



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

© 2017 Monterey Technology Group Inc.

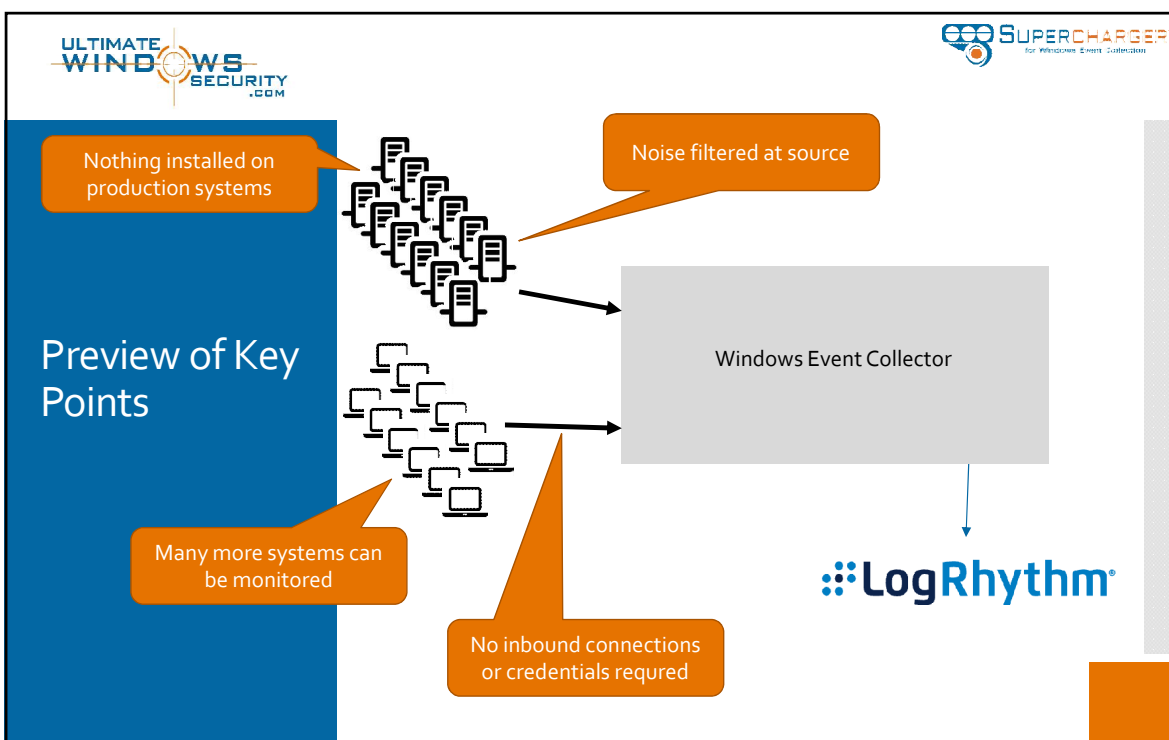
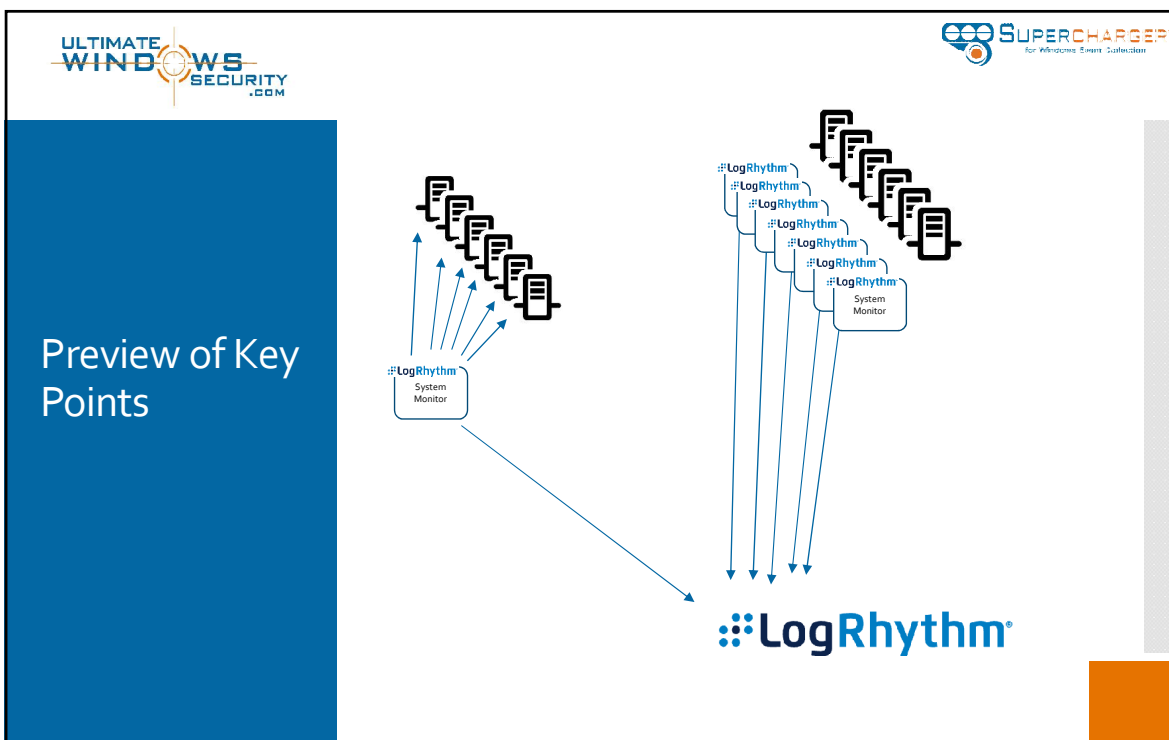
Sponsored by



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

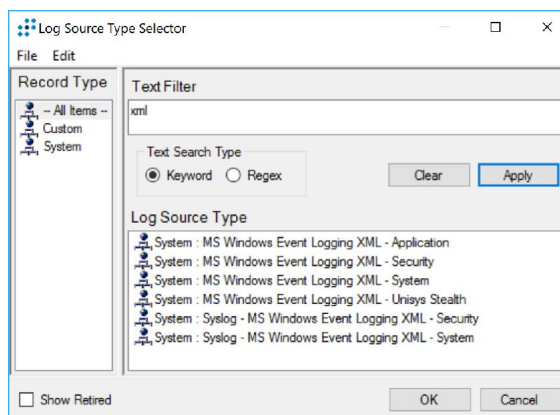
- LogRhythm supports WEC
 - LogRhythm Known Host works with WEC

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



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

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

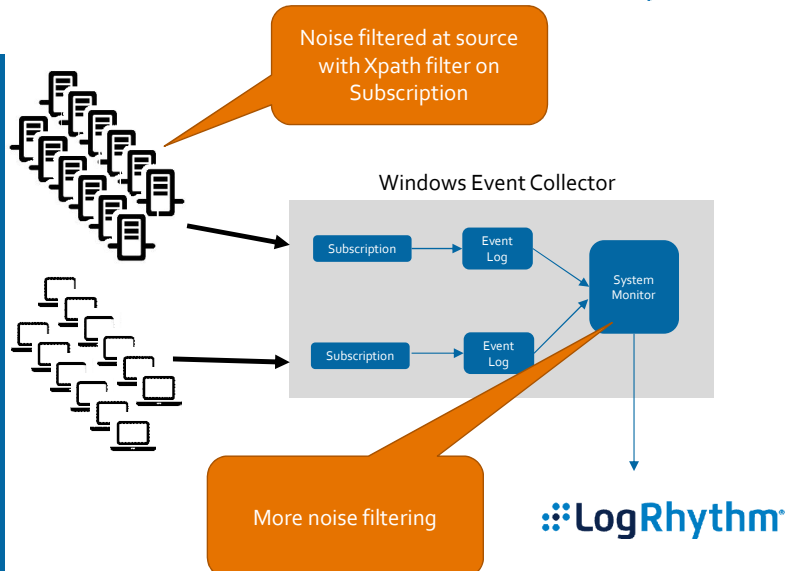
Log Message Source Properties

Basic Configuration | Additional Settings | Log Source Virtualization | Flat File Settings

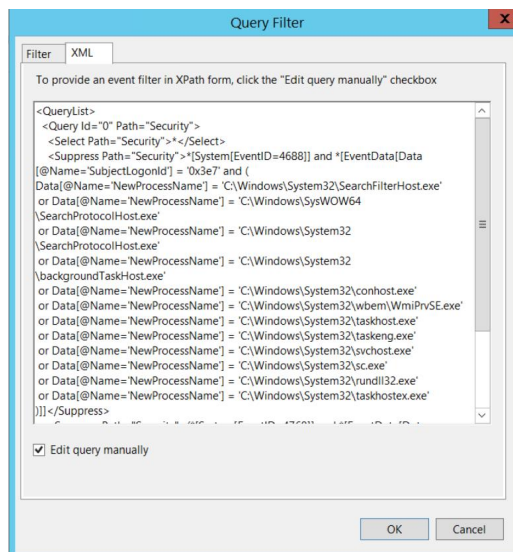
File Path
localhost:ForwardedEvents

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

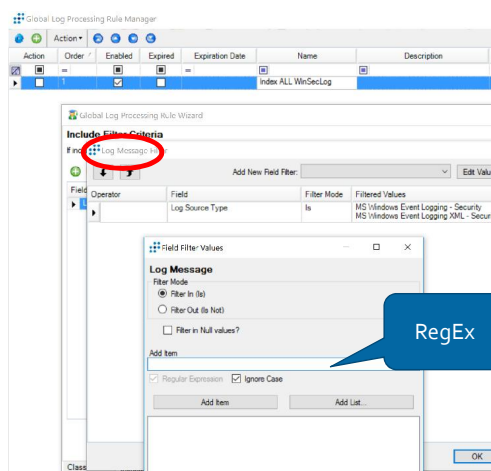
2-level noise filtering



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

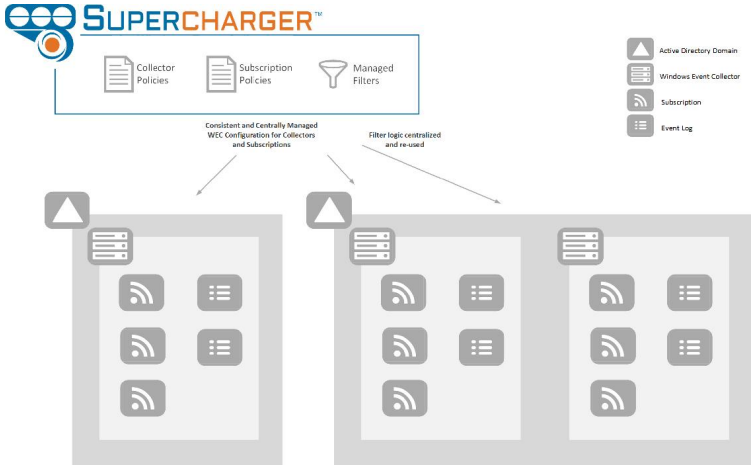
- Brings all your WEC collectors around the world onto one pane of glass










Supercharger
for Windows
Event
Collection





© 2017 Monterey Technology Group Inc.






Manage
subscriptions
consistently
across all
collectors

Security Log A-ex13-sc5-65 on ex13-sc5-65
?
↺
×


Overview
WEC
Current Forwarders
Allowed Forwarders
Filters

Description



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 ▼



10





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





Load balance computers between collectors

▲
ex13.local

Security Log A

ex13-sc5-65

List

Wi-Fi

ex13-sc6-66

List

Wi-Fi

Workstation Security L...

ex13-sc6-66

List

Wi-Fi

ex13-sc5-65

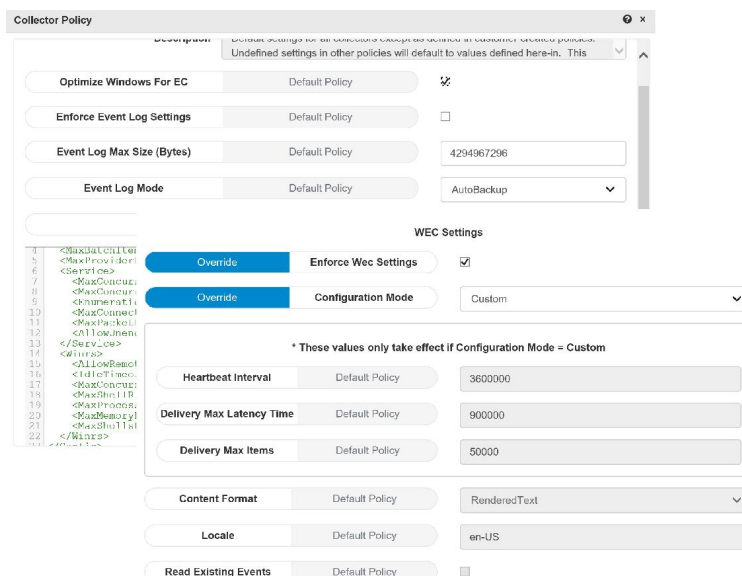
List

Wi-Fi

11

Optimize each collector automatically to support high volume WEC

All settings exposed via UI



Collector Policy

Undefined settings in other policies will default to values defined here-in. This

Optimize Windows For EC Default Policy ☒

Enforce Event Log Settings Default Policy ☐

Event Log Max Size (Bytes) Default Policy 4294967296

Event Log Mode Default Policy AutoBackup

WEC Settings

Override Enforce Wec Settings ☒

Override Configuration Mode Custom

* These values only take effect if Configuration Mode = Custom

Heartbeat Interval Default Policy 3600000

Delivery Max Latency Time Default Policy 900000

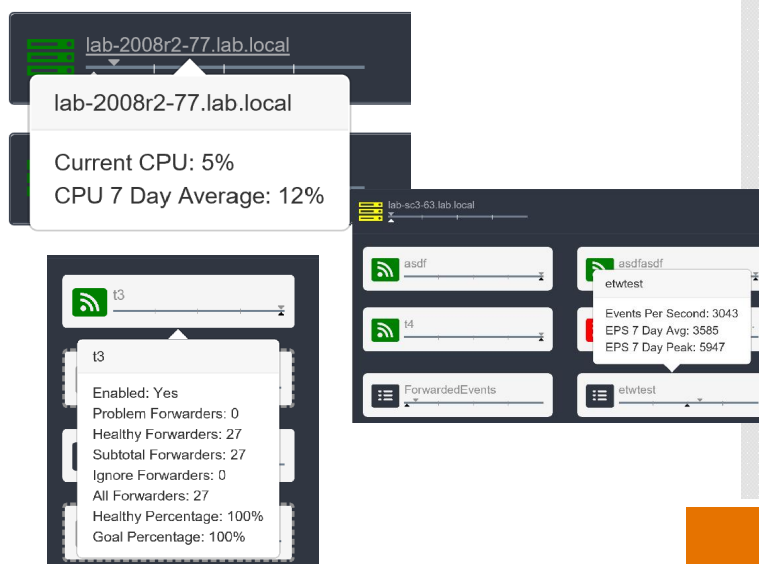
Delivery Max Items Default Policy 50000


Content Format Default Policy RenderedText


Locale Default Policy en-US

Read Existing Events Default Policy ☐

At a glance performance and health indicators







3 ways to measure health

Forwarder Analysis

Override

Health Assessment Basis

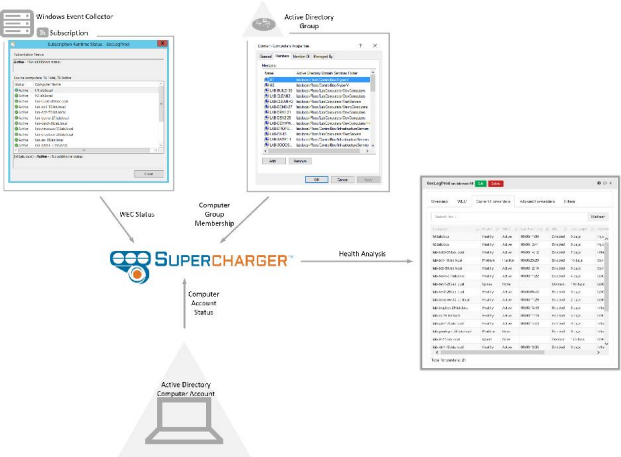
Deterministic


Override


Min Percentage Healthy

Empirical

Arbitrary







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