Hewlett Packard
Enterprise

HPE Security
Fortify Runtime

Software Version: 17.3

Performance Tuning Guide

Document Release Date: April 2017
Software Release Date: April 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise Development 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. HPE 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. Valid license from HPE 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.

The software is restricted to use solely for the purpose of scanning software for security vulnerabilities that is (i) owned by you; (ii) for which you have a valid license to use; or (iii) with the explicit consent of the owner of the software to be scanned, and may not be used for any other purpose.

You shall not install or use the software on any third party or shared (hosted) server without explicit consent from the third party.

Copyright Notice

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.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

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.protect724.hpe.com/community/fortify/fortify-product-documentation

You will receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Contents

Preface

Contacting HPE Security Fortify Support

If you have questions or comments about using this product, contact HPE Security Fortify Technical Support using one of the following options.

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account

https://support.fortify.com

To Email Support

fortifytechsupport@hpe.com

To Call Support

1.844.260.7219

For More Information

For more information about HPE Security software products: http://www.hpe.com/software/fortify

About the Documentation Set

The HPE Security Fortify Software documentation set contains installation, user, and deployment guides for all HPE Security Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following HPE Security user community website:

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will need to register for an account.

Change Log

The following table lists changes made to this document. Revisions to this document are published only if the changes made affect product functionality.

Software Release / Document Version	Changes
17.3	Updated: Minor update 17.3; No significant content changes.
16.8	Updated: Minor update for 16.8 release; no significant content changes.
16.3	Updated: Minor update for 16.3 release; no significant content changes. HP to HPE rebranding.

Chapter 1: Introduction

This document recommends ways to address performance bottlenecks you may encounter in HPE Security Fortify Runtime Agent. It is meant to supplement, not replace, the HPE Security Fortify Runtime Installation and Configuration guides.

Intended Audience

The audience for this guide is someone that is familiar with HPE Security Fortify Runtime. It assumes you are able to correctly install and run HPE Security Fortify Runtime agents.

Related Documents

This topic describes documents that provide information about HPE Security Fortify Runtime.

Note: The Protect724 site location is https://www.protect724.hpe.com/community/fortify/fortify-product-documentation.

All Products

The following documents provide general information for all products.

Document / File Name	Description	Location
HPE Security Fortify Software System Requirements HPE_Sys_Reqs_<*version*>.pdf	This document provides the details about the environments and products supported for this version of HPE Security Fortify Software.	Included with product download and on the Protect724 site
HPE Security Fortify Software Release Notes HPE_FortifySW_RN_<*version*>.txt	This document provides an overview of the changes made to HPE Security Fortify Software for this release and important information not included elsewhere in the product documentation.	Included on the Protect724 site
What's New in HPE Security	This document describes the	Included on the Protect724 site

Document / File Name	Description	Location
Fortify Software <version> HPE_Whats_New_<*version*>.pdf	new features in HPE Security Fortify Software products.	
HPE Security Fortify Open Source and Third-Party License Agreements HPE_OpenSrc_<*version*>.pdf	This document provides open source and third-party software license agreements for software components used in HPE Security Fortify Software.	Included with product download and on the Protect724 site
HPE Security Fortify Glossary HPE_Glossary.pdf	This document provides definitions for HPE Security Fortify Software terms.	Included with product download and on the Protect724 site

HPE Security Fortify Runtime

The following documents provide information about Fortify Runtime.

Document / File Name	Description	Location
HPE Security Fortify Runtime .NET Edition Designer Guide HPE_RT_DotNet_Design_Guide_<*version*>.pdf PDF only; no help file	This document provides information to aid in the configuration and customization of Fortify Runtime for a given application that operates on a .NET platform. The audience for this guide includes an HPE Security Fortify Runtime Solution Designer who often creates event handlers and chooses values for settings, sometimes writes rules, and occasionally creates a monitor. The HPE Security Fortify Runtime Solution Designer must understand both software and security.	Included with product download and on the Protect724 site

Document / File Name	Description	Location
HPE Security Fortify Runtime Java Edition Designer Guide HPE_RT_Java_Design_Guide_<*version*>.pdf PDF only; no help file	This document provides information to aid users in the configuration and customization of Fortify Runtime for a given application that operates on a Java platform. The audience for this guide includes HPE Security Fortify Runtime Solution Designers who often create event handlers and choose values for settings, sometimes write rules, and occasionally create a monitor. The Fortify Runtime Solution Designer must understand both software and security.	Included with product download and on the Protect724 site
HPE Security Fortify Runtime Application Protection (RTAP) .NET Installation Guide HPE_RTAP_DotNet_Install_<*version*>.pdf HPE_RTAP_DotNet_Install_Help_<*version*>	This document describes how to install the Fortify Runtime Agent for applications running under a supported .NET Framework on a supported version of IIS.	Included with product download and on the Protect724 site
HPE Security ArcSight Application View Runtime Agent Installation Guide HPE_AppView_RT_Agent_Install_<*version*>.pdf HPE_AppView_RT_Agent_Install_Help_<*version*>	This document describes how to install the Fortify Runtime Agent for applications running under a supported Java Runtime Environment (JRE) on a supported application server or service and applications running under a supported .NET Framework on a supported version of IIS.	Included with product download and on the Protect724 site
HPE Security Fortify Runtime Application Protection	This document provides information and procedures	Included with product download and on the

Document / File Name	Description	Location
Operator Guide HPE_RTAP_Oper_Guide_<*version*>.pdf HPE_RTAP_Oper_Help_<*version*>	that enable you to run and monitor the operation of HPE Security Fortify Runtime Application Protection.	Protect724 site
HPE Security ArcSight Application View Quick Start HPE_AppView_Quick_Start_<*version*>.pdf PDF only; no help file	This document provides brief instructions about how to get started with installing and configuring HPE Security ArcSight Application View.	Included with product download and on the Protect724 site
HPE Security Fortify RTAP Rulepack Kit Guide HPE_RTAP_Rulepack_Kit_<*version*>.pdf PDF only; no help file	This document describes the detection capabilities of HPE Security Fortify Runtime Application Protection (RTAP) and the HPE Security Fortify RTAP Rulepacks. Each category of attack, vulnerability, or audit event detected by RTAP is described in this document.	Included with product download and on the Protect724 site
HPE Security Fortify RTAL Rulepack Kit Guide HPE_RTAL_Rulepack_Kit_<*version*>.pdf PDF only; no help file	This document describes the capabilities of the HPE Security Fortify Runtime Application Logging (RTAL) Rulepack Kit. The HPE Security Fortify RTAL Rulepack is a special Runtime Kit for HPE Security Fortify Runtime. It provides information about web application internal activities to ArcSight analysis servers so that these events can be correlated with other existing ArcSight event information.	Included with product download and on the Protect724 site
HPE Security Fortify Runtime	This document recommends	Included with product

Document / File Name	Description	Location
Performance Tuning Guide HPE_RT_Perf_Tuning_<*version*>.pdf PDF only; no help file	ways to address performance bottlenecks a user might encounter in HPE Security Fortify Runtime. It is meant to supplement, not replace, the HPE Fortify Runtime Installation and Configuration guides. It is intended for users who are familiar with and can correctly install and run HPE Security Fortify Runtime.	download and on the Protect724 site

Chapter 2: Overview of Fortify Runtime Performance Tuning

This section contains the following topics:

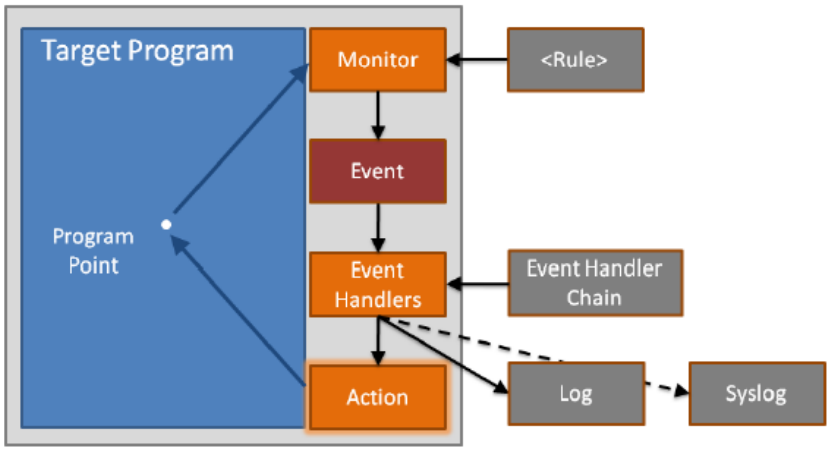
Overview of Runtime for Java Components

Specific recommendations are given for the following HPE Security Fortify Runtime solutions at the end of this document.

- Runtime Application Protection (RTAP)
- Runtime Application Logging (RTAL), the default HPE Security Fortify Runtime installation that comes with HPE Security ArcSight Application View

Introduction to Event Dispatching

The following figure shows the relationship of HPE Security Fortify Runtime components and illustrates an operational overview for HPE Security Fortify Runtime Event dispatching.



- When the target program executes a monitored Program Point (a method), the predefined Monitor is invoked.
- If the Monitor finds what it is looking for, it creates an Event.
- The Event is then passed to the Event Handler Chain as configured in `rt_config.xml`.
- When an Event Handler matches, it can dispatch the Event to a log file or to a network service.

Therefore, any of the following can cause performance issues:

- A Program Point has been executed too many times. The monitor must perform a non-trivial task even if no Event is generated.
- Too many Events have been generated. Event generation requires some thread synchronization and data copying and consumes some CPU cycles even if it is dropped immediately after being created.
- With the exception of `EventFilters`, Event Handler Chain operations usually involve simple string comparisons only and should not be performance sensitive.
- Writing Events to `event.log` and `syslog` are handled by a daemon thread. However, other actions may consume CPU cycles of the application thread.

Disabling Monitors that Generate Too Many Events

Dropping an unwanted Event is not the best way to improve performance because HPE Security Fortify Runtime must still monitor the Program Point, generate the Event, and go through the Event Handler Chain.

The best way to ignore unwanted Events is to disable the corresponding rule. This is done by adding the `<DisableRules>` block shown below to your `rt_config.xml` under the `<Rules>` section.

Example: Writing an Event

```
<DisableRules>
<MatchAttribute name="category">[Category Name Here]</MatchAttribute>
</DisableRules>
```

If you just want to disable a particular rule (for example, a particular type of SQL Injection), you can disable by rule ID or monitor ID as shown in the following example.

Example: Disable a rule

```
<DisableRules>
<MatchAttribute name="ruleID">[ruleID Here]</MatchAttribute>
</DisableRules>
<DisableRules>
<MatchAttribute name="monitorID">[monitorID Here]</MatchAttribute>
</DisableRules
```

Note:

- Each category usually consists of one or multiple rules and each rule may consist of one or multiple monitors.
- The XML tag is called DisableRules, but for <MatchAttribute name="monitorID">, only the matched monitor is disabled.

Enabling the Diagnostic Log

The diagnostic log is a powerful tool that enables you to easily and quickly locate the performance bottlenecks in an HPE Security Fortify Runtime Agent. The HPE Security Fortify Runtime agent dumps monitor counters and timers in the diagnostic log when it is enabled. To enable the diagnostic log, set `Diagnostics_Enabled` to `true` in `rt_config.xml` under the `<GlobalSettings>` section. Optionally, you may set the `Diagnostics_LogFile` to direct the diagnostic log to another file location. The default diagnostic log file path is `${FortifyHome}/log/diagnostic.log`.

Note: For .NET, notice `diagnostic1.log`, `diagnostic2.log`, and so forth, for each website processes.

Example: Diagnostic log settings

```
<Setting name="Diagnostics_Enabled">true</Setting>
<Setting name="Diagnostics_LogFile">C:/Log/diagnostic.log</Setting>
```

Add a typical diagnostic log as follows.

Example: Adding a diagnostic log

```
---2013-11-19T09:55:32.149+0800 (14168) ---
-- Timers --
ClassTransformer: 00:02.602
ConfigLoader: 00:25.316
LogDispatcher: 00:00.113
Monitor.04EF5931-35F0-42AD-A400-BD53198C876B: 00:00.017
Monitor.0A1BE2AC-BB30-4358-9065-7E25C91F18DF: 00:00.000
Monitor.0A5C02D1-44D8-4E4B-94A2-8D456808EF5A: 00:00.006
Monitor.0CE413FC-84B7-4CFE-9D1E-B84FE6F26512: 00:00.003
Monitor.12F00E3C-B936-467E-AC2D-BD2314B9F991: 00:00.000
…
…
-- Counters --
CreateEvent: 12
Monitor.04EF5931-35F0-42AD-A400-BD53198C876B: 1,486
Monitor.0A1BE2AC-BB30-4358-9065-7E25C91F18DF: 6
```

```
Monitor.0A5C02D1-44D8-4E4B-94A2-8D456808EF5A: 483
Monitor.0CE413FC-84B7-4CFE-9D1E-B84FE6F26512: 354
…
…
```

The HPE Security Fortify Runtime platform dumps the timers and counters to `diagnostic.log` every 30 seconds. Usually, you must pay attention to the last output block. Most items are self-explanatory: Monitors are in the format of `Monitor.<monitorID>`; while others are platform internal Events. Timer times are in seconds and counters are the number of executions regardless of whether an Event is generated or not.

A utility program is provided which can add extra monitor descriptions right next to the monitor IDs. To use this utility, simply run the following command.

Example: Diagnostic log utility

```
# java -jar DiagnosticLogMarker.jar < diagnostics.log
```

A typical output of `DiagnosticLogMarker` is as follows.

Example: DiagnosticLogMarker output

```
 ---2013-11-19T09:55:32.149+0800 (14168) ---
-- Timers --
ClassTransformer: 00:02.602
ConfigLoader: 00:25.316
LogDispatcher: 00:00.113
Monitor.04EF5931-35F0-42AD-A400-BD53198C876B[Javascript Hijacking]:
00:00.017
Monitor.0A1BE2AC-BB30-4358-9065-7E25C91F18DF[SQL Injection]: 00:00.000
Monitor.0A5C02D1-44D8-4E4B-94A2-8D456808EF5A[System Information Leak]:
00:00.006
Monitor.0CE413FC-84B7-4CFE-9D1E-B84FE6F26512[Method Call Failure]:
00:00.003
Monitor.12F00E3C-B936-467E-AC2D-BD2314B9F991[AppServerTypeMonitor]:
00:00.000
…
…
-- Counters --
CreateEvent: 12
Monitor.04EF5931-35F0-42AD-A400-BD53198C876B[Javascript Hijacking]: 1,486
Monitor.0A1BE2AC-BB30-4358-9065-7E25C91F18DF[SQL Injection]: 6
Monitor.0A5C02D1-44D8-4E4B-94A2-8D456808EF5A[System Information Leak]: 483
Monitor.0CE413FC-84B7-4CFE-9D1E-B84FE6F26512[Method Call Failure]: 354
…
```

```
...
```

By using the diagnostic log, you are able to discover which monitor(s) used most of the CPU times or executed too many times. You may then try to disable the corresponding monitor and re-run performance test.

Note:

- The first two items in the `Timers` section, that is, `ClassTransformer` and `ConfigLoader` are startup Events and only affect the startup time.
- The third item in the `Timers` section, that is, `LogDispatcher` is the time used to write the Event to `event.log`. This is done in a daemon thread.

Runtime Application Protection (RTAP) Specific Tuning

The following categories may cause performance issues in some applications. Disable the rule(s) if they cause performance issues in your application.

- **Insecure Randomness** - By default, rules transform insecure random numbers into secure random numbers. Although the operation does not require a great number of CPU cycles, transforming too many insecure random numbers will cause a significant degradation in performance.
- **Method Call Failure** - It has been reported that some MySQL driver versions throw an SQLException on almost every transaction. This rule is an informational rule. It is safe to disable this rule, if necessary.

Runtime Application Logging (RTAL) Specific Tuning

For Unified Logging, setting a log level to `DEBUG` or equivalent generates a large number of Events. The default level is `WARN`. It is not recommended that you set log level lower than INFO.

File Read/Write/Delete/Create trace can generate many Events. While the configuration parameter `FileTraceExclusion` supports the syntax of `%{ContextPath}`, exclude using absolute path is relatively faster and is recommended.

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 Performance Tuning Guide (HPE Security Fortify Runtime 17.3)

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 HPFortifyTechpubs@hpe.com.

We appreciate your feedback!