



Managing Large Windows Event Collection Implementations: Load Balancing Across Multiple Collectors

Sponsored by





© 2017 Monterey Technology Group Inc.



Thanks to



• Made possible by





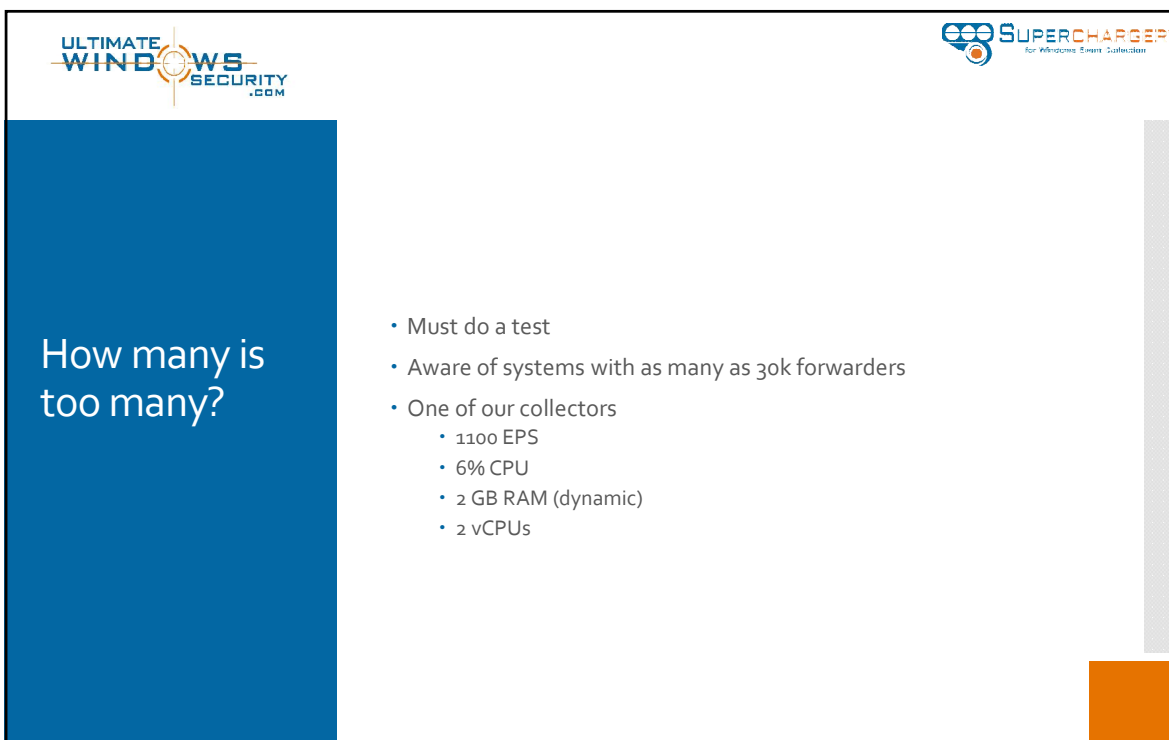
Preview of Key Points

- How many forwarders is too many?
- Key performance counters
- Optimizing performance
- Load balancing
- How do you know if WEC is healthy?



How many is too many?

- Not simply the # of forwarders
- Equally important variables
 - Audit policy
 - User/application activity
 - Xpath filter
 - Tolerance for latency
 - Optimization

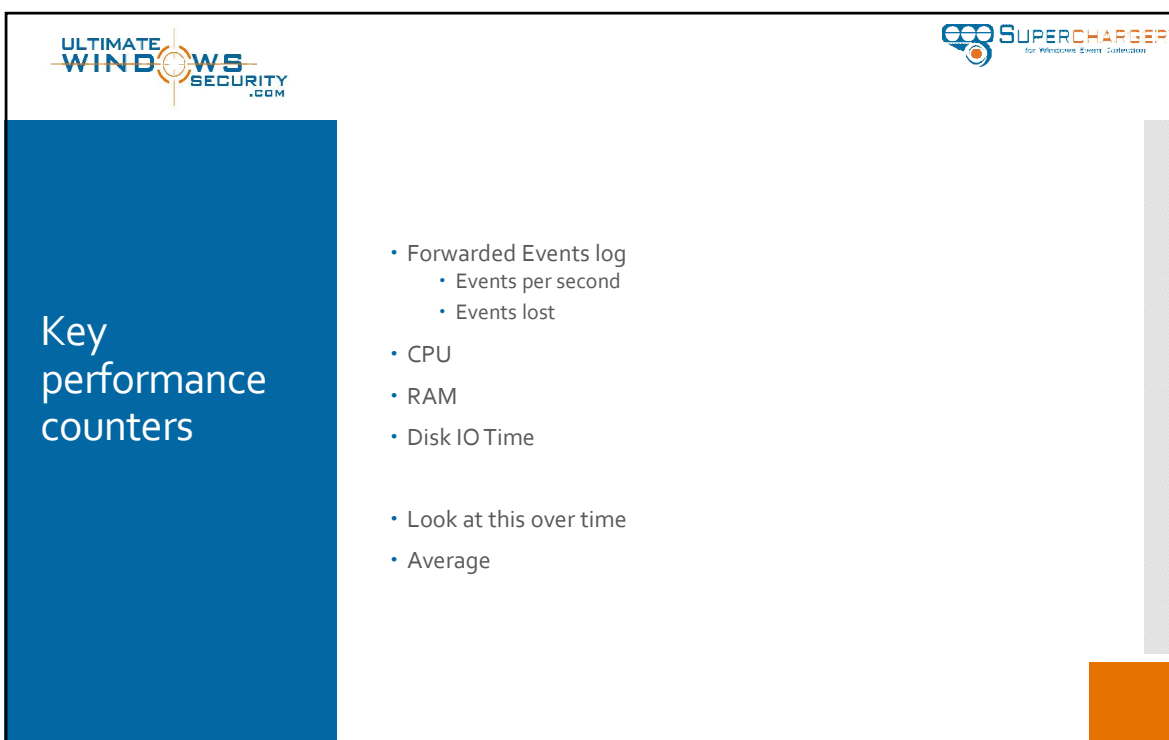


ULTIMATE WINDOWS SECURITY .COM

SUPERCHARGER[™]
For Windows Event Collection

How many is too many?

- Must do a test
- Aware of systems with as many as 30k forwarders
- One of our collectors
 - 1100 EPS
 - 6% CPU
 - 2 GB RAM (dynamic)
 - 2 vCPUs



ULTIMATE WINDOWS SECURITY .COM

SUPERCHARGER[™]
For Windows Event Collection



Key performance counters

- Forwarded Events log
 - Events per second
 - Events lost
- CPU
- RAM
- Disk IO Time
- Look at this over time
- Average



Optimizing performance

- Increase throughput
 - Larger buffers
 - Not flushing
- Increase batch sizes
 - Possibly at expense of currency
- Optimization points
 - Collector
 - Subscription
 - Forwarder



Collector performance

- sconfig wecsvctype= own
 - Stand-Alone service instead of shared
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\targetlog
 - BufferSize(Dword) -2048
 - FlushTimer(Dword) -0
 - MaximumBuffers(DWord) -8192
 - MinimumBuffers(DWord) -0
- HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
 - "TcpTimedWaitDelay – Dword – 30

Collector performance

- winrm set winrm/config @{MaxEnvelopeSizekb="500"}
- winrm set winrm/config @{MaxTimeoutms="60000"}
- winrm set winrm/config @{MaxBatchItems="32000"}
- winrm set winrm/config/client @{NetworkDelaysms="5000"}
- winrm set winrm/config/service @{MaxConcurrentOperations="4294967295"}
- winrm set winrm/config/service @{MaxConcurrentOperationsPerUser="1500"}
- winrm set winrm/config/service @{MaxConnections="500"}
- winrm set winrm/config/service @{MaxPacketRetrievalTimeSeconds="120"}
- winrm set winrm/config/winrs @{IdleTimeout="7200000"}
- winrm set winrm/config/winrs @{MaxConcurrentUsers="10"}
- winrm set winrm/config/winrs @{MaxShellRunTime="2147483647"}
- winrm set winrm/config/winrs @{MaxProcessesPerShell="25"}
- winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
- winrm set winrm/config/winrs @{MaxShellsPerUser="30"}

Subscription



Advanced Subscription Settings

Event Delivery Optimization:

- Normal
- Minimize Bandwidth
- Minimize Latency
- Custom



Protocol:

- Controls
 - Heartbeat Interval
 - Delivery Max Latency Time
 - Delivery Max Items
- Batching: - Max Items = 50,000 - Max Latency Time = 30,000 - Heartbeat Interval = 360,000



Subscription

- Turn of pre-rendering
 - `wecutilss<name of subscription> /cf:events`
 - Test impact on your SIEM
- Read existing events



Forwarder



- Audit policy
- Filtering
 - Fewer events to send
 - More processing
- Computer Configuration/Policies/Administrative Templates/Windows Components/Event Forwarding/ForwardResourceUsage
 - Events per second max

So you need multiple collectors

- How do you distribute the load?
 - Target collectors by group policy
 - On the basis of OU or WMI filter
 - Target subscriptions by group
- OU and WMI filters
 - Re-targeting collectors takes place when group policy refreshed
- Group membership
 - Re-subscribing in response to group membership change
 - Computer is rebooted
 - Kerberos tickets purged



Tempted to load balance forwarders by OU or WMI filter?

- OUs
 - You can only arrange OUs one way, one hierarchy
 - Do you really want to make it about WEC load balancing?
 - More importantly
 - How do you assess health?
 - Which computer should be hitting which subscription?
 - To add or remove collectors
 - OU created/deleted
 - GPOs created/deleted
 - To move forwarders between collectors
 - Move computer from one OU to another
- Load balancing with groups
 - No impact to OU hierarchy
 - Easy to assess health
 - Is computer account active and member of GroupA?
 - Then it should be actively forwarding events to Subscription A
 - To add or remove collectors
 - No impact changes to OUs
 - No creation/deletion of GPOs
 - To move forwarders, just change group membership



WEC subscription assignments

- Subscription assignments never instantaneous
 - Target Subscription Manager Refresh interval specified in group policy
 - AD replication
 - GPOs
 - Group membership
 - OU
 - Group Policy Refresh



The Achilles heel of group based load balancing

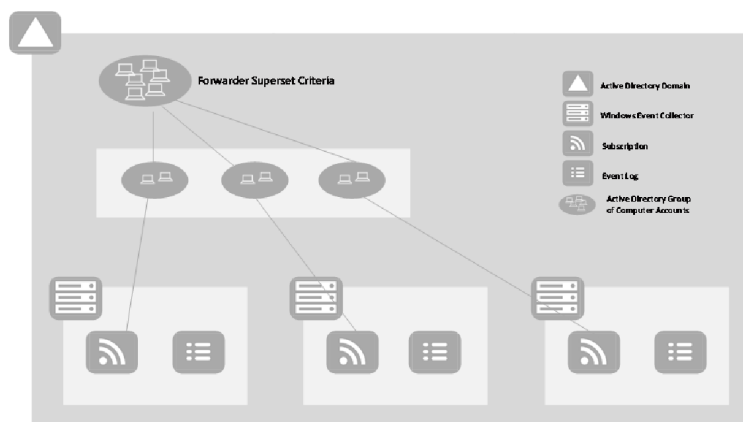
- Group membership changes don't take affect
 - Until reboot
 - Or purging tickets
- Purging tickets is safe but requires running a command on local forwarder
 - How?
 - System Center
 - Powershell remoting
 - Group Policy
 - Immediate task
- Group Policy Immediate Tasks
 - Still work even after recent security fixes
 - Create one-time only tasks
 - Limited to a date period
- Now group membership changes (and subscription assignment changes) take affect as soon as group policy refreshed

Supercharger

- The only WEC manager in the world
- The only WEC load balancing solution in the world

Supercharger

- Distributed Subscription
 - Give us a master group and 2 or more collectors
 - Define your source logs, filter and destination log



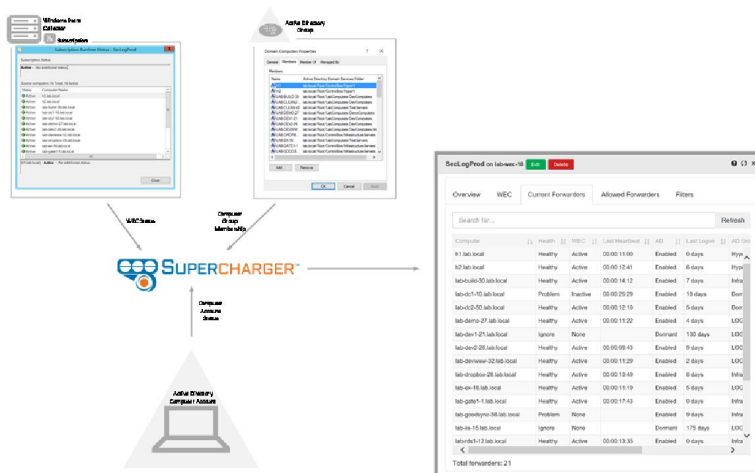




Supercharger

- Distributed Subscription
 - Creates identical subscription in WEC on each collector
 - Creates a group in AD for each subscription
 - Evenly distributes each computer in master group to one of the subscription groups
 - Taking into account computer's status in AD (e.g. dormant, disabled)
- Monitors
 - As new computers are provisioned and added to master group
 - Assigned to collector with lowest **actual** load
- Computers removed from master group
 - Removed from subscription
- New collector added or removed?
 - Computers re-distributed
 - Minimizing impact
 - Taking into account actual load



Determinist forwarder analysis





Supercharger

- Implement native Windows Event Collection fast and easily
- Monitor more endpoints while reducing load on your SIEM
- Efficiently collect every event log on your network
 - Without the noise
 - Without the agents
 - Without the polling
- Manage very large WEC environments - 100,000+ endpoints, multiple domains
- Instantly visibility
 - Who's sending events and who isn't? Why?
 - Where are the problems?
 - What is the performance?
- Detect new programs as soon as they execute anywhere on your network
- Reduce licensing costs for volume based log management technologies
- Catch intrusions earlier in the attack
- Meet compliance requirements
- Improve endpoint security

© 2017 Monterey Technology Group Inc.

Supercharger

- Download 30-day trial
 - <https://www.logbinder.com/Form/SCDownload>
- Schedule a demo
 - <https://www.logbinder.com/Form/Ask>
- Get WEC design help
 - <https://www.logbinder.com/Form/Ask>
- Instant pricing
 - <https://www.logbinder.com/Products/Supercharger/Pricing>

© 2017 Monterey Technology Group Inc.