



**Hewlett Packard**  
Enterprise

# **HPE Security ArcSight Connectors**

SmartConnector for Windows Event Log –  
Unified: Microsoft SQL Server Audit

Supplemental Configuration Guide

March 31, 2015

## Supplemental Configuration Guide

### SmartConnector for Windows Event Log – Unified: Microsoft SQL Server Audit

March 31, 2015

Copyright © 2010 – 2015 Hewlett Packard Enterprise Development LP

#### Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

#### Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>.

## Revision History

Date	Description
03/31/2015	Added support for Microsoft SQL Server 2012 SP1 event collection.
09/30/2013	Updated "Collect Events from the Event Log" procedure.
02/15/2013	Additional event support for Microsoft SQL Server 2008 events.
08/15/2012	Added support for Microsoft SQL Server 2012 event collection.
05/15/2012	Updated for new installation procedure.
03/30/2012	Added information for configuration event log type.
02/15/2012	Added support for Microsoft SQL Server 2008 SP3; corrected example entries.
11/15/2011	Updated configuration information.
02/15/2011	Added information about using connector in a clustered environment.
11/15/2010	General availability of this connector.
09/24/2010	First edition of this Configuration Guide, for initial support of MS SQL Server Audit application events with the Microsoft Windows Event Log - Unified connector on Windows Server 2008.

## Contents

Product Overview .....	7
SQL Server Audit Configuration .....	7
Customize Event Source Mapping .....	8
To Make it Work .....	8
Event Parsing in a Clustered Environment Example .....	9
Connector Installation and Configuration .....	9
Collect Events from the Event Log .....	9
Microsoft SQL Server Audit Application Event Log Mappings .....	11
Microsoft Windows Server 2012 .....	11
General .....	11
Event 615 .....	11
Event 849 .....	11
Event 852 .....	11
Event 919 .....	11
Event 958 .....	11
Event 1486 .....	12
Event 1814 .....	12
Event 1945 .....	12
Event 2007 .....	12
Event 2812 .....	12
Event 3406 .....	13
Event 3407 .....	13
Event 3408 .....	13
Event 3421 .....	13
Event 3454 .....	13
Event 5084 .....	14
Event 5579 .....	14
Event 5701 .....	14
Event 5703 .....	14
Event 6253 .....	14
Event 6527 .....	15
Event 8128 .....	15
Event 9013 .....	15
Event 9666 .....	15
Event 9688 .....	15
Event 9689 .....	15
Event 10981 .....	16
Event 15268 .....	16
Event 15457 .....	16
Event 15477 .....	16
Event 17069 .....	16
Event 17101 .....	16

Event 17103.....	16
Event 17104.....	17
Event 17107.....	17
Event 17108.....	17
Event 17110.....	17
Event 17111.....	17
Event 17115.....	17
Event 17125.....	18
Event 17126.....	18
Event 17136.....	18
Event 17137.....	18
Event 17147.....	18
Event 17148.....	18
Event 17152.....	19
Event 17162.....	19
Event 17164.....	19
Event 17176.....	19
Event 17177.....	20
Event 17199.....	20
Event 17201.....	20
Event 17550.....	20
Event 17551.....	20
Event 17656.....	21
Event 17658.....	21
Event 17561.....	21
Event 17663.....	21
Event 18456.....	21
Event 18488.....	21
Event 18496.....	22
Event 19030.....	22
Event 19031.....	22
Event 19032.....	22
Event 26018.....	22
Event 26022.....	22
Event 26037.....	23
Event 26048.....	23
Event 26067.....	23
Event 26076.....	23
Event 30090.....	23
Event 33090.....	24
Event 33204.....	24
Event 33205.....	24
Event 33217.....	25
Event 33218.....	25
Event 49903.....	25

Event 49904 .....	25
Event 49910 .....	25
Microsoft Windows Server 2008, 2008 R2, 2008 R3 .....	26
General .....	26
Event 615 .....	26
Event 849 .....	26
Event 958 .....	26
Event 1814 .....	26
Event 3406 .....	26
Event 3407 .....	26
Event 3408 .....	27
Event 3454 .....	27
Event 5579 .....	27
Event 8128 .....	27
Event 9013 .....	27
Event 9666 .....	27
Event 9688 .....	27
Event 9689 .....	27
Event 10981 .....	28
Event 15268 .....	28
Event 15457 .....	28
Event 17069 .....	28
Event 17101 .....	28
Event 17103 .....	28
Event 17104 .....	28
Event 17110 .....	28
Event 17111 .....	29
Event 17125 .....	29
Event 17126 .....	29
Event 17136 .....	29
Event 17137 .....	29
Event 17148 .....	29
Event 17152 .....	29
Event 17162 .....	29
Event 17164 .....	30
Event 17176 .....	30
Event 17177 .....	30
Event 17201 .....	30
Event 17663 .....	30
Event 18456 .....	30
Event 18496 .....	30
Event 19030 .....	31
Event 19031 .....	31
Event 19032 .....	31
Event 26018 .....	31

Event 26022.....	31
Event 26037.....	31
Event 26048.....	31
Event 33090.....	32
Event 33204.....	32
Event 33205.....	32
Event 33217.....	33
Event 33218.....	33
Event 30090.....	33

## SmartConnector for Windows Event Log – Unified: Microsoft SQL Server Audit

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Unified: Microsoft SQL Server Audit and its event mappings to ArcSight data fields. Event collection is supported as follows:

Microsoft Windows Server Version	Microsoft SQL Server Version
2008, 2008 R2, 2008 R3	2008, 2012
2012	2012 SP1

The *ArcSight SmartConnector Mappings to Windows Security Events* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the SmartConnector for Windows Event Log – Unified: Microsoft SQL Server Audit.

### Product Overview

With SQL Server 2008, Microsoft introduced an SQL Server Audit feature that provides a true auditing solution for enterprise customers. While SQL Trace can be used to satisfy many auditing needs, SQL Server Audit offers a number of advantages that can help DBAs more easily achieve their goals, such as meeting regulatory compliance requirements.

The SQL Server Audit feature is intended to replace SQL Trace as the preferred auditing solution. SQL Server Audit is meant to provide full auditing capabilities and only auditing capabilities, unlike SQL Trace, which is also used for performance debugging.

### SQL Server Audit Configuration

Auditing an instance of SQL Server or a SQL Server database involves tracking and logging events that occur on the system. The SQL Server Audit object collects a single instance of server- or database-level actions and groups of actions to monitor. The audit is at the SQL Server instance level. You can have multiple audits per SQL Server instance. The Server Audit Specification object belongs to an audit. You can create one server audit specification per audit, because both are created at the SQL Server instance scope.

There are three main objects that describe audits:

#### Server Audit Object

The Server Audit object describes the target for audit data, plus some top-level configuration settings. The Server Audit object is the declaration of the audit destination, which in the case of this SmartConnector is the Microsoft Windows Application log. The Server Audit object contains no information about what is being audited, just where the audit data is going. An SQL Server 2008 audit can be configured to log to any one of the Windows Security logs, Application logs, or instead to a file (by configuring the Server Audit object with the "Audit destination" option). This SmartConnector is designed to work specifically with SQL 2008 events posted to the Windows Application log only..

### Server Audit Specification Object

The Server Audit Specification object describes what to audit. A server audit specification is associated with a Server Audit object to define where the audit data is written. There is a one-to-one relationship between the Server Audit Specification object and the Server Audit object.

### Database Audit Specification Object

The Database Audit Specification object also describes what to audit, but is focused on actions that occur in a specific database. Where the audit data is written is defined by the association of a Database Audit Specification object with a Server Audit object. Each Database Audit Specification can be associated with only one Server Audit object. A Server Audit object, for its part, can be associated with only one Database Audit Specification object per database.

For complete information about auditing in SQL Server, see Microsoft's SQL Server 2008 and 2012 documentation. Both Microsoft Developer's Network (<http://msdn.microsoft.com/en-us/library/cc280386.aspx>) Microsoft TechNet ([http://technet.microsoft.com/en-us/library/dd392015\(SQL.100\).aspx](http://technet.microsoft.com/en-us/library/dd392015(SQL.100).aspx)) contain detailed information.

For information describing how to create a server audit, database audit specification, and server audit specification in SQL Server 2012 by using SQL Server Management Studio or Transact-SQL, see "Create a Server Audit and Database Audit Specification" or "Create a Server Audit and Server Audit Specification" in the MSDN Library.

For information describing how to write SQL Server Audit events to the security log, see "Write SQL Server Audit Events to the Security Log" in the MSDN library.

## Customize Event Source Mapping

The Windows Event Log Unified application/system event parser loading mechanism relies on the event source for each event and attempts to load a parser with the following name convention

```
event_log_type.event_source_name.sdkkeyvaluefilereader.properties
```

This convention works in the vast majority of cases but sometimes must be made a bit more flexible. For that purpose, a solution has been introduced that lets you customize where to find these parsers by redirecting these two variables (event log type and event source name). For even more flexibility, the input event source name can be matched against a regular expression to avoid duplicate entries with minimal changes.

## To Make it Work

Navigate to `$ARCSIGHT_HOME/current/user/agent/fcp/windowsfg/` and create an override map file with the name `customeventsource.map.csv` with the following four columns:

```
Original_Event_Log_Type, Original_Event_Log_Source,  
Target_Event_Log_Source, Target_Event_Log_Type
```

The `Original_Event_Log_Source` value can be a string or a regular expression.

If there is no `windowsfg` subdirectory at `$ARCSIGHT_HOME/current/user/agent/fcp/`, create one.



The last field `Target_Event_Log_Type` is optional and, if empty, will be understood as the same as `Original_Event_Log_Type`.

Note that the map file is not provided in the Windows version-specific folder. Rather it is generic and the appropriate Windows version-specific parser is loaded automatically based upon the host version for the event. See the following for examples of why and how to use this feature.

## Event Parsing in a Clustered Environment Example

The default parser filename convention can cause a problem in clustered environments, where the same event from different clusters can have different customized event source names. For example, SQL Server application events have the source names as `MSSQLSERVER`, resulting in the parser name as `application.mssqlserver.sdkkeyvaluefilereader.properties`.

In a clustered environment for SQL Server installations, you can customize and configure the event source names for each cluster as `SQLSERVER01`, `SQLSERVER02`, and so on. The connector is expecting `MSSQLSERVER`, so the default parser as above will not be loaded, causing the parsing to fail for the events with event source names `SQLSERVER01` and `SQLSERVER02`.

With the `customeventsource.map.csv` file, you can overcome this challenge easily by funneling all these source names into one. Example entries based on the above clustered environment are:

```
Application, MSSQLSERVER01, MSSQLSERVER, Application
```

or

```
Application, MSSQLSERVER\d*, MSSQLSERVER, Application
```

or

```
Application, MSSQLSERVER.*, MSSQLSERVER, Application
```

The complete contents of a sample `customeventsource.map.csv` file with two entries may appear as:

#Original_Event_Log_Type	Original_Event_Log_Source	Target_Event_Log_Source	Target_Event_Log_Type
System,	Service.*,	service_control_manager,	System
Application,	MSSQLSERVER.*,	MSSQLSERVER,	Application

## Connector Installation and Configuration

Follow the installation and configuration procedures in the [SmartConnector Configuration Guide for Microsoft Windows Event Log – Unified](#), selecting **Microsoft Windows Event Log – Unified** as the connector to be configured.

## Collect Events from the Event Log

To set up the connector to collect application events:

- 1 From `$ARCSIGHT_HOME\current\bin`, double-click **runagentsetup.bat**.
- 2 Select **Modify Connector** on the window displayed and click **Next**.
- 3 Select **Modify connector parameters** and click **Next**.

- 4 Select **Navigate** to the **Modify table parameters** window.
- 5 To collect events from an application log, modify the **Application** field by selecting **true** for event collection in the **Application** field and enter **SQL Server Audit** in the **Custom Log Names** field.  
  
You can specify multiple Custom Log Names in a comma-separated format; for example:  
  
`SQL Server Audit, Exchange Auditing`
- 6 Click **Next** to update the parameters; when you receive the successful update message, click **Next**.
- 7 Select **Exit** and click **Next** to exit the configuration wizard.
- 8 Restart the connector for your changes to take effect.

For more information about application event support, see the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Unified*.

## Microsoft SQL Server Audit Application Event Log Mappings

### Microsoft Windows Server 2012

#### General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'SQL Server'
Source User Name	extracted from NTUser (User)
Source NT Domain	extracted from NTDomain (User)

#### Event 615

ArcSight Field	Vendor Field
Name	'Could not find database'
Message	'Could not find database ID ',Key[0],', name ',Key[1]
Device Custom Number 1	Key[0] (Database ID)
Device Custom String 1	Key[1] (Database name)

#### Event 849

ArcSight Field	Vendor Field
Name	'Using locked pages for buffer pool'
Message	'Using locked pages for buffer pool'

#### Event 852

ArcSight Field	Vendor Field
Name	'Using conventional memory in the memory manager'
Message	'Using conventional memory in the memory manager'

#### Event 919

ArcSight Field	Vendor Field
Name	'User is changing database script level'
Message	'User ',Key[0],', is changing database script level entry ',Key[1],', to a value of ',Key[2]
Source User Name	Key[0]
Device Custom Number 1	Key[1] (Level entry)
Device Custom Number 2	Key[2] (Changed value)

#### Event 958

ArcSight Field	Vendor Field
Name	'The resource database build version'
Message	'The resource database build version is ',Key[0]
Device Custom String 4	Key[4] (Database build version)

**Event 1486**

ArcSight Field	Vendor Field
Name	'Database Mirroring Transport is disabled in the endpoint configuration'
Message	'Database Mirroring Transport is disabled in the endpoint configuration'

**Event 1814**

ArcSight Field	Vendor Field
Name	'Could not create tempdb'
Message	'Could not create tempdb. You may not have enough disk space available.'

**Event 1945**

ArcSight Field	Vendor Field
Name	'Warning! The maximum key length'
Message	'Warning! The maximum key length is 'Key[0],' bytes. The index 'Key[1],' has maximum length of 'Key[2],' bytes. For some combination of large values, the insert/update operation will fail.'
Device Custom String 1	Key[0] (Maximum key length)
Device Custom String 2	Key[1] (Index)
Device Custom String 3	Key[2] (Maximum index)

**Event 2007**

ArcSight Field	Vendor Field
Name	'The module depends on the missing object'
Message	'The module 'Key[0],' depends on the missing object 'Key[1]'. The module will still be created; however, it cannot run successfully until the object exists.'
Device Custom String 1	Key[0] (Module)
Device Custom String 2	Key[1] (Missing object)

**Event 2812**

ArcSight Field	Vendor Field
Name	'Could not find stored procedure'
Message	'Could not find stored procedure 'Key[0]'
Device Custom String 2	Key[0] (Stored procedure)

**Event 3406**

ArcSight Field	Vendor Field
Name	'Transactions rolled forward in database'
Message	Key[0]' transactions rolled forward in database 'Key[1], '('Key[2],')
Device Custom Number 2	Key[0] (Transactions quantity)
Device Custom String 1	Key[1] (Database name)
Device Custom Number 1	Key[2] (Database ID)

**Event 3407**

ArcSight Field	Vendor Field
Name	'Transactions rolled back in database'
Message	Key[0],' transactions rolled back in database 'Key[1],' ('Key[2],') '
Device Custom Number 2	Key[0] (Transactions quantity)
Device Custom String 1	Key[1] (Database name)
Device Custom Number 1	Key[2] (Database ID)

**Event 3408**

ArcSight Field	Vendor Field
Name	'Recovery is complete'
Message	'Recovery is complete. This is an informational message only. No user action is required.'

**Event 3421**

ArcSight Field	Vendor Field
Name	'Recovery completed for database'
Message	'Recovery completed for database 'Key[0],' (database ID 'Key[1],) in 'Key[2],' second(s) (analysis 'Key[3],' ms, redo 'Key[4],' ms, undo 'Key[5],' ms.)'
Device Custom String 1	Key[0] (Database name)
Device Custom String 2	Key[3] ms (Analysis time)
Device Custom String 3	Key[4] ms (Redo time)
Device Custom String 4	Key[5] ms (Undo time)
End Time	Key[2]

**Event 3454**

ArcSight Field	Vendor Field
Name	'Recovery is writing a checkpoint in database.'
Message	'Recovery is writing a checkpoint in database 'Key[0],' ('Key[1],')
Device Custom String 1	Key[0] (Database name)
Device Custom Number 2	Key[1] (Database ID)

**Event 5084**

ArcSight Field	Vendor Field
Name	'Setting database option'
Message	'Setting database option ',Key[0],' to ',Key[1],' for database ',Key[2],' '
Device Custom String 1	Key[2] (Database name)
Device Custom String 2	Key[0] (Old option)
Device Custom String 3	Key[1] (New option)

**Event 5579**

ArcSight Field	Vendor Field
Name	'File system access'
Message	'#FILESTREAM: effective level =',Key[0],' , configured level = ',Key[1],' , file system access share name = ',Key[2],' '
Device Custom Number 1	Key[0] (Effective level)
Device Custom Number 2	Key[1] (Configured level)
Device Custom String 4	Key[2] (Access share name)

**Event 5701**

ArcSight Field	Vendor Field
Name	'Changed database context'
Message	'Changed database context to ',Key[0]
Device Custom String 1	Key[0] (Database name)
Device Action	'Changed'

**Event 5703**

ArcSight Field	Vendor Field
Name	'Changed language setting'
Message	'Changed language setting to ',Key[0]
Device Custom String 1	Key[0] (Language setting)
Device Action	'Changed'

**Event 6253**

ArcSight Field	Vendor Field
Name	'Common language runtime (CLR) functionality initialized using CLR'
Message	'Common language runtime (CLR) functionality initialized using CLR version ',Key[0],' from ',Key[1]
File Path	Key[1]
Device Custom String 4	Key[0] (File version)

**Event 6527**

ArcSight Field	Vendor Field
Name	'.NET Framework runtime has been stopped'
Message	'.NET Framework runtime has been stopped'

**Event 8128**

ArcSight Field	Vendor Field
Name	'Execute extended stored procedure.'
Message	'Using ',Key[0],' version ',Key[1],' to execute extended stored procedure ',Key[2],'.' This is an informational message only; no user action is required.'
File Name	Key[0]
Device Custom String 3	Key[1] (File version)
Device Custom String 4	Key[2] (Extended stored procedure)

**Event 9013**

ArcSight Field	Vendor Field
Name	'Tail of the log for database is being rewritten'
Message	'Tail of the log for database ',key[0],' is being rewritten to match the new sector size of ',Key[1],' bytes. ',Key[2],' bytes at offset ',Key[3],' in file ',Key[4],' will be written'
Device Custom String 1	Key[0] (Database name)
File Size	Key[1]
Old File Size	Key[2]
Device Custom String 5	Key[3] (Offset)
File Name	Key[4]

**Event 9666**

ArcSight Field	Vendor Field
Name	'Service endpoint is in disabled or stopped state'
Message	'The ',Key[0],' endpoint is in disabled or stopped state'
Destination Service Name	Key[0]

**Event 9688**

ArcSight Field	Vendor Field
Name	'Service Broker manager has started'
Message	'Service Broker manager has started'

**Event 9689**

ArcSight Field	Vendor Field
Name	'Service Broker manager has shut down'
Message	'Service Broker manager has shut down'

**Event 10981**

ArcSight Field	Vendor Field
Name	'Resource governor reconfiguration succeeded'
Message	'Resource governor reconfiguration succeeded'

**Event 15268**

ArcSight Field	Vendor Field
Name	'Authentication mode'
Message	'Authentication mode is ',Key[0]
Device Custom String 3	Key[0] (Authentication mode)

**Event 15457**

ArcSight Field	Vendor Field
Name	'Configuration option changed'
Message	'Configuration option ',Key[0],' changed from ',Key[1],' to ',Key[2],'. Run the RECONFIGURE statement to install'
Device Custom String 3	Key[0] (Configuration option)
Device Custom Number 1	Key[1] (Old value)
Device Custom Number 2	Key[2] (New value)

**Event 15477**

ArcSight Field	Vendor Field
Name	'Caution: Changing any part of an object name could break scripts and stored procedures'
Message	'Caution: Changing any part of an object name could break scripts and stored procedures'

**Event 17069**

ArcSight Field	Vendor Field
Name	'Microsoft SQL Server 2012 (SP1)'
Message	Key[0]

**Event 17101**

ArcSight Field	Vendor Field
Name	'Microsoft Corporation'
Message	'Microsoft Corporation'

**Event 17103**

ArcSight Field	Vendor Field
Name	'All rights reserved'
Message	'All rights reserved'



**Event 17104**

ArcSight Field	Vendor Field
Name	'Server process ID'
Message	'Server process ID is ',Key[0]
Destination Process ID	Key[0]

**Event 17107**

ArcSight Field	Vendor Field
Name	'Perfmon counters for resource governor pools and groups failed to initialize and are disabled'
Message	'Perfmon counters for resource governor pools and groups failed to initialize and are disabled'

**Event 17108**

ArcSight Field	Vendor Field
Name	'Password policy update was successful'
Message	'Password policy update was successful'
Device Action	'Update'

**Event 17110**

ArcSight Field	Vendor Field
Name	'Registry startup parameters'
Message	'Registry startup parameters ',Key[0]
Device Custom String 1	Key[0] (Parameters)

**Event 17111**

ArcSight Field	Vendor Field
Name	'Logging SQL Server messages'
Message	'Logging SQL Server messages in file ',Key[0]
File Name	Key[0]

**Event 17115**

ArcSight Field	Vendor Field
Name	'Command Line Startup'
Message	'Command Line Startup Parameters: ',Key[0]
Device Action	'Startup'

**Event 17125**

ArcSight Field	Vendor Field
Name	'Using dynamic lock allocation'
Message	'Using dynamic lock allocation. Initial allocation of ',Key[0],' Lock blocks and ',Key[1],' Lock Owner blocks per node'
Device Custom Number 1	Key[0] (Lock blocks)
Device Custom Number 2	Key[1] (Lock owner blocks)

**Event 17126**

ArcSight Field	Vendor Field
Name	'SQL Server is now ready for client connections'
Message	'SQL Server is now ready for client connections'

**Event 17136**

ArcSight Field	Vendor Field
Name	'Clearing tempdb database'
Message	'Clearing tempdb database'

**Event 17137**

ArcSight Field	Vendor Field
Name	'Starting up database'
Message	'Starting up database ',Key[0]
Device Custom String 1	Key[0]

**Event 17147**

ArcSight Field	Vendor Field
Name	'SQL Server is terminating because of a system shutdown'
Message	'SQL Server is terminating because of a system shutdown. This is an informational message only. No user action is required.'

**Event 17148**

ArcSight Field	Vendor Field
Name	'SQL Server is terminating'
Message	'SQL Server is terminating in response to a 'stop' request from Service Control Manager'

**Event 17152**

ArcSight Field	Vendor Field
Name	'Node configuration'
Message	'Node configuration: node 'Key[0],': CPU mask: 'Key[1],' Active CPU mask: 'Key[3],': 'Key[4],'. This message provides a description of the NUMA configuration for this computer. This is an informational message only. No user action is required.'
Device Custom String 2	Key[0] (Node)
Device Custom String 3	Key[1] (CPU mask)
Device Custom String 4	Key[3] (Active CPU mask)
Device Custom String 5	Key[2] (Flag CPU mask)
Device Custom String 6	Key[4] (Flag Active CPU mask)

**Event 17162**

ArcSight Field	Vendor Field
Name	'SQL Server is starting'
Message	'SQL Server is starting at normal priority base (=7)'

**Event 17164**

ArcSight Field	Vendor Field
Name	'SQL Server detected sockets'
Message	'SQL Server detected 'Key[0],' sockets with 'Key[1],' cores per socket and 'Key[2],' logical processors per socket, 'Key[3],' total logical processors; using 'Key[4],' logical processors based on SQL Server licensing. This is an informational message; no user action is required.'
Device Custom Number 1	Key[0] (Detected sockets)
Device Custom Number 2	Key[1] (Cores per socket)
Device Custom Number 3	Key[2] (Processors per socket)
Device Custom String 3	Key[3] (Total processors)
Device Custom String 4	Key[4] (Using processors)

**Event 17176**

ArcSight Field	Vendor Field
Name	'This instance of SQL Server last reported using a process ID'
Message	'This instance of SQL Server last reported using a process ID of 'Key[0],' at 'Key[1],' (local) 'Key[2],' (UTC). This is an informational message only; no user action is required.'
Destination Process ID	Key[0]
Device Custom Date 1	Key[1] (Last Report Time (local))
Device Custom Date 2	Key[2] (Last Report Time (UTC))

**Event 17177**

ArcSight Field	Vendor Field
Name	'This instance of SQL Server has been using a process ID'
Message	'This instance of SQL Server has been using a process ID of 'Key[0],' since 'Key[1],' (local) 'Key[2],' (UTC). This is an informational message only; no user action is required.'
Device Process ID	Key[0]
Device Custom Date 1	Key[1] (Since Time (local))
Device Custom Date 2	Key[2] (Since Time (UTC))

**Event 17199**

ArcSight Field	Vendor Field
Name	'Restart SQL Server using the trace flag'
Message	'Dedicated administrator connection support was not started because it is disabled on this edition of SQL Server. If you want to use a dedicated administrator connection, restart SQL Server using the trace flag 'Key[0]'. This is an informational message only. No user action is required.'
Device Custom Number 1	Key[0] (Trace flag)

**Event 17201**

ArcSight Field	Vendor Field
Name	'Dedicated admin connection support was established'
Message	'Dedicated admin connection support was established for listening locally on port 'Key[0]'
Destination Port	Key[0]

**Event 17550**

ArcSight Field	Vendor Field
Name	'DBCC TRACEON, server process'
Message	'DBCC TRACEON 'Key[0],' server process ID (SPID) 'Key[1]'. This is an informational message only; no user action is required.'
Destination Process Name	Key[0]
Destination Process ID	Key[1]

**Event 17551**

ArcSight Field	Vendor Field
Name	'DBCC TRACEOFF, server process'
Message	'DBCC TRACEOFF 'Key[0],' server process ID (SPID) 'Key[1]'. This is an informational message only; no user action is required.'
Destination Process Name	All of ('DBCC TRACEON' ,Key[0])
Destination Process ID	Key[1]

**Event 17656**

ArcSight Field	Vendor Field
Name	'Warning'
Message	'Warning *****'

**Event 17658**

ArcSight Field	Vendor Field
Name	'SQL Server started in single-user mode'
Message	'SQL Server started in single-user mode. This is an informational message only. No user action is required.'

**Event 17561**

ArcSight Field	Vendor Field
Name	'index restored'
Message	'index restored for ',Key[1],'. ',Key[2]
Device Custom String 1	Key[1] (Report server database)
Device Custom String 3	Key[2] (Object name)

**Event 17663**

ArcSight Field	Vendor Field
Name	'Server name'
Message	'Server name is ',Key[0]
Destination Host Name	Key[0]

**Event 18456**

ArcSight Field	Vendor Field
Name	'Login failed for user'
Message	'Login failed for user ',Key[0],'. ',Key[21],'. ',Key[2]
Device Custom String 3	Key[1] (Login failed)
Source User Name	Key[0]
Source Address	Key[2]

**Event 18488**

ArcSight Field	Vendor Field
Name	'Login failed for user'
Message	'Login failed for user ',Key[0],'. Reason: The password of the account must be changed. ',Key[1]
Source User Name	Key[0]
Source Address	Key[1]

**Event 18496**

ArcSight Field	Vendor Field
Name	'System Manufacturer and System Model Information'
Message	'System Manufacturer: ',Key[0],' System Model: ',Key[1],' '
Device Custom String 1	Key[0] (System Manufacturer)
Device Custom String 2	Key[1] (System Model)

**Event 19030**

ArcSight Field	Vendor Field
Name	'SQL Trace was started'
Message	'SQL Trace ID ',Key[0],' was started by login ',Key[1],' '
Device Custom String 1	Key[0] (Trace ID)
Source User Name	Key[1]

**Event 19031**

ArcSight Field	Vendor Field
Name	'SQL Trace stopped'
Message	'SQL Trace stopped. Trace ID = ',Key[0],'. Login Name = ',Key[1]
Device Custom Number 1	Key[0] (Trace ID)
Source User Name	Key[1]

**Event 19032**

ArcSight Field	Vendor Field
Name	'SQL Trace was stopped due to server shutdown'
Message	'SQL Trace was stopped due to server shutdown. Trace ID = ',Key[0],'. This is an informational message only; no user action is required.'
Device Custom Number 1	Key[0] (Trace ID)

**Event 26018**

ArcSight Field	Vendor Field
Name	'A self-generated certificate was successfully loaded for encryption'
Message	'A self-generated certificate was successfully loaded for encryption'

**Event 26022**

ArcSight Field	Vendor Field
Name	'Server is listening'
Message	'Server is listening on [',Key[0],' <',Key[1], '> ',Key[2], ' ]'
Device Custom String 4	Key[0] (Listening Address)
Application Protocol	Key[1]
Destination Port	Key[2]

**Event 26037**

ArcSight Field	Vendor Field
Name	'SQL Server Network Interface library could not register the Server Principal Name'
Message	'Failure to register an SPN may cause integrated authentication to fall back to NTLM instead of Kerberos'
Reason	Key[0]
Device Custom Number 1	Key[1] (State)

**Event 26048**

ArcSight Field	Vendor Field
Name	'Server local connection provider is ready to accept connection'
Message	'Server local connection provider is ready to accept connection on [',Key[0],']'
File Path	Key[0]

**Event 26067**

ArcSight Field	Vendor Field
Name	'SQL Server Network Interface library could not register the Service Principal Name (SPN)'
Message	'The SQL Server Network Interface library could not register the Service Principal Name (SPN) ',Key[0],' for the SQL Server service. Windows return code: ',Key[1],', state: ',Key[2],'. Failure to register a SPN might cause integrated authentication to use NTLM instead of Kerberos. This is an informational message. Further action is only required if Kerberos authentication is required by authentication policies and if the SPN has not been manually registered.'
Source Service Name	Key[0]
Reason	Key[1]
Device Custom String 1	Key[2] (State)

**Event 26076**

ArcSight Field	Vendor Field
Name	'SQL Server is attempting to register a Service Principal Name (SPN)'
Message	'SQL Server is attempting to register a Service Principal Name (SPN) for the SQL Server service. Kerberos authentication will not be possible until a SPN is registered for the SQL Server service. This is an informational message. No user action is required.'

**Event 30090**

ArcSight Field	Vendor Field
Name	'New instance of full-text filter daemon host process has been successfully started.'
Message	'A new instance of the full-text filter daemon host process has been successfully started.'

**Event 33090**

ArcSight Field	Vendor Field
Name	'Attempting to load library into memory'
Message	'Attempting to load library 'Key[0],' into memory. This is an informational message only. No user action is required'
File Path	Key[0]

**Event 33204**

ArcSight Field	Vendor Field
Name	'SQL Server Audit could not write to the security log'
Message	'SQL Server Audit could not write to the security log'

**Event 33205**

ArcSight Field	Vendor Field
Source Service Name	EventSource
Source Address	Key[0]
Device Event Class ID	All of (class_type, '[', action_id)
Device Action	Action_id
Event Outcome	succeeded
File ID	object_id
File Type	class_type
File Name	object_name
Message	statement
Source User ID	One of (target_server_principal_name, '', server_principal_id)
Source User Name	One of (target_server_principal_name, '', server_principal_name)
Source NT Domain	One of (target_server_principal_name, '', server_principal_name)
Destination User ID	One of (target_server_principal_name, '', server_principal_id, target_server_principal_id)
Destination User Name	Extracted from NTUser: One of (target_server_principal_name, server_principal_name)
Destination NT Domain	Extracted from NTDomain: One of (target_server_principal_name, server_principal_name)
Device Custom Number 1	session_id
Device Custom Number 2	database_principal_id
Device Custom Number 3	target_database_principal_id
Device Custom String 1	object_name
Device Custom String 2	statement
Device Custom String 3	database_name
Device Custom String 4	Source Owner Name: One of (target_database_principal_name, database_principal_name)
Device Custom String 5	Destination Owner Name: One of (target_database_principal_name, database_principal_name)
Device Custom String 6	schema_name



**Event 33217**

ArcSight Field	Vendor Field
Name	'SQL Server Audit is starting the audits'
Message	'SQL Server Audit is starting the audits. This is an informational message. No user action is required.'

**Event 33218**

ArcSight Field	Vendor Field
Name	'SQL Server Audit has started the audits'
Message	'SQL Server Audit has started the audits. This is an informational message. No user action is required.'

**Event 49903**

ArcSight Field	Vendor Field
Name	'Detected RAM'
Message	'Detected 'Key[0],' of RAM. This is an informational message; no user action is required.'
Device Custom Number 1	Key[0] (Detected RAM)

**Event 49904**

ArcSight Field	Vendor Field
Name	'Service account'
Message	'The service account is 'Key[0]'. This is an informational message; no user action is required.'
Source Service Name	Key[0]

**Event 49910**

ArcSight Field	Vendor Field
Name	'Software Usage Metrics is disabled'
Message	'Software Usage Metrics is disabled'

## Microsoft Windows Server 2008, 2008 R2, 2008 R3

### General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'SQL Server'
Source User Name	User (extracted from NTUser)
Source NT Domain	User (extracted from NTDomain)
Destination User Name	' '

### Event 615

ArcSight Field	Vendor Field
Name	Could not find database
Message	Could not find database ID

### Event 849

ArcSight Field	Vendor Field
Name	Using locked pages for buffer pool
Message	Using locked pages for buffer pool

### Event 958

ArcSight Field	Vendor Field
Name	The resource database build version
Message	The resource database build version is ' '

### Event 1814

ArcSight Field	Vendor Field
Name	Could not create tempdb.
Message	Could not create tempdb. You may not have enough disk space available.

### Event 3406

ArcSight Field	Vendor Field
Name	Transactions rolled forward in database
Message	Transactions rolled forward in database

### Event 3407

ArcSight Field	Vendor Field
Name	Transactions rolled back in database
Message	' ' transactions rolled back in database

**Event 3408**

ArcSight Field	Vendor Field
Name	Recovery is complete.
Message	Recovery is complete. This is an informational message only. No user action is required.

**Event 3454**

ArcSight Field	Vendor Field
Name	Recovery is writing a checkpoint in database
Message	Recovery is writing a checkpoint in database ''

**Event 5579**

ArcSight Field	Vendor Field
Name	File system access
Message	FILESTREAM: effective level = '', configured level = '', file system access share name = "

**Event 8128**

ArcSight Field	Vendor Field
Name	Execute extended stored procedure
Message	Using "version " to execute extended stored procedure "

**Event 9013**

ArcSight Field	Vendor Field
Name	Tail of the log for database is being rewritten
Message	Tail of the log for database '' is being rewritten to match the new sector size of '' bytes. '' bytes at offset '' in file '' will be written

**Event 9666**

ArcSight Field	Vendor Field
Name	Protocol transport disabled or not configured
Message	The '' protocol transport is disabled or not configured

**Event 9688**

ArcSight Field	Vendor Field
Name	Service Broker manager has started
Message	Service Broker manager has started

**Event 9689**

ArcSight Field	Vendor Field
Name	Service Broker manager has shut down
Message	Service Broker manager has shut down

**Event 10981**

ArcSight Field	Vendor Field
Name	Resource governor reconfiguration succeeded
Message	Resource governor reconfiguration succeeded

**Event 15268**

ArcSight Field	Vendor Field
Name	Authentication mode
Message	Authentication mode is ''

**Event 15457**

ArcSight Field	Vendor Field
Name	Configuration option changed
Message	Configuration option '' changed from '' to ''. Run the RECONFIGURE statement to install

**Event 17069**

ArcSight Field	Vendor Field
Name	Microsoft SQL Server 2008 R2 information
Message	''

**Event 17101**

ArcSight Field	Vendor Field
Name	Microsoft Corporation
Message	Microsoft Corporation

**Event 17103**

ArcSight Field	Vendor Field
Name	All rights reserved
Message	All rights reserved

**Event 17104**

ArcSight Field	Vendor Field
Name	Server process ID
Message	Server process ID is ''

**Event 17110**

ArcSight Field	Vendor Field
Name	Server process ID
Message	Server process ID is ''

**Event 17111**

ArcSight Field	Vendor Field
Name	Logging SQL Server messages
Message	Logging SQL Server messages in file ''

**Event 17125**

ArcSight Field	Vendor Field
Name	Using dynamic lock allocation
Message	Using dynamic lock allocation. Initial allocation of '' Lock blocks and '' Lock Owner blocks per node

**Event 17126**

ArcSight Field	Vendor Field
Name	SQL Server is now ready for client connections
Message	SQL Server is now ready for client connections

**Event 17136**

ArcSight Field	Vendor Field
Name	Clearing tempdb database
Message	Clearing tempdb database

**Event 17137**

ArcSight Field	Vendor Field
Name	Starting up database
Message	Starting up database ''

**Event 17148**

ArcSight Field	Vendor Field
Name	SQL Server is terminating
Message	SQL Server is terminating in response to a 'stop' request from Service Control Manager

**Event 17152**

ArcSight Field	Vendor Field
Name	Node configuration
Message	Node configuration: node '':CPU mask: '':'' Active CPU mask: '':''

**Event 17162**

ArcSight Field	Vendor Field
Name	SQL Server is starting
Message	SQL Server is starting at normal priority base (=7)

**Event 17164**

ArcSight Field	Vendor Field
Name	Detected CPUs
Message	Detected '' CPUs

**Event 17176**

ArcSight Field	Vendor Field
Name	This instance of SQL Server last reported using a process ID
Message	This instance of SQL Server last reported using a process ID of '' at '' (local) '' (UTC)

**Event 17177**

ArcSight Field	Vendor Field
Name	This instance of SQL Server has been using a process ID
Message	This instance of SQL Server has been using a process ID of '' since '' (local) '' (UTC)

**Event 17201**

ArcSight Field	Vendor Field
Name	Dedicated admin connection support was established
Message	Dedicated admin connection support was established for listening locally on port ''

**Event 17663**

ArcSight Field	Vendor Field
Name	Server name
Message	Server name is ''

**Event 18456**

ArcSight Field	Vendor Field
Name	Login failed for user
Message	Login failed for user '', ''''
Source User Name	extracted from NTUser

**Event 18496**

ArcSight Field	Vendor Field
Name	System Manufacturer and System Model Information
Message	System Manufacturer: '', System Model: ''

**Event 19030**

ArcSight Field	Vendor Field
Name	SQL Trace was started
Message	SQL Trace ID '' was started by login ''
Source User Name	extracted from NTUser

**Event 19031**

ArcSight Field	Vendor Field
Name	SQL Trace stopped
Message	SQL Trace stopped. Trace ID = ''. Login Name = ''
Source User Name	extracted from NTUser

**Event 19032**

ArcSight Field	Vendor Field
Name	SQL Trace was stopped due to server shutdown
Message	SQL Trace was stopped due to server shutdown. Trace ID = ''

**Event 26018**

ArcSight Field	Vendor Field
Name	A self-generated certificate was successfully loaded for encryption
Message	A self-generated certificate was successfully loaded for encryption

**Event 26022**

ArcSight Field	Vendor Field
Name	Server is listening
Message	Server is listening on '', '', ''

**Event 26037**

ArcSight Field	Vendor Field
Name	SQL Server Network Interface library could not register the Service Principal Name
Message	Error: '', state: ''. Failure to register an SPN may cause integrated authentication to fall back to NTLM instead of Kerberos

**Event 26048**

ArcSight Field	Vendor Field
Name	Server local connection provider is ready to accept connection
Message	Server local connection provider is ready to accept connection on ''

**Event 33090**

ArcSight Field	Vendor Field
Name	Attempting to load library into memory
Message	Attempting to load library ' ' into memory

**Event 33204**

ArcSight Field	Vendor Field
Name	SQL Server Audit could not write to the security log
Message	SQL Server Audit could not write to the security log

**Event 33205**

ArcSight Field	Vendor Field
Destination Host Name	server_instance_name
Destination NT Domain	One of (target_server_principal_name, server_principal_name) from NTDomain
Destination User ID	One of (server_principal_id, target_server_principal_id)
Destination User Name	One of (target_server_principal_name, server_principal_name) from NTUser
Device Action	action_id
Device Custom Number 1	session_id
Device Custom Number 2	database_principal_id
Device Custom Number 3	target_database_principal_id
Device Custom String 1	object_name
Device Custom String 2	Statement
Device Custom String 3	database_name
Device Custom String 4	Source Owner Name (database_principal_name)
Device Custom String 5	Destination Owner Name (one of (target_database_principal_name, database_principal_name))
Device Custom String 6	schema_name
Device Event Class ID	Both (class_type, action_id)
Event Outcome	succeeded
File ID	object_id
File Name	object_name
File Type	class_type
Message	Statement
Source NT Domain	server_principal_name from NTDomain
Source Service Name	EventSource
Source User ID	server_principal_id
Source User Name	server_principal_name from NTUser



**Event 33217**

ArcSight Field	Vendor Field
Name	SQL Server Audit is starting the audits
Message	SQL Server Audit is starting the audits. This is an informational message. No user action is required

**Event 33218**

ArcSight Field	Vendor Field
Name	SQL Server Audit has started the audits
Message	SQL Server Audit has started the audits. This is an informational message. No user action is required

**Event 30090**

ArcSight Field	Vendor Field
Name	New instance of full-text filter daemon host process has been successfully started
Message	A new instance of the full-text filter daemon host process has been successfully started