



IBM India Software Labs

# **Tivoli Security Information and Event Manager**

## **Integration of Event sources, User Information Sources Ubiquitous and W7 event sources**

***Aslam Siddiqui***

***Boudhayan Chakrabarty***

## Integration of Event sources

- **Audit data is collected from various devices and applications using event sources**
- **To establish event monitoring in Tivoli® Security Information and Event Manager, you must deploy one or more event sources**
- **An event source can be a database, an application, an operating system, a network device, or other platform that records its events in logs and to which the Tivoli Security Information and Event Manager has access in order to collect a selection of security-relevant logs for event monitoring and reporting.**

## Event source deployment

- **After Tivoli Security Information and Event Manager is installed, you have the capability for across-the-board activity monitoring in your network environment.**
- **This activity monitoring, also known as event monitoring, is limited only by the number of event sources that Tivoli Security Information and Event Manager supports.**
- **Before an Tivoli Security Information and Event Manager supported event source can be audited, you must enable auditing and configure the event source by performing the following steps as required.**

# Auditing and Configuring the Event source

- 1. Select the audit scenario that is most suitable for collecting data from the event source.**
- 2. Ensure that the Tivoli Security Information and Event Manager Server is operational.**
- 3. If the audit scenario requires an agent on a system other than a Tivoli Security Information and Event Manager Server:**
  - a-Ensure that the system has network connectivity to the Tivoli Security Information and Event Manager Server.**
  - b-Verify that network communication on ports 5992 and 5993 is permitted through any firewalls or other network devices that are located between the server and the system.**

## Continued..

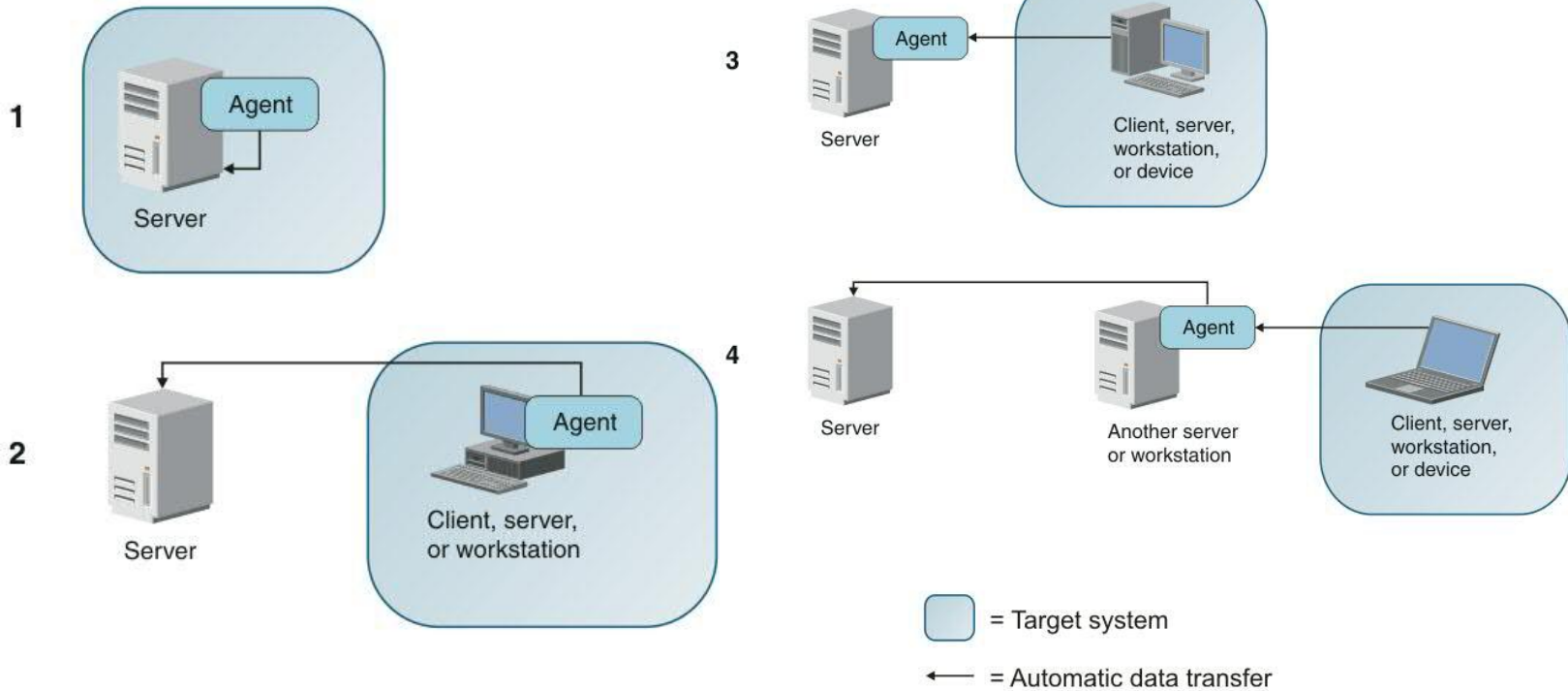
- c-If the agent is not already installed on the system, install it.**
- d-Verify that the agent can successfully communicate with the server.**
- 4. If any special configuration must be performed to enable data collection, do that now.**
- 5. Add the event source to the Tivoli Integrated Portal.**
- 6. Adjust the event source properties, if necessary.**
- 7. Verify that the Tivoli Security Information and Event Manager supports the defined event source correctly.**

**Note: The time zone for the target machine is retrieved from the agent system in most cases**

## Data Collection scenarios

- **Choose one of eight different collection scenarios to obtain data from an event source**
- **An event source data collection configuration includes the following components:**
- **Target system-The system on which events occur and are recorded in logs that provide the audit data for Tivoli® Security Information and Event Manager.**
- **Agent system- A system where the agent software is installed to collect the audit data.**
- **Tivoli Security Information and Event Manager Server - A system where audit data is collected and investigated using TSIEM.**

# Data Collection scenarios 1-4



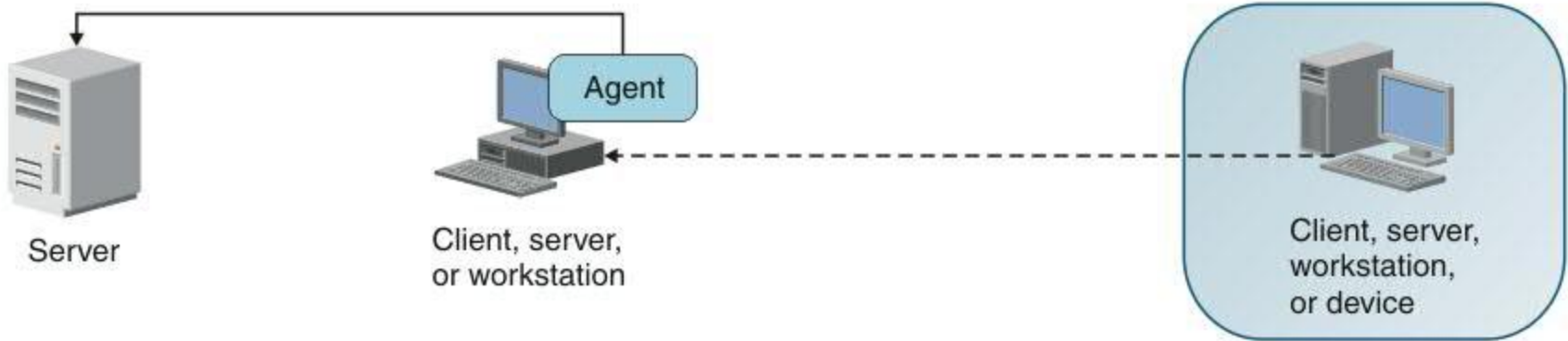


# Data Collection scenarios 5-6

5



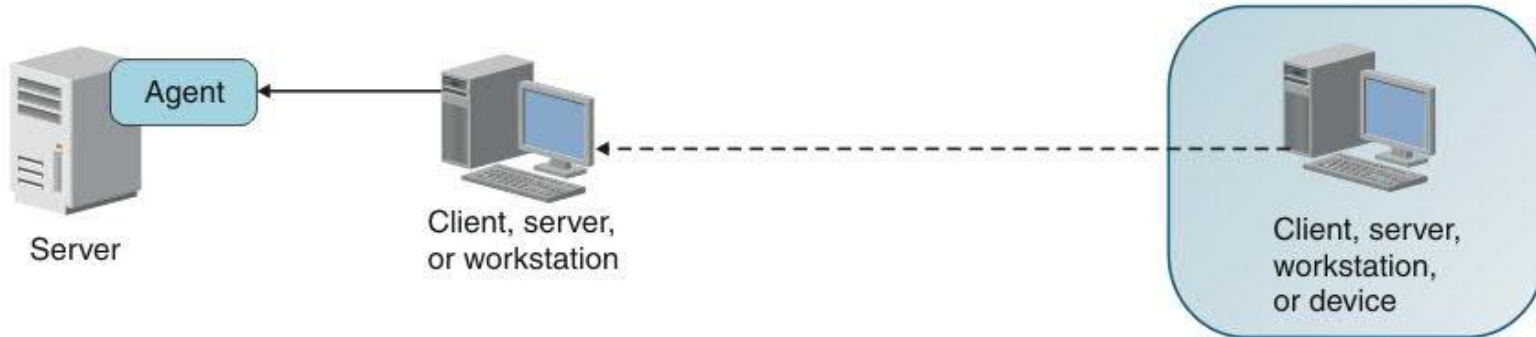
6



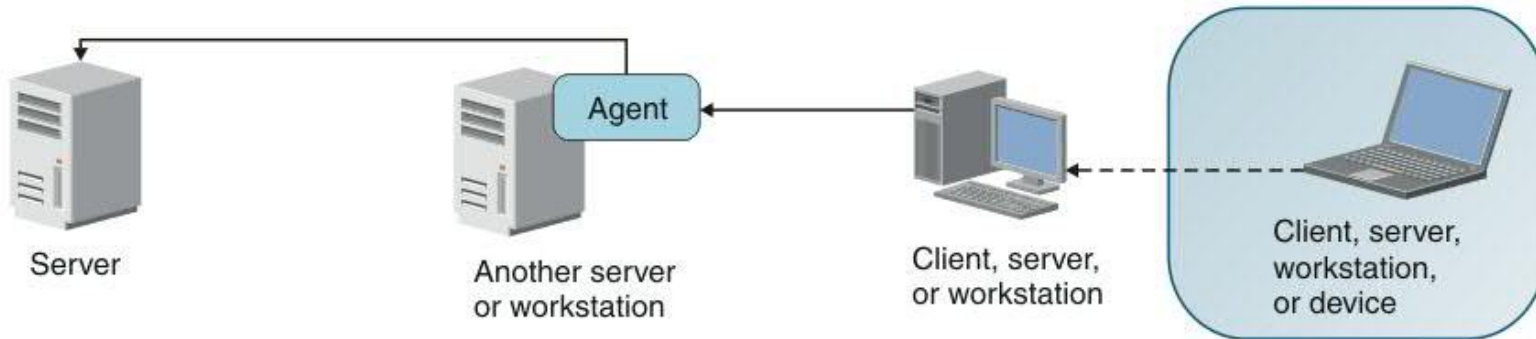


# Data Collection scenarios 7-8

7




8



 = Target system

 = Automatic data transfer

 = Data transfer initiated by administrator

## Common event source properties

- **Three read-only properties are defined for each event source.**
- **Two common event source properties are available to help ensure the proper handling of language- or locale-specific audit data.**
- **Three read-only properties are automatically defined when any event source is created:**
  - **Audited Machine-**The name of the system or device.
  - **Type -**The name of the event source, such as IBM AIX 5.1-6.1 audit trail or Solaris audit trail.

## Common event source properties(continued..)

- **Agent -The system where the agent is installed.**
- **The contents of audit data, which is gathered from various target platforms and applications, might depend on the language or locale settings that are set on the target system.**
- **Every event source attempts to automatically determine the proper encoding and language in use for the collected log data.**
- **If the automatic detection returns no results, the settings default to English language data.**

## Text encoding for audit trail

- **Specifies the text encoding of the text data for collected log data sets.**
- **The default value is the empty string, which indicates that the event source should automatically determine the text encoding for the collected data.**
- **If the encoding is not correctly determined by the event source, you can specify that a specific text encoding be applied.**

## Language code for audit trail

- Specifies the language code of the text data for collected log data sets.
- The default value is the empty string, which indicates that the event source should automatically determine the language used for the collected data

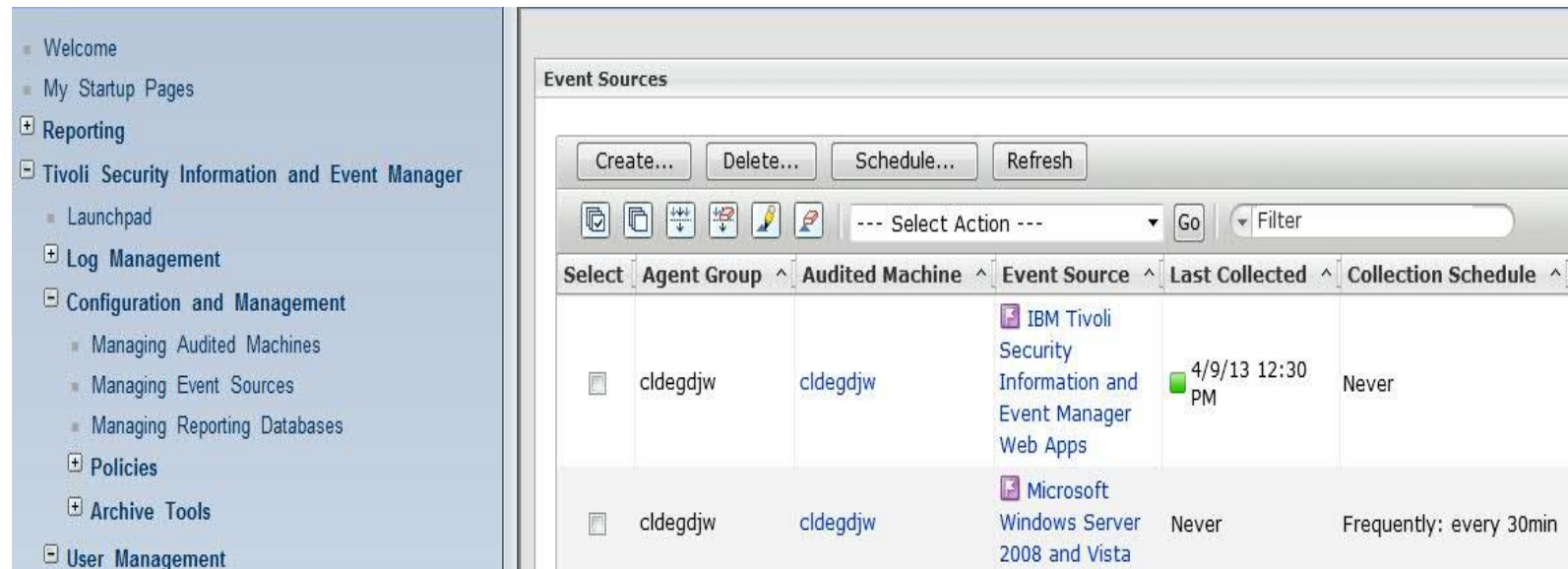
Table 1. Values for the *Language code for audit trail event source property*

Language	Language code
Brazilian Portuguese	pt_BR
French	fr
German	de
Hungarian	hu
Italian	it
Japanese	ja
Korean	ko
Polish	pl
Russian	ru
Simplified Chinese	zh_CN
Spanish	es
Traditional Chinese	zh_TW

## Example: Creating a Windows 2008 event source

- Login to TSIEM portal (as cifowner) and navigate to

**Tivoli Security Information and Event Manager>  
Configuration and Management>  
Managing Event sources as show below**



The screenshot shows the TSIEM portal interface. On the left is a navigation tree with the following items:

- Welcome
- My Startup Pages
- Reporting
- Tivoli Security Information and Event Manager
  - Launchpad
  - Log Management
  - Configuration and Management
    - Managing Audited Machines
    - Managing Event Sources
    - Managing Reporting Databases
  - Policies
  - Archive Tools
  - User Management

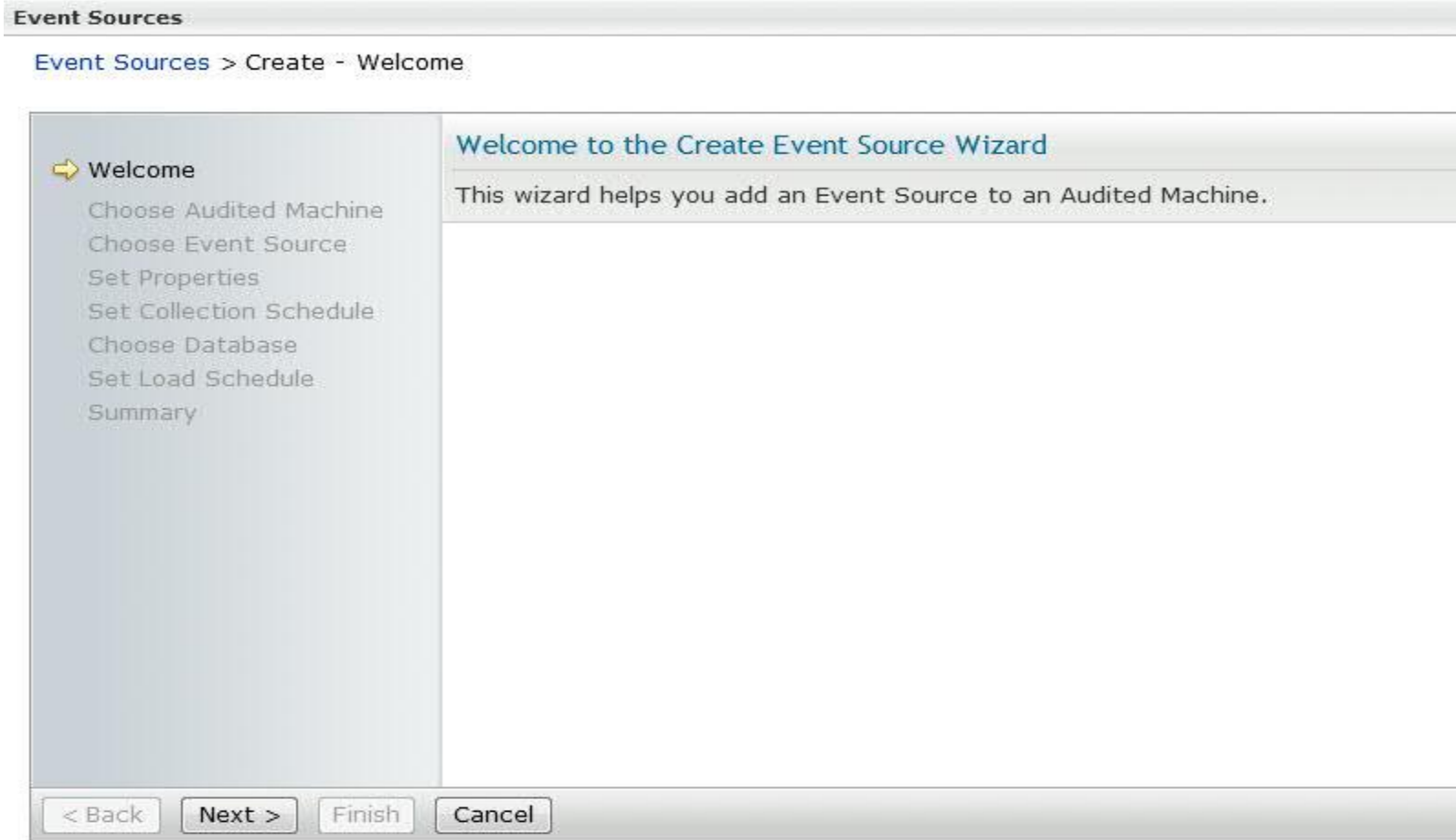
The main content area is titled 'Event Sources' and contains a table with the following data:

Select	Agent Group ^	Audited Machine ^	Event Source ^	Last Collected ^	Collection Schedule ^
<input type="checkbox"/>	cldegdjlw	cldegdjlw	IBM Tivoli Security Information and Event Manager Web Apps	4/9/13 12:30 PM	Never
<input type="checkbox"/>	cldegdjlw	cldegdjlw	Microsoft Windows Server 2008 and Vista	Never	Frequently: every 30min



# Create the event source

- Click on create and then next



# Choose the audited machine

- **Select the audited machine for the event source**

The screenshot shows a web-based wizard interface for selecting an audited machine. On the left is a navigation pane with the following items: Welcome (checked), Choose Audited Machine (active), Choose Event Source, Set Properties, Set Collection Schedule, Choose Database, Set Load Schedule, and Summary. The main content area is titled 'Choose Audited Machine' and contains the instruction: 'Select the Audited Machine for the Event Source from the table, then click Next.' Below this is a toolbar with icons for back, forward, search, and help, a 'Select Action' dropdown menu, a 'Go' button, and a 'Filter' input field. A table below the toolbar has columns for 'Select', 'Audited Machine', and 'Agent Group'. The first row shows a selected radio button, the machine name 'cldegdjw', and the agent group 'cldegdjw'. At the bottom of the table, it displays 'Page 1 of 1', 'Total: 1', 'Filtered: 1', and 'Displayed: 1'. At the very bottom of the wizard are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Choose Audited Machine

Select the Audited Machine for the Event Source from the table, then click Next.

--- Select Action --- Go Filter

Select	Audited Machine	Agent Group
<input checked="" type="radio"/>	cldegdjw	cldegdjw

Page 1 of 1 Total: 1 Filtered: 1 Displayed: 1

< Back Next > Finish Cancel

# Choose event source

- **Select the event source from the list given**

Choose Event Source

Enter the name and type of the Event Source, then click Next.

\*Name:  
Microsoft Windows Server 2008 and Vista

\*Type:  
Microsoft Windows Server 2008 and Vista  
OPICS  
Oracle 9i 10g 11g  
Oracle Applications 11.5.9 - 12.0  
Oracle Database Audit Trail 8i 9i 10g 11g  
Oracle Fine-Grained Auditing 9i 10g 11g  
Raptor File-Based  
Raptor SNMP receiver  
Raptor syslog from syslog host  
Raptor syslog receiver  
RSA Authentication Manager  
SAP NetWeaver Application Server ABAP 6.10-7.0  
SAP NetWeaver Application Server on Java 7.0 - 7.2  
SAP R/3  
ScanMail for Lotus Notes  
ScanMail for MS Exchange  
ServerProtect  
SiteMinder  
Sun Identity Manager  
Sybase Adaptive Server Enterprise

< Back   Next >   Finish   Cancel

# Set event source properties

- Enter user name and password

**Set Properties**

Define properties for Event Source Microsoft Windows Server 2008 and Vista, then click Next

Name	Value
User Name	administrator
Password	••••••••
Text encoding	Windows-1252
Language code for audit trail	

< Back   Next >   Finish   Cancel

# Set collection schedule

- Define the collection schedule

The screenshot shows a wizard window titled "Set Collection Schedule". On the left is a navigation pane with the following steps: "Welcome", "Choose Audited Machine", "Choose Event Source", "Set Properties", "Set Collection Schedule" (highlighted with a yellow arrow), "Choose Database", "Set Load Schedule", and "Summary". The main area of the wizard contains the following text and controls:

**Set Collection Schedule**

Define the collection schedule for the Event Source, then click Next.

Frequency:  
Minutes ▾

Collect every:  
30 ▾ minutes

At the bottom of the wizard are four buttons: "< Back", "Next >", "Finish", and "Cancel".

# Choose Database

- **Select a database to load event source data**

The screenshot shows a wizard window titled "Choose Database". On the left is a navigation pane with the following steps: Welcome (checked), Choose Audited Machine (checked), Choose Event Source (checked), Set Properties (checked), Set Collection Schedule (checked), Choose Database (highlighted with a yellow arrow), Set Load Schedule, and Summary. The main area of the wizard is titled "Choose Database" and contains the instruction: "Select one or more Reporting Databases to load the Event Source data into, then click Next." Below this instruction is a section titled "Reporting Databases" with two checkboxes: "SELFAUDIT" (unchecked) and "Test" (checked). At the bottom of the wizard are four buttons: "< Back", "Next >", "Finish", and "Cancel".



# Set Database load schedule

- **Define schedule for event source data to load**

The screenshot shows a wizard window titled "Set Database Load Schedule". On the left is a navigation pane with the following steps: Welcome, Choose Audited Machine, Choose Event Source, Set Properties, Set Collection Schedule, Choose Database, Set Load Schedule (highlighted with a yellow arrow), and Summary. The main area contains the following configuration options:

- Frequency:** A dropdown menu set to "Daily".
- Load every:** Radio buttons for "Working day" (selected) and "Day".
- Data that is:** Radio buttons for "New data" (selected) and "Last" (with a dropdown set to "1" days of data).
- \*Starting at:** A text box containing "4:57 AM" and a clock icon.

At the bottom of the window are four buttons: "< Back", "Next >", "Finish", and "Cancel".

# Summary of event source settings

The screenshot shows a wizard interface with a left-hand navigation pane and a main content area. The navigation pane lists several steps, with 'Summary' highlighted by a yellow arrow. The main content area has a title 'Summary' and a message: 'You have finished the Create Event Source Wizard. Verify the settings. Click Finish to define the Event Source or click Back to correct settings.' Below this is a table with two columns: 'Setting' and 'Value'. The table contains the following data:

Setting	Value
Name	Microsoft Windows Server 2008 and Vista
Type	Microsoft Windows Server 2008 and Vista
Audited Machine(s)	cldegdju
Collection Schedule	Frequently: every 30min
Reporting Database(s)	Test
Database Load Schedule	Working days: 4:57 AM

At the bottom of the wizard, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. The '< Back' button is highlighted with a blue border.

# New event source created

**Event Sources**

--- Select Action ---

Select	Agent Group ^	Audited Machine ^	Event Source ^	Last Collected ^	Collection Schedule ^
<input type="checkbox"/>	cldegdjw	cldegdjw	IBM Tivoli Security Information and Event Manager Web Apps	4/9/13 12:30 PM	Never
<input type="checkbox"/>	cldegdjw	cldegdjw	Microsoft Windows Server 2008 and Vista	Never	Frequently: every 30min
<input type="checkbox"/>	cldegdjw	cldegdjw	IBM Tivoli Security Information and Event Manager Server	5/20/13 5:15 AM	Frequently: every 15min
<input type="checkbox"/>	cldegdjw	cldegdjw	IBM DB2 for the SIM Server	5/20/13 5:15 AM	Frequently: every 15min
<input type="checkbox"/>	cldegdjw	cldegdjw	IBM Tivoli Directory Server	5/20/13 5:15 AM	Frequently: every 15min



## User Information sources

- A user information source obtains information about users and groups on the target system.
- Based on the data that is available on the target system, the user information source might return information such as:
  - the user account name (the name the user enters when logging on)
  - the internal user ID (such as a numeric user number)
  - the name of the user (as provided in the user registry)

## User Information sources(continued)..

- the groups that the user is a member of
- the roles that the user possesses
- This information can be used to improve the mapping of audit trails that feature these users. Grouping rules and policy rules can be defined directly in terms of these groups in Tivoli® Security Information and Event Manager.
- If the audit record contains only one identifier for the user, for example, the internal user ID, then the other values, such as user account name or the full name of the user can be deduced using the data from the user information source



## Configuration file for User Information sources

- **All user information sources have a Configuration file property**
- **This property governs which event sources use the user information gathered through that particular user information source.**
- **All user information sources have a default value that is appropriate for the event source that is most closely associated with that user information source.**
- **The user information is applied to all event sources that for their processing use the grouping file whose name is mentioned in the Configuration file property of the user information source.**



## Configuration file (continued)...

- If the Configuration file property is set to the value `global_group.cfg`, then the user information obtained through that user information source is taken to apply to all event sources.
- Some user information sources are applicable for multiple types of event sources.
- If those event sources do not use the same grouping file, then separate user information source instances must be defined, each with a different appropriate grouping file name specified in their Configuration file property.

# Event sources associated with each User information source

User information source	Associated event sources
Grouping HP-UX	HP-UX audit trail
Grouping IBM® AIX® 5.1-6.1	IBM AIX 5.1-6.1 audit trail
Grouping IBM AIX 5.1-6.1 from LDAP	IBM AIX 5.1-6.1 audit trail
Grouping IBM DB2® 8.1 - 9.1	IBM DB2 8.1 - 9.1 SP3
Grouping IBM DB2 9.5	IBM DB2 9.5
Grouping IBM DB2 Audit Management Expert 1.1	IBM DB2 Audit Management Expert 1.1
Grouping IBM Informix® Dynamic Server	IBM Informix Dynamic Server
Grouping IBM Proventia® Management SiteProtector 2.0 SP 6 - 6.1	IBM Proventia Management SiteProtector 2.0 SP 6.0 - 6.1
Grouping IBM Tivoli Access Manager	IBM Tivoli Access Manager for e-business IBM Tivoli Access Manager for Operating Systems
Grouping IBM Tivoli Directory Server	IBM Tivoli Directory Server
Grouping IBM Tivoli Federated Identity Manager	IBM Tivoli Federated Identity Manager
Grouping IBM Tivoli Identity Manager 4.6 - 5.0	IBM Tivoli Identity Manager 4.6 - 5.0
Grouping IBM Tivoli Key Lifecycle Manager 1.0	IBM Tivoli Key Lifecycle Manager 1.0
Grouping IBM Tivoli Security Compliance Manager 5.1.0 - 5.1.1.1	IBM Tivoli Security Compliance Manager 5.1.0 - 5.1.1.1
Grouping IBM Tivoli Security Information and Event Manager Server	IBM Tivoli Security Information and Event Manager Server
Grouping IBM Tivoli Security Information and Event Manager Web Apps	IBM Tivoli Security Information and Event Manager Web Apps
Grouping IBM Tivoli Security Policy Manager 7.0	IBM Tivoli Security Policy Manager 7.0
Grouping IBM WebSphere® Application Server 6.0 - 7.0	IBM WebSphere Application Server 6.0 - 7.0
Grouping Microsoft Exchange 2000/2003	Microsoft Windows NT-2003 Microsoft Exchange Microsoft Exchange 2000/2003

## Ubiquitous event sources

- **Event sources in the Tivoli® Security Information and Event Manager ubiquitous event source family allow you to collect log files from any file-based log sources. This is used when you want to integrate an un-supported event source to TSIEM**
- **Ubiquitous event sources eliminate the necessity for supplying special Tivoli Security Information and Event Manager add-ons for specific platforms.**
- **For example, you can use the Ubiquitous log event source to audit ubiquitous text-based log files that produce a single log record per line. Such files can be collected and retrieved from the Tivoli Security Information and Event Manager log depot using the Log Retrieval Tool**

## Ubiquitous event sources(continued)..

- **Ubiquitous event sources do not allow the loading of collected chunks in reporting databases because of functionality limitations in the default parsing script.**
- **If Tivoli Security Information and Event Manager attempts to load this type of collected chunk data into a reporting database, the reporting database issues an error.**

## Types of Ubiquitous event source

- **Ubiquitous log** – The event source collects files that are locally accessible to a Tivoli Security Information and Event Manager server or agent
- **Ubiquitous log syslog from syslog host** – The event source collects syslog messages from locally accessible files to a Tivoli Security Information and Event Manager Server or Agent.
- **Ubiquitous syslog receiver** – The event source collects real-time syslog messages that a Tivoli Security Information and Event Manager server or agent receives.



## Types of Ubiquitous event source continued(..)

- **Ubiquitous SNMP receiver** – The event source collects real-time SNMP traps that a Tivoli Security Information and Event Manager server or agent receives.
- **Ubiquitous through SSH** – The event source collects files from a UNIX or Linux machine through an SSH connection



## Example: Creating an Ubiquitous Event Source on Linux

- **To create an Ubiquitous syslog receiver on Linux:**
- **Select the Linux machine that will receive the syslog messages. Log into TSIEM, and select “Manage Event Sources”.**
- **From there, go to “Add Event Source” and choose the event source Ubiquitous syslog receive**

# Choose Event Source

## Choose Event Source

Enter the name and type of the Event Source, then click Next.

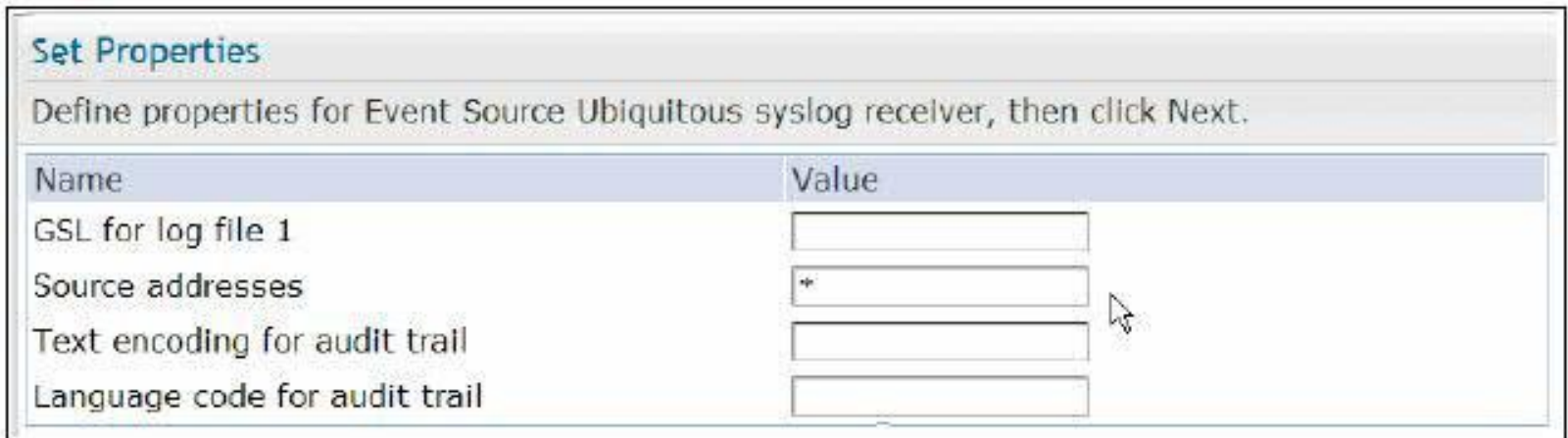
\*Name:

\*Type:  

- IBM Tivoli Security Compliance Manager 5.1.0 - 5.1.1.1 through SSH
- IBM Tivoli Security Policy Manager 7.0 through SSH
- IBM WebSphere Application Server 6.0 - 7.0 through SSH
- Lotus Notes
- Oracle 9i 10g 11g through SSH
- Oracle Applications 11.5.9 - 12.0
- Oracle Applications 11.5.9 - 12.0 through SSH
- Oracle Database Audit Trail 8i 9i 10g 11g
- Oracle Database Audit Trail 9i 10g 11g through SSH
- Oracle Fine-Grained Auditing 9i 10g 11g
- Oracle Fine-Grained Auditing 9i 10g 11g through SSH
- SAP NetWeaver Application Server ABAP 6.10-7.0 through SSH
- ScanMail for Lotus Notes
- Sun Identity Manager
- Sybase Adaptive Server Enterprise
- Sybase Adaptive Server Enterprise through SSH
- Ubiquitous log through SSH
- Ubiquitous SNMP receiver
- Ubiquitous syslog from syslog host
- Ubiquitous syslog receiver

## Creating a Ubiquitous Event Source on Linux – cont'd

- Define the machine from which the ubiquitous event source receives its messages.
- A single IP address can be specified or a range of IP addresses can be specified by using wild cards.
- The ubiquitous event source can receive messages from any origin.



**Set Properties**

Define properties for Event Source Ubiquitous syslog receiver, then click Next.

Name	Value
GSL for log file 1	<input type="text"/>
Source addresses	*
Text encoding for audit trail	<input type="text"/>
Language code for audit trail	<input type="text"/>

## Creating a Ubiquitous Event Source on Linux – cont'd

- **The goal is to receive logged syslog messages in Tivoli Security Information and Event Manager. Syslog messages are stored in text files and we can now archive them to Tivoli Security Information and Event Manager's newly created ubiquitous event source.**
- **Users can now proceed to add additional ubiquitous event sources on other platforms or servers.**

## Creating a Ubiquitous Event Source on Linux – cont'd

- Because ubiquitous event sources only collect logs, a collect schedule needs to be configured.

**Set Collection Schedule**  
Define the collection schedule

Frequency:  
Once

\*Date:  
3/14/10

\*Time:  
7:02 PM



# Creating a Ubiquitous Event Source on Linux – cont'd

- **The configuration will be similar to below example.**

**Summary**

You have finished the Create Event Source Wizard.

Verify the settings. Click Finish to define the Event Source or click Back to correct settings.

Setting	Value
Name	Ubiquitous syslog receiver
Type	Ubiquitous syslog receiver
Audited Machine(s)	FINSYS
Collection Schedule	Once: 3/14/10 7:02 PM
Reporting Database(s)	General
Database Load Schedule	Never



## Important points regarding Ubiquitous event sources

- **The ubiquitous method is the easiest type of event source to implement.**
  - Plain text only
  - No compliance reporting capabilities
- **Data that is collected using the ubiquitous method can be searched and analyzed through Forensic Investigation and basic reporting using Tivoli Common Reporting.**
- **Ubiquitous event sources are utilized for non-supported event sources, whose main requirement is to collect and archive the audit logs.**

## W7 Event Source

- **W7 Event Source or the W7Log Event source is used to integrate TSIEM 2.0 with any of the unsupported event sources.**
- **Unlike the Ubiquitous event source, using the W7 Event Source, you can not only collect but also load the collected audit events as well as generate reports and create alerts based on them.**
- **With the W7Log event source, TSIEM provides support for any software that produces log data running on IBM AIX®, Windows or Linux.**

## W7 Event Source (how it works)

- **The W7Log event source accepts adapted log data from either software or an operating system in a specially defined CSV (Comma Separated Values) or XML formats**
- **There is a diagnostic tool (Validator) for checking the format in which the W7 data has been created.**
- **This CSV or XML file is placed in the “Log File Location” that you have defined while creating the event source on the TSIEM GUI.**
- **The W7 Event Source of TSIEM 2.0 then “collects” this file and creates chunks in the depot directory which can then be loaded.**

## W7 Event Source (how it works) continued..

- **The customized script which converts the raw events into the W7 CSV or W7 XML file is to be created by the Customer and IBM does not provide support for this customized script.**
- **There are a set of Validator(s) which you can use for checking the format of the CSV or XML file that is created by this customized script. Any issues related to this script will not be supported by IBM.**
- **However if there is any issue with W7 event source, IBM would surely support it**

## Where to start from for this W7 Event Source ?

- **First collect the raw events that are being generated by the un-supported event source.**
- **Then create a script which converts this into the W7 CSV or W7 XML format.**
- **This script can be a simple shell or batch script**
- **Once done, check the resultant W7 CSV or W7 XML file using the Validator(s) to be sure that they are in the proper format.**
- **After this you can create the W7 Event Source on the TSIEM GUI with the proper values and you should be good**

## Where to start from for this W7 Event Source ?(continued)..

- **Keep in mind that with every successful collect of the W7 CSV or W7 XML file, the file that has been collected by TSIEM 2.0 will be automatically deleted from the location where you have placed it.**
- **These events would be placed as chunks in the depot directory of the TSIEM server which can then be loaded as per schedule.**
- **As it can be understood, the customized script needs to run periodically so that raw audit data is converted into the W7 CSV or XML file and placed at a location (which you have mentioned while creating the W7 Event Source on the TSIEM GUI).**



## Format of the W7 CSV file

- **W7Log CSV format is the same as Excel CSV, a file format used as a portable representation of a database. Each line is one entry or record and the fields in a record are separated by commas.**
- **If a field includes commas or new line characters, enclose the entire field in quotation marks (""). Any text that appears after the quotation marks but before the next comma is ignored. To include a quotation mark within a field already enclosed in quotation marks, use two quotation mark characters.**

## Format of the W7 CSV file(continued)..

- Empty fields are returned as a string of length zero: "". The following line has three empty fields and three non-empty fields in it. (There is an empty field on each end, and one in the middle. One token is returned as a space):
- ,second,, ,fifth,
- W7Log CSV file contents are defined as follows:
- The header line must list field names, separated by commas in a fixed order, exactly as follows (as a single line):

## Format of the W7 CSV file(continued)..

- when,whorealname,whologonname,whatverb,what noun,whatsucce ss, wheretype,wherename,wherfromtype,wherfrom name,wheretyp e, wheretoname,onwhattype,onwhatpath,onwhatnam e,info
- The description of the fields, we would be covering this in our next slides
- The remaining lines must list the field values for every log record, with one record per line. There must be exactly 16 values in each log record, describing one event that happened on the audited system.

## Format of the W7 CSV file(continued)..

- Record fields can be empty or have only spaces. However, use a single dash (-) for empty values. The size of record fields is not checked. However, the log producer must satisfy the requirements.
- The following example shows a valid CSV log file, specifying some imaginary events:  
when,whorealname,whologonname,whatverb,what noun,whatsuccess,  
wheretype,wherename,wherefromtype,wherefrom name,wheretotype, 2003-07-18T14:22:00+00:00  
John Smith, jsmith, Logon, System, Success,  
Microsoft Windows, PDC,-,

## W7 XML file format

- The W7Log XML format is defined by the XML schema for W7Log XML log files. The following example lists the XML schema definition file for the W7Log XML format, events.xsd.
- `<sample>`
- `<event>`
- `<when>2009-07-18T14:22:01-02:00</when>`
- `<what verb="Logon" noun="System" success="Success"/>`
- `<onwhat type="SYSTEM" path="-" name="PDC"/>`

## W7 XML file format(continued)..

- `<who logonname=" John Smith" realname="jsmith"/>`
- `<where type="Microsoft Windows" name="PDC"/>`
- `<whereto type="Microsoft Windows" name="PDC"/>`
- `<wherfrom type="-" name="WORKSTATION"/>`
- `<info>testing record</info>`
- `</event>`
- `<event>`



## Description of the W7 CSV or XML file fields

- The fields that have been discussed in our previous slides for the W7 CSV and the W7 XML file have got the following meanings:

Field Name	Field Description	Value
when	Time, when event occurred. This field is defined as: YYYY-MM-ddTHH:mm:ss:s	<ul style="list-style-type: none"> <li>▶ YYYY: The year in the Gregorian calendar</li> <li>▶ MM: The month number (1-12)</li> <li>▶ dd: The day number (1-31)</li> <li>▶ T: The literal separator between date and time</li> <li>▶ HH: The hours number (0-23)</li> <li>▶ mm: The minute number (0-59)</li> <li>▶ ss: The second number (0-59)</li> </ul> Optional values are fractional seconds in one-to-three decimals.
whorealname, whologonname	Platform-dependent logon ID and logon name of the user who initiated the event. The name of the system process or application can be specified here instead of the name of the actual user.	Defined as arbitrary string values of up to 64 bytes each.

## Description of the W7 CSV or XML file fields(continued)..

Field Name	Field Description	Value
whatverb, whatnoun, whatsuccess	<p>The triplet of values that indicate what kind of action the event represents:</p> <ul style="list-style-type: none"> <li>▶ The <i>verb</i> is an action type (for example, logon, create, and so on).</li> <li>▶ The <i>noun</i> is the refinement of the action type (for example, user, file, and so on).</li> <li>▶ The value of <i>success</i> can be either <i>success</i> or <i>failure</i>, depending on how the action was run.</li> </ul>	<p>For <i>whatverb</i> and <i>whatnoun</i> an arbitrary string of up to 20 characters.</p> <p>For <i>whatsuccess</i> an arbitrary string of up to eight characters.</p>
wheretype, wherename	<p>The platform (type and name) where the event happened. Examples are "SUN Solaris" or "GATEWAY", and so on.</p>	<p>For <i>wheretype</i> an arbitrary string of up to 20 characters.</p> <p>For <i>wherename</i> an arbitrary string of up to 128 characters.</p>
wherefromtype, wherefromname	<p>Platform (type and name) of the event's origin platform. Examples are "Internet", "192.168.103.104", and so on.</p>	<p>For <i>wherefromtype</i> an arbitrary string of up to 20 characters.</p> <p>For <i>wherefromname</i> an arbitrary string of up to 128 characters.</p>
wheretotype, wheretomname	<p>Platform (type and name) of the event's target platform. Examples are "Microsoft Windows", "WORKSTATION", and so on.</p>	<p>For <i>wheretomtype</i> an arbitrary string of up to 20 characters.</p> <p>For <i>wheretomname</i> an arbitrary string of up to 128 characters.</p>

## Description of the W7 CSV or XML file fields(continued)..

Field Name	Field Description	Value
onwhattype, onwhatpath, onwhatname	The triplet of values that indicate what object was involved. Examples are file, database, printer, and so on.	<ul style="list-style-type: none"> <li>▶ <i>onwhattype</i> groups all objects according to some platform-specific event type as an arbitrary string of up to 20 bytes.</li> <li>▶ <i>onwhatpath</i> groups all objects of the same type into separate names spaces (or directories) as an arbitrary string of up to 110 bytes.</li> <li>▶ <i>onwhatname</i> identifies objects within each name space (or directory) as an arbitrary string of up to 110 bytes.</li> </ul>
info	Provides additional information about an event, for example, you can use this field to provide hyperlinks to external internet resources.	This field is a text field of up to 3900 characters.



## Important Points

- **The customized script that you create for converting the raw events into the W7 CSV or W7 XML file should be able to “map” the raw data into the fields that have been discussed. Keep in mind about the blank entries for the different fields in the CSV or XML files that would be created from the raw event and you should be good. You can use the W7CSV Validator or the W7XML Validator for confirming that the resultant CSV or XML files are in the proper format for TSIEM 2.0 to work upon**

## W7Log CSV Validator

- **The UES CSV Validator is an operating-system-independent diagnostic tool, intended for third parties to check the validity of proposed CSV log data for W7Log CSV event sources.**
- **You will need a Java virtual machine, version 1.5, running on any operating system supported by Java.**
- **The Validator files which are required for the Validator to run successfully are present on the installation DVD under the location `\utils\UESValidator` on Windows and `/utils/UESValidator` on Unix**

## W7Log CSV Validator (continued)..

- They are also present on the TSIEM server under the following locations:
- On Windows installation of TSIEM Server:  
`%TSIEM_HOME%\sim\server\bin`
- On Unix based installation of TSIEM Server:  
`$TSIEM_HOME/sim/server/bin`



## Installing the W7CSV Validator

- **All you need to do for this is to copy the two files `validate.bat` and `validate.jar` from the locations mentioned before to the destination directory from where you want to run this Validator on a Windows based installation of TSIEM 2.0**
- **For Unix based installation of TSIEM 2.0, copy the two files `validate.sh` and `validate.jar` from the locations mentioned before to the destination directory from where you want to run this Validator**

## Executing the W7CSV Validator

- From the directory where you copied the Validator files, perform the following steps.
- On Windows: Open a command prompt window and launch `validate.bat` with the `-csv` switch and specify the path to the desired CSV log file

```
> cd path_to\validator  
> validate.bat -csv path_to\log.csv
```

- On Unix: Launch the `validate.sh` script with the `-csv` switch and specify the path to the desired CSV log file:

```
$ cd path_to/validator  
$ sh validate.sh -csv path_to/log.csv
```

## Executing the W7CSV Validator(continued)..

- The W7Log CSV Validator checks proposed CSV log data for compliance with the W7Log CSV format defined in the W7Log CSV format
- The W7Log CSV Validator does not check proposed CSV log data for empty fields or fields containing only blanks. However, do not use such values in the log files.
- The W7Log CSV Validator prints the following possible results to the console:
  - Success, in the case of a valid CSV log file.
  - Failure: error-message, in the case of an invalid CSV log file, where error-message can be one of the following:
    - filename: row: column wrong\_field\_name must be'correct\_field\_name - Header contains incorrect field name.

## W7XML Validator

- **The requirements for the W7XML Validator is the same as that of the W7 CSV Validator. Infact for the W7 XML Validator, you will have to copy the same files validate.bat and validate.jar on Windows and validate.sh and validate.jar on Unix from the same location as you had done for using the W7CSV Validator**
- **The only difference lies in how you execute them. In other words, the “switch” that you use while executing the Validator determines whether a W7CSV file would be validated or a W7XML file will be validated.**

## Executing the W7XML Validator

- From the directory where you copied the validator files, perform the following steps.
- **Windows:** Open a command prompt window and launch `validate.bat` with the `-xml` switch and specify the path to the desired XML log file

```
> cd path_to\validator  
> validate.bat -xml path_to\log.xml
```

- **UNIX:** Launch the `validate.sh` script with the `-xml` switch and specify the path to the desired XML log file:

```
$ cd path_to/validator  
$ sh validate.sh -xml path_to/log.xml
```

## Executing the W7XML Validator(continued)..

- **The W7Log XML Validator checks the proposed XML log data for compliance with the W7Log XML schema that we had discussed previously.**
- **The W7Log XML Validator does not check the proposed XML log data for empty fields or fields containing only blanks**
- **The W7Log XML Validator prints the following possible results to the console:**
- **Success, in the case of a valid XML log file**
- **Failure: error-message, in the case of an XML log file that is not valid, where error-message is a text description of the error provided by the underlying XML engine.**



## Next Steps

- **Once you are done with Validating the W7CSV or W7XML file, and the result shows that they are of the valid format, you can proceed with creating the W7 Event Source on the TSIEM GUI**
- **There are two Audit configurations for collecting events through the W7 Event Source. You can follow any one of them:**
  - **1. The W7CSV or W7XML data from the platforms are located on a monitored system other than the TSIEM Server. In this case, TSIEM can monitor one or more platforms within the network using the agent on each system.**
  - **2. The W7CSV or W7XML data from the platforms are located on the same system on which TSIEM Server has been installed. In this case, you will not be needing any agent**

## Next Steps (continued)..

- **If you select option 1 as discussed in our previous slide, you will be needing an agent. This agent would be specific to the type of machine on which the W7CSV or the W7XML file is being kept for TSIEM to collect. Do ensure that the agent is running before creating the W7 Event source on the TSIEM GUI**
- **Also do keep in mind that there must be system administrator credentials on the system where the platform is to be audited as well as the TSIEM server must have a TCP/IP network connection to the audited system.**

## Next Steps (continued)..

- **Place all log files that are to be processed in a separate designated directory. Remember the path to the directory where the W7CSV or W7XML file is being kept since we would be needing this while creating the W7Event Source on the TSIEM GUI.**
- **All log files are deleted from the designated directory after they are processed by TSIEM. Therefore, a backup copy of the logs must be stored in some other directory if you need them later**
- **Each log file in the designated directory should be in a valid CSV or XML format as discussed before.**
- **Each log file in the designated directory must contain only complete records. A good method for ensuring this is to construct a log file somewhere else and then move it into the designated directory.**
- **Log records must be written in UTF-8 encoding.**
- **During creation of log records, contents of different log files must not be overlapped.**

## Adding the W7 Event Source

- To start auditing a W7CSV or W7XML system, you need to add the system with W7CSV or W7XML file to TSIEM. This is a general method of adding the audited machine to TSIEM for which you can follow the steps given in the User guide of TSIEM 2.0.
- Once done, add the W7Log event source to TSIEM. For this, log into the TSIEM TIP as the cifowner user and go to Manage Event Sources. In there click on "Add Event Source" and the Add Event Source Wizard would open up. You must define an W7Log event source for each target W7Log system you want to audit.
- For every new W7Log event source: Select either the W7Log CSV or W7Log XML platform from the list of standard platforms, depending on the log type of the platform.
- Specify the platform type and the log file location to be used as event source properties as given in the next slide

## Adding the W7 Event Source(continued)..

- **Log files location** - A path to the adapted log files. There is no default value for this property, so you must specify one. Point to remember here is that every batch collect deletes all log files from the designated directory, which is specified in the event source property Log files location.
- **Platform Type** - The name of the W7Log platform type. Use the default value W7Log-CSV or W7Log-XML depending on the type of event source you configured to audit the W7Log platform.
- **Customize the W7Log event source properties for your environment** (schedule the collects and the reporting database to which it would put the data in)
- **Once done, you will see the Event Source added to TSIEM and successful collects happening as per the schedule that you have defined**

**Questions/Comments!!!!**