Characterize webTrafficParser formParameter, option NS LocationAPI

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Exemple #1 : Profil de trafic

Conclusion

Informations connexes

Introduction

Ce document décrit le filtrage de LocationAPI avec webTrafficParser contre access_log HTTP POST formParameter, puisque NS 2024.01 HTTP GET a été supprimé.

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Privilège administrateur système Cisco BroadWorks.
- Réponse aux demandes d'emplacement NS et d'API Portal.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité aux versions logicielles et matérielles spéciales.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La requête/réponse de l'API d'emplacement peut être suivie en tant qu'enregistrement du journal des requêtes HTTP GET dans Cisco BroadWorks Network Server tomcat access_log. Cette méthode a été remplacée par HTTP POST dans la fonctionnalité 2024.01. Dans cette modification, le journal d'accès tomcat a ajouté le champ formParameters. L'analyseur BroadWorks webTrafficParser intégré a depuis été amélioré pour filtrer et lire ce fieldParameters. Vous pouvez identifier le problème LocationAPI en collant et en analysant le journal d'accès NS tomcat avec webTrafficParser pour l'identifier à partir de la requête HTTP POST et du champ formParameter inclus.

Exemple #1 : Profil de trafic

L'outil webTrafficParser se trouve dans le répertoire 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

Un ou plusieurs fichiers journaux doivent être spécifiés.

Utilisation :

webTrafficParser [-a] [-m <expression régulière>] [-r] [-p <intervalle>] [-t <numéro>] <nom(s) du fichier journal>

Cet outil analyse les journaux d'accès tomcat pour caractériser le trafic entrant.

Liste des options possibles :

-a : imprime la sortie complète (toutes les entrées au lieu des 10 premières)

-m <regexp> : imprime les entrées du fichier journal correspondant à l'expression régulière

-r : affiche des informations basées sur le débit (messages par seconde)

-t <numéro> : imprime les <nombre> premiers éléments

-s <Heure_début> : heure de début du ou des fichiers. Exemple de format pour les heures 30/Jan/2013:19:22:57

La valeur par défaut est la première fois dans un ou plusieurs fichiers.

-e <Heure_fin> : heure de fin du ou des fichiers. La valeur par défaut est la dernière fois dans le dernier fichier.

-p <intervalle> : imprime un profil de trafic du début à la fin d'un intervalle

(en minutes). Il peut être enregistré dans un fichier CSV et représenté sous forme de graphique.

Le script analyse jusqu'à 10 fichiers journaux.

Les noms des fichiers journaux doivent être spécifiés dans l'ordre chronologique.

Collez le journal d'accès NS tomcat d'une période de focus dans webTrafficParser, ce qui renvoie un volume élevé pour une demande d'API d'emplacement d'utilisateur particulière (416 au total) :

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

  ns1-r25.cisco.com LE NOMBRE DE TRAFICS. HEURE DE DÉBUT = 01/Oct/2026:00:00:49. HEURE DE FIN = 08/Oct/2026:21:09:09.

  Durée totale = 677300.000 secondes
  Nombre total de demandes = 33996

  68 Taille moyenne des requêtes (octets)
  641 Taille moyenne des réponses (octets)
  0,002 Temps de réponse moyen (secondes)

  Trafic par méthode HTTP :
  POSTE 22994
  6105 GET
  OPTIONS 4599
  251-
  9 TÊTE
  8 GNUTELLA
  4 certains
  4 NESSUS
  4 PROPFIND
  4 TRACE

  Top 10 par URL :
  22389
  /servlet/GetAllHostingNewNodeAddresses?private=false&broadworksOnly=true&clusterMode=false&callIPRequest=true&request
  Adresses=10.66.82.113
  4599 *
  781/
  416 /servlet/LocateUser?url=jliangEntGrp1User5%40syd.cisco.com&returnCompatibleXSP=true&callIPRequest=true
  251-
  126 /Connexion/
  92 /login
  88 /images

  52 /login.html
  38 /index.html

  10 premiers par adresse :
  22833 10.66.82.13
  4587 10.66.82.105
  3288 <certaines adresses IP publiques>
  3288 <autre adresse publique>

  Top 10 par code de retour :
  27554 200
  5077 302
  804 404
  553 400
  4 403
  4 405

  10 premiers par ID utilisateur :
  33996-

  10 premiers par agent-utilisateur :
  ...

bwadmin@ns$

Collez l'ID utilisateur « jliangEntGrp1User5 » en tant que paramètre de l'option -m dans webTrafficParser. Ceci renvoie l'ID utilisateur particulier dans le champ 15 des entrées du journal d'accès. Le champ 15 est formParameters de la requête HTTP POST.

```
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
"BWCALLCENTER_
220f25f7-7353-4d4b-960a-4b3136897297" 10.66.82.115 80
"url=jliangEntGrp1User5&returnCompatibleXSP=true&callPRequest=false&netadmin=jli
angEntGrp1Utilisateur5"
...
10.66.82.113 - - [08/Oct/2026:21:28:04 +1100] "POST /servlet/LocateUser HTTP/1.1" 200 126 199 0.002
"COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8" 10.66.82.115.80
"url=jliangEntGrp1User5%40sys.cisco.com&returnCompatibleXSP=true&callPRequest=false&netadmin=j
bwadmin@ns$
```

Vous pouvez passer à l'étape suivante pour analyser le NSPortalLog. Accédez au répertoire de journalisation nsportal. Vous collez le paramètre userId jliangEntGrp1User5 en tant que paramètre -m dans bwTrafficParser pour analyser nsportallog. Il en résulte un problème d'API d'emplacement, où le NS ne peut pas trouver l'ID utilisateur : 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 de 10.66.82.113:57078 (reçu le 10.66.82.115:80)
  PUBLIEZ À L'ADRESSE http://10.66.82.115/servlet/LocateUser
  Header (En-tête) :
  trackingid : COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8
  x-broadsoft-corrélation-id : cc6f959b-2507-4792-b158-780c74af0d07
  x-broadworks-protocol-version : 1.1
  content-type : application/x-www-form-urlencoded
  jeu de caractères : utf-8
  ...
  hôte : 10.66.82.115

accept (accepter): text/html, image/gif, image/jpeg, */*; q = 0,2
connexion: keep-alive
content-length : 126
Paramètres :
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 de 10.66.82.113:57078 (reçu le 10.66.82.115:80)
PUBLIEZ À L'ADRESSE http://10.66.82.115/servlet/LocateUser
Header (En-tête) :
trackingid : COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8
x-broadsoft-corrélation-id : cc6f959b-2507-4792-b158-780c74af0d07
x-broadworks-protocol-version : 1.1
content-type : application/x-www-form-urlencoded
jeu de caractères : utf-8
user-agent : Java/11.0.29
hôte : 10.66.82.115
accept (accepter): text/html, image/gif, image/jpeg, */*; q = 0,2
connexion: keep-alive
content-length : 126
Paramètres :
url=jliangEntGrp1User5@sys.cisco.com
returnCompatibleXSP=true
callPRequest=false
netadmin=jliangEntGrp1User5@sys.cisco.com

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

doFilter()

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

Acceptation de la demande avec la version : 1.1 (serveur à 1.1)

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

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

<com.broadsoft.protocols.nsportal.Error detail="URL inconnue"
id="2"
summary="Impossible de terminer la demande"
>
</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 vers 10.66.82.113:57078 (envoyé depuis 10.66.82.115:80)
statusCode=200
Header (En-tête) :
X-Content-Type-Options : bouffe
Protection X-XSS : 1; mode=bloc
ID de suivi : COMMPILOT_64dadd43-ba66-4805-b397-abd3a7d512a8
X-BROADSOFT-CORRELATION-ID : cc6f959b-2507-4792-b158-780c74af0d07
Version du protocole X-BroadWorks : 1.1
Type de contenu : text/html;charset=UTF-8
Transfert-Encodage : fragmenté
Date : jeu, 08 oct. 2026 10:28:04 GMT
Maintien de la connexion : timeout=5
Connexion: keep-alive
Serveur : Serveur HTTP

Conclusion

Après ce dépannage pour identifier le LocationAPI 'Unknown URL' est la cause racine de la quantité élevée 200 OK pour HTTP POST avec formParam

"url=jliangEntGrp1User5%40sys.cisco.com&returnCompatibleXSP=true&callPRequest=false&netadmin=jl
vous pouvez vérifier que l'ID utilisateur jliangEntGrp1User5@cisco.com existe dans AS uniquement en raison d'une difficulté SyncAPI.

Informations connexes

- RemoveSensitiveInformationFromNSLocationAndPortalAPIRequestsFD-R2024_01.pdf

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.