The Economy of World of Warcraft

Making Millions of Gold and How Blizzard Knows You’re Doing It, Using Splunk!

Shawn Routhier
Sr. Security Engineer | Blizzard Entertainment
During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.
Shawn Routhier
Senior Security Engineer | Blizzard Entertainment
Shawn Routhier
Human Rogue

Blizzard Entertainment - 5 years
  • Security Professional for 11+ years… and counting
    - Booz Allen Hamilton, MIT – Lincoln Laboratory, Blizzard Entertainment

NPC “Shawn” in Nagrand (Outland)
  • Met and proposed to my wife in WoW

Defcon25 Black Badge (Uber) Winner – Telephreak

Southern California User Group Leader

.Conf19 Speaker – Winning in Starcraft 2
Disclaimer

I’m not a WoW Dev

• I work on the Security Team at Blizzard
• I do not have any direct or indirect influence on World of Warcraft or it’s development
• I cannot provide non-public information regarding Blizzard, World of Warcraft, etc.
  – For these questions, please email: pr <at> blizzard.com
• Please feel free to contact me with Splunk, Security, or WoW Economy-related questions
  – @0xShawn
  – Clock on Splunk Usergroups Slack
Agenda

I’d like you to learn:

• Methodologies to normalize 100’s of millions of events
• Parallels with SecOps, NetOps, SysOps, FraudOps
• Roadblocks, limits, & lessons learned
• Interesting WoW Metrics!

1. World of Warcraft
2. Organizing the Objective
3. Summary Indexing & Lookups
4. Datamodes
5. Interesting WoW Metrics
World of Warcraft

In the Age of Chaos, two factions battle for dominance!

World of Warcraft (2004); Classic (2019)

Massive Multi-Player Online Roleplaying Game (MMORPG)
• A networked role-playing game where a player adopts the role of a hero battling for their cause
• WoW is a high-fantasy themed game where players can adventure, dungeon delve, fight epic bosses, treasure hunt, or even go fishing!

Economy
• 10 Million+ pseudo-financial transactions per day
• An interesting data set for a universal problem
WORLD OF WARCRAFT™
Abstract

• Correlating 100,000,000+ million events is difficult to scale with traditional SPL and search methods
• Utilizing summary indexing, lookups, and accelerated data models we can pre-calculate & correlate fields to reduce system resources used to search
• Methods to correlate thousands of events do not scale to hundreds of thousands.

World of Warcraft Economy
21 billion gold moves through WoW each day!
Organizing the Objective

Leeeeeeeroy Jenkins…

Process Oriented

• Requirements Gathering
  – Individual / team goals, expectations, ease of use, etc.
  – Dashboards, reporting, automation, integrations, etc.

• Objective Planning
  – “Simple, done well” – unknown
  – Ad-Hoc data enrichment & correlation
  – Frequency of summary index builders
  – Granularity for timeseries data
  – Lookup Insertion (Index-time OR search-time)

• Writing the SPL

• Iteration
  – Most difficult part: Knowing when to stop iterating

• Finalizing Knowledge Objects
Iterations

“Maybe we need another Healer?”

Breakdown of Efforts
- Requirements & Knowledge Objects – 5%
- Objective Planning – 45%
- SPL & Iteration – 50%

Major Refactors
- Dynamic Correlation -> Lookups
  – Reduced auto-finalization by 99%
- Item Value Overhaul
- Auction House update in v8.3
  – Required a new SI & correlation of two sourcetypes
- Item Value Overhaul 2.0
## WoW Event Metrics

Summarizing & Accelerating at the Cost of Bag Space

<table>
<thead>
<tr>
<th>Format</th>
<th>Simple WoW _raw</th>
<th>Summary Index</th>
<th>Accelerated Datamodel</th>
<th>Lookup</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>JSON Structured _raw</td>
<td>KV Pair Structured _raw</td>
<td>Distributed TSIDX</td>
<td>CSV &amp; KVStore</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Location</th>
<th>Indexers</th>
<th>Indexers</th>
<th>Indexers</th>
<th>Search Heads Indexers • Replicated</th>
</tr>
</thead>
</table>

### Sample Search*

<table>
<thead>
<tr>
<th>Format</th>
<th>Simple WoW _raw</th>
<th>Summary Index</th>
<th>Accelerated Datamodel</th>
<th>Lookup</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>13,049,509,333 events 1,095.672 seconds</td>
<td>1,128,401,289 events 75.74 seconds</td>
<td>1,207,380,543 events 1.883 seconds</td>
<td>24,135,465 rows 210.079 seconds</td>
</tr>
</tbody>
</table>

| Notes | • 90d retention  
• 95% of searches using >1 sourcetype would auto-finalize (fail) | • 97.23% reduction of storage  
• 24mon retention  
• By default, event distribution is poor with Summary Indexing | • 90d acceleration  
• 600 GB TSIDX with indexed buckets | • Efficient correlation  
• Enrich Summary Indexing  
• Offload common static fields |

*All _raw & tstats searches are equivalent to: <base search> | bin span=1d _time | stats count by _time*
Data Flow Chart
As easy as playing Feral Druid
Summary Indexing
A Division of SI:7

Benefits
• Distribute computation expensive SPL to increase efficiency for extended timespan searches
• Normalize, correlate, lookup, and calculate fields at summary ingest
• Summary indexes have the same capabilities as a traditional index
  – Independent RBAC
  – Increased Retention
• Metricizing data
  – Economy data had a 97% _raw reduction

Drawbacks
• Summary time is reliant on scheduled interval
• Data redistribution is limited
  – Summary index events are written to disk as a “.stash_new” file
  – Default 30s load balance interval
• Changes to data are long-term investments
• Utilizing | Collect will also utilize license
• Unplanned execution of the summary builder will skew metrics
Summary Indexing
Auction SI Builder

earliest=-35m@m latest=-5m@m index=risk_wow sourcetype=blizzard:wow:auctionhouse message_name=AuctionHouse
stats sum(payload.gold) as auctionGold sum(payload.item.stack_count) as auctionStacks by payload.from.bnet_guid, payload.from.player_guid, payload.item.enchants, payload.item.entry, payload.to.player_guid, payload.wow_context.realm_context.native_realm.realm_id, payload.wow_context.realm_context.native_realm.realm_region, payload.wow_context.realm_context.native_realm.realm_site
rex field=payload.item.enchants "^Ench:(?<itemEnchant>.*):\sGems:(?<itemGems>.*):\sMods:(?<itemMods>.*):\sRandomPropertiesID:((?<itemPropsIDs>.*):\sContext:(?<itemContext>.*):\sBonuses:(?<itemBonuses>.*):\s)\$"
rex field=itemMods "mod = 3, value = (?<petID>\d+)"
fields - payload.item.enchants
rename payload.from.bnet_guid as "sellerBNet", payload.from.player_guid as "sellerID", payload.item.entry as "itemID", payload.to.player_guid as "buyerID", payload.wow_context.realm_context.native_realm.realm_id as "realmID", payload.wow_context.realm_context.native_realm.realm_region as "realmRegion", payload.wow_context.realm_context.native_realm.realm_site as "realmSite"
eval auctionGoldPerItem=floor(auctionGold/auctionStacks)
lookup WoW econ_itemID.csv itemID OUTPUT itemQuality itemBonding itemVendorBuy itemVendorSell itemDeleted
eval petID=if(petID="-NONE-", 0, 'petID')
fillnull value="0" petID
eval _time=now()
table _time, sellerBNet, sellerID, buyerID, realmID, realmRegion, realmSite, itemID, itemQuality, itemBonding, auctionGold, auctionStacks, auctionGoldPerItem, itemEnchant, itemGems, itemMods, itemPropsIDs, itemContext, itemBonuses, itemVendorBuy, itemVendorSell, itemDeleted, petID
collect index=wow_economy sourcetype=blizzard:wow:economy:auction
Summary Indexing
Commodity Auction SI Builder

earliest=-35m latest=-5m index=risk_wow message_name=AuctionEnd payload.reason IN (AUCTION_END_REASON_WON_BY_BID, AUCTION_END_REASON_BUYOUT)
| fields _time, message_name, payload.*, region
| rename payload.item_info().owner_context.* as seller_, payload.item_info().* as seller_, payload.buyer_context.* as buyer_, payload.transaction_context
| realm_context.native_realm.* as *
| eval seller_info = mvzip(seller_game_account_guid, seller_player_guid)
| eval seller_info = mvzip(seller_info, seller_item_id)
| eval seller_info = mvzip(seller_info, seller_stack_size_consumed)
| fields _time, message_name, buyer_bnet_account_id, buyer_game_account_guid, buyer_player_guid, seller_info, payload.sold_amount, payload.rake, payload.quantity, realm_id, realm_site, realm_region
| mexpand seller_info
| rex field=seller_info "\[\?seller_game_account_guid\[\^,\]+\],\?seller_player_guid\[\^,\]+\],\?seller_item_id\[\^,\]+\],\?seller_stack_size_consumed\[\^,\]+\]
| eval auctionGold = floor('payload.sold_amount' / 'payload.quantity' * 'seller_stack_size_consumed')
| 'comment("Removed the Rake calculation as it impacts historical item value by 10\%")'
| eval auctionGoldPerItem = floor('auctionGold' / 'payload.quantity')
| rename buyer_bnet_account_id as buyerBNet, buyer_game_account_guid as buyerWoW, buyer_player_guid as buyerID, seller_game_account_guid as sellerWoW, seller_player_guid as sellerID, seller_item_id as itemID seller_stack_size_consumed as auctionStacks, realm_id as realmID, realm_region as realmRegion, realm_site as realmSite
| lookup WoW Econ itemID.csv itemID OUTPUT itemQuality itemBonding itemVendorBuy itemVendorSell itemDeleted
| eval _time=now()
| table _time, seller WoW, sellerBNet, buyer WoW, buyerID, realm WoW, realmWoW, realmRegion, realmSite, itemID, itemQuality, itemBonding, auctionGold, auctionStacks, auctionGoldPerItem, itemVendorBuy, itemVendorSell, itemDeleted
| collect testmode=f index=wow_economy sourcetype=blizzard:wow:economy:commodity
## Lookups

/who

<table>
<thead>
<tr>
<th>itemID</th>
<th>itemName</th>
<th>itemDesc</th>
<th>itemLevel</th>
<th>itemQuality</th>
<th>itemBonding</th>
<th>itemDeleted</th>
<th>itemVendorBuy</th>
<th>itemVendorSell</th>
<th>itemHoliday</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Martin Fury</td>
<td>Test Martin Fury Programmer Test DO NOT DELETE</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>28</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Worn Shortsword</td>
<td>1H Starting Sword 01</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>18</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>Bent Staff</td>
<td>2H Starting Stave 01</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>24</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Worn Mace</td>
<td>Starting Mace</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>19</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>Worn Axe</td>
<td>1H Starting Axe 01</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>19</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>Recruit's Shirt</td>
<td>Starting Shirt Human Dwarf Gnome Warrior Undead</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>Recruit's Pants</td>
<td>Starting Pants Human Dwarf Gnome Warrior</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>13</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>Recruit's Boots</td>
<td>Starting Boots Human Dwarf Gnome Undead Warrior</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>OLDRRecruit's Belt</td>
<td>HuWa Starting Belt 01</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>OLDSquire's Belt</td>
<td>HuPa Starting Belt 01</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

### Benefits

- Translating programmatic IDs to human-readable
- Enrichment at summary index generation
- Default distribution of lookups to indexers
  - Note: Be careful on frequency of automated lookup builders.
Datamodels
+ 20 Haste

Benefits
• Datamodels (DM) fields
  – Calculated fields using Eval
  – Automated lookup fields
• Extremely fast
  – 1.2 Billion events in 1.883 seconds

Drawbacks
• Learning curve
• Modifications require datamodel to be decelerated
Lessons Learned

Did Someone Say [Thunderfury, Blessed Blade of the Windseeker]?

SPL & Process

• “Simple, Done Well”
• Frequency of summary index builders
  – Meeting granularity requirements and expectations
• Correlation with Join or Subsearch is near-impossible
  – 50,000 & 10,000 event limits, by default
• Write a CIM for your data

Replication Configs

• distsearch.conf
  [replicationSettings]
  excludeReplicatedLookupSize = 50
• collections.conf
  [wowecon_current_itemvalue]
  replicate = false

Users

• Set expectations early. This is not a simple undertaking. Give yourself enough time.
• Users want to help. Plan accordingly.
Item Tracking

Proof of Concept...

Premise for Automated Detection

- Historical & Trends
- Outliers
- Monitoring Accounts
Opening the Gates of Ahn’Qiraj
Silithid Carapace Fragments Sold on AH per Region
When to Sell?

Day of Week & Time of Day (UTC) Auction Volume

Note: Splunk Created “Punchcard” Viz
Who’s Buying?

WTB Blacksmith Hammer PST

Visualizing Relationships

• Anomalous purchasing behaviors
  – Purchasing above expected values
• Automating detections of Gold Sellers
  – Maintaining Monitoring via Lookup & DMA
## Applicability

### + 20 Versatility

<table>
<thead>
<tr>
<th>Security</th>
<th>Network</th>
<th>System</th>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Authentication</td>
<td>• Network Sessions</td>
<td>• Databases</td>
<td>• None</td>
</tr>
<tr>
<td>• Endpoint</td>
<td>• Network Resolution</td>
<td>• Inventory</td>
<td>• Make your own!</td>
</tr>
<tr>
<td>• Malware</td>
<td>• Network Traffic</td>
<td>• Updates</td>
<td></td>
</tr>
<tr>
<td>• Vulnerabilities</td>
<td>• Web</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Existing Datamodels
- Splunk CIM app on Splunkbase (required for ES)
- Extensive Documentation on CIM

### Use Cases
- New Authentication
- New Services, Daemons, Reg Keys, etc.
- New Executables Downloaded
- Traffic to New IPs or Domains
- Change Control Validation
- New Public-facing IPs
- Payment Fingerprinting
  - bin, billing, currency, ip, isp, pos
- In-Game Detections
Thank You

Please provide feedback via the SESSION SURVEY