Caratterizza webTrafficParser formParameter Option NS LocationAPI

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Premesse

Esempio 1: Profilo traffico

Conclusioni

Informazioni correlate

Introduzione

In questo documento viene descritto come filtrare LocationAPI con webTrafficParser in base a access_log HTTP POST formParameter, poiché è stato rimosso NS 2024.01 HTTP GET.

Cisco raccomanda la conoscenza dei seguenti argomenti:
- Privilegio Cisco BroadWorks System Administrator.
- Risposta alle richieste API del portale e della posizione NS.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La richiesta/risposta dell'API del percorso può essere registrata come record del log della richiesta GET HTTP nel server di rete Cisco BroadWorks per individuare access_log. Questo metodo è stato sostituito da HTTP POST nella funzionalità 2024.01. In questa modifica, il log degli accessi tomcat ha aggiunto il campo formParameters. L'oggetto webTrafficParser di BroadWorks incorporato è stato successivamente migliorato per filtrare e leggere i parametri di questo campo. È possibile identificare il problema LocationAPI incollando e analizzando il log degli accessi al sito NS con webTrafficParser per identificare dalla richiesta HTTP POST e dal campo formParameter incluso.

Esempio 1: Profilo traffico

Lo strumento webTrafficParser si trova nella directory bin (/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

Specificare uno o più file di registro.

Utilizzo:

webTrafficParser [-a] [-m <regexp>] [-r] [-p <intervallo>] [-t <numero>] <nome/i file di log>

Questo strumento analizza i log degli accessi al gatto per caratterizzare il traffico in ingresso.

Elenco delle opzioni possibili:

-a : stampa l'output completo (tutte le voci invece delle prime 10)

-m <regexp>: stampa le voci del file di log corrispondenti all'espressione regolare

-r : visualizza informazioni basate sulla velocità (messaggi al secondo)

-t <numero> : stampa i primi <number> elementi

-s <ora_iniziale> : ora di inizio per i file. Formato di esempio per l'ora 30/gen/2013:19:22:57

Per impostazione predefinita, la prima volta in uno o più file.

-e <Ora_finale>: ora di fine dei file. Per impostazione predefinita, viene utilizzata l'ultima volta nell'ultimo file.

-p <intervallo> : stampa un profilo di traffico dall'ora di inizio a quella di fine in base a un intervallo

(in minuti). che può essere salvato in un file csv e rappresentato in un grafico.

Lo script analizza fino a 10 file di registro.

I nomi dei file di log devono essere specificati in ordine temporale.

Incollare il log degli accessi al sito NS di un intervallo di tempo attivo in webTrafficParser, che restituisce un volume elevato per una richiesta API posizione utente specifica (416 in totale):

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

  ns1-r25.cisco.com CONTEGGIO TRAFFICO. ORA INIZIO = 01/ott/2026:00:00:49. ORA FINE = 08/ott/2026:21:09:09.

Tempo totale = 677300.000 secondi
Numero totale di richieste = 33996

68 Dimensione media richiesta (byte)
Dimensione media risposta 641 (byte)
0,002 Tempo medio di risposta (secondi)

Traffico per metodo HTTP:
POST 22994
GET 6105
OPZIONI 4599
251-
9 TESTINA
8 GNUTELLA
4 alcuni
4 NESSUS
4 PROPFIND
4 TRACCE

Primi 10 per URL:
22389
/servlet/GetAllHostingNetNodeAddresses?private=false&broadworksOnly=true&clusterMode=false&callPRequest=true&requesting
Indirizzi=10.66.82.113
4599 *
781/
416 /servlet/LocateUser?url=jliangEntGrp1User5%40syd.cisco.com&returnCompatibleXSP=true&callPRequest=true
251-
126 /Login/
92 /login
88 /immagini

52 /login.html
38. /index.html

Primi 10 per indirizzo:
22833 10.66.82.113
4587 10.66.82.105
3288 <indirizzo IP pubblico>
3288 <altro indirizzo pubblico>

Primi 10 per codice restituito:
27554 200
5077 302
804 404
553 400
4 403
4 405

Primi 10 per ID utente:
33996-

Primi 10 per agente utente:
...

bwadmin@ns$

Incollare l'ID utente 'jliangEntGrp1User5' come parametro dell'opzione -m in webTrafficParser. Restituisce l'ID utente specifico nel campo 15 delle voci del log degli accessi. Il campo 15 è formParametri della richiesta HTTP POST.

```
bwadmin@ns$ cd /var/broadworks/logs/tomcat/
bwadmin@ns$ webTrafficParser -m "jliangEntGrp1User5" access_log.2026.10*.txt
10.66.82.113 - - [01/ott/2026:10:34:24 +1000] "POST /servlet/LocateUser HTTP/1.1" 200 94 199 0.003 3
"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/ott/2026:21:28:04 +1100] "POST /servlet/LocateUser HTTP/1.1" 200 126 199 0.002 2
"COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8" 10.66.82.115 80
"url=jliangEntGrp1User5%40sys.cisco.com&returnCompatibleXSP=true&callPRequest=false&netadmin=j
bwadmin@ns$
```

È possibile passare alla fase successiva per analizzare NSPortalLog. Passare alla directory nsportal logging. Per analizzare nsportallog, incollare l'ID utente jliangEntGrp1User5 come parametro -m in bwTrafficParser. Ciò genera un problema relativo all'API della posizione, in cui il server NS non riesce a trovare l'ID utente: 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 Informazioni | HTTP | | HTTPhread-49 | 7669459 | COMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

  tcp - Byte HTTP IN da 10.66.82.113:57078 (ricevuti il 10.66.82.115:80)
  POST http://10.66.82.115/servlet/LocateUser
  Intestazioni:
  ID tracciamento: COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8
  id-correlazione-x-broadsoft: cc6f959b-2507-4792-b158-780c74af0d07
  x-broadworks-protocol-version: 1.1
  content-type: application/x-www-form-urlencoded
  set di caratteri: utf-8
  ...
  host: 10.66.82.115
  accetta: text/html, image/gif, image/jpeg, */*; q=0,2
  connessione: keep-alive
  content-length: 126
  Parametri:

url=jliangEntGrp1User5@sys.cisco.com
returnCompatibleXSP=true
callPRequest=falso
netadmin=jliangEntGrp1User5@sys.cisco.com

bwadmin@ns$ bwTrafficParser -m COMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8 NSPortalLog2026.10.08-00.00.03.txt
2026.10.08 21:28:04:536 AEDT Informazioni | HTTP | | HTTPhread-49 | 7669459 | COMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

tcp - Byte HTTP IN da 10.66.82.113:57078 (ricevuti il 10.66.82.115:80)
POST http://10.66.82.115/servlet/LocateUser
Intestazioni:
ID tracciamento: COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8
id-correlazione-x-broadsoft: cc6f959b-2507-4792-b158-780c74af0d07
x-broadworks-protocol-version: 1.1
content-type: application/x-www-form-urlencoded
set di caratteri: utf-8
agente utente: Java/11.0.29
host: 10.66.82.115
accetta: text/html, image/gif, image/jpeg, */*; q=0,2
connessione: keep-alive
content-length: 126
Parametri:
url=jliangEntGrp1User5@sys.cisco.com
returnCompatibleXSP=true
callPRequest=falso
netadmin=jliangEntGrp1User5@sys.cisco.com

2026.10.08 21:28:04:536 AEDT Debug | | Generico | HTTPhread-49 | 7669460 | COMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

doFilter()

2026.10.08 21:28:04:536 AEDT Debug del campo | | PortalInputChannel | HTTPhread-49 | 7669461 | COMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

Accettazione della richiesta tramite la versione: 1.1 (server a 1.1)

2026.10.08 21:28:04:537 Informazioni | API percorso | | HTTPhread-49 | 7669462 | COMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

tcp 188 HTTP Byte in uscita a 10.66.82.113:57078 (inviato da 10.66.82.115:80)
<?xml version="1.0" encoding="UTF-8"?>

<com.broadsoft.protocols.nsportal.Error detail="URL sconosciuto"
id="2"
summary="Impossibile completare la richiesta"
>
</com.broadsoft.protocols.nsportal.Error>

2026.10.08 21:28:04:537 Informazioni | HTTP | | HTTPhread-49 | 7669463 | COMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8

tcp - HTTP Bytes OUT to 10.66.82.113:57078 (inviato da 10.66.82.115:80)
statusCode=200

Intestazioni:
Opzioni X-Content-Type: nosniff
Protezione X-XS: 1; mode=blocco
ID rilevamento: COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8
ID-CORRELAZIONE-X-BROADSOFT: cc6f959b-2507-4792-b158-780c74af0d07
X-BroadWorks-Protocol-Version: 1.1
Content-Type: testo/html;charset=UTF-8
Transfer-Encoding: a pezzi
Data: GMT, 08 ott 2026 10:28:04
Keep-Alive: timeout=5
Connessione: keep-alive
Server: Server HTTP

Conclusioni

Dopo questa risoluzione dei problemi per identificare l'URL 'sconosciuto' di LocationAPI è la causa principale dell'elevata quantità 200 OK per HTTP POST con formParam

"url=jliangEntGrp1User5%40sys.cisco.com&returnCompatibleXSP=true&callPRequest=false&netadmin=jl
è possibile verificare che l'ID utente jliangEntGrp1User5@cisco.com sia presente in AS solo a causa di un problema di SyncAPI.

Informazioni correlate

- RemoveSensitiveInformationFromNSLocationAndPortalAPIRequestsFD-R2024_01.pdf

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).