TAIGA INSIGHTS

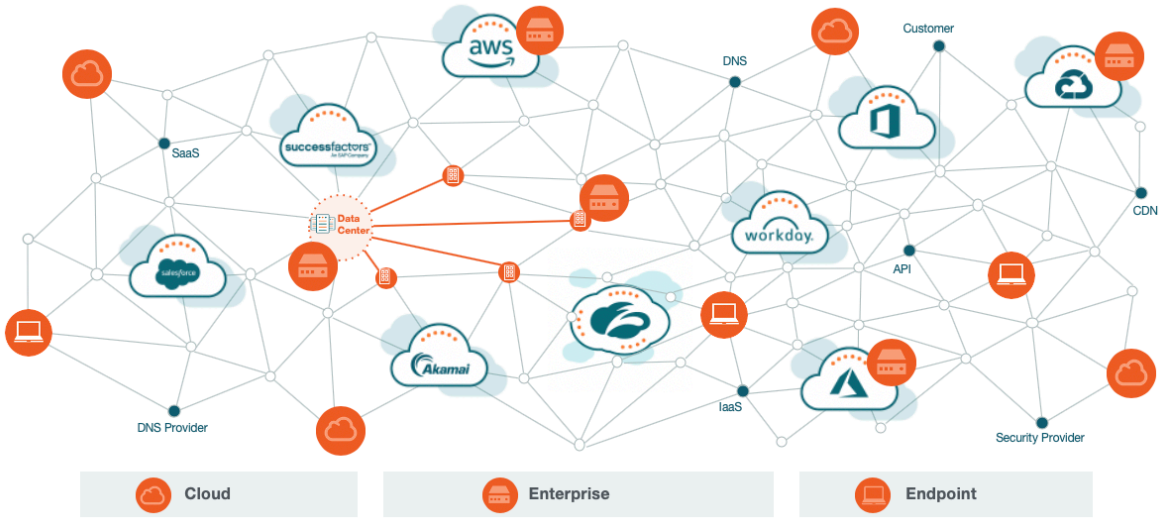
POWERED BY THOUSANDEYES

Taiga Insights powered by ThousandEyes

Internet es vasto, impredecible y está compuesto por miles de administradores de servicio independientementes de diferentes proveedores de servicios, cualquiera de los cuales puede afectar la experiencia de los usuarios que se conectan a una aplicación o sitio. Las interrupciones de la red ocurren diariamente en Internet, lo que desafía la capacidad de las operaciones y equipos para entregar un servicio. Las interrupciones no solo son muy perjudiciales, sino que pueden ser extremadamente difíciles para detectar y aislar, particularmente si tienen lugar dentro de una red de proveedores de servicios aguas arriba.

Para las empresas digitales, gestionar la prestación de servicios a través de Internet es esencial para la generación de los ingresos y reputación de marca, ya que los usuarios de hoy esperan que las aplicaciones y los sitios sean accesibles y de alto rendimiento en todo momento. Las empresas pueden no controlar directamente Internet, pero son en última instancia, responsables de la accesibilidad de su servicio y la experiencia del usuario.

UNA VISTA GLOBAL DE LA SALUD DE INTERNET



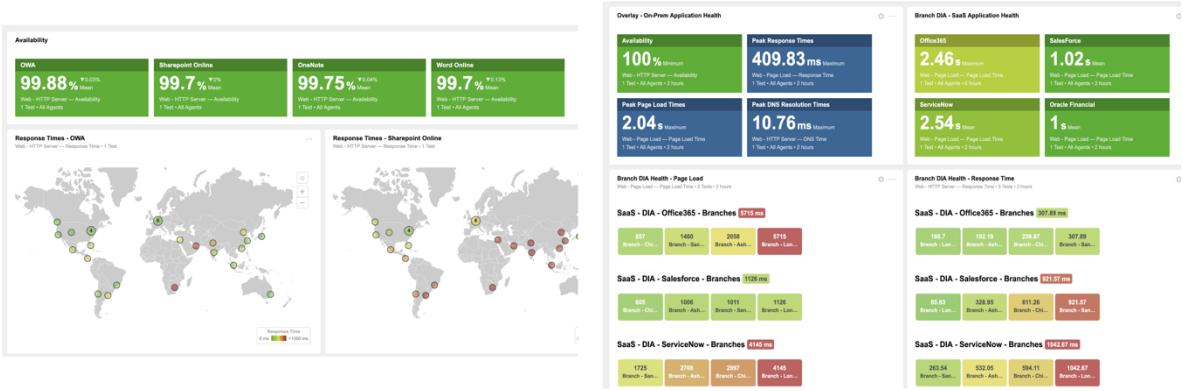
Taiga Insights

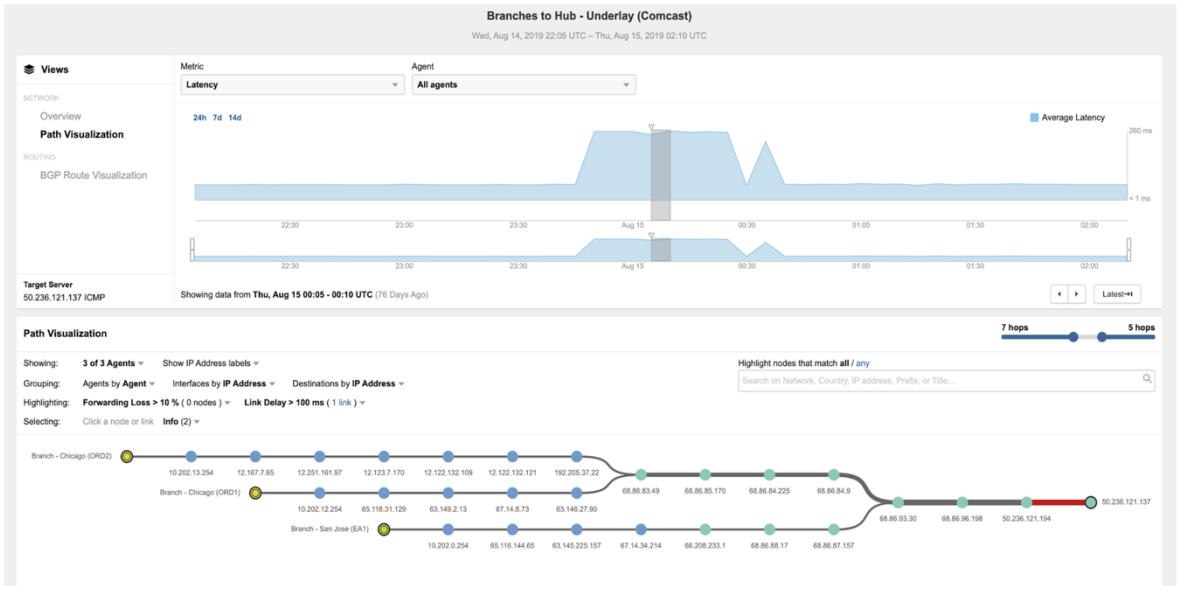
Taiga Insights powered by ThousandEyes aprovecha su visión colectiva global de las rutas de prestación de servicios en Internet para proporcionar una vista macro de las interrupciones de la red, llamada Taiga Insights. Mil agentes de los ojos ubicados en Internet realizan más de 8 mil millones de mediciones cada día, produciendo un conjunto de datos masivo que incluye información a nivel de interfaz de red sobre cuándo y dónde se interrumpen los flujos de tráfico en Internet. Una vez que Taiga Insights detecta el comportamiento de interrupción, lo aísla a un Sistema Autónomo (AS) y la ubicación lo visualiza casi en tiempo real a través de una variedad de vistas globales, macro y topológicas.

Taiga Insights permite a los equipos de operaciones aprovechar los datos anónimos de telemetría de Internet, en lugar de que el rumor público: identificar rápidamente, escalar y remediar problemas, así como comunicar más efectivamente con los clientes. Visualizando y correlacionando interrupciones con la experiencia del usuario y otros señales, las empresas pueden reducir drásticamente el tiempo medio de identificación (MTTI) de horas a minutos.

Dashboard de Interrupción

Diseñado para los Centros de operaciones de red (NOC), el panel de información general de Taiga Insights, superpone interrupciones recientes y continuas en una vista de mapa global para proporcionar a los equipos de operaciones con una visualización de alto nivel de la salud de Internet.





Data collected by ThousandEyes Endpoint Agent

Share

Last updated: Mon Feb 04 23:41:07 GMT 2019

This article covers the data collected by ThousandEyes Endpoint Agent.

Website Visits

While outside a monitored network

No data is automatically collected while an Endpoint Agent communicates with ThousandEyes from outside a monitored network. Manual recording may still be initiated by the endpoint user, targeting ANY (monitored or unmonitored) domain. These results will be collected and reported back to ThousandEyes and will appear in the Endpoint Agent views.

While inside a monitored network

All website visits will be captured. If the visit is to a domain not listed in the monitored domain list, only the target domain will be captured, not the specific resource visited. All visits to monitored domains will be collected; during a visit, two categories of information are collected (see web performance data, below)

Web Performance Data (Web and Session Details Views)

Web Performance data includes HTTP Archive (HAR) format data. HAR information collected by the Endpoint Agent includes each file accessed on a particular site, and includes request and response header information, timing, source and destination IP addresses, as well as wait and receive timing for each component loaded in each page visited. Sensitive information in headers (such as cookie information and authorization data) is suppressed at collection time.

For more information on the content of HAR format data, refer to **http://www.softwareishard.com/blog/firebug/http-archive-specification/**

Waterfall data is shown for each page visited. A “session” constitutes either:

- a user visit to a domain, using a specific protocol (ie, **http://www.google.com** and **https://www.google.com** would be separate sessions, since the protocol differs between the two domains, however, multiple subsequent visits to **https://www.google.com** would be recorded in the same session)

- a manual recording initiated by an endpoint user - the session will last from the first page that the user clicks the record button through the last page of the recording.

A waterfall ("page") will be captured each time the DOM is reloaded in a session (ie, navigation to another page, form submission and/or page refresh). Multiple pages can be shown in a single session.

Network Data (Network and Session Details Views)

Network data is collected in a number of different ways, and differs from data captured by the ThousandEyes Enterprise Agent. A detailed list of each series of packets sent is shown below:

Network probes consists of three type of probes:

- **ICMP ping**: Sends 10 ICMP packets with 1 second interval. The round trip time (RTT) is captured and the sent/received ratio.
- **ICMP path trace**: Performs an ICMP-based TTL path trace with a maximum of 32 hops. Information about each hop is captured, including RTT. If the Endpoint Agent is running on a Mac OS X client, MPLS information will also be captured and shown
- **TCP connect**: Opens a TCP connection with a 10 second timeout and closes the connection if it was able to connect. Timing, and error code (if applicable) is captured.

Based on the connection topology of the Endpoint, network probes will be sent to the following destinations:

Target	ICMP ping	ICMP path trace	TCP connect
Gateway	X		
Destination	X	X	X
Proxy (if used)	X	X	X
VPN (if used)	X	X	

Computer Information (Session Details View)

Some information about the computer where the Endpoint Agent is installed is collected as well.

Field	Description	Example
Platform	Base operating system	Windows / Mac
OS Version	Major/minor version of operating system	Microsoft Windows 8.1 Enterprise
Kernel Version	Kernel version numbers	6.3.9600
Browser	Browser used for data collection	Google Chrome (46.0.2490.80)
Endpoint Version	Major/minor version of endpoint agent	0.24.1
IP Address	Private IP address	10.1.1.100
DNS Servers	Addresses of configured DNS server	10.1.1.253, 10.1.1.254
Manufacturer	Hardware manufacturer	Lenovo
Model	Hardware model	20ARS18N00

Memory	Total memory available to Operating System	8192 MB
Computer Name	Computer Name	win81-1
Logged in user	User name	boulders\dave

Network Information (Session Details and Network Topology Views)

In addtion to the computer information, the following network information is collected

Field	Description	Example
Network Name	Name of wireless network	BOULDERS
BSSID	Base Station ID (mac address)	8e:2f:44:4a:ae:bf
Channel	Wireless channel	2 (2.4 GHz)
Signal Strength	Signal strength (dBm)	-32
Signal Quality	Signal quality (expressed as a percentage)	99%

Transmission Rate	Maximum transmission as seen by operating system	130 Mbps
Physical Mode	IEEE 802.11 specification for wireless connection	802.11n
Hardware type	Connection type (Wired/Wireless)	Wireless
Proxy method	If a proxy is used, the method (PAC file, WPAD, manual)	Network PAC Script
Proxy configuration URL	If proxy autoconfiguration is used, the URL where the file is sourced from	http://10.1.1.1/scripts/autoproxy.pac
Network Gateway	Default network gateway	10.1.1.1