

ESTATS

From AkamaiWiki



Contents

- 1 Getting Started
- 2 Input
- 3 Output
- 4 Use Cases
- 5 Known Issues
- 6 FAQ
- 7 Support
- 8 Behind the Scenes
- 9 Related KB-Articles

1 Getting Started

eSTATS is used to gather diagnostic information for errors happening in the network for a given customer. It is a great place to start troubleshooting because it allows you to gather a broader set of data before investigating the problem in a deeper level. It can be used to quickly determine the scope of an issue - widespread or localized, complete failure or partial failure, intermittent or continuous etc. eSTATS allows you to start troubleshooting even when you don't have all the information from a customer, and it allows you to do a quick check on the health of content delivery - similar to checking the vitals of a patient in an ER setting.

eStats can be accessed from GSS Tools Portal under HTTP -> Availability -> ESTATS - Direct link: <http://tools.gss.akamai.com/estats>

2 Input

- **Cpcode / URL:** CPcode or URL field.
- **Region / IP:** Region or IP field
- **Network:** (Here you can select the network of interest to run eStats on)
 - **fflow:** fflow network
 - **essl:** essl network
 - **flash:** flash network
 - **mega:** uses all aggregators - if you know the Cp Code but unsure of the network - use mega - but it is very slow
 - **sqa:** QA network (test product before roll out) used for testing tools against new aggregator
 - **ighost:** invisible ghost
 - gather data on performance tuning
 - Can use this network to check the traffic on iGhost servers. These are servers that will not serve end-users but will simulate traffic. (sample of production goes through, but does not affect end user traffic)
- **Zone:** Contains ESN, Zone 1 and Zone 2
- **Group By / Limit:** Contains different fields you can group the data by, and the number of rows you want to see the data limited to.
- **Type:**
 - **Hits:** includes status codes 100,200,204,206,301,302,304,404
 - **Errors:** any status code that is not included in the above set
 - **Edge:** Egress r lines excluding jftGKPx in obj status
 - **Midgress:** Midgress f lines not having o in obj status
 - **Origin:** Ingress f lines having o in obj status

3 Output

- **Number of Hits/Errors:** Reflects the number of hits/errors in near-real time over 10s interval.
- **Edge IP:** IP of Edge server showing the error
- **Region:** The region number of that edge server

- **Return Code:** HTTP Response code
- **Origin/Edge Errors:** Number of hits showing an non-error/error response code
- **Origin/Edge Hits:** Number of hits showing an non-error/error response code.
- **Error Code:** Ghost error code that equates to an error message
- **Object Status:** Object status information that shows more information about the transaction
- **Sample Logs:** Links to fetch sample ghost logs (ghost.access.log) or cache logs (cache.log)
- **Email Report:** to email yourself (or any internal employee) a copy of the report
- **Plot:** To visualize the results of the query in a world map

4 Use Cases

Use Case ?	When to use ?	How to use ?	How to interpret output ?
Show severity of errors (How important it is to escalate to CCare)	Used when you need to understand the severity of errors on a given Cpcode/url and Region/IP combination.	The severity of the errors will be in the top table under the input fields.	After entering a Cpcode, region and selecting a network - the top result shown is a Severity field. Definitions of each severity level are documented here: ESTATS Severity
Show live server errors	When investigating a particular server's errors	Enter the IP, and associated errors will appear	The severity, errors/hits and percentage of failure will be listed.
Investigate error patterns that are region/ip specific	When investigating patterns on a regional/ip level	Input the region number or server IP, and leave the cpcode field blank.	The results will show you what errors are happening in a given region or server, and what customers are impacted.
Check errors while doing metadata propagation	When you make a sensitive metadata change, and you want to check the errors in live traffic in zone#1 or zone#2 while the metadata is propaga	Enter the Cpcode, and choose zone#1 or zone#2.	You can stop the tarball from propagating if you encounter errors as a result of your metadata changes.
Investigate a customer DOS Attack	When a customer is experiencing a DOS, and akamai does not know where requests are coming from.	Can input the IP or URL that is experiencing high traffic and choose "Edge Hits"	With a known URL or Cpcode, you can investigate edge hits, and sort by region to find the source of requests. Get sample logs and check for any patterns based on client IP or User-Agent.
Investigate sudden high traffic to origin	When a customer is experiencing a sudden increase of unexplained traffic to their origin.	Can input the IP or URL that is experiencing high traffic and use "Origin Hits"	You can determine which regions are hitting the origin. Additionally, you can see which IPs are getting hit, then get sample logs to investigate suspicious activity.
Investigate slow response times	When experiencing slow response times and you are unaware of the impact.	You can input the Cpcode or URL and then see errors of these servers.	If there are performance issues, there are likely client aborts in edge hits or errors in forward requests. Knowing the Cpcode or URL, you can determine which regions have high origin errors (selecting Origin Errors from the Type drop-down). You can then determine if there is a faulty region, and depending on a number of other factors - follow region suspension guidelines if needed.
Check geographical proximity of servers that are serving errors for a Cpcode (See the scope of errors)	When you want to see the distribution of errors geographically	You can click on the "Plot Edge Errors in the world map" button	Can plot errors on a map to see ips plotted on a global map. With this, you can visually see regions.
Find which customers are impacted by a region issue	Useful to provide more information before suspending a region to see which customers are utilizing the region.	Enter a given region, and sort by customers	You wouldn't want to suspend a region when a top-tier customer is pushing a lot of data through that region, or if there is no general problem in the region for other customers. You should follow the standard checklisting before suspending a region, and eSTATS can help you determine if other customers in the region are impacted or whether there is top-tier customer traffic in the region.
Investigate Midgress Errors	There are no origin errors, but		You can identify if there are any issues in akamai server connecting to other regions

(Check for errors in cache header IP or sure route traffic)	there are still edge errors. Are there connectivity issues between akamai servers?	Use Midgress Error option	for cache-H etc. Cache-H and sureroute hits/errors are reported under Midgress option.
Find live traffic on a server for a given Cpcode	If you do not have a tier 1 and want to see which servers are sending traffic. Also - if LDS is not spinning and you want to do log analysis.	Can be determined by entering the specific Cpcode and using "Edge Hits"	You can determine top regions, and do a gHost grep on these regions.
Troubleshoot CMP alerts	When you have a CMP alert and you need to determine scope of the error	Enter Cpcode, run report. You can then e-mail the contents, with the ticket number in the subject line cc'ing ccare	Use the severity to access the impact, and get sample logs through eSTATS before escalating to Ccare.
Monitor Go-Live Event	Quickly find hits/errors during Go-live	Enter cpcode, and check the 'edge hits' report. Use 'automatic refresh' option to refresh automatically.	Watch for edge hits to come to Akamai and keep an eye on 'origin errors' and 'edge errors'

5 Known Issues

Bugzilla page for eSTATS (https://bugzilla.akamai.com/buglist.cgi?query_format=advanced&short_desc_type=allwordssubstr&short_desc=&product=gtools&component=eSTATS&ak_network_type=allwords&long_desc_type=substr0-0=noop&type0-0-0=noop&value0-0-0=%7C)

6 FAQ

7 Support

- Sev 1 issues - Please see Cc-infra#Escalation Process
- Questions: Email gtools-dev@akamai.com
- Enhancements: Open CR (https://bugzilla.akamai.com/enter_bug.cgi?product=gtools%7C)

8 Behind the Scenes

To be filled in by the Developer

9 Related KB-Articles

Not Found

The requested URL was not found on this server.

Apache/2.4.52 (Ubuntu) Server at kbint.akamai.com Port 443

Retrieved from "<https://api.agora.akamai.com/wiki/ESTATS>"

Category: Services Tools

- This page was last modified on September 28, 2012, at 21:24.

Except when indicated otherwise, all pages are Akamai Confidential