

splunk>enterprise App Administrator 1 Messaggi Impostazioni Attività Guida Trova

Ricerca Analytics Set di dati Report Allarmi Dashboard

Nuova ricerca

Salva come Crea vista tabella Chiudi

source="tutorialdata.zip:*" sourcetype="*" "500" Da 01/11/24 fino a 30/11/24

✓ 130 eventi (01/11/24 00:00:00,000 - 01/12/24 00:00:00,000) Nessun campionamento degli eventi

Processo

Eventi (130) Pattern Statistiche Visualizzazione

Formato timeline Zoom indietro Zoom area selezionata Deseleziona 1 giorno per colonna

Elenco Formato 50 per pagina

< Nascondi campi Tutti i campi

CAMPI SELEZIONATI

- host 1
- source 3
- sourcetype 1

CAMPI INTERESSANTI

- action 5
- bytes 63
- categoryid 2
- clientip 55
- date_hour 19
- date_mday 1
- date_minute 42
- date_month 1
- date_second 40
- date_wday 1
- date_year 1

| i | Ora | Evento |
|---|--------------------------|---|
| > | 01/11/24 18:18:59,000 | 198.35.1.75 - - [01/Nov/2024:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&JSESSIONID=SD10SL2FF4ADFF53099 HTTP/1.1" 500 2324 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 645 host = dati_test source = tutorialdata.zip:/www/access.log sourcetype = access_combined_wcookie |
| > | 01/11/24 18:18:59,000 | 198.35.1.75 - - [01/Nov/2024:18:18:59] "GET /cart.do?action=addtocart&itemId=EST-13&JSESSIONID=SD10SL2FF4ADFF53099 HTTP/1.1" 500 2324 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 645 host = dati_test source = tutorialdata.zip:/www/access.log sourcetype = access_combined_wcookie |
| > | 01/11/24 18:18:55,000 | 198.35.1.75 - - [01/Nov/2024:18:18:55] "GET /product.screen?productId=SF-BVS-G01&JSESSIONID=SD10SL2FF4ADFF53099 HTTP/1.1" 500 2809 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 370 host = dati_test source = tutorialdata.zip:/www/access.log sourcetype = access_combined_wcookie |
| > | 01/11/24 18:18:55,000 | 198.35.1.75 - - [01/Nov/2024:18:18:55] "GET /product.screen?productId=SF-BVS-G01&JSESSIONID=SD10SL2FF4ADFF53099 HTTP/1.1" 500 2809 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 370 |

Conclusioni ChatGPT:

- **Volume degli errori 500:** Sono presenti **130 eventi** che riportano errori HTTP 500 tra il 1° novembre 2024 e il 1° dicembre 2024. Un numero così elevato di errori interni può indicare un problema persistente o periodico nel sistema, che potrebbe avere un impatto significativo sull'esperienza utente.
- **Richieste specifiche con errori:** Le richieste problematiche sembrano riguardare diverse funzionalità dell'applicazione, come:
 - Endpoint /cart.do?action=addtocart&itemId=EST-13
 - Endpoint /product.screen?productId=SF-BVS-G01&itemId=EST-14
- Questi endpoint sembrano essere collegati a **funzionalità di aggiunta al carrello e dettagli di prodotto**, suggerendo che l'errore potrebbe essere legato al sistema di e-commerce o alla gestione dei prodotti.
- **Origine delle richieste:** Tutte le richieste sembrano provenire dall'IP 198.35.1.75. Questo potrebbe indicare un comportamento anomalo da parte di un singolo utente, come un bot che sta eseguendo test automatizzati o una singola sessione utente che incontra ripetutamente un errore sul server. In alternativa, se questo IP appartiene a un server di proxy, potrebbe rappresentare un numero maggiore di utenti.
- **Dettagli della richiesta e del browser:** Le richieste sono fatte con Chrome/19.0.1084.46 su Windows NT 6.1. Questo browser è una versione molto vecchia di Chrome, il che potrebbe indicare un bot o uno script automatizzato, piuttosto che un utente reale.
- **Possibili cause dell'errore HTTP 500:**
 - **Problemi nell'applicazione:** Gli errori 500 possono essere causati da bug nel codice dell'applicazione, come errori di logica, chiamate a funzioni non gestite correttamente, o dipendenze non disponibili (es. database o API esterne).
 - **Configurazioni errate:** Potrebbe esserci un problema di configurazione nel server applicativo, come impostazioni non corrette per la gestione delle sessioni o dei dati del carrello.

- **Sovraccarico del server:** Se l'IP 198.35.1.75 rappresenta un traffico elevato o un bot, potrebbe sovraccaricare il server con richieste ripetitive, causando temporaneamente errori interni.

Azioni consigliate:

- **Esaminare i log applicativi:** Verificare i log dettagliati dell'applicazione per diagnosticare la causa specifica dell'errore HTTP 500 sugli endpoint /cart.do e /product.screen. Gli errori interni spesso sono accompagnati da messaggi di errore espliciti nel log applicativo, che possono fornire ulteriori dettagli.
- **Limitare l'accesso da IP sospetti:** Se l'IP 198.35.1.75 continua a generare traffico eccessivo e richieste problematiche, considerare di limitare o bloccare temporaneamente l'IP per ridurre il carico e proteggere il server.
- **Monitoraggio delle performance:** Implementare un sistema di monitoraggio che segnali tempestivamente l'aumento di errori HTTP 500, così da poter intervenire proattivamente prima che il problema si aggravi.
- **Ottimizzazione della gestione degli errori:** Se l'applicazione continua a rispondere con errori 500, potrebbe essere utile rivedere la gestione degli errori, implementando messaggi di errore più specifici e dettagliati che permettano una diagnosi più immediata.

In sintesi, questa schermata indica la presenza di un problema ricorrente sul server, che porta a errori 500 su endpoint di e-commerce. Un'analisi più dettagliata dei log e un'indagine sulla configurazione e sulla gestione del traffico da IP sospetti potrebbero aiutare a mitigare il problema.