citrix

White Paper

Citrix Intelligent Traffic Management

Customer Content and Logs

September 15, 2020

This document provides information concerning the collection, storage and retention of Logs and other data generated in connection with Citrix Intelligent Traffic Management (ITM) service and the related products (Openmix, Fusion, Radar, Sonar, Impact and Netscope). Any capitalized terms not defined below have the meaning specified in the Citrix End User Services Agreement.

The following terms are used in this article:

- **Customer Content** means any data uploaded to Customer's account for storage or data in Customer's computing environment to which Citrix is provided access in order to perform the Services.
- **Log(s)** means a record of events related to the Services, including records that measure performance, stability, usage, security, and support.
- **Services** means the Citrix Cloud Services outlined above for purposes of ITM

Overview

Citrix Intelligent Traffic Management is designed to provide customers unmatched visibility into the network experience of shared cloud services and private infrastructures as measured by a world-wide community of website and application users. The network experience data is helpful for traffic management, evaluation of service providers and for service monitoring. Citrix ITM allows for the use of network experience data, service availability and application metrics to provide sophisticated traffic management via DNS or API-based decisions.

The Intelligent Traffic Management Community

One of the core principles behind the ITM technology is the Radar Community. The Radar Community is a group of websites and applications who contribute measurements of network performance and user experience to provide visibility into the quality of Internet services (Content Delivery Networks, clouds, etc.) and private infrastructures.

ITM aggregates distributions of performance measures for groups of users as defined by: continent, country, region, state, ISP and the destination service being tested in order to predict the user experience for future users. This prediction is then used to improve the performance and quality of service experienced by the next user that may visit a site or network delivered application.

Types of Data

There are two types of data collected and used in ITM and the related products:

Customer Content

Generated from a customer's use of the Citrix ITM Portal or APIs. This data is collected from customer's administrators interacting with the ITM product to configure and use the platform features. The data collected includes but is not limited to: administrator usernames, administrator passwords, traffic management rule definitions, service endpoints, 3rd party data feed configurations, and other configuration details contributed by the customer.

Logs

Generated from users' invocation of Radar data collection or ITM traffic management on a customer website or application. The data includes: performance measurements taken by Radar, aggregated reporting, and traffic management decisions among other Logs detailed further in this document

Data Location

ITM is a highly redundant system that runs services across multiple environments and providers globally. Customer Content and Logs are maintained in multiple locations and services including in Amazon Web Services cloud environment in Ireland and Google Cloud environment in Ireland.

The Log data is collected from the end-users and is submitted to edge servers that are part of the ITM platform in the following countries : Ireland, Netherlands, United States, China and Taiwan. The edge servers transmit Log data to the centralized locations mentioned above in order to create scores that are used to predict the network and user experience and do real-time traffic management, customer log sharing (if enabled), data aggregation and ITM Customer Content and reporting. During that collection and submission process, Logs are stored on the edge servers for up to 30 days for operational verification.

ITM may also choose, when appropriate, to store or process Logs within other third party services. These third-party services are subject to change, and unless otherwise noted, these services are US-based. For a complete list, see our Subprocessors list.

Data Collection

ITM collects Log data as services are used. Logs are collected from the following events:

Radar Benchmarking

Generated Radar Benchmarking is aimed at measuring the performance of different clouds, Content Delivery Networks (CDN) and other end-points on the Internet that deliver content to the end-users. This testing is typically executed through a JavaScript client that is loaded from a customer's web page. The aim is to collect real-time network telemetry covering 4 key metrics. This data is used at an aggregate level to predict the network connection experience to a serving infrastructure.

For Radar Benchmarking the following is collected:

- Client and Recursive Resolver IP address
- Map measurements to geographic and logical buckets by market, country, region, state and network autonomous system number (ASN)
- User-Agent String
- To determine type of device (desktop, mobile, set top box, etc.).
- Timestamp of each measurement session and individual tests
- In order to aggregate network performance over time in reporting and to ensure data quality

The timing data collected is as follows:

- **HTTP Connect** – First, Radar measures how long it takes to download the small object. This measurement includes local DNS resolution, TCP connection establishment and the HTTP Request itself. This first request has the potential for a CDN, for example, to have a "cold" cache so this measurement can be quite noisy. This is measured in milliseconds.

- **HTTP Response Time (RTT)** – As soon as that first download completes, the Radar client downloads the small object again, reusing the open TCP connection and the browser's/OS cache for DNS resolution. The request bypasses the browser cache in order to gain a good representation of basic latency from the browser to the provider. This is measured in milliseconds.

- **HTTP Throughput (KBPS)** – The large object is downloaded, reusing the TCP connection and browser DNS cache again, to measure kilobytes per second (KBps) based on start and finish times of the download. Not all providers are measured for throughput and mobile users do not measure throughput to reduce against data transfer costs.

- **Error Rate** – The Error Rate is calculated based on which of these downloads succeed or fail.

This data collected is typically from two classifications of end-user populations:

- **Private** – Only the customer's end-users contribute to the testing of a given CDN, cloud or data center. These measurements are aggregated together and the scores are only viewable or actionable by the individual customer taking the measurements.

- **Community** – Measurements are taken of common accounts on CDN's and clouds. These measurements are aggregated across all customers in the community to generate scores of these platforms. These aggregated scores are then made available to the community to view and utilize in their load-balancing applications.

More information on the community and Radar testing can be found at: https://docs.citrix.com/en-us/citrix-intelligent-traffic-management/radar.html

The Radar tag and measurement policies are configurable. For example, a customer can configure the system to not participate in community Radar measurements. However, this may negatively affect the intelligence and functionality of the reporting and load-balancing services that are being used.

Navigation Timing

Beyond probing CDN, cloud and architectures as an additional benefit, Radar can also collect Navigation Timing data from the browser for each page load. This kind of data is usually called "Real User Measurement" or "RUM" and is useful for understanding page-level performance in the browser.

The data collected includes the timing information for how a page is delivered as defined by the Navigation Timing API (see below), the User-Agent String, protocol, hostname, referrer URL, the client IP address, the DNS resolver address and a timestamp for when the metrics were recorded.

Navigation timing data collection can be turned off if required. Note however that if turned off the "Page" performance information cannot be shown within the portal.

Resource Timing

Radar can collect Resource Timing data from the browser for each page load. The data collected includes the timing information for how a page's objects (images, script files, API calls, etc.) are delivered as defined by the Resource Timing API, the User-Agent String, protocol, hostname, referrer URL for page and objects, the client IP address, the DNS resolver address and a timestamp for when the metrics were recorded.

This data is more detailed than Navigation Timing data and is typically used to identify how individual page components are being delivered to groups of end-users. This is very useful to many content owners as it allows them to see any slow or badly performing components allowing corrective action to be taken (e.g. optimize the image, review the JavaScript code, etc.).

Resource timing information is an opt-in service and can be controlled by the customer. Note however that if turned off the performance information cannot be shown within the portal as it is not collected.

Video Playback Metrics

Video Playback Metrics collects information that is focused on the quality of video network delivery and the resulting viewing quality of experience for end-users. The data collected and stored includes the User-Agent String, protocol, hostname, URL for the video asset the client IP address, the DNS resolver address and a timestamp for when the metrics were recorded. In addition to video-level metrics defined by the Streaming Video Alliance, per-chunk metrics are stored. These include:

Data	Measurement Type	Definition
Delivered Bitrate	Playback	The per-second bitrate of the video based on the size of the chunks delivered. (kb)
Re-buffering Ratio	Playback	The percentage of time spent re-buffering during the playback. (%)
Video Start Failures	Playback	The percentage of time failures occurred when viewers attempted to play video. (%)
Video Start Time	Playback	The amount of time it took to start video play after the play attempt is made. (ms)
Response Time	Per-chunk	The time it takes for the chunks to start delivery based on the resource timing measurements (responseStart – requestStart)
Throughput	Per-chunk	The speed at which video chunks were downloaded based on the resource timing measurements. (kbps)

This data is collected so a content owner can evaluate the performance of their video delivery to end-users in the aggregate. This allows them to choose which CDN, cloud or infrastructure is best utilized to deliver content to their end-users.

Video Playback Metrics is an opt-in service and can be controlled by the customer. Note however that if turned off the performance information cannot be shown within the portal as it is not collected.

Traffic Management

Radar measurement data is aggregated and processed to generate a "score". Scores are sent to the ITM traffic management infrastructure for use in real-time DNS and HTTP decisions. These scores are sent as a data-stream to the load-balancers across the globe in order to make decisions about which CDN, Cloud or other architecture should be used for content delivery.

Reporting and Analysis

Reporting data is processed and stored in Google BigQuery. Some of the reporting data is exposed via the ITM portal or the reporting APIs. All reporting data that is available in the Portal and reporting APIs are anonymized and individual users cannot be identified.

Service Logs

In many instances, it is required by ITM customers to have access to their Log information for debugging and utilization purposes. This is currently delivered within a Log file format that does include an IP address (Resolver or Client dependent on service). This data is delivered via the Amazon AWS or Google Cloud infrastructure as described and stored securely for access by the customer. Log delivery is an opt-in service.

Data Transmission

ITM Logs are transmitted securely using industry standard secure protocols such as TLS.

Data Control

IP address or other personally identifiable information collected from users is anonymized before providing reports to customers and partners. From time to time, we may release non-personally identifying information in the aggregate, such as by publishing reports on trends or supplying data at an aggregate level without the use of individual IP address or other indentifiable information.

Cookie: A HTTP "cookie" is an alphanumeric identifier that is unique to a user's browser. The cookie will identify the browser and session to us when a user visits the ITM Portal. Cookies are not used by default in Radar or other ITM services that interact with end-users.

Do Not Track: ITM Radar honors the "Do Not Track" cookie, should a browser present this header. Radar will not take performance measurements if this setting is set.

Data Retention

Customer Content is retained for the life of the account so that there is an audit trail and a history of service configuration. Customers are able to delete individual administrative users at any time and, on request, the customer account can be terminated. On deletion, we will keep Customer Content for 30 days in the event the data needs to be recovered and all Customer Content will be removed within 90 days from the original request for termination.

Performance Logs and aggregated data generated from the Logs is retained for a rolling 18 month period. This data is used to provide customers with reporting in the ITM portal or using the API. Data from the logs cannot be deleted for individual users because it is not possible to identify specific users within the data set.

The following are the maximum periods of time a data "set" is retained:

Performance Logs	548 days
Minute (Aggregation)	35 days
Hour (Aggregation)	60 days
Day (Aggregation)	390 days

Citrix Services Security Exhibit

Detailed information concerning the security controls applied to ITM, including access and authentication, security program management, business continuity, and incident management, is included in the Citrix Services Security Exhibit.

Client Logs Collected

Radar Init and Request

In general, Citrix Intelligent Traffic Management Radar Logs contain:

- IP address (from caller)
- Customer Zone Id
- Customer Id
- Timestamp
- Transaction Id

Radar Report (per provider measured)

- Provider Zone id
- Provider Customer Id
- Provider Id
- Probe Type
- Response Code
- Measurement Value
- Cache Node Identifier

- partner tag (no longer used)
- startTime
- redirectStart
- redirectEnd
- fetchStart
- domainLookupStart
- domainLookupEnd
- connectStart
- connectEnd
- secureConnectionStart
- responseStart
- responseEnd
- requestStart
- duration
- transferSize

Radar Navigation Timing Report (per provider measured)

- Measurement Type
- Provider Owner Zone Id
- Provider Owner Customer Id
- Provider Id
- File size hint
- Response Code
- navigationStart
- unloadEventStart
- unloadEventEnd
- redirectStart
- redirectEnd
- fetchStart
- domainLookupStart
- domainLookupEnd
- connectStart

- connectEnd
- secureConnectionStart
- requestStart
- responseStart
- responseEnd
- domLoading
- domInteractive
- domContentLoadedEventStart
- domContentLoadedEventEnd
- domComplete
- loadEventStart
- loadEventEnd
- Request Signature
- hash
- Cache Node Id
- Tags

Navigation Timing Report (per provider measured)

- Response Code
- navigationStart
- unloadEventStart
- unloadEventEnd
- redirectStart
- redirectEnd
- fetchStart
- domainLookupStart
- domainLookupEnd
- connectStart
- connectEnd
- secureConnectionStart
- requestStart
- responseStart

- responseEnd
- domLoading
- domInteractive
- domContentLoadedEventStart
- domContentLoadedEventEnd
- domComplete
- loadEventStart
- loadEventEnd
- Request Signature
- Custom Fields
- start render

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States