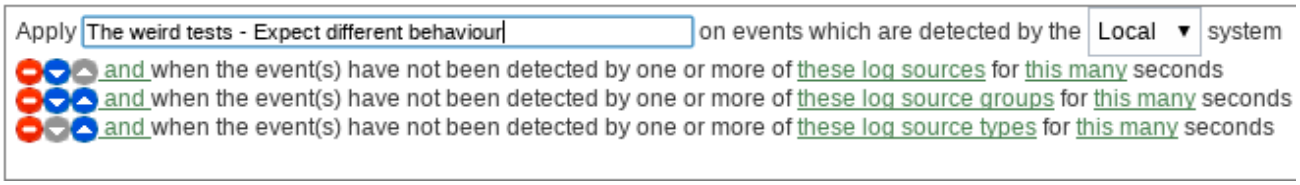
Device Stopped Sending Events
Re-implement through controllable content
v0.1

Purpose:

The purpose of this document is to describe a more workable and usable solution of the "device stopped sending events" (DSSE) test. The current test has three forms:



Problem:

The CRE is based on the presence of events. These tests are based on the absence of events! So many of the typical CRE-isms (read: actions, responses, other tests and filters in the same rule, etc..) are not available and just don't work. There are many RTC items surrounding this and many customer complaints – so there has to be a better way!

The main use case that will be addressed in the solution will be where multiple log sources are acting in an HA-type environment and no notification is necessary as long as at least one of those log sources are active and sending events. No notification is required until ALL of the log sources have stopped sending events for a period of time.

Solution:

So – we will create some new content that will mimic the behaviour of the DSSE tests.

The idea is:

Have 2 generic rules test against and populate 2 separate reference data containers (modified to suit use case).

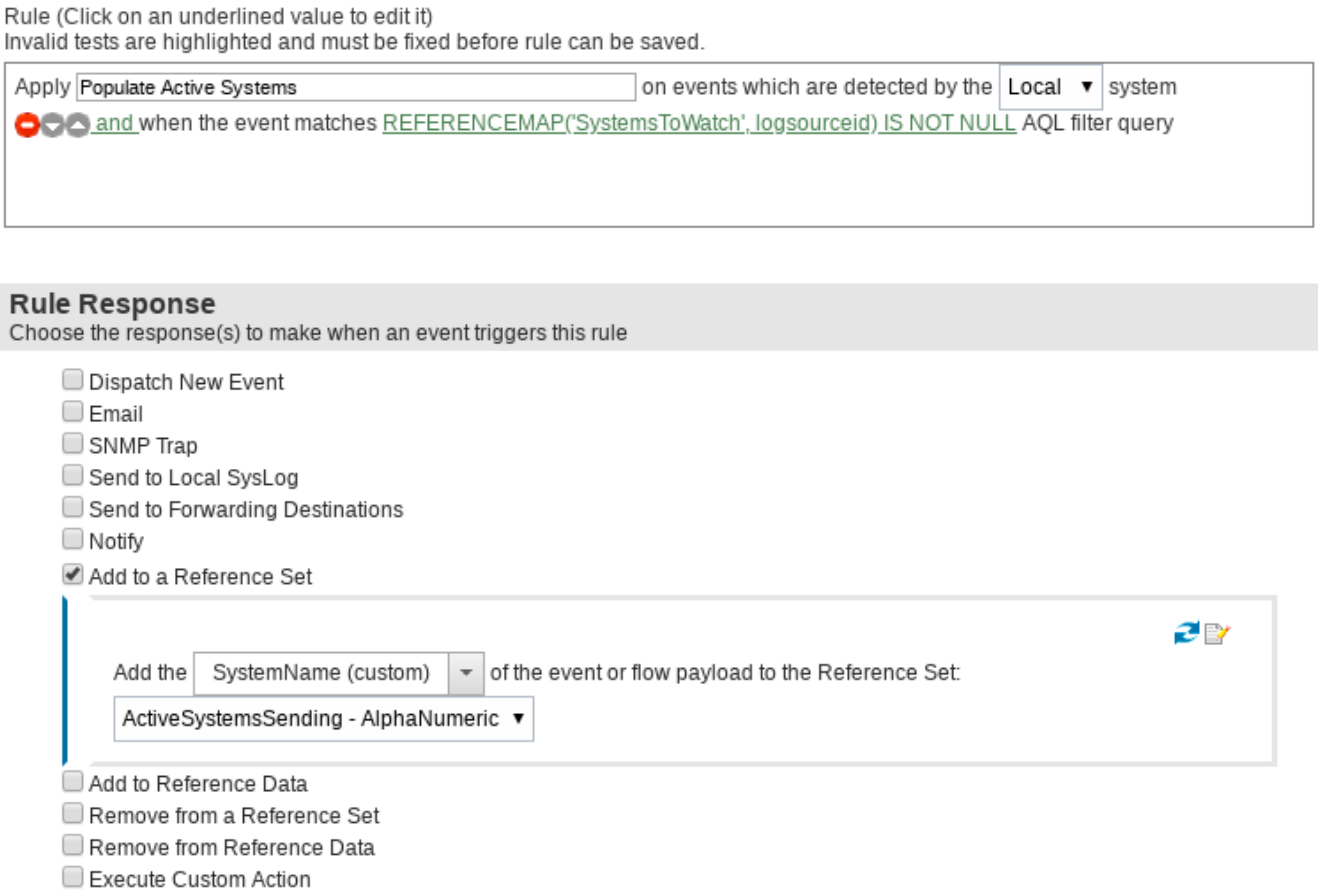
Reference Map:
SystemsToWatch - Key: Log source ID, Value: Unique Name to describe the group

Reference Set:
ActiveSystemsSending – TTL set to the length of time after which a notification is desired. Values in the set are the Unique Name(s) that have recently sent events.

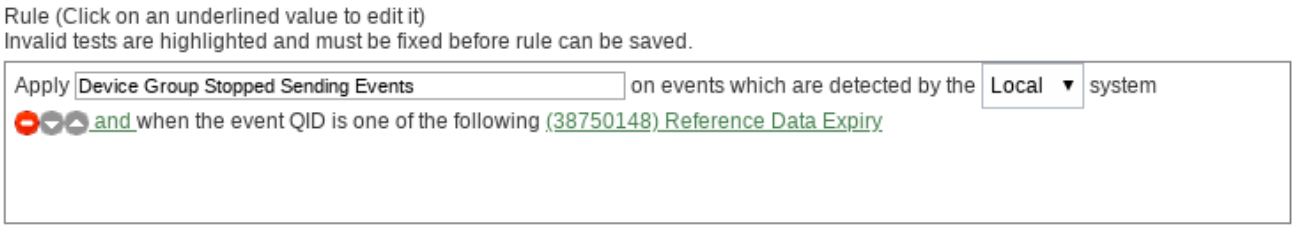
A tracker rule watches events as they come through the system. If a log source ID exists in the "SystemsToWatch" reference map, then the value gets placed in the "ActiveSystemsSending" reference

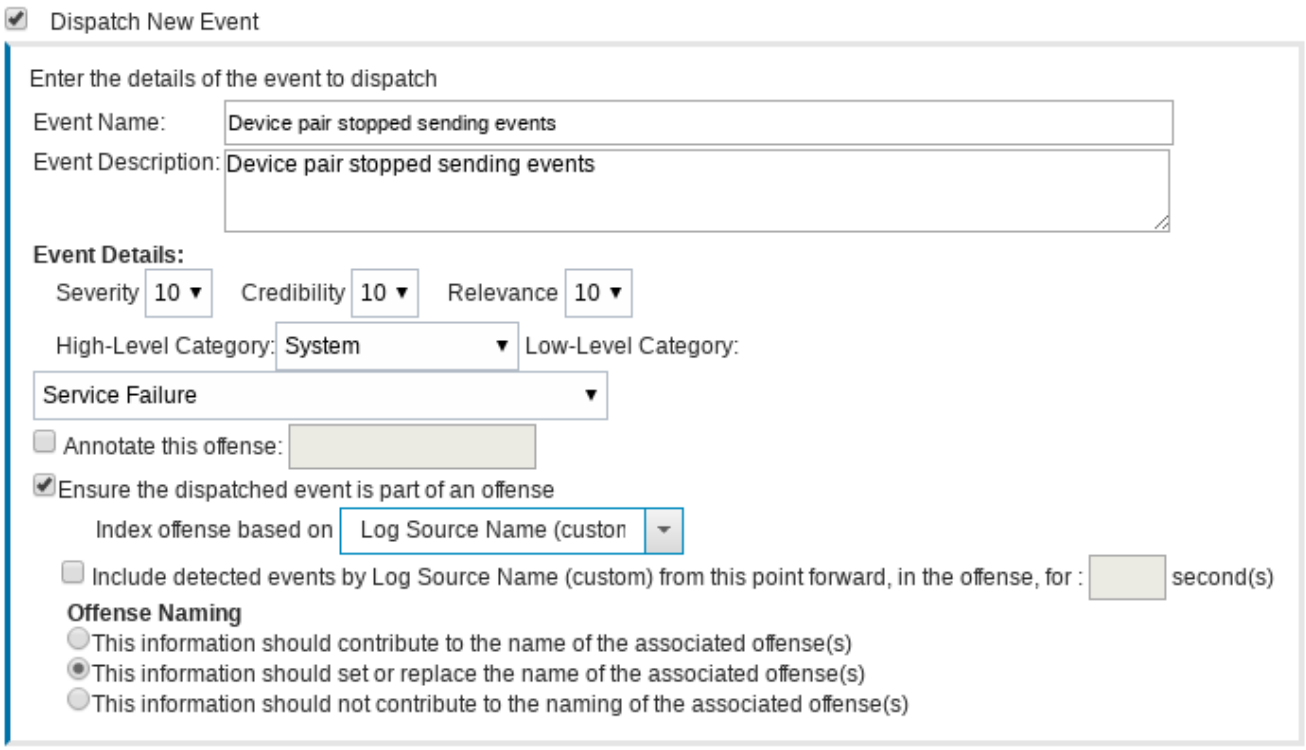
set (with a response limiter that is much smaller than the TTL of the reference set AND indexed on the log source)

Rule #1 – AKA: The Tracker Rule!



Rule #2 - AKA: The Watcher Rule!

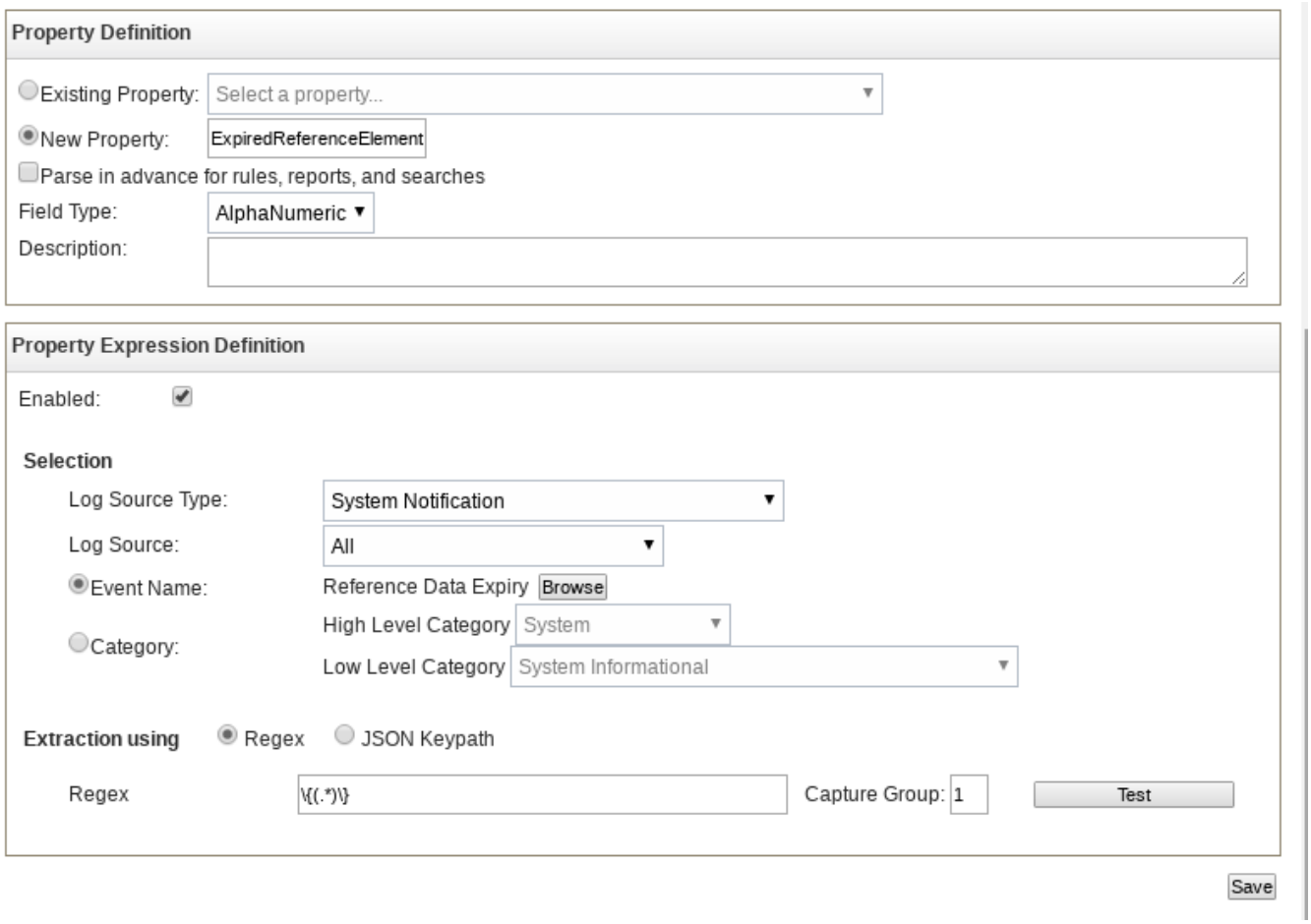




Now! As long as the system has seen as least one event from the log source since startup, then there will be values populated in the reference set.

As soon as that reference set entry expires, it means that ALL log sources tied to the Unique Name in the Reference Map have stopped sending – so we'll generate an offense and index it based on that Unique Name.

BTW: That "Log Source Name", I originally called "ExpiredReferenceElement" and it is configured like:



TODO:

- Update rules to make more generic
  - By group
  - By type
- Write an app to:
  - Visualize and update the pairings being mapped
  - Show the current pairings
  - Show which pairings are currently active and inactive
- Make this document pretty