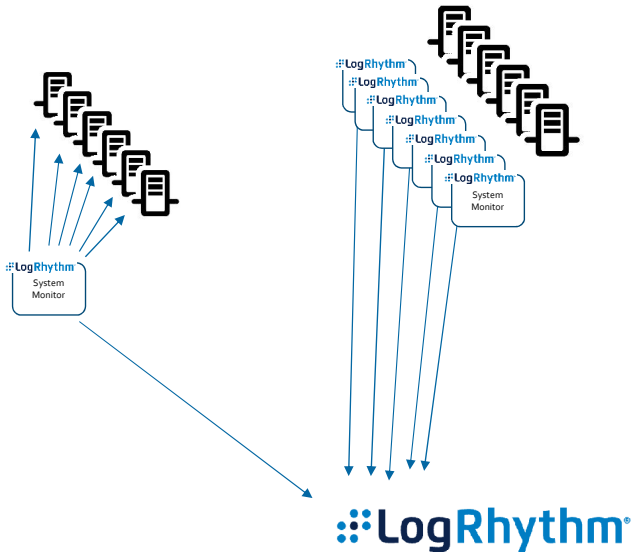
LogRhythm and Native Windows Event Forwarding: How to Do It Right, Filter the Noise and Simplify your Infrastructure

Sponsored by

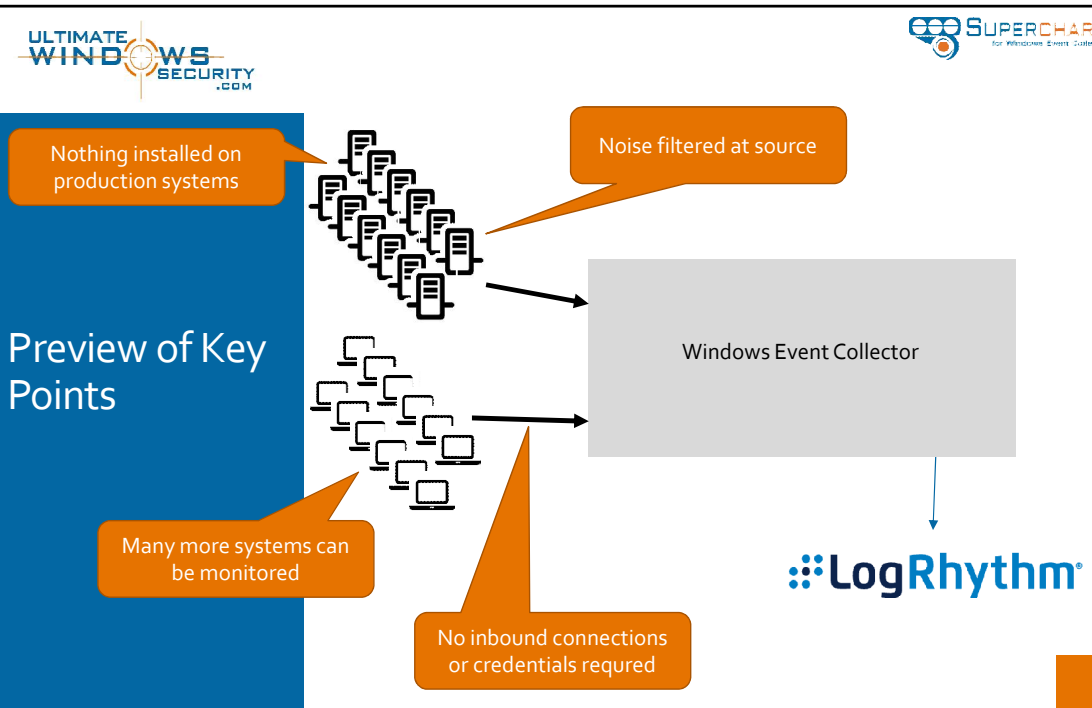
Thanks to

- Made possible by

Preview of Key Points



Preview of Key Points



Benefits of WEC with LogRhythm

- Resources and capacity
  - Network Bandwidth
  - EPS/MPS Reduction
- Simplification
  - No Service Accounts
  - No agents to
    - Install
    - Update
    - Manage
    - Convince admins to allow
- Public cloud environments
  - For environments with ephemeral hosts that would otherwise require manual configuration in the SIEM, using a WEC remove this challenge as log sources are automatically collected.
  - For ephemeral IaaS hosts WEC is best approach

Benefits of WEC with LogRhythm

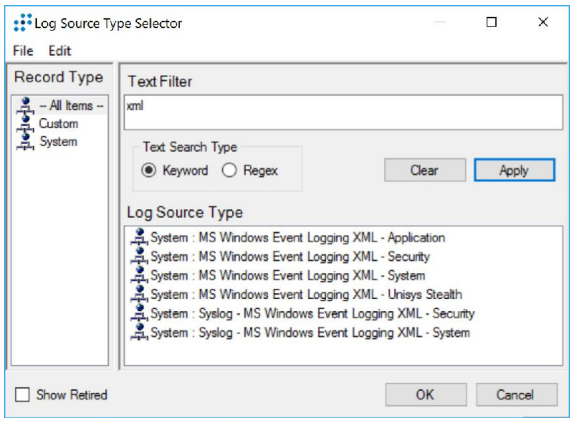
- LogRhythm supports WEC
  - LogRhythm Known Host works with WEC

How to do it

- Setup Windows Event Collector
- Setup Subscriptions and Destination Logs on collector
- Install LogRhythm System Monitor on collector
- Add Log Source to System Monitor for each Destination Log

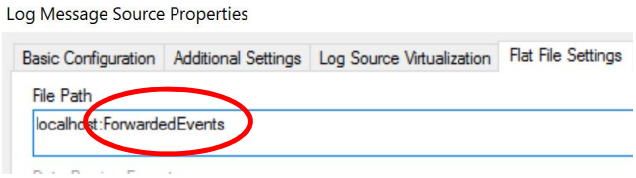
Add Log Source to System Monitor for each Destination Log

- Log Message Source Type
  - MS Windows Event Log XML - Security



Add Log Source to System Monitor for each Destination Log

- Use Flat File Settings to define the specific log

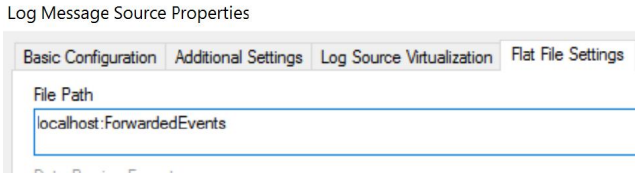


Beyond the basics

- Multiple log types
  - Don't re-use Application and System on Collector
  - Options
    - LogRhythm Log Source Virtualization
    - Using Custom Event Forwarded Destinations

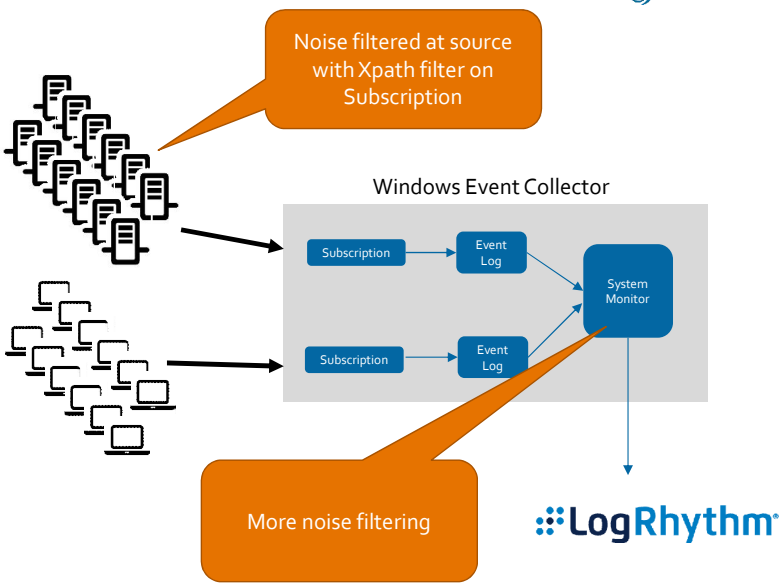
Log sources

- LogRhythm has 2 log formats for getting Windows event logs
  - Classic
  - XML
    - Use this when present for given log type
- To specify a different physical log

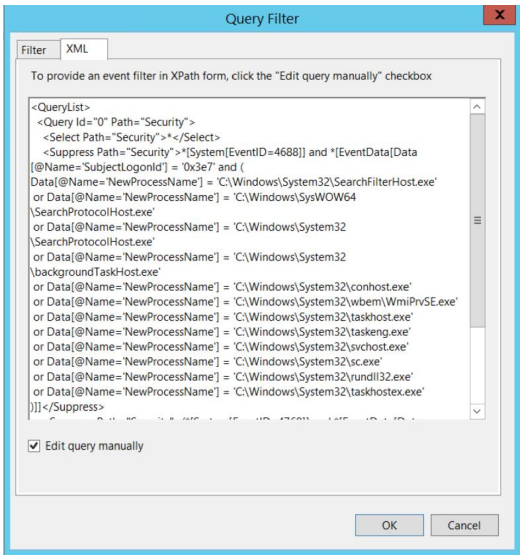


- Log Source Host = WEC collector
- Impacted or Origin Host = Forwarding computer (aka event source computer)
- LogRhythm Known Host works with WEC

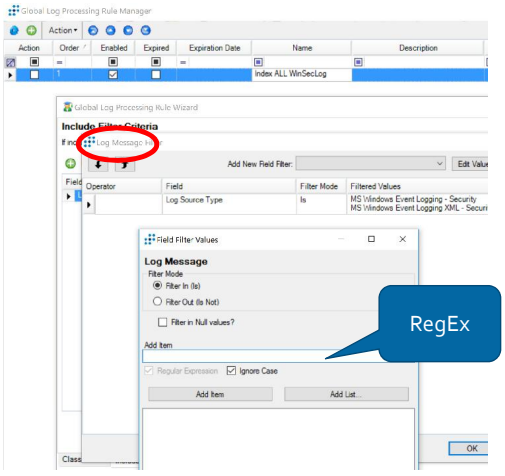
2-level noise filtering



Level 1 – WEC Subscription Xpath filters



Level 2 – Using Global Log Processing Rules



Bottom Line

- Windows Event Collection rocks
  - Built into Windows
  - No agents
  - Noise filtering at the source
  - No inbound/remote collection or configuration
  - Efficient
  - Resilient

Windows Event Collection is a foundation technology

- No management
- How to manage multiple collectors?
- Is WEC really working?
  - Which computers are failing to forward security logs?
  - Are we missing any computers?
- Is my WEC collector overloaded?
  - Dropping events?
  - Unresponsive?
  - Approaching capacity?
- How do I distribute load of many event sources between multiple collectors?

Windows Event Collection is a foundation technology

- Need for custom logs to separate sourcetypes
  - But no way to create custom logs that WEC will support as a destination
    - Build XML manifest file
    - Compile with Message Compiler mc.exe
    - Compile with Resource Compiler rc.exe
    - Register event source
    - Xpath filtering is powerful but
  - Requires knowledge and testing of cryptic syntax
  - Requires expert knowledge of security log events so that you don't suppress important security events
- Windows needs to be optimized to avoid dropped events and WEC hangs

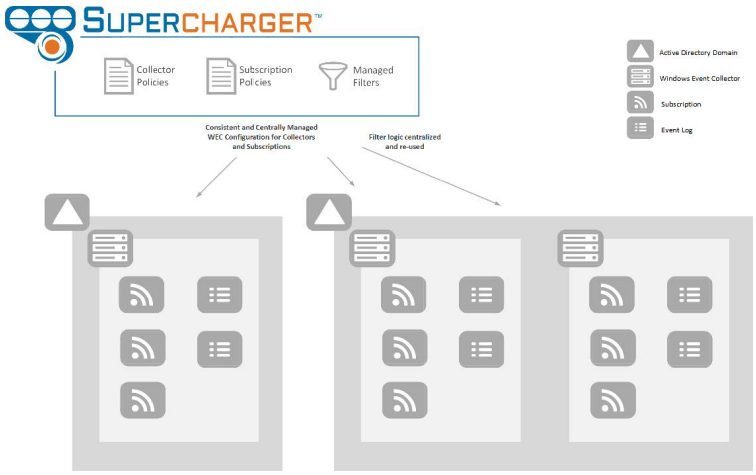
Supercharger for Windows Event Collection

- Brings all your WEC collectors around the world onto one pane of glass

ULTIMATE WINDOWS SECURITY .COM

SUPERCHARGER for Windows Event Collection

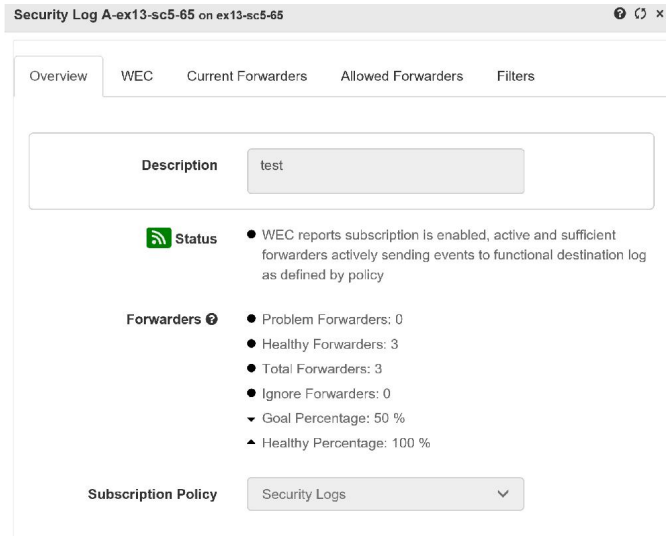
Supercharger for Windows Event Collection



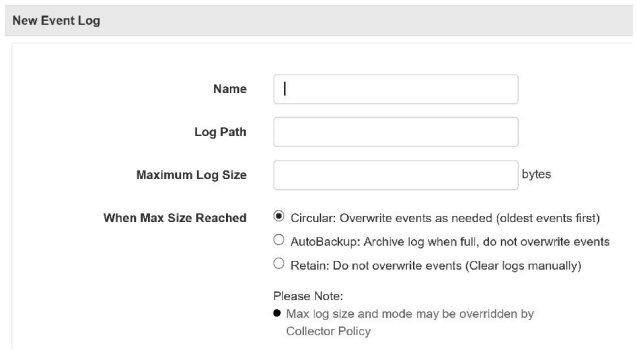
ULTIMATE WINDOWS SECURITY .COM

SUPERCHARGER for Windows Event Collection

Manage subscriptions consistently across all collectors



Create custom logs supported by WEC in seconds



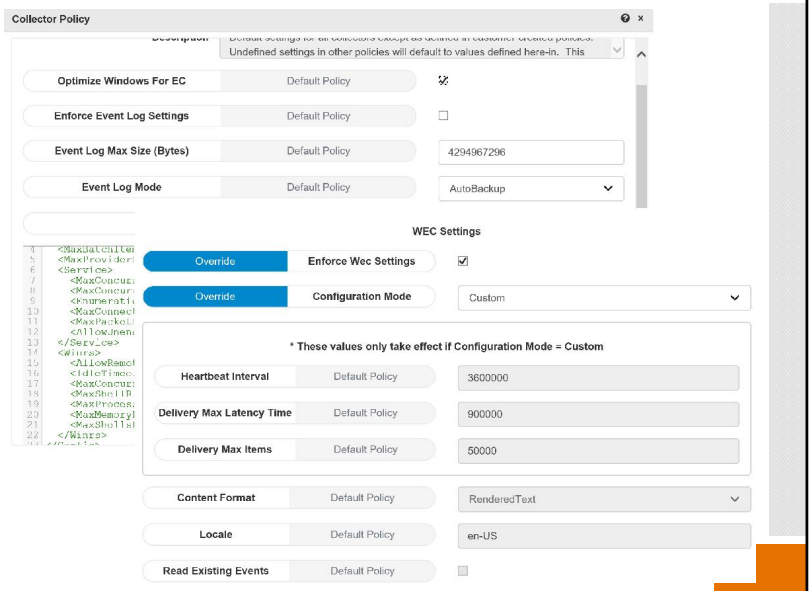
Load balance computers between collectors

ULTIMATE WINDOWS SECURITY .COM

SUPERCHARGED for Windows Event Collection

Optimize each collector automatically to support high volume WEC

All settings exposed via UI

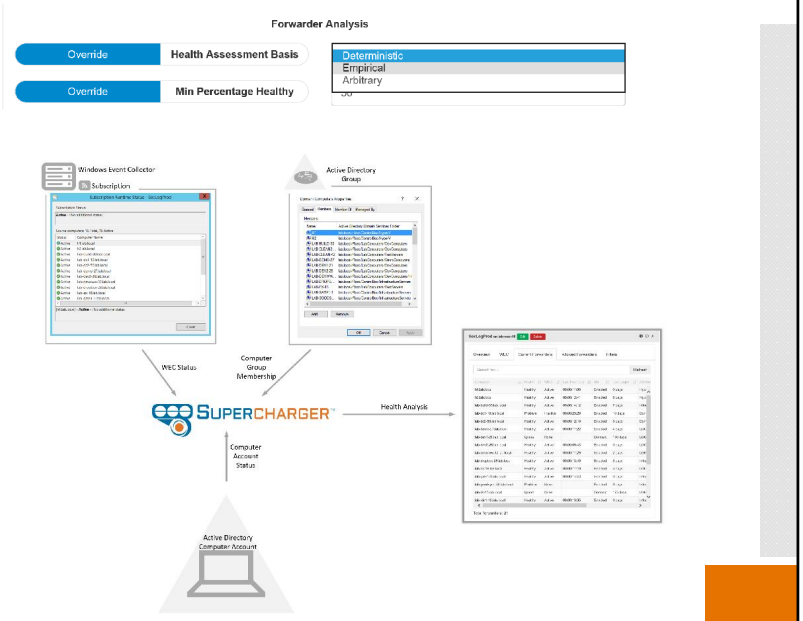


ULTIMATE WINDOWS SECURITY .COM

SUPERCHARGED for Windows Event Collection

At a glance performance and health indicators

3 ways to measure health



Supercharger for Windows Event Collection

- Download Supercharger manager at
  - https://www.logbinder.com/Form/SCDownload
  - Installs in minutes
- Install agent on each collector
  - 5 minutes
  - Automatic upgrades of all collector agents
- Get instant and global visibility and control
- Instant price quote
  - https://www.logbinder.com/Products/Supercharger/Pricing


SUPERCHARGER™
for Windows Event Collection
POLLING
NOISE
AGENTS
www.logbinder.com