Protect 2013

Tips for effective ESM ArcSight rules

Anurag Singla

Sr. Manager, R & D

Topics

- New rule types (lightweight, pre-persistence)
- Rule event processing
- Condition ordering
- Variable processing
- Consume after match

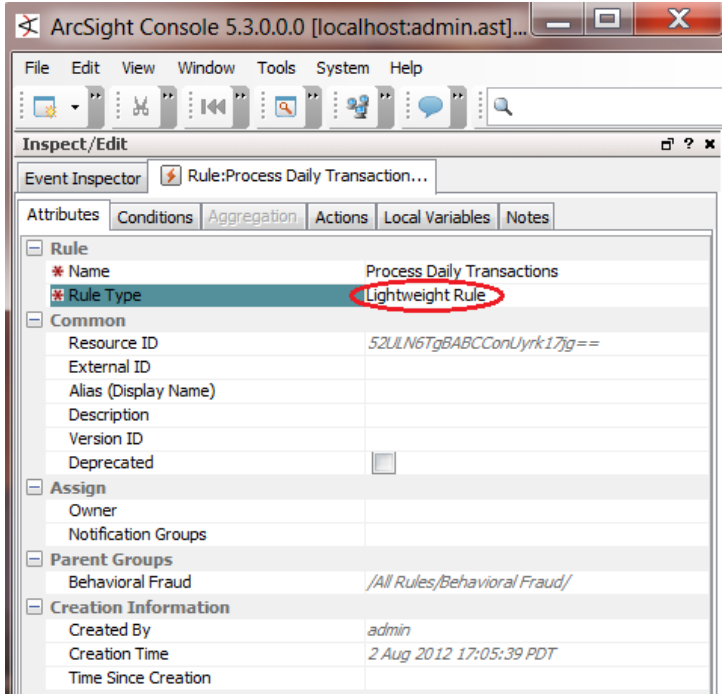
Lightweight rules

Designed for data list maintenance

- No correlation or audit event when rule fires
- No aggregation (stateless)
- Can match large # events and not get disabled

Allow separation of data maintenance and risk analysis logic.

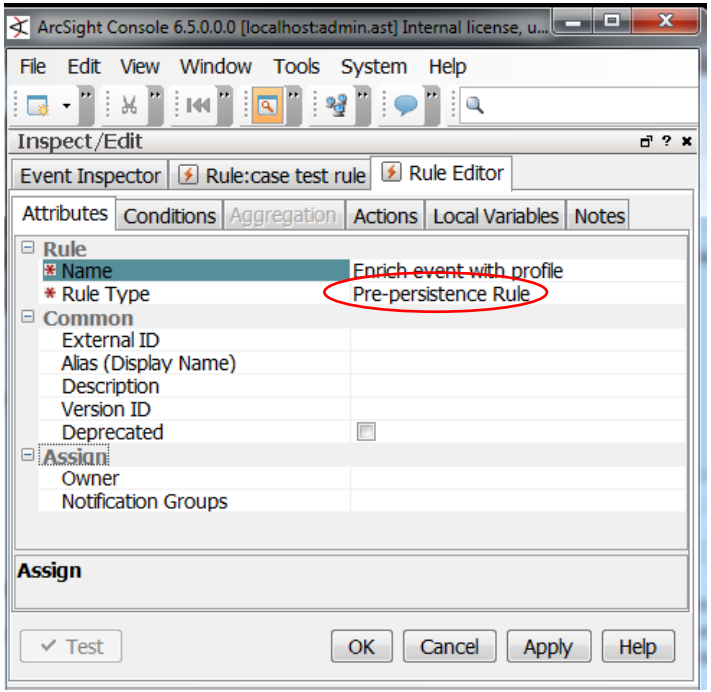
- Processed earlier than regular rules.
- Lightweight rule actions executed *before* regular rule conditions are evaluated.



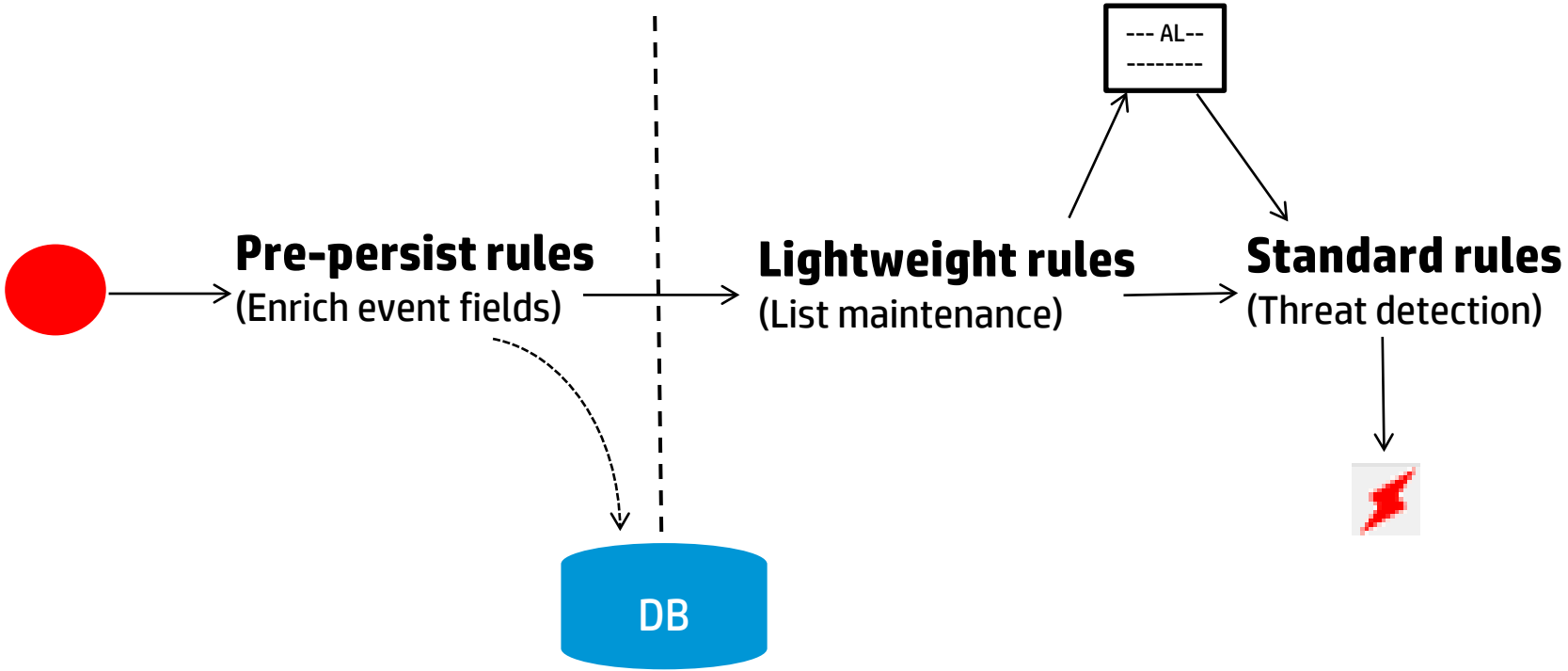
Pre-persistence rules (ESM 5.5)

Designed for event enrichment

- No correlation/audit event, aggregation
- Only action is SetEventField
- SetEventField actions processed *prior* to event persistence
- Enriched field values available to rules that are evaluated post-persistence



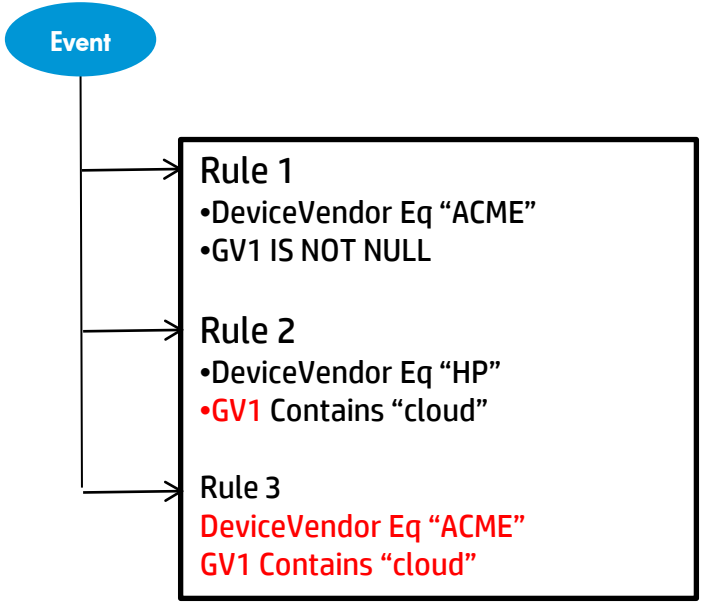
Rules in the event flow



Rule event processing

For every event received by ESM Manager, every deployed rule's conditions are evaluated against the event to determine partial match

- Identical conditions evaluated once (field, op, value)
- Global variables evaluated once
- Variables evaluated lazily



Condition evaluation

- Within AND/OR node, conditions evaluated in order of appearance until result determined
- Order conditions from cheapest to most expensive
- Tiebreaker:
  - Inside AND: order *from most to least* restrictive
  - Inside OR: order *from least to most* restrictive

Condition evaluation (cont.)

Cost of conditions evaluation

- Integer comparison, null test
- String equals
- String comparison (contains)
- Conditions on variables (cheap functions)
- InActiveList conditions
- Matches operator (depends on regex)
- Conditions on variables (expensive functions)
- MatchesFilter condition (depends on filter)

Variable processing

Function execution time varies widely

- Fastest: simple String and Arithmetic functions (ToUpperCase, Add, Subtract)
- Medium: Velocity, JME, Conditional evaluation, Get[Active/Session]ListValue
- Expensive: GetGroupsOfAsset, FormatGroupsOfAsset
- Most expensive: chains of expensive variables, GetListValue on partially cached AL

Other tips

Use global variables

- Global variables: sharable resources, can be reused in many rules.
- Local variables: local to a rule (could be copied to other rules but not shared)
- GV is evaluated *only once per event*, regardless of how many rules use it.

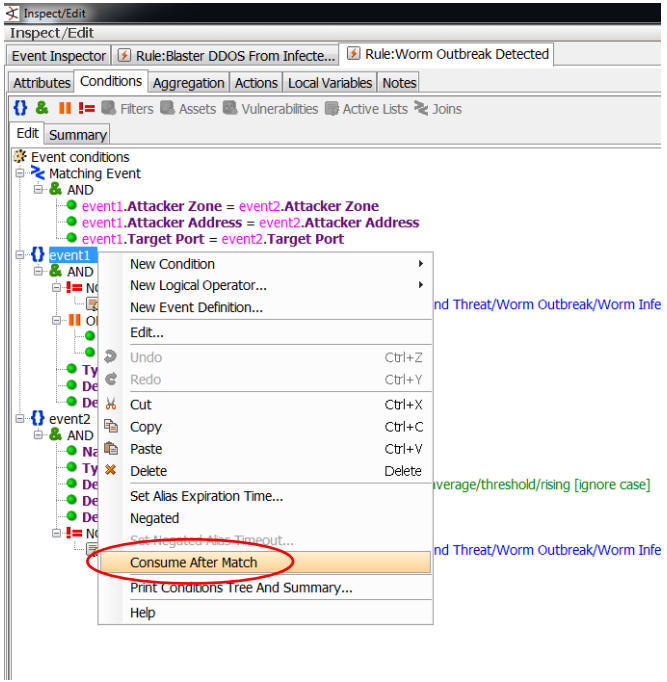
Reduce frequency of rule firings

- Use triggers OnFirstThreshold, OnTimeUnit, OnTimeWindowExpiration

Join rules

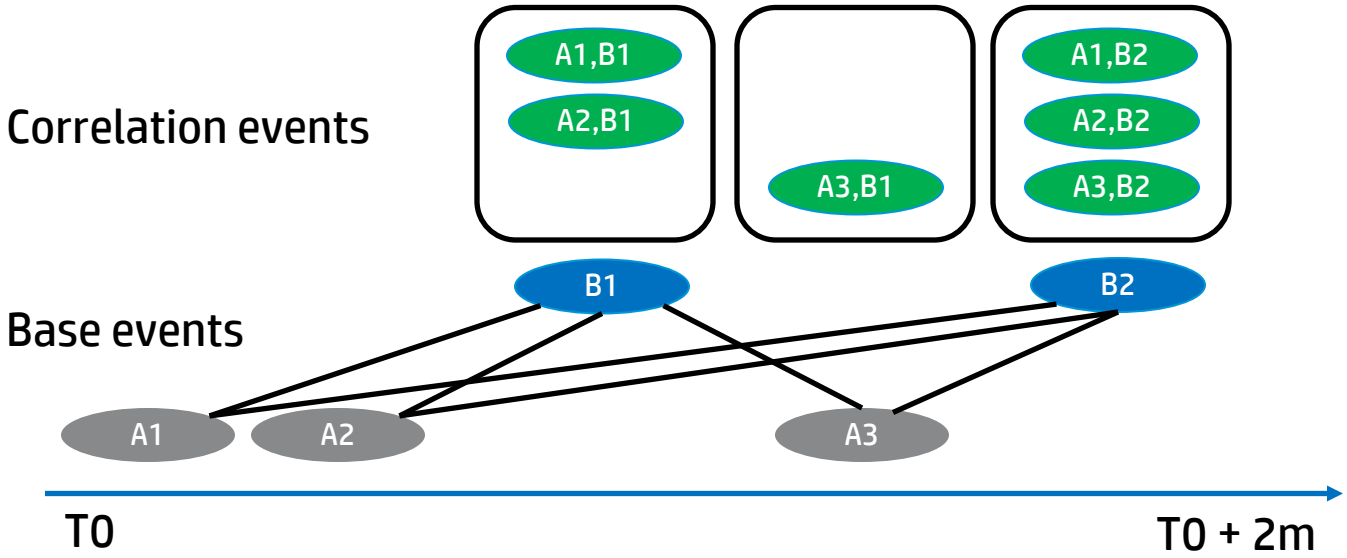
Flag: “Consume after match”

- Default behavior in join rule: once an event matches a rule alias, it stays in working memory, and continues to combine with events matching other aliases until the event expires.
- Consume event property means: consume this event (don’t perform additional joins) once it has been used to fire the rule.
  - Event consumed within specified rule, can still match other rules
  - Can reduce number of correlation alerts



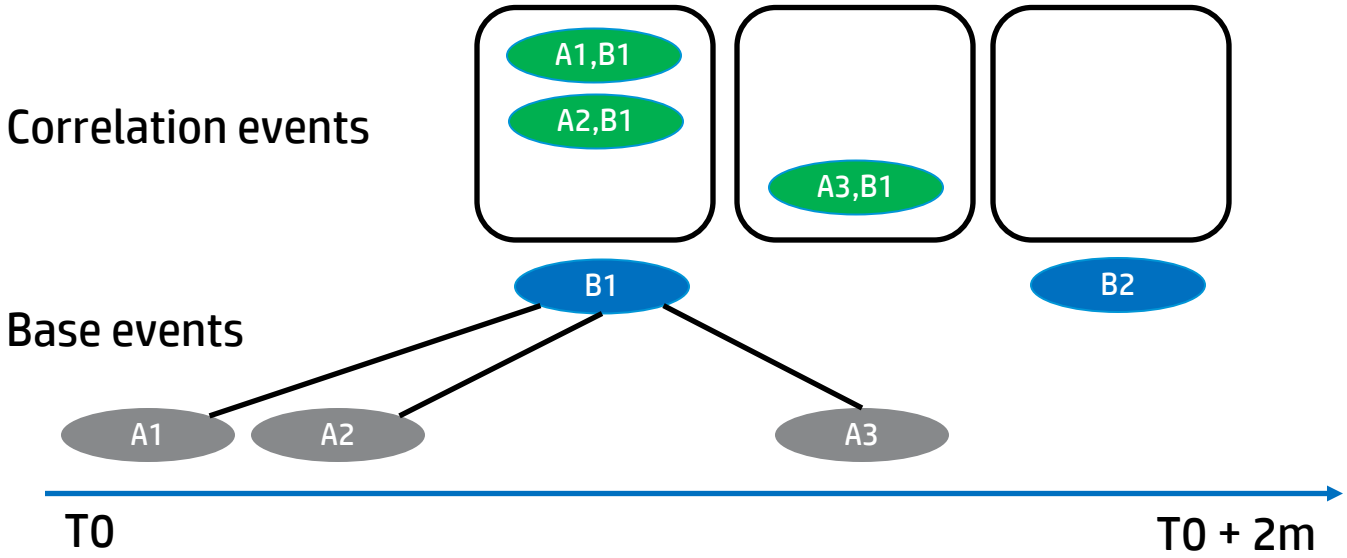
Consume event: example

Alias A (consume = false)
Alias B (consume = false)
Time window = 2m



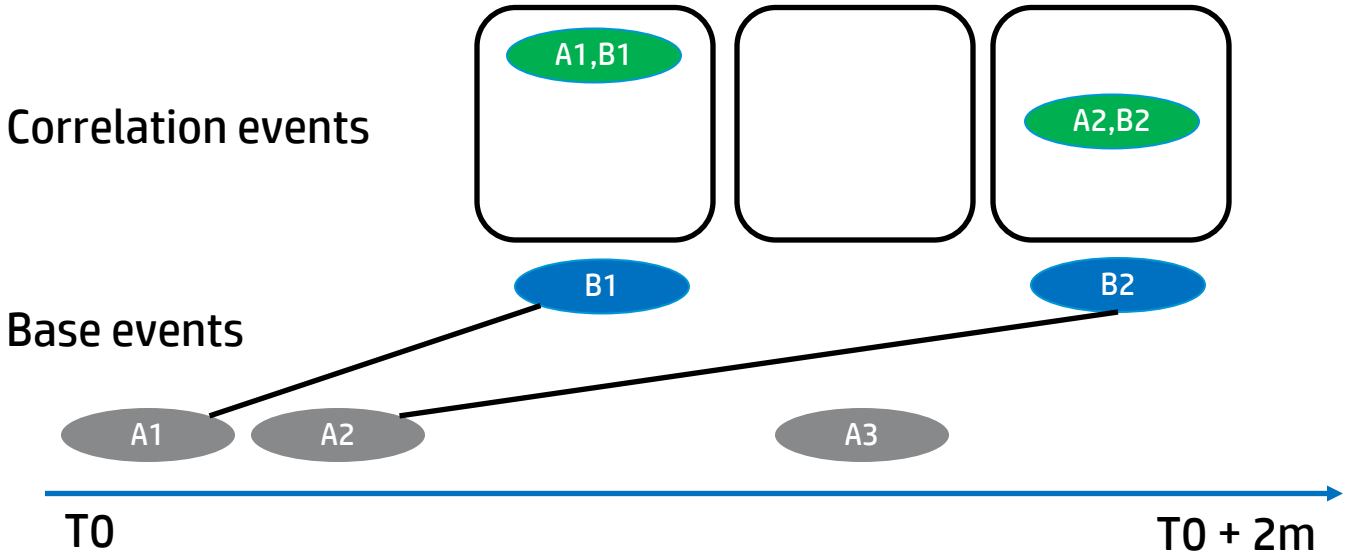
Consume event: example

Alias A (consume = **true**)
Alias B (consume = false)
Time window = 2m



Consume event: example

Alias A (consume = **true**)
Alias B (consume = **true**)
Time window = 2m



Thank you

Protect 2013

Security for the new reality