



Amazon ODBC Driver for Impala

Installation and Configuration Guide

September 8, 2014

Amazon Web Services, Inc.



Copyright © 2014 Amazon Web Services, Inc. All Rights Reserved.

Information in this document is subject to change without notice. Companies, names and data used in examples herein are fictitious unless otherwise noted. No part of this publication, or the software it describes, may be reproduced, transmitted, transcribed, stored in a retrieval system, decompiled, disassembled, reverse-engineered, or translated into any language in any form by any means for any purpose without the express written permission of Amazon Web Services, Inc.

Parts of this Program and Documentation include proprietary software and content that is copyrighted and licensed by Simba Technologies Incorporated. This proprietary software and content may include one or more feature, functionality or methodology within the ODBC, JDBC, ADO.NET, OLE DB, ODBO, XMLA, SQL and/or MDX component(s).

For information about Simba's products and services, visit: www.simba.com.

Trademarks

Simba, the Simba logo, SimbaEngine, SimbaEngine C/S, SimbaExpress and SimbaLib are registered trademarks of Simba Technologies Inc. All other trademarks and/or servicemarks are the property of their respective owners.

Cyrus SASL

Copyright (c) 1998-2003 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any other legal details, please contact

Office of Technology Transfer
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213-3890
(412) 268-4387, fax: (412) 268-7395
tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by Computing Services at Carnegie Mellon University (<http://www.cmu.edu/computing/>)."

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

ICU License - ICU 1.8.1 and later

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1995-2010 International Business Machines Corporation and others. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

OpenSSL

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Apache Hive

Copyright 2008-2011 The Apache Software Foundation.

Apache Thrift

Copyright 2006-2010 The Apache Software Foundation.

Expat

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the ""Software""), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND

NO INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Impala

Copyright 2012 Cloudera Inc.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at:

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Contact Us

Customers should check the EMR Forum:

<https://forums.aws.amazon.com/forum.jspa?forumID=52>

Or open a support case using the AWS Support Center:

<https://aws.amazon.com/support>

Table of Contents

Introduction	8
Windows Driver	8
System Requirements	8
Installing the Driver.....	9
Configuring ODBC Connections	9
Configuring Authentication	11
Using No Authentication	11
Using Kerberos.....	11
Using User Name	12
Using User Name and Password.....	12
Using User Name and Password (SSL).....	12
No Authentication (SSL)	13
Linux Driver	14
System Requirements	14
Installation	14
Setting the LD_LIBRARY_PATH Environment Variable.....	15
Mac OS X Driver	15
System Requirements	15
Installation	16
Setting the DYLD_LIBRARY_PATH Environment Variable.....	16
AIX Driver.....	16
System Requirements	16
Installation	17
Setting the LD_LIBRARY_PATH Environment Variable	17
Configuring ODBC Connections for Linux, Mac OS X and AIX.....	18
Files	18
Sample Files	18
Configuring the Environment	18
Configuring the odbc.ini File	19
Configuring the odbcinst.ini File.....	20
Configuring the amazon.impalaodbc.ini File	21
Configuring Authentication	22
Using No Authentication	22
Using Kerberos.....	22
Using User Name	22

Using User Name and Password	23
Using User Name and Password (SSL)	23
No Authentication (SSL)	23
Features	24
Data Types	24
Catalog and Schema Support	24
SQL Translation	25
Active Directory	25
Contact Us	25
Appendix A: Configuring Kerberos Authentication for Windows	26
Active Directory	26
MIT Kerberos	26
Downloading and installing MIT Kerberos for Windows 4.0.1	26
Setting up the Kerberos Configuration File	26
Setting up the Kerberos Credential Cache File	27
Obtaining a Ticket for a Kerberos Principal	28
Appendix B: Driver Configuration Options for Linux and Mac OS X	30

Introduction

Welcome to the Amazon ODBC Driver for Impala. ODBC is one the most established and widely supported APIs for connecting to and working with databases. At the heart of the technology is the ODBC driver, which connects an application to the database.

Amazon ODBC Driver for Impala is used for direct SQL and Impala SQL access to Apache Hadoop / Impala distributions, enabling Business Intelligence (BI), analytics and reporting on Hadoop / Impala-based data. The driver efficiently transforms an application's SQL query into the equivalent form in Impala SQL. Impala SQL is a subset of SQL-92. If an application is Impala-aware, then the driver is configurable to pass the query through. The driver interrogates Impala to obtain schema information to present to a SQL-based application. Queries, including joins, are translated from SQL to Impala SQL. For more information about the differences between Impala SQL and SQL, refer to the section "Features" on page 24.

Amazon ODBC Driver for Impala is available for Microsoft Windows, Linux and Mac OS X. It complies with the ODBC 3.52 data standard and adds important functionality such as Unicode and 32- and 64-bit support for high-performance computing environments on all platforms. Any version of the ODBC driver will connect to an Impala server irrespective of the server's host OS.

The *Amazon ODBC Driver for Impala Installation and Configuration Guide* is suitable for users who are looking to access data residing within Impala from their desktop environment. Application developers may also find the information helpful. Refer to your application for details on connecting via ODBC.

Windows Driver

System Requirements

You install Amazon ODBC Driver for Impala on client computers accessing data in a Hadoop cluster with the Impala server installed and running. Each computer where you install the driver must meet the following minimum system requirements:

- One of the following operating systems (32- and 64-bit editions are supported):
 - o Windows® XP with SP3
 - o Windows® Vista
 - o Windows® 7 Professional
 - o Windows® Server 2008 R2
- 25 MB of available disk space

The driver has been tested using Impala 1.0.1 and Apache Thrift 0.9.0

Important: To install the driver, you need Administrator privileges on the computer.

Installing the Driver

On 64-bit Windows operating systems, you can execute 32- and 64-bit applications transparently. You must use the version of the driver matching the bitness of the client application accessing data in Hadoop / Impala:

- **AmazonImpalaODBC32.msi** for 32-bit applications
- **AmazonImpalaODBC64.msi** for 64-bit applications

You can install both versions of the driver on the same computer.

Note: For an explanation of how to use ODBC on 64-bit editions of Windows, see <http://www.simba.com/wp-content/uploads/2010/10/HOW-TO-32-bit-vs-64-bit-ODBC-Data-Source-Administrator.pdf>

To install Amazon ODBC Driver for Impala:

1. Depending on the bitness of your client application, double-click to run **AmazonImpalaODBC32.msi** or **AmazonImpalaODBC64.msi**
2. Click **Next**
3. Select the check box to accept the terms of the License Agreement if you agree, and then click **Next**
4. To change the installation location, click the **Change** button, then browse to the desired folder, and then click **OK**. To accept the installation location, click **Next**
5. Click **Install**
6. When the installation completes, click **Finish**
7. If you received a license file via e-mail, then copy the license file into the \lib subfolder in the installation folder you selected in step 4.

Configuring ODBC Connections

To create a Data Source Name (DSN):

1. Click the **Start** button , then click **All Programs**, and then click the **Amazon ODBC Driver for Impala 2.5 (64-bit)** or the **Amazon ODBC Driver for Impala 2.5 (32-bit)** program group.
Note: If you installed both versions of the driver, you will see two program groups. Because DSNs are bit-specific, select the version that matches the bitness of your application. For example, a DSN that is defined for the 32-bit driver will only be accessible from 32-bit applications.
2. Click **64-bit ODBC Administrator** or **32-bit ODBC Administrator**. The ODBC Data Source Administrator window opens.
3. Click the **Drivers** tab and verify that the Amazon ODBC Driver for Impala appears in the list of ODBC drivers that are installed on your system.
4. Click the **System DSN** tab to create a system DSN or click the **User DSN** tab to create a user DSN.

Note: A system DSN can be seen by all users that login to a workstation. A user DSN is specific to a user on the workstation. It can only be seen by the user who creates it.

5. Click **Add**. The Create New Data Source window opens.
6. Select **Amazon ODBC Driver for Impala** and then click **Finish**. The Amazon ODBC Driver for Impala DSN Setup dialog opens.
7. In the Data Source Name field, type a name for your DSN.
8. Optionally, type relevant details related to the DSN in the Description field.
9. In the Host text box, type the IP address or hostname of the Impala server.
10. In the Port text box, type the listening port for the service.
11. Optionally, configure authentication. For detailed instructions, refer to the section "Configuring Authentication" on page 11.
12. Optionally, click **Advanced Options**. In the Advanced Options window:
 - a) Select the Use Native Query checkbox to disable translating ODBC SQL to Impala SQL.

Note: By default, the driver applies transformations to the queries emitted by an application to convert the queries into an equivalent form in Impala SQL. If the application is Impala aware and already emits Impala SQL, then turning off the translation avoids the additional overhead of query transformation.
 - b) In the Rows Fetched Per Block field, type the number of rows to be fetched per block.

Note: Any positive 32-bit integer is a valid value but testing has shown that performance gains are marginal beyond the default value of 10000 rows.
 - c) In the Socket Timeout field, type the number of seconds after which Impala closes the connection with the client application if the connection is idle.

Note: Setting the Socket Timeout value to 0 disables the timeout feature.
 - d) To allow the common name of a CA-issued SSL certificate to mismatch the hostname of the Impala server, select the Allow Common Name Hostname Mismatch checkbox.

Note: The setting only applies to the User Name and Password (SSL) and No Authentication (SSL) authentication mechanisms. Other authentication mechanisms ignore the setting.
 - e) Enter the path of the file containing the trusted certificates (for example, the certificate from the Impala server) in the Trusted Certificates edit box to configure the driver to load the certificates from the specified file to authenticate the Impala server when using SSL.

Note: The setting only applies to the User Name and Password (SSL) and No Authentication (SSL) authentication mechanisms. Other authentication mechanisms ignore the setting. SSL certificates in the trusted certificates

file must be in PEM format. If the setting is not set, then the driver defaults to using the trusted CA certificates PEM file installed by the driver.

f) Click **OK**

13. Optionally, if the operations against Impala are to be done on behalf of a user that is different than the authenticated user for the connection, enter the user name of the user to be delegated in the Delegation UID text box.
14. Click **Test** to test the connection. Review the results of testing the connection as needed, and then click **OK** in the Test Results dialog.
15. In the Amazon ODBC Driver for Impala DSN Setup dialog, click **OK**

Configuring Authentication

Impala Server supports multiple authentication mechanisms. You must determine the authentication type your server is using and configure your DSN accordingly. The authentication methods available are as follows:

- No Authentication
- Kerberos
- User Name
- User Name and Password
- User Name and Password (SSL)
- No Authentication (SSL)

Using No Authentication

For this authentication mechanism, you do not need to configure any additional settings.

To configure your DSN for connections that do not require authentication:

- In the Amazon ODBC Driver for Impala DSN Setup dialog, click the drop-down arrow next to the **Mechanism** field, and then select **No Authentication**

Using Kerberos

Kerberos must be configured before you can use this authentication mechanism. For details, see “Appendix A: Configuring Kerberos Authentication for Windows” on page 26. After Kerberos is installed and configured, configure your DSN to use Kerberos authentication.

To configure your DSN to use Kerberos authentication:

1. In the Amazon ODBC Driver for Impala DSN Setup dialog, click the drop-down arrow next to the **Mechanism** field, and then select **Kerberos**
2. If your Kerberos setup does not define a default realm or if the realm of your Impala server is not the default, then type the Kerberos realm of the Impala server host in the **Realm** field. Otherwise, leave the field blank.
3. In the **Host FQDN** field, type the fully qualified domain name of the Impala host.

4. In the **Service Name** field, type the service name of the Impala server.
For example, if the principle for the Impala server is `impala/fully.qualified.domain.name@your-realm.com`, then the value in the service name field is `impala`. If you are unsure of the correct service name to use for your particular Hadoop deployment, contact your Hadoop administrator.
5. In the **Transport Buffer Size** field, type the number of bytes to reserve in memory for buffering unencrypted data from the network.

Note: In most circumstances, the default value of 1000 bytes is optimal.

Using User Name

This authentication mechanism requires a user name but not a password. The user name labels the session, facilitating database tracking.

To configure your DSN to use User Name authentication:

1. In the Amazon ODBC Driver for Impala DSN Setup dialog, click the drop-down arrow next to the **Mechanism** field, and then select **User Name**.
2. In the **User Name** field, type a user name that is recognized by the Impala server.
3. In the **Transport Buffer Size** field, type the number of bytes to reserve in memory for buffering unencrypted data from the network.

Note: In most circumstances, the default value of 1000 bytes is optimal.

Using User Name and Password

This authentication mechanism requires a user name and a password.

Note: This authentication mechanism should not be used with an Impala configuration that does not have LDAP enabled.

To configure your DSN for User Name and Password authentication:

1. In the Amazon ODBC Driver for Impala DSN Setup dialog, click the drop-down arrow next to the **Mechanism** field, and then select **User Name and Password**.
2. In the **User Name** field, type a user name that is recognized by the Impala server.
3. In the **Password** field, type the password corresponding to the user name you typed in step 2.

Using User Name and Password (SSL)

This authentication mechanism uses SSL and requires a user name and a password. The driver accepts self-signed SSL certificates.

Note: This authentication mechanism should not be used with an Impala configuration that does not have LDAP enabled.

To configure User Name and Password (SSL) authentication:

1. In the Amazon ODBC Driver for Impala DSN Setup dialog, click the drop-down arrow next to the **Mechanism** field, and then select **User Name and Password (SSL)**
2. In the **User Name** field, type a user name that is recognized by the Impala server.
3. In the **Password** field, type the password corresponding to the user name you typed in step 2.
4. Optionally, configure the driver to allow a mismatch between the common name of a CA-issued certificate and the host name of the Impala server by clicking **Advanced Options** and selecting the **Allow Common Name Host Name Mismatch** check box.

Note: For self-signed certificates, the driver always allows the common name of the certificate to not match the host name.

5. Optionally, configure the driver to load SSL certificates from a specific file by clicking **Advanced Options** and typing the path to the file in the Trusted Certificates field.

Note: BY default, the driver uses the trusted CA certificates PEM file that is installed with the driver.

No Authentication (SSL)

This authentication mechanism uses SSL but does not require a user name or a password. The driver accepts self-signed SSL certificates.

To configure your DSN to use No Authentication (SSL) authentication:

1. In the Amazon ODBC Driver for Impala DSN Setup dialog, click the drop-down arrow next to the **Mechanism** field, and then select **No Authentication (SSL)**
2. Optionally, configure the driver to allow a mismatch between the common name of a CA-issued certificate and the host name of the Impala server by clicking **Advanced Options** and selecting the **Allow Common Name Host Name Mismatch** check box.

Note: For self-signed certificates, the driver always allows the common name of the certificate to not match the host name.

3. Optionally, configure the driver to load SSL certificates from a specific file by clicking **Advanced Options** and typing the path to the file in the Trusted Certificates field.

Note: BY default, the driver uses the trusted CA certificates PEM file that is installed with the driver.

Linux Driver

System Requirements

- One of the following distributions (32- and 64-bit editions are supported):
 - o Red Hat® Enterprise Linux® (RHEL) 5.0/6.0
 - o CentOS 5.0/6.0
 - o SUSE Linux Enterprise Server (SLES) 11
- 50 MB of available disk space.
- One of the following ODBC driver managers installed:
 - o iODBC 3.52.7 or above
 - o unixODBC 2.3.0 or above

Amazon ODBC Driver for Impala requires a Hadoop cluster with the Impala server installed and running.

Amazon ODBC Driver for Impala has been tested using Impala 1.0.1 and Apache Thrift 0.9.0

Installation

There are two versions of the driver for Linux:

- **AmazonImpalaODBC-32-bit-BuildNumber-ReleaseNumber.i686.rpm** for 32-bit
- **AmazonImpalaODBC-BuildNumber-ReleaseNumber.x86_64.rpm** for 64-bit

The version of the driver that you select should match the bitness of the client application accessing your Hadoop / Impala-based data. For example, if the client application is 64-bit, then you should install the 64-bit driver. Note that 64-bit editions of Linux support both 32- and 64-bit applications. Verify the bitness of your intended application and install the appropriate version of the driver.

Amazon ODBC Driver for Impala driver files are installed in the following directories:

- `/opt/amazon/impalaodbc/ErrorMessage`s – Error messages files directory
- `/opt/amazon/impalaodbc/Setup` – Sample configuration files directory
- `/opt/amazon/impalaodbc/lib/32` – 32-bit shared libraries directory
- `/opt/amazon/impalaodbc/lib/64` – 64-bit shared libraries directory

To install Amazon ODBC Driver for Impala:

1. In Red Hat Enterprise Linux 5.0/6.0 or CentOS 5.0/6.0, log in as the root user, then navigate to the folder containing the driver RPM packages to install, and then type the following at the command line, where *RPMFileName* is the file name of the RPM package containing the version of the driver that you want to install:

```
yum localinstall --nogpgcheck RPMFileName
```

OR

In SUSE Linux Enterprise Server 11, log in as the root user, then navigate to the folder containing the driver RPM packages to install, and then type the following at the command line, where *RPMFileName* is the file name of the RPM package containing the version of the driver that you want to install:

```
zypper install RPMFileName
```

2. If you received a license file via e-mail, then copy the license file into the `/opt/amazon/impalaodbc/lib/32` or `/opt/amazon/impalaodbc/lib/64` folder, depending on the version of the driver that you installed.

Amazon ODBC Driver for Impala depends on the following resources:

- `cyrus-sasl-2.1.22-7` or above
- `cyrus-sasl-gssapi-2.1.22-7` or above
- `cyrus-sasl-plain-2.1.22-7` or above

If the package manager in your Linux distribution cannot resolve the dependencies automatically when installing the driver, then download and manually install the packages required by the version of the driver that you want to install.

Setting the LD_LIBRARY_PATH Environment Variable

The `LD_LIBRARY_PATH` environment variable must include the paths to the installed ODBC driver manager libraries.

Refer to your Linux shell documentation for details on how to set environment variables permanently.

For details on creating ODBC connections using Amazon ODBC Driver for Impala, see “Configuring ODBC Connections for Linux, Mac OS X and AIX” on page 18.

Mac OS X Driver

System Requirements

- Mac OS X version 10.6.8 or later
- 100 MB of available disk space
- iODBC 3.52.7 or above

Amazon ODBC Driver for Impala requires a Hadoop cluster with the Impala server installed and running.

Amazon ODBC Driver for Impala has been tested using Impala 1.0.1 and Apache Thrift 0.9.0

The driver supports both 32- and 64-bit client applications.

Installation

Amazon ODBC Driver for Impala driver files are installed in the following directories:

- /opt/amazon/impalaodbc/ErrorMessage – Error messages files directory
- /opt/amazon/impalaodbc/Setup – Sample configuration files directory
- /opt/amazon/impalaodbc/lib/universal – Binaries directory

To install Amazon ODBC Driver for Impala:

1. Double-click to mount the **AmazonImpalaODBC.dmg** disk image.
2. Double-click **AmazonImpalaODBC.pkg** to run the Installer.
3. Follow the instructions in the Installer to complete the installation process.
4. When the installation completes, click **Close**
5. If you received a license file via e-mail, then copy the license file into the /opt/amazon/impalaodbc/lib/universal folder.

Setting the DYLD_LIBRARY_PATH Environment Variable

The DYLD_LIBRARY_PATH environment variable must include the paths to the installed ODBC driver manager libraries.

Refer to your Mac OS X shell documentation for details on how to set environment variables permanently.

For details on creating ODBC connections using Amazon ODBC Driver for Impala, see “Configuring ODBC Connections for Linux, Mac OS X and AIX” on page 18.

AIX Driver

System Requirements

- IBM AIX 5.3, 6.1 or 7.1 (32- and 64-bit editions are supported)
- 150 MB of available disk space
- One of the following ODBC driver managers installed:
 - o iODBC 3.52.7 or above
 - o unixODBC 2.3.0 or above

Amazon ODBC Driver for Impala requires a Hadoop cluster with the Impala server installed and running.

Amazon ODBC Driver for Impala has been tested using Impala 1.0.1 and Apache Thrift 0.9.0

Installation

There are two versions of the driver for AIX:

- **AmazonImpalaODBC-32-bit-BuildNumber-ReleaseNumber.ppc.rpm** for 32-bit
- **AmazonImpalaODBC-BuildNumber-ReleaseNumber.ppc.rpm** for 64-bit

The version of the driver that you select should match the bitness of the client application accessing your Hadoop / Impala-based data. For example, if the client application is 64-bit, then you should install the 64-bit driver. Note that 64-bit editions of AIX support both 32- and 64-bit applications. Verify the bitness of your intended application and install the appropriate version of the driver.

Amazon ODBC Driver for Impala driver files are installed in the following directories:

- **/opt/amazon/impalaodbc/ErrorMessage**—Error messages files directory
- **/opt/amazon/impalaodbc/Setup**—Sample configuration files directory
- **/opt/amazon/impalaodbc/lib/32**—32-bit shared libraries directory
- **/opt/amazon/impalaodbc/lib/64**—64-bit shared libraries directory

To install Amazon ODBC Driver for Impala:

1. Log in as the root user, then navigate to the folder containing the driver RPM packages to install, and then type the following at the command line, where *RPMFileName* is the file name of the RPM package containing the version of the driver that you want to install:

```
rpm --install RPMFileName
```
2. If you received a license file via e-mail, then copy the license file into the `/opt/amazon/impalaodbc/lib/32` or `/opt/amazon/impalaodbc/lib/64` folder, depending on the version of the driver that you installed.

Setting the LD_LIBRARY_PATH Environment Variable

The LD_LIBRARY_PATH environment variable must include the path to the installed ODBC driver manager libraries.

For details on creating ODBC connections using Amazon ODBC Driver for Impala, see “Configuring ODBC Connections for Linux, Mac OS X and AIX” on page 18.

Configuring ODBC Connections for Linux, Mac OS X and AIX

Files

ODBC driver managers use configuration files to define and configure ODBC data sources and drivers. By default, the following configuration files residing in the user's home directory are used:

- **.odbc.ini** – The file used to define ODBC data sources (required)
- **.odbcinst.ini** – The file used to define ODBC drivers (optional)
- **.amazon.impalaodbc.ini** – The file used to configure Amazon ODBC Driver for Impala (required)

Sample Files

The driver installation contains the following sample configuration files in the Setup directory:

- **odbc.ini**
- **odbcinst.ini**
- **amazon.impalaodbc.ini**

The names of the sample configuration files do not begin with a period (.) so that they will appear in directory listings by default. A filename beginning with a period (.) is hidden. For `odbc.ini` and `odbcinst.ini`, if the default location is used, then the filenames must begin with a period (.). For `amazon.impalaodbc.ini`, the filename must begin with a period (.) and must reside in the user's home directory.

If the configuration files do not already exist in the user's home directory, then the sample configuration files can be copied to that directory and renamed. If the configuration files already exist in the user's home directory, then the sample configuration files should be used as a guide for modifying the existing configuration files.

Configuring the Environment

By default, the configuration files reside in the user's home directory. However, three environment variables—`ODBCINI`, `ODBCSYSINI` and `SIMBAINI`—can be used to specify different locations for the `odbc.ini`, `odbcinst.ini` and `amazon.impalaodbc.ini` configuration files. Set `ODBCINI` to point to your `odbc.ini` file. Set `ODBCSYSINI` to point to the directory containing the `odbcinst.ini` file. Set `SIMBAINI` to point to your `amazon.impalaodbc.ini` file. For example, if your `odbc.ini` and `amazon.impalaodbc.ini` files are located in `/etc` and your `odbcinst.ini` file is located in `/usr/local/odbc`, then set the environment variables as follows:

```
export ODBCINI=/etc/odbc.ini
export ODBCSYSINI=/usr/local/odbc
```

```
export SIMBAINI=/etc/amazon.impalaodbc.ini
```

The following search order is used to locate the amazon.impalaodbc.ini file:

1. If the SIMBAINI environment variable is defined, then the driver searches for the file specified by the environment variable.
Important: SIMBAINI must contain the full path, including the filename.
2. The current working directory of the application is searched for a file named amazon.impalaodbc.ini **not** beginning with a period.
3. The directory ~/ (that is, \$HOME) is searched for a hidden file named .amazon.impalaodbc.ini
4. The directory /etc is searched for a file named amazon.impalaodbc.ini **not** beginning with a period.

Configuring the odbc.ini File

ODBC Data Sources are defined in the odbc.ini configuration file. The file is divided into several sections:

- **[ODBC]** is optional and used to control global ODBC configuration, such as ODBC tracing.
- **[ODBC Data Sources]** is required, listing DSNs and associating DSNs with a driver.
- A section having the same name as the data source specified in the [ODBC Data Sources] section is required to configure the data source.

Here is an example odbc.ini configuration file for Linux or AIX:

```
[ODBC Data Sources]
Sample Amazon Impala DSN 32=Amazon Impala ODBC Driver 32-bit
[Sample Amazon Impala DSN 32]
Driver=/opt/amazon/impalaodbc/lib/32/libamazonimpalaodbc32.so
HOST=MyImpalaServer
PORT=21050
```

Here is an example odbc.ini configuration file for Mac OS X:

```
[ODBC Data Sources]
Sample Amazon Impala DSN=Amazon Impala ODBC Driver
[Sample Amazon Impala DSN]
Driver=/opt/amazon/impalaodbc/lib/universal/libamazonimpalaodbc.dylib
HOST=MyImpalaServer
PORT=21050
```

To create a data source:

1. Open the .odbc.ini configuration file in a text editor.
2. Add a new entry to the [ODBC Data Sources] section. Type the data source name (DSN) and the driver name.
3. To set configuration options, add a new section having a name matching the data source name (DSN) you specified in step 2. Specify configuration options as key-value pairs.
4. Save the .odbc.ini configuration file.

For details on configuration options available to control the behavior of DSNs using Amazon ODBC Driver for Impala, see “Appendix B: Driver Configuration Options” on page 30.

Configuring the odbcinst.ini File

ODBC Drivers are defined in the odbcinst.ini configuration file. The configuration file is optional because drivers can be specified directly in the odbc.ini configuration file, as described in “Configuring the odbc.ini File” on page 19.

The odbcinst.ini file is divided into the following sections:

- **[ODBC Drivers]** lists the names of all the installed ODBC drivers.
- A section having the same name as the driver name specified in the [ODBC Drivers] section lists driver attributes and values.

Here is an example odbcinst.ini file for Linux or AIX:

```
[ODBC Drivers]
Amazon Impala ODBC Driver 32-bit=Installed
Amazon Impala ODBC Driver 64-bit=Installed
[Amazon Impala ODBC Driver 32-bit]
Description= Amazon Impala ODBC Driver (32-bit)
Driver=/opt/amazon/impalaodbc/lib/32/libamazonimpalaodbc32.so
[Amazon Impala ODBC Driver 64-bit]
Description=Amazon Impala ODBC Driver (64-bit)
Driver=/opt/amazon/impalaodbc/lib/64/libamazonimpalaodbc64.so
```

Here is an example odbcinst.ini file for Mac OS X:

```
[ODBC Drivers]
Amazon Impala ODBC Driver=Installed
[Amazon Impala ODBC Driver]
Description=Amazon Impala ODBC Driver
Driver=/opt/amazon/impalaodbc/lib/universal/libamazonimpalaodbc.dylib
```

To define a driver:

1. Open the .odbcinst.ini configuration file in a text editor.
2. Add a new entry to the [ODBC Drivers] section. Type the driver name, and then type **=Installed**
Note: Assign the driver name as the value of the Driver attribute in the data source definition instead of the driver shared library name.
3. In .odbcinst.ini, add a new section having a name matching the driver name you typed in step 2, and then add configuration options to the section based on the sample odbcinst.ini file provided with Amazon ODBC Driver for Impala in the Setup directory. Specify configuration options as key-value pairs.
4. Save the .odbcinst.ini configuration file.

Configuring the amazon.impalaodbc.ini File

To configure Amazon ODBC Driver for Impala to work with your ODBC driver manager:

1. Open the .amazon.impalaodbc.ini configuration file in a text editor.
2. Edit the DriverManagerEncoding setting. If you are using Linux or Mac OS X, the value usually must be **UTF-16** or **UTF-32**, depending on the ODBC driver manager you use. iODBC uses **UTF-32** and unixODBC uses **UTF-16**. Consult your ODBC Driver Manager documentation for the correct setting to use.

OR

If you are using AIX, then set the value to **UTF-16** if you are using the unixODBC driver manager. If you are using the iODBC driver manager, then set the value to **UTF-16** if you are using the 32-bit driver, or set the value to **UTF-32** if you are using the 64-bit driver.

3. Edit the ODBCInstLib setting. The value is the name of the ODBCInst shared library for the ODBC driver manager you use. The configuration file defaults to the shared library for iODBC. In Linux, the shared library name for iODBC is libiodbcinst.so. In Mac OS X, the shared library name for iODBC is libiodbcinst.dylib.

Note: Consult your ODBC driver manager documentation for the correct library to specify. You can specify an absolute or relative filename for the library. If you intend to use the relative filename, then the path to the library must be included in the library path environment variable. In Linux, the library path environment variable is named LD_LIBRARY_PATH. In Mac OS X, the library path environment variable is named DYLD_LIBRARY_PATH.

4. Save the .amazon.impalaodbc.ini configuration file.

Configuring Authentication

Impala Server supports multiple authentication mechanisms. You must determine the authentication type your server is using and configure your DSN accordingly. The authentication methods available are as follows:

- No Authentication
- Kerberos
- User Name
- User Name and Password
- User Name and Password (SSL)
- No Authentication (SSL)

For details on the keys involved in configuring authentication, see “Appendix B: Driver Configuration Options for Linux and Mac OS X” on page 30.

Using No Authentication

For this authentication mechanism, you do not need to configure any additional settings.

To configure your DSN for connections that do not require authentication:

- Set the AuthMech configuration key for the DSN to 0

Using Kerberos

For information on operating Kerberos, refer to the documentation for your operating system.

To configure your DSN to use Kerberos authentication:

1. Set the AuthMech configuration key for the DSN to 1
2. If your Kerberos setup does not define a default realm or if the realm of your Impala server is not the default, then set the appropriate realm using the KrbRealm key.
3. Set the KrbFQDN key to the fully qualified domain name of the Impala host.
4. Set the KrbServiceName key to the service name of the Impala server. For example, if the principle for the Impala server is `impala/fully.qualified.domain.name@your-realm.com`, then the value in the service name field is `impala`. If you are unsure of the correct service name to use for your particular Hadoop deployment, contact your Hadoop administrator.

Using User Name

This authentication mechanism requires a user name but does not require a password. The user name labels the session, facilitating database tracking.

To configure your DSN for User Name authentication:

1. Set the AuthMech configuration key for the DSN to 2
2. Set the UID key to a user name that is recognized by the Impala server.

Using User Name and Password

This authentication mechanism requires a user name and a password.

Note: This authentication mechanism should not be used with an Impala configuration that does not have LDAP enabled.

To configure your DSN to use User Name and Password authentication:

1. Set the AuthMech configuration key for the DSN to 3
2. Set the UID key to a user name that is recognized by the Impala server.
3. Set the PWD key to the password corresponding to the user name you provided in step 2.

Using User Name and Password (SSL)

This authentication mechanism uses SSL and requires a user name and a password. The driver accepts self-signed SSL certificates.

Note: This authentication mechanism should not be used with an Impala configuration that does not have LDAP enabled.

To configure User Name and Password (SSL) authentication:

1. Set the AuthMech configuration key for the DSN to 4
2. Set the UID key to a user name that is recognized by the Impala server.
3. Set the PWD key to the password corresponding to the user name you provided in step 2.
4. Optionally, configure the driver to allow a mismatch between the common name of a CA-issued certificate and the host name of the Impala server by setting the CAIssuedCertNamesMismatch key to 1.

Note: For self-signed certificates, the driver always allows the common name of the certificate to mismatch the host name. For more details, see “Appendix B: Driver Configuration Options for Linux and Mac OS X” on page 30.

5. Optionally, configure the driver to load SSL certificates from a specific file by setting the TrustedCerts configuration key to the path of the file.

Note: By default, the driver uses the trusted CA certificates PEM file that is installed with the driver. For more details, see “Appendix B: Driver Configuration Options for Linux and Mac OS X” on page 30.

No Authentication (SSL)

This authentication mechanism uses SSL but does not require a user name or a password. The driver accepts self-signed SSL certificates.

To configure No Authentication (SSL) authentication:

1. Set the AuthMech configuration key for the DSN to 5

2. Optionally, configure the driver to allow a mismatch between the common name of a CA-issued certificate and the host name of the Impala server by setting the `CAIssuedCertNamesMismatch` key to 1.

Note: For self-signed certificates, the driver always allows the common name of the certificate to mismatch the host name. For more details, see “Appendix B: Driver Configuration Options for Linux and Mac OS X” on page 30.

3. Optionally, configure the driver to load SSL certificates from a specific file by setting the `TrustedCerts` configuration key to the path of the file.

Note: By default, the driver uses the trusted CA certificates PEM file that is installed with the driver. For more details, see “Appendix B: Driver Configuration Options for Linux and Mac OS X” on page 30.

Features

Data Types

The following data types are supported:

- TINYINT
- SMALLINT
- INT
- BIGINT
- FLOAT
- DOUBLE
- BOOLEAN
- STRING
- TIMESTAMP
- DECIMAL(p,s)

Note: The DECIMAL(p,s) data type is supported in Impala 1.4 and later.

Note: The aggregate types (ARRAY, MAP and STRUCT) are not yet supported. Columns of aggregate types are treated as STRING columns.

Catalog and Schema Support

Amazon ODBC Driver for Impala supports both catalogs and schemas in order to make it easy for the driver to work with various ODBC applications. Since Impala only organizes tables into schema/database, we have added a synthetic catalog, called “IMPALA” under which all of the schemas/databases are organized. The driver also maps the ODBC schema to the Impala schema/database.

SQL Translation

Amazon ODBC Driver for Impala is able to parse queries locally prior to sending them to the Impala server. This feature allows the driver to calculate query metadata without executing the query, support query parameters, and support extra SQL features such as ODBC escape sequences and additional scalar functions that are not available in the Impala-shell tool.

Active Directory

Amazon ODBC Driver for Impala supports Active Directory Kerberos on Windows. There are two prerequisites for using Active Directory Kerberos on Windows:

- MIT Kerberos is not installed on client Windows machine.
- The MIT Kerberos Hadoop realm has been configured to trust the Active Directory realm so that users in the Active Directory realm can access services in the MIT Kerberos Hadoop realm.

Contact Us

Customers should check the EMR Forum:

<https://forums.aws.amazon.com/forum.jspa?forumID=52>

Or open a support case using the AWS Support Center:

<https://aws.amazon.com/support>

Appendix A: Configuring Kerberos Authentication for Windows

Active Directory

Amazon ODBC Driver for Impala supports Active Directory Kerberos on Windows. There are two prerequisites for using Active Directory Kerberos on Windows:

- MIT Kerberos is not installed on client Windows machine.
- The MIT Kerberos Hadoop realm has been configured to trust the Active Directory realm so that users in the Active Directory realm can access services in the MIT Kerberos Hadoop realm.

MIT Kerberos

Downloading and installing MIT Kerberos for Windows 4.0.1

To download and install MIT Kerberos for Windows 4.0.1:

1. To download the Kerberos installer for 64-bit computers, use the following download link from the MIT Kerberos website:
<http://web.mit.edu/kerberos/dist/kfw/4.0/kfw-4.0.1-amd64.msi>
This installer includes both 32-bit and 64-bit libraries.

OR

To download the Kerberos installer for 32-bit computers, use the following download link from the MIT Kerberos website:
<http://web.mit.edu/kerberos/dist/kfw/4.0/kfw-4.0.1-i386.msi>
This installer includes 32-bit libraries only.

2. To run the installer, double-click the .msi file that you downloaded in step 1.
3. Follow the instructions in the installer to complete the installation process.
4. When the installation completes, click **Finish**.

Setting up the Kerberos Configuration File

Settings for Kerberos are specified through a configuration file. You can set up the configuration file as a .ini file in the default location (the **C:\ProgramData\MIT\Kerberos5** directory) or as a .conf file in a custom location.

Normally, the **C:\ProgramData\MIT\Kerberos5** directory is hidden. Consult your Windows documentation if you want to view and use this hidden directory.

To set up the Kerberos configuration in the default location:

1. Obtain the **krb5.conf** configuration file from your Kerberos administrator.

OR

Obtain the configuration file from the following location on the machine that is hosting the Impala server: **/etc/krb5.conf**

2. Rename the configuration file from **krb5.conf** to **krb5.ini**

3. Copy **krb5.ini** to the **C:\ProgramData\MIT\Kerberos5** directory and overwrite the empty sample file.

Note: For more information on configuring Kerberos, consult the MIT Kerberos documentation.

To set up the Kerberos configuration file in a custom location:

1. Obtain the **krb5.conf** configuration file from your Kerberos administrator.

OR

Obtain the configuration file from the following location on the machine that is hosting the Impala server: **/etc/krb5.conf**

2. Place the **krb5.conf** file in an accessible directory and make note of the full path name.
3. Click **Start**, then right-click **Computer**, and then click **Properties**
4. Click **Advanced system settings**
5. In the System Properties dialog, click the **Advanced** tab, and then click **Environment Variables**
6. In the Environment Variables dialog, under the **System variables** list, click **New**.
7. In the New System Variable dialog, in the **Variable name** field, type **KRB5_CONFIG**
8. In the **Variable value** field, type the absolute path to the **krb5.conf** file from step 2.
9. Click **OK** to save the new variable.
10. Ensure the variable is listed in the **System variables** list.
11. Click **OK** to close the Environment Variables dialog, and then click **OK** to close the System Properties dialog.

Setting up the Kerberos Credential Cache File

Kerberos uses a credential cache to store and manage credentials.

To set up the Kerberos credential cache file:

1. Create a directory where you want to save the Kerberos credential cache file. For example, create the following directory: **C:\temp**
2. Click **Start**, then right-click **Computer**, and then click **Properties**.
3. Click **Advanced system settings**
4. In the System Properties dialog, click the **Advanced** tab, and then click **Environment Variables**
5. In the Environment Variables dialog, under the **System variables** list, click **New**
6. In the New System Variable dialog, in the **Variable name** field, type **KRB5CCNAME**
7. In the **Variable value** field, type the path to the folder you created in step 1, and then append the file name **krb5cache**

For example, if you created the folder **C:\temp** in step 1, then type **C:\temp\krb5cache**

Note: krb5cache is a file (not a directory) that is managed by the Kerberos software, and it should not be created by the user. If you receive a permission error when you first use Kerberos, check to ensure that krb5cache does not already exist as a file or a directory.

8. Click **OK** to save the new variable.
9. Ensure the variable appears in the **System variables** list.
10. Click **OK** to close the Environment Variables dialog, and then click **OK** to close the System Properties dialog.
11. To ensure that Kerberos uses the new settings, restart your computer.

Obtaining a Ticket for a Kerberos Principal

A principal is a user or service that can authenticate to Kerberos. To authenticate to Kerberos, a principal must obtain a ticket by using a password or a keytab file. You can specify a keytab file to use, or use the default keytab file of your Kerberos configuration.

To obtain a ticket for a Kerberos principal using a password:

1. Click the **Start** button , then click **All Programs**, and then click the **Kerberos for Windows (64-bit)** or the **Kerberos for Windows (32-bit)** program group.
2. Click **MIT Kerberos Ticket Manager**
3. In the MIT Kerberos Ticket Manager, click **Get Ticket**
4. In the Get Ticket dialog, type your principal name and password, and then click **OK**

If the authentication succeeds, then your ticket information appears in the MIT Kerberos Ticket Manager.

To obtain a ticket for a Kerberos principal using a keytab file:

1. Click the **Start** button , then click **All Programs**, then click **Accessories**, and then click **Command Prompt**
2. In the Command Prompt, type a command using the following syntax:
`kinit -k -t keytab_pathname principal`
keytab_pathname is the full pathname to the keytab file.
For example: C:\mykeytabs\impalaserver.keytab
principal is the Kerberos principal to use for authentication.
For example: impala/impalaserver.example.com@EXAMPLE.COM
3. If the cache location KRB5CCNAME is not set or not used, then use the `-c` option of the `kinit` command to specify the credential cache.
In the command, the `-c` argument must appear last. For example:
`kinit -k -t C:\mykeytabs\impalaserver.keytab
impala/fully.qualified.domain.name@your-realm.com -c
C:\ProgramData\MIT\krb5cache`

Note: krbcache is the Kerberos cache file, not a directory.

To obtain a ticket for a Kerberos principal using the default keytab file:

Note: For instructions on configuring a default keytab file for your Kerberos configuration, consult the MIT Kerberos documentation.

1. Click the **Start** button , then click **All Programs**, then click **Accessories**, and then click **Command Prompt**.

2. In the Command Prompt, type a command using the following syntax:

```
kinit -k principal
```

principal is the Kerberos principal to use for authentication.

For example, `impala/impalaserver.example.com@EXAMPLE.COM`

3. If the cache location KRB5CCNAME is not set or not used, then use the `-c` option of the `kinit` command to specify the credential cache. In the command, the `-c` argument must appear last. For example:

```
kinit -k impala/fully.qualified.domain.name@your-realm.com -c  
C:\ProgramData\MIT\krbcache
```

Note: krbcache is the Kerberos cache file, not a directory.

Appendix B: Driver Configuration Options for Linux and Mac OS X

The configuration options available to control the behavior of Amazon ODBC Driver for Impala are listed and described in *Table 1*.

Note: You can set configuration options in your `odbc.ini` and `.amazon.impalaodbc.ini` files. Configuration options set in a `.amazon.impalaodbc.ini` file apply to all connections, whereas configuration options set in an `odbc.ini` file are specific to a connection. Configuration options set in `odbc.ini` take precedence over configuration options set in `.amazon.impalaodbc.ini`

Key	Default Value	Description
AuthMech	0	The authentication mechanism to use. The following values are possible: • 0 – No Authentication • 1 – Kerberos • 2 – User Name • 3 – User Name and Password • 4 – User Name and Password (SSL) • 5 – No Authentication (SSL)
CAIssuedCertNamesMismatch	0	Whether to allow the common name of a CA-issued SSL certificate to mismatch the host name of the Impala server. The following values are possible: • 0 – Do not allow the names to mismatch. • 1 – Allow the names to mismatch. Note: This setting is only applicable to the User Name and Password (SSL) and No Authentication (SSL) authentication mechanisms. It is ignored by other authentication mechanisms.

Key	Default Value	Description
DelegationUID		Used to delegate all operations against Impala to a user that is different than the authenticated user for the connection.
Driver		The location of the Amazon ODBC Driver for Impala shared object file.
HOST		The IP address or hostname of the Impala server.
KrbFQDN		The fully qualified domain name of the Impala host used.
KrbRealm		If there is no default realm configured or if the realm of the Impala host is different from the default realm for your Kerberos setup, use this option to define the realm of the Impala host.
KrbServiceName		The Kerberos service principal name of the Impala server.
PORT	10000	The listening port for the service.
PWD		The password of a user account on the host running Impala. PWD is required if AuthMech is set to User Name and Password, or User Name and Password (SSL).
RowsFetchedPerBlock	10000	The maximum number of rows that a query returns at a time. Any positive 32-bit integer is a valid value, but testing has shown that performance gains are marginal beyond the default value of 10000 rows.
SocketTimeout	0	The number of seconds after which Impala closes the connection with the client application if the connection is idle.

Key	Default Value	Description
TrustedCerts	For 32-bit driver: /opt/amazon/ impalaodbc/lib/32/ cacerts.pem For 64-bit driver: /opt/amazon/ impalaodbc/lib/64/ cacerts.pem	Used to specify the location of the file containing trusted CA certificates for authenticating the Impala server when using SSL. If the setting is not set, then the driver defaults to using the trusted CA certificates file installed by the driver. Note: This setting is only applicable to User Name and Password (SSL) and No Authentication (SSL) authentication mechanisms and is ignored by other authentication mechanisms.
TSaslTransportBufSize	1000	The number of bytes to reserve in memory for buffering unencrypted data from the network. Note: In most circumstances, the default value of 1000 bytes is optimal.
UID	anonymous	The user name of an existing account on the host running Impala. UID is required if AuthMech is set to User Name and Password, or User Name and Password (SSL). UID is optional if AuthMech is set to User Name.

Key	Default Value	Description
UseNativeQuery	0	By default, the driver transforms the queries emitted by an application to convert the queries into an equivalent form in Impala SQL. Use this option to specify whether or not the driver transforms queries. The following values are possible: • 0 – Transform the queries into Impala SQL. • 1 – Do not transform the queries (use the native query instead). Note: If the application is Impala-aware and already emits Impala SQL, then set this option to 1 to avoid the extra overhead of query transformation.

Table 1 Driver Configuration Options for Linux and Mac OS X