IBM Db2 Hosted
Version 1 Release 1

User Guide
(Last udpated: 2017-06-20)

Note

Before using this information and the product that it supports, read the information in Notices and trademarks.

Edition Notice

This edition applies to version 1, release 1, modification 0 of IBM Db2 Hosted and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. About IBM Db2 Hosted for Bluemix

Db2 Hosted is a hosted Db2® database service. Provisioned on-demand when you purchase the service, Db2 database is installed on a host machine in the cloud. After the server is set up, you take over management of the server.

Overview

Here are some key details about how your Db2 Hosted server is set up.

Welcome email

After you purchase a Db2 Hosted service, you receive a “Welcome“ email that contains the IP address of your server and login credentials for a default administrative user.

The password given for the default administrative user in the “Welcome“ email is temporary:

- The first time you log in to your Db2 Hosted server, you are prompted to change the temporary password.
- If you don’t log in within 30 days of receiving the “Welcome“ email, the password is automatically reset. Contact `db2cloud@us.ibm.com` to obtain a new one.

Server security

- **SSH** - You must use Secure Shell (SSH) to log in to your Db2 Hosted server. Linux and UNIX come with the `ssh` client. On Windows, you can install an ssh client, such as one with Cygwin or Putty to connect to Db2 Hosted.
- **iptables** - Network access to your Db2 Hosted server is secured with iptables rules.

Default administrative user: adminuser

Your Db2 Hosted server is set up with a default administrative user with the username adminuser.

The default administrative user cannot run restricted commands directly, but has sudo privileges to be able to run those commands.

For example, running the command useradd fails:

```
[adminuser@123.45.678.90 ~]$ useradd testuser
-bash: /usr/sbin/useradd: Permission denied
```

But adding the sudo command succeeds, when authenticated with your password:

```
[adminuser@123.45.678.90 ~]$ sudo useradd testuser
```

Default instance: db2inst1

Your Db2 Hosted server is set up using a default root installation, with a default database manager instance named db2inst1.

The default instance is set up with some convenient features:

- **A default keystore** that you can use to create encrypted databases and access remote storage
- **A self-signed certificate** that you can use for SSL connections

You can create more instances too, but the default instance is created for you and ready to use right away.

Default instance owner: db2inst1

Your Db2 Hosted server is set up with a default instance owner with the username db2inst1.

You cannot log in to your Db2 Hosted server directly as the user db2inst1. Instead, log in to your Db2 Hosted server as the default administrative user, and then use the su command to switch the ownership of your login session to db2inst1:

```
[adminuser@123.45.678.90 ~]$ db2start
-bash: db2start: command not found
[adminuser@123.45.678.90 ~]$ sudo su - db2inst1
Last login: Sun Oct  2 11:43:48 CDT 2016 on pts/0
[db2inst1@123.45.678.90 ~]$ db2start
10/02/2016 13:32:04     0   0   SQL1026N  The database manager is already active.
SQL1026N  The database manager is already active.
[db2inst1@123.45.678.90 ~]$ logout
[adminuser@123.45.678.90 ~]$
```

Chapter 2. Recommended tools for working with your Db2 Hosted server

You can use the same, favorite tools with your Db2 Hosted sever that you use with your on-premises Db2® servers. Here are three tools that are particularly useful with Db2 Hosted for migrating, managing, and developing.

Migrate: IBM Bluemix Lift

IBM Bluemix Lift makes it simple to quickly and securely migrate your on-premises databases to your Db2 Hosted server:

- Ingests data 10 times faster than traditional data movement solutions
- Eliminates the downtime associated with database migrations
- Encrypts your data as it travels across the wire
- Allows you to kick off a large database migration and walk away without worry

Manage: IBM Data Server Manager

IBM Data Server Manager helps you administer, monitor, manage, and optimize the performance of Db2 Hosted as well as all your other data management software:

- Provides you with the information you need to manage performance proactively and prevent problems before they impact your business
- Simplifies database administrative tasks for both expert and novice users
- Access multiple IBM data management platforms without the need to install or update any client code
- Consolidates information from multiple systems in a single graphical interface that is accessible from any standard web browser

Data Server Manager is available in two editions:

- Data Server Manager Base Edition offers database administration and basic performance monitoring capabilities to all Db2 clients at no charge. All the Db2 Hosted Standard plans can use this edition.
- Data Server Manager Enterprise Edition offers more advanced capabilities such as centralized configuration management, advanced performance management, and query tuning capabilities with expert advice. Data Server Manager optionally uses the repository database to enable features that rely on historical persistence. With a repository database, you can record monitoring metrics for historical analysis, identify storage access patterns for capacity planning, and track configuration changes for problem determination. All the Db2 Hosted Advanced plans can use this edition.

Related information

- Setting up Data Server Manager

Develop: IBM Data Studio

IBM Data Studio is an integrated, modular environment for database development and administration with collaborative database development tools:

- Streamlines database development with easy-to-use query validation, object management, and system deployment features
- Improves collaboration through an integrated environment and shared platforms
- Saves time and reduces errors with advanced data management, configuration, and administration tools and features

Chapter 3. Maintaining your Db2 Hosted server

The Db2 Hosted service is hosted, not managed. That means you have the freedom and flexibility to configure your server for your purposes. It also means you are responsible for maintaining the software on your Db2 Hosted server, including the operating system, firewalls, and the Db2 database software.

You can administer Db2 Hosted with the same utilities and tools that you use for on-premises Db2 servers.

Procedure

Apply the same best practices that you would use with your on-premises Db2 servers:

- Install only properly licensed software, including any open source software.
- Regularly update the Db2 database software.
- Regularly update the operating system.
- Regularly back up your data.
- Implement a strategy that provides the level of availability you need.

Related information

- Database administration

Adding users to your Db2 Hosted server

You should not perform day-to-day activities on your Db2 Hosted server as the default administrative user. Instead, create users on your Db2 Hosted server with just enough access and privileges to perform tasks.

Procedure

Perform the following steps on your Db2 Hosted server to add a new user and grant them authority to perform Db2 commands:

1. Add a new user by issuing the **`useradd`** command.

   Example - Adding a user with the username “db2ctrluser“

   ```
   [adminuser@123.45.678.90 ~]$ sudo useradd db2ctrluser
   [adminuser@123.45.678.90 ~]$ sudo ls -l /home
   total 8
   drwxr-xr-x 2 adminuser   adminuser   4096 Jun  6 19:03 adminuser
   drwx------ 2 db2ctrluser db2ctrluser 4096 Oct  4 11:55 db2ctrluser
   ```

   Notes: - Remember that the default administrative user must use the **`sudo`** command to issue restricted commands. - Replace “db2ctrluser“ with a username you choose. - The **`useradd`** command causes a home directory to be created for the new use in /home.
2. Set the new user’s password by issuing the **`passwd`** command.

   Example - Setting the new user’s temporary password

   ```
   [adminuser@123.45.678.90 ~]$ sudo passwd db2ctrluser
   Changing password for user db2ctrluser.
   New password:
   Retype new password:
   passwd: all authentication tokens updated successfully.
   [adminuser@123.45.678.90 ~]$ sudo chage -d 0 db2ctrluser
   ```

   Notes: - You cannot see the new password as you type it. - The **`chage`** command will force the user to change the password after the first login.
3. Enable the new user to log in with SSH. In the file `/etc/ssh/sshd_config`, append the new username to the end of the line that starts with “AllowUsers“.

Example - The line that begins with “AllowUsers“ showing username “db2ctrluser“ appended

```
AllowUsers adminuser db2ctrluser
```

4. Restart the SSH server.

   ```
   sudo service sshd restart
   ```

5. Enable the new user to issue Db2 commands.

   One way to to this is to reference the .bash_profile Bash shell initialization file (.bash_profile) of the default instance owner in the .bash_profile file of the new user.

   Example - The last line of the .bash_profile file of the new user

   ```
   . /home/db2inst1/sqllib/db2profile
   ```

6. Grant the new user the needed authority.

   Example - Granting the new user SYSCTRL authority

   ```
   [adminuser@123.45.678.90 ~]$ sudo usermod -a -G g_sysctl db2ctrluser
   [adminuser@123.45.678.90 ~]$ groups db2ctrluser
   db2ctrluser : db2ctrluser g_sysctl
   ```

   Note: The groups command shows what groups the user belongs to.

Now, the new user:

- can log in to your Db2 Hosted server using SSH
- will be prompted to change the temporary password on first login
- can perform tasks permitted by their authority level

Related information

- Authorization, privileges, and object ownership

Configuring your Db2 Hosted server for HADR

The basic process for setting up a High Availability Disaster Recovery (HADR) primary-standby pair is the same with a Db2® Hosted server as it is for on-premises Db2 databases, but with one extra configuration step.

Because network access to Db2 Hosted servers is secured by using iptables rules, on the Db2 Hosted server (or servers) hosting your HADR primary and standby databases you must open the ports that are set in the `HADR_REMOTE_SVC` and `HADR_LOCATE_SVC` database configuration parameters:

Procedure

1. Switch the ownership of your login session to db2inst1 using the su command.

   ```
   [adminuser@123.45.678.90 ~]$ sudo su - db2inst1
   Last login: Sun Oct  2 11:43:48 CDT 2016 on pts/0
   ```

   Remember that the default administrative user must use the sudo command to issue restricted commands.

2. Determine the ports used for `HADR_LOCAL_SVC` and `HADR_REMOTE_SVC`.

   Example - Viewing the ports for database “hadb1“

   ```
   [db2inst1@123.45.678.90 ~]$ db2 "get db cfg for hadb1" |grep HADR_.*_SVC
   HADR local service name                (HADR_LOCAL_SVC) = 50500
   HADR remote service name              (HADR_REMOTE_SVC) = 50504
   ```

3. Switch the ownership of your login session back to adminuser.

```
[db2inst1@123.45.678.90 ~]$ logout
[adminuser@123.45.678.90 ~]$
Last login: Sun Oct  2 11:43:48 CDT 2016 on pts/0
```

4. Configure the server to accept connections on those HADR ports using iptables rules.

```
[adminuser@123.45.678.90 ~]$ sudo iptables -I INPUT -p tcp --dport 50500 -j ACCEPT
[adminuser@123.45.678.90 ~]$ sudo iptables -I INPUT -p tcp --dport 50504 -j ACCEPT
```

5. Save the changes.

```
[adminuser@123.45.678.90 ~]$ sudo iptables-save | tee /etc/sysconfig/iptables
[adminuser@123.45.678.90 ~]$ sudo iptables-save | tee /root/iptables
[adminuser@123.45.678.90 ~]$ sudo systemctl restart iptables
```

Related information

- Initializing high availability disaster recovery (HADR)

Chapter 4. Securing your Db2 Hosted server

The Db2 Hosted service is hosted, not managed. That means you have the freedom and flexibility to configure your server for your purposes. It also means you are responsible for keeping your Db2 Hosted server secure.

Procedure

Apply the same best practices that you would use with your on-premises Db2 servers:

- Actively monitor and report any security issues you encounter.
- Maintain software firewalls.
- Restrict network access. When the server is first delivered, network access to the server is secured by using iptables rules. Some examples of using the iptables command are shown below.

Example 1

Displaying the rules and the status of the iptables firewall

```
[adminuser@123.45.678.90 ~]$ sudo iptables -L
```

Remember that the default administrative user must use the **`sudo`** command to issue restricted commands.

Example 2

Allowing incoming connections from only a specified range of IP addresses

```
[adminuser@123.45.678.90 ~]$ sudo iptables -A INPUT -i eth0 -p tcp
  -s 192.168.100.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
```

Example 3

Allowing incoming connections from only a single IP address

```
[adminuser@123.45.678.90 ~]$ sudo iptables -A INPUT -i eth0 -p tcp
  -s 192.168.100.11 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
```

Related information

- Db2 security model overview

Creating encrypted databases on your Db2 Hosted server

Your Db2 Hosted server is set up ready for you to create encrypted databases.

- Your default instance, db2inst1, is set up with a default local keystore that you can use with Db2 native encryption.

  You can see the details of this default keystore by viewing the keystore-related database manager configuration parameters, `KEYSTORE_TYPE` and `KEYSTORE_LOCATION`:

  ```
  [db2inst1@123.45.678.90 ~]$ db2 "get dbm cfg" | grep KEYSTORE
   Keystore type                    (KEYSTORE_TYPE) = PKCS12
   Keystore location            (KEYSTORE_LOCATION) = /home/db2inst1/keystore/db2keystore.p12
  ```

- Your Db2 Hosted server comes with IBM® Global Security Kit (GSKit) installed and configured for managing keystores.

Procedure

To create an encrypted database with the default settings, specify the ENCRYPT option with the CREATE DATABASE command.

```
[db2inst1@123.45.678.90 ~]$ db2 "create db myencdb encrypt"
```

Related information

- Db2 native encryption

Setting up SSL connections between applications or clients and your Db2 Hosted server

Your Db2 Hosted server is set up ready for you to use Secure Sockets Layer (SSL) connections.

On the Db2 Hosted server:

- Your default instance, db2inst1, is set up already configured to support SSL connections and has a self-signed certificate, `/home/db2inst1/sqldb_ssl.arm`.
- Your default instance is configured to listen for SSL connections on port 50001.

On the client computer, some prerequisite software is needed:

- **SFTP client** - Transferring files to or from your Db2 Hosted server must be done using SSH File Transfer Protocol (SFTP). If you do not already have an SFTP client on your client computer, install one (such as Cygwin or FileZilla SFTP client on Microsoft® Windows.)
- **Keystore manager** - Certificates need to be stored in a keystore. If you do not already have keystore management software on your client computer, here are some examples you could install:
  - A Db2 client or the IBM Data Server Driver Package can do this for you.
  - The Java Runtime Environment (JRE) includes the keytool utility, which you can use to manage a keystore on the client.
  - You can use IBM Global Security Kit (GSKit) to manage a keystore on the client computer. Documentation: GSKCapiCmd User’s Guide.

Procedure

1. From the client computer, download the self-signed certificate file `/home/db2inst1/sqldb_ssl.arm` from the Db2 Hosted server.

   Example - Using SFTP in a Cygwin terminal to download the certificate

   ```
   $ sftp adminuser@123.45.678.90
   adminuser@123.45.678.90's password:
   Connected to 123.45.678.90.
   sftp> cd /home/db2inst1
   sftp> get sqldb_ssl.arm
   Fetching /home/db2inst1/sqldb_ssl.arm to sqldb_ssl.arm
   /home/db2inst1/sqldb_ssl.arm                    100%  952     0.9KB/s   00:00
   sftp>
   ```

   Notes: - Replace `123.45.678.90` with the IP address or host name of your Db2 Hosted server. - In this example, the client computer has a Windows operating system. - The certificate is now in the Cygwin user home directory.
2. Configure the application or connection to use SSL. The specific steps for doing this vary. Some examples are given below.

Examples

In the following examples, assume these details:

- The IP address of the Db2 Hosted server is 123.45.678.90.
- The database named “njsdb“ exists on the Db2 Hosted server.
- A user named “db2user“ with access to the database njsdb exists on the Db2 Hosted server.

- The self-signed certificate, `sqldb_ssl.arm`, that was downloaded from the Db2 Hosted server is located on the client computer in the Cygwin home directory of user “sally“: `D:\cygwin64\home\sally`.

Example 1

Connect through CLPPlus

In this example, assume the IBM Data Server Driver Package is installed on the client computer.

1. Register the database using a command prompt, then connect with CLPPlus:

```
c:\>db2cli writecfg add -database njsdb -host 123.45.678.90 -port 50001 -parameters
      "SecurityTransportMode=SSL;SSLServerCertificate=D:\cygwin64\home\sally\sqldb_ssl.arm"
c:\>db2cli writecfg add -dsn alias1 -database njsdb -host 123.45.678.90 -port 50001
c:\>clpplus db2user@alias1
```

2. In the CLPPlus window, complete the connection by entering the password for user db2user:

```
CLPPlus: Version 1.6
Copyright (c) 2009, 2011, IBM CORPORATION.  All rights reserved.

Enter password: ********

Database Connection Information:
--------------------------------
Hostname = 123.45.678.90
Database server = DB2/LINUXX8664 SQL10057
SQL authorization ID = db2user
Local database alias = ALIAS1
Port = 50001

SQL>
```

Example 2

Connect in a JDBC application

(In this example, assume the IBM Data Server Driver for JDBC and SQLJ is installed on the client computer.)

1. Create a keystore and import the downloaded certificate using the keytool utility:

```
c:\>keytool -importcert -file D:\cygwin64\home\sally\sqldb_ssl.arm -keystore c:\mykeystore
Enter keystore password:
Re-enter new password:
...
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

2. Create a simple Java application in the file `test.java`:

```
import java.sql.*;
public class test {
  static final String conn_str =
    "jdbc:db2://123.45.678.90:50001/njsdb:" +
    "user=db2user;password=t3st.Pwd;" +
    "sslConnection=true;";
  public static void main(String[] args) {
    try {
      Class.forName( "com.ibm.db2.jcc.DB2Driver" );
      Connection conn = DriverManager.getConnection( conn_str );
      System.out.print( "Connect successful." );
        conn.close();
    }
    catch( SQLException se ) {
      se.printStackTrace();
    }
    catch( Exception e ) {
      e.printStackTrace();
    }
  }
}
```

3. Compile the application:

   c:>javac test.java

4. Run the application, specifying the location of the keystore with the Java system property **`javax.net.ssl.trustStore`**:

   c:>java -Djavax.net.ssl.trustStore=c:\mykeystore test Connect successful.

Related information

- Configuring Secure Sockets Layer (SSL) support in non-Java Db2 clients
- IBM Data Server Driver for JDBC and SQLJ support for SSL
- The SSL protocol support in CLPPlus

Chapter 5. Accessing remote storage with your Db2 Hosted server

You can access IBM® SoftLayer Object Storage and Amazon Simple Storage Service (S3) directly through database commands, such as the **BACKUP** command, using remote storage access aliases.

- To be able to access remote cloud storage for backup, restore, load, and ingest operations, you need to create a storage access alias. When you create a storage access alias, your remote cloud storage account credentials are safely stored in an encrypted keystore.
- Your default instance, db2inst1, is set up with a default local keystore that you can use with storage access aliases.

You can see the details of this default keystore by viewing the keystore-related database manager configuration parameters, `KEYSTORE_TYPE` and `KEYSTORE_LOCATION`:

```
[db2inst1@123.45.678.90 ~]$ db2 "get dbm cfg" | grep KEYSTORE
 Keystore type                    (KEYSTORE_TYPE) = PKCS12
 Keystore location            (KEYSTORE_LOCATION) = /home/db2inst1/keystore/db2keystore.p12
```

- Your Db2 Hosted server comes with IBM Global Security Kit (GSKit) installed and configured for managing keystores.

Procedure

1. Create a storage access alias by issuing the `CATALOG STORAGE ACCESS` command.

   Example - Creating an alias called “montrealprivate“ which only the user “thomas“ may use for accessing a container called “container1“ which was previously created on the SoftLayer private authentication endpoint in Montreal

   ```
   [db2inst1@123.45.678.90 ~]$ db2 "catalog storage access alias montrealprivate vendor softlayer
   server https://mon01.objectstorage.service.networklayer.com/auth/v1.0/
   user SLOS482762-5:SL729462
   password a1b635c2556681ddd8354daa2db1dbc88bb6da3311c8904319058a9434169c3
   container container1 dbuser thomas"
   ```

2. Specify the storage access alias with the backup, restore, load, or ingest operation.

   Example 1 - Backing up to remote storage

   ```
   [db2inst1@123.45.678.90 ~]$ db2 "backup db testdb to db2remote://montrealprivate//bkupdir"
   ```

   Example 2 - Restoring from remote storage

   ```
   [db2inst1@123.45.678.90 ~]$ db2 "restore db testdb from db2remote://SwiftAlias//bkupdir/1453245697"
   ```

Related information

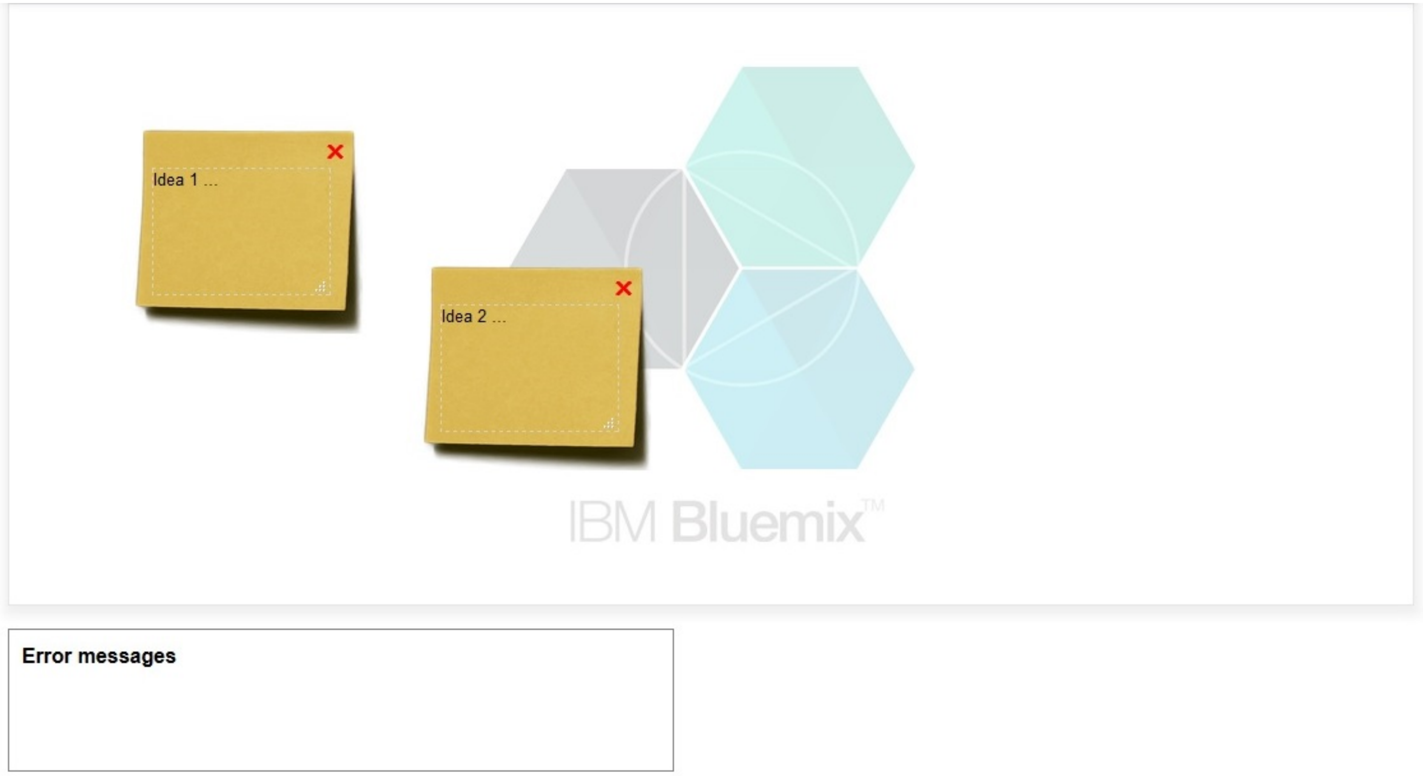
- LOAD command
- INGEST command
- BACKUP DATABASE command
- RESTORE DATABASE command
- LOAD command using the ADMIN_CMD procedure
- BACKUP DATABASE command using the ADMIN_CMD procedure

Chapter 6. Sample: Node.js app on IBM Bluemix

A Node.js web app that stores data in a Db2 Hosted database and is hosted on IBM® Bluemix®.

Goal

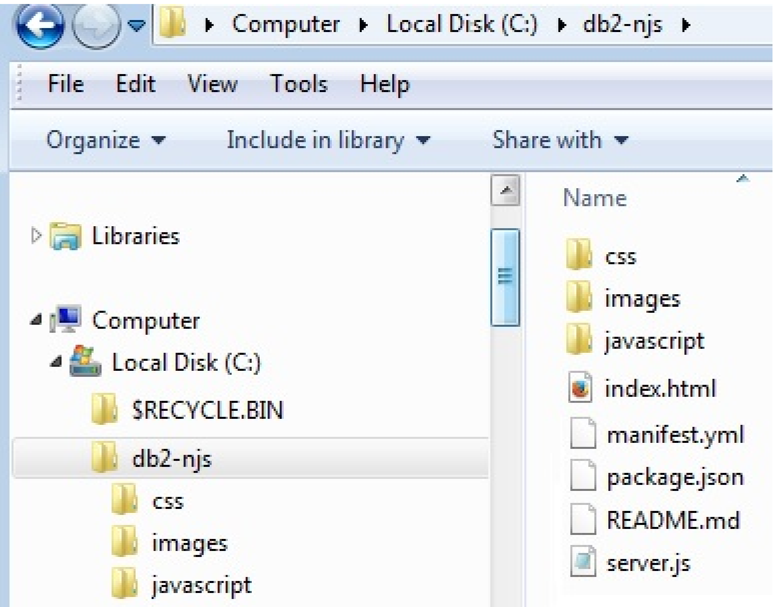
Build a Node.js web app that stores data in a Db2 Hosted database and is hosted on IBM Bluemix:



Prerequisites

1. Sign up for a Bluemix account: (https://console.ng.bluemix.net/registration)
2. Create a new user ID on your Db2 Hosted server with the following properties:
   - The user ID can connect to your Db2 Hosted server using a Secure Shell (SSH)
   - The user ID has SYSCTRL authority

   See the example in Adding users to your Db2 Hosted server.
3. Install the following software on your local computer:
   - Python (https://www.python.org/downloads)
   - Node.js (https://nodejs.org/en/download)
   - Cloud Foundry cf command line interface (http://docs.cloudfoundry.org/cf-cli/install-go-cli.html)
4. Create an empty working directory on your local computer. (Example: `C:\db2-njs`.)
5. Download the sample files from this blog post. Then, extract the sample files into your working directory:



6. From a command prompt, in your working directory, run the following command:

```
npm install
```

This will create a new subdirectory, called `node_modules`, in your working directory and install four Node.js packages that are listed as dependencies in the file `package.json`.

Step 1: Create a database for the app data

1. From your local computer, log in to the Db2 Hosted server as a user with SYSCTRL authority by issuing the following command in a SSH client:

```
ssh db2user@123.45.678.90
```

2. On the Db2 Hosted server, create a database for your app to use by issuing the following Db2 command and SQL statements:

```
db2start;
db2 "create database NJSDB";
db2 "connect to NJSDB";
db2 "create table NJSTBL( ID double, X int, Y int, TEXT varchar(500) )";
db2 "insert into NJSTBL values( 3456.78, 202, 80, 'Hello' )";
db2 "select * from NJSTBL";
```

Step 2: Run the sample code on your computer

1. Open the file `server.js` in an editor (a plain text editor is fine.)
2. In the file `server.js`, update the connection string by specifying the IP address or host name of your Db2 Hosted server as well as the credentials of a user ID able to connect to and query from your NJSDB database:

```
var connStr = 'DRIVER={DB2};' +
              'HOSTNAME=123.45.678.90' +
              'PORT=50000;' +
              'DATABASE=NJSDB;' +
              'UID=db2user;' +
              'PWD=xxxxxxx';
```

3. Save `server.js`, and then from a command prompt, in your working directory, start the app:

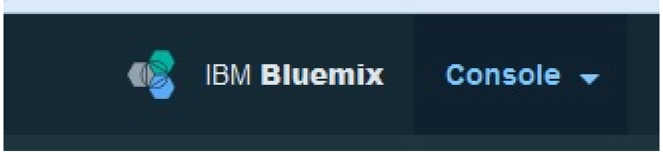
```
node server.js
```

4. Open the file `index.html` in a web browser, and click in the work space to see sticky notes added. Open `index.html` in a second browser window to see real-time updates in both windows.

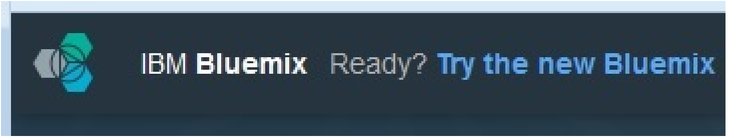
Step 3: Create an empty Node.js app in Bluemix

Note: You can view the Bluemix web interface in two different modes that look different, “New“ and “Classic“.

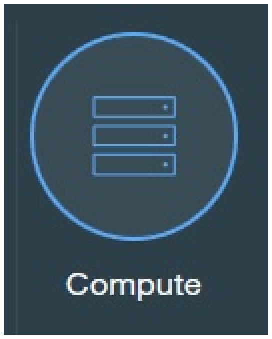
The top, left corner of the New interface looks like this:



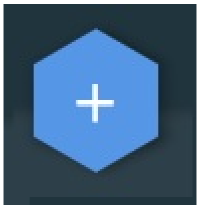
If you are in the Classic interface, you can switch to the New interface by clicking the link labeled “Try the new Bluemix“ in the top, left corner of the Classic interface:



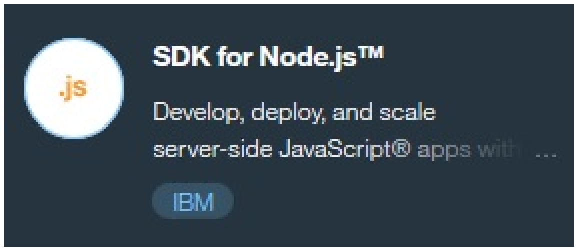
1. Connect to Bluemix: (http://www.ibm.com/cloud-computing/bluemix)
2. In the “Overview“ area of the main Bluemix console, click the “Compute“ tile:



3. Then, click the plus symbol to add a new app:

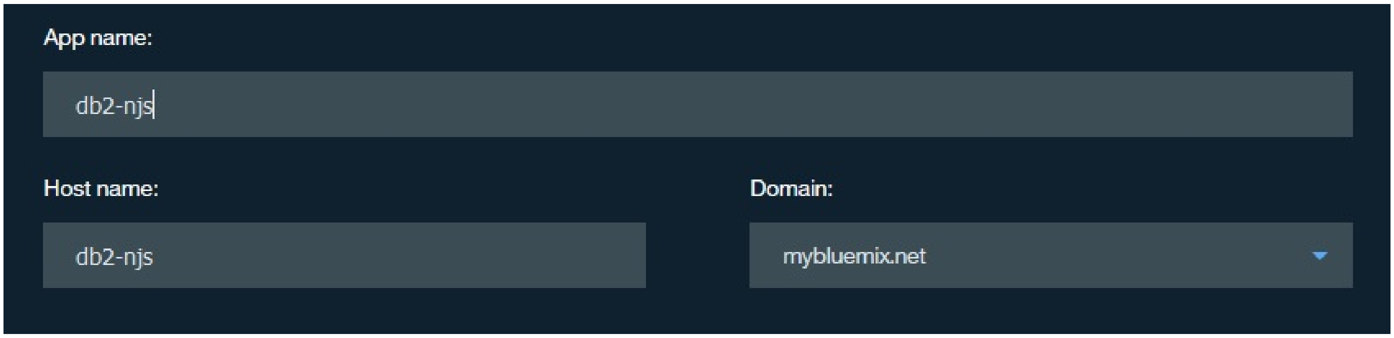


4. In the “Runtimes“ section, click on the “SDK for Node.js“ item:


SDK for Node.js™

Develop, deploy, and scale server-side JavaScript® apps with ...

5. In the page that opens, fill in the fields:


App name: db2-njs

Host name: db2-njs

Domain: mybluemix.net

- Provide a unique name for the app and specify the same name for the host (to keep things simple)
- Leave the domain as the default (`mybluemix.net`)
- Choose the “Default“ plan

In this example, the app is named “db2-njs“. However, the name you choose must be unique in Bluemix; the name must not have already been used by another Bluemix user. If you try to create a new app with a name that has already been used by someone else, you’ll get an error message that says “Someone already used the app name … “.

6. Click “CREATE“. (It takes a few seconds for the app to be staged on Bluemix.)

Step 4: Update the sample code to run on Bluemix

1. Open the following files in an editor (a plain text editor is fine):
   - `server.js`
   - `index.html`
   - `package.json`
   - `manifest.yml`
2. Update the file server.js to run on Bluemix.

   The file server.js is written to run locally by default. Specifically, the following line forces the server to listen on local port 8080:

   ```
   io.listen( 8080 );
   ```

   Comment out that line now.
3. Update the file `index.html` to run on Bluemix.

   The file `C:\db2-njs\index.html` is written to run locally by default. Specifically, the following line forces the client to connect on local port 8080:

   ```
   var appURL = 'http://localhost:8080';
   ```

   Change that line to point to the URL of your Bluemix app:

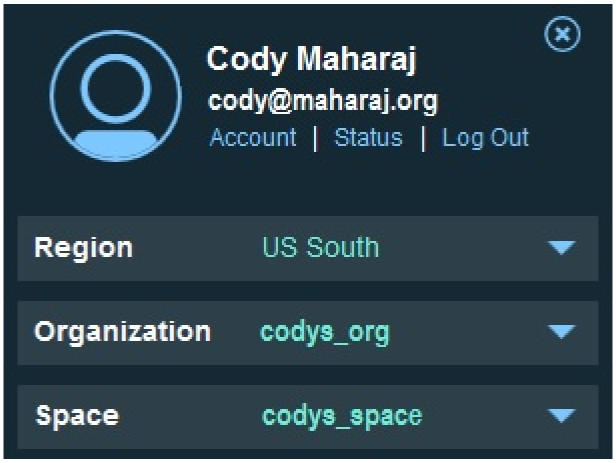
   ```
   var appURL = 'http://db2-njs.mybluemix.net';
   ```
4. Update the file `package.json` with your app name:

   ```
   "name": "db2-njs",
   ```
5. Update the file `manifest.yml` with your app name:

   ```
   name: db2-njs
   host: db2-njs
   ```

Step 5: Push your updated code to Bluemix

1. Determine your Bluemix “Organization“ and “Space“ by looking at the upper-right corner of the Bluemix console:



Cody Maharaj
cody@maharaj.org
Account | Status | Log Out

Region US South

Organization codys_org

Space codys_space

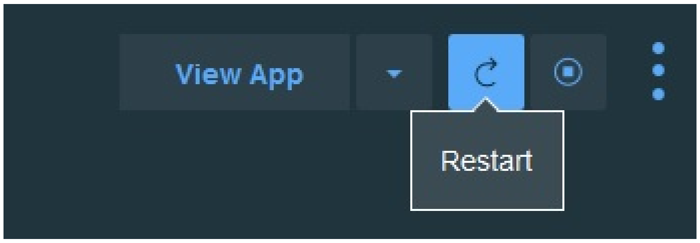
2. From a command prompt, in your working directory, issue the following commands:

```
C:\db2-njs>cf api https://api.ng.bluemix.net
C:\db2-njs>cf login
C:\db2-njs>cf push db2oncloud-nodejs
```

Notes:

- When you enter the **`cf login`** command, the Cloud Foundry tool will prompt you for your Bluemix ID (Email), Organization (Org), and Space.
- The **`cf push`** command can take several minutes to complete.

3. In the app “Overview“ area in the Bluemix console, restart your app:



4. Open the app by clicking the “View App“ button in the app Overview area in the Bluemix console.

Congratulations! You’re done. Share your app URL with your friends and then collaborate on ideas with sticky notes.

Related information

- Learning Center for Db2 Hosted

Notices

This information was developed for products and services that are offered in the USA. Information about non-IBM® products is based on information available at the time of first publication of this document and is subject to change.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Canada Limited
U59/3600
3600 Steeles Avenue East
Markham, Ontario; L3R 9Z7
CANADA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. _*enter the year or years*_. All rights reserved.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at www.ibm.com/legal/copytrade.shtml.

The following terms are trademarks or registered trademarks of other companies and have been used in at least one of the documents in the Db2 documentation library:

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Celeron, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle, its affiliates, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as a customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy, the section entitled “Cookies, Web Beacons and Other Technologies” of the IBM’s Online Privacy Statement, and the IBM Software Products and Software-as-a-Service Privacy Statement.