TIBCO® Operational Intelligence Hawk® RedTail

Release Notes

Version 7.3.0 | November 2024

Contents

New Features

The following features have been added since the last major release of TIBCO® Operational Intelligence Hawk® RedTail.

Version 7.3.0

- Added RHEL 8 and RHEL 9 support for Enterprise Installation.

- The following metrics have been added to the Hawk Console:

    - `TS_hawk_hkc_jvm_memory_total_used`

    - `TS_hawk_hkc_jvm_memory_heap_used`

    - `TS_hawk_hkc_jvm_memory_heap_usage`

    - `TS_hawk_hkc_jvm_memory_heap_max`

    - `TS_hawk_hkc_jvm_cpu_usage`

    - `TS_hawk_hkc_microagent_state`

    - `TS_hawk_hkc_microagents_total`

- The exposed Hawk Metrics can be used to monitor the number of applications at a given point.

    The Microagent metric is in the below format: `hawk_hkc_microagents_total {instance="hawkconsolenode:9687", job="redtailmetrics", tag_name="self"}`. The scenarios and outcome are shown below:

    - If a tag is newly created and no microagent is matched then the value is 0.

    - If the microagent is newly connected and is matched to the tag then the value is changed to 1. And when another microagent is connected and matched to the tag then the value is incremented by 1.

    - If the microagent is disconnected and matched to the tag, then the value is decremented by 1.

    - If the tag name is updated, then the value is changed to -1.

- If the tag is deleted, then the value is changed to -1.

- The Microagent state metric is in the given format :

```
hawk_hkc_microagent_state{display_name="Self", hk_agent_domain_
name="redtail", hk_agent_host_name="f2656bfde894", hk_agent_
ip="172.24.0.10", hk_agent_name="f2656bfde894", hk_agent_os_name="Linux",
hk_agent_os_version="5.15.49-linuxkit-pr", hk_microagent_instance="0",
instance="hawkconsolenode:9687", job="redtailmetrics",
name="COM.TIBCO.hawk.microagent.Self", tag_name="self"}
```

The values are: 1 is Running, 0 is Stopped.

- The default dashboard is shown based on the deployment Container Edition (Kubernetes) or on-premises.

Version 7.2.2

- **HawkKubernetesMA:onPodStatusChange:** This method has been introduced to monitor the life cycle of a Kubernetes pod. For more information, see *TIBCO® Operational Intelligence Hawk® RedTail Microagent Reference*.

Version 7.2.1

No new feature have been added in this release of TIBCO® OI Hawk® RedTail.

Version 7.2.0

- **Enterprise Deployment for TIBCO OI Hawk RedTail:** You can now deploy and run TIBCO OI Hawk RedTail components on Linux physical/virtual machines. Based on your requirements, you can deploy TIBCO OI Hawk RedTail components as a standalone deployment or in a High Availability (HA) deployment. For more information, see *TIBCO® Operational Intelligence Hawk® RedTail Installation, Configuration, and Administration Enterprise Edition*.

- **Grafana**: Starting from this release you can use external Grafana with TIBCO OI Hawk RedTail. For more information, see "Connecting an External Grafana Server to TIBCO OI Hawk RedTail" in *TIBCO® Operational Intelligence Hawk® RedTail Installation, Configuration, and Administration*.

- **Infra Queries**: The `USE OI_Config_Nodes` and `USE OI_Config_Machines` infra queries are introduced to get the node and components status in TIBCO OI Hawk RedTail.

- **EQL:** The following new functions are introduced in EQL:

- **topk:** This function returns the largest k elements by sample value.

- **bottomk:** This function returns the smallest k elements by sample value.

Version 7.1.0

- **gRPC Transport:** With the introduction of gRPC transport, a single Hawk RedTail Console can be used to communicate with agents and domains on different platforms. This enables TIBCO OI Hawk RedTail to seamlessly monitor and manage applications and infrastructure on hybrid deployments such as on-premises environments and private clouds.

- **Support for Multiple Domains and Agents:** TIBCO OI Hawk RedTail can now simultaneously configure, monitor, and manage multiple cross-platform domains and agents.

- **Integration with TIBCO® Operational Intelligence Agent:** You can further enhance the log collection and forwarding capabilities of TIBCO® Operational Intelligence Hawk® RedTail - Standard Edition with the TIBCO® Operational Intelligence Agent license. This includes log collection from various log sources such as Windows events, real-time files, remote files, syslog, and command-line output. You can also configure TCP Syslog and ULDP syslog forwarders. For more information, see *TIBCO® Operational Intelligence Hawk® RedTail User Guide*.

- **Relabel Configuration for Hawk Metrics Exporter:** You can now specify the relabel configurations for Hawk Metrics Exporters. This provides better flexibility for identifying metrics for collection.

- **Secured Zookeeper Communication:** The TIBCO OI Hawk RedTail now communicates with the Apache ZooKeeper over a mutually authenticated TLS channel.

- **Clear Action:** A clear action is an action that takes place only when a test makes the transition from `true` to `false`. When defining a test condition, you can now configure a clear action for a test condition in a rulebase by using the **Advanced Options**.

- **Bloks for faster querying:** To analyze your data faster, you can create different types of Bloks in TIBCO OI Hawk RedTail and accelerate the search process. A Blok is a contextual element or filter that fits with other elements to form a search query. Bloks are reusable elements of a query. You can combine many types of Bloks together to create complex queries. For more information, see *TIBCO® Operational Intelligence Hawk® RedTail User Guide*.

- **Configuration of Database Schema:** The database schema for OI Hawk Console is now externalized. This allows you to make minor modifications to the table schema such as changing the column size.

Version 7.0.0

- **Collect and Store Metrics:** The system uses Hawk Console as an exporter to collect metrics from various Hawk microagents and external metric sources, and stores them as time series metrics in the time-series database.

- **Customizable Dashboards:** It enables you to visualize the time series metrics as line charts, tables, and gauges using multiple dashboards. You can customize the panels of those dashboards and also configure multiple queries.

- **Unified Query Language:** TIBCO OI Hawk RedTail provides Operational Intelligence Query Language to query the stored time series metrics or Hawk microagent method data in the form of data models. You can run the queries via a sophisticated search UI or programmatically using the REST API.

- **Tag-Based Rulebases:** Create high-level rulebases with tags that can match microagents. With this feature, rulebases can be automatically deployed to all the relevant Hawk agents in the domain.

- **Content Pack:** The content packs provide an out-of-the-box view, which can be product or environment specific. It is a curated collection of monitoring and visualization resources that include data models (metrics), rulebases, and dashboards. For example, the Integration content pack has out of the box resources to monitor the integration environments such as BusinessWorks applications, Kafka, or Kubernetes.

- **Integration with TIBCO LogLogic® Log Management Intelligence:** TIBCO OI Hawk RedTail is a collection of microservices monitoring different assets in the clusters. It collects logs from these clusters and then forwards these logs to LogLogic® Log Management Intelligence (LMI). Once these logs are forwarded to LogLogic® LMI, the user can configure LogLogic LMI remotely and perform search operations on these logs from TIBCO OI Hawk RedTail. Moreover, the user can also use the Grafana data source "LogLogic" to display the logs from remote LogLogic LMI on the dashboard panels.

- **Administration:** Administration enables role-based access control in TIBCO OI Hawk RedTail by granting and revoking privileges to content packs. The administrator can

define roles, set up users, and give them access to resources so that operations can be conducted in a reliable and secure manner.

- **LDAP configuration via UI:** You can now configure remote LDAP authentication using the UI or REST API. (This feature is available with all types of licenses.)

- **Kubernetes Microagent:** If you have deployed TIBCO OI Hawk RedTail on Kubernetes, you can use the Kubernetes microagent methods to get information about the Kubernetes Cluster. (This feature is available with all types of licenses.)

- **Hawk Alerts:** Starting from this release, MySQL Database is used for storing alerts in TIBCO OI Hawk RedTail. This ensures that the alerts are not lost when the Hawk Console restarts or shuts down abruptly. (This feature is available with all types of licenses.)

Changes in Functionality

The following functionality and features have been changed in this release of TIBCO®
Operational Intelligence Hawk® RedTail.

- Enable selection of home dashboard for a Content Pack.

  The overview dashboard is available as the default homepage view in any **Content
  Pack**. The user can customize this view once the **Content Pack** is created. Optionally,
  the user can come back to the and update the **Content Pack** to select the default
  dashboard.

- In the previous version, Hawk Exporters can be created only on hawk methods that
  have at least one numeric value. To use the methods without any numeric column,
  Hawk Console now supports Hawk Exporters on methods with string columns only.

  Now, the data models with `hkinfo` post-fix are created and scraped in the
  Prometheus so that data can be used to fetch the details. The value for the metric
  should be fixed to 1. The sample data model name is given below:

  `hawk_Self_getcomponentinfo_hkinfo`

- The existing Exporter label names are updated with hk_ prefix as shown in the
  following table:

Current Label	Updated Label
agent_name	hk_agent_name
agent_ip	hk_agent_ip
microagent_name	hk_microagent_name
microagent_display_name	hk_microagent_display_name

  The newly added labels are `hk_agent_domain_name`, `hk_agent_os_name`, `hk_agent_os_version`, `hk_agent_host_name`, and `hk_microagent_instance`.

Deprecated Features

The following features have been deprecated as of this release of TIBCO® Operational Intelligence Hawk® RedTail.

Affected Component	Description	Deprecated Release
TCP Transport for TIBCO Hawk Transport	The TCP Transport for TIBCO Hawk Transport has been deprecated as of this release.	7.2.2

Removed Features

The following features have been removed as of this release of TIBCO® Operational Intelligence Hawk® RedTail.

Affected Component	Description	Deprecated Release	Removed Releases
Proxy Domain	The proxy domain functionality has been removed as of this release.	7.2.2	7.3.0
UniversalCollector microagent	The UniversalCollector microagent has been removed as of this release.	7.2.2	7.3.0
License	The TIBCO Operational Agent license type has been removed as of this release.		7.3.0
All data tables on Web UI	The ability to show/hide selective columns on all data tables in Web UI has been removed.		7.3.0
Administration Users and Roles	The ability to duplicate User and Role.		7.3.0

Migration and Compatibility

The following information provides migration procedures and a compatibility matrix for this release of TIBCO® Operational Intelligence Hawk® RedTail.

Changes in OpenSSL 3.0

As part of strengthening security, recent versions of TIBCO® Messaging products including TIBCO Enterprise Message Service, TIBCO FTL/eFTL, and TIBCO Rendezvous have transitioned from OpenSSL 1.1.1 to OpenSSL 3.0. To encrypt/decrypt `PKCS#12` files (in a way that is supported by OpenSSL 3.0), TIBCO OI Hawk RedTail instances must run with the following minimum versions of Java: 8u301 (Oracle), 8u342 (OpenJDK), 11.0.12, or any 17.x build (or later).

Java 17 Update for TIBCO OI Hawk RedTail

Starting from this release, Java 17.0.11 is supported for all TIBCO OI Hawk RedTail components. For information about the platforms, see the *Readme*.

- The TIBCO OI Hawk RedTail Agent is compatible with Java 8 and Java 11.

- The Legacy Hawk Console is compatible only with Java 17.

Migrating from TIBCO® Operational Intelligence Hawk® RedTail - Enterprise Edition 7.2.x

Perform the following steps before installing TIBCO OI Hawk RedTail 7.3.0 to retain the configurations of version 7.2.x if you have installed the 7.2.x agent component:

1. Navigate to *CONFIG_FOLDER*.

2. Take a backup of the autoconfig folder.

3. Take a backup of the configuration files (`.cfg, .tra` files).

4. Once the installation of TIBCO OI Hawk RedTail 7.3.0 is complete, copy the backed-up `autoconfig` folder and the configuration files in the newly installed *CONFIG_FOLDER*.

5. Excute the below command to migrate 7.2.x to 7.2.2.

```
sudo ./install.sh upgrade
```

> ℹ **Note:** Once you run the `install.sh` script with the `upgrade` option, the installer shuts down existing running services, and then upgrades the binaries while also ensuring that no data is lost.

Migrating from TIBCO® Operational Intelligence Hawk® RedTail - Container Edition 7.2.x

Postgres Data Migration

Due to changes in the base image used for Postgres in Redtail version 7.2.2, any Postgres data from previous Redtail versions will need to be manually migrated. Please contact TIBCO Support for assistance in your particular installation.

> ℹ **Note:** Take the backup of existing yaml files before migration

Procedure

1. Build all the images postinstallation. For more information, see the *Building Docker Images for TIBCO OI Hawk RedTail* section in the *TIBCO® Operational Intelligence Hawk® RedTail Installation, Configuration, and Administration Container Edition*.

   > ℹ **Note:** The newly built images will have the tag as 7.3.0.

2. (Optional) You can also build the images while reusing the previously built self-signed certificates. For more information, see *TIBCO® Operational Intelligence Hawk® RedTail Installation, Configuration, and Administration Container Edition*.

3. All TIBCO OI Hawk RedTail Kubernetes YAML files are updated with the image tag 7.3.0. `redtail_prometheus.yaml` and `redtail_db.yaml` have been updated. Update your existing TIBCO OI Hawk RedTail Kubernetes YAML's in production with all the changes in 7.3.0 sample Kubernetes YAML.

4. Upgrade your existing cluster with the newly created images.

Migrating from TIBCO® Operational Intelligence Hawk® RedTail - Container Edition 7.1.0

> ℹ **Note:** You cannot migrate your data from the version 7.1.0 to the enterprise edition of TIBCO OI Hawk RedTail.

Procedure

1. Take a backup by exporting the existing configurations (such as tag-based rulebases, metrics exporters, content packs, dashboards.) You can import these exported configurations after TIBCO OI Hawk RedTail 7.3.0 has been deployed. For more information about exporting configurations, see *TIBCO® Operational Intelligence Hawk® RedTail User Guide*.

2. (Optional) To deploy TIBCO OI Hawk RedTail 7.3.0 with existing persistent volumes, you need not take a backup of the existing configurations as the existing configurations are preserved.

Migrating from MySQL to PostgreSQL

> ℹ **Note:** You can perform this action only when you are migrating your data from version 7.0.0 or 7.0.1.

Before you begin

- Ensure that you can access the MySQL server.
- Ensure that you have not initialized the PostgreSQL server.

Procedure

1. Specify the following environment variables for the PostgreSQL deployment configuration:

Environment Variable	Description
MYSQL_MIGRATION_SERVER_HOST_PORT	Host name and port of the MySQL server from where the data is to be migrated

Environment Variable	Description
	Default Value: `mysqldbnode:3306`
`MYSQL_MIGRATION_SERVER_ PASSWORD`	MySQL server root user's password from where the data is to be migrated
	Default Value: `mypassword`

Migration Considerations

- You must manually assign the imported prometheus exporters to an agent and a domain by editing the exporter's configuration.

- The location of the certificates generated from the `build-all.sh` script has been changed as specified:

  — **Old location:** *TIBCO_HOME*/hawk/7.1/redtail/docker/build-images/build-context/loglogic/conf/certs

  — **New location:** TIBCO_HOME/hawk/7.2/redtail/docker/build-images/build-context/redtail/conf/certs

  > ℹ **Note:** The certificates generated when creating the image are placed at `/redtail/conf/certs` in the container images.

- You must manually upload the rulebases to the rulebase repository of TIBCO OI Hawk RedTail 7.3.0 using the UI.

Migrating from TIBCO Hawk® - Container Edition 2.0.0

Migrating from TIBCO Hawk® - Container Edition 2.0.0 to TIBCO OI Hawk RedTail 7.3.0 involves the following main tasks:

- Creating new container images for TIBCO OI Hawk RedTail 7.3.0

- Re-creating the deployment with the new container images

- Reconfiguring the stored data such as the rulebase repository

Here are the configuration recommendations:

1. Build the docker images for the TIBCO OI Hawk RedTail 7.3.0 components by using

the build script. For details, see the "Building Docker Images for TIBCO OI Hawk RedTail Components" in *TIBCO® Operational Intelligence Hawk® RedTail Installation, Configuration, and Administration*.

2. Go over the list of container paths and environment variables for TIBCO OI Hawk RedTail 7.3.0. The container paths and environment variables for the version 7.3.0 are different compared with Hawk® - Container Edition 2.0.0. For the complete list of configurations, see the "Environment Variables for TIBCO OI Hawk RedTail Components" in *TIBCO® Operational Intelligence Hawk® RedTail Installation, Configuration, and Administration*.

3. Export the rulebases residing in TIBCO Hawk Container Edition 2.0.0 to TIBCO OI Hawk RedTail 7.3.0 by uploading the rulebases to the rulebase repository from the UI.

> **ⓘ** **Note:** The rulebase repository storage has been moved from file-based structure to database.

4. Configure the volumes for TIBCO OI Hawk RedTail 7.3.0 components.

Compatibility

- Ensure that the associated or dependent products that you use with TIBCO OI Hawk RedTail 7.3.0 such as TIBCO Runtime Agent, TIBCO Administrator™, and various platform microagents are compatible.

- The following microagents are not compatible with the TIBCO OI Hawk RedTail 7.3.0 agent component when configured with the AMI TCP session:

  — TIBCO Hawk® Microagent for TIBCO BusinessWorks™ Container Edition 2.0.0. Apply the TIBCO Hawk® Microagent for TIBCO BusinessWorks™ Container Edition 2.0.0 hotfix-1 or later to resolve the compatibility issue.

  — TIBCO Hawk® Microagent for TIBCO ActiveMatrix BusinessWorks™ 6 6.5 - 6.7.1. Apply the TIBCO Hawk® Microagent for TIBCO ActiveMatrix BusinessWorks™ 6 6.7.1 hotfix-1 or later to resolve the compatibility issue.

Closed Issues

The following issues have been fixed in this release of TIBCO® Operational Intelligence Hawk® RedTail.

Closed Issues

Key	Summary
HK-13434	Disabled TLSv1.1 and TLSv1 communication in legacy Hawk Console.
HK-13303	The data loss on subscription of onNewLogs method Kubernetes microagent.
HK-13275	The HawkConsole retains more number of alerts than the defined retention limit.
HK-13264	Failed to derive a rulebase that was imported from Hawk 5.2.0.
HK-13132	The Prometheus back-up service unable to delete older snapshots.
HK-13013	Unable to invoke the getPods methods of Kubernetes microagent in certain scenarios.
HK-13001	Unpredictable behavior between Hawk agent and HMA when RV connection is unstable.
HK-12999	The Hawk HMA FileSystem and FileStat microagents cause the HMA process to crash while encountering file mounts that the HMA's user does not have the permissions to read.
HK-12550	The RedTail UI is not accessible if IPv6 is disabled.

Known Issues

The following issues exist in this release of TIBCO® Operational Intelligence Hawk® RedTail.

Known Issues

Key	Summary and Workaround
HK-11683	**Summary:** After restarting ZooKeeper, the Search and the Active Queries pages do not load content.
	Workaround: Restart the query node after restarting ZooKeeper.
HK-11028	**Summary:** An error occurs when you create a test condition by using the `Speed (Mb/s)` parameter for the `getConfig` microagent method.
	Workaround: None

HK-9193	**Summary:** From the **Exporter** > **Tags Rulebase** menu, new Tags with condition that include spaces in the value cannot be created.
	For Example, see the following conditions:
	`(%MicroagentDisplayName% Equals TIBCO Rendezvous)`
	`(%AgentPlatform% Equals Windows Server 2016-10.0/amd64)`

	Workaround: Use "Contains" instead of "Equals" if the value contains space (s). OR Remove the space (s) from the value when using the `Equals` operator.
HK-9187	**Summary:** After TIBCO OI Hawk RedTail is installed, you see the `7.srl` file in the *TIBCO_HOME*/hawk folder.
	Workaround: It is a harmless file and can be ignored.
HK-9179	**Summary:** TIBCO® Enterprise Administrator UI displays

Known Issues(Continued)

Key	Summary and Workaround
	TIBCO Hawk as the product name instead of **TIBCO OI Hawk RedTail**. **Workaround:** None
HK-9079	**Summary:** From the **Tag Rulebases** > **Schedules** page, you cannot import or export schedules. **Workaround:** None
HK-9010	**Summary:** Some Hawk microagent methods that require input argument(s) might not provide results using the EQL query with the `'RT_'` DataModels. It is because EQL does not provide mandatory Hawk microagent method invocation input argument(s) to the query. **Workaround:** None
HK-9002	**Summary:** If you update a method in an existing tag-based rulebase and save it, it does not update the existing rule in Hawk but instead creates a new rule. **Workaround:** Manually delete the old rule.
HK-8525	**Summary:** You cannot configure a Prometheus Exporter for Microsoft Windows platform. **Workaround:** Configure HMA for the Hawk agent deployed on the Microsoft Windows platform and then manually create Hawk exporters for all the desired metrics.
HK-8523	**Summary:** The installation logs mention Hawk WebConsole even if the actual Hawk WebConsole Component is removed from TIBCO OI Hawk RedTail 7.1.0. **Workaround:** None
HK-7840	**Summary:** Rulebase deployment fails if you use TIBCO Hawk TEA Agent with TIBCO Enterprise Administrator 2.3.0,

Known Issues(Continued)

Key	Summary and Workaround
	as the TIBCO Enterprise Administrator server is currently not compatible with Java 11. **Workaround:** Follow these steps: Run TIBCO Hawk TEA Agent with Java 8 runtime. Update the following properties in `tibhawkteaagent.tra` file to point to Java 8 specific files and folders: • `JVM_LIB_PATH` • `JVM_LIB_DIR` Restart TIBCO Hawk TEA Agent after update.
HK-7238	**Summary:** When the database server goes down and OI Hawk Console is unable to connect to the database, OI Hawk Console asks for authentication repeatedly. Even after signing out, you cannot log in again using the correct user name and password. **Workaround:** Check the database status and restart the database. Once the database has started, try to log in to the OI Hawk Console again.
HK-6677	**Summary:** In Hawk Console, you cannot simplify or reduce complex test conditions in a single edit by using the rulebase test expression UI. **Workaround:** Perform multiple edits, modifying one expression per edit. Click **Update Test** after each edit to simplify the complex test condition.
HK-6666	**Summary:** There is no facility in Hawk Admin (TEA) Agent for the user to provide Clear Action. **Workaround:** Create/Edit the rulebase to add Clear action using some other Console application such as OI Hawk Console.

Known Issues(Continued)

Key	Summary and Workaround
HK-6264	**Summary:** In the Admin Agent, the **Rulebase** page does not list the imported rulebase when imported if the Hawk Agent's configuration directory (`-auto_config_dir`) to auto-load rulebases is empty. **Workaround:** Restart the Admin Agent.
HK-6263	**Summary:** In the **Rulebase Details** page of Hawk Admin Agent, the **Deploy To** option does not deploy the rulebase to the same agent but changes the rulebase state to `Deployed`. **Workaround:** None
HK-6244	**Summary:** In Hawk Admin Agent, when you close the Derive Rulebase wizard, a derived rulebase is created instead of canceling the derive operation. **Workaround:** None
HK-6197	**Summary:** If access control is activated with restrictions on `updateRulebase` or `deleteRulebase` methods, then changing the name of an existing rulebase causes the rulebase to go into an inconsistent state. **Workaround:** None
HK-6126	**Summary:** You cannot create a Clear Action for a test in Hawk Admin Agent. **Workaround:** Create or edit the rulebase to add the clear action using some other console application such as OI Hawk Console.
HK-5736	**Summary:** The Messaging microagent's `sendMessage` method in msghma does not set the JMS timestamp. Thus, the sent messages do not expire in the TIBCO Enterprise Message Service queue and do not fill up the queue.

Known Issues(Continued)

Key	Summary and Workaround
	Workaround: None
HK-5387	**Summary:** Invoking the **JMSController->getConsumer** method fails on the CentOS platform.
	Workaround: None
HK-5379	**Summary:** Even though a database user might have full privileges, the user encounters an error when trying to upload a `.mar` file using the **Configuring Monitoring** tool from its command mode. However, all privileges work if using the GUI.
	Workaround: Select Read, Write, and Administer permissions for **Monitoring Management** folder before selecting Read Write and Administer permissions for `TIBCO Administrator` folder while creating a user.
HK-5093	**Summary:** The HMA microagent methods do not work after invoking the `getStatistics()` method in the Network microagent.
	Workaround: None
HK-5031	**Summary:** In UNIX the `getVirtualMachineInfo` and `getProcess` methods return no results when the process name in the argument is more than 15 characters. Also, when the methods are executed with empty arguments, they return all the process names truncated to 15 characters. The issue occurs because both these methods read the process details from the `/proc/<process ID>/stat` file, where the Linux kernel limits the process name to 15 characters only.
	Workaround: Run the `getVirtualMachineInfo` or `getProcess` methods with a truncated (15 characters) process name. This returns information on all processes matching the supplied first 15 characters. You can identify

Known Issues(Continued)

Key	Summary and Workaround
	the information about the required process name using the Command Line (in the `getVirtualMachineInfo` method) or Command (in `getProcess` method) column.
HK-4722	**Summary:** Start two TIBCO Enterprise Messaging Service agents (one with SSL and another without SSL) with the same name but in different Hawk domains. Now if you configure the Hawk microagent for the SSL Hawk domain and agent, only the microagent is added to both the agents. **Workaround:** None
HK-4044	**Summary:** A Hawk event cannot batch commit records in the database. Each record is written in the database using separate commit commands. **Workaround:** None
HK-3723	**Summary:** If the Java process uses IBM JDK and Hawk Agent uses Sun JDK the JVM microagent cannot discover the JVMs running in the Java process. **Workaround:** Make sure that Hawk Agent uses the same JDK (IBM JRE version 1.6 that includes the support for attach APIs) as that used by the Java process.
HK-3573	**Summary:** Adding Hawk domain with SSL to TIBCO Administrator results in errors. **Workaround:** None
HK-2912	**Summary:** On the SUSE Linux 11 64-bit platform, the `COM.TIBCO.hawk.hma.TibRendezvous:onRvDaemonStatus` method returns a wrong value for the **Inbound Data Loss** field. **Workaround:** None

Known Issues(Continued)

Key	Summary and Workaround
HK-307	**Summary:** Uploading the Monitoring Console plug-in in the TIBCO Administrator fails with an exception. **Workaround:** Performing a standalone installation of TIBCO Hawk on the same machine resolves the issue.
HK-143	**Summary:** On Windows platforms, Japanese characters are not supported for use in regular expressions in the HMA microagents `Performance`, `Process`, and `Filestat`. Currently, only ASCII characters can be used for pattern matching. **Workaround:** None
TAHK-169	**Summary:** The clear and suspension details for an alert are not displayed after alert suspension. **Workaround:** None

TIBCO Documentation and Support Services

For information about this product, you can read the documentation, contact TIBCO Support, and join TIBCO Community.

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the Product Documentation website, mainly in HTML and PDF formats.

The Product Documentation website is updated frequently and is more current than any other documentation included with the product.

Product-Specific Documentation

The documentation for this product is available on the TIBCO® Operational Intelligence Hawk® RedTail Documentation page.

How to Contact Support for TIBCO Products

You can contact the Support team in the following ways:

- To access the Support Knowledge Base and getting personalized content about products you are interested in, visit our product Support website.

- To create a Support case, you must have a valid maintenance or support contract with a Cloud Software Group entity. You also need a username and password to log in to the our product Support website. If you do not have a username, you can request one by clicking **Register** on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature

requests from within the TIBCO Ideas Portal. For a free registration, go to TIBCO Community.

Legal and Third-Party Notices

SOME CLOUD SOFTWARE GROUP, INC. ("CLOUD SG") SOFTWARE AND CLOUD SERVICES EMBED, BUNDLE, OR OTHERWISE INCLUDE OTHER SOFTWARE, INCLUDING OTHER CLOUD SG SOFTWARE (COLLECTIVELY, "INCLUDED SOFTWARE"). USE OF INCLUDED SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED CLOUD SG SOFTWARE AND/OR CLOUD SERVICES. THE INCLUDED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER CLOUD SG SOFTWARE AND/OR CLOUD SERVICES OR FOR ANY OTHER PURPOSE.

USE OF CLOUD SG SOFTWARE AND CLOUD SERVICES IS SUBJECT TO THE TERMS AND CONDITIONS OF AN AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER AGREEMENT WHICH IS DISPLAYED WHEN ACCESSING, DOWNLOADING, OR INSTALLING THE SOFTWARE OR CLOUD SERVICES (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH LICENSE AGREEMENT OR CLICKWRAP END USER AGREEMENT, THE LICENSE(S) LOCATED IN THE "LICENSE" FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE SAME TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc.

TIBCO, the TIBCO logo, the TIBCO O logo, TIB, Information Bus, Hawk, Rendezvous, Administrator, and BusinessWorks are either registered trademarks or trademarks of Cloud Software Group, Inc. in the United States and/or other countries.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only. You acknowledge that all rights to these third party marks are the exclusive property of their respective owners. Please refer to Cloud SG's Third Party Trademark Notices (https://www.cloud.com/legal) for more information.

This document includes fonts that are licensed under the SIL Open Font License, Version 1.1, which is available at: https://scripts.sil.org/OFL

Copyright (c) Paul D. Hunt, with Reserved Font Name Source Sans Pro and Source Code Pro.

Cloud SG software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. See the "readme" file for the availability of a specific version of Cloud SG software on a specific operating system platform.