TIBCO LogLogic® Log Management Intelligence
TIBCO LogLogic® Enterprise Virtual Appliance

Security Guidelines

Software Release 6.3
July 2019

TIBCO®

Important Information

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

ANY SOFTWARE ITEM IDENTIFIED AS THIRD PARTY LIBRARY IS AVAILABLE UNDER SEPARATE SOFTWARE LICENSE TERMS AND IS NOT PART OF A TIBCO PRODUCT. AS SUCH, THESE SOFTWARE ITEMS ARE NOT COVERED BY THE TERMS OF YOUR AGREEMENT WITH TIBCO, INCLUDING ANY TERMS CONCERNING SUPPORT, MAINTENANCE, WARRANTIES, AND INDEMNITIES. DOWNLOAD AND USE OF THESE ITEMS IS SOLELY AT YOUR OWN DISCRETION AND SUBJECT TO THE LICENSE TERMS APPLICABLE TO THEM. BY PROCEEDING TO DOWNLOAD, INSTALL OR USE ANY OF THESE ITEMS, YOU ACKNOWLEDGE THE FOREGOING DISTINCTIONS BETWEEN THESE ITEMS AND TIBCO PRODUCTS.

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 TIBCO Software Inc.

TIBCO, the TIBCO logo, the TIBCO O logo, TIB, Information Bus, Rendezvous, and TIBCO Rendezvous are either registered trademarks or trademarks of TIBCO Software 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.

This 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. Please see the readme.txt file for the availability of this software version on a specific operating system platform.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

This and other products of TIBCO Software Inc. may be covered by registered patents. Please refer to TIBCO's Virtual Patent Marking document (https://www.tibco.com/patents) for details.

Copyright © 2002-2019. TIBCO Software Inc. All Rights Reserved.

Contents

TIBCO Documentation and Support Services

How to Access TIBCO 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.

Product-Specific Documentation

The following documents for TIBCO LogLogic® Log Management Intelligence and TIBCO LogLogic® Enterprise Virtual Appliance can be found on the TIBCO Documentation site on the TIBCO LogLogic® documentation page:

- *TIBCO LogLogic® Log Management Intelligence Release Notes*
- *TIBCO LogLogic® Log Management Intelligence Administration Guide*
- *TIBCO LogLogic® Log Management Intelligence Configuration and Upgrade Guide*
- *TIBCO LogLogic® Log Management Intelligence Enterprise Virtual Appliance Quick Start Guide*
- *TIBCO LogLogic® Log Management Intelligence Hardware Installation Guide*
- *TIBCO LogLogic® Log Management Intelligence Log Source Report Mapping Guide*
- *TIBCO LogLogic® Log Management Intelligence Security Guidelines*
- *TIBCO LogLogic® Log Management Intelligence SSD Hardware Field Installation Guide*
- *TIBCO LogLogic® Log Management Intelligence Syslog Alert Message Format Quick Reference Guide*
- *TIBCO LogLogic® Log Management Intelligence User Guide*
- *TIBCO LogLogic® Log Management Intelligence Web Services API Implementation Guide*
- *TIBCO LogLogic® Log Management Intelligence XML Import/Export Entities Reference Guide*

The following documents for TIBCO LogLogic® Log Source Packages are available on the eDelivery website (https://edelivery.tibco.com) or TIBCO Support site (https://support.tibco.com) after logging in.

- *TIBCO LogLogic® Log Source Packages Release Notes*
- *TIBCO LogLogic® Log Source Packages Log Configuration Guides*

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit http://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.

Introduction

This document describes guidelines to ensure security within various components of TIBCO LogLogic® Log Management Intelligence (LMI) and the channels of communication between them. It also provides additional security-related guidance and recommendations for other aspects of external communication. In particular, this document provides details of product connectivity and configuration of security options.

Secure Communication Channels

LogLogic® LMI is a self-contained appliance and is available as physical hardware or as a virtual appliance. Access is limited to a few areas. Most communication with LogLogic LMI is limited to data center services.

Data Ingest and Ingress

Ingest and ingress of data into the LogLogic LMI application is limited to the following modes:

- Web GUI
- REST API
- Web Services API
- SSH
- Collectors
- (For hardware appliances only) Integrated Dell Remote Access Controller (iDRAC): The physical hardware of the LogLogic LMI appliance provides easy and secure hardware-based administrative access through iDRAC. iDRAC is secured over HTTPS and enables you to perform administrative tasks easily from a browser. Through iDRAC, you can perform all hardware operations and locally access the LogLogic LMI operating system. For more information, see Dell iDRAC.

Data Egress

Data can be sent out from LogLogic LMI in the following ways:

- Forwarder: LLTCP (used to send data to other LogLogic LMI appliances), Syslog TCP/UDP
- Alerts: SMTP, SNMP traps

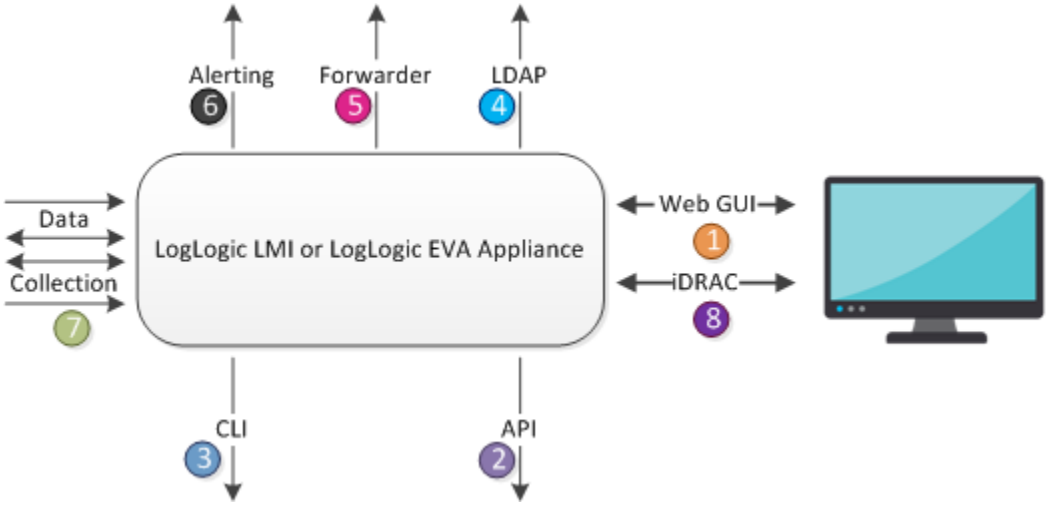
Communication Channels and Their Security Configurations

By default, some communication channels are not secure, but they can be secured by configuring the channels to use the Secure Sockets Layer (SSL) or Transfer Layer Security (TLS) protocol. For information about how to configure a component for secure communication, see the *TIBCO LogLogic® Log Management Intelligence Administration Guide*.

For configuration information about specific collectors, see the following documentation, which is available on the eDelivery website or TIBCO Support site after logging in:

- *TIBCO LogLogic® Log Source Packages Log Configuration Guides*
- *TIBCO LogLogic® Log Source Packages Log Source Packages Collector Guides*

The following diagram illustrates the components and communication protocols in a typical LogLogic LMI setup.



The following table describes the communication channels that can be configured, along with the references to more information, if applicable.

Key	Communication Channels	Connection	Description and References
1	Web GUI	HTTPS	User Interface
2	API • Web Services API • RESTful	HTTPS	OpenAPI
3	CLI	SSH	Administration console
4	LDAP authentication	LDAP/S	User authentication
5	Forwarders • Syslog • LLTCP	• Syslog: UDP or TCP • LLTCP: TCP-TLS	Data forwarding
6	Alerting • SNMP • SMTP	• SNMP: UDP or TCP • SMTP: TCP	Alerting TCP offers TLS/SSL support. For more information, see the *TIBCO LogLogic® Log Management Intelligence Administration Guide*.

Key	Communication Channels	Connection	Description and References
7	Data collection • JDBC • File • API • LogLogic proprietary • Syslog • Others	• JDBC: – (! ¥) MySQL – (! ¥) Microsoft SQL – (! ¥) Oracle – Sybase • File – SCP, SFTP – FTP, FTPS – HTTP, HTTPS – CIFS • API – (! ¥) VMware vCenter – (! ¥) Cisco SourceFire Defense Center – TIBCO Enterprise Message Service™ – (! ¥) Apache Kafka – Check Point – HDFS, Amazon S3 • TIBCO LogLogic proprietory: (!) ULDP, (!) LLTCP • Syslog: UDP, TCP • Others: NetFlow, (!) SNMP	Log and event collection (!) Offers TLS/SSL support (¥) For more information, see the *TIBCO LogLogic® Log Source Packages Log Configuration Guides* for that log source, which is available on the eDelivery website or TIBCO Support site after logging in.
8	Dell iDRAC	HTTPS	Administrative access through iDRAC is available only on hardware appliance models.

Other Recommendations

This section provides some recommendations to secure other aspects of communication when using the LogLogic LMI application.

General Security Environment

LogLogic LMI users are considered trusted users. The operating system and browsers used for accessing the Web GUI must be properly maintained and secured according to security best practices. SSH access on the appliance is enabled by default to enable configuration and maintenance of the appliance. However, the shell and CLI user accounts are separate to enable clean separation of duties. Thus, the shell account must be treated as a super-user account whose password is heavily guarded and seldom used. A proper X509 certificate, signed by a CA that is recognized by the browsers used, must be installed in place of the default certificate from the initial setup.

Selection of passwords

Specify a strong password for the LogLogic LMI administrator accounts (super user and root user), as these users perform all the critical operations. If the administrator account password is hacked, it can lead to damage or destabilization of the enterprise. The password should ideally consist of a minimum of eight characters, with a mix of uppercase and lowercase characters, numbers, and special characters.

Data Center Placement

Security and data protection recommendations when deploying your data center on-premises or on the cloud are as follows:

On-premises

While following security best practices, when deploying your LogLogic LMI to the data center, it is recommended that you place LogLogic LMI behind a firewall and other security devices. This adds extra layers of security in protecting your data, the appliance is protected by a layer of network security, and each port in use has access control lists (ACLs) that restrict access to the least range of IPs.

On the Cloud

Just as with an on-premises deployment, when deploying your LogLogic LMI to the virtual data center, it is recommended that you place LogLogic LMI behind a firewall and other security services. Running your LogLogic LMI in the same vPC as your core services provides not only additional protection, but also better performance for data collection. The appliance is protected by a layer of network security, and each port in use has ACLs that restrict access to the least range of IPs.

Backups

Backups must be exported to a secure location or put off-line and rotated to ensure quick recovery in case of failure. This also maintains a history on items such as data file checksums, which ensures that the files are not tampered in case of any suspicion.