NetBackup™ for DB2 Administrator's Guide

UNIX, Windows, and Linux

Release 11.2.0.1

COHESITY

NetBackup™ for DB2 Administrator's Guide

Last updated: 2026-09-09

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity, Inc. in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. COHESITY SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1 Introduction to NetBackup for DB2 9

Features of NetBackup for DB2 9
NetBackup for DB2 overview 10
About the NetBackup for DB2 components 11
About NetBackup for DB2 terminology 13

Chapter 2 Installing NetBackup for DB2 15

Planning the installation of NetBackup for DB2 15
Verifying the operating system and platform compatibility 16
NetBackup server and client requirements 16
DB2 server software requirements 17
Requirements for using NetBackup for DB2 in a NetBackup cluster 18
License for NetBackup for DB2 18
About log archiving 18
Using the VENDOR archive method 19
Using the user exit archive method 19
Specifying the DB2 home path (UNIX) 20
About adding new DB2 instances 21

Chapter 3 Configuring NetBackup for DB2 22

Overview of NetBackup for DB2 configuration 23
About permissions for NetBackup for DB2 log files (UNIX) 23
About configuring a backup policy for DB2 23
Add a policy for DB2 24
About policy attributes 25
Add clients to a policy 25
Specifying the primary server for a NetBackup for DB2 client 26
Configuring a policy to back up the configuration files 26
Configuring the Maximum jobs per client 27
About adding backup selections to a DB2 policy 28
About backup schedules and scripts 29
Adding a script to the backup selections list 29
Configure an application backup schedule 30

Example application backup schedule 30
Configure automatic backup schedules 31
Example automatic backup schedule 31
Schedule properties 32
NetBackup for DB2 backup types 33
Perform a manual backup 35
Reviewing the auto-discovered mappings 35
About backing up archive log files with the user exit program 38
DB2 objects in the backup window 39
Configuring a policy to back up the archive logs 40
Configuring a policy to archive the archive logs 41
Configuring the run-time environment 42
Creating a db2.conf file for use with the user exit program 42
Creating a db2.conf file (vendor method) 46
Configuring bp.conf files in a cluster environment 48
Keywords for the db2.conf file 49
NetBackup for DB2 environment variables 53
Configuring the logon account for the NetBackup Client Service for NetBackup for DB2 55
About NetBackup for DB2 shell scripts 55
Creating DB2 scripts manually 56
About NetBackup shell script storage 58
RBAC role for the DB2 administrator 58

Chapter 4 Performing backups and restores of DB2 59

NetBackup for DB2 backup overview 59
About backups from the NetBackup primary server 61
About user-directed backups 62
Using DB2 to run a user-directed backup 62
BACKUP DATABASE command options 63
About browsing DB2 backup images with bplist 65
Performing a database restore 68
Using DB2 to perform a restore 68
About an alternate restore 75
Preparing the primary server for an alternate restore 77
Performing the alternate restore on the clients 78
Restoring the transaction logs 81
About preventing the direct expiration of backup images 82

Chapter 5 Using Snapshot Client with NetBackup for DB2 83

NetBackup for DB2 with Snapshot Client features 83
About NetBackup for DB2 with Snapshot Client operations 85
About the sequence of a NetBackup for DB2 backup operation with Snapshot Client methods 86
About the sequence of a NetBackup for DB2 restore operation with Snapshot Client methods 86
About database objects supported by advanced backup methods 86
About multistreaming and DB2 snapshot backups 87
About symbolic links and DB2 backups and restores (UNIX) 87
NetBackup for DB2 stream-based operations 87
NetBackup for DB2 file-based operations 88
Example: multiple sessions for a DB2 snapshot backup 89
About configuring Snapshot Client with NetBackup for DB2 90
Configuration requirements for snapshot backups with NetBackup for DB2 90
Configuring a snapshot policy for NetBackup for DB2 91
About configuring the db2.conf for a snapshot policy 93
Restoring NetBackup for DB2 from a snapshot backup 95
About restoring individual files from a NetBackup for DB2 snapshot backup 95
About NetBackup for DB2 restores of volumes and file systems using snapshot rollback 95
Performing a NetBackup for DB2 point-in-time rollback restore from a SnapVault backup (UNIX) 96
Performing a snapshot rollback restore from the command line 97
Troubleshooting NetBackup for DB2 rollback restores 98
About configuring NetBackup for DB2 block-level incremental backups on UNIX 98
How BLI works with NetBackup for DB2 (UNIX) 99
About the Storage Checkpoint facility and NetBackup for DB2 100
Configuration requirements for BLI backups with NetBackup for DB2 101
Storage Checkpoint configuration on the NetBackup for DB2 client 101
Configuring policies for BLI backups with NetBackup for DB2 .... 1 0 1
BLI incremental backup options using NetBackup for DB2 103

About Snapshot Client effects 106
How Snapshot Client software affects backup types 106
How Snapshot Client software affects schedule properties 107
How Snapshot Client software affects scripts 108
Performing NetBackup for DB2 backups with Snapshot Client methods 108
Performing NetBackup for DB2 restores with Snapshot Client methods 109

Chapter 6 Troubleshooting NetBackup for DB2 111

NetBackup debug logs and reports 112
Enable the debug logs automatically (DB2 client) (Windows) 112
Enabling the debug logs manually (DB2 client) (Windows) 112
Enabling the debug logs manually (DB2 client) (UNIX/Linux) 114
About the bphdb directory on the Windows database client 115
About the bphdb directory on the UNIX database client 116
About the bpdb2 directory on the UNIX database client 116
Set the debug level on a DB2 client (Windows) 117
Set the debug level on a DB2 client (UNIX) 117
Minimize time-out failures on large database restores 118
Minimize the loading and unloading of tapes for database backups 118
Use the NET_BUFFER_SZ file to speed up a slow restore 119
About false restore failures reported in the Activity monitor 119
About the error message codes 120

Appendix A Configuration for a DB2 EEE (DPF) environment 127

Overview of installation and configuration for a DB2 EEE (DPF) environment 127
Configuring NetBackup for DB2 in an EEE environment 128
Adding NetBackup policies for DB2 EEE environment 128
Backing up the archive logs that are in a DB2 EEE environment 129
Creating DB2 scripts for a DB2 EEE environment 129

Appendix B Using NetBackup for DB2 with SAP® 131

About NetBackup for DB2 with SAP 131
Installation of the DB2 user exit program 131
Backup and restore of DB2 databases used by SAP 132
Archive and restore of DB2 log files used by SAP 132
Backup of SAP files 132

Appendix C Register authorized locations 133

Registering authorized locations used by a NetBackup database script-based policy 133

Chapter 1

Introduction to NetBackup for DB2

This chapter includes the following topics:

- Features of NetBackup for DB2
- NetBackup for DB2 overview

Features of NetBackup for DB2

Table 1-1 shows NetBackup for DB2's main features and introduces some terms that are used in this documentation.

Table 1-1 NetBackup for DB2 features and descriptions

Feature	Description
Media and device management	All the devices Media Manager supports are available to NetBackup for DB2.
Scheduling facilities	NetBackup scheduling facilities on the primary server can be used to schedule automatic and unattended DB2 backups. This feature also lets you choose the times when these operations can occur. For example, to prevent interference with normal daytime operations, you can schedule your database backups to occur only at night.
Multiplexed backups and restores	NetBackup for DB2 lets you take advantage of NetBackup's multiplexing capabilities. Multiplexing directs multiple data streams to one backup device, thereby reducing the time necessary to complete the operation.

Table 1-1 NetBackup for DB2 features and descriptions *(continued)*

Feature	Description
Transparent DB2 and regular file system backup and restore operations	All backups and restores run simultaneously and transparently without any action from the NetBackup administrator. The database administrator can run database backup and restore operations through NetBackup. An administrator or any other authorized user can use NetBackup to run database backups and restores.
Sharing the same storage units that are used for other file backups	Devices and media can be shared for other backups or to you can give DB2 exclusive use of certain devices and media. NetBackup for DB2 can use Media Manager, disk, and Media Server Deduplication Pool (MSDP) storage units.
Centralized and networked backup operations	From the NetBackup primary server, you can schedule database backups or start them manually for any client. The DB2 databases can also reside on any hosts that are different from the devices on which NetBackup stores the backups.
User interfaces	NetBackup provides the NetBackup web UI for policy management and server-directed backups and restores. A database administrator can also use the IBM DB2 control center or command-line processor to start user-directed backup and restore operations.
Parallel backup and restore operations	NetBackup for DB2 supports the parallel backup and restore capabilities of DB2. For example, a user can run more than one tape device at a time for a single DB2 backup or restore. This usage can reduce the time necessary to complete the operation.
Compression	Compression increases backup performance over the network and reduces the size of the backup image that NetBackup writes to the storage unit.
Database delete requests accepted and processed	Database delete requests are accepted and processed. When NetBackup receives a delete image request, it searches the NetBackup catalog. If the image is found and it is not on a legal hold, the image is removed from the NetBackup catalog.

NetBackup for DB2 overview

NetBackup for DB2 integrates the database backup and recovery capabilities of DB2 with the backup and the recovery management capabilities of NetBackup.

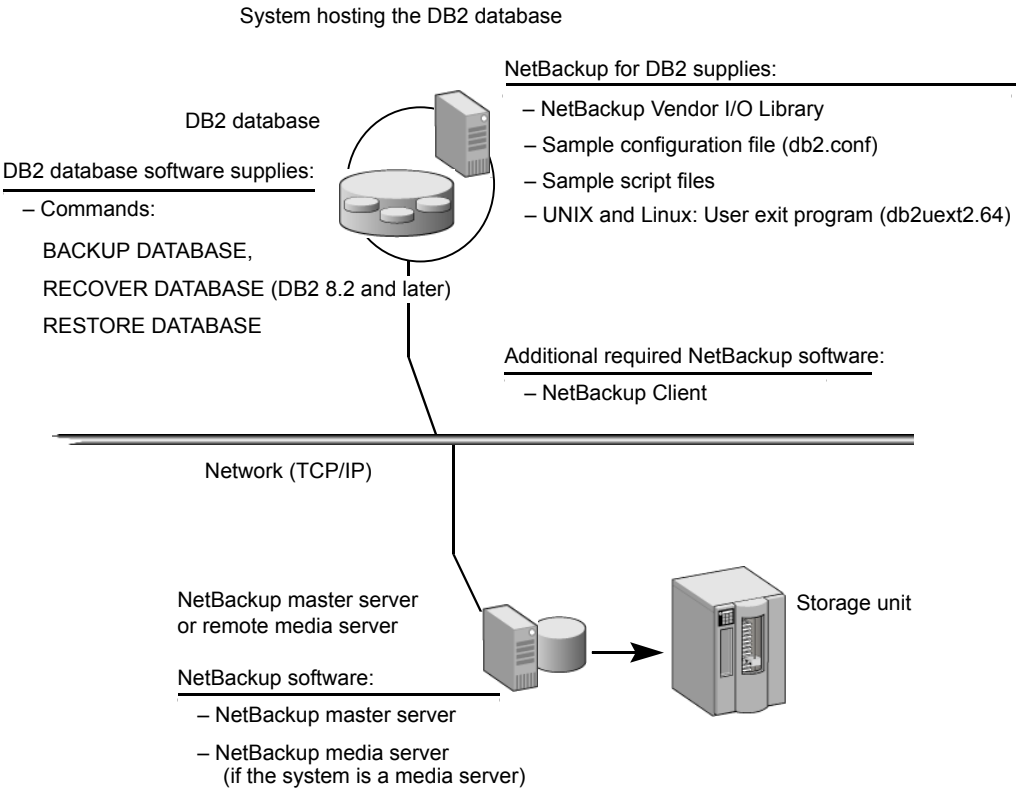
The server that hosts the DB2 database must be a NetBackup client.

On Windows, NetBackup for DB2 must be licensed on the server.

On UNIX, NetBackup for DB2 must be installed on the server.

Figure 1-1 shows the hardware components and software components for a NetBackup for DB2 environment.

Figure 1-1 NetBackup for DB2 components



About the NetBackup for DB2 components

Table 1-2 describes the main NetBackup components in a NetBackup for DB2 environment.

Table 1-2 NetBackup for DB2 component descriptions

Component	Description
NBDB2 vendor I/O library	The DB2 `BACKUP` and `RESTORE` commands use the NBDB2 vendor I/O library to send data buffers between a DB2 database and NetBackup. You specify the library as the argument to the `LOAD` parameter of the DB2 `BACKUP` and `RESTORE` commands. The installation program installs the vendor library in the following location: On Windows: *install_path*`\NetBackup\bin\nbdb2.dll` On UNIX: `/usr/openv/netbackup/bin` On UNIX, the name of the vendor library differs, depending on your platform as follows: ■ 64-bit Solaris SPARC and 64-bit Linux x86: `nbdb2.so64` ■ 64-bit AIX and HP-UX PARISC: `nbdb2.sl64` ■ 64-bit Linux Itanium, HP Itanium, and IBM pSeries: `nbdb2.so`
User exit program	The NetBackup for DB2 user exit program, `db2uext2`, provides one method for backing up and restoring the DB2 archive log files. Use this method at the following times: ■ When you use the DB2 `BACKUP` command or `ROLLFORWARD` command to back up or restore databases. ■ When the user exits the database with the DB2 `TERMINATE` or `DISCONNECT` command. ■ When the log file fills and DB2 starts writing transactions to another log file. ■ The DB2 `ARCHIVE LOG` command is issued. The user exit program backs up and restores the archive logs as files. The file is called `db2uext2.64`. NetBackup for DB2 supports this method for protecting the archive logs on all supported DB2 releases. The user exit program resides in the following location: On Windows: `%DB2_INSTANCE%\bin\db2uext2.exe` On UNIX: `$DB2_INSTANCE/sqllib/adm/db2uext2`. Other methods are available for backing up archive log files. See "About log archiving" on page 18.

Table 1-2 NetBackup for DB2 component descriptions *(continued)*

Component	Description
Sample configuration file (db2.conf) and script files	The installation software installs the following sample files: ■ A sample configuration file (`db2.conf` file). The `db2.conf` file includes specifications for backups and restores, and it provides information on policies and schedules. The NetBackup for DB2 library and user exit program use the information in this file. ■ Sample backup and restore scripts. NetBackup can invoke a script to perform a scheduled backup or restore of a DB2 database. The scripts contain DB2 `BACKUP` or `RESTORE` commands for use with NetBackup. The installation software writes these sample files to the following location: On Windows: *install_path*`\NetBackup\dbext\db2\samples` On UNIX: `/usr/openv/netbackup/ext/db_ext/db2/scripts`. To use the sample files, copy the sample files to working directories and modify them for your own use.

About NetBackup for DB2 terminology

DB2 supports archiving its log file through a user exit program or through a vendor library. DB2 supports backing up the archive log files by using a vendor library. NetBackup for DB2 supplies a user exit program and a library to support both of these methods.

The DB2 syntax for specifying these archive log methods differs from release to release. NetBackup for DB2 topics use the terms "user exit" and "VENDOR" to differentiate the methods.

Table 1-3 shows the DB2 syntax you can use to specify these methods within DB2. It indicates the term that the DB2 for NetBackup uses to describe each method.

Table 1-3 Use of user exit and VENDOR terminology

Setting used with "user exit"	Setting used with "VENDOR"

`LOGARCHMETH1=LOGRETAIN`
`LOGARCHMETH1=USEREXIT`
`USEREXIT=ON`
`USEREXIT=YES`
`LOGRETAIN=ON`
`LOGRETAIN=RECOVERY`
	`LOGARCHMETH1=VENDOR`*library*

When `VENDOR` is used, archive logs are backed up by means of the NetBackup for DB2 vendor library. The full specification for this archive log method is as follows:

On Windows: `LOGARCHMETH1=VENDOR:`*`install_path`*`\NetBackup\bin\nbdb2.dll`

On UNIX: `LOGARCHMETH1=VENDOR:/usr/openv/netbackup/bin/`*`library`*

For *library*, specify an operating system-specific library.

See "About the NetBackup for DB2 components" on page 11.

When a user exit program is used, archive logs are backed up by means of the NetBackup for DB2 user exit program. The DB2 syntax that defines the user exit program includes the `USEREXIT`, `LOGRETAIN`, and `LOGARCHMETH1` keywords that are specified in a configuration parameter.

Chapter 2

Installing NetBackup for DB2

This chapter includes the following topics:

- Planning the installation of NetBackup for DB2
- Verifying the operating system and platform compatibility
- License for NetBackup for DB2
- About log archiving
- Specifying the DB2 home path (UNIX)
- About adding new DB2 instances

Planning the installation of NetBackup for DB2

Table 2-1 shows the major installation steps that are needed to run NetBackup for DB2. Each step contains one or more links to pertinent procedures and concepts.

Table 2-1 Installation steps for NetBackup for DB2

Step	Action	Description
Step 1	Verify the installation prerequisites.	https://support.cohesity.com/s/article/article-100040093
Step 2	Verify that the primary server has a valid license for NetBackup for DB2 and any NetBackup options or add-ons.	See "License for NetBackup for DB2" on page 18.
Step 3	Specify a log archive method.	See "About log archiving" on page 18.

Table 2-1 Installation steps for NetBackup for DB2 *(continued)*

Step	Action	Description
Step 4	(UNIX) specify the DB2 home path.	See "Specifying the DB2 home path (UNIX)" on page 20.
Step 5	Add a new database instance.	See "About adding new DB2 instances" on page 21.

Verifying the operating system and platform compatibility

Verify that the NetBackup for DB2 agent is supported on your operating system or platform.

To verify operating system and compatibility

1. Go to the NetBackup compatibility list site.

   https://support.cohesity.com/s/article/article-100040093

2. Select the link for the following document:

   Application/Database Agent Compatibility List

3. For information on support for Snapshot Client, see the Snapshot Client section in the following document:

   Hardware and Cloud Storage Compatibility List (HCL).

NetBackup server and client requirements

Before you install NetBackup, review the requirements for the NetBackup server and the NetBackup clients.

NetBackup server requirements

Note: To use NetBackup for DB2 with Snapshot Client, you must have a license for NetBackup Snapshot Client.

Verify that the following requirements are met for the NetBackup server:

- The NetBackup server software is installed and operational on the NetBackup server.
  See the NetBackup Installation Guide.

- Make sure that you configure any backup media that the storage unit uses. The number of media volumes that are required depends on several things:
  - The devices that are used and the storage capacity of the media.
  - The sizes of the databases that you want to back up.
  - The amount of data that you want to archive.
  - The size of your backups.
  - The frequency of backups or archives.
  - The length of retention of the backup images.

  See the NetBackup Administrator's Guide, Volume I.

NetBackup client requirements

Verify that the following requirements are met for the NetBackup clients:

- The NetBackup client software is installed on the computer that has the databases you want to back up.
- If the database is clustered, you must use the same version of NetBackup on each node in the cluster.
- To use the new features that are included in NetBackup for DB2 in NetBackup 11.2.0.1, you must upgrade your NetBackup for DB2 clients to NetBackup 11.2.0.1. The NetBackup media server must use the same version as the NetBackup for DB2 client or a higher version than the client.

DB2 server software requirements

Verify the following regarding the DB2 server software on the NetBackup server or client:

- The DB2 server software must be installed and operational.

  Refer to the Application/Database Agent Compatibility List for supported versions of the DB2 server software.
- One or more DB2 instances must exist.

Note: In a DB2 EEE environment, install the NetBackup client software on every node and client that DB2 uses.

See "NetBackup server and client requirements" on page 16.

Requirements for using NetBackup for DB2 in a NetBackup cluster

If you plan to use NetBackup for DB2 on a NetBackup server configured in a NetBackup cluster, verify the following requirements:

- NetBackup supports your cluster environment.
  the Software Compatibility List (SCL).
- The NetBackup server software is installed and configured to work in a NetBackup cluster.
  See the NetBackup Installation Guide.
  See the NetBackup Clustered Primary Server Administrator's Guide.
- The NetBackup client software is installed and operational on each node to which NetBackup can failover.
- A valid license for NetBackup for DB2 must exist on each node where NetBackup server resides.

License for NetBackup for DB2

The NetBackup for DB2 agent is installed with the NetBackup client software. No separate installation is required. A valid license for the agent must exist on the primary server.

More information is available on how to add licenses.

See the NetBackup Web UI Administrator's Guide.

For a NetBackup cluster, a valid license for NetBackup for DB2 must exist on each node where NetBackup server resides.

About log archiving

DB2 can write database archive logs by using several different methods. For a roll-forward recovery, you need both the database itself and the archive logs from the backup media. The DB2 parameters that specify an archive log method include the `LOGRETAIN`, `USEREXIT`, and `LOGARCHMETH1` keywords.

The following topics describe the archive methods and how to specify an archive method in DB2.

See "Using the VENDOR archive method" on page 19.

See "Using the user exit archive method" on page 19.

The terms "VENDOR" and "user exit" describe the methods that DB2 supports for log archiving. Ensure that you understand how the terms are used in this manual.

See "About NetBackup for DB2 terminology" on page 13.

Using the VENDOR archive method

Note the following about the `VENDOR` log archive method:

- The archive logs are backed up by a data stream and use a schedule type of **Application Backup**.
- NetBackup for DB2 backs up and restores the archive log files as a byte stream. This method uses the DB2 backup API and the DB2 restore API.

To use the VENDOR archive method

1. Quiesce the DB2 database.

   Perform this procedure and the configuration procedures at a time when minimal changes are made to the DB2 database.

2. Specify the archive method. The syntax is as follows:

   On Windows:
   `LOGARCHMETH1=VENDOR:`*`install_path`*`\NetBackup\bin\nbdb2.dll`

   On UNIX: `LOGARCHMETH1=VENDOR:/usr/openv/netbackup/bin/`*`library`*

   For the library name, refer to the following topic.

   See "About the NetBackup for DB2 components" on page 11.

3. Verify your DB2 configuration to ensure that the appropriate log archiving method for your site is enabled.

   If necessary, edit your DB2 configuration specifications to specify the log archiving method.

Using the user exit archive method

NetBackup for DB2 includes a user exit program that you can use to back up the archive logs. Any DB2 release lets you use this log archive method. The syntax for specifying the user exit method depends on the DB2 release.

If your DB2 configuration uses the `USEREXIT`, `LOGRETAIN`, or `LOGARCHMETH1` keyword in its configuration parameters, note the following:

- NetBackup for DB2 backs up and restores the archive log files as individual files.
- DB2 supports this archive method only for backward compatibility.

To use the user exit archive method

1. Quiesce the DB2 database.

   Perform this procedure and the configuration procedures at a time when minimal changes are made to the DB2 database.

2. Specify the archive method.

   The method you use to specify these parameters and the syntax for these parameters depends on the DB2 version level. For more information on the effects of these parameters within DB2, or on the specific syntax for these parameters, see your DB2 documentation.

3. If your DB2 configuration uses the `USEREXIT`, `LOGRETAIN`, or `LOGARCHMETH1` keyword in its configuration parameters, configure one of the following:

   - On Windows, a separate MS-Windows policy that includes the archive logs.
   - On UNIX, a separate Standard policy that includes the archive logs.
   - On UNIX, directories for the user exit program to use when it copies the archive logs. You may also want to create a separate Standard policy for backing up these directories.
   - On Windows, directories for the user exit program to use when it copies the archive logs. You may also want to create a separate MS-Windows policy for backing up these directories.
   - On UNIX, modify an existing Standard policy with a user backup schedule. Include the archive log directories..
   - On Windows, modify an existing MS-Windows policy with a user backup schedule. Include the archive log directories.

4. Verify your DB2 configuration to ensure that the appropriate log archiving method for your site is enabled.

   If necessary, edit your DB2 configuration specifications to specify the log archiving method.

Specifying the DB2 home path (UNIX)

After you install NetBackup with a valid license for NetBackup for DB2, run this script on the computer where the DB2 vendor software is installed. With this script, NetBackup can gather additional information about your DB2 environment.

Complete this procedure at the following times:

- After you specify a log archiving method in DB2.
- If you licensed NetBackup for DB2 for the first time.

- After you create a new DB2 instance.

To specify the DB2 home path

1. Change to the following directory:

   `/usr/openv/netbackup/bin`

2. Run the following script:

   `./db2_config`

3. Supply the home path for the database instance.

   For example:

   `/home/db2inst1`

4. Add any other database instances, or enter `n` if you are finished.

About adding new DB2 instances

Adding new DB2 instances on a Windows system is different than adding new instances on a UNIX system.

- On Windows, the NetBackup for DB2 installation software writes the user exit program to the following location:

  install_path`\NetBackup\dbext\DB2\db2uext2.exe`

  DB2 expects the `db2uext2` executable to reside in the DB2 installation location. If you reinstall or move the DB2 installation, manually copy `db2uext2.exe` from the NetBackup location into the DB2 location.

- On UNIX, if you install a new DB2 instance after you install NetBackup, you need to add this new instance to the NetBackup configuration. This action ensures that all new DB2 instances are included in backup operations.
  See "Specifying the DB2 home path (UNIX)" on page 20.

Chapter 3

Configuring NetBackup for DB2

This chapter includes the following topics:

- Overview of NetBackup for DB2 configuration
- About permissions for NetBackup for DB2 log files (UNIX)
- About configuring a backup policy for DB2
- About adding backup selections to a DB2 policy
- Configure an application backup schedule
- Example application backup schedule
- Configure automatic backup schedules
- Example automatic backup schedule
- Schedule properties
- NetBackup for DB2 backup types
- Perform a manual backup
- Reviewing the auto-discovered mappings
- About backing up archive log files with the user exit program
- Configuring the run-time environment
- About NetBackup for DB2 shell scripts
- RBAC role for the DB2 administrator

Overview of NetBackup for DB2 configuration

Before you configure NetBackup for DB2, complete the installation procedure.

See "Planning the installation of NetBackup for DB2 " on page 15.

Table 3-1 shows the three major parts of NetBackup for DB2 configuration.

Table 3-1 Configuration tasks for DB2

Task	Description
Configure a backup policy for a DB2 database	A backup policy for a database defines the backup criteria for a specific group of one or more clients. To back up the database environment, you must define at least one DB2 policy with the appropriate schedules. See "About configuring a backup policy for DB2 " on page 23.
Configure the run-time environment	Configuring the run-time environment consists of creating a `db2.conf` file for a standard environment as well as a cluster environment. It also shows the environment variables that NetBackup creates. See "Creating a db2.conf file for use with the user exit program" on page 42. See "Creating a db2.conf file (vendor method)" on page 46. See "Keywords for the db2.conf file" on page 49.
Create a shell script	To perform a scheduled NetBackup for DB2 backup, you must create a shell script. The shell script controls the backup job on the NetBackup for DB2 client. See "About NetBackup for DB2 shell scripts" on page 55.

About permissions for NetBackup for DB2 log files (UNIX)

NetBackup uses the `/usr/openv/netbackup/logs` directory tree not only for the recording of troubleshooting information, but for progress and communication updates to users and other NetBackup applications. Restrictive permissions on these directories can not only disable the collection of troubleshooting data, but also prevent the application itself from functioning correctly.

About configuring a backup policy for DB2

A backup policy defines the backup criteria for a specific group of one or more clients.

These criteria include the following:

- Storage unit and media to use
- Policy attributes
- Backup schedules
- The clients to back up
- The script files to run on the clients

To back up the database environment, define at least one DB2 policy with the appropriate schedules. A configuration can have a single policy that includes all clients, or there can be many policies, some of which include only one client.

See "Add a policy for DB2" on page 24.

Add a policy for DB2

This topic describes how to create a policy to protect a database.

To add a policy for DB2

1. Open the NetBackup web UI.

   See "Specifying the primary server for a NetBackup for DB2 client" on page 26.

2. On the left, select **Protection > Policies**. Then select **Add**.
3. Type a unique name for the new policy.
4. From the **Policy type** list, select **DB2**.
5. Complete the entries on the **Attributes** tab.

   See "About policy attributes" on page 25.

6. Add other policy information as follows:
   - Add schedules.
     See "Configure an application backup schedule" on page 30.
     See "Configure automatic backup schedules" on page 31.
   - Add clients.
     See "Add clients to a policy" on page 25.
   - Add scripts to the backup selections list.
     See "About adding backup selections to a DB2 policy" on page 28.
7. When you have completed the policy configuration, select **Create**.

About policy attributes

With a few exceptions, policy attributes for a DB2 policy are managed in the same way as for most other policy types. Certain policy attributes vary according to your specific backup strategy and system configuration.

For more information on policy attributes, see the NetBackup Administrator's Guide, Volume I.

Table 3-2 Policy attributes for NetBackup for DB2 policies

Attribute	Description
Policy type	Determines the types of clients that can be backed up with the policy. For DB2 databases, select the policy type **DB2**.
Keyword phrase	For NetBackup for DB2, the **Keyword phrase** entry is ignored.
Snapshot Client and Replication Director	This group contains the options that enable backups with Snapshot Client. See "NetBackup for DB2 with Snapshot Client features" on page 83.

Add clients to a policy

The client list contains a list of the clients on which your scripts are run during an automatic backup. This list determines the clients that can send backup requests to the application schedule. A NetBackup client must be in at least one policy but can be in more than one.

For a NetBackup for DB2 policy, clients you want to add must have the following items installed or available:

- DB2
- NetBackup client or server
- The backup or restore scripts

To add clients to a policy

1. Open the policy and select the **Clients** tab.
2. Select **Add**.

3 Type the name of the client and select the hardware and operating system of the client.

If DB2 is installed in a cluster, specify the virtual name of the DB2 server as the client name.

Note: If you installed NetBackup on more than one node in the DB2 cluster, you must perform additional configuration.

See "Reviewing the auto-discovered mappings" on page 35.

---

4 Select **Add**.

Specifying the primary server for a NetBackup for DB2 client

After you add your NetBackup for DB2 client to a policy, specify the primary server for the client.

Note: Add the server names to the primary server before you configure the server list on the client.

To specify the primary server for a NetBackup for DB2 client

1 Open the NetBackup web UI.

2 On the left, select **Hosts > Host properties**.

3 Select the NetBackup for DB2 client name.

4 If necessary, select **Connect**. Then select **Edit client**.

5 Select **Servers**.

6 Verify that the correct server displays as the **Primary server**.

If the correct server does not display, locate the server name in the **Additional servers** list, and click **Actions > Make primary**. Alternatively, select **Add** to add a new server name to the list.

7 Click **Save**.

Configuring a policy to back up the configuration files

This topic shows how to create an automatic backup policy to back up the NetBackup configuration files. If you want users to be able to back up configuration files manually, you must also create a User Backup schedule.

To back up configuration files

1. Create an MS-Windows (Windows) or Standard (UNIX) policy.
2. Specify the attributes for the policy.
3. On the **Schedules** tab, create a full backup schedule.
4. In the **Backup selections** list, add an entry that includes the full path name of the directory that contains the configuration files.
5. Specify the clients to back up.

   The clients must have the following installed:

   - DB2
   - NetBackup for DB2

   If the client is installed in a DB2 cluster, add the virtual host name to the client list.

Note: If you installed NetBackup on more than one node in the DB2 cluster, you must perform additional configuration. You must approve each valid**Auto-Discovered Mapping** that NetBackup discovers in your environment.

See "Reviewing the auto-discovered mappings" on page 35.

Configuring the Maximum jobs per client

The **Maximum jobs per client** specifies the maximum number of concurrent backups that are allowed per client.

Note: Enter a large enough value for the **Maximum jobs per client** attribute to meet the number of jobs that DB2 runs. You may need to experiment with different values at your site.

To configure the maximum jobs per client

1. On the left, select **Hosts > Host properties**.
2. Select the primary server.
3. If necessary, select **Connect**. Then select **Edit primary server**.
4. Select **Global attributes**.
5. Select the appropriate value for **Maximum jobs per client**.

   The default is 1.

You can use the following formula to calculate a smaller value for the Maximum jobs per client setting:

Maximum jobs per client = *number_of_sessions* X *number_of_policies*

Refer to the following definitions:

number_of_sessions The number of backup sessions between the backup server and NetBackup on the client. Each separate session starts a new backup job on the client.

number_of_policies The number of policies of any type that can back up this client at the same time. This number can be greater than one. For example, a client can be in two policies to back up two different databases. These backup windows can overlap.

About adding backup selections to a DB2 policy

The backup selections list in a database policy has a different meaning than for non-database policies. For example, in a Standard or MS-Windows policy, the list contains files and directories to be backed up.

In a database policy, you specify scripts to be run.

Observe the following rules when you use scripts:

- Make sure that the scripts reside on each client in the client list.
- NetBackup installs sample scripts when you install the software; you can modify these scripts for your own use.
- All scripts must be in an authorized location.
  See "Registering authorized locations used by a NetBackup database script-based policy" on page 133.
- If you use NetBackup for DB2 in a NetBackup server cluster, make sure that the scripts reside in a location that is available after a failover.

Note: All scripts must be stored and run locally. One recommendation is that scripts should not be world-writable. Scripts are not allowed to be run from network or remote locations. Any script that is created and saved in the NetBackup `db_ext` (UNIX) or `dbext` (Windows) location needs to be protected during a NetBackup uninstall.

For more information about registering authorized locations and scripts, review the knowledge base article:

Registering authorized locations used by a NetBackup database script-based policy

---

Add scripts to the backup selections list only if you want to set up a policy for automatic backups. These scripts are run for manual backups and for automatic schedules as specified under the **Schedules** tab. NetBackup runs the scripts in the order that they appear in the backup selections list.

See "About NetBackup for DB2 shell scripts" on page 55.

See "Adding a script to the backup selections list" on page 29.

About backup schedules and scripts

Be aware of what may happen if an automatic schedule invokes a script that a user authored. NetBackup does not provide safeguards to prevent an automatic backup schedule from running a restore or a recovery script.

See "About adding backup selections to a DB2 policy" on page 28.

See "Adding a script to the backup selections list" on page 29.

Adding a script to the backup selections list

The following procedure describes how to add a script to the backup selections list.

Note: Be sure to specify the correct script name in the backup selections list to prevent an error or a wrong operation.

To add a script to the backup selections list

1. Open the policy.
2. Select the **Backup selections** tab.
3. Select **Add**.
4. In the **Script** box, type the full path name of a script on the client.

   For example:

   ```
   /backup_scripts/db/cold_backup.sh
   C:\backup_scripts\db\cold_backup.cmd
   ```

   See "Registering authorized locations used by a NetBackup database script-based policy" on page 133.
5. Select **Add** to add the script to the list.
6. Select **Save**.

Note: Be aware of what may happen if an automatic schedule invokes a script that a user authored. NetBackup does not provide safeguards to prevent an automatic backup schedule from running a restore or a recovery script.

Configure an application backup schedule

A database backup requires an application backup schedule. You cannot perform backups if this type of schedule is not included in the policy. NetBackup automatically creates this schedule and names it **Default-Application-Backup**.

The backup window for an application backup schedule must encompass the time period during which all scheduled jobs and client-initiated jobs can occur. This window is necessary because the application backup schedule accepts the backup request from NetBackup for DB2 regardless of whether the backup was initiated from an automatic schedule or from the client. You can choose to set the window for the application backup schedule for 24 hours per day, seven days per week. This window ensures that your operations are never locked out due to the application backup schedule.

To configure an application backup schedule

1. Open the policy and select the **Schedules** tab.
2. Select the schedule that is named **Default-Application-Backup** and select **Edit**.
3. Specify the other properties for the schedule.

   See "Schedule properties" on page 32.
4. Select **Add**.

Example application backup schedule

Specify the application backup schedule name in the `db2.conf` file on the client. The `db2.conf` file is located in the following directory path:

Windows: *install_path*`\NetBackup\dbext\db2\db2.conf`

UNIX: `$DB2_Instance_Home/db2.conf`

Assume the following:

- Users perform database backup operations during business hours, 08:00 to 13:00.
- The automatic backups that use this policy start between 18:00 and 22:00.

In this scenario, the application backup schedule must have a start time of 0800 and a duration of 14 hours. Alternatively, the schedule can have two windows each day; one with a start time of 0800 and duration of 5 hours, and another with a start time of 1800 and a duration of 4 hours.

Table 3-3 Example settings for a NetBackup for DB2 application backup schedule

Schedule option	Setting
Retention	2 weeks
Backup window	Sunday through Saturday 00:08:00 - 22:00:00

Configure automatic backup schedules

If you plan to have NetBackup perform automatic backups, or if you use Snapshot Client features, you need one or more automatic backup schedules.

To configure an automatic backup schedule

1. Open the policy and select the **Schedules** tab.
2. Click **Add**.
3. Specify a unique name for the schedule.
4. Select the **Type of backup**.

   See "NetBackup for DB2 backup types" on page 33.
5. Specify the other properties for the schedule.

   See "Schedule properties" on page 32.
6. Select **Add**.

Example automatic backup schedule

Table 3-4 shows example settings for automatic backup schedules.

Table 3-4 Example settings for NetBackup for DB2 automatic backup schedules

Type of backup	Schedule property	Setting
Automatic full backup	Retention (proxy backup only)	2 weeks

Table 3-4 Example settings for NetBackup for DB2 automatic backup schedules *(continued)*

Type of backup	Schedule property	Setting
	Frequency	Every week
	Backup window	Sunday, 18:00:00 - 22:00:00
Automatic differential incremental backup, **Automatic cumulative incremental backup**	Retention (proxy backup only)	1 week
	Frequency	Every day
	Backup window	Sunday through Saturday 18:00:00 - 22:00:00

Schedule properties

This topic describes the schedule properties that have a different meaning for database backups than for file system backups. Other schedule properties vary according to your specific backup strategy and system configuration. Additional information about other schedule properties is available. See the NetBackup Administrator's Guide, Volume I.

Table 3-5 Description of schedule properties

Property	Description
Type of backup	Specifies the type of backup that this schedule can control. The selection list shows only the backup types that apply to the policy you want to configure. See "NetBackup for DB2 backup types" on page 33.
Schedule type	You can schedule an automatic backup in one of the following ways: ■ **Calendar** The **Calendar** option lets you schedule the backup operations that are based on specific dates, recurring week days, or recurring days of the month. ■ **Frequency** The **Frequency** specifies the period of time that can elapse until the next backup operation begins on this schedule. For example, assume that the frequency is 7 days and a successful backup occurs on Wednesday. The next full backup does not occur until the following Wednesday. Typically, incremental backups have a shorter frequency than full backups.

Table 3-5 Description of schedule properties *(continued)*

Property	Description
Retention	Specifies a retention period to keep backup copies of files before they are deleted. The retention level also denotes a schedule priority within the policy. A higher level has a higher priority. Set the time period to retain at least two full backups of your database. In this way, if one full backup is lost, you have another full backup to restore. For example, if your database is backed up once every Sunday morning, you should select a retention period of at least 2 weeks. The retention period for an application backup type schedule refers to the length of time that NetBackup keeps backup images for stream-based backups. The retention period for an automatic backup type schedule refers to the length of time that NetBackup keeps backup images for non-stream-based backups (Example: snapshot). The DB2 database also has retention settings for backup images in the DB2 catalog. As a general recommendation, the NetBackup retention of a backup image should be longer than the database retention of the same backup image.
Effect of type of schedule on retention period	The type of schedule you select affects the retention period as follows: ■ Frequency-based scheduling Set a retention period that is longer than the frequency setting for the schedule. For example, if the frequency setting is set to one week, set the retention period to be more than one week. The NetBackup scheduler compares the latest record of the automatic backup schedule to the frequency of that automatic backup schedule. This comparison is done to determine whether a backup is due. So if you set the retention period to expire the record too early, the scheduled backup frequency is unpredictable. However, if you set the retention period to be longer than necessary, the NetBackup catalog accumulates unnecessary records. ■ Calendar-based scheduling The retention period setting is not significant for calendar-based scheduling.
Multiple copies	If you want to specify multiple copies of a backup for the policy, configure **Multiple copies** on the application backup schedule. If using Snapshot Client, also specify **Multiple copies** on the automatic schedule.

NetBackup for DB2 backup types

Each database agent has a unique set of backup schedules.

Table 3-6 shows the DB2 backup schedules you can specify.

Table 3-6 DB2 backup types

Backup type	Description
Application Backup	The Application Backup schedule enables user-controlled NetBackup operations from the client. These operations include those initiated from the client and those initiated by an automatic schedule on the primary server. NetBackup uses the Application Backup schedule when the user starts a backup manually. Configure at least one Application Backup schedule for each database policy. The Default-Application-Backup schedule is configured automatically as an Application Backup schedule.
Automatic Full Backup	An Automatic full backup contains a copy of all the data. A full backup is not the same as a whole database backup. Full means that the backup is not one of the incremental backup types. To perform a stream-based Automatic full backup, also specify an Automatic Full Backup schedule for scheduled NetBackup operations. Snapshot Client only supports this type of backup and the Block-Level Incremental (BLI) Backup.
Automatic Differential incremental backup	An Automatic Differential incremental backup is an incremental backup that is not cumulative. The backup contains a copy of the database data that has changed since the most recent backup, full or otherwise. This type of backup corresponds to the `INCREMENTAL DELTA` option of the DB2 `BACKUP` command. This type of backup takes less space and time than a cumulative incremental backup. The backup includes only the data that changed since the last backup of any type. This type of backup is supported only for stream-based backups and for BLI backups.
Automatic Cumulative incremental backup	An Automatic Cumulative incremental backup is an incremental backup that is cumulative. The backup contains a copy of the database data that changed since the most recent full backup. This type of backup corresponds to the `INCREMENTAL` option of the DB2 `BACKUP` command. Automatic Cumulative Incremental backups are supported only for stream-based backups and for BLI backups. This backup takes less time and space than a full backup; it contains only the data that changed since the last full backup.

Note: For the types of backup schedules, the information in this topic pertains to stream-based backups. If you use the Snapshot Client option, some of the information in that table may differ.

More information about backup schedules and Snapshot Client features is available.

See "NetBackup for DB2 with Snapshot Client features" on page 83.

Perform a manual backup

After you configure the servers and assets in your environment, you can test the configuration settings with a manual backup. Perform a manual backup (or backups) from a policy with the automatic backup schedules that you created.

To perform a manual backup from a policy

1. On the left, select **Protection > Policies**.
2. Select the policy you want to test.
3. Select **Manual backup**.
4. Select the schedule that you want to use for the manual backup.
5. Select the clients that you want to include for the manual backup.

Reviewing the auto-discovered mappings

In certain scenarios, a NetBackup host shares a particular name with other hosts or has a name that is associated with a cluster. To successfully perform backups and restores with NetBackup for DB2, you must approve each valid auto-discovered mapping that NetBackup discovers in your environment. Or, manually add the mappings.

See the section called "Approve the auto-discovered mappings for a cluster" on page 36.

See the section called "Manually map host names" on page 37.

Examples of the configurations that have multiple host names include:

- A host is associated with its fully qualified domain name (FQDN) and its short name or its IP address.
- If the DB2 server is clustered, the host is associated with its node name and the virtual name of the cluster.

These mappings are configured in the **Security > Host mappings** node in the NetBackup web UI. You can also use the `nbhostmgmt` command to manage the

mappings. See the NetBackup Security and Encryption Guide and NetBackup Web UI Administrator's Guide for more details.

Auto-discovered mappings for a cluster

In a DB2 cluster environment, you must map the node names to the virtual name of the cluster if the following apply:

- If the backup policy includes the cluster name (or virtual name)
- If the NetBackup client is installed on more than one node in the cluster, the virtual name must be mapped to each node.
  If the NetBackup Client is only installed on one node, then no mapping is necessary.

Approve the auto-discovered mappings for a cluster

To approve the auto-discovered mappings for a cluster

1. In the NetBackup web UI, expand **Security > Host mappings**.
2. Click the **Mappings to approve** tab.

   The list displays the hosts in your environment and the mappings or additional host names that NetBackup discovered for those hosts. A host has one entry for each mapping or name that is associated with it.

   For example, for a cluster with hosts `client01.lab04.com` and `client02.lab04.com`, you may see the following entries:

Host	Auto-discovered mapping
client01.lab04.com	client01
client01.lab04.com	clustername
client01.lab04.com	clustername.lab04.com
client02.lab04.com	client02
client02.lab04.com	clustername
client02.lab04.com	clustername.lab04.com

3. Click the name of the host.

4 Review the mappings for the host and click **Approve** if you want to use the discovered mappings.

For example, if the following mappings are valid for `client01.lab04.com`, then you approve them.

Auto-discovered mapping	Valid name for
client01	The short name of the client
clustername	The virtual name of the cluster
clustername.lab04.com	The FQDN of the virtual name of the cluster

5 When you finish approving the valid mappings for the hosts, click on the **Hosts** tab.

For hosts `client01.lab04.com` and `client02.lab04.com`, you see entries for **Mapped host or IP address** that are similar to the following:

Host	Mapped host names/IP addresses
client01.lab04.com	client01.lab04.com, client01, clustername, clustername.lab04.com
client02.lab04.com	client02.lab04.com, client02, clustername, clustername.lab04.com

6 If you need to add a mapping that NetBackup did not automatically discover, you can add it manually.

Table 3-7 Example mapped host names for a DB2 cluster environment

Environment	Host	Mapped host names
Cluster with two nodes	Physical name of *Node 1*	Virtual name of DB2 server
	Physical name of *Node 2*	Virtual name of DB2 server

Manually map host names

If you need to add a mapping that NetBackup did not automatically discover, you can add it manually.

To manually map host names

1. In the NetBackup web UI, expand **Security > Host mappings**.
2. Click on the **Hosts** tab.
3. Click **Add shared or cluster mappings**.

   For example, type the name of the virtual name of the cluster. Then click **Add** to choose the hosts to which you want to map that virtual name.

About backing up archive log files with the user exit program

You can configure the user exit program to back up the archive logs. The user exit program is `db2uext2` (UNIX) or `db2uext2.exe` (Windows).

The backup can be configured in one of the following ways:

- Save archive log files directly with NetBackup.
  To back up archive log files in this way, configure an MS-Windows or Standard policy with a User Backup schedule.
  See "Configuring a policy to back up the archive logs" on page 40.
  Then specify the `ARCFUNC SAVE` keywords in the configuration file `db2.conf`.
  See "Creating a db2.conf file for use with the user exit program" on page 42.
- Copy archive log files to another directory for later backup by NetBackup.
  To back up archive log files in this way, configure an MS-Windows or Standard policy with a User Archive schedule (this schedule is optional).
  See "Configuring a policy to back up the archive logs" on page 40.
  Specify the `ARCFUNC COPY` keywords in the `db2.conf` file.
  See "Creating a db2.conf file for use with the user exit program" on page 42.
  You can coordinate the copy of the log files to a directory with a user archive. In this case, the user exit program copies the file to an archive directory. To free disk space, later you can perform a user archive to archive all the files in the `ARCDIR` directory.

Do not specify `ARCFUNC SAVE` or `ARCFUNC COPY` if the `VENDOR DB2` configuration parameter is in effect. In environments with `VENDOR` in effect, NetBackup ignores the information that pertains to these commands.

Whether to specify `ARCFUNC SAVE` or `ARCFUNC COPY` depends on the amount of user intervention you intend to provide.

Determine which command to use, as follows:

- If you specify `ARCFUNC SAVE`, NetBackup backs up the archive logs according to the policy and schedule you specify.

  If DB2 later issues a `ROLLFORWARD` request, the user exit program looks for the archive logs on a backup volume. At restoration time, no user intervention is required. The sequential recovery can be slow if there are numerous, large log files.

- If you specify `ARCFUNC COPY`, NetBackup copies the archive logs to the location that is specified on the `ARCDIR` statement in the `db2.conf` file.

  The disk to which the archive logs are copied eventually fills with archived log files. Most users want to configure a user archive schedule so they can archive the entire `ARCDIR` directory to NetBackup volumes.

  This method requires some user intervention during the recovery. Specifically, you must restore these files before the roll-forward operation. Advanced users prefer this approach because of the performance and the flexibility benefits.

  For information about how to restore files to disk, see the NetBackup Administrator's Guide, Volume I.

DB2 objects in the backup window

Table 3-8 explains the DB2 object types displayed.

Table 3-8 DB2 database objects in the backup window

Object	Description
DB2 resource	If NetBackup for DB2 is detected on the client, the browser window displays the DB2 resource. This resource is the top-level DB2 object in the browser. `DB2` is the DB2 resource.
Instance	The second-level object is a DB2 instance. An instance represents a collection of DB2 databases.
Database	You cannot select a database for backup directly, but by selecting all partitions below it, you can effectively select the whole database. If you select the database for backup, you cannot select other databases. If you select objects within the database, you cannot select objects within other databases at the same time.

Table 3-8 DB2 database objects in the backup window *(continued)*

Object	Description
Partition	The partition is the highest selectable DB2 object. A partition represents a collection of storage within a database in which tablespaces are stored. Partitions contain tablespaces and log folders. Within a database, you can select one or more partitions. DB2 EEE/DPF environments generally consist of multiple partitions. Other DB2 UDB environments consist of a single partition, which is usually represented as partition zero (0). The display includes only partitions that reside on the same NetBackup client. It does not display other partitions on remote hosts. For more information, see the Caution that follows this table.
Tablespace	A tablespace is a logical entity representing a collection of physical storage containers. Tablespaces are comprised of containers, which represent database storage units. A tablespace is the lowest-level DB2 object that you can select in the browser.

Configuring a policy to back up the archive logs

This topic describes how to create a policy to back up the NetBackup DB2 archive log files directly to tape. Follow these instructions if you want to use the user exit program with the `ARCFUNC SAVE` command.

You do not need to perform this procedure if you use the `VENDOR` method to back up your archive log files.

To configure a policy to back up the archive logs

1. Open the NetBackup web UI.
2. Create a new MS-Windows (Windows) or Standard (UNIX) policy type.
3. Specify the attributes for the policy.
4. On the **Schedules** tab, create a **User backup** schedule.

   This schedule must encompass all of the time periods during which DB2 can call the user exit program.

   No backup selections list is necessary for this policy because it has a User backup schedule. It is not an automatic schedule.
5. On the **Clients** tab, add the clients you want to back up.

   The clients must have the following installed:

   - DB2

- NetBackup DB2

If the client is installed in a DB2 cluster, add the virtual host name to the client list.

Note: If you installed NetBackup on more than one node in the DB2 cluster, you must perform additional configuration. You must approve each valid auto-discovered mapping that NetBackup discovers in your environment.

See "Reviewing the auto-discovered mappings" on page 35.

---

6 Note the name of this policy.

7 When you configure the `db2.conf` file, specify the name of the policy you created in this procedure.

See "Creating a db2.conf file for use with the user exit program" on page 42.

Configuring a policy to archive the archive logs

This topic describes how to create a policy to archive the NetBackup DB2 archive log entries in the `ARCDIR` directory. Follow these instructions if you want to use the user exit program with the `ARCFUNC COPY` command.

When NetBackup performs an archive, it deletes the online files after they are backed up successfully.

For more information on user archive schedules, see the NetBackup Administrator's Guide, Volume I.

You do not need to perform this procedure if you use the `VENDOR` method to back up your archive log files.

To configure a policy to back up the archive logs

1 Start the NetBackup web UI.

2 Create a new MS-Windows (Windows) or Standard (UNIX) policy type.

3 Specify the attributes for the policy.

4 On the **Schedules** tab, create a **User archive** schedule.

This schedule must encompass all of the time periods during which DB2 can call the user exit program.

No backup selections list is necessary for this policy because it has a User archive schedule. It is not an automatic schedule.

5 Specify the clients to be backed up.

The clients must have the following installed:

- DB2
- NetBackup for DB2

If the client is installed in a DB2 cluster, add the virtual host name to the client list.

Note: If you installed NetBackup on more than one node in the DB2 cluster, you must perform additional configuration. You must approve each valid auto-discovered mapping that NetBackup discovers in your environment.

See "Reviewing the auto-discovered mappings" on page 35.

Configuring the run-time environment

Configuring the run-time environment consists of creating a `db2.conf` file for a standard environment as well as a cluster environment. It also shows the environment variables that NetBackup creates.

See "Creating a db2.conf file for use with the user exit program" on page 42.

See "Creating a db2.conf file (vendor method)" on page 46.

Creating a db2.conf file for use with the user exit program

The NetBackup for DB2 configuration file `db2.conf`, consists of a series of keywords and values. This file defines how to back up the database and the archive logs. It must be created on each NetBackup for DB2 client.

The installation package installed a file named `db2.conf` that you can customize. The following procedures show you how to customize this file. Follow the instructions in this section if you use the user exit program to perform backups.

To create a db2.conf file for use with the user exit program

1. Before you create the `db2.conf` file, you need to create the policies to back up the archive logs and the configuration files.

   See "Configuring a policy to back up the archive logs" on page 40.

   See "Configuring a policy to archive the archive logs" on page 41.

   See "Configuring a policy to back up the configuration files" on page 26.

2. Log on to a client computer.

3 Copy the sample `db2.conf` file from its location in the sample directory to its active location.

Its location in the sample directory is as follows:

Windows: *install_path*`\NetBackup\dbext\db2\samples`

UNIX: `/usr/openv/netbackup/ext/db_ext/db2/scripts`

The active location for the `db2.conf` file is as follows:

Windows: *install_path*`\NetBackup\dbext\db2\db2.conf`

UNIX: `$DB2_Instance_Home/db2.conf`

4 In the `db2.conf` file, create an object identifier for backing up the database.

This object identifier starts with the following keyword lines:

```
DATABASE SAMPLE
OBJECTTYPE DATABASE
...
```

5 In the `db2.conf` file, create an object identifier for backing up the archive logs.

The form depends on how the archive logs are backed up, as follows:

- If you use `ARCFUNC SAVE`:

```
DATABASE SAMPLE
OBJECTTYPE ARCHIVE

POLICY WIN_TYPE_POL_LOGPOL # an MS-Windows-NT type policy

POLICY STD_TYPE_POL_LOGPOL # a standard UNIX type policy

SCHEDULE USER_BACKUP_SCHED_LOGSCHED
```

  In the `POLICY` line, specify the name of the MS-Windows or Standard policy for backing up the archive logs.
  In the `SCHEDULE` line, specify the User Backup schedule that you created earlier for backing up the archive logs.
  See "Example db2.conf file using ARCFUNC SAVE" on page 44.

- If you use `ARCFUNC COPY`:

```
DATABASE SAMPLE
OBJECTTYPE ARCHIVE

Windows: ARCDIR C:\MyLogs\arcdir\
RETDIR C:\MyLogs\arcdir\
```

```
UNIX: ARCDIR /home/db2inst1/arcdir
RETDIR /home/db2inst1/arcdir
```

In the ARCDIR line, specify the full path to the location of the archive logs. In the RETDIR line, specify the full path to the location from which the archive logs are retrieved. Typically, the RETDIR location is the same as the ARCDIR location.

See "Example db2.conf file using ARCFUNC COPY" on page 45.

6 You may need to add other entries to the db2.conf file.

See "Keywords for the db2.conf file" on page 49.

7 Save and close the db2.conf file.

8 Repeat this procedure on each client computer.

Example db2.conf file using ARCFUNC SAVE

Assume that you need to back up a database named SAMPLE and its archive logs. USEREXIT is enabled for database SAMPLE. The policies for the database SAMPLE include the required schedules for the backups.

The policies are as follows:

- The DB2_DB_Policy backs up the database. This policy has an application backup schedule and an automatic backup schedule. The first definition in the example db2.conf file specifies this policy and its application backup schedule, which is named Default-Application-Backup. The automatic backup schedule is not specified in db2.conf.
- The DB2_Log_Policy backs up the archive logs. This policy has a user backup schedule named User. The second entry in the example file specifies this policy and its user backup schedule.

```
DATABASE SAMPLE
OBJECTTYPE DATABASE
POLICY DB2_DB_Policy
SCHEDULE Default-Application-Backup
ENDOPER

DATABASE SAMPLE
OBJECTTYPE ARCHIVE
POLICY DB2_Log_Policy
SCHEDULE User
ARCFUNC SAVE
#ARCFUNC COPY
```

```
#ARCDIR C:\MyLogs\arcdir\
#RETDIR C:\MyLogs\arcdir\

#ARCDIR /home/db2inst1/arcdir
#RETDIR /home/db2inst1/arcdir

ENDOPER
```

Example db2.conf file using ARCFUNC COPY

Assume that you need to back up a database named `SAMPLE` and its archive logs. `USEREXIT` is enabled for database `SAMPLE`. The policies for the database `SAMPLE` include the required schedules for the backups.

The policies are as follows:

- The `DB2_DB_Policy` backs up the database. This policy has an application backup schedule and an automatic backup schedule. The first definition in the example `db2.conf` file specifies this policy and its application backup schedule, which is named `Default-Application-Backup`. The automatic backup schedule is not specified in `db2.conf`.
- The `ARCFUNC COPY` command copies the archive logs to the `ARCDIR` directory.

```
DATABASE SAMPLE
OBJECTTYPE DATABASE
POLICY DB2_DB_Policy
SCHEDULE Default-Application-Backup
ENDOPER

DATABASE SAMPLE
OBJECTTYPE ARCHIVE
#POLICY DB2_Log_Policy
#SCHEDULE User
#ARCFUNC SAVE
ARCFUNC COPY

ARCDIR C:\MyLogs\arcdir\
RETDIR C:\MyLogs\arcdir\

ARCDIR /home/db2inst1/arcdir
RETDIR /home/db2inst1/arcdir
```

```
ENDOPER
```

Creating a db2.conf file (vendor method)

The NetBackup for DB2 configuration file `db2.conf` consists of a series of keywords and values. This file defines how to back up the database and the archive logs. It must be created on each NetBackup for DB2 client.

The installation package installed a file named `db2.conf` that you can customize. The following procedures show you how to customize this file. Follow the instructions in this section if you use the vendor method to perform backups.

To create a db2.conf file for use with the vendor method

1. Before you create the `db2.conf` file, you need to create the policies to back up the configuration files.

   See "Configuring a policy to back up the configuration files" on page 26.

2. Log into a client computer.

3. Copy the sample `db2.conf` file from its location in the sample directory to its active location.

   Its location in the sample directory is as follows:

   Windows: *install_path*`\NetBackup\dbext\db2\samples`

   UNIX: `/usr/openv/netbackup/ext/db_ext/db2/scripts`

   The active location for the `db2.conf` file is as follows:

   Windows: *install_path*`\NetBackup\dbext\db2\db2.conf`

   UNIX: `$DB2_Instance_Home/db2.conf`

4. In the `db2.conf` file, create an object identifier for backing up the database.

   This object identifier starts with the following keyword lines:

```
DATABASE SAMPLE
OBJECTTYPE DATABASE
. . .
```

5 In the `db2.conf` file, create an object identifier for backing up the archive logs.

```
DATABASE SAMPLE
OBJECTTYPE ARCHIVE
POLICY DB2_TYPE_POL_LOGPOL # a DB2 type policy
SCHEDULE DEFAULT-APPLICATION-BACKUP
```

In the `POLICY` line, specify the name of a DB2 policy. This policy can be the same policy that you use to back up the database.

In the `SCHEDULE` line, specify a Default-Application-Backup schedule.

6 You may need to add other entries to the `db2.conf` file.

See "Keywords for the db2.conf file" on page 49.

7 Save and close the `db2.conf` file.

8 Repeat this procedure on each client computer.

See "Example db2.conf file (vendor method)" on page 47.

Example db2.conf file (vendor method)

Assume that you need to back up a database named `SAMPLE` and its archive logs. The `VENDOR` method is enabled for database `SAMPLE`. The policies for the database `SAMPLE` specify the required schedules for the backups.

The policies are as follows:

- The `DB2_DB_Policy` backs up the database. This policy has an application backup schedule and an automatic backup schedule. The first definition in the example `db2.conf` file specifies this policy and its application backup schedule, which is named `Default-Application-Backup`. The automatic backup schedule is not specified in `db2.conf`.
- The `DB2_ARCH_Policy` backs up the archive logs. This policy has an application backup schedule named `Default-Application-Backup`. The third entry in the example file specifies this policy and its application backup schedule.

```
DATABASE SAMPLE
OBJECTTYPE DATABASE
POLICY DB2_DB_Policy
SCHEDULE Default-Application-Backup
ENDOPER

#DATABASE SAMPLE
#OBJECTTYPE ARCHIVE
#POLICY DB2_Log_Policy
```

```
#SCHEDULE User
#ARCFUNC SAVE
#ARCFUNC COPY
#ARCDIR /home/db2inst1/arcdir
#RETDIR /home/db2inst1/arcdir
#ENDOPER

DATABASE SAMPLE
OBJECTTYPE ARCHIVE
POLICY DB2_ARCH_Policy
SCHEDULE Default-Application-Backup
ENDOPER
```

Configuring bp.conf files in a cluster environment

If you configure NetBackup for DB2 in a cluster environment, you need to create the NetBackup `bp.conf` files in multiple places.

Create the file in the following places:

- In `/usr/openv/netbackup/bp.conf` on the physical client host. This file is the primary `bp.conf` configuration file.
- In the DB2 user's home directory on each virtual host.

NetBackup searches for the `bp.conf` file in the DB2 user's home directory first. Specifications in the user `bp.conf` file override those in the primary `bp.conf` file.

Configuring a primary bp.conf file

The following procedures explain how to create a primary `bp.conf` file on the physical client host. This file allows other backups to be performed on the host.

To create a system-wide primary bp.conf file

1. Log on to the physical host.
2. Open the `bp.conf` file in the `/usr/openv/netbackup` directory.
3. Set the `CLIENT_NAME` entry to the physical host name of the NetBackup for DB2 client. This action allows other backups to be performed on the host.

   For example:

   ```
   CLIENT_NAME=client_name
   ```

4. Save and close the `bp.conf` file.

See "Configuring bp.conf files in a cluster environment" on page 48.

Configuring a user bp.conf file

NetBackup options in the `bp.conf` file of the home directory of the DB2 instance owner take precedence over the same options in the primary `bp.conf` file. The following procedure explains how to create a `bp.conf` file on the virtual machine that owns the DB2 instance.

To create a system bp.conf file on the virtual host

1. Log on to the computer that owns the DB2 instance.
2. Open the file `$DB2_INSTANCE_HOME/bp.conf`.
3. Add a line that sets the `CLIENT_NAME` entry to the virtual name of the DB2 instance.

   For example:

   ```
   CLIENT_NAME=client_name
   ```

4. Save and close the `bp.conf` file.

See "Configuring bp.conf files in a cluster environment" on page 48.

Keywords for the db2.conf file

The `db2.conf` file provides definitions NetBackup uses to perform DB2 backup and restore operations.

- Each definition is a grouping of keyword value pairs.
- Each definition contains an `OBJECTTYPE` keyword and value.
- Each definition ends with the `ENDOPER` keyword.
- All other keyword value pairs are optional, depending on the `OBJECTTYPE`.
- Within a definition, the *keyword value* pairs can appear in any order.
- The keywords are not case-sensitive, but the values are case-sensitive.
- When a pound character (#) appears in the first column, the line is treated as a comment.
- Backup and restore operations have two definitions, one for `OBJECTTYPE DATABASE` or `TABLESPACE` and one for `OBJECTTYPE ARCHIVE`.
- Restore operations to a different instance or database (not the original) must also have a definition for `OBJECTTYPE ALTERNATE`.

- NetBackup searches the file from top to bottom and uses the first definition that is found for the operation being performed. Later definitions for the same operation are ignored.
- NetBackup searches each definition from top to bottom and uses the first *value* specified for each *keyword* found. Later definitions for the same *keyword* are ignored.

The `db2.conf` file specifies the keywords that are described in this topic. If `LOGARCHMETH1 VENDOR` is configured in your DB2 environment, NetBackup for DB2 ignores the following keywords.

The following keywords:

- `ARCDIR`
- `ARCFUNC SAVE`
- `ARCFUNC COPY`
- `PARTITIONTYPE RAW`
- `RETDIR`

Table 3-9 describes the keywords and values that are used.

Table 3-9 Keyword value pairs for the db2.conf file

Keyword value	Description
`ARCDIR` *`dir`*	Full path to the location of the archive logs. No default. Required if `ARCFUNC COPY` is also specified. **Note:** Ignored for `LOGARCHMETH1 VENDOR`.
`ARCFUNC SAVE` `ARCFUNC COPY`	`ARCFUNC SAVE` saves archive logs to/from NetBackup. `ARCFUNC COPY` copies archive logs to/from `ARCDIR/RETDIR` directories. You must specify either `ARCFUNC SAVE` or `ARCFUNC COPY` if `OBJECTTYPE ARCHIVE` is also specified. **Note:** Ignored for `LOGARCHMETH1 VENDOR`.
`CATALOG_HOST`	The catalog name under which backup images are cataloged.

Table 3-9 Keyword value pairs for the db2.conf file *(continued)*

Keyword value	Description
For UNIX: `BKUP_IMAGE_PERM`	Lets you set the permissions on a backup image at backup time. Possible values are the following: ■ `USER` - set the permissions to 600. Only the original user who backed up the data has access to the backup images. ■ `GROUP` - set the permissions to 660. Anyone from the same group as the original user who backed up the data has access to the backup images. ■ `ANY` - set the permissions to 664. Anyone has access to the backup images. If this variable is not specified, the permissions default to 660. Does not apply to backups by the user exit program, normal file system permissions are used. If you use `LOGARCHMETH1 VENDOR`, you can use the new keyword in the `db2.conf` or specify the keyword in the `LOGARCHOPT1` parameter in the database configuration.
`CLIENT_NAME`*`client_name`*	An alternate client name. Most commonly used to specify a different source client to use for alternate restores. May also be used on multi-homed client hosts to specify a host name that is associated with a specific local network interface. This host name can be different from the host name that is used for file system backups.
`DATABASE` *`db_name`*	DB2 database name. No default. Required for all definitions except `OBJECTTYPE ALTERNATE`.
`DB2_COPY_NUMBER`	Allows the user to explicitly specify the copy number to be used to perform restores.
`DB2_MEDIA_SERVER`	Allows the user to explicitly specify the media server to be used to perform restores. The media server must have access to the copy of the image from which the restore occurs.
`DESTALIAS` *`db_name`* `DESTINST` *`inst_name`*	`DESTALIAS` specifies the database alias name of the destination database for an alternate restore. `DESTINST` specifies the instance name of the destination instance for an alternate restore. No default. Required for `OBJECTTYPE ALTERNATE`.
`ENDOPER`	Signals the end of a definition. Required at the end of each definition.

Table 3-9 Keyword value pairs for the db2.conf file *(continued)*

Keyword value	Description
`FORCE_BACKUP_CLIENT`	The local client name. The client name is needed when DB2 performs an archive backup immediately following an alternate restore from another client. This client name allows the backup to be taken using the correct client name for the local host. The `CLIENT_NAME` still references the source client that is used to select the backup images that the restore needs.
`NODE` *`number`*	Specifies the DB2 node number that must match the local node in order for the other keywords and values to be used. Do not specify this keyword unless you operate within a DB2 Enterprise Extended Edition (EEE) environment. Not required. No default.

`OBJECTTYPE ALTERNATE`
`OBJECTTYPE ARCHIVE`
`OBJECTTYPE DATABASE`
`OBJECTTYPE TABLESPACE`
	Specify `OBJECTTYPE ALTERNATE` to indicate that the definition pertains to performing a restore from an alternate instance or alternate database.
	
	Specify `OBJECTTYPE DATABASE` or `OBJECTTYPE TABLESPACE` for database container backup or restore. Specify `OBJECTTYPE ARCHIVE` for archive log backup or restore.
	
	One of `OBJECTTYPE ALTERNATE`, `OBJECTTYPE ARCHIVE`, `OBJECTTYPE DATABASE`, or `OBJECTTYPE TABLESPACE` is required in all `db2.conf` files. `OBJECTTYPE ALTERNATE` is required only if you want to perform an alternate restore.

`PARTITIONTYPE RAW`	Specifies the NetBackup search for the archive log files that are backed up from a raw partition during a restore. Not Required. For the `POLICY`, specify the name of a DB2 policy. This policy can be the same as the one that you use to back up the database. In the `SCHEDULE` line, specify an Application Backup schedule.
`POLICY` *`pol_name`*	The name of a NetBackup policy. If not specified, NetBackup uses the first policy of the correct type that is found in the configuration on the NetBackup primary server. The policy should be of type DB2 unless the definition is `OBJECTTYPE ARCHIVE` for use with the user exit program and `ARCFUNC SAVE`. In that case it should be of type MS-Windows or Standard. Does not apply to `OBJECTTYPE ALTERNATE`. Should be specified for all other definitions.

Table 3-9 Keyword value pairs for the db2.conf file *(continued)*

Keyword value	Description
RESTORE_PRIORITY	Specifies the restore priority in NetBackup.
RETDIR *dir*	Full path to the location from which the archive logs are retrieved. No default. Required if ARCFUNC COPY is also specified.
SCHEDULE *sched_name*	NetBackup schedule name in the policy. The default is the first schedule of the correct type in the policy. The schedule should be of type Application Backup unless the definition is OBJECTTYPE ARCHIVE for use with the user exit program and ARCFUNC SAVE. In that case it should be of type User Backup. Does not apply to OBJECTTYPE ALTERNATE.
SERVER	Name of the NetBackup primary server.
SRCALIAS *src_db_name* SRCINST *src_inst_name*	SRCALIAS specifies the database alias name of the source database for an alternate restore. SRCINST specifies the instance name of the source instance for an alternate restore. No defaults. Required for OBJECTTYPE ALTERNATE.

NetBackup for DB2 environment variables

The NetBackup automatic scheduler creates the environment variables in the following table when it runs a NetBackup for DB2 backup or restore script. You can use the DB2_FULL, DB2_INCR, or DB2_CINC variables within a script to specify a backup type.

Note: Only the NetBackup backup and restore scripts use the environment variables in the following table. These variables are unknown to the DB2 backup and restore commands. For example, the backup command and the restore command do not process the DB2_POLICY variable. Instead, the scripts use the POLICY name. This policy is defined in the $DB2_INSTANCE_HOME/db2.conf file (UNIX) or the *install_path*\NetBackup\dbext\db2\db2.conf file (Windows).

Table 3-10 describes the DB2 environment variables.

Table 3-10 DB2 environment variables

Environment variable	Purpose
DB2_POLICY	Name of the NetBackup for DB2 policy from which the Automatic Backup was started. This policy name is not necessarily the same policy name that is in the db2.conf file. This variable is set only if the backup is initiated from the server, either automatically by the NetBackup scheduler or manually through the administrator interface.
DB2_SERVER	Name of the NetBackup server.
DB2_CLIENT	Name of DB2 client.
DB2_SCHED	Name of the NetBackup schedule. Enabled only if the backup is initiated from the server, either automatically by the NetBackup scheduler or manually through the administrator interface.
DB2_SCHEDULED	Set to 1 if this backup is a scheduled backup type (Automatic Backup).
DB2_USER_INITIATED	Set to 1 if this backup is a user-initiated backup type (Application Backup backup).
DB2_FULL	Set to 1 for an Automatic full backup.
DB2_INCR	Set to 1 for an Automatic Differential incremental backup.
DB2_CINC	Set to 1 for an Automatic Cumulative incremental backup.
DB2_CATALOG_HOST	The catalog name under which backup images are cataloged.

DB2_PARENT_JOBID	Parent job ID of the current backup job.
	Note: DB2_PARENT_JOBID parameter must be specified as OPTIONS for every DB2 backup command in the script.
	For Windows, the command is used as follows:
	`BACKUP DATABASE %db2_name% %db2_action% LOAD %db2_nblib% %db2_sessions% OPTIONS "DB2_PARENT_JOBID = %DB2_PARENT_JOBID%"`
	For UNIX/Linux, the command is used as follows:
	`db2 BACKUP DATABASE $MY_DB2 $MY_SCHED LOAD $MY_LIB OPEN 4 SESSIONS OPTIONS "DB2_PARENT_JOBID=$DB2_PARENT_JOBID" BUFFER 1024`
	For more information about the syntax, refer to the sample DB2 backup scripts that are installed on the client.

Configuring the logon account for the NetBackup Client Service for NetBackup for DB2

Because the NetBackup Client Service is started by default under the `SYSTEM` account, you also must give special attention to database user authentication. The `SYSTEM` account does not have permission to connect to the target database if you use OS authentication instead of passwords.

If you use OS authentication, run the NetBackup Client Service under an account that has SYSADM, SYSCTRL, or SYSMAINT privileges for DB2. The account name must comply with the DB2 naming rules.

For more information on naming rules and authentication, see your DB2 documentation.

To configure the logon account for the NetBackup Client Service for NetBackup for DB2

1. In the Windows Services application, open the **NetBackup Client Service** entry.
2. On the **Log On** tab, provide the following:
   - Provide the account name that has SYSADM, SYSCTRL, or SYSMAINT privileges.
   - Type the password.
3. Stop and start the NetBackup Client Service.

About NetBackup for DB2 shell scripts

To perform a scheduled NetBackup for DB2 backup, you must create a shell script. The shell script controls the backup job on the NetBackup for DB2 client. You add this shell script to the **Backup selections** list in the NetBackup for DB2 policy on the primary server. You can also use the shell script to manually start a backup on the client.

The following describes shell scripts.

Shell scripts

Sample backup and recovery shell scripts are installed on the client with the NetBackup for DB2 agent. Modify these scripts to meet your individual requirements.

Shell scripts the user writes must conform to DB2 syntax. On UNIX, they must conform to the UNIX shell syntax.

Note: Be aware of what may happen if an automatic schedule invokes a script that a user authored. NetBackup does not provide safeguards to prevent an automatic backup schedule from running a restore or a recovery script.

See "Creating DB2 scripts manually" on page 56.

Creating DB2 scripts manually

On Windows, the NetBackup for DB2 installation software includes the following scripts:

- `db2_backup_db_offline.cmd`
- `db2_backup_db_online.cmd`
- `db2_restore_db.cmd`
- `db2_mpp_backup_offline.cmd`
- `db2_mpp_restore_db.cmd`

On UNIX, the NetBackup for DB2 installation software includes the following scripts:

- `db2_backup`
- `db2_restore`
- `db2_all_backup_mpp`
- `db2_all_restore_mpp`

After installation, the scripts reside in the following location:

On Windows: *install_path*`\NetBackup\dbext\db2\samples\`

On UNIX: `/usr/openv/netbackup/ext/db_ext/db2/scripts`

Modify these scripts for your environment. Do not store your scripts in the sample directory because they are lost if you upgrade or reinstall. Always relocate your scripts to a safe location. For clustered environments, this location must be available after a failover.

Although each script can have multiple DB2 commands operations, a separate script is required for each type of operation. For example, you need separate scripts for backups and restore.

Note: Always specify the correct script when configuring automatic backups or when starting operations through NetBackup. NetBackup for DB2 does not generate an error if a restore script is used for a backup operation or a backup script is used for a restore operation.

Modifying DB2 backup and install scripts

The following procedure describes how to modify scripts. Special configuration is required for a DB2 EEE (DPF) environment.

See "Overview of installation and configuration for a DB2 EEE (DPF) environment" on page 127.

To modify the DB2 backup and install scripts

1. Copy the example scripts to a different directory on your client in a safe location. In clustered environments, this location should be available after a failover.
2. On UNIX, set the access permissions of these scripts to 775.

   ```
   chmod 775 script_name
   ```

3. Use a text editor to open the script.
4. Follow the instructions in the script.
5. On UNIX, include an `su - user` line (`user` is the DB2 instance account) in your scripts. Otherwise, the scripts do not run with the proper permissions and environment variables.
6. Test the scripts that you created by starting a manual backup of this policy.

   See "Perform a manual backup" on page 35.

Script parameters

The NetBackup for DB2 scripts read parameters from the environment when they perform backup and restore operations.

The parameters can come from the following sources:

- Environment variables
- UNIX: NetBackup `bp.conf`
- NetBackup `db2.conf`

Parameters from these sources can be evaluated within the scripts. For example, the `DB2_POLICY` value is the name of the policy that is used to perform the backup.

See "Creating a db2.conf file for use with the user exit program" on page 42.

About NetBackup shell script storage

NetBackup stores shell scripts in the following ways:

Shell script storage	DB2 scripts must reside on the NetBackup client. Backup scripts are associated with a policy by specifying the file name (including path) in the policy file or script list. For server-directed or scheduled backups, each client in the policy's client list must have a copy of the script with the same name in the same location. See "About adding backup selections to a DB2 policy" on page 28. The backup processes and recovery processes sometimes require passwords for DB2 database access and system user accounts.
Shell script storage in a NetBackup cluster	The shell scripts pertain to NetBackup for DB2 environments that are not installed in a cluster. If you operate within a NetBackup cluster, make sure that the restore shell scripts reside in a file system that is shared between all nodes in the cluster.

See "About backup schedules and scripts" on page 29.

RBAC role for the DB2 administrator

The RBAC role named Default DB2 Administrator provides the permissions for a DB2 administrator to view and restore DB2 backups with the command `nbdb2adutl`. For details on RBAC, see the NetBackup Web UI Administrator's Guide.

Note the following limitations for this role:

- This role only provides the ability to list, query, and restore DB2 backup images and to view and manage DB2 jobs. This role cannot manage policies or the protection of DB2 assets.
- This role does not provide asset-level or granular permissions on DB2 assets.

To add users to this RBAC role, you must have the RBAC Administrator role or the permissions to add users to roles. Contact your NetBackup administrator for assistance with creating roles and adding users to roles.

For information on the RBAC permissions and default roles, see the NetBackup API documentation at http://sort.veritas.com/.

Chapter 4

Performing backups and restores of DB2

This chapter includes the following topics:

- NetBackup for DB2 backup overview
- About backups from the NetBackup primary server
- About user-directed backups
- About browsing DB2 backup images with bplist
- Performing a database restore
- About an alternate restore
- About preventing the direct expiration of backup images

NetBackup for DB2 backup overview

After you have completed installing and configuring NetBackup for DB2, you can start DB2 backups and restores through NetBackup. You can also run DB2 commands directly.

Note: Always specify the correct DB2 script when you configure automatic backups or when operations start through NetBackup. NetBackup for DB2 does not generate an error if a restore DB2 script file is used for a backup operation. Also, NetBackup for DB2 does not generate an error when a backup DB2 script is used for a restore operation.

NetBackup for DB2 provides the following ways to perform a backup:

- Issue a DB2 command from the DB2 control center or command-line processor. The DB2 `BACKUP` and `RESTORE` commands use the policies, schedules, and settings that are specified in the following sources:
  - The NetBackup for DB2 vendor I/O library.
    On UNIX, this library is named `nbdb2.ext`, where *ext* differs depending on your platform.
    On Windows, this library is named `nbdb2.dll`.
  - The NetBackup for DB2 configuration file. This file is named `db2.conf`.
- Run a script from the operating system command line. You can create these scripts manually.
- Use the scripts that are specified in policies. When you back up a NetBackup policy, it uses the scripts that are specified in the policy.
- You can specify a catalog name during a database copy backup and an archive log backup.

The main types of DB2 backups are as follows:

database backup database copy	A copy of the entire DB2 database or tablespace. This backup is accomplished by issuing a DB2 `BACKUP DATABASE` command. A database backup can be initiated through NetBackup by an automatic backup of a DB2 policy, manual backup of a DB2 policy, or user-directed backup. You can specify the `CATALOG_HOST` in the `db2.conf` or the `DB2_CATALOG_HOST` in the `VENDOROPT` of the DB2 database configuration parameters or in the `OPTIONS` on the command line. See “About backups from the NetBackup primary server” on page 61. See “About user-directed backups” on page 62.

archive log backup	An archive log backup is a backup of an archive log file for DB2. If `VENDOR` is enabled in the DB2 configuration files, NetBackup for DB2 backups up the archive logs along with the database files. If the user exit program is enabled in the DB2 configuration file, you need a separate policy and schedule to back up the archive logs. If you specify `LOGARCHMETH1` and or `LOGARCHMETH2` equal to `VENDOR`, you can specify the `CATALOG_HOST` in the `db2.conf` or specify the `DB2_CATALOG_HOST` in the `LOGARCHOPT1` and or `LOGARCHOPT2` respectively. These `CATALOG_HOST` and `DB2_CATALOG_HOST` keywords do not apply to the archive log backups that use the user exit program.
configuration file backup	A configuration file backup is a backup of the DB2 configuration files that you need to recover the database in the case of a disaster. You can use a Standard policy (UNIX) or MS-Windows policy with a User Backup schedule to back up the files. For information on which files to back up, see your IBM DB2 documentation.

About backups from the NetBackup primary server

You can back up a DB2 policy manually or automatically. To back up manually, the administrator on the primary server uses the NetBackup administrator's interface to run an Automatic backup schedule for a DB2 policy.

The most convenient way to back up a DB2 policy is to set up schedules for automatic backups. When the NetBackup scheduler invokes a schedule for an automatic backup, the DB2 scripts are run in the same order as they appear in the file lists. Also, the scripts run on all clients that are listed in the client list.

The DB2 scripts initiate the database backup.

Further information is available on how to add a new schedule or change an existing schedule for automatic backups.

See "Configure automatic backup schedules" on page 31.

The following information applies only if you use the user exit program to back up the archive logs:

- If an online backup of a partition is requested, the user exit program must be enabled. If not, an offline partition backup is attempted. An offline backup is also attempted if the database is in a backup-pending mode.

About user-directed backups

You can run a user-directed backup in the following ways:

- You can run a user-directed backup using the DB2 command-line or DB2 script.
- Using DB2

Users must have sufficient DB2 permissions to perform backup, restore, and roll-forward operations. The user account must have `SYSADM`, `SYSCTRL`, or `SYSMAINT` privileges for DB2.

See "BACKUP DATABASE command options" on page 63.

Using DB2 to run a user-directed backup

To start a user-directed backup, run the DB2 `BACKUP DATABASE` command.

You can run this command from the DB2 command line on the client (UNIX) or from the DB2 command window on the client.

Depending on the release of DB2 that you use, issue the `BACKUP DATABASE` command in one of the following formats to perform a backup.

Table 4-1 BACKUP DATABASE command formats

Format	Description
Offline backup	Issue the command in the following format: Windows: `db2 backup db sample load` *`install_path`*`\NetBackup\bin\nbdb2.dll` UNIX: `db2 backup db sample load \` `/usr/openv/netbackup/bin/`*`lib`* The specification for *lib* differs depending on your platform.

Table 4-1 BACKUP DATABASE command formats *(continued)*

Format	Description
Online backup	Issue the command in the following format: Windows: `db2 backup db sample online load install_path\NetBackup\bin\nbdb2.dll` UNIX: `db2 backup db sample online load /usr/openv/netbackup/bin/lib` For *lib*, specify the same path as shown for the preceding format (Format 1). For more information on the DB2 `BACKUP DATABASE` command, see your DB2 documentation.

BACKUP DATABASE command options

You can back up a DB2 database to NetBackup with either the DB2 `BACKUP DATABASE` command or with its alternative syntax, `BACKUP DB`.

Table 4-2 lists the command options when used in a NetBackup for DB2 environment.

Table 4-2 DB2 `BACKUP` command options

Option	Purpose
`LOAD NBDB2_library_path`	Instructs DB2 to use the NBDB2 vendor library when it performs the backup.
`OPEN number SESSIONS`	Specifies the number of concurrent data streams used for writing data. Use this option if you have multiple backup devices available, or you have multiplexing enabled in NetBackup.
`WITH number BUFFERS`	Use this option when opening multiple sessions. See `OPEN number SESSIONS`. The number of buffers must be twice the number of sessions.
`BUFFER size`	Use this option to increase or decrease the buffer size, if necessary. Increased size can benefit performance, but decreased size might be necessary if using numerous buffers. DB2 recommends that the size be a multiple of the extent size. The DB2 `DFT_EXTENT_SZ` setting defines the default extent size.

Table 4-2 DB2 `BACKUP` command options *(continued)*

Option	Purpose
`WITHOUT PROMPTING`	This option is required for unattended backups. It must be specified in the backup scripts that NetBackup runs.
`INCREMENTAL`	Use this option to perform a cumulative backup.
`INCREMENTAL DELTA`	Use this option to perform a differential backup.
`ONLINE`	Use this option to back up hot, or active, databases.
`OPTIONS "`*`options-string`*`"`	Specifies the options that are to be used for the backup operation. The string passes to the vendor support library, for example `nbdb.so`, exactly as it was entered, without the quotes. When the options DB2_POLICY, DB2_SCHED, DB2_SERVER, DB2_CLIENT, or BKUP_IMAGE_PERM are specified, the corresponding environment variables and `db2.conf` keywords are overridden. For more details about these options: See "Keywords for the db2.conf file" on page 49. See "NetBackup for DB2 environment variables" on page 53. If multiple `key=value pairs` are specified, they are colon delimited. The following example shows colon-delimited `key=value pairs`: `DB2 BACKUP ... OPTIONS "DB2_POLICY=policy3:DB2_SCHED=sched4"` **Note:** Specifying this option overrides the value that the VENDOROPT database configuration parameter specifies.
`PARALLELISM` *`n`*	Determines the number of tablespaces which can be read in parallel by the backup utility. DB2 automatically chooses an optimal value for this parameter unless you explicitly enter a value.
`DB2_CATALOG_HOST`	The catalog name under which backup images are cataloged.

About browsing DB2 backup images with bplist

You can use the `bplist` command to search DB2 backup images. The output from `bplist` differs depending on how you manage your archive log files.

Table 4-3 bplist output

bplist option	Description
`-t 18`	This example searches all DB2 backup images for a client named `camel`, which is also the primary server. The information comes from the NetBackup catalog on the primary server. The user exit program backs up the archive files. The `bplist -t 18` option specifies the DB2 backup type. The `bplist` output shows the DB2 database backup images that are stored in the NetBackup database. Windows: *install_path*\NetBackup\bin\bplist -C camel -S camel -t 18 -R / DB2:\SAMP\node0000\2009120210515\SAMP.0.DB2.node0000.0.2009120210515.1 DB2:\SAMP\node0000\2009120210473\SAMP.0.DB2.node0000.0.2009120210473.1 DB2:\SAMP\node0000\2009112915411\SAMP.3.DB2.node0000.4.2009112915411.1 UNIX: /usr/openv/netbackup/bin/bplist -C camel -S camel -t 18 -R / /DB2/SAMP/node0000/2009120210515/SAMP.0.DB2.node0000.0.2009120210515.1 /DB2/SAMP/node0000/2009120210473/SAMP.0.DB2.node0000.0.2009120210473.1 /DB2/SAMP/node0000/2009112915411/SAMP.3.DB2.node0000.4.2009112915411.1 Where: `DB2` is the directory name for all DB2 backups. `SAMP` is the name of the database (both occurrences). `node0000` is the node name. `20091202105150` is the time that the backup occurred. `0` is the type of backup taken. Zero (0) indicates a full database backup. Three (3) indicates a tablespace backup. `DB2` is the database instance name. It is one to eight characters in length. `node0000` is the node number. In non-partitioned database systems, the node number is always zero (node0000). In partitioned database systems, the number is nodexxxx, where xxxx is the number assigned to the node in the `db2nodes.cfg` file. `0` is the last archive log number. `20091202105150` is the timestamp, which includes the date (year, month, day) and time (hour, minute, second). `1` is the session number. This file extension identifies the session number that was specified on the DB2 `BACKUP` command.

Table 4-3 bplist output *(continued)*

bplist option	Description

`-k DB2_Log_Policy`	This example searches all DB2 backup images for a client named `cow`, which is also the primary server. The information comes from the NetBackup catalog on the primary server. This example assumes that the user exit program is used to back up the archive files.
	
	The `-k DB2_Log_Policy` option specifies the files that are backed up with this policy. The policy name originates from the settings in the `db2.conf` file for archive log files. The `bplist` output shows the list of DB2 archive log files that are stored in NetBackup.
	
	Windows:
	
	`install_path\NetBackup\bin\bplist -k DB2_Log_Policy -C cow -S cow -R /`
	`C:\DB2\NODE0000\SQL00001\SQLOGDIR\S0000026.LOG`
	`C:\DB2\NODE0000\SQL00001\SQLOGDIR\S0000025.LOG`
	`C:\DB2\NODE0000\SQL00001\SQLOGDIR\S0000024.LOG`
	
	UNIX:
	
	`/usr/openv/netbackup/bin/bplist -k DB2_Log_Policy -C cow -S cow -R /`
	`/home/db2inst/NODE0000/SQL00001/SQLOGDIR/S0000026.LOG`
	`/home/db2inst/NODE0000/SQL00001/SQLOGDIR/S0000025.LOG`
	`/home/db2inst/NODE0000/SQL00001/SQLOGDIR/S0000024.LOG`

`-k log_policy`	This example uses `bplist` to search the DB2 archive log files for a client named `cow`. The `-k log_policy` option specifies the files that are backed up with this policy. The `VENDOR` is set and the user exit program is not used to back up the archive logs: Windows: `install_path\NetBackup\bin\bplist -C cow -S cow -k log_policy -R /` Example location:`C:\DB2\SAMPLE\LOGFILE\node0000\db2v864d\C0000000_S0000000.LOG` UNIX: `/usr/openv/netbackup/bin/bplist -C cow -S cow -k log_policy -R /` Example location:`/DB2/SAMPLE/LOGFILE/node0000/db2v864d/C0000000_S0000000.LOG` Where: `DB2` is the directory name for all DB2 backups. `SAMPLE` is the name of the database. `LOGFILE` identifies the entry as a log file. `node0000` is the node name. `db2v864d` is the name of the DB2 instance. `C0000000_S0000000.LOG` is the name of the log file that DB2 provides.

You can find more information on the `bplist` command in the NetBackup Commands Reference Guide.

Performing a database restore

As the DB2 user on UNIX, you can initiate a database restore with the DB2 Control Center or command-line processor.

On UNIX, a NetBackup task can run a restore script containing the necessary DB2 commands to perform the restore. You can write the scripts that contain the commands to perform a restore.

See "Using DB2 to perform a restore" on page 68.

Using DB2 to perform a restore

The exact process for recovering a DB2 database differs from site to site depending on the following: the methods that are used for backing up the archive logs, the settings that are used in the NetBackup for DB2 configuration file, `db2.conf`, and the location of the archive logs.

The following procedures show how to restore an example database to the level of a recent database backup plus archive logs:

- See "Recovering a DB2 database - Simplest case" on page 70.
  Use this procedure if the archive logs are in an accessible location and they were all created with the same parameters in `db2.conf`.
- See "Recovering a DB2 database - Restoring archive logs" on page 71.
  This case is more complex. Use this procedure if you have to browse for archive logs and restore them from secondary storage.

For more information on how to recover a DB2 database, see your DB2 documentation.

Restoring and recovering a DB2 database - with a catalog name that has been specified

A catalog name can be specified for a database backup and an archive log backup. If a user specified a catalog name during a backup, there are certain setup actions you must follow during restore operations. Follow the following options for use in a Windows and UNIX environment.

If you use a non-root service user account, specific access must be allowed for that user when you add files to the `/usr/openv/netbackup/db/altnames` directory. The service user account must have full access to these files through the ownership

or group and the permissions. For example, if the service user is `svcname` and its group is `srvgrp`, the file can have permissions of `400`. If the file owner is for a different user and group, the file permissions must allow access to the service user. For example, `777`. Equivalent permission settings must be used in a Windows environment.

Windows:

- If the catalog name is equal to the name of the client performing the restore, no special setup is needed.
- If the primary and the client are the same server and if the catalog name does not equal the name of the client performing the restore, update the `db2.conf` as follows:
  - `DATABASE` and `ARCHIVE` stanzas:
    - `CLIENT <`**`catalog name`**`>`
  - `ARCHIVE` stanza only:
    - `FORCE_BACKUP_CLIENT <`**`name of the host performing the restore`**`>`
      The newer releases of the DB2 database want to perform a backup of the archive logs after a restore.
- If the client is a different server than where the backup has occurred and if the catalog name does not equal the name of the client performing the restore:
  - `db2.conf`
    - `DATABASE` and `ARCHIVE` stanzas:
      - `CLIENT <`**`catalog name`**`>`
    - `ARCHIVE` stanza only:
      - `FORCE_BACKUP_CLIENT <`**`name of the host performing the restore`**`>`
        The newer releases of the DB2 database want to perform a backup of the archive logs after a restore.
  - The `altnames` directory must be set up:
    `install_path``\netbackup\db\altnames`

UNIX:

- If the catalog name is equal to the name of the client performing the restore, no special setup is needed.
- If the catalog name does not equal the client name performing the restore, update the `db2.conf` as follows:

- `db2.conf`
  - `DATABASE` and `ARCHIVE` stanzas:
    - `CLIENT <catalog name>`
  - `ARCHIVE` stanza only:
    - `FORCE_BACKUP_CLIENT <name of the host performing the restore>`
      The newer releases of DB2 want to perform a backup of the archive logs after a restore.
- The `altnames` directory must be set up: `/usr/openv/netbackup/db/altnames`

See "NetBackup for DB2 backup overview" on page 59.

Recovering a DB2 database - Simplest case

The DB2 commands for recovering a database differ from release to release. Use these commands to restore a database if the archive logs are in a location that is known and accessible to DB2 and NetBackup. The recovery commands you use depend on the release version of the DB2 database.

For example, you can probably use the recovery commands in this section if the following are true:

- If `ARCFUNC SAVE` was in effect in the `db2.conf` file when all archive logs were backed up.
- If `ARCFUNC COPY` was in effect in the `db2.conf` file when all archive logs were backed up and the logs were not moved from the `ARCDIR` and `RETDIR` directories.
- If `VENDOR` was in effect in DB2 at the time all the archive logs were created.

When the DB2 database archive logs are accessible to DB2 and NetBackup, use the following commands:

- Windows: `db2 restore db db_name load install_path\NetBackup\bin\nbdb2.dll db2 rollforward db db_name to end of logs and stop`
  Where *db_name* is the name of the DB2 database you want to restore.
- UNIX: `db2 restore db db_name load /usr/openv/netbackup/bin/libdb2 rollforward db db_name to end of logs and stop`
  Where:

db_name	Name of the DB2 database.

lib Full path to the NBDB2 library.

See "About the NetBackup for DB2 components" on page 11.

Recovering a DB2 database - Restoring archive logs

You can use the procedure in this section if you need to restore the archive logs before you perform the roll-forward.

Use the procedure in this section to restore the archive logs manually if the following situations exist:

- If the archive logs are not in the standard locations. When this situation exists, NetBackup cannot perform a seamless restore of DB2. You may have moved one or more of the needed archive logs to secondary storage such as tape, network storage, or some other location. For example, if `ARCFUNC COPY` is in effect and the old archive logs were moved to tape, perform the procedure in this section.
- If `ARCFUNC COPY` was in effect in the `db2.conf` file at the time the archive logs were backed up and the `ARCDIR` and `RETDIR` parameters specify two different locations.
- If `PARTITIONTYPE RAW` was in effect in the `db2.conf` file for some (not all) of the archive log backups.

For more information about the DB2 commands, see your DB2 documentation.

To restore a DB2 database when the archive logs are in a non-standard location

1. Restore the database.

   Issue the DB2 `RESTORE DATABASE` command to restore the database itself. For example:

   Windows: `db2 restore db db_name load install_path\NetBackup\bin\nbdb2.dll`

   Where *db_name* is the name of the DB2 database you are to restore.

   UNIX: `db2 restore db db_name load /usr/openv/netbackup/bin/lib`

   Where:

db_name	Name of the DB2 database.
lib	Full path to the NBDB2 library. See "About the NetBackup for DB2 components" on page 11.

2. Use NetBackup to browse the archive logs.

   If a restore requires any log files that are backed up from a file system and a raw device, retrieve the logs from the file system manually.

   You can use the `bplist` command to browse the archive logs and find those missing from the restore directories.

   If `PARTITIONTYPE RAW` is specified in the `db2.conf` file, the user exit program looks for only those logs when you perform the restore. The missing logs are those that were written when `PARTITIONTYPE RAW` was not in effect.

3. Use operating system commands to copy the missing archive logs to the correct locations in your operating system. For example:

   On Windows, use your mouse to copy the files from one location to another.

   On UNIX, use the `cp` command.

   If `ARCFUNC COPY` is in effect and the `ARCDIR` and `RETDIR` parameters specify different locations, copy the logs in the `ARCDIR` directory to the `RETDIR` directory. If `ARCDIR` and `RETDIR` specify the same location, you do not have to take any action. If some of the log files have been moved to secondary storage, restore these files to the `RETDIR` directory.

4 Use NetBackup to restore the archive logs.

Use the `bprestore` command. For example:

Windows: `bprestore` *`install_path`*`\vedb2\db2\v8\db2V82d\NODE0000\SQL0001\SQLOGDIR\S00009.LOG`

UNIX: `bprestore /vedb2/db2/v8/db2V82d/NODE0000/SQL0001/SQLOGDIR/S00009.LOG`

5 Bring the database online.

When the roll-forward is initiated, DB2 sends a request to NetBackup to restore the log files it needs. DB2 then reapplies the transaction information in the archive logs since the last full backup was performed. DB2 brings back the database online.

For example, you can use the following command options if `PARTITIONTYPE RAW` was not specified when any of the log files were backed up:

```
db2 rollforward db sample to end of logs and stop
```

The `ROLLFORWARD DATABASE` command issues messages if it cannot locate all the archive log files it needs. If you receive these messages, browse and restore the missing archive log files, and issue the `ROLLFORWARD DATABASE` command again.

After the database is successfully restored, the `ROLLFORWARD DATABASE` command restores, and reapplies the transactions that are recorded in the archive log files since the last backup was performed. For example, if the backup image was created 10 days ago and restored today, the log files are used to restore any transactions that occurred after the backup.

RESTORE DATABASE command options

You can restore a DB2 database with either the DB2 `RESTORE DATABASE` command or with its alternative syntax, `RESTORE DB`. The DB2 `RESTORE DATABASE` command restores a database from NetBackup.

Table 4-4 provides reference information for the command options when used in a NetBackup for DB2 environment.

Table 4-4 DB2 `RESTORE` command options

Option	Purpose
`LOAD` *`NBDB2_Library_Path`*	Instructs DB2 to use the NBDB2 vendor library when you perform the restore.

Table 4-4 DB2 `RESTORE` command options *(continued)*

Option	Purpose
`OPEN` *`number`* `SESSIONS`	Specifies the number of concurrent data streams used for writing data. Use this option if you have multiple backup devices available or if you have multiplexing enabled in NetBackup. Typically, you should specify the same number of sessions that were used during the backup. You can use fewer sessions, but it may degrade overall restore performance. No benefit exists if you specify more sessions.
`WITH` *`number`* `BUFFERS`	Use this option when opening multiple sessions. See `OPEN` *`number`* `SESSIONS`. The number of buffers must be twice the number of sessions. If you use fewer buffers it can degrade performance or can cause the restore to fail when it reads multiplexed images.
`BUFFER` *`size`*	Use this option to increase or decrease the buffer size if necessary. Increased size can benefit performance, while decreased size may be necessary if you use numerous buffers. DB2 alters the actual size to be a multiple of the size that is used during the backup.
`WITHOUT PROMPTING`	This option is required for unattended restores, and it must be specified in the backup scripts that NetBackup runs.
`INCREMENTAL`	When you use this option, DB2 may not read the entire image from NetBackup media. Consequently, NetBackup logs an error in the activity monitor, which can safely be ignored.
`AUTOMATIC`	Use this option to restore a series of full and incremental images. An automated restore coordinates the restoration of a full backup and all associated incremental backups. A single automated restore restores a full backup, an optional cumulative incremental backup, and one or more differential incremental backups.

Table 4-4 DB2 `RESTORE` command options *(continued)*

Option	Purpose
`HISTORY FILE`	When you use this option, DB2 may not read the entire image from NetBackup media. Consequently, NetBackup logs an error in the activity monitor, which can safely be ignored.
`OPTIONS "options-string"`	Specifies the options to be used for the restore operation. The string passes to the vendor support library, for example `nbdb2.so`, exactly as it was entered, without the quotes. When the options `DB2_POLICY`, `DB2_COPY_NUMBER`, `DB2_MEDIA_SERVER`, or `DB2_RESTORE_PRIORITY` are specified, the corresponding environment variables and `db2.conf` keywords are overridden. For more details about these options: See "Keywords for the db2.conf file" on page 49. See "NetBackup for DB2 environment variables" on page 53. If multiple `key=value pairs` are specified, they are colon delimited. The following example shows colon delimited `key=value pairs`: `DB2 RESTORE ... OPTIONS "DB2_COPY_NUMBER=2:DB2_MEDIA_SERVER=server8"` Specifying this option overrides the value that is specified by the VENDOROPT database configuration parameter.
`PARALLELISM n`	Specifies the number of buffer manipulators that are to be spawned during the restore operation. DB2 automatically chooses an optimal value for this parameter unless you explicitly enter a value.

About an alternate restore

An alternate restore lets you restore a DB2 database to a different client or to a different instance. You can also change the name of the database during the restore.

Alternate restores differ from regular restores as follows:

- Use the regular restore procedures if you want to restore a database into the same instance on the same NetBackup client that hosted it previously. In this case, the database also retains its original name.

- Use alternate restore procedures if you want to restore a database to a different instance or to a different client or if you must rename the database during the restore.

  Databases within an instance must have unique names. If you restore a database into an instance that already has a database by that name, the alternate restore process overwrites the existing database.

Table 4-5 summarizes the types of restores you can perform and whether you need to use regular or alternate restore procedures.

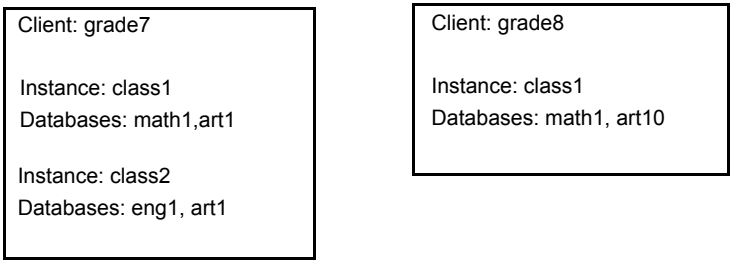
Table 4-5 Types of restores permitted

Object	Regular restore	Alternate restore	Alternate restore	Alternate restore	Alternate restore	Alternate restore	Alternate restore	Alternate restore
Database name	Same	Same	Same	Different	Same	Different	Different	Different
Instance	Same	Same	Different	Same	Different	Different	Same	Different
Client	Same	Different	Same	Same	Different	Same	Different	Different

For example, assume that you have two NetBackup clients, `grade7` and `grade8`. Instances `class1` and `class2` are on `grade7`. Instance `class1` is on `grade8`.

Figure 4-1 illustrates this example.

Figure 4-1 Alternate restore example



The following list shows some of the types of restores you can perform with alternate restore procedures:

- You can restore database `eng1` from instance `class2` on client `grade7` into instance `class1` on client `grade8`. Database `eng1` can retain its name because it is unique to instance `class1`.
- You can restore database `math1` from instance `class1` on client `grade7` into instance `class1` on client `grade8`. During the restore, you need to rename `math1`

to `math2` because `class1` on `grade8` already has a database named `math1`. Without renaming, the existing database `math1` would be overwritten.

- You can restore database `art1` from instance `class2` on client `grade7` into instance `class1` on client `grade7`. During the restore, you need to rename `art1` to `art2` because instance `class1` already has a database named `art1`. Without renaming, the existing database `art1` would be overwritten.

Preparing the primary server for an alternate restore

The examples in the following procedure assume that database `SAMPLE` was backed up by `client2`, and you want to restore `SAMPLE` to `client1`.

For more information on how to manage client restores, see the NetBackup Administrator's Guide, Volume I.

If you use a non-root service user account, specific access must be allowed for that user when you add files to the `/usr/openv/netbackup/db/altnames` directory. The service user account must have full access to these files through the ownership or group and the permissions. For example, if the service user is `svcname` and its group is `srvgrp`, the file can have permissions of `400`. If the file owner is for a different user and group, the file permissions must allow access to the service user. For example, `777`. Equivalent permission settings must be used in a Windows environment.

To prepare the NetBackup primary server for alternate restores

1. Log on to the NetBackup primary server that hosts the policy that backed up database `SAMPLE`.
2. Create a *dest_client_name* file on the NetBackup primary server.
   - Windows: *install_path*`\NetBackup\db\altnames\`*dest_client_name*
   - UNIX: `/usr/openv/netbackup/db/altnames/`*dest_client_name*

   Where *dest_client_name* is the name of a client that is allowed to be a destination client for alternate restores. For example, `client1`.
3. After creating a *dest_client_name* file, add the name of the NetBackup for DB2 source client to the *dest_client_name* file. For example, add the following line to this file:

   ```
   client2
   ```

For more information on managing a client restore, see the NetBackup Administrator's Guide, Volume I.

See "Performing the alternate restore on the clients" on page 78.

Performing the alternate restore on the clients

The following procedures explain how to restore a DB2 database and its transaction logs. The procedure builds a request to DB2 to find the backup images that correspond to the database you try to restore. Type the commands in this procedure from the client that receives the restored database.

To perform an alternate restore of a DB2 database

1. Modify the `db2.conf` file on the destination client.

   Add the following definitions:

   - One to specify the alternate restore
   - One to define the new database
   - One to define the old database
   - One to define the new log files
   - One to define the old log files

   The following example shows the definition that is needed to specify the alternate restore:

```
OBJECTTYPE ALTERNATE # Specifies an alternate restore
SRCINST db2v832d     # Names the source instance that was backed up
SRCALIAS SAMPLE      # Names the source database that was backed up
DESTINST db2v832t    # Names the destination instance name
DESTALIAS NEWSAMPL   # Names the destination database alias name
ENDOPER              # Ends the object definition
```

   The following example shows the definition that is needed to define the new database:

```
DATABASE NEWSAMPL
OBJECTTYPE DATABASE
POLICY db2-bkup
SCHEDULE Default-Application-Backup
CLIENT_NAME Client1       # Restore to (and backup from) local host
ENDOPER
```

   The following example shows the definition that is needed to define the old database:

```
DATABASE SAMPLE
OBJECTTYPE DATABASE
POLICY db2-bkup
SCHEDULE Default-Application-Backup
```

```
CLIENT_NAME Client2       # Restore from backup of remote host
ENDOPER
```

The following example shows the definition that is needed to define the new archive log files:

```
DATABASE NEWSAMPL
OBJECTTYPE ARCHIVE
POLICY db2_archive
SCHEDULE Default-Application-Backup
#SCHEDULE User            # Swap '#' on SCHEDULE for user-exit
CLIENT_NAME Client1       # Restore to (and backup from) local host
ARCFUNC SAVE
ENDOPER
```

The following example shows the definition that is needed to define the old archive log files:

```
DATABASE SAMPLE
OBJECTTYPE ARCHIVE
POLICY db2_archive
SCHEDULE Default-Application-Backup
#SCHEDULE User            # Swap '#' on SCHEDULE for user-exit
CLIENT_NAME Client2       # Restore from backup of remote host
ARCFUNC SAVE
ENDOPER
```

2 On the destination client, type the DB2 `RESTORE` command.

Type this command in the following format:

```
db2 restore db db_being_restored load lib_path into
new_db_name redirect
```

Where:

db_being_restored	Specify the name of the database that was backed up.
lib_path	Specify the full path to the NetBackup library.
new_db_name	Specify the name for the new database. If the name of the new database matches the name of a database presently included in the new instance, the new database overwrites the existing database.

For example:

Windows:

```
db2 restore db sample load install_path\NetBackup\bin\nbdb2.dll
   into newsampl redirect
```

UNIX:

```
db2 restore db sample load /usr/openv/netbackup/bin/nbdb2.sl
   into newsampl redirect
```

3 Set the location of the data files for the tablespace.

Type this command in the following format:

```
db2 set tablespace containers for 0 using "(path path)"
```

Where *path* specifies the DB2 install path.

For example, type one or more commands similar to the following:

Windows:

```
db2 set tablespace containers for 0 using "(path
DB2_install_path\db2v832t\NODE0000\SQL00001\SQLT0000.0)"
```

UNIX:

```
db2 set tablespace containers for 0 using "(path
DB2_install_path/db2v832t/NODE0000/SQL00001/SQLT0000.0)"
```

4 Restore the database.

Type the `RESTORE` command in the following format:

```
db2 restore db db_being_restored continue
```

For example:

```
db2 restore db sample continue
```

5 (Optional) Restore the transaction logs.

See "Restoring the transaction logs" on page 81.

6 Use the DB2 `ROLLFORWARD` command to restore the logs.

Type this command in the following format:

```
db2 rollforward db new_db_name to end of logs and stop
```

Restoring the transaction logs

Perform this procedure if one of the following is true:

- The archive logs did not originally reside on a raw device.
- The user exit program was used to back up the archive logs.

To restore the transaction logs

1 On the destination client, create a directory for the restored transaction log files.

For example:

Windows: `mkdir C:\db\db2_v5\home\db2inst1\NODE0000\SQL00001\SQLOGDIR`

UNIX: `mkdir /db/db2_v5/home/db2inst1/NODE0000/SQL00001/SQLOGDIR`

2 Use the `bprestore` command to restore the logs.

For example:

Windows: `bprestore install_path\db\db2_v5\home\db2inst1\NODE0000\SQL00001\SQLOGDIR\S00001.LOG`

UNIX: `bprestore /db/db2_v5/home/db2inst1/NODE0000/SQL00001/SQLOGDIR/S00001.LOG`

3. If the directory into which you restored the log files is not correct for the destination database, move the logs to the proper location.
4. Verify that the correct owner and group permissions are enabled on the log directory.

About preventing the direct expiration of backup images

Catalog maintenance operations on DB2 send requests into NetBackup to synchronize the database catalog with the NetBackup catalog. As part of the catalog synchronization, the database may initiate an image expiration (delete) request to the NetBackup catalog. These requests may also come from the DBA when command-line options are used. For compliance reasons, you may want to prevent the expiration of images in the NetBackup catalog from a database request by using a `bp.conf` entry on the primary server.

To prevent the expiration of backup images, use the following `bp.conf` entry on the primary server:

`PREVENT_DB2_DIRECT_EXPIRE`	`YES`: This setting prevents the image delete requests from the database. The delete request receives a status code of 1420 and the log message indicates that the image is on `LEGAL HOLD`. `NO`: The default setting. All image delete requests are honored from the database.

Note: The normal image expiration (retention) and the `bpexpdate` command are unaffected by this setting.

In a clustered primary server environment, these settings should be set and match in all the primary server `bp.conf` files.

The following is an example of a log entry when a status code of 1420 is produced.

The `bpdb2` log message for DB2:

```
Unable to process delete request. Image is on LEGAL HOLD
```

Chapter 5

Using Snapshot Client with NetBackup for DB2

This chapter includes the following topics:

- NetBackup for DB2 with Snapshot Client features
- About NetBackup for DB2 with Snapshot Client operations
- About configuring Snapshot Client with NetBackup for DB2
- Configuration requirements for snapshot backups with NetBackup for DB2
- Configuring a snapshot policy for NetBackup for DB2
- About configuring the db2.conf for a snapshot policy
- Restoring NetBackup for DB2 from a snapshot backup
- About configuring NetBackup for DB2 block-level incremental backups on UNIX
- About Snapshot Client effects
- Performing NetBackup for DB2 backups with Snapshot Client methods
- Performing NetBackup for DB2 restores with Snapshot Client methods

NetBackup for DB2 with Snapshot Client features

To use NetBackup for DB2 with Snapshot Client, NetBackup Snapshot Client and NetBackup for DB2 must both be licensed and installed.

The following NetBackup Snapshot Client features are available for use with NetBackup for DB2.

Table 5-1 Snapshot Client features used with NetBackup for DB2

Feature	Description
Snapshot backup	A snapshot backup occurs when NetBackup and DB2 coordinate to create a point-in-time disk image of the database for backup. This process is nearly instantaneous; so user access to the database is not interrupted during the backup. The snapshot can then be backed up to storage and or retained for instant recovery.
Instant recovery	This feature enables instant recovery of the database from a previously created snapshot. It combines snapshot technology with the ability to do rapid disk-based restores.
Off-host backup	The off-host backup shifts the burden of reading the snapshot to a separate host. The database host is only involved in performing the snapshot. The snapshot is mounted, read, and transferred to storage by an alternate client.
Block-level incremental backup	Available only on UNIX, a Block-Level Incremental (BLI) Backup uses the change tracking capabilities of the Arctera InfoScale Storage Checkpoint feature. In a BLI backup, only the changed file system blocks are backed up, not the entire file or file system. A BLI backup saves time, decreases the amount of backup media that is required, and significantly reduces CPU and network overhead during backups.
Proxy operations	A proxy backup or restore is a special type of operation where DB2 does not read or write the database files. Instead, NetBackup for DB2 acts as a proxy and performs all of the data movement. NetBackup coordinates with DB2 to ensure that the correct files are in the correct state for the operation. Snapshot, BLI backups, and Instant Recovery are examples of proxy operations. Backups and restores remain tightly integrated with DB2 and its catalog, greatly simplifying administration tasks.
File-based operations	DB2 provides the list of files that require backup or restore to NetBackup for DB2 with Snapshot Client. It then acts as a proxy to perform the data movement. Snapshot backups and user-exit log archiving are examples of file-based operations. More information is available. See “NetBackup for DB2 file-based operations” on page 88.

Table 5-1 Snapshot Client features used with NetBackup for DB2 *(continued)*

Feature	Description
Stream-based operations	Stream-based is the conventional DB2 database backup method. DB2 reads the files that require backup and provides a stream of buffers containing the contents to NetBackup for DB2. NetBackup transports the buffers to storage. At restore time, DB2 requests the return of the buffers and then writes them back onto the disk where the database resides. Database backups that do not use snapshots and vendor log archiving are examples of stream-based operations. More information is available. See "NetBackup for DB2 stream-based operations" on page 87.
`bpdb2proxy`	This NetBackup for DB2 command is used in backup and restore scripts to initiate snapshot backup and restore. **Note:** NetBackup for DB2 does not support the `USE SNAPSHOT` parameter on the `DB2 BACKUP DATABASE` command.

About NetBackup for DB2 with Snapshot Client operations

NetBackup for DB2 users can initiate snapshot operations directly from the command line using the `bpdb2proxy` command. However, it is more common to place the command into a backup or restore script and the script is then run. The script specifies the DB2 objects to be backed up or restored by the NetBackup for DB2 agent on the client. The script can either run directly on the client or can be specified as the backup selection in a DB2 policy. If a script is specified in a policy, the primary server runs the script when automatic schedules are due to run.

When the agent is started, the agent checks that the policy it uses for the backup is configured with the Snapshot Client attributes. The agent then initiates a snapshot that results in file-based backups of the DB2 files using NetBackup to perform the data movement.

The NetBackup for DB2 agent uses DB2 APIs to put the data files into a quiesced mode. NetBackup then creates a snapshot of the files. After the snapshot is created, NetBackup for DB2 uses the DB2 APIs to take the data files out of quiesced mode. The data files are in quiesced mode only for the period of time it takes to create a snapshot.

About the sequence of a NetBackup for DB2 backup operation with Snapshot Client methods

For a backup operation, the NetBackup for DB2 agent performs the following tasks in the order shown:

- Determines the list of files that make up the DB2 database.
- Suspends write activity to the data files (quiesces the database).
- Uses the Snapshot Client method to create a snapshot image of the mapped files.
- Enables DB2 write activity (unquiesces the database).
- Backs up the snapshot image of the data files.

About the sequence of a NetBackup for DB2 restore operation with Snapshot Client methods

For a restore operation, the NetBackup for DB2 agent performs the following tasks:

- Using the DB2 database and a point in time, locates the physical backup images.
- Disconnects all users from the database (brings the database offline).
- Restores the images to the original database.
- Uses DB2 APIs to take the files out of the quiesced state, which puts the database in a roll-forward pending state.
- Reruns the transactions from the log files (performs the roll-forward operation).
- Enables the user connections to the database (brings the database online).

About database objects supported by advanced backup methods

DB2 allows snapshot operations at the node level, so NetBackup can use file-based Snapshot Client backup methods to back up databases. NetBackup for DB2 cannot use Snapshot Client methods to back up individual tablespaces or container files.

Note: Before you can perform the very first snapshot backup, DB2 requires a stream-based backup of the database.

DB2 performs only conventional backups for transaction logs; use either the user-exit or `VENDOR` method. You cannot use Snapshot Client methods for transaction logs.

Snapshot backups and log archiving require different configurations. When you configure NetBackup for DB2 with Snapshot Client backups, be sure to configure the policies to allow both kinds of backups.

See "How Snapshot Client software affects backup types" on page 106.

About multistreaming and DB2 snapshot backups

To shorten the length of time to backup a snapshot of the DB2 database, the operation may perform multiple, concurrent, job streams in parallel. To configure, use the `-s` option on the `bpdb2proxy` command. When more than one stream is used, NetBackup sorts the files by size and create equal sized groups, one for each stream to process.

See "Example: multiple sessions for a DB2 snapshot backup" on page 89.

About symbolic links and DB2 backups and restores (UNIX)

NetBackup for DB2 with Snapshot Client fully supports backups and restores of the data files that consist of symbolic links and regular files. Both the symbolic link and the actual file are backed up and restored. But if you select **Retain snapshots for instant recovery**, the symbolic link must reside on the same file system as the data file. When you use instant recovery, if the symbolic link resides on a different file system than the data file it points to, the restore fails.

NetBackup for DB2 stream-based operations

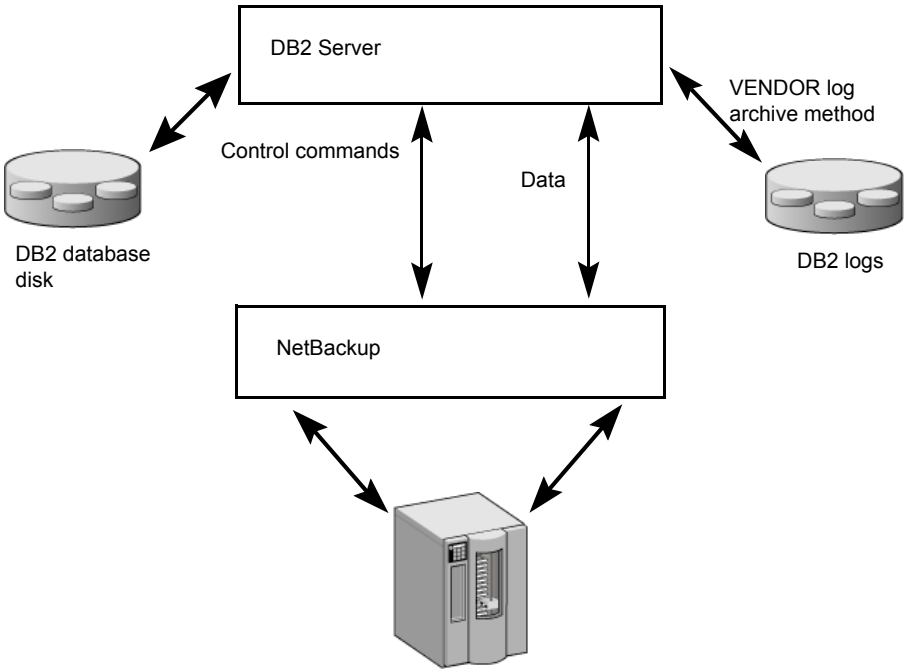
Stream-based operations are the conventional method used by DB2 and NetBackup to backup and restore the database. Log archiving using the `VENDOR` method is also stream-based.

During a stream-based backup, the DB2 server processes (for example: `db2agent`, `db2bm`, `db2med`) read the DB2 file contents into buffers. The stream of buffers is passed to NetBackup and transported to storage. At restore time, NetBackup fetches the buffers from storage and returns them to the DB2 server processes which write them back to the file system.

If the DB2 command line is configured to use multiple sessions, then there are multiple streams of buffers. Each stream of buffers is a unique application backup job and is cataloged as a unique backup image.

Figure 5-1 represents a stream-based backup or restore.

Figure 5-1 NetBackup for DB2 stream-based backup or restore



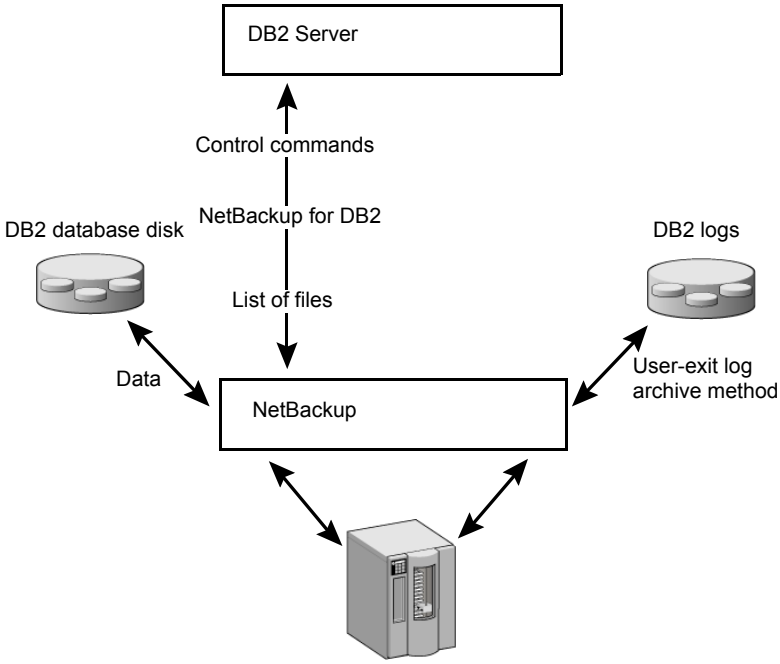
See "NetBackup for DB2 file-based operations" on page 88.

NetBackup for DB2 file-based operations

In a file-based operation, DB2 provides the list of files that require backup or restore to NetBackup for DB2. NetBackup for DB2 performs the data movement.

Figure 5-2 represents a file-based backup or restore.

Figure 5-2 NetBackup for DB2 with Snapshot Client file-based backup or restore



Example: multiple sessions for a DB2 snapshot backup

The following NetBackup for DB2 sample command initiates a snapshot backup on node 0:

```
bpdb2proxy -backup -d sample -u db2user -p password -s 3 -n 0
```

The agent groups the database files into three streams and initiates a file-based backup for each stream. After the backup is done, DB2 starts a conventional backup of the transaction logs using either the user-exit or vendor method.

Issue this command on each node of the database.

Note: If the policy used by the backup is not configured for Snapshot Client, the backup fails.

About configuring Snapshot Client with NetBackup for DB2

This topic explains how to configure snapshot and instant recovery backups for the DB2 policy. For information on how a snapshot method is automatically selected and details on the types of backup methods, see the NetBackup Snapshot Manager for Data Center Administrator's Guide.

Snapshot backups do not back up all database objects. Your backup configuration must include one or more automatic schedules to perform snapshot backups and one or more application schedules to perform stream-based backups. This configuration ensures that the entire database can be restored successfully.

For snapshot or instant recovery backups, configure the following policies and schedules as follows:

- A DB2 policy with the following attributes:
  - Snapshot methods for the file systems in which the database files reside.
  - A backup method on the policy attributes dialog box.
  - An Automatic Full Backup schedule to perform snapshot and off-host backups of the database.
  - (Conditional) For script-based policies: An Application Backup schedule to back up the transaction logs.
- DB2 does not support snapshot backups of database transaction logs. If DB2 is configured to use the user exit program, review the following topic:
  See "About backing up archive log files with the user exit program" on page 38.

Configuration requirements for snapshot backups with NetBackup for DB2

Each snapshot type has its own hardware requirements, software requirements, compatibility with certain features, and the snapshot methods that are supported. Special requirements apply for specific types of backups. See the NetBackup Hardware and Cloud Storage Compatibility List (HCL) for more information. Familiarize yourself with this information before you configure any snapshot backups.

The following list highlights some of the requirements that pertain to database agents:

- Snapshot Client backups do not back up all database objects. Your backup configuration must include schedules to perform snapshot and stream-based

backups. This configuration ensures that the entire database can be restored successfully.

- On UNIX, the user identification and group identification numbers (UIDs and GIDs) associated with the files to be backed up must be available. The UID and GID must be available to both the primary client and the alternate backup client. The UID on the primary client and the alternate backup client must be the same. Similarly, the GID on the primary client and the alternate backup client must be the same.
- Ensure that the data files reside on a volume or a file system that does not contain archive logs, control files, or executables.
- Allocate a different set of volumes or file systems to the DB2 executables versus the configuration files and transaction logs.

  One reason to have two different volumes is to separate the data files from the other files. If the logs are configured on the same volumes as the data files, the volumes the logs are temporarily frozen while NetBackup takes the snapshot. The logs and the database activity may freeze until the logs become accessible again.

  Another reason for writing the data files to their own repository is because it is required for an instant recovery point-in-time rollback. Only data files can exist on the volume that you want to restore.
- The hardware and software that is required for the appropriate snapshot method must be installed and configured correctly.
- NetBackup Snapshot Client must be installed and configured correctly, and the primary server must have a valid license for this option.
- To perform off-host backups, specify the off-host in the backup policy and ensure that host has the software and permissions to mount the snapshot.

Configuring a snapshot policy for NetBackup for DB2

The following procedure shows how to configure a snapshot policy with optional instant recovery, snapshot retention, and off-host backup.

To configure a snapshot policy

1. Open the NetBackup web UI.
2. On the left, select **Protection > Policies**.
3. Select **Add**.
4. Select the **Attributes** tab.

5. Select the **DB2** policy type.
6. Select a policy storage unit from the **Policy storage** list.

   Select a policy storage unit in this step even if you plan to select **Snapshots only** later in this procedure.
7. Click **Perform snapshot backups**.
8. (Optional) Click **Snapshot options** to choose a snapshot method.

   By default NetBackup chooses a snapshot method for you. To choose a snapshot method, click **auto** (the default) or click one of the methods that are presented in the list.

   The snapshot method that you can use depends on your hardware environment and software environment. Only certain snapshot methods are supported in certain environments. See the supported platforms matrix on the Cohesity Technical Support website for more information.

   You can configure only one snapshot method per policy. For example, assume that you want one snapshot method for clients a, b, and c, and a different method for clients d, e, and f. Then you need to create two policies for each group of clients and select one method for each policy.
9. (Optional) Select **Retain snapshots for Instant Recovery or SLP management**.

   When this option is selected, NetBackup retains the snapshot backup image on disk for later use in recovery.
10. (Optional) Select **Perform off-host backup**.

    By default, the client that hosts the database performs the backup. If you want to reduce the I/O processing load on the client that hosts the database, specify an alternate client to perform the backup.
11. (Conditional) For off-host backup method, select **Alternate client**.

    Specify the name of the client to perform the backup. This option may require additional configuration. The alternate client must be a client that shares the disk array.
12. Select the **Schedules** tab.
13. Select **Add**.
14. Configure an Automatic schedule for the database files.

15 (Conditional) In the **Instant Recovery** group, select **Snapshots only**.

This setting suppresses NetBackup's default behavior, which is to copy the snapshot to a storage unit. When you select **Snapshots only**, NetBackup creates the on-disk snapshot copy of the database, but it does not copy the snapshot to a storage unit. The on-disk snapshot becomes the only backup copy. Note that the on-disk snapshot is not considered to be a replacement for a traditional backup.

16 Configure an Application backup schedule.

NetBackup uses this storage unit for the initial stream-based backup of the database before subsequent snapshot backups are performed. It is also used for stream-based backups of the transaction logs if you use the `VENDOR` method.

17 (Conditional) For BLI backups it is permissible to create Automatic cumulative incremental and Automatic differential incremental backup schedules.

See "How BLI works with NetBackup for DB2 (UNIX)" on page 99.

18 On the **Clients** tab, specify the clients to be included in this policy.

19 On the **Backup selections** tab, specify a backup script.

More information is available about how to use scripts for a NetBackup for DB2 policy with Snapshot Client.

See "How Snapshot Client software affects scripts" on page 108.

20 Configure other attributes and add any additional schedules and backup selections.

About configuring the db2.conf for a snapshot policy

A snapshot backup requires that the `db2.conf` file be configured. The configuration is initially exactly the same as a stream-based backup because DB2 requires an initial stream-based backup before a snapshot backup can be taken. Be sure that the archive stanza is appropriate for the log archive method.

When you use the user-exit method for log archiving, configure the `db2.conf` in the following ways:

- Configuration of the `db2.conf` file for initial stream-based backup:

```
DATABASE SAMPLE
OBJECTTYPE DATABASE
POLICY DB2_DB_Policy
SCHEDULE Default-Application-Backup
```

```
ENDOPER

DATABASE SAMPLE
OBJECTTYPE ARCHIVE
POLICY DB2_Log_Policy
SCHEDULE User
ARCFUNC SAVE
#ARCFUNC COPY
#ARCDIR C:\MyLogs\arcdir\
#RETDIR C:\MyLogs\arcdir\
#ARCDIR /home/db2inst1/arcdir
#RETDIR /home/db2inst1/arcdir
ENDOPER
```

- Configuration of the `db2.conf` file for subsequent snapshot backups:
  - After the initial backup, the `db2.conf` file needs one modification to the database stanza before snapshot backups are performed. The specified schedule for the database stanza should be changed to the name of the automatic full backup schedule instead of the application backup schedule.

```
DATABASE SAMPLE
OBJECTTYPE DATABASE
POLICY DB2_DB_Policy
SCHEDULE Full
ENDOPER

DATABASE SAMPLE
OBJECTTYPE ARCHIVE
POLICY DB2_Log_Policy
SCHEDULE User
ARCFUNC SAVE
#ARCFUNC COPY
#ARCDIR C:\MyLogs\arcdir\
#RETDIR C:\MyLogs\arcdir\
#ARCDIR /home/db2inst1/arcdir
#RETDIR /home/db2inst1/arcdir
ENDOPER
```

Restoring NetBackup for DB2 from a snapshot backup

The following topics describe how to restore files, volumes, and file systems from a snapshot backup:

- See "About restoring individual files from a NetBackup for DB2 snapshot backup" on page 95.
- See "About NetBackup for DB2 restores of volumes and file systems using snapshot rollback" on page 95.
- See "Performing a NetBackup for DB2 point-in-time rollback restore from a SnapVault backup (UNIX)" on page 96.

About restoring individual files from a NetBackup for DB2 snapshot backup

Data that is backed up with Snapshot Client methods is restored in the same way as data that is backed up without Snapshot Client methods.

See "Performing a database restore" on page 68.

Use this procedure for the files that were backed up with, or without, instant recovery enabled. In all cases, DB2 determines the files that were backed up, and it initiates a corresponding restore request to the database agent.

If instant recovery is enabled,NetBackup attempts to restore the file by using the unique restore methods available with the instant recovery feature. The type of restore method thatNetBackup uses depends on your environment and the type of backup performed. IfNetBackup is unable to use any of the instant recovery methods, it restores the file in the typical manner. Data is copied from the snapshot to the primary file system. Information on the instant recovery methods that NetBackup uses is available. See the NetBackup Snapshot Manager for Data Center Administrator's Guide.

About NetBackup for DB2 restores of volumes and file systems using snapshot rollback

You can request that an entire volume or an entire file system be restored from an instant recovery Snapshot backup. This type of a restore is called a point in time rollback. All the data in the snapshot is restored; single file restore is not available in a rollback.

You can perform a snapshot rollback from an instant recovery backup that was made with the following methods:

- UNIX: VxFS_Checkpoint snapshot
- vxvm snapshot
- FlashSnap snapshots

See the NetBackup Snapshot Manager for Data Center Administrator's Guide.

The following considerations are relevant for NetBackup for DB2 restores:

- Snapshot rollback overwrites the entire volume.
- With NetBackup for DB2, snapshot rollback always performs file verification. The agent checks for the following:
  - The requested files (number and names) are identical to those in the snapshot
  - The primary volume does not contain any files that were created after the snapshot was made

  If verification fails, the rollback aborts with status 249.
- Use snapshot rollback with database files only. Database files and archive logs should exist on different file systems or volumes.

Performing a NetBackup for DB2 point-in-time rollback restore from a SnapVault backup (UNIX)

When you select a point-in-time rollback restore from a SnapVault backup, NetBackup restores the entire subvolume (qtree) to a new subvolume (qtree) on the primary host. The restore does not overwrite the existing subvolume. File verification is not performed.

The format of the new subvolume name is as follows:

`mountpointname_restore.timestamp`

For example: `subvol1_restore.2005.05.19.10h49m04s`

To perform a NetBackup for DB2 point-in-time rollback restore from a SnapVault backup (UNIX)

1. Unmount the original subvolume, which is the subvolume that the restore process did not overwrite.
2. Rename the original subvolume.
3. Rename the new subvolume with the name of the original.
4. Mount the new subvolume on the client. Use the `ALTER DATABASE RENAME DATAFILE` command to point to the restored data file on the newly created subvolume.

Performing a snapshot rollback restore from the command line

This topic describes how to perform a snapshot rollback restore with the `bpdb2proxy` command.

To specify a snapshot rollback restore from the command line

1. If the file .SQLCRT.FLG exists, delete it.

   DB2 creates the .SQLCRT.FLG file when it creates a directory (usually during tablespace creation). For volume level rollback restores this file cannot be present. The directory structure must be present at the time DB2 creates a tablespace or you must delete this file after DB2 creates the directory during tablespace creation.

2. Use the `bpdb2proxy` command in the following format:

   UNIX: `/usr/openv/netbackup/bin/bpdb2proxy -rollbkrestore -d <DBALIAS> [-u <user> -p <password>] [-s <sessions>] [-n <node number>] [-t <mm/dd/yyyy [HH:MM:SS]>] [-S <ServerName>] [-options <options string>]`

   Windows: `install_path\NetBackup\bpdb2proxy -rollbkrestore -d <DBALIAS> [-u <user> -p <password>] [-s <sessions>] [-n <node number>] [-t <mm/dd/yyyy [HH:MM:SS]>] [-S <ServerName>] [-options <options string>]`

   Where:

`-rollbkrestore`	Specifies that this restore is from a snapshot rollback.
-d *dbalias*	Database alias.
-u *user*	Username of the DB2 user.
-p *password*	Password for the DB2 user.
-s *session*	The number of sessions. Optional.
-n *node_number*	The node number. The default is 0. Optional.

-t *mm*/*dd*/*yyyy* [*HH*:*MM*:*SS*]	(Optional) The time of the backup. The values are as follows: ■ For *mm*, type the month. ■ For *dd*, type the day of the month. ■ For *yyyy*, type the year. ■ For *HH*, type the hour of the day. Optional. ■ For *MM*, type the minute of the hour. Optional. ■ For *SS*, type the second of the minute. Optional.
-S <*ServerName*>	The name of the server the restore is performed on.
-options <*options string*>	Specifies the options that are to be used for the restore operation. Currently, the only option is `DB2_RESTORE_PRIORITY`. By default, the preset priority for restore jobs is 90000, which is the highest preset job priority of any other NetBackup job. The available range is 0 - 99999. The higher the number, the greater the job priority. You must use an = sign to specify the value of the option. Example: `bpdb2proxy -options "DB2_RESTORE_PRIORITY=100"`

Troubleshooting NetBackup for DB2 rollback restores

If the rollback restore fails, it may be because the database still has a file open. Shut down and restart the database to try to correct this problem.

About configuring NetBackup for DB2 block-level incremental backups on UNIX

If only a small portion of a database changes on a daily basis, full database backups are costly in terms of time and media. The Block-Level Incremental (BLI) Backup interface extends the capabilities of NetBackup to back up only the file system blocks that contain changed data blocks.

A database BLI backup is done at the file system block level, which means only changed file blocks are backed up. Unchanged blocks within the files are not backed up. The Arctera InfoScale Storage Checkpoint facility tracks changed blocks in real time. Accordingly, a BLI backup does not need to search the entire volume for the modified blocks at backup time. BLI backup saves time, decreases the amount of

backup media that is required, and significantly reduces CPU and network overhead during backups. In addition, BLI backup allows more frequent backups, so backup images are more up to date.

BLI backup is particularly useful for any large databases that are sized in terms of hundreds of gigabytes or terabytes. Most traditional methods for database backup require that any change in the database—no matter how small—requires that the entire database is backed up. With BLI backup, only modified blocks (or file) need to be backed up.

BLI backups support the other features of NetBackup for DB2, including policy types and schedules. It also remains tightly integrated with DB2 and its catalog, which greatly simplifies administration tasks.

See "Configuring policies for BLI backups with NetBackup for DB2" on page 101.

How BLI works with NetBackup for DB2 (UNIX)

NetBackup supports BLI full backups and BLI incremental backups of DB2 databases.

BLI backup supports two types of incremental backups: differential and cumulative. Full, differential incremental, and cumulative incremental backups are specified as part of the policy schedule configuration. When a restore is performed, NetBackup restores an appropriate full backup. Then it applies the changed blocks from the incremental backups.

Restoring any of the incremental backup images requires NetBackup to restore the last full backup image and all the subsequent incremental backups. The restore process continues until the specified incremental backup image is restored. NetBackup performs this restore process automatically, and it is completely transparent. The media that stored the last full backup and the subsequent incremental backups must be available, or the restore cannot proceed.

Note that restoring a file rewrites all blocks in that file. The first subsequent differential incremental backup and or all subsequent cumulative incremental backups back up all the blocks in the restored file. After an entire database is restored, the first subsequent backup results in a full backup.

The restore destination can be a Arctera InfoScale, UFS (Solaris), JFS (AIX), or HFS (HP-UX) file system. The destination VxFS file system does not need to support the Storage Checkpoint feature to restore files. However, a Arctera InfoScale file system with the Storage Checkpoint feature is needed to perform BLI backups of the restored data.

This topic uses the following terms to describe BLI backups:

- Full Backup.

A backup in which NetBackup backs up each database file completely, not just data blocks that have changed since the last full or incremental backup.

- Cumulative BLI Backup.
  This type of backup is a backup of all the changed blocks in the database files since the last full backup. A cumulative BLI backup image contains only the data blocks of database files that changed since the last full backup. A cumulative BLI backup can reduce the number of incremental backup images that must be applied during a restore operation. This speeds up the restore process.
- Differential BLI backup.
  A backup in which NetBackup performs a backup of only those data blocks (within the database files) that changed since the last backup. The previous backup can be of type full, cumulative incremental, or differential incremental.

When NetBackup initiates BLI backups, it creates, manages, and uses the appropriate Storage Checkpoints of the filesystem(s) hosting the DB2 container files. These Storage Checkpoints identify and maintain a list of modified blocks.

About the Storage Checkpoint facility and NetBackup for DB2

The BLI backup methodology uses the Storage Checkpoint facility in Arctera InfoScale.

The Storage Checkpoint facility keeps track of the file blocks modified by the database since the last backup. NetBackup with BLI backup leverages this facility to back up only changed blocks for an incremental backup. The entire volume or file is not backed up.

Storage Checkpoint is a disk-efficient and I/O-efficient snapshot of file systems. A Storage Checkpoint provides a consistent, stable view of a file system at the instant when the file system was snapped or checkpointed. Instead of making a physically separate copy of the file system, a Storage Checkpoint tracks changed file system blocks. Disk space is saved and I/O overhead is significantly reduced.

Because the changed blocks are tracked, the Storage Checkpoint enables BLI backups. The Storage Checkpoint facility provides a consistent view of file systems, which allows BLI backup to freeze the database image during database backups.

The Storage Checkpoint operation is similar to the snapshot file system mechanism. However, the Storage Checkpoint persists after a system restart which is unlike a snapshot. Also, the Storage Checkpoint operation is totally transparent to backup administrators. The Checkpoint image is managed and available only through NetBackup or through the VxDBA utility for database backup available with the Arteca InfoScale.

For more information on Storage Checkpoints, see the Arctera InfoScale documentation.

You can take a Storage Checkpoint while the database is online or offline. To take a Storage Checkpoint while the database is online, you must enable archive logging. During the creation of the Storage Checkpoint, all tablespaces are placed in backup mode.

Configuration requirements for BLI backups with NetBackup for DB2

Before you configure BLI backups, make sure that your configuration meets the following requirements:

- NetBackup for DB2 is installed, licensed, and configured.
- NetBackup Snapshot Client is installed and configured, and the primary server must have a valid license for this option.
- Arctera InfoScale for DB2 must be installed and configured.
- Arctera InfoScale must have Storage Checkpoint licensed.

Storage Checkpoint configuration on the NetBackup for DB2 client

By default, the NetBackup for DB2 with Snapshot Client for proxy BLI backups uses the Fulldata Storage Checkpoint. When Fulldata Storage Checkpoint is in effect, the NetBackup for DB2 agent keeps the DB2 database quiesced. The database is quiesced (write suspend) only for the time that is needed to create a Storage Checkpoint.

To change the default option to use Nodata Storage Checkpoint, a user must create the following file, which can remain empty:

```
/usr/openv/netbackup/ext/db_ext/NODATA_CKPT_PROXY
```

If the agent finds this file during run time, it uses Nodata Storage Checkpoint, and it keeps the database containers in quiesced (write suspend). The database containers are kept in this mode for the duration of the backup.

Configuring policies for BLI backups with NetBackup for DB2

This topic explains how to configure BLI backups for DB2 policies. BLI backups do not back up the transaction logs. Include policies or schedules to perform file-based or stream-based backups.

Your backup configuration must ensure that the entire database can be successfully restored.

To configure a policy for BLI backups, configure the following:

- The BLI backup method on the policy attributes dialog box.

- An **Automatic backup** schedule to perform full and incremental snapshot backups of the data files. These backups automatically include the history file.
- An **Application backup** schedule to perform an initial stream-based backup of the database. Then, conditionally, perform a stream-based backup of transaction logs. Specify this schedule if you use the `VENDOR` method for backing up the transaction logs. These files are backed up with the standard NetBackup for DB2 operations.
- (Conditional) A Standard or MS-Windows policy with a User backup schedule to perform a file-based backup of transaction logs. Specify this policy and schedule if you use the user exit program to back up the transaction logs.

To configure a policy for BLI backups

1. On the left, select **Protection > Policies**.
2. Select **Add**.
3. Select the **Attributes** tab.
4. From the **Policy type** list, select **DB2**.
5. Select the **Policy storage**.
6. Select **Perform block-level incremental backups**.
7. To configure schedules, select the **Schedules** tab.

   DB2 does not support proxy backups of transaction logs.

   To perform a whole database proxy backup, configure the following:

   - One or more Automatic backup schedules to perform BLI backups of the data files.
     This backup automatically includes a backup of the history file.
   - An Application backup schedule type for the initial backup of the database and transaction log backups using the `VENDOR` method.
8. On the **Clients** tab, specify the clients to back up with this policy.
9. On the **Backup selections** tab, specify the script.

See "Configuration requirements for BLI backups with NetBackup for DB2" on page 101.

About the types of NetBackup for DB2 BLI backups

NetBackup performs BLI backups with Automatic Full Backup, Automatic Differential Incremental Backup, and Automatic Cumulative Incremental Backup schedules.

NetBackup for DB2 checks that a full backup was performed before it proceeds with an incremental backup. If the NetBackup scheduler or user initiates an

incremental backup, and NetBackup for DB2 finds no record of a full backup using the same policy, it performs a full backup.

To ensure that it has a proper set of images to restore, NetBackup performs a full backup when it encounters the following situations:

- If the number of backup streams that is specified changed from the previous backup. This change can be made through the GUI or through a DB2 command.
- If NetBackup does not have a valid full backup image for the same policy in its database. For example, this situation can occur if images were expired.

NetBackup for DB2 always initiates a full backup under these conditions, even if you want to perform an incremental backup.

BLI incremental backup options using NetBackup for DB2

DB2 BLI incremental backups can be initiated in several ways. Initiating them from the primary server is the recommended method because it requires no special configuration. Operational constraints may necessitate initiating the backups from the client host, two options are available.

Note: BLI is not currently supported for DB2 Snapshot backups on Microsoft Windows clients, the examples in this section use UNIX Bourne shell syntax. Modify as appropriate if using a different shell.

The following three options describe how to initiate DB2 BLI incremental backups. Some of these options also contain examples of a policy setup that you use and how to modify the backup script.

Server-initiated DB2 BLI incremental backups (recommended)

We recommend that you initiate BLI backups from the primary server. Initiate the BLI backups using automatic schedules and a Backup Selection that is a script. When NetBackup controls the initiation, no special configuration is needed. The policy and the schedule information are provided to the client from the primary server. The agent queries the policy and the schedule information and performs the appropriate type of checkpoint; full, cumulative incremental, or differential incremental.

Client-initiated DB2 BLI incremental backups using environment variables

If the backup is initiated from the client, then the schedule from the `db2.conf` file is used by default. To perform both the full and the incremental backups, the backup

script must be enhanced. The enhancement is to ensure the correct type of schedule and associated checkpoint is used. This enhancement can be accomplished by setting the same environment variables that the primary server sets before the backup is initiated.

- Create appropriate automatic full, automatic cumulative incremental, and automatic differential incremental schedules in the DB2 backup policy.
- Set environment variables to specify the automatic schedule to use before the agent program runs.
- Create one `db2.conf` file in the $DB2_Instance_Home directory. Update the schedule keyword in the database stanza with the name of the application backup schedule to use for any stream-based backups that might occur. The value is overridden with automatic schedule names in the following example.

The following is an example of a policy that has automatic schedules for the snapshot backups and an application schedule for the stream-based backups.

```
primary$ bpplsched DB2_Policy -L | egrep '^Schedule:|^  Type:'
Schedule:              Full
  Type:                FULL SDB2 (0)
Schedule:              Cum
  Type:                CINC (4)
Schedule:              Diff
  Type:                INCR (1)
Schedule:              Default-Application-Backup
  Type:                UBAK DB2 (2)
```

The policy only has one `db2.conf` file, and it is set for stream-based backups.

```
client$ head -4 $DB2_Instance_Home/db2.conf
DATABASE SAMPLE
OBJECTTYPE DATABASE
POLICY DB2_Policy
SCHEDULE Default-Application-Backup
```

The backup script sets and exports the appropriate environment variables before the backup is initiated.

```
DB2_INCR=0
DB2_CINC=0
DB2_FULL=0
if [ <some_condition> ]; then
  DB2_INCR=1
  DB2_SCHED="Diff"
elif [ <some_other_condition> ]; then
```

```
  DB2_CINC=1
  DB2_SCHED="Cum"
else
  DB2_FULL=1
  DB2_SCHED="Full"
fi

DB2_POLICY=DB2_Policy
DB2_SCHEDULED=1

export DB2_INCR DB2_CINC DB2_FULL DB2_SCHED DB2_POLICY DB2_SCHEDULED

/usr/openv/netbackup/bin/bpdb2proxy <options>
```

Client-initiated DB2 BLI incremental backups using multiple db2.conf files

If the backup is initiated from the client, then the schedule from the `db2.conf` file is used by default. The `db2.conf` file can specify only one policy and schedule for a specific database. To perform both the full and the incremental backups, the backup script must be enhanced. The enhancement is to ensure the correct type of schedule and associated checkpoint is used. This enhancement can be accomplished by updating the `db2.conf` file before the backup is initiated.

- Create appropriate automatic full, automatic cumulative incremental, and automatic differential incremental schedules in the DB2 backup policy.
- Create a `db2.conf` file to be used with each schedule. In each file, update the schedule keyword in the database stanza with the associated schedule name.
- Copy the appropriate `db2.conf` file into place before you run the agent program.

The following is an example of a policy that has automatic schedules for the snapshot backups and an application schedule for the stream-based backups.

```
primary$ bpplsched DB2_DB_Policy -L | egrep '^Schedule:|^  Type:'
Schedule:               Full
  Type:                 FULL SDB2 (0)
Schedule:               Cum
  Type:                 CINC (4)
Schedule:               Diff
  Type:                 INCR (1)
Schedule:               Default-Application-Backup
  Type:                 UBAK DB2 (2)
```

The policy has three `db2.conf` files, one for each type of automatic backup schedule.

```
client$ head -4 db2.conf.with_full_schedule
DATABASE SAMPLE
OBJECTTYPE DATABASE
POLICY DB2_DB_Policy
SCHEDULE Full

client$ head -4 db2.conf.with_cum_schedule
DATABASE SAMPLE
OBJECTTYPE DATABASE
POLICY DB2_DB_Policy
SCHEDULE Cum

client$ head -4 db2.conf.with_diff_schedule
DATABASE SAMPLE
OBJECTTYPE DATABASE
POLICY DB2_DB_Policy
SCHEDULE Diff
```

The backup script copies the correct `db2.conf` file into place before the backup is initiated.

```
... <setup the rest of the DB2 backup environment> ...

if [ <some_condition> ]; then
  cp db2.conf.with_diff_sched $DB2_Instance_Home/db2.conf
elif [ <some_other_condition> ]; then
  cp db2.conf.with_cum_sched $DB2_Instance_Home /db2.conf
else
  cp db2.conf.with_full_sched $DB2_Instance_Home /db2.conf
fi

/usr/openv/netbackup/bin/bpdb2proxy <options>
```

About Snapshot Client effects

The following topics describe how the Snapshot Client software affects backup types, schedule properties, and scripts.

How Snapshot Client software affects backup types

The backup types available on the **Schedules** tab of the policy play a different role for NetBackup for DB2 with Snapshot Client backups.

See Table 5-2 on page 107.

Table 5-2 Backup types for DB2 policies

Backup type	Description
Application Backup	The Application Backup schedule stores stream-based backups. The Default-Application-Backup schedule is automatically configured as an Application Backup schedule.
Full backup Differential incremental backup, Cumulative incremental backup	The automatic backup schedule types automatically start the backups by running the NetBackup for DB2 scripts. They also store the snapshot backups. **Note:** For most snapshot types, any automatic backup schedule (full, cumulative, or differential) results in a full volume snapshot. BLI is the only snapshot method that can perform an incremental backup.

See "About NetBackup for DB2 with Snapshot Client operations" on page 85.

See "How Snapshot Client software affects schedule properties" on page 107.

How Snapshot Client software affects schedule properties

Some schedule properties have a different meaning for Snapshot Client database backups than for a regular database backup. For a description of other schedule properties, see the information that is specific to standard database agent backups.

See "Schedule properties" on page 32.

Table 5-3 explains the properties for Snapshot Client backups.

Table 5-3 Schedule properties

Property	Description
Retention	Automatic Schedules: Determines how long to retain history of the backups that the primary server schedules and also how long to retain snapshot backups. Application Schedules: Determines how long to retain stream-based backups.
Multiple Copies	For snapshot backup, configure **Multiple copies** on the automatic backup schedule. For stream-based backups, configure **Multiple copies** on the Application backup schedule.

Table 5-3 Schedule properties *(continued)*

Property	Description
Frequency	Determines how often an Automatic schedule runs a backup. Does not apply to Application backup schedules.

How Snapshot Client software affects scripts

When you use a script, you must enable the advanced backup method for your clients. Configure this method on the **Attributes** tab of the policy. At run time, the agent checks the policy attributes to determine if a Snapshot Client backup method is configured and performs a proxy file-based backup.

See "About NetBackup for DB2 shell scripts" on page 55.

If you use a script, the script must reside on each client that is included in the policy. Include the NetBackup `bpdb2proxy` command in the script to perform the advanced backup method. Sample scripts are included with the installation.

See "Performing a snapshot rollback restore from the command line" on page 97.

See "Configuring a snapshot policy for NetBackup for DB2" on page 91.

Performing NetBackup for DB2 backups with Snapshot Client methods

After configuration is complete, performing NetBackup for DB2 with Snapshot Client backups and restores is similar to conventional NetBackup for DB2 operations. The following sections describe some of the differences.

NetBackup for DB2 performs backups with Snapshot Client in the following ways:

- User-directed, from the command line or the script as a DB2 user (with the `bpdb2proxy` command)
- Server-directed, from an automatic schedule on the primary server

All of these methods require a DB2 policy with Snapshot Client configuration.

User-directed backups using `bpdb2proxy`

Use the `bpdb2proxy` command to perform a Snapshot Client backup of your DB2 database from the command line. You must be the DB2 user to use the `bpdb2proxy` command. For backups, specify the `-backup` option with `bpdb2proxy`.

Use the `bpdb2proxy` command in the following format to back up a DB2 database with a Snapshot Client method:

Windows: *install_path*\NetBackup\bin\bpdb2proxy -backup -d *dbalias* -u *user* -p *password*

UNIX: /usr/openv/netbackup/bin/bpdb2proxy -backup -d *dbalias* -u *user* -p *password*

Server-directed backups

The following describes the process for configuring policies for DB2 backups with Snapshot Client.

See "Configuring a snapshot policy for NetBackup for DB2" on page 91.

These policies specify Snapshot Client backups for the DB2 database.

Performing NetBackup for DB2 restores with Snapshot Client methods

Perform NetBackup for DB2 Snapshot Client restores from the DB2 client. The following describes two methods of user-directed restores and restoring from a snapshot backup:

Restore using the command line (user-directed)

Use the `bpdb2proxy` command. You must be the DB2 user to use the `bpdb2proxy` command. When performing a restore, specify the `-restore` option with `bpdb2proxy`.

Note: The backup image you restore with `bpdb2proxy` must be from a Snapshot Client method backup. Otherwise, the restore fails.

Use the `bpdb2proxy` command in the following format to restore a DB2 database with a Snapshot Client method:

Windows: *install_path*\NetBackup\bin\bpdb2proxy -restore -d *dbalias* -u *user* -p *password*

UNIX: /usr/openv/netbackup/bin/bpdb2proxy -restore -d *dbalias* -u *user* -p *password*

Restore from a snapshot backup	See "About NetBackup for DB2 restores of volumes and file systems using snapshot rollback" on page 95.

Chapter 6

Troubleshooting NetBackup for DB2

This chapter includes the following topics:

- NetBackup debug logs and reports
- Enable the debug logs automatically (DB2 client) (Windows)
- Enabling the debug logs manually (DB2 client) (Windows)
- Enabling the debug logs manually (DB2 client) (UNIX/Linux)
- About the bphdb directory on the Windows database client
- About the bphdb directory on the UNIX database client
- About the bpdb2 directory on the UNIX database client
- Set the debug level on a DB2 client (Windows)
- Set the debug level on a DB2 client (UNIX)
- Minimize time-out failures on large database restores
- Minimize the loading and unloading of tapes for database backups
- Use the NET_BUFFER_SZ file to speed up a slow restore
- About false restore failures reported in the Activity monitor
- About the error message codes

NetBackup debug logs and reports

Debug logs

The NetBackup server and client software let you enable detailed debugging logs. The information in these log files can help you troubleshoot the problems that occur outside of either the database agent or DB2 commands.

Note the following for these logs:

- These logs do not reveal the errors that occur when DB2 commands is running unless those errors also affect NetBackup. DB2 may (or may not) write errors in the application to the NetBackup logs. Your best sources for DB2 error information are the logs provided by DB2.
- Generally, each debug log corresponds to a NetBackup process and executable.

Information about the debugging log files is available in the NetBackup Troubleshooting Guide.

Also refer to the following file:

```
UNIX: /usr/openv/netbackup/logs/README.debug file
```

Reports

NetBackup provides other reports that are useful in isolating problems. One such report is **All logs entries** on the server. For more information see the NetBackup Web UI Administrator's Guide.

Enable the debug logs automatically (DB2 client) (Windows)

You can enable debug logging by running a batch file that creates each log directory. To create all log file directories automatically, run the following:

```
install_path\NetBackup\logs\mklogdir.bat
```

Or, you can manually create the directories for the log files you want created.

Enabling the debug logs manually (DB2 client) (Windows)

To enable the debug logs manually

1. Create the following directories on the client:

- `bpubsdb2`

  For any DB2 instance browse problems when `bpdb2proxy` is used for backup or restore.

  install_path\NetBackup\logs\bpubsdb2

- `bphdb`

  For any backup that is initiated from an automated schedule on the primary server.

  install_path\NetBackup\logs\bphdb

- `bpdb2`

  For any backup or restore of the database and or `LOGARCHMETH2=VENDOR` log backups.

  install_path\NetBackup\logs\bpdb2

- `bpbkar`

  For any snapshot backup and or user-exit log backup.

  install_path\NetBackup\logs\bpbkar

- `tar`

  For any snapshot restore and or user-exit log restore.

  install_path\NetBackup\logs\tar

2 Verify the user or group that the DB2 process (process that loads `bpdb2`) has appropriate permissions to access the following directories if they exist. If the following directories do not exist, the directories are created automatically with the correct permissions.

```
install_path\NetBackup\logs\user_ops

install_path\NetBackup\logs\user_ops\dbext

install_path\NetBackup\logs\user_ops\dbext\logs
```

Also verify that the user or group that the DB2 process runs as has appropriate permissions to access the log directories in step 1.

3 On the NetBackup server or servers, create the debug log directories for the legacy processes that interact with the DB2 agent.

   On the primary server:

   `install_path\NetBackup\logs\bprd`

   On the media server or servers:

   `install_path\NetBackup\logs\bpbrm`

   `install_path\NetBackup\logs\bptm`

4 The debug logs for unified processes on the server and the client hosts are created automatically by NetBackup.

   NetBackup writes unified logs to `install_path\NetBackup\logs`.

   For information on how to use logs and reports, see the NetBackup Troubleshooting Guide.

Enabling the debug logs manually (DB2 client) (UNIX/Linux)

To enable the debug logs manually

1 Create the following directories on the client:

   - `bpubsdb2`

     For any DB2 instance browse problems when `bpdb2proxy` is used for backup or restore.

     `/usr/openv/netbackup/logs/bpubsdb2`

   - `bphdb`

     For any backup that is initiated from an automated schedule on the primary server.

     `/usr/openv/netbackup/logs/bphdb`

   - `bpdb2`

     For any backup or restore of the database and or `LOGARCHMETH2=VENDOR` log backups.

     `/usr/openv/netbackup/logs/bpdb2`

   - `bpbkar`

For any snapshot backup or user-exit log backup.

```
/usr/openv/netbackup/logs/bpbkar
```

- `nbtar`

  For any snapshot restore or user-exit log restore.

  ```
  /usr/openv/netbackup/logs/tar
  ```

2. Verify the user or group that the DB2 process (process that loads `bpdb2`) has appropriate permissions to access the following directories if they exist. If the following directories do not exist, the directories are created automatically with the correct permissions.

   ```
   /usr/openv/logs/user_ops
   ```

   ```
   /usr/openv/logs/user_ops/dbext
   ```

   ```
   /usr/openv/logs/user_ops/dbext/logs
   ```

   Also verify that the user or group that the DB2 process runs as has appropriate permissions to access the log directories in step 1.

3. On the NetBackup server or servers, create the debug log directories for the legacy processes that interact with the DB2 agent.

   On the primary server:

   ```
   /usr/openv/logs/bprd
   ```

   On the media server or servers:

   ```
   /usr/openv/logs/bpbrm
   ```

   ```
   /usr/openv/logs/bptm
   ```

4. The debug logs for unified processes on the server and the client hosts are created automatically by NetBackup.

   NetBackup writes unified logs to `/usr/openv/logs`.

   For information on how to use logs and reports, see the NetBackup Troubleshooting Guide.

About the bphdb directory on the Windows database client

The *install_path*`\NetBackup\logs\bphdb` directory contains log files.

The following types of logs exist:

- `db2_stdout.mmddyy.hhmmss.txt`

  Unless it is redirected elsewhere, NetBackup writes DB2 script output to this file.

- `db2_stderr.log.mmddyy.hhmmss.txt`

  Unless it is redirected elsewhere, NetBackup writes DB2 script errors to this file.

- `mmddyy.log`

  This log contains debugging information for the `bphdb` process. `bphdb` is the NetBackup database backup binary. It is invoked when an automatic backup schedule is run. NetBackup for DB2 uses this client process for DB2 script execution.

About the bphdb directory on the UNIX database client

The `/usr/openv/netbackup/logs/bphdb` directory contains logs.

The following types of logs exist:

- `db2_stdout.mmddyy`

  Unless it is redirected elsewhere, NetBackup writes DB2 script output to this file.

- `db2_stderr.mmddyy`

  Unless it is redirected elsewhere, NetBackup writes DB2 script errors to this file.

- `log.mmddyy`

  This log contains debugging information for the `bphdb` process. `bphdb` is the NetBackup database backup binary. It is invoked when an automatic backup schedule is run. NetBackup for DB2 uses this client process for DB2 script execution.

About the bpdb2 directory on the UNIX database client

The `/usr/openv/netbackup/logs/bpdb2` directory contains run logs.

The following run log exists:

- `log.mmddyy`

This log contains debugging information and run status for the NetBackup for DB2 client process.

Set the debug level on a DB2 client (Windows)

To control the amount of information that is written to the debug logs, change the Database debug level. Typically, the default value of 0 is sufficient. However, technical support may ask you to set the value higher to analyze a problem.

The debug logs are located in *install_path*\NetBackup\logs.

Note: Information from both the Verbose and the Database debug settings is logged to the same file, *mmddyy*.log.

To set the debug level

1. Open the **Backup, Archive, and Restore** interface.
2. Select **File > NetBackup Client Properties**.
3. Click the **Troubleshooting** tab.
4. Set the **General** debug level.
5. Set the **Verbose** debug level.

   Set this level to adjust the amount of information from the user exit program.
6. Set the **Database** debug level.

   Set this level to adjust the amount of information from the NBDB2 vendor library.
7. Click **OK** to save your changes.

Set the debug level on a DB2 client (UNIX)

To control the amount of information that is written to the debug logs, change the “Database” debug level. Typically, the default value of 0 is sufficient. However, Technical Support may ask you to set the value higher to analyze a problem.

The debug logs are located in /usr/openv/netbackup/logs.

To set the debug level

- Enter the following line in the bp.conf file.

  ```
  VERBOSE = X
  ```

  Where *X* is the debug level you want.

Minimize time-out failures on large database restores

Large database restores sometimes fail when multiple restore sessions compete for resources. In this situation, a restore session can be delayed while NetBackup waits for media or device access. If the delay is too long, the restore session times out. Use the following procedure to minimize session time-outs and to allow the restore jobs to complete successfully.

To minimize time out failures on large database restores

1. Open the NetBackup web UI.
2. On the left, select **Hosts > Host properties**.
3. Select the check box for the client.
4. If necessary, select **Connect**.
5. Select **Edit client**.
6. Select **Timeouts**.
7. Set the **Client read timeout** property to a large value.

   The default for the **Client read timeout** setting is 300 seconds (5 minutes). For database agent clients, increase the value significantly from the recommended value.

   See the NetBackup Web UI Administrator's Guide.

   For example, change this setting to 30-60 minutes to minimize time-out errors.
8. Select **Save**.

Note: This change may delay detecting problems during subsequent backups. Consider putting the original value back in place once any restore that requires a change is complete.

Minimize the loading and unloading of tapes for database backups

You can minimize excessive unloading and reloading of tapes between multistreamed database backups by changing the media settings for the primary or the media server.

See the NetBackup Administration Guide, Volume 1 for details.

To minimize loading and unloading of tapes

1. Open the NetBackup web UI.
2. On the left, click **Hosts > Host properties**.
3. Select the primary or the media server.
4. If necessary, click **Connect**.
5. Click **Edit primary server** or **Edit media server**.
6. Click **Media**.
7. Configure the following settings:
   - **Media unmount delay**
   - **Media request delay**
     Use this variable only with non-robotic drives, such as tape stackers.

Use the NET_BUFFER_SZ file to speed up a slow restore

If file restores are slow and your NetBackup primary server is a Linux machine, you can increase file restore speeds. Create a file that is called `NET_BUFFER_SZ` on the NetBackup primary server in the NetBackup install directory.

To create the NET_BUFFER_SZ file

1. Log into a Linux primary server.
2. Use `vi`(1) or another editor to create file `/usr/openv/netbackup/NET_BUFFER_SZ`.
3. Add a line that specifies the socket size, in bytes.

   For example:

   ```
   32768 bytes = 32K
   ```

4. Save and close the file.

About false restore failures reported in the Activity monitor

In some restore scenarios, DB2 reports a successful restore status, but the NetBackup activity monitor reports failures. This situation can occur during restores if DB2 reads a portion of a backup image but not the entire image.

About the error message codes

The following table describes the DB2 and NetBackup reason codes. For more information about an error message, see the log files.

Errors can occur in the NetBackup shared library (UNIX) or DLL (Windows) if these are accessed during the processing of a DB2 database utility `BACKUP` or `RESTORE`.

Table 6-1 DB2 and NetBackup error codes

Error code	Description
300	Message: ERR - No match for a database image file was found based on the following criteria. Cause: The restore criteria of database name, instance, type, and backup time object cannot be found in the NetBackup database. Action: Use `bplist` to make sure that the image you want to restore exists. Make sure that the correct instance is used. Make sure that the correct values are set in `db2.conf`. Also, on UNIX check the values in `bp.conf`. If logging is enabled, check the current log file in the following directory for more information: Windows: *`install_path`*`\NetBackup\logs\bpdb2\` UNIX: `/usr/openv/NetBackup/logs/bpdb2`
305	Message: ERR - found more than one object. Cause: Multiple DB2 backup images were found in the NetBackup database that matched the restore criteria of database name, instance, type, and backup time. Action: This error should not occur under typical operations. If logging is enabled, check the current log file in the following directory for more information: Windows: *`install_path`*`\NetBackup\logs\bpdb2\` UNIX: `/usr/openv/NetBackup/logs/bpdb2`

Table 6-1 DB2 and NetBackup error codes *(continued)*

Error code	Description
310	Message: ERR - bp.config failed with *status* status. Cause: Windows: Unable to read configuration file. UNIX: Unable to read configuration file `/usr/openv/NetBackup/bp.conf` Action: Make sure that the file exists and is properly configured. If logging is enabled, check the current log file in the following directory for more information: Windows: *install_path*`\NetBackup\logs\bpdb2\` UNIX: `/usr/openv/NetBackup/logs/bpdb2`
330	Message: ERR - Invalid options encountered for action *action*. Cause: Invalid option(s) encountered for *action*. Action: Make sure that the action parameters are used properly.
335	Message: ERR - in get DB2 UDB level. Cause: NetBackup server and the NetBackup for DB2 shared library (UNIX) DB2 DLL (Windows) or are not at the same level. Action: Make sure that the NetBackup and the NetBackup for DB2 shared library (UNIX) or the DB2 DLL (Windows) are at the same level. Check the log file in the following directory: Windows: *install_path*`\NetBackup\logs\` UNIX: `/usr/openv/NetBackup/logs/bpdb2` Check the version number of the shared library and the version number for NetBackup. If they are not the same, install the same level.
380	Message: ERR - `db2.conf` read status error *error*. Cause: `db2.conf` read status error. Action: Make sure that the directory is accessible with read and write permissions. Make sure that the file exists and has read permission.

Table 6-1 DB2 and NetBackup error codes *(continued)*

Error code	Description
385	Message: ERR - Found multiple <DATABASE> entries before an <ENDOPER> entry was encountered. Cause: Found multiple `DATABASE` entries before an `ENDOPER` entry was encountered in the following file: Windows: *`install_path`*`\NetBackup\dbext\db2.conf` UNIX: `$HOME/db2.conf` Action: Remove the extra `DATABASE` entry.
390	Message: ERR - Found multiple <OBJECTTYPE> entries before an ENDOPER entry was encountered. Cause: Found multiple `OBJECTTYPE` entries before an `ENDOPER` entry was encountered in the following file: Windows: *`install_path`*`\NetBackup\dbext\db2.conf` UNIX: `$HOME/db2.conf` Action: Remove the extra `OBJECTTYPE` entry.
395	Message: ERR - Found multiple <POLICY> entries before an <ENDOPER> entries was encountered. Cause: Found multiple `POLICY` entries before an `ENDOPER` entry was encountered in the following file: Windows: *`install_path`*`\NetBackup\dbext\db2.conf` UNIX: `$HOME/db2.conf` Action: Remove the extra `POLICY` entry.
400	Message: ERR - Found multiple <SCHEDULE> entries before an <ENDOPER> entries was encountered. Cause: Found multiple `SCHEDULE` entries before an `ENDOPER` entry was encountered in the following file: Windows: *`install_path`*`\NetBackup\dbext\db2.conf` UNIX: `$HOME/db2.conf` Action: Remove the extra `SCHEDULE` entry.

Table 6-1 DB2 and NetBackup error codes *(continued)*

Error code	Description
405	Message: ERR - Found multiple <ARCFUNC> entries before an <ENDOPER> entries was encountered. Cause: Found multiple `ARCFUNC` entries before an `ENDOPER` entry was encountered in the following file: Windows: *`install_path`*`\NetBackup\dbext\db2.conf` UNIX: `$HOME/db2.conf` Action: Remove the extra `ARCFUNC` entry.
410	Message: ERR - Found multiple <ARCDIR> entries before an <ENDOPER> entries was encountered. Cause: Found multiple `ARCDIR` entries before an `ENDOPER` entry was encountered in the following file: Windows: *`install_path`*`\NetBackup\dbext\db2.conf` UNIX: `$HOME/db2.conf` Action: Remove the extra `ARCDIR` entry.
415	Message: ERR - Found multiple <RETDIR> entries before an <ENDOPER> entries was encountered. Cause: Found multiple `RETDIR` entries before an `ENDOPER` entry was encountered in the following file: Windows: *`install_path`*`\NetBackup\dbext\db2.conf` UNIX: `$HOME/db2.conf` Action: Remove the extra `RETDIR` entry.
420	Message: ERR - need to specify a valid POLICY or SCHEDULE in `db2.conf` for <DATABASE *database*> and <OBJECTTYPE *objecttype*>. Cause: Policy name or schedule name is not specified in the `POLICY` or `SCHEDULE` entry in the following file: Windows: *`install_path`*`\NetBackup\dbext\db2.conf` UNIX: `$HOME/db2.conf` Action: Add an appropriate policy name or schedule name to the `POLICY` or `SCHEDULE` entry.

Table 6-1 DB2 and NetBackup error codes *(continued)*

Error code	Description
425	Message: ERR - need to specify a valid ARCDIR in `db2.conf`: Errno =*error_no* : *string*. Cause: Invalid `ARCDIR` is specified in `db2.conf`. Action: Add an appropriate directory name to the `ARCDIR` entry.
430	Message: ERR - ARCDIR field needs to be specified in the `db2.conf` file. Cause: No `ARCDIR` entry is found in the following file: Windows: *`install_path`*`\NetBackup\dbext\db2.conf` UNIX: `$HOME/db2.conf` Action: Add an `ARCDIR` field with an appropriate directory name to the following file:
435	Message: ERR - RETDIR field needs to contain a valid file when OBJECTTYPE is equal to ARCHIVE: *string*. Cause: `RETDIR` field does not contain a valid file. Action: `RETDIR` field must contain a valid file when `OBJECTTYPE ARCHIVE` is specified in the following file: Windows: *`install_path`*`\NetBackup\dbext\db2.conf` UNIX: `$HOME/db2.conf`
440	Message: ERR - COPY or SAVE needs to be specified for ARCFUNC when OBJECTTYPE is equal to ARCHIVE. Cause: Found `OBJECTTYPE ARCHIVE` but no `ARCFUNC` in the `db2.conf` file. Action: Specify a copy or save parameter for `ARCFUNC` if `OBJECTTYPE ARCHIVE` is also specified.
445	Message: ERR - Invalid <OBJECTTYPE> entries: *entry*. Cause: Invalid `OBJECTTYPE` entry in the following file: Windows: *`install_path`*`\NetBackup\dbext\db2.conf` UNIX: `$HOME/db2.conf` Action: Add the appropriate object type.

Table 6-1 DB2 and NetBackup error codes *(continued)*

Error code	Description
450	Message: ERR - OBJECTTYPE entry needs to be specified. Cause: `OBJECTTYPE` entry is not specified in the following file: Windows: *install_path*`\NetBackup\dbext\db2.conf` UNIX: `$HOME/db2.conf` Action: Add the appropriate object type.
455	Message: ERR - POLICY entry needs to be specified. Cause: `POLICY` entry is not specified in the following file: Windows: *install_path*`\NetBackup\dbext\db2.conf` UNIX: `$HOME/db2.conf` Action: Add the appropriate policy name.
502	Message: NetBackup DB2 Handle Invalid Cause: Internal communication between DB2 and NetBackup failed.
505	Message: The input parameters supplied by DB2 are not valid. Cause: This error can occur when you use an unsupported version of DB2.
507	Message: NetBackup Initialize Failed Cause: NetBackup encountered errors in preparing for the requested operation. This error can result from improper configuration.
510	Message: NetBackup Read Config Failed Cause: NetBackup encountered errors in reading configuration settings. Action: Check that the NetBackup client and server settings are configured. Also verify that the `db2.conf` file exists and that it is configured.
511	Message: NetBackup Write Config Failed Cause: NetBackup encountered errors in preparing for the requested operation. This error can result from improper configuration.
513	Message: NetBackup Begin Action Failed Cause: NetBackup encountered errors attempting to start the requested operation. This error can indicate a problem in obtaining necessary resources.

Table 6-1 DB2 and NetBackup error codes *(continued)*

Error code	Description
514	Message: NetBackup Create Image Failed Cause: NetBackup encountered errors attempting to create a backup image.
515	Message: NetBackup Get Image Failed Cause: NetBackup encountered errors attempting to access a backup image.
516	Message: NetBackup Find Image Failed Cause: NetBackup encountered errors attempting to locate a backup image.
518	Message: NetBackup Write Failed Cause: NetBackup encountered errors writing a backup image.
520	Message: NetBackup Read Failed Cause: NetBackup encountered errors reading a backup image.
523	Message: NetBackup Commit Data Failed Cause: NetBackup encountered errors attempting to close the backup image.
524	Message: NetBackup Commit Action Failed Cause: NetBackup encountered errors attempting to complete the requested operation.
526	Message: NetBackup Abort Action Failed Cause: NetBackup encountered errors attempting to abort the previously requested operation.
528	Message: NetBackup Delete Image Failed Cause: NetBackup encountered errors attempting to expire an incomplete backup image. This error typically indicates that the previous operation has failed, and DB2 tried to delete any incomplete images. **Note:** Database delete requests are accepted and processed. When NetBackup receives a delete image request, it searches the NetBackup catalog. If the image is found and it is not on a legal hold, the image is removed from the NetBackup catalog.

Appendix A

Configuration for a DB2 EEE (DPF) environment

This appendix includes the following topics:

- Overview of installation and configuration for a DB2 EEE (DPF) environment
- Configuring NetBackup for DB2 in an EEE environment
- Adding NetBackup policies for DB2 EEE environment
- Backing up the archive logs that are in a DB2 EEE environment
- Creating DB2 scripts for a DB2 EEE environment

Overview of installation and configuration for a DB2 EEE (DPF) environment

The IBM DB2 Enterprise Extended Edition (EEE) environment is a database that is distributed across multiple hosts or partitions. In a non-EEE environment, the database is typically centralized on a single host. The Database Partitioning Feature (DPF) is equivalent to the EEE.

All instructions that refer to an EEE environment are also applicable for a DPF environment.

In a DB2 EEE (DPF) environment, install the NetBackup client on every client using DB2.

See “Configuring NetBackup for DB2 in an EEE environment” on page 128.

See “Adding NetBackup policies for DB2 EEE environment” on page 128.

See “Backing up the archive logs that are in a DB2 EEE environment” on page 129.

See "Creating DB2 scripts for a DB2 EEE environment" on page 129.

Configuring NetBackup for DB2 in an EEE environment

The configuration process for NetBackup for DB2 in a DB2 EEE environment is the same as the configuration process in a DB2 non-EEE environment. However one exception for this configuration process is the procedure for adding a backup policy.

- Set the **Maximum jobs per client** property.
  The instructions for setting this property for DB2 EEE are the same as those for DB2.
  See "Configuring the Maximum jobs per client" on page 27.
- Add NetBackup policies for the DB2 EEE environment.
  The instructions for adding policies to NetBackup are different for DB2 EEE.
  See "Adding NetBackup policies for DB2 EEE environment" on page 128.
- Create DB2 scripts for the DB2 EEE environment.
  The instructions for creating scripts for DB2 EEE are the same as those for DB2.
  See "About NetBackup for DB2 shell scripts" on page 55.
- See "Creating DB2 scripts for a DB2 EEE environment" on page 129.
- Create a `$DB2_Instance_Home/db2.conf` file.
  The instructions for configuring the `db2.conf` files for DB2 EEE are the same as those for DB2.
  See "Configuring the run-time environment" on page 42.
- Test NetBackup for DB2 EEE configuration settings.
  The instructions for testing DB2 EEE configuration settings are the same as those for DB2.

Adding NetBackup policies for DB2 EEE environment

The following policies must be configured for a DB2 EEE environment:

- A DB2 type policy with an Application Backup schedule type.
  - Include only one Application Backup schedule type. Delete the schedule that is called Default-Application-Backup.
    For complete instructions on how to create this type of schedule, see the following:

See "Configure an application backup schedule" on page 30.

  - In the client list, include all clients you want to back up, including the DB2 catalog node.

- A DB2 policy with an Automatic backup schedule.
  - Include one of the following schedule types: Automatic full backup, Automatic differential incremental backup, or Automatic cumulative incremental backup. This policy should contain only one automatic backup schedule type.

    For complete instructions on how to create this type of schedule, see the following:

    See "Configure automatic backup schedules" on page 31.
  - Do not specify the automatic backup schedule name in the `$DB2_Instance_Home/db2.conf file`. For a proxy backup, do include the automatic backup schedule name.
  - Include only the clients that contain the DB2 catalog node and that run a DB2 script. The script uses the IBM `db2_all` command to archive the DB2 catalog nodes before any other node is backed up.
- Create a Standard type policy with a User Backup type schedule if the following apply:
  - The user exit program for logging is turned on in DB2 UDB.
  - The client is a UNIX machine.

  See "About backing up archive log files with the user exit program" on page 38.
- If you use the VENDOR method, see the following:

  See "Creating a db2.conf file (vendor method)" on page 46.

Backing up the archive logs that are in a DB2 EEE environment

The policy you use to back up the archive logs depends on the method you use for log archiving. If you use the user exit program, create a **Standard** policy. If you use the VENDOR method, you can use the DB2 Application Backup schedule.

Creating DB2 scripts for a DB2 EEE environment

Scripts operate on a single NetBackup client. If your EEE/DPF environment spans multiple computers, create at least one script for each computer.

For example, assume your database spans two hosts, and the host `H1` contains partition `P1`, and the host `H2` contains partitions `P2` and `P3`.

You need at least two scripts, as follows:

- One script for partition `P1` on host `H1`
- One script for partitions `P2` and `P3` on host `H2`.

Note: The successful backup and restore of the catalog partition is the user's responsibility. Generally, it is recommended that the catalog partition is the first node backed up and the first partition restored. For more information, see your DB2 documentation.

Roll-forward recovery to a point-in-time (PIT) is not supported. DB2 requires that PIT recovery runs the same operation for all partitions and tablespaces on all computers.

Appendix B

Using NetBackup for DB2 with SAP®

This appendix includes the following topics:

- About NetBackup for DB2 with SAP
- Installation of the DB2 user exit program
- Backup and restore of DB2 databases used by SAP
- Archive and restore of DB2 log files used by SAP
- Backup of SAP files

About NetBackup for DB2 with SAP

When SAP software uses a DB2 database, NetBackup for DB2 can be used within that environment for backup and restore of SAP data. Follow the recommended installation, backup, and restore guidelines to ensure that SAP, DB2, and NetBackup work together.

Installation of the DB2 user exit program

DB2 allows for the presence of a single user exit program to manage archiving of database log files. Both SAP and NetBackup deliver user exit programs for exclusive use by DB2. The user exit program resides in the DB2 database directory as `db2uext2`.

The use of the NetBackup user exit program is required because it automatically archives log files to a storage unit. It also enables on-demand recovery of log files by DB2.

Take precautions when installing SAP to prevent overwriting the NetBackup user exit program. Always preserve the NetBackup `db2uext2` file before installing SAP and restore afterwards.

Backup and restore of DB2 databases used by SAP

Follow the standard NetBackup instructions in this document for backup and restore of the DB2 databases that SAP uses. You can use either DB2 or NetBackup to initiate database backups and restores.

Note: Do not use `SAP CCMS`, `sapdba`, `brbackup`, or `brrestore` commands to initiate backups or restores. They do not invoke NetBackup.

Note: SAP must not be running when you attempt to restore the database.

Archive and restore of DB2 log files used by SAP

Follow the standard NetBackup instructions in this document for configuring the user exit program. DB2 automatically invokes the user exit program to archive and recover the necessary log files.

Note: Do not use `SAP CCMS`, `sapdba`, `brarchive` commands, or the SAP Logfile Management window in the DB2 Control Center for log file archival. They depend on the SAP user exit program for proper operation.

Backup of SAP files

Be certain to include any and all SAP files when planning for SAP recovery, not only the DB2 database. For instance, if you use standard NetBackup file backup procedures you can backup any regular files that SAP uses.

For file backup instructions, see the NetBackup Backup, Archive, and Restore help.

Appendix C

Register authorized locations

This appendix includes the following topics:

- Registering authorized locations used by a NetBackup database script-based policy

Registering authorized locations used by a NetBackup database script-based policy

During a backup, NetBackup checks for scripts in the default script location and any authorized locations. The default, authorized script location for UNIX is `usr/openv/netbackup/ext/db_ext` and for Windows is *`install_path`*`\netbackup\dbext`. If the script is not in the default script location or an authorized location, the policy job fails. You can move any script into the default script location or any additional authorized location and NetBackup recognizes the scripts. You need to update the policy with the script location if it has changed. An authorized location can be a directory and NetBackup recognizes any script within that directory. An authorized location can also be a full path to a script if an entire directory does need to be authorized.

If the default script location does not work for your environment, use the following procedure to enter one or more authorized locations for your scripts. Use `nbsetconfig` to enter an authorized location where the scripts reside. You can also use `bpsetconfig`, however this command is only available on the primary or the media server.

Note: One recommendation is that scripts should not be world-writable. NetBackup does not allow scripts to run from network or remote locations. All scripts must be stored and run locally. Any script that is created and saved in the NetBackup `db_ext` (UNIX) or `dbext` (Windows) location needs to be protected during a NetBackup uninstall.

For more information about registering authorized locations and scripts, review the knowledge base article:

https://support.cohesity.com/s/article/article-100039639

To add an authorized location

1. Open a command prompt on the client.
2. Use `nbsetconfig` to enter values for an authorized location. The client privileged user must run these commands.

   The following examples are for paths you may configure for the Oracle agent. Use the path that is appropriate for your agent.

   - On UNIX:

     ```
     [root@client26 bin]# ./nbsetconfig
     nbsetconfig>DB_SCRIPT_PATH = /Oracle/scripts
     nbsetconfig>DB_SCRIPT_PATH = /db/Oracle/scripts/full_backup.sh
     nbsetconfig>
     <ctrl-D>
     ```

   - On Windows:

     ```
     C:\Program Files\Cohesity NetBackup\NetBackup\bin>nbsetconfig
     nbsetconfig> DB_SCRIPT_PATH=c:\db_scripts
     nbsetconfig> DB_SCRIPT_PATH=e:\oracle\fullbackup\full_rman.sh
     nbsetconfig>
     <ctrl-Z>
     ```

Note: Review the NetBackup Command Reference Guide for options, such as reading from a text file and remotely setting clients from a NetBackup server using `bpsetconfig`. If you have a text file with the script location or authorized locations listed, `nbsetconfig` or `bpsetconfig` can read from that text file. An entry of `DB_SCRIPT_PATH=none` does not allow any script to run on a client. The `none` entry is useful if an administrator wants to completely lock down a server from running scripts.

3 (Conditional) Perform these steps on any clustered database or agent node that can perform the backup.

4 (Conditional) Update any policy if the script location was changed to the default or authorized location.