TIBCO LogLogic® Log Source Packages

Release Notes

Version 36.0.0
January 2021

Contents

Preface iii

Related Documentation iv
- Product-Specific Documentation iv
- Other TIBCO Product Documentation iv

TIBCO Product Documentation and Support Services v
- How to Contact TIBCO Support v
- How to Join TIBCO Community v

Release Notes 1

New Features 2
- New Log Sources 2
- Advanced Application Packs 2
- Other Enhancements 3

Changes in Functionality 4
- Updates to Existing Log Sources 4
- Advanced Application Pack 5

Deprecated and Removed Features 6

End of Support for Log Sources 7

Migration and Compatibility 9
- Advanced Features 9
- Advanced Application Pack 10

Closed Issues 11

Known Issues 12

Legal and Third-Party Notices 13

Preface

The TIBCO LogLogic® Log Source Packages (LSP) solution analyzes log data from TIBCO log sources and others including IoT, database, and monitoring products. LogLogic® LSP contains parsing rules, filters, and dashboards for data visualization, and uses TIBCO LogLogic® Log Management Intelligence (LMI) to provide meaningful reports of operational activity. By using LogLogic LSP, you can also manage distinct device types that require specific collection methods.

Topics

- Related Documentation, page iv
- TIBCO Product Documentation and Support Services, page v

Related Documentation

This section lists documentation resources you might find useful.

Product-Specific Documentation

The following documents form the TIBCO LogLogic® Log Source Packages documentation set:

- *TIBCO LogLogic® Log Source Packages Release Notes*
- *TIBCO LogLogic® Log Source Packages Installation and Upgrade Guide*
- *TIBCO LogLogic® Log Source Packages Log Configuration Guides*

Other TIBCO Product Documentation

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

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product. To access the latest documentation, visit https://docs.tibco.com.

You might find it useful to read the documentation for the following TIBCO products:

- TIBCO LogLogic® Log Management Intelligence
- TIBCO LogLogic® Universal Collector
- TIBCO® Operational Intelligence Agent

TIBCO Product Documentation and Support Services

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

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit https://www.tibco.com/services/support.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at https://support.tibco.com.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to https://support.tibco.com. If you do not have a user name, 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 https://community.tibco.com.

Release Notes

The release notes list the major updates in version 36.0.0 of TIBCO LogLogic® Log Source Packages. For information about an earlier version, see the release notes provided with the corresponding version.

In addition, it also includes the migration and compatibility considerations.

For information about changes to the product documentation after this LogLogic® LSP release, visit https://support.tibco.com.

Topics

- New Features, page 2
- Changes in Functionality, page 4
- Deprecated and Removed Features, page 6
- End of Support for Log Sources, page 7
- Migration and Compatibility, page 9
- Closed Issues, page 11
- Known Issues, page 12

New Features

This section lists the new log sources and new features in this release of LogLogic LSP. For more information about a log source, see the corresponding configuration guide.

New Log Sources

The following new log sources have been added in this release of LogLogic LSP:

Table 1 New Log Sources

Log Source	Versions or Platforms	Device Category	Requires Collector or Script on the Source	Collection Method
Check Point	R80.10, R80.20, R80.30	Firewall	No	Syslog
Cisco Firepower	v6.0-v6.5	IPS	Yes	eStreamer API

- For a list of the existing log sources that have been updated in this release, see Table 2, Updated Log Sources.
- For the complete list of supported log sources up to LogLogic LSP 36.0.0, see "Appendix A, Supported Log Sources" in the *TIBCO LogLogic® Log Source Packages Installation and Upgrade Guide.*

Advanced Application Packs

The following new Advanced Application Packs (AAPs) for Third-party products are provided in this release of LogLogic LSP:

- Check Point
- Cisco ESA
- Cisco Firepower

For more information

For the complete list of AAPs available with this release, see "Appendix B, Advanced Application Packs Reference" in the *TIBCO LogLogic® Log Source Packages Installation and Upgrade Guide.*

Other Enhancements

Added a new data model as **TIBCO Operational Intelligence Agent** in LogLogic® LMI to map the internal logs of the agent.

Changes in Functionality

The following log sources have been changed in this release of LogLogic LSP.

For more information about a log source, see the corresponding configuration guide.

Updates to Existing Log Sources

The following table lists log sources that were updated in this release.

Table 2 Updated Log Sources

Log Source or Collector	Versions or Platforms	Device Category	Requires Collector or Script on the Source	Collection Method	Changes in This Release
Apache Kafka Message Bus Collector	2.11-2.0.0 or later	Messaging Bus, Streaming Platform, Messaging Service	Yes	SASL, API, TCP	Added support for Kafka SASL-PLAIN mechanism to authenticate with Microsoft Azure Event Hub.
Check Point	R75-80 **Note:** R80 support requires LogLogic LMI 6.1.0 or later	Firewall	No	Log Export API (LEA)	Added support for Check Point Log Exporter feature.
Cisco Email Security Appliance (ESA)	v11.1	Mail Security	Yes (Script)	File Transfer	Added support for v11.1
General UNIX	AIX 5L, HP-UX 11i v2, Solaris 8, 9, 10, RHEL 5-8	System	No	Syslog	Added support for RHEL v8

Table 2 Updated Log Sources (Cont'd)

Log Source or Collector	Versions or Platforms	Device Category	Requires Collector or Script on the Source	Collection Method	Changes in This Release
Linux Operating System	RHEL 5-8 or SUSE 10; platform general parser	Operating System	No	Syslog	Added support for RHEL v8
Microsoft Windows Server	2008, 2008R2, 2012, 2012R2, 2016, 2019	Operating System	Yes (UC)	Syslog (for Snare or UC) or ULDP	Added support for Microsoft Windows Server 2019
Microsoft Active Directory (English)	2012, 2012R2, 2016, 2019	Directory Service	Yes (UC)	Syslog or ULDP	Added support for 2019 Microsoft Active Directory Services (ADS)

- For a list of the new log sources that are supported starting from this release, see Table 1, New Log Sources.
- For the complete list of log sources supported up to LogLogic LSP version 36.0.0, see "Appendix A, Supported Log Sources" in the *TIBCO LogLogic® Log Source Packages Installation and Upgrade Guide.*

Advanced Application Pack

The following Advanced Application Pack changes have been made in this release:

- All Advanced Application Pack objects are imported in LogLogic LMI during the installation of LogLogic LSP. Earlier, you had to import the required AAP archive into LogLogic LMI as a postinstallation task.
- For LogLogic LMI 6.3.0 or later, spaces are not supported in the names of Advanced Features such as Data Models, Enrichment Lists, Bloks, and Dashboards.

Deprecated and Removed Features

No features have been deprecated or removed as of this release of LogLogic LSP.

End of Support for Log Sources

The following log sources are no longer officially supported as of the specified LogLogic LSP version because their vendors have withdrawn support for the log sources. While the functionality is not being removed, there are no further updates forthcoming, and continued functionality of the noted versions cannot be guaranteed.

Table 3 End-of-Support Notice

Log Source	LogLogic LSP Version
Cisco Email Security Appliance (ESA) v7.0, v7.1	36.0.0
Cisco PIX	36.0.0
Juniper IDP	36.0.0
Microsoft Active Directory (English) v2008 R2	36.0.0
VMware ESX v5.5	35.0.0
VMware ESX v5.0, v5.1	33.0.0
VMware vCenter v5.5	35.0.0
VMware vCenter v5.0, v5.1	33.0.0
VMware Orchestrator	34.1.0
Cisco Firewall Services Module (FWSM)	34.0.0
HP NonStop Agent **Note**: For more information about this device, see the TIBCO Community portal.	34.0.0
IBM Resource Access Control Facility (RACF) Agent **Note**: For more information about this device, see the TIBCO Community portal.	34.0.0
IBM AS400 aka i5/OS Agent **Note**: For more information about this device, see the TIBCO Community portal.	34.0.0

Table 3 End-of-Support Notice (Cont'd)

Log Source	LogLogic LSP Version
Juniper (Netscreen) Firewall	34.0.0
Cisco Intrusion Prevention System (IPS) v7.3	33.0.0
Fortinet v5.2	33.0.0
Microsoft Exchange 2007	33.0.0
VMware vCloud Director	33.0.0
VMware vShield	33.0.0
TIBCO LogLogic® Database Security Manager	32.0.0

Migration and Compatibility

This section explains the migration and compatibility considerations when installing version 36.0.0 of LogLogic LSP.

LogLogic LSP 36.0.0 is compatible with LogLogic LMI versions 6.2.1, 6.3.0, and 6.3.1.

With LogLogic LSP 36.0.0, for Check Point device you can migrate from Check Point LEA to Check Point Log Exporter feature.

For more information, see "Migration from Check Point LEA to Check Point Log Exporter Feature" in *TIBCO LogLogic® Log Source Packages Log Configuration Guide for Check Point*.

Advanced Features

Advanced Features are supported on the appliance models listed in the following table:

Table 4 Appliance Models that Support Advanced Features

Appliance family	TIBCO LogLogic® LX Appliances	TIBCO LogLogic® ST Appliances	TIBCO LogLogic® MX Appliances
H5 appliances	• LX1035 • LX4035	• ST2035-SAN • ST4035	N/A
H4R2 appliances	• LX1025R2 • LX4025R2	• ST2025-SANR2 • ST4025R2	N/A
H4R1 appliances	• LX1025R1 • LX4025R1	• ST2025-SANR1 • ST4025R1	N/A

Important Consideration

When enabling Advanced Features on the appliance models (Table 5, Appliance Models with Low Memory) be cautious as the memory requirements of these features when in use might cause performance issues. Also, continuous use of Advanced Features on these models can cause the appliance to run out of memory and lead to engine restarts or failure.

Table 5 Appliance Models with Low Memory

Appliance family	TIBCO LogLogic® LX Appliances	TIBCO LogLogic® ST Appliances	TIBCO LogLogic® MX Appliances
H4R1	LogLogic® LX1025R1	N/A	N/A
H4R2 appliances	• LX1025R2 • LX4025R2	• ST2025-SANR2 • ST4025R2	N/A

Advanced Application Pack

The following appliance models do not have enough physical memory to support AAP features. Therefore, AAPs are not available on these models.

Table 6 Appliance Models on which AAP are not available

Appliance family	TIBCO LogLogic® LX Appliances	TIBCO LogLogic® ST Appliances	TIBCO LogLogic® MX Appliances
H4R1	TIBCO LogLogic® LX1025R1	N/A	N/A

Closed Issues

The following issues have been fixed in this release of LogLogic LSP:

Table 7 Closed Issues

Key	Summary
LLSP-6575	Logs of Windows eventID 4688 were not parsed in the Advanced Search with 3 different pRule ID.
LLSP-6525	Logs of Cisco Adaptive Security Appliance (ASA) device with eventID 722051 were not parsed in the Advanced Search.
LLSP-6467	Logs of Cisco ASA device with eventID 106023, 106010, and 106011 were not parsed in the Advanced Search.
LLSP-6458	Logs of Symantec Endpoint Protection device were mapped to the **General Syslog** data type instead of the **Symantec Endpoint Protection** data type.
LLSP-6346	In a LogLogic LMI 6.2.1 and LogLogic LSP 35.0.0 setup, when adding a **TIBCO Spotfire** device from the Management > Devices page, if the database in the **Logging Database Configuration** section and **JDBC Driver** list were both set to **Oracle**, the following error was displayed: `Error Message: No suitable driver found for jdbc:oracle:thin:@10.114.86.150:1521:orcl`
LLSP-4641	At times, the Kafka collector displayed a memory-related error. On the **Management > Devices** tab, if the **Kafka TLS** option was set to **disable**, but the Kafka server port was enabled with SSL parameters, the Kafka collector sometimes ran out of memory and displayed an error message.

Known Issues

The following issues exist in this release of LogLogic LSP.

Table 8 Known Issues

Key	Summary and Workaround
LLSP-6600	**Summary:** In a LogLogic LMI 6.3.0 and LogLogic LSP 36.0.0 setup, when TIBCO® Operational Intelligence Agent (TIBCO OI Agent) logs are sent to LogLogic LMI, the logs are mapped to the **General Syslog** data type instead of the **TIBCO Operational Intelligence Agent** data type. **Workaround:** Use LogLogic LMI 6.3.1 and LogLogic LSP 36.0.0 setup.
LLSP-4271	**Summary**: In General Database Collector, if a database column that is configured in the **Timestamp Column** field does not use a timestamp data type, LogLogic LMI uses the `cast()` function to convert it to a timestamp data type. **Workaround**: Contact the database administrator of your organization to consider adding a function-based index to the **Timestamp Column** field.
LLSP-3958	**Summary**: After making changes in the configuration of a log source that uses a LogLogic LSP collector, the associated collector restarts. The collector starts storing log data after LogLogic LMI has successfully started the collector. **Workaround**: None
LLSP-2393	**Summary**: The Cisco NetFlow collector does not support Raw Data Forwarding over IPv6. **Workaround**: None
LLSP-2248	**Summary**: In a High Availability (HA) setup, Sourcefire Defense Center (SFDC) might collect duplicate events when switching from the master node to the standby node. **Workaround**: None

Legal and Third-Party Notices