

Understanding EdgeSight Network Data

EdgeSight Overview

Citrix EdgeSight is implemented as an agent based solution for monitoring end user experience with either their local Windows based desktop, laptop, or a Citrix XenApp environment. This agent transparently monitors user experience with both the computer and any applications which are run on that computer. No modification of any application is required in order for EdgeSight to collect data. Network information is collected by the agent from within the application performing the network access. This provides EdgeSight a unique perspective on the network performance, and can lead to some confusion when comparing EdgeSight network metrics with those collected from other means such as server logs or network sniffers. This document seeks to define EdgeSight network data such that this powerful perspective can be leveraged fully.

In the context of this document, the following types of user application based network data are collected for any network enabled application.

- TCP based WinSock socket data
- HTTP based web data

Glossary

Citrix EdgeSight defines several data monitoring concepts whose terminology may differ from other monitoring solutions.

Round Trip Time (RTT) – Overall duration associated with the initial socket connection.

Network Error – The WinSock return code associated with TCP connection attempts.

Transaction Error – The HTTP return code associated with HTTP requests.

Delay – Overall duration associated with the entire connection to response of a request.

Duration – The length of time either the network connection was open, or the HTTP request took to process depending on the data type.

Site – The FQDN of a network resource, including its port. If the FQDN can not be determined, for example due to the network resource being referenced in the application by direct IP address, then the Site will be defined using the IP address.

Host – A synonym for Site.

Virtual Host – The FQDN or IP address that the site operator wishes their server to be referenced as. This value is determined based on the requested site name and the returned site name. An example of this process is someone browsing to `mysite.com` and being redirected to `www.mysite.com`.

Transaction – An HTTP based request with associated response. Within the EdgeSight reports, a transaction refers to a specific request to a Site.

Network Calculations

In order to provide meaningful context to the low level network statistics EdgeSight collects, the EdgeSight agent performs a number of calculations on the raw data. This section describes those calculations.

Network Round Trip Time

Citrix EdgeSight agents calculate the round trip time associated with a given TCP connection passively during the creation of the network socket. The round trip time is only recorded during the initial connection attempt and then used as a reference during the lifespan of the given socket connection.

Note: Since the agent records network data from within the actual application performing the network requests, it is possible that the round trip time for non-blocking socket calls can be zero depending on the underlying network drivers and any connection caches. Additionally, in the event of a TCP error during connection the round trip time is effectively undefined and will be recorded as a zero value.

Transaction Delay

The EdgeSight agent passively measures transaction delay from within the actual application performing the transaction. The transaction delay is measured as the total duration of the transaction divided by the number of TCP socket read and write operations required to perform the transaction.

Note: The EdgeSight agent imposes a maximum on the delay value of ten seconds corresponding to two samples of a long running socket connection. This value will typically appear for high latency or low bandwidth networks.

Average Total Delay

Average total delay is the average request to response delay associated with the TCP socket operations performed by the monitored application. Depending upon the lifespan of the socket, this value is calculated either when the socket is closed or at five second intervals. Regardless of the calculation point, the average request to response delay metric is measured from successive read and write operations occurring on the TCP socket. All network delay calculations are based on this metric.

Network Delay

The EdgeSight agent calculates the network delay for a given connection or transaction by first estimating the number of round trips which were required for the given operation. The factors used in the estimation include the number of bytes written to and read from the socket and the maximum segment size for the network interface used in the connection.

Note: In order to maintain the efficiency of the EdgeSight agent, network delay associated with any operation which contains a single network segment, or where there are fewer than two round trips are ignored. This is consistent with the goal of balancing the overhead of network monitoring with an accurate assessment of actual end user network experience.

Once the number of round trips is established, the network delay is simply the number of round trips multiplied by the round trip time and divided by the average total delay associated with each request response operation.

$$\text{Network Delay} = (\text{RTT} * (\text{Number of Round Trips})) / (\text{Average Total Delay})$$

Client Delay

Since the EdgeSight agent is monitoring all network usage by an application from within the application, it is uniquely positioned to determine how application performance impacts overall network experience. The client delay metric is calculated based on successive read or write operations to the TCP socket. Effectively this measures the amount of time taken by the client to process the network buffers which make up the network operation. The client delay is simply the total client time divided by the average total delay associated with each request response action.

$$\text{Client Delay} = (\text{Client Processing Time}) / (\text{Average Total Delay})$$

Server Delay

Once the network and client components of the overall socket delays are established, the server delay can be derived. The server delay metric will include all portions of the socket delay not calculated to be related to the client operations on the socket or within the network itself. The server delay metric will include the impact not only of the server the socket is connected to, but also any backend servers used by that initial server to complete the response. Server Delay can be calculated using this formula.

$$\text{Server Delay} = ((\text{Average Total Delay}) - (\text{RTT} * (\text{Number of Round Trips})) - (\text{Client Processing Time})) / (\text{Average Total Delay})$$

If you look at the data as percentages of the total delay experienced by the application, this calculation simplifies to provide the server delay as a percentage indicating the amount of time spent on the server processing the request.

$$\text{Server Processing Percent} = 100 - ((\text{Network Delay}) + (\text{Client Delay})) * 100$$

Network Volume

Network volume is calculated as the total number of kilobytes of data sent and received on the TCP socket connected to the given site.

Network Bandwidth

Network bandwidth is calculated as the bit rate experienced on the TCP socket connected to the given site. It is measured independent of read or write operations, and will only be calculated for network operations containing a minimum of 1024 bytes of data transferred. Network bandwidth is stored in kilobytes per second.

Socket Lifetime Impact

Depending upon how the network application is authored, TCP sockets can be either long and short lived. Typically, an application author will use a long lived socket if they expect to make repeated calls to the site, if the protocol being used requires long lived sockets, or when large volumes of data need to be transferred. In order to accurately record the performance of all types of network requests, EdgeSight implements two distinct monitoring models. For short lived sockets, EdgeSight records all network metrics when the socket is closed, and determines if data will be stored for the socket based on the rules described above.

Accurate recording of data for long lived sockets requires that the socket performance be polled. The polling interval is every 5 seconds, and the timer is based on actual socket transitions resulting from data transferred. When a long running socket closes, the EdgeSight agent will automatically consider all traffic occurring from the last 5 second interval to the socket close as occurring within the same 5 second interval.

Data Grooming Impact

The EdgeSight agent automatically tunes its data collection based on the volume of data seen, and the agent configuration settings for data retention. With Citrix EdgeSight for Endpoints, the default agent data retention interval is seven days, and for EdgeSight for XenApp the default agent data retention interval is three days. Since the quantity of network sockets created will vary considerably with application usage, application architecture and the number of users accessing an application, collecting data for all network sockets may not always be feasible. In order to balance the impact of network monitoring on the monitored system with the collection of network data; if the number of unique data collection points exceeds 360, 000 within the data retention interval any network operations occurring after the limit has been reached will not be recorded. Once the number of data collection points drops below this threshold, network monitoring will once again occur. For the purposes of data grooming, data collection points are the combination of short live socket connections and poll intervals on long lived sockets. The data collection threshold for network data is not user configurable.

Proxy Impact

The Citrix EdgeSight agent transparently monitors the application experience with the network resources accessed by the application. Proxies, firewalls, and NAT devices are considered part of the network, unless the application is specifically configured to use a proxy. When an application is configured to use a proxy, the EdgeSight agent automatically considers the proxy as the site for all traffic.

Conclusion

Citrix EdgeSight provides a powerful and unique perspective on network monitoring. By virtue of monitoring application usage of the underlying network, EdgeSight can clearly show not only the performance of site resources, but also the impact application and computer performance on the user experience with those site resources.