Delinea

Server Suite

DB2 Integration Guide

Version: 2024.x

Publication Date: 7/11/2025

Server Suite DB2 Integration Guide

Version: 2024.x, Publication Date: 7/11/2025

© Delinea, 2025

Table of Contents

Table of Contents

About this Guide

In DB2, user and group authentication is performed by a facility that is external to the DB2 database management system, such as the operating system, a domain controller, or a Kerberos security system. It is accomplished using dynamically loadable libraries called security plug-ins.

The default IBM DB2 username/password plug-in authenticates users only in an NIS domain or in the `/etc/passwd` password file. If another security plug-in has not been explicitly configured, the user credentials provided in the connection request are authenticated by the security facility on the DB2 Universal Database (UDB) server. That is, the default plug-in sends the user ID and password to the operating system for validation.

About Server Suite DB2

DirectControl for DB2 extends the Authentication Service to DB2 database instances. This solution allows you to use Microsoft Active Directory as the central authentication and access control data store in a heterogeneous environment that contains both Windows and UNIX computers as well as DB2 relational database management systems.

Delinea software is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103; 9,112,846; 9,197,670; 9,378,391 and 9,442,962. (Ref: CS-44575)

Adopt a Service Account

This section describes how to adopt a service account and the permission required depends on the option chosen.

In a Kerberized environment, there are times when a service account needs to obtain a Kerberos credential and infinitely renew that credential for a long running process.

Another scenario configuring a clustered environment where a virtual host account needs to provide services using an additional ServicePrincipalName (SPN).

One way to achieve goals such as, but not limited to, the above scenarios, is to use the Delinea command `adkeytab` to adopt a service account and build a `keytab` file.

Option 1: Reset the Service Account Password

Let the `adkeytab` command reset this service account's password while adopting the account. The current password of the service account is not required.

With this option, the account adopting the service account needs to have reset password and change password permission of the service account. For example:

```
adkeytab --adopt -u svcadmin -K /etc/svcacct.keytab svcacct
```

From the example, the account svcadmin is performing the adoption so it must have permission to reset password and change password for the adopted account svcacct. After the adoption, the password of this service account, svcacct, is reset to a randomly generated password.

Option 2: Provide the Existing Service Account Password

Provide this service account's current password with `adkeytab` command while adopting the account. The current password for this service account is required.

With this option, the account adopting the service account does not need any extra permission; the default read permission is enough. With this option, the `-local` and `-w` flags are required to adopt this account. For example:

```
adkeytab --adopt -u svcadmin --local -w password> -K /etc/ svcacct.keytab svcacct
```

where <password> is replaced by account svcacct's current password. After the adoption, the password of this service account is not changed or reset.

See the `adkeytab` main page for a complete list of options and description.

Authentication and Authorization in IBM DB2

Authorization is the process of determining access information about specific database objects and actions based on a supplied user ID. Privileges can be granted to specific users or to groups of users. Users that are a member of a group automatically inherit the group's privileges. As mentioned before, these users and groups are defined outside the DB2 UDB; for example, in Active Directory.

DB2 supports replacement plug-ins for authentication and authorization. The authentication plug-ins can replace the default user name and password method, and support alternative authentication methods including GSSAPI. DB2 also supports the use of multiple plug-ins for authentication.

Authentication for DB2 Security and Authentication Plug-Ins

Authentication Service for IBM DB2 package provides plug-ins that allow you to connect or attach to a DB2 database using either an Active Directory or a UNIX user identity. In addition, the package includes a group plug-in used for authorization.

The package provides two security plug-ins for authentication:

- `centrifydc_db2userpass`: a username/password plug-in to replace the DB2 default.
- `centrifydc_db2gsskrb5`: a GSSAPI plug-in for single sign on support.

The security plug-ins can be used independently or in conjunction with one another.

- If you specify and configure both the username/password plug-in and the GSSAPI plug-in, the GSSAPI plug-in is used when the user connects without specifying a user name and password. The user account can be on an Active Directory domain controller or UNIX computer. If the user does specify a user name and password, the username/password plug-in is used instead.

- If only the GSSAPI plug-in is configured, only Active Directory users can connect to the database instance. In addition, the Active Directory user name instead of the UNIX user name must be used in the SQL GRANT or REVOKE statements when granting or revoking permissions. In this case, the Active Directory user name should follow the DB2 user naming conventions.

DB2 and Delinea Plug-In Compatibility

Starting with DB2 release 10.5.4, DB2 does not allow security plug-ins to fork a process to authenticate DB2 users. To support this behavior, the Delinea plugins starting with Delinea for DB2 5.2.3 use the CentrifyDC service to authenticate Active Directory and local users.

If your environment contains DB2 10.5.4 or later:

- Only Delinea for DB2 5.2.3 or later plug-ins are supported, *and*

- Before you install Delinea for DB2, you must install the Server Suite 2015.1 or later agent (that is, agent version 5.2.3+) on each DB2 server, *and*

- You must ensure that the agent (that is, the `centrifydc` service) is running on each DB2 server.

Username-Password Plug-In

The Delinea username/password plug-in, `centrifydc_db2userpass`, supports authentication from both Active Directory and non-Active Directory users. A non-Active Directory user may be one of the following:

- a UNIX user from local stores such as `/etc/passwd` and Name Service Switch (NSS)

- any user who has been authenticated using Pluggable Authentication

  Modules (PAM)

- any user who has been authenticated using the AIX Loadable Authentication Module (LAM)

The Delinea username/password plug-in, like the IBM default username/password plug-in, gives you the option to allow users who are already logged in to a DB2 server machine to connect to a database instance without entering a user name or password. However, the default is to require a logged in user to re-enter the user name and password to access the database instance.

GSSAPI Plug-In

The GSSAPI plug-in, `centrifydc_db2gsskrb5`, supports single sign on to a DB2 instance using the user's Active Directory account. This plug-in assumes that the user requesting access to the database is already logged in to the client computer and has been authenticated through the Kerberos mechanism.

The GSSAPI plug-in allows users to run the `connect` and `attach` commands without specifying a user name and password even if the user is connecting from a remote DB2 client. It requires the user to have a valid Kerberos ticket. Generally, users obtain a Kerberos ticket automatically when they log in as an Active Directory user. However, in the following situations the user does not obtain a ticket automatically:

- The user logs in to the DB2 server as a local, non-Active Directory user.

- The user enters the UNIX command `su - ` *user* as root to get a shell owned by another Active Directory user or local user.

- The user logs in as a user who has both an Active Directory account and a local user account. However, the Active Directory account is not in the same zone as the machine you logged in to.

In each of these cases, the user needs to obtain Kerberos tickets before single sign-on support is provided.

To obtain tickets for an Active Directory user, type `kinit` *user*. The user is prompted for a password. To avoid being prompted, you can create a keytab file in advance using the `adkeytab` command, set the environment variable `KRB5_KTNAME` to the full path of your `keytab` file, and then run `kinit -k` *user@DOMAIN* to obtain the tickets.

> 📝 **Note:** If a user name is explicitly provided when only the GSSAPI plug-in is installed (for example, by entering the DB2 command `connect to testdb user username using password`), the plug-in first authenticates the given user to the Kerberos Key Distribution Center (KDC), and then obtains a ticket-granting ticket (TGT) upon success. The plug-in next uses the TGT to get a service ticket for the DB2 server.

Group Plug-in

You install the Group plug-in, `centrifydc_db2group` to retrieve the list of groups to which a user belongs for authorization. The group plug-in is called automatically after user authentication by DB2. The group info retrieved is used by DB2 to check a user's access rights and determine whether the user has privilege to do specific tasks; for example, connect, query, perform database management, and so on.

The Group plug-in queries Active Directory first for the groups to which the user belongs, and then it looks in the local groups on the host. The two lists are then merged, with duplicates removed and returned to DB2.

Make Connections to the DB2 Administration Server

The DB2 Administration Server (DAS) allows administrators to manage DB2 instances remotely. Using utilities such as DB2 Control Center (`db2cc`) to perform operations such as creating, removing, starting, or stopping a database instance remotely require a DAS connection. Tasks that can be performed on a running instance (such as creating or dropping a table in the instance) do not require a DAS connection.

The DAS uses a separate authentication scheme from the instance authentication. The DAS does not call into the DB2 security plug-ins or PAM when authenticating users. If you want to log in as an Active Directory user and use utilities such as DB2 Control Center to remotely administer an instance, you have the following options, irrespective of the plug-ins that you select:

- Run the utility that connects to the DAS (such as `db2cc`) on the DB2 server machine as the user who can perform the desired administrative tasks.

  Make sure that this user is in the same zone as the DB2 server machine.

- Install and configure either the Microsoft or Delinea password synchronization service. For more details about the Delinea password synchronization service, refer to the *Administrator's Guide for Windows*.

- Create a local user on the DB2 server machine and enter that user's user name and password when DB2 Control Center (or other utility connecting to the DAS) requests a user name and password.

Next Step:

Install and Configure the Server

Install and Configure the Server

This section describes how to install and configure the Authentication Service for IBM DB2 package on a DB2 server.

To automate Authentication Service for IBM DB2 plug-in installation and configuration, use the `setupdb2.sh` script provided in the Authentication Service for IBM DB2 package.

To manually install, set up, configure, and verify the Identity Broker Service for IBM DB2 plug-in without using the `setupdb2.sh` script, see Install Manually.

Use the uninstallation script, `/usr/share/centrifydc/bin/ uninstalldb2.sh`, included in the Authentication Service for IBM DB2 package, to remove the Authentication Service for IBM DB2:

- When there is partially installed Authentication Service for IBM DB2 release after a failed installation attempt.

- Before upgrading an existing Authentication Service for IBM DB2 to a new release.

- For details about using this script, see Execute the uninstalldb2 Script.

The following sections describe how to install and configure the Authentication Service for IBM DB2 package on each supported platform using the `setupdb2.sh` script:

1. Install and Configure the Server

    a. Software Requirements

    b. Unzip and Restore the Authentication Service for DB2 Package

        i. Unzip and Restore AIX Files

        ii. Unzip and Restore Linux Files

        iii. Unzip and Restore Solaris files

    c. Install Authentication Service for DB2 Using the Platform Install Program

        i. Install the AIX Files

        ii. Install the Linux Files

        iii. Install the Solaris Files

    d. Install and Configure Plug-Ins Using the setupdb2 Script

        i. Run the setupdb2.sh Script

    e. Install Manually

        i. Copy the plug-ins

        ii. Setup for the Username-Password Plug-In

        iii. DB2 Group Plug-in Setup

        iv. GSSAPI Plug-in Setup

        v. Configure the DB2 Instance

        vi. Verify the Setup

Software Requirements

You must have the Delinea agent installed on each DB2 server, and the DB2 servers must be joined to an Active Directory domain.

If you use the GSSAPI plug-in, the plug-in must be installed on the DB2 server and each DB2 client. In addition, both the DB2 client and the DB2 server computers must be joined to the same Active Directory domain.

If you use the username/password plug-in, you must install the PAM library. You can install the PAM library after you install the Delinea for DB2 package.

See *DB2 and Delinea Plug-in Compatibility* under [Authentication and Authorization in IBM DB2](#)

See the release notes for the Delinea software, DB2 versions and versions of Red Hat, SuSE, Solaris, and AIX operating systems supported in this release.

Unzip and Restore the Authentication Service for DB2 Package

> 📝 **Note:** If Authentication Service for IBM DB2 is already installed, uninstall it now as described in [Execute the uninstalldb2 Script](#).

To begin the installation, unzip and restore the Authentication Service for IBM DB2 package on each DB2 server.

Depending on the platform, download the plug-ins from the [customer support portal](#).

The following sections describe how to unzip and restore the package on each supported platform. In each example:

- *release* is the release number of the Authentication Service for IBM DB2 software (for example, 6.1.0)
- *os_release* is the release number of the operating system (for example, 8)
- *architecture* is the processor architecture that is supported (for example, x86_64)

Unzip and Restore AIX Files

Execute the following commands to unzip and restore the Authentication Service for IBM DB2 package files on an AIX computer:

```
gunzip delinea-db2-release-aixos_release-ppc.tgz

tar -xvf delinea-db2-release-aixos_release-ppc-bff.tar

gunzip delinea-db2-release-aixos_release-ppc-bff.gz
```

After you execute these commands, the file `centrify-db2-release-aixos_release-ppc-bff` is ready to be installed using the native AIX installer. Go to [Install Authentication Service for DB2 Using the Platform Install Program](#) and continue from there.

Unzip and Restore Linux Files

Execute the following commands to unzip and restore the Authentication Service for IBM DB2 package files on a Linux computer. The examples shown here assume that you are installing on Red Hat Linux.

```
gunzip delinea-db2-release-rhelos_release-architecture.tgz
```

```
tar -xvf delinea-db2-release-rhelos_release-architecture.tar
```

After you execute these commands, the file `centrify-db2-release-rhelos_release-architecture.rpm` is ready to be installed using the native Linux installer. Go to Install Authentication Service for DB2 Using the Platform Install Program and continue from there.

Unzip and Restore Solaris files

Execute the following commands to unzip and restore the Authentication Service for IBM DB2 package files on a Solaris computer:

```
gunzip delinea-db2-release-solos_release-architecture.tgz
```

```
tar -xvf delinea-db2-release-solos_release-architecture.tar
```

After you execute these commands, the file `centrify-db2-release-solos_release-ppc-bff` is ready to be installed using the native Solaris installer. Go to Install Authentication Service for DB2 Using the Platform Install Program and continue from there.

Install Authentication Service for DB2 Using the Platform Install Program

After you have unzipped and restored the Authentication Service for IBM DB2 package files, install the package using the platform's native installation program. The following sections describe the installation procedure on each supported platform. In each example:

- *release* is the release number of the Authentication Service for IBM DB2 software
- *os_release* is the release number of the operating system.
- *architecture* is the processor architecture that is supported.

Install the AIX Files

Execute the following command to install the Authentication Service for IBM DB2 package using the native AIX installation program:

```
installp -d centrify-db2-release-aixos_release-ppc-bff CentrifyDC.db2
```

After you execute this command, you are ready to install and configure the Authentication Service for IBM DB2 plug-ins. You can install and configure the plug-ins using the `setupdb2.sh` script, or manually without using the `setupdb2.sh` script. See Install and Configure PlugIns Using the setupdb2 Script or Install Manually for details about these procedures.

Install the Linux Files

Execute the following command to install the Authentication Service for IBM DB2 package using the native Linux installation program. The examples shown here assume that you are installing on Red Hat Linux.

If you are installing the Authentication Service for IBM DB2 package for the first time:

```
rpm -ivh centrify-db2-release-rhelos_release-architecture.rpm
```

After you execute this command, you are ready to install and configure the Authentication Service for IBM DB2 plug-ins. You can install and configure the plug-ins using the `setupdb2.sh` script, or manually without using the `setupdb2.sh` script. See the next section or Install Manually for details about these procedures.

Install the Solaris Files

Execute the following command to install the Authentication Service for IBM DB2 package using the native Solaris installation program.

```
tar -xvf centrifydc-db2-release-solos_release-architecture-local.tgz
pkgadd -a admin -n -d CentrifyDC-db2
```

After you execute this command, you are ready to install and configure the Authentication Service for IBM DB2 plug-ins. You can install and configure the plug-ins using the `setupdb2.sh` script, or manually without using the `setupdb2.sh` script. See Install and Configure PlugIns Using the setupdb2 Script or Install Manually for details about these procedures.

Install and Configure Plug-Ins Using the setupdb2 Script

The `/usr/share/centrifydc/bin/setupdb2.sh` script is an interactive script. Provide the following information at the script prompts:

- The DB2 authentication you want to use (both user name/ password and single sign on, single sign on only, or username/ password only)
- What data sent to DB2 you want to encrypt
- The Active Directory administrator password

For GSSAPI-related plug-in installation using the `setupdb2.sh` script, additionally provide the following information at the prompts:

- An account name, password, and container for an Active Directory user with administrator privileges on the domain controller.

The scripts then installs, configures, and verifies the plug-in(s) according to your entries.

The following table lists the `setupdb2.sh` command line options:

Options	Required	Values	Description
inst	Yes	A string value	The name of a DB2 database instance.
verbose	No	0 or 1 The default is 1	If the value is 0, only the basic questions are asked. All 3 Authentication Service for IBM DB2 plug-ins are installed. If the value is 1, the script prompts for different installation and setup options.

Options	Required	Values	Description
debug	No	0 or 1 The default is 0	If the value is 0, installation and setup are performed. If the value is 1, the script simulates the steps without actually performing them. Each command is displayed with a "#" prefix. Use this option to preview what commands are executed in an actual invocation.

The format for all command options is option=value. Separate each option with a space.

Run the setupdb2.sh Script

Perform the steps described in this section to run the setupdb2.sh script now.

In the example used here, db2inst1 is the name of a DB2 database instance, you want to run the script in verbose mode, and you do not want to run the script in debug mode.

To run the setupdb2.sh script:

1. Change to the /usr/share/centrifydc/bin directory:

   `cd /usr/share/centrifydc/bin`

2. Run the setupdb2.sh script. The instance name that you specify with the setupdb2.sh command cannot exceed 8 bytes. In this example, the database instance is named db2inst1, verbose mode is invoked so that all prompts for different installation and setup options are displayed, and debug mode is not invoked.

   `./setupdb2.sh inst=db2inst1 verbose=1`

   In this example, the database instance is named db2inst1, verbose mode is invoked so that all prompts for different installation and setup options are displayed, and debug mode is not invoked.

3. Type y or n at the prompt, Is db2inst1 a DB2 server install?

   In this example, db2inst1 is a server installation, so select the default (y for yes).

   This is confirming that the running component is a DB2 server. Entering yes directs the script to also install the DB2 client component. A message indicates if the script determined the instance is 32 or 64 bit.

   `db2inst1 is a 64 bit instance. DB2 server and client setup will be done.`

4. Enter a number at the prompt, Which DB2 auth method do you want to use?

   Select an authentication method. From the listed choices, enter the corresponding number.

   `[1] Username/Password and Single sign-on`

   [2] Single Sign-on only

   [3] Username/Password only

   [4] Skip this step

   Select a number from the menu [1]:

   See Username-Password Plug-In and GSSAPI Plug-In for details about these choices. In this example, select username/password only.

5. Enter a number at the prompt, Which data sent to DB2 should be encrypted?

Select if or which data sent to DB2 should be encrypted. This step is optional.

[1] Nothing

[2] The username and their password

[3] All data going to the server

[4] Encrypt and compress all data going to the server

[5] Skip this step

In this example, select [1] Nothing. Selecting [2], [3], or [4] changes the SRVCON_AUTH to Server_ Encrypt. Selecting [5] Skip this step exits the plug-in setup program.

6. Type y or n at the prompt, Use the CentrifyDC group plugin?

   Specify whether to use the CentrifyDC group plug-in. See Group Plug-In for details about this choice.

   Install the Group plug-in centrifydc_db2group, to retrieve the list of groups to which a user belongs for authorization. The group plug-in is called automatically after user authentication by DB2.

   The group information retrieved is used by DB2 to check a user's access rights and determine whether the user has privilege to do specific tasks. For example: connect, query, db management, and so forth.

   The Group plug-in queries Active Directory first for the groups to which the user belongs and then it looks in the local groups on the host. The two lists are then merged with duplicates removed and returned to DB2.

   In this example, select yes.

7. Enter a number at the prompt, Do you want to configure the instance user db2inst1 as a service account?

   Specify whether to configure the instance user as a service account.

   You must do this step if you want to use the GSS-Plugin. If you already did this step for this instance, select the option to indicate the keytabfile name.

   [1] Useadkeytab to create a service account in Active Directory and keytabfile`.

   NOTE: You need to specify a user name with administrator privileges on the domain to use adkeytab.

   [2] Provide the name of an already existingkeytabfile.

   [3] Skip this step

   Generally, if you are starting from nothing, enter 1, otherwise enter 2.

   If you are setting up the GSSAPI plug-in (that is, if you selected a single sign-on option in Step 5) and you have not yet configured the instance user as a service account, you must select option 1, Use adkeytab to create a service account in Active Directory and keytab file. You will be prompted later for the Active Directory Administrator password.

   If you have already configured the instance user as a service account, the necessary keytab file already exists. If this is the case, select option 2, "Provide the name of an already existing keytab file," and provide the full path and file name of the keytab file.

   If you are not setting up the GSSAPI plug-in, you can optionally skip this step.

In this example, even though the GSSAPI plug-in is not being set up (that is, a single sign-on option was not selected in Step 5), you can still choose to configure the instance user as a service account. To do so, select option 1.

8. Enter a filename or press return to accept the default, at the prompt, `what is the file name thatadkeytabshould use when creating thekeytabfile?`

    Choose the default or specify any location.

    `Full path please.`

    Note: the file needs to be accessible to the db2inst1 user.

    [/home/db2inst1/db2inst1.keytab]

9. Enter at the prompt, `Enter the password for db2inst1.`

    Provide the password for the database instance that you specified in Step 2.

    Create a new password for `db2inst1` or enter an existing password (if configured earlier).

10. Enter at the prompt, `Enter a user name that has administrator privileges for the domain.`

    Specify a user name (for example, flast@company.com). The username must be a SamAccount, and must have administrator privileges for the domain (that is, Active Directory Administrator privileges).

11. Enter at the prompt, `Enter the container where to store the db2inst1 user.`

    Specify the container object in which to create the service account.

    `[CN=Users]:`

    The default OU is CN=Users

    PAM setup not required for AIX. Skipping...

    If a service account name other than the DB2 instance name is chosen to adopt and build the Kerberos `keytab` file, this service account needs to meet the following two requirements:

    ■ The account name must be 8 characters long at most. This is required by the DB2 server.

    ■ This account must have the same permission granted as the instance owner in DB2 server

    The `setupdb2.sh` script can use only the container objects in the domain to which the computer is currently joined. You cannot specify another domain for the container object when you use the `setupdb2.sh` script to install and configure plug-ins. If you want to specify a different domain, you must install the plug-ins manually without using the `setupdb2.sh` script. See Step 2 in Set up for the GSSAPI plug-in for details about specifying a different domain.

    Type the name of the container object in relative DN format (that is, do not specify the domain portion of the DN). For example, if you wanted to create the service account in the users container in the currently joined domain, you would type the following:

    `CN=users`

12. Enter at the prompt, `What group should be used as the group owner of this file?`

    Specify the group name or select the default.

All `DB2` instances that you want to use the username/password plugin must be in this group. [db2iadm1]:

You are prompted for more information depending on which plug-ins you are setting up:

- The password for the user with Active Directory Administrator privileges that you specified in Step 11. You are prompted for this information if you are setting up the GSSAPI plug-in.

Example return output from this step.

```
************adkeytabsetup (required for GSS-plugin) ***********
```

Using /home/db2inst1/db2inst1.keytab for thekeytabfile for instance: db2inst1

NOTE:adkeytabwill prompt you for the password of the Active Directory admin user: rsriniva.

#adkeytab-n -c CN=Users -u rsriniva -K /home/db2inst1/ db2inst1.keytab -P db2inst1/vaix61-2.corp.contoso.com db2inst1 rsriniva@CORP.CONTOSO.COM's password:

Success: New Account: db2inst1

NOTE:adkeytabwill prompt you for the password of the Active Directory admin user: rsriniva again.

#adkeytab-C db2inst1 -u rsriniva -w XXX-PASS-NOT-DISPLAYED- XXX -K /home/db2inst1/db2inst1.keytab rsriniva@CORP.CONTOSO.COM's password:

Success: Change Password: db2inst1

chmod 600 /home/db2inst1/db2inst1.keytab

chown db2inst1 /home/db2inst1/db2inst1.keytab # db2set DB2ENVLIST=KRB5_KTNAME

adkeytab setup successfully!

************* username/password plugin setup *************

chmod 750 /usr/share/centrifydc/bin/db2userpass_checkpwd

chown root:db2iadm1 /usr/share/centrifydc/bin/ db2userpass_checkpwd

chmod u+s /usr/share/centrifydc/bin/db2userpass_checkpwd username/password setup successfully

******* Installing the plugins into instance: db2inst1 *******

Installing client side auth plugin

rm -f sqllib/security32/plugin/client/ centrifydc_db2gsskrb5.so

cp /usr/share/centrifydc/lib/libcentrifydc_db2gsskrb5.so sqllib/security32/plugin/client/centrifydc_db2gsskrb5.so

Installing group plugin

rm -f sqllib/security32/plugin/group/centrifydc_db2group.so

cp /usr/share/centrifydc/lib/libcentrifydc_db2group.so sqllib/security32/plugin/group/centrifydc_db2group.so

Installing server side auth plugin

rm -f sqllib/security64/plugin/server/ centrifydc_db2gsskrb5.so

rm -f sqllib/security64/plugin/server/ centrifydc_db2userpass.so

cp /usr/share/centrifydc/lib64/libcentrifydc_db2gsskrb5.so sqllib/security64/plugin/server/centrifydc_db2gsskrb5.so

cp /usr/share/centrifydc/lib64/ libcentrifydc_db2userpass95.so sqllib/security64/plugin/ server/centrifydc_db2userpass.so

Installing client side auth plugin

rm -f sqllib/security64/plugin/client/ centrifydc_db2gsskrb5.so

cp /usr/share/centrifydc/lib64/libcentrifydc_db2gsskrb5.so sqllib/security64/plugin/client/centrifydc_db2gsskrb5.so

Installing group plugin

rm -f sqllib/security64/plugin/group/centrifydc_db2group.so

cp /usr/share/centrifydc/lib64/libcentrifydc_db2group.so sqllib/security64/plugin/group/centrifydc_db2group.so

******* Updating settings for DB2 instance: db2inst1 ******

Old configuration (You may want to copy these settings down in case you need to revert to the old settings):

Group Plugin (GROUP_PLUGIN) =

GSS Plugin for Local Authorization (LOCAL_GSSPLUGIN) = Server List of GSS Plugins (SRVCON_GSSPLUGIN_LIST) = Server Userid-Password Plugin (SRVCON_PW_PLUGIN) = Server Connection Authentication (SRVCON_AUTH) =

NOT_SPECIFIED

Database manager authentication (AUTHENTICATION) = SERVER The DB2 configuration will be updated to:

LOCAL_GSSPLUGIN = centrifydc_db2gsskrb5 SRVCON_GSSPLUGIN_LIST = centrifydc_db2gsskrb5 SRVCON_PW_PLUGIN = centrifydc_db2userpass SRVCON_AUTH = GSS_SERVER_ENCRYPT AUTHENTICATION = SERVER

GROUP_PLUGIN = centrifydc_db2group

13. Review the script displayed content.

From this point the script stops the DB2 instance: db2inst1, updates the configuration, and then restarts the instance.

System information displays as files are configured. When the `setupdb2.sh` script finishes the configuration, a completion message displays.

Examples output when the instance is stopped.

```
Stopping instance: db2inst1
```

\# db2stop

SQL1064N DB2STOP processing was successful.

\# db2 update dbm config using LOCAL_GSSPLUGIN centrifydc_db2gsskrb5

DB20000I The UPDATE DATABASE MANAGER CONFIGURATION command completed successfully.

\# db2 update dbm config using SRVCON_GSSPLUGIN_LIST centrifydc_db2gsskrb5

DB20000I The UPDATE DATABASE MANAGER CONFIGURATION command completed successfully.

\# db2 update dbm config using SRVCON_PW_PLUGIN centrifydc_db2userpass

DB20000I The UPDATE DATABASE MANAGER CONFIGURATION command completed successfully.

\# db2 update dbm config using SRVCON_AUTH GSS_SERVER_ENCRYPT DB20000I The UPDATE DATABASE MANAGER CONFIGURATION command completed successfully.

\# db2 update dbm config using AUTHENTICATION SERVER DB20000I The UPDATE DATABASE MANAGER CONFIGURATION command completed successfully.

\# db2 update dbm config using GROUP_PLUGIN centrifydc_db2group DB20000I The UPDATE DATABASE MANAGER CONFIGURATION command completed successfully.

New configuration:

Group Plugin (GROUP_PLUGIN) = centrifydc_db2group

GSS Plugin for Local Authorization (LOCAL_GSSPLUGIN) = centrifydc_db2gsskrb5

Server List of GSS Plugins (SRVCON_GSSPLUGIN_LIST) = centrifydc_db2gsskrb5

Server Userid-Password Plugin (SRVCON_PW_PLUGIN) = centrifydc_db2userpass

Server Connection Authentication (SRVCON_AUTH) = GSS_SERVER_ENCRYPT

Database manager authentication (AUTHENTICATION) = SERVER

Starting Instance # db2start

SQL1063N DB2START processing was successful.

The plugins for DB2 instance: db2inst1 were setup successfully!

14. Verify if the setup completed properly or not by running the command as the DB2 instance user:

```
db2 get dbm config |egrep -i "auth|gss|group|srvcon"
```

Example of return output from the command for a scenario where all three DirectControl for DB2 security plug-ins have been configured as shown below. The lines of interest are in **bold**.

```
SYSADM group name (SYSADM_GROUP) = DB2GRP1
```

SYSCTRL group name (SYSCTRL_GROUP) = SYSMAINT group name (SYSMAINT_ GROUP) =

SYSMON group name (SYSMON_GROUP) =

Group Plugin (GROUP_PLUGIN) = centrifydc_db2group

GSS Plugin for Local Authorization (LOCAL_GSSPLUGIN) = centrifydc_ db2gsskrb5

Server List of GSS Plugins (SRVCON_GSSPLUGIN_LIST) = centrifydc_ db2gsskrb5

Server Userid-Password Plugin (SRVCON_PW_PLUGIN) = centrifydc_ db2userpass

Server Connection Authentication (SRVCON_AUTH) = SERVER_ENCRYPT

Database manager authentication (AUTHENTICATION) = SERVER

Cataloging allowed without authority (CATALOG_NOAUTH) = NO

Trusted client authentication (TRUST_CLNTAUTH) = CLIENT

Bypass federated authentication (FED_NOAUTH) = NO

This completes the automated installation on the DB2 server. If you selected single sign-on and username/password or single sign-on only, you need to install the GSSAPI client on every client computer. Go to Set up the GSSAPI DB2 Client for information about that procedure.

If you selected username/password only, you are done with the installation. Go to Test the Installation to finish.

Install Manually

Perform the following steps if you want to install Authentication Service for IBM DB2 manually without using the `setupdb2.sh` script. If you already installed Authentication Service for IBM DB2, skip this section and go to Set up the GSSAPI DB2 Client.

- Perform the procedures described in Unzip and Restore the Authentication Service for DB2 package and Install Authentication Service for DB2 Using the Platform Install Program

- Copy the Authentication Service for IBM DB2 shared libraries to the appropriate DB2 locations. See Copy the plug-ins.

- If you plan to use username/password for authentication, configure the operating system to load the username/password plug libraries. See Set Up for the Username-Password Plug-in

- If you plan to use single sign-on, configure the operating system to use the GSSAPI plug-in and set up the key table. See Set up for the GSSAPI plug-in

- Configure DB2 to use the three plug-ins. See Configure the DB2 instance

- Confirm that the DB2 configuration is correct. See Verify the Setup

Note: The Authentication Service for IBM DB2 Group plug-in requires no setup.

Copy the plug-ins

Use the following commands to copy the Authentication Service for IBM DB2 shared libraries from the installation directory to the proper DB2 directory for each instance—db2inst1 in the commands that follow.

The `libcentrifydc_db2userpass.so` that you use is version-dependent.

Copy Commands for 64-bit Instances:

```
cp /usr/share/centrifydc/lib64/libcentrifydc_db2userpass.so
~db2inst1/sqllib/security64/plugin/server/centrifydc_db2userpass.so

cp /usr/share/centrifydc/lib64/libcentrifydc_db2gsskrb5.so
~db2inst1/sqllib/security64/plugin/server/centrifydc_db2gsskrb5.so

cp /usr/share/centrifydc/lib64/libcentrifydc_db2gsskrb5.so
~db2inst1/sqllib/security64/plugin/client/centrifydc_db2gsskrb5.so

cp /usr/share/centrifydc/lib64/libcentrifydc_db2group.so
~db2inst1/sqllib/security64/plugin/group/centrifydc_db2group.so

cp /usr/share/centrifydc/lib/libcentrifydc_db2gsskrb5.so
~db2inst1/sqllib/security32/plugin/client/centrifydc_db2gsskrb5.so
```

Copy Commands for 32-bit Instances:

```
cp /usr/share/centrifydc/lib/libcentrifydc_db2userpass.so
~db2inst1/sqllib/security32/plugin/server/centrifydc_db2userpass.so

cp /usr/share/centrifydc/lib/libcentrifydc_db2gsskrb5.so
~db2inst1/sqllib/security32/plugin/server/centrifydc_db2gsskrb5.so

cp /usr/share/centrifydc/lib/libcentrifydc_db2gsskrb5.so
~db2inst1/sqllib/security32/plugin/client/centrifydc_db2gsskrb5.so

cp /usr/share/centrifydc/lib/libcentrifydc_db2group.so
~db2inst1/sqllib/security32/plugin/group/centrifydc_db2group.so
```

Setup for the Username-Password Plug-In

The username/password plug in library, `centrifydc_db2userpass.so` is now in place. Three more procedures are required to finish Authentication Service for IBM DB2 username/password plug-in installation and configuration:

- Configure the instance's Linux computer(s) to use the Authentication Service for IBM DB2 library for PAM authentication.

    Note: The Authentication Service for IBM DB2 username/password security plug-in uses PAM to authenticate users. This step is required only for DB2 servers running on Linux platforms. On AIX-based computers, the Authentication Service for IBM DB2 username/password plug-in uses the native LAM authentication framework which is already configured for authentication against Active Directory accounts.

- Set parameters in the `/etc/centrifydc/centrifydc.conf` file.
- Assign permissions for the program that checks the password for local users.

1. Configure Linux-based Computers:

    Note: This operation requires root user privileges.

You need to tell the PAM service to use Authentication Service for IBM DB2 plug-in for authentication and account management. The name of the Authentication Service for IBM DB2 username/password plug-in is `centrifydc_db2userpass`.

Each PAM service has its own configuration file in the `/etc/pam.d` directory. To add the Authentication Service for IBM DB2 username/password plug-in on a Red Hat Linux computer, create the file

`/etc/pam.d/centrifydc_db2userpass`

with the following contents:

```
# Delinea PAM service for DB2 username/password support

# %PAM-1.0

auth required pam_stack.so service=system-auth

auth required pam_nologin.so

account required pam_stack.so service=system-auth

#######################################
```

If you are configuring a SUSE Linux 10 computer, the contents of `/etc/pam.d/centrifydc_db2userpass` should be as follows:

```
auth include common-auth

account include common-account
```

If you are configuring a SUSE Linux 8 or 9 computer, the contents of `/etc/pam.d/centrifydc_db2userpass` should be as follows:

```
auth required pam_unix2.so

auth required pam_nologin.so

auth required pam_env.so

account required pam_unix2.so

account required pam_nologin.so
```

2. Set /etc/centrifydc/centrifydc.conf parameters

The following configuration options require you to edit the `/etc/centrifydc/centrifydc.conf` file on the DB2 server.

- If you want to allow users who are already logged in to the DB2 server to log in to the database instance without entering their user name and password, add the following line to `/etc/centrifydc/centrifydc.conf`:

  `db2.userpass.allow.localnopasswd.db2_instance_name: true`

  The default value is `false`, meaning that users already logged in to the server must enter their user name and password to access the database instance.

- If you have an environment in which the user name case used for database authentication differs from user name case stored in `/etc/passwd`, you need to add the following parameter to the

```
/etc/centrifydc/centrifydc.conf file:
db2.userpass.username.lower: true
```

When this parameter is present and set to `true`, the DB2 username/password plug-in converts the user name to lowercase before attempting authentication. When this parameter is set to false, it leaves the case as-is.

- By default, the Delinea DB2 agent authenticates all Active Directory users even if the Active Directory user is not in the zone. To optionally constrain the authentication to zone enabled Active Directory users only, add the following parameter to the `/etc/centrifydc/centrifydc.conf file:`

```
db2.user.zone_enabled.db2_instance_name: true
```

After you add this parameter, restart the DB2 instance to pick up the new setting.

Stop and start the agent after you modify `centrifydc.conf` to enable the conversion.

DB2 Group Plug-in Setup

The following configuration options require you to edit the `/etc/centrifydc/centrifydc.conf` file on the DB2 server.

- By default, the Server Suite group plug-in allows DB2 to get all Active Directory groups even if the Active Directory group is not visible in the zone. You can choose to constrain the DB2visibility to just the zone-visible Active Directory groups. To do so, add the following parameter to the `/etc/centrifydc/centrifydc.conf` file:

```
db2.group.zone_enabled.db2_instance_name: true
```

After you add or edit this parameter, restart the DB2 instance to apply the changes.

GSSAPI Plug-in Setup

This section describes how to configure the server to use the Authentication Service for IBM DB2 GSSAPI plug-in.

1. As root, use the `adjoin` command to join the UNIX DB2 server machine and each UNIX DB2 client using GSSAPI to the same Active Directory domain. See the *Administrator's Guide for Windows* for the `adjoin` command options. Be careful to join the appropriate Active Directory organizational unit and Delinea zone for your configuration.

   > Note: You must have the account name and password for an Active Directory user that has administrator privileges on the Active Directory domain controller to use `adjoin`. If you do not specify the account name in the `adjoin` command line you will be prompted to enter the administrator password.

2. As root, use the `adkeytab` command to create a Kerberos service account for the DB2 instance and generate a `keytab` file. (The `adkeytab` tool is included in the Delinea Server Suite package; see `/usr/sbin`.)

   The following example creates the account for the database instance `db2inst1` in the Users container in the currently joined domain. The account resides on a DB2 server with host name (not fully-qualified) `hostname`, and generates a `keytab` file (`db2inst1.keytab`) in the `$INSTHOME` directory. Substitute your own instance, host, and `keytab` file names as appropriate.

   ```
   adkeytab -n -c CN=Users -u Administrator -K \
   ```

   $INSTHOME/db2inst1.keytab -P db2inst1/hostname db2inst1

If you had wanted to create the account in a different domain than the currently joined domain, you would have used the `adkeytab -d` option.

This example uses the domain controller's Administrator account to generate the `keytab` file and requires root to know the administrator password. If you do not know the administrator password, use the `-u` option to specify any user with administrator privileges on the Active Directory domain controller.

The `adkeytab` command always sets the password of the domain account to a random value regardless of whether the account already exists. Use the following command to change the Active Directory password. This example uses `db2inst1` for the DB2 instance name and `password` for the password string for the instance user's account in Active Directory. Substitute your own instance and password as appropriate.

```
adkeytab -C db2inst1 -w password
```

> **Note:** If there is a local user (for example, in `/etc/passwd` or `/etc/shadow`) with the same account name as the instance user, the `adkeytab` command does not change the local password.

In both examples, you are prompted for the Active Directory Administrator password before the command is executed.

After you have generated the `keytab` file with the `adkeytab` command, do not move or delete it. If you do, the agent will not renew the `keytab`.

In addition, set the service account password in Active Directory to *never expire*.

3. Open the file `/etc/centrifydc/user.ignore` and add the instance user to the end of the file. (This file contains user names that are always treated as local—for example, root, mail, and daemon—when looking up user information.) This allows the instance user to log in as a local user to perform maintenance tasks.

4. Set appropriate permissions to protect the `keytab` file generated in Step 2.

   For the GSSAPI plug-in to work, the `keytab` file must be made readable by the DB2 instance owner. In addition, because the `keytab` file contains sensitive information such as the secret key associated with the DB2 instance service account, it should be properly protected. Execute the following commands as root to achieve this. The following example uses db2inst1 for the DB2 instance name and `db2grp1` for the primary group of the instance user. Substitute your own instance and group names as appropriate.

   ```
   chmod 600 $INSTHOME/db2inst1.keytab
   ```

   ```
   chown db2inst1:db2grp1 $INSTHOME/db2inst1.keytab
   ```

5. Set up the DB2 environment variables to use the new `keytab` file. By default, DB2 uses the `keytab` file defined in the `KRB5_KTNAME` environment variable for authentication. The default is `/etc/krb5.keytab`. The following procedures describe how to set the variable for different UNIX shells. Perform the action as the DB2 instance owner, and replace `db2inst1` with your actual instance name.

   For Bourne, Korn and bash shell users, add the following lines to `$INSTHOME/sqllib/userprofile`:

   ```
   KRB5_KTNAME=$INSTHOME/db2inst1.keytab
   ```

   ```
   export KRB5_KTNAME
   ```

   For C shell users, add the following line to `$INSTHOME/sqllib/usercshrc`:

   ```
   setenv KRB5_KTNAME $INSTHOME/db2inst1.keytab
   ```

By default, DB2 filters out all user environment variables except for those prefixed with `DB2` or `db2`. To pass the value stored in `KRB5_KTNAME` to the DB2 instance, the variable must be added to the `DB2ENVLIST` parameter. To do so, run the following command as the DB2 instance user: `db2set DB2ENVLIST=KRB5_KTNAME`

Before executing `db2set`, you must either:

- Log out after updating the `userprofile` and `usercshrc` files to set the KRB5_KTNAME environment and log back in again; or

- Set the environment variable in your shell before issuing the command.

Then run the `db2set` command as the DB2 instance user:

```
db2set DB2ENVLIST="KRB5_KTNAME"
```

Configure the DB2 Instance

Enter the following commands to modify each DB2 instance's configuration parameters to use the Authentication Service for IBM DB2 plug-ins for authentication and authorization.

All of the following commands should be executed as an instance user.

Case 1: Use the username/password plug-in only:

```
db2 update dbm cfg using SRVCON_PW_PLUGIN centrifydc_db2userpass
```

```
db2 update dbm cfg using SRVCON_AUTH NOT_SPECIFIED
```

```
db2 update dbm cfg using AUTHENTICATION SERVER
```

> **Note:** If you select the SRVCON_AUTH option, the user name and password are transmitted in the clear. This library also includes the following options to encrypt different parts of the message:

- SERVER_ENCRYPT: The user name and password are encrypted in messages sent from DB2 client to DB2 server.

- DATA_ENCRYPT: User data as well as the authentication data (user name and password) are encrypted in messages sent from DB2 client to DB2 server.

- DATA_ENCRYPT_CMP: DATA_ENCRYPT with backwards compatibility to older versions of the DB2 client. (If you have an older version of the DB2 client that does not support the DATA_ENCRYPT option, only the authentication data is encrypted unless you select the DATA_ENCRYPT_CMP option.)

For example, to set the username/password plug-in to encrypt all data going to the server you would use the following command:

```
db2 update dbm cfg using SRVCON_AUTH DATA_ENCRYPT
```

Case 2: Use the GSSAPI plug-in only:

```
db2 update dbm cfg using SRVCON_PW_PLUGIN NULL
```

```
db2 update dbm cfg using SRVCON_GSSPLUGIN_LIST centrifydc_db2gsskrb5
```

```
db2 update dbm cfg using LOCAL_GSSPLUGIN centrifydc_db2gsskrb5
```

```
db2 update dbm cfg using SRVCON_AUTH GSSPLUGIN
```

```
db2 update dbm cfg using AUTHENTICATION SERVER
```

Case 3: Use the username/password plug-in and the GSSAPI plug-in together:

```
db2 update dbm cfg using SRVCON_PW_PLUGIN centrifydc_db2userpass

db2 update dbm cfg using SRVCON_GSSPLUGIN_LIST centrifydc_db2gsskrb5

db2 update dbm cfg using LOCAL_GSSPLUGIN centrifydc_db2gsskrb5

db2 update dbm cfg using SRVCON_AUTH GSS_SERVER_ENCRYPT

db2 update dbm cfg using AUTHENTICATION SERVER
```

For all cases: Run the following command as the DB2 instance user to configure the instance to use the Authentication Service for IBM DB2 group plug-in:

```
db2 update dbmcfg using GROUP_PLUGIN centrifydc_db2group
```

This completes the Authentication Service for IBM DB2 package manual installation and configuration. Next, verify that the configuration parameters are set properly.

Verify the Setup

Execute the following command as the DB2 instance user to verify the setup:

```
db2 get dbm config |egrep -i "auth|gss|group|srvcon"
```

A sample output of this command for a scenario where all three Authentication Service for IBM DB2 security plug-ins have been configured is as follows. The lines of interest are in **bold**.

```
SYSADM group name (SYSADM_GROUP) = DB2GRP1

SYSCTRL group name (SYSCTRL_GROUP) =

SYSMAINT group name (SYSMAINT_GROUP) =

SYSMON group name (SYSMON_GROUP) =
```

Group Plugin (GROUP_PLUGIN) = centrifydc_db2group

GSS Plugin for Local Authorization (LOCAL_GSSPLUGIN) = centrifydc_ db2gsskrb5

Server List of GSS Plugins (SRVCON_GSSPLUGIN_LIST) = centrifydc_ db2gsskrb5

Server Userid-Password Plugin (SRVCON_PW_PLUGIN) = centrifydc_ db2userpass

Server Connection Authentication (SRVCON_AUTH) = GSS_SERVER_ENCRYPT
Database manager authentication (AUTHENTICATION) = SERVER

```
Cataloging allowed without authority (CATALOG_NOAUTH) = NO

Trusted client authentication (TRUST_CLNTAUTH) = CLIENT

Bypass federated authentication (FED_NOAUTH) = NO
```

After installing the plug-ins, the database instance needs to be stopped and restarted. Enter the `db2stop` and `db2start` commands as the instance user.

Upgrade from an Earlier Release

If you are upgrading from an earlier release of Authentication Service for IBM DB2, you have to stop the DB2 instance before the upgrade by using the `db2stop` command. After stopping the DB2 instance, you can upgrade using the `setupdb2.sh` script, or manually by copying the new plug-ins into their corresponding DB2 directories.

Upgrade Using the setupdb2.sh Script

1. Ensure that you have stopped the DB2 instance.

2. Remove the Authentication Service for IBM DB2 software as described in Uninstall DB2 Plug-ins

3. Install the new release of the Authentication Service for IBM DB2 package as described in Install and Configure Server

Upgrade Manually

1. Ensure that you have stopped the DB2 instance.

2. Remove the Authentication Service for IBM DB2 software as described in Uninstall DB2 Plug-ins

3. Perform the procedures described in Install Manually.

4. Restart the DB2 instance after the files are in place using `db2start`.

   If you are currently using a Beta version of the software, refer to Delinea Knowledge Base article KB-0938 for information about how to perform the upgrade.

If an Installation Attempt Fails

If you attempt to install the Authentication Service for IBM DB2 package and the installation fails, before retrying the installation you must uninstall any files that were installed by performing the procedures described in Uninstall DB2 Plug-ins

Next Step:

Set Up the GSSAPI Client

Set up the GSSAPI DB2 Client

The Authentication Service for IBM DB2 GSSAPI security plug-in has a client component that must be installed on each DB2 UNIX-based client computer accessing the DB2 server.

DB2 Client Installation on a UNIX Computer

Copy the Delinea for DB2 package to each client. Unzip, restore, and install the package as described in Install and Configure Server.

Just like the DB2 server, you can use either use the `setupdb2.sh` setup script or manually install and configure the software. The following sections describe these procedures.

Install on UNIX Using the `setupdb2.sh` Script

To install the Delinea for DB2 package using the `setupdb2.sh` script, perform the steps described in Install and Configure Plug-ins Using the setupdb2.sh Script

> 📝 **Note:** The `setupdb2.sh` script may wrongly identify a DB2 version 8 client as a DB2 server. If this happens, when the script prompts you to confirm the detection, answer **no**. The script will then install the GSSAPI plug-in for DB2 client.

Install on UNIX Manually

Perform the following steps to install the Delinea for DB2 package manually.

To install the Authentication Service for IBM DB2 manually:

1. Copy the shared libraries. Run the following commands as the instance user to copy the shared libraries to the target directories where `db2inst1` is the instance name:

   - For a 64-bit DB2 instance:

   `cp /usr/share/centrifydc/lib64/libcentrifydc_db2gsskrb5.so`

   ~db2inst1/sqllib/security64/plugin/client/centrifydc_db2gsskrb5.so

   cp /usr/share/centrifydc/lib/libcentrifydc_db2gsskrb5.so

   ~db2inst1/sqllib/security32/plugin/client/centrifydc_db2gsskrb5.so

   - For 32-bit instances, run:

   `cp /usr/share/centrifydc/lib/libcentrifydc_db2gsskrb5.so`

   ~db2inst1/sqllib/security32/plugin/client/centrifydc_db2gsskrb5.so

2. Set up the DB2 configuration variables. As the DB2 instance user, run the following commands to tell DB2 to use server authentication schemes:

   `db2 update dbm cfg using LOCAL_GSSPLUGIN centrifydc_db2gsskrb5`

   db2 update dbm cfg using AUTHENTICATION SERVER

Test the Installation

This section describes how to test the Authentication Service for IBM DB2 security plug-ins after installation. The test can be performed on the DB2 server or from a computer with DB2 client software installed.

The procedure described below shows how an Active Directory user accesses a DB2 instance. The user joe is the Active Directory user in the same zone as the DB2 computer from which the test is executed. The DB2 database instance name is `db2inst1`, and `sample` is the database.

1. Grant the user joe access to select from a table. Log in as the instance user and run the following commands to grant user joe the right to select from the PROJECT table in the sample database:

```
db2 connect to sample
```

db2 GRANT SELECT on PROJECT to USER joe

db2 terminate

2. After joe logs in, he should set up the environment variables before connecting to the database. From the shell prompt:

- Set the `INSTHOME` environment variable to the home directory of the instance user. For example, if you are using Bourne shell or equivalent, type:

```
eval export INSTHOME=~db2inst1
```

- Set up the database environment using the following commands.

  Bourne shell or equivalent:

  ```
  . $INSTHOME/sqllib/db2profile
  ```

  C-shell or equivalent:

  ```
  source $INSTHOME/sqllib/db2cshrc
  ```

These commands can also be added to joe's login script such as

`.cshrc` or `.profile`

3. Connect to the sample database as joe using the following commands:

- To test single sign-on, type:

  ```
  db2 connect to sample
  ```

- To test connecting using user name and password, type:

  ```
  db2 connect to sample user joe
  ```

  You should see output similar to the following:

  ```
  Database Connection Information
  ```

  Database server = DB2/Linux 9.0

  SQL authorization ID = JOE

  Local database alias = SAMPLE

4. Verify that the database is functioning by querying the `PROJECT` table:

```
db2 select '*' from db2inst1.project
```

Uninstall DB2 Plug-Ins

Perform the uninstallation procedures described in the following sections on each instance from which you want to remove the Authentication Service for IBM DB2 plug-in software. You must perform these procedures before you upgrade to a new Authentication Service for IBM DB2 release, or to remove a partially installed Authentication Service for IBM DB2 release after a failed installation attempt.

The uninstallation procedures are as follows. Unless otherwise noted, each procedure is required.

- **Execute the uninstalldb2.sh Script** on DB2 clients and servers to revert DB2 to the settings that existed before the Authentication Service for IBM DB2 package was installed.
- **Manually Reset DB2 Configuration Variables**. This procedure is optional. In most situations, the `uninstalldb2.sh` script automatically resets DB2 configuration variables to their default values, or to the values that they had before the Authentication Service for IBM DB2 package was installed.

Execute the uninstalldb2 Script

The uninstallation script /usr/share/centrifydc/bin/uninstalldb2.sh will undo the Authentication Service for IBM DB2 installation and revert DB2 to its previous settings. The uninstalldb2.sh script can be run on a DB2 client and a DB2 server. The following table lists the uninstalldb2.sh options.

Options	Required	Values	Description
inst	Yes	A string value	The name of a DB2 database instance.
verbose	No	0 or 1 The default is 1	If the value is 0, only the basic questions are asked. All 3 Authentication Service for IBM DB2 plug-ins are uninstalled. If the value is 1, the script prompts for different options, such as which plug-ins to remove.
debug	No	0 or 1 The default is 0	If the value is 0, uninstallation is performed. If the value is 1, the script displays the steps without actually performing them. Each command is displayed with a "#" prefix. Use this option to preview what commands are executed in an actual invocation.

Because the `inst` option is required, you must know the name of the instance from which you are removing the Authentication Service for IBM DB2 plug-in software. The following section describes how to determine the instance name.

Determine the Instance Name

You can determine the instance name in one of these ways:

- By reviewing the DB2 log in this location:

    `$INSTHOME/sqllib/db2dump/`
- By executing the following command:

    `$INSTHOME/sqllib/bin/db2ilist`

Run the uninstalldb2.sh Script

The format for script options is *option=value*. In the following example, `db2inst1` is the name of a DB2 database instance, the verbose option is selected, and the debug mode is not invoked:

`uninstalldb2.sh inst=db2inst1 verbose=1`

Execute the `uninstalldb2.sh` script now using options that are appropriate for your DB2 server or client.

Manually Reset DB2 Configuration Variables

> **Note:** This procedure is optional, as configuration variables are typically reset by the `uninstalldb2.sh` script.

Perform the procedure described in this section to manually set the DB2 configuration variables back to the values they had before the plug-ins were installed. If you know the original plug-in values, reset them accordingly.

If you do not know the original values, use the following commands to reset the variables to their default values. Run these commands as the instance owner:

```
db2 update dbm cfg using SRVCON_AUTH NOT_SPECIFIED

db2 update dbm cfg using AUTHENTICATION SERVER

db2 update dbm cfg using GROUP_PLUGIN NULL

db2 update dbm cfg using LOCAL_GSSPLUGIN NULL

db2 update dbm cfg using SRVCON_GSSPLUGIN_LIST NULL

db2 update dbm cfg using SRVCON_PW_PLUGIN NULL
```

> **Note:** These commands work for both a DB2 client and a DB2 server.

References

For further information about setting up DB2, see the following documentation:

- Quick Beginnings for DB2 Servers
- DB2 DB2 UDB Security Part 1: Understand how user and group accounts interact with DB2 UDB