Performance Management Advisors Deployment Guide

Configure Administrative Actions Logs

5/5/2025

Contents

Configure Administrative Actions Logs

All administration actions carried out in the Pulse Advisors environment are logged. The following sections give information about how to configure the logging. See also Adjust the Log File Roll and Retention Settings.

Modules for which Actions are Logged

The following modules have administrative logging available:

- Advisors administration for Contact Center Advisor and Workforce Advisor
- Advisors Genesys Adapter

You can find logs related to administrative changes in the `AdministrationAudit.log` file. The file records changes to configuration and metrics such as creating/deleting metrics and other configuration changes.

Modules for which Actions are Not Logged

Administrative actions are not logged for the following modules:

- Configuration Server, for actions on objects that are used by Contact Center Advisor and Workforce Advisor
- Frontline Advisor administration
- Resource Management administration

Actions Not Logged by This Functionality

The administrative actions logging functionality does not capture changes made to contact groups when the contact groups are imported from a WFM system.

Information Logged

The following information is logged for each action:

- A timestamp of when the action's data was saved in the format specified by the log configuration properties. For additional information, see Configuring the Audit Logs on this page.

- The username of the user who performed the action.
- The properties or relationships of the object that are being changed by the action, showing their values both before and after the action.
- Whether the action succeeded or not.

Configuring the Audit Logs

The audit logs are in a file called:

- `AdministrationAudit.log` (Release 9.0.000)
- `advisors-admin-audit.log` (Release 9.0.001+)

The file is written to the following directory by default:

- `<advisors>\apache-tomcat-<version>\logs` (Release 9.0.000)
- On Windows: `c:\genesys\log\advisors\platform\` (Release 9.0.001+)
- On Linux: `/mnt/log/advisors/platform/` (Release 9.0.001+)

You can configure the audit log using the `log4j` properties in the `log4j.properties` file, which is located in the following directory:
`Advisors\conf`

Sample log4j Appender

The following information is the definition of the appender that configures the audit logs:

```
log4j.appender.ADMINISTRATIONAUDIT.append=true
# For 9.0.000
log4j.appender.ADMINISTRATIONAUDIT.file=${catalina.base}/var/log/
AdministrationAudit.log
# For 9.0.001+
log4j.appender.ADMINISTRATIONAUDIT.file=${advisors.logs.dir}/advisors-admin-audit.log

log4j.appender.ADMINISTRATIONAUDIT.threshold=INFO

log4j.appender.ADMINISTRATIONAUDIT.datePattern=yyyy-MM-dd
# For 9.0.000
log4j.appender.ADMINISTRATIONAUDIT.suffixPattern='.'yyyy-MM-dd_HH-mm-ss'.log'
# For 9.0.001+
log4j.appender.ADMINISTRATIONAUDIT.suffixPattern='.'yyyy-MM-dd'T'HHmmss'.log'
log4j.appender.ADMINISTRATIONAUDIT.maxFileSize=10MB

log4j.appender.ADMINISTRATIONAUDIT.maxRollFileCount=10

log4j.appender.ADMINISTRATIONAUDIT.scavengeInterval=600000
```

```
log4j.appender.ADMINISTRATIONAUDIT.layout=com.informiam.platform.core.logging.StdHeaderPatternLa

log4j.appender.ADMINISTRATIONAUDIT.layout.ConversionPattern=%d{ISO8601} %t %-5p
[%c{1}] %m%n

log4j.appender.ADMINISTRATIONAUDIT.layout.ComponentName=Administration Audit

log4j.appender.ADMINISTRATIONAUDIT.layout.VersionNumber=@platform.version@
```

The appender ensures the log file names indicate the day on which they were written. If more than one file is written per day, then the name also indicates the order in which the file was produced on that day. For example, in release 9.0.000:

```
AdministrationAudit.log

AdministrationAudit.log.2011-12-01.1

AdministrationAudit.log.2011-12-01.2

AdministrationAudit.log.2011-11-31.1

AdministrationAudit.log.2011-11-31.2
```

Definitions

- `MaxFileSize of 10 MB`—Indicates that the largest size of any individual log file is 10 MB.
- `MaxBackupIndexOf3`—Indicates that on any day, a maximum of three files will be written. If more than that are actually produced, the oldest ones will be deleted.