



**Protect 2014**

Washington, D.C. September 8-11

# Using Windows Event Forwarding with the Windows Unified Connector

Steve Maxwell, Solutions Architect

#HPProtect

# Agenda

- What is Windows Event Forwarding?
- How does HP ArcSight work with Windows Event Forwarding?
- Benefits
- Tips & tricks



# What is Windows Event Forwarding?



# What is Windows Event Forwarding?

- Centralized Windows event collection
  - Collect events from Windows systems and store them centrally
- Introduced in Windows Server 2008 and Windows Vista
  - Built-in support in Windows Server 2008+ and Windows Vista+
  - Add-on support in Windows Server 2003 and Windows XP
- Uses Windows Remote Management 1.1 or later
  - Microsoft implementation of the WS-Management protocol



# Microsoft terminology

- Event Collector
  - Where events from Sources are centrally forwarded to and stored
- Event Source
  - Where events are generated



# Platforms – Event Collector

- Windows Server 2008/2012
  - Microsoft Recommended Platforms
- Windows 7/8
- Windows Vista



# Platforms – Event Source

- Windows Server 2008/2012
- Windows 7/8
- Windows Vista
- Windows Server 2003 SP1+
- Windows XP SP2+



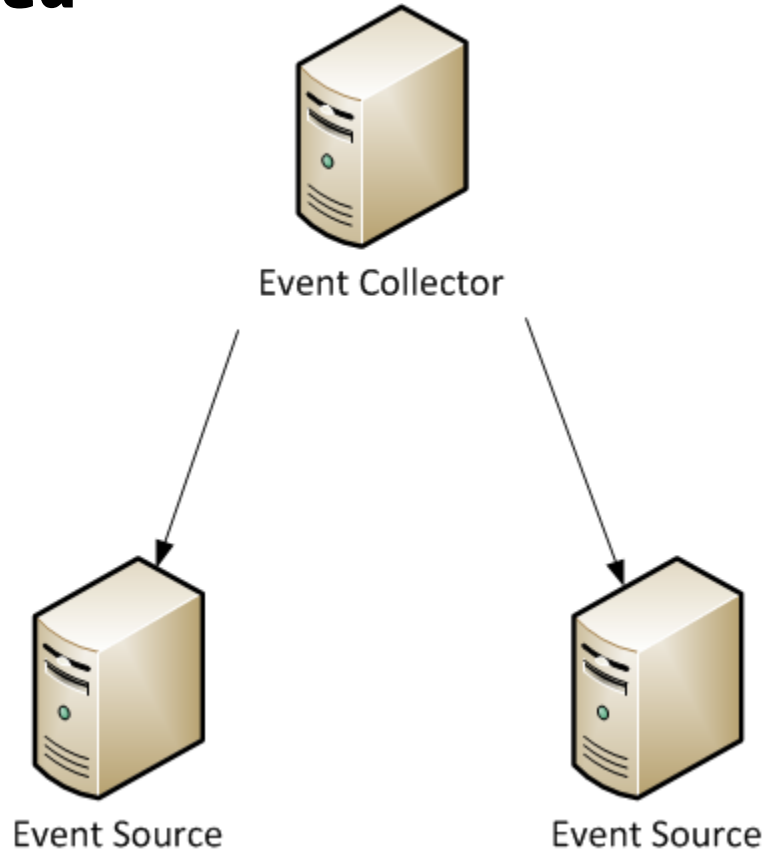
# Subscription

- What events do I want to collect?
- What systems do I want to collect from?
- What event log do I want to forward the collected events to?
- Collector or Source initiated?
- Advanced Subscription Settings

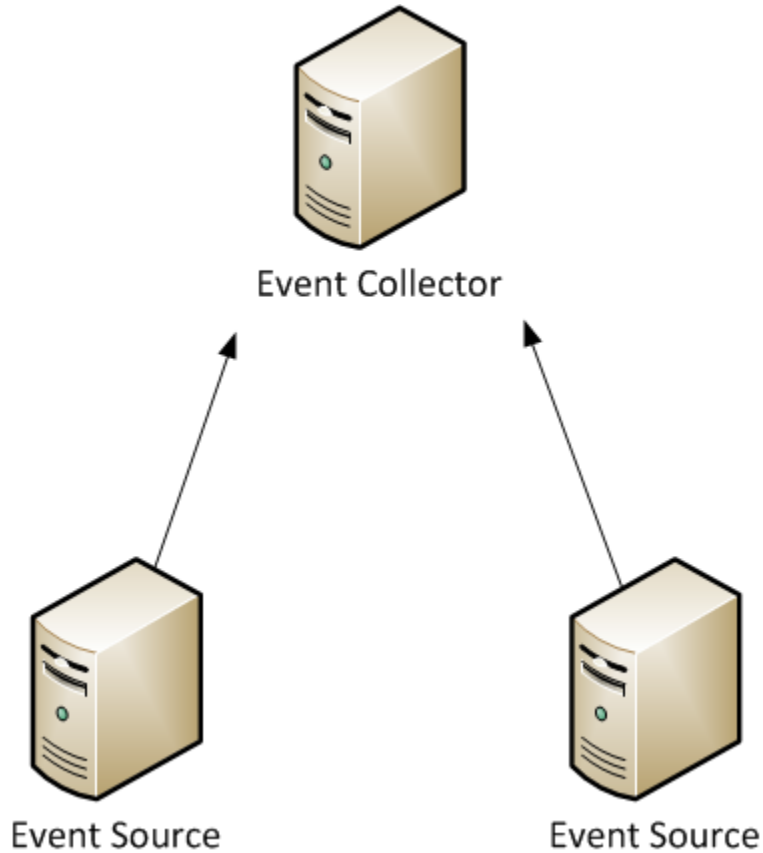




# Collector initiated



# Source initiated



Subscription Properties

Subscription name:

Description:

Destination log: Hardware Events

Subscription type and source computers

Collector initiated

This computer contacts the selected source computers and provides the subscription.

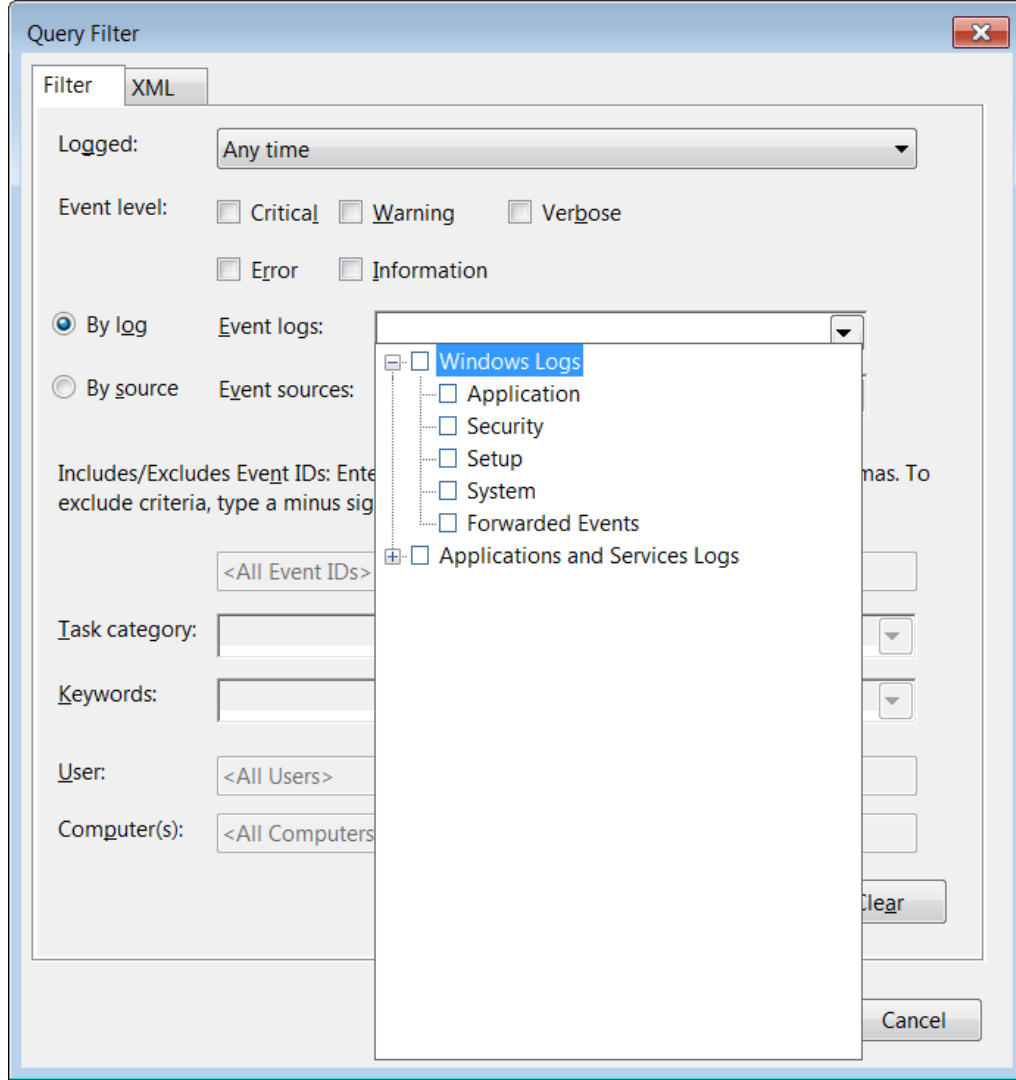
Source computer initiated

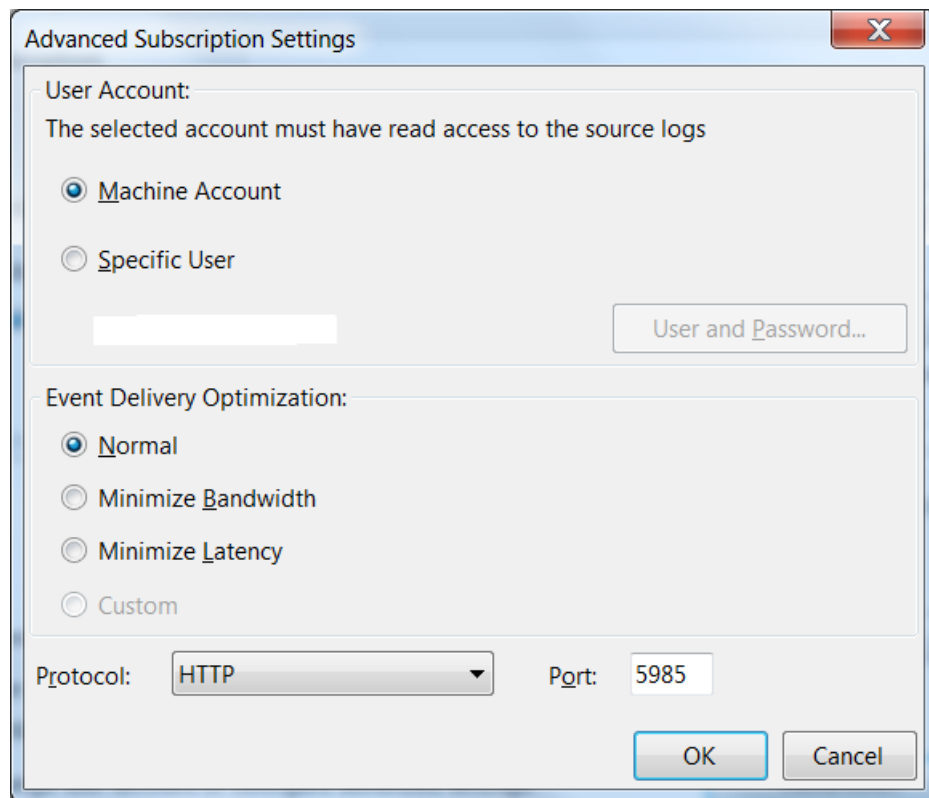
Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect: <filter not configured>

User account (the selected account must have read access to the source logs):  
Machine Account

Change user account or configure advanced settings:





# How does HP ArcSight work with Windows Event Forwarding?



# Acronyms used in this presentation

- Windows Unified Connector
  - WUC
- Windows Event Forwarding
  - WEF



# SmartConnector

- Support for WEF added to the WUC
  - SmartConnector 6.0.6.6865 released on September 30, 2013
- Microsoft Windows Event Log – Unified
  - Forwarded Events Collection
    - Disabled
    - Enabled (use AD for sources)
    - Enabled (do not use AD for sources)
  - Custom Log Names
    - HardwareEvents **is** Supported
    - ForwardedEvents **is not** Supported (subscription default)





# WEF Log Forwarding – options

- WEF has a lot of granularity on where to forward Source logs to on the Collector
  - For example...
    - Sources/Application Logs → Collector/Application Log
    - Sources/System Logs → Collector/System Log
    - Sources/Application Logs → Collector/System Log
    - Sources/System Logs → Collector/Application Log
    - Sources/Security Logs → Collector/HardwareEvents Log
    - Sources/“Applications and Services Logs” → Collector/System/Application/HardwareEvents Log



# WEF Log Forwarding – best practices

- Security logs
  - Sources/Security Logs → Collector/HardwareEvents Log
    - Source Security logs cannot be forwarded to the Collector Security log
- Application logs
  - Sources/Application Logs → Collector/Application Log
- System logs
  - Sources/System Logs → Collector/System Log



Connector Setup

### Configure

Enter the parameter details

Forwarded Events Collection	Disabled
Domain Name	Disabled
Domain User Name	Enabled (use AD for sources)
Domain User Password	Enabled (do not use AD for sources)
Active Directory Server	
Active Directory Base DN	ou=<Organizational Unit>,dc=<Domain>
Active Directory Filter	(&(cn=*)(operatingsystem=*)(whencr
Active Directory User Name	
Active Directory User Password	
Active Directory Protocol	non_ssl
Active Directory Port	389
Active Directory Max Page Size	300

< Previous   Next >   Cancel




Connector Setup

### Configure

Enter the parameter details

Forwarded Events Collection	Enabled (do not use AD for sources)
Domain Name	example.com
Domain User Name	arcsight
Domain User Password	●●●●●●●●
Active Directory Server	windows2008.example.com
Active Directory Base DN	dc=example,dc=com
Active Directory Filter	(&(cn=*)(operatingsystem=*)(whencr
Active Directory User Name	arcsight
Active Directory User Password	●●●●●●●●
Active Directory Protocol	non_ssl
Active Directory Port	389
Active Directory Max Page Size	300

< Previous   Next >   Cancel



Configure

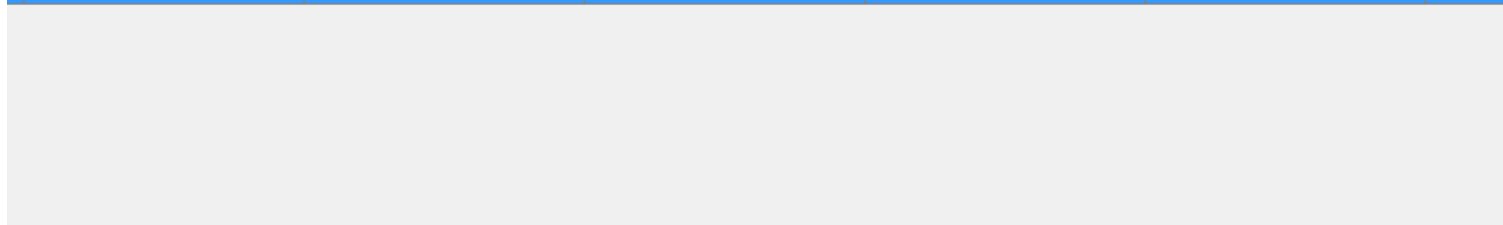
Enter the device details

Domain Name	Host Name	User Name	Password	Security Logs	System Logs	Application	Custom Log Names	Microsoft OS Version	locale
example	WINDOWS2008	arcsight	*****	false	false	false	HardwareEvents	Windows Server 2008 R2	en_US





Security Logs	System Logs	Application	Custom Log Names	Microsoft OS Version	locale
false	false	false	HardwareEvents	Windows Server 2008 R2	en_US



# Windows OS Version

- WEF events can be from different Windows versions than the WEF Collector
  - For example: Collector is Windows Server 2008; Sources are Windows XP, Windows Server 2003
- SmartConnector needs to know what OS in order to parse the events properly
  - It assumes Windows 2008 R2 by default
- Sources
  - Active Directory
    - Enabled (use AD for sources)
  - sourcehosts.csv
    - Enabled (do not use AD for sources)



# Benefits





# Windows Event Forwarding

- Integrated and Free
- Secure and Reliable
- Filtering
- Multi-Tier
- Group Policy
- Laptops/Desktops
  - Source Initiated Subscription



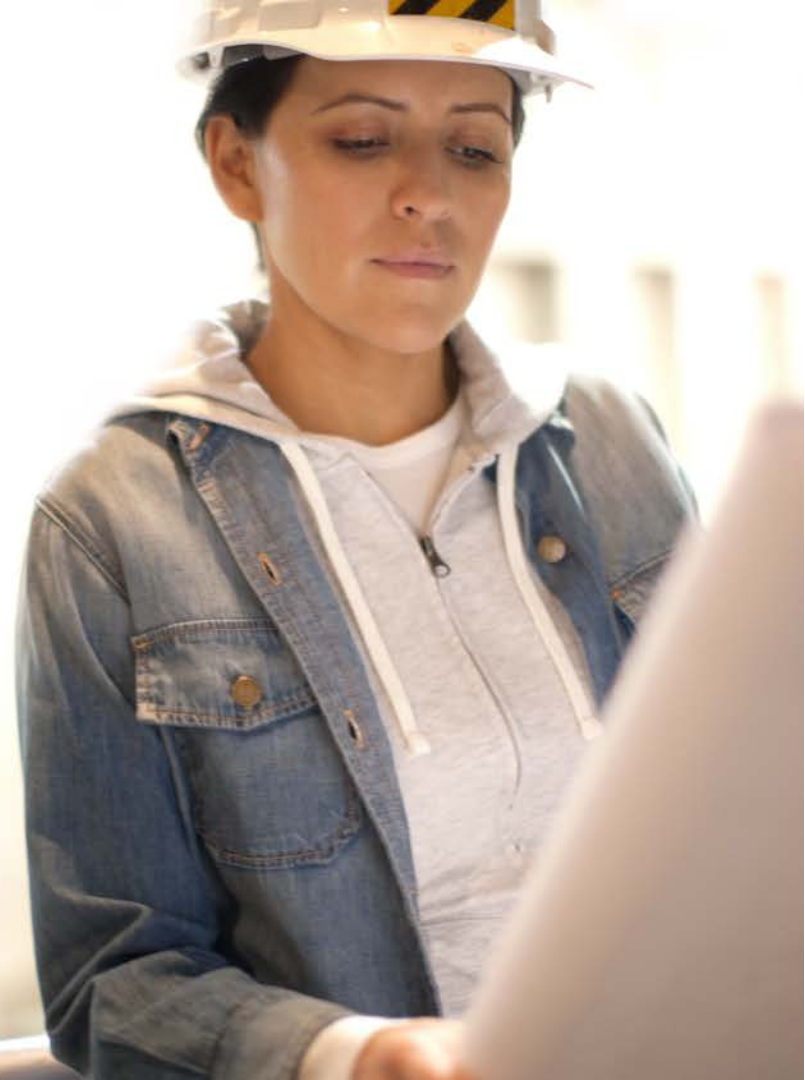
# SmartConnector

- Filtering
- Aggregation
- Caching
- Batching
- Bandwidth Throttling
- Time Correction
- Platforms
  - Windows
  - Linux/Unix
  - Connector Appliance/ArcMC



# Use both!

- The best of both worlds!
- Use both where/when appropriate



# Tips & tricks



# Tips & tricks

- Lab Environment
  - Use a single virtual machine or physical server and forward the event logs locally
- Nested Event Logs
  - All logs under “Applications and Services Logs” in the Windows Event Viewer
    - AppLocker, Windows Defender, etc.
  - We cannot collect these logs
    - These **are not** supported by the WUC
  - Use WEF to forward these to the Application, System, or HardwareEvents log
    - These **are** supported by the WUC
- EVENTCREATE
  - `EVENTCREATE /T ERROR /ID 1000 /L APPLICATION /D "My custom error event for the application log"`
  - `EVENTCREATE /T ERROR /ID 1000 /L SYSTEM /D "My custom error event for the system log"`



# Please give me your feedback

**Session** TB3044     **Speaker** Steve Maxwell

## Use the mobile app

1. Click on **Sessions**
2. Click on **this session**
3. Click on **Rate Session**

## Or use the hard copy surveys

Thank you for providing your feedback, which helps us enhance content for future events.



# Thank you





**Make it matter.**