TIBCO® Gemini – Powered by Apache Cassandra®

Installation

Version 4.1.5 | June 2024

Contents

About this Product

TIBCO announces the release of TIBCO® Gemini - Powered by Apache Cassandra® version 4.1.5.

Apache Cassandra is an open source, distributed database published by the Apache Foundation (see cassandra.apache.org). Known for its linear scalability and high availability, it provides high performance and maintains redundant, fault tolerant copies of data using an eventually consistent model. To learn more about TIBCO products, visit us at www.tibco.com.

As Apache Cassandra is often used with mission-critical data, understanding and implementing the available security features is crucial. For more information about these features and TIBCO's commitment to security, see TIBCO's Security Priority section in the TIBCO® Gemini - Powered by Apache Cassandra® *Installation*.

Preparing for Installation

Perform the following steps before you begin the installation process:

Procedure
1. Verify that the product is compatible with your platform and version from the Readme file for version 4.1.5.

2. For more information about the permissions required for installation, see Guidelines.

3. See Requirements to verify that the host computer satisfies the requirements for installation, and the prerequisite software is already installed.

Default Log Location

By default, log files are stored in the `/opt/tibco/acd/core/logs/` directory.

Default Data Location

By default, data files are stored in the `/opt/tibco/acd/core/data/` directory.

Requirements

Before running the installers, ensure that the following requirements are met and you have appropriate permissions to run the installers.

Required Software

Java version 8 or 11 is required to run Apache Cassandra 4.1.5.

Installer Account

Platform	Account Privileges
Linux	For system-based installers, you need sudo permission for installation. To extract the TAR files, no special permissions are required.

Platform-Specific Instructions

Before using the installer, read the guidelines for your operating system platform.

Guidelines for Linux

Installer Privileges

To install this product, you must have `sudo` privileges.

Installation Packages

Apache Cassandra is available for 64-bit Linux operating systems (Intel x86_64). For the latest changes, see the Readme file for version 4.1.5.

The Linux installer package filename is `TIB_acd-core_4.1.5_linux_x86_64.zip`.

Installation

You can install this product by using platform-native installers.

Installing on Linux

Use the platform-native installer to install the product on Linux platforms. The package provides a collection of RPM, DEB, and TAR files.

Before you begin

On SUSE Linux, ensure that the `libjvm` library is already installed.

Procedure

1. Download the installation package.

   ```
   TIB_acd_4.1.5_linux_x86_64.zip
   ```

2. Change the directory to the download directory or move the file to a preferred extraction location and extract the Apache Cassandra archive files.

   ```
   unzip TIB_acd_4.1.5_linux_x86_64.zip
   ```

   This command creates a directory `TIB_acd_4.1.5`, and places the RPM, DEB, and TAR installation archives in that directory.

3. Change the directory to the installation directory.

   ```
   cd TIB_acd_4.1.5
   ```

4. Depending on the Linux variant, install using one of the following commands.

Linux Variant	Command
Red Hat, CentOS	`yum install -y rpm/*.rpm`
Debian, Ubuntu, Fedora	`dpkg -i deb/*.deb`
SUSE	`zypper install rpm/*.rpm` **Note:** If you encounter issues with dependencies, you can safely ignore those dependencies and proceed with the installation.

Other Linux variants	If your Linux variant does not include `yum`, `dpkg`, or `zypper`, you can use `TAR` as follows:
	
	a. Create the /tmp/tib-acd-installation/ directory.
	
	`mkdir -p /tmp/tib-acd-installation/`
	
	Note: You can use different directories to install different versions of the product simultaneously.
	
	b. Copy the tar files into this directory.
	
	`cp tar/* /tmp/tib-acd-installation`
	
	c. Change directory to the copied directory and run the following:
	
	`cd /tmp/tib-acd-installation`
	`for f in *; do tar xvf $f; done`
	
	d. Move the extracted files to /opt/tibco/acd/.

Linux Variant	Command
| | ```
sudo mkdir -p /opt/tibco/acd/
sudo cp -R TIB_ACD_4.1.5/* /opt/tibco/acd
``` |
| | e. To create symlinks in `/var/lib/cassandra` and `/var/log/cassandra`, use the `post_install.sh` script from the `TIB_acd_4.1.5_linux_x86_64-extras.tar.gz` package. |

The installation utilities `yum`, `dpkg`, or `zypper` install Apache Cassandra in the `/opt/tibco/` directory.

The archive utility `TAR` installs the software that is then moved to the `/opt/tibco/` directory.

Installing on Linux in Silent Mode

To install Apache Cassandra on Linux platforms silently, perform the following steps.

Procedure

1. Download the installation package.

   ```
   TIB_acd_4.1.5_linux_x86_64.zip
   ```

2. Change the director to the download directory or move the package file to a preferred extraction location and extract the Apache Cassandra archive files.

   ```
   unzip TIB_acd_4.1.5_linux_x86_64.zip
   ```

   This command creates a directory `TIB_acd_4.1.5`, and places the installation RPM, DEB, and TAR archive files in that directory.

3. Change the directory to the installation directory.

   ```
   cd TIB_acd_4.1.5
   ```

4. Install using one of these commands, depending on the Linux platform variant.

Linux Variant	Command
Red Hat, CentOS	`yum install -q -y rpm/*.rpm > /dev/null 2>&1`
Debian, Ubuntu, Fedora	`dpkg -i deb/*.deb > /dev/null 2>&1`
SUSE	`zypper in -y --allow-unsigned-rpm rpm/*.rpm > /dev/null 2>&1`

The installation utilities `yum`, `dpkg`, or `zypper` install the software under `/opt/tibco/`.

Uninstallation

You can uninstall this product by performing operating system-specific steps.

Uninstalling on Linux

Procedure

1. To list the packages to uninstall, run the command that is applicable to your Linux variant.

Linux Variant	Command
Red Hat	```yum list installed	grep "tib_acd"```
Debian	```dpkg-query -l	grep "tib_acd"```
SUSE	```zypper se	grep "tib_acd"```
Other Linux variants	If your Linux variant does not include `yum`, `dpkg`, or `zypper`, use the following command. ```ls -R /opt/tibco/acd```

2. To uninstall the packages, run the command that is applicable to your Linux variant.

Linux Variant	Command
Red Hat	`yum remove -y tib_acd*`
Debian	`apt-get remove -y tib_acd*`
SUSE	`zypper rm tib_acd*`
Other Linux variants	If your Linux variant does not include `yum`, `dpkg`, or `zypper`, use this command. `rm -rf /opt/tibco/acd`

TIBCO's Security Priority

At TIBCO, security is our highest priority. TIBCO maintains a company-wide information security management system and control program that include security policies, standards, and procedures based on ISO/IEC 27001:2013.

TIBCO incorporates the STRIDE model to help analyze and find threats to ensure system and service integrity and reliability in processes, data stores, data flows, and trust boundaries. Our approaches ensure that applications and systems fulfill the CIA triad (confidentiality, integrity, and availability).

Threat	TIBCO Assurance
Spoofing identity	Authenticity - authentication
Tampering with data	Integrity and auditing
Repudiation threats	Non-repudiability
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

TIBCO adheres to privacy and security requirements related to the protection and processing of individual personal data (collectively, the "Protected Data"). For more information, see Customer Privacy and Security Statement.

TIBCO has adopted policies and practices in alignment with industry best-practices, including quickly addressing and disclosing vulnerabilities. TIBCO has an incident response policy and plan. The policy ensures that security incidents are identified, contained, investigated, and remedied. For more information or to report a potential security issue, see Security@TIBCO.

TIBCO has policies that guide our software development lifecycle (SDLC). They include peer reviews, static code analysis, and both manual and automated QA processes. In addition, we routinely run performance testing on any new or updated software to ensure the

highest quality. There is a clear division between devops and development. All changes are logged in our source code repository. We use standard deployment tools. Our iterative methodology ensures a functional view of the processes, milestones, activities, and artifacts, or records.

TIBCO's Business Continuity Plan (BCP)

TIBCO has a Business Continuity Plan (BCP) to ensure the effects of an emergency event are minimized. If a disaster or emergency situation occurs, the Support Emergency Team (SEMT) coordinates the recovery effort and uses the Employee Communication Chains to notify staff that the BCP is activated.

TIBCO has an Information Security Management System (ISMS) to preserve the confidentiality, integrity, and availability of information. Information security is considered in the design of processes, information systems, and controls.

TIBCO's Quality Management System (QMS) is based on ISO 9001, which is an internationally recognized standard that sets out the criteria for a quality management system incorporating the Plan-Do-Check-Act (PDCA) cycle. TIBCO's QMS is a formalized system of business processes, procedures, and responsibilities focused on:

- Customer Excellence - Meeting customer requirements and enhancing customer satisfaction by providing high-quality products and services.

- Quality - Meeting TIBCO requirements for quality policies and objectives with measurable goals.

TIBCO's Quality Management System is documented and structured in levels.

Product Security

At TIBCO, security is our highest priority. You can be sure that TIBCO software is secure based on our own high standards and the best practices of our infrastructure providers.

TIBCO® Gemini - Powered by Apache Cassandra® offers logging, transport security, authentication and authorization, and compatibility with other products.

This section is useful to security officers, deployers, administrators, and purchasers.

Security Features

Apache Cassandra® can be configured with the following security features and boundaries:

- TLS/SSL encryption for client and inter-node communication

- Client authentication

- Authorization

- Logging
  Apache Cassandra logs key activities
  (https://cassandra.apache.org/doc/stable/cassandra/operating/auditlogging.html).
  The security of log data requires an unbroken chain of secure connections. Your
  organization is responsible for protecting and reviewing logging files.

For more information about security, see the Apache Cassandra® Documentation.

TIBCO Documentation and Support Services

For information about this product, you can read the documentation, contact 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® Gemini - Powered by Apache Cassandra® Documentation page.

How to Access Related Third-Party Documentation

When working with TIBCO® Gemini - Powered by Apache Cassandra®, you may find it useful to read the Apache Cassandra Documentation.

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 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, and the TIBCO O logo 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.

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. CLOUD SG MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S), THE PROGRAM(S), AND/OR THE SERVICES DESCRIBED IN THIS DOCUMENT AT ANY TIME WITHOUT NOTICE.

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 "README" FILES.

This and other products of Cloud SG may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal.