



Predict, Sanke Diagrams, and advanced Alerts

Predict

Transaction

Alerts

Predict

- To understand **future trends** based on your existing data
 - ex) Labs/Apache/Access logs looking for status_code 404 for the last 60 minutes.
 - Sliced by 1-minute increments
 - count your 404 status codes by timeslice.
 - Predict future trend of 404s in 1-minute increments and plot results on a line graph.

```
_sourceCategory=Labs/Apache/Access status_code=404  
| timeslice 1m  
| count(status_code) as error_count by _timeslice  
| predict error_count by 1m
```

Transaction

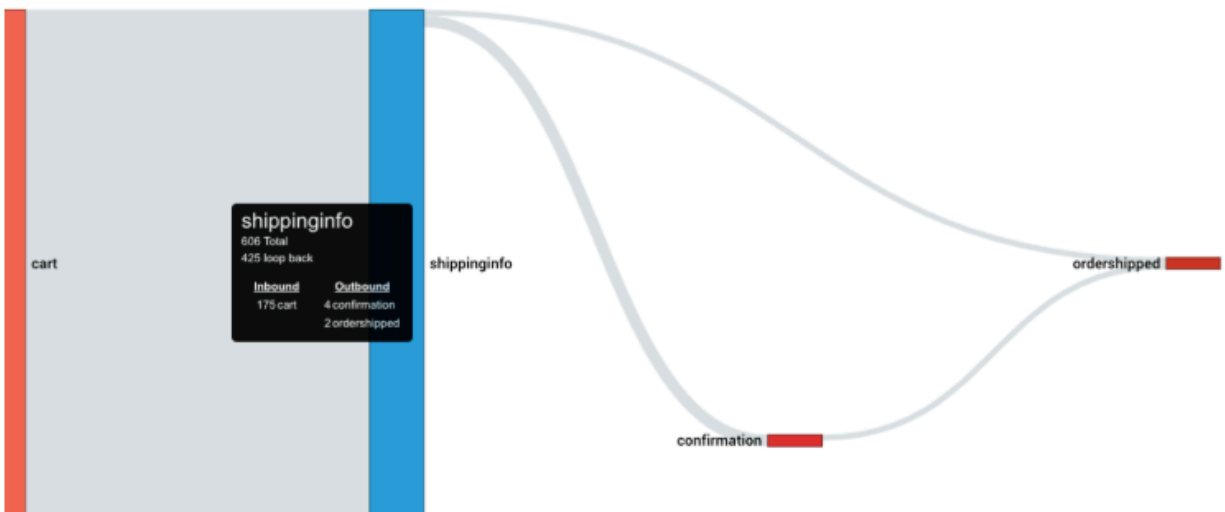
- Allows you to **analyze related sequences of messages** based on a unique transaction identifier such as a **SessionID** or **IP Address**

- **Transaction** uses the unique identifier you specify to group related messages together and arrange them based on states which you define.
- ex) Search using the transaction operator to capture some possible states using IP address as the unique identifier

```

_sourceCategory=Labs/ecommark
| parse regex "(?<ip>0-9 {1,3}\.0-9 {1,3}\.0-9 {1,3}\.0-9 {1,3})" nodrop
| transaction on ip
  with "*/confirmation*" as confirmation,
  with "*Order shipped*" as ordershipped,
  with "*/cart*" as cart,
  with "*/shippingInfo*" as shippinginfo,
  with "*/billinginfo*" as billinginfo
results by flow
| count by fromstate, tostate

```



Alerts

- ex) Query to use if you want to be notified if 404 response increases

```

_sourceCategory=Labs/Apache/Access (status_code=200 or status_code=404)

```

```
| timeslice 1m  
| if (status_code = "200", 1, 0) as successes  
| if (status_code = "404", 1, 0) as fails  
| sum(successes) as success_cnt, sum(fails) as fail_cnt by _timeslice  
| (fail_cnt/(success_cnt+fail_cnt)) * 100 as failure_rate_pct  
| sort _timeslice desc  
| outlier failure_rate_pct window=5, threshold=3, consecutive=1, direction=+  
| where failure_rate_pct_indicator > 0
```