



Micro Focus Security ArcSight Connectors

SmartConnector for Microsoft Windows Event
Log – Unified: Active Directory

Supplemental Configuration Guide

July 15, 2017

Supplemental SmartConnector Configuration Guide for

Microsoft Windows Event Log – Unified: Active Directory

July 15, 2017

© Copyright 2010 - 2018 Micro Focus or one of its affiliates

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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.

Copyright Notice

© Copyright 2010 - 2018 Micro Focus or one of its affiliates.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Revision History

Date	Description
07/15/2017	Removed platform support for Windows 2003.
09/30/2014	Removed Windows 2000 event mappings.
09/30/2013	Updated "Collect Events from the Event Log" procedure.
05/15/2013	Added mappings for events 1138, 1139, 1213, 1215, 1216, 1317, 1535, 1655, 2041, 2089 ,2889
03/29/2013	Added mappings for Windows 2012 Server/Windows 8 support.
05/15/2012	Updated for new installation procedure.
03/30/2012	Added information for setting eventlogtypes parameter.
11/15/2011	Updated configuration information.
09/24/2010	Editorial update to document name and overview information.

Date	Description
05/26/2010	General availability of this support. Updated the mappings for Active Directory Windows events.
02/11/2010	First edition of this Configuration Guide, for initial beta support of this connector.

Contents

Revision History	2
Product Overview	5
Audit Active Directory Objects in Windows	5
Configure an Audit Policy Setting for a Domain Controller	5
Configure Auditing for Specific Active Directory Objects	6
Connector Installation and Configuration	8
Collect Events from the Event Log	8
General Mappings	8
Windows 2008 NTDS Database Mappings	9
Windows 2008 General NTDS Mappings	10
Windows 2008 NTDS ISAM Mappings	16
Windows 2008 NTDS KCC Mappings	19
Windows 2008 NTDS LDAP Mappings	20
Windows 2008 NTDS Replication Mappings	24
Windows 2012/Windows 8 NTDS LDAP Mappings	25

SmartConnector for Microsoft Windows Event Log – Unified: Active Directory

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Unified: Active Directory and its event mappings to ArcSight data fields.

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 Microsoft Active Directory Windows Event Log – Unified: Active Directory.

Product Overview

Active Directory, an essential component of the Windows architecture, presents organizations with a directory service designed for distributed computing environments. Active Directory lets organizations centrally manage and share information on network resources and users while acting as the central authority for network security.

Audit Active Directory Objects in Windows

When you use Windows auditing, you can track both user activities and Windows activities. When you use auditing, you can specify which events are written to the Security log. For example, the Security log can maintain a record of both valid and invalid logon attempts and events that relate to creating, opening, or deleting files or other objects.

When you audit Active Directory events, Windows writes an event to the Security log on the domain controller. For example, if a user attempts to log on to the domain using a domain user account and the logon attempt is unsuccessful, the event is recorded on the domain controller and not on the computer on which the logon attempt was made. This is because it is the domain controller that attempted to authenticate the logon attempt but could not do so.

To enable auditing of Active Directory objects:

- 1 Configure an audit policy setting for a domain controller. (When you configure an audit policy setting, you can audit objects, but you cannot specify which object you want to audit.)
- 2 Configure auditing for specific Active Directory Objects. After you specify the events to audit for files, folders, printers, and Active Directory Objects, Windows tracks and logs these events.

Configure an Audit Policy Setting for a Domain Controller

Auditing is turned off by default. For domain controllers, an audit policy setting is configured for all domain controllers in the domain. To audit events that occur on domain controllers, configure an audit policy setting that applies to all domain controllers in a non-Local Group Policy object (GPO) for the domain. You can access this policy setting through the Domain Controller's organizational unit. To audit user access to Active Directory objects, configure the Audit Directory Service Access event category in the audit policy setting.

The computer on which you want to configure an audit policy setting must be granted the Manage Auditing and Security Log user right. By default, Windows grants these rights to the Administrators group.



The files and folders you want to audit must be on Microsoft Windows NT file system (NTFS) volumes.

To configure an audit policy setting for a domain controller (steps may vary for differing Windows operating systems):

- 1 Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- 2 From the **View** menu, click **Advanced Features**.
- 3 Right-click **Domain Controllers**; then click **Properties**.
- 4 Click the **Group Policy** tab, click **Default Domain Controller Policy**, and then click **Edit**.
- 5 Click **Computer Configuration**, double-click **Windows Settings**, double-click **Security Settings**, double-click **Local Policies**, and then double-click **Audit Policy**.
- 6 In the right pane, right-click **Audit Directory Services Access**, and then click **Security**.
- 7 Click **Define These Policy Settings**, then click to select one or both of the following check boxes:

Success: Click to audit successful attempts for the event category
Failure: Click to audit failed attempts for the event category
- 8 Right-click any other event category that you want to audit; then click **Security**.
- 9 Click **OK**.
- 10 Because the changes you make to your computer's audit policy setting takes affect only when the policy setting is propagated (or applied) to your computer, to initiate policy propagation, either enter `secedit/refreshpolicy machine_policy` at the command prompt and then restart the computer or wait for automatic policy propagation, which occurs at regular intervals you can configure. By default policy propagation occurs every eight hours.

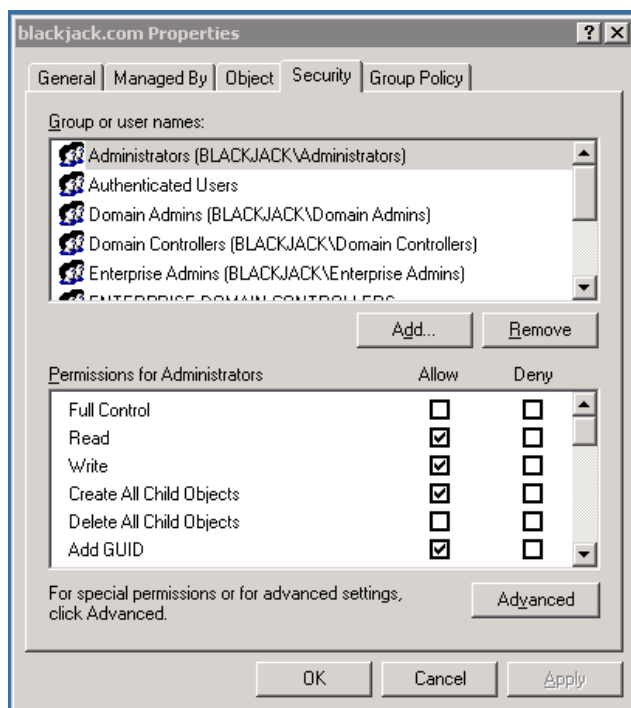
Configure Auditing for Specific Active Directory Objects

After you configure an audit policy setting, you can configure auditing for specific objects, such as users, computers, organizational units, or groups, by specifying both the types of access and the users whose access you want to audit.

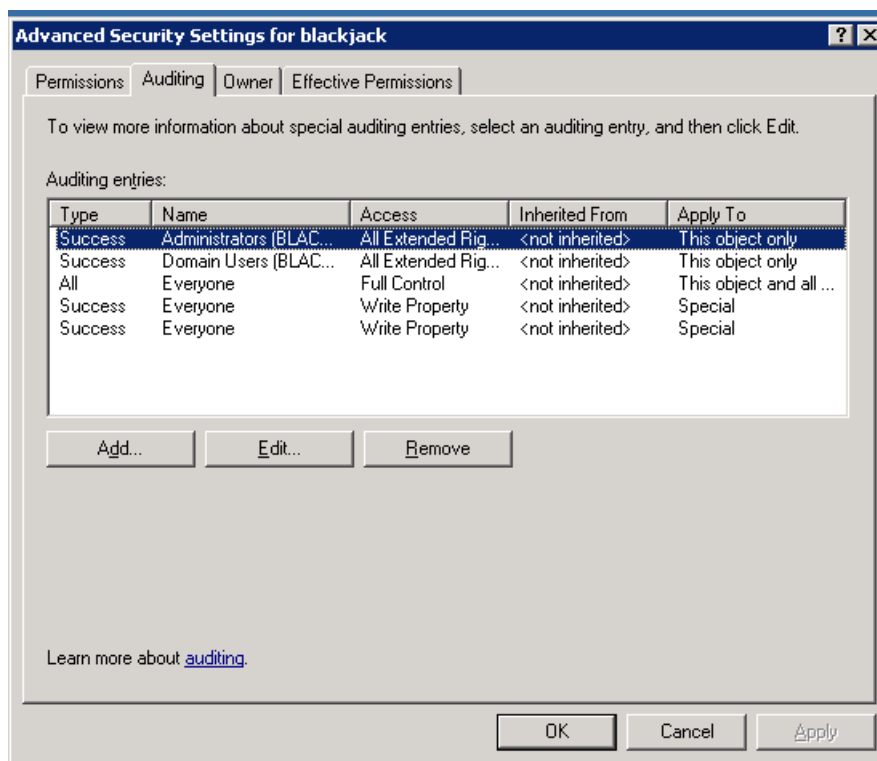
To configure auditing for specific Active Directory objects (steps may vary for differing Windows operating systems):

- 1 Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
- 2 Verify that **Advanced Features** is selected on the **View** menu (the command has a checkmark beside it).

- 3 Right-click on the Active Directory object you want to audit (`blackjack.com` in the example) and select **Properties**.



- 4 Click the **Security** tab, then click the **Advanced** button; **Advanced Security Settings** for the object is displayed. Click the **Auditing** tab.



- 5 To add an object, click **Add**.
- 6 Either enter the name of either the user or the group whose access you want to audit in the **Enter the object name to select** box, then click **OK**, or browse the list of names and then double-click either the user or the group whose access you want to audit.
- 7 Click to select either the **Successful** checkbox or the **Failed** checkbox for the actions you want to audit, then click **OK**. Click **OK** on the next two windows to exit.

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 **Directory Service** in the **Custom Log Names** field.

You can specify multiple Custom Log Names in a comma-separated format; for example:

`Directory Service, 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*.

General Mappings

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Windows 2008 NTDS Database Mappings

General

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	Microsoft Active Directory Domain services version

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	Microsoft Active Directory Domain services version

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared. New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1404

ArcSight Field	Vendor Field
Name	'This directory service is now the intersite topology generator and has assumed responsibility for generating and maintaining intersite replication topologies for this site'

Event 1844

ArcSight Field	Vendor Field
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code

Event 2064

ArcSight Field	Vendor Field
Name	'Active Directory has detected that the quota-tracking table is either missing or not completely built'
Message	'Active Directory has detected that the quota-tracking table is either missing or not completely built. The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'

Event 2065

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has completed rebuilding the quota-tracking table. Quota enforcement is now in effect'

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

Windows 2008 General NTDS Mappings**Event 1000**

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory startup complete'
Device Version	Microsoft Active Directory Domain Services version

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	Destination network address
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service

ArcSight Field	Vendor Field
Source User Name	User

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory was unable to establish a connection with the global catalog'
Message	'Make sure a global catalog is available in the forest, and is reachable from this domain controller. You may use the nltest utility to diagnose this problem'
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Directory service

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1463

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected and deleted some possibly corrupted indices as part of initialization'

Event 1844

ArcSight Field	Vendor Field
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID
Destination Host name	source directory service address

Event 1863

ArcSight Field	Vendor Field
Name	'This directory server has not received replication information from a number of directory servers within the configured latency interval'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of directory servers in all sites
Device Custom Number 2	Number of directory servers in this site
Device Custom Number 3	Latency Interval (Hours)
File Type	Registry Key
File Name	Registry Key

Event 1864

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'Directory servers that do not replicate in a timely manner may encounter errors. They may miss password changes and be unable to authenticate. A DC that has not replicated in a tombstone lifetime may have missed the deletion of some objects, and may be automatically blocked from future replication until it is reconciled'
Device Custom String 1	Directory partition
Device Custom Number 1	More than 24 hours
Device Custom Number 2	More than a week
Device Custom Number 3	More than one month

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory has located a global catalog'
Device Custom String 5	Site
Destination Host Name	Global catalog

Event 1898

ArcSight Field	Vendor Field
Name	'Internal event: Schema object was modified'

Device Custom String 5	Schema object
File Name	Schema object name
File Type	'Schema object'

Event 1925

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link for writable directory partition failed'
Message	'This directory service will be unable to replicate with the source directory service until this problem is corrected'
Destination Host Name	Source directory service address
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source directory service
Source User Name	User

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	Source domain controller address
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
Source User Name	User

Event 2013

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services is rebuilding indices as part of the initialization process'
Device Custom Number 3	Indices

Event 2014

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services successfully completed rebuilding indice'
Device Custom Number 3	Indices

Event 2041

ArcSight Field	Vendor Field
Name	'Duplicate event log entries were suppressed'
Message	'See the previous event log entry for details. An entry is considered a duplicate if the event code and all of its insertion parameters are identical. The time period for this run of duplicates is from the time of the previous event to the time of this event'
Device Custom String 1	Event Code
Device Custom Number 3	Number of duplicate entries

Event 2064

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected that the quota-tracking table is either missing or not completely built'
Message	'The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	'Registry key'
Destination Host Name	Failing DNS host name

Event 2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 4	Reason or Error Code

Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	'Registry key'
Destination Host Name	Failing DNS host name

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	FSMO Role

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

Windows 2008 NTDS ISAM Mappings**Event 102**

ArcSight Field	Vendor Field
Name	'The database engine started a new instance'
Device Version	database engine version
Device Custom String 5	Instance ID

Event 103

ArcSight Field	Vendor Field
Name	'The database engine stopped the instance'
Device Custom String 5	Instance ID

Event 300

ArcSight Field	Vendor Field
Name	'The database engine is initiating recovery steps'

Event 301

ArcSight Field	Vendor Field
Name	'The database engine has begun replaying logfile'
File Name	logfile

Event 302

ArcSight Field	Vendor Field
----------------	--------------

Name	'The database engine has successfully completed recovery steps'
------	---

Event 609

ArcSight Field	Vendor Field
Name	'The database engine is initiating index cleanup of database as a result of a Windows version upgrade'
Message	'This message is informational and does not indicate a problem in the database'
File Name	database
Device Version	version
Device Custom String 5	old device version

Event 611

ArcSight Field	Vendor Field
Name	'The secondary index of table will be rebuilt as a precautionary measure after the Windows version upgrade of this system'
File Name	database
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 612

ArcSight Field	Vendor Field
Name	'The database engine has successfully completed index cleanup on database'
File Name	database

Event 614

ArcSight Field	Vendor Field
Name	'The secondary index of table may be corrupt'
Message	'If there is no later event showing the index being rebuilt, then please defragment the database to rebuild the index'
File Name	database
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 626

ArcSight Field	Vendor Field
Name	'The database engine updated index entries in database because of a change in the NLS version'
Message	'This message is informational and does not indicate a problem in the database'
Device Custom Number 3	Index entries
File Name	database

Event 700

ArcSight Field	Vendor Field
Name	'Online defragmentation is beginning a full pass on database'
File Name	database

Event 701

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed a full pass on database'
File Name	database

Event 702

ArcSight Field	Vendor Field
Name	'Online defragmentation is resuming its pass on database'
File Name	database

Event 703

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed the resumed pass on database'
File Name	database

Event 704

ArcSight Field	Vendor Field
Name	'Online defragmentation of database was interrupted and terminated'
Message	'The next time online defragmentation is started on this database, it will resume from the point of interruption'
File Name	database

Windows 2008 NTDS KCC Mappings

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	Destination network address
Destination User Name	User
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service

Event 1128

ArcSight Field	Vendor Field
Name	'A replication connection was created from source directory service to the local directory service'
Device Custom String 1	Creation Point Internal ID
Device Custom String 4	Reason or Error Code
Device Custom String 5	Local directory service
Device Custom String 6	Source directory service

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Domain service

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	Source domain controller address
Destination User Name	User
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller

Windows 2008 NTDS LDAP Mappings**Event 1000**

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	Microsoft Active Directory Domain Services version

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was unable to establish a connection with the global catalog'
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID

Event 1220

ArcSight Field	Vendor Field
Name	'LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server was unable to obtain a certificate'
Device Custom String 4	Reason or Error Code

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Directory service

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has located a global catalog'
Device Custom String 5	Site
Destination Host Name	Global catalog

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	'Registry key'
Source Host Name	Failing DNS host name

Event 2088

ArcSight Field	Vendor Field
----------------	--------------

Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	Registry key'
Source Host Name	Failing DNS host name

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'
Device Custom Number 1	Number of simple binds performed without SSL/TLS
Device Custom Number 2	Number of Negotiate/Kerberos/NTLM/Digest binds performed without signing

Windows 2008 NTDS Replication Mappings

Event 1188

ArcSight Field	Vendor Field
Name	'A thread in Active Directory Domain Services is waiting for the completion of a RPC made to directory service'
Message	'Active Directory Domain Services has attempted to cancel the call and recover this thread. If this condition continues, restart the directory service'
Device Custom String 1	Thread ID
Device Custom String 5	Operation
Device Custom String 6	Directory service
Device Custom Number 2	Timeout period (minutes)

Event 1232

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services attempted to perform a remote procedure call (RPC) to server. The call timed out and was cancelled'
Destination Host Name	Server
Device Custom Number 2	Call Timeout (Mins)
Device Custom String 1	Thread ID
Device Custom String 5	Internal ID
Source User Name	User

Event 1863

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'This directory server has not received replication information from a number of directory servers within the configured latency interval. To identify the directory servers by name, use the dcdiag.exe tool. You can also use the support tool repadmin.exe to display the replication latencies of the directory servers. The command is \"repadmin /showvector /latency <partition-dn>\"'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of domain controllers in all sites
Device Custom Number 3	Number of domain controllers in this site
Device Custom Number 2	Latency Interval (Hours)
File Type	Registry Key
File Name	Registry Key

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address. This error prevents additions, deletions and

	changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Source Host Name	Failing DNS host name
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	'Registry key'

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	FSMO Role

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \"LDAP Interface Events\" event logging category to level 2 or higher'
Device Custom Number 1	Number of simple binds performed without SSL/TLS
Device Custom Number 2	Number of Negotiate/Kerberos/NTLM/Digest binds performed without signing

Windows 2012/Windows 8 NTDS LDAP Mappings

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	Version

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was unable to establish a connection with the global catalog'
Device Custom String 5	Internal ID
Device Custom String 4	Reason or Error Code
Reason	Reason or Error Code

Event 1138

ArcSight Field	Vendor Field
Name	'Function entered'
Message	'Internal event: Function entered'

Event 1139

ArcSight Field	Vendor Field
Name	'Function exited'
Message	'Internal event: Function exited'

Event 1213

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because it was disconnected on the client side'
Device Custom String 5	Internal ID

Event 1215

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because the client closed the connection'
Device Custom String 5	Internal ID

Event 1216

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because of an error'
Source Address	Source address
Reason	Reason or Error Code
Device Custom String 5	Internal ID

Event 1220

ArcSight Field	Vendor Field
Name	'LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server was unable to obtain a certificate'
Device Custom String 4	Reason or Error Code

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed.'
Device Custom Number 3	Attempts
Device Custom String 6	Directory service
Device Custom Number 2	Period of time (minutes)
Device Custom String 4	Reason or Error Code

Event 1317

ArcSight Field	Vendor Field
Name	'The directory service has disconnected the LDAP connection'
Message	'The directory service has disconnected the LDAP connection from the following network address due to a time-out'
Source Address	Source address

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted.'

Event 1535

ArcSight Field	Vendor Field
Name	'The LDAP server returned an error'
Message	'The LDAP server returned an error'
Reason	Reason or Error Code

Event 1655

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services attempted to communicate with the following global catalog and the attempts were unsuccessful'
Device Host Name	Host name
Reason	Reason or Error Code

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has located a global catalog'
Destination Host Name	Host name
Device Custom String 5	Site

Event 2041

ArcSight Field	Vendor Field
Name	'Duplicate event log entries were suppressed'
Message	'See the previous event log entry for details. An entry is considered a duplicate if the event code and all of its insertion parameters are identical. The time period for this run of duplicates is from the time of the previous event to the time of this event'
Device Custom Number 3	Number of duplicate entries

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions, and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources.'
Device Custom String 6	Source domain controller
Source Host Name	Host name
Device Custom String 4	Reason or Error Code
File Type	'Registry Key'
File Name	File name

Event 2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers, or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 6	Alternate server name
Source Host Name	Host name
Device Custom String 4	Reason or Error Code
File Type	'Registry Key'
File Name	File name

Event 2089

ArcSight Field	Vendor Field
Name	'This directory partition has not been backed up'
Message	'This directory partition has not been backed up since at least the following number of days'
Device Custom String 1	Directory partition
Device Custom Number 2	Latency interval (hours)
File Type	'Registry Key'
File Name	File name

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a clear text (non-SSL/TLS-encrypted) connection.'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher.'

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkID=87923 . Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \"LDAP Interface Events\" event logging category to level 2 or higher.'
Device Custom Number 1	Simple binds performed without SSL/TLS
Device Custom Number 2	Negotiate/Kerberos/NTLM/Digest binds performed without signing

Event 2889

ArcSight Field	Vendor Field
Name	'LDAP bind without requesting signing or performed a simple bind'
Message	'The following client performed a SASL (Negotiate/Kerberos/NTLM/Digest) LDAP bind without requesting signing (integrity verification), or performed a simple bind over a cleartext (non-SSL/TLS-encrypted) LDAP connection'
Source User Name	User name
Source Address	Source address