Micro Focus Security ArcSight Micro Focus Security ArcSight Connectors

Software Version: 8.3.0

Configuration Guide for Oracle WebLogic Server File 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

© Copyright 2022 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.

Document Revision History

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

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to ArcSight Product Documentation Community on the Micro Focus Security Community.

Document Changes

Date	Product Version	Description
MM/DD/YYYY	X.X.X.X	Description of change

Contents

Configuration Guide for Oracle WebLogic Server File SmartConnector

Configuration Guide for Oracle WebLogic Server File SmartConnector

This guide provides information for installing the SmartConnector for Oracle WebLogic Server File and configuring the device for 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

Oracle WebLogic Server is a scalable, enterprise-ready Java Platform, Enterprise Edition (Java EE) application server. The WebLogic Server infrastructure supports the deployment of many types of distributed applications and is a foundation for building applications based on Service Oriented Architectures (SOA). SOA is a design methodology aimed at maximizing the reuse of application services.

System administration of a WebLogic Server environment includes tasks such as creating WebLogic Server domains, deploying applications, migrating domains from development environments to production environments, monitoring and configuring the performance of the WebLogic Server domain, and diagnosing and troubleshooting problems. WebLogic Server provides many tools for system administrators to help with these tasks, including a browser-based Administration Console.

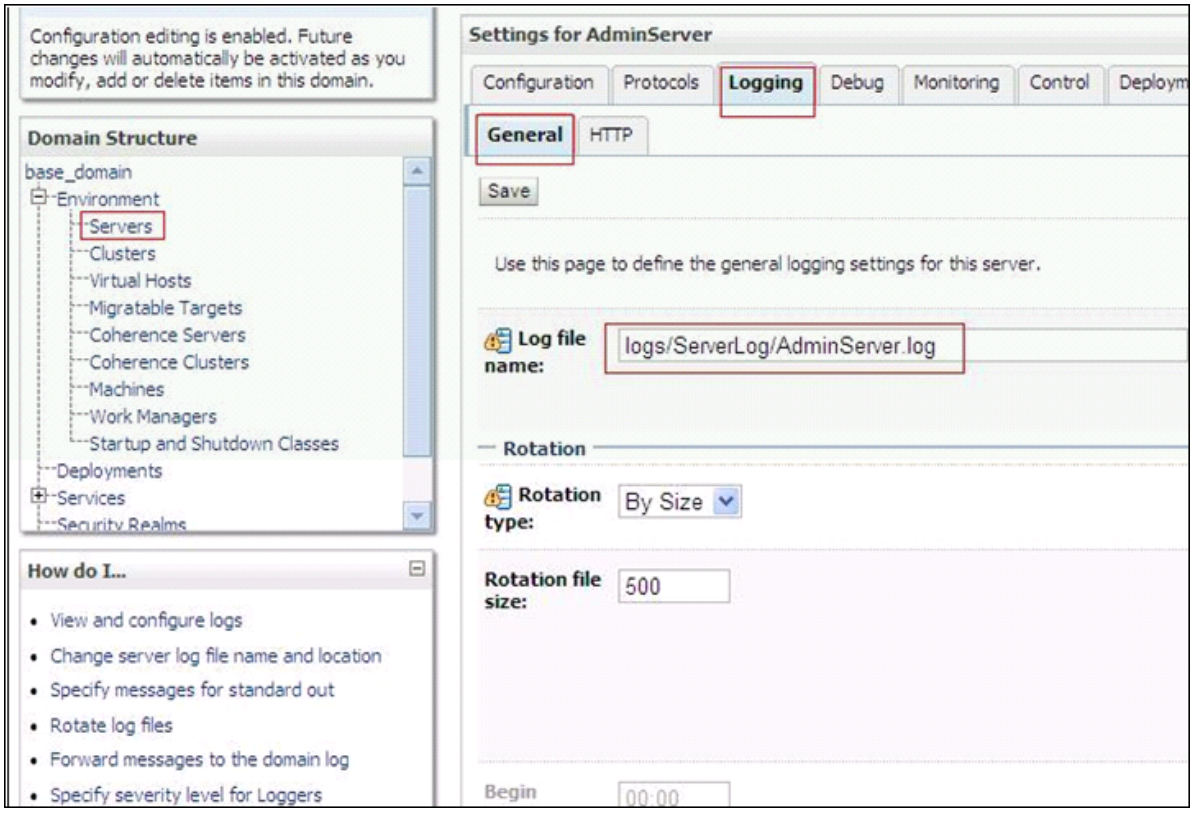
This connector supports event collection from server and access logs. The server log records information about events such as the startup and shutdown of servers, the deployment of new applications, or the failure of one or more subsystems. The messages include information about the time and date of the event as well as the ID of the user who initiated the event. The server log file is located on the computer that hosts the server instance. The HTTP subsystem keeps a log of all HTTP transactions. The default location and rotation policy for HTTP access logs is the same as the server log.

Configuration

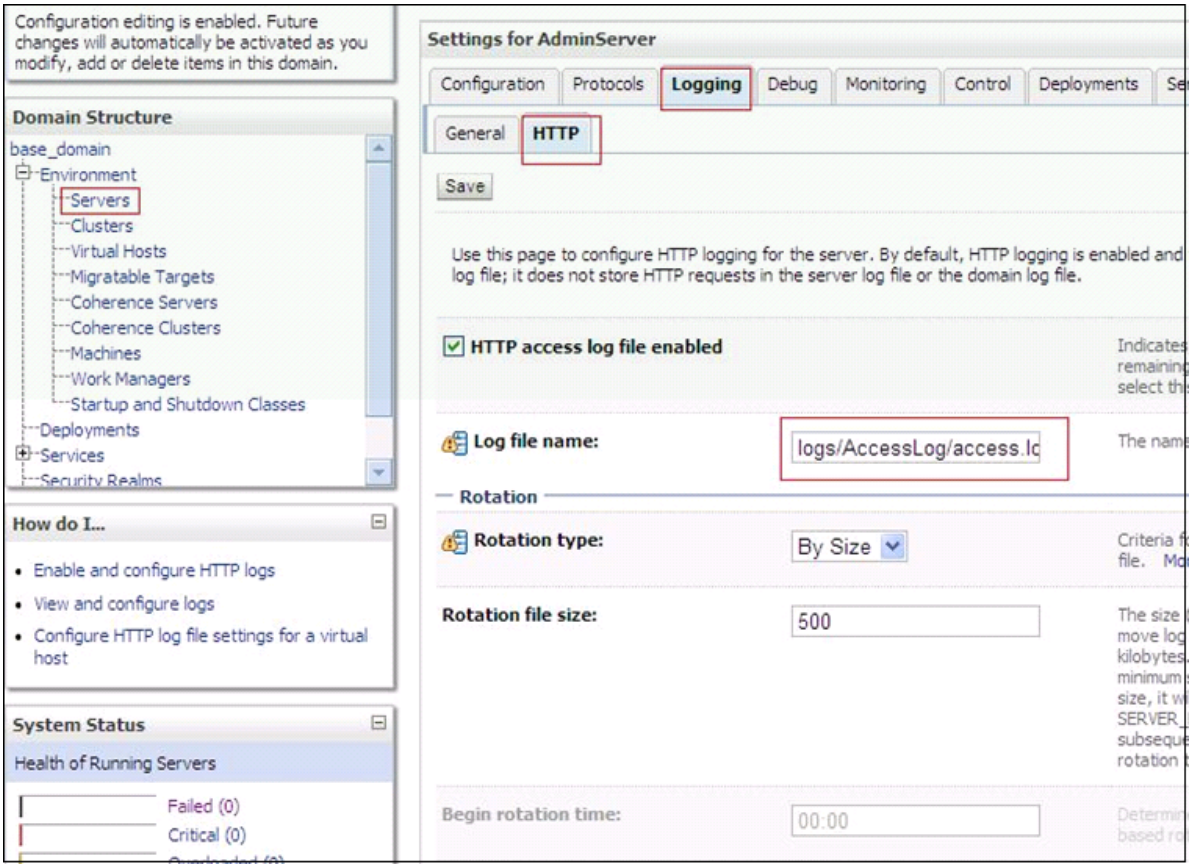
For complete information about WebLogic logging, see the Oracle WebLogic Server Administration Console Online Help. You can access the online help either through the Console itself, or online at http://download.oracle.com/docs/cd/E15523_01/apirefs.1111/e13952/core/index.html.

You must configure logging before installing the SmartConnector:

1. In the left pane of the Administration Console, click the name of the domain.
2. In the right pane, click the **Logging** tab and the **General** tab.
3. In the **Log file name** box, enter an absolute pathname or a pathname that is relative to the server's root directory and a file name.



4. Click **Save**.
5. Select the **HTTP** tab.
6. Enter the **Log file name** for the Access log; enter an absolute pathname or a pathname that is relative to the server's Access log directory. Make sure **HTTP access log file enabled** is selected.
   a.


Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.
Domain Structure
base_domain
Environment
Servers
Clusters
Virtual Hosts
Migratable Targets
Coherence Servers
Coherence Clusters
Machines
Work Managers
Startup and Shutdown Classes
Deployments
Services
Security Realms
How do I...
Enable and configure HTTP logs
View and configure logs
Configure HTTP log file settings for a virtual host
System Status
Health of Running Servers
Failed (0)
Critical (0)
Settings for AdminServer
Configuration
Protocols
Logging
Debug
Monitoring
Control
Deployments
General
HTTP
Save
Use this page to configure HTTP logging for the server. By default, HTTP logging is enabled and log file; it does not store HTTP requests in the server log file or the domain log file.
HTTP access log file enabled
Log file name:
logs/AccessLog/access.lo
Rotation
Rotation type:
By Size
Rotation file size:
500
Begin rotation time:
00:00

7. Click **Save**.

Installing the SmartConnector

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

Connector Appliance/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.

Preparing to Install 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.

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

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 WebLogic Server File** from the **Type** drop-down, then click **Next**.

   Specify the following parameters to configure the SmartConnector, then click **Next**:

Parameter	Description
Log Files Folder Name	Each WebLogic Server instance writes all messages from its subsystems and applications to a log file on its host machine. Enter the full path to the log file folder here; for example, <domain-name>/servers/<server_name>/logs/<server-name>.log
File Name Pattern	For the file name pattern, enter anything that matches files to be processed for real-time mode. For example, if the directory has 'exampleServer.log, exampleServer.log.1, ..., medServer.log, medServer.log1', you want to eliminate processed files (such as 'example.Server.log.1') and process real-time log files. Entering 'ex*.log' as the pattern would cause the example.Server.log to be read; 'med*.log' would cause the medServer.log to be read; '*Server.log' would cause the connector to read all log files with 'Server.log' as the last part of the file name.
Log Type	Select 'access' or 'server' as the log file type. If you have both access and server logs in the same folder, enter a separate line in the table for each log type.

5. Select a destination and configure parameters.
6. Specify a name for the connector.
7. 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.
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.

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.

WebLogic Access Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 400..599; Medium = 300..399; Low = 100..299
Application Protocol	httpVersion
Bytes Out	bytes
Destination User Id	authUser
Device Action	status
Device Event Class Id	status
Device Product	'WebLogic Server'
Device Receipt Time	date
Device Severity	status
Device Vendor	'Oracle'
Name	All ('Method: ',method,' Error Code:',status)
Request Method	method
Request Url	requestURI
Source Host Name	Host Name
Source User Name	RFC931

WebLogic Server Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector Severity)	High = Critical, Alert, Emergency; Medium = Error, Warning, Notice; Low = Info, Debug
Application Protocol	Protocol
Destination Host Name	machineName

ArcSight ESM Field	Device-Specific Field
Destination Port	Port
Destination Process Name	threadID
Destination Service Name	Service Name
Destination User Name	user
Device Custom IPv6 Address 2	Source IPv6 address
Device Custom String 1	SubSystem
Device Custom String 2	serverName
Device Event Class ID	One of (messageID, both (Prefix message, messageID))
Device Product	'WebLogic Server'
Device Receipt Time	Timestamp
Device Severity	severity
Device Vendor	'Oracle'
Device Version	WebLogic Server version
External ID	transactionID
File Name	File Name
File Path	File Path
Name	message
Source Address	Address

WebLogic Access v10.3.6 Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 400..599; Medium = 300..399; Low = 100..299
Bytes Out	bytes
Destination User Id	verintUserName
Device Action	status
Device CustomString3	timeTaken
Device CustomString3 Label	Time Taken
Device Event Class ID	status
Device Product	'WebLogic Server'

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	date
Device Severity	status
Device Vendor	'Oracle'
Name	All('Method: ',method,' Error Code:',status)
Request Method	method
Request Url	url
Source HostName	hostName

WebLogic Access v12.1.3 Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity High	400..599; Medium = 300..399; Low = 100..299
Application Protocol	x-Protocol
Bytes Out	bytes
Destination Address	One of (x-ClientIP,x-ForwardedFor)
Destination HostName	x-Host
Destination Port	x-Host
Destination User Name	x-AuthUser
Device Action	sc-status
Device Class ID	sc-status
Device CustomString2	x-AcceptLanguage
Device CustomString3	timeTaken
Device CustomString4	x-Scheme
Device CustomString5	x-Referer
Device Product	stringConstant("WebLogic Server")
Device Receipt Time	date
Device Severity	sc-status
Device Vendor	stringConstant("Oracle")
Name	All of("Method: ",cs-method," Error Code: ",sc-status)
Request Client Application	x-UserAgent

ArcSight ESM Field	Device-Specific Field
Request Method	cs-method
Request Url	cs-uri
Source Address	c-ip

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 WebLogic Server File SmartConnector (Micro Focus Security ArcSight Connectors 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!