Best practices

Securely deploying and configuring the DB2 pureScale Feature by using db2ssh

Walid Rjaibi
Senior Technical Staff Member,
Chief Security Architect, IBM Information Management

Venkata S Vanukuru
DB2 for Linux, UNIX and Windows Installation Development

Mihai Iacob
DB2 for Linux, UNIX and Windows Security Development

Prashant S. Naik
DB2 for Linux, UNIX, and Windows Quality Assurance

Vikash Banka
DB2 for Linux, UNIX, and Windows Quality Assurance

Serge Boivin
DB2 Information Development

Table of Contents

Executive summary

The main objective of this paper is to highlight the best practices for securely deploying and configuring the DB2 pureScale Feature by using `db2ssh`. The `db2ssh` is a wrapper around the Secure Shell (SSH) protocol and Secure Copy Protocol (SCP).

DB2 Version 10.1 Fix Pack 2 introduced `db2ssh`. You can use `db2ssh` to run commands as a root user on any host in the General Parallel File System (GPFS) domain. This functionality is achieved by communicating between hosts as a designated non-root ID, thereby removing the requirement of enabling passwordless SSH and remote root login for the root user. As of DB2 Version 10.5, along with GPFS, the installer uses db2ssh to install and configure the DB2 pureScale Feature. Thus, the dependency on passwordless SSH for the root user is removed.

This paper provides the following information:

- An introduction to db2ssh and its configuration
- Information about various methods for installing and configuring the DB2 pureScale Feature with db2ssh enabled
- Troubleshooting tips to resolve problems

Introduction to db2ssh

Before DB2 Version 10.5, to install and configure the DB2 pureScale Feature, you had to enable the remote root login setting and passwordless SSH for the root user. These requirements posed security concerns such as a lack of accountability of who logged in as the root user and allowing root to root SSH without a password or passphrase.

Along with the DB2 installer, the General Parallel File System (GPFS) required the enablement of the remote root login setting and passwordless SSH for the root user for some of the cluster operations. DB2 Version 10.1 Fix Pack 2 introduced `db2ssh` to eliminate these dependencies for GPFS. However, the DB2 installer continued to have these dependencies until DB2 Version 10.5. In that release the DB2 installer was enhanced to use `db2ssh`.

The `db2ssh` is installed in the /var/db2/db2ssh directory. It consists of three executables:

- `db2locssh`, which is invoked on the local host
- `db2remssh`, which the db2locssh program invokes on the remote host
- `db2scp`, which uses both the db2locssh and db2remssh files

The `db2ssh` is an SSH wrapper. To use db2ssh, you must set up a dedicated non-root user i.e. <db2sshid>, with passwordless SSH on the hosts where GPFS is installed.

You can specify the <db2sshid> user in the /var/db2/db2ssh/db2ssh.cfg file.

Configuring `db2ssh` includes a set of private and public root keys that are generated in the /var/db2/db2ssh directory. The public keys on each host are exchanged with every other host's public keys. After you configure `db2ssh`, if you want to run a command on the remote host as the root user, you must invoke `db2locssh` utility on the local host as the root user.

The `db2locssh` utility digitally signs the command with the local host's private key and invokes the db2remssh through the SSH protocol as the <db2sshid> user on the remote host. Once on the remote host, db2remssh verifies the digital message signature by using the originating host's public key. At this point, replay attacks are prevented in one of two ways. For DB2 Version 10.5 FP2 or earlier, 20 seconds are allowed to pass from the time that the message originates to the time that it is received. As of DB2 Version 10.5 FP3, you configure the SSH protocol to protect itself from replay attacks. Regardless of the fix pack, the final steps are to run the command and to return the result to the originating host.

Useful commands of db2ssh

The following commands are useful for verifying the `db2ssh` configuration and for troubleshooting `db2ssh` issues:

- `/var/db2/db2ssh/db2locssh version`

  Displays the version of the `db2locssh`.

- `/var/db2/db2ssh/db2remssh version`

  Displays the version of the `db2remssh`.

- `/var/db2/db2ssh/db2scp version`

  Displays the version of the `db2scp`.

- `/var/db2/db2ssh/db2locssh display_config`

  Displays the `db2ssh` configuration. Sample output is as follows:

```
version = 1

time_delta = 0 second(s)

debug_level = 2

db2sshid = db2ssh1

gskit_path = /var/db2/db2ssh/lib64/gskit_db2/

fips_mode = off

success
```

- `/var/db2/db2ssh/db2locssh reset_config`

  Resets the `db2ssh` configuration to the default values (`set_time_delta` = 20s and `gskit_path` =’’).

- `/var/db2/db2ssh/db2locssh set_gskit_path`

  Sets the path to the IBM® Global Security Kit (GSKit), which provides libraries and utilities for SSL and TLS communication. The `db2ssh` uses GSKit to digitally sign messages.

- `/var/db2/db2ssh/db2locssh set_time_delta x`

  Sets the amount of time that `db2remssh` uses to decide whether to run a message as the root user. The `set_time_delta` option takes an integer value *x* that represents the amount of time in seconds.

- `/var/db2/db2ssh/db2locssh generate_keys -keysize keysize -exponent exponent`

  Generates a pair of RSA public and private keys (*root@host.priv* and *root@host.pub*). The `keysize` and `exponent` options are optional. If you specify only the generate_keys option, keys of 2048 are generated.

- `/var/db2/db2ssh/db2locssh set_db2sshid`

  Sets the non-root ID to use to SSH between hosts. You must set up passwordless SSH for this ID.

- `/var/db2/db2ssh/db2locssh discover_gskit`

  Attempts to discover any available GSKit installations.

- `/var/db2/db2ssh/db2locssh set_icc_fips_mode on|off`

  Turns FIPS on or off. The default is `off`. For information about FIPS compliance, see the IBM Crypto Information Center.

- `/var/db2/db2ssh/db2locssh root@remotehost command`

  Runs the command that is specified for the *command* parameter on the remote host.

Configuring db2ssh by using the setup_db2locssh utility

As of DB2 for Linux, UNIX, and Windows V10.5, an installation utility called `setup_db2locssh` is included to help configure `db2ssh`. The `setup_db2locssh` utility deploys the binaries that `db2ssh` requires and generates the root private and public DSA keys.

To use the setup_`db2locssh` utility to configure db2ssh :

1. Disable remote root login, as follows:

   a. Modify the SSH configuration file as follows:
   `/etc/ssh/sshd_config:`
   `PermitRootLogin no #disabled`

   b. Make the changes take effect by restarting the SSH daemon.
   To restart the SSH daemon, issue the following commands:

   Linux operating systems:
   `/etc/init.d/sshd restart`

   AIX operating systems:
   `stopsrc –s sshd`
   `startsrc –s sshd`

2. On all hosts, create a non-root user ID <db2sshid> with the same UID and GID. The <db2sshid> ID establishes an SSH network protocol between a local host and a remote host.

3. From the *media_ path*/db2/*platform*/utilities directory, run the setup_db2locssh utility:

   `./setup_db2locssh <db2sshid>`
   Setup_db2locssh utility generates two pairs of keys, as follows:

   - A pair of RSA public and private keys for the root user: `root@host.priv` and `root@host.pub`, in the /var/db2/db2ssh directory.
   - A pair of DSA public and private keys for the SSH user: id_dsa and id_dsa.pub, in the *$HOME* /.ssh directory, where *$HOME* is the home directory of the <db2sshid> user.

Consider the following example:

Assume that there are four hosts: sles227, sles231, sles235, and sles239. The following commands generate the keys for the sles227 host:

```
sles227 : media_path/db2/linuxamd64/utilities #
./setup_db2locssh db2ssh1
DBI1070I Program setup_db2locssh completed successfully
```

The pair of RSA public and private keys that are generated for the root user for the host sles227 are as follows:

```
sles227:~ #  ls /var/db2/db2ssh/root*
/var/db2/db2ssh/root@sles227.priv
/var/db2/db2ssh/root@sles227.pub
```

The DSA public and private keys that are generated for the SSH user (db2ssh1 in this example) for the host sles227 are as follows:

```
db2ssh1@sles227:~/.ssh> ls -rlt
-rw-r--r-- 1 db2ssh1 db2grp1 605 Jun 11 11:46 id_dsa.pub
-rw------- 1 db2ssh1 db2grp1 672 Jun 11 11:46 id_dsa
```

The following `setup_db2locssh` commands generate keys for the other three hosts:

```
sles231:media_path/db2/linuxamd64/utilities #
./setup_db2locssh db2ssh1
DBI1070I  Program setup_db2locssh completed successfully.

sles235:media_path /db2/linuxamd64/utilities #
./setup_db2locssh db2ssh1
DBI1070I  Program setup_db2locssh completed successfully.

sles239:media_path /db2/linuxamd64/utilities #
./setup_db2locssh db2ssh1
DBI1070I  Program setup_db2locssh completed successfully.
```

4. Exchange the root public keys, root@*host*.pub, that were generated in the /var/db2/db2ssh directory on each host. After this exchange, every host has the public keys of all other hosts in its /var/db2/db2ssh directory.

In the example of the four hosts sles227, sles231, sles235, and sles239, after the keys are exchanged among the hosts, the following keys are in the /var/db2/db2sssh directory on all the hosts mentioned above

```
ls /var/db2/db2ssh
.metadata  .remote_shell_cmd  db2locssh  db2remssh  db2scp
db2ssh.cfg  gskit  lib32  lib64  root@sles227.priv
root@sles227.pub  root@sles231.pub  root@sles235.pub
root@sles239.pub
```

5. As an SSH user, for example, db2ssh1, create a file called authorized_keys in the *$HOME*/.ssh directory, where *$HOME* is the home directory of the db2ssh1 user.

6. Append the contents of each id_dsa.pub public key from each host to the authorized_keys file.

7. Copy the authorized_keys file to the *$HOME*/.ssh directory on each host, where *$HOME* is the home directory of the db2ssh1 user.

8. Change the permission of the authorized keys on all the hosts by issuing `chmod 644 authorized_keys`.

9. On each host, perform the following steps:

    a. Log in to each host as an SSH user, for example, db2ssh1.
    b. SSH to all the hosts to check whether you can communicate across all hosts without a password prompt. Examples for the sles227, sles231, sles235, and sles239 hosts follow:

On sles227 as db2ssh1 user (su – db2ssh1)

```
ssh sles227

ssh sles231

ssh sles235

ssh sles239
```

On sles231 as db2ssh1 user (su – db2ssh1)

```
ssh sles227

ssh sles231

ssh sles235

ssh sles239
```

On sles235 as db2ssh1 user (su – db2ssh1)

```
ssh sles227

ssh sles231

ssh sles235

ssh sles239
```

On sles239 as db2ssh1 user (su – db2ssh1)

```
ssh sles227

ssh sles231

ssh sles235

ssh sles239
```

Note : To populate the known_hosts with both the short and fully qualified host names, authenticate both types of names.

10. Verify the db2locssh utility configuration by issuing the following remote commands as the root user on each host:

For example, the following list shows the commands to issue as the root user on sles227 and the associated output:

- `/var/db2/db2ssh/db2locssh sles227 'hostname'`

  The command output is sles227.

- `/var/db2/db2ssh/db2locssh sles231 'hostname'`

  The command output is sles231.

- `/var/db2/db2ssh/db2locssh sles235 'hostname'`

  The command output is sles235.

- `/var/db2/db2ssh/db2locssh sles239 'hostname'`

  The command output is sles239.

The following list shows the commands to issue as the root user on sles231and the associated output:

- `/var/db2/db2ssh/db2locssh sles227 'hostname'`

  The command output is sles227.

- `/var/db2/db2ssh/db2locssh sles231 'hostname'`

  The command output is sles231.

- `/var/db2/db2ssh/db2locssh sles235 'hostname'`

  The command output is sles235.

- `/var/db2/db2ssh/db2locssh sles239 'hostname'`

  The command output is sles239.

The following list shows the commands to issue as the root user on sles235 and the associated output:

- `/var/db2/db2ssh/db2locssh sles227 'hostname'`

  The command output is sles227.

- `/var/db2/db2ssh/db2locssh sles231 'hostname'`

  The command output is sles231.

- `/var/db2/db2ssh/db2locssh sles235 'hostname'`

  The command output is sles235.

- `/var/db2/db2ssh/db2locssh sles239 'hostname'`

  The command output is sles239.

The following list shows the commands to issue as the root user on sles239and the associated output:

- `/var/db2/db2ssh/db2locssh sles227 'hostname'`

  The command output is sles227.

- `/var/db2/db2ssh/db2locssh sles231 'hostname'`

  The command output is sles231.

- `/var/db2/db2ssh/db2locssh sles235 'hostname'`

  The command output is sles235.

- `/var/db2/db2ssh/db2locssh sles239 'hostname'`

  The command output is sles239.

Installing and configuring a DB2 pureScale with db2ssh enabled

Three methods are available to install and configure a DB2 pureScale instance with the `db2ssh` enabled: the script installation the graphical user interface (GUI) method, and the silent installation.

Script installation method

With this method, you install and configure the DB2 pureScale Feature by using the command-line interface. Although the `db2_install` command installs all components for the DB2 product that you specify, it does not perform instance creation, DAS creation, or configuration. You might prefer this method of installation if you want to do the configuration after the installation.

To install by using the script installation method:

1. From the DB2 media, configure db2ssh and verify its functionality as described in the section "Configuring db2ssh by using the setup_db2locssh utility".

2. Check whether all the hosts meet the minimum requirements for the DB2 pureScale installation by issuing the `db2prereqcheck` command. (Refer to the knowledge center for details)

3. From the media, install the DB2 pureScale Feature by issuing the `db2_install` command. An example follows:

```
sles227: # ./db2_install -b /opt/IBM/db2/V10.5 -p server -f

PURESCALE -l /tmp/install.log -t /tmp/install.trc
```

4. Create an instance by issuing the `db2icrt` command, providing member and CF details. An example follows:

```
db2icrt -d  -instance_shared_dev /dev/sdt  -tbdev /dev/sde

-cf sles227 -cfnet sles227-ib0 -m  sles231 -mnet sles231-ib0

-u db2inst1 db2inst1
```

5. Extend the DB2 instance by issuing the `db2iupdt` command to add a member and CF. Examples follow:

```
root@sles227 ~ /opt/ibm/db2/V10.5/instance/db2iupdt -add -m
sles235 -mnet sles235-ib0 db2inst1

The execution completed successfully.

For more information see the DB2 installation log at
"/tmp/db2iupdt.log.17370".
DBI1070I  Program db2iupdt completed successfully.
```

```
root@sles227 ~ /opt/ibm/db2/V10.5/instance/db2iupdt -add -cf
sles235 -cfnet sles235-ib0 db2inst1

The execution completed successfully.

For more information see the DB2 installation log at
"/tmp/db2iupdt.log.17372".
DBI1070I  Program db2iupdt completed successfully.
```

6. Check that the DB2 software starts on all hosts by issuing the `db2start` command:

```
db2start
ADM12026W  The DB2 server has detected that a valid license for
the product "DB2 Enterprise Server Edition" has not been
registered.
07/16/2013 02:23:20     1   0   SQL1063N  DB2START processing was
successful.
07/16/2013 02:23:20     0   0   SQL1063N  DB2START processing was
successful.
SQL1063N  DB2START processing was successful.
```

Graphical User Interface installation method

The DB2 Setup wizard provides an easy-to-use GUI for installing DB2 software, including the DB2 pureScale Feature. The interface helps perform initial setup and configuration tasks as well. The DB2 Setup wizard can also create DB2 instances and a response file to duplicate an installation on other machines.

1. From the DB2 installation media, configure db2ssh and verify its functionality as described in the section "Configuring db2ssh by using the setup_db2locssh utility".

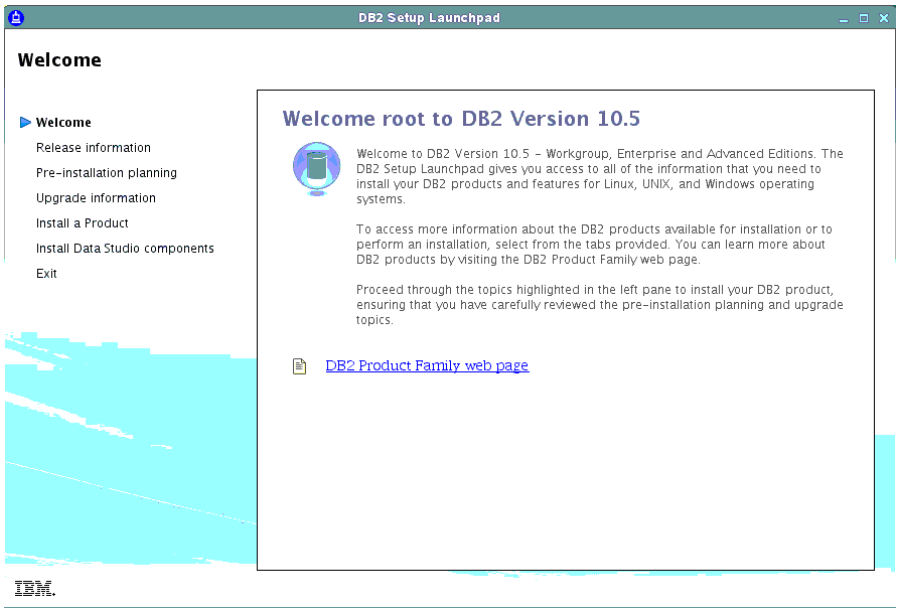
2. Check whether all the hosts meet the minimum requirements for the DB2 pure Scale Feature installation by issuing the `db2prereqcheck` command.(Refer to the knowledge center for details)

3. Launch the DB2 graphical installer by going to the SERVER folder on the downloaded product image or to the root directory of the product installation DVD and issue the `db2setup` command:

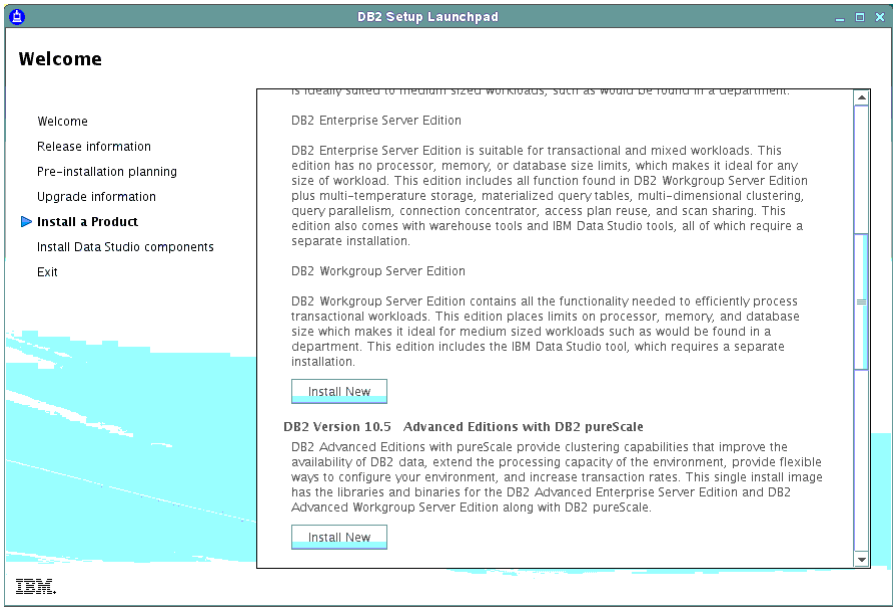
   #./db2setup -t /tmp/db2setup.trc -l /tmp/db2setup.log

The following steps show an example of how to use the DB2 setup wizard

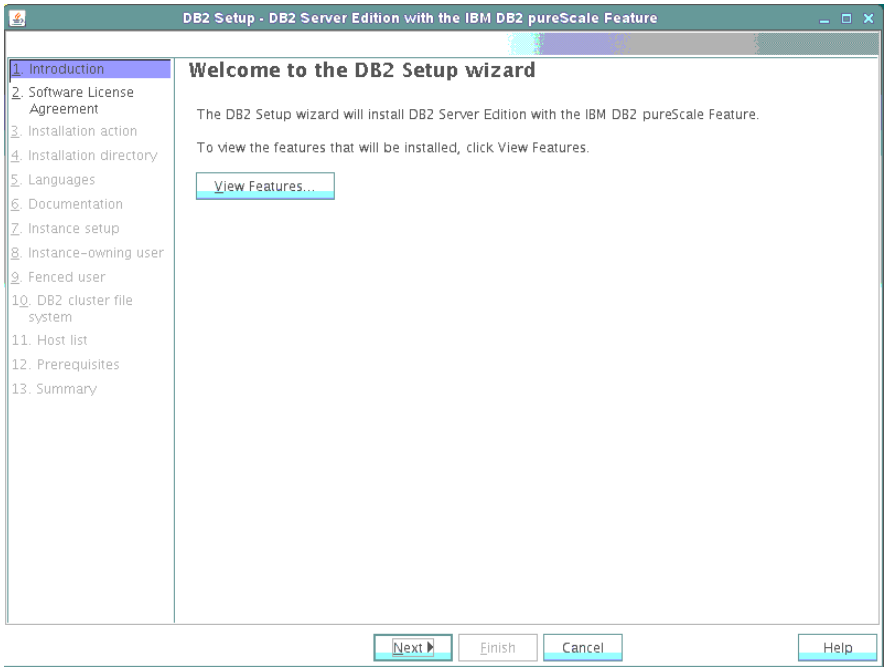
1. In the left pane of the DB2 Setup Launchpad, click **Install a Product:**



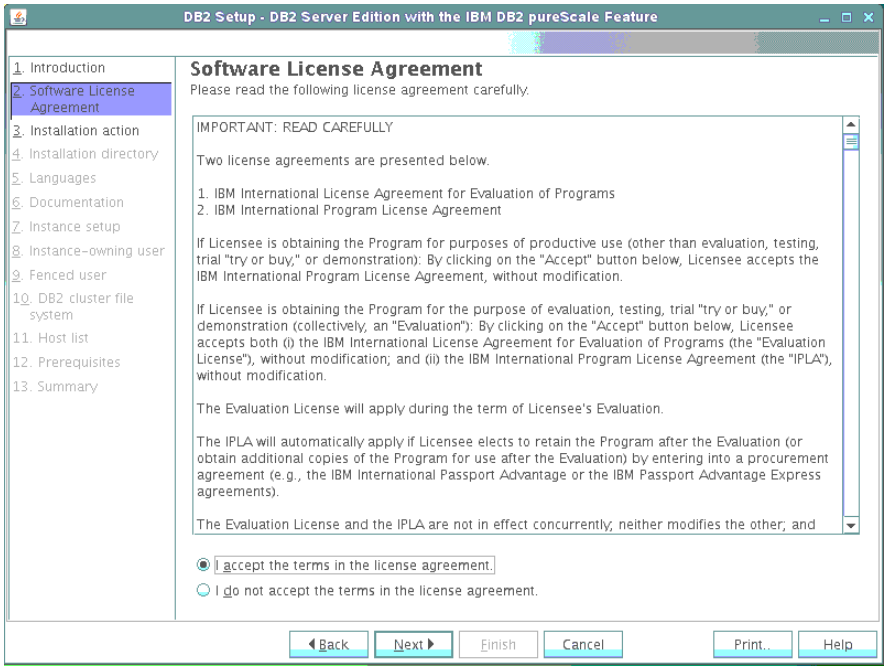
2. Under " DB2 Setup Launchpad" panel a, select **Advanced Editions with DB2 pureScale**, and click **Install New**:



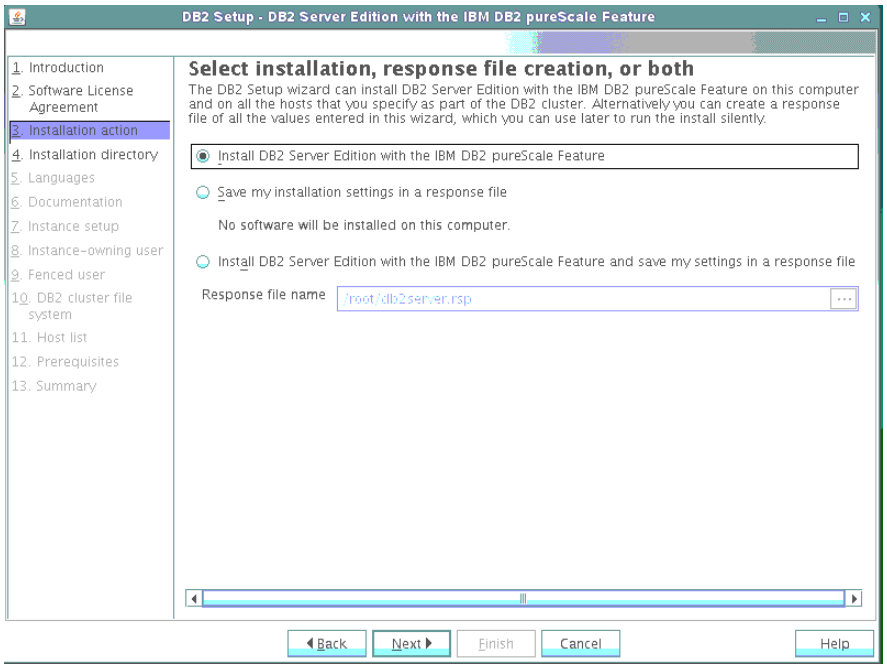
3. Select "Introduction panel " and click **Next:**



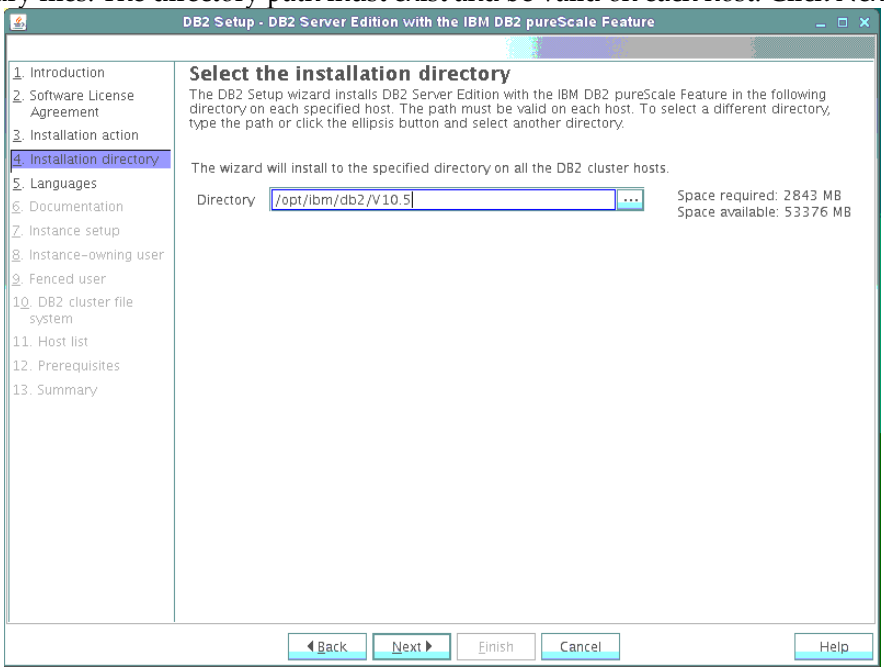
4. Select “Software License Agreement panel”, click **I accept the terms in the license agreement** and then click **Next**.



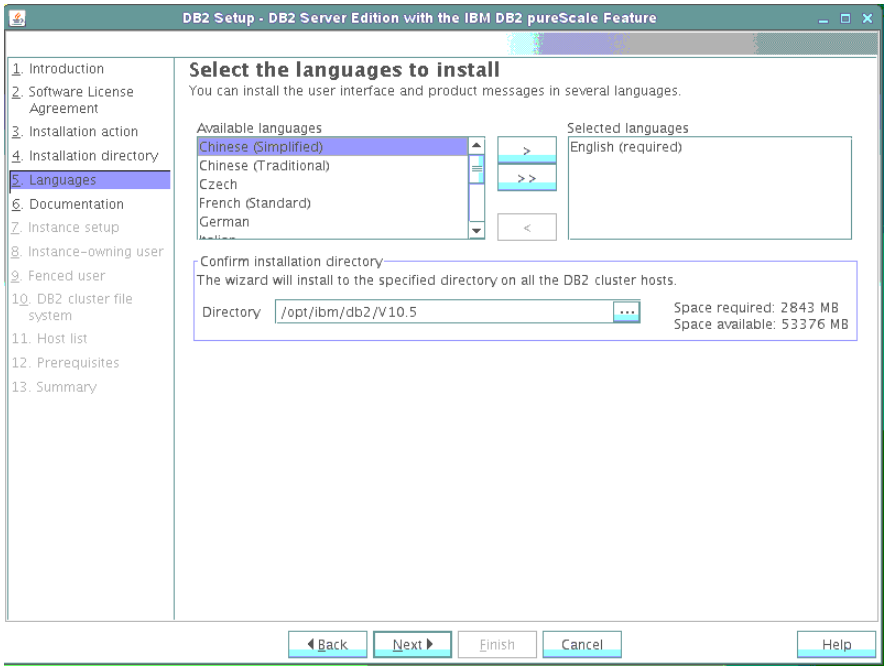
5. Select “ Installation action ” panel, click **Install DB2 Server Edition with the IBM DB2 pureScale Feature**. (Alternatively, you can save settings in a response file without installing or both install and save settings in a response file.) Click **Next**.



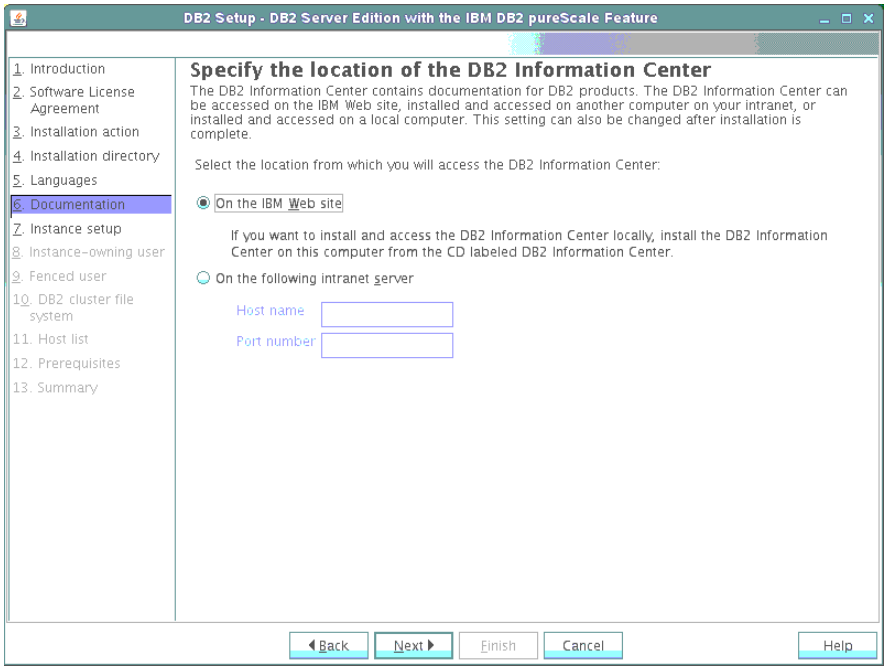
6. Select " Installation directory" panel, specify the installation directory for the DB2 binary files. The directory path must exist and be valid on each host. Click Next



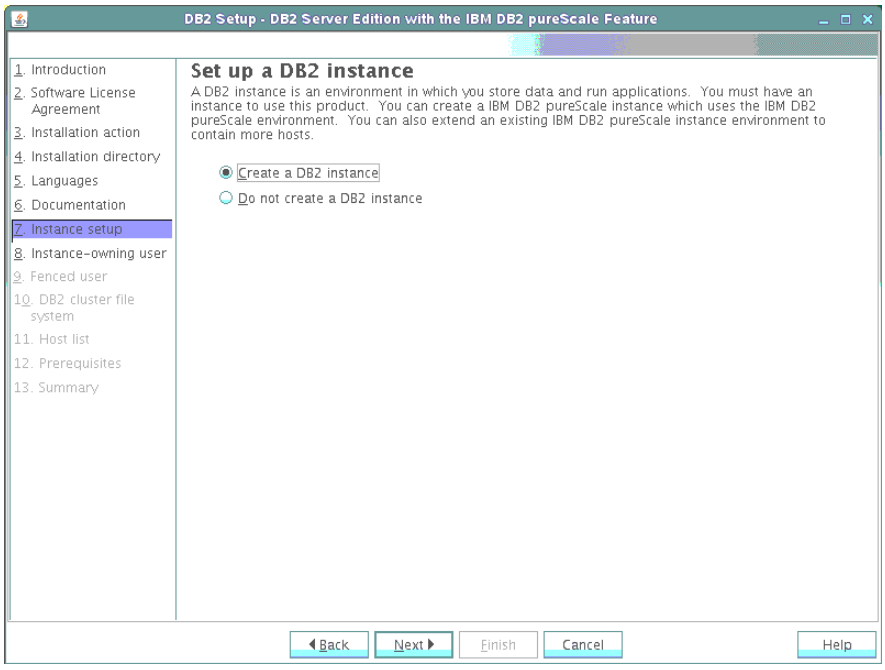
7. Select " Languages" panel, choose the language that you want to use in your environment. Click **Next**.



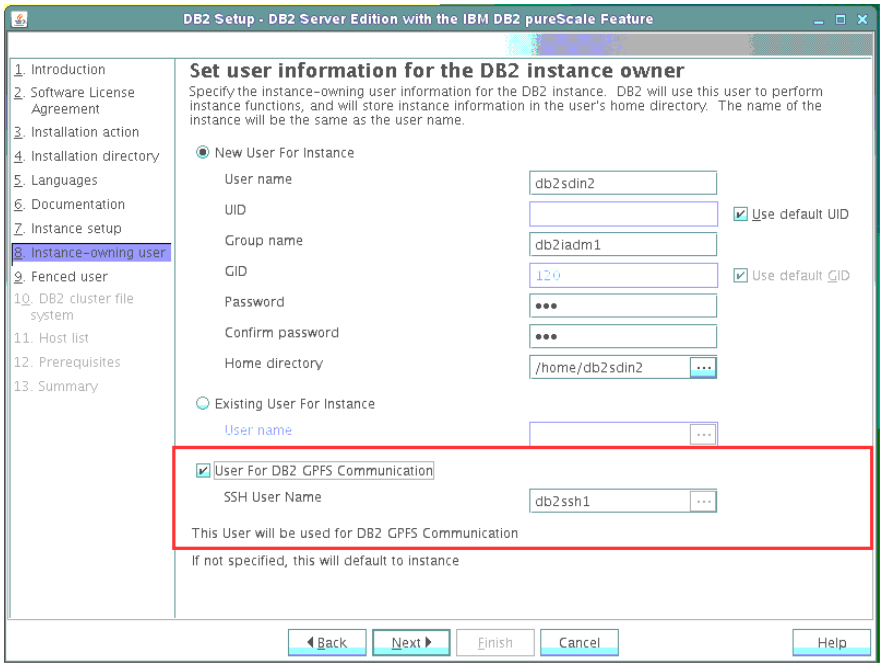
8. Select “Documentation” panel, specify whether you want to access the DB2 Information Center on the IBM website or on an intranet server. You can change the setting after the installation is complete. Click **Next**.



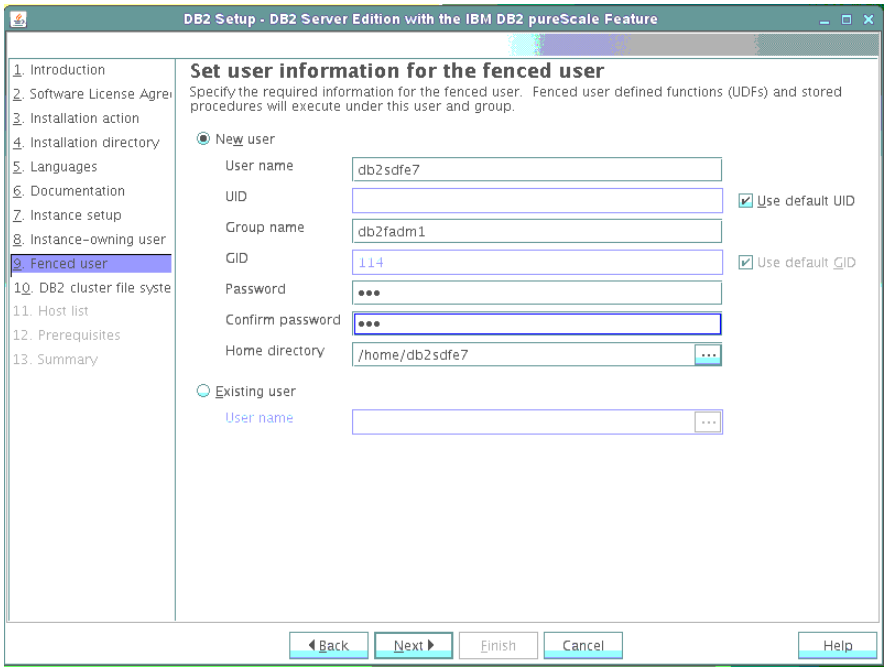
9. Select “ Instance setup” panel, click **Create a DB2 instance.** Click **Next**



10. Select “Instance-owning user” panel, enter a password for the DB2 instance owner and select the **User For DB2 GPFS Communication** check box. By default, the value of the <db2sshid> user is used, as shown in red. Click **Next**

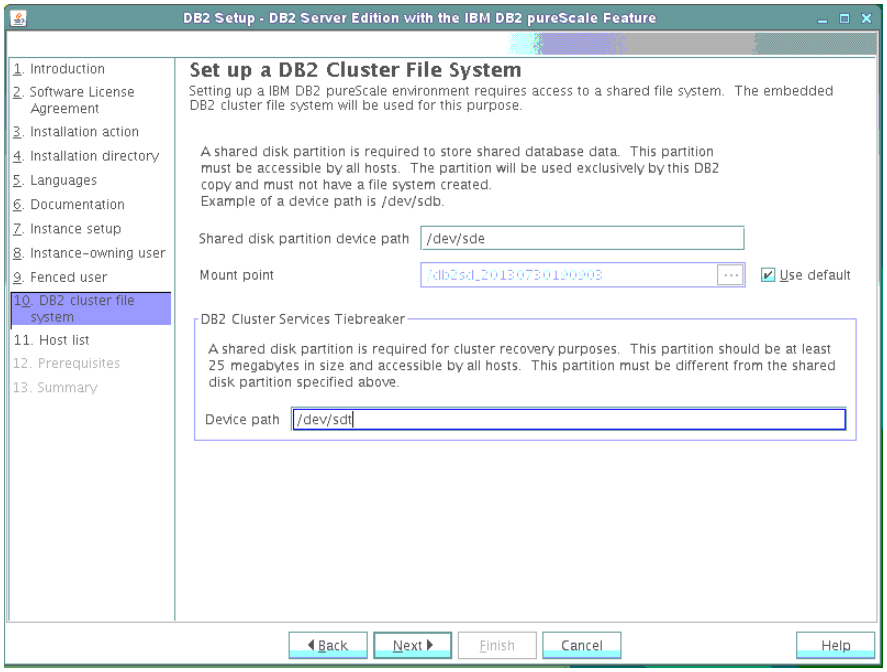


11. Select "Fenced user" panel, enter a password for the fenced user. User-defined functions and stored procedures are run under this user ID and group. Click **Next**.

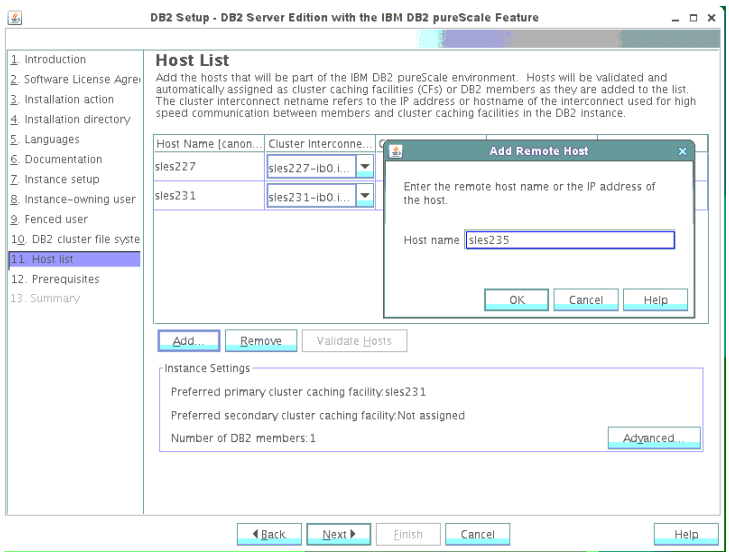


12. Select “S DB2 Cluster File System” panel, specify shared disk and tiebraker disk
    - A shared disk partition device path. Use one of the predefined disks to create a shared file system that is used by the DB2 pureScale environment for instance files that are shared across all machines.
    - A DB2 cluster services tiebreaker device path. A small disk is enough for the tiebreaker device path.

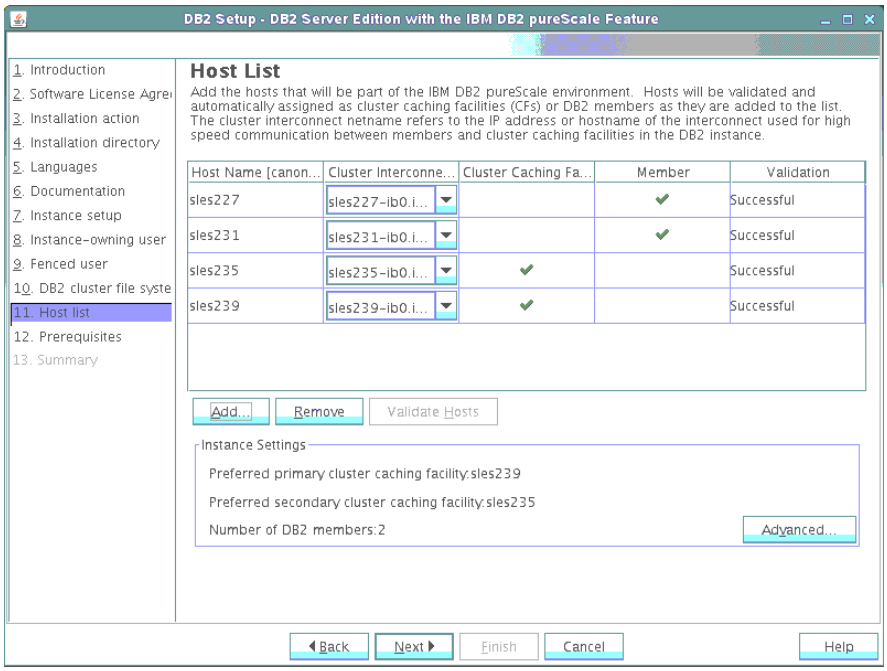
    Click **Next**.



13. On the “Host List” panel, specify each participating machine by clicking **Add** and entering the remote host name



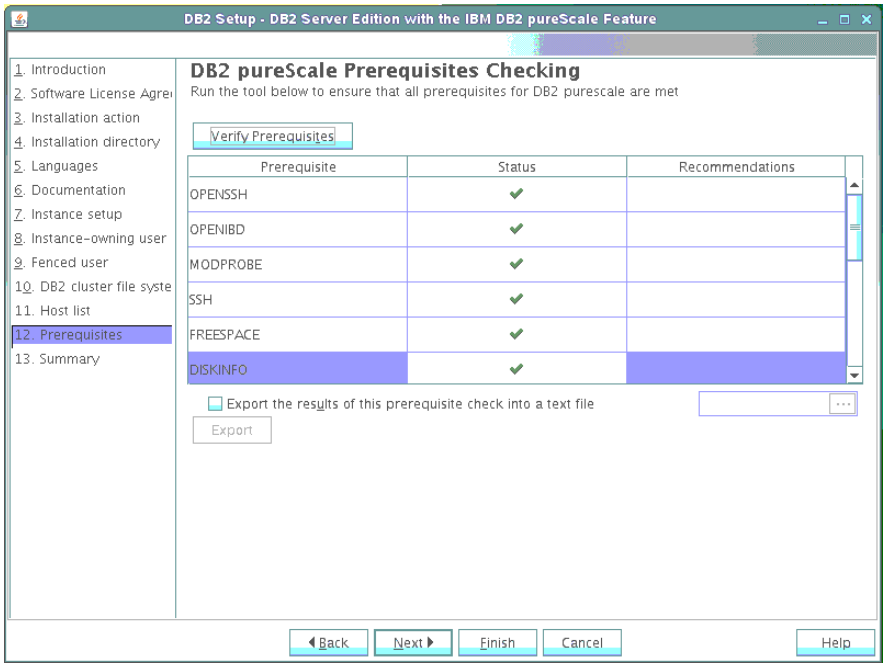
After you add all the participating machines, the panel should look similar to the following one. Click **Next**



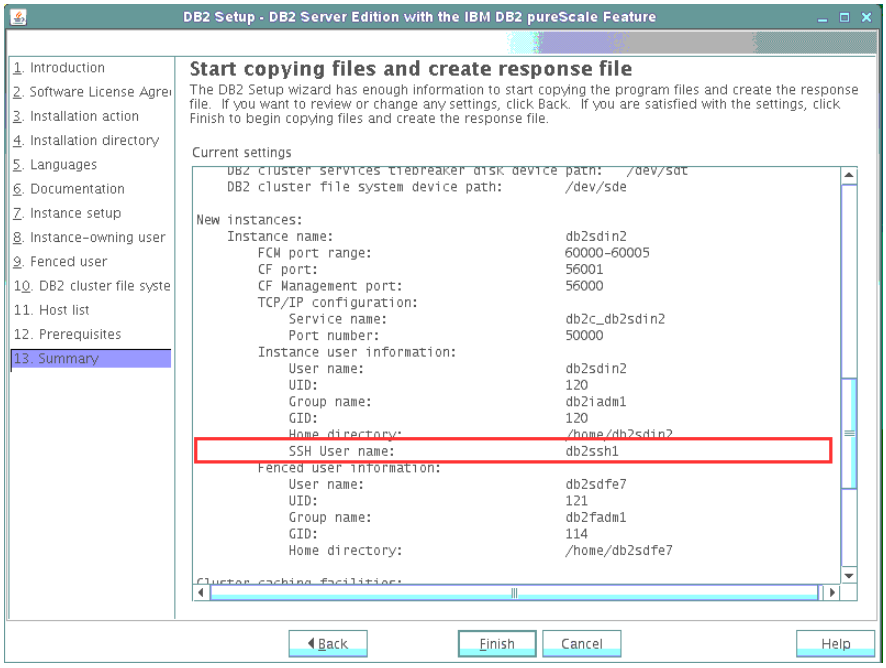
14. On the "DB2 pureScale prerequisites Checking" panel, ensure that all the prerequisites are met on all the participating machines:

    1. Click **Verify prerequisites**.
    2. Correct any errors.

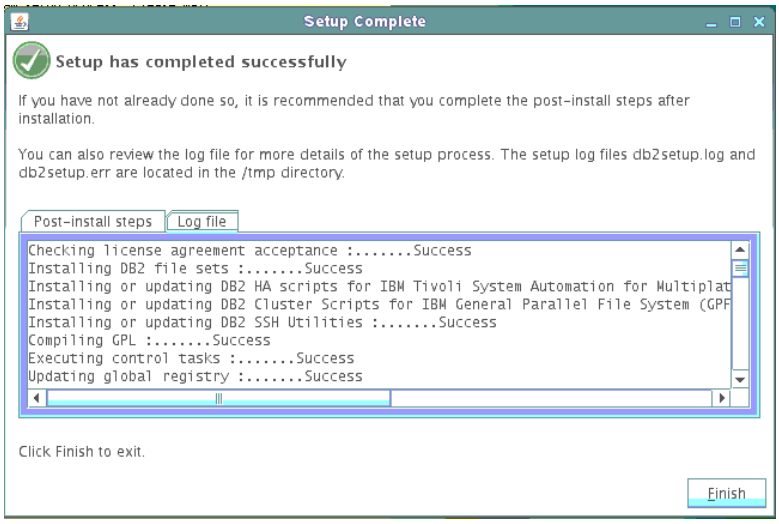
Click **Next**.



15. On the "Summary" panel, which displays all the instance user settings, including the SSH user name (marked in red in the following screen capture), click **Finish**



16. On the "Setup Complete" panel, review the post-installation steps or log file contents by clicking the applicable tab. Click **Finish**



Silent installation method

You can install and configure the DB2 pureScale Feature by using a silent interface, which refers to using a response file. You can create a response file in the following ways:

- By manually creating a file and typing in values.
- By saving settings while using the DB2 Setup wizard.
- By copying one of the sample response files from the DVD and modifying it. Samples are typically available in the db2/platform/samples directory.

To install silently:

1. From the DB2 media configure db2ssh and verify its functionality as described in the "Configuring db2ssh by using the setup_db2locssh utility" section.

2. Check whether all the hosts meet the minimum requirements for the DB2 pureScale Feature installation by issuing the `db2prereqcheck` command (Refer Knowledge center for details).

3. Choose the response file from the media path. In the response file, ensure that the value of the `DB2_INST.DB2SSHID_USERNAME` keyword is the same as the user name that you provided while configuring the `db2ssh`.

4. From the media, install and configure the DB2 pure Scale Feature by issuing the `db2setup` command with the `-r` parameter. An example follows:

```
./db2setup -r /root/db2server.rsp -t /tmp/pure.log -t
/tmp/pure.trc

The execution completed successfully.

For more information see the DB2 installation log at
"/tmp/pure.log".
```

Creating a user-managed GPFS cluster with db2ssh enabled

In a DB2 pureScale environment, all data and logs must be on a GPFS system. The only supported user-managed file system is a GPFS system.

The main way to manage DB2 cluster services is by using the `db2cluster` utility. The utility acts on both the cluster manager and shared file system cluster of the DB2 pureScale® Feature.

The `db2cluster_prepare` utility is a wrapper around the `db2cluster` utility. You can use the `db2cluster_prepare` utility to create a GPFS file system. You can also use the utility to convert a user-managed GPFS file system to a GPFS file system that is managed by the DB2 software. The utility is also helpful for converting an instance that is not a pureScale instance to a pureScale instance.

The following sections show how to use the `db2cluster_prepare` and `db2cluster` utilities to create a user-managed file system with `db2ssh` enabled.

Using the db2cluster_prepare utility

To create a user-managed GPFS file system by using the `db2cluster_prepare` utility:

1. From the DB2 media, configure db2ssh and verify its functionality as described in the "Configuring db2ssh by using the setup_db2locssh utility" section.

2. Check whether all the hosts meet the minimum requirements for the DB2 pureScale Feature installation by issuing the db2prereqcheck command. [Refer Knowledge center for details]

3. From the media, install the DB2 pureScale Feature by issuing the `db2_install` command.

4. From the DB2 installation path, run the `db2cluster_prepare` utility. An example follows:

```
root@sles227 ~ /opt/ibm/db2/V10.5/instance/db2cluster_prepare -
instance_shared_dev /dev/sdf -l /tmp/cluster.log -t
/tmp/cluster.trc
DBI1446I  The db2cluster_prepare command is running.


For more information see the DB2 installation log at
"/tmp/cluster.log".
DBI1070I  Program db2cluster_prepare completed successfully.
```

5. Extend the GPFS cluster, using `db2cluster` utility. An example follows:

```
sles227:/opt/ibm/db2/V10.5/bin # ./db2cluster -cfs -create -host
sles227 -domain gpfsdomain
The shared file system cluster has been successfully created.


sles227:/opt/ibm/db2/V10.5/bin # ./db2cluster -cfs -add -host
sles231
Host 'sles231' has been successfully added to the shared file
system cluster.

sles227:/opt/ibm/db2/V10.5/bin # ./db2cluster -cfs -add -host
sles235
Host 'sles235' has been successfully added to the shared file
system cluster.

sles227:/opt/ibm/db2/V10.5/bin # ./db2cluster -cfs -add -host
sles239
Host 'sles239' has been successfully added to the shared file
system cluster.
```

6. Issue the `mmlscluster` command and ensure db2ssh is configured by looking at value for Remote shell command and Remote file copy command:

```
sles227:/opt/ibm/db2/V10.5/bin # /usr/lpp/mmfs/bin/mmlscluster

GPFS cluster information
========================
 GPFS cluster name:         db2cluster_20130716012315.in.ibm.com
 GPFS cluster id:           14512172381151178504
 GPFS UID domain:           db2cluster_20130716012315.in.ibm.com
 Remote shell command:      /var/db2/db2ssh/db2locssh
 Remote file copy command:  /var/db2/db2ssh/db2scp

GPFS cluster configuration servers:
-----------------------------------
  Primary server:    sles227.in.ibm.com
  Secondary server:  sles231.in.ibm.com

 Node  Daemon node name    IP address     Admin node name
Designation
-------------------------------------------------------------------
---------
   1   sles227.in.ibm.com  9.122.215.227  sles227.in.ibm.com
quorum-manager
   2   sles231.in.ibm.com  9.122.215.231  sles231.in.ibm.com
quorum-manager
   3.  sles235.in.ibm.com  9.122.215.235  sles235.in.ibm.com
quorum-manager
   4. sles239.in.ibm.com  9.122.215.239  sles239.in.ibm.com
quorum-manager
```

Using the db2cluster utility

To create a user-managed GPFS file system by using the `db2cluster` utility:

1. From the DB2 media, configure db2ssh and verify its functionality as described in the "Configuring db2ssh by using the setup_db2locssh utility" section.

2. From the media, install the DB2 pureScale Feature by issuing the `db2_install` command.

3. Run t db2cluster utility from <InstallPath>/bin/. An example follows:

```
    sles227:/opt/ibm/db2/V10.5/bin #./db2cluster -cfs -create -
host hostname1 -domain domainname
    sles227:/opt/ibm/db2/V10.5/bin #./db2cluster -cfs -add -host
hostname2
    sles227:/opt/ibm/db2/V10.5/bin #./db2cluster -cfs -start -all
    sles227:/opt/ibm/db2/V10.5/bin #./db2cluster -cfs -create -
filesystem fsname -disk dev_path -mount mount_point
```

4. On all the hosts in the cluster, issue the mount command and check whether the new file system is mounted on all machines. An example follows:

```
sles227:/opt/ibm/db2/V10.5/bin # ./db2cluster -cfs -create -host
sles227 -domain gpfsdomain
The shared file system cluster has been successfully created.


sles227:/opt/ibm/db2/V10.5/bin # ./db2cluster -cfs -add -host
sles231
Host 'sles231' has been successfully added to the shared file
system cluster.

sles227:/opt/ibm/db2/V10.5/bin # ./db2cluster -cfs -add -host
sles235
Host 'sles235' has been successfully added to the shared file
system cluster.

sles227:/opt/ibm/db2/V10.5/bin # ./db2cluster -cfs -add -host
sles239
Host 'sles239' has been successfully added to the shared file
system cluster.
```

5. Issue the `mmlscluster` command. An example follows:

```
sles227:/opt/ibm/db2/V10.5/bin # /usr/lpp/mmfs/bin/mmlscluster

GPFS cluster information
```

```
=======================
  GPFS cluster name:         gpfsdomain.in.ibm.com
  GPFS cluster id:           14512172381151178504
  GPFS UID domain:           gpfsdomain.in.ibm.com
  Remote shell command:      /var/db2/db2ssh/db2locssh
  Remote file copy command:  /var/db2/db2ssh/db2scp

GPFS cluster configuration servers:
-----------------------------------
  Primary server:    sles227.in.ibm.com
  Secondary server:  sles231.in.ibm.com

 Node  Daemon node name    IP address     Admin node name
Designation
-------------------------------------------------------------------
---------
   1   sles227.in.ibm.com  9.122.215.227  sles227.in.ibm.com
quorum-manager
   2   sles231.in.ibm.com  9.122.215.231  sles231.in.ibm.com
quorum-manager
   3   sles235.in.ibm.com  9.122.215.235  sles235.in.ibm.com
quorum-manager
   4   sles239.in.ibm.com  9.122.215.239  sles239.in.ibm.com
quorum-manager
```

6. Start the GPFS cluster by issuing the following command:

```
sles227:/opt/ibm/db2/V10.5/bin # ./db2cluster -cfs -start -all
All specified hosts have been started successfully.
```

7. On all the machines, mount the file system. An example follows:

```
sles227:/opt/ibm/db2/V10.5/bin #./db2cluster -cfs -create -
filesystem gpfsfs -disk /dev/sdk -mount /gpfs1


./db2cluster -cfs -list -filesystem
FILE SYSTEM NAME                        MOUNT POINT
--------------------------------      -------------------------
gpfsfs                                  /gpfs1
```

Enabling db2ssh logging for AIX operating system

By default, an AIX system does not do syslogging. To enable `db2ssh` logging for AIX operating system:

1. In the /etc/syslog.conf file (syslog configuration file), add the following lines:

```
*.debug    /tmp/syslog.out  rotate size   10m time 1w files
10 # 10 files, 10MB each, weekly rotate

kern.debug /var/log/kern.log    rotate files 12 time 1m
compress  # 12 files, monthly rotate, compress
```

2. As the root user, issue the following commands. The syslog files must exist before syslogd writes to them.

```
touch /tmp/syslog.out

touch /var/log/kern.log
```

3. Restart syslogd by issuing the following command:

```
refresh -s syslogd
```

Troubleshooting tips

If you do not follow the best practice procedures in this paper for installing and configuring the DB2 pureScale Feature with `db2ssh` enabled, you might encounter problems. This section provides some troubleshooting tips to help you to resolve the problems without having to contact IBM support for help.

Failure of remote command execution using db2locssh

Error condition:

sles227: /var/db2/db2ssh/db2locssh <hostname> 'hostname'
failure

Solution:

If you missed any of the steps for configuring `db2ssh` or manually changed the contents of the /var/db2/db2ssh directory after successful configurations, you might encounter this error. If so, perform the following steps:

1. On each host, check each whether the public keys of all the hosts are in the /var/db2/db2ssh directory. As a <db2sshid>. user, verify SSH from every host to all other hosts without being prompting for a password.

2. Check whether the system clocks across all the hosts are in sync. Setting the `time_delta` keyword requires that the system clocks are in sync across the cluster

3. If you performed the previous steps but the command still fails, collect system logs and contact IBM support.

Changing the value of the db2sshid user to a different user ID

Error condition:

If you change the <db2sshid> user to a different user ID by using the `setup_db2locssh` utility, an error message is returned. For example, assume that you configured the `db2ssh` to use the db2ssh1 user ID and then tried to configure it to use a different user ID, db2ssh2.

```
root@sles227 ~./setup_db2locssh db2ssh2
```

The following error message is returned:

```
db2ssh is already configured on the host sles227.in.ibm.com with
user db2ssh1
```

Solution:

1. Create the db2ssh2 user on every host in the GPFS domain with the same user ID and password.

2. Across all the hosts, configure passwordless SSH for the db2ssh2 user ID.

3. On each of the hosts, update the `db2ssh` configuration by issuing the following command: `/var/db2/db2ssh/db2locssh set_db2sshid db2ssh2`

Converting GPFS configuration from openSSH to the db2ssh

Error condition:

Ideally, after you create a DB2 pureScale instance, GPFS uses `db2locssh` as the remote shell command and `db2scp` as the remote copy command. However, in some cases, you might get an error or warning during instance creation that indicates that the installer is not able to set the GPFS configuration to use `db2ssh`.

Solution:

1. Check the GPFS configuration by issuing the `mmlscluster` native command. A sample command and its output below

```
root@sles227 ~/usr/lpp/mmfs/bin/mmlscluster


GPFS cluster information
========================
GPFS cluster name:         db2cluster_20130705055540.in.ibm.com
GPFS cluster id:           15328668191225714717
GPFS UID domain:           db2cluster_20130705055540.in.ibm.com
Remote shell command:      /usr/bin/ssh
Remote file copy command:  /usr/bin/scp
```

2. Perform one of the following steps:
   - To change the GPFS configuration to use the `db2locssh` and `db2scp` commands, issue the `mmchcluster` command. An example follows:

     ```
     root@sles227 ~/usr/lpp/mmfs/bin/mmchcluster -r
    /var/db2/db2ssh/db2locssh -R /var/db2/db2ssh/db2scp
     ```

   - To change the GPFS configuration to use openSSH and the `scp` program instead of the db2locssh and db2scp utilities, issue the `mmchcluster` command. An example follows:

     ```
     root@sles227 ~/usr/lpp/mmfs/bin/mmchcluster -r
      /usr/bin/ssh -R /usr/bin/scp
     ```

Instance upgrade failure

Error condition:

If you try to upgrade a pureScale instance to DB2 Version 10.5, the `db2iupgrade` command fails if the GPFS configuration does not use the `db2locssh` and `db2scp` utilities.

Solution:

Before performing the upgrade, perform the following steps:

1. Configure db2ssh with the <db2sshid> user, as described in the "Configuring db2ssh by using the setup_db2locssh utility" section.
2. Check whether the GPFS configuration is using openSSH and the `SCP` program.
3. If the configuration is using openSSH and the `SCP` program, change the configuration to use the `db2locssh` and `db2scp` utilities by issuing the `mmchcluster` command.

Removing db2ssh configuration for a user

Error condition:

If changes to the /var/db2/db2ssh directory resulted in missing keys or file corruption, you must clean up the db2ssh and start fresh.

Solution:

1. On all the hosts remove all the contents of the /var/db2/db2ssh directory.
2. On all the hosts, delete the <db2sshid> user.
3. On all the hosts, create a new <db2sshid> user with the same UID and GID.
4. Configure the db2ssh with the <db2sshid> user, as described in the "Configuring the db2ssh by using the setup_db2locssh utility" section.

Best practices

- To install and configure the DB2 pureScale Feature securely, always use db2ssh instead of passwordless SSH for the root user.
- Before deploying and configuring DB2 software, always run the db2prereqcheck utility. Fix all the errors that are reported by the utility.
- Ensure that the UID and GID of the <db2sshid> user are the same across all the hosts that participate in the cluster.
- Before installing the DB2 software, perform `db2ssh` verification. That is, ensure that each host can connect to every other host in the cluster by using the db2locssh utility.
- Before switching the GPFS configuration to use the `db2locssh` utility instead of openSSH and the `db2scp` utility instead of the `scp` program, perform `db2ssh` verification.
- After successfully installing and configuring DB2 software, avoid changing the value of the <db2sshid> user to a different user ID.
- After creating a DB2 pureScale instance, ensure that GPFS is using the `db2locssh` command as the remote shell command and the db2scp command as the remote copy command.
- If you extend the cluster, configure db2ssh with the same user ID on the new host.
- Don’t remove the contents of the /var/db2/db2ssh directory unless IBM support suggests doing so.
- Don’t forget to disable the remote root login setting after configuring db2ssh.

Conclusion

Security is a vital aspect of any database management software because the information that is stored in the database is very valuable and sensitive. From DB2 Version 10.5, the DB2 install and cluster utilities have been enhanced to make use of db2ssh (if configured) for pureScale operations. This paper highlights the best practices for installing and configuring the DB2 pureScale Feature in a highly secure way by using the `db2ssh`, without having to enable passwordless SSH for the root user.

Further reading

- Information Management best practices (http://www.ibm.com/developerworks/data/bestpractices/)

- DB2 for Linux, UNIX, and Windows best practices (http://www.ibm.com/developerworks/data/bestpractices/db2luw)

- IBM DB2 Knowledge Center (http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.kc.doc/welcome.html)

Contributors

Paolo Cirone, *DB2 technical writer*

Notices

This information was developed for products and services offered in the U.S.A.

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
Armonk, NY 10504-1785
U.S.A.

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.

Without limiting the above disclaimers, IBM provides no representations or warranties regarding the accuracy, reliability or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any recommendations or techniques herein is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Anyone attempting to adapt these techniques to their own environment does so at their own risk.

This document and the information contained herein may be used solely in connection with the IBM products discussed in this document.

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.

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.

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.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Windows is a trademark of Microsoft Corporation in the United States, other countries, 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.

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

Contacting IBM

To provide feedback about this paper, write to db2docs@ca.ibm.com.

To contact IBM in your country or region, check the IBM Directory of Worldwide Contacts (http://www.ibm.com/planetwide).

To learn more about IBM Information Management products, see the Information Management website (http://www.ibm.com/software/data/).