GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Network Monitoring and Threat Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

EVTX and Windows Event Logging

GCIA Gold Certification

Author: Brandon Charter, bcharter@secureworks.com

Adviser: Brent Deterding

Accepted:

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

Outline

1. **Abstract** 3

2. **What Is EVTX** 4

EVTX Event Definition 4

EVTX Components 11

Event Viewer 11

Windows Event Log Service 13

3. **Working with EVTX Events** 13

Configuring Log Subscriptions 14

Subscription Security 17

4. **Conclusion** 25

5. **References** 25

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

1. Abstract

Auditing and compliance are far more important to an organization than ever before due to security incidents and digital threats. Security professionals are under increasing pressure to understand the changes that occur in increasingly complex IT environments. The collection and aggregation capability of the technology in these complex environments is constantly changing to adapt to the auditing and compliance requirements that many organizations must meet.

Many organizations use Microsoft's Windows platform for desktop, workstation, or server environments. Microsoft has recently reworked the log collection and aggregation functionality of Windows Vista based platforms. The new Windows Event Logging framework and EVTX log format include increased functionality for security professionals to collect and correlate logs.

This paper will explore Microsoft's EVTX log format and Windows Event Logging framework. The EVTX data stream and structure will be defined as a basis for the Windows Event Logging framework and log subscription components that can be used to collect and correlate logs in a complex Windows-based environment.

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

2. What Is EVTX

EVTX is Microsoft's new log format which has been implemented in Vista and Server 2008. The main reason for reworking the previous EVT log format is that there have been very few updates since Windows NT 4.0 to accommodate for the increasing level of compliance that is required today. EVTX includes many new features and enhancements which include many new event properties, the use of channels to publish events, an Extensible Markup Language (XML) format, a new Event Viewer, and a rewritten Windows Event Log service.

EVTX Event Definition

EVTX includes many new event properties which make up each event that is published. One of the new properties introduced in EVTX is the Keywords field. This property stores values which may have previously been stored in the Type field in the EVT format. In the EVT format, the Type field stored the severity and any keywords for each event. In EVTX, the Level property is used to store the severity of the event instead of the Type field. Although not a new property, many Event ID field values changed significantly in EVTX. The Event ID is a unique identifier that is allocated for each type of event and is the most common way to reference a unique event. The Event ID relationship for most security-related events is EVTXEventId = EVTEventId + 4096 (Fitzgerald, 2007).

The following table is a list which Microsoft (*Event Properties,* 2008) has defined as the most common event properties.

Property Name	Description

© SANS Institute 2008, Author retains full rights.

Source	The software that logged the event, which can be either a program name, such as "SQL Server", or a component of the system or of a large program, such as a driver name. For example, "Elnkii" indicates an EtherLink II driver.
Event ID	A number identifying the particular event type. The first line of the description usually contains the name of the event type. For example, 6005 is the ID of the event that occurs when the Event Log service is started. The first line of the description of such an event is "The Event log service was started." The Event ID and the Source can be used by product support representatives to troubleshoot system problems.
Level	A classification of the event severity. The following event severity levels can occur in the system and application logs: **Information.** Indicates that a change in an application or component has occurred, such as an operation has successfully completed, a resource has been created, or a service started. **Warning.** Indicates that an issue has occurred that can impact service or result in a more serious problem if action is not taken. **Error.** Indicates that a problem has occurred, which might impact functionality that is external to the application or component that triggered the event. **Critical.** Indicates that a failure has occurred from which the application or component that triggered the event cannot automatically recover. The following event severity levels can occur in the security log: **Success Audit.** Indicates that the exercise of a user right has succeeded. **Failure Audit.** Indicates that the exercise of a user right has failed.

© SANS Institute 2008, Author retains full rights.

	In the Event Viewer normal list view, these are represented by a symbol.
User	The name of the user on whose behalf the event occurred. This name is the client ID if the event was actually caused by a server process or the primary ID if impersonation is not taking place. Where applicable, a security log entry contains both the primary and impersonation IDs. Impersonation occurs when the server allows one process to take on the security attributes of another.
Operational Code	Contains a numeric value that identifies the activity or a point within an activity that the application was performing when it raised the event. For example, initialization or closing.
Log	The name of the log where the event was recorded.
Task Category	Used to represent a subcomponent or activity of the event publisher.
Keywords	A set of categories or tags that can be used to filter or search for events. Examples include "Network", "Security", or "Resource not found."
Computer	The name of the computer on which the event occurred. The computer name is typically the name of the local computer, but it might be the name of a computer that forwarded the event or it might be the name of the local computer before its name was changed.
Date and Time	The date and time that the event was logged.
Process ID	The identification number for the process that generated the event.
Thread ID	The identification number for the thread that generated the event.
Processor ID	The identification number for the processor that processed the event.
Session ID	The identification number for the terminal server session in which the

© SANS Institute 2008, Author retains full rights.

	event occurred.
Kernal Time	The elapsed execution time for kernal-mode instructions, in CPU time units.
User Time	The elapsed execution time for user-mode instructions, in CPU time units.
Processor Time	The elapsed execution time for user-mode instructions, in CPU ticks.
Correlation Id	Identifies the activity in the process for which the event is involved. This identifier is used to specify simple relationships between events.
Relative Correlation Id	Identifies a related activity in a process for which the event is involved.

One of the most noticeable changes in the EVTX implementation is the use of channels to store events. The Windows Event Log Software Developer Kit defines channels as streams of events which are used by the OS and applications to publish events to a log (*Event Logs and Channels in Windows Event Log,* 2008). The main channels that are included in Vista and Server 2008 are broken up into two groups. The first group is called Windows Logs and this includes the Application, Security, and System channels. It also includes two new channels which are called Setup and ForwardedEvents. The second group of channels is called the Application and Services Logs. This group contains many individual channels which publish events from a single application or component. Figure 1 displays the relationship between channel groups and individual channels.

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

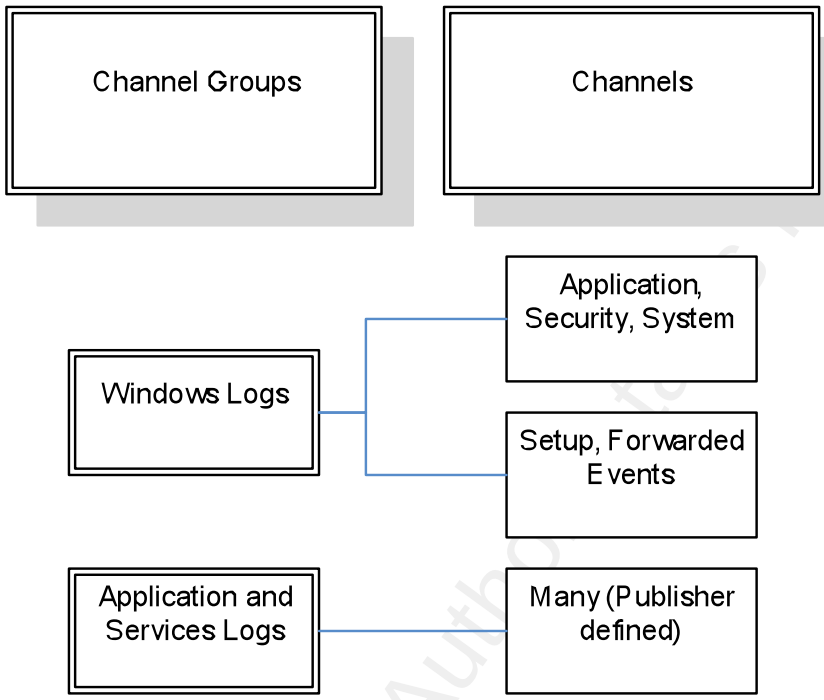


Figure 1

Each channel group has two channel types and each event has an event type. The serviced channel type contains Admin and Operational events. The direct channel type contains Analytic and Debug events. The main difference between the two channel types is that serviced channels can be forwarded and/or collected remotely and direct channels cannot (*Event Logs and Channels in Windows Event Log,* 2008). Figure 2 displays the relationship between channel types and event types.

© SANS Institute 2008, Author retains full rights.

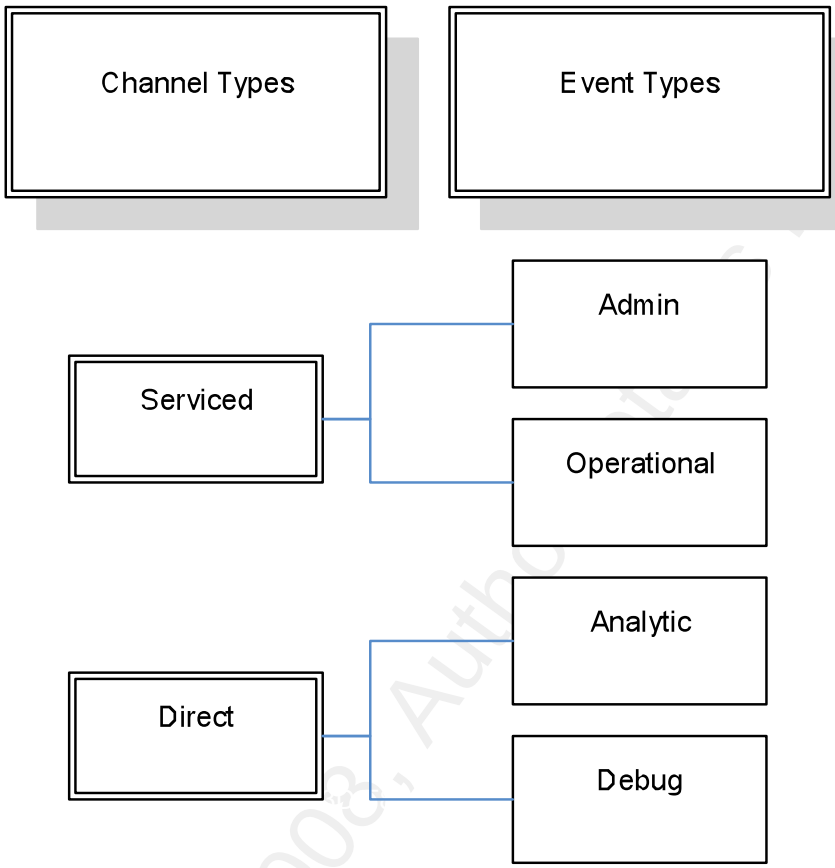


Figure 2

As mentioned above, EVTX logs are stored using a XML format. XML was created to provide a format that could be used to share structured data in a format which allows developers to define their own elements. The characteristics of XML make it the ideal language to use for event logs. The XML log format greatly increases the granularity that can be applied when viewing events in Event Viewer or any other 3rd party application. An example of the XML format in a view from Event Viewer is shown in figure 3.

© SANS Institute 2008, Author retains full rights.

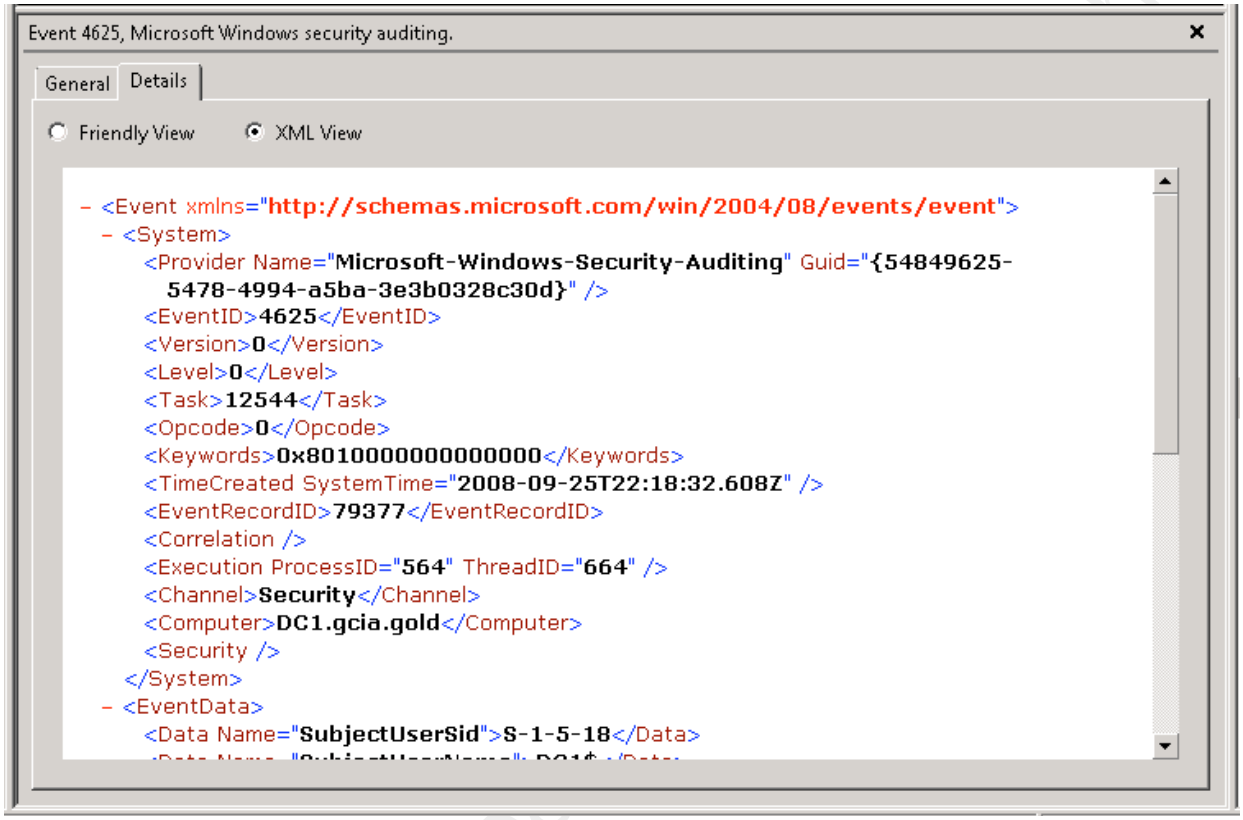


Figure 3

The image displays the XML elements which are defined by the <Element> tags and the data which is defined by the element. The <System> element is required and contains information about the event, while the <EventData> element is not required and it contains the reason the event was published (*Event Representation for Event Consumers,* 2008). XML provides a much more structured format than the EVT format. The default location for the log files are in the following directory: %SystemRoot%\System32\Winevt\Logs\ and they contain the .evtx extension. The default behavior for logs is to overwrite events as needed starting with the oldest events first.

© SANS Institute 2008, Author retains full rights.

EVTX Components

The EVTX log format which has been integrated into all versions of Microsoft Vista and Server 2008 is officially known as Windows Event Log whereas the former EVT format is known simply as Event Logging. Windows Event Log includes a new Event Viewer as well as a rewritten Windows Event Log service.

Event Viewer

Although a detailed review of the new Event Viewer is outside the scope of this paper, understanding the new features of the application are critical to investigating the changes that have been introduced in EVTX. Some of the new features of the new Event Viewer include advanced filtering based on XML, the ability to attach tasks to events, and the ability to use log subscriptions to collect events from remote computers. The new Event Viewer that is included in Vista and Server 2008 is capable of opening event logs that have been stored in the former EVT format. This becomes important when working in a mixed environment or looking at historical data. Using the new Event Viewer is almost a necessity because the previous version that is found in operating systems such as Windows XP and Server 2003 is not capable of reading the new EVTX format. The new Event Viewer is capable of exporting logs in EVTX, XML, TXT, and CSV format.

One of the most useful new features of the Event Viewer is the ability to create a custom view to filter the events which are displayed. The ability to create a custom view can greatly reduce the amount of time that is needed to locate a particular event when compared to the previous version of Event Viewer. Since the EVTX events are stored using XML, custom views allow end users to filter events on each property or field that defines an event. Custom views can also be saved and imported into the Event Viewer to save additional time

© SANS Institute 2008, Author retains full rights.

in the future. The custom view window allows filtering based on when the event was logged, the level, log, source, event ID, keyword, user, and computer. If additional filtering is needed, the custom view window has an XML tab which allows the end user to create a custom view by editing the XML query directly. The XML syntax for a query for all Audit Failures from the Security log is shown in figure 4.

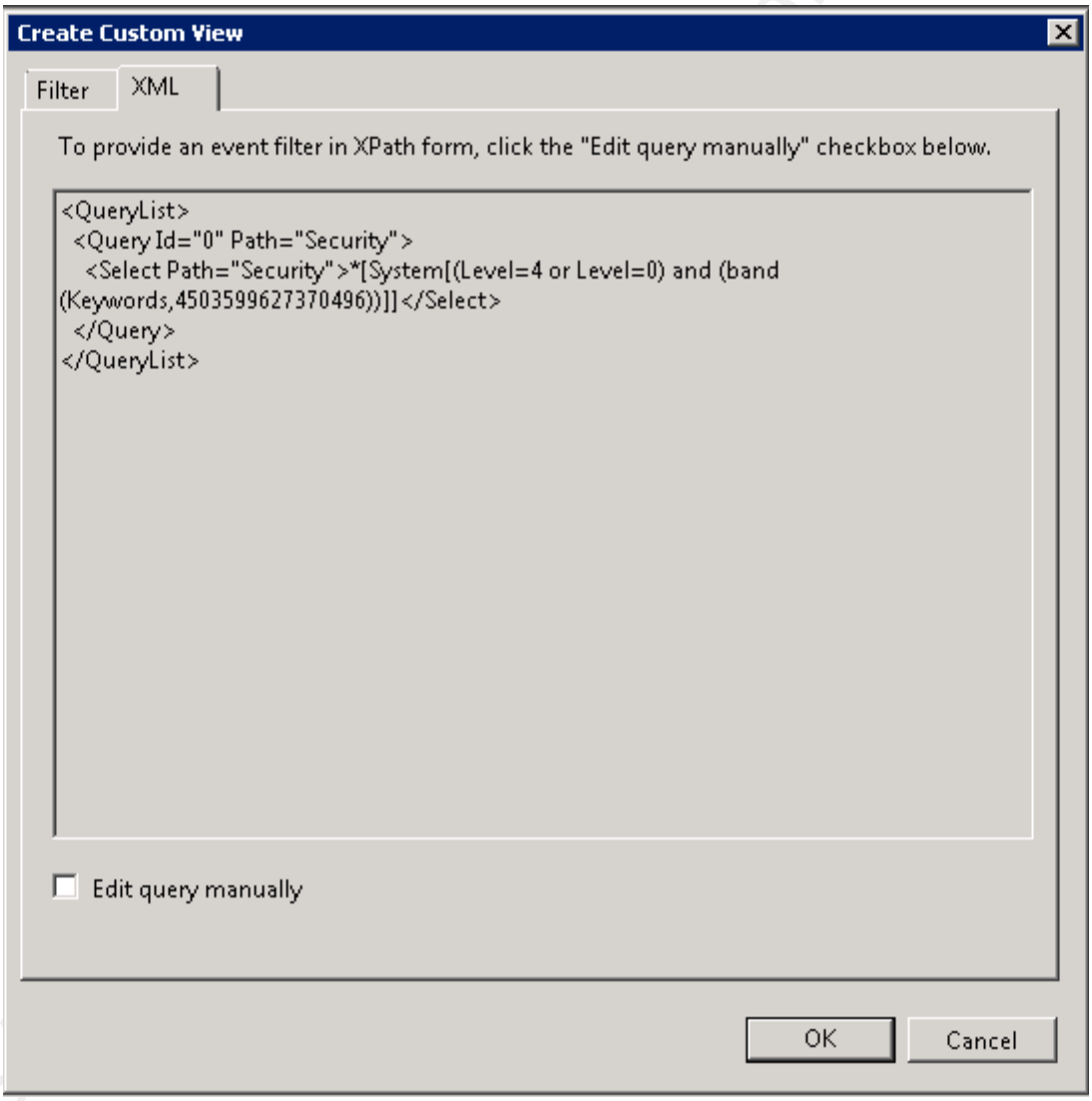


Figure 4

© SANS Institute 2008, Author retains full rights.

The Event Viewer also contains an interface which can be used to attach a task to an event. This new feature has many uses which are virtually limitless. Tasks can be attached to an event which matches a filter that is defined using the same options as the custom views which were described above. This includes the ability to attach a task to an event based on a custom XML filter. In order to attach a task to an event with a custom XML filter, the Task Scheduler must be used instead of the Attach a Task to this Log wizard that is found in the Event Viewer.

Windows Event Log Service

The main reason the Windows Event Log service was rewritten was to eliminate the performance and scalability restrictions that are found in previous versions of Microsoft Windows products. The Windows Event Log service is capable of publishing events in an asynchronous manner which prevents the publishing application from waiting for the service to store the event (Menn, 2006). Once the event is published, the Windows Log Service then performs additional processing based on the type of event. Certain types of events are then handled differently based on the impact they may have on overall system performance. Specifically, Analytic and Debug events are immediately written to a file due to the large volume of these types of events whereas the Admin and Operational events may be delivered to subscribers such as the event forwarder.

3. Working with EVTX Events

The scalability and architecture changes that are included in EVTX are just as important as the changes in the format itself. Log Subscriptions can be used to collect and correlate logs from multiple EVTX enabled hosts throughout a network.

© SANS Institute 2008, Author retains full rights.

Configuring Log Subscriptions

In order to work with Subscriptions, the Windows Event Collector service must be running on the host that will be collecting logs (subscriber). The Windows Remote Management service must be configured and running on the subscriber and any forwarding hosts (forwarder). Although there are various configuration options available, the quickest and easiest way to configure the Windows Remote Management service is to execute the command “winrm quickconfig” on the command line as a privileged user. The quickconfig option will setup the Windows Remote Management service to listen on port 80/tcp on all interfaces, update the Windows Firewall to allow this service on this port, and set the service to start automatically.

Another requirement in configuring a log subscription is that the appropriate user and/or computer permissions must be added on the forwarding host. Log subscriptions can be configured to use user or computer accounts to forward the logs securely from the forwarder to the subscriber. If computer accounts are chosen, the computer account of the subscriber must be added to the local Administrators group of the forwarder. The subscription can also be configured to use any user account which is a member of the local Administrators group on the forwarder.

A log subscription can be setup in the Event Viewer by selecting the Create Subscription link inside the Subscriptions view. The subscriptions properties wizard will then present the user with a view that looks similar to the image show in figure 5. Once a name and description are filled in, the user is presented with a drop down list containing all existing log destinations on the subscriber. The destination log configuration option allows the end user to easily combine logs from multiple forwarders into one central log location. The source

© SANS Institute 2008, Author retains full rights.

computers which will forward logs to the subscriber must then be selected. Subscriptions can be setup as Collector or Source computer initiated types. The user and computer permissions will be setup in this step and vary depending on which subscription type is selected. A filter can be applied to select only the desired events to be forwarded to the subscriber. Filters are configured via same wizard and XML syntax that is described above.

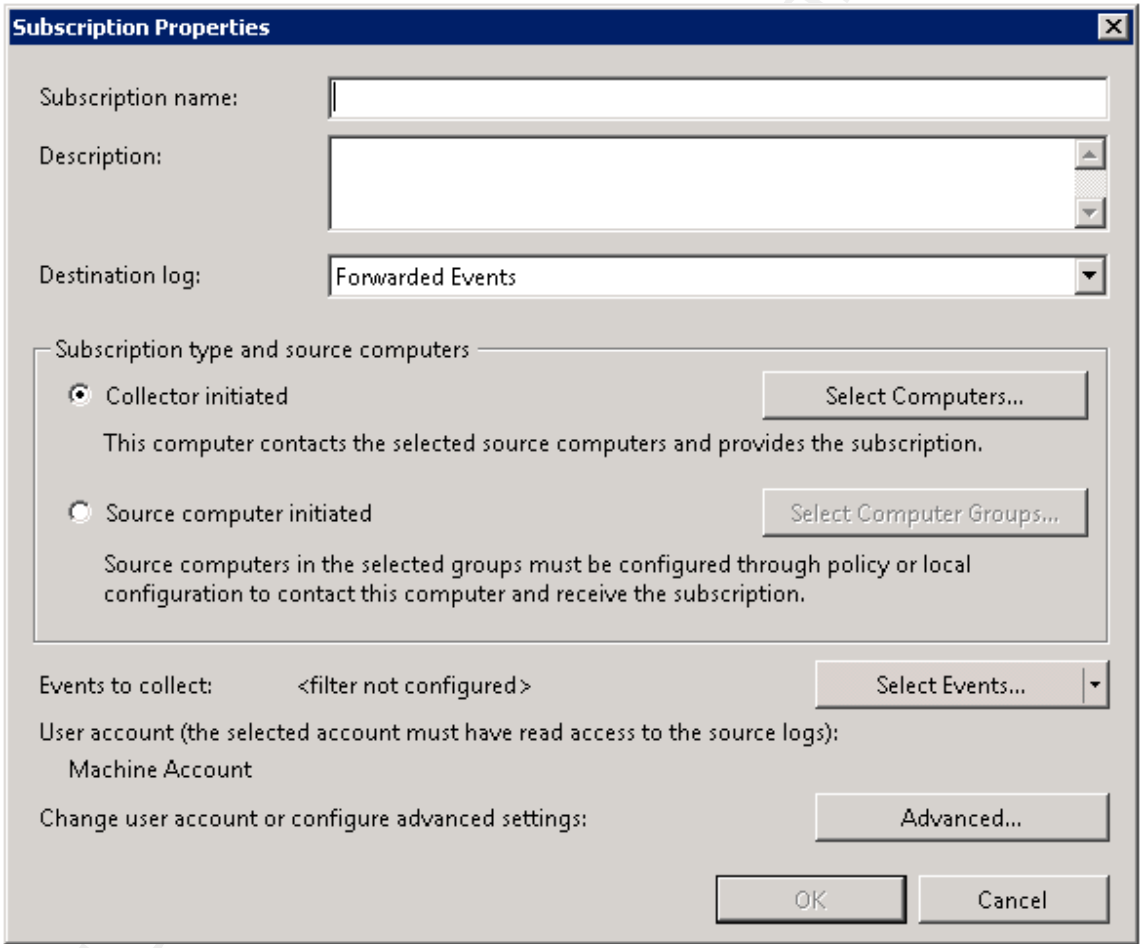


Figure 5

Selecting the advanced settings button loads a wizard which lists options for the user account, speed settings, and the port that will be used by the subscription. There are three

© SANS Institute 2008, Author retains full rights.

speed settings which can be configured when setting up a subscription via the subscription wizard. There is a fourth setting which is to use custom settings via the Windows Event Collector Utility (wecutil) (*Setting up a Source Initiated Subscription,* 2008). The following list describes the three subscription speed settings which can be configured via the wizard (Shields, 2007).

- "Normal mode" configures the target computer to pull event information from the source computer five items at a time, with a batch timeout of 15 minutes.
- "Minimize bandwidth" reverses the direction of the delivery, pushing the data from source to destination. This is helpful if bandwidth is an issue. The influx of log data at the destination is slowed with the batch timeout and the heartbeat interval increases to six hours.
- "Minimize latency" mode works well for gathering real-time or near real-time data. This also uses push mode, but significantly dials up the timeout to every 30 seconds.

The settings for the log subscription are saved to a registry key located at: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\EventCollector\Subscriptions. The settings in the registry key can be viewed by running “wecutil gs” and modified by running “wecutil ss” with the appropriate parameters. Figure 6 shows the output from “wecutil gs” for a subscription named Test.

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, Author retains full rights.

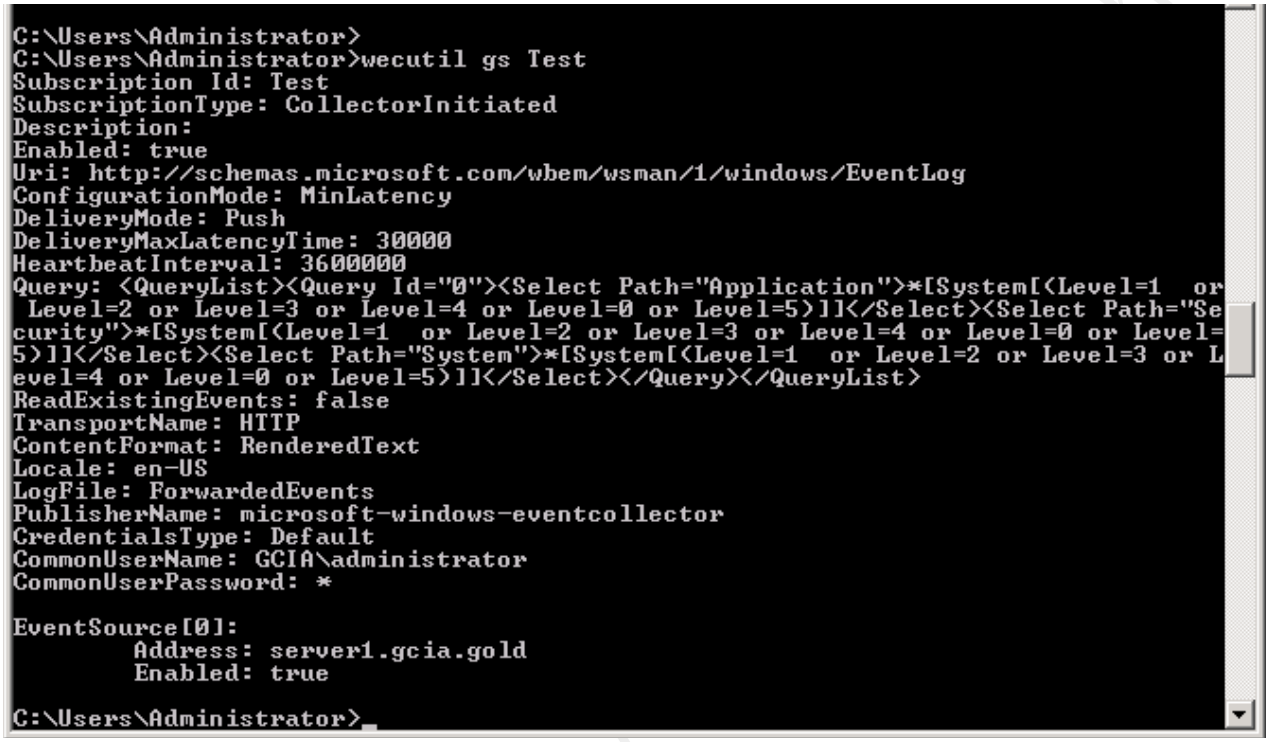


Figure 6

The wecutil contains many configuration options that are not displayed in the subscription wizard. One such option allows fine tuning of the latency and heartbeat intervals described above when the value of ConfigurationMode is set to Custom. The wecutil has many additional command line options which can be used to configure and troubleshoot a subscription. The best documentation on the utility can be found by using the built in help which is displayed by running “wecutil /?” on the command line.

Subscription Security

As described above, there are two services which subscriptions use to forward and receive events from remote hosts. The main focus on security will be based around the Windows Remote Management service which handles the network communication between

© SANS Institute 2008, Author retains full rights.

the subscriber and the forwarder. There are two configuration options when setting up Windows Remote Management which control how the data being transferred is encrypted. The first option is to use HTTP (TCP port 80) which will transmit the data in clear text. The second configuration option is to use HTTPS (TCP port 443) which will use a certificate to encrypt the data via an SSL tunnel.

A test environment was created in order to investigate the security of the HTTP and HTTPS options of the Windows Remote Management service. The test environment includes an Active Directory Domain (GCIA.GOLD) which contains two Windows Server 2008 Standard 32-bit hosts. The domain contains a single domain controller (DC1.GCIA.GOLD/10.1.1.200) which the log subscriber, and the log forwarder (SERVER1.GCIA.GOLD/10.1.1.201). Wireshark 1.0.3 was used to perform multiple packet captures on the subscriber (DC1.GCIA.GOLD).

The packet captures in figures 7 and 8 are from a standard log subscription between DC1 and SERVER1. The TCP three-way-handshake and Ethernet layer is not shown. The log subscription in figure 7 was configured using the HTTP option. Although the HTTP layer of the packet is not encrypted, the Windows Remote Management service does not accept traffic that is not encrypted using the Kerberos Security Service Provider or negotiate authentication (*Authentication for Remote Connections,* 2008). The Windows Remote Management service utilizes Simple Object Access Protocol (SOAP) to transfer data and commands to/from the service (*Configuration and Security,* 2008). The yellow highlighting in figure 7 shows the Content-Type field of the HTTP header has a value of application/soap + xml indicating that the HTTP header in this transmission was not encrypted. The red highlighting shows that the data portion of the log transmission was encrypted via an encrypted HTTP Kerberos session.

© SANS Institute 2008, Author retains full rights.

```
No.     Time        Source                Destination           Protocol Info
     10 0.719618    10.1.1.200            10.1.1.201            HTTP     POST /wsman HTTP/1.1
Internet Protocol, Src: 10.1.1.200 , Dst: 10.1.1.201
Transmission Control Protocol, Src Port: 49205 (49205), Dst Port: http (80), Seq: 1, Ack: 1,
Len: 2149
Hypertext Transfer Protocol

0000  00 0c 29 4a 79 36 00 0c 29 f6 3d 9e 08 00 45 00   ..)Jy6..).=...E.
0010  08 8d 1a 16 40 00 80 06 00 00 0a 01 01 c8 0a 01   ....@...........
0020  01 c9 c0 35 00 50 14 6b 5c f0 33 b4 6d 86 50 18   ...5.P.k\.3.m.P.
0030  40 29 17 99 00 00 50 4f 53 54 20 2f 77 73 6d 61   @)....POST /wsma
0040  6e 20 48 54 54 50 2f 31 2e 31 0d 0a 41 75 74 68   n HTTP/1.1..Auth
0050  6f 72 69 7a 61 74 69 6f 6e 3a 20 4b 65 72 62 65   orization: Kerbe
0060  72 6f 73 20 59 49 49 46 72 51 59 4a 4b 6f 5a 49   ros YIIFrQYJKoZI
0070  68 76 63 53 41 51 49 43 41 51 42 75 67 67 57 63   hvcSAQICAQBuggWc
0080  4d 49 49 46 6d 4b 41 44 41 67 45 46 6f 51 4d 43   MIIFmKADAgEFoQMC
0090  41 51 36 69 42 77 4d 46 41 43 41 41 41 41 43 6a   AQ6iBwMFACAAAACj
…snip…
07d0  43 7a 42 35 55 6b 54 79 50 67 31 39 63 58 34 42   CzB5UkTyPg19cX4B
07e0  6f 58 6b 6e 6c 79 58 76 48 4b 50 72 6e 4d 6d 2b   oXknlyXvHKPrnMm+
07f0  55 33 67 59 78 44 62 68 59 4e 59 3d 0d 0a 43 6f   U3gYxDbhYNY=..Co
0800  6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c   ntent-Type: appl
0810  69 63 61 74 69 6f 6e 2f 73 6f 61 70 2b 78 6d 6c   ication/soap+xml
0820  3b 63 68 61 72 73 65 74 3d 55 54 46 2d 31 36 0d   ;charset=UTF-16.
0830  0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 69 63   .User-Agent: Mic
0840  72 6f 73 6f 66 74 20 57 69 6e 52 4d 20 43 6c 69   rosoft WinRM Cli
0850  65 6e 74 0d 0a 48 6f 73 74 3a 20 53 45 52 56 45   ent..Host: SERVE
0860  52 31 2e 67 63 69 61 2e 67 6f 6c 64 0d 0a 43 6f   R1.gcia.gold..Co
0870  6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 0d   ntent-Length: 0.
0880  0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65   .Connection: Kee
0890  70 2d 41 6c 69 76 65 0d 0a 0d 0a                   p-Alive....


No.     Time        Source                Destination           Protocol Info
     17 1.410407    10.1.1.200            10.1.1.201            HTTP     POST /wsman HTTP/1.1
(multipart/encrypted)
Internet Protocol, Src: 10.1.1.200, Dst: 10.1.1.201
```


© SANS Institute 2008, Author retains full rights.

```
Transmission Control Protocol, Src Port: 49205 (49205), Dst Port: http (80), Seq: 2150, Ack:
342, Len: 953
Hypertext Transfer Protocol
Media Type

0000  00 0c 29 4a 79 36 00 0c 29 f6 3d 9e 08 00 45 00   ..)Jy6..).=...E.
0010  03 e1 1a 19 40 00 80 06 00 00 0a 01 01 c8 0a 01   ....@...........
0020  01 c9 c0 35 00 50 14 6b 65 55 33 b4 6e db 50 18   ...5.P.keU3.n.P.
0030  3f d3 1b 66 00 00 50 4f 53 54 20 2f 77 73 6d 61   ?..f..POST /wsma
0040  6e 20 48 54 54 50 2f 31 2e 31 0d 0a 55 73 65 72   n HTTP/1.1..User
0050  2d 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66   -Agent: Microsof
0060  74 20 57 69 6e 52 4d 20 43 6c 69 65 6e 74 0d 0a   t WinRM Client..
0070  43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 6d 75   Content-Type: mu
0080  6c 74 69 70 61 72 74 2f 65 6e 63 72 79 70 74 65   ltipart/encrypte
0090  64 3b 70 72 6f 74 6f 63 6f 6c 3d 22 61 70 70 6c   d;protocol="appl
00a0  69 63 61 74 69 6f 6e 2f 48 54 54 50 2d 4b 65 72   ication/HTTP-Ker
00b0  62 65 72 6f 73 2d 73 65 73 73 69 6f 6e 2d 65 6e   beros-session-en
00c0  63 72 79 70 74 65 64 22 3b 62 6f 75 6e 64 61 72   crypted";boundar
00d0  79 3d 22 45 6e 63 72 79 70 74 65 64 20 42 6f 75   y="Encrypted Bou
00e0  6e 64 61 72 79 22 0d 0a 48 6f 73 74 3a 20 53 45   ndary"..Host: SE
00f0  52 56 45 52 31 2e 67 63 69 61 2e 67 6f 6c 64 0d   RVER1.gcia.gold.
0100  0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a   .Content-Length:
0110  20 37 30 33 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e    703..Connection
0120  3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d 0a   : Keep-Alive....
0130  2d 2d 20 45 6e 63 72 79 70 74 65 64 20 42 6f 75   -- Encrypted Bou
0140  6e 64 61 72 79 0d 0a 09 43 6f 6e 74 65 6e 74 2d   ndary...Content-
0150  54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f   Type: applicatio
0160  6e 2f 48 54 54 50 2d 4b 65 72 62 65 72 6f 73 2d   n/HTTP-Kerberos-
0170  73 65 73 73 69 6f 6e 2d 65 6e 63 72 79 70 74 65   session-encrypte
0180  64 0d 0a 09 4f 72 69 67 69 6e 61 6c 43 6f 6e 74   d...OriginalCont
0190  65 6e 74 3a 20 74 79 70 65 3d 61 70 70 6c 69 63   ent: type=applic
01a0  61 74 69 6f 6e 2f 73 6f 61 70 2b 78 6d 6c 3b 63   ation/soap+xml;c
01b0  68 61 72 73 65 74 3d 55 54 46 2d 31 36 3b 4c 65   harset=UTF-16;Le
01c0  6e 67 74 68 3d 33 39 38 0d 0a 2d 2d 20 45 6e 63   ngth=398..-- Enc
01d0  72 79 70 74 65 64 20 42 6f 75 6e 64 61 72 79 0d   rypted Boundary.
01e0  0a 09 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20   ..Content-Type:
01f0  61 70 70 6c 69 63 61 74 69 6f 6e 2f 6f 63 74 65   application/octe
```


© SANS Institute 2008, Author retains full rights.

```
0200  74 2d 73 74 72 65 61 6d 0d 0a 3c 00 00 00 05 04   t-stream..<.....
0210  06 ff 00 00 00 1c 00 00 00 00 53 f9 9c 74 22 42   ..........S..t"B
0220  e7 3c 38 54 47 42 49 01 30 94 1e 3a f0 ae cf 6c   .<8TGBI.0..:...l
0230  63 32 25 28 63 b2 ef 62 27 82 0b e7 5d d2 94 c8   c2%(c..b'...]...
0240  7d 79 8b 35 17 90 da f7 1c 7f 30 c8 cd 6c 89 67   }y.5......0..l.g
0250  8d 94 58 e3 97 98 12 0e 8f 81 76 d1 b4 1b 6e 3b   ..X.......v...n;
0260  79 50 f2 ef 42 93 33 0e 22 38 27 16 c5 d5 ba 1c   yP..B.3."8'.....
0270  73 77 51 23 4a bb dd 6c 54 39 56 f1 9c f3 43 a1   swQ#J..lT9V...C.
0280  fe 82 cc 7a 74 0e f9 70 a7 bf 6e bf 62 b8 a2 5f   ...zt..p..n.b.._
0290  90 6c 3d 9b d8 19 c2 89 20 9c 38 8d 0b 93 43 a9   .l=..... .8...C.
02a0  bc ac 17 e2 34 89 6a c1 30 7a 5f 09 9e 83 e1 51   ....4.j.0z_....Q
02b0  b5 9b b3 dc 03 ad 44 fb 17 df e7 6d 05 58 cc b5   ......D....m.X..
02c0  e9 70 4d e1 97 71 db 96 c4 95 0c 99 cb 5e a5 75   .pM..q.......^.u
02d0  77 2e b8 e7 1c 02 01 20 18 55 d7 83 01 32 b1 7f   w..... .U...2..
02e0  8e 3d 28 ad 7d cc 1c 75 17 09 8a 3b e3 6c a1 ab   .=(.}..u...;.l..
02f0  13 76 e9 1b b5 31 d1 5d 73 72 e8 0b 81 f6 df 02   .v...1.]sr......
0300  2e 6d b4 80 d5 b3 4a 68 82 d9 e6 4c 1b 0d a1 0d   .m....Jh...L....
0310  f4 74 e1 c1 98 7e 0b ca d7 d2 32 bf 8b 81 6f a6   .t...~....2...o.
0320  53 ef f5 e0 0c 64 5e 8a 48 11 13 08 c5 e4 d4 f4   S....d^.H.......
0330  6b ec a3 da c1 08 48 56 fb 8f 6f 26 b7 9d ec c9   k.....HV..o&....
0340  e2 95 08 be 41 b9 ea 3f 16 5a 93 e2 92 31 e6 e5   ....A..?.Z...1..
0350  b3 60 2f 52 fa d5 2e b7 49 36 4b 75 fd 03 d4 87   .`/R....I6Ku....
0360  69 cb 27 36 7b 33 29 e6 0f 60 71 3d 86 20 18 14   i.'6{3)..`q=. ..
0370  08 4f 49 3f e1 e3 72 00 c2 47 38 9f f7 81 5e f6   .OI?..r..G8...^.
0380  5c f4 61 3e c5 ee c3 79 7b 39 27 6b 38 0d 36 f7   \.a>...y{9'k8.6.
0390  17 e1 9e 22 48 a9 b7 21 ff e2 52 e5 2f 51 4d bf   ..."H..!..R./QM.
03a0  36 7f e7 e8 c9 a8 ce 34 e2 fa 76 c8 8e 65 5f d6   6......4..v..e_.
03b0  68 8f 88 b9 67 41 fb e4 42 40 16 47 76 df e0 4a   h...gA..B@.Gv..J
03c0  a8 3b 2d 5d 63 a9 63 28 08 58 d1 b6 33 1c c5 fa   .;-]c.c(.X..3...
03d0  ba 3a 95 69 84 a8 f5 2c 2d 2d 20 45 6e 63 72 79   .:.i...,-- Encry
03e0  70 74 65 64 20 42 6f 75 6e 64 61 72 79 0d 0a      pted Boundary..
```

Figure 7

A log subscription that is configured using the HTTPS option will not contain an unencrypted HTTP header as all data is encrypted in a standard SSL tunnel. Figure 8 shows

© SANS Institute 2008, Author retains full rights.

a full SSL handshake and log transmission from a log subscription configured to use HTTPS. The yellow highlighting shows that this traffic is using TLSv1 and the green highlighting shows the TLS handshake steps as identified by Wireshark. The red highlighting shows the Application Data packet containing the encrypted HTTP header.

```
No.     Time        Source                Destination           Protocol Info
      5 167.645910  10.1.1.201            10.1.1.200            TLSv1    Client Hello
Internet Protocol, Src: 10.1.1.201 , Dst: 10.1.1.200
Transmission Control Protocol, Src Port: 64392 (64392), Dst Port: https (443), Seq: 1, Ack: 1,
Len: 146
Secure Socket Layer

0000  00 0c 29 f6 3d 9e 00 0c 29 4a 79 36 08 00 45 00   ..).=...)Jy6..E.
0010  00 ba 4e 51 40 00 80 06 94 5a 0a 01 01 c9 0a 01   ..NQ@....Z......
0020  01 c8 fb 88 01 bb 0b fe f7 77 31 05 84 dd 50 18   .........w1...P.
0030  40 29 0d 97 00 00 16 03 01 00 8d 01 00 00 89 03   @).............
0040  01 48 e5 62 3c 92 7b 41 36 4f fa 50 d9 91 a9 62   .H.b<.{A6O.P...b
0050  e7 26 c7 37 2e 1b 76 1f bc 2e 3d 64 85 70 c0 bb   .&.7..v...=d.p..
0060  f4 20 54 23 00 00 30 bd 60 f9 ad f8 e0 81 a0 c1   . T#..0.`.......
0070  76 de 76 76 0b 85 ea e8 19 04 08 9c e7 09 8d d1   v.vv............
0080  c2 f9 00 18 00 2f 00 35 00 05 00 0a c0 09 c0 0a   ...../.5........
0090  c0 13 c0 14 00 32 00 38 00 13 00 04 01 00 00 28   .....2.8.......(
00a0  00 00 00 12 00 10 00 00 0d 64 63 31 2e 67 63 69   .........dc1.gci
00b0  61 2e 67 6f 6c 64 00 0a 00 08 00 06 00 17 00 18   a.gold..........
00c0  00 19 00 0b 00 02 01 00                           ........

No.     Time        Source                Destination           Protocol Info
      6 167.648401  10.1.1.200            10.1.1.201            TLSv1    Server Hello, Change Cipher
Spec, Encrypted Handshake Message
Internet Protocol, Src: 10.1.1.200 , Dst: 10.1.1.201
Transmission Control Protocol, Src Port: https (443), Dst Port: 64392 (64392), Seq: 1, Ack:
147, Len: 138
Secure Socket Layer

0000  00 0c 29 4a 79 36 00 0c 29 f6 3d 9e 08 00 45 00   ..)Jy6..).=...E.
```


© SANS Institute 2008, Author retains full rights.

```
0010  00 b2 05 26 40 00 80 06 00 00 0a 01 01 c8 0a 01   ...&@...........
0020  01 c9 01 bb fb 88 31 05 84 dd 0b fe f8 09 50 18   ......1.......P.
0030  01 00 18 37 00 00 16 03 01 00 4a 02 00 00 46 03   ...7......J...F.
0040  01 48 e5 62 3c 3f 3f 11 b7 cd 0e dd 67 1c da 08   .H.b<??.....g...
0050  6e a0 8f 8c f2 27 51 f5 fd 0e 4a 28 aa 38 46 d8   n....'Q...J(.8F.
0060  69 20 54 23 00 00 30 bd 60 f9 ad f8 e0 81 a0 c1   i T#..0.`.......
0070  76 de 76 76 0b 85 ea e8 19 04 08 9c e7 09 8d d1   v.vv............
0080  c2 f9 00 2f 00 14 03 01 00 01 01 16 03 01 00 30   .../...........0
0090  a7 12 fe 74 81 55 3b cf 8b 8d 4b 43 c8 4b 75 e6   ...t.U;...KC.Ku.
00a0  bf 46 bd 6d 5a 52 9a 8a 14 c4 a8 26 04 d5 90 4e   .F.mZR.....&...N
00b0  dd 13 ab 5c c6 72 d2 0c 43 d3 b3 08 5b 24 70 aa   ...\.r..C...[$p.
```

No. Time Source Destination Protocol Info
7 167.651713 10.1.1.201 10.1.1.200 TLSv1 Application Data
Internet Protocol, Src: 10.1.1.201 , Dst: 10.1.1.200
Transmission Control Protocol, Src Port: 64392 (64392), Dst Port: https (443), Seq: 147, Ack: 139, Len: 293
Secure Socket Layer

```
0000  00 0c 29 f6 3d 9e 00 0c 29 4a 79 36 08 00 45 00   ..).=...)Jy6..E.
0010  01 4d 4e 53 40 00 80 06 93 c5 0a 01 01 c9 0a 01   .MNS@...........
0020  01 c8 fb 88 01 bb 0b fe f8 44 31 05 85 67 50 18   .........D1..gP.
0030  40 06 0d b5 00 00 17 03 01 01 20 86 b0 ac 4f ed   @.........  ...O.
0040  f6 33 df bc 80 41 9c 26 e8 25 82 0b 94 ea 6f 18   .3...A.&.%....o.
0050  36 29 83 ac 6c cd eb 69 8b 1a 95 3c 28 4a eb 29   6)..l..i...<(J.)
0060  98 03 8f 51 f0 85 d6 ce f4 22 a7 9e 15 53 68 15   ...Q....."...Sh.
0070  72 38 d5 fb 8a 5a b2 ea c0 22 fc a0 4e 42 3a 05   r8...Z..."..NB:.
0080  4e 9b cc 69 ee df 7b 36 a9 67 5d 3e 76 68 64 9b   N..i..{6.g]>vhd.
0090  10 55 aa 78 26 98 f2 88 e0 bc 31 4c 47 2d 20 e7   .U.x&.....1LG- .
00a0  e2 4a ef 38 4d bf 6c 21 c2 ff 58 c4 eb 93 74 29   .J.8M.l!..X...t)
00b0  af b0 c8 d8 38 d4 2b fa b1 a4 c4 23 ab 36 53 f0   ....8.+....#.6S.
00c0  ee 28 be 03 1b 54 5a 95 e5 4b cc 68 47 0c e3 d8   .(...TZ..K.hG...
00d0  51 4f 00 33 12 8a ce 98 7b 48 95 79 01 68 b3 a9   QO.3....{H.y.h..
00e0  61 82 0e c0 70 39 45 18 be a8 ff be dd 27 fc 04   a...p9E......'..
00f0  e8 64 b7 22 b2 f5 ba ac 75 4a fd 30 65 e0 99 7e   .d."....uJ.0e..~
0100  d3 cb c5 fd 73 ba 9e 9e c7 d2 cd 41 a4 f5 a1 25   ....s......A...%
0110  31 0c a3 f3 00 03 0d 31 4c 4b f3 2a da df 4d e0   1......1LK.*..M.
```


© SANS Institute 2008, Author retains full rights.

```
0120  08 ae d6 dd f6 ce 3e 11 2e 20 ed 4e 2d 82 e6 1c   ......>.. .N-...
0130  f1 1d 81 b5 35 1b d7 5e 72 67 5c d0 86 fb f6 1f   ....5..^rg\.....
0140  d3 0a 84 51 9e 4a c9 95 03 30 78 a6 3e f3 07 ce   ...Q.J...0x.>...
0150  6b 9c 5b b3 14 3b 55 09 5e ed ac                  k.[..;U.^..
```

Figure 8

Authentication to the Windows Remote Management service supports four types of authentication which is used to validate the incoming connection request. According to the Microsoft Developer Network documentation, Windows Remote Management supports four types of authentication (*Authentication for Remote Connections,* 2008).

- Basic - the username and password are sent in the authentication exchange. Basic authentication is the least secure authentication type and is disabled by default.
- Negotiate – Windows implementation of Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO). This is also known as Windows Integrated Authentication.
- Kerberos – a mutual authentication using encrypted keys. The client and server must be members of a domain to use Kerberos authentication.
- Client Certificate-based – uses SSL certificate to authenticate and map a certificate to a local account. This authentication type is required for communication between non-members and members of a domain.

A log subscription can be configured to forward events from both members and non-members of a domain. Hosts which are members of a domain can forward events using the HTTPS option without the use of a certificate. Non-members of a domain can only forward events using the HTTPS option and a certificate is required using the default configuration. This default setting can be modified in the Windows Remote Management configuration by allowing Basic authentication and adding the remote host to the TrustedHosts list (*Windows*

© SANS Institute 2008, Author retains full rights.

Remote Management Glossary, 2008).

4. Conclusion

EVTX and Windows Event Logging framework include many new features which give security professionals and IT administrators more power to accurately correlate and aggregate logs in a Windows environment. The EVTX format includes new fields which can store data that can be filtered and sorted via the underlying XML structure. The use of log subscriptions takes the pain out of log aggregation in a Windows environment. Log subscriptions can be deployed across an entire domain with the help of Active Directory. These changes and enhancements should allow organizations to meet the auditing and compliance requirements that may be required in many environments.

5. References

Authentication for Remote Connections. (2008, May 15). Retrieved July 18, 2008, from Microsoft Web site: http://msdn.microsoft.com/en-us/library/aa384295(VS.85).aspx

Configuration and Security. Retrieved September 28, 2008, from Microsoft Web site: http://technet.microsoft.com/en-us/library/cc782312.aspx

Event Logs and Channels in Windows Event Log. (2008, September 19). Retrieved September 22, 2008, from Microsoft Web site: http://msdn.microsoft.com/en-us/library/aa385225.aspx

Event Properties. Retrieved July 18, 2008, from Microsoft Web site: http://technet.microsoft.com/en-us/library/cc765981.aspx

Event Representation for Event Consumers. (2008, September 19). Retrieved September 22, 2008, from Microsoft Web site: http://msdn.microsoft.com/en-us/library/aa385229.aspx

© SANS Institute 2008, Author retains full rights.

Fitzgerald, E. (2007, April 18). Vista Security Events Get Noticed. Message posted to http://blogs.msdn.com/ericfitz/archive/2007/04/18/vista-security-events-get-noticed.aspx

Menn, V. (2006, November). Windows Vista: New Tools for Event Management in Windows Vista . *TechNet Magazine*. Retrieved September 10, 2008, from Microsoft Web site: http://technet.microsoft.com/en-us/magazine/cc160886.aspx

Setting up a Source Initiated Subscription. (2008, September 19). Retrieved September 23, 2008, from Microsoft Web site: http://msdn.microsoft.com/en-us/library/bb870973(VS.85).aspx

Shields, G. (2007, August). Syslog…20 Years Later. *Redmond Magazine*. Retrieved August 2, 2008, from: http://redmondmag.com/columns/article.asp?editorialsid=1868

Windows Remote Management Glossary. (2008, May 15). Retrieved July 18, 2008, from Microsoft Web site: http://msdn.microsoft.com/en-us/library/aa384465(VS.85).aspx

© SANS Institute 2008, Author retains full rights.

© SANS Institute 2008, Author retains full rights.