TIBCO LogLogic® Log Source Packages

Installation and Upgrade Guide

Version 36.1.0
February 2022

Contents

Overview

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.

Installation and Upgrade

The following sections describe how to install or upgrade to version 36.0.0 of LogLogic LSP on a LogLogic® LMI appliance.

Installing LogLogic LSP involves preparing for installation and installing the product package. In addition, after the installation is complete, you can perform tasks such as migrating data; and importing alerts, filters, and reports.

The procedures for installation and upgrade are identical. See Installing the Package.

Topics

Preparing for Installation

To prepare for installing LogLogic LSP, perform the following tasks:

- Check system and permission requirements.

  See System and Permission Requirements.

- (Only for a High Availability (HA) setup) Check the setup on the active and standby nodes.

  See Preinstallation Checks for a High Availability Setup.

- Download the installation package and other components.

  See Downloading the LogLogic LSP Installation Package.

The procedures for installation and upgrade are identical.

System and Permission Requirements

Before installing LogLogic LSP 36.0.0, you must meet the following requirements:

- You must have an appliance running LogLogic LMI versions 6.2.1, 6.3.0, or 6.3.1.
- You must have the permissions to access:
  - The appliance GUI
  - The appliance CLI by using the `toor` user account
- You must check if the log sources and devices you use are supported in this version of LogLogic LSP.
  - For a complete list of devices supported up to version 36.0.0 of LogLogic LSP, see Appendix A, Supported Log Sources.
  - For a list of new devices supported starting version 36.0.0 of LogLogic LSP, see the "New Features" section in *TIBCO LogLogic® Log Source Packages Release Notes*.

Preinstallation Checks for a High Availability Setup

If you are installing in a High Availability (HA) setup, ensure that you complete the following prerequisites before installing the new version of LogLogic LSP:

- The active and standby nodes must be in sync.

- The **Dashboard > System Status** page must not display any warning messages.

For more information about installing in an HA setup, see the *TIBCO LogLogic® Log Management Intelligence Configuration and Upgrade Guide.*

Downloading the LogLogic LSP Installation Package

You can use any of the following procedures to download the LogLogic LSP package files:

- Downloading from the eDelivery Website
- Downloading from the TIBCO Support Website

Prerequisites

Before you start downloading, you must perform the following checks as applicable.

For a Management Station setup

If you are installing LogLogic LSP on a Management Station appliance, then the LogLogic LSP version on the Management Station appliance must match the LogLogic LSP version on all the Remote Appliances that are being managed by the Management Station appliance. Ensure that you download the appropriate version of LogLogic LSP.

When upgrading, you must upgrade LogLogic LSP on the Remote Appliances first and then on the Management Station.

For using Enterprise Message Service™ as a log source

To use Enterprise Message Service™ as a log source, check if any of the following scenarios is true:

- You are using LogLogic LMI version 6.2.0 or later
- You are upgrading to LogLogic LSP 34.0.0 or later

If any of these scenarios is true, you must download TIBCO Enterprise Message Service™ as described at step 7 in Downloading from the eDelivery Website.

If you are an existing user, then you must upgrade the Enterprise Message Service™ client library to version 8.4.0 or later. For upgrade instructions, see the *TIBCO LogLogic® Log Source Packages Log Configuration Guide for TIBCO Enterprise Message Service™*.

For more information about Enterprise Message Service™ license restrictions, see the LogLogic LMI Readme file.

Downloading from the eDelivery Website

1. Log in to the eDelivery website (requires a valid TIBCO account).
2. Search for the product name **TIBCO LogLogic Log Source Packages**.
3. Scroll down to the **Components found** section and click the required LogLogic LSP version.
4. On the Download page, from the Operating Systems list, select **ISO (DVD Image)**.
5. Accept the End User License Agreement (EULA) declaration.
6. Under Installation Method, click the **Individual file download** option.
7. (Optional) If you are using Enterprise Message Service™ as a log source, click **TIBCO Enterprise Message Service Software** to download TIBCO Enterprise Message Service™.
8. Click **+** to expand the list of files in the LogLogic LSP package.
9. To download the installer, click `TIB_loglsp_<pkgversion>_installer.bin`.
10. In the list, click any other file that you want to download.

    For a list of files in the package, see Contents of the LogLogic LSP package.
11. Copy `TIB_loglsp_<pkgversion>_installer.bin` to any directory on the TIBCO LogLogic® appliance by using a secure copy utility such as WinSCP.

Downloading from the TIBCO Support Website

1. Log in to the TIBCO Support website (requires a TIBCO Support account).
2. From the **Downloads** menu, select **Hotfixes**.
3. In the directory list, expand **AvailableDownloads**.
4. Expand **LogLogic** > **Log Source Packages (LSP)** > **LSP <*pkgversion*>**.
5. To download the installer, click `TIB_loglsp_<pkgversion>_installer.bin`.
6. In the list, click any other file that you want to download. For a list of files in the package, see Contents of the LogLogic LSP package.
7. Copy `TIB_loglsp_<pkgversion>_installer.bin` to the TIBCO LogLogic® appliance by using a secure copy utility such as WinSCP.

Contents of the LogLogic LSP package

The following table lists the files included in the LogLogic LSP package.

Table 1

#	File	Description
	`TIB_loglsp_<pkgversion>_documents.zip`	An archive that contains the license and release notes files
	`TIB_loglsp_<pkgversion>_guides.zip`	An archive that contains the LogLogic LSP log source configuration guides
	`TIB_loglsp_<pkgversion>_install_upgrade.pdf`	The PDF file for TIBCO LogLogic® Log Source Packages Installation and Upgrade Guide
	`TIB_loglsp_<pkgversion>_installer.bin`	A self-extracting executable file
	`TIB_loglsp_<pkgversion>_license.pdf`	The license PDF file
	`TIB_loglsp_<pkgversion>_license.txt`	The license text file **Note**: This file is not available on the TIBCO Support website.
	`TIB_loglsp_<pkgversion>_mcbundle.zip`	The LogLogic LSP installation package for TIBCO LogLogic® Management Center
	`TIB_loglsp_<pkgversion>_readme.txt`	The readme file
	`TIB_loglsp_<pkgversion>_relnotes.pdf`	The release notes PDF file

Table 1

#	File	Description
	`TIB_loglsp_<pkgversion>_supplemental.zip`	The archive containing the following files: • `scripts.tar`: The archive that contains collectors and sample or required scripts that allow LogLogic LSP to support certain log sources. For more information about log source-related collectors or scripts, see the LogLogic LSP documentation for the log source. • `SearchFilters_Reports_Alerts.xml`: The XML file for alerts, custom reports, and search filters • `mc-upgrade-policy.zip`: The archive that contains LogLogic LMI policy files for upgrading LogLogic LSP via LogLogic® Management Center

Installing the Package

This section includes instructions to install or upgrade LogLogic LSP.

The procedures for installation and upgrade are identical.

Installing LogLogic LSP version 32.1.0 or later on LogLogic LMI version 6.1.0 or later includes installing content for Advanced Features. Therefore, the installation process might take longer than in earlier versions.

If you are upgrading from an older version of LogLogic LSP, you must sequentially install from your current version up to LogLogic LSP version 36.0.0. You can skip at the most one version at a time for each upgrade in the sequence. For example, if you are currently using LogLogic LSP version 34.1.0, you can upgrade to version 36.0.0 (by skipping version 35.0.0).

When installing multiple versions within a short time span, you must start the next installation only after the previous data migration process is complete.

Data cannot be recovered after subsequent upgrades or installations are performed. Existing data is not available until the data migration process is complete.

Prerequisites

- Ensure that you have performed the tasks in the Preparing for Installation section.
- If you are installing in an HA setup, ensure that you have completed the Preinstallation Checks for a High Availability Setup. Upgrade simultaneously on the active and standby nodes without disabling HA and retaining the role for each node. Start installation on the active node first and then on the standby node.
- In some cases, the LogLogic LSP installer might fail to detect that data migration has been performed. In these cases, it is good practice to run the migration process again prior to the LogLogic LSP installation unless you are sure that the migration was performed. For more information, see Data Migration.

Procedure

1. Using the `toor` account, log in to the LogLogic LMI appliance.
2. Make the LogLogic LSP installation file executable by running any of the following commands:

   ```
   $ chmod 0755 TIB_loglsp_<pkgversion>_installer.bin
   ```

   ```
   $ chmod +x TIB_loglsp_<pkgversion>_installer.bin
   ```

3. Start the installation by running the following command:

   ```
   $ ./TIB_loglsp_<pkgversion>_installer.bin
   ```

Do not resize the terminal window during the installation procedure.

The installation menu is displayed:

```
LSP 36.0 Installation Menu
** PLEASE BE SURE TO SEE RELEASE NOTES FOR ANY **
** KNOWN DEVICE CHANGES PRIOR TO LSP INSTALL   **
1) New Device Package Installation
2) Review Device Packgage Installation History
3) Review Device Versions
4) Verify Installation Prerequisites
Q) Exit (type Q or q)
Enter choice:
```

It is good practice to verify installation prerequisites before performing the installation. Doing so gives you an opportunity to review the prerequisite check results before the installation.

4. After the installation menu is displayed, enter **`4`** (without carriage return [\r]) to verify installation prerequisites.

   Messages indicating the progress of the prerequisite checks are displayed. If the prerequisite checks fail, the option to install the package is disabled.

5. When the installation menu is displayed again, enter **`1`** to continue with the installation.
6. The following message is displayed:

   ```
   Installing the package will restart the application. Do you wish
   to continue? (Y/N)
   ```

Enter **Y**.

The installer extracts and installs the contents of LogLogic LSP, saves the existing configuration in a temporary directory, updates the database, and restarts `mtask`. Messages indicating the progress of installation are displayed. For example:

```
Installation has been started
Stopping the Appliance
Starting Mysql Daemon
Performing Database Updates
Starting Post-Installation Tasks
Starting the Appliance
Installation Successful
-- Press Any Key to Exit --
```

7. View the following log files to check if there are any errors during installation:
   - `/var/log/pkg_install_lsp_<`*lspVersion-timestamp*`>.log`
   - `/var/log/aap_import_<`*lspVersion-timestamp*`>.log`
8. Log in to the appliance GUI and ensure that LogLogic LSP version 36.0.0 is installed. The appliance model and LogLogic LSP version are displayed in the upper-right corner of the window.

Advanced Application Packs

The LogLogic LSP installation package contains Advanced Application Pack (AAP), which is imported to LogLogic LMI during the installation of LogLogic LSP.

The AAP includes built-in objects such as Bloks, Dashboards, Correlation rules, and Aggregation rules for use in the Advanced Features of LogLogic LMI. The objects included in the AAP vary from one log source to another. You can use these objects as is or customize them. To customize the objects, you must duplicate them and then modify as required.

For a list of appliance models on which Advanced Features are supported and models on which AAP cannot be imported, see the "Migration and Compatibility" section in the *TIBCO LogLogic® Log Source Packages Release Notes*.

For a complete list of AAPs available in this release, see Appendix B, Advanced Application Packs Reference.

For more information about Advanced Features, see the *TIBCO LogLogic® Log Management Intelligence User Guide*.

Postinstallation Tasks

To import additional objects, perform the following tasks after the installation is complete:

- Importing Filters, Alerts, and Custom Reports
- Data Migration

The procedures for installation and upgrade are identical.

Importing Filters, Alerts, and Custom Reports

After installing LogLogic LSP, you can import search filters, alerts, and custom reports to LogLogic LMI from the `SearchFilters_Reports_Alerts.xml` file.

Prerequisites

Ensure that you fulfill the following requirements:

- You must have downloaded the archive `TIB_loglsp_<pkgversion>_supplemental.zip` and extracted its contents.

  See Downloading the LogLogic LSP Installation Package.
- You must have administrator access to LogLogic LMI GUI.

Procedure

To import filters, alerts, and reports:

1. Log in as an administrator to the GUI of the appliance where you want to import the filters, alerts, and reports.
2. Navigate to **Administration > Import/Export**.
3. On the **Import** tab, click **Browse** and select the XML file saved on the local system. The XML file is included in `TIB_loglsp_<pkgversion>_supplemental.zip`.
4. Click **Load** to list the package under **Available Entities**.
5. Select the package under **Available Entities** and click the right-arrow button to move it to **Selected Entities**.
6. Click **Display Info** to view the contents of the XML file in the text area.

7. Click **Import** to import the package to the appliance.

After importing, the package is listed on the **Management > Suites** page.

Data Migration

Data migration in LogLogic LMI includes migrating all data from one appliance to another. However, data migration in LogLogic LSP applies only to the databases that store real-time reports.

The data migration process in LogLogic LSP includes updating data in the databases, for example, updating the existing data to make it compatible with updated table structures for the current LogLogic LSP version.

During data migration, the existing data is moved into a temporary location. The relevant tables for which the schema or table structure is updated are recreated on the appliance and the data from the temporary location is inserted back into the database tables.

Depending upon the volume of existing data on your appliance, data migration can take several hours to complete.

Procedure

To perform data migration after the installation:

1. Log in to the appliance CLI through SSH by using the `toor` account.
2. Run the following command:

   ```
   $ rundbm
   ```

   The following configuration menu appears:

   ```
   Configuration Menu:
   1) Modify the above configuration
   2) Start the Post Upgrade Process
   3) Help
   4) Exit the Post Upgrade Process
   Enter choice:
   ```

3. (Optional) To modify the configuration, type **`1`** and press Enter.

   By default, LogLogic LSP preserves the past seven days of existing alert history or parsed log data. If you have such data and want to preserve more than the past seven days of data, you can modify the configuration to change the number of days to preserve the data.

The modify configuration menu appears, as follows:

```
Modify Configuration Menu:
1) module_<LMI_version>_DatabaseAudit
2) module_<LMI_version>_i5OSAudit
3) module_<LMI_version>_Authentication
4) module_lsp_smtplog
5) Return to Configuration Menu
6) Help
Enter 1 - 6:
```

For example, for SMTP Log:

a. Type **4**.

b. Enter the amount of preexisting SMTP log data, in days, which you want accessible on the appliance after the migration. For example, if you want access to the SMTP log data for the past month, enter **31**. The default setting is seven, which converts to the past week.

   The higher the number of days you enter, the longer the migration takes to complete. To preserve the ability to search on all log data collected from SMTP Log sources, enter a number (in days) that includes the first collection of SMTP log information that is still stored in parsed data retention. Data that is on the system can be converted; however, raw or indexed data cannot be converted.

Repeat this step for each option, as required.

4. Type **5** to return to the configuration menu.
5. When the configuration menu is displayed, type **2** to start the migration process. The time for the migration process depends on the volume of data to be migrated. When the migration is complete, the configuration menu is displayed again.
6. When the message: "`All migrations complete`" is displayed, press **Enter** to exit the migration process. The following message is displayed:

```
"""2017-07-05 13:33:46,030 - dbmLogger - INFO : ** All
migrations complete!"""
```

Appendix A Supported Log Sources

Each LogLogic LSP release package cumulatively contains all log sources supported by LogLogic LSP starting from release 1.0 through release 36.0.0.

For a list of supported platforms for a log source, see the Log Configuration guide for that log source.

Important Considerations

- The support for Windows Server event collection is available through the following products:
  - Snare for Windows version(s) 1.1.x - 4.3.5
  - TIBCO LogLogic® Universal Collector
  - TIBCO® Operational Intelligence Agent

  For more information about the TIBCO products, see the product documentation at https://docs.tibco.com.
- When using a JDBC collector like Microsoft SQL Server, the collector uses the appliance time zone information when storing the collection start time. For example, if the appliance has a time zone set to PST8PDT, then the collector adds eight hours to the configured value of "Start Collection From Date".
- When using the General Database Collector to retrieve logs from a table that contains more than one TimeStamp column, you must define the columns to be collected using the **Query Columns** field. But if there is only one TimeStamp column, it must be the same column defined in the **TimeStamp Column** field.

For a list of new and updated log sources in this release, see *TIBCO LogLogic® Log Source Packages Release Notes*.

Table 2 Supported Log Sources

Log Source or Collector	Log Source Versions and Supported Platforms	Device Category	Requires collector or script on the source?	Collection Method
Amazon CloudWatch	N/A	Monitoring	Script	Syslog over AWS Lambda
Amazon Elastic Load Balancing	N/A	Load Balancer	Script	Syslog over AWS Lambda
Apache Kafka Message Bus Collector	2.11-2.0.0 or later	Messaging Bus, Streaming Platform, Messaging Service	Yes	SASL, API, TCP
Apache Web Server	v2.2.4	Apache WebServer	No	File Transfer
AWS CloudTrail	N/A	Auditing	Script	Syslog over AWS Lambda
Blue Coat	v3.4	WebProxy	No	File Transfer
Blue Coat ProxySG Syslog	v5.4, v6.1-v6.3.0	WebProxy	No	Syslog
BMC Remedy Action Request (AR) System	7.0 on Microsoft Windows 2000 or 2003 Server	BMC Remedy ARS	No	File Transfer
CA SiteMinder – Access Management System	5.5, 6.0 SP1 or SP2 on Windows 2000 with SP4, 2003, or Solaris 8 or 9	Access Control	No	File Transfer
Check Point	R80.10 R80.20 R80.30	Firewall	No	Syslog

Table 2 Supported Log Sources (Cont'd)

Log Source or Collector	Log Source Versions and Supported Platforms	Device Category	Requires collector or script on the source?	Collection Method
Check Point	R75-80 **Note**: R80 support requires LogLogic LMI 6.1.0 or later	Firewall	No	Log Export API (LEA)
Check Point Firewall (CP Audit)	R80	Firewall	No	OPSec API
Check Point LEA Server	R80	Firewall	No	LEA
Cisco (Nexus) NX-OS	v8.3	Switch	No	Syslog
Cisco ACS for Windows	v3.0	Access Control	No	File Transfer
Cisco Adaptive Security Appliance (ASA)	v7.2, v8.0, v8.2 – v8.4, v8.5 - v8.7, v9.0 - v9.7	Unified Threat Management (UTM)	No	Syslog
Cisco Content Engine	Content Engine with Cisco Application and Content Networking System (ACNS) 4.2 or 5.5	Cisco Content Engine	No	File Transfer
Cisco Email Security Appliance (ESA)	v11.1	Mail Security	Yes (Script)	File Transfer
Cisco Firepower	v6.0-v6.5	IPS	Yes	eStreamer API
Cisco Identity Services Engine (ISE)	v1.0.2, v1.1.3	Access Control	No	Syslog
Cisco IOS	v12.x, v15.0(M), v15.1(M), v15.1	Router and Switches, UTM	No	Syslog

Table 2 Supported Log Sources (Cont'd)

Log Source or Collector	Log Source Versions and Supported Platforms	Device Category	Requires collector or script on the source?	Collection Method
Cisco NetFlow	Cisco NetFlow v5 or v9, NSEL. IOS XE v15.1(3)M NAT64 NetFlow v9	Router	No	NetFlow
Cisco Router	v12.x	Router / Access Control	No	Syslog
Cisco Secure ACS	v5.2, v5.3, v5.4	Access Control	No	Syslog
Cisco Switch	IOS v12	Switch	No	Syslog
Cisco Web Security Appliance (WSA)	Async OS v6.3, v7.1, or v7.5	Web Security	No	File Transfer
CyberArk Enterprise Password Vault	v4.0	Application	No	Syslog
F5 BIGIP Traffic Management Operating System (TMOS)	ASM v11.0.0, v12.1, v12.4 LTM v11.0.0, v12.1, v12.4	Firewall, Load Balancer	No	Syslog
FireEye NX	v7.8	IPS	No	Syslog
Forcepoint Web Security	v7.x, v8.x	UTM	No	Syslog
Fortinet (FortiOS)	FortiOS v5.6.x, v6.0.x	Firewall	No	Syslog
General Database Collector for Microsoft SQL Server	2012 SP4, 2014, 2016, 2017 Standard or Enterprise	Database	Yes	Database Transfer
General Database Collector for MySQL Server	v5.5.9	Database	No	Database Transfer

Table 2 Supported Log Sources (Cont'd)

Log Source or Collector	Log Source Versions and Supported Platforms	Device Category	Requires collector or script on the source?	Collection Method
General Database Collector for Oracle	Oracle 9.2, 10.1, 10.2, 11g, 12c	Database	No	Database Transfer
General UNIX	AIX 5L, HP-UX 11i v2, Solaris 8, 9, 10, RHEL 5-8	System	No	Syslog
Generic W3C	Web Server/ Firewall	General	No	File Transfer
GuardiumSQLGuard	v6.1	DB IDS/ IPS	No	Syslog
GuardiumSQLGuard Audit	v6.1	DB IDS/ IPS	No	File Transfer
HP NonStop	HP NonStop running D48 or later on a K-series System; G06.20 or later on an S-series System; H06 or later on an Integrity NonStop System	System	Yes (Collector)	Syslog
HP-UX Operating System Audit	HP-UX 11i v2, HP-UX 11i.31	System Audit	No	File Transfer
HP-UX UNIX Operating System	HP-UX 11i v2, HP-UX 11i v3	Operating System	No	Syslog
IBM AIX Audit	v5.3, v6.0, v6.1, v7.1	System	Yes (script)	File Transfer
IBM AIX Operating System	v5.3, v6.0, v6.1, v7.1	Operating System	No	Syslog
IBM AS400 aka i5/OS	v5R2, v5R3, v6R1, v7R1	Operating System	Yes (Collector)	Syslog

Table 2 Supported Log Sources (Cont'd)

Log Source or Collector	Log Source Versions and Supported Platforms	Device Category	Requires collector or script on the source?	Collection Method
IBM DB2 Universal Database (UDB)	v8.1, v8.2, v9.0, v9.5, v9.7, v11.1 Enterprise Server Edition on Windows, Solaris, HP-UX, Linux, or AIX	Database	Yes (script)	File Transfer, Database Transfer
IBM ISS RealSecure NIDS	7.0	IDS	No	Syslog
IBM ISS SiteProtector	v2.0 Sp5.0, 5.1, 6.1, 6.2, 8.0, 9.0	IPS	Yes (Collector)	Syslog
IBM Resource Access Control Facility (RACF)	SMF record types 80, 81, 83, for RACF on z/OS versions 1.6, 1.7, 1.8, 1.9, 1.10, 1.11-1.13	Access Control	Yes (Collector)	File Transfer
Juniper (JunOS)	v11-v13	UTM	No	Syslog
Juniper (Neoteris) SSL VPN	v5.1R2	VPN	No	Syslog
Juniper SSL VPN Secure Access	v5.5, v6.0 R3, v6.1 R1, v6.2, v6.5, v7.0, v7.1	VPN	No	Syslog
KEPServer EX	v6.1	IoT	No	Syslog
Linux Operating System	RHEL 5-8 or SUSE 10; platform general parser	Operating System	No	Syslog
McAfee Enterprise Firewall (G2 Sidewinder)	FW v7.x, v8.0-v8.3	Firewall/ VPN	No	Syslog
McAfee ePO (Host Intrusion Prevention)	ePO v4.5, v4.6.0, v4.6.1, v4.6.2; HIPS v7.0, v8.0	IPS	No	Database

Table 2 Supported Log Sources (Cont'd)

Log Source or Collector	Log Source Versions and Supported Platforms	Device Category	Requires collector or script on the source?	Collection Method
McAfee ePO (McAfee AntiSpyware Enterprise)	ePO v4.5, v4.6.0, v4.6.1, v4.6.2; VSE with ASE v8.5i, v8.7i	AntiVirus	No	Database
McAfee ePO (McAfee AntiVirus Enterprise)	ePO v5.0, v5.1, v5.3, v5.9; VSE v8.5i, v8.7i, v8.8i	AntiVirus	No	Database
McAfee ePO (McAfee Rogue System Detection)	ePO v4.5; VSE v8.5i, v8.7i; RSD v2.0	AntiVirus	No	Database
Microsoft Active Directory (English)	2012, 2012R2, 2016, 2019	Directory Service	Yes (UC)	Syslog or ULDP
Microsoft DHCP	2008 or 2008 R2 with SP1, 2012	Microsoft DHCP Application	No	File Transfer
Microsoft DNS	2008 or 2008R2	Microsoft DNS Application	Yes (UC)	Syslog or ULDP
Microsoft Exchange	2013, 2016	Mail	No	Syslog and File Transfer
Microsoft Internet Authentication Service (IAS)	Microsoft Windows Servers	Access Control	No	File Transfer
Microsoft Internet Information Server (IIS)	7.0 on Windows 2008, 2012 Server	Microsoft IIS Server	No	File Transfer
Microsoft Internet Security and Acceleration (ISA)	Microsoft ISA Servers	Firewall	No	File Transfer

Table 2 Supported Log Sources (Cont'd)

Log Source or Collector	Log Source Versions and Supported Platforms	Device Category	Requires collector or script on the source?	Collection Method
Microsoft Office 365	Microsoft Office 365	Collaboration Platform	No	REST API
Microsoft Office SharePoint Server	2007, 2010	Content Management	No	Database Transfer
Microsoft Operations Manager	2007 running on Windows 2008 Server	System	No	Database Transfer
Microsoft SQL Server (Application Logs)	2012 SP4, 2014, 2016, 2017 Standard or Enterprise	Database	Yes (UC)	Syslog or ULDP
Microsoft SQL Server Audit	2012 SP4, 2014, 2016, 2017 Standard or Enterprise	Database	No	Database Transfer
Microsoft Windows Server	2008, 2008R2, 2012, 2012R2, 2016, 2019	Operating System	Yes (UC)	Syslog (for Snare or UC) or ULDP
Microsoft Windows Server (Chinese)	2008R2, 2012, 2012R2	Operating System	Yes (UC)	Syslog (for Snare or UC) or ULDP
Microsoft Windows Server (French)	2008R2, 2012, 2012R2	Operating System	Yes (UC)	Syslog (for Snare or UC) or ULDP
Microsoft Windows Server (German)	2008R2, 2012, 2012R2	Operating System	Yes (UC)	Syslog (for Snare or UC) or ULDP
Microsoft Windows Server (Japanese)	2008R2, 2012, 2012R2	Operating System	Yes (UC)	Syslog (for Snare or UC) or ULDP
Microsoft Windows Server (Korean)	2008R2, 2012, 2012R2	Operating System	Yes (UC)	Syslog (for Snare or UC) or ULDP

Table 2 Supported Log Sources (Cont'd)

Log Source or Collector	Log Source Versions and Supported Platforms	Device Category	Requires collector or script on the source?	Collection Method
NetApp Decru DataFort	DataFort FC-series: FC525, FC520, FC1020, E-series: E510, E515, and S-series: S110 appliances	Decru DataFort	No	Syslog
NetApp Filer	NetApp Data ONTAP v7.0, v7.3, v8.0, v8.1-v8.2 on FAS900, FAS200, F800, GF900, GF800, NearStore R200, 150, 100, F87 (Not supported on F700 or F85)	Storage System	Yes (Collector)	Syslog
NetApp NetCache	Internet Access and Security Appliances	Web	No	File Transfer
Nortel Contivity	4.7, 4.9, 5.0, 5.05, 6.05, 7.0	VPN	No	Syslog
Novell eDirectory	eDirectory 8.8 on Windows 2000 Server with Service Pack 4; Windows 2003 Server Enterprise Edition with Service Pack 1; Windows XP Professional with Service Pack 2; Red Hat Linux Advanced Server 4; or Novell NetWare 6.5 Support Pack 7	LDAP Directory Service	Yes (Collector)	Syslog
Open Source HIDS SECurity (OSSEC)	v2.8.3	Host Intrusion Protection System (HIPS)	No	Syslog

Table 2 Supported Log Sources (Cont'd)

Log Source or Collector	Log Source Versions and Supported Platforms	Device Category	Requires collector or script on the source?	Collection Method
Oracle Database Audit	11g, 12c	Database	No	Database Transfer
Oracle Database Server	Oracle 9i R2, 10g R1/R2, 10.2.0.4g, 11g, 11.2.0.1.0g, 12c, on Linux (Fedora Core 3), Solaris 9 (64-bit SPARC and Intel i386), HP-UX 11i, or AIX 5.3	Database	No	Database Transfer
Oracle Database Syslog	v12c	Database	No	Syslog
Other File Device	General file collection	General File	No	File Transfer
Palo Alto Networks PanOS	v5.0, v6.0, v6.1.4-v7.0, v7.1	UTM	No	Syslog
Pulse Connect Secure	v8.1R5 - 8.1R9.1	VPN	No	Syslog
Remote Authentication Dial-In User Service (RADIUS) Acct Client	unknown	Access Control	No	Syslog
Reuters KondorPlus	All versions	Application	No	File Transfer
RSA ACE/Server	4.x, 5.x, 6.x, and v8.0 on Solaris	Access Control	No	Syslog
ServiceNow	London	Service Management	No	Syslog
Snort	v2.4, v2.6, v2.8, v2.9	Intrusion Detection	No	Syslog
Sourcefire Defense Center (SFDC)	v4.10.0.0. v5.0.0-v5.1.0, v5.2.0	IDS/IPS	No	eStreamer WEB API
Sourcefire Sensor	v4.1, v4.6, v4.7 – v4.10	IDS/IPS	No	Syslog
Squid	Squid-2	WebProxy	No	File Transfer

Table 2 Supported Log Sources (Cont'd)

Log Source or Collector	Log Source Versions and Supported Platforms	Device Category	Requires collector or script on the source?	Collection Method
Sun Solaris	8, 9, 10	Operating System	No	Syslog
Sun Solaris Basic Security Module (BSM)	8, 9, 10 on Sun SPARC or Intel i386 platforms	Operating System	Yes (Script)	File Transfer
Sybase Adaptive Server Enterprise (ASE)	Sybase ASE 12.5.x, 15, or 15.7 running on Windows XP Professional, Windows Server 2003 Standard or Enterprise, Red Hat Enterprise Linux 4, SUSE Linux Enterprise Server 9, or Sun Solaris 8,9 or 10 (32 or 64-bit SPARC or Intel i386) platforms	Database	No	Database Transfer
Symantec Endpoint Protection	v11, v12, v14	AntiVirus	No	Syslog
TIBCO ActiveMatrix® Administrator	v3.3.0	Management Server	Yes (UC or TIBCO EMS API)	Syslog or TIBCO EMS API
TIBCO ActiveMatrix BusinessWorks™	v5.11	Business Process	Yes (UC or TIBCO EMS API)	Syslog or TIBCO EMS API
TIBCO ActiveMatrix® BPM	v3.0	Business Process	Yes (UC)	ULDP
TIBCO ActiveSpaces®	v2.1.5	Container	Yes (UC)	ULDP
TIBCO Administrator™	v5.0, v7.0	Management Server	No	TIBCO EMS API
TIBCO BusinessConnect™	v6.3, v6.4	Business Process	Collector	Syslog and Database transfer

Table 2 Supported Log Sources (Cont'd)

Log Source or Collector	Log Source Versions and Supported Platforms	Device Category	Requires collector or script on the source?	Collection Method
TIBCO BusinessEvents®	V5.1.0	Business Process	Yes (UC)	ULDP
TIBCO Enterprise Message Service Collector	v6.1.0, v6.3.0, v8.3.0, v8.4.0	EMS	No	TIBCO EMS API
TIBCO GridServer®	v6.2	Computing	No	Syslog
TIBCO Hawk® Agent	v5.11, Docker	Business Process	Yes (UC or TIBCO EMS API)	Syslog or TIBCO EMS API
TIBCO LogLogic® Custom KVP	1.0.0	Custom	No	Syslog
TIBCO LogLogic® LMI Appliance	All versions	Log Management	No	Syslog
TIBCO LogLogic® Unity	1.0.0	Log Management	No	File Pull
TIBCO Mashery Cloud	N/A	Web System	Yes	Amazon S3 collector
TIBCO Mashery Local	v4.4, v5.0	Web System	No	Syslog
TIBCO Silver® Fabric	v5.7.0	Cloud Management	Yes (UC)	ULDP
TIBCO Spotfire®	v7.x, v10.x	Data Visualization and Analytics	No	Database transfer
TIBCO®API Exchange	v2.1.0	Business Process	Yes (UC)	ULDP
TrendMicro Control Manager	v5.0	AntiVirus	Yes (UC or TIBCO EMS API)	Syslog or TIBCO EMS API

Table 2 Supported Log Sources (Cont'd)

Log Source or Collector	Log Source Versions and Supported Platforms	Device Category	Requires collector or script on the source?	Collection Method
TrendMicro OfficeScan	v10.0, v10.5	AntiVirus	No	Syslog
VMware ESX Server	v6.0, v6.5, v6.7	Hypervisor	No	Syslog
VMware vCenter	v6.0, v6.5, v6.7	Management Server	No	vCenter Web API

Appendix B Advanced Application Packs Reference

In the current release 36.0.0, AAPs are available for the following TIBCO and third-party log sources:

TIBCO Products

AAPs are available for the following TIBCO products:

- TIBCO ActiveMatrix BusinessWorks™
- TIBCO ActiveSpaces®
- TIBCO BusinessConnect™
- TIBCO BusinessEvents®
- TIBCO Enterprise Message Service™
- TIBCO GridServer® Engine
- TIBCO Mashery Local
- TIBCO Mashery Cloud
- TIBCO Spotfire

Third-Party Products

AAPs are available for the following third-party products:

- AWS CloudTrail
- Amazon Elastic Load Balancing
- Check Point
- Cisco ESA
- Cisco Firepower
- FireEye
- FortiGate
- IBM DB2 Universal Database
- Microsoft Active Directory Server

- Microsoft SQL Server
- Microsoft Windows Server
- Oracle Database
- ServiceNow
- Sybase Adaptive Server Enterprise (ASE)
- Symantec Endpoint Protection
- VMWare ESX
- VMWare vCenter

Appendix C Troubleshooting

This section contains troubleshooting information about installing or upgrading LogLogic LSP. The sections list errors that might be displayed during installation or upgrade, and the description of the errors.

Topics

Installation scenarios

Message: `LSP <version> cannot be installed until the postupgrade exits`

Description: The installer exits after detecting the data migration script executing. For more information about the postupgrade, see the Data Migration section.

Message: `Error: Current product release version is <LMI_version>.`

`Package can be installed only on versions <min_LMI_version> through <max_LMI_version>.`

`For details, see the Troubleshooting section in the Installation and Upgrade Guide.`

Description: The installer exits after displaying this message. The error occurs when LogLogic LSP version 36.0.0 is not compatible with LogLogic LMI versions.

The LogLogic LMI version on your appliance is displayed on the GUI in the top right corner. For the compatible LogLogic LMI version, see System and Permission Requirements before you start LogLogic LSP installation.

Message: `Existing package version is newer than that of the new package.`

Description: This message appears if the installer detects that you are attempting to install a LogLogic LSP version earlier than the version currently installed. See System and Permission Requirements before you start installation.

Message: `WARNING: Existing package version is the same version as the new package.`

Description: The installer exits after comparing its build number with the version of LogLogic LSP that is currently installed.

Message:

```
WARN 2019-09-20 02:42:11,583 c.l.l.c.l.EnableLmiCollection -
[MANAGER - lspc ] - Unable to discover HA mode due to
org.codehaus.plexus.util.cli.CommandLineException: Error executing
/bin/sh -c
'/loglogic/tomcat/webapps/logapp20/WEB-INF/cgi/rtstatus'
```

Description: In LogLogic LSP 35.0.0 or later, sometimes this message might be entered in `/loglogic/logsource/collector/logs/collectors.log` in any of the following scenarios:

- If `mtask` restarts after installing LogLogic LSP
- If you reinstall LogLogic LSP

If you see this error, perform the following steps:

1. Run the following command to check if `llcollector` is running:
   `/loglogic/logsource/collector/bin/LLCollectors status`
2. If `llcollector` is not running, run the following command to restart `llcollector`:

   `/loglogic/logsource/collector/bin/LLCollectors start`

Message: `Error stopping collector framework: installation will continue.`

Description: The installer is attempting to stop the LogLogic LSP Collector Framework (LLCollectors). To manually stop this process, run the following command:

`/loglogic/logsource/collector/bin/LLCollectors stop`

Upgrade scenarios

Message: `Current Installed LSP is not supported by upgrade. For details, see the Troubleshooting section in the Installation and Upgrade Guide.`

Description: LogLogic LSP can be installed only on certain LogLogic LMI versions. For a list of compatible versions, see System and Permission Requirements.

Further, if you are upgrading from an older version of LogLogic LSP, you must sequentially install from your current version up to LogLogic LSP version 36.0.0. You can skip at the most one version at a time for each upgrade in the sequence. For installation and upgrade instructions, see Installing the Package.

TIBCO Product Documentation and Support Services

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

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

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.

Legal and Third-Party Notices