Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

Configuration Guide for Oracle Solaris Basic Security Module SmartConnector

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

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

https://www.microfocus.com

Copyright Notice

Trademark Notices

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

Contents

Configuration Guide for Oracle Solaris Basic Security Module SmartConnector

Configuration Guide for Oracle Solaris Basic Security Module SmartConnector

Solaris versions 8 and 9 are no longer supported for SmartConnector installation and have been removed from connector configuration selections. To continue running these versions with the SmartConnector, do not upgrade the connector. To upgrade, you must be using Solaris version 10 or later.

This guide provides information for installing the SmartConnector for Oracle Solaris Basic Security Module on a Solaris platform and configuring the device for audit log event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector 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.
- *Configuration Guide for ArcSight SmartConnector Load Balancer*, which provides detailed information about installing Load Balancer.
- *Release Notes for ArcSight SmartConnectors and ArcSight SmartConnector Load Balancer*, 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 Oracle Solaris Basic Security Module (BSM) provides a security auditing subsystem. The auditing mechanism lets administrators detect potential security breaches. It performs kernel auditing and provides a device allocation mechanism for the Solaris operating system, which enable Solaris to meet C2 level criteria.

C2 is a security rating originally defined in the Trusted Computer System Evaluation Criteria (TCSEC), published by the United States National Computer Security Center (NCSC), commonly referred to as the Orange Book.

The BSM audit trail is written to binary files on the location system (or NFS mount). Audit records are initiated from two distinct places in Solaris-privileged user land programs (such as login) and the Solaris kernel. All security-sensitive kernel system calls generate an audit record when BSM auditing is enabled.

Reading or executing privileged audit files requires administrator access.

BSM is not enabled by default under Solaris. The administrator is required to run the `bsmconv` script to set up the initial auditing environment for the system.

Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Preparing to Install the SmartConnector

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*, available on ArcSight Documentation.

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

Installing and Configuring the SmartConnector

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. Select **Oracle Solaris Basic Security Module** from the **Type** drop-down, then click **Next**.\
5. Specify the following parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Solaris Version	Select your Solaris version: 10.x or 11.x
Log Directory	Enter the absolute path to the directory containing the log files. The default value is /var/audit.

6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the**

certificate to connector from destination, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

9. Select whether you want to run the connector as a service or in the standalone mode.
10. Complete the installation.
11. Run the SmartConnector.

For instructions about upgrading the connector or modifying parameters, see SmartConnector Installation and User Guide.

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.

Oracle Solaris 10 and 11 BSM Common Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Destination Host Name	Host
Destination User Name	subject-audit-uid
Device Action	return-errval
Device Custom Number 1	subject-sid
Device Custom Number 1 Label	'Session ID'
Device Custom String 2	exec_args
Device Custom String 2 Label	'exec_args'
Device Custom String 3	subject-tid-host
Device Custom String 3 Label	'Terminal Host'
Device Custom String 4	One of (return-retval, return-errval-reason)
Device Custom String 4 Label	'Reason or Error Code'
Device Custom String 5	subject-rgid or subject-gid
Device Custom String 5 Label	'Source User Group'
Device Custom String 6	subject-rgid
Device Custom String 6 Label	'Destination User Group'
Device Event Class ID	Event
Device Host Name	Host
Device Process Name	'auditid'
Device Product	'BSM'

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	DateTime
Device Vendor	'Oracle'
Device Version	_DEVICE_VERSION
External ID	subject-pid
File Name	Path
Message	text
Name	Event

Event Type AUE_su

ArcSight ESM Field	Device-Specific Field
Destination User Name	Text
Device Custom String 4	Text
Device Custom String 5	subject-rgid
Device Custom String 6	NA
Source Host Name	subject-tid-host
Source User Name	subject-ruid

Event Type AUE_rexecd

ArcSight ESM Field	Device-Specific Field
Source Host Name	Text

Event Type AUE_passwd

ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (subject-audit-uid,text)
Device Custom String 6	NA
Source Host Name	host
Source User Name	subject-audit-uid

Event Type AUE_rexd

ArcSight ESM Field	Device-Specific Field
Source Host Name	text

Event Type AUE_ftp_access

ArcSight ESM Field	Device-Specific Field
Device Custom String 4	text
Source Host Name	subject-tid-host

Event Type AUE_login-ssh

ArcSight ESM Field	Device-Specific Field
Source Host Name	subject-tid-host

Event Type AUE_role_login

ArcSight ESM Field	Device-Specific Field
Destination User Name	subject-ruid
Device Custom String 5	subject-gid
Device Custom String 6	subject-rgid
Source Host Name	subject-tid-host
Source User Name	subject-audit-uid

Event Type AUE_newgrp_login

ArcSight ESM Field	Device-Specific Field
Destination User Name	subject-ruid
Device Custom String 5	subject-rgid

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	text
Source Host Name	host
Source User Name	subject-ruid

Event Type AUE_zlogin

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	Zone

Event Type AUE_sudo

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	subject-gid
Source User Name	subject-audit-uid

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 Oracle Solaris Basic Security Module SmartConnector (SmartConnectors 8.3.0)

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!