
Micro Focus Security ArcSight SmartConnectors

Software Version: 8.2.2

Configuration Guide for Linux Audit File SmartConnector

Document Release Date: October 2021

Software Release Date: October 2021



Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

Copyright Notice

© Copyright 2021 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

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.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

- Configuration Guide for Linux Audit File SmartConnector 5
- Product Overview 5
- Configuration 7
- Preparing to Install the SmartConnector 7
- Installing and Configuring the SmartConnector by Using the Wizard 9
- Configuring Event Merging 10
- Device Event Mapping to ArcSight Fields 11
 - Linux Audit Mappings to ArcSight Fields 11
- Send Documentation Feedback 14

Configuration Guide for Linux Audit File SmartConnector

This guide provides information for installing the SmartConnector for Linux Audit File and configuring the device for event collection. Linux auditd is the userspace component to the Linux Auditing System that is responsible for writing audit records to the disk.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectors to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact [Micro Focus Customer Care](#).

Product Overview

The Linux auditd daemon is similar to network-based intrusion detection systems and host-based intrusion detection systems and can help you detect violations of your

security policies. It however, does not enforce security policies. Because the audit daemon is part of the Linux kernel, it is included in most major Linux distributions by default.

Supported versions for Linux auditd to collect events from Red Hat Enterprise Linux (RHEL) are:

6.4, 6.5, 6.7, 7.1, 7.2, 7.4, 7.5, 7.6, 8.1, 8.2, 8.3, and 8.4

Configuration

For complete information about the Linux auditd daemon, see the man pages for auditd, auditd.conf, and auditctl. You can access these man pages by running the `man auditd` or `man auditctl` commands, from the command line of your Linux system.

- `auditctl` is responsible for controlling the status and some basic system parameters of auditd. Using audit rules, `auditctl` controls which components of your system are subjected to the audit and to what extent they are audited. Audit rules can be passed to auditd on the `auditctl` command line as well as by composing a rule set and instructing auditd to process this file.
- `auditd` has built-in functions to watch access attempts to files without needing to monitor the applicable system calls. Administrators can add rules by amending the provided configuration files or at run time using the command line. The default location for the audit daemon rules in `/etc/audit/audit.rules`.

`auditd` adds events to the audit log file as they occur. By default, the system stores audit logs in `/var/log/audit/`.

Before you can start generating audit logs and processing them, configure how the daemon is started in the `/etc/sysconfig/auditd` configuration file and configure how the audit system functions once the daemon has been started in `/etc/audit/auditd.conf`.

Preparing to Install the SmartConnector

The following sections provide instructions for installing and configuring the Linux Audit File SmartConnector.



Connector Appliance or ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Before you install any SmartConnectors, make sure that the Micro Focus ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform* guide, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector by Using the Wizard

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. From the **Type** drop-down list, select **Linux Audit File** as the type of connector, then click **Next**.
5. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Log File Name	Enter the path to and name of the log file. The default value is /var/log/audit/audit.log.

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. Select whether you want to [run the connector as a service or in the standalone mode](#).
9. Complete the installation.
10. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [SmartConnector Installation and User Guide](#).



When using Windows authentication, after completing the connector installation, if running on a Windows Server, change the service account to use the Windows account that should log in to the database. The connector will use the account used to start the service, regardless of the account value setting entered in the connector setup process.

Configuring Event Merging

The Linux Audit system provides a way to track security-relevant information on the system. Based on pre-configured rules, Linux Audit generates log entries to record as much information as possible about the events happening on your system. These events often contains multiple sub-events that can span multiple lines. The event merging feature aggregates the related sub-events into one large event with a concatenated long message.

To enable event merging:

1. Set up Linux Audit connector. See [Installing the SmartConnector](#).
2. Edit the `fcv.version` parameter in the `agent.properties` file (located in the `$ARCSIGHT_HOME/current/user/agent` folder) as follows: `agents [0].fcv.version=1`
3. [Run the SmartConnector](#).

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Linux Audit Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	proto
Destination Address	One of (daddr,laddr,dst)
Destination Mac Address	dmac
Destination Port	One of (dest, dport, lport)
Destination Process ID	One of (egid,opid)
Destination Process Name	One of (exe, comm, cmd ,ocomm)
Destination Service Name	One of (com, ocomm, grantors)
Destination User ID	One of (auid, new auid, old auid, old-auid, oid)
Destination User Name	One of (new-seuder, acct, OUID)
Destination User Privilege	new-role
Device Action	op
Device Custom Number 1	calipso_doi
Device Custom Number 2	One of (oses,ses,new ses, oldses,old-ses)
Device Custom Number 3	uid
Device Custom String 1	One of (dev, old, nsec)
Device Custom String 2	One of (key, calipso_type, new, sec)
Device Custom String 3	One of (success, res)
Device Custom String 4	One of(syscall,SYSCALL,op)
Device Custom String 5	subj
Device Custom String 6	One of (terminal, tty)
Device Event Category	type
Device Event Class ID	One of (res, type, both (type, res))

Configuration Guide for Linux Audit File SmartConnector

Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Host Name	node
Device Inbound Interface	inif
Device Outbound Interface	outif
Device Process Name	'auditd'
Device Product	'auditd'
Device Receipt Time	timestamp
Device Vendor	'Unix'
Device Version	One of (ver, kernel)
Event Destination	ProcessId egid
Event Outcome	One of (result, res, __simpleMap(success, "yes=Successful", "no=Failed"))
Event Reason	One of (reason, cause)
External ID	callid
File Hash	One of (proctitle, data, cmd, fp)
File ID	One of (watch_inode, cap_fver, sw)
File Name	One of (path, name, watch, obj)
File Path	cwd One of (cwd, root_dir)
File Permission	One of (mode, perm)
File Size	ksize
Flex String 2	One of (ppid, direction)
Message	msg
Name	One of (res, type, both (res, type), 'Linux Audit Message')
Old File Hash	mac
Old File ID	All of (a0, a1, a2, ...)
Old File Name	cipher
Old File Path	cmdline
Request URL	pfs
Source Address	One of (addr, saddr, src)
Source Host Name	hostname
Source Mac Address	smac
Source Port	One of (sport, rport)

ArcSight ESM Field	Device-Specific Field
Source Process ID	One of (pid, Spid, spid)
Source User ID	One of (savid, uid, oavid,AUID)
Source User Name	One of (user, old-seuser, EUID,OAUID)
Source User Privileges	One of (old-role, EGID)



Note: The connector will not receive events if MySQL JDBC driver 5.1.38 was used when you configured it. To fix this issue, apply MySQL JDBC driver 5.0.8.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for Linux Audit File SmartConnector (SmartConnectors 8.2.2)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!