Characterize webTrafficParser formParameter Option NS LocationAPI

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Example #1: Traffic Profile

Conclusion

Related Information

Introduction

This document describes filtering LocationAPI with webTrafficParser against access_log HTTP POST formParameter, since NS 2024.01 HTTP GET was removed.

Cisco recommends that you have knowledge of these topics:

- Cisco BroadWorks System Administrator privilege.
- NS Location and Portal API Requests Response.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to special software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The Location API request/response can be tracked as HTTP GET request log record in Cisco BroadWorks Network Server tomcat access_log. This method was replaced by HTTP POST in the 2024.01 feature. In this change, the tomcat access log added the field formParameters. The build-in BroadWorks webTrafficParser has since been enhanced to filter and read this fieldParameters. You can identify LocationAPI issue by paste and analyse the NS tomcat access log with webTrafficParser to identify from the HTTP POST request and the enclosed formParameter field.

Example #1: Traffic Profile

The tool webTrafficParser is located in the bin directory (/user/local/broadworks/bw_base/bin):

bwadmin@ns$ **cd /usr/local/broadworks/bw_base/bin**
bwadmin@ns$ **ls -ltr webTrafficParser**

lrwxrwxrwx. 1 bworks bwadmin 58 Apr 15 13:16 webTrafficParser ->
../../apps/WebContainer_2026.02_1.261/bin/webTrafficParser

bwadmin@ns$ **webTrafficParser**

Must specify one or more log files.

Usage:

webTrafficParser [-a] [-m <regexp>] [-r] [-p <interval>] [-t <number>] <log file name(s)>

This tool parses tomcat access logs to characterize incoming traffic.

List of possible options:

-a : prints full output (all entries instead of top 10)

-m <regexp> : prints out log file entries matching regular expression

-r : displays rate-based (messages per second) information

-t <number> : prints top <number> items

-s <Start_time> : start time for file(s). Example format for times 30/Jan/2013:19:22:57

Defaults to first time in file(s).

-e <End_time> : end time for file(s). Defaults to last time in last file.

-p <interval> : prints a traffic profile from start to end time at an interval

(in minutes). This can be saved to a csv file and graphed.

The script parses up to 10 log files.

The log file names must be specified in time order.

Paste the NS tomcat access log of a focus time frame to webTrafficParser, this return a high volume for a particular user Location API request (416 in total):

- bwadmin@ns$ **webTrafficParser access_log.2026.10*.txt**

  ns1-r25.cisco.com TRAFFIC COUNTS. START TIME = 01/Oct/2026:00:00:49. END TIME = 08/Oct/2026:21:09:09.

  Total Time = 677300.000 seconds
  Total Number of Requests = 33996

  68 Average Request Size (bytes)
  641 Average Response Size (bytes)
  0.002 Average Response Time (seconds)

  Traffic by HTTP method:
  22994 POST

6105 GET
4599 OPTIONS
251 -
9 HEAD
8 GNUTELLA
4 some
4 NESSUS
4 PROPFIND
4 TRACE

Top 10 by URL:
22389
/servlet/GetAllHostingNeNodeAddresses?private=false&broadworksOnly=true&clusterMode=false&callPRequest=true&requestingAddresses=10.66.82.113
4599 *
781 /
416 /servlet/LocateUser?url=jliangEntGrp1User5%40syd.cisco.com&returnCompatibleXSP=true&callPRequest=true
251 -
126 /Login/
92 /login
88 /images

52 /login.html
38 /index.html

Top 10 by Address:
22833 10.66.82.113
4587 10.66.82.105
3288 <some public IP address>
3288 <some other public address>

Top 10 by Return Code:
27554 200
5077 302
804 404
553 400
4 403
4 405

Top 10 by User ID:
33996 -

Top 10 by User-Agent:
...

bwadmin@ns$

Paste the userId 'jliangEntGrp1User5' as a parameter of the -m option to webTrafficParser. This returns the particular userId in field 15 of the access log entries. Field 15 is formParameters of the HTTP POST request.

bwadmin@ns$ **cd /var/broadworks/logs/tomcat/**
bwadmin@ns$ **webTrafficParser -m "jliangEntGrp1User5" access_log.2026.10*.txt**
10.66.82.113 - - [01/Oct/2026:10:34:24 +1000] "POST /servlet/LocateUser HTTP/1.1" 200 94 199 0.003 3 "-" "Java
"BWCALLCENTER_
220f25f7-7353-4d4b-960a-4b3136897297" 10.66.82.115 80
"url=jliangEntGrp1User5&returnCompatibleXSP=true&callPRequest=false&netadmin=jli
angEntGrp1User5"
...
10.66.82.113 - - [08/Oct/2026:21:28:04 +1100] "POST /servlet/LocateUser HTTP/1.1" 200 126 199 0.002 2 "-" "Jav
"COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8" 10.66.82.115 80
"url=jliangEntGrp1User5%40sys.cisco.com&returnCompatibleXSP=true&callPRequest=false&netadmin=jliangEnt
bwadmin@ns$

You can move on to next step to analyze the NSPortalLog. Change to the nsportal logging directory. You paste the userId jliangEntGrp1User5 as -m parameter to bwTrafficParser to analyse the nsportallog. This results in a location API issue, where the NS cannot find the userid: jliangEntGrp1User5@cisco.com:

- bwadmin@ns$ **cd /var/broadworks/logs/nsportal/**
  bwadmin@ns$ **bwTrafficParser -m "jliangEntGrp1User5" NSPortalLog2026.10.08-00.00.03.txt**
  2026.10.08 21:28:04:536 AEDT | Info | HTTP | HTTPThread-49 | 7669459 | COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

  tcp - HTTP Bytes IN from 10.66.82.113:57078 (received on 10.66.82.115:80)
  POST http://10.66.82.115/servlet/LocateUser
  Headers:
  trackingid: COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8
  x-broadsoft-correlation-id: cc6f959b-2507-4792-b158-780c74af0d07
  x-broadworks-protocol-version: 1.1
  content-type: application/x-www-form-urlencoded
  charset: utf-8
  ...
  host: 10.66.82.115
  accept: text/html, image/gif, image/jpeg, */*; q=0.2
  connection: keep-alive
  content-length: 126
  Parameters:
  url=jliangEntGrp1User5@sys.cisco.com
  returnCompatibleXSP=true
  callPRequest=false
  netadmin=jliangEntGrp1User5@sys.cisco.com

  bwadmin@ns$ **bwTrafficParser -m COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8 NSPortalLog2026.10.08-00.00.03.txt**
  2026.10.08 21:28:04:536 AEDT | Info | HTTP | HTTPThread-49 | 7669459 | COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

  tcp - HTTP Bytes IN from 10.66.82.113:57078 (received on 10.66.82.115:80)
  POST http://10.66.82.115/servlet/LocateUser
  Headers:
  trackingid: COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8
  x-broadsoft-correlation-id: cc6f959b-2507-4792-b158-780c74af0d07
  x-broadworks-protocol-version: 1.1
  content-type: application/x-www-form-urlencoded

charset: utf-8
user-agent: Java/11.0.29
host: 10.66.82.115
accept: text/html, image/gif, image/jpeg, */*; q=0.2
connection: keep-alive
content-length: 126
Parameters:
url=jliangEntGrp1User5@sys.cisco.com
returnCompatibleXSP=true
callPRequest=false
netadmin=jliangEntGrp1User5@sys.cisco.com

2026.10.08 21:28:04:536 AEDT | Debug | Generic | HTTPThread-49 | 7669460 | COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

doFilter()

2026.10.08 21:28:04:536 AEDT | FieldDebug | PortalInputChannel | HTTPThread-49 | 7669461 | COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

Accepting request using version: 1.1 (server at 1.1)

2026.10.08 21:28:04:537 AEDT | Info | LocationAPI | HTTPThread-49 | 7669462 | COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

tcp 188 HTTP Bytes OUT to 10.66.82.113:57078 (sent from 10.66.82.115:80)
<?xml version="1.0" encoding="UTF-8"?>

<com.broadsoft.protocols.nsportal.Error detail="Unknown URL"
id="2"
summary="Cannot complete request"
>
</com.broadsoft.protocols.nsportal.Error>

2026.10.08 21:28:04:537 AEDT | Info | HTTP | HTTPThread-49 | 7669463 | COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

tcp - HTTP Bytes OUT to 10.66.82.113:57078 (sent from 10.66.82.115:80)
statusCode=200
Headers:
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
TrackingID: COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8
X-BROADSOFT-CORRELATION-ID: cc6f959b-2507-4792-b158-780c74af0d07
X-BroadWorks-Protocol-Version: 1.1
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Date: Thu, 08 Oct 2026 10:28:04 GMT
Keep-Alive: timeout=5
Connection: keep-alive
Server: HTTP Server

Conclusion

After this troubleshooting to identify the LocationAPI 'Unknown URL' is the root cause of high amount 200 OK for HTTP POST with formParam

"*url=jliangEntGrp1User5%40sys.cisco.com&returnCompatibleXSP=true&callPRequest=false&netadmin=jliangE*
you can verify the userId jliangEntGrp1User5@cisco.com is existing in AS only due to a SyncAPI difficulty.

Related Information

- RemoveSensitiveInformationFromNSLocationAndPortalAPIRequestsFD-R2024_01.pdf