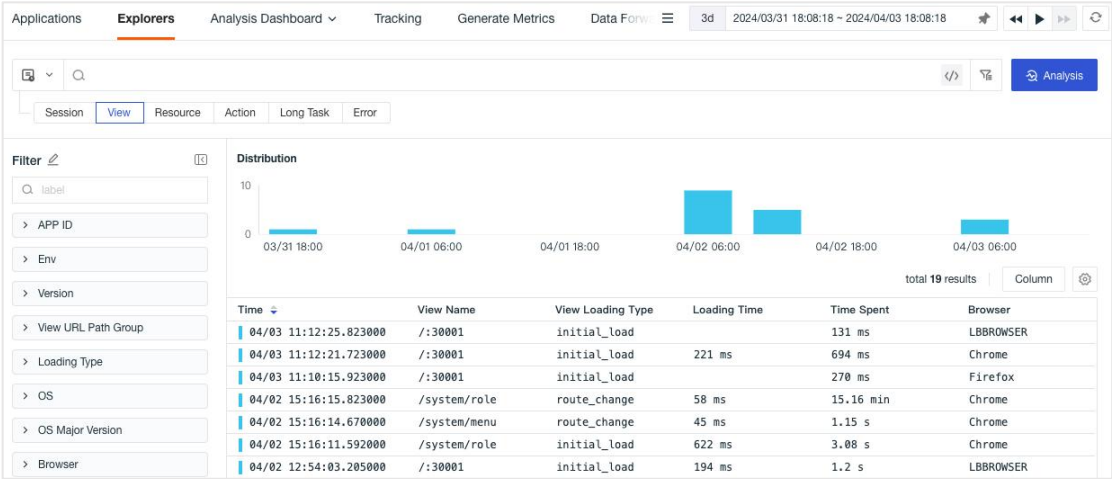
## Session Explorer

Select **Session Explorer** in the upper left corner to query and analyze the session data when the user accesses. This includes the session duration when the user accesses (that is, the time from opening an application to closing), session type, number of page visits, number of operations, number of errors, initial page visits, and last page browsing by the user. The **Play** button can be clicked to view the session replay of the changed session.



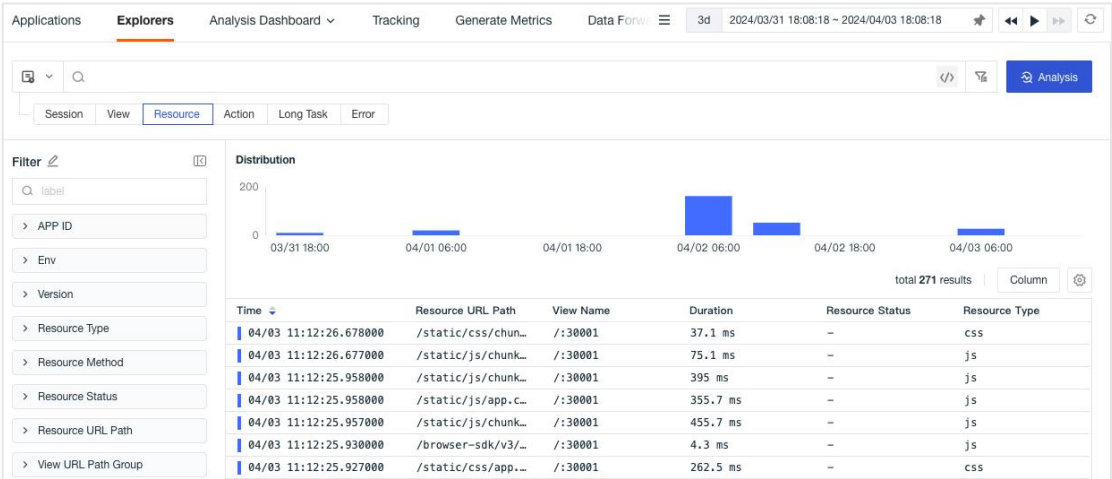
## View Explorer

Select **Session Explorer** in the upper left corner to query and analyze the session data when the user accesses. This includes the session duration when the user accesses (that is, the time from opening an application to closing), session type, number of page visits, number of operations, number of errors, initial page visits, and last page browsing by the user.



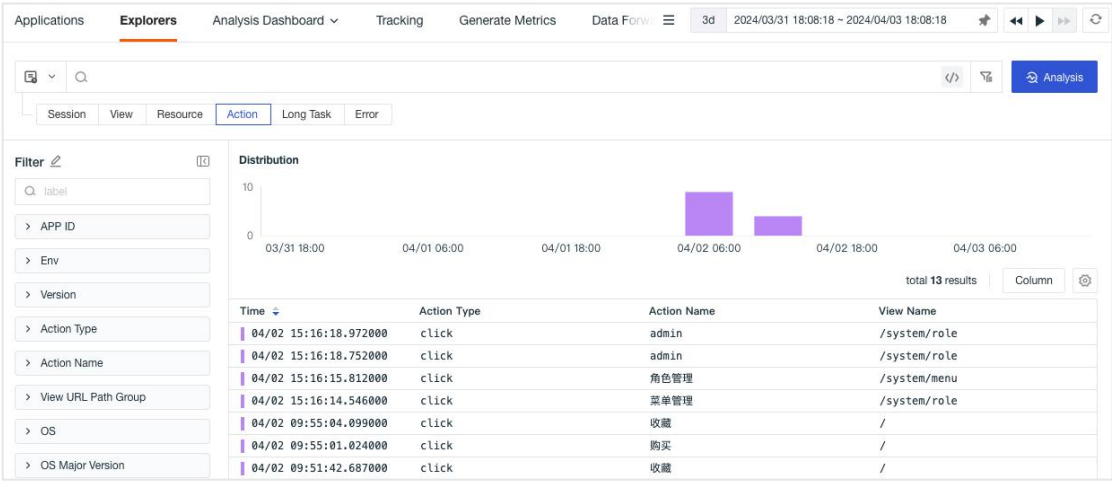

## Resource Explorer

Select **Resource Explorer** in the upper left corner to query and analyze resource loading performance when the user accesses. This includes the resource address, status code, request mode, resource loading time, and so on.



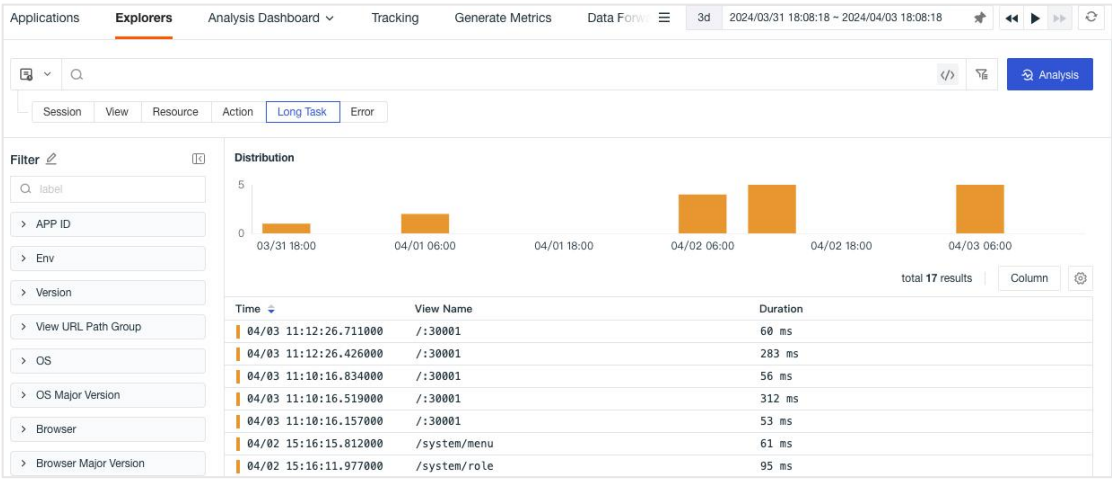
## Action Explorer

Select **Action Explorer** in the upper left corner to query and analyze the operation behavior when the user accesses. This includes the operation type, operation content, and operation time when the user accesses.




## Long Task Explorer

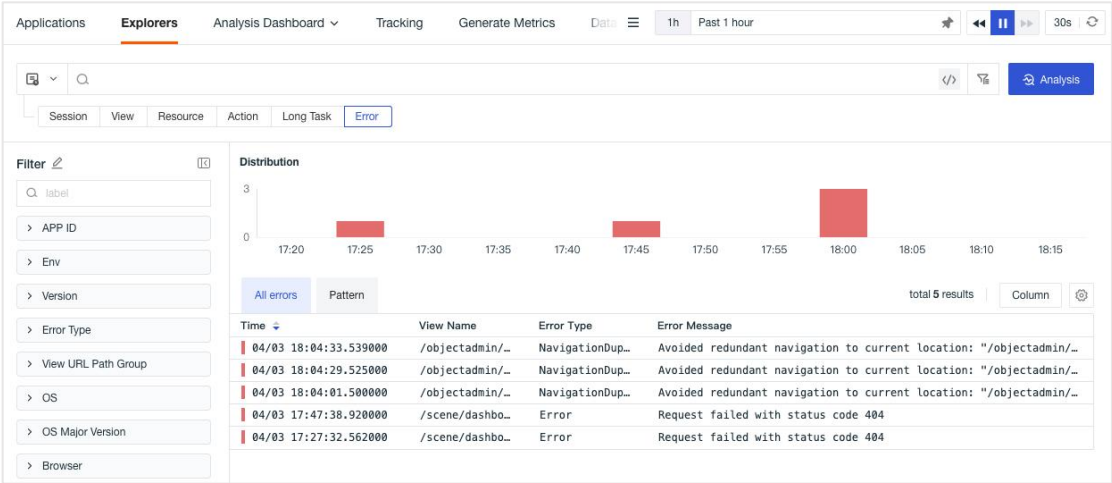
Select **Long Task Explorer** in the upper left corner to query and analyze the resource loading performance when the user accesses. This includes the resource address, status code, request mode, and resource loading time when the user accesses.



# Error Explorer

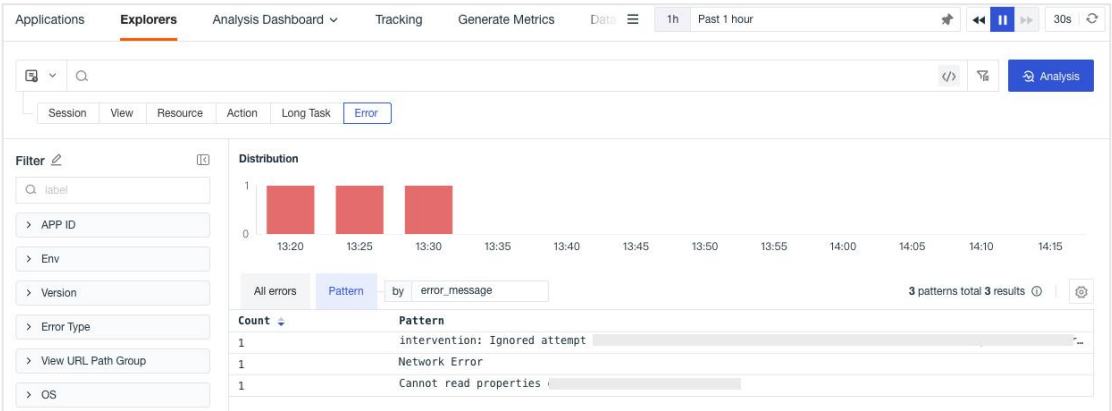
1. All errors

Select **Error Explorer** in the upper left corner to query and analyze the code errors when users visit. This includes the page address, code error type, and error content when users visit.




2. Pattern

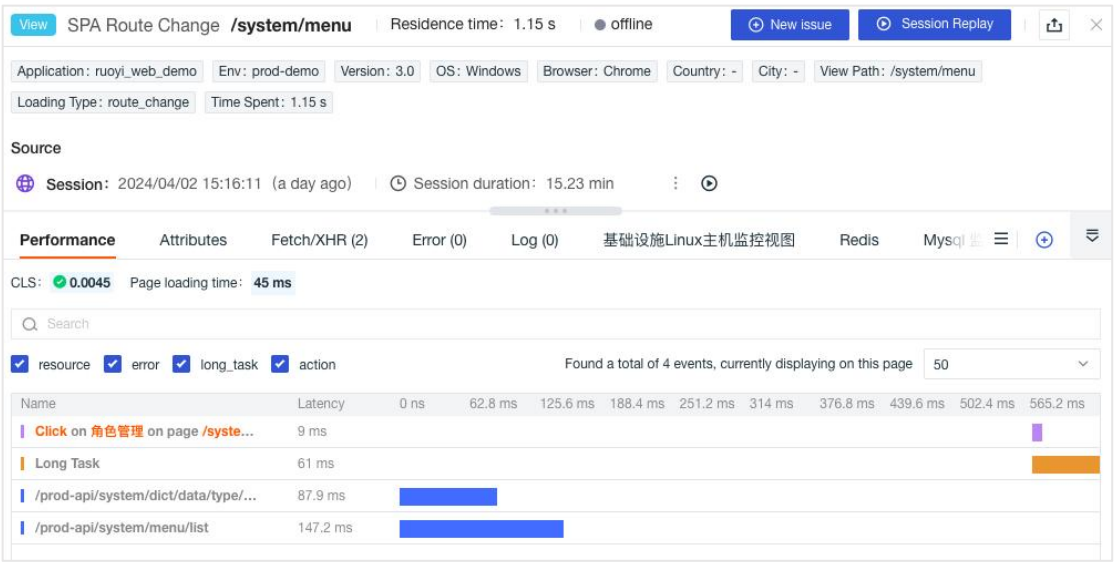
Support fixed current time period based on the selected time range in the upper right corner. Retrieve 10,000 data points within this time period for cluster analysis. Aggregate errors with high similarity and extract and count common patterns for clustering. This helps quickly discover abnormal links and troubleshoot issues.



# User Access Details

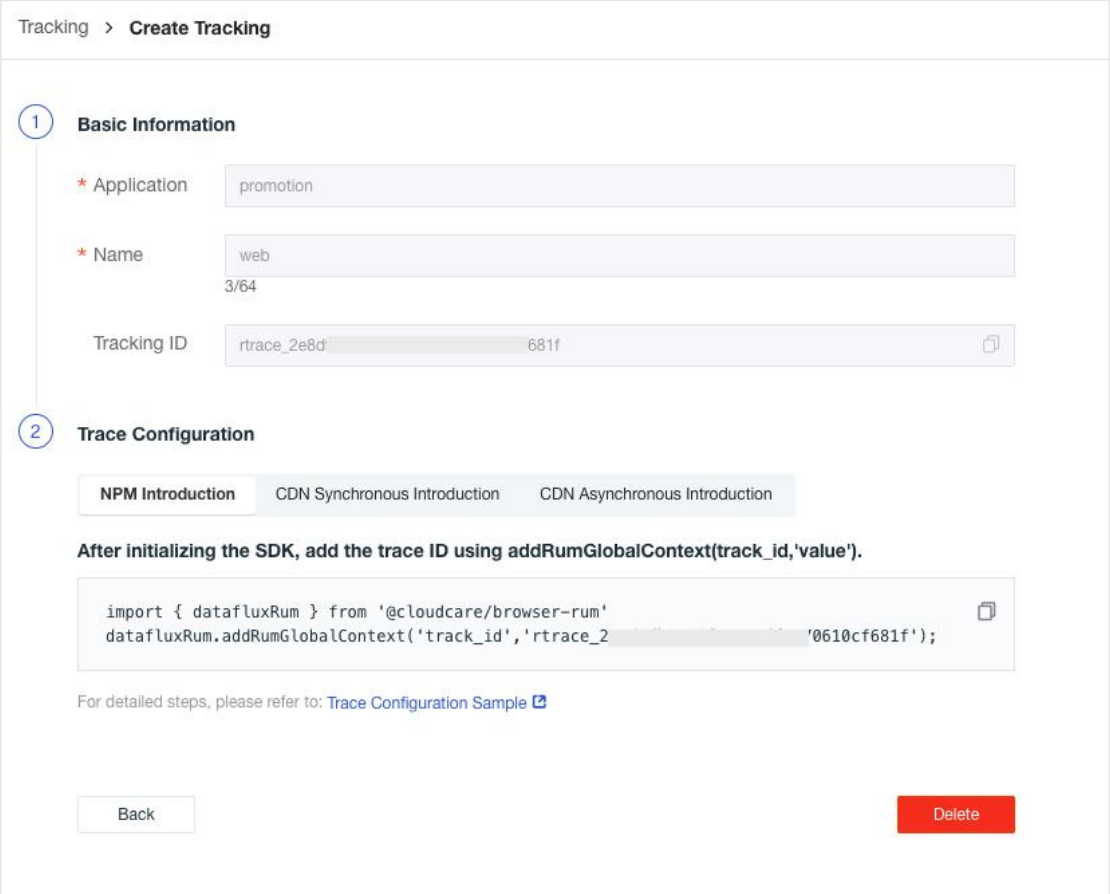
In the explorer, clicking on the data list will provide details of the user's access. This includes session replay, performance, extended fields, Fetch/XHR, errors and logs.

- Session replay: View the whole session process of the user, including the visited pages, operation records, and error data. Click to play the user's operation process.
- Performance: View the front-end page performance when the user accesses the specified application, including page loading time, content drawing time, interaction time, input delay, and so on.
- Extended Fields: Support for quick filter viewing by selecting extended fields, including Filter Field Values, Reverse Filter Field Values, Add to Display Columns, and Copy.
- Fetch/XHR: View every request made to the backend application when the user accesses, including the occurrence time, the link of the request, and the duration. Click Request to jump to the details page of the corresponding link.
- Errors: View the error data information, the type of error, and when the error occurred at this user access. Click on the error message to jump to the details page of the corresponding error. The function of Sourcemap is supported to restore confused code, which is convenient to debug and locate code problems in source code when troubleshooting errors.
- Log: Associated logs can be viewed based on current user access. Support keyword search and multi-label filtering of logs. Click **Logs** to jump to the corresponding log page.



# Tracking

Guance supports users to create new tracking tasks through RUM and monitor the customized link tracking trajectory in real time. By preset link tracking trajectory, link data can be screened centrally, user access experience can be queried accurately, and loopholes, anomalies and risks can be found in time.

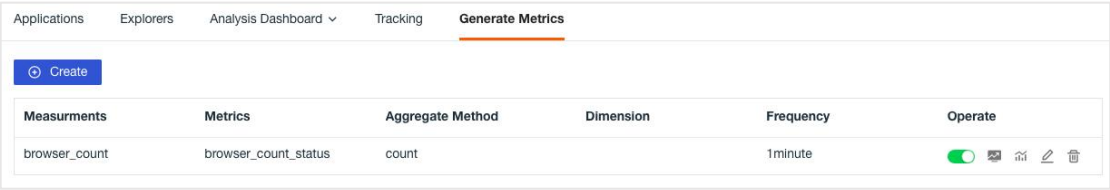



### Automatic Call Tracing

Guance supports the implementation of **Browser Plug-in**, using a browser to record user access behavior and create codeless end-to-end tests.

# Generate Metrics

Guance supports configuring aggregation rules based on user access data to generate new index data, which is convenient for deeper data analysis.




## Data Forward

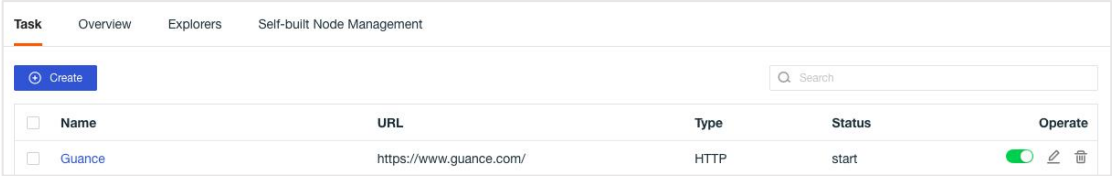
Guance supports forwarding logs, links, and user access data that meets certain criteria to Guance's object storage and external storage, including Alibaba Cloud OSS, AWS S3, Huawei Cloud OBS, Kafka message queues, etc.


## Synthetic Tests

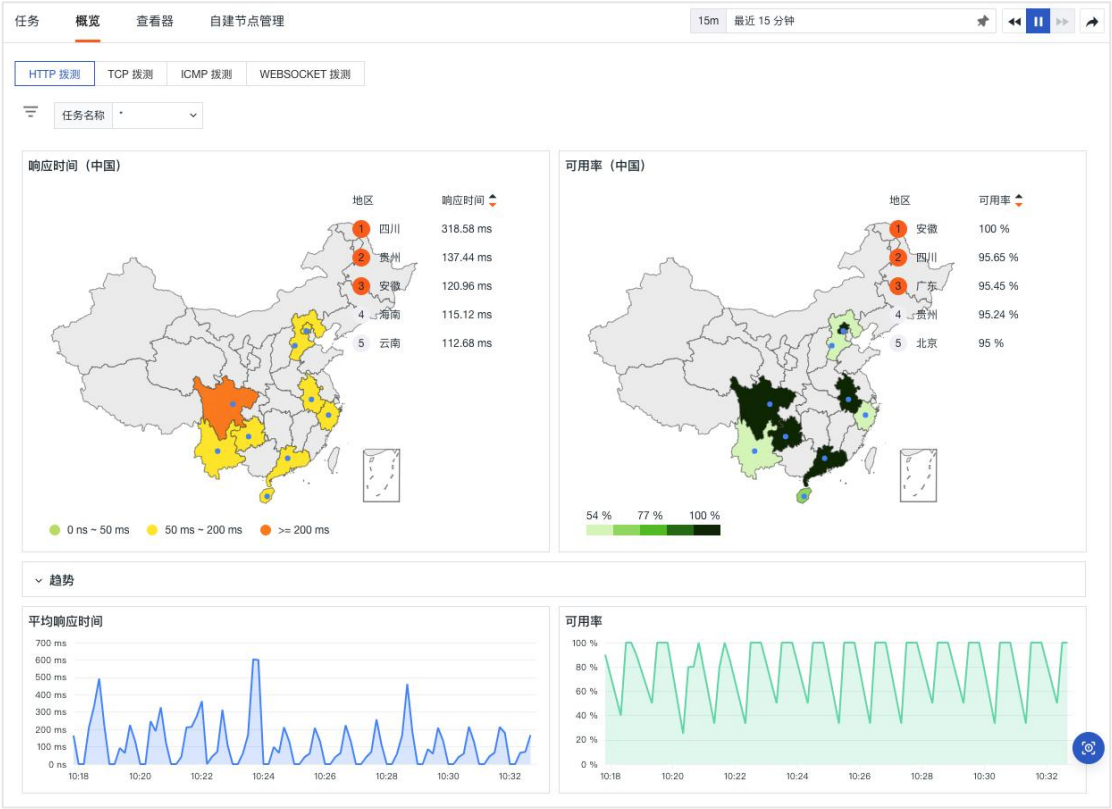
Guance provides an out-of-the-box availability monitoring solution, which uses a global monitoring network to comprehensively monitor the network performance, network quality, and network data transmission stability of different regions and operators to various services by creating dialing tasks based on different protocols such as HTTP, TCP, ICMP, and WEBSOCKET. Through real-time monitoring and statistics of the availability of dialing and testing tasks, dialing and testing task logs, and real-time alarms are provided to help you quickly find network problems and improve network access quality.

## Synthetic Tests Management

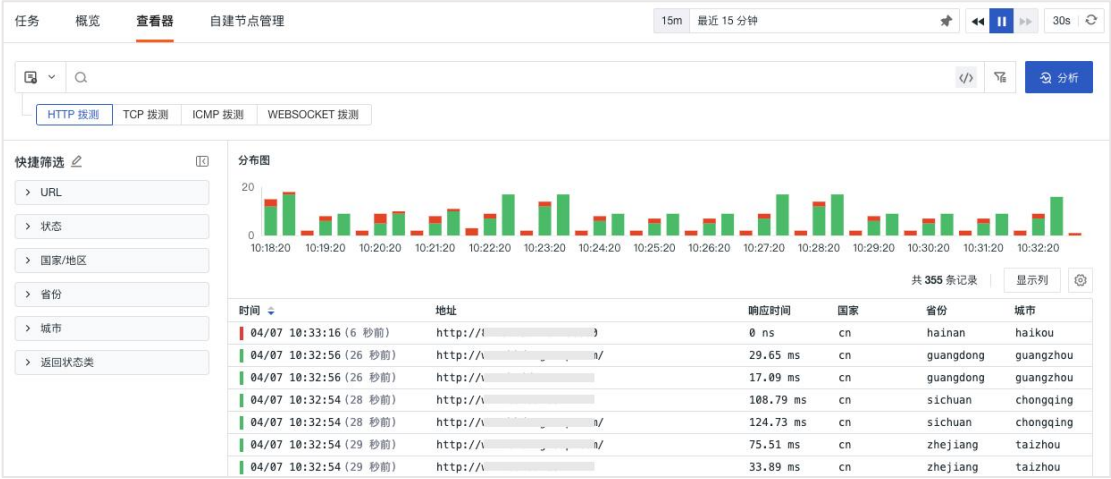
In **Synthetic Tests**, click **Create** to add a new dialing test task. After creating a completed dialing task, you can analyze the response time and availability of the current dialing task from both the geography and trend dimensions on the overview page.




After creating a monitoring task, you can analyze the response time and availability of the current monitoring task from two dimensions: geography and trends on the overview page.




Synthetic Tests Explorer supports such operations as viewing, searching, multi-label filtering, shortcut filtering, data export, and adding display columns. It supports the statistics of dialing test data according to the selected time range through stacked histogram, save the current display content, time range, and filter conditions to snapshot and view the historical snapshot, and click the list data to view the details of dialing test results.




## Self-built Node Management

Guance supports self-building of new dialing and testing nodes on a global scale. After creating the self-built nodes, the configuration information of the designated nodes is obtained through "Get Configuration" and configured in DataKit. After the configuration is completed, you can choose to use it in dialing and testing.


## Security Check

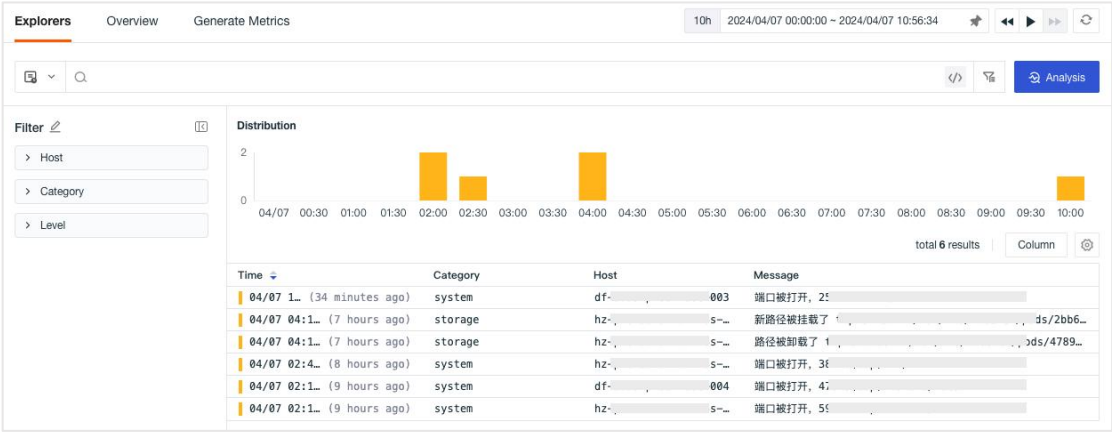
Guance supports timely monitoring, inquiring, and associating all inspection events through Security Check. It helps improve inspection quality, problem analysis, and problem handling ability while finding loopholes, anomalies, and risks in time. And it supports the generation of new index data based on the existing data in the current space, which is convenient for designing and implementing new technical metrics according to requirements.

## Overview

In **Security Check > Overview**, you can view the overview of security check events in different hosts by screening hosts, security check levels, and security check categories, including the number of security check events in different levels and visual chart analysis, and the ranking list of security check events in different categories and rules.

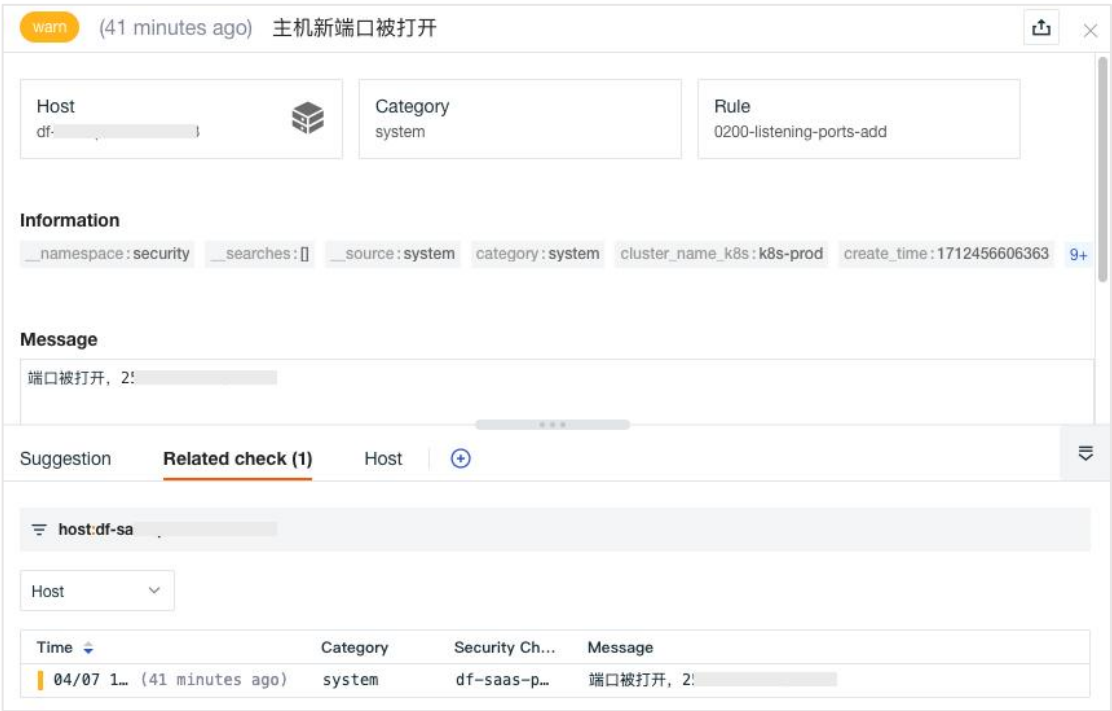

## Explorer

In **Security Check > Overview**, it supports viewing, searching, multi-label filtering, quick filtering, data export, and adding display columns to reported security check events. Support the statistics of security check data according to the selected time range through stacked histogram, save the current display content, time range, and filter conditions to snapshot and view the historical snapshot, and click the list data to view the details of security check.




# Security Check Details

Click on the inspection event you want to view, and in the underlined details page, you can view the handling suggestions for this security check event, including the theoretical basis, risk items, audit methods and remedial measures, and at the same time, you can view the related inspection events and hosts, etc.



## Generate Metrics

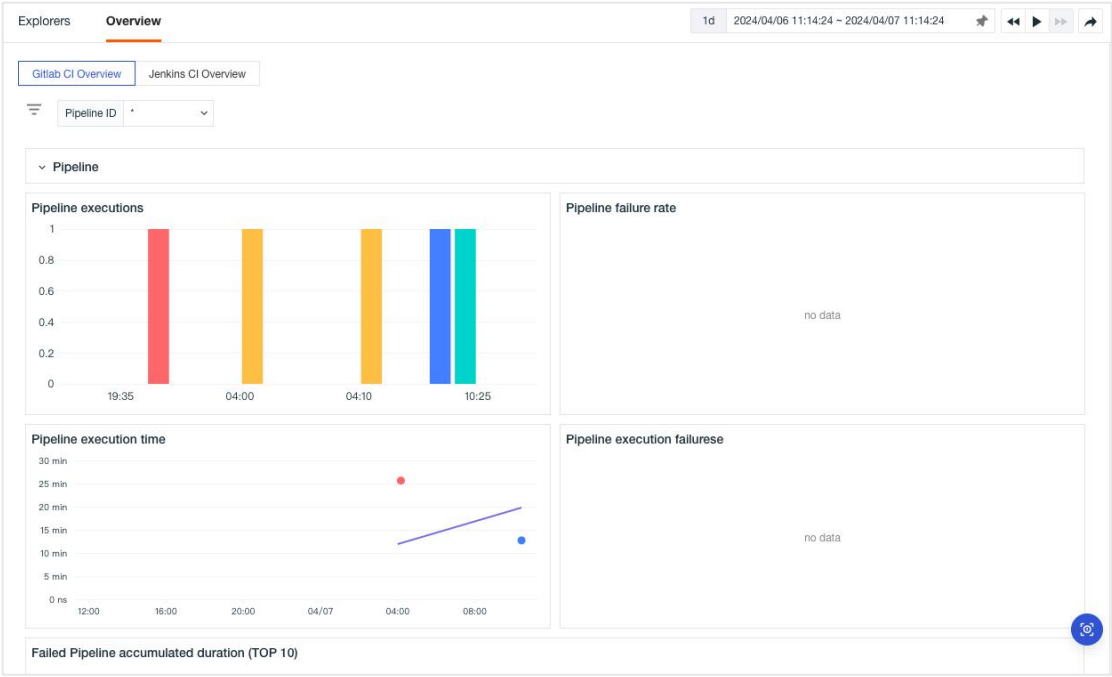
Guance supports configuring aggregation rules based on security check data to generate new metric data, so as to facilitate deeper data analysis.。


## CI Visibility

Guance supports visualization of CI processes and results built into Gitlab/Jenkins. You can directly view CI results in Gitlab/Jenkins through the CI Visibility feature of Guance. The process of CI is continuous integration. If developers encounter problems when pushing code, they can check the pipeline of all CI and its success rate, failure reasons, and specific failure links in Guance to help you provide code update guarantee.

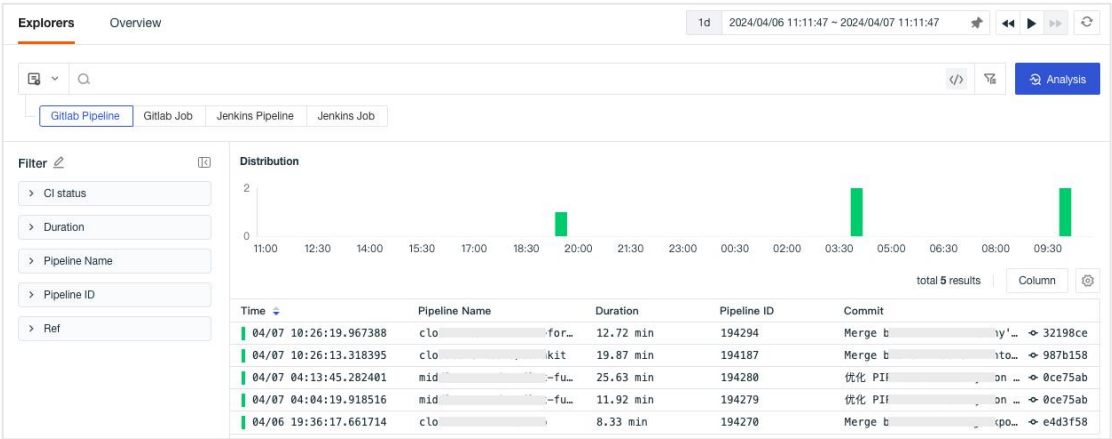
## Overview

In **CI Visibility > Overview**, you can switch to the overview view of Pipeline and Job in Gitlab/Jenkins, including the number of executions, success rate, execution time, and the number of execution failures.



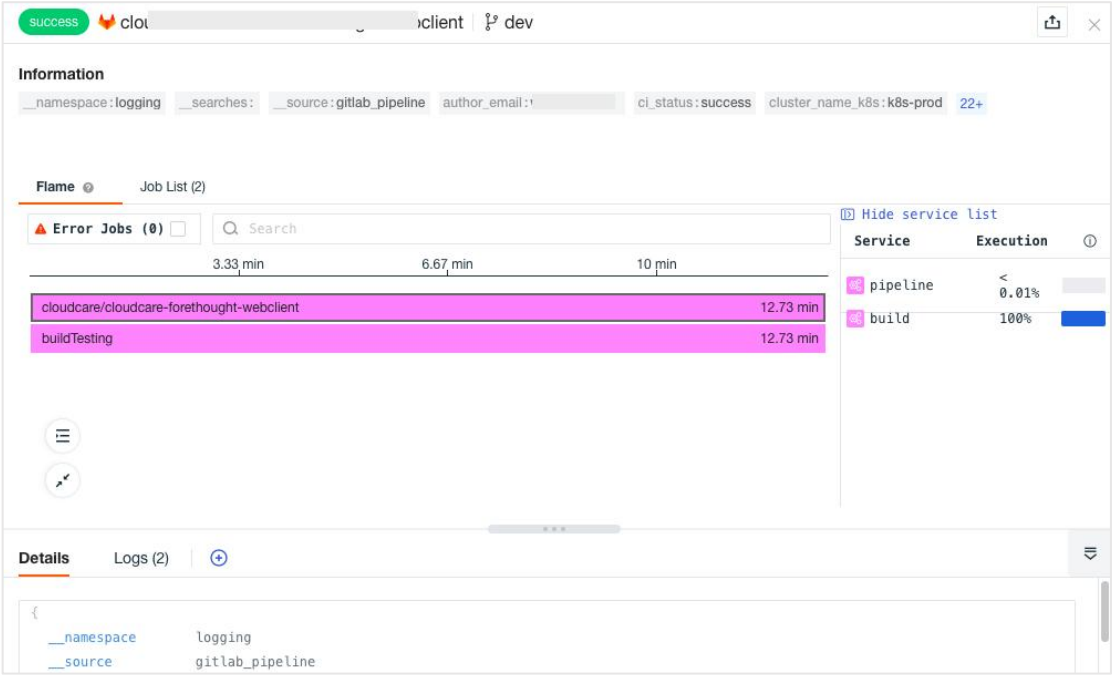

# Explorer

In **CI Visibility > Explorer**, It supports for switching the entire process of viewing and analyzing Gitlab/Jenkins Pipeline and Job, support for search, multi-label filtering, shortcut filtering, data export, and adding display columns. It also supports stacking histogram to count CI process according to selected time range, saving current display content, time range, and filtering conditions to snapshot and viewing historical snapshot.



## CI Details

Click on the CI Visibility process you want to view, and in the underlined details page, you can view the CI process and results through the flame diagram and Job list, including the duration of Pipeline, all Jobs, and their duration, etc. At the same time, you can view the associated logs, hosts, etc.

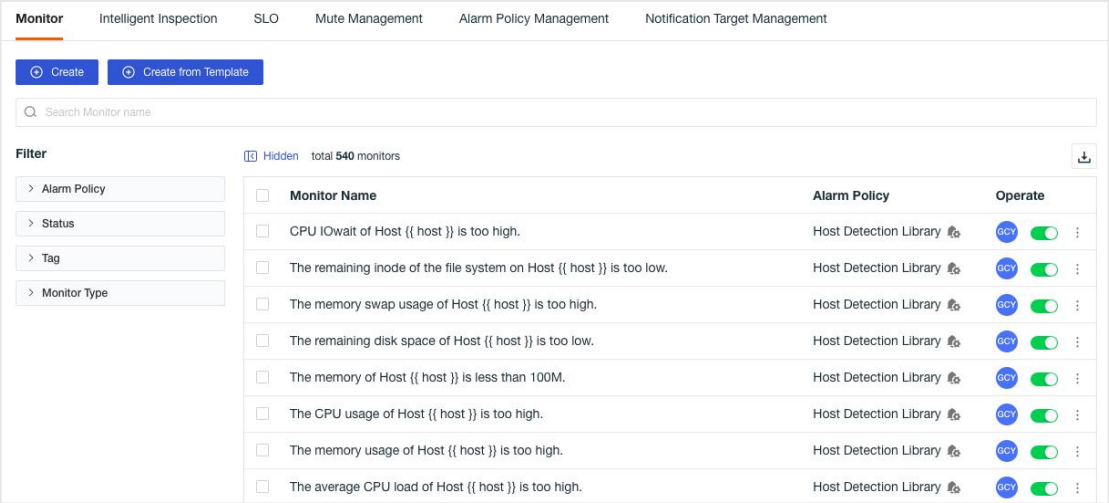



## Monitors

Guance has powerful anomaly monitoring capability, it supports custom monitors and provides more than 20 kinds of monitoring templates, including Docker, Elasticsearch, Host, etc. With alarm notification and related events, it can help users quickly find problems, locate problems, and solve problems. At the same time, Guance provides intelligent inspection function based on intelligent algorithms to help users foresee potential problems of infrastructure and applications in advance. In addition, Guance supports SLO (Service Level Objective) monitoring to accurately control service levels and targets.

# Monitors

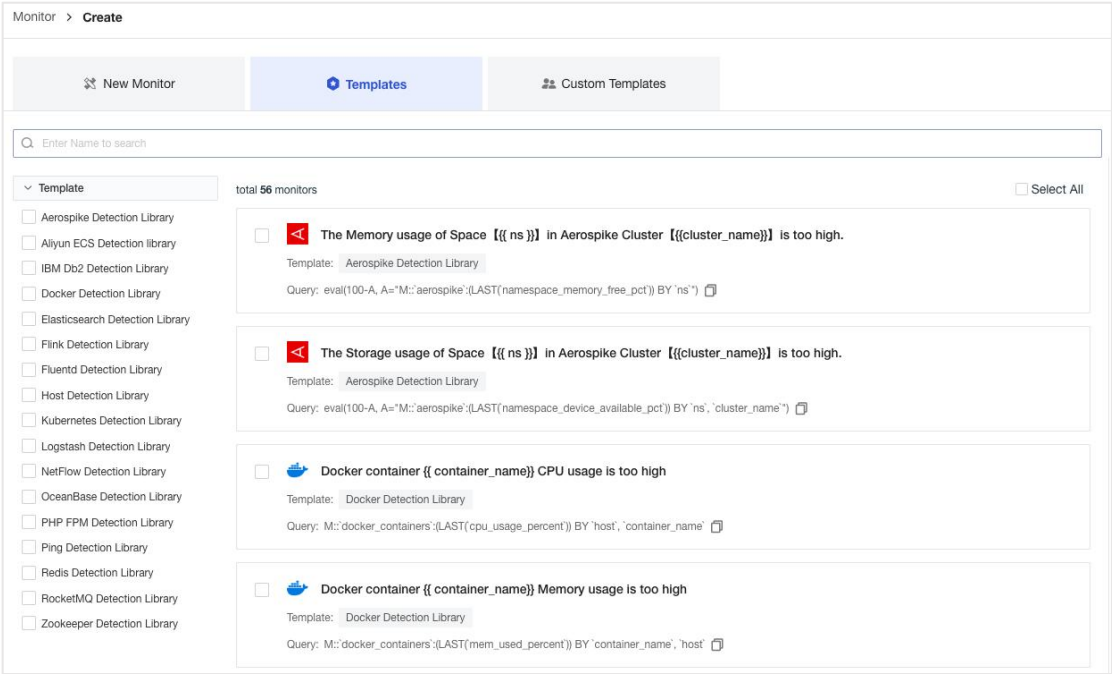
In the Guance **Monitors**, it supports creating a new custom monitor, creating a new monitor from a template, viewing and restoring the historical configuration of the monitor, and managing the monitor, including filtering alarm policies, searching, importing/exporting, enabling/disabling, editing, deleting, manually triggering monitor detection, viewing related events, setting alarm policies, and other operations.




## Monitor Template

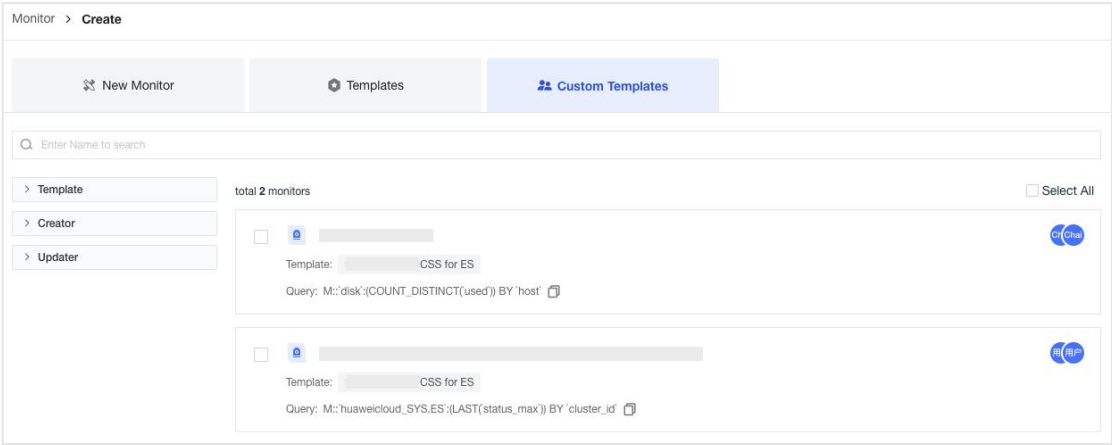
### Template

A variety of monitor templates are built into Guance, which can be used out of the box, including dozens of templates such as host, Docker, Elasticsearch, Redis, Alibaba Cloud and Flink monitoring. After successfully creating a new template, the corresponding monitor will be automatically added to the current workspace.




### Custom Templates

In the Monitor list, you can save the created monitor as a template. Based on this type of template, you can quickly edit monitor configuration conditions and quickly create monitor monitors of the same type.



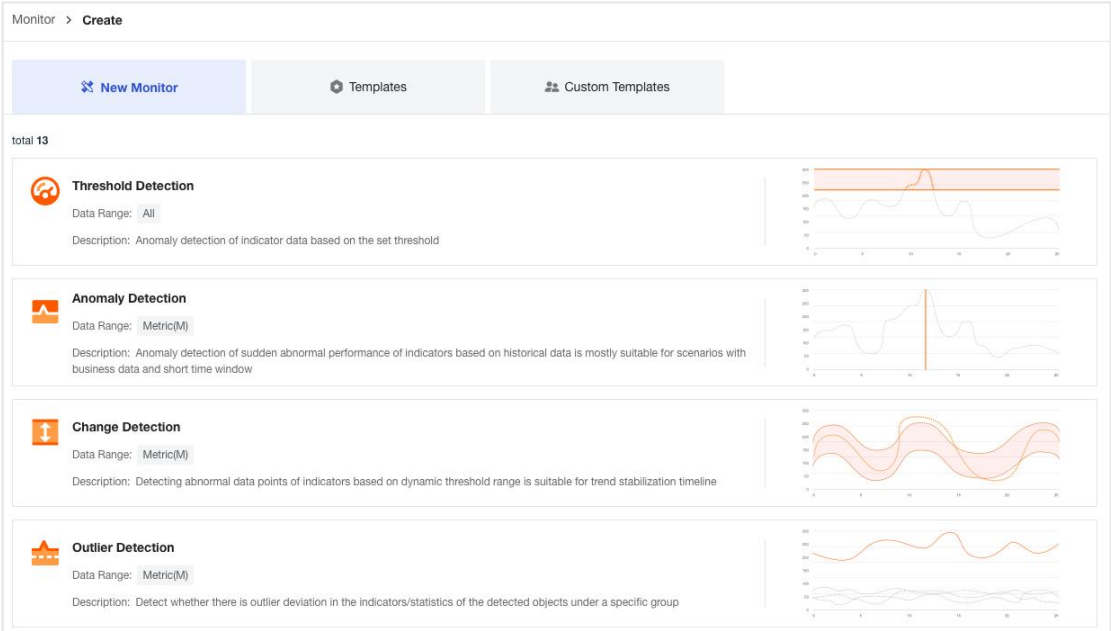

## Custom Monitor

Guance supports a variety of custom monitors, allowing users to customize and configure detection metrics and trigger conditions and receive alarm notifications at

the first time by setting alarms. In **Monitors**, click **Create** to customize and add a new monitor.

| Detection Rules | Descriptions |
| --- | --- |
| Threshold Detection | Threshold detection performs anomaly detection on metric data based on the set threshold. |
| Log Detection | Log detection is used to monitor all log data generated based on log collectors in the workspace. |
| Anomaly Detection | Anomaly detection is to detect the sudden abnormal performance of metrics based on historical data, which is mostly suitable for business data and short time window scenarios. |
| Change Detection | Change detection is to detect the abnormal data points of the metrics based on the dynamic threshold range, which is suitable for the trend stabilization timeline. |
| Outlier Detection | Outlier detection can detect whether there is outlier deviation in the metric/statistical data of the detected object under a specific grouping by the algorithm. |
| SecurityCheck Anomaly Detection | Security check is a series of checks on systems, software and logs through a new type of safety script, which supports discovering facility defects and potential safety hazards and taking effective measures in time. |
| APM Metric Detection | Based on application performance monitoring data, APM metric detection sets threshold rules and detects abnormal situations. |
| RUM Metric Detection | Based on application performance monitoring data, RUM metric detection sets threshold rules and detects abnormal situations. |
| Process Anomaly Detection | Based on infrastructure object data, process anomaly detection is used to detect process data regularly and |

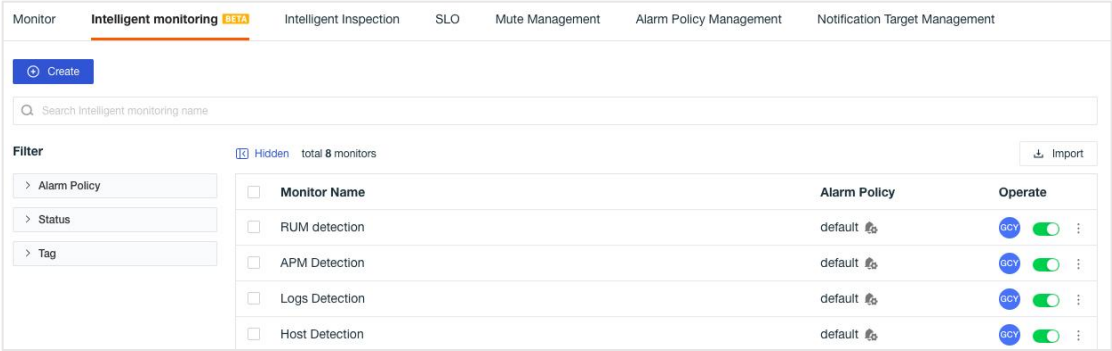
| | |
|---|---|
| | understand process anomaly. |
| Infrastructure Active Detection | Infrastructure survival detection sets survival conditions and monitors the stability of infrastructure. |
| Testing Anomaly Detection | Based on the availability monitoring data, testing anomaly detection sets threshold rules and detects abnormal conditions. |
| Network Anomaly Detection | Network data detection is based on network data, setting threshold rules to detect the stability of network performance. |
| Third-party Event Check | To generate Guance event data, send the exception events or records generated by a third-party system to a specified URL address using the POST request method to an HTTP server. |
| Composite Detection | Combine the results of multiple monitors into a single monitor through an expression, and alert based on the combined results. |



# Intelligent monitoring

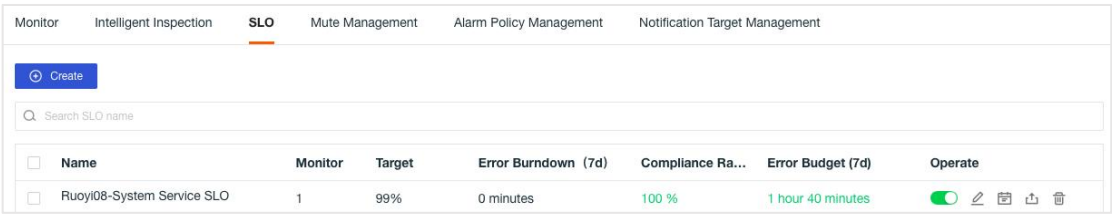
Intelligent monitoring provides a mechanism for quickly identifying abnormal nodes for business analysis, user behavior analysis, and root cause analysis of failures. It is suitable for business metrics and metrics with high volatility. By analyzing the scenarios, it constructs a key dimension for locating multidimensional metrics. After locating the business dimension, it quickly analyzes and identifies exceptions based on the service calls and resource dependencies within microservices.

Monitoring is configured using detection rules such as Host Detection, Logs Detection, APM Detection and RUM Detection. Set the detection scope and notification recipients, and use intelligent detection algorithms to identify abnormal data and predict future trends.



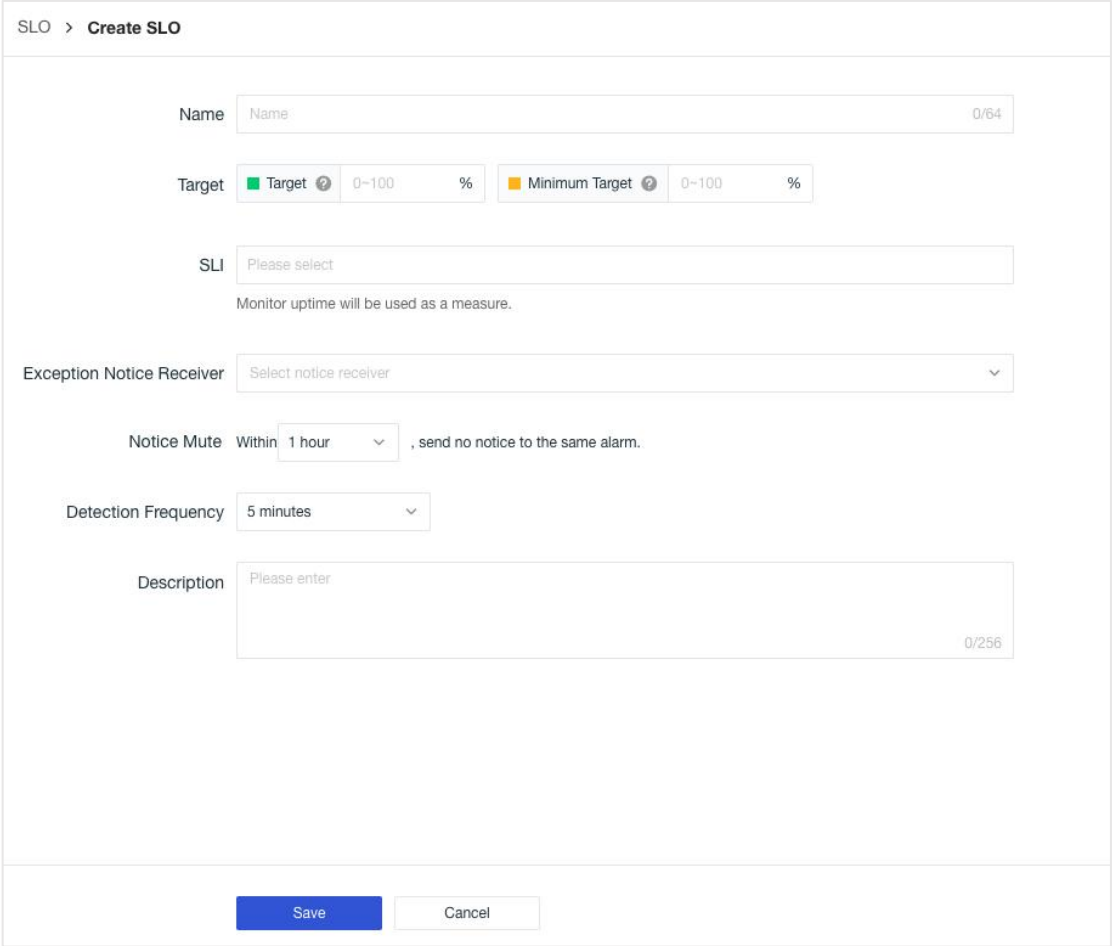

# SLO

Guance SLO monitoring tests whether the availability of system services meets the target needs around various metrics of DevOps. It can help users monitor the service quality provided by service providers and protect service providers from SLA violations. Export dashboards and view associated events.



## SLO Management

In Monitor **SLO > Create SLO**, you can customize the task of creating a new SLO.




Note: Once the SLO configuration is saved, the SLO name, target and detection period cannot be changed.

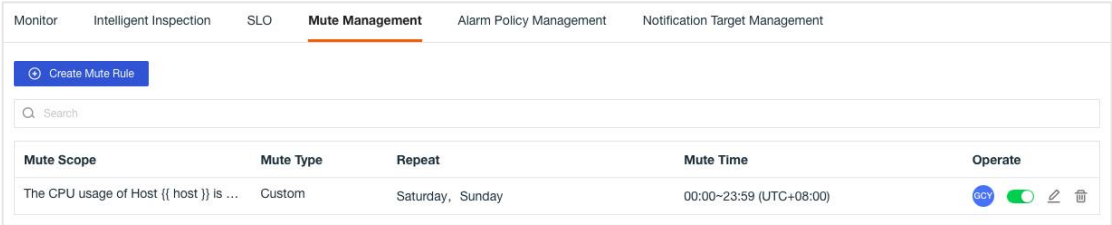
| Field | Description |
|---|---|
| Name | SLO task name. Support up to 64 character input. |
| Goals | Percentage of SLO goals (0-100%), supporting the selection of two goals, including "goal" and "minimum goal":<br>• Goals: An unhealthy SLA is considered when the SLO percentage is < the target percentage and > = the minimum target percentage<br>• The minimum target: When the SLO percentage is less than the minimum target percentage, it is considered as a **substandard**. |

| | |
|---|---|
| SLI | An metric to measure the stability of a system. Support user-defined addition of one or more monitors as metrics. |
| Abnormal Notification Object | Alarm notification object, support workspace members, mail groups, enterprise WeChat robots, DingTalk robots, Lark robots, SMS and other notification methods. |
| Mute Notification | Notification is not sent for the same alarm within the mute time range. If the same event is not very urgent, but the alarm notification frequency is high, the notification frequency can be reduced by setting the notification mute. **Note: Events will continue to be generated after notification** mute **is set, but notifications will not be sent again, and generated events will be stored in event management.** |
| Detection Frequency | SLO detection frequency, that is, to monitor whether abnormal events occur in the monitor of SLO task with a certain time range as a period. At present, it supports two detection frequencies: 5 minutes and 10 minutes. |
| Description | Descriptive information, up to 256 characters. |

# Mute Management

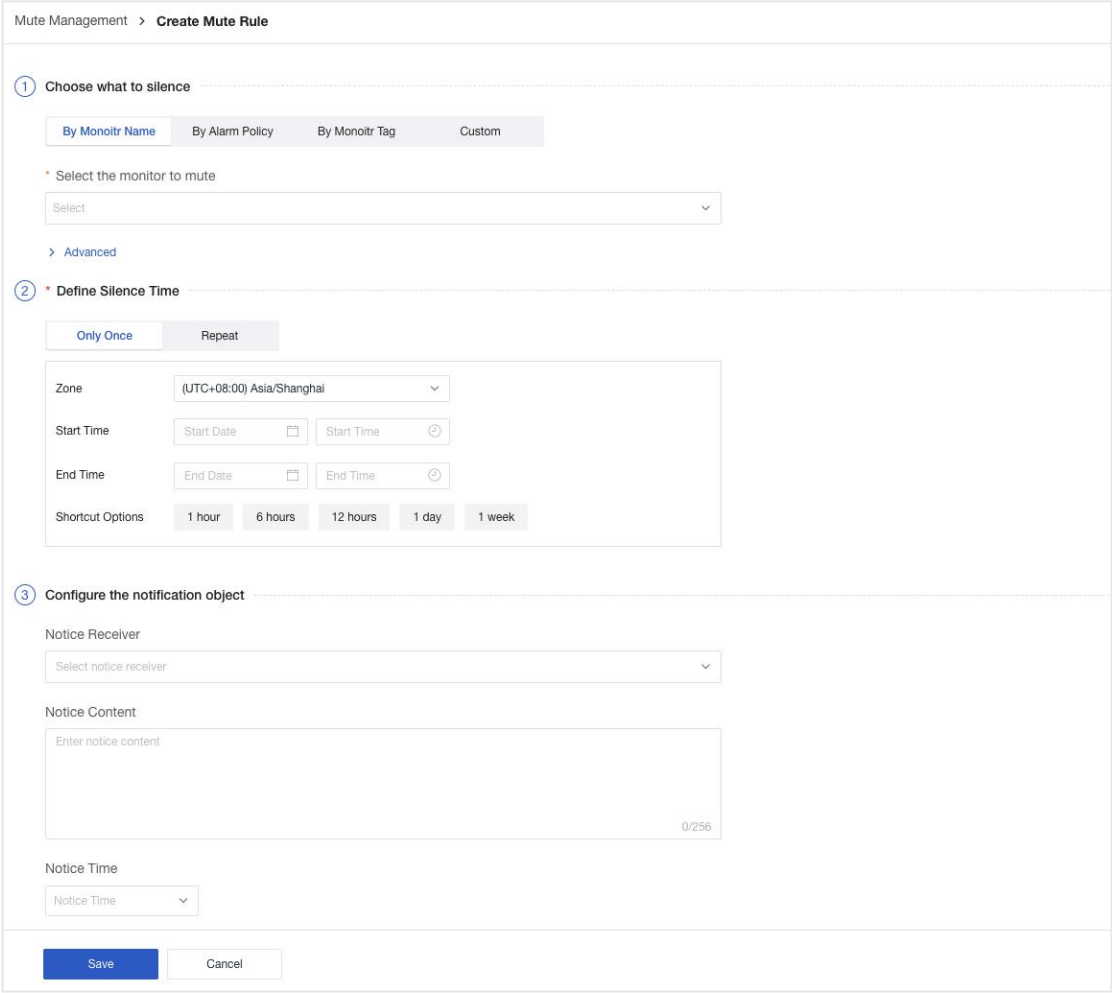
Mute management is used to manage all mute rules in the current space. You can quickly view the type, mute range, label, mute time, and operator of mute rules. You can also search, edit, delete, disable/enable mute rules.

Note: the Mute Rules Management list only displays silent rules that have not expired.




To configure Mute Rules, click Create Mute Rule, and fill in the Mute Range, Label, Mute Time, Mute Notification Object, Notification Content, Notification Time, etc.

Note: muteness will only take effect if the conditions of **Mute Range** and **Label** are met at the same time.

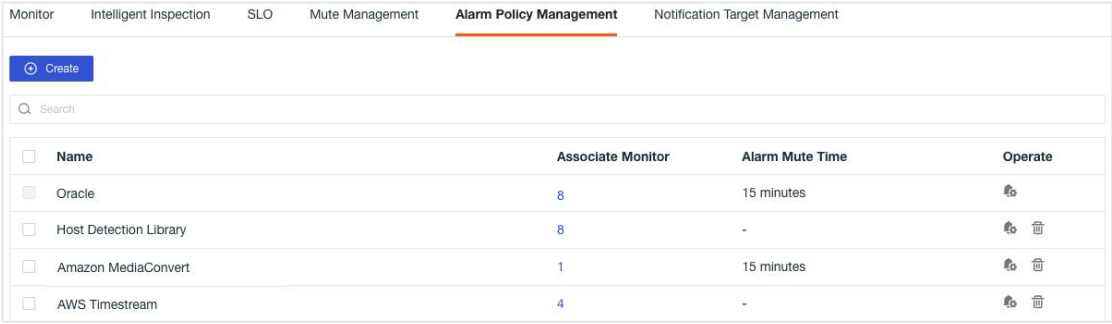



# Alarm Policy Management

Guance supports the alarm policy management of the detection results of the monitor. By sending alarm notification emails or group message notifications, you can know the abnormal data monitored in time, find problems, and solve problems. After configuring the alarm policy, you can perform a quick filter view in the monitor.

Note:

- each monitor must select an alarm policy when it is created, and "Default" is selected by default;
- When an alarm policy is deleted, the monitor under the alarm policy will be automatically classified under "default".

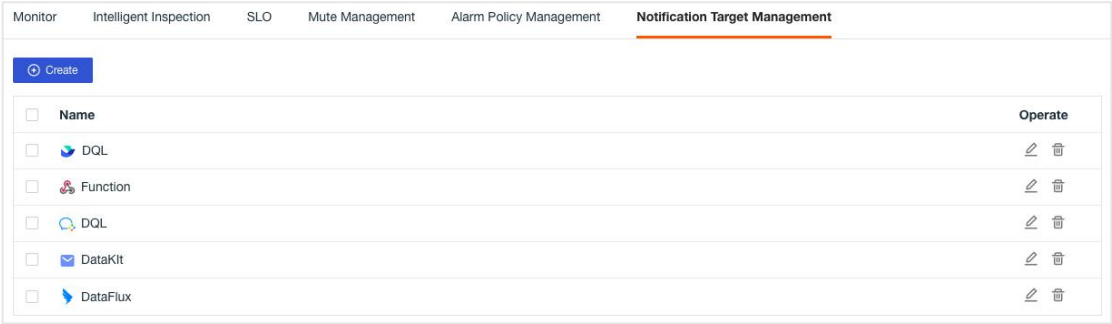



# Notification Object Management

Guance allows for setting alarm notifications for notification targets. The supported notifications are:

- Space Member
- Mail Group
- Dingtalk Robot
- WeCom Robot
- Lark Robot
- Webhook Customization
- SMS
- HTTP Request

Enter the required information on the corresponding page, and click **Confirm**.



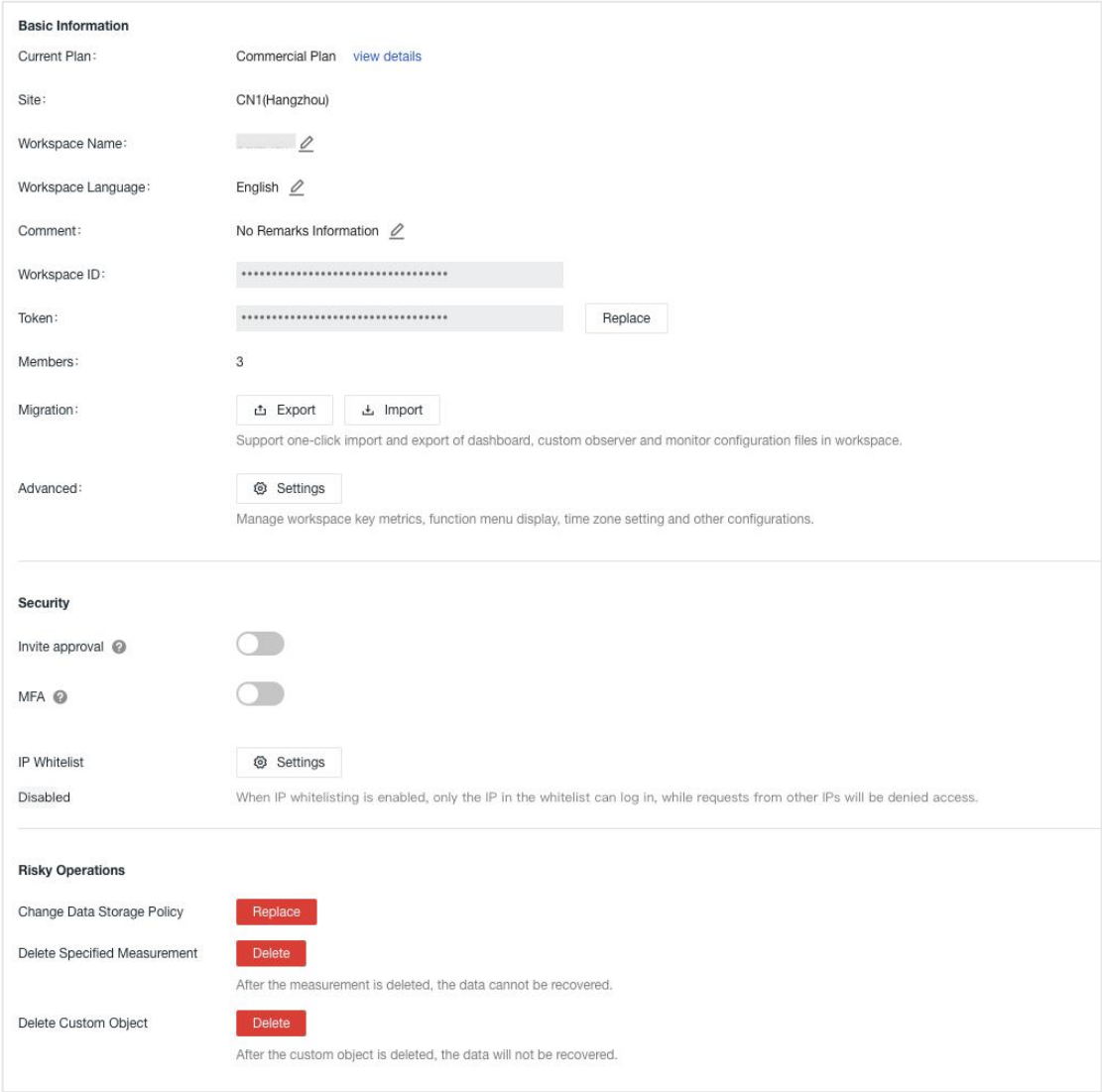

# Workspace Management

Workspace management is the setting, management, and operation of the current workspace. After joining the workspace and being assigned permissions, you can

change the basic information, members and permissions of the workspace through Management.

## Basic Settings

In the workspace **Management> Settings**, you can view the current Guance version, workspace name and ID, Token, number of members, security operation audit, and other information. Support administrators to modify space names, change Token, configure migration (import/export dashboard, custom explorer, monitor configuration files), set key metrics of war room, configure function menus, invite approval、MFA、set IP whitelist, delete measurements, delete custom objects, and other operations. Owners can change data storage policies.



## Attribute Claims

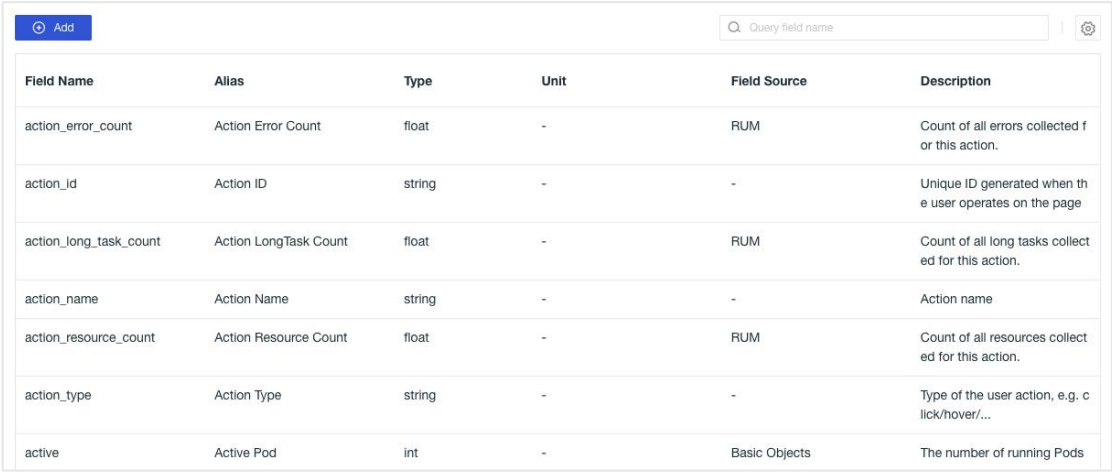
In the Guance workspace **Management > Attribute Claims**, you can see the attribute information in JSON format. Guance will default two fixed attribute fields organization and business.

- organization: automatically generated by the system, that is, organization ID, which is the unique ID generated by the billing center account bound by the current workspace. All commercial workspaces will belong to one organization. If the billing accounts bound by multiple workspaces are the same, the IDs are also the same;
- business: deletion is not supported, with business attributes, you can filter and view in the workspace list.


## Field Management

Guance supports unified management of field data in the current workspace, including system fields and custom fields. You can view field descriptions in scene chart queries, monitor detection metrics, use the simple query mode of DQL queries, and analyze metrics, among other features. This helps you quickly understand the meaning of fields and apply them.

To create a new field, go to **Management > Field Management** in the workspace and click **Create** and enter the field name, field type, and field description in the pop-up dialog box.



Add

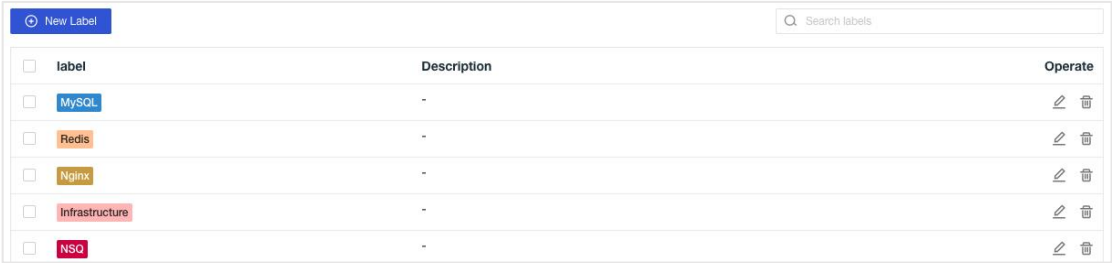
Query field name

| Field Name | Alias | Type | Unit | Field Source | Description |
|---|---|---|---|---|---|
| action_error_count | Action Error Count | float | - | RUM | Count of all errors collected f or this action. |
| action_id | Action ID | string | - | - | Unique ID generated when th e user operates on the page |
| action_long_task_count | Action LongTask Count | float | - | RUM | Count of all long tasks collect ed for this action. |
| action_name | Action Name | string | - | - | Action name |
| action_resource_count | Action Resource Count | float | - | RUM | Count of all resources collect ed for this action. |
| action_type | Action Type | string | - | - | Type of the user action, e.g. c lick/hover/... |
| active | Active Pod | int | - | Basic Objects | The number of running Pods |

# Global Labels

Global tags refer to tags that can be directly accessed within the Guance workspace. With global tags, data that meets certain criteria can be classified, filtered, and linked together to achieve global data linkage.

To create a new tag, go to Workspace Management > Global Tags and click on Create New Tag. In the pop-up dialog box, enter the tag name, description, and select a color to create a new tag.



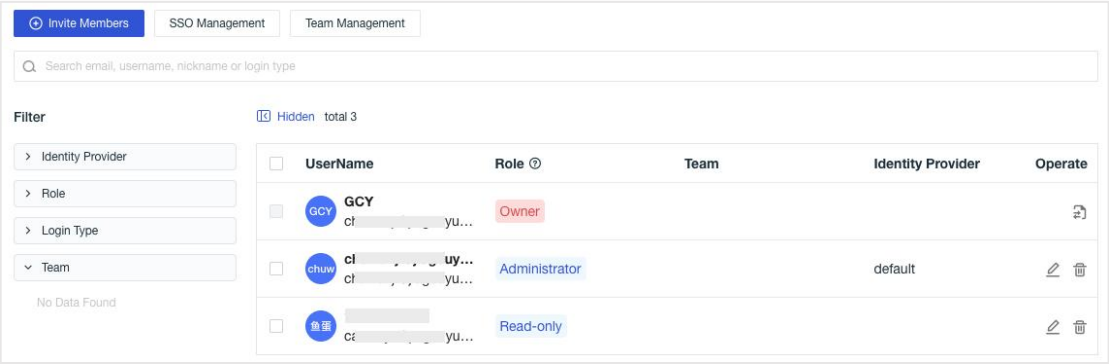
New Label

Search labels

| label | Description | Operate |
|---|---|---|
| MySQL | - | |
| Redis | - | |
| Nginx | - | |
| Infrastructure | - | |
| NSQ | - | |

# Member Management

In **Management > Member Management**, you can display the information of all members of the current workspace. It supports the unified management of all members of the current workspace, including setting role permissions, inviting members, and setting permissions for members, configuring member groups, setting SSO and setting member alias.



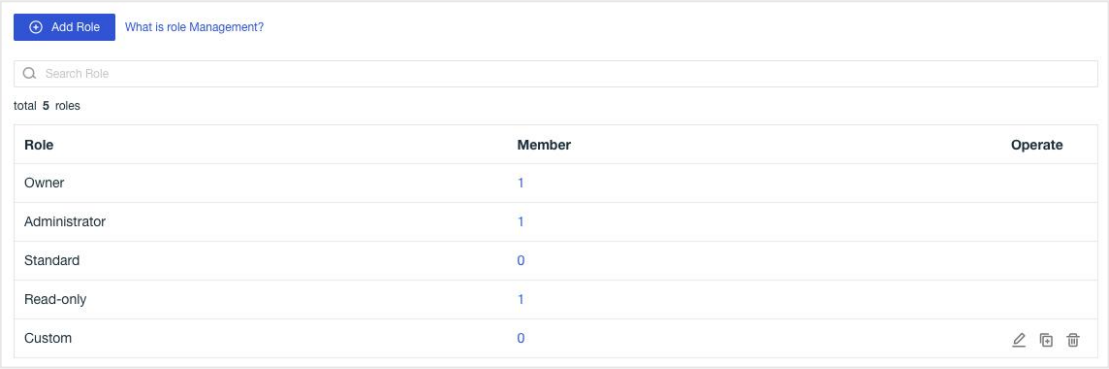

# Role Management

In **Management > Role Management**, four member roles are provided by default: owner, administrator, standard member, and read-only member. You can create new roles for users and give permission scope to roles to meet the permission needs of different users.

- Owner: The owner of the current workspace has all the operation permissions in the workspace, including adjusting the role permissions of other members;
- Administrator: Administrator of the current workspace has read and write permissions of the workspace. The role is able to adjust the permissions of other member roles except Owner.
- Standard: Standard member of the current workspace have read and write permissions to the workspace.
- Read-only: Read-only member of the current workspace can view the data of the workspace, and has no write permission.
- Custom Role: You can customize the permission range of a role according to your requirements.

Note:

- If the current workspace is upgraded to commercial version, upgrading to Administrator requires the owner to pass the verification in the expense center before it can take effect.
- Read-only members do not have permission to view member management lists.
- Distinguishing by tags is supported by four SSO members.



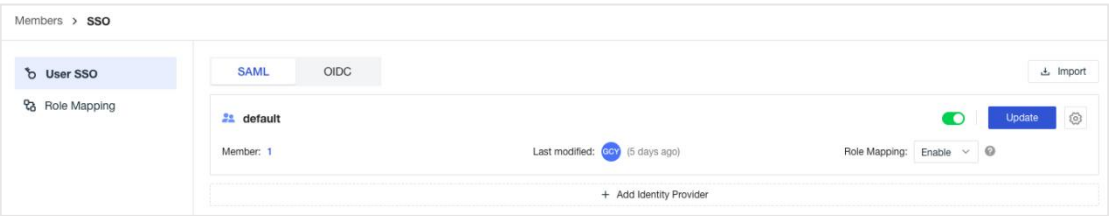

# SSO Management

Guance supports SSO management based on SAML, OIDC/ Oauth2.0 protocol. It supports enterprises to manage employee information in local IdP (Identity Provider). Without user synchronization between Guance and enterprise IdP, enterprise employees can log in and access Guance through designated roles.

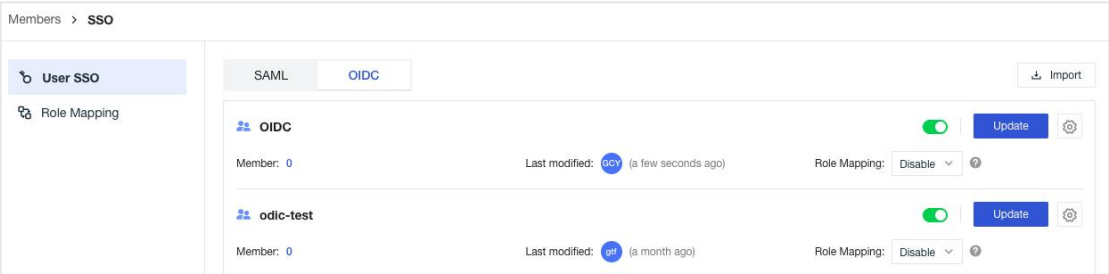
## Enable SSO Login

Go to Guance workspace **Management > Member Management > SSO Management,** select SAML or OIDC, and set SSO for employees.

- SAML

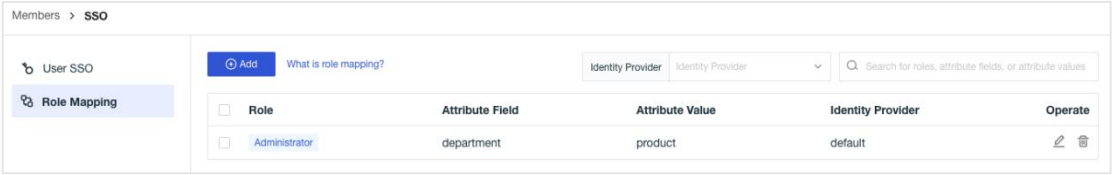



- OIDC



### Enable SAML Mapping

In the Guance workspace **Management > Member management > SSO Management > Role Mapping > Add**, enable role permissions and mapping fields.

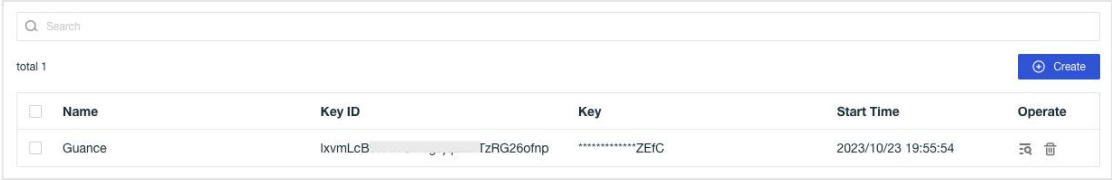



## API Key Management

Guance supports obtaining and updating the data of the Guance workspace by calling the Open API interface. Before calling the API interface, you need to create an API Key as an authentication method.

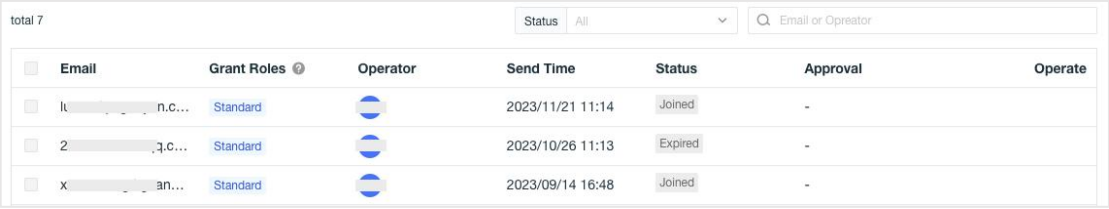
To create an API Key, go to **Management > API Key Management** in the Guance workspace, and click **Create** in the upper right corner. Enter the Key name to create it.

Note: Only administrators and owners can edit the API Key.




## Invited history

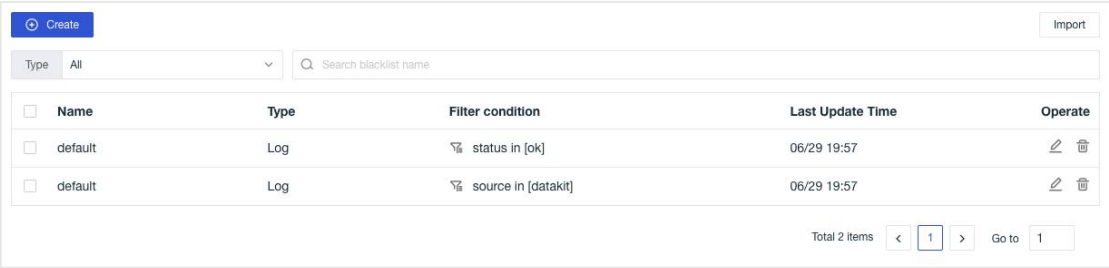
In the Guance workspace **Management > Invited history**, supports viewing all members' invitation actions in the current workspace, including their email, grant roles, operator, send time, status, approval and other information.




# Blacklist

Guance supports filtering out different types of qualified data by setting a blacklist. After configuring the blacklist, qualified data will no longer be reported to the Guance workspace, which helps you save data storage costs.

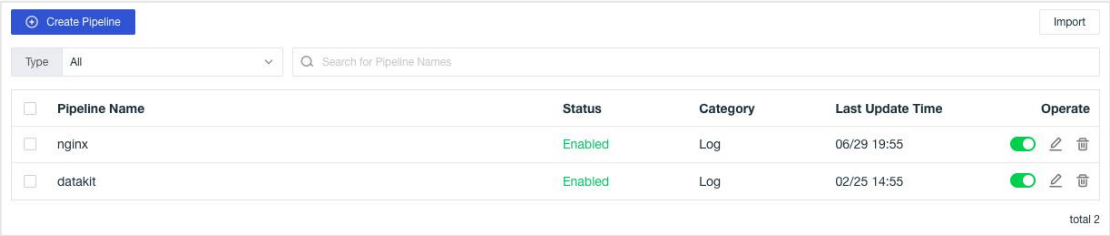
To create a new blacklist, go to **Management > Blacklist** in the Guance workspace, and select the data type to open the data blacklist filtering rules. Data types include log, basic object, custom object, network, application performance monitoring, user access monitoring, security inspection, events, metrics, and profile. You can manually input a preset blacklist or package data source and field name, and then configure the data source and field through DataKit and reporting data.




# Pipelines

Text processing (Pipeline) is used for data parsing. By defining parsing rules, various data types, including logs, metrics, user access monitoring, application performance monitoring, basic objects, custom objects, networks, and security check, can be cut into structured data that meet our requirements.

To automatically generate a Pipeline with the same name according to the field value corresponding to the selected data type, go to **Management > Pipeline** in the Guance workspace and click **Create** .




## Data Forward

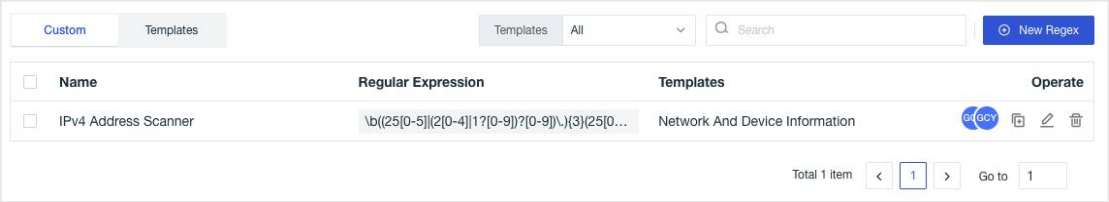
Guance supports forwarding logs, links, and user access data that meets certain criteria to Guance's object storage and external storage, including Alibaba Cloud OSS, AWS S3, Huawei Cloud OBS, Kafka message queues, etc.

In the Guance workspace **Management > Data Forward > Forward rules**, click **Create Rule** to select the data to be forwarded and the storage type.

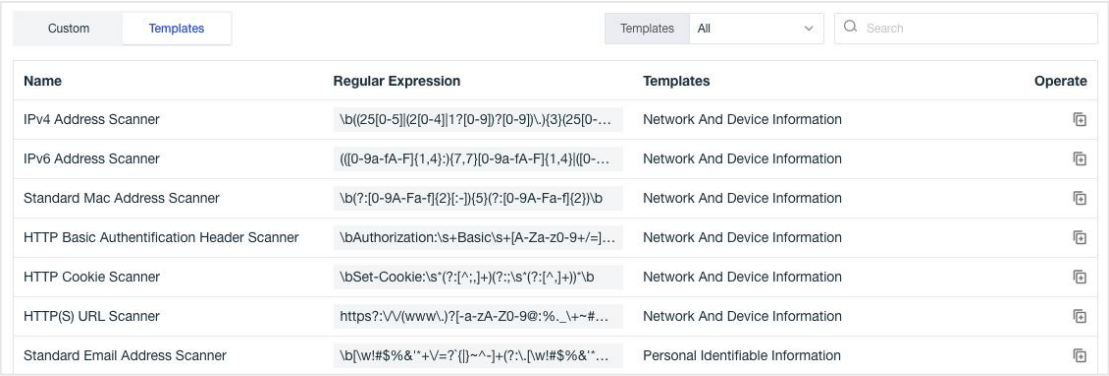

## Regular Expression

Regular expression is one of the effective means to realize data security. In Guance, regular expression are supported to be applied to snapshot sharing, sensitive data desensitization and other scenarios.

In the Guance workspace **Management > Regular Expression > Custom**, click "New Regex" to customize the regular expression and save it as a rule base for subsequent use.




In the **Templates**, Guance provides a variety of regular expression templates, which can be used by direct cloning.




# Audition

In the Guance workspace **Management > Audition**, it supports viewing operation audit events generated by user in the workspace, and recording project usage, user behavior operations and resource changes in the workspace in real time.


# Sharing

In the Guance workspace **Management > Sharing**, it supports unified management of charts and snapshots shared in the current space.

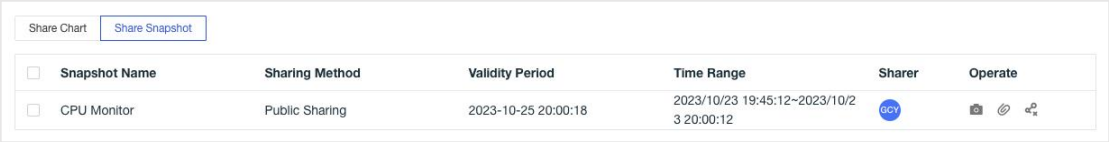
1. Sharing Chart

To share charts, edit the dashboard in **Scene**. After sharing, you can view the chart sharing list in the current space through **Management > Sharing Management - Sharing Chart**. You can view shared charts, embedded codes, and cancel sharing.

Chart sharing can be used to insert charts into platform code outside Guance for visual data presentation and analysis.


2. Sharing Snapshot

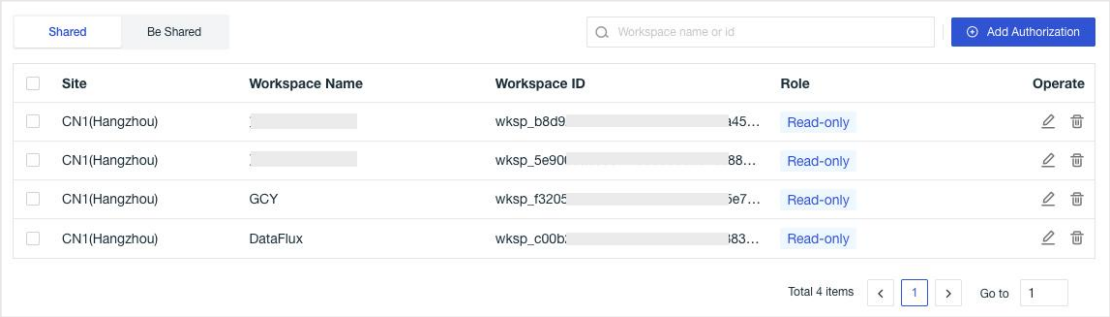
After saving a snapshot in the explorer such as **Scenes** and **Logs**, you can share it in **Snapshot**. After sharing, you can view the snapshot sharing list through **Management > Sharing Management > Sharing Snapshot**. The list includes the snapshot name, sharing method, sharer, expiration date, time range, view snapshot, and view sharing link.




# Data Authorization

Guance supports the way of data authorization, authorizes the data of multiple workspaces to the current workspace, and queries and displays them through the scene dashboard and the chart components of notes. If you have multiple workspaces, configure data authorization to view data for all workspaces in one workspace.

In the workspace **Management > Data Authorization > Shared**, click **Add Authorization**, select site, workspace ID and role to authorize to view the current workspace.



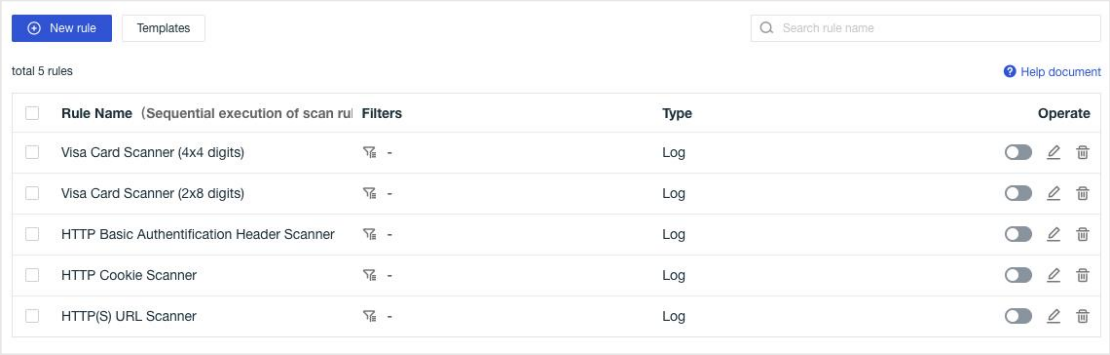

In the workspace **Management > Data Authorization > Be Shared**, click **Add Authorization**, you can view the list of workspaces that has been authorized.


## Data Masking

Guance supports desensitization of sensitive fields. In the workspace **Management > Data Masking** , click **Add Rule** to add desensitization fields.

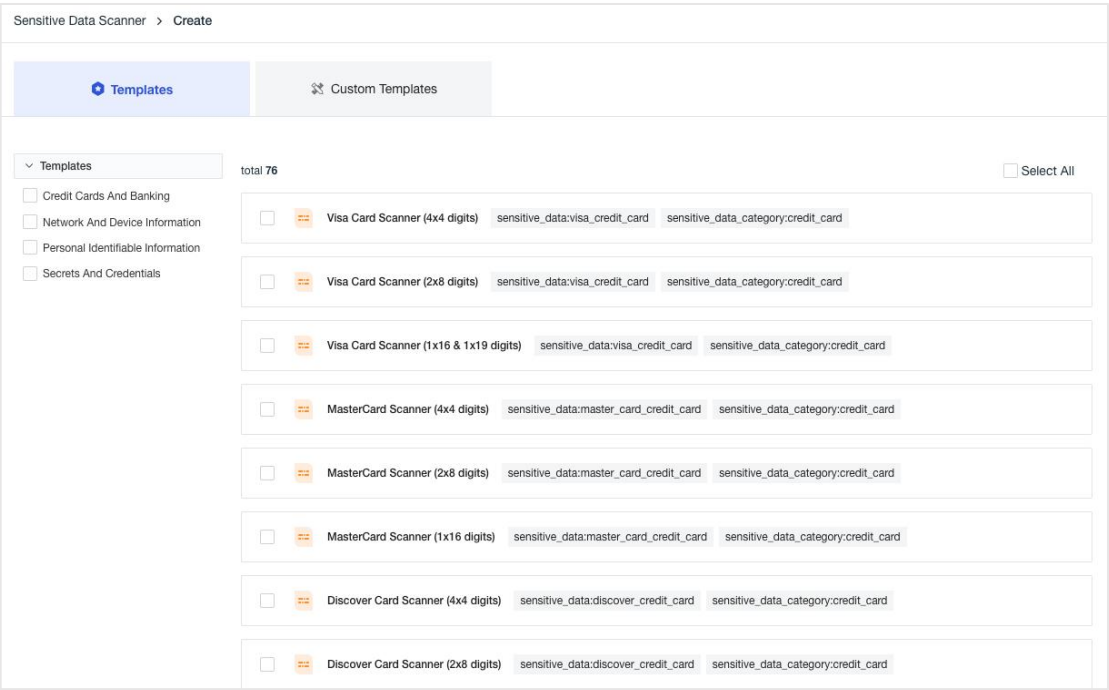

## Data Scanner

Guance supports the functionality of sensitive data scanning, which allows for the creation of desensitization rules for data, enabling custom information masking to prevent information leakage and ensure information security. You can configure this in the workspace under **Management > Data Scanning**.




### Templates

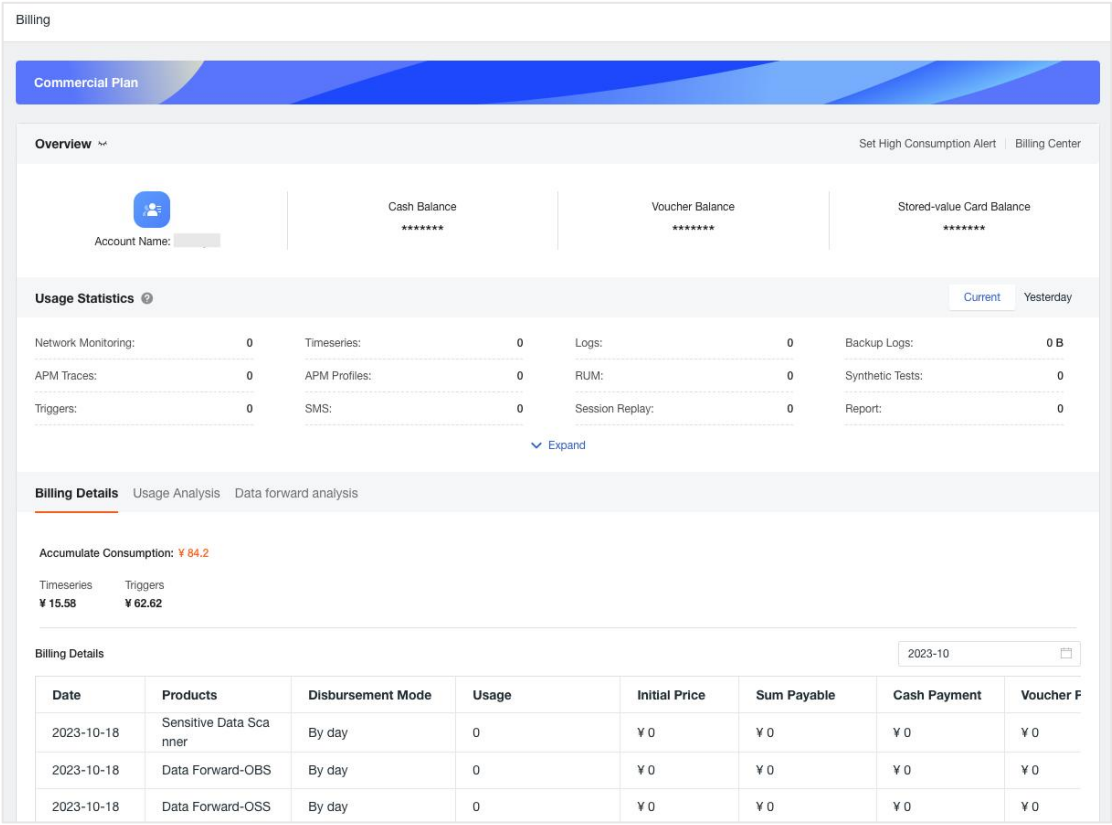
Guance provides a official rule library for scanning sensitive data. In the Guance workspace, go to **Management > Data Scanning > Templates** to view and create rules. This includes scanning for overseas credit cards, network and device information, personal sensitive information, key and credential scanning, and more.




## Billing

On the Billing page, you can view the current usage plan of the workspace and the usage of each item. Guance is divided into the Experience plan, Commercial plan, and Deployment plan. Experience plan users can upgrade to the commercial plan online,

but cannot retreat after upgrading. After upgrading to the commercial plan, you can view the bill list, and the workspace owner can enter the expense center, change the bound account, recharge, and perform other operations.




## Pay as you go

Guance supports the billing method of purchasing on demand and paying according to quantity. Prices are calculated according to multiple dimensions, such as Sensitive Data Scanner, Regular Report, Timeseries, Logs, Data Forward, Network Monitoring, APM Traces / Profiles, RUM, Session replay, Synthetic Tests, Triggers, SMS, etc.

## Billing Price

The charging price of Guance is divided into two charging modes: one is the basic charging mode based on data statistics, and the other is the gradient charging mode based on data statistics and data storage policy.

## Basic Billing Mode

Guance provides the basic charging mode based on data statistics, including Sensitive Data Scanner, Regular Report, Data Forward, Network Monitoring, Session replay, Synthetic Tests, Triggers, SMS.

## Gradient Charging Mode

Guance provides the gradient charging mode based on data statistics and data storage strategy, including timeseries, log data, application performance Trace and application performance Profile, user access PV.