



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

Sponsored by



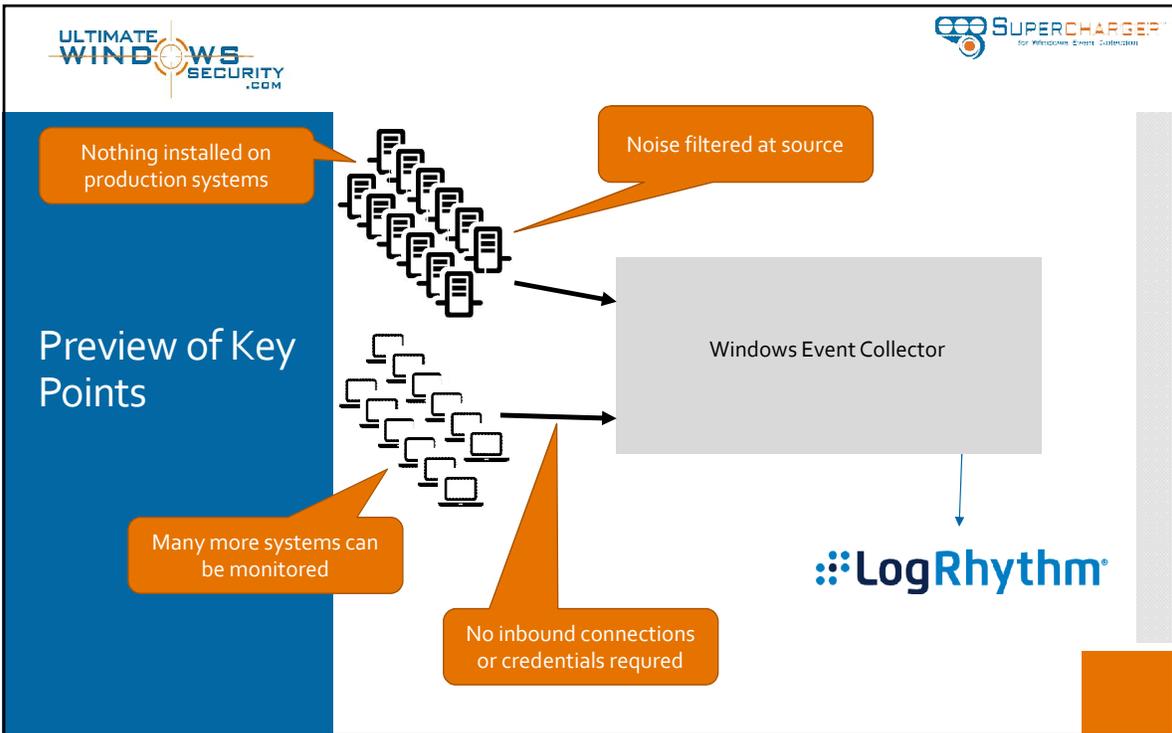
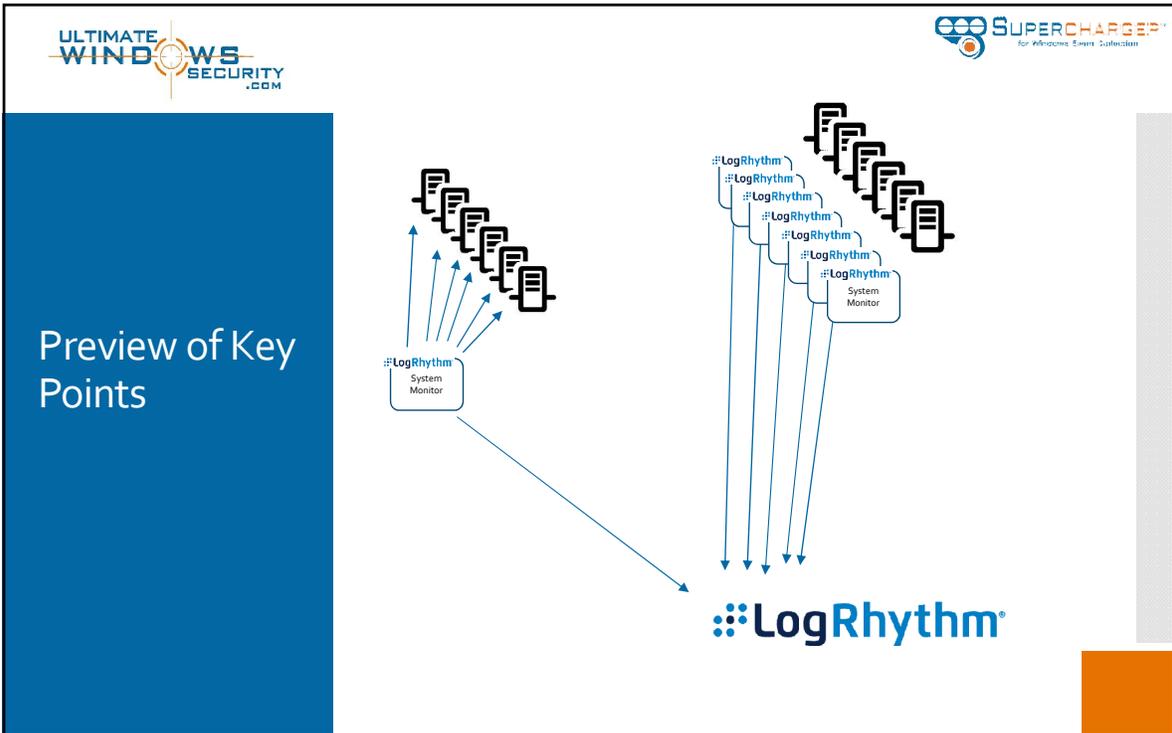
© 2017 Monterey Technology Group Inc.



Thanks to

• Made possible by







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

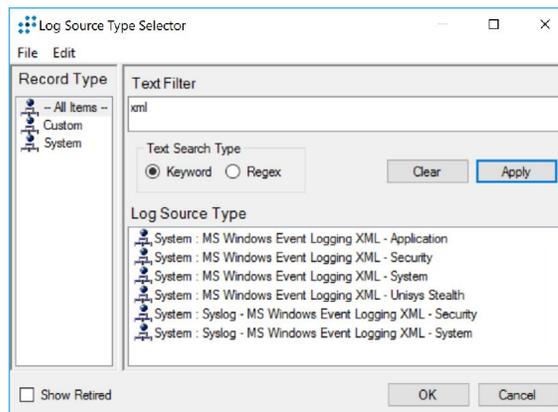


How to do it

- 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



ULTIMATE
WINDOWS
SECURITY
.COM

SUPERCHARGER[™]
for Windows Event Collection

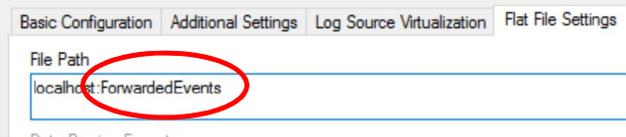
Add Log Source to System Monitor for each Destination Log

- Use Flat File Settings to define the specific log

Log Message Source Properties

Basic Configuration Additional Settings Log Source Virtualization Flat File Settings

File Path
localhost:ForwardedEvents



ULTIMATE
WINDOWS
SECURITY
.COM

SUPERCHARGER[™]
for Windows Event Collection

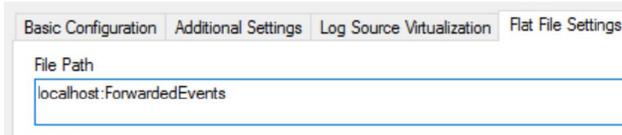
Beyond the basics

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

Log sources

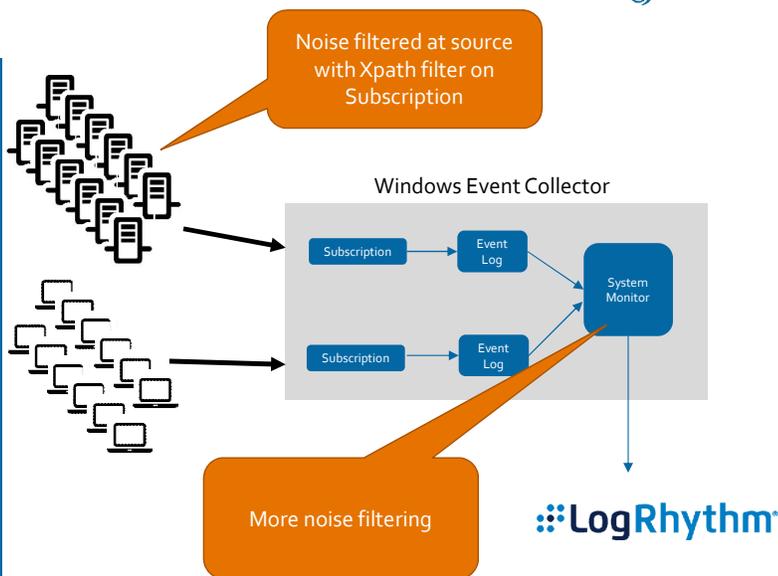
- LogRhythm has 2 log formats for getting Windows event logs
 - Classic
 - XML
 - Use this when present for given log type
- To specify a different physical log

Log Message Source Properties

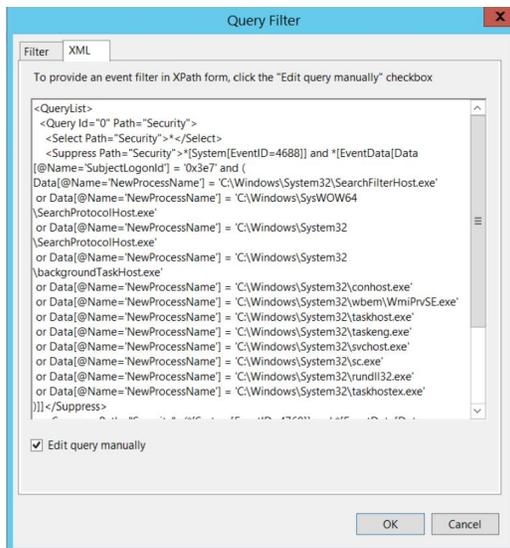


- Log Source Host = WEC collector
- Impacted or Origin Host = Forwarding computer (aka event source computer)
- LogRhythm Known Host works with WEC

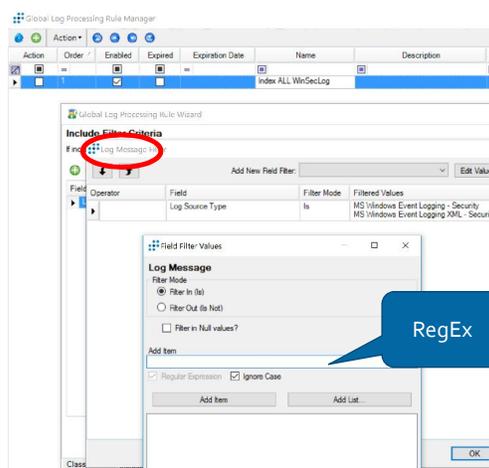
2-level noise filtering



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

© 2017 Monterey Technology Group Inc.

Collector Policies | Subscription Policies | Managed Filters

Consistent and Centrally Managed WEC Configuration for Collectors and Subscriptions

Filter logic centralized and re-used

- Active Directory Domain
- Windows Event Collector
- Subscription
- Event Log

ULTIMATE WINDOWS SECURITY .COM

SUPERCHARGER™
For Windows Event Collection

Manage subscriptions consistently across all collectors

Security Log A-ex13-sc5-65 on ex13-sc5-65

Overview | WEC | Current Forwarders | Allowed Forwarders | Filters

Description: test

Status: ● WEC reports subscription is enabled, active and sufficient forwarders actively sending events to functional destination log as defined by policy

Forwarders: ● Problem Forwarders: 0
● Healthy Forwarders: 3
● Total Forwarders: 3
● Ignore Forwarders: 0
▼ Goal Percentage: 50 %
▲ Healthy Percentage: 100 %

Subscription Policy: Security Logs

ULTIMATE WINDOWS SECURITY .COM

SUPERCHARGERSM
for Windows Event Collector

Create custom logs supported by WEC in seconds

New Event Log

Name

Log Path

Maximum Log Size bytes

When Max Size Reached

- Circular: Overwrite events as needed (oldest events first)
- AutoBackup: Archive log when full, do not overwrite events
- Retain: Do not overwrite events (Clear logs manually)

Please Note:

- Max log size and mode may be overridden by Collector Policy

ULTIMATE WINDOWS SECURITY .COM

SUPERCHARGERSM
for Windows Event Collector

Load balance computers between collectors

ex13.local

Security Log A

Workstation Security L...

The screenshot displays two main log collector panels. The left panel is titled 'Security Log A' and contains two sub-panels with bar charts. The first sub-panel is labeled 'ex13-sc5-65' and the second is 'ex13-sc6-66'. The right panel is titled 'Workstation Security L...' and also contains two sub-panels with bar charts, labeled 'ex13-sc6-66' and 'ex13-sc5-65'. Each sub-panel includes a green bar chart, a list icon, and a Wi-Fi signal icon.



Optimize each collector automatically to support high volume WEC

All settings exposed via UI

The screenshot shows the 'Collector Policy' configuration window. It includes sections for 'Optimize Windows For EC', 'Enforce Event Log Settings', and 'Event Log Max Size (Bytes)'. The 'WEC Settings' section is expanded, showing options like 'Enforce Wec Settings' (checked), 'Configuration Mode' (set to Custom), and various performance metrics such as 'Heartbeat Interval' (3600000), 'Delivery Max Latency Time' (900000), and 'Delivery Max Items' (50000). A note states: '* These values only take effect if Configuration Mode = Custom'.



At a glance performance and health indicators

The screenshot displays a dashboard with several performance and health indicators. At the top, it shows 'lab-2008r2-77.lab.local' with a tooltip indicating 'Current CPU: 5%' and 'CPU 7 Day Average: 12%'. Below this, there are several collector cards. One card for 't3' shows: 'Enabled: Yes', 'Problem Forwarders: 0', 'Healthy Forwarders: 27', 'Subtotal Forwarders: 27', 'Ignore Forwarders: 0', 'All Forwarders: 27', 'Healthy Percentage: 100%', and 'Goal Percentage: 100%'. Another card for 'etwtest' shows: 'Events Per Second: 3043', 'EPS 7 Day Avg: 3585', and 'EPS 7 Day Peak: 5947'. Other collectors shown include 'asdf', 't4', and 'ForwardedEvents'.





3 ways to measure health

Forwarder Analysis

Override

Health Assessment Basis

Deterministic

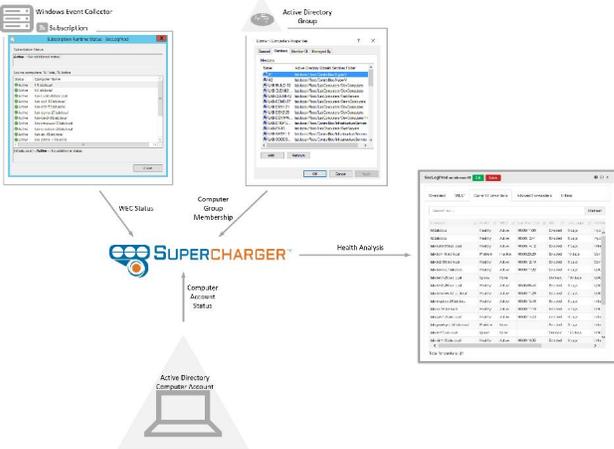
Override

Min Percentage Healthy

Empirical

Arbitrary

None







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