Cloud Automated Testing Practical Tutorial

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Practical Tutorial
Getting User Performance Experience When Accessing Websites

Last updated: 2025-07-24 16:10:42

Practical Background

During business development, there is often excessive focus on designing highly available and reliable architectures while ignoring actual user experience. After the business truly goes live, it will face a series of experience issues. This document introduces how to proactively discover website problems and preemptively perceive faults and user experience.

Practice Objective

Leverage Cloud Automated Testing (CAT) to continuously detect the application. Perform comprehensive analysis on probe data through multiple dimensions analysis, locate the application's problem failures, identify root causes, and fix issues. Conduct continuous iterative updates and optimizations to maximize the enhancement of the application's user experience and reduce user churn rate.

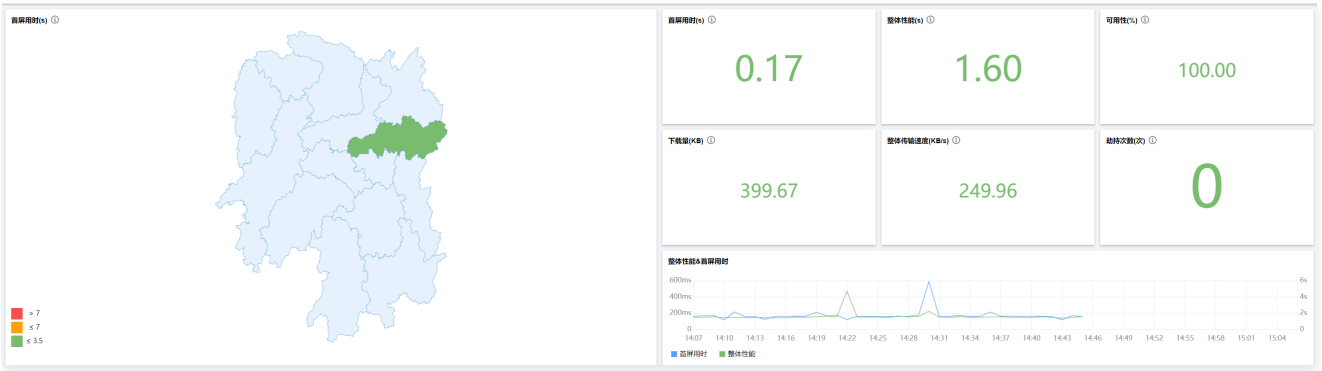
Directions

Step 1: Creating a Dial Test Task

1. Log in to the TCOP console.
2. Click in the left menu bar **CAT > Task List**.
3. Click **Create Task** in the top-left corner to create a dial test task. Instructions are as follows:
   i. Select the **Page Performance** task type and **PC (PC)** test point.
   ii. Fill in the probe address and task name.
   iii. Select a dial test frequency of **5 minutes**.
   iv. Select **Advanced Scenario Test Point** and choose the test point method, region, type, and test point as needed.
   v. The test parameter configuration is optional. By configuring test point parameters, modifications are allowed to achieve more customized test requirements.

Step 2: Multi-Dimensional Analysis to View Dial Test Data

After configuring the dial test task, you can view the dial test data of the configured domain name on the Multidimensional Analysis Page. You can choose the domain name and task type, and perform drill-down analysis on the dial test data by operator, region, and task status.

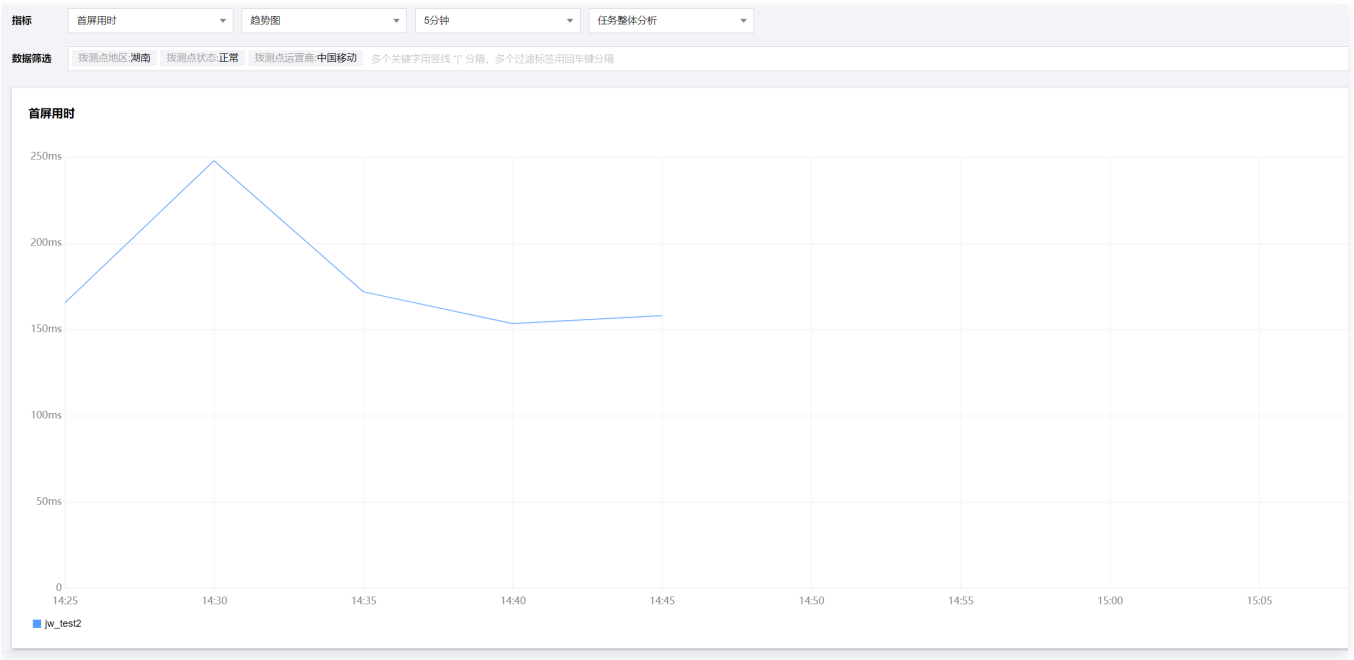


As shown in the figure, you can quickly view the dial test data of regions from the China map or World map. The display area for Changsha city is green, indicating that the website's performance in this region is generally good, with the first screen usually loading within 1s.
The page performance dashboard has preset the page performance metrics that require attention. Usually, website performance focuses on first screen time and availability. These two metrics directly affect the user experience.

Using the step time proportion panel, you can obtain the performance of each step when users access the website and perform targeted optimizations.

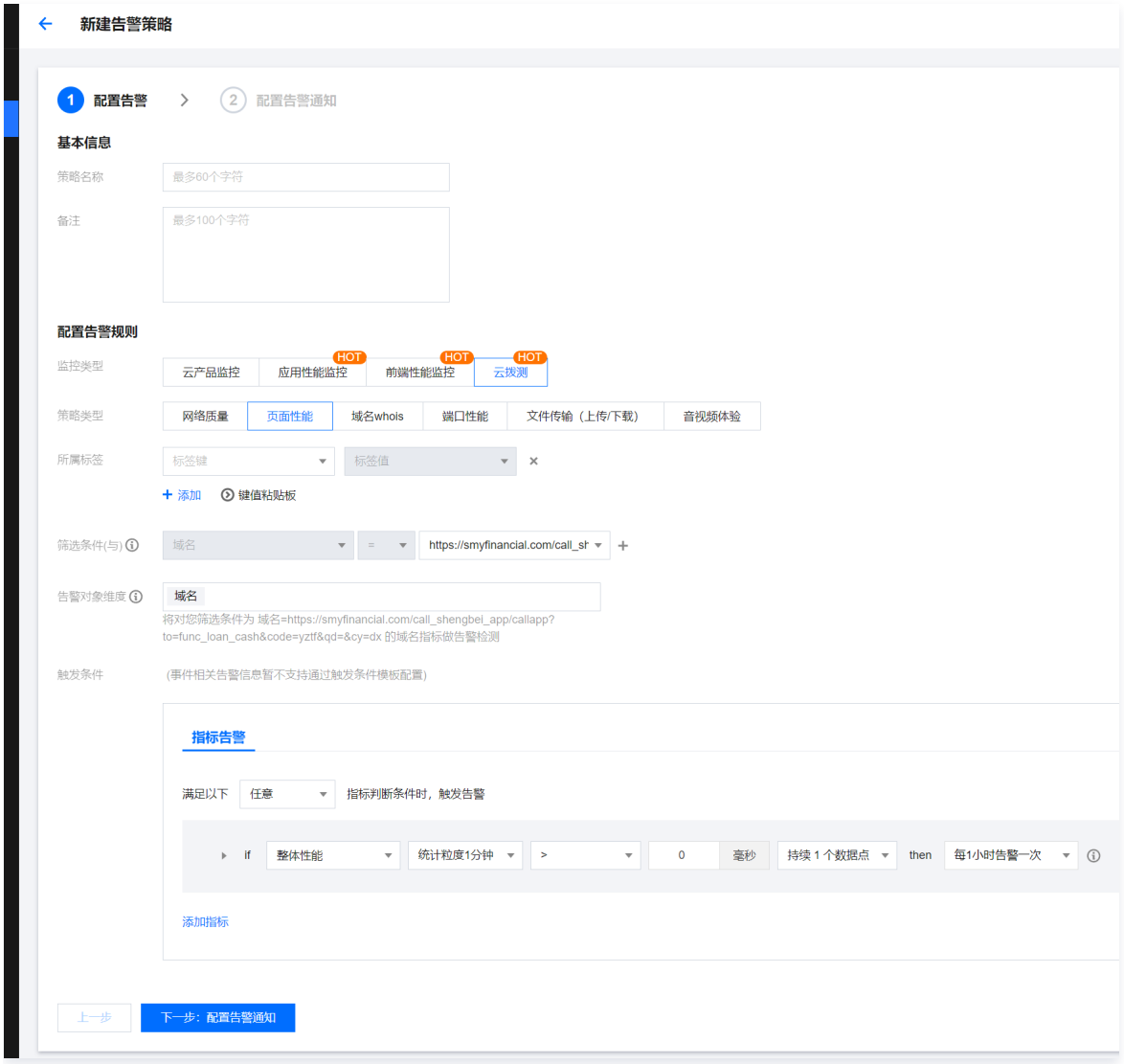
The Top panel makes it very convenient to see errors occurring during the dial test process, as well as the slowest operators, identify issues, and continuously optimize.

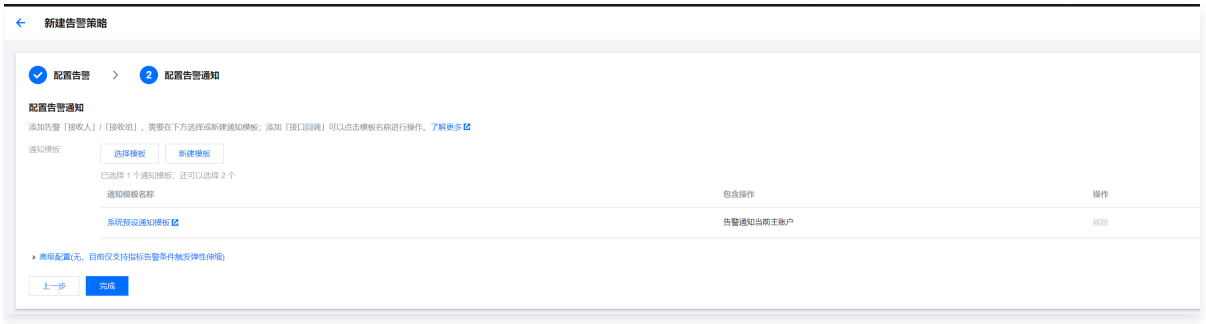
Enter the metric exploration page, which supports multiple charts such as maps, trend charts, and scatter charts. You can conduct comprehensive analysis of dial test data.



Step 3: Configuring Alarms

Enter Alarm Configuration > Policy Management, click **Create Policy**, and configure the corresponding alarm information. Configure dial-up performance metric alarms through the alarm configuration interface. It supports setting alarms from the dimensions of domain name, carrier, region, and city. Multiple metrics can be set for alarms, with corresponding thresholds configured. When an alarm is triggered, the alarm information will be immediately pushed to the set recipient.





CDN Service Quality Monitoring

Last updated: 2025-07-24 16:10:54

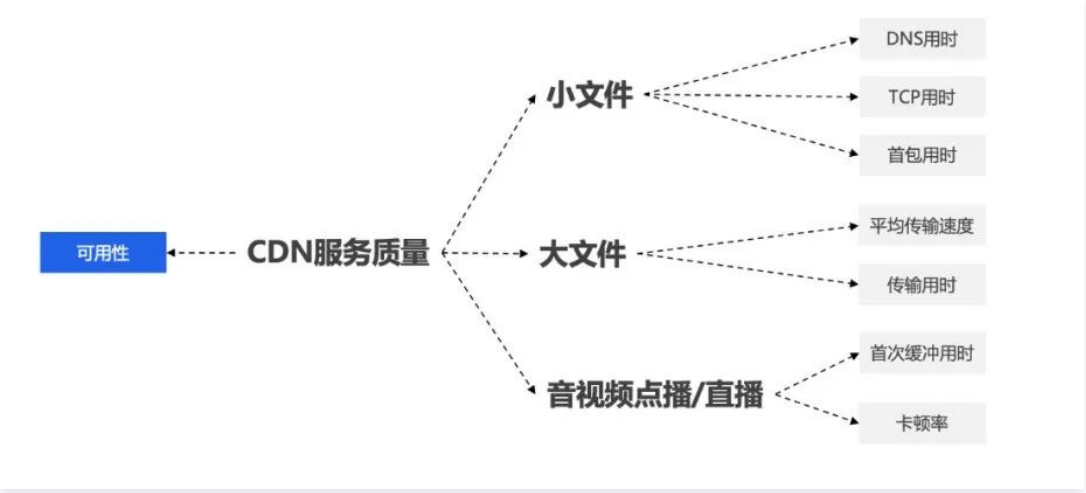
Using CDN Encountered Issues

Using CDN to accelerate a website mainly faces two issues:

- **CDN Selection:**
  The first step in using a CDN to accelerate a website is to select a CDN provider. There are numerous vendors offering CDN services both domestically and internationally. When choosing a CDN service provider, service quality should be the top priority, followed by other factors. After all, the primary purpose of purchasing a CDN service is to accelerate a website, so selecting a suitable CDN provider is very important.
- **CDN Quality Monitoring:**
  After using a CDN to accelerate a website, the CDN becomes a black box for us. We cannot solely rely on the monitoring data provided by the CDN vendor to measure the service quality of the CDN. Therefore, how to measure the quality of the CDN becomes a bottleneck. If the CDN is unavailable or the duration is relatively large, it would not be worth the cost.

CDN Service Quality Measurement Standards

To solve these issues encountered during CDN usage, it is first necessary to determine how to measure the service quality of a CDN. It requires formulating some core metrics to quantify the data of the CDN acceleration process. Through these data, the quality of CDN acceleration can be measured.



The scenarios for using CDN acceleration can be divided into four categories: small files, large files, audio and video on demand, and audio and video live streaming. Among these four scenarios, the first factor to consider is certainly availability. Whether the CDN can normally provide acceleration service is the premise of everything. The premise for measuring CDN service availability is to ensure origin server availability. Based on the method proposed in this document, the service of the origin server can also be monitored.

> **Description**
> Small files are generally web page materials, usually html, js, jpg, png, css, and other such files. These small files are most sensitive to delay.

Network Request

A frontend request for a network resource involves analyzing four processes: DNS query, TCP connection, request response, and content transfer. For small files, the time consumption of the first three processes is generally focused on, while the time

consumption of content transfer is minimal and has little reference significance.

The metrics for the first three processes are:

- **DNS time**
  DNS time is a metric for measuring domain name resolution time. The length of DNS time is also related to the scheduling policy of the CDN.
- **TCP time**
  TCP time refers to the time taken to establish a TCP connection with the resolved IP. The process of establishing a TCP connection follows a fixed three-way handshake. TCP time can reflect the capacity of a CDN's node resources and scheduling policy. Generally, the closer the node is to the user, the shorter the TCP time.
- **Time to first packet**
  Time to first packet is a key metric for measuring CDN performance in small file scenarios. It represents the time from when a user initiates a request to when the CDN responds with the first packet content. This process provides the maximum extent of measuring the CDN's processing capability.
- **Large file**
  Large file types mainly include some download installation packages, typically apk, rar, zip, etc., which are files greater than or equal to 10M. In the scenario of large files, it is relatively simpler compared to small files. Generally, the quality requirements for CDN are not as demanding, and the core metrics are download speed or download time.

Network requests mainly focus on two core metrics:

- **Average transmission speed:** Average transmission speed is used to measure the average speed of large file transmission.
- **Transfer duration:** Transfer duration is used to measure the time required for downloading large files.

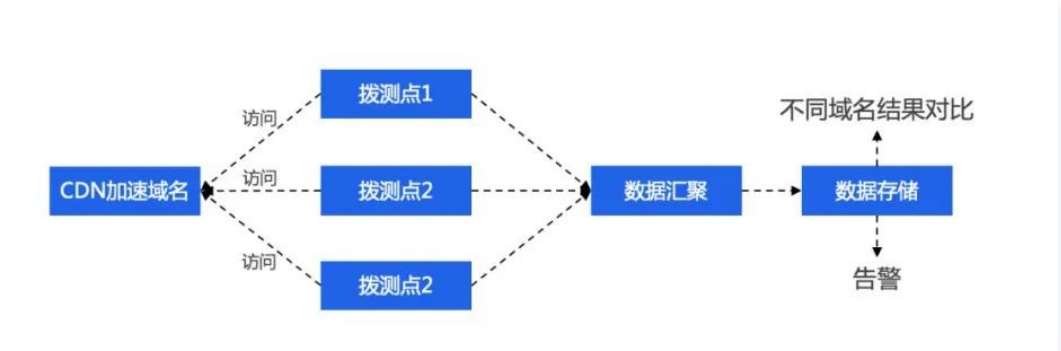
Audio and Video on Demand/Live Stream

Audio and video on demand typically involves audio/video files such as mp4, flv, mkv, wmv, etc., while live streams usually use protocols like rtmp, hls, httpflv. Audio and video scenarios are quite similar to large file scenarios, but in this case, the quality requirements for CDN services are much stricter.

- **First cache time:** First cache time is the time from when a user opens the page until they see the video image. It is subject to the impact of domain name resolution, TCP connection, and first packet loading.
- **Stutter rate:** Stutter rate is an important metric for measuring user playback experience. If 90 out of 100 users experience no stuttering during playback, the stutter rate is 10%.

CDN Monitoring Cases

After defining the metrics for CDN, the next step is to monitor CDN acceleration. A platform needs to be built to monitor the service quality of CDN and enable continuous follow-up and assurance of CDN quality through methods such as comparative analysis and alarms.



For CDN acceleration domains, numerous probe points need to be deployed to access the acceleration domains. Core metric data during the access process is collected, then aggregated and stored. The results are then subjected to comparative analysis and alarms.

Key Point 1: Probe Point Setup

Obtain the core metric data of CDN by accessing the CDN accelerated domain name. After writing the programs to collect these core metrics, these programs need to be deployed to the probe points in each district.

Key Point 2: Data Aggregation

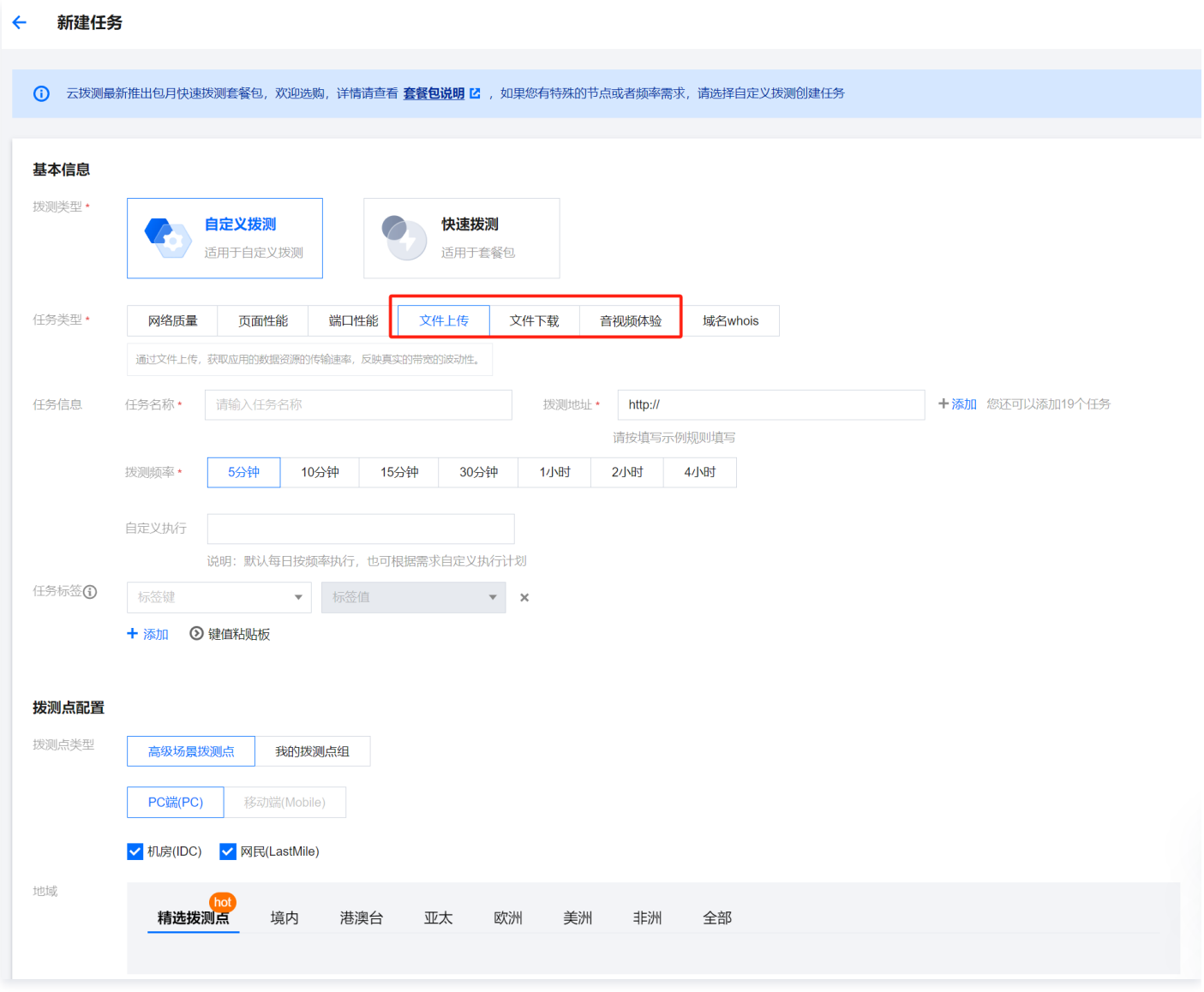
For the core metric data collected at each probe point, data aggregation and calculation need to be performed. For example, the DNS time at a certain moment should be the average or 95th percentile of the DNS times at each probe point at the current moment.

Key Point 3: Alarm Capabilities

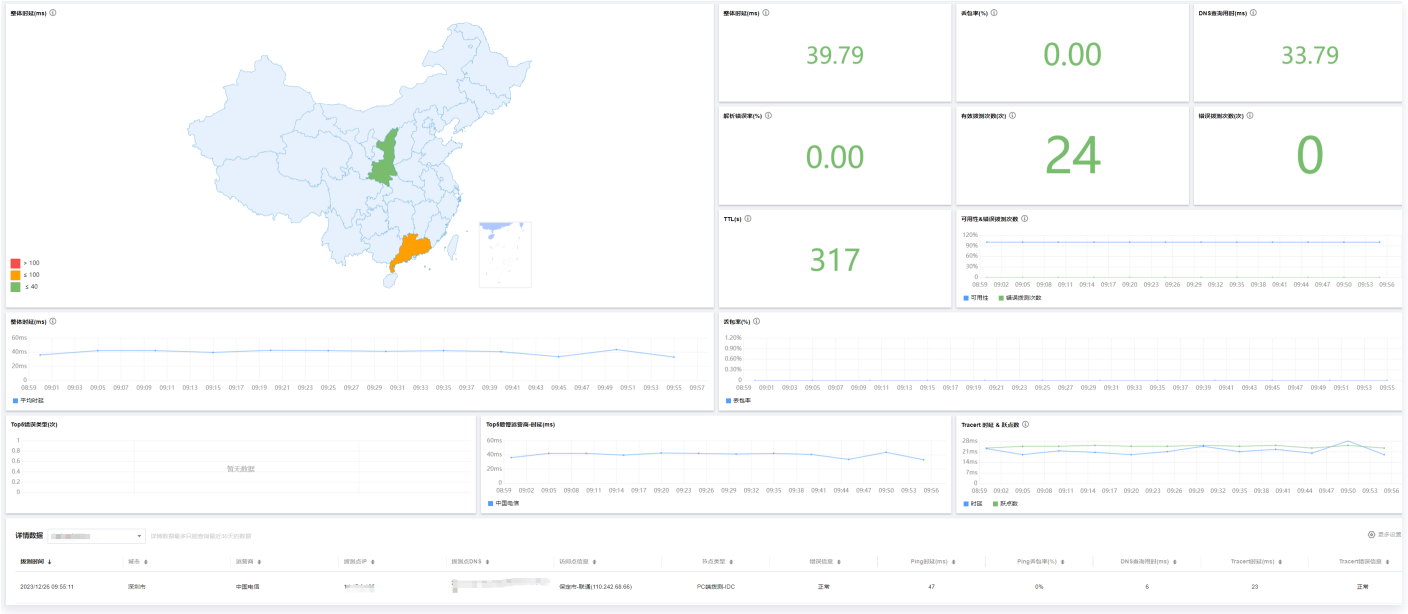
Continuously detect the core metric data. The most critical metric is availability. When availability declines, issue an alarm in a timely manner.

Operation Steps

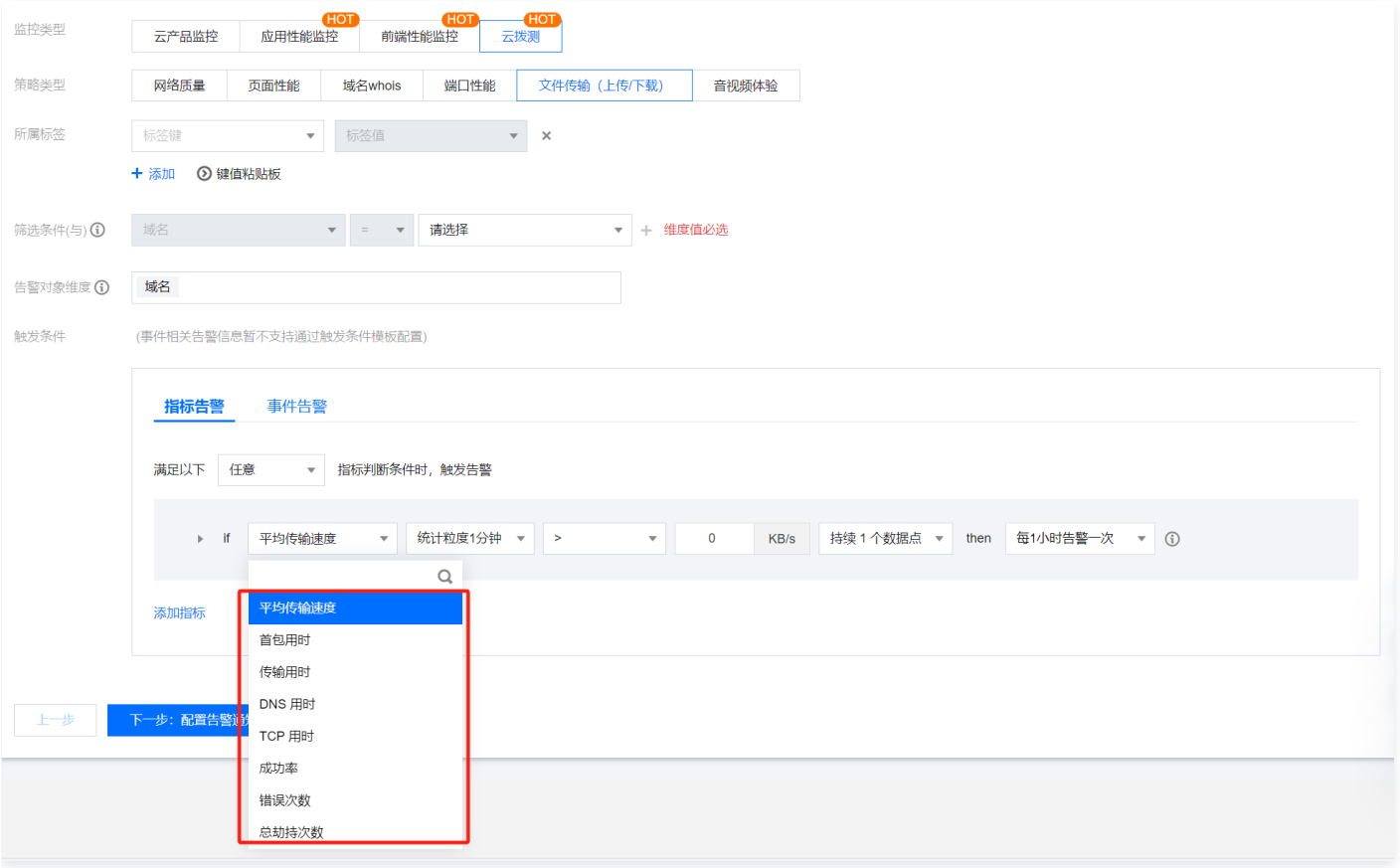
1. Log in to the cloud probing console.
2. Click **Task List** in the left sidebar, then click **Create Task** in the task list.
3. Create fileUpload, file download, and audio and video experience task separately.
4. After the instance is created, the corresponding dial test task will be issued to each dial test point for testing.



Dial testing data display:
CAT aggregates the result data of dial test points. You can view the metric data through the Multi-dimensional Analysis Page.



You can also enter the alarm policy page to configure alarms for key metrics, set thresholds for corresponding metrics, and promptly trigger alarms when the access quality of the CDN is abnormal.



How to Perform Network Quality Monitoring

Last updated：2025-07-24 16:11:07

Pain Points in Network Quality Monitoring

Network quality serves as the first checkpoint for service availability, having a profound impact on user experience. However, the methods for monitoring network quality are not complex. With just a PC and simple command line instructions such as Ping, Dig, and Telnet, network issues can be quickly detected. So why can most businesses still not achieve effective network monitoring? The core obstacles mainly include the following points:

- **Wide user distribution and diverse network environments – difficult to cover**
  The first challenge of network monitoring is coverage. For most services targeting end users, the network environment where users connect is the complexity of city × ISP. Domestically, the majority of user traffic is concentrated in over 200 cities, with mainstream and secondary network operators totaling more than 200. Not to mention overseas, where different countries each have 4-5 mainstream operators. User access methods are divided into PC and mobile terminals, and the network environment may be mobile networks or WI-FI. Enterprises hope to establish comprehensive network quality monitoring relying on their own capabilities. Even for top-tier internet giants, this presents an extremely high barrier.
- **Lack of authoritative data – difficulty in liability determination**
  Some companies, due to the wide distribution of their Ops teams and resource regions, can leverage internal resources to build a high-coverage network quality detection network. They conduct regular testing on services and domain names, enabling timely detection of network quality issues. However, when it comes to issue feedback and liability determination from various resource providers (CDN, DNS, gateway providers, network operators) within the network, they often face challenges due to detection methods and data processing approaches, leading to doubts about data credibility.
- **Passive post-event investigation – difficult to reproduce**
  Most Ops teams detect network faults through feedback from frontline operations (e.g., user complaints, operational observations of a sharp drop in traffic in a specific region). On one hand, this post-event feedback mechanism often fails to compensate for already incurred business losses; at the same time, due to the complex and diverse nature of the network environment and routing uncertainty, even if the corresponding region's machine is found for quick verification, it cannot be guaranteed that the issue can be reproduced to avoid similar problems and continuously mitigate business impact.

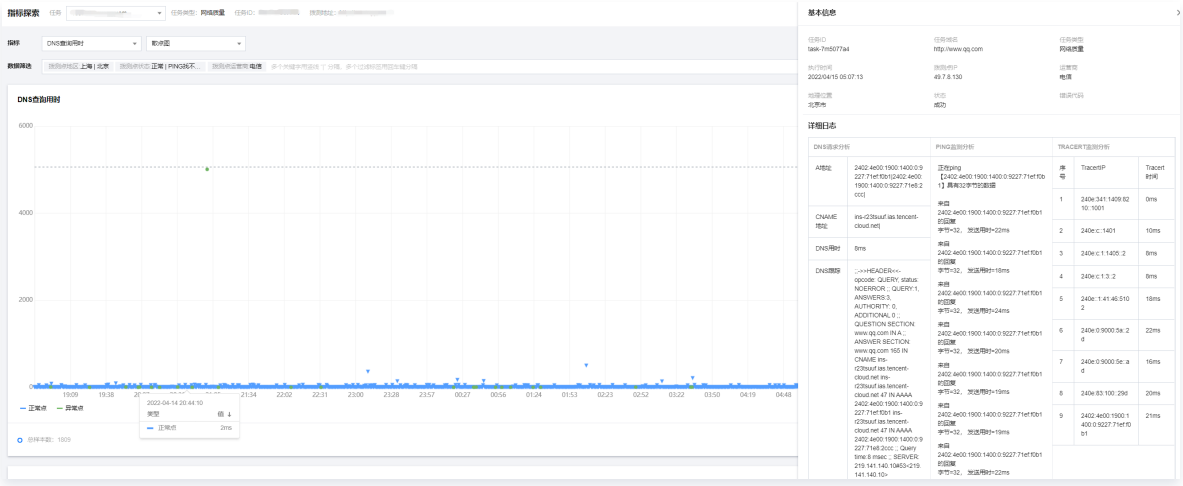
How to Help You Perform Network Quality Monitoring?

Use cloud CAT in the network quality monitoring scenario to perform Ping, DNS, and Tracert tests on specified servers (IP or domain). Retrieve link node network data and metrics such as latency and packet loss during the monitoring process. Real-time understand network link fluctuations. Effectively reduce issues like invalid website access, lag, slow response, and time-consuming operations, thereby enhancing user experience.

- **Extensively distributed monitoring points – comprehensive coverage of multiple network environments**
  Tencent Cloud CAT leverages rich network resources to cover 99% of user access methods and network environments, achieving truly full-coverage monitoring.

- **Multi-dimensional aggregation and comparison of regions and operators – Quickly locate impact range**
  All regions, clear at a glance for ISP network quality comparison. Quickly detect regional and ISP network issues, promptly fix them, and maximize minimizing business impact.

- **Detailed log information – fully retain failure site**
  For each probe, Tencent Cloud CAT provides you with basic information of the monitoring point, and fully retains Dig, Ping logs, and hop information. No need to reproduce, directly retain the failure site.



- **Automatic packet capture – Full-coverage transmission status capture**
  If detailed logs are insufficient to support fault troubleshooting, packet capture analysis is the ultimate solution. During Tencent Cloud dial test task configuration, it supports automatic packet capture targeting "error requests" or "all requests" during detection. Subsequently, you can download data packages on the detailed log page for in-depth analysis.