Configuring Recovery Manager

Item: 1 (Ref:1Z0-043.3.2.1)

You are maintaining your database in Oracle10*g*. You are not using the recovery catalog to maintain the backup information of your database.

Which file can be used as a repository to store information regarding the RMAN backup?

- online redo log files
- alert log files
- control file
- datafiles associated with the SYSTEM tablespace

Answer:

control file

Explanation:

The control file of the target database can be used as a repository for storing information regarding the RMAN backups. If you use RMAN without the recovery catalog, you are storing most of the necessary information about each target database's control file. In this case, the target database's control file is the repository. The CONTROL_FILE_RECORD_KEEP_TIME initialization parameter determines the duration for which the information that can be used by RMAN is kept in the control file. The default value for the CONTROL_FILE_RECORD_KEEP_TIME parameter can range from 7 days to 365 days.

The option stating that the online redo log files can be used as a repository to store information regarding the RMAN backup is incorrect. The online redo log files contain redo log entries. The redo log entries include every change made to the database.

The option stating that the alert log file can be used as the repository to store information regarding the RMAN backup is incorrect. The alert log file contains information regarding any change made to the database structure. While working on the database, if any problem occurs regarding database processing, the alert log file is examined to determine the cause of the problem.

The option stating that the datafiles associated with the SYSTEM tablespace can be used to store information regarding the RMAN backup is incorrect. No datafile can be used as repository to store information about the RMAN backup. The datafiles are used to store the actual data in the database.

Item: 2 (Ref:1Z0-043.3.2.5)

You are maintaining your database in Oracle10*g*. You want to store the information about the backup of the database in the control file. You issue the following statement:

```
SQL>ALTER SYSTEM SET CONTROL_FILE_RECORD_KEEP_TIME=400;
```

What is the outcome of this statement?

- The statement will not execute successfully.
- The statement will execute successfully, and the backups metadata will be maintained in the control file for 400 days
- The statement will execute successfully, and the backups metadata will be maintained in the recovery catalog for 400 days.
- Backups will be deleted from the media after 400 days.

Answer:

The statement will not execute successfully.

Explanation:

In the given scenario, the statement will not execute successfully because 400 days is an invalid value for the `CONTROL_FILE_RECORD_KEEP_TIME` parameter. The `CONTROL_FILE_RECORD_KEEP_TIME` initialization parameter is used to specify the minimum duration for which information about a backup that can be used by `RMAN` will be stored in the control file of the target database. The default vale for this parameter is 7 days. The valid range for this parameter is 0 to 365 days.

The options stating that the statement will execute successfully, and the backup metadata will be maintained in the control file for 400 days is incorrect. The option stating that the statement will be executed, and the backup metadata will be maintained in the recovery catalog for 400 days is also incorrect. This is because the statement will not execute successfully.

The option stating that after 400 days, the backups will be deleted from the media is incorrect. The `CONTROL_FILE_RECORD_KEEP_TIME` initialization parameter is used to specify the duration for which backup metadata is stored in the control file. The `CONTROL_FILE_RECORD_KEEP_TIME` parameter does not force the backups to be deleted for the media.

Item: 3 (Ref:1Z0-043.3.2.8)

You have issued the following command:

```
RMAN>CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 100 DAYS;
```

What will be the result of using the above command?

- The backup metadata will be maintained in the control file for 100 days.
- The backup metadata will be maintained in the recovery catalog for 100 days.
- The backup metadata will be maintained in the flash recovery area for 100 days.
- After 100 days, the backup sets and image copies will be deleted from the media.

Answer:

The backup metadata will be maintained in the recovery catalog for 100 days.

Explanation:

The `CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 100 DAYS;` command specifies that the metadata of the backup sets and image copies are maintained in the recovery catalog for 100 days. The retention policy configured using the command is used to determine the length of time for which a backup is retained in the recovery catalog.

The option stating that the backup metadata will be maintained in the control file for 100 days by using the `CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 100 DAYS;` command is incorrect. This is because the `CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF n DAYS;` setting is used to specify the number of days for which the backup sets and the image copies will be maintained in the recovery catalog. If you use RMAN without the recovery catalog, the information about the target database will be stored in the control file of the target database. In this scenario, the control file of the target database is the repository. The `CONTROL_FILE_RECORD_KEEP_TIME` initialization parameter is used to specify the duration for which the information that can be used by the `RMAN` is stored in the control file. The default value for the initialization parameter is 7 days and the maximum limit you can specify is 365 days.

The option stating that the backup metadata will be maintained in the flash recovery area for 100 days by using the `CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 100 DAYS;` command is incorrect. The `CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 100 DAYS;` command is used to ensure that the metadata of the backup sets and image copies is maintained in the recovery catalog.

The option stating that the backup sets and image copies will be deleted from the media after 100 days is incorrect. After 100 days, the backup sets and image copies will be marked as obsolete instead of being automatically deleted from the media. After that, you have to delete backup sets and image copies by using the `DELETE OBSOLETE` command.

Item: 4 (Ref:1Z0-043.3.3.1)

You are performing a backup of your database across the network. While taking the backup, you want to save space on the storage media and reduce the network bandwidth.

Which command will you issue to configure the required type of backup?

- `CONFIGURE DEVICE TYPE TO sbt BACKUP TYPE TO BACKUPSET;`
- `CONFIGURE DEVICE TYPE TO disk BACKUP TYPE TO COPY;`
- `CONFIGURE DEVICE TYPE TO sbt BACKUP TYPE TO COMPRESSED BACKUPSET;`
- `CONFIGURE DEVICE TYPE TO sbt BACKUP TYPE TO COMPRESSED COPY;`

Answer:

`CONFIGURE DEVICE TYPE TO sbt BACKUP TYPE TO COMPRESSED BACKUPSET;`

Explanation:

In this scenario, the required backup type is compressed backup set. You should issue the `CONFIGURE DEVICE TYPE TO sbt BACKUP TYPE TO COMPRESSED BACKUPSET;` command to configure the required backup type. In earlier versions of Oracle, only used blocks were backed up and the unused blocks were skipped to reduce the sizes of the backups. This method reduced the backup sizes of only those datafiles that had substantial free space. In Oracle 10*g*, you can compress the backups regardless of the contents of the datafiles. You can perform compressed backup on databases, tablespaces, and datafiles. The compressed backups work only with backup sets and not with image copies. The compressed backup sets save storage space and reduce the network bandwidth if you are performing backups across a network.

The option stating that you will issue the `CONFIGURE DEVICE TYPE TO sbt BACKUP TYPE TO BACKUPSET;` command to configure the required backup type is incorrect. This is because the `CONFIGURE DEVICE TYPE TO sbt BACKUP TYPE TO BACKUPSET;` command is used to configure the backup type as a backup set. The backup set created neither saves storage space nor reduces network bandwidth. The required backup type is compressed backup set.

The option stating that you will issue the `CONFIGURE DEVICE TYPE TO disk BACKUP TYPE TO COPY;` command to configure the required backup type is incorrect. This is because the `CONFIGURE DEVICE TYPE TO disk BACKUP TYPE TO COPY;` command is used to configure the backup type as an image copy. The image copy is neither used to save storage space nor reduce network bandwidth. The image copy is a copy of the datafile or control files. The required backup type is compressed backup set.

The option stating that you will issue the `CONFIGURE DEVICE TYPE TO sbt BACKUP TYPE TO COMPRESSED COPY;` command to configure the required backup type is incorrect. The `CONFIGURE DEVICE TYPE TO sbt BACKUP TYPE TO COMPRESSED COPY;` command is an invalid command. The compressed backup works only with backup sets and not with image copies.

Item: 5 (Ref:1Z0-043.3.2.6)

You are maintaining the SALES database of a company. You have never backed up the USERS tablespace that is currently offline.

On Sunday, you issued the following commands:

```
CONFIGURE DEFAULT DEVICE TYPE TO sbt;
CONFIGURE BACKUP OPTIMIZATION ON;
CONFIGURE RETENTION POLICY TO REDUNDANCY 3;
```

From Monday to Saturday, you performed the following actions:

Day	Action
Monday	BACKUP DATABASE
Tuesday	BACKUP DATABASE
Wednesday	BACKUP DATABASE
Thursday	BACKUP DATABASE
Friday	BACKUP DATABASE
Saturday	BACKUP DATABASE

How many times will the backup of the USERS tablespace be performed?

- The backup will not be performed at all.
- three times
- four times
- six times

Answer:

four times

Explanation:

The backup of the USERS tablespace will be performed four times. If backup optimization is enabled and the redundancy-based retention policy is configured by using the `CONFIGURE RETENTION POLICY TO REDUNDANCY n` command, then RMAN skips the backup of the offline or read-only datafiles when there are already n+1 backups of these offline or read-only datafiles. Backup optimization is an RMAN feature that is used to specify that the BACKUP command skips the backup of the datafiles that have not changed since the last backup. In this scenario, the USERS tablespace is an offline tablespace and the datafiles associated with the USERS tablespace are not changed after the last backup. In addition, the `CONFIGURE RETENTION POLICY TO REDUNDANCY 3;` command sets the redundancy to 3. Therefore, the backup of the offline tablespace USERS will be taken four times, that is, on Monday, Tuesday, Wednesday, and Thursday.

The other options are incorrect because the backup of the offline USERS tablespace is four according to the backup optimization and redundancy-based retention policy setting.

Item: 6 (Ref:1Z0-043.3.3.4)

You issued the RMAN>SHOW ALL; command. The output of the command is as follows:

```
CONFIGURE RETENTION TO REDUNDANCY 1; # default
CONFIGURE BACKUP OPTIMIZATION OFF; # default
CONFIGURE DEFAULT DEVICE TYPE TO DISK BACKUP AS COPY;
CONFIGURE CONTROLFILE AUTOBACKUP OFF;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '%F';
#default
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE DISK TO 1; #default
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT
'oracle/flash_recovery_area/ora101c/rec_area_%s_%p.bak';
CONFIGURE MAXSETSIZE TO UNLIMITED; # default
CONFIGURE ARCHIVELOG DELETION POLICY TO NONE; #default
CONFIGURE SNAPSHOT CONTROLFILE NAME TO
'C:\ORACLE\PRODUCT\10.1.0\DB_1\DATABASE\SNCFOR101C.ORA'; # default
```

After analyzing this output, what conclusion can you draw? (Choose two.)

- [ ] If you perform a backup across a network, then the backup will reduce the bandwidth.
- [ ] If you perform a backup of a datafile, then the backup will be the same as the operating system copy of the datafile.
- [ ] If you perform a backup of a single datafile, then the control file will not be backed up.
- [ ] The maximum size of each backup set is 10MB.
- [ ] The backups will be performed on the disk.

Answer:

The maximum size of each backup set is 10MB.
The backups will be performed on the disk.

Explanation:

In this scenario, the CONFIGURE MAXSETSIZE TO 10MB setting specifies that the maximum size of each backup set is 10MB. The CONFIGURE DEFAULT DEVICE TYPE TO DISK BACKUP AS BACKUPSET setting also specifies that the backups will be performed on the disk.

The MAXSETSIZE parameter is used to configure the maximum size of each backup set. This parameter limits the number of datafiles within a backup set. For example, there are two datafiles associated with a tablespace. The size of the first datafile is 12MB, and the size of the second datafile is 10MB. The value of the MAXSETSIZE parameter is 15MB. While performing a backup of the tablespace, RMAN will create two backup sets, one for each datafile.

The CONFIGURE DEFAULT DEVICE TYPE TO DISK BACKUP AS BACKUPSET setting specifies that the backup type to be performed is a backup set and the backup is performed on a disk.

The option stating that if you perform a backup across a network, then the backup will reduce the bandwidth is incorrect. This is because reducing the network bandwidth while performing the backup is the feature of the compressed backup. In this scenario, the CONFIGURE DEVICE TYPE DISK BACKUP TYPE TO BACKUPSET; setting indicates that the default backup type is backup set. The CONFIGURE DEVICE TYPE DISK BACKUP TYPE TO COMPRESSED BACKUPSET; command is used to configure compressed backup set as the default backup type. A compressed backup set saves storage space on the storage media. Compressed backup sets save storage space; therefore, the size of compressed backup sets is smaller than that of image copies or backup sets. A compressed backup set reduces network bandwidth if you are performing backups across a network.

The option stating that if you perform a backup of a datafile, then the backup will be the same as the operating system copy of the datafile is incorrect. The default backup type is configured as a backup set. The backup set is not the same as the operating system copy. Image copy is the same as the operating system copy. Image copies are actual copies of the database files, archive logs, or control files. The image copies can be stored only on disk. An image copy in RMAN is equivalent to an operating system copy.

The option stating that if you perform a backup of a single datafile, then the control file will not be backed up is incorrect. This is

because the `CONFIGURE CONTROLFILE AUTOBACKUP ON` command is used to configure `RMAN` to back up the control file whenever a backup of the database, tablespace, or datafile is performed.

Item: 7 (Ref:1Z0-043.3.3.3)

You issued the RMAN> SHOW ALL; command. The output of this command is as follows:

```
CONFIGURE RETENTION TO REDUNDANCY 1; # default
CONFIGURE BACKUP OPTIMIZATION OFF; # default
CONFIGURE DEFAULT DEVICE TYPE TO DISK BACKUP AS COPY;
CONFIGURE CONTROLFILE AUTOBACKUP OFF;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '%F';
#default
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE DISK TO 1; #default
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT
'oracle/flash_recovery_area/ora101c/rec_area_%s_%p.bak';
CONFIGURE MAXSETSIZE TO UNLIMITED; # default
CONFIGURE ARCHIVELOG DELETION POLICY TO NONE; #default
CONFIGURE SNAPSHOT CONTROLFILE NAME TO
'C:\ORACLE\PRODUCT\10.1.0\DB_1\DATABASE\SNCFOR101C.ORA'; # default
```

After analyzing the output, which conclusion will you draw?

- The backups consist of backup pieces.
- The datafiles can be multiplexed within the backup.
- The backups can be stored only on the disk.
- While performing the backup across a network, the network bandwidth is reduced.

Answer:

The backups can be stored only on the disk.

Explanation:

The CONFIGURE DEFAULT DEVICE TYPE TO DISK BACKUP AS COPY setting specifies that the backup type of the backups is an image copy and the backups will be stored on the disk. The image copies are actual copies of the database files, archive logs, or control files. The image copies can be stored only on disk. An image copy in RMAN is equivalent to an operating system copy. Image copies can be created and restored by using RMAN or operating system commands for copying files. If you create image copies by using RMAN, then the image copies are recorded in the repository and are available for recovering a database. If you are using the operating system command for creating image copies, then you must use the CATALOG command at the RMAN prompt to record the image copy in the RMAN repository.

The option stating that the backups that are to be performed on disk consist of backup pieces is incorrect. This is because the image copies do not contain backup pieces. A backup set consists of backup pieces. The image copies are actual copies of datafiles, control files, and archive logs.

The option stating that the datafiles can be multiplexed within the backup is incorrect. This is because the CONFIGURE DEFAULT DEVICE TYPE TO DISK BACKUP AS COPY setting specifies that the backup type is image copy. Datafiles cannot be multiplexed in an image copy. The datafiles can be multiplexed only within backup sets. Multiplexing the datafiles occurs in a backup set when multiple files are read and each file's blocks are written to the same backup set.

The option stating that the network bandwidth is reduced while performing backups across a network is incorrect. This is because reducing the network bandwidth while taking the backup across a network is not a feature of the backup set. This is a function of the compressed backup set. In this scenario, the CONFIGURE DEFAULT DEVICE TYPE TO DISK BACKUP AS COPY setting specifies that the backup type of the backups is an image copy and the backups will be stored on the disk. The CONFIGURE DEVICE TYPE DISK BACKUP TYPE TO COMPRESSED BACKUPSET; command is used to configure a compressed backup set as the default backup type. In earlier versions of Oracle, to reduce the sizes of the backups, only used blocks were backed up and the unused blocks were skipped. This method reduced the backup sizes of only those datafiles that contained significant amount of free space. In Oracle 10*g*, you can compress the backups regardless of the contents of the datafiles. You can perform compressed backup on databases, tablespaces, and datafiles. The compressed backups work only with backup sets and not with image copies. Compressed backup sets save storage space; therefore, the size of compressed backup sets is smaller than that of image copies or backup sets. A compressed backup set, therefore, reduces network bandwidth if you are performing backups across a network.

Item: 8 (Ref:1Z0-043.3.1.1)

You issued the following RMAN command:

```
RMAN> CONFIGURE CONTROLFILE AUTOBACKUP ON;
```

What is **NOT** an impact of using the above command?

- When a successful backup is recorded in the RMAN repository, then a backup of the current control file is performed.
- When a structural change is made to the database, then a backup of the current control file is performed.
- When a successful backup is performed in the RMAN repository, then a backup of the spfile is performed.
- When a structural change is made to the database, then a backup of the alert log file will be performed.

Answer:

When a structural change is made to the database, then a backup of the alert log file will be performed.

Explanation:

When a structural change is made to the database, then a backup of the alert log file will not be performed. The RMAN command CONFIGURE CONTROLFILE AUTOBACKUP ON; is used to configure the RMAN to perform a backup of the control file and the spfile in one of the following two situations:

- Whenever a successful backup is recorded in the RMAN repository.
- Whenever a structural change is made to the database.

Therefore the option stating that when a successful backup is recorded in the RMAN repository, then a backup of current control file is not performed, the option stating that when a structural change is made to the database, then a backup of the current control file is not performed and the option stating that when a structural change is made to the database, then a backup of the alert log file is performed are incorrect.

Item: 9 (Ref:1Z0-043.3.4.1)

You administer an Oracle Database 10*g* and a third-party database. You use Recovery Manager (RMAN) to perform backup and recovery operations. You have configured a recovery catalog to act as an RMAN repository.

To which of the following databases can you **NOT** connect using the `RMAN CONNECT` command?

- target database
- auxiliary database
- third-party database
- recovery catalog database

Answer:

third-party database

Explanation:

Using the `RMAN CONNECT` command, you cannot connect to a third-party database. Therefore, you must back up the third-party databases by using either the operating system utility (if allowed) or a third-party backup tool.

All the other options are incorrect because by using the `RMAN CONNECT` command, you can connect to either a target database, an auxiliary database, or a recovery catalog.

The target database is the database that you are backing up or recovering. An auxiliary database is the standby or duplicate database. A recovery catalog is a database that stores the metadata for backup, recovery, and restore operations.

Item: 10 (Ref:1Z0-043.3.2.7)

You issue the following RMAN command to set a retention policy on a database:

```
RMAN>CONFIGURE RETENTION POLICY TO REDUNDANCY 2;
```

What will be the outcome of the above command?

- After two days, the backup will be marked obsolete.
- After two days, the backup will be deleted from the media.
- If the RMAN repository has records of two or more recent backups of a file, then the older backup will be deleted from the media.
- If the RMAN repository has records of two or more recent backups of a file, then the older backup will be marked obsolete.

Answer:

If the RMAN repository has records of two or more recent backups of a file, then the older backup will be marked obsolete.

Explanation:

The `CONFIGURE RETENTION POLICY TO REDUNDANCY` command is used to configure the retention policy for redundancy of backups. Retention policy is used for the management of space in the flash recovery area. The retention policy can be configured by using the redundancy-based retention policy or the recovery window-based retention policy. If the redundancy-based retention policy is configured, then the flash recovery area considers the backup of a file to be obsolete when the RMAN repository contains a specified number of records of more recent backups. The older backups of the file are marked obsolete.

In this scenario, the `CONFIGURE RETENTION POLICY TO REDUNDANCY 2;` command configures the RMAN repository to store two recent backups of the file and marks the other older backups of this file as obsolete.

The option stating that the backup will be marked obsolete after two days is incorrect. This is because the `CONFIGURE RETENTION POLICY TO REDUNDANCY` command is used to configure the redundancy-based retention policy. You can specify that after n days, the backup will be marked obsolete by configuring the recovery window-based retention policy. The recovery window-based retention policy is configured by using the following command:

```
CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF n DAYS;
```

The option stating that the backup will be deleted from the media after two days is incorrect and the statement stating that the older backup will be deleted from the media if the RMAN repository has records of two more recent backups of a file is also incorrect. This is because the backups are not deleted from the media for any type of retention policy.

Item: 11 (Ref:1Z0-043.3.2.10)

You are using Recovery Manager (RMAN) for backup and recovery operations. Your backup and recovery policy is such that you are performing full database backup every Tuesday and Friday. You configure RMAN using the following command:

```
RMAN>CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 4 DAYS;
```

All backup and archived redo logs generated during the current week are as follows:

Day	Backup	Archived Redo Logs
Monday	-	Log Sequence 520
Tuesday	Full Database Backup	-
Wednesday	-	Log Sequence 521
Thursday	-	Log Sequence 522
Friday	Full Database Backup	-
Saturday	-	Log Sequence 523
Sunday	-	Log Sequence 524

Which of the following files will be listed when issuing the REPORT OBSOLETE command on Sunday?

- the archived redo log with the log sequence 520
- the backup files from the full database backup performed on Tuesday
- the archived redo log with the log sequence 520 and the backup files from the full database backup performed on Tuesday
- archived redo logs with the log sequences 520, 521, 522 and the backup files from the full database backup performed on Tuesday

Answer:

the archived redo log with the log sequence 520

Explanation:

If the REPORT OBSOLETE command is issued on Sunday, only the archived redo log with the log sequence 520 will be listed. The retention policy is configured to a recovery window of four days. This means that RMAN retains all the backups and copies of datafiles, control files, and archived redo logs that are needed to recover the database, to a point in time in the last four days. In the given scenario, point of recoverability is Wednesday. Therefore, all archived redo logs from the log sequence 521 through 524 are retained by RMAN. The backup files from the full database backup performed on Tuesday are also retained because, if needed, these backup files are used to recover the database up to Wednesday.

The backup files from the full database backup performed on Tuesday are not obsolete according to the given retention policy and, therefore, will not be listed using the REPORT OBSOLETE command.

The archived redo log with the log sequence 520 and the backup files from the full database backup performed on Tuesday are not obsolete because the backup files are required in the recovery process if the database has to be recovered up to Wednesday.

The REPORT OBSOLETE will not list the archived redo logs from the log sequence 520 through 522 and backup files from the full database backup performed on Tuesday. The archived redo logs with the log sequence 521 and 522, along with the backup files from the full database backup that is performed on Tuesday, are protected by the recovery window.

Item: 12 (Ref:1Z0-043.3.3.5)

The size of the largest datafile, `data1.dbf`, in your database is 30MB. You issued the following command:

```
RMAN>CONFIGURE MAXSETSIZE 10MB;
```

What will be the impact of the above setting?

- While performing the backup of the datafile, `data1.dbf`, one backup set is created.
- While performing the backup of the datafile, `data1.dbf`, two backup sets are created.
- While performing the backup of the datafile, `data1.dbf`, three backup sets are created.
- While performing the backup of the datafile, `data1.dbf`, the command for performing a backup of the datafile, `data1.dbf,` will fail.

Answer:

While performing the backup of the datafile, `data1.dbf`, the command for performing a backup of the datafile, `data1.dbf,` will fail.

Explanation:

The `MAXSETSIZE` parameter is used to configure the maximum size of each backup set. This parameter limits the number of datafiles within a backup set and forces `RMAN` to create another backup set. In this scenario, the size of the `data1.dbf` datafile is larger than the value of the `MAXSETSIZE` configuration parameter. Therefore, the command for performing the backup of the datafile will fail. No backup set will be created. You must ensure that the value of the `MAXSETSIZE` parameter is larger than the size of the largest datafile in your database.

The other options are incorrect because the command for performing the backup of the datafile, `data1.dbf,` will fail.

Item: 13 (Ref:1Z0-043.3.2.9)

Your database is running in the ARCHIVELOG mode. You have configured RMAN for backup and recovery operations. You execute the following command from the RMAN prompt:

```
RMAN> CONFIGURE CONTROLFILE AUTOBACKUP ON;
```

After executing this command, in which of the following cases will RMAN make an auto-backup of the control file? (Choose all that apply.)

- ☐ when you change the name of a datafile
- ☐ when you drop a table from the database
- ☐ when you take an export of the database
- ☐ when you back up the database using OS utilities
- ☐ when you issue an ALTER SYSTEM SWITCH LOGFILE statement
- ☐ when you issue a BACKUP command from inside the RMAN run block

Answer:

when you change the name of a datafile

when you issue an ALTER SYSTEM SWITCH LOGFILE statement

when you issue a BACKUP command from inside the RMAN run block

---

Explanation:

After you configure auto-backup for a control file using RMAN, RMAN will make an auto-backup of the control file in the following cases:

- when you issue a BACKUP command from the RMAN prompt
- when you use a RUN block in which the last command is a BACKUP command
- when you use a RUN block in which a BACKUP command is not followed by another BACKUP command
- when there is a structural change in the database; for example adding a datafile or redo log file to the database, renaming a datafile or redo log file, etc.

However, the control file is not backed up:

- when you drop a table from the database
- when you take an export of the database
- when you back up a database using OS utilities

Item: 14 (Ref:1Z0-043.3.3.2)

You issued the RMAN>SHOW ALL; command. The output of this command is as follows:

```
CONFIGURE RETENTION TO REDUNDANCY 1; # default
CONFIGURE BACKUP OPTIMIZATION OFF; # default
CONFIGURE DEFAULT DEVICE TYPE TO DISK BACKUP AS BACKUPSET;
CONFIGURE CONTROLFILE AUTOBACKUP ON;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '%FF';
#default
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE DISK TO 1; #default
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT
'oracle/flash_recovery_area/ora101c/rec_area_%s_%p.bak'bak';
CONFIGURE MAXSETSIZE TO UNLIMITED; # default
CONFIGURE ARCHIVELOG DELETION POLICY TO NONE; #default
CONFIGURE SNAPSHOT CONTROLFILE NAME TO
'C:\ORACLE\PRODUCT\10.1.0\DB_1\DATABASE\SNCFOR101C.ORA'ORA'; # default
```

After analyzing the output, which conclusion will you draw?

- The current control file is not automatically backed up every time you perform a backup.
- The backups save space on the storage media.
- While performing backups across a network, the network bandwidth is reduced.
- The backups consist of backup pieces.

Answer:

The backups consist of backup pieces.

Explanation:

In this scenario, the CONFIGURE DEFAULT DEVICE TYPE TO DISK BACKUP AS BACKUPSET; setting specifies that the backup type to be performed on the disk is a backup set. A backup set is a backup in a special RMAN format that can contain more than one file, each called backup piece. A backup piece is the smallest unit of backup in the RMAN utility. The backup piece is the actual file within the backup set.

The option stating that the current control file is not automatically backed up every time you perform a backup is incorrect. This is because the CONFIGURE CONTROLFILE AUTOBACKUP ON setting is used to configure RMAN to back up the control file whenever a backup of the database, tablespace, or datafile is performed.

The option stating that the backups save space on the storage media is incorrect. This is because a backup set does not save storage space on the storage media. A compressed backup set saves storage space on the storage media. In this scenario, the CONFIGURE DEVICE TYPE DISK BACKUP TYPE TO BACKUPSET; setting indicates that backup set is the default backup type. The CONFIGURE DEVICE TYPE DISK BACKUP TYPE TO COMPRESSED BACKUPSET; command is used to configure a compressed backup set as the default backup type. In earlier versions of Oracle, to reduce the sizes of the backups, only used blocks were backed up and the unused blocks were skipped. This method reduced the backup sizes of only those datafiles that had significant amount of free space. In Oracle 10*g*, you can compress the backups regardless of the contents of the datafiles. You can perform compressed backup on databases, tablespaces, and datafiles. Compressed backups work only with backup sets and not with image copies. Compressed backup sets save storage space and reduce the network bandwidth if you are performing backups across a network

The option stating that the network bandwidth is reduced while performing backups across a network is incorrect. This is because reducing the network bandwidth while taking the backup across a network is not a feature of the backup set. This is a function of the compressed backup set. In this scenario, the CONFIGURE DEVICE TYPE DISK BACKUP TYPE TO BACKUPSET; setting indicates that backup set is the default backup type. The CONFIGURE DEVICE TYPE DISK BACKUP TYPE TO COMPRESSED BACKUPSET; command is used to configure a compressed backup set as the default backup type. A compressed backup set saves storage space on the storage media. Compressed backup sets save storage space; therefore, the size of compressed backup sets is smaller than that of an image copy or a backup set. A compressed backup set reduces network bandwidth if you are performing backups across a network.

Item: 15 (Ref:1Z0-043.3.2.3)

You are maintaining your database in Oracle10*g*. You are not using the recovery catalog to maintain the backup metadata information. You want to enable the reusable section of the control file to expand itself if the oldest record cannot be reused, and whenever a new record is added to the reusable section of the control file.

Which value will you set for the CONTROL_FILE_RECORD_KEEP_TIME parameter?

- Zero
- One or more
- NONE
- DEFAULT

Answer:

One or more

Explanation:

You will set the value of the CONTROL_FILE_RECORD_KEEP_TIME initialization parameter to one or more to allow the reusable section to expand itself if the oldest record cannot be reused, and whenever a new record is added to the reusable section of the control file. The CONTROL_FILE_RECORD_KEEP_TIME initialization parameter is used to specify the minimum duration for which the information about a backup that can be used by RMAN will be stored in the control file of the target database. The default value for this parameter is 7 days. The valid range for this parameter is 0 to 365 days. If you specify the value of the CONTROL_FILE_RECORD_KEEP_TIME parameter to be zero, then the circular reusable section never expands, and the records are reused as per requirements.

The option stating that you will set the value of the CONTROL_FILE_RECORD_KEEP_TIME initialization parameter to zero to allow the reusable section to expand itself if the oldest record cannot be reused, and whenever a new record is added to the reusable section of the control file is incorrect. If you specify the value of the CONTROL_FILE_RECORD_KEEP_TIME parameter as zero, then the circular reusable section never expands, and the records are reused as per requirements.

The options stating that you will set the value of the CONTROL_FILE_RECORD_KEEP_TIME initialization parameter to NONE is incorrect. The option stating that you will set the value of the CONTROL_FILE_RECORD_KEEP_TIME initialization parameter to DEFAULT to allow the reusable section to expand itself if the oldest record cannot be reused and whenever a new record is added to the reusable section of the control file is also incorrect. The values, NONE and DEFAULT, are incorrect values for the CONTROL_FILE_RECORD_KEEP_TIME parameter. The value is specified in number of days.

Item: 16 (Ref:1Z0-043.3.4.2)

You want to implement the backup and recovery strategy in your database using Recovery Manager (RMAN). You have chosen the control file of the target database for the RMAN repository.

Which command-line RMAN command would you use to establish a local connection between RMAN and the RMAN repository if your database is using password file authentication?

- `rman TARGET / NOCATALOG`
- `rman TARGET sys/password`
- `rman TARGET sys/password AS SYSDBA`
- `rman TARGET sys/password@db_name CATALOG rman_user/rman_password@rcat`

Answer:

`rman TARGET sys/password`

Explanation:

When you are using password file authentication in your database, you must specify the username and password to connect to the target database. RMAN stores its metadata in the control file of the target database when it runs in the `NOCATALOG` mode. Therefore, the following command-line RMAN command is required to establish a local connection between RMAN and the target database:

```
rman TARGET sys/password NOCATALOG
```

However, specifying `NOCATALOG` is optional. By default, RMAN runs in `NOCATALOG` mode. Therefore, you can start RMAN without specifying the `NOCATALOG` option as follows:

```
rman TARGET sys/password
```

The `rman TARGET /` command is only used for a local RMAN connection when you have configured operating system authentication in your database. Executing this command when you are using password file authentication will return an error.

You connect to RMAN using the SYSDBA privilege. However, you do not need to specify the `AS SYSDBA` option because RMAN uses this option implicitly and automatically. Including `AS SYSDBA` in the command will return an error. The SYSDBA privilege is a system privilege that is required for performing certain administrative tasks like starting a database, shutting down a database, and creating databases.

The `rman TARGET sys/password@db_name CATALOG rman_user/rman_password@rcat` command is used to establish a connection between RMAN and the recovery catalog database. Therefore, in the given scenario, this is an invalid option.

Item: 17 (Ref:1Z0-043.3.2.4)

You are maintaining your production database in Oracle10*g*. You want the circular reuse records in the control file of the target database to be reused as required.

Which value will you set for the CONTROL_FILE_RECORD_KEEP_TIME initialization parameter?

- 0
- 1
- NONE
- DEFAULT

Answer:

0

Explanation:

You will set the value of the CONTROL_FILE_RECORD_KEEP_TIME initialization parameter to 0. The CONTROL_FILE_RECORD_KEEP_TIME initialization parameter is used to specify the minimum duration for which the information about a backup that can be used by RMAN will be stored in the control file of the target database. The default vale for this parameter is 7 days. The valid range for this parameter is 0 to 365 days. If you specify the value of the CONTROL_FILE_RECORD_KEEP_TIME parameter to zero, the circular reusable section never expands, and the records are reused as required.

The option stating that you will set the value of the CONTROL_FILE_RECORD_KEEP_TIME initialization parameter to 1 is incorrect. If you set the value, 1, for the CONTROL_FILE_RECORD_KEEP_TIME parameter, then the backup metadata will be maintained in the control file for a minimum of one day.

The options stating that you will set the value of the CONTROL_FILE_RECORD_KEEP_TIME initialization parameter to NONE, and the option stating that you will set the value of the CONTROL_FILE_RECORD_KEEP_TIME initialization parameter to DEFAULT are incorrect. The values, NONE and DEFAULT, are incorrect for the CONTROL_FILE_RECORD_KEEP_TIME parameter. The value is specified in number of days.

Using Recovery Manager

Item: 1 (Ref:1Z0-043.7.1.2)

Your PROD database has been started using the server parameter file. In your PROD database you are using RMAN for backup and recovery operations. You issue the following commands from the RMAN prompt:

```
RMAN> CONFIGURE CONTROLFILE AUTOBACKUP OFF;
RMAN> BACKUP DATABASE;
```

Which files from the database will be backed up as a result of this BACKUP command? (Choose all that apply.)

- control file
- all datafiles
- password file
- online redo log file
- archive redo log file
- server parameter file
- only the SYSTEM datafile

Answer:

control file
all datafiles
server parameter file

Explanation:

When you issue the BACKUP DATABASE command from the RMAN prompt, RMAN backs up all the datafiles, the current control file, and the server parameter file. The current control file will be backed up even if the control file autobackup is set to OFF. If the control file autobackup is ON the control file will be backed up twice as a result of this command.

The password file is not backed up when you issue this BACKUP command. You cannot use the RMAN BACKUP command to back up a password file. This command can only be used to back up a database, tablespace, control file, datafiles, archive log files, backup sets, and the server parameter file.

The online redo log files are not backed up when you issue this command. RMAN does not support backup of online redo log files. The RMAN BACKUP command can only be used to back up a database, tablespace, control file, datafiles, archive log files, backup sets, and the server parameter file.

The archive redo log files are not backed up when you issue this command. To back up the archive redo log files along with the database, you should issue the following command:

```
RMAN> BACKUP DATABASE PLUS ARCHIVELOG;
```

The option that states that only the SYSTEM datafile will be backed up is incorrect because all the datafiles will be backed up with the given command.

Item: 2 (Ref:1Z0-043.7.1.4)

You have configured your database to use RMAN for backup and recovery. You must back up the datafile contained in the TS1 tablespace. The size of the datafile in the TS1 tablespace is 200 MB.

You issue the following command from the RMAN prompt to perform a backup of the tablespace:

```
RMAN> BACKUP TABLESPACE TS1 MAXSETSIZE 100M;
```

Which statement is true about executing this command?

- The command generates an error.
- The command backs up the tablespace and creates a backup set of size 200 MB.
- The command backs up the tablespace and creates two backup sets of size 100 MB each.
- The command backs up the tablespace and creates a backup set with backup pieces of size 100 MB each.

Answer:

The command generates an error.

Explanation:

The command generates an error because the size of the file contained in the tablespace is greater than the MAXSETSIZE specified in the command. The MAXSETSIZE should always be greater than the size of the file that is being backed up.

The other options are incorrect because the command will not execute, but will generate an error.

Item: 3 (Ref:1Z0-043.7.2.5)

You issued the following command:

```
ALTER DATABASE ENABLE BLOCK CHANGE TRACKING;
```

What will be the result of issuing this command?

- The block change tracking feature is enabled, and the information about the system change number is written in the change tracking file.
- The block change tracking feature is enabled, and the information about the log sequence number is written in the change tracking file.
- The block change tracking feature is enabled, and the information about the blocks that are changed since the last backup is written in the change tracking file.
- The block change tracking feature is enabled, and the information about the locations of the datafiles and the online redo log files are written in the change tracking file.

Answer:

The block change tracking feature is enabled, and the information about the blocks that are changed since the last backup is written in the change tracking file.

Explanation:

The result of issuing the `ALTER DATABASE ENABLE BLOCK CHANGE TRACKING;` command is that the block change tracking feature is enabled, and the information about the blocks that are changed since the last backup is written in the change tracking file. The `CTWR` background process records the blocks since the last backup and stores the information in the block change tracking file. `RMAN` uses this file to determine the blocks that were backed up in an incremental backup. This improves the performance because `RMAN` does not have to scan the entire database during backup. In prior versions of Oracle, `RMAN` had to scan the entire datafile. However, in Oracle10*g*, the backup process is initiated with `RMAN` querying the block change tracking file to determine the changed blocks. `RMAN` backs up only the changed blocks and skips the unchanged blocks. This reduces the amount of blocks required in backup to the amount of changes.

The option stating that the block change tracking feature is enabled, and the system change number is written in the change tracking file is incorrect. This is because the change tracking file does not contain the system change number. The system change number is written in the control file.

The option stating that the block change tracking feature is enabled, and the information about the log sequence number is written in the change tracking file is incorrect. This is because the change tracking file does not contain the log sequence number. The log sequence number is written in the control file.

The option stating that the locations of the redo log files are written in the change tracking file are incorrect. This is because the change tracking file does not contain the information about the locations of the redo log files. The control file contains the information about the locations of the redo log files.

Item: 4 (Ref:1Z0-043.7.3.1)

In which scenario, will you issue the following command?

```
RMAN> REPORT NEED BACKUP DAYS 7;
```

- to configure RMAN to maintain backup information in the RMAN repository for seven days
- to configure RMAN to maintain backup information in the control file for at least seven days
- to display the list of files that have not been backed up for the last seven days
- to display the list of files that must be backed up within seven days

Answer:

to display the list of files that have not been backed up for the last seven days

---

Explanation:

You will issue the REPORT NEED BACKUP DAYS 7 command at the RMAN prompt to display the list of files that have not been backed up for the last 7 days. The REPORT NEED BACKUP command is used to query the RMAN repository and obtain data regarding files that require a backup.

You will not issue the above command to configure RMAN to maintain backup information in the RMAN repository for seven days. To configure RMAN to maintain the backup information in the RMAN repository for seven days, you will issue the following command:

```
RMAN>CONFIGURE RETENTION POLICY TO RECOVERY WINDOW OF 7 DAYS;
```

You will not issue the above command To configure RMAN to maintain backup information in the control file for at least seven days. To configure RMAN to maintain backup information in the control file for at least seven days, you will set the value of the CONTROLFILE_RECORD_KEEP_TIME initialization parameter to seven days.

You will not issue the above command to display the list of files that must be backed up within 7 days. You cannot list the files that must be backed up within the specified number of days.

Item: 5 (Ref:1Z0-043.7.2.4)

You have configured OMF in your database. You enabled the `ALTER DATABASE ENABLE BLOCK CHANGE TRACKING;` statement to enable the block change tracking feature.

What information will be written in the change tracking file?

- the system change number
- the locations of the redo log files
- the locations of the datafiles
- the physical location of all the database changes

Answer:

the physical location of all the database changes

Explanation:

The `CTWR` background process records the blocks since the last backup and stores the information in the block change tracking file. `RMAN` uses this file to determine the blocks that were backed up in an incremental backup. This improves the performance because `RMAN` does not have to scan the entire database during backup. In prior versions of Oracle, `RMAN` had to scan the entire datafile. In Oracle10*g*, the backup process is initiated when `RMAN` queries the block change tracking file to determine the changed blocks. `RMAN` backs up only the changed blocks and skips the unchanged blocks. This reduces the number of blocks to be backed up during the incremental backup.

The option stating that the information about the system change number is written in the change tracking file is incorrect. The information about the system change number is written in the control file. The system change number is used while performing database recovery.

The option stating that the locations of the redo log files are written in the change tracking file is incorrect. The location of the online redo log files are written in the control file and the spfile. The control file and the spfile contains information, such as database name, locations of the datafiles and the online redo log files, the SCN number, the log sequence number, and the date and time of creation of the database.

The control file and the spfile are required for database startup.

The option stating that the locations of the datafiles are written in the change tracking file is incorrect. The locations of the datafiles are written in the control file and the spfile. The control file and the spfile contains information, such as database name, locations of the datafiles and the online redo log files, the SCN number, the log sequence number, and the date and time of creation of the database.

Item: 6 (Ref:1Z0-043.7.1.3)

Your database in running in the ARCHIVELOG mode. You issue the following command to back up datafile 2 in your database.

```
RMAN> COPY DATAFILE 2 TO 'D:\ORACLE\ORA90\MYNEWDB\DA2.DBF';
```

Which two statements are true regarding the backup created using this command? (Choose two.)

- The copy of the datafile created is stored in the RMAN repository.
- The copy of the datafile created can be viewed using the LIST BACKUP command.
- The copy of the datafile created using this COPY command can be placed only on the disk.
- The copy of the datafile created is similar to the backup of the file created using the BACKUP command.
- The copy of the datafile created can be used for recovering the database using the user-managed recovery method.

Answer:

The copy of the datafile created using this COPY command can be placed only on the disk.

The copy of the datafile created can be used for recovering the database using the user-managed recovery method.

Explanation:

The given command will create a copy of datafile 2 and store it as D:\ORACLE\ORA90\MYNEWDB\DA2.DBF on a disk. This copy of the datafile can be used for recovering the database using the user-managed recovery method. The copy created can be viewed using the LIST COPY command.

The option that states that the copy is stored in the RMAN repository is incorrect because the copy is stored on the disk.

The option that states that the copy created can be viewed using the LIST BACKUP command is incorrect because it cannot be viewed using the LIST BACKUP command. It can be viewed using the LIST COPY command. To view the backup using the LIST BACKUP command you must have backed it up using the BACKUP command and not the COPY command.

The option that states that the copy created will be similar to the backup of the file created using the BACKUP command is incorrect because it is not similar to the backup created using the BACKUP command. The copies created using the BACKUP command are different from the OS files because they can be used only by the RMAN utility.

Item: 7 (Ref:1Z0-043.7.1.1)

You are maintaining your database in Oracle10*g*. You are performing the backup by using the BACKUP AS BACKUPSET command at the RMAN prompt. Which file cannot be backed up by using the BACKUP AS BACKUPSET command?

- Datafiles
- Current control file
- Server parameter file (spfile)
- Password file

Answer:

Password file

Explanation:

You cannot perform backup of the password file by using the BACKUP command at the RMAN prompt. A password file is used to authenticate administrative users who can have the SYSDBA privilege. A password file is created by using the ORAPWD utility. The users having SYSDBA privileges can start up and shut down the database. The password file is outside of the database because sometimes the password file is referenced, when the database is not running.

The other three files including the datafiles, current control file and the server parameter file can be backed up using the BACKUP command at the RMAN prompt. When performing backups using RMAN utility, you can specify what to backup. The valid values are DATABASE, DATAFILE, TABLESPACE, ARCHIVELOG, CURRENT CONTROLFILE and SPFILE. You can perform backup of entire databases, specific tablespaces, archive log files, and the current control file. When you configure RMAN to perform an automatic backup of the current control file, then the SPFILE is also backed up.

Item: 8 (Ref:1Z0-043.7.2.3)

You have not configured Oracle Managed Files (OMF) in your database. You do not want to scan the entire datafile every time an incremental backup is performed. You decide to enable the block change tracking feature.

Which statement will you use to enable the block change tracking feature?

- `ALTER SYSTEM ENABLE BLOCK CHANGE TRACKING;`
- `ALTER DATABASE ENABLE BLOCK CHANGE TRACKING;`
- `ALTER SYSTEM ENABLE BLOCK CHANGE TRACKING USING FILE <path>;`
- `ALTER DATABASE ENABLE BLOCK CHANGE TRACKING USING FILE <path>;`

Answer:

`ALTER DATABASE ENABLE BLOCK CHANGE TRACKING USING FILE <path>;`

Explanation:

If OMF is configured in your database, then you need not specify the name of block change tracking file in the statement used for enabling the block change tracking feature. The file is automatically located in the directory specified by the `DB_CREATE_FILE_DEST` parameter. In this scenario, OMF is not configured. Therefore, you must specify the location of the block change tracking file in the command that is used for enabling the block change tracking feature in your database. You will issue the following statement to enable the change tracking feature:

```
ALTER DATABASE ENABLE BLOCK CHANGE TRACKING USING FILE <path>;
```

The option stating that you will issue the `ALTER SYSTEM ENABLE BLOCK CHANGE TRACKING` statement to enable the block change tracking feature is incorrect. The option stating that you will issue the `ALTER SYSTEM ENABLE BLOCK CHANGE TRACKING USING FILE <path>` statement to enable the block change tracking feature is also incorrect. These two statements will generate an error because the block change tracking feature is enabled at the database level and not at the system level.

The option stating that you will issue the `ALTER DATABASE ENABLE BLOCK CHANGE TRACKING` statement to enable the block change-tracing feature is incorrect. This is because OMF is not configured in the database. If OMF is not configured, then you need to specify the location of the block change tracking file in the command for enabling the block change tracking feature.

Item: 9 (Ref:1Z0-043.7.3.2)

You are maintaining your database in Oracle10*g*. You are required to view the list of files that have not been backed up for the last seven days. Which RMAN command will you use?

- LIST command
- CROSSCHECK command
- REPORT command
- SHOW command

Answer:

REPORT command

Explanation:

You will use the REPORT command at the RMAN prompt to display a list of files that have not been backed up for the last seven days. You will issue the following command:

```
RMAN>REPORT NEED BACKUP DAYS 7;
```

You will not use the LIST command at the RMAN prompt to display the list of files that have not been backed up for the last seven days. The LIST command is used to query the RMAN repository and obtain data regarding the BACKUP command or the COPY command.

You will not use the CROSSCHECK command at the RMAN prompt to display the list of the files that have not been backed up for the last seven days. The CROSSCHECK command determines whether the files managed by RMAN, such as archived logs, datafile copies, and the backup pieces, exist on the disk or tape or not.

You will not use the SHOW command at the RMAN prompt to display the list of the files that have not been backed up for the last seven days. The SHOW command is used to display any configuration set by the CONFIGURE command. You can issue the SHOW ALL command at the RMAN prompt to display all current configurations.

Item: 10 (Ref:1Z0-043.7.2.1)

You are maintaining your database in Oracle10*g*. While performing an incremental backup of the database, you want to back up only those blocks that have changed since the last backup.

Which file will you create to increase the performance of the backup operation while performing the incremental backup of the database?

- redo log files
- password file
- control file
- change tracking file

Answer:

change tracking file

Explanation:

If you want to perform the incremental backup of the database and increase the performance while performing the backup operation, then you will create the change tracking file. The CTWR background process writes the physical locations of the changes made to the database in the change tracking file. RMAN uses the change tracking file to determine the blocks that must be backed up during an incremental backup. Using the change tracking file, improves the performance of the backup process by eliminating the requirement of reading the entire datafile.

You will not create redo log files to increase the performance of the backup operation while performing the incremental backup of the database. The redo log file contains redo log entries. The redo log entries consist of changes made to the database. The online redo log files are automatically created when the database is created.

You will not create the password file to increase the performance of the backup operation while performing the incremental backup of the database. A password file is used to authenticate administrative users who can have the SYSDBA privilege. A password file is created by using the ORAPWD utility. The users having the SYSDBA privilege can start up and shut down the database.

You will not create the control file to increase the performance of the backup operation while performing the incremental backup of the database. The control file is used to start your database. The control file contains information, such as instance names, locations of the datafiles, online redo log files, date and time of the database creation, the current SCN number, the log sequence number, and so on. The control file is automatically created when the database is created.

Item: 11 (Ref:1Z0-043.7.3.3)

You issue the following command on the RMAN prompt.

```
RMAN> REPORT NEED BACKUP DAYS = 5 DATABASE;
```

Which statement is true about executing this command?

- It will display a list of files that need incremental backup.
- It will display a list of files that need backup after five days.
- It will display a list of files that were backed up in the last five days.
- It will display a list of files that have not been backed up in the last five days.
- It will apply the current retention policy to determine the files that need to be backed up.

Answer:

It will display a list of files that have not been backed up in the last five days.

Explanation:

The `REPORT NEED BACKUP DAYS` command is used to display a list of files that have not been backed up since the specified number of days. In this case, the command displays all the database files that have not been backed up in the last five days. The command overrides the current retention policy set for backup retention because the clause `DAYS = 5` is used in the command.

The option that states that the command will display the list of files that need incremental backup is incorrect because the command will list the files that have not been backed up in the last five days. The command does not display files that need an incremental backup.

The option that states that the command will display a list of files that need a backup after five days is incorrect because the command will list the files that have not been backed up in the last five days.

The option that states that the command will display a list of files that were backed up in the last five days is incorrect because the command will list the files that have not been backed up in the last five days.

The option that states that the command will apply the current retention policy to determine the files that need backup is incorrect. When you include the `DAYS` clause with the `REPORT` command, the current retention policy is overridden. If you want to use the retention policy to list the files needing backup, you should omit the `DAYS` clause and use only the `REPORT NEED BACKUP` command. This will use the retention policy to determine which files need to be backed up.

Recovering from Non-Critical Losses

Item: 1 (Ref:1Z0-043.9.1.2)

Twenty database users are connected to your database. Five of the users are running long queries involving sort operations. The TEMP tablespace is the default temporary tablespace for your database. You are performing offline tablespace backups of individual tablespaces and erroneously execute the following statement:

```
SQL>ALTER TABLSPACE temp OFFLINE NORMAL;
```

What is the result of this statement?

- The TEMP tablespace is taken offline. The users using the TEMP tablespace for sorting are disconnected after their queries complete.
- The TEMP tablespace is taken offline. The users using the TEMP tablespace for sorting are disconnected and must re-execute their queries.
- The TEMP tablespace is taken offline. The users using the TEMP tablespace for sorting are not disconnected, but these users must re-execute their queries.
- The TEMP tablespace is not taken offline. The users using the TEMP tablespace for sorting are not disconnected, and their queries execute successfully.

Answer:

The TEMP tablespace is not taken offline. The users using the TEMP tablespace for sorting are not disconnected, and their queries execute successfully.

Explanation:

In this scenario, the TEMP tablespace is not taken offline, the users using the TEMP tablespace for sorting are not disconnected, and their queries execute successfully. This is because you cannot place a temporary tablespace offline regardless of whether the connected users are using the temporary tablespace for sorting. If you attempt to take a temporary tablespace offline, you receive the following error:

```
ORA-03217: invalid option for alter of TEMPORARY TABLESPACE
```

The option stating that the TEMP tablespace is taken offline and the users are disconnected after their queries complete is incorrect because the TEMP tablespace cannot be taken offline. The users will remain connected after their queries complete.

The option stating that the TEMP tablespace is taken offline, the users are disconnected, and the queries must be re-executed is incorrect because the TEMP tablespace cannot be taken offline. The users will continue to be connected and their queries are not aborted.

The option stating that the TEMP tablespace is not taken offline and the users are not disconnected is incorrect because you cannot take a temporary tablespace offline. The currently executing queries are not affected.

Item: 2 (Ref:1Z0-043.9.3.3)

At database startup, you discover that one of the disks containing an index tablespace has been lost due to a media failure. A backup of the lost index tablespace is not available. You have all the necessary scripts to recreate the indexes. You need to re-create the indexes in a new index tablespace.

Which action must you perform before re-creating the indexes?

- Start the database in OPEN mode, and create a new index tablespace.
- Start the database in OPEN mode, and drop the lost index tablespace from the database.
- Start the database in MOUNT mode, create a new index tablespace, and drop the lost index tablespace from the database.
- Start the database in MOUNT mode, drop the lost index tablespace from the database, open the database, and create a new index tablespace.

Answer:

Start the database in MOUNT mode, drop the lost index tablespace from the database, open the database, and create a new index tablespace.

Explanation:

You must start the database in MOUNT mode, drop the lost index tablespace from the database, and create a new index tablespace prior to re-creating the indexes. If you have lost an index tablespace and do not have a backup, you can re-create the indexes using the scripts that contain the CREATE INDEX statements. Before re-creating the indexes in a new index tablespace, you must perform the following steps:

- Start the database in the MOUNT mode by issuing the STARTUP MOUNT statement. This is required because a database cannot be opened unless you perform media recovery on the lost index tablespace.
- Drop the existing tablespace from the database by issuing the DROP TABLESPACE statement. This ensures that the corresponding entry for this tablespace is removed from the control file.
- Open the database and create a new tablespace by issuing the CREATE TABLESPACE statement. This statement will enable you to create a tablespace for storing the indexes that you need to re-create.

The option stating that you must start the database in OPEN mode, and create a new index tablespace is incorrect because you cannot open the database unless you perform a media recovery, or drop the lost tablespace from the database.

The option stating that you must start the database in OPEN mode, and drop the lost index tablespace from the database is incorrect. Oracle will not allow you to open the database unless you perform a media recovery on the lost index tablespace.

The option stating that you must start the database in MOUNT mode, create a new index tablespace, and drop the lost index tablespace from the database is incorrect because the CREATE TABLESPACE statement cannot be executed in MOUNT mode.

Item: 3 (Ref:1Z0-043.9.2.1)

Your database is in NOARCHIVELOG mode. The database has three online redo log groups, and each group contains three online redo log members. The online redo log members are stored across three hard disks, E, F, and G, respectively. Hard disk G crashed while the LGWR background process was writing redo information to the online redo log files.

What effect will this crash have on the database?

- The database will operate normally without generating any redo.
- The database will hang, and you must shut down and restart the instance.
- The database will crash, and you must recover the database from the point of failure.
- The database will operate normally and will generate minimal redo for the tables created with the NOLOGGING clause.

Answer:

The database will operate normally and will generate minimal redo for the tables created with the NOLOGGING clause.

Explanation:

In this scenario, the database will operate normally and will generate minimal redo for the tables created with the NOLOGGING clause. When you place the members of a redo group across different hard disks, only the member of the group stored on the failed disk becomes unavailable. All the other members of the group remain accessible to the LGWR background process, and the database continues to function normally. The database always generates minimal redo for tables that are created with the NOLOGGING clause.

The option stating that the database operates normally without generating any redo is incorrect because the database always generates redo entries and stores them in the online redo log files. The only exception occurs when the NOLOGGING clause is used in the CREATE TABLE...AS SELECT statement. Oracle generates minimal redo for the tables created using the NOLOGGING option.

The option stating that the database will hang is incorrect because the LGWR background process will continue to write redo information to the redo log files available on E and F, the other hard disks, in this scenario. The LGWR background process cannot write redo entries to the online redo log files stored on the inaccessible hard disk, in this scenario G.

The option stating that the database will crash is incorrect because the instance does not abort, and the database continues to operate normally.

Item: 4 (Ref:1Z0-043.9.1.3)

Your database contains two temporary tablespaces named TEMP and TEMP1. The TEMP tablespace is the default temporary tablespace for the database, and the TEMP1 tablespace was created at database creation. You want to increase the size of the tempfile for the TEMP tablespace and drop the TEMP1 tablespace from the database. The database is not using Oracle-Managed Files (OMF).

Which statement must you use to ensure that when you drop the TEMP1 tablespace from the database, its corresponding operating system file is also deleted?

- `DROP TABLESPACE temp1;`
- `DROP TABLESPACE temp1 INCLUDING CONTENTS;`
- `DROP TABLESPACE temp1 INCLUDING CONTENTS AND DATAFILES;`
- `DROP TABLESPACE temp1 INCLUDING CONTENTS CASCADE CONSTRAINTS;`

Answer:

`DROP TABLESPACE temp1 INCLUDING CONTENTS AND DATAFILES;`

Explanation:

You must use the `DROP TABLESPACE temp1 INCLUDING CONTENTS AND DATAFILES` statement to delete both the tempfile from the TEMP1 tablespace and the corresponding operating system file simultaneously. If the database is using Oracle-Managed Files (OMF) when you drop the TEMP1 tablespace, the tempfile of the TEMP1 tablespace is automatically deleted from the operating system, and it is not necessary to specify the `INCLUDING CONTENTS AND DATAFILES` option.

The option stating that you must use the `DROP TABLESPACE temp1` statement to delete the corresponding operating system file for the TEMP1 tablespace is incorrect. In this scenario, OMF is not being used so this statement deletes the TEMP1 tablespace from the control file but does not delete its corresponding operating system file.

The option stating that you must use the `DROP TABLESPACE temp1 INCLUDING CONTENTS` statement to delete the corresponding operating system file for the TEMP1 tablespace is incorrect because the TEMP1 tablespace, not its corresponding operating system file, will be deleted using this statement. You must delete the operating system file by using an operating system command. When you drop a tablespace by using the `DROP TABLESPACEINCLUDING CONTENTS` statement, all the objects contained in this tablespace are deleted. A temporary tablespace does not contain any permanent objects. Therefore, this command will have the same effect as the `DROP TABLESPACE temp1` statement.

The option stating that you must use the `DROP TABLESPACE temp1 INCLUDING CONTENTS CASCADE CONSTRAINTS` statement to delete the TEMP1 tablespace and its corresponding operating system file is incorrect because the TEMP1 tablespace is dropped from the database, but the operating system file remains. You must delete the operating system file by using an operating system command. When you drop a tablespace by using the `DROP TABLESPACEINCLUDING CONTENTS CASCADE CONSTRAINTS` statement, the contents of the tablespace are deleted. All the referential integrity constraints from tables outside this tablespace are also dropped. Because a temporary tablespace does not contain any permanent objects, this command will have the same effect as the `DROP TABLESPACE temp1` statement.

Item: 5 (Ref:1Z0-043.9.3.5)

You have created an Oracle 10*g* database named SALES, which will be used by an application named SalesOrders.

Users of the SalesOrders application complain that application response time is slow when they generate reports. The SalesOrders application accesses a table that contains 10 million rows. You decide to create an index on this table using the NOLOGGING option so that the index creation process is completed in the least amount of time.

Which of the following is **NOT** true about an index created with the NOLOGGING option?

- The index can be changed from NOLOGGING to LOGGING.
- The index cannot be recovered even in the ARCHIVELOG mode.
- The index can only be created if the base table is created with the NOLOGGING option.
- The index can be recovered if you perform a backup after the CREATE INDEX statement.

Answer:

The index can only be created if the base table is created with the NOLOGGING option.

Explanation:

The option stating that the index can be created with the NOLOGGING option only if the base table is also created with the NOLOGGING option is not true. You can successfully create an index with the NOLOGGING option even if the base table is created with the LOGGING option. The NOLOGGING option primarily speeds up the index creation by not generating any redo entries.

The option stating that the index created with the NOLOGGING option can be changed any time to LOGGING is true. You can change from NOLOGGING to LOGGING, or vice versa, using the ALTER INDEX statement. When the index is changed from NOLOGGING to LOGGING, Oracle starts generating the redo entries in the online redo log files. When you change the index from LOGGING to NOLOGGING, Oracle stops generating the redo entries in the redo log files.

Because Oracle does not store redo information in the online redo log files for an index created with the NOLOGGING option, this index cannot be recovered even in ARCHIVELOG mode, unless you perform a backup after the index creation.

When an index is created with the NOLOGGING option, Oracle will not store the redo information in the online redo log files. Therefore, this index is not protected through the redo logs. However, you can recover this type of index if you perform a backup after creating this index.

Item: 6 (Ref:1Z0-043.9.5.5)

You are part of the DBA team working for a multinational bank. The team is responsible for performing administrative tasks on the database server located at the home office. The database server at the home office has a production database and a test database named TESTDB. The test database is primarily used for testing database commands and configuration settings before implementing these settings on the production database. The test database is also used for the development of database applications.

You have been asked by the senior DBA to grant the SYSDBA privilege to a new team member, John, so that he can perform some administrative tasks, such as shutdown and startup operations, on TESTDB. You use the password file to configure remote authentication on the TESTDB database.

You execute the following statement to grant the SYSDBA privilege to John:

```
SQL>GRANT SYSDBA TO john;
```

However, you receive the following error:

```
ORA-01996: GRANT failed: password file
'c:\oracle\ora9i\dbs\testdb.pwd' is full
```

Which action should you take to add the user john to the password file without removing any of the existing users?

- Create another password file and then re-execute the GRANT statement.
- Re-create the password file, specifying a larger number of allowed entries, and then re-execute the GRANT statement.
- Change the value of the REMOTE_LOGIN_PASSWORDFILE initialization parameter in the initialization parameter file to NONE and then re-execute the GRANT statement.
- Change the value of the REMOTE_LOGIN_PASSWORDFILE initialization parameter in the initialization parameter file to SHARED and then re-execute the GRANT statement.

Answer:

Re-create the password file, specifying a larger number of allowed entries, and then re-execute the GRANT statement.

Explanation:

You should re-create the password file, specifying a larger number of allowed entries, and then re-execute the GRANT statement. When you exceed the maximum number of users allowed in the password file, you must re-create the password file. When specifying the ENTRIES parameter in the ORAPWD command, you should allocate a larger number of allowed entries than required. This minimizes the chances of receiving an ORA-01996 error.

The option stating that you should create another password file and then re-execute the GRANT statement is incorrect because creating another password file will not resolve the ORA-01996 error. You need to shut down the database, remove the existing password file, and re-create the password file. When you re-create the password file, you must specify a larger value for the ENTRIES parameter in the ORAPWD command in order to avoid the ORA-01996 error.

The option stating that you should change the value of the REMOTE_LOGIN_PASSWORDFILE initialization parameter in the initialization parameter file to NONE and then re-execute the GRANT statement is incorrect. This is because the GRANT statement will fail. If the initialization parameter REMOTE_LOGIN_PASSWORDFILE is set to NONE, the database server will generate an error when you try to grant the SYSDBA or SYSOPER privilege to another user.

The option stating that you should change the value of the REMOTE_LOGIN_PASSWORDFILE initialization parameter in the initialization parameter file to SHARED and then re-execute the GRANT statement is incorrect. This is because if the REMOTE_LOGIN_PASSWORDFILE parameter changes to SHARED, you cannot add users to the password file. The only user allowed in the password file is SYS.

Item: 7 (Ref:1Z0-043.9.4.1)

Your database is in ARCHIVELOG mode. On Friday evening, you perform an online database backup by using the BACKUP DATABASE command at the Recovery Manager (RMAN) prompt and close the database.

On Monday, the System Administrator informs you about the failure of two hard disks. One of the lost disks contains two datafiles, HR1.DBF and HR2.DBF, both of which belong to a read/write tablespace named HR. The disk also contains a datafile, USERS.DBF, which belongs to a read/write tablespace named USERS.

You need to restore and recover the database backup that was performed on Friday evening. After mounting the database, you issue the following RMAN commands:

```
RMAN>RESTORE DATABASE;
RMAN>RECOVER DATABASE;
```

After successfully executing these RMAN commands, you issue the following statement using SQL*Plus:

```
SQL>ALTER DATABASE OPEN;
```

You receive the following errors when attempting to open the database:

```
ORA-01157: cannot identify/lock data file 10 see DBWR trace
file
ORA-01110: data file 10: 'D:\USERS.DBF'
```

What is the cause of these errors?

- The USERS.DBF datafile is corrupted and cannot be restored by RMAN.
- The USERS.DBF datafile was not backed up using the RMAN BACKUP DATABASE command.
- The USERS.DBF datafile was not restored using the RMAN RESTORE DATABASE command.
- The USERS.DBF datafile was not recovered using the RMAN RECOVER DATABASE command.

Answer:

The USERS.DBF datafile was not restored using the RMAN RESTORE DATABASE command.

Explanation:

In this scenario, the ORA-01157 and ORA-01110 errors occur because the USERS.DBF datafile was not restored by using the RESTORE DATABASE command through Recovery Manager (RMAN). The datafile belonging to a read-only tablespace requires special handling in the restore and recovery operations that use RMAN. By default, the read-only datafile is skipped in the restore and recovery operation when using RMAN. As a result, when you issue the RESTORE DATABASE command, all the datafiles of the database except the read-only datafile are restored. When you attempt to open the database, Oracle checks for the USERS.DBF datafile. When Oracle does not find the file, it generates the ORA-01157 and ORA-01110 errors.

You can use the following RMAN command to restore the missing datafiles belonging to a read-only tablespace:

```
RMAN>RESTORE DATABASE CHECK READONLY;
```

Alternatively, you can issue the following commands to explicitly restore and recover USERS.DBF from the RMAN backup set:

```
RMAN>RESTORE TABLESPACE USERS;
RMAN>RECOVER TABLESPACE USERS;
```

The option stating that the ORA-01157 and ORA-01110 errors occur because the USERS.DBF datafile is corrupted and cannot be restored through RMAN is incorrect because if RMAN encounters a corrupted file at the time of restoration, it will return an error stating that the file is corrupted. The question states that the RESTORE DATABASE statement has been executed successfully.

The option stating that the ORA-01157 and ORA-01110 errors occur because the USERS.DBF datafile was not backed up by using the RMAN BACKUP DATABASE command is incorrect. When you back up the database by using RMAN, the read-only tablespaces are backed up. If this is the first time you are backing up a read-only tablespace, RMAN backs up the read-only tablespace. If this is not the first backup, RMAN compares the System Change Number (SCN), which was recorded at backup, with the SCN that is generated when the tablespace was made read-only. If the SCN values are equal, RMAN does not back up

the read-only tablespace. If they are different, RMAN backs up the read-only tablespace.

The option stating that the ORA-01157 and ORA-01110 errors occur because the USERS.DBF datafile is not recovered by using the RMAN RECOVER DATABASE command is incorrect. The USERS.DBF datafile was backed up on Friday evening when it was read-only. The status of this file did not change to read/write before Monday. As a result, USERS.DBF does not require recovery because you are restoring a read-only tablespace from the backup that was performed when the file was read-only.

Item: 8 (Ref:1Z0-043.9.4.4)

Your database is configured in NOARCHIVELOG mode. Due to a media failure, you have lost one of the datafiles belonging to a read-only tablespace. You know that the last backup was performed after the tablespace was made read-only.

Which action should you take to restore the missing datafile in the minimum amount of time?

- Restore all the datafiles from the backup.
- Restore only the lost datafile from the backup.
- Restore all the datafiles for the lost tablespace from the backup.
- Restore all the datafiles for the lost tablespace and all the SYSTEM and SYSAUX datafiles from the backup.

Answer:

Restore only the lost datafile from the backup.

Explanation:

In the given scenario, you should restore only the lost datafile from the backup. This will recover the lost datafile in the minimum amount of time. Whether you are running your database in NOARCHIVELOG or ARCHIVELOG mode, you only need to restore the lost datafile for the read-only tablespace from the backup. This is because the tablespace is read-only and the backup you have was made after the tablespace was made read-only. Therefore, you can be sure that no changes would have been made to these read-only datafiles.

Restoring all the datafiles from the backup is not required. There is also no need to restore all the datafiles for the lost read-only tablespace from the backup. Both these options would require significantly more time and are not necessary because the datafiles for the read-only tablespace would not have changed since the last backup.

In NOARCHIVELOG mode, you cannot restore a database partially. You must restore all the database files and control files. Therefore, the option stating that in the given scenario, you should restore all the datafiles for the lost tablespace and the SYSTEM and SYSAUX datafiles from the backup is incorrect. You must restore all the datafiles and control files.

Item: 9 (Ref:1Z0-043.9.4.3)

In which of the following scenarios is a tablespace recovery required?

- when recovering a lost read-only tablespace from a read-only tablespace backup
- when recovering a lost read-only tablespace from a read-write tablespace backup when the database is running in ARCHIVELOG mode
- when recovering a lost read-only tablespace from a read-write tablespace backup when the database is running in NOARCHIVELOG mode and the changes in the online redo log files have been overwritten
- when recovering a lost read-only tablespace from a read-only tablespace backup using the backup of the control file, the control file was created using the ALTER DATABASE BACKUP CONTROLFILE TO TRACE statement, and this statement was issued when the tablespace was read-only

Answer:

when recovering a lost read-only tablespace from a read-write tablespace backup when the database is running in ARCHIVELOG mode

---

Explanation:

A tablespace recovery is required when recovering a lost read-only tablespace from a read-write tablespace backup when the database is running in ARCHIVELOG mode. When a tablespace status is changed from read-only to read-write or from read-write to read-only, the current System Change Number (SCN) is stamped in the tablespace's datafile and in the control file. When you restore the datafile for the lost tablespace, Oracle verifies the SCN stored in the datafile with the control file. If these SCNs are different, recovery is required for the tablespace.

The option stating that tablespace recovery is required when recovering a lost read-only tablespace from a read-only tablespace backup is incorrect. The SCN would not have been changed, and no transactions would have been applied to this tablespace if the tablespace was read-only.

In NOARCHIVELOG mode, if you try to recover a lost read-only tablespace from a read-write tablespace backup, a media recovery is required. You can only perform a media recovery in NOARCHIVELOG mode when the changes in the online redo log files have not been overwritten. If the online redo log files have been overwritten, you cannot recover the lost read-only tablespace. In this case, you need to restore all the database files and open the database. You also need to re-apply all the transactions since the backup to the lost tablespace. Therefore, the option stating that tablespace recovery is required when recovering a lost read-only tablespace from a read-write tablespace backup when the database is running in NOARCHIVELOG mode and the changes in the online redo log files have been overwritten is incorrect. In this scenario a tablespace recovery is not required, but rather a complete database restoration.

When you lose all the control files and a read-only tablespace, and if you have a backup of the read-only tablespace after it was made read-only, you can recover the database without performing any recovery for this tablespace. If you are recovering the database using the control trace file, then the information about the read-only tablespace is not present in the CREATE CONTROLFILE statement. The read-only tablespace is added to the database after recovery has been performed. The database is recovered without the lost read-only tablespace and you simply need to restore the lost tablespace. You only need to restore the lost read-only tablespace from the backup and run the control trace file. Therefore, the option stating that tablespace recovery is required when recovering a lost read-only tablespace from a read-only tablespace backup using the backup of the control file is incorrect.

Item: 10 (Ref:1Z0-043.9.4.2)

Your database is running in NOARCHIVELOG mode with two online redo log files. The SALES table contains sales information for the organization. The SALES table belongs to the SALESTB tablespace.

On Monday, you insert 10 rows into the SALES table. The current log sequence number is 14. You change the tablespace status from READ WRITE to READ ONLY for the SALESTB tablespace. You shut down the database and take a backup of the SALESTB tablespace.

On Tuesday, you start the database. You change the status for the SALESTB tablespace from READ ONLY to READ WRITE. You insert 10 more rows into the SALES table and shut down the database. The current log sequence number is 15.

When you try to open the database on Wednesday morning, you discover that the SALESTB tablespace was lost because of a media failure.

Which of the following options is true about recovering the SALES table?

- The SALES table cannot be recovered because the database is running in NOARCHIVELOG mode.
- The SALES table can be recovered by restoring the SALESTB tablespace from the backup and performing a media recovery.
- The SALES table can be recovered by restoring the SALESTB tablespace from the backup without performing any media recovery.
- The SALES table can be recovered by restoring the SALESTB tablespace from the backup, but the rows inserted on Tuesday need to be inserted again.

Answer:

The SALES table can be recovered by restoring the SALESTB tablespace from the backup and performing a media recovery.

Explanation:

The SALES table can be recovered by restoring the SALESTB tablespace from the backup and performing a media recovery. If you are recovering a read-write tablespace from a backup that was performed when the tablespace was read-only, you must perform a media recovery. For performing a media recovery, you must have all the necessary online redo log files. If you have all the online redo log files required for the recovery for this read-write tablespace, you can recover the tablespace from the read-only tablespace backup even in NOARCHIVELOG mode. In the given scenario, it is mentioned that on Monday after the rows are inserted into the SALES table, the log sequence number was 14. After changing the tablespace status from read-only to read-write and inserting 10 more rows into the SALES table on Tuesday, the log sequence number was 15. Therefore, in the given scenario, despite running the database in NOARCHIVELOG mode, you still have all the required changes in the online redo log files.

The option stating that the SALES table cannot be recovered because the database is running in NOARCHIVELOG mode is incorrect. This is because even in NOARCHIVELOG mode, you can recover the read-write tablespace from a read-only tablespace backup provided that the changes recorded in the online redo log files have not been overwritten.

In this scenario, the option stating that the SALES table can be recovered by restoring the SALESTB tablespace from the backup without performing any media recovery is incorrect.
The only time the recovery is not needed is when you are trying to recover a read-only tablespace from a backup that was performed when the tablespace was read-only. In this case, you only need to restore the tablespace and no recovery is required.

When you recover the SALESTB tablespace, all the rows inserted into the SALES table on Tuesday are automatically recovered when you perform the media recovery on the tablespace. Therefore, the option stating that the SALES table can be recovered by restoring the SALESTB tablespace from the backup but the rows inserted on Tuesday need to be inserted again is incorrect.

Item: 11 (Ref:1Z0-043.9.5.1)

You are working as a Database Administrator. Despite having a password in the data dictionary as `change_on_install`, you always log on to the database `MYNEWDB` using operating system authentication. Your organization is planning to recruit two junior-level DBAs. You decide to enable remote authentication in your database so that the new DBAs can log on to the database from their workstations to carry out administrative tasks.

To allow the new DBAs to perform the administrative tasks, you create a password file on the database server using the following command:

```
ORAPWD file=d:\oracle\ora9i\orapwU01 password=admin entries=4
```

After creating the password file, you remove the operating system authentication and change the value of the `REMOTE_LOGIN_PASSWORDFILE` parameter to `EXCLUSIVE`. You also create a net service name as `MYNEWDB` that allows the new DBAs to connect to the database server from their workstations using this net service name.

Which command must you use to connect to the database to start it?

- `CONNECT / AS SYSDBA`
- `CONNECT sys/admin AS SYSDBA`
- `CONNECT sys/admin@mynewdb AS SYSDBA`
- `CONNECT sys/change_on_install AS SYSDBA`

Answer:

`CONNECT sys/change_on_install AS SYSDBA`

Explanation:

You must use the `CONNECT sys/change_on_install AS SYSDBA` command to connect to the database `MYNEWDB`. When you create a password file using the `ORAPWD` utility, you must supply the password for the `SYS` user. Even if you supply an incorrect password in the `ORAPWD` command, you must use the original password for the `SYS` user when attempting to connect to the database.

The option stating that you must use the `CONNECT / AS SYSDBA` command to connect to the database is incorrect because you must provide the username and password in the `CONNECT` command when connecting to the database using remote authentication. Otherwise, an error is generated.

The option stating that you must use the `CONNECT sys/admin AS SYSDBA` command to connect to the database is incorrect because the password for the `SYS` user in the data dictionary is still stored as `change_on_install` and not `admin`. Therefore, this command will also generate an error.

The option stating that you must use the `CONNECT sys/admin@mynewdb AS SYSDBA` command to connect to the database is incorrect because a net service name is required when you are connecting to the remote database. You can also use a net service name to connect to the local database. However, you will receive an error when you try to connect to either the local or remote database using this command because you are specifying an incorrect password for the `SYS` user in the `CONNECT` command.

Item: 12 (Ref:1Z0-043.9.2.3)

Your database is in ARCHIVELOG mode. You have two online redo log groups each of which contains one redo member. When you attempt to start the database, you receive the following errors:

```
ORA-00313: open failed for members of log group 1 of thread 1
ORA-00312: online log 1 thread 1: 'D:\REDO01.LOG'
```

You discover that the online redo log file of the current redo group is corrupted.

Which statement should you use to resolve this issue?

- SQL>ALTER DATABASE DROP LOGFILE GROUP 1;
- SQL>ALTER DATABASE CLEAR LOGFILE GROUP 1;
- SQL>ALTER DATABASE CLEAR UNARCHIVED LOGFILE GROUP 1;
- SQL>ALTER DATABASE DROP LOGFILE MEMBER 'D:\REDO01.LOG';

Answer:

SQL>ALTER DATABASE CLEAR UNARCHIVED LOGFILE GROUP 1;

Explanation:

You should use the ALTER DATABASE CLEAR UNARCHIVED LOGFILE GROUP 1 statement to clear the corrupted online redo log file. When you issue this statement, the contents of the online redo log file are cleared and the log file is initialized. Because the log file has not been archived, the UNARCHIVED keyword is used. This keyword overrides archiving of the online redo log file in redo group 3, and the cleared redo log files become available for use.

The option stating that you will use the ALTER DATABASE DROP LOGFILE GROUP 1 statement to resolve the corrupted online redo log file is incorrect because if you attempt to drop the online redo log group that belongs to a current redo group, you will receive the following errors:

```
ORA-01623: log 1 is current log for thread 1 cannot drop
ORA-00312: online log 1 of thread 1: 'D:\REDO01.LOG'
```

The option stating that you will use the ALTER DATABASE CLEAR LOGFILE GROUP 1 statement to resolve the corrupted online redo log file is incorrect because if you attempt to clear an online redo log file that must be archived without using the UNARCHIVED keyword, you will receive the following errors:

```
ORA-00350: log 1 of thread 1 needs to be archived
ORA-00312: online log 1 thread 1: 'D:\REDO01.LOG'
```

The option stating that you will use the ALTER DATABASE DROP LOGFILE MEMBER 'D:\REDO01.LOG' statement to resolve the corrupted online redo log file is incorrect because Oracle does not allow you to drop an online redo log member that belongs to an active or current redo group. Therefore, if you attempt to drop such a member, you will receive the following error:

```
ORA-00361: cannot remove last log member 'D:\redo01.log for group
1'
```

Item: 13 (Ref:1Z0-043.9.1.5)

Your database contains a temporary tablespace, index tablespace, undo tablespace, and a read-only tablespace apart from the SYSTEM and SYSAUX tablespaces. If a media failure occurs resulting in the loss of any of these tablespaces, which tablespace is **NOT** required for the database to start?

- undo tablespace
- index tablespace
- read-only tablespace
- temporary tablespace

Answer:

temporary tablespace

Explanation:

A temporary tablespace is not mandatory when the database is started. A temporary tablespace is primarily used for sort operations in the database, such as queries involving join conditions, ORDER BY clauses, and GROUP BY clauses and index building. A temporary tablespace does not store permanent objects. If a temporary tablespace does not exist when the database is started, the DBWn background process writes to the alert log and the DBWn trace file indicates that the temporary tablespace is missing. For example, when the default temporary tablespace in the database becomes inaccessible due to missing datafile, a message will be written to the alert log file indicating the missing status of the tablespace. In this scenario, you should create a new temporary tablespace and assign it as the default temporary tablespace for the database. Later the temporary tablespace with a missing datafile can be dropped. However, the database is started normally. In the event of loss of a temporary tablespace, the database users might not be able to run queries or create indexes until they have been assigned a new temporary tablespace.

If your database is configured with an undo tablespace, you cannot start your database if the undo tablespace does not exist. An undo tablespace must be available for the database to open and therefore, your database will not start if the undo tablespace is missing.

You are unable to start your database if your index tablespace is missing. For a database to open all the permanent tablespaces that are online in the database must be available.

You are unable to start your database if a read-only tablespace is missing. For a database to open all the permanent tablespaces that are online in the database must be available.

Item: 14 (Ref:1Z0-043.9.5.3)

You are a Database Administrator with WonderWeb. You use a password file to establish connections to the Sales database located on the server. You created the password file using the following command:

```
ORAPWD file=d:\oracle\ora9i\orapwU01 password=admin entries=4
```

You erroneously deleted the password file while the database was running. You re-create the password file using the following command:

```
ORAPWD file=d:\oracle\ora9i\orapwU01 password=change_on_install
entries=4
```

However, when you try to connect as the SYS user, you receive the following error:

```
ORA-01031: insufficient privileges
```

What should you do to resolve this error?

- Delete the newly created password file and re-create another password file with the password admin, without shutting down the database.
- Enable the operating system authentication, shut down the database, disable the operating system authentication, and restart the database using the password file.
- Enable the operating system authentication, shut down the database, re-create the password file using the same ORAPWD command, and restart the database using the password file.
- Delete the newly created password file, enable operating system authentication and shut down the database. Then, re-create another password file using the same ORAPWD command and restart the database using this password file.

Answer:

Delete the newly created password file, enable operating system authentication and shut down the database. Then, re-create another password file using the same ORAPWD command and restart the database using this password file.

Explanation:

In this scenario, you should delete the newly created password file, enable operating system authentication, and shut down the database. Then, you should re-create another password file using the same ORAPWD command and restart the database using this password file. You should not remove or modify the password file when the database is mounted or opened and the REMOTE_LOGIN_PASSWORD parameter is set to a value other than NONE. If the password file is deleted or changed, you must re-create another password file. However, you must re-create the password file after shutting down the database. If you re-create the password file without shutting down the database, you cannot connect to the database using the password file. Moreover, if the password file is not available and remote authentication is enabled using the password file, you cannot connect to the database using the SYSDBA or SYSOPER privilege. Therefore, you must log into the database using operating system authentication and then shut down the database.

The option stating that you should delete the newly created password file and re-create another password file with the password admin, without shutting down the database is incorrect because re-creating the password file requires restarting the database at least once. To restart your database you must use an authentication method, and as the password file is missing you cannot use password file authentication. Therefore, you must enable operating system authentication to connect to the database.

The option stating that you should enable the operating system authentication and shut down the database and then restart the database using the password file is incorrect because shutting down and restarting the database will not resolve the error. You must re-create another password file after shutting down the database.

The option stating that you should enable the operating system authentication and shut down the database, re-create the password file using the same ORAPWD command, and restart the database using the password file is incorrect. The operating system will not allow you to re-create the password file with the same name without deleting the newly created password file.

Item: 15 (Ref:1Z0-043.9.5.2)

You are a Database Administrator with TXGlobal. You use a password file to establish remote connections to the HR database on the server located at the home office. Currently, two active remote sessions exist to this database. These sessions were established using the SYSDBA privilege from the remote machines. You accidentally deleted the password file.

What will be the consequence of this action?

- Both the sessions will be killed, and no new sessions will be created using the SYSDBA or SYSOPER privilege.
- Both the sessions will remain active, but no new sessions will be created using the SYSDBA or SYSOPER privilege.
- Both the sessions will be killed, but new sessions will be created using the SYSDBA or SYSOPER privilege when the database restarts.
- The database will crash, and no new sessions will be created using the SYSDBA or SYSOPER privilege when the database restarts.

Answer:

Both the sessions will remain active, but no new sessions will be created using the SYSDBA or SYSOPER privilege.

Explanation:

When two sessions are active and a password file is deleted, both the sessions will remain active, but no new sessions will be created using the SYSOPER or SYSDBA privilege. You must re-create the password file and then restart the database at least once. The password file will not be used to connect to the database until you restart the database.

The option stating that both the sessions will be killed, and no new sessions will be created using the SYSDBA or SYSOPER privilege is incorrect because deleting the password file will not kill the connected sessions.

The option stating that both the sessions will be killed, but new sessions will be created using the SYSDBA or SYSOPER privilege when the database restarts is incorrect because deleting the password file will not kill the connected users' sessions. Moreover, the users will not be able to connect to the database using the SYSDBA or SYSOPER privilege until you re-create the password file.

The option stating that the database will crash, and no new sessions will be created using the SYSDBA or SYSOPER privilege when the database restarts is incorrect because deleting the password file will not cause the database instance to crash.

Item: 16 (Ref:1Z0-043.9.3.2)

The ORDERS table in the database of a company contains one million records. The table is stored in the DATA tablespace and the index created on the ORDERS table is stored in the index tablespace named INDEXES. On Monday, you failed to start the database because the datafiles of the INDEXES tablespace were missing. You dropped and recreated the INDEXES tablespace by issuing the following command:

```
SQL>DROP TABLESPACE INDEXES INCLUDING CONTENTS;

SQL> CREATE TABLESPACE INDEXES DATAFILE
'C:\ORACLE\ORADATA\ORA101t\INDEX01.DBF' SIZE 50m;
```

After that, you issued the following command to recreate the index:

```
CREATE UNIQUE INDEX sales_index_pk
ON sales
(order_id)
PCTFREE 10
INITRANS 2
MAXTRANS 255
TABLESPACE indexes
STORAGE (
INITIAL 1m
NEXT 1m
PCTINCREASE 0
MINEXTENTS 1
MAXEXTENTS 8192
)
NOLOGGING
PARALLEL( degree 4)
```

Which two clauses are responsible for reducing the time for the recreation of the index? (Choose two.)

- ☐ PCTFREE
- ☐ MAXTRANS
- ☐ PCTINCREASE
- ☐ INITIAL
- ☐ NOLOGGING
- ☐ PARALLEL

Answer:

NOLOGGING
PARALLEL

Explanation:

The NOLOGGING and the PARALLEL clauses are used to reduce the time for the recreation of the index. The NOLOGGING clause will not create the redo information; therefore, a backup should be performed immediately after the index is created. The PARALLEL clause in the CREATE INDEX command specifies that multiple processes can work simultaneously to create an index. By dividing the task of creating the index among multiple server processes, the Oracle Server can create the index faster than a single server process.

The option stating that the PCTFREE clause is used to reduce the index build time is incorrect. The PCTFREE clause is used to specify the percentage area of a block that must be left free for future updates in the block.

The option stating that the MAXTRANS clause is used to reduce the index build time is incorrect. The MAXTRANS clause is used to specify the maximum number of transactions that can work simultaneously on a block.

The option stating that the PCTINCREASE clause is used to reduce the index build time is incorrect. The PCTINCREASE clause is the storage clause of the CREATE INDEX command and is used to specify that the index will occupy more space each time an extent is required.

The option stating that the `INITIAL` clause is used to reduce the index build time is incorrect. The `INITIAL` clause is the storage clause of the `CREATE INDEX` command and is used to specify the size of the initial extent in the index segment.

Item: 17 (Ref:1Z0-043.9.2.5)

You are working on the PROD database, which is in NOARCHIVELOG mode. You lost the active online redo log group due to a media failure.

How should you recover your database?

- Restore the database from a whole consistent backup and start the database in MOUNT mode. Then, open the database with the RESETLOGS option after performing a cancel-based recovery.
- Restore the database from a whole consistent backup and start the database in MOUNT mode. Then, drop the lost redo log group and open the database with the RESETLOGS option after performing a cancel-based recovery.
- Restore the database from a whole consistent backup and start the database in MOUNT mode. Then, clear the lost redo log group and open the database with the RESETLOGS option after performing a cancel-based recovery.
- Do nothing. You do not need to recover the database in this case; an instance recovery will be performed by the SMON process on startup.

Answer:

Restore the database from a whole consistent backup and start the database in MOUNT mode. Then, open the database with the RESETLOGS option after performing a cancel-based recovery.

Explanation:

If you lose an active redo log group while your database is up and running, the database crashes. However, if your active redo group is lost in a database running in NOARHCHIVELOG mode because of a media failure, you can recover the database by performing the following steps:

1. Restore the datafiles and the control files from the most recent consistent whole database backup.
2. Mount the database.
3. Perform a cancel-based recovery.
4. Open the database with the RESETLOGS option.

The option stating that the redo log group must be dropped and opened with *RESETLOGS* option after performing a cancel-based recovery is incorrect because you cannot drop an active redo log group. You can drop a redo log group or a group member only if it is inactive.

You cannot clear an online redo log group or a group member if it is active. Therefore, the option stating that the redo log group must be cleared and the database opened with the RESETLOGS option after performing a cancel-based recovery is an invalid option.

If your database is in NOARCHIVELOG mode and you lost all the members of an active redo group, you cannot open the database without performing an incomplete recovery. Moreover, the instance recovery is performed by the SMON process when the database state changes from MOUNT mode to OPEN mode. Therefore, in this scenario, this option is incorrect because the database state cannot be changed to OPEN mode unless you perform an incomplete recovery.

Item: 18 (Ref:1Z0-043.9.2.4)

You are operating your database in the manual archiving mode. Currently, your database is configured with the following online redo log groups and members:

Redo log files:

Group1	'/disk1/oradata/redo01a.log'
	'/disk1/oradata/redo01b.log'
Group2	'/disk2/oradata/redo02a.log'
	'/disk2/oradata/redo02b.log'

You tried to drop Group 1 from the database but received the following errors:

```
ORA-01623: log 1 is current log for thread 1 cannot drop
ORA-00312: online log 1 thread 1:
'D:\ORACLE\ORADATA\TESTDB\REDO01a.LOG'
```

What might be the reason for these errors?

- Group 1 is an active or current online redo log group.
- Group 1 is an inactive online redo group that has not been archived yet.
- The members of the Group 1 are temporarily asymmetric with the members of other groups.
- The size of the online redo log members of Group 1 is different from the size of the members in other groups.

Answer:

Group 1 is an active or current online redo log group.

Explanation:

You cannot drop an active or current online redo log group from the database. The errors `ORA-01623` and `ORA-00312` are raised when you try to drop an active or current online redo log group. If you want to drop an active or current redo log group, you must first force a log switch and then, ensure that the log is archived, if archiving is enabled.

You cannot drop even an inactive online redo group if the group has not finished archiving. Attempting to do so will result in the same `ORA-01623` and `ORA-00312` errors, but with a different error message that is as follows:

```
ORA-01623: log 1 of thread 1 needs to be archived
ORA-00312: online log 1 thread 1:
'D:\ORACLE\ORADATA\TESTDB\REDO01a.LOG'
```

You can successfully drop an online redo log group even if its members are temporarily asymmetric with the members of the other groups provided that the group that you are dropping is not an active or current group and has finished archiving, if archiving is enabled.

You can drop an online redo group without any errors if the size of the members of the group you want to drop is different from the size of the members in other groups. However, you cannot drop this group if it is an active or current group. If archiving is enabled, you cannot drop the redo group if it has not been archived yet.

Item: 19 (Ref:1Z0-043.9.2.2)

Your database is in manual archive mode. Your online redo log groups are configured as follows:

Disk 1	Disk 2	Disk 3
REDO01A.LOG	REDO01B.LOG	REDO01C.LOG
REDO02A.LOG	REDO02B.LOG	REDO02C.LOG
REDO03A.LOG	REDO03B.LOG	REDO03C.LOG

You discover that DISK 3 has encountered a media failure that has resulted in a loss of all the multiplexed copies of online redo log files.

You decide to delete the REDO01C.LOG, REDO02C.LOG, and REDO3C.LOG files to prevent the LGWR background process from attempting to access these files. When you query the V$LOG dynamic view, you receive the following output:

```
SQL> SELECT group#, archived, status FROM v$log;

    GROUP# ARC   STATUS
    ------ ---   --------
         1 NO    CURRENT
         2 YES   INACTIVE
         3 NO    INACTIVE
```

Which sequence of statements should you use to drop the missing online redo log files from the database?

```
1.  ALTER DATABASE DROP LOGFILE MEMBER 'E:\REDO01C.LOG';
2.  ALTER SYSTEM SWITCH LOGFILE;
3.  ALTER DATABASE DROP LOGFILE MEMBER 'E:\REDO03C.LOG';
4.  ALTER SYSTEM ARCHIVE LOG GROUP 3;
5.  ALTER DATABASE DROP LOGFILE MEMBER 'E:\REDO02C.LOG';
6.  ALTER SYSTEM ARCHIVE LOG GROUP 1;
```

- 5, 3, 2, and 1
- 1, 5, 3, and 2
- 4, 3, 2, 5, 1, and 6
- 5, 4, 3, 2, 6, and 1

Answer:

5, 4, 3, 2, 6, and 1

Explanation:

You cannot drop a redo log member that belongs to an active or current online redo log group. If you attempt to drop a redo log member from an active group, you will receive the following errors:

```
ORA-01623: log 1 is current log for thread - cannot drop
ORA-00312: online log 1 thread 1: 'E:\REDO01C.LOG'
```

You must force a log switch before you drop a redo log member that belongs to an active or current redo group.

If archiving is enabled, you must ensure that the archiving for the online redo log group is complete before you drop its member. If you attempt to drop a redo log member from a group that has not yet been archived, you will receive the following errors:

```
ORA-01623: log 1 of thread 1 needs to be archived
ORA-00312: online log 1 thread 1: 'E:\REDO03C.LOG'
```

In this scenario, you can issue the following sequence of statements to drop the missing online redo log files from the database:

Drop the redo member 'E:\REDO02B.LOG' by using the ALTER DATABASE DROP LOGFILE MEMBER 'E:\REDO02B.LOG' statement. The status of the online redo log member 'E:\REDO02c.LOG' is INACTIVE and the member is archived.

The online redo log member 'E:\REDO03C.LOG' has not been archived. Archive this member by using the ALTER SYSTEM ARCHIVE LOG GROUP 3 statement.

Drop the redo member 'E:\REDO03C.LOG' by using the ALTER DATABASE DROP LOGFILE MEMBER 'E:\REDO03C.LOG' statement.

The online redo log group 1 is active. You cannot drop the redo member 'E:\REDO01C.LOG' because it belongs to the active group 1. Use the ALTER SYSTEM SWITCH LOGFILE statement to force a log switch.

Archive the online redo log member 'E:\REDO01C.LOG' by using the ALTER SYSTEM ARCHIVE LOG GROUP 1 statement.

Drop the redo log member 'E:\REDO01C.LOG' from the database by using the ALTER DATABASE DROP LOGFILE MEMBER 'E:\REDO01C.LOG' statement.

However, the sequence is not the only possible sequence to solve the problem. You can archive the log group 3, drop it first, and then drop the log group 2 which has been archived.

All the other options are incorrect.

Item: 20 (Ref:1Z0-043.9.4.5)

Adam is working as a Database Administrator (DBA) for TeleSoft Corporation. His database is running in the ARCHIVELOG mode. During database startup, he discovers that one of the disks crashed, resulting in the permanent loss of a read-write USERS tablespace. The USERS01.dbf datafile belongs to the USERS tablespace and is 500 MB in size. He needs to recover the USERS tablespace from the backup. While reviewing the backup details, he discovers that the most recent available backup is five days old. This backup was taken when the USERS tablespace was read-only.

After correcting the hardware problem that caused the failure, what should Adam do to recover the USERS tablespace?

- Restore the USERS01.dbf file from the backup, and open the database using the STARTUP command.
- Restore the USERS01.dbf file using the RECOVER TABLESPACE command, and open the database using the ALTER DATABASE OPEN statement.
- Restore the USERS01.dbf file from the backup, recover the USERS tablespace using the RECOVER TABLESPACE command, and open the database using the ALTER DATABASE OPEN statement.
- Restore the USERS01.dbf file from the backup and change the status of the USERS tablespace from read-only to read-write using the ALTER TABLESPACE USERS READ WRITE statement. Then, recover the USERS tablespace using the RECOVER TABLESPACE command, and open the database using the ALTER DATABASE OPEN statement.

Answer:

Restore the USERS01.dbf file from the backup, recover the USERS tablespace using the RECOVER TABLESPACE command, and open the database using the ALTER DATABASE OPEN statement.

Explanation:

Adam should restore the USERS01.dbf file from the backup, recover the USERS tablespace using the RECOVER TABLESPACE command, and open the database using the ALTER DATABASE OPEN statement. If you have all the necessary redo logs or archived redo logs, you can recover a tablespace to the state it was when the media failure occurred. However, to recover a read-write tablespace from a read-only tablespace backup, you need to restore the datafiles for this tablespace from the backup. Next, you need to recover the tablespace using the RECOVER TABLESPACE command. Finally, you need to open the database using the ALTER DATABASE OPEN statement.

After restoring the lost tablespace from the backup, you cannot open the database unless you perform recovery on the tablespace. Doing so will return an error message specifying that the tablespace needs a media recovery.

Recovering the lost tablespace using the RECOVER TABLESPACE command without restoring the tablespace from the backup is an invalid option.

You cannot change the status of the tablespace from read-only to read-write, or vice versa, without opening the database. Therefore, the ALTER TABLESPACE USERS READ WRITE statement will fail if it is executed at the mount stage.

Item: 21 (Ref:1Z0-043.9.5.4)

You have created a password file using the following command:

```
ORAPWD file=d:\oracle\ora9i\orapwU01 password=change_on_install
entries=3
```

Which of the following is true about this password file?

- If the REMOTE_LOGIN_PASSWORDFILE parameter is set to SHARED in the initialization parameter file, then a maximum of three users can be granted the SYSDBA or SYSOPER privileges.
- If the REMOTE_LOGIN_PASSWORDFILE parameter is set to EXCLUSIVE in the initialization parameter file, then a maximum of three users can be granted the SYSDBA or SYSOPER privileges.
- If the REMOTE_LOGIN_PASSWORDFILE parameter is set to SHARED in the initialization parameter file, then the SYSDBA and SYSOPER privileges can be granted to other users as long as space in the password file is available.
- If the REMOTE_LOGIN_PASSWORDFILE parameter is set to EXCLUSIVE in the initialization parameter file, then the SYSDBA and SYSOPER privileges can be granted to other users as long as space in the password file is available.

Answer:

If the REMOTE_LOGIN_PASSWORDFILE parameter is set to EXCLUSIVE in the initialization parameter file, then the SYSDBA and SYSOPER privileges can be granted to other users as long as space in the password file is available.

Explanation:

If the REMOTE_LOGIN_PASSWORDFILE parameter is set to EXCLUSIVE in the initialization parameter file, then the SYSDBA and SYSOPER privileges can be granted to other users as long as space in the password file is available.

You have created the password file using the following command:

```
ORAPWD file=d:\oracle\ora9i\orapwU01 password=change_on_install
entries=3
```

With this command, ideally three users are allowed to be added to the password file. However, you can continue to add users to the password file until the operating system block size is full. The value of the entries parameter in the ORAPWD utility specifies that three users can be granted the SYSDBA or SYSOPER privilege. If your operating system block size is 512 bytes, then the password file can store only four entries.

The option stating that if the REMOTE_LOGIN_PASSWORDFILE parameter is set to SHARED in the initialization parameter file, then a maximum of three users can be granted the SYSDBA or SYSOPER privileges is incorrect. Users cannot be granted the SYSDBA or SYSOPER privilege when the REMOTE_LOGIN_PASSWORDFILE parameter is set to SHARED.

The option stating that if the REMOTE_LOGIN_PASSWORDFILE parameter is set to EXCLUSIVE in the initialization parameter file, then a maximum of three users can be granted the SYSDBA or SYSOPER privileges is incorrect because you can continue to add users to the password file until the operating system block size is full. This means that the password file could contain four users if the space permits.

The option stating that if the REMOTE_LOGIN_PASSWORDFILE parameter is set to SHARED in the initialization parameter file, then the SYSDBA and SYSOPER privileges can be granted to other users if there is space in the password file is incorrect because you cannot grant the SYSDBA and SYSOPER privileges to other users when the REMOTE_LOGIN_PASSWORDFILE is set to SHARED.

Item: 22 (Ref:1Z0-043.9.3.1)

You are maintaining your database in Oracle10*g*. You find that the INDEXES index tablespace should be recovered. How will you recover the index tablespace?

- by using the Flashback Database feature
- by using RMAN incomplete recovery
- by performing a user-managed incomplete recovery
- by dropping and re-creating the index tablespace

Answer:

by dropping and re-creating the index tablespace

Explanation:

You will recover the INDEXES index tablespace by dropping and re-creating the index tablespace. If the index tablespace should be recovered, you should compare the time it would take to rebuild all the indexes in the tablespace with the time it would take to restore and recover the datafiles. If the indexes can be easily re-created by using a script, then complete the following steps:

1. Execute the following statement when the index tablespace is dropped and the instance continues to run:

```
SQL> DROP TABLESPACE INDEXES INCLUDING CONTENTS AND DATAFILES;
```

2. Re-create the INDEXES tablespace.

```
SQL> CREATE TABLESPACE INDEXES
   DATAFILE <path> SIZE <value>;
```

3. Re-create all the indexes in the new tablespace.

The option stating that you will recover the INDEXES index tablespace by using the Flashback Database feature is incorrect. Flashback Database is a new feature in Oracle 10*g* that allows you to quickly restore the entire database to its previous state.

The option stating that you will recover the INDEXES tablespace by using RMAN based incomplete recovery is incorrect. You need not perform the recovery to recover the index tablespace. You can drop and re-create the index tablespace. An RMAN-based incomplete recovery is performed when you are required to recover a dropped table that is purged from the Recycle Bin or to recover the database when all the control files are missing.

The option stating that you will recover the INDEXES tablespace by using a user-managed incomplete recovery is incorrect. You need not perform the recovery to recover the index tablespace. You can drop and re-create the index tablespace. A user-managed incomplete recovery is performed if you are required to recover a dropped table that is purged from the Recycle Bin or to recover the database when all the control files are missing. A user-managed incomplete recovery is performed by copying the files to the desired location using operating system commands.

Item: 23 (Ref:1Z0-043.9.3.4)

Your database is in ARCHIVELOG mode. You lost an index tablespace due to a disk failure while the database was open. You have neither a backup of the lost index tablespace nor the scripts containing the CREATE INDEX statements to recreate the indexes. Currently, several users are executing long-running queries on the database.

What will happen to the ongoing activity in the database?

- The queries that are currently executing will abort and an error message will be returned to the user.
- The queries that are currently executing will execute normally but future queries will not executed.
- Data Manipulation Language (DML) statements cannot be performed on the tables on which the indexes are based.
- The currently executing and future queries will execute normally, but will be slower.

Answer:

The currently executing and future queries will execute normally, but will be slower.

Explanation:

If an index tablespace is lost, currently executing and future queries will execute normally except that the queries will be slower. Indexes are used to speed up query execution time. When the indexes are unavailable, the performance of the queries will be affected. This means that the queries will now take more time to complete.

The option stating that currently executing queries will be aborted and an error message will be returned to the user is incorrect. If the index is unavailable, the queries that are already running will not abort. These queries execute normally but will take more time to complete.

The option stating that currently executing queries will be execute normally but future queries will not be executed is incorrect. The loss of the index tablespace only increases the query response time but does not prevent the query from executing.

The option stating that the DML statements cannot be performed on the tables on which indexes are based is incorrect because both queries and DML statements, such as INSERT, UPDATE and DELETE, continue to modify the data in the base tables.

Database Recovery

Item: 1 (Ref:1Z0-043.13.1.4)

You are working as a DBA in a company. The datafiles in the database are as follows:

Tablespace	Datafiles	Mode
SYSTEM	SYSTEM01.dbf	Read/write
SYSAUX	SYSAUX01.dbf	Read/write
INDEX	INDEX.dbf	Read/write
UNDO	UNDO.dbf	Read/write
DATA	DATA1.dbf	Read/write
	DATA2.dbf	Read-Only
	DATA3.dbf	Read-Only

On Monday, you tried to start up the database but failed because all the control files were missing. You recreated the control file using the script you have created by issuing the ALTER DATABASE BACKUP CONTROLFILE TO TRACE command.

What is the prerequisite for recreating the control file?

- All the datafiles should be listed in the CREATE CONTROLFILE statement.
- The DATA2.dbf and DATA3.dbf datafiles should be listed in the CREATE CONTROLFILE statement.
- The SYSTEM01.dbf datafile should be listed in the CREATE CONTROLFILE statement.
- The SYSAUX01.dbf datafile should be listed in the CREATE CONTROLFILE statement.

Answer:

The DATA2.dbf and DATA3.dbf datafiles should be listed in the CREATE CONTROLFILE statement.

Explanation:

If all the control files are missing and the backup control file is unavailable for recovery, then you can execute a script created by issuing the ALTER DATABASE BACKUP CONTROLFILE TO TRACE command. The read-only files should not be listed in the script because no recovery is required for these files. After recreating the control file, when you attempt to mount and open the database, then the database checks the data-dictionary against the datafiles listed in the control file. The files that were not listed in the CREATE CONTROLFILE statement but are available in the data-dictionary have entries in the control file. These files are marked as MISSINGnnnnn, where nnnnn is a five digit number. After opening the database, you must rename the read-only datafiles whose names are prefixed with MISSINGnnnnn by using the ALTER DATABASE RENAME FILE statement.

The option stating that all the datafiles should be listed in the CREATE CONTROLFILE statement is incorrect. This is because the read-only datafiles should not be listed in the CREATE CONTROLFILE statement.

The option stating that the SYSTEM01.dbf datafile should not be listed in the CREATE CONTROLFILE statement is incorrect. This is because SYSTEM01.dbf is the datafile related to the SYSTEM tablespace. The datafiles related to the SYSTEM tablespace must be listed in the CREATE CONTROLFILE statement.

The option stating that the SYSAUX01.dbf datafile should not be listed in the CREATE CONTROLFILE statement is incorrect. This is because SYSAUX01.dbf is the datafile related to the SYSAUX tablespace. The datafiles related to the SYSAUX tablespace must be listed in the CREATE CONTROLFILE statement.

Item: 2 (Ref:1Z0-043.13.2.3)

In which scenario will you perform an incomplete recovery?

- when a table is dropped and stored in the Recycle Bin
- when all the control files are deleted
- when a member of a multiplexed redo log group is dropped
- when you are required to recover a table to its previous state

Answer:

when all the control files are deleted

Explanation:

You will perform an incomplete recovery when all the control files are deleted. You be required to perform an incomplete recovery from the last full database backup. All the transactions since the last backup will be lost.

The option stating that you will perform the incomplete recovery when a table is dropped and stored in the Recycle Bin is incorrect. You need not perform the incomplete recovery to recover the dropped table. When you drop a table, the table is not dropped from the database but stored in the Recycle Bin. If the table exists in the Recycle Bin then you can recover the dropped table by using the Flashback Drop feature. If you are recovering a dropped table that is purged from the Recycle Bin, then you must restore all the datafiles from the last backup and perform the incomplete recovery.

The option stating that you will perform an incomplete recovery when a member of a multiplexed redo log group is dropped is incorrect. If a member of a redo log group that is multiplexed is dropped, you can recover the member by copying the multiplexed image to the desired location.

The option stating that you will perform an incomplete recovery when you are required to recover a table to its previous state is incorrect. You need not perform the incomplete recovery when you are required to recover a table to its previous state. You can use the Flashback Table feature to recover a table to its previous state. The Flashback Table feature allows you to recover one or more tables to a specific point in time without performing time-consuming recovery operations, such as point-in-time recovery, which may also affect the availability of the rest of the database. The Flashback Table feature recovers the table by rolling back only the changes made to the tables or to their dependent objects, such as indexes.

Item: 3 (Ref:1Z0-043.13.1.1)

In which scenario will you issue the following command?

```
SQL> RECOVER DATABASE UNTIL TIME '2005-10-04 : 12:09:08' USING
   BACKUP CONTROLFILE;
```

- when all the control files are missing and only a binary backup of the current control file exists
- when a multiplexed copy of the current control file is missing
- when all the control files are missing and only a script containing the `CREATE CONTROLFILE` statement exists
- when the `SPFILE` is missing

Answer:

when all the control files are missing and only a binary backup of the current control file exists

---

Explanation:

You will issue the `RECOVER DATABASE UNTIL TIME '2005-10-04 : 12:09:08' USING BACKUP CONTROLFILE;` command when all the control files are missing and only the binary backup of the control file exists. You are recovering the database to a previous point in time. The restored database has a different structure from the current database.

The option stating that you will issue the `RECOVER DATABASE UNTIL TIME '2005-10-04 : 12:09:08' USING BACKUP CONTROLFILE;` command when a multiplexed copy of the current control file is missing is incorrect. If a multiplexed copy of the current control file is missing, you can perform the recovery by copying the multiplexed image to the desired location.

The option stating that you will issue the `RECOVER DATABASE UNTIL TIME '2005-10-04 : 12:09:08' USING BACKUP CONTROLFILE;` command when all the control files are missing and only a script containing the `CREATE CONTROLFILE` statement exists is incorrect. If all the control files are missing and you have only the script containing the `CREATE CONTROLFILE` statement, then you will create the new control file by executing the script at the SQL prompt.

The option stating that you will issue the `RECOVER DATABASE UNTIL TIME '2005-10-04 : 12:09:08' USING BACKUP CONTROLFILE;` command when the `SPFILE` is missing is incorrect. When the `SPFILE` is missing, you can recreate the `SPFILE` by using the `CREATE SPFILE FROM PFILE` statement.

Item: 4 (Ref:1Z0-043.13.1.5)

You are maintaining the PROD database for NetFx Corporation. You have configured controlfile autobackup in your database. At 6:00 P.M. on Monday, you issue the following command:

```
RMAN>BACKUP DATABASE;
```

At 8:00 A.M. on Tuesday, you are unable to start the database because all the control files are missing. You decide to restore the control files from the backup by using the `RMAN> RESTORE CONTROLFILE FROM AUTOBACKUP;` command.

Which operation should you perform before using the `RMAN> RESTORE CONTROLFILE FROM AUTOBACKUP;` command?

- Start the database in the MOUNT stage.
- Back up the control file to trace.
- Set the DBID.
- Issue the RECOVER DATABASE command.

Answer:

Set the DBID.

Explanation:

Before restoring the control file from the autobackup, you are required to specify the database ID (DBID) to identify the database that you are connecting to. The control file contains information about the database ID, and the failure makes the control file unavailable. The syntax for specifying the database ID is as follows:

```
RMAN>SET DBID database_id;
```

The option stating that you must start the database in the MOUNT stage before restoring the control file is incorrect. This is because the control file is used to start the database in the MOUNT stage. You are required to start the database in the MOUNT stage after restoring the control file from the autobackup.

The option stating that you must back up the control file to trace before restoring the control file from the autobackup is incorrect. You must back up the control file to determine whether you are re-creating the control file because the BACKUP CONTROLFILE TO TRACE command creates a script that is used to re-create the control file.

The option stating that you must execute the RECOVER DATABASE command before restoring the control file from the autobackup is incorrect. This is because the RECOVER DATABASE command must be issued after restoring the control file from the autobackup.

Item: 5 (Ref:1Z0-043.13.5.3)

In which scenario will you perform a cancel-based recovery?

- when a tablespace is dropped and you have only RMAN-based backup of the database
- when a table is dropped and stored in the Recycle Bin
- when you are required to recover an existing table to its previous state
- when a tablespace is dropped and you have only a user-managed full backup of the database

Answer:

when a tablespace is dropped and you have only a user-managed full backup of the database

---

Explanation:

You will perform a cancel-based recovery when a tablespace is dropped and you have only user-managed backup of the database. A cancel-based recovery is performed when you are performing a user-managed recovery. Oracle stops performing recovery when the database administrator issues the CANCEL command. This behavior of Oracle enables you to create a test database from backup if the transactional stopping point is not important to the validity of the database.

The option stating that you will perform a cancel-based recovery when a tablespace is dropped and that you have only an RMAN-based backup of your database is incorrect. When you have only an RMAN-based backup of your database, and a tablespace is dropped, you will perform an RMAN-based incomplete recovery.

The option stating that you will perform a cancel-based recovery when a table is dropped and stored in the Recycle Bin is incorrect. If you are recovering a dropped table that is stored in the Recycle Bin, then you should use the Flashback Drop feature.

The option stating that you will perform a cancel-based recovery to recover an existing table to its previous state is incorrect. If you are required to recover an existing table to its previous state, you can use the Flashback Table feature. The Flashback Table feature allows you to recover one or more tables to a specific point in time without performing time-consuming recovery operations, such as point-in-time recovery, which may also affect the availability of the rest of the database. The Flashback Table feature recovers the table by rolling back only the changes made to the tables or to their dependent objects such as indexes.

Item: 6 (Ref:1Z0-043.13.2.4)

In which situation are you **NOT** required to perform an incomplete recovery?

- when all the control files are lost
- when all the members of a redo log group are lost
- when a table is dropped and purged from the Recycle Bin
- when a temporary file of the default temporary tablespace is lost

Answer:

when a temporary file of the default temporary tablespace is lost

---

Explanation:

You need not perform an incomplete recovery if a temporary file of the default temporary tablespace is lost. If a temporary file is lost, you are required to create a new temporary tablespace, convert the new temporary tablespace to the default temporary tablespace, and drop the old temporary tablespace.

The option stating that you need not perform the incomplete recovery when all the control files are lost is incorrect. You are required to perform an incomplete recovery if all the control files are missing or lost. After performing the recovery, you are required to restore the control file from autobackup or re-create the control file output of the `ALTER DATABASE BACKUP CONTROLFILE TO TRACE` statement and open the database with the `RESETLOGS` clause. The `RESETSLOGS` clause reincarnates the redo log files and resets the `SCNs` of the online redo log files.

The option stating that you need not perform an incomplete recovery when all the members of a redo log group are missing is incorrect. This is because you are required to perform an incomplete recovery if all the online redo logs are missing or corrupt. The database should be opened with the `RESETLOGS` clause after performing the recovery. The `RESETSLOGS` clause reincarnates the redo log files and resets the `SCNs` of the online redo log files

The option stating that you need not perform incomplete recovery when a table is dropped and purged from the flash recovery area is incorrect. This is because if a table is dropped, it is stored in the Recycle Bin. You can restore this table from the Recycle Bin by using the `FLASHBACK TABLE table_name TO BEFORE DROP` statement. If the table is purged from the Recycle Bin, you are required to perform an incomplete recovery up to a time in the past when the table was not dropped.

Item: 7 (Ref:1Z0-043.13.4.6)

You are performing an incomplete recovery because certain important tables were deleted and purged from the Recycle Bin. In which mode will you perform the recovery?

- MOUNT mode
- RESTRICTED mode
- OPEN mode
- NOMOUNT mode

Answer:

MOUNT mode

Explanation:

To perform an incomplete recovery, the database must be in the MOUNT mode. The incomplete recovery results in loss of data because the database is restored and recovered to a point in time before the failure. You should understand the situations that result in incomplete recovery. If the archive log files, redo log files, control files, or one or more datafiles are missing, then incomplete recovery is required. After performing an incomplete recovery, the database must be started with the RESETLOGS option. This option gives the online redo logs a new time stamp and SCN. You cannot recover some datafiles to a time before the RESETLOGS and others to after the RESETLOGS. You must recover all the datafiles to the same SCN. The only exception is offline datafiles. These offline datafiles can be brought online after the RESETLOGS. This is because no transactional changes are stored for these files in the redo logs.

The option stating that you are required to perform an incomplete recovery in the RESTRICTED mode is incorrect. The database is started in the RESTRICTED mode for maintenance purposes. Only a database administrator can work in the RESTRICTED mode.

The option stating that you are required to perform an incomplete recovery in the OPEN mode is incorrect. To perform the incomplete recovery, the database must be in the MOUNT mode. If you perform the incomplete recovery for some datafiles in the OPEN mode, then you are required to take the datafiles offline to perform the recovery. You can perform the RMAN restore operation only if the backups were taken or registered with RMAN.

The option stating that you are required to perform the incomplete recovery in the NOMOUNT mode is incorrect. While performing the incomplete recovery, the control file is read. The database must be in the MOUNT mode because the control file is read in the MOUNT mode. In the NOMOUNT mode, only the database instance is created.

Item: 8 (Ref:1Z0-043.13.4.7)

You took the DATA1 tablespace offline at 10:00 A.M. At 12:30 P.M., a schema of a user is dropped and purged from the Recycle Bin. You noticed this at 2:00 P.M. and decided to perform an incomplete recovery.

Which datafiles will you recover?

- all the datafiles in the database
- the datafiles associated with the SYSTEM tablespace
- the datafiles associated with the DATA1 tablespace
- all the datafiles in the database except those associated with the DATA1 tablespace

Answer:

all the datafiles in the database except those associated with the DATA1 tablespace

---

Explanation:

You will recover all the datafiles in the database except those that are associated to the DATA1 tablespace because the DATA1 tablespace is offline. After performing an incomplete recovery, you are required to open the database with the RESETLOGS option. If you have offline datafiles, then you can bring them online after RESETLOGS. This is because there are no transactional changes for the files stored in the redo logs.

The option stating that you will recover all the datafiles in the database is incorrect. You are not required to recover the datafiles that are associated to the offline tablespace. The datafiles associated to the offline tablespace can be brought online after RESETLOGS.

The option stating that you will recover only the datafiles associated to the SYSTEM tablespace is incorrect. The SYSTEM tablespace is a permanent online tablespace that contains fixed tables critical to the database. You are required to recover the datafiles associated to all the online tablespaces.

The option stating that you will recover only the datafiles associated to the DATA1 tablespace is incorrect. The DATA1 tablespace is offline, and you are not required to recover the datafiles associated to the DATA1 tablespace.

Item: 9 (Ref:1Z0-043.13.5.4)

In which scenario will you perform a user-managed incomplete recovery?

- when a table is dropped and stored in the Recycle Bin
- when a table is dropped and purged from the Recycle Bin
- when you are required to recover an existing table to its previous state
- when you are required to view all the versions of a row of an existing table between a specific time period

Answer:

when a table is dropped and purged from the Recycle Bin

Explanation:

You will perform a user-managed incomplete recovery when a table is dropped and purged from the Recycle Bin. When you drop a table then it is not dropped from the database. The dropped table is stored in the Recycle Bin. If the table exists in the Recycle Bin, then you can recover the dropped table by using the Flashback Drop feature. If you are recovering a dropped table that is purged from the Recycle Bin, you must restore all the datafiles from the last backup and perform an incomplete recovery.

The option stating that you will perform a user-managed incomplete recovery when a table is dropped and stored in the Recycle Bin is incorrect. When a table is dropped and stored in the Recycle Bin, you need not perform an incomplete recovery. You can use the Flashback Drop feature to recover the dropped table.

The option stating that you will perform a user-managed incomplete recovery to recover an existing table to its previous state is incorrect. To recover an existing table to its previous state, you can use the Flashback Table feature. The Flashback Table feature allows you to recover one or more tables to a specific point in time without performing time-consuming recovery operations, such as point-in-time recovery, which may affect the availability of the rest of the database. The Flashback Table feature recovers the table by rolling back only the changes made to the tables or to their dependent objects such as indexes.

The option stating that you will perform a user-managed incomplete recovery to view all the versions of a row of an existing table between a specific time period is incorrect. If you are required to view all the versions of a row of an existing table within a specific time period, you will use the Flashback Version Query feature. The Flashback Version Query feature is used to retrieve all the versions of the rows that exist or existed between the times the query was executed to a determined point in time in the past. The Flashback Version Query returns all the committed occurrences of the rows for an object without displaying the uncommitted versions of the rows.

Item: 10 (Ref:1Z0-043.13.6.2)

You have performed an incomplete recovery because some important user's schema is dropped and purged from the Recycle Bin. The current logs are sequenced 1005 and 1006. After performing the recovery, you issued the following statement:

```
SQL>ALTER DATABASE OPEN RESETLOGS;
```

What will be the resultant log sequence numbers?

- 0 and 1
- 1 and 2
- 1005 and 1006
- 1006 and 1007

Answer:

1 and 2

Explanation:

The log sequence number will be 1 and 2. When you perform an incomplete recovery, you are required to open the database by using the RESETLOGS option. This option gives the online redo logs a new timestamp and SCN. Therefore, you cannot recover some datafiles to a time before the RESETLOGS and others to a time after the RESETLOGS. In this scenario, when you open the database with the RESETLOGS, then the log sequence will be 1 and 2. The current redo logs are archived, the contents of the redo log files are erased, and the information about the log sequence number is written to the control file and all the online datafile headers.

The other options are incorrect because the new log sequence numbers are reset to 1 and 2.

Item: 11 (Ref:1Z0-043.13.5.6)

You are maintaining your database in ARCHIVELOG mode. An important table, SCOTT.EMPLOYEE, is dropped and purged from the Recycle Bin on Monday at 2:00 P.M. You do not use RMAN to perform backups. You performed the last full user-managed backup at 9:00 P.M. on Sunday.

How will you recover the dropped table, SCOTT.EMPLOYEE?

- by using the Flashback Table feature
- by using the Flashback Database feature
- by performing incomplete recovery using RMAN utility
- by performing incomplete recovery using user-managed recovery

Answer:

by performing incomplete recovery using user-managed recovery

---

Explanation:

You will recover the dropped table, SCOTT.EMPLOYEE, by performing incomplete recovery using user-managed recovery. If you are recovering a dropped table that is purged from the Recycle Bin, then you must restore all the datafiles from the last backup and perform an incomplete recovery.

The option stating that you will recover the dropped table, SCOTT.EMPLOYEE, by using the Flashback Table feature is incorrect. You cannot use the Flashback Table feature to recover the SCOTT.EMPLOYEE table because the table is purged from the Recycle Bin. The Flashback Table feature allows you to recover one or more tables to a specific point in time without performing time-consuming recovery operations, such as point-in-time recovery, which may also affect the availability of the rest of the database. The Flashback Table feature recovers the table by rolling back only the changes made to the tables or to their dependent objects such as indexes.

The option stating that you will recover the dropped table, SCOTT.EMPLOYEE, by using the Flashback Database feature is incorrect. You cannot use the Flashback Database feature to recover the SCOTT.EMPLOYEE table. Flashback Database is a new feature in Oracle 10*g* that allows you to quickly restore the entire database to its previous state.

The option stating that you will recovery the dropped table, SCOTT.EMPLOYEE, by using the RMAN utility to perform an incomplete recovery is incorrect. This is because you do not perform the backup of the database by using the RMAN utility. You can perform recovery by using the RMAN utility only if you have performed the RMAN backup.

Item: 12 (Ref:1Z0-043.13.4.5)

You are maintaining the database in Oracle10*g*. You are performing an incomplete recovery by using RMAN because an important table, EMPLOYEE, is dropped and purged from the Recycle Bin. Which statement is **NOT** true regarding an incomplete recovery?

- The target database must be in the MOUNT mode to ensure restoration of the datafiles.
- You can restore the datafiles from the backup by using the RMAN utility only if the backups were taken using the RMAN utility.
- The control file must be recreated.
- The database must be opened with the RESETLOGS option.

Answer:

The control file must be recreated.

Explanation:

If an important table is dropped, then it is not necessary to re-create the control file to perform an incomplete recovery. The control file contains the physical map of an Oracle database. In other words, the control file has all the locations of the physical files, including the datafiles and redo logs. The control files also contain indicate whether the database is in the ARCHIVELOG mode or not.

To perform the incomplete recovery, the database must be in MOUNT mode. The incomplete recovery results in a loss of data because the database is restored and recovered to a point in time before the failure. You can restore the datafiles from the backup by using the RMAN utility only if the backups were taken using the RMAN utility. After performing the incomplete recovery, the database must be started with the RESETLOGS option. This option gives the online redo logs a new time stamp and SCN. You cannot recover certain datafiles to a time before using the RESETLOGS option and other files to a time after using the RESETLOGS option. You must recover all the datafiles to the same SCN. The only exception is the offline datafiles which can be brought online after the RESETLOGS because no transactional changes for these files are stored in the redo logs.

Item: 13 (Ref:1Z0-043.13.1.3)

You issued the following statement:

```
SQL> ALTER DATABASE BACKUP CONTROLFILE TO TRACE;
```

What will be the result of issuing the statement?

- The control file will be multiplexed.
- The control file will be recreated.
- The script containing the CREATE CONTROLFILE statement will be created.
- The binary backup of the control file will be created.

Answer:

The script containing the CREATE CONTROLFILE statement will be created.

Explanation:

The script containing the CREATE CONTROLFILE statement will be created. The script is created by using the ALTER DATABASE BACKUP CONTROLFILE TO TRACE statement. This statement generates an ASCII representation of the binary control file as an Oracle trace file. The ASCII backup control file can be used to rebuild the binary control file.

The option stating that the control file will be multiplexed is incorrect. The control file is multiplexed by copying the control file to another disk and by making the changes in the initialization parameter file, the spfile, and the current control file.

The option stating that the control file will be re-created is incorrect. To re-create the control file, you are required to run the script created by the ALTER DATABASE BACKUP CONTROLFILE TO TRACE statement.

The option stating that the binary backup will be created by executing the ALTER DATABASE BACKUP CONTROLFILE TO TRACE statement is incorrect. The binary backup will be created by executing the ALTER DATABASE BACKUP CONTROLFILE TO <path> statement. The control file can be created by using the RECOVER DATABASE UNTIL TIME <value> USING BACKUP CONTROLFILE command.

Item: 14 (Ref:1Z0-043.13.6.1)

You are maintaining your database in Oracle10*g*. You are performing an incomplete recovery because the tablespace, DATA1, was dropped and purged from the Recycle Bin. After performing an incomplete recovery, you open the database with the RESETLOGS option.

What will **NOT** be the impact of using the RESETLOGS option?

- The log sequence for the database will restart from 1.
- The log sequence number will be written to the control file.
- The log sequence number will be written to the datafile headers.
- The log sequence number will be written to the initialization parameter file.

Answer:

The log sequence number will be written to the initialization parameter file.

Explanation:

The log sequence number is not written to the initialization parameter file. When you perform the incomplete recovery, you are required to open the database by using the RESETLOGS option. This option provides a new time stamp and SCN to the online redo logs. You cannot recover some datafiles to a time before the RESETLOGS and others to after the RESETLOGS.

When you open the database with the RESETLOGS, then the log sequence restarts from 1. The new log sequence number is written to the control file, the datafile headers, and the initialization parameter file.

Item: 15 (Ref:1Z0-043.13.4.3)

You are performing an incomplete recovery because some important tables have been dropped and purged from the Recycle Bin. Which clause can you **NOT** use to perform the incomplete recovery by using the RMAN utility?

- UNTIL CANCEL
- UNTIL SCN
- UNTIL SEQUENCE
- UNTIL TIME

Answer:

UNTIL CANCEL

Explanation:

You cannot use the UNTIL CANCEL clause to perform an incomplete recovery by using the RMAN utility. An RMAN-based incomplete recovery does not have a CANCEL-based option. The UNTIL CANCEL clause is used while performing a user-managed incomplete recovery. RMAN stops performing a recovery when the administrator issues the CANCEL command.

You can use the UNTIL SCN clause to perform an incomplete recovery by using the RMAN utility. The UNTIL SCN clause specifies that RMAN will stop the recovery operation before a known SCN that introduces corruption or an undesired event, which cannot be rolled back, in the database.

You can use the UNTIL SEQUENCE clause to perform an incomplete recovery by using the RMAN utility. The UNTIL SEQUENCE clause specifies that RMAN will stop the recovery operation before a known redo log sequence that introduces corruption or an undesired event, which cannot be rolled back, in the database. The database is recovered to the sequence number without including the log sequence number.

You can use the UNTIL TIME clause to perform the incomplete recovery by using the RMAN utility. The UNTIL TIME clause specifies that RMAN stops recovery operation before a known time that introduces corruption or an undesired event, which cannot be rolled back, in the database.

Item: 16 (Ref:1Z0-043.13.2.1)

In which scenario is a Database Administrator **NOT** required to perform an incomplete recovery?

- when all the online redo log groups are multiplexed and one of the members of a group is missing
- when all the online redo log groups are not multiplexed and one log group is missing
- when all the control files are missing
- when some important tables are deleted from the database and purged from the Recycle Bin

Answer:

when all the online redo log groups are multiplexed and one of the members of a group is missing

---

Explanation:

If all the online redo log groups are multiplexed and one member of a redo log group is missing, then the DBA must not perform an incomplete recovery. The DBA can restore the missing redo log file from a multiplexed copy. Mirrored or multiplexed redo logs include more than one redo log file in an online redo log group. Each file in a group is called a redo log member. Re-creating a redo log member is a fairly straightforward process. The `ALTER DATABASE ADD LOGFILE MEMBER` statement creates a log file member if a redo log member is lost or deleted.

The option stating that the DBA should not perform an incomplete recovery if the online redo log files are not multiplexed and one redo log file is missing is incorrect. If the online redo log groups are not multiplexed and a redo log file is missing, then incomplete recovery is required. You should first determine the amount of data you can recover. To do this, start the database in the `MOUNT` stage and then query the `V$LOG` view to find the system change number (SCN) that you can recover to.

The value in the `FIRST_CHANGE#` column is the first `SCN` stamped in the missing log. This implies that the last `SCN` stamped in the previous log is `290254 (FIRST_CHANGE#-1)`. This is the highest `SCN` that you can recover to. To perform the recovery, the DBA must first restore all the datafiles to this `SCN`, and then perform a recovery up to this `SCN`. This is an incomplete recovery; therefore, the DBA must open the database with the `RESETLOGS` option.

```
RMAN TARGET /
RMAN> RESTORE DATABASE UNTIL SCN 290254;
RMAN> RECOVER DATABASE UNTIL SCN 290254;
RMAN> ALTER DATABASE OPEN RESETLOGS;
```

The option stating that the DBA should not perform an incomplete recovery if all the control files are missing is incorrect. This is because if one or all the control files are missing, then the database will not be started. To solve this problem, the DBA must perform an incomplete recovery. For example, while starting the database, the DBA receives the following error:

```
SQL> STARTUP;

ORACLE instance started.

Total System Global Area 135338868 bytes
Fixed Size 453492 bytes
Variable Size 109051904 bytes
Database Buffers 25165824 bytes
Redo Buffers 667648 bytes
ORA-00205: error in identifying controlfile, check alert log for
more info

SQL>
```

To perform the recovery, all the log files including the archived and current online log files should be available since the last backup. The logs are required because all the datafiles must also be restored from the backup. The database will then have to be recovered up to the time of failure. The syntax to accomplish this is as follows:

```
RMAN TARGET /
RMAN> SET DBID <value>
RMAN> RESTORE CONTROLFILE FROM AUTOBACKUP;
RMAN> ALTER DATABASE MOUNT;
RMAN> RECOVER DATABASE;
RMAN> ALTER DATABASE OPEN RESETLOGS;
```

The option stating that the DBA should not perform an incomplete recovery if some of the important tables are dropped from the database and purged from the Recycle Bin is incorrect. If one or more important tables are dropped from the database and purged from the Recycle Bin, then you must perform an incomplete recovery. You can perform an incomplete recovery by using the `UNTIL TIME`, or `UNTIL SEQUENCE` clause, for example:

```
RMAN>RUN
     {
     SET UNTIL TIME '16-DEC-2004 15:30:00';
     RESTORE DATABASE;
     RECOVER DATABASE;
     }
```

or

```
RMAN>RUN
     {
     SET UNTIL SEQUENCE 3 THREAD 1;
     RESTORE DATABASE;
     RECOVER DATABASE;
     }
```

Item: 17 (Ref:1Z0-043.13.3.1)

You are using Recovery wizard for performing incomplete recovery. Which of the following object types is **NOT** available in the Perform Recovery :Type screen?

- Whole database
- Tablespaces
- Datafiles
- Archive logs
- Redo logs

Answer:

Redo logs

Explanation:

The Redo logs object type is not available in the Perform Recovery : Type screen of the Oracle Enterprise Manager. The available type values are:

- Whole database
- Tablespaces
- Archive logs
- Datafiles
- Tables

To perform recovery, in the Perform Recovery :Type screen, select Whole Database from the Object Type list box. Enter the appropriate username and password with administrator privilege and click on Next button. The Recovery Wizard screen opens. During this process, you are asked to wait until `RMAN` performs shutdown the database and startup the database and opens in the `MOUNT` stage.

The other options stating that Whole database, Tablespaces, Datafiles, Archive logs are not available in the Perform Recovery : Type screen.

Item: 18 (Ref:1Z0-043.13.2.5)

You are maintaining the SALES database of TeleStar Corporation. The online redo log configuration of the database is as follows:

Redo log group	Redo log members
Group1	redo1a.log
	redo1b.log
Group2	redo2a.log
	redo2b.log
Group3	redo3a.log
	redo3b.log

One of the redo log members, redo3b, is lost due to disk failure.

How will you recover the redo log member redo3b?

- by performing an incomplete recovery from the last backup
- by performing an import operation
- by performing a complete database recovery
- by dropping the lost member and adding a new redo log member

Answer:

by dropping the lost member and adding a new redo log member

Explanation:

If a redo log member is lost or deleted and a mirrored log member continues to exist, then the redo log member can be easily rebuilt. This is an example of a noncritical recovery. Recreating a redo log file is a straightforward process. The ALTER DATABASE ADD LOGFILE MEMBER command will create a log file member if a log member has been lost or deleted. In this scenario, you are required to drop the lost redo log member, redo3b.log, and add a new redo log member by using the ALTER DATABASE ADD LOGFILE MEMBER command.

The option stating that you should perform an incomplete recovery to recover the lost redo log member, redo3b.log, is incorrect. You have one member, redo3a.log, of the redo log group, Group3, and you can recover the lost redo log group by dropping the lost redo log member and adding a new redo log member. Incomplete recovery is used if all the members of a redo log group are lost. For example, if all the members of a redo log group are lost, you must determine the amount of data that can be recovered. To determine the amount of data, you should start the database in the MOUNT stage and query the V$LOG view. A system change number (SCN) that is obtained enables you to recover the data. The first SCN stamped in the missing log is FIRST_CHANGE#. This implies that the last SCN stamped in the previous log is 290254 (FIRST_CHANGE#-1). This is the highest SCN that you can recover to. To perform an incomplete recovery, you must first restore all the datafiles to this SCN and then perform a database recovery up to this SCN.

The option stating that you should perform the import operation to recover the lost online redo log member is incorrect. This is because the import operation is used to recover logical components, such as tables and tablespaces, of the database.

The option stating that you should perform a complete recovery to recover the lost redo log member, redo3b.log, is incorrect. If one multiplexed redo log member is missing, then you can recover the missing redo log member by dropping the lost redo log member and adding a new online redo log member. A complete recovery is used to recover one or more datafiles from the last backup if the database is in ARCHIVELOG mode.

Item: 19 (Ref:1Z0-043.13.1.6)

You are the Database Administrator (DBA) of your company. You execute the following statement on an Oracle 10*g* instance:

```
SQL> ALTER SYSTEM SWITCH LOGFILE;
```

Which two tasks are performed when the statement is executed? (Choose two.)

- The DBWn process writes to the datafile.
- Changes in the background process are recorded.
- The log file is updated with the current SCN number.
- The System Change Number (SCN) is recorded in the control file.
- The changes to the listener configuration in the `listener.ora` file are recorded.

Answer:

The DBWn process writes to the datafile.

The System Change Number (SCN) is recorded in the control file.

Explanation:

The ALTER SYSTEM SWITCH LOGFILE statement initiates a log switch followed by a checkpoint in the database. Whenever there is a checkpoint, the SCN number is updated in the control file and headers of the datafiles. In addition, the DBWn process writes the committed data to the datafiles.

Issuing this statement does not make any changes in the background processes.

Issuing this statement does not update the log files with the current SCN number. When this statement is issued the current redo log will be switched and LGWR will start writing to another active redo log group in the database. The redo log files will not be updated with the current SCN number.

Issuing this statement does not make any changes to the `listener.ora`. Changes will be made to the `listener.ora` file when you update or delete information related to the listeners or the databases for which the listener is listening. The Change Tracking Write (CTWR) background process will record the changes to the listened configuration in the `listener.ora` file.

Item: 20 (Ref:1Z0-043.13.1.2)

In which situation will you run the script containing the following statement?

```
CREATE CONTROLFILE REUSE DATABASE SALES NORESETLOGS ARCHIVELOG
   MAXLOGFILES 20
   MAXLOGMEMBERS 3
   MAXDATAFILES 30
   MAXINSTANCES 10
   MAXLOGHISTORY 1200
   LOGFILE
   GROUP 1 (
   '/disk1/prod/orders/db/log1a.dbf',
   '/disk2/prod/orders/db/log1b.dbf'
   ) SIZE 100K
   GROUP 2 (
   '/disk1/prod/orders/db/log2a.dbf',
   '/disk2/prod/orders/db/log2b.dbf'
   ) SIZE 100K,
   DATAFILE
   '/disk1/prod/orders/db/database1.dbf',
   '/disk2/prod/orders/db/file1.dbf ';
```

- when all the control files are missing and only a binary backup of the current control file exists
- when a multiplexed copy of the current control file is missing
- when all the control files are missing and only an ASCII representation of the binary control file exists
- when the SPFILE is missing

Answer:

when a multiplexed copy of the current control file is missing

---

Explanation:

You will run the script containing this statement to re-create the control file when all the control files are missing and only the ASCII representation of the binary control file exists. The script re-creates the control file. The script is created by using the `ALTER DATABASE BACKUP CONTROLFILE TO TRACE` statement. This statement generates an ASCII representation of the binary control file as an Oracle trace file. The ASCII backup control file can be used to rebuild the binary control file.

The option stating that you will run the script containing the statement to re-create the control file when all the control files are missing and only a binary backup of the current control file exists is incorrect. If all the control files are missing and only a binary backup of the control file exists, you will recover the control file by using the `RECOVER DATABASE UNTIL TIME USING BACKUP CONTROLFILE` command.

The option stating that you will run the script containing the statement to re-create the control file when a multiplexed copy of the current control file is missing is incorrect. When a multiplexed copy of the current control file is missing, you can perform the recovery by copying the multiplexed image to the desired location.

The option stating that you will run the script containing the statement to re-create the control file when the `SPFILE` is missing is incorrect. When the `SPFILE` is missing, you can re-create the `SPFILE` by using the `CREATE SPFILE FROM PFILE` statement.

Item: 21 (Ref:1Z0-043.13.5.2)

You are maintaining your database in Oracle10*g*. You perform a full user-managed backup every Sunday at 8:00 P.M. Your database is running in ARCHIVELOG mode. On Monday, at 9:00 A.M., a tablespace is dropped. You decide to perform incomplete recovery to recover the dropped tablespace.

Which two clauses can you use with the RECOVER command? (Choose two.)

- UNTIL SEQUENCE
- UNTIL SCN
- UNTIL CHANGE
- UNTIL CANCEL

Answer:

UNTIL CHANGE
UNTIL CANCEL

Explanation:

You can use either the UNTIL CHANGE or the UNTIL CANCEL clause with the RECOVER command at the SQL prompt to perform a user-managed recovery. The UNTIL CANCEL clause specifies that Oracle will stop the recovery process when the administrator issues the CANCEL command. The UNTIL CHANGE specifies that Oracle will stop the recovery process before an SCN that introduces corruption or some undesired event that cannot be rolled back in the database. The SCN can be a more finite stopping point compared to a time or redo log sequence because it is generated by transaction.

The option stating that you can use the UNTIL SEQUENCE clause with the RECOVER command at the SQL prompt to perform a user-managed recovery is incorrect. The UNTIL SEQUENCE clause works with only the RMAN utility. The UNTIL SEQUENCE clause specifies that RMAN will stop the recovery operation before a known redo log sequence that introduces corruption or some undesired event that cannot be rolled back in the database. The database is recovered to the sequence number without including the log sequence number.

The option stating that you can use the UNTIL SCN clause with the RECOVER command at the SQL prompt to perform the user-managed recovery is incorrect. The UNTIL SCN clause works with only the RMAN utility. The UNTIL SCN clause specifies that RMAN will stop the recovery operation before a known SCN that introduces corruption or some undesired event that cannot be rolled back in the database.

Item: 22 (Ref:1Z0-043.13.6.3)

You have recovered your Oracle Database 10*g* by using the control file backup because all copies of the current control file have been lost due to a media failure. You open your database by using the following statement:

```
SQL>ALTER DATABASE OPEN RESETLOGS;
```

Which of the following options is true about using the RESETLOGS option?

- The log sequence is reset to 0.
- All the online redo logs are deleted.
- All the archived redo logs from a previous incarnation become useless.
- The full database backup taken from a previous incarnation can be used in future.
- Only the control file and online redo log files are updated with a new RESETLOGS SCN and time stamp.

Answer:

The full database backup taken from a previous incarnation can be used in future.

Explanation:

The full database backup taken from a previous incarnation can be used in the future. You can use the complete database backup from a previous incarnation in the current recovery process. This feature has been introduced in the Oracle 10*g*.

Opening the database with a RESETLOGS option resets the log sequence to 1, not 0.

When you open the database with a RESETLOGS option, the online redo logs are cleared, not deleted.

The option stating that all the archived redo logs from a previous incarnation become useless after opening the database with a RESETLOGS option is incorrect. Before Oracle 10*g*, you were not concerned about the archived redo logs from a previous incarnation because you would not be able to apply them in future. However, in Oracle 10*g*, you can reuse the archived redo logs from a previous incarnation.

Generation of the System Change Number (SCN) at the time of RESETLOGS option is known as RESETLOGS SCN. This information is stored in all datafiles, control files and online redo log files.

Item: 23 (Ref:1Z0-043.13.2.2)

You are maintaining your database in Oracle10*g*. On Tuesday at 8:00 A.M., while starting the database, you discover that all the control files are missing. The backup of the full database was performed on Sunday at 6:00 P.M.

Which type of recovery will you perform?

- incomplete recovery
- complete recovery
- recovery using the Flashback Database feature
- recovery using the export/import utility

Answer:

incomplete recovery

Explanation:

You will perform an incomplete recovery. The last available backup is Sunday's backup. You will perform the recovery using Sunday's backup. You will be required to perform an incomplete recovery. All the transactions performed between 6:00 P.M. on Sunday and 8:00 A.M. on Tuesday will be lost.

The option stating that you will perform a complete recovery is incorrect. You will not perform a complete recovery if all the control files are missing. A complete recovery involves using redo data or incremental backups with a backup of the database, the tablespace, or the datafile.

The option stating that you will perform the recovery by using the Flashback Database feature is incorrect. Flashback Database is a new feature in Oracle 10*g* that allows you to quickly restore the entire database to its previous state.

The option stating that you will perform the recovery by using the export/import utility is incorrect. The export/import utility is used to perform the logical backup of the database, the tablespaces, the user's schema, or the objects in the schema.

Item: 24 (Ref:1Z0-043.13.5.5)

Your database is running in ARCHIVELOG mode. The SCOTT.EMP table belongs to the DATA1 tablespace. The junior DBA erroneously runs a script that executes the following statement:

```
SQL> DROP TABLE SCOTT.EMP PURGE;
```

After one hour, you are performing the user managed incomplete recovery. Which datafiles will you restore from the last full backup?

- the datafiles associated with the SYSTEM tablespace
- the datafiles associated to the DATA1 tablespace
- the datafiles associated to the SYSTEM and DATA1 tablespaces
- all the datafiles in the database

Answer:

all the datafiles in the database

Explanation:

The option, all the datafiles in the database, is correct. You will recover the dropped table, SCOTT.EMPLOYEE, by using the user-managed recovery to perform an incomplete recovery. The DROP TABLE SCOTT.EMP PURGE statement will drop the SCOTT.EMP table and purge the table from the Recycle Bin. If you are recovering a dropped table that is purged from the Recycle Bin, you must restore all the datafiles from the last backup and perform an incomplete recovery.

You must restore all the datafiles in the database from the last full backup. The other three options are incorrect.

Item: 25 (Ref:1Z0-043.13.4.4)

You are performing an incomplete recovery because a tablespace is dropped and purged from the Recycle Bin.

In which mode will you execute the following code?

```
RMAN>RUN
{
SET UNTIL SEQUENCE <sequence_number> THREAD <thread_number>;
RESTORE DATABASE;
RECOVER DATABASE;
}
```

- NOMOUNT
- MOUNT
- OPEN
- RESTRICTED

Answer:

MOUNT

Explanation:

You will execute the above code in the MOUNT mode. To perform an incomplete recovery, the database must be in the MOUNT mode. An incomplete recovery results in a loss of data because the database is restored and recovered to a point in time before the failure. You should understand the situations that result in incomplete recovery. If the archive log files, redo log files, control files, or one or more datafiles are missing, then incomplete recovery is performed. In this scenario, you are performing database recovery by using the UNTIL SEQUENCE clause. The database will be recovered to the specified sequence number without including the log sequence number.

You will not execute the code in the NOMOUNT mode. While performing an incomplete recovery, the control file is read. The database must be in the MOUNT mode because the control file is read in the MOUNT mode. In the NOMOUNT mode, only the database instance is created.

You will not execute the code in the OPEN mode. To perform an incomplete recovery, the database must be in the MOUNT mode. To perform an incomplete recovery for some datafiles in the OPEN mode, you are required to take the datafiles offline. You can perform an RMAN restore operation only if the backups were taken or registered with RMAN.

You will not execute the code in the RESTRICTED mode. The database is started in the RESTRICTED mode for maintenance purposes. Only the database administrator can work in the RESTRICTED mode.

Item: 26 (Ref:1Z0-043.13.4.2)

You are performing a database recovery because a user's schema is dropped. While performing the recovery, you use the UNTIL SEQUENCE clause. Which type of database recovery are you performing?

- user managed complete recovery
- user managed incomplete recovery
- RMAN-based complete recovery
- RMAN-based incomplete recovery

Answer:

RMAN-based incomplete recovery

Explanation:

You are performing the RMAN-based incomplete recovery to recover the dropped user's schema. Incomplete recovery is a recovery that does not recover the data completely. All the archived redo logs are applied to the database to make the database complete. Incomplete recovery is also called database point-in-time recovery because the recovery is recovered up to a determined point in time. The RMAN incomplete recovery is performed by using the SET UNTIL TIME or the SET UNTIL SEQUENCE clause before the RECOVER command. The UNTIL TIME clause specifies that the RMAN stops the recovery operation before a known time that introduced corruption or some undesired event that cannot be rolled back in the database. The UNTIL SEQUENCE clause specifies that RMAN will stop the recovery operation before a known redo log sequence that introduced corruption or some undesired event that cannot be rolled back in the database. The database is recovered to the sequence number by not including the log sequence number.

The option stating that you are performing a user-managed complete recovery is incorrect. While performing a user-managed complete recovery, you recover the backup to the current SCN. In this scenario, you are specifying the log sequence number up to which the database must be recovered. You can perform a user-managed complete recovery to recover the whole database, tablespaces, or datafiles.

The option stating that you are performing the user-managed incomplete recovery is incorrect. While performing the user-managed incomplete recovery, you use the UNTIL TIME, UNTIL CANCEL, or UNTIL CHANGE clauses.

The option stating that you are performing the RMAN-based complete recovery is incorrect. If you are recovering the user's schema, you are required to perform an incomplete point-in-time recovery. The RMAN-based complete recovery is used in case of a media failure.

Flashback Database

Item: 1 (Ref:1Z0-043.14.2.7)

You are managing a single instance Oracle 10*g* database that utilizes the following parameters:

Which of the following set of commands must you execute to enable Flashback Database?

- STARTUP MOUNT EXCLUSIVE
  ALTER DATABASE FLASHBACK ON;
  ALTER DATABASE OPEN;
- STARTUP MOUNT
  ALTER DATABASE FLASHBACK ON;
  ALTER DATABASE OPEN RESETLOGS;
- STARTUP MOUNT EXCLUSIVE
  ATLER DATABASE ARCHIVELOG;
  ALTER DATABASE FLASHBACK ON;
  ALTER DATABASE OPEN RESETLOGS;
- STARTUP MOUNT
  ALTER DATABASE ARCHIVELOG;
  ALTER DATABASE FLASHBACK ON;
  ALTER DATABASE OPEN;

Answer:

STARTUP MOUNT
ALTER DATABASE ARCHIVELOG;
ALTER DATABASE FLASHBACK ON;
ALTER DATABASE OPEN;

Explanation:

You must use the following set of commands to enable Flashback Database in the given scenario:

```
STARTUP MOUNT
ALTER DATABASE ARCHIVELOG;
ALTER DATABASE FLASHBACK ON;
ALTER DATABASE OPEN;
```

Before the introduction of the Oracle Database 10*g* Database, recovery could take hours. With Flashback Database, the time to correct errors equals the time taken to commit the error. If Flashback Database is enabled in the database, Oracle stores flashback logs that can be used to recover the database to a specific point in time without having to restore files from the backup. However, the flash recovery area must be configured before enabling Flashback Database. The flash recovery area can be enabled by setting up two initialization parameters, `DB_RECOVERY_FILE_DEST_SIZE` and `DB_RECOVERY_FILE_DEST`, in the initialization parameter file.

The `ALTER DATABASE FLASHBACK ON` statement is used to enable Flashback Database. To successfully execute this statement, your database must be mounted in the `EXCLUSIVE` mode. The `STARTUP MOUNT EXCLUSIVE` command can be used to mount the database in the `EXCLUSIVE` mode. The `STARTUP MOUNT EXCLUSIVE` command is required when multiple instances are accessing your database and you want only the first instance to mount the database. However, subsequent instances cannot mount the database if it has been mounted in the `EXCLUSIVE` mode by the first instance. Whereas, if you are running your database in a single-instance configuration, the `STARTUP MOUNT` command will have the same effect as the `STARTUP MOUNT EXCLUSIVE` command.

The option,

```
STARTUP MOUNT EXCLUSIVE
ALTER DATABASE FLASHBACK ON;
ALTER DATABASE OPEN;
```

is incorrect because before enabling Flashback Database, you must ensure that the database is running in the `ARCHIVELOG` mode and the flash recovery area is configured. Otherwise, you will receive errors. For example, on executing the `ALTER DATABASE FLASHBACK ON` statement when archiving is not enabled, you will receive the following errors:

```
ORA-38706: Cannot turn on FLASHBACK DATABASE logging.
ORA-38707: Media recovery is not enabled.
```

Similarly, if the flash recovery area is not configured and you execute the ALTER DATABASE FLASHBACK ON statement to enable Flashback Database, you receive the following errors:

```
ORA-38706: Cannot turn on FLASHBACK DATABASE logging.
ORA-38709: Recovery Area is not enabled.
```

The option,

```
STARTUP MOUNT
ALTER DATABASE FLASHBACK ON;
ALTER DATABASE OPEN RESETLOGS;
```

is incorrect because after enabling Flashback Database, the ALTER DATABASE OPEN statement brings the database online. The ALTER DATABASE OPEN RESETLOGS statement should only be used to open the database after performing an incomplete media recovery. Therefore, opening the database using the ALTER DATABASE OPEN RESETLOGS statement after enabling Flashback Database will produce the following error:

```
ORA-01139: RESETLOGS option only valid after an incomplete
database recovery
```

The option,

```
STARTUP MOUNT EXCLUSIVE
ATLER DATABASE ARCHIVELOG;
ALTER DATABASE FLASHBACK ON;
ALTER DATABASE OPEN RESETLOGS;
```

is incorrect because the STARTUP MOUNT EXCLUSIVE command is required when multiple instances are accessing your database and you want only the first instance to mount the database. However, subsequent instances cannot mount the database if it has been mounted in the EXCLUSIVE mode by the first instance. Whereas, if you are running your database in a single-instance configuration, then the STARTUP MOUNT command will have the same effect as the STARTUP MOUNT EXCLUSIVE command.

Item: 2 (Ref:1Z0-043.14.2.3)

Adam is the senior DBA at United Sales Corporation. The junior DBA in the organization dropped the user Scott at 10:00 A.M. At 10:15 A.M., the user Scott requests Adam to recover the schema and all the objects in the schema. Adam decides to flash back the database.

Which block of code should Adam use?

- ```
  SHUTDOWN IMMEDIATE;
  STARTUP MOUNT;
  FLASHBACK DATABASE TO TIMESTAMP (SYSDATE(1/48));
  ALTER DATABASE OPEN RESETLOGS;
  ```
- ```
  SHUTDOWN IMMEDIATE;
  STARTUP MOUNT EXCLUSIVE;
  FLASHBACK DATABASE TO TIMESTAMP (SYSDATE-(1/48));
  ALTER DATABASE OPEN;
  ```
- ```
  SHUTDOWN IMMEDIATE;
  STARTUP NOMOUNT
  FLASHBACK DATABASE TO TIMESTAMP (SYSDATE-(1/48));
  ALTER DATABASE OPEN RESETLOGS;
  ```
- ```
  SHUTDOWN IMMEDIATE;
  STARTUP MOUNT EXCLUSIVE;
  FLASHBACK DATABASE TO TIMESTAMP (SYSDATE-1/48));
  ALTER DATABASE OPEN RESETLOGS;
  ```

Answer:

```
SHUTDOWN IMMEDIATE;
STARTUP MOUNT EXCLUSIVE;
FLASHBACK DATABASE TO TIMESTAMP (SYSDATE-1/48));
ALTER DATABASE OPEN RESETLOGS;
```

Explanation:

Adam must execute the following statements to recover the schema of the user, Scott, and all the objects in the schema. To ensure recovery, the database should be in the `MOUNT EXCLUSIVE` mode. In addition, after the backup operation is performed, the database must be opened with `RESETLOGS`.

```
SHUTDOWN IMMEDIATE;
STARTUP MOUNT EXCLUSIVE;
FLASHBACK DATABASE TO TIMESTAMP (SYSDATE-1/48));
ALTER DATABASE OPEN RESETLOGS;
```

The `SHUTDOWN IMMEDIATE;` statement will shut down the database immediately. The `STARTUP MOUNT EXCLUSIVE;` statement will start the database in `MOUNT EXCLUSIVE` mode. The `FLASHBACK DATABASE TO TIMESTAMP (SYSDATE-1/48));` statement will perform the flashback operation and the `ALTER DATABASE OPEN RESETLOGS;` statement will open the database, reset the redo log groups, and create a new incarnation of the database.

Consider the following block of code:

```
SHUTDOWN IMMEDIATE;
STARTUP MOUNT;
FLASHBACK DATABASE TO TIMESTAMP (SYSDATE-1/48));
ALTER DATABASE OPEN RESETLOGS;
```

The above code will not recover Scott's schema together with all the objects in the schema because the `STARTUP MOUNT;` statement will start the database in `MOUNT` mode. The database should be in `MOUNT EXCLUSIVE` mode before a flashback operation is performed because you can only enable Flashback Database when the database is mounted in the exclusive mode.

Consider the following block of code:

```
SHUTDOWN IMMEDIATE;
STARTUP MOUNT EXCLUSIVE;
FLASHBACK DATABASE TO TIMESTAMP (SYSDATE-(1/48));
ALTER DATABASE OPEN;
```

The above code will recover Scott's schema together with all the objects in the schema, but the database will not open because the log sequence number should be reset after performing an incomplete recovery. To reset the log sequence number, you can use the `ALTER DATABASE OPEN RESETLOGS` statement.

Consider the following block of code:

```
SHUTDOWN IMMEDIATE;
STARTUP NOMOUNT;
FLASHBACK DATABASE TO TIMESTAMP (SYSDATE-(1/48));
ALTER DATABASE OPEN RESETLOGS;
```

The above code will not recover the user Scott's schema together with all the objects in the schema because the `STARTUP NOMOUNT;` statement will start the database in `NOMOUNT` mode. The database should be in `MOUNT EXCLUSIVE` mode before performing a flashback operation. The `NOMOUNT` mode is used to perform incomplete recovery when all the control files are missing.

Item: 3 (Ref:1Z0-043.14.2.8)

Which background process sequentially writes Flashback Database data from the flashback buffer to the Flashback Database logs?

- DBWn
- RECO
- RVWR
- LGWR

Answer:

RVWR

Explanation:

When you enable Flashback Database, the Recovery Writer (RVWR) process is started. This background process sequentially writes Flashback Database data from the flashback buffer to the Flashback Database logs.

The Database Writer (DBWn) background process writes the dirty buffers from the database buffer cache to the datafiles.

The Recoverer (RECO) background process is used for automatically resolving failures involving distributed transactions in a distributed database environment.

The Log Writer (LGWR) background process writes the redo buffers from the redo buffer cache to the online redo log files on disk.

Item: 4 (Ref:1Z0-043.14.3.3)

You are maintaining the SALES database for an organization. You have enabled the Flashback Database feature and want to estimate the flashback space required for future operations.

Which view would you query to estimate the flashback space required?

- V$DATABASE
- V$FLASHBACK_DATABASE_STAT
- V$FLASHBACK_DATABASE_LOG
- V$RECOVERY_FILE_DEST

Answer:

V$FLASHBACK_DATABASE_STAT

Explanation:

You will query the V$FLASHBACK_DATABASE_STAT view to estimate the flashback space required for future operations. The V$FLASHBACK_DATABASE_STAT view is used to monitor the overhead of maintaining data in the Flashback Database logs. This view allows you to estimate the space required for future Flashback database operations. The V$FLASHBACK_DATABASE_STAT view consists of the following columns:

BEGIN_TIME: displays the start of the time interval
END_TIME: displays the end of the time interval
FLASHBACK_DATA: displays the number of bytes of flashback data written during the interval
DB_DATA: displays the number of bytes of database data read and written during the interval
REDO_DATA_TIME: displays the number of bytes of redo data written during the interval
ESTIMATED_FLASHBACK_SIZBEGIN_TIME: displays the value of the ESTIMATED_FLASHBACK_SIZE column in the V$FLASHBACK_DATABASE_LOG view at the end of the time interval

The option stating that the V$DATABASE view can be used to estimate the flashback space required for future operations is incorrect. The V$DATABASE view displays whether the Flashback Database is on or off, which indicates whether the Flashback Database feature is enabled or disabled.

The option stating that the V$FLASHBACK_DATABASE_LOG view can be used to estimate the flashback space required for future operations is incorrect. The V$FLASHBACK_DATABASE_LOG view is used to determine the estimated size of the flashback data that you need for your current target retention. The V$FLASHBACK_DATABASE_LOG view was created to support the Flashback Database feature and was introduced in Oracle 10*g*. The V$FLASHBACK_DATABASE_LOG view allows you to determine the space required in the recovery area to support the flashback activities generated by the changes in the database.

The option stating that the V$RECOVERY_FILE_DEST view is used to estimate the flashback space required for future operations is incorrect. The V$RECOVERY_FILE_DEST view provides information regarding the disk quota and current disk usage in the flash recovery area.

Item: 5 (Ref:1Z0-043.14.5.5)

You are working as a DBA in an organization. The flash recovery area files are created in '+disk1'. You want to create new flash recovery area files in the '+disk2' location. The new location of the flash recovery area files should be written in the control file and the spfile.

Which command will you issue to change the location of the flash recovery area files?

- `ALTER SYSTEM SET DB_RECOVERY_FILE_DEST = '+disk2' ;`
- `ALTER SYSTEM SET DB_RECOVER_FILE_DEST = '+disk2' SCOPE = BOTH;`
- `ALTER SYSTEM SET DB_CREATE_FILE_DEST = '+disk2';`
- `ALTER SYSTEM SET DB_CREATE_ONLINE_LOG_DEST_n = '+disk2';`

Answer:

`ALTER SYSTEM SET DB_RECOVER_FILE_DEST = '+disk2' SCOPE = BOTH;`

Explanation:

The `DB_RECOVERY_FILE_DEST` initialization parameter is used to specify the location for the creation of the `RMAN` backups, archive logs, and flashback logs. The `DB_RECOVERY_FILE_DEST` parameter is also used to specify the location of the redo log files and the control files if the `DB_CREATE_ONLINE_LOG_DEST_n` parameter is not specified. In this scenario, you must issue the following command to change the location the new flash recovery area files to 'disk2':

```
ALTER SYSTEM SET DB_RECOVER_FILE_DEST = '+disk2' SCOPE = BOTH;
```

The `SCOPE = BOTH` clause specifies that the new location of the flash recovery files are written in the control file and the spfile.

The option stating that the `ALTER SYSTEM SET DB_RECOVER_FILE_DEST = '+disk2'` command is used to specify the new location for the flash recovery files and the new location is written in the control file and the spfile is incorrect. The new location will not be written in the spfile. To make the changes in the spfile and the control file, the `SCOPE = BOTH` clause should be used in the `ALTER SYSTEM SET DB_RECOVER_FILE_DEST = '+disk2'` command.

The option stating that the `ALTER SYSTEM SET DB_CREATE_FILE_DEST = '+disk2'` command is used to specify the new location for the flash recovery files and the new location is written in the control file and spfile is incorrect. The `DB_CREATE_FILE_DEST` initialization parameter is used to specify the location of the datafiles when no file destination is specified during tablespace creation. The `DB_CREATE_FILE_DEST` parameter also specifies the location of the online redo log files and the control files if the `DB_CREATE_ONLINE_LOG_DEST_n` parameter is not specified. To change the location of the flash recovery files, the value of the `DB_RECOVER_FILE_DEST` initialization parameter should be changed.

The option stating that the `ALTER SYSTEM SET DB_CREATE_ONLINE_LOG_DEST_n = '+disk2'` command is used to specify the new location for the flash recovery files and the new location is written in the control file and spfile is incorrect. This is because the `DB_CREATE_ONLINE_LOG_DEST_n` initialization parameter is not related to the flash recovery files. The `DB_CREATE_ONLINE_LOG_DEST_n` parameter is used to specify the location of the control files and the online redo log files. To multiplex the control files and the online redo log files, you can specify up to five different values for the `DB_CREATE_ONLINE_LOG_DEST_n` parameter. To change the location of the flash recovery files, the value of the `DB_RECOVER_FILE_DEST` initialization parameter should be changed.

Item: 6 (Ref:1Z0-043.14.5.3)

You are maintaining an OLTP database in Oracle10*g*. You have configured the Flash Recovery Area in your database. The Flash Recovery Area is full because you have set the retention policy to NONE. What will you do to resolve the problem?

- Increase the value of the FAST_START_MTTR_TARGET initialization parameter.
- Increase the value of the DB_RECOVERY_FILE_DEST_SIZE parameter.
- Increase the value of the PGA_AGGREGATE_TARGET initialization parameter.
- Increase the value of the SGA_TARGET initialization parameter.

Answer:

Increase the value of the DB_RECOVERY_FILE_DEST_SIZE parameter.

Explanation:

You will increase the value of the DB_RECOVERY_FILE_DEST_SIZE parameter. When you enable the flash recovery area, you set the following initialization parameters:

- DB_RECOVERY_FILE_DEST
- DB_RECOVERY_FILE_DEST_SIZE

The DB_RECOVERY_FILE_DEST parameter is used to define the default location at which the database creates the RMAN backups when no format option is specified, the archive logs when no other local destination is configured, and the flashback logs. The DB_RECOVERY_FILE_DEST parameter is used to specify the default location of the online redo log files and the control files if the DB_CREATE_ONLINE_LOG_DEST_n parameter is not specified. The DB_RECOVERY_FILE_DEST_SIZE parameter is used to specify the size of the flash recovery area. If the retention policy is set to NONE, the flash recovery area can be filled completely with no reclaimable space. The database issues a warning level alert when 85 percent of the flash recovery area is used. When 97 percent of the flash recovery area is used, the database issues a critical level alert. The database continues to consume space until the flash recovery area becomes completely full. When the flash recovery area is full, you receive the following error:

```
ORA-19809: limit exceeded for recovery files
ORA-19804: cannot reclaim nnnnn bytes disk space from mmmmm limit
```

To resolve the problem, increase the value of the DB_RECOVERY_FILE_DEST_SIZE initialization parameter in the pfile.

Increasing the value of the FAST_START_MTTR_TARGET initialization parameter will not resolve the above problem. The FAST_START_MTTR_TARGET initialization parameter is used to specify the time required for instance recovery in seconds.

Increasing the value of the PGA_AGGREGATE_TARGET initialization parameter will not resolve the above problem. Automatic PGA Memory Management (APMM) functionality is implemented by using the PGA_AGGREEGATE_TARGET initialization parameter. The memory allocated to APPM by this parameter is dynamically managed and allocated by Oracle to meet the SQL work area requirements of all the Oracle sessions.

Increasing the value of the SGA_TARGET initialization parameter will not resolve the above problem. The SGA_TARGET initialization parameter is used to specify the total size of the system global area.

Item: 7 (Ref:1Z0-043.14.5.4)

You decided to configure the flash recovery area in your database to centralize the storage of all the recovery files in a certain location on disk. Which two parameters will you specify in the init.ora file? (Choose two.)

- DB_CREATE_FILE_DEST
- DB_RECOVERY_FILE_DEST
- DB_RECOVERY_FILE_DEST_SIZE
- DB_ONLINE_LOG_DEST_n

Answer:

DB_RECOVERY_FILE_DEST
DB_RECOVERY_FILE_DEST_SIZE

Explanation:

You are required to specify the DB_RECOVERY_FILE_DEST and DB_RECOVERY_FILE_DEST_SIZE parameters to configure the flash recovery area in your database. The DB_RECOVERY_FILE_DEST parameter is used to specify the location of the recovery files to be created and the DB_RECOVERY_FILE_DEST_SIZE parameter is used to specify the size of the flash recovery area

The option stating that you are required to specify the DB_CREATE_FILE_DEST initialization parameter to configure the flash recovery area in your database is incorrect. This is because the DB_CREATE_FILE_DEST parameter is used to specify the location of the datafiles. If the names and locations of the datafiles are not specified at tablespace creation, then the datafiles are stored in the location specified by the value of the DB_CREATE_FILE_DEST parameter

The option stating that you are required to specify the DB_CREATE_ONLINE_LOG_DEST_n parameter to configure the flash recovery area in your database is incorrect. This is because the DB_CREATE_ONLINE_LOG_DEST_n parameter is used to specify the default locations of the control files and online redo log files.

Item: 8 (Ref:1Z0-043.14.5.2)

You receive the following error:

```
ORA-19804: cannot reclaim nnnnn bytes disk space from mmmmm limit
```

Identify the reason for receiving the above error message?

- The sort area is very small.
- There is no more space in the Undo tablespace.
- The flash recovery area is full.
- The online redo log file is full.

Answer:

The flash recovery area is full.

Explanation:

If the retention policy is set to `NONE`, then the flash recovery area can be completely filled with no reclaimable space available. The database issues a warning level alert when 85 percent of the flash recovery area is used. When 97 percent of the flash recovery area is used, then the database issues a critical level alert. The database continues to consume space until the flash recovery area becomes completely full. When the flash recovery area is full, you receive the following error:

```
ORA-19809: limit exceeded for recovery files
ORA-19804: cannot reclaim nnnnn bytes disk space from mmmmm
limit
```

To resolve the problem, increase the value of the `DB_RECOVERY_FILE_DEST_SIZE` initialization parameter in the Pfile

You will not receive the `ORA-19804: cannot reclaim` *`nnnnn`* `bytes disk space from` *`mmmmm`* `limit` error when the sort area size is very small. If the sort area size is small, then you will receive the ORA-01690: sort area size too small error.

You will not receive the `ORA-19804: cannot reclaim` *`nnnnn`* `bytes disk space from` *`mmmmm`* `limit` error when there is no more space in the Undo tablespace. When a server process requires the undo space and there is no more space in the Undo tablespace, then the `ORA-01555 Snapshot too old` error is generated.

You will not receive the `ORA-19804: cannot reclaim` *`nnnnn`* `bytes disk space from` *`mmmmm`* `limit` error when the online redo log file is full. When the redo log file is full and the `LGWR` process requires more space in the redo logfiles for writing the redo log entries, then the log switch occurs and the `LGWR` process starts writing redo log entries to the next available online redo log group.

Item: 9 (Ref:1Z0-043.14.1.5)

In which two scenarios should you issue the following command? (Choose two.)

```
FLASHBACK TABLE SCOTT.EMP TO TIMESTAMP SYSTIMESTAP- INTERVAL '15'
MINUTE;
```

- ☐ when the schema of the user, SCOTT, was deleted by mistake 15 minutes ago
- ☐ when the table EMP of the SCOTT schema was dropped by mistake 15 minutes ago
- ☐ when some rows of the table, EMP, in the SCOTT schema were deleted by mistake 15 minutes ago
- ☐ when some incorrect values were inserted in the EMP table in the user Scott's schema during the last 15 minutes
- ☐ never, because FLASHBACK TABLE is not a valid command in Oracle 10*g*.

Answer:

when some rows of the table, EMP, in the SCOTT schema were deleted by mistake 15 minutes ago

when some incorrect values were inserted in the EMP table in the user Scott's schema during the last 15 minutes

---

Explanation:

The option stating that you will issue the FLASHBACK TABLE SCOTT.EMP TO TIMESTAMP SYSTIMESTAP - INTERVAL '15' MINUTE; command because some rows of the table, EMP, in the SCOTT schema were deleted by mistake 15 minutes ago is correct. The Flashback Table feature allows you to recover one or more tables to a specific point in time without performing time-consuming recovery operations, such as point-in-time recovery, which affect the availability of the rest of the database. The Flashback Table feature is different from the Flashback Drop feature because the FLASHBACK TABLE command performs an undo operation on the recent transactions of an existing table and recovers a dropped table.

The option stating that you will issue the FLASHBACK TABLE SCOTT.EMP TO TIMESTAMP SYSTIMESTAP - INTERVAL '15' MINUTE; command because some incorrect values were inserted in the table during the last 15 minutes is correct. The FLASHBACK TABLE command performs an operation to undo the changes made by the DML statements on the table.

The option stating that you will issue the FLASHBACK TABLE SCOTT.EMP TO TIMESTAMP SYSTIMESTAP - INTERVAL '15' MINUTE; command when the schema of the user, SCOTT, was deleted by mistake 15 minutes ago is incorrect. This is because if the schema of the user, SCOTT, is deleted, then the FLASHBACK DATABASE command will be used to recover the schema of the user, SCOTT, and all the objects in the schema.

The option, stating that you will issue the command FLASHBACK TABLE SCOTT.EMP TO TIMESTAMP SYSTIMESTAP - INTERVAL '15' MINUTE; when the table EMP was deleted from the schema of the user, SCOTT, by mistake 15 minutes ago is incorrect. This is because if a table is deleted from the schema of the user, SCOTT, then the FLASHBACK TABLE SCOTT.EMP TO BEFORE DROP command is used to restore the table in the user Scott's schema.

The option stating that you will never issue the FLASHBACK TABLE SCOTT.EMP TO TIMESTAMP SYSTIMESTAP - INTERVAL '15' MINUTE command because the FLASHBACK TABLE is not a valid command in Oracle 10*g* is incorrect. This is because the FLASHBACK TABLE command is used to recover one or more tables to a specific point in time.

Item: 10 (Ref:1Z0-043.14.3.1)

You are required to flashback your database. You want to find the amount of flashback data generated since the database was opened.

Which task will you perform to obtain the required information?

- Query the V$FLASHBACK_DATABASE_LOG view.
- Query the V$FLASHBACK_DATABASE_STAT view.
- Check the value of the DB_FLASHBACK_RETENTION_TARGET initialization parameter.
- Query the V$RECOVERY_FILE_DEST view.

Answer:

Query the V$FLASHBACK_DATABASE_STAT view.

Explanation:

The V$FLASHBACK_DATABASE_STAT view is used to estimate the amount of flashback data generated since the database was opened.

The V$FLASHBACK_DATABASE_STAT view is used to monitor the overhead of maintaining data in the Flashback Database logs. This view allows you to estimate the space required for future Flashback database operations. The V$FLASHBACK_DATABASE_STAT view consists of the following columns:

BEGIN_TIME: displays the start of the time interval
END_TIME: displays the end of the time interval
FLASHBACK_DATA: displays the number of bytes of flashback data written during the interval
DB_DATA: displays the number of bytes of database data read and written during the interval
REDO_DATA_TIME: displays the number of bytes of redo data written during the interval
ESTIMATED_FLASHBACK_SIZBEGIN_TIME: displays the value of the ESTIMATED_FLASHBACK_SIZE column in the V$FLASHBACK_DATABASE_LOG view at the end of the time interval

The option stating that the V$FLASHBACK_DATABASE_LOG view can be used to estimate the amount of the flashback data generated since the database was opened is incorrect. The V$FLASHBACK_DATABASE_LOG view is used to determine the estimated size of the flashback data that you require for your current target retention. The V$FLASHBACK_DATABASE_LOG view was introduced in Oracle 10*g* to support the Flashback Database feature. The V$FLASHBACK_DATABASE_LOG view allows you to determine the space required in the recovery area to support the flashback activities generated by the changes in the database.

The option stating that you check the value of the DB_FLASHBACK_RETENTION_TARGET initialization parameter in the initialization parameter file to find the amount of flashback data generated since the database was opened is incorrect. The value of the DB_FLASHBACK_RETENTION_TARGET initialization parameter specifies the retention period of the data that will be retained in the flash recovery area.

The option stating that the V$RECOVERY_FILE_DEST view is used to estimate the flashback space required for future operations is incorrect. The V$RECOVERY_FILE_DEST view provides information regarding the disk quota and the current disk usage in the flash recovery area. The columns of this view are as follows:

NAME	Displays the name of the flash recovery area
SPACE_LIMIT	Displays the maximum amount of disk space that the database can use for the flash recovery area
SPACE_USED	Displays the space used by the flash recovery area
SPACE_RECLAIMABLE	Displays the space which consists of obsolete and redundant data that can be deleted and the space reclaimed for reuse.
NUMBER_OF_FILES	Displays the number of files in the flash recovery area

Item: 11 (Ref:1Z0-043.14.2.2)

You dropped a schema of a user in an Oracle 10*g* by mistake. You decide to flash the database back to its previous state to restore the deleted schema.

Which process writes the before images of the physical database blocks to the flashback database logs?

- LGWR
- DBWR
- MMON
- RVWR

Answer:

RVWR

Explanation:

The Flashback Database Architecture consists of the recovery writer (RVWR) background process and the Flashback Database logs. When the Flashback Database feature is enabled, the RVWR process is started. Flashback Database logs are new type of files that contain a before image of physical database blocks. The RVWR process writes the Flashback Database logs in the flash recovery area. Writing Flashback Database logs are a prerequisite to using the Flashback Database feature because the Flashback database logs are written in the flash recovery area.

The option stating that the LGWR process writes the before images of the physical database blocks to the Flashback Database logs is incorrect. The LGWR process writes the redo entries from the redo log buffer to the online redo log files. Redo log buffer is a part of the SGA that contains the redo log entries. The writer writes redo entries to the redo log files under the following conditions:

- When a transaction is committed
- Every three seconds
- When the redo log buffer is 1/3 full
- When the DBWn process signals the writing of the redo records to disk

The option stating that the DBWR process writes the before images of the physical database blocks to the Flashback Database logs is incorrect. The DBWR process writes the dirty data blocks from the buffer cache to the datafiles. The DBWR process writes dirty buffers from the buffer cache to the datafiles under the following conditions:

- When a checkpoint occurs
- When a server space requires more space than the available space in the buffer cache
- Every three seconds

The option stating that the MMON process writes the before images of the physical database blocks to the Flashback Database logs is incorrect. The MMON, known as Manageability Monitor, process is responsible for filtering and transferring the memory statistics to the disk every hour. The snapshots of the memory statistics are captured at specific intervals and stored on the disk. The MMON process makes the snapshots and stores the information in the Automatic Workload Repository. The default interval is one hour or the duration over which the in-memory area becomes full.

Item: 12 (Ref:1Z0-043.14.2.1)

You are maintaining a database that is in ARCHIVELOG mode. You have configured the flash recovery area in your database. The database is in MOUNT EXCLUSIVE mode, and you want to configure the Flashback Database feature.

Which two options are **NOT** required to configure the Flashback Database feature? (Choose two.)

- Open the database in read-only mode.
- Set the retention target with the DB_FLASHBACK_RETENTION_TARGET initialization parameter.
- Enable the block change tracking feature.
- Execute the ALTER DATABASE FLASHBACK ON statement.

Answer:

Open the database in read-only mode.
Enable the block change tracking feature.

Explanation:

To configure the Flashback Database feature in a database, you need not open the database in read-only mode. The database should be in MOUNT EXCLUSIVE mode. Also, you need not enable the block change tracking feature in your database to configure the Flashback Database feature. The block change tracking feature is used to increase the performance of the backup process while performing an incremental backup.

The option stating that you need not set the retention target with the DB_FLASHBACK_RETENTION_TARGET initialization parameter to configure the Flashback Database feature in a database is incorrect. You should issue the following statement to set the value of the DB_FLASHBACK_RETENTION_TARGET parameter:

```
SQL>ALTER DB_FLASHBACK_RETENTION_TARGET=<value>;
```

The DB_RETENTION_TARGET parameter determines the point-in-time in the past to which you can flash back the database. The value of the DB_FLASHBACK_RETENTION_TARGET parameter is specified in minutes.

The option stating that you are required to execute the ALTER DATABASE FLASHBACK ON statement to configure the Flashback Database in a database is incorrect. After executing the ALTER DB_FLASHBACK_RETENTION_TARGET=<value> statement, you are required to execute the ALTER DATABASE FLASHBACK ON statement to configure the Flashback Database feature.

Item: 13 (Ref:1Z0-043.14.1.4)

At 10:30 A.M., you ran a batch job by mistake, which executed a transaction in the database. The transaction identifier of the transaction that made to the changes in the database is 0500A00627B000. At 11:10 A.M., you stopped the batch job. Now, you want to identify the changes made to the database tables by the batch job.

Which view will you query?

- DBA_PENDING_TRANSACTIONS
- DBA_AUDIT_STATEMENT
- V$FLASHBACK_DATABASE_STATS
- FLASHBACK_TRANSACTION_QUERY

Answer:

FLASHBACK_TRANSACTION_QUERY

Explanation:

You will query the FLASHBACK_TRANSACTION_QUERY view to identify the changes made to the database tables by the batch job. The FLASHBACK_TRANSACTION_QUERY view lists all the changes made by a transaction. The FLASHBACK_TRANSACTION_QUERY view also provides the SQL statements that can be used to undo the changes made by the transaction.

The option stating that you will query the DBA_PENDING_TRANSACTIONS view to identify the changes made to the database table by the job table is incorrect. The DBA_PENDING_TRANSACTIONS view is used to identify unresolved transactions.

The option stating that you will query the DBA_AUDIT_STATEMENT view to identify the changes made to the database tables by the batch job is incorrect. The DBA_AUDIT_STATEMENT view is used to display the audit trail records related to the GRANT, REVOKE, AUDIT, and ALTER SYSTEM statements.

The option stating that you will query the V$FLASHBACK_DATABASE_STATS view to identify the changes made to the database tables by batch job is incorrect. The V$FLASHBACK_DATABASE_STAT view is used to display the bytes of the flashback data logged to the database.

Item: 14 (Ref:1Z0-043.14.2.4)

Your Oracle Database 10*g* is online when you execute the following statement:

```
SQL>ALTER TABLESPACE MY_TABLESPACE FLASHBACK OFF;
```

What is the result of executing this statement if the Flashback Database feature is already enabled in the database?

- The database does not record flashback logs for MY_TABLESPACE.
- The tables residing in MY_TABLESPACE are not protected by the Recycle Bin.
- All the tablespaces except MY_TABLESPACE can be recovered using Flashback Database feature.
- None of the flashback technologies, such as Flashback Table, Flashback Transaction Query and Flashback Version Query can be used to recover individual rows within the objects from MY_TABLESPACE.

Answer:

The database does not record flashback logs for MY_TABLESPACE.

Explanation:

When the ALTER TABLESPACE MY_TABLESPACE FLASHBACK OFF statement is executed, the database does not record flashback logs for MY_TABLESPACE. The MY_TABLESPACE is excluded from participating in the flashback of the database.

The Flashback Database feature depends entirely on the flashback logs. Therefore, you cannot flash back the database if you do not have all the necessary flashback logs. However, flashback technologies such as Flashback Drop are based on the undo data rather than on the flashback logs. Also, flashback technologies are enabled by default. This means that even if the tablespace is excluded from participating in the flashback of the database, objects within this tablespace are protected through the Recycle Bin. For example, if a table residing in MY_TABLESPACE is dropped, you can recover the table by using Flashback Drop which uses the Recycle Bin to store copies of the dropped tables. Therefore, the option stating that the database does not record flashback logs for MY_TABLESPACE is incorrect.

If a tablespace is dropped, you cannot recover it even by using Flashback Database. For example, if a tablespace is dropped around 5:00 P.M, you cannot undo the result of a dropped tablespace operation even if you recover the database up to 4:59 P.M. Therefore, the option stating that all tablespaces except MY_TABLESPACE can be recovered using Flashback Database is incorrect.

Because all flashback technologies except Flashback Database are not based on flashback logs, you can use flashback technologies such as Flashback Table, Flashback Transaction Query, and Flashback Version Query to recover individual rows within objects from MY_TABLESPACE. Therefore, the option stating that none of the flashback technologies can be used to recover individual rows within the objects from MY_TABLESPACE is incorrect.

Item: 15 (Ref:1Z0-043.14.5.8)

You have configured the flash recovery area to store online redo log files, control files, archived redo logs and RMAN backups. Which of the following files can you successfully delete from the flash recovery area if you want to reclaim the space within it?

- multiplexed control files
- RMAN obsolete backups
- multiplexed online redo log files
- archived redo logs that have not been copied to tape

Answer:

RMAN obsolete backups

Explanation:

RMAN obsolete backups can be deleted from the flash recovery area. Within the flash recovery area, transient files are those files that can be deleted when they become obsolete as per the retention policy or when they have been backed up to tape. When the backups become obsolete they are not needed for recovery and they can be deleted. Files such as archived redo logs, backup copies and control file auto-backups are some examples of transient files. Transient files should only be deleted from the flash recovery area after they have been backed up to tape or are no longer needed.

Multiplexed control files are considered to be permanent files within the flash recovery area and cannot be deleted.

Multiplexed online redo log files are considered to be permanent files within the flash recovery area and cannot be deleted.

Archived redo logs that have not been copied to tape should not be deleted from the flash recovery area. They should only be deleted after they have been backed up or are no longer needed.

Item: 16 (Ref:1Z0-043.14.5.7)

You are working as a DBA on Oracle Database 9*i*. You plan to upgrade your 9*i* database to Oracle 10*g*. To be familiar with the new database technology, you decide to install Oracle Database 10*g* on your workstation at home. You create a general purpose database.

After the installation, you make the following changes in your initialization parameter file:

```
LOG_ARCHIVE_DEST_1='LOCATION=USE_DB_RECOVERY_FILE_DEST'
DB_RECOVERY_FILE_DEST =
'LOCATION=d:\product\10.1.0\flash_recovery_area'
DB_RECOVERY_FILE_DEST_SIZE=10g
```

Where are the archived redo logs stored for your database?

- The archived redo logs are stored in an operating system-dependent location.
- The archived redo logs are stored in the location specified by LOG_ARCHIVE_DEST_1.
- The archived redo logs are stored in the location specified by DB_RECOVERY_FILE_DEST.
- The archived redo logs are stored in the locations specified by both LOG_ARCHIVE_DEST_1 and DB_RECOVERY_FILE_DEST.

Answer:

The archived redo logs are stored in the location specified by DB_RECOVERY_FILE_DEST.

Explanation:

In the given scenario, the archived redo logs are stored in the location specified by DB_RECOVERY_FILE_DEST. The LOG_ARCHIVE_DEST_1 through LOG_ARCHIVE_DEST_10 parameters specify up to ten archive log destinations. The DB_RECOVERY_FILE_DEST parameter specifies the location for the flash recovery area. If the LOG_ARCHIVE_DEST_1 and DB_RECOVERY_FILE_DEST parameters have been set to different locations in your initialization parameter file, then the value of the LOG_ARCHIVE_DEST_1 parameter overrides the value of the DB_RECOVERY_FILE_DEST parameter, and the archived redo logs are stored in the location specified by LOG_ARCHIVE_DEST_1. However, if LOG_ARCHIVE_DEST_1 specifies a location of USE_DB_RECOVERY_FILE_DEST, then the archived redo logs are stored only in the flash recovery area, as identified by the DB_RECOVERY_FILE_DEST parameter. Also, if the LOG_ARCHIVE_DEST_1 parameter is not included in the initialization parameter file but the DB_RECOVERY_FILE_DEST parameter is included, the archived redo logs are stored in the flash recovery area. In this case, Oracle implicitly sets LOG_ARCHIVE_DEST_1 to use the flash recovery area.

The option stating that the archived redo logs are stored in an operating system-dependent location is incorrect because archived redo logs are only stored in an operating system-dependent location if neither the LOG_ARCHIVE_DEST_n nor the DB_RECOVERY_FILE_DEST parameter is specified.

The option stating that archived redo logs are stored in the location specified by LOG_ARCHIVE_DEST_1 is incorrect because no distinct location has been set up for the LOG_ARCHIVE_DEST_1 parameter. You have set up the LOG_ARCHIVE_DEST_1 parameter so that it uses the location of the flash recovery area to archive redo log files.

The option stating that archived redo logs are stored in locations specified by both LOG_ARCHIVE_DEST_1 and DB_RECOVERY_FILE_DEST is incorrect because the archived redo logs are stored in only one location.

Item: 17 (Ref:1Z0-043.14.3.4)

Flashback Database is enabled in your Oracle 10*g* database. One of your database users erroneously purged an important table residing in his schema. The table was purged sometime between 10:00 P.M. and 10:30 P.M. The next day, you decide to flash back the database. Before you flash back the database, you want to ensure that you have all the necessary flashback data.

Which dynamic performance view must you use to determine whether you have the required flashback data to recover the purged table?

- V$DATABASE
- V$UNDOSTAT
- V$FLASHBACK_DATABASE_LOG
- V$FLASHBACK_DATABASE_STAT

Answer:

V$FLASHBACK_DATABASE_LOG

Explanation:

You can use the V$FLASHBACK_DATABASE_LOG dynamic performance view to determine whether you have the required flashback data to recover the purged table. You can execute the following query to determine whether you can flash back the database to its state before the table was dropped:

```
SELECT oldest_flashback_time FROM v$flashback_database_log;
```

The column OLDEST_FLASHBACK_TIME from the V$FLASHBACK_DATABASE_LOG returns the time of the lowest System Change Number (SCN) from the flashback data. If the time mentioned in the OLDEST_FLASHBACK_TIME column is less than the time at which the table was dropped, you can flash back the database to the time before the DROP TABLE statement was issued.

The V$DATABASE dynamic performance view cannot be used to determine the availability of the necessary flashback data. You can use the V$DATABASE dynamic performance view to verify whether Flashback Database is enabled in the database.

You cannot use the V$UNDOSTAT dynamic performance view to determine the availability of the necessary flashback data. This view is used to display the statistics about the undo data, such as undo space consumption, transaction concurrency, and length of queries executed in the instance. You can use this view to help in tuning the undo usage in your database.

The V$FLASHBACK_DATABASE_STAT dynamic performance view cannot be used to determine the availability of the necessary flashback data. The V$FLASHBACK_DATABASE_STAT is used to show the bytes of flashback data logged by the database and also displays an estimate of flashback space required based on previous workload.

Item: 18 (Ref:1Z0-043.14.4.1)

An important tablespace of your database is dropped by mistake. You use the Flashback Database feature to retrieve the tablespace. You perform the following steps to retrieve the tablespace:

1. You log on to Enterprise Manager as SYSDBA.
2. You select the maintenance screen.
3. You choose Perform Recovery option on the maintenance screen.
4. You choose Whole Database in the Object Type drop-down list Perform Recovery: Type screen.
5. You choose Recover to Current Time from the Operation Type on the Perform Recovery: Type screen.
6. You provide the Host Credentials for a database user. on the Perform Recovery: Type screen.
7. You click the continue button.

An information screen appears saying that the database is unavailable. What is this information screen?

- Recovery Manager
- Recovery Window
- Recovery Wizard
- Enterprise Manager Home Page

Answer:

Recovery Wizard

Explanation:

The information screen saying that the database is unavailable is the Recovery Wizard. The Recovery Wizard is used to Flashback a Database using Enterprise Manager.

After you select the recovery operation type, the Recovery Wizard appears. This screen informs you that the database will be shutdown and restarted in mount stage. This operation will take several minutes.

The option stating that the information screen is the Recovery Manager is incorrect. The Recovery Manager is a tool used to perform the backup and recovery operations. Recovery Manager provides the automatic backup management.

The option stating that the information screen is the Recovery Window is incorrect. The Recovery Window is implemented by RMAN to control backups from being expired.

The option stating that the information screen is the Enterprise Manager Home Page is incorrect. The Enterprise Manager Home Page appears when you log on to the Enterprise Manager.

Item: 19 (Ref:1Z0-043.14.1.1)

In which scenario do you use the Flashback Database feature?

- when a table is dropped and you restore it from the Recycle Bin
- when a user's schema is dropped and you recover the user's schema
- when some incorrect data is inserted in the table and you retrieve the table to a state that was at a certain timestamp
- when a row of a table is updated frequently and committed, and you view all the versions of the row within a specific duration

Answer:

when a user's schema is dropped and you recover the user's schema

---

Explanation:

When a user's schema is dropped the Flashback Database feature is used to recover the schema of the user. The Flashback Database feature enables you to retrieve the entire database back to a specific point-in-time. Therefore, this feature helps you recover from errors, such as a large table truncated, a batch job not completed, or a user schema dropped.

The option stating that when a table is dropped, you use the Flashback Database feature restore it from the Recycle Bin is incorrect. The Flashback Drop feature is used to restore the dropped table from the Recycle Bin.

The option stating that when some incorrect data is inserted in the table and you use the Flashback Database feature to retrieve the table to a state that was at a certain timestamp is incorrect. The Flashback Table feature enables you to recover a table to a specific point-in-time without performing an incomplete recovery.

The option stating that when a row of a table is updated frequently and committed, you use the Flashback Table feature to view all the versions of the row within a specific duration is incorrect. The Flashback Version Query feature enables you to view all the versions of a particular row within a specific duration.

Item: 20 (Ref:1Z0-043.14.2.6)

You have joined a new organization as a Database Administrator. The Security Administrator in your organization has kept human errors, such as erroneously dropping users, tables, and important data, to a minimum by carefully granting only the necessary privileges to each user. As a result of several ongoing transactions within your database, you discover that the flashback logs are rapidly increasing in the flash recovery area. To avoid out-of-space errors, you decide to delete the flashback logs from the flash recovery area.

How can you delete the flashback logs from the database if your database is up and running?

- Shut down the database using the SHUTDOWN command. Mount the database using the STARTUP MOUNT EXCLUSIVE command and disable Flashback Database using the ALTER DATABASE FLASHBACK OFF statement.
- Change the parameter setting in the SPFILE for the DB_RECOVERY_FILE_DEST parameter using the ALTER SYSTEM SET DB_RECOVERY_FILE_DEST='' SCOPE=BOTH statement while the database is up and running.
- Shut down the database using the SHUTDOWN command. Mount the database using the STARTUP MOUNT EXCLUSIVE command. Change the parameter setting in the SPFILE for the DB_RECOVERY_FILE_DEST parameter using the ALTER SYSTEM SET DB_RECOVERY_FILE_DEST='' SCOPE=BOTH statement. Disable Flashback Database using the ALTER DATABASE FLASHBACK OFF statement.
- Change the parameter setting in the SPFILE for the DB_RECOVERY_FILE_DEST parameter using the ALTER SYSTEM SET DB_RECOVERY_FILE_DEST='' SCOPE=BOTH statement. Shut down the database using the SHUTDOWN command. Mount the database using the STARTUP MOUNT EXCLUSIVE command and disable Flashback Database using the ALTER DATABASE FLASHBACK OFF statement.

Answer:

Shut down the database using the SHUTDOWN command. Mount the database using the STARTUP MOUNT EXCLUSIVE command and disable Flashback Database using the ALTER DATABASE FLASHBACK OFF statement.

Explanation:

You can use the following set of commands to delete the flashback logs from the flash recovery area if your database is up and running:

```
SHUTDOWN
STARTUP MOUNT EXCLUSIVE
ALTER DATABASE FLASHBACK OFF;
```

When you disable Flashback Database using the ALTER DATABASE FLASHBACK OFF statement, the flashback logs will be automatically deleted from the flash recovery area.

The option stating that only the parameter setting for the DB_RECOVERY_FILE_DEST initialization parameter needs to be changed to disable Flashback Database is an incorrect option because changing this parameter setting will not disable Flashback Database. This operation will continue to result in the ORA-02097 and ORA-38775 errors. To disable the flashback database feature you must issue the SHUTDOWN, STARTUP, and ALTER DATABASE statements mentioned above.

Executing the ALTER SYSTEM SET DB_RECOVERY_FILE_DEST='' SCOPE=BOTH statement while the database is up and running, and then executing the ALTER DATABASE FLASHBACK OFF statement when the database is in the MOUNT mode, will result in the ORA-02097 and ORA-38775 errors. The DB_RECOVERY_FILE_DEST initialization parameter specifies the location of the flash recovery area within the database. The setup of the flash recovery area is a prerequisite for using the Flashback Database feature. You must have a setting for this parameter in your initialization parameter file before you enable Flashback Database. You must also disable Flashback Database before disabling the flash recovery area. Attempting to disable the flash recovery area before disabling Flashback Database using the ALTER SYSTEM SET DB_RECOVERY_FILE_DEST='' SCOPE=BOTH statement, will result in the following errors:

```
ORA-02097: parameter cannot modified because specified value is
invalid
ORA-38775: cannot disable flash recovery area flashback
database is enabled
```

You will still receive the ORA-02097 and ORA-38775 errors if you try to change the parameter setting using the ALTER SYSTEM SET DB_RECOVERY_FILE_DEST='' SCOPE=BOTH statement in the MOUNT mode, before executing the ALTER DATABASE FLASHBACK OFF statement. The DB_RECOVERY_FILE_DEST initialization parameter specifies the location of the flash recovery area within the database. The setup of the flash recovery area is a prerequisite for using the Flashback Database

feature. You must have a setting for this parameter in your initialization parameter file before you enable Flashback Database. You must disable Flashback Database before disabling the flash recovery area. Attempting to disable the flash recovery area before disabling Flashback Database using the `ALTER SYSTEM SET DB_RECOVERY_FILE_DEST='' SCOPE=BOTH` statement, will result in an error.

Item: 21 (Ref:1Z0-043.14.3.2)

You are working as a DBA at NetFx Corporation. You discover that the SCOTT schema is deleted by mistake. You decide to flash the database back to the time when the schema existed.

Which view will you query to determine the estimated size of the flashback data that you require for your current target retention?

- V$FLASHBACK_DATABASE_LOG
- V$FLASHBACK_DATABASE_STAT
- V$DATABASE
- V$UNDOSTAT

Answer:

V$FLASHBACK_DATABASE_LOG

Explanation:

The V$FLASHBACK_DATABASE_LOG view is used to determine the estimated size of the flashback data that you require for your current target retention. The V$FLASHBACK_DATABASE_LOG view was created to support the Flashback Database feature and was introduced in Oracle 10*g*. The V$FLASHBACK_DATABASE_LOG view allows you to determine the space required in the recovery area to support the flashback activity generated by the changes in the database. The ESTIMATED_FLASHBACK_SIZE column is used to estimate the required size of the flashback data for your current target retention.

The option stating that the V$FLASHBACK_DATABASE_STAT view is used to determine the estimated size of the flashback data that you require for your current target retention is incorrect. The V$FLASHBACK_DATABASE_STAT view is used to monitor the overhead of maintaining the data in the Flashback Database logs.

The option stating that the V$DATABASE view is used to determine the estimated size of the flashback data that you require for your current target retention is incorrect. The V$DATABASE view displays whether the Flashback Database is on or off, which indicates whether the Flashback Database feature is enabled or disabled.

The option stating that the V$RECOVERY_FILE_DEST view is used to determine the estimated size of the flashback data that you require for your current target retention is incorrect. The V$RECOVERY_FILE_DEST view provides information about the disk quota and current disk usage in the flash recovery area.

Item: 22 (Ref:1Z0-043.14.1.2)

In which scenario will you use the Flashback Version Query feature?

- when you want to restore a table that has been dropped from the Recycle Bin
- when you want to identify the transaction ID of the transaction that deleted some important records from a table
- when you want to recover the schema of a dropped user
- when you want to restore a dropped tablespace

Answer:

when you want to identify the transaction ID of the transaction that deleted some important records from a table

---

Explanation:

You will use the Flashback Version Query feature if you want to identify the transaction ID of a transaction that deleted some important records from a table. The Flashback Version Query feature provides a history of the changes made to a row along with the corresponding identifiers of the transactions that made the changes. You should use the transaction identifier provided by the Flashback Version Query feature in the Flashback Transaction Query to identify the user who made the changes in the database by running the specific transaction. The Flashback Transaction Query feature provides Undo SQL statements to undo the changes made by a specific transaction.

The option stating that you will use the Flashback Version Query feature when you want to restore a table that has been dropped from the Recycle Bin is incorrect. This is because the Flashback Version Query feature is not used to restore a dropped table from the Recycle Bin. The Flashback Drop feature is used to restore a dropped table from the Recycle Bin.

The option stating that you use the Flashback Version Query feature when you want to recover the schema of a dropped user is incorrect. This is because the Flashback Version Query feature is not used to recover a dropped user's schema. The Flashback Database feature is used to recover a dropped user's schema.

The option stating that you will use the Flashback Version Query feature when you want to restore a dropped tablespace is incorrect. If a tablespace is dropped from the database and you want to restore the dropped tablespace, then you must use the Flashback Database feature.

Item: 23 (Ref:1Z0-043.14.5.6)

You decide to enable Flashback Database in your Oracle 10*g* database so that future recoveries will take less time than traditional recoveries.

Which of the following parameters must be included in your initialization parameter file before enabling Flashback Database?

- DB_RECOVERY_FILE_DEST only
- DB_FLASHBACK_RETENTION_TARGET only
- DB_RECOVERY_FILE_DEST_SIZE and DB_RECOVERY_FILE_DEST only
- DB_RECOVERY_FILE_DEST and DB_FLASHBACK_RETENTION_TARGET only
- DB_RECOVERY_FILE_DEST_SIZE, DB_RECOVERY_FILE_DEST and
- DB_FLASHBACK_RETENTION_TARGET

Answer:

DB_RECOVERY_FILE_DEST_SIZE and DB_RECOVERY_FILE_DEST only

Explanation:

You must include the DB_RECOVERY_FILE_DEST_SIZE and DB_RECOVERY_FILE_DEST parameters in your initialization parameter file before enabling Flashback Database. Both these parameters enable the flash recovery area, which is a prerequisite for using Flashback Database. The DB_RECOVERY_FILE_DEST_SIZE initialization parameter specifies the maximum size in bytes allowed for the flash recovery area. The DB_RECOVERY_FILE_DEST initialization parameter specifies the location of the flash recovery area. These two initialization parameters must be included in the initialization parameter file because there are no default values for these parameters. If either of these parameters is not specified in the initialization parameter file, the instance does not start and you receive the following errors:

```
LRM-00109: could not open parameter file 'd:\init.ora'
ORA-01078: failure in processing system parameters
```

Therefore, you must set both these parameters to enable Flashback Database. Not setting any of these parameters in the initialization parameter file will start the instance, but the Flashback Database feature will not be enabled. Of the two parameters, the DB_RECOVERY_FILE_DEST_SIZE must be set *before* DB_RECOVERY_FILE_DEST.
When enabling Flashback Database, you can also include the DB_FLASHBACK_RETENTION_TARGET parameter in the initialization parameter file. This parameter defines the retention period in minutes allowed for the flash recovery area. This parameter has a default value of 1440 minutes, which corresponds to one day. Therefore, this parameter setting is not mandatory. If you do not include the DB_FLASHBACK_RETENTION_TARGET parameter in the initialization parameter file, you will not receive any error and the default value for this parameter will be used.

Specifying only the DB_RECOVERY_FILE_DEST initialization parameter in the initialization parameter file will result in the LRM-00109 and ORA-01078 errors because both the DB_RECOVERY_FILE_DEST and DB_RECOVERY_FILE_DEST_SIZE parameters must have values when enabling Flashback Database.

Specifying only the DB_FLASHBACK_RETENTION_TARGET initialization parameter will result in the LRM-00109 and ORA-01078 errors because when enabling Flashback Database the DB_RECOVERY_FILE_DEST_SIZE and DB_RECOVERY_FILE_DEST parameters are mandatory in the initialization parameter file.

If you include only the DB_RECOVERY_FILE_DEST and DB_FLASHBACK_RETENTION_TARGET parameters in the initialization parameter file, you will still receive the LRM-00109 and ORA-01078 errors because the DB_RECOVERY_FILE_DEST_SIZE parameter is mandatory when enabling Flashback Database.

Specifying all the three parameters, DB_RECOVERY_FILE_DEST_SIZE, DB_RECOVERY_FILE_DEST and DB_FLASHBACK_RETENTION_TARGET, in the initialization parameter file before enabling Flashback Database is not mandatory. Only the DB_RECOVERY_FILE_DEST_SIZE and DB_RECOVERY_FILE_DEST parameters are mandatory.

Item: 24 (Ref:1Z0-043.14.2.5)

You erroneously dropped a user from the database. You must undo the effects of the DROP USER statement. You know that you dropped the user between 11:35 A.M. and 11:45 A.M. You decide to rewind the database up to 11:32:09 A.M. by using the following statement:

```
SQL>FLASHBACK DATABASE TO BEFORE TIMESTAMP
(TO_TIMESTAMP('2005-04-23 11:32:09', 'YYYY-MM-DD HH24:MI:SS'));
```

However, you encounter the following errors:

```
ORA-38753: Cannot flashback data file 6; no flashback log data
ORA-01110: data file 6: 'c:\A.DBF'
```

You verify the flashback details and discover that the maximum point in time at which your database can be rewound is 2005-04-20 12:00:09 P.M.

How would you resolve these errors?

- Increase the size of the flash recovery area and re-execute the FLASHBACK DATABASE statement.
- Increase the flashback retention period and re-execute the FLASHBACK DATABASE statement.
- Take the c:\A.DBF datafile offline and re-execute the FLASHBACK DATABASE statement.
- Decrease the flashback retention period and re-execute the FLASHBACK DATABASE statement.

Answer:

Take the c:\A.DBF datafile offline and re-execute the FLASHBACK DATABASE statement.

Explanation:

You must take the c:\A.DBF datafile offline before performing flashback on the database because the tablespace is excluded from participating in Flashback Database. You query the V$FLASHBACK_DATABASE_LOG to determine the maximum point in time at which your database can be flashed back. You query this dynamic performance view and discover that the database can be recovered up to April 20, 2005 at 12:00:09 P.M. This means the database already has the necessary flashback logs to flash back the database up to the time desired, '2005-04-23 11:32:09'. The errors ORA-38753 and ORA-01110 indicate that for one datafile, c:\A.DBF, there are insufficient flashback logs. This situation can only be possible if the c:\A.DBF datafile is excluded from participating in Flashback Database. You can query the V$TABLESPACE dynamic performance view to check whether the datafile c:\A.DBF is excluded from participating in Flashback Database using the following query:

```
SQL>SELECT flashback_on FROM v$tablespace WHERE name='A';
```

Before executing the FLASHBACK DATABASE statement, you must bring the tablespace offline by using the following statement:

```
SQL>ALTER TABLESPACE a OFFLINE;
```

Then, you can execute the given FLASHBACK DATABASE statement to rewind the database up to the desired time.

The option stating that increasing the size of the flash recovery area and re-executing the FLASHBACK DATABASE statement resolves the ORA-38753 and ORA-01110 errors is incorrect. Increasing the DB_RECOVERY_FILE_DEST_SIZE will not resolve these errors because the errors are specific to the c:\A.DBF datafile. To resolve the error you must take the datafile offline so that it does not participate in Flashback Database.

The option stating that increasing the flashback retention period and re-executing the FLASHBACK DATABASE statement resolves the problem is incorrect. The oldest flashback time to which the database can be flashed back is less than the specified time. In the given scenario, the maximum time up to which the database can be flashed back is '2005-04-20 12:00:09', which is less than the specified time '2005-04-23 11:32:09'. Increasing the retention period will not help to solve the problem.

The option stating to decrease the flashback retention period and re-execute the FLASHBACK DATABASE statement does not resolve the ORA-38753 and ORA-01110 errors. In this scenario, the retention period is sufficient. If the retention period decreases, you might not be able to flash back the database to the desired time if there is inadequate space in the flash recovery area.

Item: 25 (Ref:1Z0-043.14.1.6)

You query the ORDERS table and discover that order number 1101 is missing. One of your reports, generated at 5:00 A.M. on April 23, 2005 using Oracle Reports, includes this order number in the output. You have inserted 100 new orders into the ORDERS table since generating this report.

Which flashback technology would you use to recover order number 1101 into the ORDERS table without losing the 100 orders that you added after the report was generated?

- Flashback Table
- Flashback Query
- Flashback Version Query
- Flashback Transaction Query

Answer:

Flashback Query

Explanation:

In the given scenario, you can use Flashback Query to insert order number 1101 back into the ORDERS table. Flashback Query is used to query data which existed at a given time. To do this, the undo data stored in the database is used by the Flashback Query feature. In this scenario, you know the exact time at which this order existed in the ORDERS table. You can use the following statement to insert the row for order number 1101 back into the ORDERS table:

```
INSERT INTO orders
SELECT * FROM orders AS OF TIMESTAMP
TO_TIMESTAMP('2005-04-23 05:00:00', 'YYYY-MM-DD HH24:MI:SS')
WHERE order_no=1101;
```

Flashback Table allows you to recover a table to a specific time without performing an incomplete media recovery. You can use this technology to recover the ORDERS table to a time before order number 1101 was deleted. This would recover order number 1101, but all the inserted orders would also be flashed back. Therefore, Flashback Table would not recover order number 1101 without losing the 100 orders that you added after the report was generated.

Using Flashback Version Query, you can view all the versions of the rows of a table that existed within a specific time period. This feature can only be used to view this information and cannot be used to perform any action on the lost data in the table. This feature cannot be used to insert the missing order number into the ORDERS table.

Flashback Transaction Query is used to access all the changes made by a given transaction or all the transactions within a particular time period. This feature can only be used to retrieve this information and cannot be used to perform any action on the lost data in the table. Therefore, it cannot be used to recover missing order number 1101.

Item: 26 (Ref:1Z0-043.14.1.3)

In which scenario will you use the Flashback Transaction Query feature?

- when you want to restore an important table that is dropped from the Recycle Bin
- when you want to obtain the SQL statements to undo the deletion of some important records from a table by a transaction
- when you want to restore a dropped user's schema
- when a row of a table is updated many times within a specific time period and you want all the versions of the row in the specified time period

Answer:

when you want to obtain the SQL statements to undo the deletion of some important records from a table by a transaction

---

Explanation:

You will use the Flashback Version Query feature and the Flashback Transaction Query feature when you want to obtain the SQL statements to undo the deletion of some important records from a table by a transaction. The Oracle Flashback Version Query feature provides a history of the changes made to a row along with the corresponding identifiers of the transactions that made the changes. You should use the transaction identifier provided by the Flashback Version Query feature in the Flashback Transaction Query to identify the user who made the changes in the database by running the specific transaction. The Flashback Transaction Query feature provides the Undo SQL statements to undo the changes made by a specific transaction.

The option stating that you should use the Flashback Transaction Query feature when you want to restore an important table that is dropped from the Recycle Bin is incorrect. This is because the Flashback Transaction Query feature is not used to restore the dropped table from the Recycle Bin. The Flashback Drop feature is used to restore the dropped table from the Recycle Bin. The Flashback Transaction Query feature provides the Undo SQL statements to undo the changes made by a specific transaction.

The option stating that you should use the Flashback Transaction Query when you want to restore a dropped user's schema is incorrect. The Flashback Database feature is used to recover the schema of a dropped user.

The option stating that you should use the Flashback Transaction Query feature when a row of a table is updated many times within a specific time period and you want all the versions of the row in the specified time period is incorrect. The Flashback Version Query is used to view all the versions of a row within a specific time period.

Recovering from User Errors

Item: 1 (Ref:1Z0-043.4.5.3)

You are employed as a DBA in an organization. You are informed that the record of EMP_NO 1000 is missing from the SCOTT.EMP table. You are required to identify the user who deleted the record, the SQL statement that will undo the deletion, and the transaction ID of the transaction that deleted the employee record.
Which feature will you use to perform the tasks?

- Only the Flashback Table
- Both the Flashback Transaction Query and the Flashback Version Query
- Only the Flashback Drop
- Only the Flashback Version

Answer:

Both the Flashback Transaction Query and the Flashback Version Query

---

Explanation:

Both the Flashback Version Query and the Flashback Transaction Query should be used to identify the user who deleted the record, the transaction ID of the transaction that deleted the employee record, and the undo SQL statements that will undo the deletion of the record. Oracle Flashback Version Query and Oracle Flashback Transaction Query are referred to as complementary features. The Oracle Flashback Version Query feature provides a history of the changes made to a row along with the corresponding identifiers of the transactions that made the changes. You should use the transaction identifier provided by the Flashback Version Query feature in the Flashback Transaction Query to identify the user who made the changes in the database by running the specific transaction. The Flashback Transaction Query feature provides the Undo SQL statements to undo the changes made by a specific transaction.

The option stating that the Flashback Table feature can be used to identify the user who deleted the record, the transaction ID of the transaction that deleted the employee record, and the Undo SQL statements that will undo the deletion of the record is incorrect. The Flashback Table feature cannot be used for this purpose. The Flashback Table feature is used to flash a table back to its previous state. The Flashback Table feature allows you to recover one or more tables to a specific point in time without having to use more time-consuming recovery operations, such as a point-in-time recovery, which may also affect the availability of the rest of the database. The Flashback Table feature recovers the table by rolling back only the changes made to the tables and to their dependent objects, such as indexes.

The option stating that the Flashback Drop feature can be used to identify the user who deleted the record, the transaction ID of the transaction that deleted the employee record, and the Undo SQL statements that will undo the deletion of the record is incorrect. The Flashback Drop feature is used to restore a dropped table from the Recycle Bin. The Flashback Drop feature allows you to restore a dropped table without performing a point-in-time recovery that was required in previous versions of Oracle. While a point-in-time recovery effectively restores a table and its contents to a point in time before the table was dropped, the process is potentially time consuming. Another disadvantage of using the point-in-time recovery is that you might lose work from other transactions that occurred within the same tablespace after the table was dropped.

The option stating that the Flashback Version Query feature can only be used to identify the user who deleted the record, the transaction ID of the transaction that deleted the employee record, and the Undo SQL statements that will undo the deletion of the record is incorrect. To identify the user, it is necessary to use both the Flashback Version Query and the Flashback Transaction Query features.

To view information about the transaction ID, user and undo SQL statements used to reverse the deletion, first use the following flashback version query to identify the transaction identifier for the transaction that deleted EMP_NO 1000:

```
SQL> SELECT versions_xid,
versions_operation
2 FROM hr.emp
3 VERSIONS BETWEEN SCN MINVALUE AND MAXVALUE
4 WHERE employee_id = 100;

VERSIONS_XID VERSIONS_OPERATION
-------------------- --------------------
0100043E23456 D
```

Next, specify the transaction identifier, 0100043E23456, in the flashback transaction query to determine the user who deleted the record. The transaction identifier also enables you to determine the SQL statements that can be used for reversing the

deletion.

```
SELECT operation, undo_sql, logon_user
FROM FLASHBACK_TRANSACTION_QUERY
WHERE xid=
HEXTORAW('0100043E23456');
```

Item: 2 (Ref:1Z0-043.4.4.2)

At 5:30 PM, a database administrator, William, is informed that an important record of employee no E0025 is missing from the SCOTT.EMPLOYEE table. At 4:30 P.M, the table contained the record of employee no E0025. William issues the following command to find the SQL statements that are used to undo the deletion:

```
SELECT operation, undo_sql, logon_user
FROM FLASHBACK_TRANSACTION_QUERY
WHERE xid=
HEXTORAW('0100043E23456');
```

where '0100043E23456' is the transaction ID of the transaction that deleted the row.

Before issuing the above statement, which task did William perform to identify the transaction ID of the transaction that deleted the row?

- William used the Flashback Version Query feature.
- William issued the CROSSCHECK command at the RMAN prompt.
- William viewed the alert log file.
- William used the Flashback Table feature.

Answer:

William used the Flashback Version Query feature.

Explanation:

In this scenario, William used the Flashback Version Query feature to identify the transaction ID of the transaction that deleted the row. The Oracle Flashback Version Query feature provides a history of the changes made to a row along with the corresponding identifiers of the transactions that made the changes.

Both the Flashback Version Query and the Flashback Transaction Query features should be used to identify the user who deleted the record, the transaction ID of the transaction that deleted the employee record, and the undo SQL statements that will undo the deletion of the record. Oracle Flashback Version Query and Oracle Flashback Transaction Query are referred to as complementary features. The Oracle Flashback Version Query feature provides a history of the changes made to a row along with the corresponding identifiers of the transactions that made the changes. You should use the transaction identifier provided by the Flashback Version Query feature in the Flashback Transaction Query to identify the user that made the changes in the database by running the specific transaction. The Flashback Transaction Query feature provides the Undo SQL statements to undo the changes made by a specific transaction.

The option stating that William identified the transaction ID of the transaction that deleted the row of employee no E0025 by issuing the CROSSCHECK prompt is incorrect. The CROSSCHECK command is used to verify the physical existence of the backup sets and image copies on the storage media.

The option stating that William identified the transaction ID of the transaction that deleted the row of the employee no E0025 by viewing the alert log file is incorrect. This is because the transaction IDs of the transactions are not written in the alert log file. The alert log file contains information regarding the log switch, nondefault parameter values, and so on.

The option stating that William identified the transaction ID of the transaction that deleted the row of the employee no E0025 by using the Flashback Table feature is incorrect. This is because the Flashback Table feature does not provide the transaction IDs of the transactions made to the database. The Flashback Table feature allows you to recover a table to a specific point-in-time without performing an incomplete recovery. All the dependent objects are also recovered when you use the Flashback Table feature.

Item: 3 (Ref:1Z0-043.4.5.1)

You want to use the Flashback Transaction Query feature to identify all the changes made to your database within a specific time period. What is a prerequisite for using the Flashback Transaction Query feature?

- You must use automatic undo management in the database.
- You must configure OMF in your database.
- You must configure ASM for storing the datafiles.
- You must multiplex the online redo log file.

Answer:

You must use automatic undo management in the database.

Explanation:

To use the Flashback Transaction Query feature, you must use automatic undo management in your database. The Flashback Transaction Query, which is based on undo data, utilizes the `UNDO_RETENTION` initialization parameter to determine the amount of time for which committed undo data is retained in the database. The `UNDO_RETENTION` initialization parameter, which is specified in seconds, determines the amount of committed undo data that should be kept in the database. If transactions require additional undo space and there is no more space in the `UNDO` tablespace, then Oracle starts reusing the undo space. The `RETENTION GUARANTEE` option, which can be set on the `UNDO` tablespace, protects undo data from being overwritten.

The option stating that you must configure OMF in your database for using the Flashback Transaction Query is incorrect. It is not necessary to configure OMF in the database to use the Flashback Transaction Query feature. The Oracle Managed Files (OMF) feature is configured for the control file, the names, and the datafiles. If OMF is configured in your database and you do not specify the names and sizes of the datafiles during tablespace creation, then Oracle automatically assigns names and sizes to the datafiles associated with that tablespace.

The option stating that you must configure ASM for storing the datafiles is incorrect. It is not necessary to configure ASM to use the Flashback Transaction Query feature for storing the datafiles. The ASM is used to enhance the performance because ASM automatically spreads database objects over multiple devices. ASM increases the availability by allowing new disk devices to be added to the database without shutting down the database.

The option stating that you must multiplex the online redo log file for using the Flashback Transaction Query Feature is incorrect. Multiplexing of the redo log files is used to ensure the safety of online redo log files. If redo log files are multiplexed, then the `LGWR` process writes the same information to the multiple, identical redo log files.

Item: 4 (Ref:1Z0-043.4.2.1)

On Jan 11, 2005 at 2:30 P.M., an erroneous update operation modified all the values of column LASTNAME in the EMPLOYEE table in the Scott schema to an empty string. You are the system administrator, and you want to return the original values in the table. To do so, you decided to flash back the table.

Which two options can you use to flash back a table? (Choose two.)

- by using Oracle Enterprise Manager
- by issuing the FLASHBACK TABLE statement at the RMAN prompt
- by issuing the FLASHBACK TABLE statement at the SQL prompt
- by issuing the FLASHBACK TABLE statement at the LSNRCTL prompt

Answer:

by using Oracle Enterprise Manager

by issuing the FLASHBACK TABLE statement at the SQL prompt

Explanation:

You can flash back a table using two methods, by using the Oracle Enterprise Manager or by issuing the FLASHBACK TABLE statement at the SQL prompt. To flash back a table by using Oracle Enterprise Manager, perform these steps:

1. Click the Perform Recovery option in the Backup/Recover section on the Maintenance Page.
2. Select Tables for the Object Type, and then select Flashback Existing Tables for the Operation Type. Click the Continue button.
3. To enable row movement, go to the Administration page, and choose Table in the Schema section. Select the table that you want to flash back and click Edit. Then, click the Options tab and select Yes in the Enable Row Movement field. Click the Apply button to apply the changes.

The Flashback Table feature is used to flash back a table to its previous state. The FLASHBACK TABLE <table_name> TO TIMESTAMP statement is used to flash back a table to a specific timestamp. The FLASHBACK TABLE <table_name> TO SCN statement is used to flash back a table to the specified SCN number.

The option stating that you can use the FLASHBACK TABLE statement at the RMAN prompt is incorrect. The FLASHBACK TABLE statement is issued at the SQL prompt. RMAN backup and recovery related commands are issued at the RMAN prompt.

The option stating that you can use the FLASHBACK TABLE statement at the LSNRCTL prompt is incorrect. The FLASHBACK TABLE statement is issued at the SQL prompt. The net services commands are issued at the LNSRCTL prompt.

Item: 5 (Ref:1Z0-043.4.1.3)

You are working as a Database Administrator. You erroneously dropped an important table named WAREHOUSE_DETAILS. The table resides in a non-SYSTEM tablespace.

The following dependent objects have been defined on the dropped table:

Type of Dependent Object	Number of Dependent Objects
Index	40
NOT NULL Constraint	20
Primary Key Constraint	1
Referential Integrity Constraint	15
Trigger	12

Due to limited space, some of the indexes and triggers have been removed from the Recycle Bin. You decide to recover the table by using Flashback Drop. You execute the following statement:

```
SQL>FLASHBACK TABLE warehouse_details TO BEFORE DROP;
```

What will be the implication of executing this statement?

- Only the WAREHOUSE_DETAILS table is recovered, and none of the dependent objects are recovered.
- The WAREHOUSE_DETAILS table is recovered along with the NOT NULL constraints, primary key constraint, and the referential integrity constraints.
- The WAREHOUSE_DETAILS table is recovered along with all the dependent objects except the indexes and triggers previously removed from the Recycle Bin.
- The WAREHOUSE_DETAILS table is recovered along with all the dependent objects except the referential integrity constraints and the indexes and triggers previously removed from the Recycle Bin.

Answer:

The WAREHOUSE_DETAILS table is recovered along with all the dependent objects except the referential integrity constraints and the indexes and triggers previously removed from the Recycle Bin.

Explanation:

In the given scenario, the WAREHOUSE_DETAILS table is recovered along with all the dependent objects except the referential integrity constraints and the indexes and triggers previously removed from the Recycle Bin. When a table is dropped, the table and all its dependent objects such as indexes, triggers and constraints move to the Recycle Bin. The referential integrity constraints are not protected by the Recycle Bin. Therefore, when the table is recovered using Flashback Drop, all its dependent objects are recovered except the referential integrity constraints. The dropped objects are kept in the Recycle Bin until the tablespace to which the dependent objects belong is able to allocate new extents. When space pressure arises, such as when the user quota reaches its maximum limit, the space utilized by the dropped objects in the Recycle Bin is automatically reclaimed by Oracle. In this case, the dropped objects are purged from the Recycle Bin on a First In First Out (FIFO) basis. Objects that are purged from the Recycle Bin due to space pressure cannot be recovered. As a result, if the dependent objects are removed from the Recycle Bin due to space pressure, they cannot be recovered when you try to recover the dropped table by using Flashback Drop.

The option stating that only the WAREHOUSE_DETAILS table is recovered is incorrect because some dependent objects are recovered along with the WAREHOUSE_DETAILS table.

The option specifying that the WAREHOUSE_DETAILS table is recovered along with the NOT NULL constraints, primary key constraint and the referential integrity constraints is incorrect because the referential integrity constraints cannot be recovered using Flashback Drop.

The option that states that the WAREHOUSE_DETAILS table is recovered along with all the dependent objects except the indexes and triggers previously removed from the Recycle Bin is incorrect because the referential integrity constraints are not protected by the Recycle Bin.

Item: 6 (Ref:1Z0-043.4.5.2)

You performed the following series of actions:

```
CREATE TABLE employee
   (emp_no NUMBER PRIMARY KEY, emp_name VARCHAR2(16), salary
   NUMBER);
   INSERT INTO emp VALUES (500, 'WILLIAM', 1100);
   COMMIT;

   CREATE TABLE department (dept_no NUMBER, dept_name
   VARCHAR2(32));
   INSERT INTO dept VALUES (4, 'SALES');
   COMMIT;

   GRANT INSERT, UPDATE,DELETE ON employee TO PUBLIC;
```

At 10:00 A.M., a user issues an erroneous statement that deletes the row of EMP_NO 500 from the EMPLOYEE table:

```
DELETE FROM employee WHERE emp_no = 500;
   COMMIT;
```

At 10:05 A.M., another user issues a statement that inserts new values for the EMP_NO 500:

```
   INSERT INTO EMPLOYEE VALUES(500,'CHRIS',1000);
   COMMIT;
```

At this point in time, you have used the Flashback Transaction Query feature. What will be the result of using the Flashback Transaction Query feature?

- The table will be retrieved in the state that it was at 10:00 A.M.
- The database will be retrieved in the state that it was at 10:00 A.M.
- All the versions of the EMP_NO 500 row are displayed.
- Undo SQL statements are provided to undo the changes made to the EMPLOYEE table over the last five minutes.

Answer:

Undo SQL statements are provided to undo the changes made to the EMPLOYEE table over the last five minutes.

Explanation:

In the given scenario, when you use the Flashback Transaction Query feature, undo SQL statements are provided to undo the changes made to the EMPLOYEE table over the last five minutes. The Flashback Transaction Query feature is designed to function as a diagnostic tool to identify changes made to the database at the transactional level. Using the Flashback Transaction Query feature, you can identify all the changes made within a specific time period and perform the transactional recovery of tables. The Flashback Transaction Query feature is based on undo data and utilizes the UNDO_RETENTION initialization parameter to determine the duration for which the committed undo data will be retained in the database. The FLASHBACK_TRANSACTION_QUERY view can be used to identify the operations that are performed on a table.

The option stating that the table is retrieved in the state that it was at 10:00 A.M. is incorrect. This is because flashing tables back to their previous states is the function of the Flashback Table feature. The Flashback Table feature allows you to recover one or more tables to a specific point in time without the requirement of performing more time-consuming recovery operations, such as point-in-time recovery, which may also affect the availability of the rest of the database. The Flashback Table feature recovers the table by rolling back only the changes made to the tables and to their dependent objects, such as indexes.

The option stating that the database is in the state that it was at 10:00 A.M. is incorrect because flashing back the database to its previous state is the function of the Flashback Database feature. Flashback Database is a new feature in Oracle 10*g* that allows you to quickly restore the entire database to the state it was at a previous point in time.

The option stating that all the versions of the EMP_NO 500 row are displayed is incorrect. This is because displaying all the versions of a row within a specific time period is a function of the Flashback Version Query feature. The Flashback Version Query feature offers an easy method to display all the versions of all the rows in a table between two SCN or time stamps. The Flashback Version Query feature also displays all the rows that are inserted, deleted, or updated in a table between two SCNs

or time stamps.

Item: 7 (Ref:1Z0-043.4.2.4)

You are performing flashback of the EMPLOYEE table in SCOTT's schema because some incorrect data was inserted into the table and committed by mistake.

Which two clauses will you use in the FLASHBACK TABLE statement for using the Flashback Table feature? (Choose two.)

- RESETLOGS
- TO TIMESTAMP
- TO BEFORE DROP
- RENAME TO
- TO SCN

Answer:

TO TIMESTAMP
TO SCN

Explanation:

The TO SCN and TO TIMESTAMP clauses can be used in the FLASHBACK TABLE statement for using the Flashback Table feature. The TO SCN clause is used to flash back a table to a certain system change number. The TO TIMESTAMP clause is used to flash back a table to a certain point in time. For example, the following statement is used to flash back the EMPLOYEE table to a certain point in time:

```
SQL> FLASHBACK TABLE EMPLOYEE
   TO TIMESTAMP (SYSTIMESTAMP - INTERVAL '1' minute);
```

And, the following statement is used to flash back the EMPLOYEE table to a certain system change number:

```
SQL> FLASHBACK TABLE EMPLOYEE TO SCN <value>;
```

The option stating that the RESETLOGS clause can be used in the FLASHBACK TABLE statement for using the Flashback Table is incorrect. The RESETLOGS clause is used with ALTER DATABASE OPEN statement to perform a new incarnation of online redo log files. If you open a database using the RESETLOGS clause, the online redo log files are reset.

The option stating that the TO BEFORE DROP clause can be used in the FLASHBACK TABLE statement for using the Flashback Table is incorrect. The TO BEFORE DROP clause is used with the FLASHBACK TABLE statement to restore a dropped table from the Recycle Bin. The FLASHBACK TABLE <table_name> TO BEFORE DROP statement uses the Flashback Drop feature and not the Flashback Table feature.

The option stating that the RENAME TO clause can be used in the FLASHBACK TABLE statement for using the Flashback Table is incorrect. The RENAME TO clause is used to change the name of the table when the table is restored from the Recycle Bin. The syntax of using the RENAME TO clause is as follows:

```
SQL>FLASHBACK TABLE <old_name> TO BEFORE DROP RENAME TO
   <new_name>;
```

Item: 8 (Ref:1Z0-043.4.4.3)

You performed the following series of actions:

```
CREATE TABLE employee
   (emp_no NUMBER PRIMARY KEY, emp_name VARCHAR2(16), salary
   NUMBER);
   INSERT INTO emp VALUES (101, 'JAMES', 800);
   COMMIT;

   CREATE TABLE department (dept_no NUMBER, dept_name
   VARCHAR2(32));
   INSERT INTO dept VALUES (5, 'FINANCE');
   COMMIT;
```

At 11:00 A.M., a user issues an erroneous statement that deletes the row of EMP_NO 101 from the EMPLOYEE table:

```
DELETE FROM employee WHERE emp_no = 101;
   COMMIT;
```

At 11:05 A.M., another user issues a statement that inserts new values for EMP_NO 101.

```
INSERT INTO employee VALUES(101,'SMITH',700);
   COMMIT;
```

At this point in time, you have used the Flashback Version Query feature. What will be the result of using the Flashback Version Query feature?

- The EMPLOYEE table is retrieved in the state it was at 11:00 A.M.
- The database is in the state it was at 11:00 A.M.
- All versions of the row of EMP_NO 101 are displayed.
- Undo SQL statements are provided to undo the changes made to the EMPLOYEE table over the last five minutes.

Answer:

All versions of the row of EMP_NO 101 are displayed.

Explanation:

The Flashback Version Query returns all the versions of the row of EMP_NO 101.The Flashback Version Query feature is used to retrieve all the versions of the rows that exist or existed between the times the query was executed to a determined point-in-time in the past. The Flashback Version Query returns all the committed occurrences of the rows for an object without displaying the uncommitted versions of the rows. The Flashback Versions Query works by retrieving data from the UNDO tablespace. The UNDO_RETENTION initialization parameter, which is specified in seconds, determines how much committed undo data should be kept in the database. If the transactions require additional undo space and there is no additional space in the UNDO tablespace, then Oracle will start reusing the undo space. The RETENTION GUARENTEE option, which can be set on the UNDO tablespace, will protect the unexpired undo data in this scenario.

The option stating that the table is retrieved in the state it was at 11:00 A.M. is incorrect. This is because flashing back the tables to their previous states is the function of the Flashback Table feature. The Flashback Table feature allows you to recover one or more tables to a specific point-in-time without the requirement of performing more time-consuming recovery operations, such as point-in-time recovery, which may also affect the availability of the rest of the database. The Flashback Table feature recovers the table by rolling back only the changes made to the tables or to their dependent objects such as indexes.

The option stating that the database is in the state it was at 11:00 A.M. is incorrect. This is because flashing back the database to its previous state is the function of the Flashback Database feature. Flashback Database is a new feature in Oracle 10*g* that allows you to quickly restore the entire database to its previous state.

The option stating that you will be provided the SQL statements to undo the changes made to the EMPLOYEE table over the last five minutes is incorrect. This is the function of the Flashback Transaction Query feature. The Flashback Transaction Query feature is designed to function as a diagnostic tool to identify changes made to the database at the transactional level. Using the Flashback Transaction Query feature, you can identify all the changes made within a specific time period and perform the transactional recovery of tables. The Flashback Transaction Query feature is based on undo data and utilizes the UNDO_RETENTION initialization parameter to determine the duration for which the committed undo data will be retained in the

database. The FLASHBACK_TRANSACTION_QUERY view can be used to identify the operations that are performed on a table.

Item: 9 (Ref:1Z0-043.4.3.1)

You issued the following command:

```
SQL> DROP TABLE MYTABLE;

SQL> SHOW RECYCLEBIN
```

The following output is returned:

```
ORIGINAL NAME RECYCLEBIN NAME                OBJECT TYPE      DROP TIME
------------- ------------------------------ -------------- -------------------
MYTABLE BIN$04LhcpndanfgMAAAAAANPw==$0     TABLE          2005-01-13:20:11:31
```

You want to drop the table, MYTABLE, from the Recycle Bin. Which two commands can you issue to accomplish the desired task? (Choose two.)

- DROP TABLE MYTABLE PURGE;
- PURGE RECYCLEBIN;
- PURGE TABLE MYTABLE;
- PURGE TABLE BIN$04LhcpndanfgMAAAAAANPw==$0;

Answer:

PURGE TABLE MYTABLE;
PURGE TABLE BIN$04LhcpndanfgMAAAAAANPw==$0;

Explanation:

You can issue the PURGE TABLE MYTABLE; command or the PURGE TABLE BIN$04LhcpndanfgMAAAAAANPw==$0; command to remove the table from the Recycle Bin. When you drop a table by using the DROP TABLE statement, the table is not removed completely from the database. The dropped table is stored in the Recycle Bin. After dropping a table, you can view the table and its dependent objects in the Recycle Bin. These objects have a unique naming convention to support objects of the same name dropped by different users. The naming convention consists of a globalUID that is a unique, 24-character long identifier and a version number assigned by the database. If the table is dropped by mistake, then you can restore the dropped table from the Recycle Bin by using the Flashback Drop feature.

The option stating that you can issue the DROP TABLE MYTABLE PURGE; statement to remove the table from the Recycle Bin is incorrect. This is because the DROP TABLE MYTABLE PURGE; statement is issued to drop the table completely without storing the table in the Recycle Bin. In this scenario, the table is already dropped and stored in the Recycle Bin; therefore, this command cannot be used.

The option stating that you can issue the PURGE RECYCLEBIN; command to remove only the table, MYTABLE, from the Recycle Bin is incorrect. This is because the PURGE RECYCLEBIN; command is issued to clear the entire Recycle Bin of a user's schema. This command will not remove a specific table from the Recycle Bin.

Item: 10 (Ref:1Z0-043.4.1.2)

At the end of the financial year, an accounts accumulation batch is run. This batch updates the company's accounting records. During the batch run process, some incorrect entries were inserted into the ACCOUNT table. You identified the bug and immediately stopped the batch run process, but 3000 incorrect records were inserted into the ACCOUNT table before the batch process was stopped. You want to recover the table to the state it was at 11:50 P.M.

Which flashback feature will you use?

- Flashback Drop
- Flashback Database
- Flashback Table
- Flashback Version Query

Answer:

Flashback Table

Explanation:

You will use the Flashback Table feature to recover the table to the state it was at 11:50 P.M. The Flashback Table feature allows you to recover a table to a specific point-in-time without performing an incomplete recovery. All dependent objects are also recovered using the Flashback Table feature. Flashback Table has the following benefits over incomplete recovery:

It is much faster and easier to use than incomplete recovery.
Flashback Table does not impact the availability of the database.
A database user can flash back a table to quickly recover from logical corruptions.

To use Flashback Table, a user must be granted either the FLASHBACK ANY TABLE or the FLASHBACK TABLE system privileges as well as the SELECT, INSERT, DELETE, and ALTER object privileges on the table.

The Flashback Drop option incorrect because this feature is used to restore dropped objects. Flashback Drop saves a copy of the dropped database object and the dependent objects in the Recycle Bin to recover the objects if necessary. The dropped database object is not removed from the database until the Recycle Bin is emptied. In this scenario, the ACCOUNT table was not dropped.

The Flashback Database option is incorrect because this feature allows you to flash the entire database back to a specific point-in-time. This is extremely useful to recover from errors such as truncating a large table, an incomplete batch job, or a dropped user.

The Flashback Database option is incorrect because this feature is used to retrieve all the versions of the rows that exist or existed between the times the query was executed to a determined point-in-time in the past. The Flashback Version Query feature returns all the committed occurrences of the rows for an object without displaying the uncommitted row versions.

Item: 11 (Ref:1Z0-043.4.1.1)

You are working as a DBA at NetFx Corporation. A user, Scott, is maintaining the records of all the employees in the EMPLOYEE table. Initially, the salary of the employee, 'E0025', was $1800. On 1 May 2004, the salary of the employee, 'E0025', was increased by $200.
The user, Scott, issued the following statement to modify the record of the employee, 'E0025':

```
SQL>UPDATE EMPLOYEE
SET SALARY = 2000
WHERE EMPNO = 'E0025';
SQL>COMMIT;
```

On December 1, 2004, the salary of the employee, 'E0025', was increased by $400. The user, Scott, issued the following statement to modify the record of the employee, 'E0025':

```
SQL>UPDATE EMPLOYEE
SET SALARY = 2400
WHERE EMPNO = 'E0025';
SQL>COMMIT;
```

On July 1, 2005, the salary of the employee, 'E0025', was increased by $500. The user, Scott, issued the following statement to modify the record of the employee, 'E0025'

```
SQL>UPDATE EMPLOYEE
SET SALARY = 2900
WHERE EMPNO = 'E0025';
SQL>COMMIT;
```

On July 5, 2005, the HR manager asked you to generate the increment report of the employee, 'E0025', for the period between 1 May 2004 and 1 July 2005.

Which flashback feature will you use to generate the increment report?

- Flashback Drop
- Flashback Table
- Flashback Database
- Flashback Version Query

Answer:

Flashback Version Query

Explanation:

You will use the Flashback Version Query feature to generate the increment report. The Flashback Version Query feature is used to retrieve all the versions of the rows that exist or existed between the times the query was executed to a specified point-in-time in the past. The Flashback Version Query feature returns all the committed occurrences of the rows for an object without displaying the uncommitted row versions. The Flashback Version Query feature retrieves data from the UNDO tablespace. The UNDO_RETENTION initialization parameter, which is specified in seconds, determines how much committed undo data must be stored in the database. If the transactions require additional undo space and there is no space in the UNDO tablespace, Oracle starts reusing the undo space. The RETENTION GUARENTEE option, which can be set on the UNDO tablespace, prevents unexpired undo data from being overwritten.

The Flashback Drop option is incorrect because this feature is used to restore dropped objects. Flashback Drop is the process of saving a copy of the dropped database object and the dependent objects in the Recycle Bin to ensure that the objects can be recovered if required. The dropped database object is not removed from the database until the Recycle Bin is emptied. In the given scenario, the table, EMPLOYEE, was not dropped.

The Flashback Table option is incorrect because this feature allows you to recover a table to a specific point-in-time without performing an incomplete recovery. All dependent objects are also recovered when you use the Flashback Table feature. In the given scenario, you want to view only the versions of the row that maintain the record of the employee, 'E0025'. You do not want to flash the entire table back one and half years.

The Flashback Database option is incorrect because this feature allows you to flash the entire database back to a specific point-in-time. This feature enables you to recover from errors such as truncating a large table, an incomplete batch job, or a dropped

user.

Item: 12 (Ref:1Z0-043.4.2.3)

You are performing flashback of the ORDERS table in the Scott's schema because some important data is deleted in the table by mistake. The SCN number was 771513 at the time of deletion. You issued the following statement to perform Flashback Table:

```
SQL> FLASHBACK TABLE ORDERS TO SCN 771513;
```

What is the prerequisite to perform Flashback Table?

- You must configure OMF in your database.
- You must enable block change tracking feature in your database.
- You must enable ROW MOVEMENT feature on the ORDERS table.
- You must use the Flashback Version Query before using the Flashback Table feature.

Answer:

You must enable ROW MOVEMENT feature on the ORDERS table.

Explanation:

To use the Flashback Table feature, you must enable ROW MOVEMENT on the ORDERS table. To enable ROW MOVEMENT, you issue the following command:

```
SQL> ALTER TABLE ORDERS ENABLE ROW MOVEMENT;
```

The option stating that to use the Flashback Table feature, you must enable OMF in your database is incorrect. Configuring Oracle Managed Files (OMF) in the database is not a prerequisite for using the Flashback Table feature. OMF is used to specify the default locations of the datafiles, control files, and the online redo log files. If OMF is configured in your database and you do not specify the names and sizes of the datafiles during tablespace creation, then Oracle automatically assigns names and sizes to the datafiles associated with that tablespace and stores them in the location specified by the DB_CREATE_FILE_DEST parameter. The DB_CREATE_ONLINE_LOG_DEST_n parameter is used to specify the default locations of online redo log files and the control files.

The option stating that to use the Flashback Table feature, you must enable the block change tracking feature in your database is incorrect. The block change tracking feature is enabled to improve the performance of the backup process while performing the incremental backup. If block change tracking feature is enabled, then a change tracking file keeps track of the blocks that are changed since the last backup. While performing the incremental backup, only the changed blocks are read instead of scanning the entire datafile.

The option stating that you must use the Flashback Version Query feature before using the Flashback Table feature is incorrect. Using the Flashback Version Query feature is a prerequisite for using the Flashback Transaction Query feature. Both the Flashback Version Query and the Flashback Transaction Query are used to identify the user who deleted the record, the transaction ID of the transaction that deleted the record, and the undo SQL statements that will undo the deletion of the record. Oracle Flashback Version Query and Oracle Flashback Transaction Query are referred to as complementary features. The Oracle Flashback Version Query feature provides a history of the changes made to a row along with the corresponding identifiers of the transactions that made the changes. You should use the transaction identifier provided by the Flashback Version Query feature in the Flashback Transaction Query to identify the user who made the changes in the database by running the specific transaction. The Flashback Transaction Query feature provides the Undo SQL statements to undo the changes made by a specific transaction.

Item: 13 (Ref:1Z0-043.4.3.2)

What will be the result of using the `SQL> DROP USER SCOTT CASCADE;` command?

- The user, Scott, is dropped, all the objects in Scott's schema are placed in the Recycle Bin, and the objects that are already in the Recycle Bin are dropped.
- The user, Scott, is dropped, all the objects in Scott's schema are placed in the Recycle Bin, and all the objects in the Recycle Bin, belonging to the user Scott, are not dropped.
- The user, Scott, is dropped, all the objects in the Scott's schema are not placed in the Recycle Bin, and the objects in the Recycle Bin, belonging to the user, Scott, are not dropped.
- The user, Scott, is dropped, all the objects in Scott's schema are not placed in the Recycle Bin, and the objects in the Recycle Bin are dropped.

Answer:

The user, Scott, is dropped, all the objects in Scott's schema are not placed in the Recycle Bin, and the objects in the Recycle Bin are dropped.

Explanation:

The `DROP USER user_name CASCADE` command drops the specified user and all the objects owned by that user. The objects owned by that user are not placed in the Recycle Bin. The objects that are already in the Recycle Bin and belong to the user are also dropped. The `DROP USER` command bypasses the Recycle Bin and deletes the objects immediately from the database. In this scenario, the user, Scott, is dropped, all the objects in Scott's schema are not placed in the Recycle Bin, and the objects that are already in the Recycle Bin are dropped.

The option stating that the user, Scott, is dropped, all the objects in Scott's schema are placed in the Recycle Bin, and all the objects in the Recycle Bin, belonging to the user, Scott, are dropped is incorrect. The option stating that the user Scott is dropped, all the objects in Scott's schema are placed in the Recycle Bin, and all the objects in the Recycle Bin belonging to the user, Scott, are not dropped is also incorrect. This is because the objects in the Scott's schema are not placed in the Recycle Bin.

The option stating that the user, Scott is dropped, all the objects in Scott's schema are not placed in the Recycle Bin, and the objects in the Recycle Bin belonging to the user, Scott, are not dropped is incorrect. This is because the objects that are in the Recycle Bin belonging to the user Scott are dropped.

Item: 14 (Ref:1Z0-043.4.4.1)

You are maintaining your OLTP database in Oracle10*g*. You are performing the Flashback Transaction Query to find the undo SQL statements that can be used to undo the changes made to the database in the specific time period.

Which pseudocolumn will you use to perform the Flashback Transaction Query?

- VERSIONS_STARTSCN
- VERSIONS_STARTTIME
- VERSIONS_XID
- VERSIONS_OPERATION

Answer:

VERSIONS_XID

Explanation:

You will use the VERSIONS_XID pseudocolumn to perform a Flashback Transaction Query to find the undo SQL statements that can be used to undo the changes made to the database in the specific time period. Oracle Flashback Version Query and Oracle Flashback Transaction Query are referred to as complementary features. The Oracle Flashback Version Query feature provides a history of the changes made to a row along with the corresponding identifiers of the transactions that made the changes. The VERSIONS_XID pseudocolumn displays the transaction identifiers of the transactions that made the changes within the specific time period. The transaction identifiers provided by the Flashback Version Query feature are used in the Flashback Transaction Query.

The option stating that you will use the VERSIONS_STARTSCN pseudocolumn to perform a Flashback Transaction Query to find the undo SQL statements that can be used to undo the changes made to the database in the specific time period is incorrect. The VERSIONS_STARTSCN pseudocolumn is used to display the SCN number at which the version of a row was created.

The option stating that you will use the VERSIONS_STARTTIME pseudocolumn to perform a Flashback Transaction Query to find the undo SQL statements that can be used to undo the changes made to the database in the specific time period is incorrect. The VERSIONS_STARTTIME pseudocolumn is used to display the timestamp at which the version of a row was created.

The option stating that you will use the VERSIONS_OPERATIONS pseudocolumn to perform the Flashback Transaction Query to find the undo SQL statements that can be used to undo the changes made to the database in the specific time period is incorrect. The VERSIONS_OPERATION pseudocolumn is used to display the operation performed by the transaction. In this pseudocolumn, I indicates insertion, D indicates deletion, and U indicates update.

Dealing with Database Corruption

Item: 1 (Ref:1Z0-043.5.5.4)

You are using the Block Media Recovery feature to recover the blocks that are marked corrupt since the last backup. Which view will you query to display information about the data blocks that are marked corrupt since the last backup?

- V$BACKUP_CORRUPTION
- V$COPY_CORRUPTION
- V$DATABASE_BLOCK_CORRUPTION
- RC_BACKUP_CORRUPTION

Answer:

V$DATABASE_BLOCK_CORRUPTION

Explanation:

The V$DATABASE_BLOCK_CORRUPTION view is used to display information about the blocks that are marked corrupt since the last backup.

You cannot query the V$BACKUP_CORRUPTION view to display the information about blocks that are marked corrupt since the last backup. The V$BACKUP_CORRUPTION view is used to display information about the corrupt blocks in the datafile backups from the control file.

You cannot query the V$COPY_CORRUPTION view to display the information about blocks that are marked corrupt since the last backup. The V$COPY_CORRUPTION view displays information about the corrupted blocks in the datafile copy from the control file.

You cannot query the RC_BACKUP_CORRUPTION view to display information about blocks that are marked corrupt since the last backup. The RC_BACKUP_CORRUPTION view is used to display information about the corrupted blocks in the datafile backups. This view corresponds with the V$BACKUP_CORRUPTION view in the control file.

Item: 2 (Ref:1Z0-043.5.4.2)

You are maintaining the PROD database of TeleSoft Corporation. You have initialized the following DB_BLOCK_CHECKING parameter in the init.ora file:

```
DB_BLOCK_CHECKING = TRUE;
```

What will be the result of setting this parameter?

- Only data blocks of the SYSTEM tablespace will be checked.
- Only data blocks of the SYSAUX tablespace will be checked.
- A checksum will occur only on the checkpoint.
- A checksum will occur every time a block is modified.

Answer:

A checksum will occur every time a block is modified.

Explanation:

In the given situation, when you initialize the DB_BLOCK_CHECKING parameter in the init.ora file, a checksum occurs every time a block is modified. The DB_BLOCK _CHECKING parameter sets block checking at the database level. This parameter is used to check the corrupt blocks each time the blocks are modified at the tablespace level. A checksum occurs every time a block is modified.

The option stating that only data blocks of the SYSTEM tablespace are checked is incorrect. If the value of the DB_BLOCK_CHECKING parameter is FALSE, then only the blocks of the SYSTEM tablespace will be checked. If the value of the DB_BLOCK_CHECKING parameter is set to TRUE, then the blocks of all the SYSTEM and the non SYSTEM tablespaces will be checked.

The option stating that only the data blocks of the SYSAUX tablespace are checked is incorrect.
If the value of the DB_BLOCK_CHECKING parameter is FALSE, then only the blocks of the SYSTEM tablespace will be checked. If the value of the DB_BLOCK_CHECKING parameter is set to TRUE, then the blocks of all the SYSTEM and the non SYSTEM tablespaces will be checked.

The option stating that a checksum occurs only on the checkpoint is incorrect. If the value of the DB_BLOCK_CHECKING parameter is set to TRUE, then a checksum occurs every time a block is modified. A checkpoint occurs when every dirty block in the buffer cache is written to the datafiles. The DBWR process is responsible for writing the dirty block, writing the latest System Change Number (SCN) into the datafile header, and writing the latest System Change Number (SCN) into the control files.

Item: 3 (Ref:1Z0-043.5.2.1)

The datafiles of your database are ASM files. You are performing a check for datafile block corruption by using the DBVERIFY utility.

What is a prerequisite for checking block corruption on an ASM datafile by using the DBVERIFY utility?

- The block change tracking feature must be enabled.
- OMF must be configured on your database.
- The database must be in ARCHIVELOG mode.
- A USERID must be supplied.

Answer:

A USERID must be supplied.

Explanation:

If you are checking an ASM datafile for block corruption, then you must supply a USERID. This is because the DBVERIFY utility has to connect to the ASM instance to access ASM files. The DBVERIFY utility is used to check datafiles for block corruption. The name and location of the DBVERIFY utility is dependent on the operating system. The DBVERIFY utility can be used only with datafiles. This utility checks the data blocks from the starting block in the file to the end of the file. You can also explicitly specify the starting and ending data block in a file to be checked. For example, to perform an integrity check on the tbs_52.f datafile on the UNIX operating system, you can issue the following dbv command:

```
% dbv file=tbs_52.f
```

The syntax of the DBVERIFY utility is as follows:

```
% dbv file=<name of file> <parameter_1>=<value of parameter_1>
<parameter_2>=<value of parameter_2>...
```

The different parameters of the DBVERIFY utility are as follows:

USERID: used to specify the username and password for the user who runs the command. If you are checking ASM files, then this parameter must be specified.
FILE: used to specify the name of the file to be checked for block corruption.
START: used to specify the starting block address that is to be checked. The block address is specified for Oracle data blocks. If you do not specify this parameter, then Oracle starts checking from the first block.
END: used to specify the ending block address that is to be checked. If you do not specify this parameter, then Oracle performs a check up to the last block.
BLOCKSIZE: used to specify the block size of the database. The value of this parameter should be the same as the value of the DB_BLOCK_SIZE init.ora parameter.
LOGFILE: used to specify a file that contains logging information about the processing of the DBVERIFY utility.
FEEDBACK: used to trigger the DBVERIFY utility to display the progress of the file being checked for block corruption.
HELP: used to provide online help regarding the use of the DBVERIFY utility.
PARAFILE: used to specify the name of a parameter file. In a parafile, you can specify various values for the parameters used in a DBVERIFY utility.

The option stating that you must enable the block change tracking feature to check the ASM datafiles by using the DBVERIFY utility is incorrect. The change tracking feature is used to enhance the performance of the backup process while an incremental backup is being performed.

The option stating that you must configure OMF in your database to check the ASM datafiles by using the DBVERIFY utility is incorrect. OMF is used to specify the default names and locations of the datafiles, redo log files, and control files.

The option stating that the database must be in ARCHIVELOG mode to check the ASM datafiles by using the DBVERIFY utility is incorrect. If your database is in ARCHIVELOG mode, then the data of the redo log files are written in archive files when log switch occurs. Archive files are copies of online redo log groups. If the database is in ARCHIVELOG mode and log switching occurs, then the ARCn process writes the redo log entries from the filled online redo log file to the archive log file. After a redo log file is full, the LGWR process starts writing to the next redo log file. This event is called log switching. You can also perform log switching by using the ALTER SYSTEM SWITCH LOGFILE; command.

Item: 4 (Ref:1Z0-043.5.5.2)

You issue the following statement:

```
SQL> SELECT FIRSTNAME, LASTNAME FROM HR.EMPLOYEE;
```

You receive the following error:

```
01578: ORACLE data block corrupted (file# 6, block # 54)
ORA-01110 : data file 6: 'u01/oracle/oradata/data1.dbf'
```

How will you resolve this problem of data block corruption by reducing the mean time to recover (MTTR)?

- by using the DBMS_REPAIR package
- by using the DBVERIFY utility
- by using Block Media Recovery
- by issuing the ANALYZE TABLE HR.EMPLOYEES VALIDATE STRUCTURE command

Answer:

by using Block Media Recovery

Explanation:

The Block Media Recovery (BMR) is an RMAN feature that is used to recover an individual block or a group of corrupt blocks in a datafile. This allows you to recover individual data blocks instead of the whole datafile. BMR is best used where block corruption is minimal. BMR reduces the mean time to recovery (MTTR) because only the affected data blocks are restored and recovered instead of the whole datafile. To perform Block Media Recovery, the BLOCKRECOVER command is issued at the RMAN prompt. In this scenario, you must issue the following command to perform Block Media Recovery:

```
RMAN>BLOCKRECOVER DATAFILE 6 BLOCK 54;
```

You cannot resolve the problem of data block corruption by using the DBMS_REPAIR package. The DBMS_REPAIR package is a set of procedures that enables you to detect and fix corrupted blocks in tables and indexes. Each procedure performs different actions. For example, the CHECK_OBJECT procedure and the FIX_CORRUPT_BLOCKS procedures of the DBMS_PACKAGE are used to check the object and fix the corrupted blocks of the object, respectively.

You cannot resolve the problem of data block corruption by using the DBVERIFY utility. This is because the DBVERIFY utility is used to check whether a datafile is corrupted. The DBVERIFY utility is not used to repair the corrupted blocks. The name and location of the DBVERIFY utility is dependent on the operating system. The DBVERIFY utility can be used only with datafiles. This utility checks the data blocks from the starting block in the file to the end of the file. You can specify the starting and ending data block in a file to ensure explicit checks. For example, to perform an integrity check on the tbs_52.f datafile on the UNIX operating system, you can run the following dbv command:

```
% dbv file=tbs_52.f
```

You cannot resolve the problem of block corruption by issuing the ANALYZE TABLE HR.EMPLOYEE VALIDATE STRUCTURE command at the RMAN prompt. This is because the ANALYZE utility validates the integrity of the structure of the object being analyzed. The ANALYZE TABLE table_name VALIDATE STRUCTURE command is either successful or unsuccessful at the object level. If this command returns an error for the object to be analyzed, then you will be required to completely rebuild the object. If no error is returned, then the object is not corrupted and should be re-created.

Item: 5 (Ref:1Z0-043.5.3.2)

You want to rebuild a free list in the free lists of the EMPLOYEE table in the Scott schema. Which package will you use to accomplish this?

- DBMS_REPAIR
- DBMS_SCHDULER
- DBMS_STATS
- DBMS_RESOURCE_MANAGER

Answer:

DBMS_REPAIR

Explanation:

You will use the DBMS_REPAIR package to rebuild a free list in the free lists of the EMPLOYEE table in the Scott schema. The DBMS_REPAIR package is a set of procedures that enables you to detect and fix corrupt blocks in tables and indexes. The DBMS_REPAIR package consists of multiple stored procedures. Each of these procedures perform different actions. The REBUILD_FREELISTS procedure of the DBMS_REPAIR package is used to rebuild free lists for a specified object. After these free lists are rebuilt and reset, all the entries for the free blocks are entered in the master free list.
The syntax for rebuilding the free lists is as follows:

```
BEGIN
DBMS_REPAIR.REBUILD_FREELISTS (
SCHEMA_NAME => 'SCOTT',
OBJECT_NAME => 'EMPLOYEE',
OBJECT_TYPE => dbms_repair.table_object);
END;
/
```

The option stating that you will use the DBMS_SCHEDULER package to rebuild the free lists of the EMPLOYEE table in the Scott schema is incorrect. This because the DBMS_SCHEDULER package is used to create jobs, programs, windows, and so on.

The option stating that the DBMS_STATS package is used to rebuild the free lists of the EMPLOYEE table in the Scott schema is incorrect. This is because the DBMS_STATS package is used to gather statistics about the physical storage characteristics of a table or an index. These statistics are stored in the data dictionary.

The option stating that the DBMS_RESOURCE_MANAGER package is used to rebuild the free lists of the EMPLOYEE table in the Scott schema is incorrect. This is because the DBMS_RESOURCE_MANAGER package is used to manage the resource consumer groups. This package also provides the functionality for assigning users to groups and switching the group for user sessions.

Item: 6 (Ref:1Z0-043.5.1.1)

You received the following error:

```
ORA-01578: ORACLE data block corrupted
(file # %s, block # %s)
```

Which file will you check to view additional information regarding the cause of this error?

- the alert log file and the trace files
- the redo log files
- the control file
- the change tracking file

Answer:

the alert log file and the trace files

Explanation:

You will check the alert log file and the trace files to view additional information regarding the cause of the `ORA-01578` error. This `ORA-01578` error is the result of a hardware problem. If the `ORA-1578` error always displays the same arguments, the block is probably media corrupted. You should view the alert log file and the trace files for more details about the error. Block corruption can be caused by different sources. Block corruption can be defined by human error through the use of software and hardware bugs. If the `ORA-01578` error displays the changed arguments, then there may be a hardware problem, and you should check the memory and page space. You should also check the I/O subsystem for bad controllers. This problem will not be completely resolved until the hardware fault is corrected.

The option stating that you will check the redo log files for additional information regarding the `ORA-01578` error is incorrect. The redo log files contain the redo entries for a database. These redo log entries include every change made to the database. The `LGWR` process is responsible for writing the information from the redo log buffer to the redo log files.

The option stating that you will check the control file for additional information about the `ORA-01578` error is incorrect. The control file contains the current state of the database. The control file contains information, such as database name, date and time of database creation, current log sequence number, names and locations of the datafiles and the online redo log files, and so on.

The option stating that you will check the change tracking file for additional information regarding the `ORA-01578` error is incorrect. The block change tracking file is used by `RMAN` to identify the blocks that should be read during the incremental backup. After the blocks are identified, `RMAN` directly accesses the blocks to back them up.

Item: 7 (Ref:1Z0-043.5.1.2)

You issued the following command to analyze the SCOTT.EMP table for block corruption:

```
ANALYZE TABLE SCOTT.EMP VALIDATE STRUCTURE;
```

You received the following error:

```
ORA-01578: ORACLE data block corrupted
(file # %s, block # %s)
```

How will you resolve the block corruption problem?

- by using the DBMS_REPAIR package
- by using the DB_BLOCK_CHECKING parameter
- by using the DBVERIFY utility
- will not be completely resolved until the hardware fault is corrected

Answer:

will not be completely resolved until the hardware fault is corrected

---

Explanation:

The ANALYZE TABLE SCOTT.EMP VALIDATE STRUCTURE; command is not executed successfully due to a hardware problem. The ORA-01578 error is the result of the hardware problem. If the ORA-1578 error always displays the same arguments, the block is media corrupted. You should view the alert log file and trace files for more details about this error. Block corruption can be caused by different sources. Block corruption, which uses software and hardware bugs, can be defined by human error. If the ORA-01578 error displays changed arguments, there may be a hardware problem and you should check the memory and page space. You should also check the I/O subsystem for bad controllers. This problem will not be completely resolved until the hardware fault is corrected. Therefore, the other three options are incorrect.

Item: 8 (Ref:1Z0-043.5.5.6)

Which two statements are true about Block Media Recovery (BMR)? (Choose two.)

- [ ] BMR increases the Mean Time To Recover (MTTR).
- [ ] BMR can only be implemented using Recovery Manager (RMAN).
- [ ] The blocks that need to be recovered are accessible during BMR.
- [ ] BMR cannot be performed using cumulative incremental backups.
- [ ] The datafile must be restored if most of the blocks in the datafile are corrupt.

Answer:

BMR can only be implemented using Recovery Manager (RMAN).
BMR cannot be performed using cumulative incremental backups.

Explanation:

Recovery Manager (RMAN) must be used to perform Block Media Recovery (BMR). BMR is implemented through the RMAN BL0CKREC0VER command. BMR can only be performed using full RMAN backups. It is not possible to recover the corrupted blocks from any type of incremental backup as the incremental backup contains only the changed blocks.

BMR does not increase the Mean Time To Recover (MTTR). On the contrary, it reduces MTTR because you can recover individual data blocks instead of recovering the entire datafile.

If most of the blocks within a datafile are corrupt in the database, only these blocks rather than the entire datafile must be recovered. It does not matter whether the blocks to be recovered are more or less.

The blocks that need to be recovered are not accessible during BMR. BMR is possible when the database is open. During BMR, the datafile remains online and only the blocks being recovered are made inaccessible.

Item: 9 (Ref:1Z0-043.5.5.5)

You executed the following code:

```
BACKUP VALIDATE DATABASE;
BLOCKRECOVER CORRUPTION LIST;
```

What will be the result of executing the above code?

- The code will run a backup validation to populate the V$BACKUP_CORRUPTION view and repair corrupt blocks, if any, recorded in the view.
- The code will run a backup validate to populate the V$COPY_CORRUPTION view and then repair any corrupt blocks recorded in the view.
- The code will runs a backup validate to populate the V$DATABASE_BLOCK_CORRUPTION view and then repair corrupt blocks, if any, recorded in the view.
- The code will run a backup validate to populate the RC_BACKUP_CORRUPTION view and then repair corrupt blocks, if any, recorded in the view.

Answer:

The code will runs a backup validate to populate the V$DATABASE_BLOCK_CORRUPTION view and then repair corrupt blocks, if any, recorded in the view.

Explanation:

By using the CORRUPTION LIST clause, you can recover blocks that are listed in the V$DATABASE_BLOCK_CORRUPTION view. After a block has been repaired using block media recovery, V$DATABASE_BLOCK_CORRUPTION will not be updated until you take a new backup. This view displays information about the blocks that are marked corrupt since the last backup.

The option stating that the code will run a backup validation to populate the V$BACKUP_CORRUPTION view and then repairs corrupt blocks, if any, recorded in the view is incorrect. The CORRUPTION LIST clause is used to specify that the blocks listed in the V$DATABASE_BLOCK_CORRUPTION view will be recovered by using the Block Media Recovery feature. The V$BACKUP_CORRUPTION view displays information about the corrupted blocks in the datafile backups taken from the control file.

The option stating that the code will run a backup validation to populate the V$COPY_CORRUPTION view and then repairs any corrupt blocks recorded in the view is incorrect. The CORRUPTION LIST clause is used to specify that the blocks listed in the V$DATABASE_BLOCK_CORRUPTION view will be recovered by using the Block Media Recovery feature. The V$COPY_CORRUPTION view displays information about the corrupted blocks in the datafile copy from the control file.

The option stating that the code will run a backup validation to populate the RC_BACKUP_CORRUPTION view and then repair any corrupt blocks recorded in the view is incorrect. The CORRUPTION LIST clause is used to specify that the blocks listed in the V$DATABASE_BLOCK_CORRUPTION view will be recovered by using the Block Media Recovery feature. The RC_BACKUP_CORRUPTION view is used to display information about the corrupted blocks in the datafile backups. This view corresponds with the V$BACKUP_CORRUPTION view in the control file.

Item: 10 (Ref:1Z0-043.5.5.3)

While working on the database, you receive the following error:

```
01578: ORACLE data block corrupted (file# 6, block # 54)
ORA-01110 : data file 6: 'u01/oracle/oradata/data1.dbf'
```

You decide to recover the corrupted data block by using the Block Media Recovery feature. Which option is **NOT** a disadvantage of using block media recovery?

- Block Media Recovery must be used with RMAN.
- You must perform complete recovery of individual blocks.
- You must have a full RMAN backup, not an incremental backup.
- You must use the DBVERIFY utility before using the Block Media Recovery feature.

Answer:

You must use the DBVERIFY utility before using the Block Media Recovery feature.

Explanation:

You need not use the DBVERIFY utility before using the Block Media Recovery feature. The DBVERIFY utility is used to check whether or not corruption exists in a particular datafile. The name and location of the DBVERIFY utility is dependent on the operating system. The DBVERIFY utility can be used only with datafiles.

The Block Media Recovery (BMR) is an RMAN feature that is used to recover an individual block or a group of corrupt blocks in a datafile. This allows you to recover individual data blocks instead of the whole datafile. BMR is best used when block corruption is minimal. BMR reduces the mean time to recovery (MTTR) because only the affected data blocks are restored and recovered instead of the whole datafile. To perform Block Media Recovery, the BLOCKRECOVER command is issued at the RMAN prompt. In this scenario, you must issue the following command to perform Block Media Recovery:

```
RMAN>BLOCKRECOVER DATAFILE 6 BLOCK 54;
```

BMR has the following limitations:

- BMR must be used with RMAN.
- You must perform complete recovery of individual blocks. All redo logs must be applied to the block.
- You can only recover blocks marked as media corrupt.
- You must have a full RMAN backup, not an incremental backup.
- Media corrupt blocks are not accessible to users until the recovery is complete.

The other options are not disadvantages of using Block Media Recovery.

Item: 11 (Ref:1Z0-043.5.2.3)

You are using the DBVERIFY utility to check the datafiles for any block corruption. You want to write the output of the dbv command to a file not to the screen.

Which parameter of the DBVERIFY utility will you use?

- FILE
- PARFILE
- LOGFILE
- FEEDBACK

Answer:

LOGFILE

Explanation:

In this scenario, you will use the LOGFILE parameter. The LOGFILE parameter is used to specify the file in which the result of the dbv command will be written. The result of using the DBVERIFY utility is written in the file specified by the LOGFILE parameter and not on the screen. The DBVERIFY utility is used to check datafiles for any block corruption. The name and location of the DBVERIFY utility is dependent on the operating system. The DBVERIFY utility can be used only with datafiles. This utility checks the data blocks from the starting block in the file to the end of the file. You can specify the starting and ending data block in a file to be checked explicitly. For example, to perform an integrity check on the tbs_52.f datafile on the UNIX operating system, you can run the following dbv command:

```
% dbv file=tbs_52.f
```

The syntax of the DBVERIFY utility is as follows:

```
% dbv file=<name of file> <parameter_1>=<value of parameter_1>
<parameter_2>=<value of parameter_2>...
```

The different parameters of the DBVERIFY utility are as follows:

USERID: used to specify the username and password for the user who runs the command. If you are checking ASM files, then this parameter must be specified.
FILE: used to specify the name of the file to be checked for block corruption.
START: used to specify the starting block address that is to be checked. The block address is specified for Oracle data blocks. If you do not specify this parameter, then Oracle starts checking from the first block.
END: used to specify the ending block address that is to be checked. If you do not specify this parameter, then Oracle performs a check up to the last block.
BLOCKSIZE: used to specify the block size of the database. The value of this parameter should be the same as the value of the DB_BLOCK_SIZE init.ora parameter.
LOGFILE: used to specify a file that contains logging information about the processing of the DBVERIFY utility.
FEEDBACK: used to trigger the DBVERIFY utility to display the progress of the file being checked for block corruption.
HELP: used to provide online help regarding the use of the DBVERIFY utility.
PARFILE: used to specify the name of a parameter file. In a parfile, you can specify various values for the parameters used in a DBVERIFY utility.

The option stating that FILE parameter specifies that the result of the dbv command will be written in the specified file not to the screen is incorrect. This is because the FILE parameter is used to specify the datafile that is to be checked for block corruption.

The option stating that PARFILE parameter specifies that the result of the dbv command will be written in the specified file not to the screen is incorrect. This is because the PARFILE parameter is used to specify the name of a parameter file. In a parfile, you can specify various values for the parameters used in a DBVERIFY utility.

The option stating that FEEDBACK parameter specifies that the result of the dbv command will be written in the specified file not to the screen is incorrect. This is because the FEEDBACK parameter is used to trigger the DBVERIFY utility to display the progress of the file being checked for block corruption.

Item: 12 (Ref:1Z0-043.5.3.1)

You want to check the EMP table in the user, Scott's schema for block corruption. You also want to fix the corrupted blocks, if any. How will you accomplish the required task?

- by using the ANALYZE utility
- by using the DBVERIFY utility
- by using the DB_BLOCK_CHECKING parameter
- by using the DBMS_REPAIR package

Answer:

by using the DBMS_REPAIR package

Explanation:

You will use the DBMS_REPAIR package to check the objects for block corruption and fix corrupted blocks, if any. The DBMS_REPAIR package contains multiple stored procedures. Each procedure performs different actions. The CHECK_OBJECT procedure of the DBMS_REPAIR package is used to check the objects for corruption and the FIX_CORRUPT_BLOCKS procedure of the DBMS_REPAIR package is used to fix the corrupted blocks. For example, to check the SCOTT.EMP table for corrupted blocks, you should use the following code:

```
SET SERVEROUTPUT ON
DECLARE corrupt_num INT;
BEGIN
corrupt_num := 0;
DBMS_REPAIR.CHECK_OBJECT (
SCHEMA_NAME => 'SCOTT',
OBJECT_NAME => 'EMP',
REPAIR_TABLE_NAME => 'REPAIR_TABLE',
CORRUPT_COUNT => corrupt_num);
DBMS_OUTPUT.PUT_LINE('number corrupt: ' || TO_CHAR
(corrupt_num));
END;
/
```

The above code enables you to identify the corrupt blocks in the SCOTT.EMP table.
The following code enables you to fix the corrupted blocks in the SCOTT.EMP table:

```
SET SERVEROUTPUT ON
DECLARE fix_num INT;
BEGIN
fix_num := 0;
DBMS_REPAIR.FIX_CORRUPT_BLOCKS (
SCHEMA_NAME => 'SCOTT',
OBJECT_NAME=> 'EMP',
OBJECT_TYPE => dbms_repair.table_object,
REPAIR_TABLE_NAME => 'REPAIR_TABLE',
FIX_COUNT=> num_fix);
DBMS_OUTPUT.PUT_LINE('num fix: ' || TO_CHAR(fix_num));
END;
/
```

The option stating that you will use the ANALYZE utility to check the SCOTT.EMP table and fix the corrupted blocks of the SCOTT.EMP table is incorrect. The ANALYZE TABLE table_name VALIDATE STRUCTURE command is either successful or unsuccessful at the object level. If this command returns an error for the object to be analyzed, then you must completely rebuild the object. If no error is returned, then the object is not corrupted and should not be re-created. This utility is not used for fixing corrupted blocks.

The option stating that you will use the DBVERIFY utility to check the SCOTT.EMP table and fix the corrupted blocks of the SCOTT.EMP table is incorrect. The DBVERIFY utility is an Oracle utility that is used to check whether corruption exists in a particular datafile or not. This utility is mostly used on the backup of the database or when the database is not running. This utility is not used for fixing the corrupted blocks.

The option stating that you will use the DB_BLOCK_CHECKING parameter to check the SCOTT.EMP table and fix the corrupted blocks of the SCOTT.EMP table is incorrect. The DB_BLOCK_CHECKING initialization parameter sets block checking at the database level. The default value of the DB_BLOCK_CHECKING initialization parameter is set to FALSE for all the nonsystem tablespaces. The SYSTEM tablespace is enabled by default. The DB_BLOCK_CHECKING parameter can be dynamically set by using the ALTER SYSTEM SET statement. This parameter forces checks for corrupted blocks if blocks are modified at the tablespace level. A checksum occurs every time a block is modified. This utility is not used for fixing corrupt blocks.

Item: 13 (Ref:1Z0-043.5.4.3)

William specified the following initialization parameter settings in the pfile:

```
BACKGROUND_DUMP_DEST = 'u01\oradata\dir_A'
USER_DUMP_DEST = 'u01\oradata\dir_B'
DB_CREATE_FILE_DEST = 'u01\oradata\dir_C'
DB_CREATE_ONLINE_LOG_DEST_n = 'u01\oradata\dir_D'
```

William enabled the change-tracking feature because he does not want to scan the entire datafile during backup. What is the default storage location for the change tracking file?

- 'u01\oradata\dir_A'
- 'u01\oradata\dir_B'
- 'u01\oradata\dir_C'
- 'u01\oradata\dir_D'

Answer:

'u01\oradata\dir_C'

Explanation:

When you enable the change-tracking feature, the default location of the change tracking file is the value that is specified for the DB_CREATE_FILE_DEST initialization parameter. In this scenario, the default location of the change tracking file will be 'u01\oradata\dir_C' because this is the value of the DB_CREATE_FILE_DEST parameter specified in the pfile. The DB_CREATE_FILE_DEST and the DB_CREATE_ONLINE_LOG_DEST_n parameters are used to configure Oracle Managed Files (OMF). If OMF is configured, then Oracle automatically maintains the name and location of the change tracking file. Oracle stores the change tracking file in the location specified by the value of the DB_CREATE_FILE_DEST parameter.

The 'u01\oradata\dir_A' option is incorrect because it is the default location of the block change tracking file as specified by the BACKGROUND_DUMP_DEST parameter. This parameter is used to specify the location of the alert log files and the trace files for background processes. Alert log files are used to view information regarding internal errors (ora-600), block corruption errors (ora-1578), and deadlock errors (ora-60). Alert log files also store the values of the initialization parameters that have non-default values. If the LGWR process fails to write information to the redo log groups, then an error will be stored in the trace files. The trace files are used to store detailed information regarding the causes of failure of the background processes.

The 'u01\oradata\dir_B' option is incorrect because it is the default location of the change tracking file as specified by the USER_DUMP_DEST parameter. This parameter is used to specify the location of user trace files. All trace files for server processes are stored in the location specified by the USER_DUMP_DEST parameter. If the server process encounters a problem, the information about the problem is written to these trace files.

The 'u01\oradata\dir_D' option is incorrect because it is the default location of the change tracking file as specified by the DB_CREATE_ONLINE_LOG_DEST_n parameter. This parameter is used to specify the default location of the redo log groups and control files.
If this parameter is specified in the pfile and the names and locations of the log files and control files are not specified at the time of database creation, Oracle automatically creates these files at the location specified by the value of this parameter.

Item: 14 (Ref:1Z0-043.5.4.1)

You want to check all the data blocks being written to the datafiles by analyzing the data on each block every time the DBWn process writes.

Which action will you perform to check the data blocks?

- Set the value of the DB_BLOCK_CHECKING initialization parameter to TRUE.
- Use the ANALYZE utility.
- Use the DBVERIFY utility.
- Use the DBMS_REPAIR package.

Answer:

Set the value of the DB_BLOCK_CHECKING initialization parameter to TRUE.

Explanation:

The DB_BLOCK_CHECKING initialization parameter sets block checking at the database level. The default is set to FALSE for all nonsystem tablespaces. The SYSTEM tablespace is enabled by default. The DB_BLOCK_CHECKING parameter can be dynamically set by using the ALTER SYSTEM SET statement. This parameter forces checks for corrupt blocks each time blocks are modified at the tablespace level. A checksum occurs every time a block is modified.

The option stating that you will use the ANALYZE utility is incorrect. This is because the ANALYZE utility validates the integrity of the structure of the object being analyzed. The ANALYZE TABLE table_name VALIDATE STRUCTURE command is either successful or unsuccessful at the object level. If this command returns an error for the object to be analyzed, then you will be required to completely rebuild the object. If no error is returned, then the object is not corrupted and should be recreated.

The option stating that you will use the DBVERIFY utility is incorrect. The DBVERIFY utility is an Oracle utility that is used to check whether corruption exists in a particular datafile or not. This utility is mostly used on the backup of the database or when the database is not running.

The option stating that you will use the DBMS_REPAIR package is incorrect. The DBMS_REPAIR package is a set of procedures that enables you to detect and fix corrupted blocks in tables and indexes. The DBMS_REPAIR package consists of the following procedures:

CHECK_OBJECT	Detects and reports corruption in a table or an index
FIX_CORRUPT_BLOCKS	Marks blocks that were previously identified by the CHECK_OBJECT procedure as corrupted
DUMP_ORPHAN_KEYS	Reports index entries into an orphan key table. These index entries point to rows in the corrupted data blocks
REBUILD_FREELISTS	Rebuilds the freelists of the object
SEGMENT_FIX_STATUS	Provides the capability to fix the corrupted state of a bitmap entry when segment space management is set to AUTO
SKIP_CORRUPT_BLOCKS	When used, ignores blocks that are marked corrupt during table and index scans. If not used, you will receive an ORA-1578 error while encountering corrupted blocks
ADMIN_BLOCKS	Provides administrative functions, such as CREATE, DROP, and PURGE, to repair orphan key tables that are always created in the SYS schema.

Each procedure performs different actions. For example, the CHECK_OBJECT procedure and the FIX_CORRUPT_BLOCKS procedure of the DBMS_PACKAGE are used to check the object and fix the corrupted blocks of the object respectively.

Automatic Database Management

Item: 1 (Ref:1Z0-043.6.1.2)

You create a table in your database that contains 50,000 rows approximately. The queries performed on the table are complex and performed on the table frequently.

Which advisor helps you achieve the best performance of database for queries by recommending the appropriate indexes?

- SQL Access Advisor
- Memory Advisor
- SQL Tuning Advisor
- Segment Advisor

Answer:

SQL Access Advisor

Explanation:

The SQL Access advisor recommends the appropriate indexes and materialized views to achieve the best performance of the database when the workload on the database is high. This advisor recommends both, the bitmap indexes and the B-tree indexes. A bitmap index is used to reduce the response time for many types of ad hoc queries. Moreover, this index requires less storage space as compared to other types of indexes. The B-tree indexes are most commonly used in a data warehouse.

The option stating that the Memory Advisor helps achieve the best performance by recommending the appropriate indexes is incorrect. The Memory Advisor helps tune the size of different Oracle memory structures.

The option stating that the SQL Tuning Advisor helps achieve the best performance by recommending the appropriate indexes is incorrect. The SQL Tuning Advisor is used to analyze individual SQL statements and provide recommendations to enhance performance.

The option stating that the Segment Advisor helps achieve the best performance by recommending the appropriate indexes is incorrect. The Segment Advisor analyzes space fragmentation within segments and identifies the segments for online shrink operation.

Item: 2 (Ref:1Z0-043.6.2.3)

You are creating a SQL Tuning Set to allow a group of SQL statements to be passed into the SQL Tuning Advisor.

Which packages will you use to create the SQL Tuning Set?

- DBMS_WORKLOAD_REPOSITORY
- DBMS_RESOURCE_MANAGER
- DBMS_SQLTUNE
- DBMS_ADVISOR

Answer:

DBMS_SQLTUNE

Explanation:

You will use the DBMS_SQLTUNE package to create the SQL Tuning package. The DBMS_SQLTUNE package allows running tasks to be created and executed. It also allows you to process the recommendations provided by tuning tasks. The syntax of the SQL Tuning Set is as follows:

```
BEGIN
DBMS_SQLTUNE.CREATE_SQLSET(
Sqlset_name => 'name',
Description => 'SQL used in load procedure');
END;
```

The option stating that you will use the DBMS_WORKLOAD_REPOSITORY package to create the SQL Tuning Advisor is incorrect. This Application Program Interface(API) allows management of all AWR functionality. The DBMS_WORKLOAD_REPOSITORY package consists of the following procedures:

CREATE_SNAPSHOT	Creates manual snapshots
DROP_SNAPSHOT_RANGE	Drops a range of snapshots at once
CREATE_BASELINE	Creates a single baseline
MODIFY_SNAPSHOT_SETTINGS	Changes the RETENTION and the INTERVAL settings

The option stating that you will use the DBMS_RESOURCE_MANAGER package to create the SQL Tuning Advisor is incorrect. The DBMS_RESOURCE_MANAGER package is used to manage resource consumer groups. The DBMS_RESOURCE_MANAGER package offers procedures that allow you to create, delete, and modify the resource consumer groups.

The option stating that you will use the DBMS_ADVISOR package to create the SQL Tuning Advisor is incorrect. The DBMS_ADVISOR package is new to Oracle10*g*. The DBMS_ADVISOR package represents an API to execute advisor procedures declarations. The procedures available in the DBMS_ADVISOR package are as follows:

CREATE_TASK	Adds a new task to the repository
DELETE_TASK	Removes a task from the repository
EXECUTE_TASK	Executes a task
INTERRUPT_TASK	Is used to suspend a running task
CREATE_TASK_REPORT	Generates a recommendations report
RESUME_TASK	Resumes execution of a suspended task
UPDATE_TASK_ATTRIBUTESD	Updates the attributes of a task
SET_TASK_PARAMETER	Sets or modifies the parameters for a task
MARK_RECOMMENDATION	Accepts, rejects, or ignores one or more recommendations
CREATE_TASK_SCRIPT	Creates a SQL script of all the accepted recommendations

Item: 3 (Ref:1Z0-043.6.2.1)

You accepted the recommended SQL Profile by executing the following code:

```
DECLARE
sqlprofile_name varchar2(30);
BEGIN
sqlprofile_name := DBMS_SQLTUNE.ACCEPT_SQL_PROFILE(
task_name => 'my_task',
profile_name => 'my_profile');
END;
```

Which advisor will analyze this profile?

- SQL Access Advisor
- Undo Advisor
- Segment Advisor
- SQL Tuning Advisor

Answer:

SQL Tuning Advisor

Explanation:

The SQL Tuning Advisor will analyze the profile created by the following code:

```
DECLARE
sqlprofile_name varchar2(30);
BEGIN
sqlprofile_name := DBMS_SQLTUNE.ACCEPT_SQL_PROFILE(
task_name => 'my_task',
profile_name => 'my_profile');
END;
```

SQL Profiles contain auxiliary statistics specific to a single query that help the optimizer to generate an optimal execution path. Oracle automatically builds a profile by using sampling, partial execution, and execution history. This profile is stored in the data dictionary. When the above query is executed, the optimizer includes the profile while performing an analysis. After this, the optimizer generates an execution plan.

The SQL Access Advisor does not analyze the SQL profiles. The SQL Access Advisor is used to analyze a SQL workload that can consist of one or more SQL statements. The SQL Access Advisor also recommends appropriate access structures to improve the performance of the workload. These access structures include materialized views and indexes.

The Undo Advisor does not analyze the SQL profiles. The Undo Advisor enables you to determine appropriate sizing for Undo tablespaces and optimal `UNDO_RETENTION` settings. The Undo Advisor prevents the Snapshot too old error from being generated. The Snapshot too old error is a common error generated for long running queries. The Undo Advisor enables you to identify problems related to the Undo tablespace and provides solutions to the problems.

The Segment Advisor does not analyze the SQL profiles. The Segment Advisor is a component of Oracle Advisory that analyzes space fragmentation within segments and identifies segments that are good candidates for a new, online shrink operation. In earlier versions of Oracle, repairing fragmentation generally meant dropping and recreating objects or using a command such as `ALTER TABLE MOVE.` The Segment Advisor notifies you of fragmented segments and can reclaim the wasted space by using the online shrink operation.

Item: 4 (Ref:1Z0-043.6.1.6)

You are maintaining the SALES database for eSoft Corporation. You have not configured ASMM on the database. You want to know what size of the SGA will provide the best performance.

Which advisor would you use to determine the suitable size of the SGA?

- SQL Tuning Advisor
- Undo Advisor
- ADDM
- Memory Advisor

Answer:

Memory Advisor

Explanation:

You will use Memory Advisor to determine the suitable size of your database. The Memory Advisor helps you to tune the size of the Oracle memory structures. Within the Memory Advisor, the following advisors are available to help optimize individual areas of memory:

- SGA Advisor
- PGA Advisor
- Buffer Cache Advisor
- Shared Pool Advisor

Each of these sub-advisors helps you in determining the optimum size for its associated Oracle memory structure. These sub-advisors also help you to identify and resolve problems relating to the structure.

The SQL Tuning Advisor is incorrect because this advisor is used to analyze individual SQL statements and provide recommendations to increase query performance. The SQL Tuning Advisor can be run against SQL statements identified as problematic by ADDM, against the most resource intensive SQL statement from AWR, or against any user-defined SQL statement.

The Undo Advisor is incorrect because this advisor helps determine appropriate sizing for Undo tablespaces and helps determine the optimal `UNDO_RETENTION` settings. The Undo Advisor prevents the error: Snapshot too old from being generated. The Snapshot too old error is a common problem for long running queries. The Undo Advisor helps you in identifying problems related to the Undo tablespace and provides recommendations to help correct those problems.

ADDM is incorrect because the Automatic Database Diagnostic Monitor (ADDM) is a self diagnostic engine built into the database server. The ADDM is automatically invoked by the Oracle 10*g* database and performs analysis to determine any issues in the database. The ADDM recommends solutions to the issues it identifies. ADDM provides automated proactive tuning of an Oracle 10*g* instance and identifies performance issues and bottlenecks within the database.

Item: 5 (Ref:1Z0-043.6.1.4)

You find pockets of empty space in the USER_DATA tablespace due to a lot of DML operations on the objects in the USER_DATA tablespace. The pockets of empty spaces are too small to be reused individually. This is leading to wastage of space. You decide to perform the shrink operation to reclaim the wasted space.

Which advisor will you use to determine the objects in the USER_DATA tablespace that are good candidates for the shrink operation?

- SQL Tuning Advisor
- SQL Access Advisor
- Undo Advisor
- Segment Advisor

Answer:

Segment Advisor

Explanation:

You can use the Segment Advisor to determine the objects in the USER_DATA tablespace that are good candidates for the shrink operation. The Segment Advisor analyzes space fragmentation within segments and identifies the segments that are good candidates for a new, online shrink operation. In earlier versions of Oracle, repairing fragmentation generally meant dropping and recreating objects or using a command such as ALTER TABLE MOVE. The Segment Advisor notifies you of fragmented segments and can reclaim the wasted space using the online shrink operation.

The option stating that you can use a SQL Tuning Advisor to determine the objects in the USER_DATA tablespace that are good candidates for a shrink operation is incorrect. The SQL Tuning Advisor is used to analyze individual SQL statements and provides recommendations to increase performance. The SQL Tuning Advisor can be run against the SQL identified by ADDM as problematic over the most resource-intensive SQL from AWR or any user-defined SQL.

The option stating that you can use a SQL Access Advisor to determine the objects in the USER_DATA tablespace that are good candidates for a shrink operation is incorrect. The SQL Access Advisor is used to analyze a SQL workload that can consist of one or more SQL statements and recommend appropriate access structures to improve the performance of the workload. These access structures include materialized views, indexes, and so on.

The option stating that you can use Undo Advisor to determine the objects in the USER_DATA tablespace that are good candidates for a shrink operation is incorrect. The Undo Advisor enables you to determine appropriate sizing for Undo tablespaces and optimal UNDO_RETENTION settings. The Undo Advisor prevents the error: Snapshot too old from being generated. The Snapshot too old error is a common problem for long running queries. The Undo Advisor assists in identifying problems related to the Undo tablespace and offers advice for the solution to those problems.

Item: 6 (Ref:1Z0-043.6.1.5)

You find that some queries on a table are taking a long time to execute because there are no indexes created on the table. You decide to invoke the SQL Access Advisor to determine the appropriate index to be created.

Which package will you use to invoke the SQL Access Advisor?

- DBMS_SERVER_ALERT
- DBMS_ADVISOR
- DBMS_RESOURCE_MANAGER
- DBMS_REPAIR

Answer:

DBMS_ADVISOR

Explanation:

You will use the DBMS_ADVISOR package to invoke the SQL Access Advisor that determines the appropriate index to be created. This package represents an API to execute advisor procedures. The DBMS_ADVISOR package can be used to access all advisors because it contains all the necessary constants and procedure declarations. The procedures available in the DBMS_ADVISOR package are as follows:

Procedure	Description
CREATE_TASK	Adds a new task in the repository
DELETE_TASK	Removes a task from the repository
EXECUTE_TASK	Executes a task
INTERRUPT_TASK	Suspends a running task
CREATE_TASK_REPORT	Generates a recommendation report
RESUME_TASK	Resumes execution of a suspended task
UPDATE_TASK_ATTRIBUTES	Updates the attributes of a task
SET_TASK_PARAMETER	Sets or modifies parameters for a task
MARK_RECOMMENDATION	Accepts, rejects, or ignores one or more recommendations
CREATE_TASK_SCRIPT	Creates a SQL script of all accepted recommendations

The option stating that the DBMS_SERVER_ALERT package is used to invoke the SQL Access Advisor that determines the appropriate index to be created is incorrect. The DBMS_SERVER_ALERT package is used to explicitly set the warning level and the critical level threshold values. For example if you are changing the value of warning threshold to 70 percent and critical threshold to 90 percent, you will use the following code:

```
DBMS_SERVER_ALERT.SET_THRESHOLD(
   DBMS_SERVER_ALERT.TABLESPACE_FULL,
   DBMS_SERVER_ALERT.OPERATOR_GE, 70,
   DBMS_SERVER_ALERT.OPERATOR_GE, 90, 1, 1, null,
   DBMS_SERVER_ALERT.OBJECT_TYPE_TABLESPACE, 'USERS');
```

These threshold levels will be compared to the percentage of space used in the USERS tablespace every minute, causing an alert the first time the value exceeds the threshold value for the USERS tablespace.

The option stating that the DBMS_RESOURCE_MANAGER package is used to invoke the SQL Access Advisor to determine the appropriate index to be created is incorrect. The DBMS_RESOURCE_MANAGER package is used to manage resource consumer groups. A resource consumer group is a method of classifying users based on their resource consumption tendencies or requirements. This package offers procedures that enable you to create, delete, and modify resource consumer groups. You must have the ADMINISTER_RESOURCE_MANAGER system privilege to administer the Database Resource Manager.

The option stating that the DBMS_REPAIR package is used to invoke the SQL Access Advisor to determine the appropriate index to be created is incorrect. The DBMS_REPAIR package is a set of procedures that enables you to detect and fix corrupt blocks in tables and indexes. The DBMS_REPAIR package consists of multiple stored procedures. Each procedure performs different actions. The different procedures and their descriptions are as follows:

Procedure	Description
CHECK_OBJECT	Detects and reports corruptions in a table or index
FIX_CORRUPT_BLOCKS	Marks blocks that were previously identified by the

	CHECK_OBJECT procedure as software corrupt
DUMP_ORPHAN_KEYS	Reports index entries into an orphan key table that points to rows in corrupt data blocks
REBUILD_FREELISTS	Rebuilds the freelists of the object
SEGMENT_FIX_STATUS	Provides the capability to fix the corrupted state of a bitmap entry when segment space management is set to AUTO
SKIP_CORRUP_BLOCKS	Ignores blocks marked corrupt during table and index scans. If this procedure is not used, you receive an ORA-1578 error when encountering blocks marked corrupt
ADMIN_TABLES	Provides administrative functions, such as create or drop, for the repair of orphan key tables

Item: 7 (Ref:1Z0-043.6.2.4)

Which component does the SQL Tuning Advisor **NOT** analyze for the SQL statements?

- ADDM
- AWR
- Cursor Cache
- SQL Tuning Sets
- Flash Recovery Area

Answer:

Flash Recovery Area

Explanation:

The SQL Tuning Advisor does not analyze the Flash Recovery Area for the SQL statements. The Flash Recovery Area is not related to the generation of recommendations for badly written SQL statements. Recovery related files can be stored in the Flash Recovery Area. The Flash Recovery Area can be a single directory, an entire file system, or an Automatic Storage Management (ASM) disk group. The SQL Tuning Advisor uses an enhanced mode to run a heavily used and resource-intensive SQL statement and performs a number of analyses to generate an optimal execution plan. This optimal execution plan can be far superior to the execution plan generated by the traditional cost-based optimizer algorithm. The SQL Tuning Advisor also uses the information from ADDM to compensate for stale or missing statistics until the statistics can be recomputed. The input sources of SQL Tuning Advisor are as follows:

- ADDM (Automatic Database Diagnostic Monitor) a primary input source for the SQL Tuning Advisor. Statistics on the performance of the database are stored in the AWR. ADDM analyzes these statistics every hour and if it finds high-load SQL statements, recommends that the SQL Tuning Advisor be run.
- High-load SQL statements another important input source for the SQL Tuning Advisor. High-load SQL statements are captured in the AWR and the snapshots of the system activities, including high-load SQL statements, CPU wait time, CPU consumption, and so on are taken at regular intervals. You can view these statistics to identify the high-load SQL statements and run the SQL Tuning Advisor on them.
- Cursor cache includes the recent SQL statements that are to be captured by the AWR. To tune high-load SQL statements going back in time to as far as the AWR retention time allows, the AWR and the cursor cache are together used to identify the statements on which you will run the SQL Tuning Advisor.
- SQL Tuning Set a set of SQL statements along with their execution information, such as the schema name under which the SQL statement was executed, average time for the execution, the values of the bind variables, and so on.

SQL Tuning Advisor is used to provide a quick and efficient technique for optimizing SQL statements without modifying any statement. The valid input sources for SQL Tuning Advisor are as follows:

- AWR captures high load SQL statements
- ADDM is used as a primary input source for the SQL Tuning Advisor
- Cursor Cache stores SQL statements that are yet to be captured by AWR
- SQL Tuning Sets are user-defined sets of SQL statements combined in an object

Item: 8 (Ref:1Z0-043.6.1.1)

While running long running queries, you receive the `Snapshot too old` error. Which advisor can help you to avoid the `Snapshot too old` error?

- Memory Advisor
- Segment Advisor
- Undo Advisor
- SQL Tuning Advisor

Answer:

Undo Advisor

Explanation:

The Undo Advisor helps you to determine appropriate sizing for the Undo tablespace and helps to determine optimal `UNDO_RETENTION` settings. The `Snapshot too old` error is generated when the undo data required by a long running query is overwritten. This error can be avoided by using the appropriate size of the Undo tablespace and value of the `UNDO_RETENTION` parameter. The Undo Advisor also helps to identify the problems relating to the Undo tablespaces and offers advice to correct the problems.

The option stating that the Memory Advisor can help you to avoid the `Snapshot too old` error is incorrect. This is because the Memory Advisor helps you to tune the size of different Oracle memory structures. Within a Memory Advisor, the following advisors are available to help you optimize individual area of memory:

- SGA Advisor Helps in determining the size of the SGA.
- PGA Advisor Helps in determining the size of the PGA
- Buffer Cache Advisor Helps in determining the size of buffer cache.
- Library Cache Advisor helps in determining the size of the shared pool

The option stating that the Segment Advisor can be used to avoid the `Snapshot too old` error is incorrect. This is because the Segment Advisor is used to determine the objects in a tablespace that are good candidates for the shrink operation. The Segment Advisor analyzes space fragmentation within segments and identifies the segments that are good candidates for online shrink operation.

The option stating that the SQL Tuning Advisor can be used to avoid the `Snapshot too old` error is incorrect. This is because the SQL Tuning Advisor is used to analyze individual SQL statements and provides recommendations to increase performance. The SQL Tuning Advisor can be run against the SQL identified by ADDM as problematic over the most resource-intensive SQL from `AWR`, or any user-defined SQL. The SQL Tuning Advisor can be run against the user defined SQL statements. The SQL Tuning Advisor can also be run against the SQL statements that are identified as problematic because the statements are most resource consuming.

Item: 9 (Ref:1Z0-043.6.1.3)

You use the Memory Advisor to tune the memory structures of your database. What is the prerequisite to use the Memory Advisor?

- The database must be in the ARCHIVELOG mode.
- The automatic memory tuning must be enabled.
- The change tracking feature must be enabled.
- The automatic memory tuning must be disabled.

Answer:

The automatic memory tuning must be disabled.

Explanation:

For using the Memory Advisor to tune the memory structures, the automatic memory-tuning feature must be disabled. Memory Advisor helps tune the size of the different Oracle memory structures. Within a Memory Advisor, the following advisors are available to optimize individual memory areas:

- SGA Advisor
- PGA Advisor
- Buffer Cache Advisor
- Library Cache Advisor

The option stating that for using the Memory Advisor to tune the memory structures, the database must be in the ARCHIVELOG mode is incorrect. ARHCHIVELOG mode is not a prerequisite for using the Memory Advisor. If the database is in the ARCHIVELOG mode and log switching occurs, then the ARCn process writes the redo log entries from the filled online redo log file to the archive log file. After a redo log file is full, the LGWR process starts writing to the next redo log file. This event is called log switching. You can also perform log switching by using the ALTER SYSTEM SWITCH LOGFILE; command.

The option stating that for using the Memory Advisor to tune the memory structures, the automatic change-tracking feature must be enabled is incorrect. The block change-tracking feature is used to increase the performance of the backup process while performing the incremental backup.

The option stating that for using the Memory Advisor to tune the memory structures, the automatic memory-tuning feature must be enabled is incorrect.

Item: 10 (Ref:1Z0-043.6.3.1)

You are maintaining your database in Oracle10*g*. You set the value of the UNDO_RETENTION initialization parameter to zero in the initialization parameter file.
What will be the impact of specifying this setting?

- The database will not start.
- The database will start but will not retain the undo data in the undo segment.
- The database will start, and the undo segment will contain the undo data for at least one hour.
- The database will start, and the undo segment will retain the undo data for at least 15 minutes.

Answer:

The database will start, and the undo segment will retain the undo data for at least 15 minutes.

Explanation:

The database will start and the undo segment will retain the undo data for at least 15 minutes. The value of the UNDO_RETENTION parameter has an impact on the automatic autotuning. The default value of the UNDO_RETENTION parameter is 900 seconds. If you do not specify a value or if you specify the value, zero, for the UNDO_RETENTION parameter, Oracle10*g* automatically tunes the undo retention for the current undo tablespace by using 900 seconds as the minimum value. If you specify a value other than zero for the UNDO_RETENTION parameter, then Oracle10*g* continues to autotune the undo retention by using the specified value of the UNDO_RETENTION parameter as the minimum value. In this scenario, the UNDO_RETENTION parameter value will be used as 900 seconds, that is, 15 minutes.

The option stating that the database will not start is incorrect. The database will start and the undo segment will contain the undo data in the undo segment for 15 minutes.

The option stating that the database will start but will not retain the undo data in the undo segment is incorrect. This is because the database cannot work properly if the undo segment cannot retain the undo data. The database will retain the undo data in the undo segments for the default value of the UNDO_RETENTION parameter, that is, 900 seconds.

The option stating that the database will start and the undo segment will contain the undo data for at least one hour is incorrect. The default value of the UNDO_RETENTON parameter is 900 seconds. The database will retain the undo data in the undo segments for the default value of the UNDO_RETENTION parameter, which is equal to 900 seconds.

Automatic Storage Management

Item: 1 (Ref:1Z0-043.11.2.1)

Which statement will **NOT** create a tablespace?

- `CREATE TABLESPACE DATA1 DATAFILE '+grp1/abc(datafile)';`
- `CREATE TABLESPACE DATA1 DATAFILE '+grp1';`
- `CREATE TABLESPACE DATA1 DATAFILE '+data1(tempfile)';`
- `CREATE TABLESPACE DATA1 DATAFILE '+grp1.256.34359';`

Answer:

`CREATE TABLESPACE DATA1 DATAFILE '+grp1.256.34359';`

Explanation:

The `CREATE TABLESPACE DATA1 DATAFILE '+grp1.256.34359';` statement cannot be used to create a tablespace. This is because `'+grp1.256.34359'` is a numeric form of the ASM file name. You cannot specify an ASM filename in the numeric form during tablespace creation. The numeric form of the ASM file name consists of a diskgroup name, a file number, and an incarnation number. In the `CREATE TABLESPACE DATA1 DATAFILE '+grp1.256.34359';` command, `'+grp1'` is a diskgroup name, `256` the file number, and `34359` the incarnation number of the disk. The numeric form of ASM files can be used to reference the existing files.

The option stating that the `CREATE TABLESPACE DATA1 DATAFILE '+grp1/abc(datafile)'`; statement will not create a tablespace is incorrect. The statement will create a tablespace with an alias by using a template for the tablespace, `DATA1`. You can use an alias with a template only while creating a new ASM file.

The option stating that the `CREATE TABLESPACE DATA1 DATAFILE '+grp1'`; statement will not create a tablespace is incorrect. You can use an incomplete filename format either for single file or multiple file creation operations. You should specify only the disk group name and use a default template depending on the type of the file.

The option stating that the `CREATE TABLESPACE DATA1 DATAFILE '+data1(tempfile)'`; statement will not create a tablespace is incorrect. While creating a tablespace, you can use the characteristics of a tempfile as the attributes for a datafile.

Item: 2 (Ref:1Z0-043.11.4.3)

You are maintaining the SALES database on Oracle 10*g*. You have added a new disk to a disk group. Automatic Storage Management performs the rebalancing activity. You want to speed up the rebalancing activity.

Which parameter will you specify to control the speed of the rebalancing activity?

- ASM_POWER_LIMIT
- ASM_DISKSTRING
- ASM_DISKGROUPS
- LARGE_POOL_SIZE

Answer:

ASM_POWER_LIMIT

Explanation:

You will use the ASM_POWER_LIMIT parameter to control the speed of the rebalancing activity. To ensure that rebalancing operations do not interfere with the ongoing user I/O, the ASM_POWER_LIMIT parameter controls the speed of rebalancing operations. The value for the ASM_POWER_LIMIT parameter ranges from 0 to 11 where 11 is the highest possible value. The default value, 1, indicates low overhead. This is a dynamic parameter; therefore, you can set this to a low value during the day and to a higher value overnight whenever a disk rebalancing operation must occur.

The option stating that the ASM_DISKSTRING parameter is used to control the speed of rebalance is incorrect. The ASM_DISKSTRING parameter specifies one or more strings, which are operating system dependent, to limit the disk devices that can be used to create disk groups.

The option stating that the ASM_DISKGROUPS parameter is used to control the speed of rebalance is incorrect. The ASM_DISKGROUPS parameter specifies a list containing the names of the disk groups that will be automatically mounted by the ASM instance at startup or by the ALTER DISKGROUP ALL MOUNT command.

The option stating that the LARGE_POOL_SIZE parameter is used to control the speed of rebalance is incorrect. The LARGE_POOL_SIZE parameter is useful for both regular and ASM instances. However, this pool is used differently for an ASM instance. All ASM packages are executed from this pool; therefore, the value of the LARGE_POOL_SIZE parameter should be set to at least 8 MB.

Item: 3 (Ref:1Z0-043.11.4.1)

Consider the following configuration:

/devices/diskP1 is a member of disk group grp1.
/devices/diskP2 is a member of disk group grp1.
/devices/diskP3 is a member of disk group grp1.
/devices/diskP4 is a candidate disk.
/devices/diskQ1 is a member of disk group grp2.
/devices/diskQ2 is a member of disk group grp2.
/devices/diskQ3 is a member of disk group grp2.
/devices/diskQ4 is a candidate disk.

Which command will add the disk /devices/diskP4 to the disk group, grp1?

- ALTER DISKGROUP grp1
  ADD DISK '/devices/diskP1',
  ADD DISK '/devices/diskP4';
- ALTER DISKGROUP grp1
  ADD DISK '/devices/disk*4';
- ALTER DISKGROUP grp1
  ADD DISK '/devices/diskP*';
- ALTER DISKGROUP grp1
  ADD DISK '/devices/diskQ*',
  ADD DISK '/devices/diskP*';

Answer:

```
ALTER DISKGROUP grp1
ADD DISK '/devices/diskP*';
```

Explanation:

The following command will add the disk /devices/diskP4 to the disk group, grp1:

```
ALTER DISKGROUP grp1
   ADD DISK '/devices/diskP*';
```

The above command will ignore '/devices/diskP1', '/devices/diskP2', and '/devices/diskP3' because they already belong to grp1. The above command will not fail because the other disks that match the search string are not members of any other disk group.

The option stating that the following command will add the disk /devices/diskP4 to the disk group grp1 is incorrect.

```
ALTER DISKGROUP grp1
   ADD DISK '/devices/diskP1',
   ADD DISK '/devices/diskP4';
```

The above command will fail because the '/device/diskP1' search matches a disk that is already a member of the group, grp1.

The option stating that the following command will add the disk /devices/diskP4 to the disk group grp1 is incorrect.

```
ALTER DISKGROUP grp1
ADD DISK '/devices/disk*4';
```

The above command will fail because the search string matches a disk that is a member of another disk group, grp2.

The option stating that the following command will add the disk /devices/diskP4 to the disk group grp1 is incorrect.

```
ALTER DISKGROUP grp1
   ADD DISK '/devices/diskQ*',
   ADD DISK '/devices/diskP*';
```

The above command will fail because the search string matches disks that are members of another disk group, grp2.

Item: 4 (Ref:1Z0-043.11.1.3)

You are the Database Administrator for WonderWeb, which has recently acquired a media company TXGlobal. You have been assigned the task to migrate all the database applications of TXGlobal to the database server of WonderWeb. To accommodate more database applications, you need to add disks to the existing disk group.

Whenever you add or remove disks from the disk group, Automatic Storage Management (ASM) rebalancing distributes the data evenly across all the disks of the disk group.

Which background process performs this actual rebalancing activity, resulting in the movement of data extents in the disk groups?

- ASMB
- ARBn
- RBAL in the ASM instance
- RBAL in the database instance

Answer:

ARBn

Explanation:

The ARBn background process performs the actual rebalancing activity resulting in the movement of data extents in the disk groups in an ASM instance. The variable n can have a value from 0 to 9.

The ASMB background process communicates with the ASM instance. It does not perform the actual rebalancing activity to move data extents between disks in the disk groups.

The RBAL background process in the ASM instance coordinates the rebalancing activity for disk groups.

The RBAL background process in the database instance performs global opens of the disks in the disk groups on behalf of the database instance.

Item: 5 (Ref:1Z0-043.11.5.4)

You are performing backup and recovery operations by using RMAN. You are using a recovery catalog for the RMAN repository.

You are planning to migrate to ASM disk storage to enable new disks to be added to the database without shutting down the database.

Which information is **NOT** required during the migration process?

- Database Identifier (DBID)
- names and location of datafiles
- names and location of control files
- names and location of online redo log files

Answer:

Database Identifier (DBID)

Explanation:

If you are using a recovery catalog, the Database Identifier (DBID) is not required when migrating from non-ASM disk storage to ASM disk storage. The DBID is only needed when you are not using a recovery catalog, that is, when you are using a control file for the RMAN repository.

All the other options are incorrect because you will need the names and locations of datafiles, control files, and online redo log files in the migration process. This information is helpful if you need to move back to non-ASM disk storage.

Item: 6 (Ref:1Z0-043.11.1.2)

You included the following Automatic Storage Management (ASM) initialization parameter settings in the ASM initialization parameter file:

```
INSTANCE_TYPE = ASM
ASM_POWER_LIMIT = 11
LARGE_POOL_SIZE = 4M
ASM_DISKGROUPS = DG1, DG2
DB_UNIQUE_NAME = +ASM
```

You are unable to start the ASM instance. Which initialization parameter file setting(s) is not allowing the ASM instance to start?

- only the INSTANCE_TYPE initialization parameter is set to an invalid value
- only the ASM_POWER_LIMIT initialization parameter is set to an invalid value
- only the LARGE_POOL_SIZE initialization parameter is set to an invalid value
- both the LARGE_POOL_SIZE and INSTANCE_TYPE initialization parameters are set to invalid values

Answer:

both the LARGE_POOL_SIZE and INSTANCE_TYPE initialization parameters are set to invalid values

---

Explanation:

Both the LARGE_POOL_SIZE and INSTANCE_TYPE initialization parameters are set to invalid values.

The LARGE_POOL_SIZE initialization parameter can be used for both database instances and ASM instances. When the large pool memory component is used for an ASM instance, all ASM packages are executed from this pool. The large pool must be set to at least 8M.

The INSTANCE_TYPE initialization parameter specifies whether the instance is an ASM instance or a database instance. The value for this parameter must be set to ASM in the ASM instance initialization parameter file. The other valid value for the INSTANCE_TYPE initialization parameter is RDBMS which indicates that the instance is a database instance.

The option stating that the ASM instance fails to start because only the INSTANCE_TYPE initialization parameter is set to an invalid value is incorrect. Your ASM instance initialization parameter file contains another invalid parameter setting, that is, LARGE_POOL_SIZE = 4M.

The option stating that the ASM instance fails to start because the ASM_POWER_LIMIT initialization parameter is set to an invalid value is incorrect. ASM_POWER_LIMIT = 11 is a valid parameter setting. The ASM_POWER_LIMIT initialization parameter controls the speed of a rebalance operation. Its value ranges from 1 to 11. The higher the value, the faster the rebalancing will be complete.

The option stating that the ASM instance fails to start because only the LARGE_POOL_SIZE initialization parameter is set to an invalid value is incorrect. Your ASM instance initialization parameter file contains another invalid parameter setting, INSTANCE_TYPE = RDBMS.

Item: 7 (Ref:1Z0-043.11.2.2)

During tablespace creation, which filename format is **NOT** used for creating datafiles associated with a tablespace?

- incomplete names
- incomplete names with templates
- alias with template names
- numeric names

Answer:

numeric names

Explanation:

Numeric names are used only when referencing an existing ASM file. Therefore, numeric names cannot be used for creating datafiles associated with a tablespace during tablespace creation. The numeric name format allows you to refer to the existing ASM file by only the disk group name and the file number/incarnation pair. The syntax of the numeric names format is as follows:

```
+<group>.<file#>.<incarnation#>
```

For example:

```
+grp1.256.324
```

The option stating that incomplete names cannot be used to create a tablespace is incorrect. You can use an incomplete filename format either while creating a single filename or during multiple file-creation operations. To create a tablespace, you should specify only the disk group name and use a default template depending on the type of the file. The syntax of the incomplete names is as follows:

```
+<group>
```

For example:

```
+grp1
```

The option stating that incomplete names with templates cannot be used to create a tablespace is incorrect. You can use an incomplete filename with a template while creating a single filename or during multiple file-creation operations. Regardless of the actual file type, the template name determines the characteristics of the file. The syntax of the incomplete names with templates is as follows:

```
+dgroup1(datafile)
```

For example:

```
+grp1(datafile)
```

The option stating that alias with template names cannot be used to create a tablespace is incorrect. You can use an alias with a template only while creating a new ASM file. Templates provide a convenient method for specifying a file type and a tag while creating a new ASM file. The syntax of alias with template names is as follows:

```
+dgroup(template_name)/alias
```

For example:

```
+grp1/abc (datafile)
```

Item: 8 (Ref:1Z0-043.11.4.2)

You have configured the ASM instance for the PROD database of iPod Corporation. You have specified the following parameter values in the initialization parameter file:

```
DB_CREATE_FILE_DEST='devices/grp1/P'
DB_CREATE_ONLINE_LOG_DEST_1='devices/d_grp2/Q'
DB_CREATE_ONLINE_LOG_DEST_2='devices/d_grp3/R'
BACKGROUND_DUMP_DEST='devices/d_grp1/S'
```

You have added a new redo log group that contains two redo log members. Where are the redo log members stored?

- Both the members will be stored in the 'devices/grp1/P' directory.
- Both the members will be stored in the 'devices/d_grp2/Q' directory.
- Both the members will be stored in the 'devices/d_grp3/R' directory.
- One member will be stored in the 'devices/d_grp2/Q' directory and the other in the 'devices/d_grp3/R' directory.

Answer:

One member will be stored in the 'devices/d_grp2/Q' directory and the other in the 'devices/d_grp3/R' directory.

Explanation:

You have configured Oracle Managed Files (OMF) in your database. If the names and locations of the datafiles are not specified at tablespace creation, then the datafiles are stored in the location specified by the value of the DB_CREATE_FILE_DEST parameter. If the names and locations of the online redo log files are not specified in the ALTER DATABASE ADD LOGFILE command, then the online redo log files will be stored in the location specified by the DB_CREATE_ONLINE_LOG_DEST_n parameter. You have specified the value, devices/d_grp2/Q, for the DB_CREATE_ONLINE_LOG_DEST_1 parameter and the value, devices/d_grp3/R, for the DB_CREATE_ONLINE_LOG_DEST_2 parameter. If you add a redo log group that contains two redo log members, then one redo log member is stored in the 'devices/d_grp2/Q' directory and the other in the 'devices/d_grp3/R' directory.

The option stating that both the online redo log members will be stored in the devices/grp1/P directory is incorrect because the members of the redo log group are stored in the devices/d_grp2/Q and devices/d_grp3/R directories. The datafiles are stored in the devices/grp1/P directory for those tablespaces for which the datafiles names and locations are not specified at the time of tablespace creation.

The option stating that both the online redo log members will be stored in the devices/grp2/Q directory, and the option stating that both the online redo log members will be stored in the devices/grp3/R directory are incorrect. This is because the members of the redo log group are stored in the devices/d_grp2/Q and devices/d_grp3/R directories.

Item: 9 (Ref:1Z0-043.11.5.1)

You are migrating your production database from non-ASM to ASM storage. You used the RMAN utility to migrate the database from non-ASM to ASM storage.

Which type of backup command script will you use for migrating the database from non-ASM to ASM storage?

- BACKUP AS BACKUPSET
- BACKUP AS COPY
- BACKUP AS COMPRESSED BACKUPSET
- BACKUP INCREMENTAL LEVEL n CUMULATIVE

Answer:

BACKUP AS COPY

Explanation:

The BACKUP AS COPY command is written in the script that is used for migrating the database from non-ASM to Automatic Storage Management (ASM) storage. The RMAN is the only method for copying the ASM files because the normal operating system interfaces cannot access ASM files. The steps for migrating the database from non-ASM to ASM are as follows:

1. Note the filenames of the control files and the online redo log files.
2. Shutdown the database using the NORMAL, IMMEDIATE, or TRANSACTIONAL keywords.
3. Backup the database.
4. Edit the SPFILE to use the OMF for all file destinations.
5. Edit the SPFILE to remove the CONTOL_FILES parameter.
6. Run the following RMAN script:

```
STARTUP NOMOUNT;
RESTORE CONTROLFILE FROM '<controlfile_locations>';
ALTER DATABASE MOUNT;
BACKUP AS COPY DATABASE FORMAT '+<disk group destination>';
SWITCH DATABASE TO COPY;
SQL ALTER DATABASE RENAME <logfile> TO '+<disk group
destination>';
ALTER DATABASE OPEN RESETLOGS;
```

7. Delete or archive the old database files.

The option stating that the RMAN script used for migrating the database from non-ASM to ASM storage contains the command BACKUP AS BACKUPSET is incorrect. The script contains BACKUP AS COPY command. The BACKUP AS BACKUPSET command creates RMAN backup sets, which contain the backup pieces.

The option stating that the RMAN script used for migrating the database from non-ASM to ASM storage contains the command BACKUP AS COMPRESSED BACKUPSET is incorrect. The BACKUP AS COMPRESSED BACKUPSET command creates RMAN backup sets in a compressed format.

The option stating that the RMAN script used for migrating the database from non-ASM to ASM storage contains the command BACKUP INCREMENTAL LEVEL n CUMULATIVE is incorrect. The cumulative incremental level backup is different from the differential incremental backup in that it requires more space. The benefit of the cumulative incremental backup is that the cumulative incremental backups are faster and easier to restore because only one backup for a given level is needed to restore.

Item: 10 (Ref:1Z0-043.11.3.2)

You execute the following command to start an Automatic Storage Management (ASM) instance:

```
SQL>STARTUP;
```

In which of the following modes will the ASM instance start?

- OPEN
- MOUNT
- NORMAL
- NOMOUNT

Answer:

MOUNT

Explanation:

When you issue the STARTUP command to an ASM instance, the ASM instance will be started in the MOUNT mode. The default mode for the STARTUP command issued to an ASM instance is MOUNT. Therefore, as a result of the given STARTUP command, the ASM instance will mount the disk groups.

The option stating that the ASM instance will be started in the OPEN mode is incorrect because the default startup mode is MOUNT. Moreover, issuing the STARTUP OPEN command to an ASM instance will generate an error because OPEN is an invalid mode for an ASM instance. The STARTUP OPEN command is used to start a database instance, but is not used for an ASM instance.

The option stating that the ASM instance will be started in the NORMAL mode is incorrect because the ASM instance will be started in the MOUNT mode. Unlike a database instance, which always starts in the OPEN mode, the ASM instance starts in the MOUNT mode if no mode is specified in the STARTUP command.

The option stating that the ASM instance will be started in the NOMOUNT mode is incorrect. This is because to start the ASM instance in the NOMOUNT mode, you must execute the STARTUP NOMOUNT command. The ASM instance starts, but does not mount any disk groups when started using the STARTUP NOMOUNT command.

Item: 11 (Ref:1Z0-043.11.5.3)

Your database is configured on non-ASM disk storage. You need to migrate your database to ASM disk storage.

Which statement is true about migrating from non-ASM disk storage to ASM disk storage?

- You can use the operating system utility to migrate from non-ASM disk storage to ASM disk storage.
- You cannot perform a database backup from non-ASM disk storage to tape and then move it to ASM disk storage.
- You can use the `SWITCH DATABASE TO COPY` Recovery Manager (RMAN) command to switch back to non-ASM disk storage if you have not deleted your original datafiles.
- You cannot use Recovery Manager (RMAN) to migrate from non-ASM disk storage to ASM disk storage if you are not using RMAN for your backup and recovery strategies.

Answer:

You can use the `SWITCH DATABASE TO COPY` Recovery Manager (RMAN) command to switch back to non-ASM disk storage if you have not deleted your original datafiles.

Explanation:

You can use the `SWITCH DATABASE TO COPY` RMAN command to switch back to non-ASM disk storage if you have not deleted your original datafiles. If you have not deleted your original datafiles after migrating from non-ASM disk storage to ASM disk storage, you can use the `SWITCH DATABASE TO COPY` RMAN command to switch back to non-ASM disk storage without going through the whole migration process.

The option stating that you can use the operating system utility to migrate from non-ASM disk storage to ASM disk storage is incorrect because you cannot use the operating system utility to move files from non-ASM disk storage to ASM disk storage. ASM files cannot be accessed by using the operating system commands. You must use RMAN to move database files from non-ASM disk location to an ASM disk group.

The option stating that you cannot perform a database backup from non-ASM disk storage to tape and then move it ASM disk storage is incorrect. Using RMAN, you can back up the database to tape and then move the database to ASM disk storage. This process is useful when your database is so large that it is not possible to have copies of the database on non-ASM disk storage and ASM disk storage simultaneously.

The option stating that you cannot use the RMAN to migrate from non-ASM disk storage to ASM disk storage if you are not using RMAN for your backup and recovery strategies is incorrect. Even if you are not using RMAN for backup and recovery strategies, you can still use RMAN to migrate from non-ASM disk storage to ASM disk storage.

Item: 12 (Ref:1Z0-043.11.1.1)

You have a single Automatic Storage Management (ASM) instance running on the node on which your Oracle Database 10*g* resides.

Which ASM instance initialization parameters must be included in the ASM instance initialization parameter file?

- INSTANCE_TYPE
- DB_UNIQUE_NAME
- ASM_DISKSTRING
- ASM_POWER_LIMIT

Answer:

INSTANCE_TYPE

Explanation:

The INSTANCE_TYPE initialization parameter is the only parameter that must be included in the ASM initialization parameter file. The INSTANCE_TYPE initialization parameter specifies whether the instance is an ASM instance or a database instance. The value for this parameter must be set to ASM in the ASM instance initialization parameter file.

All the other options are incorrect because these parameters contain default values that are suitable for most environments.

The DB_UNIQUE_NAME initialization parameter specifies a unique name for a group of ASM instances on a single node. It defaults to +ASM value. This default value needs to be modified only when multiple ASM instances are running on a single node.

The ASM_DISKSTRING initialization parameter specifies one or more strings to limit the disks that can be used to create disk groups. Its default value is NULL, which implies that the ASM discovery feature locates all disks in an operating system path that the ASM instance can access.

The ASM_POWER_LIMIT initialization parameter controls the speed of a rebalance operation. If this parameter is not included in the ASM initialization parameter file, its value defaults to 1. The higher the limit, the faster the rebalancing will be completed.

Item: 13 (Ref:1Z0-043.11.3.4)

Which of the following options is true about shutting down an Automatic Storage Management (ASM) instance?

- If the SHUTDOWN IMMEDIATE command is issued to the ASM instance, the ASM instance immediately shuts down.
- If the SHUTDOWN ABORT command is issued to the ASM instance, the ASM instance will shut down all the database instances and then shut down immediately.
- If the SHUTDOWN NORMAL command is issued to the ASM instance, before shutting down, the ASM instance waits for the dependent database instances to shut down.
- If the SHUTDOWN TRANSACTIONAL command is issued to the ASM instance, the ASM instance passes the same SHUTDOWN command to the dependent database instances, but does not wait for any active transactions to complete before it shuts down.

Answer:

If the SHUTDOWN NORMAL command is issued to the ASM instance, before shutting down, the ASM instance waits for the dependent database instances to shut down.

Explanation:

When the SHUTDOWN command is issued to an ASM instance including the NORMAL, IMMEDIATE or TRANSATIONAL modes, the ASM instance waits for the dependent database instances to shut down before it shuts down.

The option stating that the ASM instance immediately shuts down if the SHUTDOWN IMMEDIATE command is issued to the ASM instance is incorrect because using this command, the ASM instance waits for any active transactions to complete and then shuts down. However, it does not wait for the sessions to exit. The SHUTDOWN IMMEDIATE command, when issued to an ASM instance, works exactly the same way as the SHUTDOWN TRANSACTIONAL command.

The option stating that the ASM instance will shut down all the database instances and then shut down immediately when the SHUTDOWN ABORT is issued is incorrect. The ASM will immediately abort operation when this command is issued and will not shut down any database instances. All the open connections and dependent databases will be terminated immediately.

The option stating that if the SHUTDOWN TRANSACTIONAL command is issued to the ASM instance the ASM instance passes the same SHUTDOWN command to the dependent database instances, but does not wait for any active transactions to complete before it shuts down is incorrect. When the SHUTDOWN TRANSACTIONAL command is issued to an ASM instance, the ASM instance waits for any active transactions to complete and then shuts down.

Item: 14 (Ref:1Z0-043.11.5.2)

You are migrating your database to Automatic Storage Management (ASM). In which order will you follow these steps?

1. Delete or archive the old database files.
2. Shutdown the database using the NORMAL, IMMEDIATE, or TRANSACTIONAL keywords.
3. Backup the database.
4. Edit the SPFILE to remove the CONTOL_FILES parameter.
5. Run the following RMAN script:

```
STARTUP NOMOUNT;
RESTORE CONTROLFILE FROM '<controlfile_locations>';
ALTER DATABASE MOUNT;
BACKUP AS COPY DATABASE FORMAT '+<disk group destination>';
SWITCH DATABASE TO COPY;
SQL ALTER DATABASE RENAME <logfile> TO '+<disk group
destination>';
ALTER DATABASE OPEN RESETLOGS;
```

6. Note the filenames of the control files and the online redo log files.
7. Edit the SPFILE to use the OMF for all file destinations.

- 2,5,3,7,4,6,1
- 2,3,5,4,1,6,7
- 6,2,3,7,4,5,1
- 1,3,7,5,6,4,2

Answer:

2,3,5,4,1,6,7

Explanation:

You will follow the steps for migrating the database from non-ASM to ASM in following order:

6,2,3,7,4,5,1

The ASM files cannot be access via the operating system. You must use the Recovery manager (RMAN) to move the database objects from a non-ASM disk location to an ASM disk group. To migrate the database from non-ASM to ASM, follow these steps:-

1. Note the filenames of the control files and the online redo log files.
2. Shutdown the database using the NORMAL, IMMEDIATE, or TRANSACTIONAL keywords.
3. Backup the database.
4. Edit the SPFILE to use the OMF for all file destinations.
5. Edit the SPFILE to remove the CONTOL_FILES parameter.
6. Run the following RMAN script:

```
STARTUP NOMOUNT;
RESTORE CONTROLFILE FROM '<controlfile_locations>';
ALTER DATABASE MOUNT;
BACKUP AS COPY DATABASE FORMAT '+<disk group destination>';
SWITCH DATABASE TO COPY;
SQL ALTER DATABASE RENAME <logfile> TO '+<disk group
destination>';
ALTER DATABASE OPEN RESETLOGS;
```

1. Delete or archive the old database files.

All other options are incorrect because step sequence is incorrect.

Item: 15 (Ref:1Z0-043.11.3.3)

Which statement must you issue to an already-running Automatic Storage Management (ASM) instance to prevent database instances from connecting to the ASM instance?

- `ALTER SYSTEM KILL SESSION`
- `ALTER SYSTEM DISCONNECT SESSION`
- `ALTER SYSTEM QUIESCE RESTRICTED`
- `ALTER SYSTEM ENABLE RESTRICTED SESSION`

Answer:

`ALTER SYSTEM ENABLE RESTRICTED SESSION`

Explanation:

You must issue the `ALTER SYSTEM ENABLE RESTRICTED SESSION` statement to an already-running ASM instance to prevent database instances from connecting to the ASM instance. This statement will enable restricted session on the ASM instance and when an ASM instance is open in the restricted mode, it prevents database instances to connect to the ASM instance.

The option stating that you must use the `ALTER SYSTEM KILL SESSION` statement to prevent the database instances from connecting to the ASM instance is incorrect because this statement will not prevent the database instances from connecting to the ASM instance. This statement is generally used to terminate a user session that is holding system resources. The user receives an error message indicating that the session has been terminated. This statement is also issued to the database instance.

The option stating that you must use the `ALTER SYSTEM DISCONNECT SESSION` statement to prevent the database instances from connecting to the ASM instance is incorrect. This statement is used to disconnect the current session by destroying the dedicated server process or the virtual circuit, depending on whether the database is using dedicated server process or shared server process for connections. Moreover, this statement is issued to the database instance and not to the ASM instance.

The `ALTER SYSTEM QUIESCE RESTRICTED` statement is not used to prevent the database instances from connecting to the ASM instance. This statement, when issued to a database instance, prevents all inactive sessions, except the sessions created by SYS and `SYSTEM`, from becoming active. This statement ensures that no user other than SYS and `SYSTEM` can start a transaction or issue a query.

Using Globalization Support Objectives

Item: 1 (Ref:1Z0-043.1.3.2)

You created the ORDERS table in your database by using the following code:

```
SQL> CREATE TABLE ORDERS (ORDER_DATE TIMESTAMP(0) WITH TIME
ZONE);
```

Then, you inserted data in the ORDERS table and saved it by issuing the following statements:

```
SQL> INSERT INTO ORDERS VALUES('18-AUG-00 10:26:44 PM
America/New_York');
SQL> INSERT INTO ORDERS VALUES('23-AUG-02 12:46:34 PM
America/New_York');
SQL> COMMIT;
```

Next, you issued the following statement to change the time zone for the database:

```
SQL> ALTER DATABASE SET TIME_ZONE='Europe/London';
```

What will be the result of executing the above statement?

- The statement will fail.
- The statement will be executed successfully, and the new time zone will be set for the database.
- The statement will be executed successfully, but the new time zone will be set for the current session.
- The statement will be executed successfully, but the new time zone will neither be set for the database nor for a specific session.

Answer:

The statement will fail.

Explanation:

The `ALTER DATABASE SET TIME_ZONE ='Europe/London'` statement will fail because the `ALTER DATABASE SET TIME_ZONE` statement is used only when the database contains no table with `TIMESTAMP TO LOCAL TIME ZONE` column. If the database contains a table with a `TIMESTAMP TO LOCAL TIME ZONE` column and the column contains the data, then the `ALTER DATABASE SET TIME_ZONE=<value>` will return an error. In this scenario, the ORDERS table contains the ORDER_DATE column with the `TIMESTAMP TO LOCAL TIME ZONE` data type. The ORDERS table contains the data. Therefore, the `ALTER DATABASE SET TIME_ZONE='Europe/London';` statement will return an error.

The option stating that the statement will be executed successfully and a new time zone will be set for the database is incorrect because the `ALTER DATABASE SET TIME_ZONE ='Europe/London';` will not be executed successfully.

The option stating that the statement will be executed successfully but a new time zone will be set for the current session is incorrect. The statement `ALTER DATABASE SET TIME_ZONE ='Europe/London';` will not be executed successfully. The `ALTER SESSION SET TIME_ZONE` statement is used to set the time zone for a session.

The option stating that the statement will be executed successfully, but a new time zone will neither be set for the database nor for a specific session is incorrect. This is because the statement `ALTER DATABASE SET TIME_ZONE ='Europe/London';` will not be executed successfully.

Item: 2 (Ref:1Z0-043.1.2.1)

You are specifying French case-insensitive sorts by using the NSL_SORT parameter for the user session of the user, Scott. Which value will you set for the NLS_SORT parameter?

- FRENCH_AI
- FRENCH_CI
- AI_FRENCH
- CI_FRENCH

Answer:

FRENCH_CI

Explanation:

To enable the case-insensitive sort, you should suffix _CI to the value of the NLS_SORT initialization parameter for the user session of the user, Scott. The NLS_SORT initialization parameter used to specify the linguistic sort name takes the value of the NLS_LANGUAGE initialization parameter. The sorting behavior of the sort is binary. When you use the ORDER BY clause with the query, then the values are sorted based on the numeric values of the characters. The overhead is increased by enabling the linguistic sort because the linguistic sort takes more time to be performed than the binary sort. In this scenario, the name of the sort should be specified as FRENCH_CI.

You cannot specify the name of the sort as FRENCH_AI because the _AI suffix is not used to enable the case-insensitive sort. The _AI suffix is used to enable the accent-insensitive sort feature.

The options, AI_FRENCH and CI_FRENCH, are incorrect because AI and CI are specified as suffixes and not prefixes to the value of the NLS_SORT parameter.

Item: 3 (Ref:1Z0-043.1.3.4)

You are maintaining your Oracle10*g* database in the UNIX environment. An application requires one of the user sessions to exist in the operating system local time zone. You decide to set the time zone for a session using the operating system environment variable.
Which command will you issue?

- `setenv ORA_SDTZ 'DB_TZ'`
- `setenv ORA_SDTZ '+10:00'`
- `setenv ORA_SDTZ 'OS-TZ'`
- `setenv ORA_SDTZ 'Europe/London'`

Answer:

`setenv ORA_SDTZ 'OS-TZ'`

Explanation:

You will issue the `setenv ORA_SDTZ 'OS-TZ'` command to set the operating system local time zone for a user session. `ORA-SDTZ` is an operating system environment variable that may be used to set the default time zone for a session. It may be set to the following time zones:

Absolute offset or time zone region
`OS_TZ`: The operating system local time zone
`DB_TZ`: The database local time zone

The option stating that you will issue the `setenv ORA_SDTZ 'DB_TZ'` command for setting the operating system local time zone for a user session is incorrect. The `DB_TZ` value of the `ORA_SDTZ` environment variable is used to set the database local time zone for a user session.

The option stating that you will issue the `setenv ORA_SDTZ '+10:00'` command for setting the operating system local time zone for a user session is incorrect. The `ORA_SDTZ` is an operating system environment variable that may be used to set the default time zone for a session. The valid range of offsets is -12:00 to +14:00.

The option stating that you will issue the `setenv ORA_SDTZ 'Europe/London'` command for setting the operating system local time zone for a user session is incorrect. The `'Europe/London'` value for the `ORA_SDTZ` environment variable sets the time zone region name as `'Europe/London'`.

Item: 4 (Ref:1Z0-043.1.3.3)

You issued the following command at the UNIX environment:

```
% setenv ORA_SDTZ 'OZ_TZ'
```

What will be the impact of issuing the above command?

- The operating system local time zone will be set for a user session using the operating system environment variable.
- The database local time zone will be set for a user session using the operating system environment variable.
- The operating system local time zone will be set for the database using the operating system environment variable.
- The database local time zone will be set for the database using the operating system environment variable.

Answer:

The operating system local time zone will be set for a user session using the operating system environment variable.

Explanation:

When you issue the `% setenv ORA_SDTZ 'OZ_TZ'` command at the UNIX prompt, the operating system local time zone will be set for a user session using the operating system environment variable. `ORA_SDTZ` is an operating system environment variable that may be used to set the default time zone for a session. It may be set to the following time zones:

Absolute offset or time zone region
`OS_TZ`: the operating system local time zone
`DB_TZ`: the database local time zone

The option stating that the database local time zone will be set for a user session using operating system environment variable is incorrect. The `OS_TZ` value of the `ORA_SDTZ` system environment is used to set the operating system local time zone for a user session. The `DB_TZ` value of the `ORA_SDTZ` environment variable is used to set the database local time zone for a user session.

The option stating that the operating system local time zone will be set for the database using the operating system environment variable is incorrect. The `ORA_SDTZ` system environment variable is used to set the time zone for a session and not for the database. The time zone for the database is set by issuing the `ALTER DATABASE SET TIMEZONE` statement.

The option stating that the database local time zone will be set for the database using the operating system environment variable is incorrect. The `ORA_SDTZ` system environment variable is used to set the time zone for a session not for the database. The time zone for the database is set by issuing the `ALTER DATABASE SET TIMEZONE` statement.

Item: 5 (Ref:1Z0-043.1.4.1)

Click the Exhibit(s) button to view the EMPLOYEES table.

The EMPLOYEE table contains thousands of rows. The EMP_CODE column is the primary key column. At the end of every month, you are required to perform search queries based on the BASIC_SAL+COMM column values.

Which type of index will you create?

- B-tree Index
- Bitmap Index
- Function-based Index
- Partitioned Index

Answer:

Function-based Index

EMP_CODE(PK)	FIRST_NAME	BASIC_SAL	COMM
E001	William	$2500	$500
E002	David	$3000	$650
E003	James	$3500	$950
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.

Explanation:

You will create a function-based index to perform search queries according to the BASIC_SAL+COMM column values of the EMPLOYEE table. The function-based indexes enable you to perform queries on the composite columns to generate a derived result. You will create the function-based index by using the following statement that will enable faster case-insensitive searches in the EMPLOYEE table:

```
CREATE INDEX EMP_IDX ON EMPLOYEE(BASIC_SAL+COMM);
```

The option stating that you will create a B-tree index is incorrect. To perform search queries on the result of an expression, you create a function-based index. If an index is not created on a table, then a full table scan will be performed to search for a value by using the B-tree index that can retrieve data quickly.

The option stating that you will create a bitmap index is incorrect. To perform search queries based on a column that contains few distinct values, you can create a bitmap index on the column. A bitmap index stores rowids associated with a key value as a bitmap. In this scenario, you are required to create an index based on the expression, BASIC_SAL+COMM. Expression-based indexes are always function-based indexes.

The option stating that you will create a partitioned index is incorrect. A partitioned index consists of partitions containing an entry for each value that appears in the index column of the table. You typically create a partitioned index on a partitioned table. You can also create a partitioned index on a table that is not partitioned. If the index on the partitioned table is not partitioned, then the index is called a global index. If the index is partitioned in exactly the same manner as its parent table, then the index is called a local prefixed index. In this scenario, you are required to create an index based on the expression, BASIC_SAL+COMM. Expression based indexes are always function-based indexes.

Item: 6 (Ref:1Z0-043.1.5.1)

You are maintaining your database in Oracle10*g*. You find that the number of languages that should be supported in your database has increased. The character set of your database is UTF8. You decide to migrate your database to the AL16UTF16 national character set.

How will you migrate your database from UTF8 to AL16UTF16?

- by using the RMAN utility
- by using the export/import utility
- by using the ALTER DATABASE command
- by enabling the change tracking feature

Answer:

by using the ALTER DATABASE command

Explanation:

You will migrate your database from the UTF8 character set to the AL16UTF16 character set by using the ALTER DATABASE command. The ALTER DATABASE CHARACTER SET command is used to migrate the database to a new character set only if the new character set is a strict superset of the current character set. In every other situation, you are required to perform a complete export/import operation to properly convert all the data to a new character set.

You cannot migrate your database from the UTF8 character set to the AL16UTF16 character set by using the RMAN utility. The RMAN utility is used to perform backup and recovery of a database.

You cannot migrate the database from the UTF8 character set to the AL16UTF16 character set by using the export/import utility. If the new character set is not the superset of the current character set, then you must use the export/import utility to migrate the database from one character set to another.

You cannot migrate the database from the UTF8 character set to the AL16UTF16 character set by enabling the change tracking feature. The change tracking feature is enabled to improve the performance of the incremental backup. If the change tracking feature is enabled, those blocks that are updated since the last backup are backed up while performing the incremental backup.

Item: 7 (Ref:1Z0-043.1.3.1)

Your Oracle10*g* database contains a table with a TIMESTAMP TO LOCAL TIME ZONE column. There are about two hundred column values for the column. You issued the following statement:

```
SQL> ALTER DATABASE SET TIME_ZONE ='Europe/London';
```

What will be the result of issuing the above statement?

- The statement will be executed successfully, and a new time zone will be set for the database.
- The statement will be executed successfully, but a new time zone will not be set for the database.
- The statement will not be executed successfully because the SET TIME_ZONE clause can be used only with the ALTER SESSION statement.
- The statement will not be executed successfully because the ALTER DATABASE SET TIME_ZONE statement is used only when the database contains no table with the TIMESTAMP TO LOCAL TIME ZONE column.

Answer:

The statement will not be executed successfully because the ALTER DATABASE SET TIME_ZONE statement is used only when the database contains no table with the TIMESTAMP TO LOCAL TIME ZONE column.

Explanation:

The ALTER DATABASE SET TIME_ZONE ='Europe/London' statement will fail because the ALTER DATABASE SET TIME_ZONE statement is used only when the database contains no table with the TIMESTAMP TO LOCAL TIME ZONE column. If the database contains a table with a TIMESTAMP TO LOCAL TIME ZONE column and the column contains the data, then the ALTER DATABASE SET TIME_ZONE=<value> will return an error.

The option stating that the statement will be executed successfully and a new time zone will be set for the database is incorrect. This is because the ALTER DATABASE SET TIME_ZONE ='Europe/London' statement will not be executed successfully.

The option stating that the statement will be executed successfully but a new time zone will not be set for the database is incorrect. This is because the ALTER DATABASE SET TIME_ZONE ='Europe/London' statement will not be executed successfully.

The option stating that the statement will not be executed successfully because the SET TIME_ZONE clause can be used only with ALTER SESSION statement is incorrect. The ALTER SESSION SET TIME_ZONE statement is used to set the time zone at the session level, and the ALTER DATABASE SET TIME_ZONE statement is used to set the time zone at the database level. The ALTER SESSION SET TIME_ZONE statement is used to set the time zone for a session.

Item: 8 (Ref:1Z0-043.1.1.1)

You issued the following statement:

```
SQL> ALTER SESSION SET NLS_LANG=FRENCH_CANADA.WE8ISO8859P1;
```

Which parameter is **NOT** overridden by using the above statement?

- the value of the NLS_LANGUAGE variable
- the value of the NLS_TERRITORY variable
- the value of the NLS_CURRENCY variable
- the character encoding scheme used by the client application

Answer:

the value of the NLS_CURRENCY variable

Explanation:

The value of the NLS_CURRENCY variable is not overridden by using the ALTER SESSION SET NLS_LANG=FRENCH_CANADA.WE8ISO8859P1 statement. L number format mask is specified by the NLS_CURRENCY parameter. The L number format mask is the local currency symbol.

The NLS_LANG environment variable specifies the local behavior for the Oracle software. The setting of the NLS_LANG variable also sets the character set for the data entered or displayed at the client end.

The NLS_LANG=<language>_<territory>.<charset>
<Language> syntax is used to override the value of the NLS_LANGUAGE variable. The <territory> variable is used to override the value of the NLS_TERRITORY variable. The <charset> variable is used to override the character encoding scheme used by the client application. In this scenario, the value of the NLS_LANGUAGE variable will be overridden by FRENCH. The value of the NLS_TERRITORY variable is overridden by CANADA, and the character encoding scheme is overridden by WE8ISO8859P1.

Managing Resources

Item: 1 (Ref:1Z0-043.15.3.4)

Click the Exhibit(s) button to view the MY_PLAN resource plan.

Which code will you execute to create the simple resource plan, MY_PLAN?

- BEGIN
  DBMS_RESOURCE_MANAGER.CREATE_SIMPLE_PLAN(SIMPLE_PLAN => 'MY_PLAN',
  CONSUMER_GROUP1 =>'SYS_GROUP', GROUP1 => 100%,
  CONSUMER_GROUP2 => 'GRP1', GROUP2_CPU => 75,
  CONSUMER_GROUP3 => 'GRP2', GROUP3_CPU => 15,
  CONSUMER_GROUP4 => 'OTHER_GROUPS', GROUP4_CPU => 100%);
  END;
- BEGIN
  DBMS_RESOURCE_MANAGER.CREATE_SIMPLE_PLAN(SIMPLE_PLAN => 'MY_PLAN',
  CONSUMER_GROUP1 => 'GRP1', GROUP1_CPU => 75,
  CONSUMER_GROUP2 => 'GRP2', GROUP2_CPU => 15,
  CONSUMER_GROUP3 => 'OTHER_GROUPS', GROUP3_CPU => 100%);
  END;
- BEGIN
  DBMS_RESOURCE_MANAGER.CREATE_SIMPLE_PLAN(SIMPLE_PLAN => 'MY_PLAN',
  CONSUMER_GROUP1 => 'GRP1', GROUP1_CPU => 75,
  CONSUMER_GROUP2 => 'GRP2', GROUP2_CPU => 15);
  END;
- BEGIN
  DBMS_RESOURCE_MANAGER.CREATE_SIMPLE_PLAN(SIMPLE_PLAN => 'MY_PLAN',
  CONSUMER_GROUP1 =>'SYS_GROUP', GROUP1 => 100%,
  CONSUMER_GROUP2 => 'GRP1', GROUP2_CPU => 75,
  CONSUMER_GROUP3 => 'GRP2', GROUP3_CPU => 15);
  END;

Answer:

```
BEGIN
DBMS_RESOURCE_MANAGER.CREATE_SIMPLE_PLAN(SIMPLE_PLAN => 'MY_PLAN',
CONSUMER_GROUP1 => 'GRP1', GROUP1_CPU => 75,
CONSUMER_GROUP2 => 'GRP2', GROUP2_CPU => 15);
END;
```

Consumer group	Level 1	Level 2	Level 3
SYS_GROUP	100%		
GRP1		75%	
GRP2		25%	
OTHER_GROUPS			100%

Explanation:

The following code will create the MY_PLAN resource plan:

```
BEGIN
DBMS_RESOURCE_MANAGER.CREATE_SIMPLE_PLAN(SIMPLE_PLAN =>
'MY_PLAN',
CONSUMER_GROUP1 => 'GRP1', GROUP1_CPU => 75,
CONSUMER_GROUP2 => 'GRP2', GROUP2_CPU => 15);
END;
```

While creating a simple plan, Oracle automatically adds two additional consumer groups, SYS_GROUP and OTHER_GROUPS. The SYS_GROUP consumer group represents the SYS and SYSTEM users. The OTHER_GROUPS group must be included in any resource plan. The OTHER_GROUPS group ensures that users who are not assigned to any group in the active resource plan will continue to have resources allocated.

The other options are incorrect because you do not specify the SYS_GROUPS and OTHER_GROUPS groups while creating a simple plan.

Item: 2 (Ref:1Z0-043.15.3.3)

Click the Exhibit(s) button to view the DEPARTMENTS plan.

After analyzing the Exhibit, what conclusion will you draw?

- The CPU cannot be assigned to the members of the SYS_GROUP group.
- The members of the OTHER_GROUPS group will always be assigned 100 percent CPU.
- The members of the OTHER_GROUPS group will never be assigned 100 percent CPU.
- The members of the OTHER_GROUPS group will be assigned 100 percent CPU if the CPU is not assigned to the members of the SYS_GROUP group and the PAYROLL, SALES, and MARKETING groups.

Answer:

The members of the OTHER_GROUPS group will be assigned 100 percent CPU if the CPU is not assigned to the members of the SYS_GROUP group and the PAYROLL, SALES, and MARKETING groups.

Level	SYS_GROUP	PAYROLL	SALES	MARKETING	OTHER_GROUPS
1	100%				
2		50%	25%	25%	
3					100%

Explanation:

The DEPARTMENTS plan is a multi-level plan. The elements that you defined are assigned to the second level. This ensures that members of the SYS_GROUP at level 1 will have no CPU restriction. The groups at level 2 will share CPU resources not used by the group at level 1. The users not assigned to any group in the plan at level 3 will receive CPU time only after level 1 and 2 have satisfied their requirements.

The option stating that CPU cannot be assigned to the members of the SYS_GROUP group is incorrect. This is because the members of the SYS_GROUP group will have no CPU restriction. The members of the SYS_GROUP group have the maximum priority for allocated CPU.

The option stating that the members of the OTHER_GROUPS group will always be assigned 100 percent CPU, and the option stating that the members of the OTHER_GROUPS group will never be assigned 100 percent CPU are incorrect. The members of the OTHER_GROUPS at level 3 will be assigned 100 percent CPU only if CPU is not assigned to the members of the SYS_GROUP at level 1, and to the PAYROLL, SALES, and MARKETING groups at level 2.

Item: 3 (Ref:1Z0-043.15.4.3)

You are using the Database Resource Manager to manage database resources. You created a resource plan directive for the MANAGERS resource consumer group under the SALES_PLAN by using the following statement:

```
SQL>EXEC DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE
(PLAN => 'SALES_PLAN',
GROUP_OR_SUBPLAN => 'MANAGERS',
CPU_P1 => 100, CPU_P2 =>0,
SWITCH_GROUP => 'CLERKS',
SWITCH_TIME_IN_CALL => 600);
```

A user, SCOTT, who is assigned to the MANAGERS group, starts a database session and executes a query on the database.

What is the outcome if the query takes approximately 15 minutes to complete?

- The query starts under the CLERKS group and the user, SCOTT, switches back to the MANAGERS group after the query completes.
- The query starts under the MANAGERS group but terminates with an error when the execution time exceeds 10 minutes.
- The query starts under the MANAGERS group and switches automatically to the CLERKS group when the execution time exceeds 10 minutes. The query does not switch back to the MANAGERS group after the query completes.
- The query starts under the MANAGERS group, the user SCOTT switches automatically to the CLERKS group when the execution time exceeds 10 minutes, and then switches back to the MANAGERS group after the query completes.

Answer:

The query starts under the MANAGERS group, the user SCOTT switches automatically to the CLERKS group when the execution time exceeds 10 minutes, and then switches back to the MANAGERS group after the query completes.

Explanation:

In this scenario, the query starts under the MANAGERS group, the user SCOTT switches automatically to the CLERKS group when the execution time exceeds 10 minutes, and then finally switches back to the MANAGERS group after the query completes.

According to the plan directive for the MANAGERS resource group, the SWITCH_GROUP parameter specifies a resource group to which a user session is switched when the execution time exceeds the maximum time allowed for the execution of a top call. A top call is an entire PL/SQL block or an individual SQL statement that is currently executing. The maximum time allowed for the execution of a top call is specified in the SWITCH_TIME_IN_CALL parameter. The value for the SWITCH_TIME_IN_CALL parameter is specified in seconds. After the completion of the top call, the user is switched back to its original resource group.

When the user SCOTT executes the query, the query is initially started under the MANAGERS resource group. During the execution, when the execution time exceeds 10 minutes, the user is switched to the CLERKS resource group. When the query completes, the user SCOTT automatically switches back to the MANAGERS resource group.

The option stating that the query starts under the CLERKS group and the user SCOTT switches back to the MANAGERS group after the query completes is incorrect. The query is initially started under the MANAGERS resource group.

The option stating that the query starts under the MANAGERS group but terminates with an error when the execution time exceeds 10 minutes is incorrect. The query starts under the MANAGERS resource group but does not terminate with an error when the execution time exceeds 10 minutes. Rather, the user is switched automatically to the CLERKS resource group when the execution time exceeds 10 minutes.

The option stating that the query starts under the MANAGERS group and switches automatically to the CLERKS group when the execution time exceeds 10 minutes and does not switch back to the MANAGERS group after the query completes is incorrect. When the query completes, the user is automatically switched back to the CLERKS resource group.

Item: 4 (Ref:1Z0-043.15.1.2)

The Database Resource Manager is not currently active in your database that is up and running. You created a resource plan named DAY_PLAN that contains two sub-plans named MANAGERS_PLAN and CLERKS_PLAN. You decided to activate DAY_PLAN by executing the following statement:

```
SQL>ALTER SYSTEM SET RESOURCE_MANAGER_PLAN = 'managers_plan';
```

What will be the outcome of this statement?

- The statement will deactivate DAY_PLAN.
- The statement will activate DAY_PLAN as the top plan.
- The statement will activate MANAGERS_PLAN as the top plan.
- The statement will return an error because MANAGERS_PLAN is not the top plan.

Answer:

The statement will activate MANAGERS_PLAN as the top plan.

Explanation:

Using the ALTER SYSTEM statement, you can activate or deactivate the Database Resource Manager. When you execute the ALTER SYSTEM SET RESOURCE_MANAGER_PLAN = 'managers_plan' statement, the MANAGERS_PLAN becomes active as a top plan. However, if the MANAGERS_PLAN does not exist in the data dictionary, then this statement returns an error.

You can deactivate the Database Resource Manager by issuing the following statement:

```
SQL>ALTER SYSTEM SET RESOURCE_MANAGER_PLAN = '';
```

If your database is not up and running, you can enable a resource plan at startup by including the RESOURCE_MANAGER_PLAN initialization parameter in your parameter file. The resource plan specified in the RESOURCE_MANAGER_PLAN initialization parameter becomes the top plan. The database will not start if the resource plan specified in the parameter file does not exist in the data dictionary.

The option stating that the ALTER SYSTEM SET RESOURCE_MANAGER_PLAN = 'managers_plan' statement will deactivate the DAY_PLAN is incorrect because this statement will not deactivate a resource plan. To deactivate the current resource plan, you must either deactivate the Database Resource Manager or change the current resource plan.

The option stating that the ALTER SYSTEM SET RESOURCE_MANAGER_PLAN = 'managers_plan' statement will activate the DAY_PLAN as the top plan is incorrect because this statement will activate the MANAGERS_PLAN as the top plan.

The option stating that the ALTER SYSTEM SET RESOURCE_MANAGER_PLAN = 'managers_plan' statement returns an error because the MANAGERS_PLAN is not the top plan is incorrect. Because the MANAGERS_PLAN is a valid resource plan that exists in the data dictionary, the statement will not return an error.

Item: 5 (Ref:1Z0-043.15.4.5)

You updated the resource plan directive for the resource consumer group, DSS_USERS. The resource plan directive is assigned to the DSS_PLAN by using the following statement:

```
SQL>EXEC DBMS_RESOURCE_MANAGER.UPDATE_PLAN_DIRECTIVE
(PLAN => 'DSS_PLAN',
GROUP_OR_SUBPLAN => 'DSS_USERS',
NEW_CPU_P1 => 80,
NEW_SWITCH_GROUP => 'CANCEL_SQL',
NEW_SWITCH_ESTIMATE => TRUE,
NEW_SWITCH_TIME => 600);
```

A user connects to the database and starts an operation. What is the outcome if Oracle estimates that the execution time for this operation will exceed 600 seconds?

- The session is killed before starting the operation.
- The session generates an error before starting the operation.
- The session switches to the CANCEL_SQL resource consumer group before starting the operation.
- The session hangs before starting the operation.

Answer:

The session generates an error before starting the operation.

Explanation:

In this scenario, the session generates an error before starting the operation if Oracle estimates that the execution time for an operation will exceed 600 seconds.

The NEW_SWITCH_GROUP parameter of the DBMS_RESOURCE_MANAGER.UPDATE_PLAN_DIRECTIVE packaged procedure specifies a resource consumer group to which the session is switched when the switch criteria is met. The value of the NEW_SWITCH_GROUP parameter can be set to any valid resource consumer group. If the value of the NEW_SWITCH_GROUP parameter is set to CANCEL_SQL, the session returns an error when the switch criteria is met and prevents the operation from starting.

The NEW_SWITCH_ESTIMATE parameter specifies whether Oracle estimates the execution time for an operation before actually starting the operation. If the NEW_SWITCH_ESTIMATE parameter is set to TRUE, Oracle calculates the estimated time for the operation. If the parameter is set to FALSE, Oracle starts the operation without calculating the estimated time for the operation.

The NEW_SWITCH_TIME parameter specifies the execution time that is allowed for an operation. If the estimated execution time exceeds the value specified by the NEW_SWITCH_TIME parameter, the operation will start under the consumer group specified by the NEW_SWITCH_GROUP parameter.

In this scenario, Oracle estimates the execution time for an operation before starting the operation. If the estimated execution time exceeds 600 seconds as specified in the NEW_SWITCH_TIME parameter, the session is not switched to the CANCEL_SQL group and the operation is terminated with an error before starting.

The option, stating that the session is killed before starting the operation if Oracle estimates that the execution time for the operation will exceed 600 seconds, is incorrect. The session is not killed. The user remains connected to the database but the operation is not started. When you set the NEW_SWITCH_GROUP parameter to KILL_SESSION, the session is killed when the switch criteria is met.

The option, stating that the session switches to the CANCEL_SQL group before starting the operation if Oracle estimates that the execution time for the operation will exceed 600 seconds, is incorrect. The session is not switched to the CANCEL_SQL group. CANCEL_SQL is not a consumer resource group defined in the resource plan. CANCEL_SQL is a value defined in the DBMS_RESOURCE_MANAGER package specifying that the operation will be killed when the switch criteria is met.

The option, stating that the session hangs before starting the operation if Oracle estimates that the execution time for an operation will exceed 600 seconds, is incorrect. When Oracle estimates that the execution time to complete an operation exceeds 600 seconds, the database does not hang. The session is automatically switched to the consumer group as specified in the NEW_SWITCH_GROUP parameter.

Item: 6 (Ref:1Z0-043.15.2.1)

You issue the following code:

```
EXEC DBMS_RESOURCE_MANAGER_PRIVS.GRANT_SWITCH_CONSUMER_GROUP
   ('SCOTT' 'GRP1', TRUE);
```

What will be the result of executing the above code?

- The switch privilege will be granted to the user, Scott, for changing the consumer group to GRP1.
- The switch privilege will be granted to the user, Scott, for changing the consumer group from GRP1 to any other group.
- The code will not execute successfully because there is no GRANT_SWITCH_CONSUMER_GROUP procedure in the DBMS_RESOURCE_MANAGER_PRIVS package.
- The code will execute successfully but no privilege will be granted to the user, Scott.

Answer:

The switch privilege will be granted to the user, Scott, for changing the consumer group to GRP1.

Explanation:

The DBMS_RESOURCE_MANAGER_PRIVS.GRANT_SWITCH_CONSUMER_GROUP procedure is used to grant the switch privilege to the users or roles. Before users can switch their own consumer group, they must have the switch privilege.

The option stating that the switch privilege is granted to the user, Scott, for changing the consumer group from GRP1 to any other group is incorrect. The users will be granted the switch privilege to change the existing consumer group to the group specified as the value of the CONSUMER_GROUP argument of the DBMS_RESOURCE_MANAGER_PRIVS.GRANT_SWITCH_CONSUMER_GROUP procedure.

The option stating that the code will not execute successfully because there is no GRANT_SWITCH_CONSUMER_GROUP procedure in the DBMS_RESOURCE_MANAGER_PRIVS package is incorrect. The GRANT_SWITCH_CONSUMER_GROUP is a valid procedure in the DBMS_RESOURCE_MANAGER_PRIVS package.

The option stating that the code will be executed successfully but no privilege will be granted to the user, Scott, is incorrect. The switch privilege will be granted to the user, Scott.

Item: 7 (Ref:1Z0-043.15.2.2)

You want to enable the user, Scott, to change to the GRP1 consumer group by issuing the following code:

```
SQL> EXEC DBMS_SESSION.SWITCH_CURRENT_CONSUMER_GROUP ('SCOTT',
'GRP1', FALSE);
```

How will you grant the switch privilege to the user, Scott?

- by using the DBMS_SESSION package
- by granting the DBA role
- by using the DBMS_RESOURCE_MANAGER package
- by using the DBMS_RESOURCE_MANAGER_PRIVS package

Answer:

by using the DBMS_RESOURCE_MANAGER_PRIVS package

Explanation:

Before a user can switch between consumer groups, the user must have the switch privilege or be granted a role that has been granted the switch privilege. The switch privilege is granted to users and to roles through the DBMS_RESOURCE_MANAGER.PRIVS GRANT_SWITCH_CONSUMER_GROUP procedure. The parameters for this procedure are as follows:

Parameter	Description
GRANTEE_NAME	indicates the username or role name receiving the grant
CONSUMER_GROUP	indicates the name of the consumer group to which the grantee will be allowed to switch
GRANT_OPTION	indicates whether the grantee can grant the switch privilege to another user or not. If TRUE, the grantee can grant the switch privilege to another user. If FALSE, the grantee cannot grant the switch privilege to another user.

The option stating that you will grant the switch privilege to the user by using the DBMS_SESSION package is incorrect. If the user has the switch privilege, the user can change the existing consumer group by using the DBMS_SESSION.SWITCH_CURRENT_CONSUMER__GROUP package.

The option stating that you will grant the switch privilege to the user by granting the DBA role is incorrect. The DBA role is created at the time of the database installation. The DBA role contains most system privileges. Therefore, the DBA role should be granted to the Database Administrator only.

The option stating that you will grant the switch privilege to the user by using the DBMS_RESOURCE_MANAGER package is incorrect. The DBMS_RESOURCE_MANAGER package is used to administer the database resource manager.

Item: 8 (Ref:1Z0-043.15.2.3)

You issued the following block of code:

```
SQL>BEGIN
DBMS_RESOURCE_MANAGER_PRIVS.GRANT_SWITCH_CONSUMER_GROUP(
'PROG_ROLE', 'DEVELOPERS' ,FALSE);
END;
SQL>/
```

Which option is **NOT** a result of executing the above code?

- The switch privilege is granted to the PROG_ROLE role.
- The users granted the role PROG_ROLE will be able to switch to the DEVELOPERS group.
- The users cannot grant the switch privilege to other users.
- The above code will not be executed successfully because the GRANT_SWITCH_CONSUMER_GROUP procedure is an invalid procedure in Oracle10*g*.

Answer:

The above code will not be executed successfully because the GRANT_SWITCH_CONSUMER_GROUP procedure is an invalid procedure in Oracle10*g*.

Explanation:

The option stating that the code will not be executed successfully because the GRANT_SWITCH_CONSUMER_GROUP procedure is an invalid procedure in Oracle10*g* is incorrect. The DBMS_RESOURCE_MANAGER_PRIVS.GRANT_SWITCH_CONSUMER_GROUP procedure is used to grant the switch privilege to the users or the roles. Before a user can switch its own consumer group, the user must have the switch privilege. The parameters of the GRANT_SWITCH_CONSUMER_GROUP procedure are as follows:

Parameter	Description
GRANTEE_NAME	indicates the username or role name receiving the grant.
CONSUMER_GROUP	indicates the name of the consumer group to which the grantee will be allowed to switch
GRANT_OPTION	indicates whether the grantee can grant the switch privilege to another user or not. If TRUE, the grantee can grant the switch privilege to another user. If FALSE, the grantee cannot grant the switch privilege to another user.

In this scenario, the switch privilege is granted to the PROG_ROLE. The users granted the PROG_ROLE will be able to switch to the DEVELOPERS group. The value of the GRANT_OPTION parameter is set to FALSE. Therefore, the users cannot grant the switch privilege to other users.

The option stating that the code will not be executed successfully because GRANT_SWITCH_CONSUMER_GROUP is an invalid procedure in Oracle10*g* is incorrect.

Item: 9 (Ref:1Z0-043.15.3.2)

You are creating the simple resource plan using the DBMS_RESOURCE_MANAGER.CREATE_SIMPLE_PLAN procedure.

Which resource allocation policy will be used for the resource plan?

- RATIO
- EMPHASIS
- ACTIVE_SESS_POOL_MTH
- RESOURCE_DEGREE_LIMIT_ABSOLUTE

Answer:

EMPHASIS

Explanation:

The EMPHASIS resource allocation policy will be used. When you create a simple resource plan and you want to impose a restriction on the utilization of resources by the database users, you assign users to the consumer group. The simple resource plans always uses the EMPHASIS CPU resource allocation policy. This means that the value for the CPU allocations will be interpreted as a percentage of total CPU.

The option stating that the RATIO resource allocation policy will be used is incorrect. The allocated amount is treated as a ratio of the total CPU resources. The RATIO method can be defined only on single-level plans.

The option stating that the ACTIVE_SESS_POOL_MTH resource allocation policy will be used is incorrect. The ACTIVE_SESS_POOL_MTH represents active session resource allocation method. The ACTIVE_SESS_POOL_MTH resource allocation policy controls the maximum concurrent users.

The option stating that the RESOURCE_DEGREE_LIMIT_ABSOLUTE resource allocation policy will be used is incorrect. The RESOURCE_DEGREE_LIMIT_ABSOLUTE represents a resource allocation method for specifying a limit on the degree of parallelism of any operation.

Item: 10 (Ref:1Z0-043.15.4.6)

You set the undo pool resource plan directive for the consumer group named DSS_USERS that is assigned to the DAY_SHIFT plan.

The database users, SCOTT and BLAKE, belong to the DSS_USERS resource group. The user, SCOTT, initiates a database session and executes a batch operation that inserts millions of rows into the HISTORY table.

Which two options are true if the total undo space allocated to the DSS_USERS group exceeds the value specified in the undo pool resource plan directive? (Choose two.)

- ☐ The batch operation started by the user, SCOTT, terminates with an error.
- ☐ The batch operation started by the user, SCOTT, hangs and you are required to increase the undo pool resource plan directive.
- ☐ The batch operation started by the user, SCOTT, runs uninterrupted because the database uses the SYSTEM tablespace for the undo operation.
- ☐ The user, BLAKE, cannot start a transaction that uses any DML operations until you increase the value of the undo pool resource plan directive.
- ☐ The user BLAKE can start a transaction that uses any DML operations after the batch operation started by the user, SCOTT, terminates with an error.

Answer:

The batch operation started by the user, SCOTT, terminates with an error.

The user, BLAKE, cannot start a transaction that uses any DML operations until you increase the value of the undo pool resource plan directive.

Explanation:

In this scenario, the batch operation started by the user, SCOTT, terminates with an error. Also, the user, BLAKE, cannot start a transaction that uses any DML operations until you increase the value of the undo pool resource plan directive.

If you set the undo pool resource plan directive for a consumer group and the total undo space used by the sessions belonging to this consumer group exceeds the amount specified in the undo pool resource plan directive, the current operation will be aborted with an error. The other sessions that have been assigned to this consumer group cannot execute the INSERT, UPDATE, and DELETE statements unless the undo space is freed by other sessions of the same group or the value of the undo pool resource plan directive the group is increased. The queries are not blocked and are allowed to execute even if the sessions exceed the undo space specified in the undo pool resource plan directive.

The option stating that the batch operation started by the user SCOTT hangs and you are required to modify the undo pool resource plan directive is incorrect. When the total undo space used by the DSS_USERS resource group exceeds the value of the undo pool resource plan directive, the database does not hang. The batch operation started by the user SCOTT is terminated with an error.

The option stating that the batch operation started by the user SCOTT runs uninterrupted because the database uses the SYSTEM tablespace for the undo operation is incorrect because the batch operation is terminated with an error. The SYSTEM tablespace will not be used for the undo operation and the user, SCOTT, continues to use the undo tablespace assigned to him.

The option stating that the user, BLAKE, can start a transaction that uses any DML operation after the batch operation started by the user, SCOTT, terminates with an error is incorrect. The user, BLAKE, cannot start a transaction that uses any DML operations until the undo space used by the other sessions of the DSS_USERS group is freed or the value for the undo pool resource plan directive is increased.

Item: 11 (Ref:1Z0-043.15.3.1)

You are creating a resource consumer group using the DBMS_RESOURCE_MANAGER.CREATE_CONSUMER_GROUP procedure. Which parameter will you use to define the resource scheduling method used between sessions within the resource group?

- CPU_MTH
- NEW_CPU_MTH
- CPU_P1
- CPU_P2

Answer:

CPU_MTH

Explanation:

You will use the CPU_MTH parameter to define the resource scheduling method used between sessions within the resource group. This method governs only the CPU resources between group members. You must assign users to consumer groups before using the resource plan. The total CPU available to the resource group may have been limited by the active resource plan.

The option stating that you will use the NEW_CPU_MTH parameter to define the resource scheduling method used between sessions within the resource group is incorrect. The NEW_CPU_MTH parameter is used with the UPDATE_COSUMER_GROUP procedure. The NEW_CPU_MTH parameter updates the CPU allocation methods.

The option stating that you will use the CPU_P1 parameter to define the resource scheduling method used between sessions within the resource group is incorrect. The parameter, CPU_P1, is a CREATE_PLAN_DIRECTIVE procedure parameter. The CPU_P1 parameter represents either the CPU allocated at level 1 or the ratio weight for CPU resources, depending on the allocation method defined for the resource plan. If the resource plan uses the EMPHASIS allocation method for the CPU resources, the CPU_P1 parameter defines the percentage of CPU allocated at level 1 for the subplan. If the plan uses the RATIO allocation method for the CPU resources, the CPU_P1 parameter defines the weight of the CPU usage for the subplan. The default value, which is NULL, does not allocate the CPU resources.

The option stating that you will use the CPU_P2 parameter to define the resource scheduling method used between sessions within the resource group is incorrect. The CPU_P2 parameter represents the percentage of CPU allocated at level 2 for the subplan.

Item: 12 (Ref:1Z0-043.15.4.2)

You have created a resource plan, DAY. You execute the following code:

```
SQL> BEGIN
DBMS_RESOURCE_MANAGER.CREATE_SIMPLE_DIRECTIVE
(
PLAN => 'DAY',
COMMENT => 'DEPARTMENTS PLAN',
GROUP_OR_SUBPLAN => 'DEPARTMENTS',
CPU_P1=0);
END;
```

Then, you issue the following code:

```
SQL> BEGIN
DBMS_RESOURCE_MANAGER.CREATE_SIMPLE_DIRECTIVE
(
PLAN => 'DAY',
COMMENT => 'DEPARTMENTS PLAN',
GROUP_OR_SUBPLAN => 'DEVELOPERS',
CPU_P2=100);
END;
```

What will be the impact of executing the above code?

- The DEVELOPERS and DEPARTMENTS subplans will be allocated CPU equally.
- The DEVELOPERS subplan will be allocated 100 percent CPU if there are no resources allocated to the DEPARTMENTS subplan.
- The DEPARTMENT subplan will be allocated 100 percent CPU if there are no resources allocated to the DEVELOPERS subplan.
- The second code will not execute because one resource plan cannot be used by more than one subplan.

Answer:

The DEVELOPERS subplan will be allocated 100 percent CPU if there are no resources allocated to the DEPARTMENTS subplan.

Explanation:

The subplan DEPARTMENT will be allocated 100 percent CPU if no resources are allocated to the DEPARTMENTS subplan. To create a subplan directive, a plan directive that allocates CPU resources to a subplan is created. The subplan retains its original functionality. However, the total CPU resources it can allocate are limited to those it receives from the top level plan. In this scenario, the plan DEVELOPERS is defined as a subplan of the DAY plan and is limited to 100 percent of the level 2 CPU resources. The value of the CPU_P2 parameter indicates the percentage of the CPU allocated at the level 2 for the group or subplan. You can specify up to eight levels of subplans, with level 1 being the highest priority and level 8 being the lowest. Level 1 recipients receive the total available CPU based on their respective CPU_P1 parameter value. Level 1 recipients share only the CPU resources that are not consumed at level 1 and so on.

The option stating that the DEVELOPERS and DEPARTMENTS subplans will allocate CPU equally, and the option stating that subplan DEPARTMENTS will allocate 100 percent CPU if there are no resources allocated to the DEVELOPERS subplan are incorrect.

The option stating that the second code will not execute because one resource plan cannot be used by more than one subplan is incorrect. A subplan can be used by more than one subplan.

Item: 13 (Ref:1Z0-043.15.1.3)

You recently activated a resource plan named OLTP_PLAN in your database. Several users are concurrently running long transactions. You decide to monitor the resource manager to determine if the resource allocation formulated in the OLTP_PLAN is sufficient for peak database hours.

Which dynamic performance view should you use to display the CPU time consumed by all the sessions within the resource groups?

- V$SYSSTAT
- V$SESSSTAT
- V$RSRC_PLAN
- V$RSRC_CONSUMER_GROUP

Answer:

V$RSRC_CONSUMER_GROUP

Explanation:

You should use the V$RSRC_CONSUMER_GROUP dynamic performance view to display the CPU time consumed by all the sessions within the resource groups. The V$RSRC_CONSUMER_GROUP dynamic performance view is used to monitor the CPU usage for the active resource plan. For example, the following statement will display the cumulative amount of CPU time consumed by all the sessions in each consumer group:

```
SQL>SELECT NAME, CONSUMED_CPU_TIME FROM V$RSRC_CONSUMER_GROUP;
```

The V$SYSSTAT dynamic performance view is incorrect because this view is used to display the CPU usage per session in the database.

The V$SESSSTAT dynamic performance view is incorrect because this view is used to display the aggregate CPU usage for all the sessions in the database.

The V$RSRC_PLAN dynamic performance view is incorrect because this view is used to display the names of all the currently active resource plans in the database. You cannot display CPU statistics by using the V$RSRC_PLAN dynamic performance view.

Item: 14 (Ref:1Z0-043.15.3.5)

You execute the following block of code:

```
SQL>BEGIN
DBMS_RESOURCE_MANAGER.CREATE_SIMPLE_PLAN
(
SIMPLE_PLAN => 'DEPARTMENTS',
CONSUMER_GROUP1 => 'PAYROLLL',
GROUP1_CPU => 50,
CONSUMER_GROUP2 => 'SALES',
GROUP2_CPU => 25,
CONSUMER_GROUP3 => 'MARKETING',
GROUP3_CPU => 25);
END;
SQL>/
```

What is a prerequisite for using the simple resource plan created by executing the above code?

- You must assign users to consumer groups.
- You must grant the switch privilege to the users.
- You must create a resource plan directive.
- You must specify the complex resource plan.

Answer:

You must assign users to consumer groups.

Explanation:

Before using the resource plan, you must assign users to the consumer group. The `DBMS_RESOURCE_MANAGER.CREATE_SIMPLE_PLAN` procedure is used to create the simple resource plans. Simple resource plans are limited only to the CPU resource plan directive. This means that the only resource that can be allocated is the CPU. Simple plans also limit the total number of resource groups to eight.

The option stating that you must grant the switch privilege to the users is incorrect. The switch privilege is granted to a user to enable the user to change the existing consumer group to a specified group. The `DBMS_RESOURCE_MANAGER_PRIVS.GRANT_SWITCH_CONSUMER_GROUP` procedure is used to grant the switch privilege to the user.

The option stating that you must create the resource plan directive before using the simple resource plan is incorrect. The resource plan directive assigns consumer groups to resource plans and defines the resource allocations to each group. In addition to consumer groups, resource plan directives can also allocate resources to subplans.

The option stating that you must create a complex resource plan before using the simple resource plan is incorrect. The complex resource plans differ from simple resource plans in the methods in which they are defined. Simple plans involve creation of a plan, resource consumer groups, and plan directives in a single operation. However, in complex plans, all the elements are defined and stored separately.

Item: 15 (Ref:1Z0-043.15.1.4)

You recently created a complex resource plan named DB_PLAN that has two subplans named OLTP_PLAN and DSS_PLAN. The OLTP_PLAN and DSS_PLAN subplans are allotted 70 percent and 30 percent of the total CPU resources, respectively. The OLTP_PLAN subplan allocates 35 percent of the available CPU resources to a resource consumer group named ACCT_CLERKS. According to the OLTP_PLAN subplan, the remaining 65 percent of the available CPU resources is allocated to a second resource consumer group named MKT_CLERKS. The CPU resources available to the DSS_PLAN subplan are divided into two resource consumer groups named MKT_MANAGERS and FIN_MANAGERS. The MKT_MANAGERS group receives 65 percent of the available CPU resources, and the FIN_MANAGERS group receives 35 percent of the available CPU resources.

What percentage of actual CPU resources will the resource consumer group, MKT_CLERKS, receive, if the DSS_PLAN subplan does **NOT** consume any CPU resources?

- 45.5
- 65
- 70
- 100

Answer:

65

Explanation:

In this scenario, the MKT_CLERKS group receives 65 percent of the total CPU resources. If the DSS_PLAN subplan does not consume any CPU resources, then the resource consumer group MKT_CLERKS receives 65 percent of the total CPU resources. In the absence of the consumption of resources by the DSS_PLAN subplan, the OLTP_PLAN subplan receives 100 percent of the total CPU resources. According to the OLTP_PLAN subplan, the MKT_CLERKS consumer group receives 65 percent of the CPU resources available to the plan.

The 45.5 percent option is incorrect because the MKT_CLERKS group receives 65 percent of the total CPU resources. The MKT_CLERKS consumer group will receive 45.5 percent of the total CPU resources if there are resource consumers who are consuming the CPU resources under the DSS_PLAN subplan. In this scenario, the OLTP_PLAN subplan will receive 70 percent of the total CPU resources, and the MKT_CLERKS consumer group will receive 45.5 percent (that is, 65 percent of 70 percent) of the total CPU resources.

The 70 percent option is incorrect because the MKT_CLERKS group receives 65 percent of the total CPU resources. The MTK_CLERKS group receives 70 percent of the total CPU resources only when there are consumers for the resources allocated to the DSS_PLAN subplan but none of the CPU resources are consumed by the ACCT_CLERKS resource group. In this scenario, the OLTP_PLAN subplan receives 70 percent of the total CPU resources. The resources received are entirely allocated to the MKT_CLERKS group.

The 100 percent option is incorrect because the MKT_CLERKS group receives 65 percent of the total CPU resources. The MKT_CLERKS group receives 100 percent of the total CPU resources when there are no consumers for the CPU resources under the DSS_PLAN subplan and the ACCT_CLERKS consumer group. In such a scenario, the OLTP_PLAN subplan receives 100 percent of the total CPU resources. These resources are entirely allocated to the MKT_CLERKS consumer group.

Item: 16 (Ref:1Z0-043.15.4.4)

You want to create the resource plan directives for the IT_MANAGERS group to enforce the following requirements:

- If a user starts an operation, Oracle should estimate the execution time for the operation before starting the operation.
- If the estimated execution time is more than 600 seconds, the operation should be allowed to run under the LOW_GROUP consumer group.
- If the estimated execution time is more than 5400 seconds, the operation should not be allowed to start.
- After switching to the LOW_GROUP consumer group, the switched sessions should not be switched back to the IT_MANAGERS group.

Which statement must you execute to create the resource plan directives for the IT_MANAGERS?

- SQL>EXEC DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE
  (PLAN => 'DSS_PLAN',
  GROUP_OR_SUBPLAN => 'IT_MANAGERS',
  CPU_P1 => 100, CPU_P2 => 0,
  SWITCH_GROUP => 'LOW_GROUP',
  SWITCH_ESTIMATE => TRUE,
  SWITCH_TIME => 5400);
- SQL>EXEC DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE
  (PLAN => 'DSS_PLAN',
  GROUP_OR_SUBPLAN => 'IT_MANAGERS',
  CPU_P1 => 100, CPU_P2 => 0,
  SWITCH_GROUP => 'LOW_GROUP',
  SWITCH_ESTIMATE => FALSE,
  SWITCH_TIME => 600,
  MAX_EST_EXEC_TIME => 5400);
- SQL>EXEC DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE
  (PLAN => 'DSS_PLAN',
  GROUP_OR_SUBPLAN => 'IT_MANAGERS',
  CPU_P1 => 100, CPU_P2 => 0,
  SWITCH_GROUP => 'LOW_GROUP',
  SWITCH_ESTIMATE => TRUE,
  SWITCH_TIME => 600,
  MAX_EST_EXEC_TIME => 5400);
- SQL>EXEC DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE
  (PLAN => 'DSS_PLAN',
  GROUP_OR_SUBPLAN => 'IT_MANAGERS',
  CPU_P1 => 100, CPU_P2 => 0,
  SWITCH_GROUP => 'LOW_GROUP',
  SWITCH_ESTIMATE => TRUE,
  SWITCH_TIME_IN_CALL => 600,
  MAX_EST_EXEC_TIME => 5400);

Answer:

```
SQL>EXEC DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE
(PLAN => 'DSS_PLAN',
GROUP_OR_SUBPLAN => 'IT_MANAGERS',
CPU_P1 => 100, CPU_P2 => 0,
SWITCH_GROUP => 'LOW_GROUP',
SWITCH_ESTIMATE => TRUE,
SWITCH_TIME => 600,
MAX_EST_EXEC_TIME => 5400);
```

Explanation:

In this scenario, you must execute the following statement to create the resource plan directives for the IT_MANAGERS resource group:

```
SQL>EXEC DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE
(PLAN => 'DSS_PLAN',
```

```
GROUP_OR_SUBPLAN => 'IT_MANAGERS',
CPU_P1 => 100, CPU_P2 => 0,
SWITCH_GROUP => 'LOW_GROUP',
SWITCH_ESTIMATE => TRUE,
SWITCH_TIME => 600,
MAX_EST_EXEC_TIME => 5400);
```

You must set the value of the SWITCH_GROUP parameter of the DBMS_RESOURCE_MANAGER.CREATE_PLAN_DIRECTIVE packaged procedure to LOW_GROUP to ensure that the user session is switched to the LOW_GROUP resource group when the estimated execution time is more than 600 seconds. The SWITCH_GROUP parameter specifies the resource consumer group to which the user sessions will be switched if this switch criteria is met.

You must set the value of the SWITCH_ESTIMATE parameter to TRUE so that Oracle estimates the execution time for an operation before starting the operation. If the estimated execution time exceeds the time allowed, specified by the SWITCH_TIME parameter, to complete an operation, the user session automatically switches to the consumer group before starting the operation. If the SWITCH_ESTIMATE parameter is set to FALSE, then Oracle does not calculate the estimated execution time and starts the operation under the current resource group. During execution, the user session is switched to the consumer group only when the execution time exceeds the time allowed to complete the operation. You must set the value of the SWITCH_TIME parameter to 600 seconds. This is because the user session should be switched to the LOW_GROUP resource group if the execution time is more than 600 seconds.

You must set the value of the MAX_EST_EXEC_TIME parameter to 5400 to ensure that Oracle estimates the execution time to complete the operation before starting the operation. If the estimated execution time exceeds the maximum time allowed for an operation, the operation will not be started.

The basic difference between the SWITCH_TIME and SWITCH_TIME_IN_CALL parameters is that when you specify the SWITCH_TIME_IN_CALL parameter, the user is switched back to its original resource group after the end of the top call. When you specify the SWITCH_TIME parameter, the user remains in the current resource group and does not switch back to its original resource group. In this scenario, you must set the SWITCH_TIME parameter and not the SWITCH_TIME_IN_CALL parameter.

All the other options are incorrect.

Automating Tasks with the Scheduler

Item: 1 (Ref:1Z0-043.16.4.2)

Which view will you use to view information regarding the jobs that are currently running in a database?

- DBA_SCHEDULER_RUNNING_JOBS
- DBA_SCHEDULER_JOB_RUN_DETAILS
- DBA_SCHEDULER_JOBS
- DBA_SCHEDULER_JOB_LOG

Answer:

DBA_SCHEDULER_RUNNING_JOBS

Explanation:

The DBA_SCHEDULER_RUNNING_JOBS view is used to view information regarding the currently jobs that are currently running in a database. The columns of the DBA_SCHEDULER_RUNNING_JOBS view are as follows:

Column	Description
OWNER	Indicates the owner of the running job
JOB_NAME	Indicates the name of the running job
SESSION_ID	Indicates the session identifier of the running job
SLAVE_PROCESS_ID	Indicates the process ID of the slave process running the job
RUNNING_INSTANCE	Indicates the database instance ID of the slave process
RESOURCE_CONSUMER_GROUP	Indicates the resource consumer group of the session in which the job is running
ELAPSED_TIME	Indicates the time elapsed since the start of the job
CPU_USED	Indicates the CPU time consumed by the job

The option stating that you will query the DBA_SCHEDULER_JOB_RUN_DETAILS view to find information regarding the jobs that are currently running in a database is incorrect. This is because the DBA_SCHEDULER_JOB_RUN_DETALS view is used to display the log run details about a particular job in the database.

The option stating that you will query the DBA_SCHEDULER_JOBS view to find information regarding jobs that are currently running in a database is incorrect. This is because the DBA_SCHEDULER_JOBS view is used to view the information about all the jobs in the database. This view displays information about jobs that have been executed in the past, jobs that have been stopped, currently executing jobs, and jobs that will be run in the future.

The option stating that you will query the DBA_SCHEDULER_JOB_LOG view to find information regarding the jobs that are currently running in a database is incorrect. This is because the DBA_SCHEDULER_JOB_LOG view is used to view the log entries for previously executed jobs.

Item: 2 (Ref:1Z0-043.16.2.2)

You are creating a job class. You have issued the following command to create the job class:

```
SQL> BEGIN
DBMS_SCHEDULER.CREATE_JOB_CLASS(
JOB_CLASS_NAME => 'LOW_PRIORITY_CLASS',
RESOURCE_CONSUMER_GROUP => 'LOW_GROUP',
LOGGING_LEVEL => DBMS_SCHEDULER.LOGGING_FULL,
LOG_HISTORY => 1200,
COMMENTS => 'LOW JOB PRIORITY CLASS');
END;
SQL> /
```

What will be the result of the above command?

- The command will be executed successfully.
- The command will fail because RESOURCE_CONSUMER_GROUP is an invalid parameter in the DBMS_SCHEDULER.CREATE_JOB_CLASS procedure.
- The command will fail because LOGGING_LEVEL is an invalid parameter in the DBMS_SCHEDULER.CREATE_JOB_CLASS procedure.
- The command will fail because LOG_HISTORY is an invalid parameter in the DBMS_SCHEDULER.CREATE_JOB_CLASS procedure.
- The command will fail because 1200 is an invalid value for the LOG_HISTORY parameter in the DBMS_SCHEDULER.CREATE_JOB_CLASS procedure.

Answer:

The command will fail because 1200 is an invalid value for the LOG_HISTORY parameter in the DBMS_SCHEDULER.CREATE_JOB_CLASS procedure.

Explanation:

The command will fail because 1200 is an invalid value for the LOG_HISTORY parameter. The LOG_HISTORY parameter determines the number of days for which the logged information should be retained. The default value for the LOG_HISTORY parameter is 30 days. Valid values range between 1 and 999 days. When the records exceed this duration, the Scheduler will automatically purge them.

The option stating that the command will be executed successfully is incorrect. This is because the value of the LOG_HISTORY parameter in the DBMS_SCHEDULER.CREATE_JOB_CLASS procedure is set to an incorrect value of 1200 days. The valid values range between 1 and 999 days. The LOG_HISTORY parameter determines the number of days for which the logged information should be retained.

The option stating that the command will fail because the RESOURCE_CONSUMER_GROUP is an invalid parameter in the DBMS_SCHEDULER.CREATE_JOB_CLASS procedure is incorrect. This is because the RESOURCE_CONSUMER_GROUP parameter is a valid parameter in the DBMS_SCHEDULER.CREATE_JOB_CLASS procedure. This parameter associates the job group with a specific consumer group. The consumer group will automatically govern all the jobs assigned to the job class.

The option stating that the command will fail because LOGGING_LEVEL is an invalid parameter in the DBMS_SCHEDULER.CREATE_JOB_CLASS procedure is incorrect. This is because LOGGING_LEVEL is a valid parameter in the DBMS_SCHEDULER.CREATE_JOB_CLASS procedure. The Oracle Scheduler can maintain the job logs of all the job activities. Job logging is determined by setting the LOGGING_LEVEL parameter of the job class. The LOGGING_LEVEL parameter specifies the amount of job information that is logged. There are three valid settings for the LOGGING_LEVEL parameter:

DBMS_SCHEDULER.LOGGING_OFF	No logging will be performed for any jobs in the class.
DBMS_SCHEDULER.LOGGING_RUNS	The detailed information will be written for all the runs of each job in the class.
DBMS_SCHEDULER.LOGGING_FULL	The detailed information will be written for all the runs of each job in the class and every operation performed on any job in the class will be logged.

The option stating that the LOG_HISTORY parameter is an invalid parameter in the DBMS_SCHEDULER.CREATE_JOB_CLASS procedure is incorrect. This is because LOG_HISTORY is a valid parameter that is used to specify the number of days for which the logged information should be retained. The default value is 30 days.

Item: 3 (Ref:1Z0-043.16.2.4)

William is creating a job class. William specifies the LOGGING_FULL setting for the LOGGING_LEVEL attribute at the time of job class creation.

What is the impact of using this setting?

- Detailed information regarding the first run of each job in the class will be written in the job log, and every operation performed on the job class will be logged.
- Detailed information regarding each run of only the first job in the class will be written in the job log, and every operation performed on the job class will be logged.
- Detailed information regarding each run of each job in the class will be written in the job log, and every operation performed on the job class will be logged.
- Detailed information regarding each run of each job in the class will be written in the job log, but operations performed on the job class will not be logged.

Answer:

Detailed information regarding each run of each job in the class will be written in the job log, and every operation performed on the job class will be logged.

Explanation:

When the LOGGING_FULL setting is specified for the LOGGING_LEVEL attribute at the time of the job class creation, detailed information will be written in the job log for each run of each job in the class, and every operation performed on the job class will be logged. The Oracle Scheduler can maintain the job logs for all the job activities. Job logging is determined by setting the LOGGING_LEVEL attribute of the job class. The LOGGING_LEVEL parameter specifies how much job information is logged. The three valid settings for this attribute are as follows:

```
DBMS_SCHEDULER.LOGGING_OFF
DBMS_SCHEDULER.LOGGING_RUNS
DBMS_SCHEDULER.LOGGING_FULL
```

The DBMS_SCHEDULER.LOGGING_FULL setting for the LOGGING_LEVEL attribute specifies that detailed information will be written for all the runs in each job in the class and every operation, such as CREATE, ENABLE, and DROP, performed on any job in the class will be logged.

The option stating that the detailed information will be written in the job log for only the first run of each job in the job class, and every operation performed on the job class will be logged is incorrect. The LOGGING_LEVEL parameter is set to DBMS_SCHEDULER.LOGGING_FULL. This specifies that the detailed information will be written for all the runs of each job in the class and every operation, such as CREATE, ENABLE, and DROP, performed on any job in the class will be logged.

The option stating that the detailed information will be written in the job log for each run of only the first job in the job class, and that every operation performed on the job class will be logged is incorrect. The option stating that the detailed information will be written in the job log for each run of each job in the class but that no operations performed on the job class will be logged is also incorrect. This is because the LOGGING_LEVEL parameter is set to DBMS_SCHEDULER.LOGGING_FULL. The setting specifies that the detailed information will be written for all the runs of each job in the class and every operation, such as CREATE, ENABLE, and DROP, performed on any job in the class will be logged.

Item: 4 (Ref:1Z0-043.16.1.1)

You executed the following code:

```
BEGIN
DBMS_SCHEDULER.SET_ATTRIBUTE (
NAME => 'JOB_A',
ATTRIBUTE => 'JOB_PRIORITY',
VALUE => 7);
END;
/
```

After analyzing the above code, what conclusion will you draw?

- The code will be executed successfully.
- The code will not be executed successfully because the value of the VALUE parameter must be 1, 2, or 3.
- The code will not be executed successfully because the value of the VALUE parameter must range between 1 and 5.
- The code will not be executed successfully because no SET_ATTRIBUTE procedure exists in the DBMS_SCHDULER package.

Answer:

The code will not be executed successfully because the value of the VALUE parameter must range between 1 and 5.

Explanation:

In this scenario, the code will not be executed successfully because the value of the VALUE parameter in the DBMS_SCHEDULER.SET_ATTRIBUTE stored procedure can range between 1 and 5. The priorities of the jobs can be changed by using the SET_ATTRIBUTE procedure of the DBMS_SCHEDULER package. The job priorities must range between 1 and 5. The highest priority is 1. The syntax for changing the priority of the jobs is as follows:

```
BEGIN
DBMS_SCHEDULER.SET_ATTRIBUTE (
name => <job_name>,
attribute => 'job_priority',
value => <value>);
END;
/
```

The option stating that the code will be executed successfully is incorrect. The option stating that the code will not be executed successfully because the value of the VALUE parameter must be 1, 2, or 3 is incorrect. This is because the value of the VALUE parameter of the DBMS_SCHEDULER.SET_ATTRIBURE package can range between 1 and 5.

The option stating that the code will not be executed successfully because no SET_ATTRIBUTE procedure exists in the DBMS_SCHDULER package is incorrect. This is because the SET_ATTRIBUTE procedure in the DBMS_SCHEDULER package is used to set the priorities of the jobs. The syntax of the SET_ATTRIBUTE procedure is as follows:

```
DBMS_SCHEDULER.SET_ATTRIBUTE (
name IN VARCHAR2,
attribute IN VARCHAR2,
value IN[VARCHAR2, TIMESTAMP WITH TIMEZONE,
PLS_INTEGER, BOOLEAN, INTERVAL DAY TO SECOND]);
```

Item: 5 (Ref:1Z0-043.16.2.3)

Your system performs heavy transaction processing between 8:00 A.M. and 5:00 P.M. but runs batch processing and reports after that. You decide to create a separate resource plan to govern resource allocation for each time period.

Which scheduler object will you use to switch automatically between the two resource plans?

- Window
- Program
- Job_Class
- Window group

Answer:

Window

Explanation:

The Window scheduler object can be used to switch automatically between two resource plans. While creating the window scheduler object, the RESOURCE_PLAN parameter specifies the name of the resource plan that will govern the timeframe window. When the window opens, the system switches to the specified resource plan. When the window closes, the system either switches back to the prior resource plan or to the resource plan of the new window if another window is opening.

The option stating that the program can be used to switch automatically between two resource plans is incorrect. A program defines the action that will occur when a job runs. It can be a PL/SQL block, a stored procedure, or an operating system executable.

The option stating that the job class can be used to switch automatically between two resource plans is incorrect. A job class is a container object for the logical grouping of jobs into a larger unit. From an administrative perspective, it is easier to manage a small number of job classes than a large number of individual jobs. Certain job characteristics that can be assigned at the group level will be inherited by all the jobs within the group. Job classes can be assigned to a resource consumer group. This allows you to control resource allocation for all the jobs within the group.

The option stating that the job class can be used to switch automatically between two resource plans is incorrect. A window group is a named collection of windows created in the SYS schema. A window group simplifies the management of windows by allowing the members of the group to be manipulated as an object.

Item: 6 (Ref:1Z0-043.16.1.2)

You want to purge job entries older than 5 days from the job log. You do not want to purge window log entries. Which command will you use to accomplish this task?

- `EXECUTE DBMS_SCHEDULER.PURGE_LOG(log_history => 5, job_name => 'JOB1');`
- `EXECUTE DBMS_SCHEDULER.PURGE_LOG( log_history => 5, job_name => 'JOB_LOG');`
- `EXECUTE DBMS_SCHEDULER.PURGE_LOG( log_history => 5, which_log => 'JOB1');`
- `EXECUTE DBMS_SCHEDULER.PURGE_LOG( log_history => 5, which_log =>'JOB_LOG');`

Answer:

`EXECUTE DBMS_SCHEDULER.PURGE_LOG( log_history => 5, which_log =>'JOB_LOG');`

Explanation:

Job entries can be purged from the job log without purging the window log entries. You can accomplish the required task by executing the following command:

```
EXECUTE DBMS_SCHEDULER.PURGE_LOG( log_history => 5, which_log =>
'JOB_LOG');
```

The option stating that the `EXECUTE DBMS_SCHEDULER.PURGE_LOG(log_history => 5, job_name => 'JOB1')` command will be used to purge the job log without purging the window log entries is incorrect. This is because the `DBMS_SCHEDULER.PURGE_LOG(log_history => 5, job_name => 'JOB1')` command is used to clear all the job entries related to `JOB1` and all the window log entries older than 5 days from the job log and the window log.

The option stating that the `EXECUTE DBMS_SCHEDULER.PURGE_LOG(log_history => 5, job_name=>'JOB_LOG')` command will be used to purge the job log without purging the window log entries is incorrect. This is because this command is used to clear all the job-specific entries from the job log with `JOB_LOG` as the name of the job instead of clearing all the job entries for the specified job name.

The option stating that you will use the `EXECUTE DBMS_SCHEDULER.PURGE_LOG( log_history => 5, which_log => 'JOB1')` command to purge the job log without purging the window log entries is incorrect because `'JOB1'` is the incorrect value for the which_log parameter. The correct value for the which_log parameter is `'WINDOW_LOG'`.

Item: 7 (Ref:1Z0-043.16.4.1)

You want to view the name of a program associated with a job for making some changes to the program. Which view will you query to find the name of the program associated with the job?

- DBA_SCHEDULER_JOB_RUN_DETAILS
- DBA_SCHEDULER_RUNNING_JOBS
- DBA_SCHEDULER_JOBS
- DBA_SCHEDULER_JOB_LOG

Answer:

DBA_SCHEDULER_JOBS

Explanation:

The DBA_SCHEDULER_JOBS view is used to view the name of the program associated with a job for making changes to the program. The DBA_SCHEDULER_JOBS view is used to view the information about the jobs in the database.

The option stating that the DBA_SCHEDULER_JOB_RUN_DETAILS view is used to view the name of the program associated with the job is incorrect. This is because the DBA_SCHEDULER_JOB_RUN_DETALS view is used to display the log run details of a particular job in the database.

The option stating that the DBA_SCHEDULER_RUNNING_JOBS view is used to view the program name associated with the job is incorrect. This is because the DBA_SCHEDULER_RUNNING_JOBS view is used to view information regarding the jobs that are currently running in the database.

The option stating that the DBA_SCHEDULER_JOB_LOG view is used to view the program name associated with the job is incorrect. This is because the DBA_SCHEDULER_JOB_LOG view can be used to view the log entries for previously executed jobs.

Item: 8 (Ref:1Z0-043.16.2.1)

You are creating a job class. You want access to the detailed information for all the runs of each job in the class and every operation performed on every job in the class.

Which setting will you use for the LOGGING_LEVEL parameter?

- LOGGING_OFF
- LOGGING_RUNS
- LOGGING_FULL
- LOGGING_NULL

Answer:

LOGGING_FULL

Explanation:

The Oracle Scheduler can maintain the job logs for all the activities. Job logging is determined by setting the LOGGING_LEVEL attribute of the job class. The LOGGING_LEVEL parameter specifies how much job information is logged. The three valid settings for this attribute are as follows:

- DBMS_SCHEDULER.LOGGING_OFF
- DBMS_SCHEDULER.LOGGING_RUNS
- DBMS_SCHEDULER.LOGGING_FULL

The DBMS_SCHEDULER.LOGGING_FULL setting for the LOGGING_LEVEL attribute specifies that the detailed information will be written for all the runs in each job in the class and every operation performed on any job in the class will be logged.

The option stating that the LOGGING_OFF setting for the LOGGING_LEVEL parameter specifies that the detailed information will be written in the job log for all the runs of each job in the class and that every operation performed on any job in the class will be logged is incorrect. This is because the LOGGING_OFF setting for the LOGGING_LEVEL attribute specifies that no logging will be performed for any job in the class.

The option stating that the LOGGING_RUNS setting for the LOGGING_LEVEL parameter specifies that the detailed information will be written in the job log for all the runs of each job in the class and that every operation performed on any job in the class will be logged is incorrect. This is because the LOGGING_RUNS setting for the LOGGING_LEVEL attribute specifies that detailed information will be written for all the runs of each job in the class but operations performed on any job in the class are not logged.

The option stating that the LOGGING_NULL setting for the LOGGING_LEVEL parameter specifies that the detailed information will be written in the job log for all the runs of each job in the class and that every operation performed on any job in the class will be logged is incorrect. This is because LOGGING_NULL is not a valid setting for the LOGGING_LEVEL parameter. Only the following three settings are valid for the LOGGING_LEVEL parameter:

- LOGGING_OFF
- LOGGING_RUNS
- LOGGING_FULL

Monitoring and Managing Storage

Item: 1 (Ref:1Z0-043.10.6.2)

You executed the following code:

```
SQL> CERATE TABLE COUNTRY
(COUNTRY_ID CHAR(2) CONSTRAINT COUNTRY_ID_nn NOT NULL,
COUNTRY_NAME VARCHAR2(20),
CURRENCY_NAME VARCHAR2(20),
CONSTRAINT COUNTRY_ID_PK PRIMARY KEY (COUNTRY_ID))
ORGANIZATION INDEX;
```

Which types of tables will be created automatically?

- journal table
- clustered table
- mapping table
- partitioned table

Answer:

mapping table

Explanation:

When you create an index-organized table, then a mapping table is automatically created in the tablespace in which the index-organized table is created. The mapping table stores logical rowids of the index-organized table (IOT). Each mapping table row stores one rowid for the corresponding rowid of the IOT.

The option, when you create an index-organized table, then a journal table is automatically created, is incorrect. The journal table is used to allow the users to access the existing index while performing the rebuild operation. When you move an index from one tablespace to another, you need to rebuild the index.

The option, when you create an index-organized table, then a clustered table is automatically created, is incorrect. The clustered table provides another alternative to the traditional, heap-organized table to provide performance benefits. A cluster consists of a group of two or more tables that share the same data blocks.

The option, when you create an index-organized table, then a partitioned table is automatically created, is incorrect. The partitioned table allows you to break your data into smaller pieces referred to as partitions. Each partition can be stored in its own segment and managed individually.

Item: 2 (Ref:1Z0-043.10.1.7)

The performance of your database is affected by the presence of two log members in each online redo log group and the placement of redo log members of a group on the same disk. You decide to place the redo log members of a group on separate disks.

Which view will you query to find the name and location of all the online redo log members?

- V$LOG
- V$LOGFILE
- DBA_LOG_GROUPS
- V$LOG_HISTORY

Answer:

V$LOGFILE

Explanation:

The V$LOGFILE view is used to identify the online redo log groups, the members of each group, and their status. The columns of the V$LOGFILE view are as follows:

- GROUP#: Displays the redo log group identifier number
- STATUS: Indicates the status of the log member:
- INVALID: - File is inaccessible
- STALE: - File's contents are incomplete
- DELETED: - File is no longer used
- Null: - File is in use
- TYPE: Displays the type of the logfile:
- ONLINE
- STANDBY
- MEMBER: Indicates the redo log member name
- IS_RECOVERY_DEST_FILE: Indicates whether the file was created in the flash recovery area (YES) or not (NO)

The V$LOGFILE view can be queried to find the filename, group number, and status of each redo log file. For example, to find all the files of group 1, you use the following query:

```
SELECT MEMBER FROM V$LOGFILE WHERE GROUP# = 1
```

You will not query the DBA_LOG_GROUPS view to identify the names and locations of all the online redo log members. The DBA_LOG_GROUPS view is used to display the log group definitions on all the tables in the database. The columns of the DBA_LOG_GROUPS view are as follows:

- OWNER: displays the owner of the log group definition
- LOG_GROUP_NAME: displays the name of the log group definition
- TABLE_NAME: displays the name of the table on which the log group is defined
- LOG_GROUP_TYPE: displays the following types of log group:

```
PRIMARY KEY LOGGING
UNIQUE KEY LOGGING
FOREIGN KEY LOGGING
ALL COLUMN LOGGING
USER LOG GROUP
```

  - ALWAYS: If the value is Y, then the log group is logged each time a row is updated. The value, N, indicates that the log group is logged each time a member column is updated.
- GENERATED: indicates whether the name of the supplemental log group is system generated (GENERATED NAME) or not (USER NAME)

You will not query the V$LOG_HISTORY view to identify the names and locations of all the online redo log members. The V$LOG_HISTORY view displays the log history information from the control file. The columns of the V$LOG_HISTORY view are as follows:

- RECID: displays the control file record ID
- STAMP: displays the control file record stamp
- THREAD#: displays the thread number of the archived log
- SEQUENCE#: displays the sequence number of the archived log
- FIRST_CHANGE#: displays the lowest system change number (SCN) in the log
- FIRST_TIME: displays the time of the first entry (lowest SCN) in the log
- NEXT_CHANGE#: displays the highest SCN in the log
- RESETLOGS_CHANGE#: displays the resetlogs change number of the database when the log was written
- RESETLOGS_TIME: displays the resetlogs time of the database when the log was written

Item: 3 (Ref:1Z0-043.10.6.4)

In which scenario will you create a hash cluster?

- when you want the data to be returned automatically in chronological order
- if the application uses queries joining tables only occasionally
- if the queries against the clustered table use the equality operator (=) to retrieve the desired row
- if the full table scan is executed often on only one of the clustered tables

Answer:

if the queries against the clustered table use the equality operator (=) to retrieve the desired row

---

Explanation:

If the queries against the clustered table use the equality operator (=) to retrieve the desired row, then you will create a hash cluster. A hash cluster uses the hashing algorithm on the row's cluster key to find the physical location of the row in the table. Hash clusters work best for queries that use the equality operator (=). The attributes of a table that make the table suitable for use in a hash cluster are as follows:

- The values in the index column of the table in the cluster should be uniformly distributed.
- The tables should have little or no insert, update, or delete operations performed on them.
- The tables in the cluster should have a predictable number of values in the index column.
- The queries against the clustered table should use the equality operator (=) to retrieve the desired row.

The option stating that when you want the data to be returned automatically in the chronological order is incorrect. When you want the data to be returned automatically in the chronological order, then you will use the sorted hash cluster. The sorted hash cluster is introduced in Oracle10*g*. Sorted hash clusters extend the functionality of hash clusters of previous versions of Oracle by maintaining a sort order for rows that are retrieved by the same cluster key. In traditional heap organized tables and hash clusters, rows are not returned in a sorted order. In sorted hash clusters for each hash cluster key, Oracle maintains a list of rows sorted by one or more sort columns.

The option stating that if the application uses queries joining tables only occasionally, then you will create hash clusters is incorrect. If the application uses queries joining tables occasionally or modifies their common values frequently, then you should not use the clusters. Modifying a row's cluster key value takes longer than modifying the value in an unclustered table because Oracle might need to migrate the modified row to another block to maintain the cluster.

The option stating that if the full table scan is executed often on only one table of the clustered tables then you should create a hash cluster is incorrect. If a full table scan is executed often on only one table of the clustered tables, then you should not use clusters. This table is stored on more blocks than if it had been created alone.

Item: 4 (Ref:1Z0-043.10.7.3)

You are a DBA of your company. You created a database named SALES on an Oracle 10*g* instance. You have defined an index named INDEX1 on the database table named INVENTORY.

Users are complaining that queries accessing the INVENTORY table are running slow. Upon investigation you determine that the tablespace where the index is located is experiencing high I/O and you decide to relocate the index to another tablespace.

Which of these will be the best way to accomplish this objective?

- Rebuild the index.
- Coalesce the index.
- Drop and re-create the index in the new tablespace.
- Relocate the index using the ALTER INDEX...MOVE statement.

Answer:

Rebuild the index.

Explanation:

You must rebuild the index to relocate the index to another tablespace. Indexes can be rebuilt to improve the performance of queries, to move indexes from one tablespace to another, and to change the storage options of an index. To rebuild the INDEX1 index, you would use the ALTER INDEX INDEX1 REBUILD statement. To rebuild an index in your database, you use the following syntax:

```
ALTER INDEX index_name REBUILD;
```

Coalescing the index will not achieve the objective of relocating the index to a different tablespace. Coalescing of an index reduces fragmentation within the index. Coalescing cannot be used to relocate an index to a different tablespace. To coalesce an index in your database, you use the following syntax:

```
ALTER INDEX index_name COALESCE;
```

Dropping the index and re-creating it in the new tablespace will not be the best option because you will need to completely remove and re-create the index. A rebuild is preferable in this case as you only need to specify the other tablespace name in the statement and the index can be used when it is being rebuilt. If you drop the index, database users will not be able to access the index until it is re-created in the other tablespace.

The index cannot be relocated using the ALTER INDEX...MOVE statement. This option is invalid. The ALTER TABLE...MOVE statement is used to move a table from one tablespace to another.

Item: 5 (Ref:1Z0-043.10.2.1)

You issued the following statement:

```
SQL>ALTER DATABASE ENABLE RESUMABLE TIMEOUT n;
```

What will be the result of issuing the above statement?

- The command will not execute successfully because TIMEOUT is an invalid clause with the ALTER DATABASE ENABLE RESUMABLE command.
- The command will not execute successfully because resumable space allocation is enabled at the session level.
- The command will execute successfully and resumable space will be allocated at the session level.
- The command will execute successfully and resumable space will be allocated at the instance level.

Answer:

The command will not execute successfully because resumable space allocation is enabled at the session level.

Explanation:

The command will not execute successfully because resumable space allocation is enabled at the session level. The ALTER DATABASE ENABLE RESUMABLE TIMEOUT n command is an invalid command. Resumable Space Allocation allows you to suspend and resume the execution of large database operations that fail due to errors associated with space limits and out-of-space conditions. Resumable Space Allocation is enabled by issuing the ALTER SESSION ENABLE RESUMABLE[TIMEOUT timeout][NAME name]; command.

The option stating that the ALTER DATABASE ENABLE RESUMABLE TIMEOUT n command will not execute successfully because TIMEOUT is an invalid clause with the ALTER DATABASE ENABLE RESUMABLE command is incorrect. The command will not execute because the Resumable Space Allocation is enabled at the session level. The ALTER DATABASE ENABLE RESUMABE command is an invalid command. The TIMEOUT clause is not an invalid clause, but the clause is used with the ALTER SESSION ENABLE RESUMABLE command. The TIMEOUT clause specifies the time duration for which the session is suspended.

The option stating that the command will execute successfully and resumable space will be allocated at the session level is incorrect. The resumable space is allocated at the session level by using the ALTER SESSION ENABLE RESUMABLE command.

The option stating that the command will execute successfully and the resumable space will be allocated at the instance level is incorrect. To enable Resumable Space Allocation at the instance level, you must specify a nonzero value for the RESUMABE_TIMEOUT initialization parameter in the initialization parameter file.

Item: 6 (Ref:1Z0-043.10.6.3)

You executed the following code:

```
SQL> CREATE TABLE COUNTRY
(COUNTRY_ID CHAR(2) CONSTRAINT COUNTRY_ID_nn NOT NULL,
COUNTRY_NAME VARCHAR2(20),
CURRENCY_NAME VARCHAR2(20),
CONSTRAINT COUNTRY_ID_PK PRIMARY KEY (COUNTRY_ID))
ORGANIZATION INDEX;
```

In which tablespace will the mapping table be created?

- SYSTEM tablespace
- SYSAUX tablespace
- Undo tablespace
- The tablespace of the Index Organized Table (IOT)

Answer:

The tablespace of the Index Organized Table (IOT)

Explanation:

The mapping table will be created in the tablespace of the IOT. A bitmap index on an IOT is similar to a bitmap index on a heap organized table, except that the rowids used in the bitmap index on an IOT are those of a mapping table as opposed to the base table and the mapping table is used by all the bitmap indexes created on that IOT.

The options stating that the mapping table is created in the SYSTEM tablespace is incorrect. The SYSTEM tablespace contains the fixed tables that are critical for the database,

the option stating that the mapping table is created in the SYSAUX tablespace is incorrect. The SYSAUX tablespace is an auxiliary tablespace to the SYSTEM tablespace.

The option stating that the mapping table is created in the Undo tablespace is incorrect. The Undo tablespace contains undo segments. The mapping table is created in the tablespace of the IOT.

Item: 7 (Ref:1Z0-043.10.4.2)

You are performing the shrink operation on the SCOTT.EMP table. You want to perform the same operation on all dependent objects of the SCOTT.EMP table.

What is **NOT** a prerequisite for the operation?

- You must enable the row movement on the SCOTT.EMP table.
- You must define the tablespace of the SCOTT.EMP table for automatic segment space management.
- You must use the CASCADE clause in the ALTER TABLE SHRINK SPACE statement.
- You must use the COMPACT clause in the ALTER TABLE SHRINK SPACE statement.

Answer:

You must use the COMPACT clause in the ALTER TABLE SHRINK SPACE statement.

Explanation:

If you want to perform the shrink operation on the dependent objects of the SCOTT.EMP table, it is not necessary to use the COMPACT clause in the ALTER TABLE SHRINK SPACE statement for the shrinking operation. If the COMPACT clause is not specified, the segment space is made compact and at the end of the compaction phase, the HWM is adjusted and the unused space is released.

The option stating that you need not enable the row movement on the SCOTT.EMP table for the shrink operation is incorrect. The shrink operation may cause ROWIDs to change in heap-organized tables. You must enable the row movement on the corresponding segment before executing the shrink operation. To enable the row movement on the SCOTT.EMP table, the ALTER TABLE ENABLE ROW MOVEMENT statement is issued.

You must use the CASCADE clause in the ALTER TABLE SHRINK SPACE statement. If you want to perform the same operation on all the dependent objects of the SCOTT.EMP table, then you will issue the ALTER TABLE SCOTT.EMP SHRINK SPACE CASCADE statement. If CASCADE is specified, then shrink behavior is cascaded to all the dependent segments that support a shrink operation, except materialized views, LOB indexes, IOT mapping tables, and overflow tables.

The option stating that for shrink operation on the table SCOTT.EMP, you need not define the tablespace of the SCOTT.EMP table for automatic segment space management is incorrect. You must define the tablespace of the SCOTT.EMP table for automatic segment space management. Segment shrink operations have one major restriction. Segments managed using freelists cannot be shrunk. As a result, the tablespace containing the segments must be defined with automatic segment space management.

Item: 8 (Ref:1Z0-043.10.4.3)

You issued the following command:

```
ALTER TABLE SCOTT.EMP SHRINK SPACE;
```

The SCOTT.EMP table is stored in the DATA1 tablespace that has the following properties:

DATA1 is a read/write tablespace.
DATA1 is not autoextensible to an unlimited size.
DATA1 is online.
Segment space management for the DATA1 tablespace is manual.

You issued the ALTER TABLE SCOTT.EMP SHRINK SPACE; command that generates the following error:

```
ORA-10635: Invalid segment or tablespace type
```

What could be the reason for the failure of the command?

- The tablespace, DATA1, is not read-only.
- The tablespace, DATA1, is not autoextensible.
- The tablespace, DATA1, is not offline.
- The segment space management for the tablespace, DATA1, is manual.

Answer:

The segment space management for the tablespace, DATA1, is manual.

Explanation:

You have received the ORA-10635: Invalid segment or tablespace type error because the segment space management of the DATA1 tablespace is manual. For the shrink operation, the segment must be stored in an automatic, segment space-managed tablespace. You can specify automatic segment space management in a tablespace that is permanent and locally managed. Automatic segment space management is an efficient way to manage the space within a segment. If you specify automatic segment space management for a tablespace, then you need not specify the PCTUSED, FREELISTS, and FREELIST GROUPS storage parameters for the objects created in the tablespace.

The option stating that the reason for the command failure is that the tablespace, DATA1, is not read-only is incorrect. This is because it is not necessary to make the tablespace read-only at the location where you store the segment. The purpose of making the tablespaces read-only is to eliminate the need to perform the backup and recovery of large sections of the database. Oracle never updates the datafiles of the read-only tablespaces.

The option stating that the reason for the command failure is that the tablespace, DATA1, is not autoextensible is incorrect. This is because it is not necessary to make the tablespace autoextensible at the location where the segment is stored. If you make a datafile autoextensible during tablespace creation, then the database increases the size of the datafile by 100MB or by the size of the file itself.

The option stating that the reason for the command failure is that the tablespace, DATA1, is not offline is incorrect. This is because it is not necessary to make the tablespace offline at the location where the segment is stored. If a tablespace goes offline, then Oracle does not permit you to issue the SQL statements that are referenced to the objects within the tablespace.

Item: 9 (Ref:1Z0-043.10.6.7)

You are creating a cluster. The tables in the cluster have a relatively uniform distribution of values in the index column and the queries against the clustered table will almost use an equality operator to retrieve the desired row.

Which type of cluster will you create?

- Index cluster
- Hash cluster
- Sorted Hash cluster
- Real Application Cluster

Answer:

Hash cluster

Explanation:

You will create a hash cluster. A hash cluster uses the hashing algorithm on the row's cluster key to find the physical location of the row in the table. Hash clusters work best for queries that use the equality operator (=). The attributes of a table that makes the table suitable for use in a hash cluster are:

- The values in the index column of the table in the cluster should be uniformly distributed.
- The tables should have little or no insert, update, or delete operations performed on them.
- The tables in the cluster should have a predictable number of values in the index column.
- The queries against the clustered table should use the equality operator (=) to retrieve the desired row.

The option stating that you will create an index cluster is incorrect. An index cluster functions like a B-tree index to ensure quick access to the rows in a cluster table. The attributes of a table that makes the table suitable for use in an index cluster are as follows:

- The tables in a cluster will always be queried together.
- The tables should have little or no insert, update, or delete operations performed on them.

The option stating that you will create a sorted hash cluster is incorrect. The sorted hash cluster is introduced in Oracle10*g*. Sorted hash clusters extend the functionality of hash clusters of previous versions of Oracle by maintaining a sort order for rows that are retrieved by the same cluster key. In traditional heap organized tables and hash clusters, rows are not returned in a sorted order. In sorted hash clusters for each hash cluster key, Oracle maintains a list of rows sorted by one or more sort columns.

The option stating that you will create Real Application Cluster is incorrect. Oracle Real Application Cluster is a cluster database that contains a shared cache architecture and provides the highest availability and scalability of a database.

Item: 10 (Ref:1Z0-043.10.1.6)

You are maintaining your database in Oracle10*g*. You have set the value of the STATISTICS_LEVEL initialization parameter to TYPICAL and the value of the FAST_START_MTTR_TARGET parameter to 900 seconds. To increase the performance of the database, you want to determine the log file size that should equal the minimum size of all the online redo log files.

Which column will enable you to perform the desired task?

- the WRITES_LOGFILE_SIZE column of the V$INSTANCE_RECOVERY view
- the column of the V$INSTANCE_RECOVERY view
- the OPTIMAL_LOGFILE_SIZE column of the V$INSTANCE_RECOVERY view
- the LOG_FILE_SIZE_REDO_BLKS column of the V$INSTANCE_RECOVERY view

Answer:

the OPTIMAL_LOGFILE_SIZE column of the V$INSTANCE_RECOVERY view

---

Explanation:

The OPTIMAL_LOGFILE_SIZE column value displays, in megabytes, the redo log file size that is considered optimal based on the current setting of the FAST_START_MTTR_TARGET initialization parameter. It is recommended that you should configure the redo log file size of all online redo log files to at least the value of the OPTIMAL_LOGFILE_SIZE column. For example, the OPTIMAL_LOGFILE_SIZE view displays the required size of 49 MB.

```
SQL> SELECT OPTIMAL_LOGFILE_SIZE FROM V$INSTANCE_RECOVERY;

OPTIMAL_ LOGFILE_SIZE
---------------------
49
1 row selected.
```

The option stating that you can determine the redo log file size that should equal the minimum size of all the online redo log files by viewing the WRITES_LOGFILE_SIZE column value of the V$INSTANCE_RECOVERY view is incorrect. The WRITES_LOGFILE_SIZE column value displays the number of writes written by the smallest redo log file size.

The option stating that you can determine the redo log file size that should equal the minimum size of all the online redo log files by viewing the TARGET_REDO_BLKS column value of the V$INSTANCE_RECOVERY view is incorrect. The TARGET_REDO_BLKS column value displays the current target number of redo blocks that must be processed for recovery.

The option stating that you can determine the redo log file size that should equal the minimum size of all the online redo log files by viewing the LOG_FILE_SIZE_REDO_BLKS column value of the V$INSTANCE_RECOVERY view is incorrect. The LOG_FILE_SIZE_REDO_BLOKS column value displays the maximum number of redo blocks required to guarantee that a log switch does not occur before the checkpoint is completed.

Item: 11 (Ref:1Z0-043.10.4.1)

You are shrinking the SCOTT.EMP table by executing the ALTER TABLE SCOTT.EMP SHRINK SPACE CASCADE statement. What is a prerequisite for shrinking the SCOTT.EMP table?

- You must enable the block change tracking feature.
- You must have enable the flashback feature.
- You must use the OMF in your database.
- You must define the tablespace of the SCOTT.EMP table for automatic segment space management.

Answer:

You must define the tablespace of the SCOTT.EMP table for automatic segment space management.

Explanation:

You must define the tablespace of the SCOTT.EMP table for automatic segment space management. Segment shrink operations have one major restriction. Segments managed using freelists cannot be shrunk. As a result, the tablespace containing the segment must be defined with automatic segment space management.

The option stating that you must enable the block change tracking feature for a shrinking operation is incorrect. Block change tracking is a new capability in Oracle 10*g*. The block change tracking process records the blocks modified since the last backup and stores them in a block change tracking file. RMAN uses this file to determine the blocks that were backed up in the incremental backup. This improves the performance because RMAN does not have to scan the entire datafile during the backup. The block change writer CTWR process is a new background process responsible for writing data to the block change-tracking file

The option stating that you must have flashback feature enabled in your database to perform the shrinking operation is incorrect. Flashback Technologies were first developed in Oracle9*i* after which the Flashback Query was introduced. In Oracle10*g*, there has been a significant extension of this technology. Flashback technology consists of the following features:

- Flashback Database
- Flashback Drop
- Flashback Version Query
- Flashback Transaction Query
- Flashback Table

The option stating that you must use OMF in your database to perform a shrinking operation is incorrect. OMF is used to specify the default locations of the datafiles, control files, and online redo log files. If OMF is configured in your database and you do not specify the names and sizes of the datafiles during tablespace creation, then Oracle automatically assigns names and sizes to the datafiles associated with that tablespace and stores them in the location specified by the DB_CREATE_FILE_DEST parameter. The DB_CREATE_ONLINE_LOG_DEST_n parameter is used to specify the default locations of the online redo log files and the control files.

Item: 12 (Ref:1Z0-043.10.3.2)

Your database block size is 4 KB. In this database, you are required to create a tablespace with a block size of 8 KB.

Which is the prerequisite for creating this tablespace?

- The parameter DB_CACHE_SIZE must be a multiple of 8.
- The value of the parameter SGA_MAX_SIZE must be increased.
- The tablespace must be created with a uniform extent size of 8 KB.
- The parameter DB_8K_CACHE_SIZE must be defined in the parameter file.

Answer:

The parameter DB_8K_CACHE_SIZE must be defined in the parameter file.

Explanation:

If you want to create a tablespace with a non-standard block size, you must have set the parameter DB_nK_CACHE_SIZE in the parameter file, where n is the block size. In this scenario, if you want to create an 8 KB block size tablespace, you must have defined DB_8K_CACHE_SIZE parameter in the parameter file.

It is not necessary that the DB_CACHE_SIZE parameter be a multiple of 8 to create a tablespace with an 8 KB block size. A non-standard block size tablespace can be created by specifying a buffer cache for the non-standard block size. For example, if you want to create a tablespace with block size 16k and the standard block size if 4k, you must define a non-standard block size cache by specifying the DB_16K_CACHE_SIZE parameter.

It is not necessary to increase the value of the SGA_MAX_SIZE parameter to create a tablespace with an 8KB block size. The value of the SGA_MAX_SIZE parameter should be increased when the SGA is not big enough to accommodate all its memory components.

It is not necessary that the tablespace be created with a uniform extent size of 8 KB to create a tablespace with an 8 KB block size. The size of the tablespace does not affect the creation of non-standard block size tablespace.

Item: 13 (Ref:1Z0-043.10.1.9)

The configuration of the online redo log files is as follows:

Group1	'ora01/oradata/redo01a.log'
	'ora02/oradata/redo01b.log'
Group2	'ora01/oradata/redo02a.log'
	'ora02/oradata/redo02b.log'

Based on this configuration, which statement is true?

- The LGWR process concurrently writes the redo log entries to both the members of a group.
- When a member of a group becomes corrupt, the database crashes.
- The sizes of the redo01a.log and redo01b.log online redo log members of group Group1 can be different.
- When redo02a.log and redo02b.log files become corrupt, then the database operations will proceed as normal.

Answer:

The LGWR process concurrently writes the redo log entries to both the members of a group.

Explanation:

According to the table given in the question, the online redo log groups, Group1 and Group2, are multiplexed in your database. When online redo log groups are multiplexed, then the LGWR process concurrently writes the same redo log information to multiple identical online redo log files. While multiplexing the online redo log files, it is advised that you keep the members of a group on different disks to ensure that one disk failure will not affect the ongoing operation of the database.

The option stating that when a member of a group becomes corrupt, the database will crash is incorrect. If the LGWR process can write to at least one member of the group, the database operation proceeds as normal and an entry is written to the alert log file.

The option stating that the sizes of the redo01a.log and redo01b.log members of the group, Group1, can be different is incorrect. This is because the redo01a.log and redo01b.log files are the members of the online redo log group Group1. The online redo log group, Group1, is multiplexed. To multiplex the redo log groups, the size of each redo log member in a redo log group should be same.

The option stating that when redo02a.log and redo02b.log files become corrupt, the database operations will proceed as normal is incorrect. When all the members of an online redo group are corrupt, the database will hang.

Item: 14 (Ref:1Z0-043.10.7.2)

You moved the index EMP_NO_INDX from one tablespace to another and then issued the following command to rebuild the index EMP_NO_INDX:

```
SQL> ALTER INDEX EMP_NO_INDX REBUILD ONLINE;
```

Which table allows the users to access the EMP_NO_INDX index while performing the rebuild operation?

- Index-organized table
- Mapping Table
- Clustered Table
- Journal Table

Answer:

Journal Table

Explanation:

The journal table allows the users to access the existing index while performing the rebuild operation. When you move an index from one tablespace to another, you need to rebuild the index. In this scenario, you are using the ONLINE keyword, therefore the current index is left intact while a new copy of the index is built, allowing the users to access the old index with SELECT statements or other DML statements. Any changes to the old index are saved in a special table known as journal table. After the index is rebuilt, the changes recorded in the journal table are merged to the new index. Once the merge operation is complete, the data dictionary is updated and the old index is dropped. The index is available nearly 100 percent of the time that the rebuild operation is in progress.

The option stating that the index-organized table allows the users to access the index while performing the rebuild operation is incorrect. An index-organized table (IOT) is different from traditional heap-organized table. An index-organized table is a special type of table in which data is stored in a B-tree structure in a sorted order based on primary key values, whereas data in a heap-organized table is unordered. Index-organized tables are mostly used in OLTP which requires fast access of primary key.

The option stating that the mapping table allows the users to access the index while performing the rebuild operation is incorrect. The mapping table stores logical rowids of the index-organized table (IOT). Each mapping table row stores one rowid for the corresponding rowid of the IOT.

The option stating that the clustered table is responsible for allowing the users to access the index while performing the rebuild operation is incorrect. The clustered table provides another alternative to the traditional heap-organized table to provide performance benefits. A cluster consists of a group of two or more tables that share the same data blocks.

Item: 15 (Ref:1Z0-043.10.6.5)

In which scenario will you create a sorted hash cluster?

- if the application uses queries joining tables only occasionally
- if the full table scan is executed often on only one table of the clustered tables
- if the data for all the rows of a cluster key value exceeds one or two Oracle blocks
- when you want the data to be returned automatically in the chronological order

Answer:

when you want the data to be returned automatically in the chronological order

---

Explanation:

When you want the data to be returned automatically in the chronological order, then you will create a sorted hash cluster. The sorted hash cluster is introduced in Oracle10*g*. Sorted hash clusters extend the functionality of hash clusters of previous versions of Oracle by maintaining a sort order for rows that are retrieved by the same cluster key. In traditional, heap organized tables and hash clusters, rows are not returned in a sorted order. In sorted hash clusters for each hash cluster key, Oracle maintains a list of rows sorted by one or more sort columns.

The option stating that if the application uses queries joining tables only occasionally, then you will create a sorted hash cluster is incorrect. If the application uses queries joining tables occasionally or modifies their common values frequently, then you should not use the clusters. Modifying a row's cluster key value takes longer than modifying a value in an unclustered table. This is because Oracle might be required to migrate the modified row to another block to maintain the cluster.

The option stating that if the full table scan is executed often only on one table of the clustered tables, then you should create a sorted hash cluster is incorrect. If a full table scan is executed often on only one table of the clustered tables, then you should not use clusters. This table is stored on more blocks than if it had been created alone.

The option stating that if the data for all the rows of a cluster key value exceeds one or two Oracle blocks, then you should create the sorted hash cluster is incorrect. If the data for all the rows of a cluster key value exceeds one or two Oracle blocks, then you should not use the clusters. To access an individual row in a clustered key table, the Oracle server reads all blocks containing rows with the same value.

Item: 16 (Ref:1Z0-043.10.1.5)

You are maintaining your database in Oracle10*g*. You have set the value of the STATISTICS_LEVEL initialization parameter to TYPICAL and the value of the FAST_START_MTTR_TARGET parameter to 900 seconds. To increase the performance of the database, you want to determine the optimal size of the online redo log files.

Which tool enables you to determine the optimal size of the online redo log files?

- Oracle Enterprise Manager
- The V$LOG view
- The V$LOGFILE view
- The V$FLASHBACK_DATABASE_LOGS view

Answer:

Oracle Enterprise Manager

Explanation:

You can use Oracle Enterprise Manager to determine the optimal size of the online redo log files.
It is recommended that you configure the redo log file size of all the online redo log files to at least the optimal redo log file size.
To determine the optimal size of the online redo log files by using Oracle Enterprise Manager, perform the following steps:

1. Open the Redo Log Groups screen.
2. In the Actions drop-down list on the right, select Sizing Advice.
3. Click the Go button to display the recommendation for the redo log file size that coincidentally corresponds to the information obtained from the V$INSTANCE_RECOVERY view.

The option stating that the V$LOG view is used to retrieve the optimal log file size is incorrect. The V$LOG view displays the redo log file information. The V$LOG view displays information regarding the redo log group number, log sequence number, number of members in the group, and so on. For example, you can execute the following query to find the status of the redo log groups:

```
SELECT STATUS FROM V$LOG;
```

The common values for the STATUS column are as follows:

- UNUSED: indicates that redo log entries are never written to this group
- CURRENT: indicates that this is the active group
- ACTIVE: indicates that information regarding redo log entries is written to the log that has an ACTIVE status and that this log group is required for instance recovery
- INACTIVE: indicates that information about redo log entries is written to the log that has an INACTIVE status and that this log group is not required for instance recovery

The option stating that the V$LOGFILE view is used to retrieve the optimal log file size is incorrect. The V$LOGFILE view can be queried to find the file names, group numbers, and status of redo log files. For example, to find all files of group 1, you use the following syntax:

```
SELECT MEMBER FROM V$LOGFILE WHERE GROUP# = 1
```

The option stating that the V$FLASHBACK_DATABASE_LOG view is used to retrieve the optimal log file size is incorrect. The V$FLASHBACK_DATABASE_LOG view is used to determine the estimated size of the flashback data that you require for your current target retention. The V$FLASHBACK_DATABASE_LOG view was introduced in Oracle 10*g* to support the Flashback Database feature. The V$FLASHBACK_DATABASE_LOG view allows you to determine the space required in the recovery area to support the flashback activity generated by the changes in the database. The ESTIMATED_FLASHBACK_SIZE column is used to identify the estimated size of the flashback data that you require for your current target retention.

Item: 17 (Ref:1Z0-043.10.2.4)

You set the RESUMABLE_TIMEOUT initialization parameter to a value of 1800 in the server initialization parameter file.

Another DBA issues the following statement:

```
SQL>ALTER SYSTEM SET RESUMABLE_TIMEOUT = 0;
```

What is the result of this statement?

- The statement returns an error.
- The Resumable Space Allocation feature is disabled for all the sessions in the database.
- The Resumable Space Allocation feature is disabled for only the session that belongs to the other DBA.
- The statement is ignored, and the RESUMABLE_TIMEOUT initialization parameter is not altered.

Answer:

The Resumable Space Allocation feature is disabled for all the sessions in the database.

Explanation:

If you issue the following statement, the Resumable Space Allocation feature is disabled for all the sessions in the database:

```
SQL>ALTER SYSTEM SET RESUMABLE_TIMEOUT = 0;
```

Dynamically setting the RESUMABLE_TIME initialization parameter to zero disables the Resumable Space Allocation feature for all the database sessions.

The option stating that the statement returns an error is incorrect because no error is returned to the user. The Resumable Space Allocation feature will be disabled as a result of this ALTER SYSTEM SET statement.

The option stating that the Resumable Space Allocation feature is disabled only for the session that belongs to the other DBA is incorrect because the Resumable Space Allocation feature is disabled for all the sessions in the database, not just for the session belonging to the other DBA.

The option stating that the statement is ignored and the RESUMABLE_TIMEOUT initialization parameter is not altered is incorrect. This ALTER SYSTEM SET statement changes the value of the RESUMABLE_TIMEOUT initialization parameter in the server initialization parameter file

Item: 18 (Ref:1Z0-043.10.1.4)

You are maintaining your OLTP database in Oracle10*g*. While observing the performance of the database, you find that the log switch occurs more than once for every 20 minutes, affecting the database performance.

Which factor is responsible for frequent log switches?

- the value of the UNDO_RETENTION initialization parameter
- the value of the optimal redo log file size provided by the Redo Logfile Size Advisor
- the online redo log files size
- the number of redo log members in a group

Answer:

the online redo log files size

Explanation:

The sizes of the online redo groups are responsible for frequent log switches. The LGWR process writes redo log entries from the redo log buffer to the online redo log files. There are two or more online redo log groups in the database. If a redo log file is full, the LGWR process starts writing redo log entries to the next available redo log file. This event is called log switch. If the size of the online redo log group is large, then the log switch event will occur less frequently. If the size of the online redo log group is small, then the log switch event will occur more frequently.

The option stating that the value of the UNDO_RETENTION initialization parameter is responsible for frequent log switches is incorrect. The UNDO_RETENTION parameter is used to specify the minimum amount of time for which the undo data will be retained in the undo segments.

The option stating that the value of the optimal redo log file size provided by the Redo Logfile Size Advisor is responsible for frequent log switches is incorrect. The optimal redo log file size is displayed by the value in the OPTIMAL_LOGFILE_SIZE column of the V$INSTANCE_RECOVERY view. It is recommended that you configure the size of redo log files to at least the value displayed in the OPTIMAL_LOGFILE_SIZE parameter.

The option stating that the number of the redo log members in a group is responsible for frequent log switches is incorrect. The log switch depends on the redo log file size and not on the number of members in a redo log group.

Item: 19 (Ref:1Z0-043.10.1.2)

This is the online redo log files and the control file configurations:

Redo log files:

Group1	'/disk1/oradata/redo01a.log'
	'/disk1/oradata/redo01b.log'
Group2	'/disk2/oradata/redo02a.log'
	'/disk2/oradata/redo02b.log'

Control files:

'/disk1/oradata/control01.ctl'
'/disk2/oradata/control02.ctl'

Based on these configurations, which statement is true?

- Both the control files and the online redo log files are configured properly.
- The control files are configured properly, but the online redo log files are not configured properly.
- The online redo log files are configured properly, but the control files are not configured properly.
- Neither the control files nor the online redo log files are configured properly.

Answer:

The control files are configured properly, but the online redo log files are not configured properly.

Explanation:

In the given scenario, the control files are configured properly, but the online redo log files are not configured properly. Maintaining identical copies of the online redo log files or the control files is called multiplexing. While multiplexing, you should place identical copies of the online redo log files or the control files on different disks. If identical copies of the control file or the redo log file are on the same disk, then the performance of the database is degraded. In the given scenario, the identical copies of the control file are placed on different disks; therefore, the control file is multiplexed properly. Identical copies of the online redo log files are placed on the same disk; therefore, the online redo log files are not multiplexed properly.

The option stating that both the control files and the online redo log files are configured properly is incorrect. The control files are configured properly, but the online redo log files are not configured properly. Identical copies of the online redo log files are placed on the same disk, degrading the performance of the database.

The option stating that the online redo log files are configured properly, but the control files are not configured properly is incorrect. The control files are configured properly because an identical copy of the control file is placed on a different disk. The online redo log files are not configured properly because the identical copies of the online redo log files are placed on the same disk, degrading the performance of the database.

The option stating that neither the control files nor the online redo log files are configured properly is incorrect. The control files are configured properly, but the redo log file are not configured properly.

Item: 20 (Ref:1Z0-043.10.4.4)

You created the DEPT table by using the following command:

```
CREATE TABLE scott.dept
(deptno NUMBER(3),
dname VARCHAR2(15),
loc VARCHAR2(15) )
STORAGE (INITIAL 100K NEXT 50K
MAXEXTENTS 10 PCTINCREASE 5
FREELIST GROUPS 6 FREELISTS 4);
```

You are required to shrink the DEPT table. While performing the shrink operation, you want to ensure that the recovered space is returned to the tablespace in which the DEPT table is stored. You do not want to shrink the indexes created on the DEPT table.

What will you do to shrink the SCOTT.EMP table?

- Issue the ALTER TABLE SCOTT.DEPT SHRINK SPACE COMPACT; statement.
- Issue the ALTER TABLE SCOTT.DEPT SHRINK SPACE; statement.
- Issue the ALTER TABLE SCOTT.DEPT SHRINK SPACE CASCADE; statement.
- You cannot shrink the SCOTT.EMP table.

Answer:

You cannot shrink the SCOTT.EMP table.

Explanation:

In this scenario, you cannot shrink the SCOTT.DEPT table because the table with the freelist cannot be shrunk. Segment shrink operations have one major restriction. Segments managed using freelists cannot be shrunk. As a result, the tablespace containing the segment must be defined with automatic segment space management.

The option stating that the ALTER TABLE SCOTT.DEPT SHRINK SPACE COMPACT; command can be used to shrink the SCOTT.DEPT table is incorrect. This is because the SCOTT.DEPT table is managed using freelists and the segments managed using freelists cannot be shrunk by a shrink operation. A shrink operation of an automatic segment space managed table can be split into commands by using the following COMPACT clause to compress the rows without moving the high water mark:

```
ALTER TABLE table_name SHRINK SPACE COMPACT;
```

Later, when the database is slightly unoccupied, you can complete the rest of the operation by omitting the following COMPACT clause:

```
ALTER TABLE table_name SHRINK SPACE;
```

The option stating that the ALTER TABLE SCOTT.DEPT SHRINK SPACE; command can be used to shrink the SCOTT.DEPT table is incorrect. This is because the SCOTT.DEPT table is managed using freelists and the segments managed using freelists cannot be shrunk by a shrink operation. The ALTER TABLE table_name SHRINK SPACE; command can be used only with tables on which automatic segment space management is performed.

The option stating that the ALTER TABLE SCOTT.DEPT SHRINK SPACE CASCADE; command can be used to shrink the SCOTT.DEPT table is incorrect. This is because the SCOTT.DEPT table is managed using freelists and the segments managed using freelists cannot be shrunk by a shrink operation. The ALTER TABLE table_name SHRINK SPACE CASCADE; command can only be used with tables on which automatic segment space management is performed. The CASCADE clause in the ALTER TABLE table_name SHRINK SPACE command specifies that the dependent objects of the table will be automatically shrunk while performing a shrink operation on the table.

Item: 21 (Ref:1Z0-043.10.5.2)

You are using Oracle Enterprise Manager to estimate the size of a table to be created. You have typed data regarding the column names, data types, sizes of the columns, and the projected number of rows in the table.

Which additional information does the Oracle Enterprise Manager return?

- space allocated in the tablespace
- space required for the bitmap index on a column of the table
- space remaining in the tablespace after creating the table
- estimated value of the PCTFREE storage parameter

Answer:

space allocated in the tablespace

Explanation:

When you type the required information, such as data about the column names, data types, sizes of the columns, and the projected number of rows in the table, regarding the table to be created and click on the Estimate Table Size button in the Create Table page, the Oracle Enterprise Manager returns the estimated size of the table and the corresponding space allocated in the tablespace.

The other three options stating that the Oracle Enterprise Manager returns the space required for the bitmap index on a column of the table, the space remaining in the tablespace after creating the table, and the estimated value of PCTFREE storage parameter are incorrect. This is because Oracle Enterprise Manager returns only the estimated size of the table to be created and the corresponding space allocated in the tablespace.

Item: 22 (Ref:1Z0-043.10.2.2)

You discover an out-of-space condition in the database. You decide to suspend a session for five minutes. You issue the following command to suspend the session:

```
ALTER SESSION ENABLE RESUMABLE;
```

Which command could you issue to enable the resumable space allocation feature at the session level?

- `ALTER SESSION ENABLE RESUMABLE_TIMEOUT = 5;`
- `ALTER SYSTEM ENABLE RESUMABLE_TIMEOUT = 5;`
- `ALTER SESSION ENABLE RESUMABLE_TIMEOUT = 300;`
- `ALTER SYSTEM ENABLE RESUMABLE TIMEOUT = 300;`

Answer:

`ALTER SESSION ENABLE RESUMABLE_TIMEOUT = 300;`

Explanation:

You can issue the `ALTER SESSION ENABLE RESUMABLE_TIMEOUT = 300` command to specify the duration for which a session will be suspended. The duration for which a session will be suspended is specified in seconds. No changes can be made to the database using a suspended session.

The `ALTER SESSION ENABLE RESUMABLE TIMEOUT = 5` command will suspend a session for five seconds.

The `ALTER SYSTEM ENABLE RESUMABLE TIMEOUT = 5` command will suspend all the database sessions for five seconds. No user session can make changes in the database during these five seconds.

The `ALTER SYSTEM ENABLE RESUMABLE TIMEOUT = 300` command will suspend all the database sessions for five minutes. No user session can make changes in the database during these 5 minutes.

Item: 23 (Ref:1Z0-043.10.6.1)

You issued the following statement to monitor the usage of the index:

```
SQL> ALTER INDEX SCOTT.EMP_IDX MONITORING USAGE;
```

Which view will you query to ensure that the index is being monitored?

- INDEX_STATS
- DBA_INDEXES
- DBA_IND_COLUMNS
- V$OBJECT_USAGE

Answer:

V$OBJECT_USAGE

Explanation:

You will query the V$OBJECT_USAGE view to ensure that the index is being monitored. The V$OBJECT_USAGE view is used to display information regarding the index usage when the ALTER INDEX.....MONITORING_USAGE statement is run. The USED column in the V$OBJECT_USAGE view displays the YES or NO value. If the column value is YES, then the index is used within the time period being monitored. If the column value is NO, then the index is not used within the time period being monitored.

The option stating that you will query the INDEX_STATS view to ensure that the index is being monitored is incorrect. For a given index, you can determine whether an index should be rebuilt by validating the structure of the index and checking the value of the PCT_USED column of the INDEX_STATS view. After gathering the statistics, you can query the INDEX_STATS view to obtain the following values:

LF_ROWS	Displays number of values in the index.
LF_ROWS_LEN	Displays the sum of all the length of values, in bytes.
DEL_LF_ROWS	Displays the number of values deleted from the index.
DEL_LF_ROWS_LEN	Displays the length of all deleted values.
PCT_USED	Displays the percent of space allocated in the index that is being used.

The option stating that you will query the DBA_INDEXES view to ensure that the index is being monitored is incorrect. The DBA_INDEXES view displays information about all the indexes in the database.

The option stating that you will query the DBA_IND_COLUMNS view to ensure that the index is being monitored is incorrect. The DBA_IND_COLUMNS view is used to display the expressions of the function-based indexes on tables.
DBA_INDEXES view to ensure that the index is being monitored is incorrect. The DBA_INDEXES view displays information about all the indexes in the database.

The option stating that you will query the DBA_IND_COLUMNS view to ensure that the index is being monitored is incorrect. The DBA_IND_COLUMNS view is used to display the expressions of the function-based indexes on tables.

Item: 24 (Ref:1Z0-043.10.3.1)

You are maintaining your OLTP database in Oracle10*g*. You have not set the warning level and critical level threshold values for space usage of the DATA1 tablespace.

What will be the impact?

- No warning level or critical level alert will be generated.
- A warning level alert will never be generated, but a critical level alert will be generated when 97 percent space of the DATA1 tablespace is used.
- A critical level alert will never be generated, but a warning level alert will be generated when 85 percent space of the DATA1 tablespace is used.
- A warning level alert will be generated at 85 percent space usage of the DATA1 tablespace, and a critical level alert is generated at 97 percent space usage of the DATA1 tablespace.

Answer:

A warning level alert will be generated at 85 percent space usage of the DATA1 tablespace, and a critical level alert is generated at 97 percent space usage of the DATA1 tablespace.

Explanation:

A warning level alert will be generated at 85 percent space usage of the DATA1 tablespace and a critical level alert will be generated at 97 percent space usage of the DATA1 tablespace. Tablespace thresholds are defined in terms of a percentage of the tablespace size. You can specify the critical level and warning level thresholds. If thresholds are not specified, then default thresholds are applied. By default, the warning level threshold is at 85 percent, and the critical level threshold at 97 percent. In this scenario, you have not set the warning level or critical level thresholds for the DATA1 tablespace; therefore, these default values for the thresholds will be applied.

The option stating that no warning level or critical level alerts will be generated is incorrect. The warning level alert will be generated at 85 percent space usage of the DATA1 tablespace, and the critical level alert will be generated at 97 percent space usage of the DATA1 tablespace.

The option stating that the warning level alert will never be generated, but a critical level alert will be generated at 97 percent space usage of the DATA1 tablespace is incorrect. The warning level alert will be generated at 85 percent space usage of the DATA1 tablespace.

The option stating that the critical level alert will never be generated, but a warning level alert will be generated at 85 percent space usage of the DATA1 tablespace is incorrect. The critical level alert will be generated at 97 percent space usage of the DATA1 tablespace.

Item: 25 (Ref:1Z0-043.10.1.3)

You have the following online redo log configuration:

Group	Member
1	'/disk1/oradata/redo01a.log'
2	'/disk2/oradata/redo02a.log'
3	'/disk3/oradata/redo03a.log'

You decide to multiplex the online redo log groups for recovery of redo log files in case of any disaster. Which two statements will you **NOT** issue to multiplex the online redo log files? (Choose two.)

- ☐ `ALTER DATABASE ADD LOGFILE MEMBER '/disk1/oradata/redo01b.log' TO GROUP 1;`
- ☐ `ALTER DATABASE ADD LOGFILE MEMBER '/disk2/oradata/redo01b.log' TO GROUP 1;`
- ☐ `ALTER DATABASE ADD LOGFILE MEMBER '/disk1/oradata/redo02b.log' TO GROUP 2;`
- ☐ `ALTER DATABASE ADD LOGFILE MEMBER '/disk2/oradata/redo02b.log' TO GROUP 2;`
- ☐ `ALTER DATABASE ADD LOGFILE MEMBER '/disk1/oradata/redo3b.log' TO GROUP 3;`
- ☐ `ALTER DATABASE ADD LOGFILE MEMBER '/disk2/oradata/redo3b.log' TO GROUP3;`

Answer:

`ALTER DATABASE ADD LOGFILE MEMBER '/disk1/oradata/redo01b.log' TO GROUP 1;`
`ALTER DATABASE ADD LOGFILE MEMBER '/disk2/oradata/redo02b.log' TO GROUP 2;`

Explanation:

You will not issue the `ALTER DATABASE ADD LOGFILE MEMBER /disk1/oradata/redo01b.log' TO GROUP 1` and the `ALTER DATABASE ADD LOGFILE MEMBER '/disk2/oradata/redo02b.log' TO GROUP 2` statements to multiplex the online redo log files. While multiplexing the online redo log files, you place identical copies of the online redo log files on different disks. The member of the online redo log group 1 is placed on disk1, and the member of the online redo log group 2 is placed on disk2. The `ALTER DATABASE ADD LOGFILE MEMBER /disk1/oradata/redo01b.log' TO GROUP 1` and the `ALTER DATABASE ADD LOGFILE MEMBER '/disk2/oradata/redo02b.log' TO GROUP 2` statements will place identical copies of the online redo log files to the same disks, and the performance of the database will be degraded.

The option stating that you will not issue the `ALTER DATABASE ADD LOGFILE MEMBER '/disk2/oradata/redo01b.log' TO GROUP 1` statement to multiplex the online redo log file is incorrect. The member of the redo log group 1 is placed on disk1. The `ALTER DATABASE ADD LOGFILE MEMBER '/disk2/oradata/redo01b.log' TO GROUP 1` statement will place the identical copy of the member of group 1 on disk2. Therefore, the `ALTER DATABASE ADD LOGFILE MEMBER '/disk2/oradata/redo01b.log' TO GROUP 1` statement can be used to multiplex the online redo group.

The option stating that you will not issue the `ALTER DATABASE ADD LOGFILE MEMBER '/disk1/oradata/redo02b.log' TO GROUP 2` statement to multiplex the online redo log file is incorrect. The member of the redo log group 2 is placed on disk2. The `ALTER DATABASE ADD LOGFILE MEMBER '/disk1/oradata/redo02b.log' TO GROUP 2` statement will place an identical copy of the member of group 2 on disk1. Therefore, the `ALTER DATABASE ADD LOGFILE MEMBER '/disk1/oradata/redo02b.log' TO GROUP 2` statement can be used to multiplex the online redo group.

The options stating that you will not issue the `ALTER DATABASE ADD LOGFILE MEMBER '/disk1/oradata/redo03b.log' TO GROUP 3` and the `ALTER DATABASE ADD LOGFILE MEMBER '/disk2/oradata/redo3b.log' TO GROUP3` statements to multiplex the online redo log file are incorrect. The member of the redo log group 3 is placed on disk3. The `ALTER DATABASE ADD LOGFILE MEMBER '/disk1/oradata/redo03b.log' TO GROUP 3` statement will place an identical copy of the member of group 3 on disk1. The `ALTER DATABASE ADD LOGFILE MEMBER '/disk2/oradata/redo03b.log' TO GROUP 3` statement will place an identical copy of the member of group 3 on disk2. Any of these two statements can be used to multiplex the online redo log group3.

Item: 26 (Ref:1Z0-043.10.2.3)

You issued the following statement in your SQL*Plus session:

```
SQL>ALTER SESSION ENABLE RESUMABLE TIMEOUT 600;
```

Which operation is neither suspended nor resumed using the Automatic Resumable Allocation feature in your database?

- creating a table in your schema and you exceed your allocated space quota on the tablespace
- executing a long query that involves a sort operation and the statement runs out of temporary space
- loading data into tables by using the SQL*Loader and the number of extents in the table reaches the maximum limit
- creating a table in a dictionary-managed tablespace with an explicit MAXEXTENTS setting which results in an out of space error

Answer:

creating a table in a dictionary-managed tablespace with an explicit MAXEXTENTS setting which results in an out of space error

---

Explanation:

The Resumable Space Allocation feature is not used when creating a table in a dictionary-managed tablespace with an explicit MAXEXTENTS setting which results in out of space error. This operation will be aborted. If you are running a Data Manipulation Statement (DML) statement, such as INSERT, and the table reaches the maximum allowed extents as specified by the MAXEXTENTS setting, the operation can be suspended and resumed later.

The option stating that if you can suspend an operation and resume it later if you are executing a long query that involves a sort operation and the SELECT statement runs out of temporary space is incorrect. The out of space condition is generated when querying data using a sort operation. This out of space condition can be managed by the Resumable Space Allocation feature.

The option stating that if you are creating a table in your schema but you exceed your space quota on the tablespace, you can suspend the operation and resume later is incorrect. The conditions under which you exceeded the space quota when creating the table can be managed by the Resumable Space Allocation feature.

The option stating that if you are loading data into tables using the SQL*Loader, but the number of extents in the table has reached the maximum limit, you can suspend the operation and resume it later is incorrect. The condition under which the maximum extent value is reached using SQL*Loader can be managed by the Resumable Space Allocation feature.

Item: 27 (Ref:1Z0-043.10.5.1)

You want to estimate the size of a table by using the Oracle Enterprise Manager.

On which data is the size of the table **NOT** based?

- column sizes
- column data types
- PCTFREE
- projected number of row
- PCTUSED

Answer:

PCTUSED

Explanation:

The size of the table to be created is not based on the value of the PCTUSED parameter. The PCTUSED parameter specifies the threshold limit for data in the block. When data exceeding the threshold limit is deleted from a block the block is marked as free and added to the freelist. This free data block can be further used for storing data.

The other options stating that the size of the table to be created is not based on the column sizes, column data types, and value of the PCTFREE parameter is incorrect. You can estimate the size of the table to be created based on the column sizes, column data types, and the value of the PCTFREE storage parameter. To estimate the size of the table to be created, you must enter the column names and the data types and click on the Estimate Table Size button on the Create Table page. You will be prompted to enter the projected number of rows in the table. After entering the projected number of rows in the table, click on the Estimate Table Size button. The Enterprise Manager returns the estimated size of the table. This estimated size is in megabytes (MB). The PCTFREE storage parameter specifies the free space in a block for future updates.

The option stating that the size of the table to be created is based on rowids of rows in the table is incorrect. The rowids are used to uniquely identify the rows of the table.

Item: 28 (Ref:1Z0-043.10.6.6)

You are maintaining a database of credit card transactions. You want the data to be returned automatically in the chronological order of the credit card numbers without using the `ORDER BY` clause in the query.

Which type of cluster will you use to obtain the desired result?

- Hash cluster
- Index cluster
- Sorted hash cluster
- Real Application cluster

Answer:

Sorted hash cluster

Explanation:

You will use the sorted hash cluster to return the data in the chronological order. The sorted hash cluster is introduced in Oracle10*g*. Sorted hash clusters extend the functionality of hash clusters of previous versions of Oracle by maintaining a sort order for rows that are retrieved by the same cluster key. In traditional, heap organized tables and hash clusters, rows are not returned in a sorted order. In sorted hash clusters for each hash cluster key, Oracle maintains a list of rows sorted by one or more sort columns. In this scenario, the credit card number will be used as a hash key to return the data in the chronological order

The option stating that you will use the hash cluster to return the data in the chronological order is incorrect. An index cluster functions like a B-tree index to ensure quick access to the rows in a cluster table. The attributes of a table that makes the table suitable for use in an index cluster are as follows:

- The tables in a cluster will always be queried together.
- The tables should have little or no insert, update, or delete operations performed on them.

The option stating that you will create a hash cluster to return the data in the chronological order is incorrect. A hash cluster uses the hashing algorithm on the row's cluster key to find the physical location of the row in the table. Hash clusters work best for queries that use the equality operator (=). The attributes of a table that makes the table suitable for use in a hash cluster are as follows:

- The values in the index column of the table in the cluster should be uniformly distributed.
- The tables should have little or no insert, update, or delete operations performed on them.
- The tables in the cluster should have a predictable number of values in the index column.
- The queries against the clustered table should use the equality operator (=) to retrieve the desired row.

The option stating that you will create an index cluster is incorrect. An index cluster functions like a B-tree index to ensure quick access to the rows in a cluster table. The attributes of a table that makes the table suitable for use in an index cluster are as follows:

- The tables in a cluster will always be queried together.
- The tables should have little or no insert, update, or delete operations performed on them.

Item: 29 (Ref:1Z0-043.10.1.8)

The online redo log group configuration for your database is as follows:

What will happen if the online redo log file `'ora02/oradata/redo02b.log'` is corrupted while working on the database?

- The database will hang.
- The database will be crashed.
- The database will be shut down.
- The `LGWR` process writes redo log entries to the other redo log member of the Group2 group.

Answer:

The `LGWR` process writes redo log entries to the other redo log member of the Group2 group.

Explanation:

In this scenario, the online redo log groups are multiplexed. While multiplexing the online redo log files, it is preferable to keep the members of a group on different disks to ensure that one disk failure does not affect the ongoing operation of the database. If the `LGWR` process can write the redo log entries to at least one member of the group, the database operation proceeds as normal. An entry is written to the `alert.log` file.

The other options stating that the database will hang or crash, or shut down due to the failure of a redo log member are incorrect.

Item: 30 (Ref:1Z0-043.10.7.1)

You executed the following procedure to collect statistics regarding an index:

```
SQL>ANALYZE INDEX EMP_ID VALIDATE STRUCTURE;
```

Which view will you use to determine whether you need to rebuild the index or not?

- INDEX_STATS
- DBA_INDEXES
- DBA_IND_COLUMNS
- V$OBJECT_USAGE

Answer:

INDEX_STATS

Explanation:

You must rebuild an index when you need to change the storage options or you need to move the index tablespace. For a given index, you can determine if an index needs to be rebuilt by validating the structure of the index and checking the value of the PCT_USED column of the INDEX_STATS view. After gathering the statistics, you can query the INDEX_STATS view the INDEX_STATS to obtain the following values:

LF_ROWS	Displays number of values in the index
LF_ROWS_LEN	Displays the sum of all the length of values, in bytes
DEL_LF_ROWS	Displays the number of values deleted from the index
DEL_LF_ROWS_LEN	Displays the length of all deleted values
PCT_USED	Displays the percent of space allocated in the index that is being used

The option stating that you will query the DBA_INDEXES view to determine whether an index needs to be rebuilt or not is incorrect. The DBA_INDEXES view displays information about all the indexes in the database.

The option stating that you will query the DBA_IND_COLUMNS view to determine whether an index needs to be rebuilt or not is incorrect. The DBA_IND_COLUMNS view is used to display the expressions of the function-based indexes on tables.

The option stating that you will query the V$OBJECT_USAGE view to determine whether an index needs to be rebuilt or not is incorrect. The V$OBJECT_USAGE view is used to display the information about the index usage displayed when the ALTER INDEX.....MONITORING_USAGE statement is run.

Securing the Oracle Listener

Item: 1 (Ref:1Z0-043.2.2.1)

You are required to remove the default EXTPROC entry from the default listener configuration to create a listener that will listen specifically for EXTPROC calls.

Which two methods can you use to remove the default EXTPROC entry from the default listener configuration? (Choose two.)

- the RMAN utility
- the import/export utility
- the Oracle Enterprise Manager
- the change tracking feature
- the Net Manager utility

Answer:

the Oracle Enterprise Manager
the Net Manager utility

Explanation:

You can use the Oracle Enterprise Manager or the Oracle Net Manager utility to remove the default EXTPROC entry from the default listener configuration. You can configure the listener to listen for external procedure calls. When an application calls an external procedure, the listener starts an external procedure agent named EXTPROC. Before you create a listener specifically for EXTPROC calls, you must remove the EXTPROC entry from the listener configuration. To remove the default EXTPROC entry by using the Oracle Enterprise Manager, perform the following steps:

1. Click the Listener link on the General section of the Database Control home page.
2. Click the Net Services Administration link from Related Links.
3. Click the Go button. Provide Host login credentials such as username and password.
4. Click the Listener link to the right of the Select button. Select the EXTPROC entry by clicking the IPC radio button.
5. Click the Remove button to complete the operation.

You can remove the default EXTPROC entry by using the Oracle Enterprise Manager in the following sequence:

1. Start the Net Manager.
2. On the left navigation pane, expand listeners in the Net Configuration directory tree and select LISTENER.
3. Select Other Services from the drop-down list, and select the EXTPROC tab.
4. Click the Remove Service button.
5. On the File menu, click the Save Network Configuration command.

The option stating that you will remove the default EXTPROC entry by using the RMAN utility is incorrect. The RMAN utility is used to perform backup and recovery of the database.

The option stating that you will remove the default EXTPROC entry by using the import/export utility is incorrect. The import/export utility is used to perform the backup of the logical structures of the database, such as backups of tables, tablespaces, and user schemas.

The option stating that you will remove the default EXTPROC entry by enabling the change tracking feature is incorrect. The change tracking feature is enabled to improve the performance of the incremental backup. If change tracking feature is enabled, only those blocks that are updated since the last backup are backed up in an incremental backup.

Item: 2 (Ref:1Z0-043.2.1.1)

You are maintaining the database of a company. The listener process, `listener1`, is configured for remote access. You have issued the following command:

```
LSNRCTL>STATUS listener1
```

Which information will **NOT** be displayed when you issue the above command?

- whether the password is set in the listener or a file or not
- the number of client connections the service handler has refused
- the information will be displayed whether the instance can accept connections or not
- the protocol addresses on which the listener is configured to listen

Answer:

the number of client connections the service handler has refused

---

Explanation:

The information regarding the number of client connections that the service handler has refused is not retrieved by using the STATUS command at the LNSRCTL prompt. This information will be displayed by using the SERVICE command at the LNSRCTL prompt. The SERVICE command displays information about the services associated to the listener, the number of service handlers handling the services, and so on.

The option stating that the STATUS command will display the information whether the instance can accept more connections or not is incorrect. This is because the STATUS command displays this information. A READY status indicates that the instance can accept connections. A BLOCK status indicates that the instance cannot accept connections.

The option stating that information regarding whether the password is set in the `listener.ora` file or not is not displayed is incorrect. This is because the STATUS command displays the information regarding whether the password is set in the `listener.ora` file or not. For security purposes, the password must be set. If the password is set on the `listener.ora` file, then you are required to provide the password to perform privileged operations, such as stopping a listener or saving configuration changes.

The option stating that the STATUS command will not display the protocol addresses that the listener is configured to listen on is incorrect. The STATUS command displays the protocol addresses on which the listener is configured to listen.

Item: 3 (Ref:1Z0-043.2.1.2)

The listener has shut down unexpectedly. You want to view the listener log file and listener trace file to find the cause of the problem.

How can you view the contents of the listener log file and the listener trace file?

- Open the file at the location specified by the BACKGROUND_DUMP_DEST parameter in the pfile.
- Open the file at the location specified by the USER_DUMP_DEST parameter in the pfile.
- Issue the SERVICES command at the LSNRCTL> prompt.
- Issue the STATUS command at the LSNRCTL> prompt.

Answer:

Issue the STATUS command at the LSNRCTL> prompt.

Explanation:

You will use the STATUS command of the listener control utility to find the locations of the listener log file and listener trace file. The syntax of the STATUS command is:

```
LNSRCTL> STATUS <listener_name>
```

where listener_name is the name of the listener defined in the listener.ora fie. If you are using the default listener, named LISTENER, then it is not necessary to identify the listener. Listener log file and trace files are used to find the cause of problems such as connectivity problems or an unexpected shutdown of the listener. The above command shows the information about log files and trace file locations, start date of the listener, trace level, and information about password protection. The Oracle TNS listener is a server process that provides network connectivity to the Oracle database. The listener is configured to listen for connection requests on a specified port on the database server. When an incoming connection request is received on a port, the listener will attempt to resolve the request and forward the connection information to the appropriate database instance.

The option stating that to view the contents of the listener log file and the listener trace file, you must look the location specified by the BACKGROUND_DUMP_DEST initialization parameter file is incorrect. The value of the BACKGROUND_DUMP_DEST parameter specifies the location of the alert log file and the background trace files.

The option stating that to view the contents of the listener log file and the listener trace file, you must look the location specified by the USER_DUMP_DEST initialization parameter file is incorrect. The value of the USER_DUMP_DEST parameter specifies the location of the server trace files.

The option stating that to find the locations of the listener log file and the listener trace file, you must issue the SERVICES command at the LSNRCTL prompt is incorrect. This command provides the information about the service name, name of the instance associated with the service, and the name of the service handler.

Item: 4 (Ref:1Z0-043.2.1.3)

You previously secured your listener with an encrypted password. However, you need to set a new password for security reasons.

What is the correct method for setting a new encrypted password for the listener using the Listener Control utility?

- executing the SET PASSWORD command and then the SAVE_CONFIG command
- executing the CHANGE_PASSWORD command and then the SAVE_CONFIG command
- executing the CHANGE_PASSWORD command and then the SET PASSWORD command
- executing the SET PASSWORD command, then the CHANGE_PASSWORD command and finally, the SAVE_CONFIG command

Answer:

executing the SET PASSWORD command, then the CHANGE_PASSWORD command and finally, the SAVE_CONFIG command

---

Explanation:

If the listener is already configured with an encrypted password, you can set a new password by executing the CHANGE_PASSWORD command, and save this setting permanently using the SAVE_CONFIG command. However, changing the password is a privileged operation that requires the password to be entered. Therefore, SET PASSWORD must be issued before the CHANGE_PASSWORD and the SAVE_CONFIG commands.

The SET PASSWORD command is not used to create or change the password. Some commands of the Listener Control utility, such as SAVE_CONFIG and STOP, require you to enter the password before executing the actual commands. Therefore, executing the SET PASSWORD command and then the SAVE_CONFIG command is used to save the settings permanently. However, these commands will not change the password for the listener.

Executing the CHANGE_PASSWORD and the SAVE_CONFIG commands will create a new password, and save the settings if no password has been previously set. In order to change the old password, the SET PASSWORD command is required before issuing these commands.

Executing the CHANGE_PASSWORD command and then the SET PASSWORD command is an invalid option because the SET PASSWORD command is required before the CHANGE_PASSWORD command.

Diagnostic Sources

Item: 1 (Ref:1Z0-043.8.2.1)

While performing monitoring and tuning the database, you want to view the summarized information about the warning level alerts and critical level alerts. Which section of the Oracle Enterprise manager displays the summarized information about the warning and critical level alerts?

- General
- High Availability
- Space Usage
- Diagnostic Summary

Answer:

Diagnostic Summary

Explanation:

The Diagnostic Summary section of the Oracle Enterprise Manager Home page summarizes the database performance findings of the Automatic Database Diagnostic Monitor (ADDM). ADDM is a diagnostic tool that is used to diagnose the performance statistics and to determine how any problem within the database can be resolved. The diagnostic summary section also summarizes any warning level or critical level alerts.

The option stating that the General second of the Oracle Enterprise Manager home page is summarizes the warning level and critical level alerts is incorrect. The General section of the Oracle Enterprise Manager displays the status of the database, instance name, time zone of the database, version of Oracle, and so on.

The option stating that the High Availability section of the Oracle Enterprise Manager displays the summarized information about of the warning level and critical level alerts is incorrect. The High Availability section displays the information about the time needed for the instance recovery, whether the database is in ARCHIVELOG or NOARCHIVELOG mode, whether the flashback logging is disabled or enabled.

The option stating that the Space Usage section of the Oracle Enterprise Manager displays the summarized information about the warning level and critical level alerts is incorrect. The Space Usage section displays the information about the space usage related problematic tablespaces, fragmentation issues, and so on.

Item: 2 (Ref:1Z0-043.8.1.2)

Matthew has recently joined NetFx Corporation as a junior-level Database Administrator (DBA). He is asked by his supervisor to verify the database for data block corruptions. He uses the `DBVERIFY` utility and finds that two data blocks are corrupted in the database.

What should Matthew use to identify the corrupted blocks as well as datafiles containing these blocks?

- datafile
- alert log
- dynamic views
- control file script

Answer:

alert log

Explanation:

Matthew should use the alert log to identify the corrupted blocks and the datafiles containing these blocks. The alert log is a readable file that records the information about the significant events that occur in the database, such as database startup and shutdown operations, checkpoints, redo log switches, and database errors. The data block corruption errors are recorded in the alert log along with the data block numbers and the datafile numbers. Using this information, you can identify which particular data blocks are corrupted in the database and to which datafiles they belong.

Datafiles are binary files in Oracle which contain the actual data. The block corruption information is not recorded in the datafiles.

Dynamic views are underlying views that contain information about the physical and memory structures of the database. They are continuously updated while a database is open and in use, and their contents relate primarily to performance. Using dynamic views, you cannot identify the data blocks and the datafiles containing corruptions.

When you use the `ALTER DATABASE BACKUP CONTROLFILE TO TRACE` statement, Oracle creates a control file script which is a readable file containing all the SQL statements that can be used to recreate the control file in case it is lost or damaged. The data block corruption errors are not recorded in the control file scripts.

Item: 3 (Ref:1Z0-043.8.3.3)

You have created a locally managed tablespace by issuing the following command:

```
CREATE TABLESPACE data1
DATAFILE 'data1_file1.dbf' SIZE 10M AUTOEXTEND ON MAXSIZE
UNLIMITED;
```

For the DATA1 tablespace, you have set the warning level alert limit to 70 percent.

In which situation will a warning level alert be generated?

- when 700 KB is used
- when 700 KB is left as free space
- when 7MB is used
- when 7MB is left as free space
- no alert will be generated because an autoextensible datafile is included in the tablespace

Answer:

when 7MB is used

Explanation:

The warning level threshold value for the DATA1 tablespace space is set to 70 percent. When 70 percent of the DATA1 tablespace is used, a warning level limit is generated. The size of the tablespace was set to 10 MB when the tablespace was created so 70 percent is 7 MB. When 7 MB of the DATA1 tablespace is used, a warning level alert is generated because the 70 percent threshold is met. Threshold alerts are based on the metrics computed by the Manageability Monitor (MMON) process to determine potential performance problems. This is accomplished by comparing the current metrics to the preset threshold levels. If the threshold is exceeded, an alarm is generated. A threshold alert can be defined to monitor the metric and raise an alert based on the current value of the metric against the two threshold settings, warning and critical. The warning threshold is the lowest level at which an alert is generated. When the current value of a metric is greater than the warning threshold limit, a warning level alert is generated and a notification that contains a predefined warning message is sent. When a critical threshold is exceeded, a critical level alert is generated and a notification that contains a predefined critical message is sent.

The option stating that a warning level alert is generated when 700 KB space of the tablespace is used is incorrect because the warning level is set to 70 percent. 70 percent of the tablespace is 7 MB, not 70 KB.

The options stating that a warning level alert is generated when 700 KB and 7 MB is left as free space are incorrect because the warning level threshold limit for tablespace space usage is set for used space, not free space.

The option stating that the 'DATA1_FILE1.DBF' datafile is auto extensible; therefore, no warning level alert will be generated is incorrect because alerts are based on the space used and not on the free space left in a tablespace.

Item: 4 (Ref:1Z0-043.8.4.1)

You are maintaining an OLTP database in Oracle10*g*. You find that the database is generating a large number of trace files. You decide to disable the trace files generated by the ARCn background process.

Which action will enable you to disable the trace files generated by the ARCn background process?

- Remove the LOG_ARCHIVE_DEST parameter from the init.ora file.
- Set the value of the SQL_TRACE parameter to FALSE in the init.ora file.
- Use the DBMS_MONITOR.SESSION_TRACE_DISABLE procedure.
- Set the value of the LOG_ARCHIVE_TRACE initialization parameter to zero.

Answer:

Set the value of the LOG_ARCHIVE_TRACE initialization parameter to zero.

Explanation:

You will set the value of the LOG_ARCHIVE_TRACE initialization parameter to zero to disable the trace files generated by the ARCn process. Each server process and background process can write associated trace files. Whenever the background process is unable to continue, it generates the associated trace file. The LOG_ARCHIVE_TRACE initialization parameter is used to control the trace files generated by the ARCn background process. You can disable the trace files generated by the ARCn process by setting the value of the LOG_ARCHIVE_TRACE parameter to zero.

You cannot disable the trace files generated by the ARCn process by removing the LOG_ARCHIVE_DEST parameter. If you delete this parameter from the init.ora file, then the database will be set to NOARCHIVELOG mode. No archive file will be generated.

You cannot disable the trace files generated by the ARCn process by setting the SQL_TRACE parameter to FALSE in the init.ora file. If you set the value of the SQL_TRACE parameter to FALSE, then SQL tracing will be disabled.

You cannot disable the trace files to be generated for the ARCn process by using the DBMS_MONITOR.SESSION_TRACE_DISABLE procedure. This is because the DBMS_MONITOR.SESSION_TRACE_DISABLE procedure is used to disable the tracing for a session. No trace files will be generated for the current session.

Item: 5 (Ref:1Z0-043.8.3.1)

Which code will set the thresholds for the DATA1 tablespace to 60% and 95%?

- DBMS_SERVER_ALERT.SET_THRESHOLD
  (
  DBMS_SERVER_ALERT.TABLESPACE_PCT_FULL,
  DBMS_SERVER_ALERT.OPERATOR_GE,60,
  DBMS_SERVER_ALERT.OPERATOR_GE,95,
  1, 1, null,
  DBMS_SERVER_ALERT.OBJECT_TYPE_TABLESPACE, NULL);
- DBMS_SERVER_ALERT.SET_THRESHOLD
  (
  DBMS_SERVER_ALERT.TABLESPACE_PCT_FULL,
  DBMS_SERVER_ALERT.OPERATOR_GE,60,
  DBMS_SERVER_ALERT.OPERATOR_GE,95,
  1, 1, null,
  DBMS_SERVER_ALERT.OBJECT_TYPE_DATAFILE, 'DATA1');
- DBMS_SERVER_ALERT.SET_THRESHOLD
  (
  DBMS_SERVER_ALERT.TABLESPACE_PCT_FULL,
  DBMS_SERVER_ALERT.OPERATOR_LE,60,
  DBMS_SERVER_ALERT.OPERATOR_LE,95,
  1, 1, null,
  DBMS_SERVER_ALERT.OBJECT_TYPE_TABLESPACE, DATA1);
- DBMS_SERVER_ALERT.SET_THRESHOLD
  (
  DBMS_SERVER_ALERT.TABLESPACE_PCT_FULL,
  DBMS_SERVER_ALERT.OPERATOR_GE,60,
  DBMS_SERVER_ALERT.OPERATOR_GE,95,
  1, 1, null,
  DBMS_SERVER_ALERT.OBJECT_TYPE_TABLESPACE, DATA1);

Answer:

```
DBMS_SERVER_ALERT.SET_THRESHOLD
(
DBMS_SERVER_ALERT.TABLESPACE_PCT_FULL,
DBMS_SERVER_ALERT.OPERATOR_GE,60,
DBMS_SERVER_ALERT.OPERATOR_GE,95,
1, 1, null,
DBMS_SERVER_ALERT.OBJECT_TYPE_TABLESPACE, DATA1);
```

Explanation:

The following code will set the thresholds for the DATA1 tablespace to 60% and 95%:

```
DBMS_SERVER_ALERT.SET_THRESHOLD
(
DBMS_SERVER_ALERT.TABLESPACE_PCT_FULL,
DBMS_SERVER_ALERT.OPERATOR_GE,60,
DBMS_SERVER_ALERT.OPERATOR_GE,95,
1, 1, null,
DBMS_SERVER_ALERT.OBJECT_TYPE_TABLESPACE, DATA1);
```

You must specify the TABLESPACE_PCT_FULL metric, the two thresholds, and the object type of the tablespace and the tablespace name.

The option:

```
DBMS_SERVER_ALERT.SET_THRESHOLD
(
DBMS_SERVER_ALERT.TABLESPACE_PCT_FULL,
DBMS_SERVER_ALERT.OPERATOR_GE,60,
DBMS_SERVER_ALERT.OPERATOR_GE,95,
1, 1, null,
```

```
DBMS_SERVER_ALERT.OBJECT_TYPE_TABLESPACE, NULL);
```

is incorrect. This is because specifying `NULL` for the tablespace name will set the threshold for all the tablespaces and not just the `DATA1` tablespace.

The option:

```
DBMS_SERVER_ALERT.SET_THRESHOLD
(
DBMS_SERVER_ALERT.TABLESPACE_PCT_FULL,
DBMS_SERVER_ALERT.OPERATOR_GE,60,
DBMS_SERVER_ALERT.OPERATOR_GE,95,
1, 1, null,
DBMS_SERVER_ALERT.OBJECT_TYPE_DATAFILE, 'DATA1');
```

is incorrect. This is because the object type in the above code must be specified as `OBJECT_TYPE_TABLESPACE` instead of `OBJECT_TYPE_DATAFILE`.

The option:

```
DBMS_SERVER_ALERT.SET_THRESHOLD
(
DBMS_SERVER_ALERT.TABLESPACE_PCT_FULL,
DBMS_SERVER_ALERT.OPERATOR_LE,60,
DBMS_SERVER_ALERT.OPERATOR_LE,95,
1, 1, null,
DBMS_SERVER_ALERT.OBJECT_TYPE_TABLESPACE, DATA1);
```

is incorrect. This is because to specify the thresholds for the tablespace, you must use `OPERATOR_GE` operators instead of `OPERATOR_LE` operators.

Item: 6 (Ref:1Z0-043.8.4.2)

You are maintaining an OLTP database in Oracle10*g*. You set the value of the LOG_ARCHIVE_TRACE parameter to zero.

What is the impact of this setting?

- The trace files will be disabled only for a specific session.
- Tracing will be disabled for a client identifier.
- Tracing will be disabled only for the ARCn process.
- The SQL Trace facility will be disabled for the instance.

Answer:

Tracing will be disabled only for the ARCn process.

Explanation:

If you set the value of the LOG_ARCHIVE_TRACE parameter to zero, then tracing will be disabled only for the ARCn process. Each server process and background process can write associated trace files. Whenever a background process is unable to continue, it generates the associated trace file. The LOG_ARCHIVE_TRACE initialization parameter is used to control the generation of the trace files associated with the ARCn process. You can disable the trace files associated with the ARCn process by setting the value of the LOG_ARCHIVE_TRACE parameter to zero.

The option stating that tracing will be disabled for only a specific session by setting the value of the LOG_ARCHIVE_TRACE initialization parameter to zero is incorrect. Tracing can be disabled for a specific session by using the ALTER SESSION SET SQL_TRACE=FALSE; statement

The option stating that tracing will be disabled for a client identifier by setting the value of the LOG_ARCHIVE_TRACE initialization parameter to zero is incorrect. The tracing can be disabled for a client identifier by using the BMS_MONITOR.SESSION_TRACE_DISABLE(session_id => value, serial_num => value); procedure.

The option stating that the SQL Trace facility will be disabled for the instance by setting the value of the LOG_ARCHIVE_TRACE initialization parameter to zero is incorrect. The trace facility can be disabled for the instance by setting the value of the SQL_TRACE initialization parameter to FALSE in the initialization parameter file.

Item: 7 (Ref:1Z0-043.8.4.3)

You are maintaining the PROD database of NetFx Corporation. You set the value of the SQL_TRACE parameter to TRUE.

What will be the impact of this setting?

- The SQL trace facility will generate the performance statistics for all the SQL statements for an instance and write them in the USER_DUMP_DEST directory.
- The SQL trace facility will generate the performance statistics for all the SQL statements for a session and write them in the USER_DUMP_DEST directory.
- The SQL trace facility will generate the performance statistics for all the SQL statements for an instance and write them in the BACKGROUND_DUMP_DEST directory.
- The SQL trace facility will generate the performance statistics for all the SQL statements for a session and write them in the BACKGROUND_DUMP_DEST directory.

Answer:

The SQL trace facility will generate the performance statistics for all the SQL statements for an instance and write them in the USER_DUMP_DEST directory.

Explanation:

Setting the value of the SQL_TRACE parameter to TRUE causes the SQL trace facility to generate the performance statistics for all the SQL statements for an instance and write them in the USER_DUMP_DEST directory. In the ARCHn background process, it is possible to control the type and amount of trace information to be produced. The trace files are generated on behalf of the server processes if any internal error occurs. However, you can cause the SQL trace facility to generate the performance statistics for all the SQL statements for an instance by setting the value of the initialization parameter SQL_TRACE to TRUE. This is because setting the SQL_TRACE parameter causes the SQL trace facility to generate performance statistics for all the SQL statements for an instance and write them in the USER_DUMP_DEST directory. Regardless of the value of the SQL_TRACE initialization parameter, you can enable or disable trace logging for a session by using the ALTER SESSION SET SQL_TRACE statement.

The option stating that setting the value of the SQL_TRACE parameter to TRUE causes the SQL trace facility to generate performance statistics for all the SQL statements for an instance and write them in the BACKGROUND_DUMP_DEST directory is incorrect. This is because the performance statistics for all the SQL statements are written in the USER_DUMP_DEST directory. The BACKGROUND_DUMP_DEST directory is used to specify the location of the alert log file and the trace files generated when the background processes fail.

The option stating that setting the value of the SQL_TRACE parameter to TRUE causes the SQL trace facility to generate the performance statistics for all SQL statements for a session and write them in the BACKGROND_DUMP_DEST directory is incorrect. This is because setting the SQL_TRACE parameter causes the SQL trace facility to generate performance statistics for all the SQL statements for an instance and write them in the USER_DUMP_DEST directory. You can enable or disable the trace logging for a session by using the ALTER SESSION SET SQL_TRACE statement.

Item: 8 (Ref:1Z0-043.8.1.1)

A junior level Database Administrator erroneously deleted the database alert log while users were accessing the database. Which action should you take to recover the alert log?

- Do nothing.
- Restart the database.
- Perform recovery on the database.
- Restore the alert log from the last backup.

Answer:

Do nothing.

Explanation:

If the alert log is erroneously deleted while the database is up and running, no action is required because the alert log is automatically re-created by the database instance. When the database instance is active, the database continuously updates the alert log with the database events, such as startup, shutdown, log switches, block corruption errors, `CREATE`, `ALTER`, and `DROP` statements. The database checks for the alert log in the directory path specified by the value of the `BACKGROUND_DUMP_DEST` initialization parameter. If it does not find the alert log there, it creates another alert log in the same directory path.

The option stating that you should restart the database is incorrect because it is not mandatory to restart your database if you lose the alert log.

The option stating that you should restore the alert log from the last backup is incorrect because Oracle will re-create the alert log for you.

The option stating that you should perform recovery on the database is incorrect because there is no need to recover the database if you lose the alert log.

Item: 9 (Ref:1Z0-043.8.3.2)

The warning level threshold value for a tablespace, DATA1, is set to 60% and the critical level threshold value is set to 80%. The tablespace, DATA1, is infrequently used and is not a part of the production environment.

You issued the following command:

```
SQL> EXECUTE
   DBMS_SERVER_ALERT.SET_THRESHOLD
   (dbms_server_alert.tablespace_pct_full,
   dbms_server_alert.operator_ge,80,
   dbms_server_alert.operator_ge,90,
   1,1,NULL,
   dbms_server_alert.object_type_tablespace,'DATA');
```

What will be the result of the command?

- The command will be executed successfully only if the tablespace DATA1 is a dictionary-managed tablespace.
- The total numbers of alerts that you receive every day will be reduced.
- The total number of alerts that you receive every day will be increased.
- No more data will be added to the DATA1 tablespace if 80% of the space allocated to the DATA1 tablespace is used.

Answer:

The total numbers of alerts that you receive every day will be reduced.

Explanation:

The DATA1 tablespace is not used frequently and is not a part of the production environment. If the warning threshold value is increased from 60% to 80% and the critical threshold value is increased from 80% to 90%, then the total number of alerts will be reduced. The new threshold values are compared to the percentage of space used in the DATA1 tablespace every minute, causing an alert the first time the threshold is exceeded for the DATA1 tablespace.

The option stating that the command will be executed successfully only if DATA1 is a dictionary-managed tablespace is incorrect. This is because the DBMS_SERVER_ALERT package is not supported by dictionary-managed tablespaces. The DBMS_SERVER_ALERT package is supported by locally-managed tablespaces. The DBMS_SERVER_ALERT package is used to specify the warning level and the critical level threshold values for space usage of the tablespace.

The option stating that the total number of alerts that you receive everyday will be increased is incorrect. This is because the warning level threshold value is increased from 60% to 80% and the critical level threshold value is increased from 80% to 90%. The new threshold values are compared to the percentage of space used in the DATA1 tablespace every minute, causing an alert the first time the threshold is exceeded for the DATA1 tablespace. The total number of alerts you receive everyday is reduced.

The option stating that you cannot add more data to the DATA1 tablespace if 80% of the space allocated to the DATA1 tablespace is used is incorrect. Data can be added to the DATA1 tablespace if 80% of the space allocated to the DATA1 tablespace is used. You will only receive a warning message indicating that 80% of the space allocated to the tablespace has been used.

Monitoring and Managing Memory

Item: 1 (Ref:1Z0-043.12.1.4)

The Automatic Shared Memory Management feature is enabled for the PROD database. Currently, a lot of insert activity is taking place in the database, and the memory structures are allocated according to the database workload. As the workload reduces, you decide to perform batch jobs in the database.

Which of the following initialization parameters are **NOT** automatically resized according to the new workload and continue to remain unchanged? (Choose two.)

- LOG_BUFFER
- DB_CACHE_SIZE
- JAVA_POOL_SIZE
- LARGE_POOL_SIZE
- SHARED_POOL_SIZE
- STREAMS_POOL_SIZE

Answer:

LOG_BUFFER
STREAMS_POOL_SIZE

Explanation:

The LOG_BUFFER and STREAMS_POOL_SIZE initialization parameters are not affected by the automatic resizing of the memory components. These components are manually tuned SGA parameters. If the current size of the database buffer cache is 512M and the auto-tuning algorithm must shrink by 50M of memory, the memory components that are not auto-tuned, remain unaffected.

The auto-tuned SGA parameters are as follows:

```
DB_CACHE_SIZE
JAVA_POOL_SIZE
LARGE_POOL_SIZE
SHARED_POOL_SIZE
```

The manually tuned SGA parameters are as follows:

```
LOG_BUFFER
DB_KEEP_CACHE_SIZE
DB_RECYCLE_CACHE_SIZE
DB_nK_CACHE_SIZE (n=2, 4, 8, 16, 32)
STREAMS_POOL_SIZE
```

All other options are incorrect.

Item: 2 (Ref:1Z0-043.12.2.4)

The SPFILE for your database contains the following parameter settings:

```
SGA_TARGET = 1000M
DB_CACHE_SIZE = 512M
SHARED_POOL_SIZE = 128M
LOG_BUFFER = 10M
DB_8K_CACHE_SIZE = 50M
```

What is the total memory that can be distributed across the auto-tuned memory components?

- 940M
- 990M
- 690M
- 1000M

Answer:

940M

Explanation:

In the current scenario, the total memory that will be distributed across the auto-tuned memory components is 940M.

The total memory that can be distributed across the auto-tuned memory components is calculated as follows:

SGA_TARGET *minus* memory components not auto-tuned.

The shared pool, the java pool, the large pool, and the database buffer cache are the automatically tuned memory components of the SGA and the log buffer, keep and recycle buffer caches, non standard block size buffer caches, and the streams pool are the SGA components that are not auto tuned. These components take their memory from the SGA_TARGET parameter. The memory left after the deduction of the non auto tuned memory components is distributed across the auto-tuned memory components.

All the other options are incorrect.

Item: 3 (Ref:1Z0-043.12.2.5)

You create an Oracle 10*g* database and configure the SPFILE as follows:

```
SGA_TARGET=2G
DB_CACHE_SIZE=512M
LOG_BUFFER=50M
DB_KEEP_CACHE_SIZE=128M
```

You modify the SGA_TARGET initialization parameter using the following statement:

```
SQL>ALTER SYSTEM SET SGA_TARGET = 1G SCOPE = BOTH;
```

Which entity does this statement affect?

- only the auto-tuned memory components
- only the memory components that are not auto-tuned
- both the auto-tuned memory components and the non-auto-tuned memory components
- neither the auto-tuned memory components nor the non-auto-tuned memory components

Answer:

only the auto-tuned memory components

Explanation:

When you modify the SGA_TARGET initialization parameter, only the auto-tuned memory components are affected. The shared pool, the java pool, the large pool, and the database buffer cache are the automatically tuned memory components of SGA, and the log buffer, keep and recycle buffer caches, non standard block size buffer caches, and the streams pool are the SGA components that are not auto-tuned. The memory left after the deduction of the non-auto-tuned memory components is distributed across the auto-tuned memory components. Therefore, when you increase or decrease the value of SGA_TARGET, only the automatically tuned memory components of the SGA are affected. The memory components that are not automatically tuned do not change because they have a fixed size as defined by the initialization parameters.

If you increase the SGA_TARGET initialization parameter, the additional memory is reallocated across the auto-tuned memory components using an auto-tuning sizing policy. If you decrease the SGA_TARGET initialization parameter, the memory is reallocated from one or more auto-tuned memory components.

Therefore, all other options are incorrect.

Item: 4 (Ref:1Z0-043.12.2.3)

Your SPFILE contains the following parameter settings:

```
SGA_TARGET = 8G
DB_CACHE_SIZE = 4G
SHARED_POOL_SIZE = 2G
LARGE_POOL_SIZE = 512M
JAVA_POOL_SIZE = 512M
LOG_BUFFER = 100M
SGA_MAX_SIZE = 10G
```

You query the V$SGA_DYNAMIC_COMPONENTS dynamic performance view and discover that the large pool component is currently sized at 1G.

You want the value of the SGA_TARGET initialization parameter to 10G, but instead of specifying a value of 10G for the SGA_TARGET initialization parameter, you erroneously execute the following statement:

```
SQL>ALTER SYSTEM SET SGA_TARGET = 0 SCOPE = BOTH;
```

What is the result of this statement?

- The database crashes.
- The large pool releases 512M of memory.
- The large pool retains 1G of allocated memory.
- The large pool increases to 1,512M of memory.

Answer:

The large pool retains 1G of allocated memory.

Explanation:

In this scenario, the memory allocated to the large pool remains at 1G. This overrides the original parameter values in the SPFILE.

You can disable the Automatic Shared Memory Management feature by dynamically setting the SGA_TARGET initialization parameter to 0. When you disable the Automatic Shared Memory Management feature, the values of all the auto-tuned parameters are set to the current sizes, overriding the original values included in the SPFILE. Disabling the Automatic Shared Memory Management feature does not affect the settings of manually controlled parameters, such as DB_nK_CACHE_SIZE, DB_KEEP_CACHE_SIZE, DB_RECYLE_CACHE_SIZE, and STREAMS_POOL_SIZE.

The option stating that the database crashes is incorrect because the database continues to perform normally. Only the Automatic Shared Memory Management feature of the database is disabled.

The option stating that the large pool releases 512M memory is incorrect because disabling the Automatic Shared Memory Management feature sets all the auto-tuned parameters to their current sizes.

The option stating that the large pool can increase up to a total of 1,512M of memory is incorrect because the large pool is an auto-tuned parameter. All the auto-tuned parameters are set to their current values after the Automatic Shared Memory Management feature is disabled. Therefore, the large pool neither shrinks nor increases after this statement executes. The parameter maintains its current size of 1G.

Item: 5 (Ref:1Z0-043.12.2.7)

You set the value of the SGA_TARGET initialization parameter to 1G to enable Oracle to automatically resize most of the memory components according to the current workload in the database. You issue the following statement:

```
SQL> SELECT name, value, isdefault
2 FROM v$parameter
3 WHERE name LIKE '%size%';
```

The output of this statement displays that the DB_CACHE_SIZE, SHARED_POOL_SIZE, LARGE_POOL_SIZE, and JAVA_POOL_SIZE initialization parameters contain a zero value.

What does this imply? (Choose two.)

- The SGA_TARGET initialization parameter cannot be set to a value less than 1G.
- The SGA_TARGET initialization parameter cannot be set to a value greater than 1G.
- The Memory Advisor of the Oracle Enterprise Manager 10*g* cannot be used to obtain advice on the important memory components of the SGA.
- The values of the DB_CACHE_SIZE, SHARED_POOL_SIZE, LARGE_POOL_SIZE, and JAVA_POOL_SIZE initialization parameters cannot be set manually.
- No minimum limits are imposed on the DB_CACHE_SIZE, SHARED_POOL_SIZE, LARGE_POOL_SIZE, and JAVA_POOL_SIZE initialization parameters.
- The Automatic Shared Memory Management feature cannot be disabled unless you specify values for the DB_CACHE_SIZE, SHARED_POOL_SIZE, LARGE_POOL_SIZE, and JAVA_POOL_SIZE initialization parameters in the initialization parameter file.

Answer:

The Memory Advisor of the Oracle Enterprise Manager 10*g* cannot be used to obtain advice on the important memory components of the SGA.

No minimum limits are imposed on the DB_CACHE_SIZE, SHARED_POOL_SIZE, LARGE_POOL_SIZE, and JAVA_POOL_SIZE initialization parameters.

Explanation:

If Automatic Shared Memory Management is enabled, the Memory Advisor of the Oracle Enterprise Manager 10*g* cannot be used to obtain advice on the important memory components of the SGA, such as the database buffer cache and the shared pool. You must disable the Automatic Shared Memory Management to use the Memory Advisor of the Oracle Enterprise Manager 10*g*.

When the SGA_TARGET initialization parameter is set to a nonzero value without specifying values for the auto-tuned memory structures of the SGA, no minimum limits are imposed on the database buffer cache, the shared pool, the large pool, and the java pool. For example, if Automatic Shared Memory Management is enabled and the DB_CACHE_SIZE initialization parameter is set to a value of 512M, even the auto-tuning algorithm cannot shrink the size of the database buffer cache below 512M. When no size is specified for the database buffer cache, no limit is imposed on its minimum size. Depending upon the workload and internal auto-tuning algorithm, its size can be minimized only up to a value that is determined by the internal auto-tuning algorithm.

The option stating that the SGA_TARGET initialization parameter cannot be set to a value less than 1G is incorrect because you can decrease the SGA_TARGET initialization parameter even if no values are specified for the auto-tuned memory components in the initialization parameter file.

The option stating that the SGA_TARGET initialization parameter cannot be set to a value more than 1G is incorrect because you can increase the SGA_TARGET initialization parameter even if no values are specified for the auto-tuned memory components in the initialization parameter file.

The option stating that the values of the DB_CACHE_SIZE, SHARED_POOL_SIZE, LARGE_POOL_SIZE, and JAVA_POOL_SIZE initialization parameters cannot be set manually is incorrect. You can change the values of these initialization parameters by using the ALTER SYSTEM statement even if no values are specified for the auto-tuned memory components in the initialization parameter file. If the new size of an auto-tuned memory component is greater than the current size, the memory component is immediately resized. If the new size for the auto-tuned memory component is less than the current size, the memory component is not resized immediately. This allows the auto-tuning algorithm to reduce the size of this component depending upon the database workload. The auto-tuning algorithm never reduces the size of this component to less than the specified size.

The option stating that the Automatic Shared Memory Management cannot be disabled unless you specify values for the DB_CACHE_SIZE, SHARED_POOL_SIZE, LARGE_POOL_SIZE, and JAVA_POOL_SIZE initialization parameters in the initialization parameter file is incorrect. You can disable the Automatic Shared Memory Management even if no values are specified for the auto-tuned memory structures in the initialization parameter file. The current sizes of the auto-tuned memory components are recorded in the SPFILE, which is persistent during database startup and shutdown operations.

Item: 6 (Ref:1Z0-043.12.2.6)

The PROD database requires a large database buffer cache during the day time when transaction volume is very high. At night, the PROD database requires a large amount of memory dedicated to the large pool to perform parallel batch jobs.

The SPFILE contains the following values:

```
DB_CACHE_SIZE = 2G
SHARED_POOL_SIZE = 1G
LARGE_POOL_SIZE = 1G
JAVA_POOL_SIZE = 1G
DB_KEEP_CACHE_SIZE = 3G
LOG_BUFFER = 100M
```

To minimize the manual resizing of memory components for day and night, you implement the Automatic Shared Memory Management feature by issuing the following statement:

```
SQL>ALTER SYSTEM SET SGA_TARGET = 8G SCOPE = BOTH;
```

You receive the following errors:

```
ORA-02097: parameter cannot be modified because specified value is invalid
ORA-00824: cannot set sga_target due to existing internal settings
```

What is the cause of these errors?

- The STATISTICS_LEVEL initialization parameter is set to BASIC.
- The STATISTICS_LEVEL initialization parameter is set to TYPICAL.
- The SGA_MAX_SIZE initialization parameter is not specified in the SPFILE.
- The SGA_TARGET initialization parameter is not set in multiples of the granule.
- The Automatic Shared Memory Management feature is not installed on your Oracle Database 10*g*.

Answer:

The STATISTICS_LEVEL initialization parameter is set to BASIC.

Explanation:

You cannot enable the Automatic Shared Memory Management feature in the Oracle Database 10*g* if the STATISTICS_LEVEL initialization parameter is set to BASIC. You cannot set the SGA_TARGET initialization parameter to a nonzero value if the STATISTICS_LEVEL is set to BASIC.

The option stating that the ORA-02097 and ORA-00824 errors are returned because the STATISTICS_LEVEL initialization parameter is set to TYPICAL is incorrect. When the STATISTICS_LEVEL is set to either TYPICAL or ALL, you can set the SGA_TARGET initialization parameter to a nonzero value without generating any errors.

The option stating that you cannot set the SGA_TARGET initialization parameter to a nonzero value because the SGA_MAX_SIZE initialization parameter is not specified in the SPFILE is incorrect. If you do not specify the SGA_MAX_SIZE initialization parameter, Oracle selects a default value that is the sum of all the memory components and does not return an error.

The option stating that the SGA_TARGET initialization parameter cannot be set to a nonzero value if the SGA_TARGET initialization parameter is not set in multiples of the granule is incorrect. All SGA components allocate and deallocate space in units of granules. The granule size is determined by the total SGA size. For most platforms, if the total size of the SGA is less than or equal to 1G, the size of one granule is 4M. If the total size of the SGA is greater than 1G, the size of one granule is 16M. For some platforms, the sizing of granule is different. For example, on 32-bit Windows NT, the granule size is 8M if the total size of the SGA exceeds 1G.

If you specify the size of a memory component that is not a multiple of granules, you will not receive an error. Oracle rounds the value up to the nearest multiple. For example, if the granule size is 4M and you specify the database buffer cache to be 10M, Oracle rounds the size of the database buffer cache to 12M.

The option stating that the cause of the ORA-02097 and ORA-00824 errors is that the Automatic Shared Memory Management

feature is not installed on your Oracle Database 10*g* is incorrect. By default, the Automatic Shared Memory Management is always installed on the Oracle Database 10*g*. You only need to enable this feature by setting the SGA_TARGET initialization parameter to a nonzero value or by using Enterprise Manager.

Item: 7 (Ref:1Z0-043.12.1.5)

You are upgrading to the Oracle 10*g* Database and will use the Automatic Shared Memory Management feature of the Oracle 10*g* Database.

Which background process serves as the SGA memory broker that coordinates the sizing of the memory components?

- MMAN
- PMON
- MMON
- MMNL

Answer:

MMAN

Explanation:

The Memory Manager (MMAN) background process of the Oracle Database 10*g* serves as the SGA memory broker that coordinates the sizing of the memory components. Depending upon the database workload requirement, MMAN captures statistics periodically in the background. It uses different memory advisories to perform a what-if-analysis that helps to determining the best distribution of the memory. On the basis of the what-if-analysis, the MMAN background process moves memory from one memory component to another. The Automatic Shared Memory Management feature uses different memory advisors and redistributes the memory across memory components depending upon the database workload, without the intervention of a Database Administrator (DBA).

The Process Monitor (PMON) background process is incorrect because the PMON process performs a process recovery when a user process fails. It is responsible for cleaning up the database buffer cache and releasing resources that the user process was using.

The Memory Monitor (MMON) background process is incorrect because the MMON background process performs various manageability-related background tasks, such as issuing alerts whenever a given metrics violates its threshold value and capturing statistics value for SQL objects that have been recently modified.

The Memory Monitor Light (MMNL) background process is incorrect because the MMNL background process performs frequent and lightweight manageability-related tasks, such as capturing session history and computing metrics.

Item: 8 (Ref:1Z0-043.12.2.2)

You are configuring the PROD database to use an internal tuning algorithm to monitor the performance of the workload. To achieve this configuration, you specify the following parameter settings in the SPFILE:

```
SGA_TARGET = 512M
SHARED_POOL_SIZE = 256M
```

Which two statements are true when modifying the SHARED_POOL_SIZE initialization parameter in the SPFILE? (Choose two.)

- Modifying the SHARED_POOL_SIZE initialization parameter cannot be accomplished if the SGA_TARGET initialization parameter is set to a non-zero value.
- Modifying the value of the SHARED_POOL_SIZE initialization parameter to zero is not allowed if the SGA_TARGET initialization parameter is set to a nonzero value.
- Increasing the value of the SHARED_POOL_SIZE initialization parameter does not increase the shared pool component size. It sets the lower limit for the size of this component.
- Decreasing the value of the SHARED_POOL_SIZE initialization parameter does not reduce the size of the shared pool component immediately. It sets the lower limit for the size of this component.
- Increasing the value of the SHARED_POOL_SIZE initialization parameter immediately increases the shared pool component to the desired size by reallocating the additional memory from the auto-tuned memory components.
- Decreasing the value of the SHARED_POOL_SIZE initialization parameter immediately shrinks the shared pool component to the desired size while reallocating the released memory to the memory components that are not auto-tuned.

Answer:

Decreasing the value of the SHARED_POOL_SIZE initialization parameter does not reduce the size of the shared pool component immediately. It sets the lower limit for the size of this component.

Increasing the value of the SHARED_POOL_SIZE initialization parameter immediately increases the shared pool component to the desired size by reallocating the additional memory from the auto-tuned memory components.

Explanation:

Decreasing the value of the SHARED_POOL_SIZE initialization parameter does not reduce the size of the shared pool component but sets a lower limit for the size of this component. Increasing the value of the SHARED_POOL_SIZE initialization parameter results in immediately increasing the shared pool component to the desired size, while reallocating the additional memory from the other auto-tuned memory components.

When you decrease the value of an auto-tuned memory component, there is no immediate effect. This means that if the SHARED_POOL_SIZE is reduced to 128M, the memory is not released immediately. The effect will take place only when the workload of the database changes. This requires an additional memory to be allocated to the other auto-tuned memory components such as the database buffer cache, large pool, or java pool. If the workload requires that the size of the java pool must be increased, then memory can be reallocated from the shared pool. The new value for the SHARED_POOL_SIZE parameter setting will serve as the lower limit size, preventing the shared pool from being resized to a value less than 128M.

When you increase the value of an auto-tuned memory component, Oracle immediately changes the size of the component. The additional memory required for this operation is reallocated from the other auto-tuned memory components. If this setting is saved in the SPFILE, the specified size of this auto-tuned memory component is the minimum size allowed for this component. If the other auto-tuned memory components require additional memory due to the database workload, Oracle will allow this memory component to shrink below the new size.

The option stating that the SHARED_POOL_SIZE initialization parameter cannot be modified manually if the SGA_TARGET initialization parameter is set to a nonzero value is incorrect. You can modify the auto-tuned parameters manually even if Automatic Shared Memory Management is enabled.

The option stating that modifying the value of the SHARED_POOL_SIZE initialization parameter to zero is not allowed if the SGA_TARGET initialization parameter is set to a nonzero value is incorrect. You can modify the auto-tuned memory parameters to a zero value if the Automatic Shared Memory Management is enabled. However, setting the size of an automatically sized component to zero disables the enforcement of any minimum limit on the size of the component.

The option stating that increasing the value of the SHARED_POOL_SIZE initialization parameter does not increase the shared pool component size but serves as a lower limit for the size of this component is incorrect. If you increase an automatically sized

memory component, the component will immediately increase to the new value. The additional memory is immediately reallocated from the other auto-tuned memory components.

The option stating that decreasing the value of the SHARED_POOL_SIZE initialization parameter immediately shrinks the shared pool component to the desired size while reallocating the released memory to the non-auto-tuned memory components is incorrect. When you decrease an automatically sized component, the component is not resized immediately. The new value is considered the minimum component size when the workload changes. Therefore, when you decrease an auto-tuned component, memory is not immediately released.

Item: 9 (Ref:1Z0-043.12.2.8)

You have included the following parameter settings in your SPFILE:

```
SGA_MAX_SIZE=8G
SGA_TARGET=6G
DB_CACHE_SIZE=2G
SHARED_POOL_SIZE=1G
LOG_BUFFER=64M
DB_KEEP_CACHE_SIZE=960M
```

Which statement is true if you modify the SGA_TARGET initialization parameter?

- The SGA_TARGET initialization parameter cannot be set to a value greater than 8G.
- The DB_CACHE_SIZE initialization parameter cannot be set to a value less than 2G.
- The DB_CACHE_SIZE initialization parameter cannot be set to a value greater than 2G.
- The DB_KEEP_CACHE_SIZE initialization parameter cannot be set to a value greater than 960M.
- The DB_KEEP_CACHE_SIZE initialization parameter cannot be set to a value less than 960M.

Answer:

The SGA_TARGET initialization parameter cannot be set to a value greater than 8G.

Explanation:

In this scenario, the SGA_TARGET initialization parameter cannot be set a value greater than 8G. When the SGA_MAX_SIZE parameter is specified, then the SGA_TARGET initialization parameter cannot be set to a value higher than that of the SGA_MAX_SIZE initialization parameter. Attempting to do so will result in the following errors:

```
ORA-02097: parameter cannot be modified because specified valueis invalid
ORA-00823: Specified value of sga_target greater than
sga_max_size
```

The option stating that the DB_CACHE_SIZE initialization parameter cannot be set to a value less than 2G is incorrect because you can manually decrease the size of the DB_CACHE_SIZE initialization parameter by using the ALTER SYSTEM statement.

The option stating that the DB_CACHE_SIZE initialization parameter cannot be set to a value greater than 2G is incorrect because you can manually set the DB_CACHE_SIZE initialization parameter to a value greater than 2G even if Automatic Shared Memory Management is enabled. You can use the ALTER SYSTEM statement to accomplish this.

The option stating that the DB_KEEP_CACHE_SIZE initialization parameter cannot be set to a value greater than 960M is incorrect because you can manually increase the value of the DB_KEEP_CACHE_SIZE initialization parameter even if the SGA_TARGET initialization parameter is set to a nonzero value. You can modify the setting of this parameter by using the ALTER SYSTEM statement.

The option stating that the DB_KEEP_CACHE_SIZE initialization parameter cannot be set to a value less than 960M is incorrect because you can manually set the DB_KEEP_CACHE_SIZE initialization parameter by using the ALTER SYSTEM statement even if the automatic tuning of memory structures feature is enabled.

Item: 10 (Ref:1Z0-043.12.3.2)

You have included the following parameter setting in your server parameter file:

```
PGA_AGGREGATE_TARGET = 800M
SORT_AREA_SIZE = 100M
HASH_AREA_SIZE = 100M
BITMAP_MERGE_AREA_SIZE = 100M
CREATE_BITMAP_AREA_SIZE = 100M
```

Which statement is true?

- All the *_AREA_SIZE parameters are ignored.
- The Automatic PGA Memory Management feature cannot be disabled.
- The total Program Global Area (PGA) memory cannot be manually increased above 800M.
- The total memory for the PGA can automatically exceed 800M using the Automatic PGA Memory Management feature.

Answer:

All the *_AREA_SIZE parameters are ignored.

Explanation:

In this scenario, all the *_AREA_SIZE parameters are ignored. When the WORKAREA_SIZE_POLICY initialization parameter is not included in the initialization parameter file, its value is set to the default value. The default value for the WORKAREA_SIZE_POLICY initialization parameter is AUTO, which specifies that the Automatic PGA Memory Management feature is enabled.

The option stating that the Automatic PGA Memory Management feature cannot be disabled is incorrect because changing the value of the PGA_AGGREGATE_TARGET initialization parameter to zero disables the Automatic PGA Memory Management feature.

The option stating that the total PGA memory cannot be cannot be manually increased above 800M is incorrect because you can dynamically change the value of the PGA_AGGREGATE_TARGET initialization parameter by using the ALTER SYSTEM statement.

The option stating that the PGA memory can automatically exceed 800M using the Automatic PGA Memory Management feature is incorrect. Oracle does not automatically exceed the maximum limit imposed by the PGA_AGGREGATE_TARGET initialization parameter even if this memory is not sufficient for performing a long-running query that involves a sort operation.

Item: 11 (Ref:1Z0-043.12.1.3)

You are enabling the Automatic Shared Memory Management feature in the Oracle Database 10*g* to ensure that the important memory structures of the System Global Area (SGA) are automatically adjusted depending on the database workload.

You are using Enterprise Manager 10*g* to enable this feature. You are currently on the **Administration** tab page.

Which two links should you click to go to the Memory Advisor page? (Choose two.)

- [ ] Advisor Central
- [ ] Global Attributes
- [ ] Resource Monitors
- [ ] Memory Parameters

- [ ] Database Usage Statistics
- [ ] All Initialization Parameters
- [ ] Automatic Workload Repository

Answer:

Advisor Central
Memory Parameters

Explanation:

You can click either the Advisor Central or the Memory Parameters links on the Administration tab page of the Enterprise Manager 10*g* to go to the Memory Advisor page.

Using the Enterprise Manager 10*g*, you can enable the Automatic Shared Memory Management feature in the Oracle Database 10*g* by navigating through the following steps:

1. Click the Administration tab.
2. Select Memory Parameters under the Instance heading.
3. Click the SGA tab.
4. Click the Enable button for Automatic Shared Memory Management, and then type the total SGA size in MB for Automatic Shared Memory Management.
5. Click the OK button to activate the change.

Alternatively, you can enable the Automatic Shared Memory Management feature by navigating through the following steps:

1. Click the Administration tab.
2. Select Advisor Central under the Related Links heading.
3. Click the Memory Advisor link.
4. Click the SGA tab.
5. Click the Enable button for Automatic Shared Memory Management, and then type the total SGA size in MB for Automatic Shared Memory Management.
6. Click the OK button to activate the change.

All the other options are incorrect because they will not take you to the Memory Advisor page.

Item: 12 (Ref:1Z0-043.12.1.2)

You recently added a third-party application to your database and do not have access to the SQL code of this application. Database users are complaining of performance-related issues, such as increased time required to complete a query. While investigating, you discover from the STATSPACK utility that some of the memory structures have low hit ratios. You plan to resize some of the memory structures by using the Memory Advisor.

For which memory structure will you fail to obtain optimal settings by using the Memory Advisor?

- java pool
- shared pool
- buffer cache
- program global area

Answer:

java pool

Explanation:

Using the Memory Advisor of the Oracle Enterprise Manager 10*g*, you cannot obtain advice on the optimal setting for the java pool. You can use the V$SGASTAT dynamic performance view to monitor and resize the java pool. For example, you can execute the following statement to obtain an optimal size for the java pool:

```
SQL> SELECT name, bytes FROM v$sgastat WHERE pool='java pool';

NAME                         BYTES
-------------------------- ----------
joxs heap                    233856
free memory                44626368
joxlod exec hp              5471424
```

From the output of the above statement, the value of free memory can be used to tune the size of the java pool. A higher value for free memory indicates that you probably oversized the java pool. A lower value indicates an under-configured java pool.

All the other options are incorrect because you can obtain the optimal settings for all the memory structures listed below by using the Memory Advisor:

- shared pool
- buffer cache
- program global area

The Memory Advisor helps you to tune the size of most of the memory components. However, this advisor can only be used when the automatic tuning of memory structures is disabled.

Item: 13 (Ref:1Z0-043.12.3.1)

You recently created a database and configured the SPFILE with the following parameter settings to ensure that Oracle automatically adjusts the memory for the Program Global Area (PGA):

```
SORT_AREA_SIZE = 150M
HASH_AREA_SIZE = 150M
BITMAP_MERGE_AREA_SIZE = 150M
CREATE_BITMAP_AREA_SIZE = 150M
WORKAREA_SIZE_POLICY = AUTO
```

You have not included the PGA_AGGREGATE_TARGET initialization parameter in the SPFILE and the System Global Area (SGA) is currently sized at 4G.

What is the total PGA memory allocated across all database server processes?

- 10M
- 400M
- 600M
- 800M

Answer:

800M

Explanation:

In this scenario, the total PGA memory allocated across all database server processes is 800M. When the PGA_AGGREGATE_TARGET initialization parameter is not specified in the initialization parameter file and the WORKAREA_SIZE_POLICY initialization parameter is set to AUTO, the value of the PGA_AGGREGATE_TARGET initialization parameter defaults to 10M or 20 percent of the size of the SGA, whichever is higher. The current size of the SGA is 4G. Twenty percent of the SGA size is 800M so the total PGA memory allocated across all database server processes will be 800M.

All the other options are incorrect.

Item: 14 (Ref:1Z0-043.12.2.1)

The SPFILE for the PROD database specifies the following initialization parameter values:

```
SGA_TARGET = 2G
DB_8K_CACHE_SIZE = 128M
```

You create a tablespace named HR with the non-standard block size of 8K. Four database users are running queries on a table in the HR tablespace. These users complain that the queries are taking longer than usual to complete. While investigating the reasons for this delay, you discover that the database encounters extensive cache misses on the database buffer cache with the block size of 8K.

You issue the following statement to increase the value of the DB_8K_CACHE_SIZE initialization parameter to 256M:

```
SQL>ALTER SYSTEM SET DB_8K_CACHE_SIZE=256M SCOPE = BOTH;
```

What is the result of this statement?

- The statement fails because you cannot set the memory components manually if the SGA_TARGET initialization parameter is set to a nonzero value.
- The statement fails because the DB_8K_CACHE_SIZE initialization parameter is not a dynamic parameter.
- The statement increases the value of the DB_8K_CACHE_SIZE initialization parameter to 256M and extracts an additional 128M of memory from the automatically sized memory components.
- The statement increases the value of the DB_8K_CACHE_SIZE initialization parameter to 256M and reallocates an additional 128M memory from the memory components that are not auto-tuned.

Answer:

The statement increases the value of the DB_8K_CACHE_SIZE initialization parameter to 256M and extracts an additional 128M of memory from the automatically sized memory components.

Explanation:

The statement increases the value of the DB_8K_CACHE_SIZE initialization parameter to 256M and extracts an additional 128M of memory from the automatically sized memory components.

To increase the size of a memory component that is not auto-tuned, extra memory is extracted from one or more automatically sized memory components. When decreasing the size of components that are not auto-tuned, the released memory is reallocated to the automatically sized memory components.

The option stating that the statement fails because you cannot set the memory components manually if the SGA_TARGET initialization parameter is set to a nonzero value is incorrect. You can modify the memory components that are not auto-tuned even if the SGA_TARGET initialization parameter is set to a nonzero value.

The option stating that the statement fails because the DB_8K_CACHE_SIZE initialization parameter is not a dynamic parameter is incorrect. The DB_8K_CACHE_SIZE initialization parameter is a dynamic parameter that can be modified by using the ALTER SYSTEM statement. The modification of this parameter is immediately effective without restarting the database instance.

The option stating that the statement increases the value of the DB_8K_CACHE_SIZE initialization parameter to 256M and reallocates an additional 128M of memory from the non-auto-tuned memory components is incorrect. Increasing the size of the non-auto-tuned memory components reallocates the additional memory from the automatically sized memory components. The additional memory is never extracted from the memory components that are non-auto-tuned.